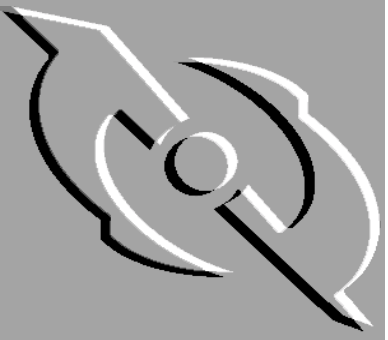

McAfee VirusScan
Logiciel antivirus

Guide d'utilisateur

Sommaire

Préface

Que s'est-il passé ?

S'il vous est déjà arrivé de perdre des fichiers importants stockés sur votre disque dur, ou d'observer avec consternation votre ordinateur s'arrêter pour faire apparaître sur son écran le message puéril d'un plaisantin, ou si vous vous êtes retrouvé dans la situation de devoir vous excuser pour des messages électroniques injurieux que vous n'avez jamais envoyés, nous n'avons pas besoin de vous expliquer comment des virus informatiques et d'autres programmes nuisibles peuvent perturber votre productivité. Si vous n'avez jamais subi une « infection » par un virus vous pouvez vous estimer heureux. Toutefois, étant donné qu'il circule plus de 50,000 virus capables d'attaquer les systèmes informatiques travaillant sous Windows et DOS, ce n'est vraiment plus qu'une question de temps avant que vous soyez victime d'une infection à votre tour.

La bonne nouvelle est que parmi ces milliers de virus en circulation, on n'en trouve qu'un nombre relativement limité capables de causer de réels dommages à vos données. En fait, le terme « virus informatique » définit un large éventail de programmes qui n'ont qu'un point commun : ils « s'auto-reproduisent » en s'attachant à des logiciels hôtes ou à des secteurs de votre disque, généralement à votre insu. La plupart des virus ne causent que des problèmes mineurs, allant du simplement gênant au franchement insignifiant. Souvent, la première conséquence d'une infection par un virus se mesure par les dépenses de temps et d'énergie consacrées à rechercher la source de l'infection et éradiquer toutes ses traces.

Pourquoi s'inquiéter ?

Alors, pourquoi s'inquiéter des infections causées par les virus, si la majorité des attaques ne sont que peu nuisibles ? Le problème est double : D'abord, même si relativement peu de virus ont des effets destructeurs, cela ne dit rien de l'étendue des virus nuisibles. Dans de nombreux cas, les virus les plus nocifs sont les plus difficiles à détecter : le concepteur de virus qui cherche à causer du tort prendra des mesures supplémentaires pour éviter d'être découvert. Deuxièmement, même les virus les plus « bénins » peuvent interférer avec le fonctionnement normal de votre ordinateur et entraîner un comportement imprévisible dans d'autres logiciels. Certains virus contiennent des bogues qui sont des codes à l'écriture élémentaire, ou d'autres problèmes suffisamment sérieux pour causer des incidents lorsqu'ils sont exécutés.

Dans d'autres cas, un logiciel légitime connaît des difficultés d'exécution lorsqu'un virus a, intentionnellement ou non, modifié les paramètres du système ou d'autres aspects de l'environnement informatique. Rechercher l'origine de l'infection causant des arrêts ou des pannes du système peut entraîner une dépense de temps et d'argent que vous ne consacrez pas à des activités plus productives.

Au-delà de ces problèmes, il y a la question de la perception : une fois qu'il est infecté, votre ordinateur peut infecter à son tour d'autres ordinateurs. Si vous échangez des données avec vos collègues ou clients de façon régulière, vous pouvez à votre insu transmettre un virus qui pourrait être plus nuisible à votre réputation ou à vos transactions qu'à votre propre ordinateur.

La menace que représentent les virus et d'autres logiciels nuisibles est réelle et s'aggrave. L'association internationale pour la sécurité informatique a estimé à plus de $10 milliards de dollars les dépenses en termes de temps et de perte de productivité consacrées dans le monde entier, uniquement à détecter et à nettoyer des virus ; Ce chiffre n'inclut pas les coûts engendrés par la perte et le rétablissement des données à la suite d'attaques ayant entraîné leur destruction.

D'où viennent les virus ?

Après avoir éliminé un virus qui s'était attaqué à vous-même ou à l'un de vos collègues, ou après avoir entendu parler de nouvelles formes de logiciels nuisibles rencontrés dans des programmes d'usage courant, vous vous êtes sans doute posé certaines questions sur la manière dont nous, les utilisateurs d'ordinateurs, en sommes arrivés là. D'où viennent les virus et les autres programmes nuisibles ? Qui les écrit ? Pourquoi ceux qui les écrivent cherchent-ils à interrompre le déroulement des opérations, détruire des données ou causer aux personnes des dépenses de temps et d'argent afin de les éradiquer ? Qu'est-ce qui peut les arrêter ?

Pourquoi moi ?

Il vous sera sans doute de maigre consolation de savoir que le programmeur qui a conçu le virus qui a effacé la table d'attribution des fichiers de votre disque dur ne vous visait pas précisément vous ou votre ordinateur. Il ne vous sera pas plus réconfortant d'apprendre que le problème des virus ne sera sans doute jamais réglé. Cependant, connaître un peu l'histoire des virus informatiques et la manière dont ils fonctionnent peut vous aider à mieux vous en protéger.

Préhistoire des virus

Des historiens ont identifié un certain nombre de programmes qui présentent des caractéristiques qui sont aujourd'hui associées à un logiciel de virus. Le chercheur et enseignant canadien Robert M. Slade a remonté la lignée des virus jusqu'à des programmes utilitaires spécialisés qui servaient à récupérer de l'espace disque occupé par des fichiers non utilisés et à exécuter d'autres tâches utiles aux premiers âges des réseaux d'ordinateurs. Slade rapporte que des chercheurs de Xerox Corporation ont donné à ces programmes le nom de « vers », après avoir remarqué des « trous » sur les impressions papier des vidages mémoires, comme si elles avaient été dévorées par des vers. Le terme a survécu jusqu'à aujourd'hui pour désigner des programmes capables de se copier eux-mêmes, mais qui n'utilisent pas nécessairement le logiciel qui les abrite dans le processus.

Une tradition universitaire très répandue consistant à faire des canulars informatiques a très certainement contribué à l'abandon des programmes utilitaires pour des utilisations plus pernicieuses des techniques de programmation que l'on retrouve dans les logiciels de type vers. Des étudiants en informatique, souvent pour tester leurs talents de programmeurs, concevaient des programmes vers dévoyés et les libéraient pour qu'ils « combattent » entre eux dans une compétition visant à connaître l'inventeur du programme qui avait « survécu » après avoir détruit ses rivaux. Ces mêmes étudiants utilisaient également les programmes vers pour faire des farces à leurs collègues qui ne se doutaient de rien.

Certains de ces étudiants ont bientôt découvert qu'ils pouvaient utiliser certains éléments du système d'exploitation de l'ordinateur hôte pour se procurer, sans autorisation, l'accès aux ressources qu'il contenait. D'autres ont profité de la relative méconnaissance informatique de certains utilisateurs pour substituer leurs propres programmes, conçus pour servir leurs propres desseins, aux utilitaires ordinaires ou inoffensifs. Ces utilisateurs peu chevronnés lançaient ce qu'ils croyaient être leur logiciel habituel pour se rendre compte alors que leurs fichiers avaient été effacés, le mot de passe de leur compte dérobé ou d'autres mauvaises surprises encore. De tels programmes de type « cheval de Troie », surnommés ainsi pour leur ressemblance métaphorique au cadeau fait par les Grecs à la cité de Troie, continuent aujourd'hui à faire peser une menace considérable sur les utilisateurs d'ordinateur.

Les virus et la révolution des PC

Ce que nous considérons aujourd'hui comme un authentique virus informatique est apparu, selon Robert Slade, peu de temps après que les premiers ordinateurs personnels ont accédé au marché de masse au début des années 80. D'autres chercheurs datent l'avènement des programmes de virus en 1986, avec l'apparition du virus « Brain ». Quoi qu'il en soit, le lien entre la menace des virus et l'ordinateur personnel n'est pas un hasard.

La vente en masse des ordinateurs a entraîné la prolifération des virus vers d'autres hôtes beaucoup plus nombreux que par le passé, à l'époque où des systèmes de macro-ordinateurs, relativement peu nombreux et étroitement surveillés, dominaient le monde informatique depuis leurs bastions situés dans les grandes entreprises et les universités. Parallèlement, les utilisateurs individuels qui achetaient les PC n'avaient pas un grand besoin des mesures de sécurité sophistiquées pour protéger leurs données sensibles dans ces environnements. Le facteur le plus déterminant vient du fait que les concepteurs des virus ont trouvé les technologies des PC faciles à exploiter pour servir leurs propres desseins.

Les virus de la zone système

Par exemple, les premiers PC « amorçaient » ou chargeaient leurs systèmes d'exploitation à partir de disquettes. Les créateurs du virus Brain ont découvert qu'ils pouvaient substituer leur propre programme au code exécutable présent dans la zone système de chaque disquette formatée sous MS-DOS de Microsoft, qu'elle contienne ou non des fichiers système. Par ce biais, les utilisateurs chargeaient le virus dans la mémoire de l'ordinateur à chaque démarrage quelle que soit la disquette formatée introduite dans le lecteur. Une fois dans la mémoire, un virus peut se copier lui-même vers les zones système d'autres disquettes ou disques durs. Ceux qui ont, sans le vouloir, chargé le virus Brain à partir d'une disquette infectée se sont retrouvés en train de lire une « message publicitaire » de substitution pour une entreprise de conseil en informatique pakistanaise.

Par cette publicité, Brain a marqué le coup d'envoi d'un autre trait caractéristique des virus modernes : la charge utile. Le charge utile est un virus farceur ou nuisible qui, s'il est déclenché, provoque des effets qui vont des messages ennuyeux à la destruction des données. C'est la manifestation virale la plus marquante : de nombreux auteurs de virus conçoivent aujourd'hui leurs virus dans le but spécifique de délivrer leur charge utile au plus grand nombre possible d'ordinateurs.

Pendant une certaine période, les descendants sophistiqués de ce premier virus de la zone système constituaient la menace la plus sérieuse pour les utilisateurs d'ordinateurs. Des variantes de virus de la zone système peuvent aussi infecter la partition d'amorçage (MBR), qui stocke les informations du secteur de partition dont votre ordinateur a besoin pour localiser chacune des parties de votre disque dur et de la zone système elle-même.

Concrètement, presque toutes les étapes du processus d'amorçage, de la lecture du MBR au chargement du système d'exploitation, sont vulnérables au sabotage viral. Certains des virus les plus tenaces et les plus destructeurs possèdent encore dans l'arsenal de leurs ruses la capacité d'infecter de la zone système et le MBR de votre ordinateur. Entre autres avantages, le chargement au moment du temps d'amorçage peut offrir au virus l'occasion d'exécuter sa tâche avant que votre logiciel antivirus n'ait eu le temps de démarrer. De nombreux produits antivirus McAfee anticipent en vous permettant de créer une disquette d'urgence que vous pouvez utiliser pour amorcer votre ordinateur et supprimer la contamination.

Cependant, les virus de la zone système et du MBR ont un point faible particulier : ils se propagent par l'intermédiaire de disquettes ou d'autres supports amovibles, et circulent parfaitement dissimulés dans cet espace disque réduit. Avec la diminution des échanges de disquettes entre les utilisateurs et avec l'émergence de nouveaux moyens de distribution des logiciels, tels que les CD-ROM et les téléchargements depuis Internet, d'autres types de virus ont éclipsé la menace émanant de la zone système. Mais l'évolution ne s'arrête pas là ; nombre de virus de dernière génération incorporent régulièrement des fonctions qui infectent la zone système ou le MBR de votre disque dur, même s'ils utilisent d'autres méthodes comme principal moyen de transmission.

Ces mêmes virus ont également bénéficié de plusieurs générations d'évolution et incorporent aujourd'hui des techniques d'infection et de dissimulation beaucoup plus sophistiquées. Leur détection devient ainsi plus difficile, même s'ils se cachent dans des endroits plus ou moins prévisibles.

Virus infectant les fichiers

À peu près à la même époque où les auteurs du virus Brain découvraient des points faibles dans de la zone système de DOS, d'autres concepteurs de virus ont trouvé comment utiliser d'autres logiciels pour les aider à reproduire leurs créations. Un premier exemple de ce type de virus est apparu dans les ordinateurs de l'université de Lehigh en Pennsylvanie. Le virus a infecté une partie de l'interpréteur de commande du DOS, COMMAND.COM, qu'il a utilisé pour se charger dans la mémoire. Une fois en place, il se propageait vers d'autres fichiers COMMAND.COM sains chaque fois qu'un utilisateur exécutait n'importe quelle commande DOS standard qui impliquait l'accès au disque. Cela limitait sa propagation aux disquettes qui contenaient, normalement, un système d'exploitation complet.

Plus tard, des virus ont rapidement surmonté cette limitation, parfois par le biais d'une programmation assez rusée. Les concepteurs de virus pouvaient notamment leur commander d'ajouter leur code au début d'un fichier exécutable de manière à ce que, lorsque les utilisateurs démarraient un programme, le code du virus s'exécutait immédiatement puis redonnait le contrôle au logiciel légitime, qui fonctionnait comme si de rien n'était. Une fois activé, le virus « crochète » ou « piège » les ordres donnés par le logiciel légitime au système d'exploitation et leur substitue ses propres réponses.

Des virus particulièrement intelligents sont capables de faire échec à des opérations visant à les éradiquer de la mémoire en piégeant la combinaison des touches du clavier CTRL+ALT+SUPPR qui commande une réinitialisation à chaud puis en émulant un redémarrage. Parfois le seul signe extérieur indiquant que quelque chose ne va pas sur votre système, c'est-à-dire avant l'explosion d'une charge utile, pourrait être une légère modification de la taille du fichier du logiciel légitime infecté.

Virus furtifs, mutants, cryptés et polymorphes

En dépit de leur discrétion, les changements dans la taille des fichiers et les autres signes imperceptibles d'une infection virale mettent suffisamment la puce à l'oreille à la plupart des logiciels antivirus pour qu'ils localisent et suppriment le code offensif. Ainsi, l'un des principaux défis que doit relever le concepteur du virus est de trouver des méthodes pour dissimuler son œuvre. Les premiers camouflages combinaient des programmes innovateurs avec d'autres systèmes beaucoup moins transparents. Par exemple, le virus Brain redirigeait les demandes de consultation de la zone système d'un disque de l'emplacement réel du secteur contaminé vers le nouvel emplacement des fichiers d'amorçage que le virus avait déplacés. Ce caractère « furtif » permettait à ce virus et à d'autres d'échapper aux techniques de recherche conventionnelles.

En raison du fait que les virus devaient éviter de réinfecter continuellement les systèmes hôtes—sous peine de faire rapidement gonfler la taille d'un fichier infecté jusqu'à ce qu'il atteigne des proportions facilement détectables ou de consommer suffisamment les ressources du système pour permettre une localisation rapide du coupable—leurs auteurs devaient aussi leur indiquer de ne pas toucher à certains fichiers. Ils ont réglé ce problème en faisant écrire une séquence d'octets caractéristique ou, dans les systèmes d'exploitation Windows 32 bits, en créant une clé de registre particulière qui marquait les fichiers infectés avec l'équivalent logiciel d'une pancarte « ne pas déranger ». Bien que cela ait retardé la détection des virus, cela a ouvert la voie à l'utilisation par les logiciels antivirus de la séquence «ne pas déranger» elle-même, ainsi que d'autres signes caractéristiques écrits par le virus dans les fichiers infectés, pour identifier sa « signature codée ». La plupart des fournisseurs de logiciels antivirus compilent et mettent à jour régulièrement une base de données de « définitions » de virus utilisée par leurs produits pour reconnaître les signatures codées dans les fichiers qu'ils analysent.

La réponse des concepteurs de virus a été de trouver des méthodes pour dissimuler les signatures codées. Certains virus « mutaient » ou transformaient leurs signatures codées à chaque nouvelle infection. D'autres se cryptaient eux-mêmes et, par conséquent, cryptaient leurs signatures codées, ne laissant que quelques octets pour servir de clé de décryptage. Les nouveaux virus les plus sophistiqués étaient à la fois des virus furtifs, mutants et cryptés apparaissant sous une variété de nouvelles formes qui les rendait pratiquement indécelables. La recherche de ces virus « polymorphes » a obligé les ingénieurs en informatique à concevoir des techniques de programmation très élaborées dans le domaine des logiciels antivirus.

Virus de macro

Avant 1995 environ, la guerre des virus était parvenue à une sorte d'équilibre. De nouveaux virus apparaissaient sans cesse, favorisés en partie par la possibilité de se procurer des virus préfabriqués en « kit » qui permettaient même à des individus qui n'étaient pas des programmeurs de créer un nouveau virus en un rien de temps. Cependant, la plupart des logiciels antivirus pouvaient être facilement mis à jour pour détecter et traiter les nouvelles formes de virus, qui étaient pour la plupart des modèles bien connus ayant subi des modifications mineures.

Mais 1995 marque l'émergence du virus Concept, qui a contribué à un nouveau et surprenant revirement de situation dans l'histoire des virus. Avant Concept, la majorité des chercheurs de virus considéraient les fichiers de données (textes, tableurs et dessins) crées par votre logiciel, comme étant immunisés contre les infections. Les virus n'étaient après tout que des programmes et, en tant que tels, ils avaient besoin d'être activés comme le sont les logiciels exécutables pour causer leurs dommages. Les fichiers de données, quant à eux, se contentaient de stocker les informations que vous chargiez en travaillant avec votre logiciel.

Cette distinction est devenue floue lorsque Microsoft a commencé à ajouter des outils macro à Word et Excel, les deux logiciels vedettes de son ensemble Office. En utilisant la version épurée du langage Visual Basic inclus dans l'ensemble Office, les utilisateurs étaient en mesure de créer des modèles de document capables de se mettre automatiquement au format et d'ajouter de nouvelles fonctionnalités aux documents créés avec Word et Excel. D'autres fournisseurs appliquèrent la même innovation à leurs produits, soit en utilisant une variation du même langage macro Microsoft, soit en incorporant un langage propre. Les concepteurs de virus, à leur tour, saisirent l'opportunité que cela représentait pour dissimuler et propager des virus dans des documents que vous, l'utilisateur, avez crées vous-même.

La popularité croissante d'Internet et des logiciels e-mail qui permettaient aux utilisateurs de joindre des fichiers aux messages a renforcé la propagation très rapide et très étendue des virus de macro. En l'espace d'un an, les virus de macro devenaient la menace virale la plus forte jamais connue auparavant.

À la frontière

Alors même que les virus se faisaient de plus en plus sophistiqués et continuaient de menacer l'intégrité des systèmes informatiques dont nous avions tous fini par dépendre, d'autres dangers commencèrent à émerger d'où on ne les attendait pas : le World Wide Web. D'abord outil de stockage pour les rapports de recherche et les traités universitaires, le Web s'est transformé en ce qui est peut-être l'instrument le plus souple et le plus adaptable jamais inventé pour la communication et le commerce.

De par l'immense étendue de son potentiel, le Web a focalisé l'attention et les énergies créatrices de pratiquement toutes les sociétés d'informatique de l'industrie.

La concentration des technologies qui a résulté de ce rythme effréné d'inventions a procuré aux concepteurs de sites Web des outils qu'ils peuvent utiliser pour collecter et montrer des informations par des moyens dont ils n'avaient jamais disposé auparavant. Nous avons assisté à la naissance rapide de sites Web capables de transmettre et de recevoir du courrier électronique, de mettre en forme et d'exécuter des requêtes vers des bases de données par l'emploi de moteurs de recherche perfectionnés, de transmettre et de recevoir des sons et des images vidéo, et de distribuer des données et des ressources en multimédia à un public mondial.

Une grande partie de la technologie qui a autorisé de tels systèmes consistait en de petits programmes faciles à télécharger capables d'interagir avec votre navigateur et, parfois, avec d'autres logiciels présents sur votre disque dur. Ce même chemin a servi de point d'entrée dans votre système informatique à d'autres programmes (moins inoffensifs) qu'ils utilisent à leurs propres fins.

objets Java, ActiveX et cryptés

Ces programmes, qu'ils soient bénéfiques ou nuisibles, se présentent sous des formes variées. Certains sont des applications miniatures à but spécialisé aussi nommés « applets » écrits en Java, une langage de programmation conçu par Sun Microsystems. D'autres ont créé, avec ActiveX, une technologie Microsoft que les programmeurs peuvent utiliser aux mêmes fins.

Java et ActiveX emploient très couramment des modules de logiciel pré-écrits, ou « objets », que les programmeurs peuvent concevoir eux-mêmes, ou aller chercher dans les ressources existantes et qu'ils transforment en plug-ins, applets, pilotes de périphérique et en d'autres logiciels nécessaires au fonctionnement du Web. Les objets Java sont appelés « classes » et les objets ActiveX sont appelés « contrôles ». Ce qui les différencie principalement tient dans la manière dont ils fonctionnent au sein du système qui les abrite. Les applets Java fonctionnent à l'intérieur d'une « machine virtuelle » conçue spécialement pour interpréter la programmation Java et la traduire en acte sur la machine hôte, alors que les contrôles ActiveX fonctionnent comme des programmes natifs de Windows qui relient et transfèrent les données entre les logiciels Windows existants.

L'écrasante majorité de ces objets sont des éléments utiles, voire nécessaires, à tout site Web interactif. Cependant, malgré les meilleurs efforts déployés par les ingénieurs de Sun et de Microsoft afin de concevoir des mesures de sécurité les protégeant de l'intérieur, des programmeurs bien décidés peuvent utiliser les outils de Java et d'ActiveX pour implanter des objets nuisibles sur les sites Web, où ils peuvent restés tapis en attendant que des visiteurs, à leur insu, leur ouvrent l'accès aux systèmes informatiques vulnérables.

Contrairement aux virus, les objets nocifs Java et ActiveX ne cherchent généralement pas à se reproduire. Le Web leur fournit de nombreuses occasions de se propager vers des systèmes informatiques cible, d'autant que leur taille réduite et leur nature inoffensive leur permettent d'échapper facilement aux détections. En fait, à moins de préciser à votre navigateur de les bloquer, les objets Java et ActiveX se téléchargent automatiquement à chaque fois que vous visitez un site Web qui les accueille.

Quant aux objets hostiles, ils ne sont là que pour délivrer ce qui se rapproche d'une charge utile virale. Les programmeurs ont conçu des objets qui peuvent, notamment, lire les données contenues sur votre disque dur et les renvoyer vers le site Web que vous avez visité, « pirater » votre compte e-mail et transmettre vers l'extérieur des messages injurieux en utilisant votre nom, ou surveiller les données échangées entre les autres ordinateurs et le vôtre.

Des agent encore plus puissants ont commencé à apparaître dans les applications qui s'exécutent directement à partir des sites Web que vous visitez. JavaScript, un langage de script qui porte un nom similaire à celui du langage Java, mais avec lequel il n'a aucune relation, est apparu pour la première fois dans Netscape Navigator, avec la mise en place de la version 3.2 de la norme HTML (Hyper Text Markup Language). Depuis son introduction, JavaScript a développé considérablement ses capacités et sa puissance, de même que les hôtes des autres technologies de script qui l'ont suivi, tels que Microsoft VBScript, Active Server Pages, Allaire Cold Fusion, entre autres.

Ces technologies permettent à présent aux concepteurs de logiciels de créer des applications complètes qui s'exécutent sur des serveurs Web, interagissent avec des bases de données et autres sources de données et gèrent directement des fonctionnalités dans le navigateur Web et dans les logiciels clients de messagerie exécutés sur votre ordinateur.

À l'instar des objets Java et ActiveX, d'importantes mesures de sécurité ont été mises en place pour éviter les actions nuisibles, mais les concepteurs de virus et les pirates de la sécurité ont trouvé les moyens de les contourner. Dans la mesure où les avantages que représentent ces innovations pour le Web l'emportent généralement sur les risques, la plupart des utilisateurs préfèrent favoriser les échanges que fuir les nouvelles technologies.

Quelle sera leur prochaine cible ?

Des logiciels nuisibles se sont même introduits dans des zones dont on a d'abord pensé qu'elles étaient complètement inviolables. Les utilisateurs du serveur client mIRC Internet Relay Chat, par exemple, ont rapporté avoir rencontré des virus construits à partir du langage de script du mIRC. Le client de conversation envoie des virus Script sous forme de texte clair, ce qui d'ordinaire les empêche d'infecter les systèmes. Cependant, des versions plus anciennes du logiciel client mIRC interprétaient les instructions codées contenues dans le script et exécutaient des actions non voulues sur l'ordinateur destinataire.

Les vendeurs se sont empressés de désactiver cette capacité dans les versions mises à jour du logiciel, mais l'incident du mIRC illustre la règle générale selon laquelle là où il y a un moyen de profiter d'une brèche dans le système de protection d'un logiciel, quelqu'un trouvera ce moyen et l'utilisera. Vers la fin de l'année 1999, un autre concepteur de virus confirma à nouveau cette règle avec un virus très évolué, appelé VBS/Bubbleboy, qui s'exécutait directement à partir du client e-mail Microsoft Outlook en violant son support VBScript intégré. Ce virus traversa la frontière qui séparait les messages électroniques en texte clair et les pièces jointes qu'ils comportaient, susceptibles d'être infectées. Avec VBS/Bubbleboy, vous n'aviez même plus besoin d'ouvrir le message pour infecter votre système, il suffisait de l'afficher dans la fenêtre de prévisualisation de Outlook.

Comment vous protéger

Le logiciel antivirus de McAfee vous procure déjà un rempart solide contre les infections et les dégâts causés à vos données, mais il ne constitue qu'un volet des mesures de sécurité indispensables à votre protection. Un logiciel antivirus n'est jamais aussi efficace que lorsque qu'il est actualisé. De 200 à 300 nouveaux virus ou des variantes de virus apparaissent tous les mois, c'est pourquoi les fichiers de définition de virus (.DAT) permettant au logiciel McAfee de détecter et de supprimer les virus peuvent être très vite dépassés. Si vous n'avez procédé à aucune mise à jour des fichiers qui vous ont été fournis à l'origine avec le logiciel, vous risquez une infection provoquée par des virus encore inconnus à ce jour. C'est pourquoi McAfee a rassemblé les chercheurs les plus expérimentées dans la recherche antivirus au sein du plus grand groupe de recherche, AVERT (Anti-Virus Emergency Response Team)*. Cela signifie que les fichiers dont vous avez besoin pour combattre les nouveaux virus sont disponibles de suite, voire avant l'infection.

La plupart des mesures de sécurité vont de soi : la vérification des disquettes que vous recevez de sources non identifiées ou peu fiables, soit au moyen d'un logiciel antivirus, soit au moyen d'un instrument de vérification, est toujours une bonne idée. Les programmeurs nuisibles sont même allés jusqu'à imiter les programmes sur lesquels vous vous reposez pour assurer la sécurité de votre ordinateur, en donnant une apparence familière à un logiciel dont l'objectif n'a rien d'amical. Cependant, ni McAfee ni aucun autre logiciel antivirus ne peut détecter une infection lorsque quelqu'un remplace l'un de vos utilitaires contributifs ou commerciaux favoris par un cheval de Troie ou un autre programme nuisible non encore identifié ; c'est-à-dire, pas avant que cela n'arrive.

L'accès au Web et à Internet engendre ses propres risques. Le logiciel antivirus VirusScan* vous donne la capacité de bloquer les sites Web dangereux afin que les utilisateurs ne puissent pas télécharger, par inadvertance, un logiciel nuisible à partir d'une source à risques identifiée ; il piège également les objets hostiles qui ont malgré tout été téléchargés. Cependant, avoir à votre disposition un pare-feu au niveau supérieur pour protéger votre réseau et mettre en œuvre d'autres mesures garantissant sa sécurité sont une nécessité lorsque des attaquants sans scrupules peuvent pénétrer votre réseau depuis pratiquement tous les points de la planète, que ce soit pour dérober des données sensibles ou implanter des codes nuisibles. Vous devez aussi vous assurer que votre réseau n'est pas accessible aux utilisateurs non autorisés, et que vous possédez un programme de formation adéquat installé pour instruire et renforcer les normes de sécurité. Pour connaître l'origine, le comportement et d'autres caractéristiques d'un virus particulier, consultez la bibliothèque d'information sur les virus disponible sur le site Web du groupe AVERT.

McAfee propose également deux ensembles de logiciels puissants, Active Virus Defense* (AVD) et Total Virus Defense (TVD), les solutions antivirus les plus complètes à ce jour. Des entreprises associées, faisant partie de la famille Network Associates, fournissent d'autres technologies permettant de protéger aussi votre réseau, notamment la ligne de produits PGP Security CyberCop et l'ensemble de produits de contrôle de réseaux Sniffer Technologies. Contactez votre représentant Network Associates ou visitez le site Web de Network Associates afin de savoir comment bénéficier de toute la puissance offerte par ces solutions de sécurité.

Comment contacter McAfee et Network Associates

Service clientèle

Le 1er décembre 1997, McAfee Associates a fusionné avec Network General Corporation, Pretty Good Privacy, Inc. et Helix Software, Inc. pour créer Network Associates, Inc. Cette dernière a à son tour acheté Dr Solomon's Software, Trusted Information Systems, Magic Solutions et CyberMedia, Inc.

En janvier 2000, suite à une réorganisation de l'entreprise, quatre unités commerciales indépendantes ont été créées, chacune chargée de la gestion d'une ligne de produits spécifique. Ces unités commerciales sont les suivantes :

- **Magic Solutions**. Cette unité fournit la ligne de produits de bureau Total Service et les produits associés
- **McAfee**. Cette unité fournit l'ensemble de produits Active Virus Defense et les solutions logicielles antivirus associées aux entreprises et aux clients individuels.
- **PGP Security**. Cette unité fournit les meilleures solutions de cryptage et de sécurité disponibles à ce jour, notamment la ligne de produits de cryptage et de sécurité de données PGP, la ligne de produits pare-feu Gauntlet, la ligne de matériels E-ppliance de WebShield et l'ensemble de produits de contrôle et d'analyse CyberCop.
- **Sniffer Technologies**. Cette unité fournit les utilitaires d'analyse, de rapport et de contrôle de réseaux Sniffer, leaders du marché, ainsi que les logiciels associés.

Network Associates assure la commercialisation et le support technique des lignes de produits de chacune des nouvelles unités commerciales indépendantes. Vous pouvez adresser vos questions, commentaires ou demandes relatives au logiciel que vous avez acheté, à votre inscription ou toute autre question similaire au service clientèle de Network Associates, à l'adresse suivante :

Service clientèle de Network Associates.
Network Associates International
Gatwickstraat 25
1043 GL Amsterdam Pays-Bas

Le service est ouvert du lundi au vendredi, de 08 heures « à 18 heures » (heure du centre des États-Unis)

Les clients disposant d'une licence d'entreprise peuvent nous contacter :

Par téléphone : 00 31 20 586 6100

Par fax : +31 (0) 20 586 61 01 (24 heures sur 24, télécopieur Group III)

Par e-mail : services_corporate_division@nai.com

Par le Web : http://www.nai.com

Les clients disposant d'une licence individuelle peuvent nous contacter :

Par téléphone : 00 31 20 586 6100

Par fax : +31 (0) 20 586 61 01 (24 heures sur 24, télécopieur Group III)

Par e-mail : cust_care@nai.com

Par le Web : http://www.mcafee.com/

Support technique

McAfee et Network Associates ont toujours mis un point d'honneur à satisfaire leurs clients. Ces entreprises ont continué cette tradition en consentant des investissements considérables en temps et en efforts pour faire de leurs sites Web des sources précieuses d'informations et de réponses aux questions des utilisateurs. McAfee vous encourage à visiter son site Web sur lequel vous trouverez les réponses aux questions les plus courantes, les mises à jour des logiciels McAfee et Network Associates et les dernières informations concernant les virus..

World Wide Web	http://www.nai.com/asp_set/services/technical_support/tech_intro.asp

Si vous ne trouvez pas ce que vous cherchez ou si vous n'avez pas accès au Web, consultez l'un de nos services d'information automatisés ou électroniques :

Internet	techsupport@mcafee.com
CompuServe	GO NAI
America Online	Mot clé MCAFEE

Si les services automatisés ne vous fournissent pas les réponses dont vous avez besoin, contactez Network Associates à l'un des numéros suivants du lundi au vendredi entre 8 h 00 et 18 h 00. pour découvrir les plans de support technique proposés par Network Associates.

Pour les clients détenteurs d'une licence d'entreprise :

Téléphone	00 31 20 586 6100
Fax	+31 (0) 20 586 61 01

Pour les clients détenteurs d'une licence individuelle :

Téléphone	00 31 20 586 6100
Fax	+31 (0) 20 586 61 01

Ce guide inclut un résumé des plans PrimeSupport disponibles pour les clients McAfee. Pour en savoir plus sur les plans, reportez-vous à l Annexe B, « Network Associates Support technique ».

Afin de fournir rapidement et efficacement les réponses dont vous avez besoin, le personnel du support technique de Network Associates a besoin de certaines informations relatives à votre ordinateur et à votre logiciel. Veuillez inclure les informations suivantes dans votre courrier :

- Nom et numéro de version du produit
- Marque et modèle de l'ordinateur
- Matériel ou périphériques connectés à l'ordinateur
- Type et numéro de version du système d'exploitation
- Type et numéro de version du réseau, le cas échéant
- Contenu de vos fichiers AUTOEXEC.BAT, CONFIG.SYS et du script de connexion
- Étapes spécifiques permettant de reproduire le problème

Aide au téléchargement

Pour obtenir l'aide à la navigation ou au téléchargement de fichiers à partir du site Web ou FTP de Network Associates ou de McAfee, appelez :

Entreprises	(801) 492-2650
Particuliers	(801) 492-2600

Formation de Network Associates

Pour obtenir des informations sur les programmes de formation sur site pour les produits Network Associates, contactez notre service clientèle au : 00800-122-55-624.

Commentaires

McAfee apprécie vos commentaires et se réserve le droit d'utiliser toute information fournie par vous de toutes les manières jugées appropriées, sans encourir d'obligations à votre égard. Veuillez adresser vos commentaires sur la documentation qui accompagne un produit antivirus McAfee à : Network Associates International B.V., Gatwickstraat 25, 1043 GL Amsterdam, Pays-Bas. Vous pouvez également envoyer vos commentaires par télécopie au (31) 20 586 6101 ou par courrier électronique à tvd_documentation@nai.com.

Signalement de nouveaux virus à incorporer dans les mises à jour de fichiers de données antivirus

Les logiciels antivirus McAfee utilisent des algorithmes de détection fondés, entre autres, sur l'analyse heuristique avancée capable de déceler les nouveaux virus émergeants. Ils offrent donc les meilleurs taux de détection et d'éradication des virus. Il peut toutefois arriver qu'un type de virus entièrement nouveau apparaisse sur votre système, et échappe à la détection de VirusScan.

Pour aider les chercheurs de McAfee à tenir leur engagement de fourniture d'outils efficaces de pointe pour la protection des systèmes, veuillez leur signaler tout nouveau contrôle ActiveX, classe Java, site Web dangereux ou virus que le logiciel ne détecte pas. Il est à noter que McAfee se réserve le droit d'utiliser toute information fournie par vous de toutes les manières jugées appropriées, sans encourir d'obligation à votre égard. Envoyez vos questions ou échantillons de virus à l'adresse :

virus_research@nai.com	Utilisez cette adresse pour envoyer des questions ou des échantillons de virus à nos bureaux d'Amérique du Nord et du Sud
vsample@nai.com	Utilisez cette adresse pour envoyer vos questions ou vos échantillons de virus détectés par le logiciel Anti-Virus Toolkit* de Dr Solomon à nos bureaux du Royaume-Uni

Pour signaler les virus au bureau de recherche européen de McAfee, utilisez l'adresse e-mail suivante :

virus_research_europe@nai.com	Utilisez cette adresse pour envoyer des questions ou des échantillons de virus à nos bureaux en Europe de l'Ouest
virus_research_de@nai.com	Utilisez cette adresse pour envoyer des questions ou des échantillons de virus groupés avec le logiciel antivirus du Dr Solomon à nos bureaux en Allemagne

Pour signaler les virus au bureau de recherche de McAfee au Japon et dans la zone Asie du Pacifique, utilisez l'une des adresses suivantes :

virus_research_japan@nai.com	Utilisez cette adresse pour envoyer des questions ou des échantillons de virus à nos bureaux au Japon et dans l'est de l'Asie.
virus_research_apac@nai.com	Utilisez cette adresse pour envoyer vos questions ou vos échantillons de virus à nos bureaux d'Australie et d'Asie du Sud-Est

Informations sur les contacts internationaux

Pour contacter Network Associates en dehors des États-Unis, utilisez les adresses et numéros de téléphone / télécopie ci-dessous.

Network Associates
Australie

Level 1, 500 Pacific Highway
St. Leonards, NSW
Sydney, Australie 2065
Téléphone : 61-2-8425-4200
Télécopie : 61-2-9439-5166

Network Associates
Autriche

Pulvermuehlstrasse 17
Linz, Autriche
Code postal : A-4040
Téléphone : 43-732-757-244
Télécopie : 43-732-757-244-20

Network Associates
Belgique

BDC Heyzel Esplanade, boîte 43
1020 Bruxelles
Belgique
Téléphone : 0032-2 478.10.29
Télécopie : 0032-2 478.66.21

Network Associates
Brésil

Rua Geraldo Flausino Gomez, 78
Cj. - 51 Brooklin Novo - São Paulo
SP - 04575-060 - Brésil
Téléphone : (55 11) 5505 1009
Télécopie : (55 11) 5505 1006

Network Associates Canada

139 Main Street, Suite 201
Unionville, Ontario
Canada L3R 2G6
Téléphone : (905) 479-4189
Télécopie : (905) 479-4540

Network Associates Danemark

Lautruphoej 1-3
2750 Ballerup
Danemark
Téléphone : 45 70 277 277
Télécopie : 45 44 209 910

Network Associates France S.A.

50 rue de Londres
75008 Paris
France
Téléphone : 33 1 44 908 737
Télécopie : 33 1 45 227 554

Network Associates Hong Kong

19th Floor, Matheson Centre
3 Matheson Way
Causeway Bay
Hong Kong 63225
Téléphone : 852-2832-9525
Télécopie : 852-2832-9530

Network Associates République populaire de Chine

New Century Office Tower, Room 1557
No. 6 Southern Road Capitol Gym
Beijing
République populaire de Chine 100044
Téléphone : 8610-6849-2650
Télécopie : 8610-6849-2069

NA Network Associates Oy

Mikonkatu 9, 5. krs.
00100 Helsinki
Finlande
Téléphone : 358 9 5270 70
Télécopie : 358 9 5270 7100

Network Associates Allemagne GmbH

Ohmstraße 1
D-85716 Unterschleißheim
Allemagne
Téléphone : 49 (0)89/3707-0
Télécopie : 49 (0)89/3707-1199

Network Associates Srl

Centro Direzionale Summit
Palazzo D/1
Via Brescia, 28
20063 - Cernusco sul Naviglio (MI)
Italie
Téléphone : 39 02 92 65 01
Télécopie : 39 02 92 14 16 44

Network Associates Japon, Inc.

Toranomon 33 Mori Bldg.
3-8-21 Toranomon Minato-Ku
Tokyo 105-0001
Téléphone : 81 3 5408 0700
Télécopie : 81 3 5408 0780

Network Associates Amérique latine

1200 S. Pine Island Road, Suite 375
Plantation, Floride 33324
États-Unis d'Amérique
Téléphone : (954) 452-1731
Télécopie : (954) 236-8031

Network Associates Mexique

Andres Bello No. 10, 4 Piso
4th Floor
Col. Polanco
Mexico City, Mexico D.F. 11560
Téléphone : (525) 282-9180
Télécopie : (525) 282-9183

Network Associates International B.V.

Gatwickstraat 25
1043 GL Amsterdam
Pays-Bas
Téléphone : 31 20 586 6100
Télécopie : 31 20 586 6101

Network Associates Portugal

Av. da Liberdade, 114
1269-046 Lisboa
Portugal
Téléphone : 351 1 340 4543
Télécopie : 351 1 340 4575

Net Tools Network Associates Afrique du Sud

Bardev House, St. Andrews
Meadowbrook Lane
Epson Downs, P.O. Box 7062
Bryanston, Johannesburg
2021 Afrique du Sud
Téléphone : 27 11 706-1629
Télécopie : 27 11 706-1569

Network Associates Asie du Sud-Est

78 Shenton Way
#29-02
Singapour 079120
Téléphone : 65-222-7555
Télécopie : 65-220-7255

Network Associates Espagne

Orense 4, 4ª Planta.
Edificio Trieste
28020 Madrid, Espagne
Téléphone : 34 9141 88 500
Télécopie : 34 9155 61 404

Network Associates Suède

Datavägen 3A
Box 596
S-175 26 Järfälla
Suède
Téléphone : 46 (0) 8 580 88 400
Télécopie : 46 (0) 8 580 88 405

Network Associates Suisse

Baeulerwisenstrasse 3
8152 Glattbrugg
Switzerland
Téléphone : 0041 1 808 99 66
Télécopie : 0041 1 808 99 77

Network Associates Taiwan

Suite 6, 11F, No. 188, Sec. 5
Nan King E. Rd.
Taipei, Taiwan, République de Chine
Téléphone : 886-2-27-474-8800
Télécopie : 886-2-27-635-5864

Network Associates International Ltd.

227 Bath Road
Windsor, Berkshire
SL1 5PP
Royaume-Uni
Téléphone : 44 (0)1753 217 500
Télécopie : 44 (0)1753 217 520

À propos du logiciel VirusScan 1

Présentation du logiciel antivirusVirusScan

Quatre-vingt pour cent des 100 entreprises les plus puissantes et plus de 50 millions d'utilisateurs dans le monde entier choisissent le logiciel antivirus VirusScan pour protéger leurs ordinateurs contre un nombre croissant de virus et d'autres agents malveillants apparus au cours des dix dernières années pour s'attaquer aux réseaux d'entreprise et provoquer des dégâts au préjudice des utilisateurs. Ils ont choisi VirusScan parce que ce logiciel offre la solution de sécurité antivirus de bureau la plus complète, avec des fonctions qui décèlent les virus, bloquent les objets ActiveX et Java hostiles, identifient les sites Web dangereux, arrêtent les messages électroniques infectés et vont jusqu'à extirper les agents « zombies » qui s'attaquent à Internet. S'ils ont choisi VirusScan c'est également parce qu'ils reconnaissent à quel point la recherche et le développement antivirus effectués par McAfee viennent s'associer à leurs efforts pour préserver l'intégrité du réseau et les niveaux de service, garantir la sécurité des données et réduire les coûts de possession.

Avec plus de 50 000 virus et agents nuisibles actuellement en circulation, les enjeux de cette bataille sont considérables. Les virus et les vers ont maintenant des capacités qui peuvent occasionner de grosses pertes aux entreprises, non seulement en termes de productivité et de frais engagés pour le nettoyage des virus, mais aussi en termes de réduction des revenus dans la mesure où les entreprises font de plus en plus appel au commerce électronique et aux ventes en ligne et que les virus ne cessent de proliférer.

Le logiciel VirusScan est le premier à avoir mis à profit son avance technologique pour créer des utilitaires d'avant-garde développés pour combattre les toutes premières infections par des virus de l'ère des ordinateurs personnels. VirusScan s'est développé considérablement au cours des dernières années afin de contrecarrer chaque nouveau subterfuge inventé par les auteurs des virus. Figurant parmi l'une des premières application antivirus pour Internet, VirusScan conserve aujourd'hui sa renommée en tant qu'utilitaire commercial indispensable pour la nouvelle économie électronique. Maintenant, avec cette nouvelle version, le logiciel VirusScan ajoute un nouveau système de gestion et d'intégration avec d'autres outils antivirus McAfee.

Une amélioration architecturale signifie que chaque composant VirusScan travaille étroitement avec les autres, partageant des données et des ressources, afin d'obtenir une meilleure réponse de l'application et une diminution des demandes sur votre système. Une prise en charge totale du logiciel de gestion McAfee ePolicy Orchestrator signifie que les administrateurs du réseau peuvent gérer les détails de la configuration des composants et des tâches, vous laissant ainsi libre pour vous concentrer sur votre propre travail.

Une nouvelle technologie de mise à jour incrémentielle signifie des téléchargements de moteur d'analyse et de fichiers de définitions de virus plus rapides et une bande passante moins importante. La protection qu'il vous faut pour faire face aux taux de distribution élevés des virus de nouvelle génération peut arriver chez vous très rapidement. Pour en savoir plus sur ces fonctions, reportez-vous à la section « Nouveautés de cette version » à la page 39.

La nouvelle version inclut également la prise en charge de plusieurs plates-formes pour Windows 95, Windows 98, Windows NT Workstation v4.0 et Windows 2000 Professionnel, toutes dans un kit unique et avec un seul installateur, mais optimisées pour tirer profit des avantages offerts par chaque plate-forme. Les utilisateurs de Windows NT Workstation v4.0 et Windows 2000 Professionnel par exemple, peuvent exécuter le logiciel VirusScan avec des niveaux de sécurité différents qui offrent aux administrateurs système un vaste choix d'options d'application. Ainsi, la mise en œuvre d'une stratégie antivirus d'entreprise peut aller d'une application aléatoire, où l'administrateur peut verrouiller quelques paramètres critiques, à une application stricte avec des paramètres prédéfinis que l'utilisateur ne peut en aucun cas modifier ou désactiver.

Parallèlement, en tant que pilier de la gamme de logiciels de sécurité Active Virus Defense et Total Virus Defense de McAfee, le logiciel VirusScan conserve les mêmes fonctions essentielles qui ont fait de lui le principal utilitaire de bureau des entreprises. Ces fonctions incluent un taux de détection de virus sans pareil, de puissantes capacités heuristiques, détection et suppression des programmes du cheval de Troie, des mises à jour rapides grâce à des versions hebdomadaires des fichiers de définition de virus (.DAT), des versions bêta journalières du fichier .DAT et la prise en charge du fichier EXTRA.DAT en cas de crise ou de danger imminent. Dans la mesure où plus de 300 nouveaux virus ou agents logiciels nuisibles apparaissent chaque mois, McAfee renforce son logiciel VirusScan par une couverture mondiale, 24 heures sur 24, assurée par son équipe de recherche AVERT (Anti-Virus Emergency Response Team).

Malgré l'augmentation des virus et des vers qui se propagent via le courrier électronique, qui inondent les serveurs de messagerie, ou qui infectent directement les logiciels de productivité de groupe et les serveurs de fichiers, le bureau individuel reste la source d'infection individuelle la plus répandue, et constitue souvent le point d'entrée le plus vulnérable. Le logiciel VirusScan agit comme un sentinelle de bureau infatigable qui sauvegarde votre système contre les virus les plus connus, mais aussi contre les dernières menaces qui se cachent dans les sites Web, souvent sans que l'auteur du site en soit conscient ou qui se propagent par l'intermédiaire du courrier électronique, qu'il soit ou non sollicité.

Dans de telles conditions, prendre des précautions pour se protéger des logiciels nuisibles n'est plus un luxe mais une nécessité. Considérez l'importance des données de votre ordinateur, et le temps, les inconvénients, et les dépenses que le remplacement de ces données impliqueraient si elles étaient altérées ou inutilisables en raison d'une infection virale. D'après les estimations, les coûts de nettoyage pour une entreprise, à la suite d'une infection par un virus, ont représenté 16 milliards de dollars pour la seule année 1999. Comparez la probabilité d'infection et les coûts que cela entraînerait pour votre entreprise, avec le peu de temps et d'efforts que demande la mise en place de quelques mesures de sécurité évidentes ; vous pouvez rapidement vous rendre compte de l'utilité de se protéger contre des infections.

Vos données ne sont peut-être pas très importantes pour vous, mais sans protection, votre ordinateur pourrait abriter involontairement des virus se propageant sur les ordinateurs de vos collègues. La vérification périodique de votre disque dur à l'aide du logiciel VirusScan réduit potentiellement la vulnérabilité de votre machine face aux contaminations et vous permet de ne pas perdre de temps, d'argent et de données inutilement.

Principe de fonctionnement du logiciel VirusScan

Le logiciel VirusScan combine le moteur d'analyse le plus performant de l'industrie antivirus avec des améliorations d'interface de premier ordre, vous permettant de bénéficier de toute la puissance de ce moteur d'analyse. L'interface utilisateur graphique de VirusScan réunit tous ses composants de programme spécialisés, tout en conservant la flexibilité dont vous avez besoin pour adapter le logiciel à votre environnement informatique. Le moteur d'analyse combine de son côté les meilleures fonctions des technologies développées indépendamment par les chercheurs de McAfee et du Dr Solomon pendant plus d'une décennie.

Détection de virus rapide et précise

Ceci repose sur un environnement de développement unique construit pour le moteur d'analyse par les chercheurs de McAfee et du Dr Solomon. Cet environnement inclut Virtran, un langage de programmation spécialisé doté d'une structure et d'un « vocabulaire » optimisés pour les besoins spécifiques de la détection et la suppression de virus. À l'aide de fonctions de bibliothèque spécifiques à ce langage, par exemple, les chercheurs de virus peuvent déceler avec précision les sections généralement infectées par les virus à l'intérieur d'un fichier, d'une zone système ou d'une partition d'amorçage (MBR), soit parce qu'ils peuvent accéder aux zones infectées à l'insu des virus, soit parce qu'ils peuvent détourner les routines d'exécution des virus. Ainsi, le moteur d'analyse n'a plus besoin d'examiner la totalité du fichier à la recherche du code de virus ; il peut simplement échantillonner le fichier à des endroits bien définis à la recherche des signatures codées de virus qui indiquent une infection.

L'environnement de développement accélère la construction du fichier .DAT autant que les routines du moteur d'analyse. L'environnement fournit des outils pouvant être utilisés par les chercheurs pour écrire des définitions « génériques » capables d'identifier des familles entières de virus et de détecter facilement les dizaines ou centaines de variantes qui constituent la majorité des nouveaux virus. Les améliorations apportées régulièrement à cette technique ont déplacé la plupart des définitions de virus qui résidaient auparavant dans les mises à jour du fichier .DAT directement vers le moteur d'analyse, en tant que groupements de routines génériques. Les chercheurs peuvent même utiliser une fonction d'architecture Virtran pour insérer dans le nouveau moteur des « verbes » qui, une fois combinés avec des fonctions de moteur existantes, peuvent apporter des fonctionnalités supplémentaires requises pour faire face aux nouvelles techniques d'infection, aux nouvelles variantes, ou à d'autres problèmes posés par une nouvelle génération de virus.

Cela se traduit par des améliorations rapides et efficaces au niveau des capacités de détection du moteur, ce qui élimine le besoin d'exécuter des mises à jour continuelles destinées à identifier les nouvelles variantes des virus.

Détection des virus polymorphes cryptés

Parallèlement à la détection des variantes des virus génériques, le moteur d'analyse inclut maintenant un moteur de décryptage générique, qui est un jeu de routines permettant au logiciel VirusScan de suivre les virus qui tentent de se dissimuler par le cryptage et la mutation de leurs signatures codées. Ces virus « polymorphes » sont particulièrement difficiles à détecter, car leur signature codée change à chaque réplication.

Cela signifie que la méthode de correspondance sur modèle simple utilisée par les premiers moteurs d'analyse pour identifier de nombreux virus n'est plus applicable, car la séquence d'octets constante à détecter n'existe plus. Pour contrer cette menace, les chercheurs de McAfee ont développé le moteur de décryptage PolyScan, qui retrouve et analyse l'algorithme utilisé par ces types de virus pour se crypter et se décrypter. PolyScan exécute ensuite ce code dans une machine virtuelle émulée afin de comprendre la façon dont les virus parviennent à muter par eux-mêmes. Une fois cette opération effectuée, le moteur peut déceler la nature « réelle » de ces virus et les détecter de manière fiable, quelle que soit la méthode utilisée par les virus pour se cacher.

« Double analyse heuristique »

Une autre amélioration apportée au moteur d'analyse par les chercheurs de McAfee repose sur le perfectionnement des premières technologies d'analyse heuristique, conçues à l'origine pour détecter le gros flux de variantes de virus de macro apparu après 1995, rassemblées dans un ensemble d'instruments de haute précision. Les techniques d'analyse heuristique reposent sur l'expérience du moteur d'analyse avec les virus précédents pour déterminer les probabilités qu'un fichier suspect soit un nouveau virus non encore identifié ou non classé.

Le moteur d'analyse inclut à présent ViruLogic, qui est une technique heuristique capable d'observer le comportement d'un programme et d'évaluer à quel point il ressemble à un virus de macro *ou* à un virus de fichier. ViruLogic recherche les comportements caractéristiques d'un virus dans les fonctions de programme, tels que les modifications cachées des fichiers, les appels à l'arrière plan des clients de messagerie et d'autres méthodes utilisées par les virus pour se répliquer. Lorsque ces types de comportements atteignent un seuil de tolérance prédéfini, le moteur désigne le programme comme un éventuel virus.

Le moteur réalise également une évaluation « triangulaire » en recherchant dans le programme un comportement qui ne serait pas caractéristique d'un virus, en demandant certaines interventions de l'utilisateur par exemple, afin d'éliminer toute fausse identification de virus. Cette double combinaison heuristique des techniques « positive » et « négative » se traduit par un taux de détection inégalé avec peu ou pas de fausses identifications de virus.

Domaine d'application étendu

Les agents nuisibles ayant évolué pour tirer profit du caractère instantané et du succès de la communication par Internet, le logiciel VirusScan s'est lui aussi transformé pour contrecarrer les menaces qu'ils représentent. Un virus informatique désignait autrefois un type d'agent conçu pour se répliquer lui-même et provoquer peu de dégâts sur l'ordinateur cible. Cependant, au cours des dernières années, un large éventail d'agents nuisibles est apparu dans le but de s'attaquer aux ordinateurs personnels en utilisant des moyens très diversifiés. Nombre de ces agents, dont les vers à propagation rapide par exemple, utilisent des versions actualisées des anciennes techniques pour infecter les systèmes, mais d'autres utilisent toutes les capacités offertes par les nouvelles techniques de script et d'hébergement d'applications sur le Web.

D'autres agents nuisibles ouvrent des « portes arrière » dans les systèmes de bureau ou créent des trous de sécurité qui ressemblent à une tentative délibérée de pénétration du réseau, plutôt qu'aux dégâts que la plupart des virus laissent derrière eux.

En conséquence, les dernières versions du logiciel VirusScan n'attendent pas l'apparition des virus dans votre système, mais analysent de manière proactive la source ou le travail afin de dévier les agents nuisibles de votre système. Le moteur d'analyse VShield, livré avec le logiciel VirusScan, contient trois modules centrés sur les agents nuisibles qui arrivent par Internet, qui se propagent via le courrier électronique ou qui se cachent dans les sites Internet. Il peut rechercher des objets Java et ActiveX qui représentent un danger, ou bloquer l'accès aux sites Internet risqués. Entre-temps, l'extension Analyse E-Mail, destinée à protéger des clients e-mail Microsoft Exchange, tels que Microsoft Outlook, peut « soumettre aux rayons x » votre boîte aux lettres sur le serveur, à la recherche d'agents malveillants avant que ces derniers n'arrivent sur votre bureau.

Le logiciel VirusScan va jusqu'à se protéger lui-même contre les tentatives d'utilisation de ses propres fonctionnalités contre votre ordinateur. Certains auteurs de virus imbriquent leurs virus dans des documents qu'ils imbriquent à leur tour dans d'autres fichiers dans un souci d'éviter la détection. Il y en a qui appliquent cette technique de manière insensée, allant jusqu'à construire des fichiers d'archives compressés hautement récursifs et très volumineux dans le but de ligoter le moteur d'analyse lors qu'il analyse le fichier en profondeur à la recherche d'un virus. Le logiciel VirusScan analyse avec précision la plupart des formats de fichier compressé et de fichier d'archives courants, mais il inclut également une logique qui l'empêche de se retrouver coincé dans une recherche interminable de virus non existants.

Composants fournis avec VirusScan

Le logiciel VirusScan comprend plusieurs composants qui combinent un ou plusieurs programmes liés, ayant chacun un rôle à jouer dans la protection de votre ordinateur contre les virus et autres logiciels nuisibles. Les composants sont les suivants :

- **L'application VirusScan.** Ce composant vous permet de contrôler vos analyses de la manière la plus efficace. Vous pouvez configurer et démarrer une analyse à tout moment - fonction appelée analyse « à la demande » -, spécifier des disques réseau et locaux comme cibles à analyser, choisir la façon dont VirusScan traitera les infections détectées et afficher des rapports sur ses actions. Vous pouvez démarrer avec la fenêtre VirusScan classique, un mode de configuration de base, puis passer au mode VirusScan avancé pour obtenir une flexibilité optimale. Une extension shell Windows associée vous permet de faire un clic droit sur n'importe quel objet de votre système pour l'analyser. Pour plus de détails, reportez-vous à la section voir « Utilisation de l'application VirusScan » à la page 197.
- **La console VirusScan**. Ce composant vous permet de créer, de configurer et d'exécuter des tâches VirusScan aux heures que vous spécifiez. Une « tâche » peut aller de l'exécution d'une opération d'analyse sur un ensemble de disquettes, à un moment ou à intervalle donné, à l'exécution d'une mise à jour ou d'une mise à niveau. Vous pouvez également activer ou désactiver le moteur d'analyse Vshield à partir de la fenêtre de la console.

  La console est fournie avec une liste de tâches prédéfinies qui garantissent un niveau de protection minimal pour votre système ; vous pouvez, par exemple, analyser et nettoyer immédiatement votre lecteur C: ou tous les disques de votre ordinateur. Pour plus de détails, reportez-vous à la section voir « Création et configuration des tâches planifiées » à la page 231.

- **Le moteur d'analyse VShield**. Ce composant fournit une protection anti-virale permanente contre les virus provenant de disquettes, du réseau ou de diverses sources sur Internet. VShield est lancé lorsque vous démarrez votre ordinateur et reste en mémoire jusqu'à ce que vous l'éteigniez. Un ensemble de pages de propriétés flexibles vous permet d'indiquer à VShield les parties de votre système que vous souhaitez analyser, les éléments à rechercher, les parties à ne pas toucher et la réaction à adopter face aux fichiers infectés localisés. En outre, VShield peut vous prévenir en cas de détection d'un virus et générer des rapports résumant chacune de ses actions.

  Le moteur d'analyse Vshield est livré avec trois autres modules spécialisés qui protègent votre système contre les applets Java et les contrôles ActiveX nocifs. Ces modules peuvent analyser les messages électroniques et les pièces jointes que vous recevez via Internet au moyen de Lotus cc:Mail, Microsoft Mail ou un autre client de messagerie utilisant le standard MAPI (Messaging Application Programming Interface) Microsoft et bloquer l'accès aux sites Internet dangereux. Pour éviter que d'autres utilisateurs effectuent des modifications non autorisées, adoptez une protection de mot de passe sûr pour vos options de configuration. Une seule boîte de dialogue fonctionnelle contrôle les options de configuration de tous les modules VShield. Pour plus de détails, reportez-vous à la section voir « Utilisation du moteur d'analyse VShield » à la page 101.

- **L'extension Analyse E-Mail**. Ce composant vous permet d'analyser votre boîte aux lettres Microsoft Exchange ou Outlook ou des dossiers publics auxquels vous avez accès, directement sur le serveur. Cette surveillance de type « rayon x » appliquée à votre boîte aux lettres signifie que le logiciel VirusScan peut détecter des infections potentielles avant même qu'elles n'arrivent sur votre bureau et neutraliser des virus de type Melissa. Pour plus de détails, reportez-vous à la section voir « Analyse des systèmes de messagerie Microsoft Exchange et Outlook » à la page 303.

- **Le moteur d'analyse cc:Mail**. Ce composant applique une technologie optimisée pour analyser les boîtes aux lettres Lotus cc:Mail n'utilisant pas le standard MAPI. Procédez à l'installation et à l'application de ce composant si votre groupe de travail ou votre réseau utilise cc:Mail v7.x ou une version antérieure. Pour plus de détails, reportez-vous à la section voir « Sélection des options de détection » à la page 138.

- **L'utilitaire de configuration cliente du Gestionnaire d'alerte**. Ce composant vous permet de choisir un emplacement de destination pour les « événements » du Gestionnaire d'alerte générés par le logiciel VirusScan chaque fois qu'il détecte un virus ou qu'il entreprend une autre action importante. Vous pouvez également spécifier un répertoire de destination pour les messages d'alerte centralisée anciens ou compléter ces méthodes avec les alertes DMI (Desktop Management Interface) envoyées via votre logiciel client DMI. Pour plus de détails, reportez-vous à la section voir « Utilisation de l'utilitaire de Configuration cliente du Gestionnaire d'alerte » à la page 338.

- **L'utilitaire ScreenScan**. Ce composant facultatif analyse votre ordinateur pendant que l'écran de veille occupe les périodes d'inactivité. Pour plus de détails, reportez-vous à la section voir « Utilisation de l'utilitaire ScreenScan » à la page 323.

- **L'utilitaire SendVirus**. Ce composant vous offre un moyen facile et convivial de soumettre des fichiers susceptibles d'être infectés directement aux chercheurs de McAfee. Un Assistant vous guide pendant que vous choisissez les fichiers à envoyer, spécifiez les détails du contact et, si vous le souhaitez, supprimez des données personnelles ou confidentielles dans les fichiers document. Pour plus de détails, reportez-vous à la section voir « Utilisation de l'utilitaire SendVirus pour soumettre un exemple de fichier » à la page 91.

- **L'Utilitaire de création d'une disquette de secours**. Cet utilitaire indispensable vous aide à créer une disquette pouvant être utilisée pour amorcer votre ordinateur dans un environnement exempt de tout virus et analyser ensuite des zones système critiques afin de supprimer les virus pouvant être chargés au démarrage. Pour plus de détails, reportez-vous à la section voir « Utilisation de l'utilitaire de création d'une disquette de secours » à la page 59.

- **Moteurs d'analyse de ligne de commande**. Ce composant contient un jeu de moteurs d'analyse dotés de multiples fonctions et pouvant être utilisés pour exécuter des analyses ciblées à partir de l'invite MS-DOS, de l'invite de commande, ou du mode MS-DOS protégé. Ce jeu de moteurs d'analyse inclut :

  – SCAN.EXE, un moteur d'analyse réservé aux environnements 32 bits. Ce composant constitue la principale interface de ligne de commande. Lorsque vous exécutez ce fichier, il vérifie d'abord son environnement afin de déterminer s'il peut être exécuté par lui-même. Si votre ordinateur fonctionne en mode 16 bits ou en mode protégé, SCAN.EXE transmet le contrôle à un autre moteur d'analyse.

  – SCANPM.EXE, un moteur d'analyse destiné aux environnements 16 et 32 bits. Le moteur d'analyse met à votre disposition un ensemble complet d'options d'analyse pour les environnements DOS fonctionnant en mode protégé à 16 ou à 32 bits. Il prend également en charge l'allocation de mémoire étendue et de mémoire flexible. SCAN.EXE transfère le contrôle à ce moteur d'analyse lorsque ces fonctions spécialisées lui permettent d'effectuer une analyse plus efficace.

- SCAN86.EXE, un moteur d'analyse réservé aux environnements 16 bits. Ce moteur d'analyse inclut un jeu de fonctions limitées réservé aux environnements 16 bits. SCAN.EXE transfère le contrôle à ce moteur d'analyse si votre ordinateur fonctionne en mode 16 bits, mais sans aucune configuration de mémoire particulière.
- BOOTSCAN.EXE, un moteur d'analyse spécialisé, de plus petite taille, utilisé principalement avec l'utilitaire de création d'une disquette de secours. Ce moteur d'analyse s'exécute généralement à partir d'une disquette que vous créez afin d'obtenir un environnement de départ exempt de tout virus.

  Lorsque vous exécutez l'Assistant de création de la disquette de secours, VirusScan copie sur une même disquette le fichier BOOTSCAN.EXE et un ensemble de fichiers .DAT spéciaux. BOOTSCAN.EXE ne détectera ni ne nettoiera pas les virus de macro, mais détectera et éliminera tous les autres virus susceptibles de menacer la sécurité de votre installation VirusScan ou d'infecter des fichiers au démarrage du système. Une fois ces virus identifiés et éliminés, vous pouvez en toute sécurité exécuter VirusScan pour nettoyer le reste de votre système.

Tous les moteurs d'analyse de ligne de commande vous permettent d'effectuer des analyses ciblées à partir de l'invite MS-DOS, de l'invite de commande, ou du mode MS-DOS protégé. En temps normal, vous utiliserez l'interface utilisateur graphique VirusScan (GUI) pour effectuer la plupart des analyses. Toutefois, si vous rencontrez des problèmes pour lancer Windows ou si les composants de la GUI VirusScan ne peuvent être exécutés dans votre environnement, utilisez les moteurs d'analyse de ligne de commande comme recours.

- **Documentation.** La documentation VirusScan se compose des éléments suivants :
  - Un *Guide de démarrage rapide*, qui présente le produit et les instructions d'installation, indique la procédure à suivre si vous suspectez la présence d'un virus sur l'ordinateur, et offre une vue d'ensemble du produit. Le *Le Guide de démarrage rapide* est fourni avec la version de VirusScan sur CD-ROM. Vous pouvez également le télécharger sous le nom VSC45WGS.PDF à partir du site Web de Network Associates ou à partir d'autres services électroniques.

- Ce guide d'utilisateur est enregistré sur le CD-ROM de VirusScan ou installé sur votre disque dur au format .PDF d'Adobe Acrobat. Vous pouvez aussi le télécharger sous le nom VSC45WUG.PDF à partir du site Web de Network Associates ou à partir d'autres services électroniques. Le Guide d'utilisateur VirusScan offre une description détaillée de l'utilisation de VirusScan, ainsi que d'autres informations utiles, telles que les options de configuration avancées. Les fichiers .PDF d'Acrobat sont des documents en ligne maniables contenant des liens hypertexte, des définitions et d'autres options qui facilitent la navigation au sein de ces documents, et donc l'accès à l'information.

- Un guide de l'administrateur est enregistré sur le CD-ROM de VirusScan ou installé sur votre disque dur au format .PDF d'Adobe Acrobat. Vous pouvez aussi le télécharger sous le nom VSC45WAG.PDF à partir du site Web de Network Associates ou à partir d'autres services électroniques. Le *Guide de l'administrateur VirusScan* offre une description détaillée de la gestion et de la configuration du logiciel VirusScan à partir d'un bureau local ou distant.

- Un fichier d'aide en ligne. Ce fichier vous permet d'accéder rapidement à une gamme complète de rubriques décrivant le logiciel VirusScan. Pour ouvrir ce fichier, choisissez **Rubriques d'aide** dans le menu **Aide** de la fenêtre principale de VirusScan, ou cliquez sur l'un des boutons **Aide** qui s'affichent dans les boîtes de dialogue de VirusScan.

  Le fichier d'aide inclut également une aide contextuelle étendue ou « Qu'est-ce que c'est ? ». Pour afficher l'aide contextuelle, faites un clic droit sur un bouton, une liste, une icône, une zone de texte ou tout autre élément présent dans une boîte de dialogue. Vous pouvez également cliquer sur le symbole **?** à l'angle supérieur droit dans la plupart des boîtes de dialogue, puis cliquer sur l'élément dont vous souhaitez obtenir une description pour afficher la rubrique correspondante. Les boîtes de dialogue comportant le bouton **Aide** ouvrent le fichier d'aide sur la rubrique qui décrit l'ensemble de la boîte de dialogue.

- Un fichier LICENSE.TXT. Ce fichier stipule les termes de la licence d'utilisation du logiciel VirusScan. Lisez-le avec attention, car l'installation de VirusScan implique l'acceptation de ces termes.

– Un fichier README.TXT. Ce fichier présente les modifications et/ou les ajouts de dernière minute, énumère les aspects ou autres questions relatifs à la version du produit, et décrit généralement les nouvelles fonctions incorporées dans la mise à jour du produit. Le fichier README.TXT se trouve au niveau de la racine dans l'arborescence du CD-ROM de VirusScan, ou dans le dossier programme de VirusScan. Vous pouvez l'ouvrir et l'imprimer à partir du Bloc-notes de Windows ou de toute autre application de traitement de texte.

Nouveautés de cette version

Cette version de VirusScan introduit plusieurs fonctions innovatrices aux fonctionnalités de base du produit, à son domaine d'application, et aux détails de l'architecture de son application. La plupart de ces fonctions sont expliquées en détail dans une section précédente, « Principe de fonctionnement du logiciel VirusScan » à la page 31. La seule différence majeure entre les versions antérieures et la version actuelle de VirusScan est l'intégration de deux versions différentes de VirusScan optimisées pour fonctionner sur des plates-formes Windows différentes dans un produit unique pouvant être exécuté sur les deux plates-formes. Ce produit unique bénéficie également des avantages propres à chaque plate-forme.

Les sections suivantes décrivent d'autres modifications introduites dans cette version de VirusScan.

Fonctions d'installation et de distribution

Les produits antivirus McAfee, y compris le logiciel VirusScan, utilisent dorénavant l'utilitaire Microsoft Windows Installer (MSI), livré avec tous les systèmes Windows 2000 Professionnel. Cet utilitaire d'installation offre un vaste choix de fonctions d'installation et de configuration, ce qui facilite le déploiement du logiciel VirusScan dans les entreprises de grande taille. Pour plus d'informations sur l'exécution d'opérations d'installation personnalisées à l'aide de MSI, reportez-vous au Chapitre 2, « Installation du logiciel VirusScan » du *Guide de l'administrateur* VirusScan.

Cette version de VirusScan offre également une prise en charge complète de l'outil de distribution de logiciels ePolicy Orchestrator de McAfee . Une version spéciale de VirusScan est livrée avec le logiciel ePolicy Orchestrator, conçue pour une large distribution au sein des entreprises. Vous pouvez distribuer le logiciel VirusScan, le configurer à partir de la console ePolicy Orchestrator, mettre à jour à tout moment cette configuration, un autre programme ou des fichiers .DAT, et planifier les opérations d'analyse et ceci pour l'ensemble des utilisateurs du réseau. Pour plus d'informations sur l'utilisation du logiciel ePolicy Orchestrator pour la distribution et la configuration de VirusScan, reportez-vous au *Guide de l'administrateur* ePolicy Orchestrator.

Cette version de VirusScan inclut également la description des kits pour d'autres outils de distribution, y compris les produits de gestion de logiciels Microsoft System Management Server et Tivoli Systems.

Améliorations au niveau de l'interface

Cette version amène l'interface VirusScan, pour toutes les plates-formes prises en charge, sur le terrain où VirusScan pour Windows 95 et Windows 98 ont été les pionniers avec la version v4.0.1. Ainsi, le moteur d'analyse VShield a été enrichi avec de nouvelles options de configuration étendues pour les plates-formes Windows NT Workstation v4.0 et Windows 2000 Professionnel, tout en réduisant la complexité de certaines options de configuration antérieures. La configuration du serveur du Gestionnaire d'alerte, par exemple, est entièrement déplacée vers la ligne de produit NetShield, ce qui permet au logiciel VirusScan d'agir strictement en tant qu'application cliente configurable.

Cette version ajoute également un nouveau panneau de configuration VirusScan, qui fonctionne comme un point central à partir duquel vous pouvez activer et désactiver tous le composants VirusScan. Ce panneau de configuration vous permet également de définir un plafond qui s'appliquera au nombre d'éléments que vous pouvez inclure ou exclure dans chaque opération d'analyse, et de configurer le moteur d'analyse VShield et le panneau de configuration VirusScan pour être activés au démarrage. Parmi les autres modifications figurent :

- De nouvelles icônes dans la barre d'état système VShield vous donnent des informations supplémentaires sur les modules VShield actifs. Ces états sont les suivants :
  -  Tous les modules VShield sont actifs
  -  Le module Analyse système est actif, mais un ou plusieurs autres modules VShield sont inactifs
  -  Le module Analyse système est inactif, mais un ou plusieurs autres modules VShield sont actifs
  -  Tous les modules VShield sont actifs
- De nouveaux paramètres d'interface pour la configuration des tâches vous permettent d'indiquer à VirusScan la façon dont il doit s'afficher lors de l'exécution d'une tâche planifiée et la démarche à suivre une fois l'opération terminée. Vous pouvez également définir un mot de passe pour protéger des paramètres d'une tâche isolée contre toute modification, ou une configuration entière de tâches.

- Une fonction de randomisation actualisée pour les tâches planifiées vous permet de définir une heure pour l'exécution d'une tâche, puis de définir une « fenêtre » de randomisation. La console VirusScan choisit ensuite une heure aléatoire à l'intérieur de cette fenêtre pour démarrer l'exécution de la tâche.

- Le module Analyse système inclut maintenant une nouvelle option de configuration, Type d'invite, pour les systèmes Windows 95 et Windows 98. Cette option vous permet de déterminer la façon dont l'alerte **Interroger l'utilisateur** doit apparaître.

Modifications au niveau de la fonctionnalité du produit

- Un nouvel utilitaire de configuration cliente du Gestionnaire d'alerte vous permet de choisir un serveur du Gestionnaire d'alerte installé sur votre réseau comme emplacement de destination pour les messages d'alerte, ou un partage réseau comme emplacement de destination pour les messages d'alerte centralisée. Vous pouvez également compléter ces méthodes d'alerte avec les messages d'alerte DMI (Desktop Management Interface).

- Le serveur du Gestionnaire d'alerte prend en charge les numéros de série du processeur Intel Pentium III pour identifier chaque ordinateur dans le cadre d'une notification en cas de virus. Pour plus d'informations sur les numéros de série du processeur Intel, consultez le forum aux questions Intel à l'adresse http://support.intel.com/support/processors/pentiumiii/psqa.htm.

De nouvelles options de mise à jour pour votre logiciel VirusScan

Même si la plupart des définitions de virus requises sont intégrées directement dans son moteur sous la forme de routines génériques, le logiciel VirusScan nécessite encore des mises à jour régulières du fichier .DAT pour contrecarrer la menace que représentent les 200 à 300 nouveau virus qui apparaissent chaque mois. Pour répondre à cette demande, McAfee a incorporé une technologie de mise à jour dans le logiciel VirusScan depuis les débuts de sa conception. Dans la version actuelle de VirusScan, cette technologie a fait un pas un avant avec la nouvelle mise à jour incrémentielle des fichiers .DAT.

Les fichiers .DAT incrémentiels sont des petits kits de fichiers de définition de virus rassemblant des données sur un ensemble de versions de fichiers .DAT donné. Les dernières versions des utilitaires AutoUpdate et AutoUpgrade fournissent un support transparent pour les nouvelles mises à jour, en vous permettant de télécharger et d'installer uniquement les définitions de virus qui ne sont pas encore installées sur votre système. Cela se traduit par une forte diminution du temps de téléchargement et d'installation et par une diminution équivalente de la demande de bande passante sur le réseau.

Installation du logiciel VirusScan 2

Avant de commencer

McAfee assure la distribution du logiciel VirusScan sous deux formats : 1) sous la forme d'un fichier archivé que vous pouvez télécharger à partir du site Web de McAfee et 2) sur CD-ROM. Même si la méthode utilisée pour transférer les fichiers VirusScan depuis un archive que vous téléchargez diffère de celle utilisée pour transférer les fichiers stockés sur un CD-ROM que vous placez dans votre lecteur, la procédure d'installation que vous utilisez par la suite est identique pour les deux types de distribution. Vérifiez que VirusScan pourra fonctionner sur votre système en vous reportant à la configuration requise détaillée ci-dessous, puis passez à la section « Préparation de l'installation du logiciel VirusScan » à la page 44.

Configuration requise

VirusScan peut être installé et exécuté sur un PC IBM ou compatible équipé de :

- Un processeur Pentium Intel ou compatible. McAfee recommande un processeur Intel Pentium ou un processeur Celeron de 166 MHz minimum.
- Un lecteur de CD-ROM. Si vous avez téléchargé votre exemplaire de VirusScan, cet élément est optionnel.
- 40 Mo minimum d'espace libre sur le disque dur pour une installation complète. McAfee recommande 75 Mo.
- 16 Mo minimum de mémoire vive disponible (RAM). McAfee recommande 20 Mo.
- Microsoft Windows 95, Windows 98, Windows NT Workstation v4.0 avec Service Pack 4 ou version ultérieure, ou Windows 2000 Professionnel. McAfee recommande également l'utilisation de Microsoft Internet Explorer v4.0.1, déjà installé ou installé par la suite, en particulier si votre système utilise une version de Windows 95.

Autres recommandations

Afin de bénéficier des fonctionnalités de mise à jour automatique de VirusScan, vous devez disposer d'une connexion à Internet, via votre réseau local ou via un modem grande vitesse et un fournisseur de services Internet.

Préparation de l'installation du logiciel VirusScan

Pour préparer vos fichiers en vue de l'installation, suivez la procédure correspondant au mode de distribution de VirusScan que vous avez adopté.

- **Si vous avez téléchargé VirusScan** à partir du site Web de Network Associates, d'un serveur situé sur votre réseau local, ou d'un autre service électronique, créez un répertoire sur votre disque dur, dans lequel vous extrairez ensuite les fichiers d'installation de VirusScan à l'aide d'un utilitaire de compression / décompression tel que WinZip ou PKZIP. Vous pouvez télécharger ce type d'utilitaire depuis la plupart des services en ligne.

  IMPORTANT : Si vous pensez que votre ordinateur est susceptible d'être infecté par un virus, téléchargez les fichiers d'installation de VirusScan sur un ordinateur ***non*** infecté. Installez votre exemplaire de VirusScan sur l'ordinateur non contaminé, puis, à l'aide de l'utilitaire Disquette de secours, créez une disquette qui vous permettra ensuite d'amorcer l'ordinateur infecté et d'éliminer le virus. Pour en savoir plus, consultez la section « Si vous suspectez la présence d'un virus... » à la page 71.

- **Si vous disposez du CD-ROM de VirusScan**, insérez celui-ci dans votre lecteur de CD-ROM.

Si vous insérez un CD-ROM, l'écran d'accueil de VirusScan doit s'afficher automatiquement. Pour installer le logiciel VirusScan maintenant, cliquez sur **Installer**, puis passez à l'Étape 4 à la page 47 pour continuer l'installation. Si l'écran d'accueil ne s'affiche pas ou si vous installez VirusScan à partir de fichiers téléchargés, commencez la procédure à partir de l'Étape 2 à la page 45.

IMPORTANT : Dans la mesure où le programme d'installation installe certains fichiers VirusScan en tant que services sur les systèmes Windows NT Workstation v4.0 et Windows 2000 Professionnel, vous devez vous connecter au système avec des droits d'administrateur pour installer ce produit. Pour lancer l'installation sur Windows 95 ou Windows 98, vous n'avez pas besoin de vous connecter avec des profils ou des droits spécifiques.

Options d'installation

La section "Procédure d'installation" décrit la procédure d'installation du logiciel VirusScan avec les options courantes sur un seul ordinateur ou une seule station de travail. Vous pouvez choisir l'installation Par défaut pour installer les composants VirusScan utilisés couramment, mais certains modules VShield et l'utilitaire ScreenScan ne seront pas installés. Si vous choisissez l'installation Personnalisée, vous pourrez installer tous les composants VirusScan.

Pour connaître la procédure d'installation du logiciel VirusScan sur plusieurs ordinateurs en même temps, ou pour modifier votre installation afin de mettre en œuvre une stratégie antivirus d'entreprise, reportez-vous au *Guide de l'administrateur* VirusScan, qui décrit comment installer et configurer le logiciel VirusScan en fonction des besoins spécifiques à chaque entreprise. Vous pouvez également utiliser le logiciel ePolicy Orchestrator de McAfee pour distribuer et configurer VirusScan sur des milliers d'ordinateurs de bureau d'un réseau. Pour plus de détails, reportez-vous au *Guide de l'administrateur* ePolicy Orchestrator.

Procédure d'installation

McAfee recommande de fermer d'abord toutes les applications en cours d'exécution sur votre système avant de démarrer l'installation. Ceci réduit les probabilités de conflit logiciel au cours de l'installation.

Pour installer le logiciel VirusScan, procédez comme suit :

1. Si votre ordinateur fonctionne avec Windows NT Workstation v4.0 ou Windows 2000 Professionnel, ouvrez une session sur votre système en tant qu'administrateur. Vous devez disposer des droits d'administrateur pour installer VirusScan sur votre système.

2. Dans le menu **Démarrer** de la barre des tâches Windows, choisissez **Exécuter**.

   La boîte de dialogue Exécuter s'affiche (Figure 2-1).

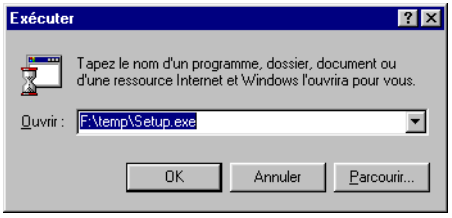

Figure 2-1. Boîte de dialogue Exécuter

3. Tapez <X>:\SETUP.EXE dans la zone de texte, puis cliquez sur **OK**.

   <X> représente la lettre correspondant à votre lecteur de CD-ROM ou le chemin d'accès au répertoire contenant les fichiers d'installation téléchargés de VirusScan. Pour rechercher les fichiers sur le disque dur ou le CD-ROM, cliquez sur **Parcourir**.

   ❑ **REMARQUE :** Si vous disposez de VirusScan sur un CD-ROM Active Virus Defense ou Total Virus Defense, vous devez également préciser le dossier qui contient le logiciel VirusScan.

   Avant de poursuivre, le programme d'installation vérifie d'abord si la version 1.1 de l'utilitaire Microsoft Windows Installer (MSI) est déjà en cours d'exécution en tant que partie intégrante de votre logiciel système.

   Si votre ordinateur fonctionne avec Windows 2000 Professionnel, cette version de MSI est déjà installée sur votre système. Si votre ordinateur utilise une version antérieure de Windows, il est probable que cette version de MSI soit déjà présente sur votre système si vous avez installé auparavant un autre logiciel qui utilise MSI. Dans les deux cas, le programme d'installation affiche immédiatement le premier écran de l'Assistant. Passez à l'Étape 4 pour continuer.

   Si le programme d'installation ne trouve pas MSI v1.1 sur votre ordinateur, il installe les fichiers requis pour continuer l'installation, puis vous invite à redémarrer votre ordinateur. Cliquez sur **Redémarrer l'ordinateur**. Pour obtenir la liste des circonstances dans lesquelles le programme d'installation ou les mises à jour du système nécessitent le réamorçage du système, reportez-vous à la section « Circonstances qui exigent le redémarrage de votre ordinateur » à la page 66.

   Lorsque l'ordinateur redémarre, le programme d'installation reprend le processus au stade qui a précédé l'arrêt de l'ordinateur. L'écran d'accueil Installation s'affiche (Figure 2-2 à la page 47).

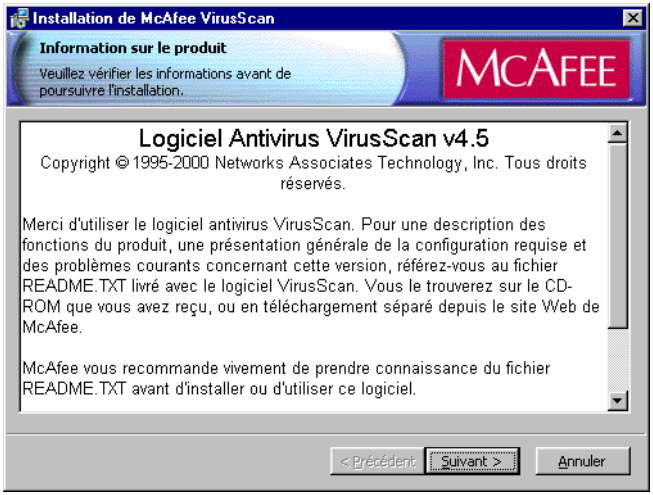

Figure 2-2. Écran d'accueil Installation

4. Ce premier écran vous indique l'emplacement où vous allez placer le fichier README.TXT, qui décrit les fonctions du produit, les problèmes connus, et fournit les toutes dernières informations disponibles sur cette version de VirusScan. Après avoir lu le texte, cliquez sur **Suivant>** pour continuer.

5. L'écran suivant affiche le contrat de licence utilisateur final de VirusScan. Lisez ce contrat attentivement, car l'installation de VirusScan implique l'acceptation des termes de la licence.

   Si vous n'acceptez pas les termes du contrat de licence, sélectionnez **Je n'accepte pas les termes du contrat de licence**, puis cliquez sur **Annuler**. Vous quitterez alors le programme d'installation. Sinon, cliquez sur **J'accepte les termes du contrat de licence**, puis cliquez sur **Suivant>** pour continuer.

   Le programme d'installation vérifie alors si des versions antérieures de VirusScan ou des logiciels incompatibles sont installés sur votre ordinateur. Si aucun autre logiciel antivirus ou aucune version précédente de VirusScan ne sont installés sur votre ordinateur, le programme d'installation affiche l'écran Type d'installation (Figure 2-6). Passez à l'Étape 8 à la page 50 pour continuer.

   Si le programme d'installation détecte une version antérieure de VirusScan sur votre ordinateur, il vous informe qu'il doit la supprimer. Si votre ordinateur fonctionne avec Windows 95 ou Windows 98, le programme d'installation vous offre la possibilité de préserver les paramètres de configuration de VShield que vous avez choisies pour la version antérieure (Figure 2-3 à la page 48).

Si votre ordinateur utilise Windows NT Workstation v4.0 ou Windows 2000 Professionnel, le programme d'installation supprimera la version antérieure de VirusScan, mais *ne* conservera pas les paramètres de l'ancienne installation du moteur d'analyse VShield.

Figure 2-3. écran Version précédente détectée

6. Sélectionnez **Préserver les paramètres lors de l'accès**, si cette option est disponible, puis cliquez sur **Suivant>** pour continuer.

   Si le programme d'installation détecte un logiciel incompatible, il affiche un écran vous permettant de supprimer le logiciel en conflit (voir Figure 2-4 à la page 49).

   Si aucun logiciel incompatible n'est détecté et si votre ordinateur fonctionne avec Windows 95 ou Windows 98, passez à l'Étape 9 à la page 51 pour continuer l'installation. Si aucun logiciel incompatible n'est détecté et si votre ordinateur fonctionne avec Windows NT Workstation v4.0 ou Windows 2000 Professionnel, passez à l'Étape 8 à la page 50 pour continuer. Sinon, passez à l'Étape 7.

Figure 2-4. Écran Logiciel incompatible

7. Cochez la case qui s'affiche, puis cliquez sur **Suivant>**. Le programme d'installation lance l'utilitaire de désinstallation utilisé normalement par le logiciel en conflit, lui permettant de supprimer le logiciel de votre ordinateur. L'utilitaire de désinstallation peut vous demander de redémarrer l'ordinateur pour supprimer complètement le logiciel en conflit. Vous n'avez *pas* besoin de redémarrer votre ordinateur pour continuer l'installation de VirusScan ; tant que l'autre logiciel n'est pas actif, le programme d'installation peut continuer sans générer de conflits.

❑ **REMARQUE :** McAfee recommande fortement de supprimer les logiciels incompatibles. La plupart des logiciels antivirus fonctionnant à un niveau très bas au sein de votre système, deux programmes antivirus qui tentent simultanément d'accéder aux mêmes fichiers ou qui exécutent des opérations critiques peuvent rendre votre système très instable.

Si votre ordinateur fonctionne avec Windows NT Workstation v4.0 ou Windows 2000 Professionnel, le programme d'installation vous demande alors le mode de sécurité que vous souhaitez utiliser pour exécuter le logiciel VirusScan sur votre système (voir Figure 2-5 à la page 50).

Les options proposées dans cet écran vous permettent de déterminer si d'autres utilisateurs auront ou non la possibilité de modifier les options de configuration que vous avez choisies, de planifier et d'exécuter des tâches et d'activer et désactiver les composants VirusScan. Le logiciel VirusScan inclut de nombreuses mesures de sécurité afin de garantir qu'aucun utilisateur non autorisé ne modifiera la configuration du logiciel en mode Sécurité maximale. Le mode Sécurité standard permet à tous les utilisateurs d'accéder à l'ensemble des options de configuration.

Quelle que soit l'option choisie, le programme installera la même version de VirusScan, les mêmes options de configuration et les mêmes tâches planifiées pour tous les utilisateurs du système.

Figure 2-5. Écran Type de sécurité

8. Sélectionnez le mode de sécurité que vous préférez. Vous avez le choix entre les options suivantes :

   - **Utiliser la sécurité maximale**. Choisissez cette option pour exiger des droits d'administrateur à tout utilisateur souhaitant modifier des options de configuration, activer ou désactiver des composants VirusScan, ou configurer et exécuter des tâches planifiées.

     Les utilisateurs ne disposant pas des droits d'administrateur requis pourront toujours configurer et exécuter leurs propres opérations d'analyse avec l'application VirusScan et enregistrer les paramètres de ces opérations dans un fichier .VSC, mais ils ne seront pas en mesure de modifier les paramètres par défaut de l'application VirusScan. Pour plus d'informations sur la configuration et l'enregistrement des paramètres de l'application VirusScan, reportez-vous au Chapitre 5, « Utilisation de l'application VirusScan ».

- **Utiliser la sécurité standard**. Choisissez cette option pour permettre à tout utilisateur ouvrant une session sur votre ordinateur de modifier des options de configuration, d'activer ou de désactiver des composants VirusScan, ou de configurer et d'exécuter des tâches planifiées.

Le programme d'installation vous demande ensuite de choisir entre une installation par défaut et une installation personnalisée pour cet ordinateur (voir Figure 2-6).

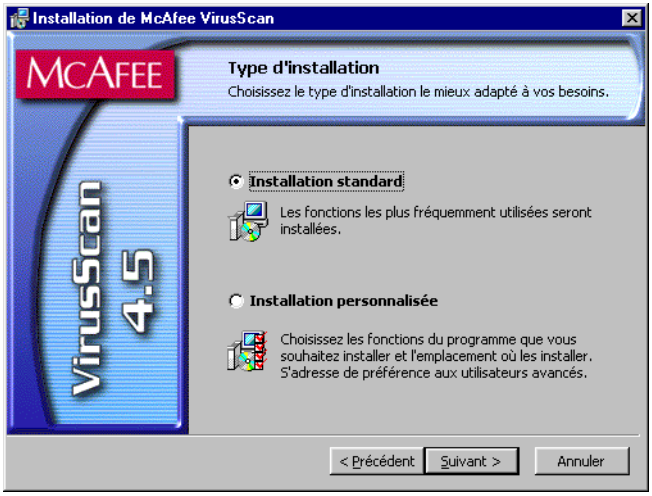

Figure 2-6. Écran Type d'installation

9. Choisissez le type d'installation que vous préférez. Vous avez le choix entre les options suivantes :

   - **Installation par défaut**. Cette option installe un jeu de composants de base qui inclut :

     – l'application VirusScan et des extensions d'application vous permettant de démarrer une opération d'analyse en faisant un clic droit sur n'importe quel objet de votre disque dur

     – la console VirusScan

     – le module Analyse système VShield

     – l'utilitaire de configuration cliente du Gestionnaire d'alerte

     – l'utilitaire Send Virus

     – l'utilitaire de création d'une disquette de secours

     – le moteur d'analyse de ligne de commande VirusScan

- **Installation personnalisée**. Cette option démarre avec les mêmes composants que l'installation par défaut, mais vous permet de choisir parmi les éléments supplémentaires suivants :
  - Les modules Analyse E-Mail, Analyse au téléchargement et Filtre Internet VShield.
  - L'utilitaire ScreenScan

Pour en savoir plus sur le rôle de chaque composant, reportez-vous à la section « Composants fournis avec VirusScan » à la page 34.

10. Choisissez l'option que vous préférez, puis cliquez sur **Suivant>** pour continuer.

    Si vous choisissez **Installation personnalisée**, l'écran qui apparaît dans la Figure 2-7 s'affiche. Sinon, passez à l'Étape 13 à la page 53 pour continuer l'installation.

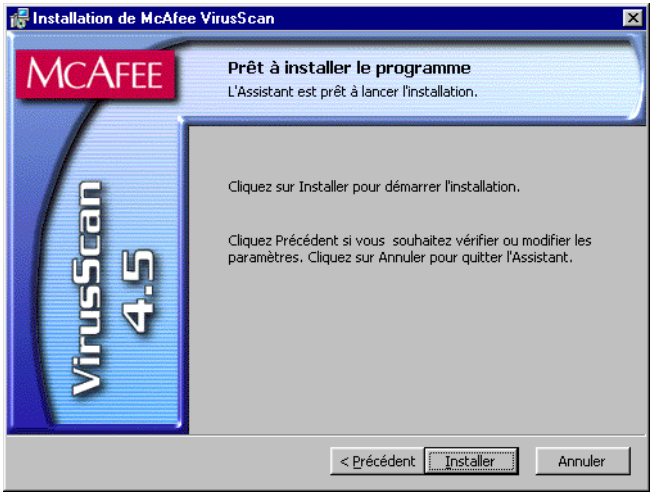

Figure 2-7. Écran Installation personnalisée

11. Sélectionnez les composants VirusScan que vous souhaitez installer. Vous pouvez :
    - Ajouter un composant à l'installation. Cliquez en regard d'un nom de composant, puis choisissez **Ce composant sera installé pour être exécuté à partir du disque dur local** dans le menu qui s'affiche. Pour ajouter un composant et tout module associé à ce composant, choisissez **Cette fonction et toutes ses sous-fonctions seront installées plutôt sur le lecteur de disque dur local**. Vous pouvez choisir cette option uniquement pour les composants qui ont des modules associés.

- Supprimer un composant de l'installation. Cliquez en regard d'un nom de composant, puis choisissez **Ce composant ne sera pas disponible** dans le menu qui s'affiche.

> **REMARQUE :** L'utilitaire d'installation de VirusScan ne prend pas en charge les autres options de ce menu. Vous ne pouvez pas installer des composants VirusScan pour être exécutés à partir d'un réseau et le logiciel VirusScan n'inclut pas des composants pouvant être installés en fonction des besoins.

Vous pouvez également spécifier un disque et un répertoire de destination différents pour l'installation. Cliquez sur **Changer**, puis recherchez le lecteur ou le répertoire de votre choix dans la boîte de dialogue qui s'affiche. Pour afficher un résumé de l'espace disque requis pour installer VirusScan par rapport à l'espace disponible sur votre disque, cliquez sur **Espace disque requis**. L'Assistant met en surbrillance les disques dont l'espace disponible est insuffisant.

12. Après avoir choisi les composants à installer, cliquez sur **Suivant>** pour continuer.

    Le programme d'installation affiche un écran indiquant qu'il est prêt pour commencer l'installation des fichiers (Figure 2-8).

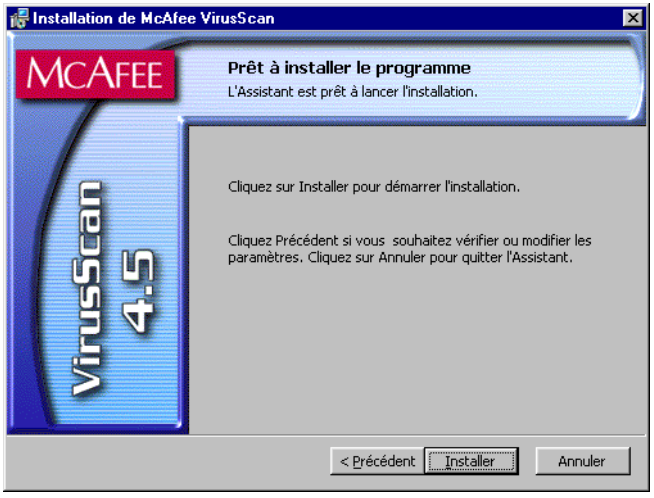

Figure 2-8. Écran Prêt pour l'installation

13. Cliquez sur **Installer** pour commencer la copie des fichiers sur votre disque dur. Sinon, cliquez sur **<Précédent** pour modifier les options d'installation choisies.

Le programme d'installation supprime d'abord toute version antérieure de VirusScan ou tout logiciel incompatible installés sur votre ordinateur, puis copie les fichiers du programme VirusScan sur votre disque dur. Une fois ces opérations terminées, le programme d'installation affiche un écran vous demandant si vous souhaitez configurer le produit que vous avez installé (Figure 2-9).

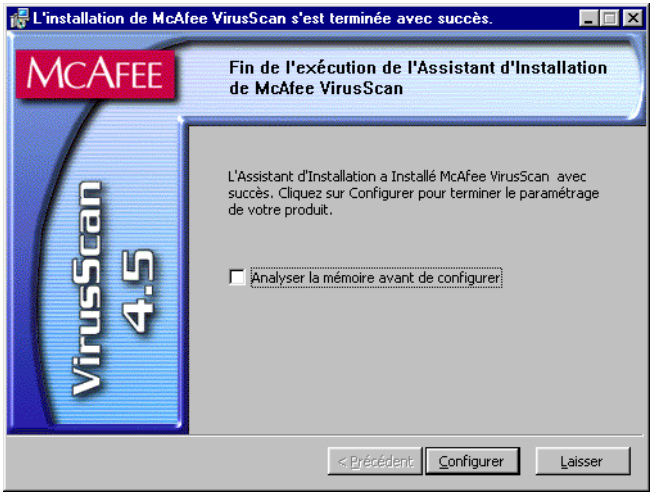

Figure 2-9. Écran Terminer l'installation

14. À ce stade, deux possibilités s'offrent à vous :

    - Terminer votre installation. Laissez la case **Analyser la mémoire avant la configuration** décochée, puis cliquez sur **Ignorer la configuration** pour terminer votre installation. Le programme d'installation vous demande si vous souhaitez démarrer le moteur d'analyse VShield et la console VirusScan immédiatement. Pour ce faire, cochez la case **Démarrer VirusScan**, puis cliquez sur **Terminer**. Votre logiciel VirusScan est prêt.

      REMARQUE : Si une version antérieure de VirusScan est installée sur votre ordinateur, vous devez réamorcer votre système pour démarrer le moteur d'analyse VShield. Le programme d'installation vous demande de redémarrer votre ordinateur.

    - Choisir les options de configuration pour votre installation. Avant de démarrer le moteur d'analyse VShield et la console VirusScan, vous pouvez choisir d'analyser votre système, de créer une disquette de secours ou de mettre à jour les fichiers de définition de virus.

Pour ce faire, cochez la case **Analyser la mémoire avant la configuration** pour que le programme d'installation démarre brièvement l'application VirusScan afin d'analyser votre mémoire système. Puis, cliquez sur **Configurer**.

Le programme d'installation lance l'application VirusScan afin de vérifier l'absence de virus dans la mémoire système avant de poursuivre. En cas d'infection, VirusScan vous en avertit et vous demande la démarche à suivre. Pour en savoir plus sur les choix qui s'offrent à vous, reportez-vous au Chapitre 3, « Suppression d'une infection dans votre système ». S'il n'y a pas de virus, VirusScan s'affiche brièvement pendant l'analyse du système, puis le programme d'installation affiche les deux premiers écrans de configuration (Figure 2-10).

Figure 2-10. Écran Configuration

15. Si votre ordinateur utilise Windows 95 ou Windows 98, vous pouvez choisir l'une des options de configuration présentées ci-dessous. Ces options sont les suivantes :

    - **Analyser la zone système au démarrage**. Cochez cette case pour que le programme d'installation ajoute les lignes suivantes dans votre fichier Windows AUTOEXEC.BAT :

      ```
      C:\PROGRA~1\NETWOR~1\MCAFEE~1\SCAN.EXE C:\
      @IF ERRORLEVEL 1 PAUSE
      ```

Cette instruction demande à votre système de lancer le moteur d'analyse de ligne de commande VirusScan lors du démarrage du système. Si le moteur d'analyse détecte un virus sur votre système, il interrompt son exécution pour vous permettre d'arrêter l'ordinateur et d'utiliser la disquette de secours VirusScan pour le redémarrer.

- **Créer une disquette de secours**. Cette option est sélectionnée par défaut. Elle demande au programme d'installation de quitter sa séquence normale afin de démarrer l'utilitaire de création de disquette de secours. L'utilitaire formate et copie un moteur d'analyse et des fichiers de support sur une disquette amorçable que vous pouvez utiliser pour démarrer le système dans un environnement exempt de virus. Vous pouvez également utiliser cette disquette pour analyser des portions du disque dur. Après avoir créé la disquette, l'utilitaire revient à la séquence d'installation normale. Décochez cette case pour ignorer la création d'une disquette de secours. Vous pouvez démarrer l'utilitaire à tout moment une fois l'installation terminée.
- **Exécuter l'analyse par défaut après l'installation**. Cette option est sélectionnée par défaut. Elle demande au programme d'installation d'achever l'installation, puis d'exécuter immédiatement l'application VirusScan afin d'analyser entièrement la partition de démarrage. Si l'application détecte un virus sur la partition, elle vous en avertit, sinon elle quitte sans afficher d'autres messages. Décochez cette case pour ignorer l'opération d'analyse.

REMARQUE : Si vous avez demandé au programme d'installation de supprimer les versions antérieures de VirusScan installées sur votre système, il exécute l'opération d'analyse *après* avoir redémarré votre ordinateur. L'application VirusScan s'affiche immédiatement après le démarrage du système.

Si votre ordinateur utilise Windows NT Workstation v4.0 ou Windows 2000 Professionnel, vous ne pouvez pas choisir **Analyser le secteur d'amorçage au démarrage**, mais vous pouvez choisir toutes les autres options proposées. Ni Windows NT Workstation ni Windows 2000 n'autorisent le logiciel à analyser ou à modifier les secteurs d'amorçage du disque dur ou les partitions d'amorçage (MBR). En outre, ces systèmes d'exploitation n'utilisent pas de fichier AUTOEXEC.BAT pour démarrer le système.

16. Une fois les options sélectionnées, cliquez sur **Suivant>** pour continuer.

    Si vous avez sélectionné l'option Créer une disquette de secours, l'Assistant de création de disquette de secours démarre immédiatement. Pour en savoir plus sur l'utilisation de cet utilitaire, reportez-vous à la section « Utilisation de l'utilitaire de création d'une disquette de secours » à la page 59.

    Après avoir créé la disquette de secours, l'utilitaire revient à ce stade de la séquence d'installation. Pour ignorer l'utilitaire de création de disquette de secours une fois démarré, cliquez sur **Annuler** dans le premier écran.

    Le programme d'installation affiche un deuxième écran de configuration vous permettant de mettre à jour les fichiers de définition de virus et de configurer l'utilitaire AutoUpdate pour les futures opérations de mise à jour (voir Figure 2-11).

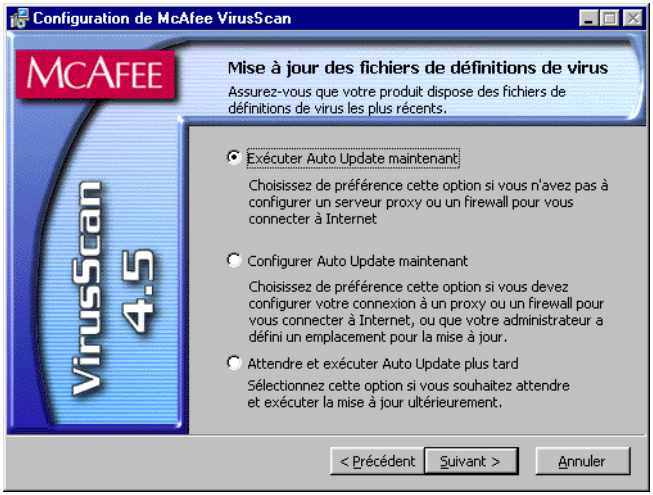

Figure 2-11. Écran Mettre à jour les fichiers de définition de virus

17. Choisissez l'option de mise à jour que vous préférez. Vous pouvez :

    - **Exécuter AutoUpdate maintenant**. Cette option utilise les options de configuration de mise à jour automatique par défaut pour se connecter directement au site Web de McAfee et télécharger les dernières mises à jour des fichiers .DAT incrémentiels. Sélectionnez cette option si votre entreprise n'a pas désigné un emplacement de votre réseau comme site de mise à jour, et si vous n'avez pas besoin de configurer des paramètres de serveur proxy ou de pare-feu. Ceci garantit l'utilisation de fichiers actualisés dans toute opération d'analyse que vous exécutez.

- **Configurer AutoUpdate maintenant**. Cette option ouvre la boîte de dialogue Actualisation automatique, où vous pouvez ajouter et configurer un site de mise à jour à partir duquel vous allez télécharger les nouveaux fichiers. Sélectionnez cette option si votre entreprise a désigné un serveur pour les mises à jour des fichiers .DAT au sein de votre réseau, ou si vous souhaitez modifier la façon dont votre ordinateur se connecte au site Web de McAfee ; modifier les paramètres de pare-feu ou de serveur proxy, par exemple.

  Pour en savoir plus sur la configuration de l'utilitaire AutoUpdate, reportez-vous à la section « Configuration de l'utilitaire AutoUpdate » à la page 278.

- **Attendre et exécuter AutoUpdate plus tard**. Cette option ignore l'opération de mise à jour automatique. Vous pouvez configurer et planifier une tâche de mise à jour automatique pour télécharger de nouveaux fichiers .DAT ultérieurement. Pour en savoir plus sur la planification d'une tâche, reportez-vous à la section Chapitre 6, « Création et configuration des tâches planifiées ».

18. Une fois les options sélectionnées, cliquez sur **Suivant>**.

    Si vous choisissez d'exécuter une opération AutoUpdate immédiatement, l'utilitaire se connecte au site Web de McAfee pour télécharger les nouveaux fichiers .DAT incrémentiels. Une fois les fichiers téléchargés, le programme d'installation reprend son exécution.

    Si vous choisissez de configurer l'utilitaire AutoUpdate, la boîte de dialogue Actualisation automatique s'affiche. Sélectionnez vos options de configuration, puis cliquez sur **Mettre à jour maintenant** pour démarrer immédiatement une opération de mise à jour, ou cliquez sur **OK** pour enregistrer les options choisies.

    Le programme d'installation affiche ensuite son dernier écran et vous demande si vous souhaitez démarrer le moteur d'analyse VShield et la console VirusScan immédiatement (Figure 2-12 à la page 59).

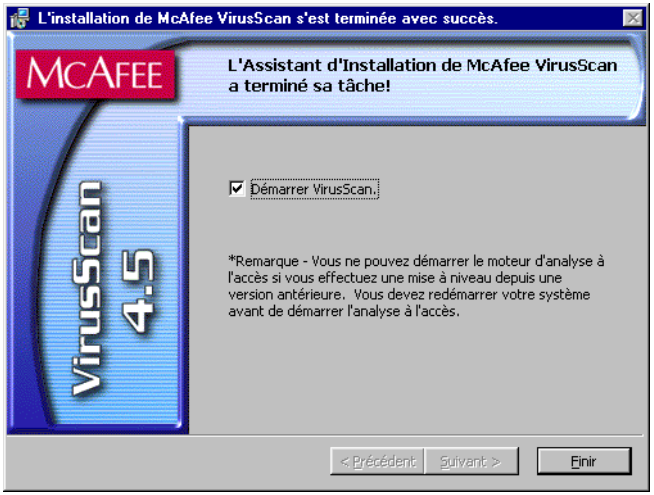

Figure 2-12. Écran Installation terminée

19. Pour ce faire, cochez la case **Démarrer VirusScan**, puis cliquez sur **Terminer**. Les « écrans de démarrage » du logiciel VirusScan s'affichent et les icônes du moteur d'analyse VShield et de la console VirusScan apparaissent dans la barre d'état système Windows. Votre logiciel est prêt.

❑ **REMARQUE :** Si une version antérieure de VirusScan est installée sur votre ordinateur, vous devez réamorcer votre système pour démarrer le moteur d'analyse VShield. Le programme d'installation vous demande de redémarrer votre ordinateur.

Utilisation de l'utilitaire de création d'une disquette de secours

Si vous avez choisi de créer une disquette de secours pendant l'installation, le programme d'installation démarre l'Assistant de la disquette de secours au milieu de l'installation du logiciel VirusScan puis, une fois la disquette créée, il reprend la séquence d'installation. Pour en savoir plus sur la création d'une disquette de secours, commencez par l'Étape 1 à la page 61. Vous pouvez également démarrer l'Assistant de la disquette de secours à n'importe quel moment après l'installation du logiciel VirusScan.

REMARQUE : Network Associates vous recommande vivement de créer une disquette de secours pendant la procédure d'installation, mais après avoir analysé le système à l'aide de VirusScan. Si VirusScan détecte un virus sur votre système, *ne créez pas* de disquette de secours sur l'ordinateur infecté.

La disquette de secours que vous créez inclut le fichier BOOTSCAN.EXE, qui est un moteur d'analyse de ligne de commande spécialisé, de petite taille, conçu pour analyser les zones systèmes et les partitions d'amorçage (MBR) de votre disque dur. Le fichier BOOTSCAN.EXE travaille avec un ensemble de fichiers .DAT spécialisés ayant pour but de traquer les virus de zone système. Si vous avez déjà installé le logiciel VirusScan avec les options par défaut, vous trouverez ces fichiers .DAT sur votre disque dur, à l'emplacement suivant :

C:\Program Files\Common Files\Network Associates\VirusScan Engine\4.0.xx

Les fichiers .DAT spéciaux portent les noms suivants :

- EMCLEAN.DAT
- EMNAMES.DAT
- EMSCAN.DAT

McAffee met à jour régulièrement ces fichiers .DAT afin de détecter les nouveaux virus de zone système. Vous pouvez télécharger les fichiers .DAT de secours actualisés depuis l'emplacement suivant :

http://www.nai.com/asp_set/anti_virus/avert/tools.asp

REMARQUE : McAfee vous recommande de télécharger les nouveaux fichiers .DAT de secours directement sur une disquette que vous venez de formater afin de réduire les risques d'infection.

Dans la mesure où l'Assistant renomme les fichiers et les prépare pour leur utilisation lors de la création de la disquette, vous ne devez pas copier ces fichiers directement sur une disquette de secours que vous créez vous-même. Utilisez l'Assistant de la disquette de secours pour préparer votre disquette de secours.

Pour démarrer l'Assistant après l'installation, cliquez sur **Démarrer** dans la barre des tâches Windows, pointez sur **Programmes**, puis sur **Network Associates**. Sélectionnez ensuite **Créer une disquette de secours**.

L'écran d'accueil de l'Assistant de la disquette de secours s'affiche (Figure 2-13 à la page 61).

Figure 2-13. Écran d'accueil de l'Assistant de la disquette de secours

1. Cliquez sur **Suivant>** pour continuer.

   L'écran suivant de l'Assistant s'affiche (Figure 2-14).

Figure 2-14. Deuxième écran de la disquette de secours

Si votre ordinateur fonctionne avec Windows NT Workstation ou Windows 2000 Professionnel, l'Assistant vous informe qu'il va formater votre disquette de secours avec le NAI-OS.

Vous devez utiliser ces fichiers de système d'exploitation propriétaires pour créer votre disquette de secours, car les fichiers système de Windows NT Workstation v4.0 et de Windows 2000 Professionnel ne rentrent pas en seule disquette.

Si votre ordinateur fonctionne avec Windows 95 ou Windows 98, l'Assistant vous offre la possibilité de formater votre disquette de secours avec le NAI-OS ou avec des fichiers de démarrage Windows.

2. Si l'Assistant vous le permet, choisissez les fichiers de système d'exploitation que vous souhaitez utiliser, puis cliquez sur **Suivant>** pour continuer. L'Assistant affiche ensuite un écran qui varie en fonction du système d'exploitation que vous choisissez :

   - Si vous décidez de formater votre disquette avec le NAI-OS, l'Assistant affiche un écran d'information (Figure 2-15).

Figure 2-15. Écran d'information de la disquette de secours

Pour continuer, procédez comme suit :

a. Insérez une disquette non verrouillée et non formatée de 1,44 Mo dans votre lecteur, puis cliquez sur **Suivant>**.

   L'Assistant de la disquette de secours copie les fichiers requis depuis une image disque stockée dans le répertoire du programme VirusScan. Pendant la copie des fichiers, il affiche leur progression dans un écran.

b. Cliquez sur **Terminer** pour quitter l'Assistant une fois la disquette créée.

Retirez ensuite la disquette du lecteur, verrouillez-la, collez une étiquette intitulée *Disquette de secours démarrage McAfee* et placez-la en lieu sûr.

- Si vous décidez de formater votre disquette avec les fichiers système Windows, l'Assistant affiche un écran vous permettant de formater la disquette (voir Figure 2-16 à la page 63).

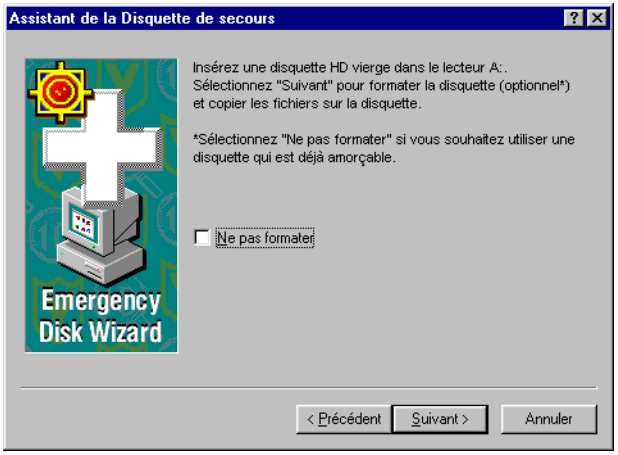

Figure 2-16. Troisième écran de la disquette de secours

Vous avez le choix entre les options suivantes :

- Si vous disposez d'une disquette formatée et *exempte de virus*, contenant uniquement des fichiers système DOS ou Windows, insérez-la dans le lecteur. Cochez ensuite la case **Ne pas formater**, puis cliquez sur **Suivant>** pour continuer.

  Vous indiquez ainsi à l'Assistant de la disquette de secours de ne copier sur la disquette que le composant Ligne de commande de VirusScan, les fichiers .DAT de secours, et les fichiers de support. Passez à l'Étape 3 à la page 64 pour continuer.

- Si vous ne possédez *pas* de disquette formatée et parfaitement saine, abritant les fichiers système DOS ou Windows, vous devez en créer une afin d'utiliser la disquette de secours pour démarrer l'ordinateur. Procédez comme suit :

  a. Insérez une disquette non verrouillée et non formatée dans votre lecteur. McAfee vous recommande d'utiliser une disquette toute neuve non formatée afin d'éviter tout risque d'infection de votre disquette de secours.

  b. Assurez-vous que la case **Ne pas formater** n'est pas cochée.

  c. Cliquez sur **Suivant>**.

     La boîte de dialogue de formatage de disquette Windows s'affiche (voir Figure 2-17 à la page 64).

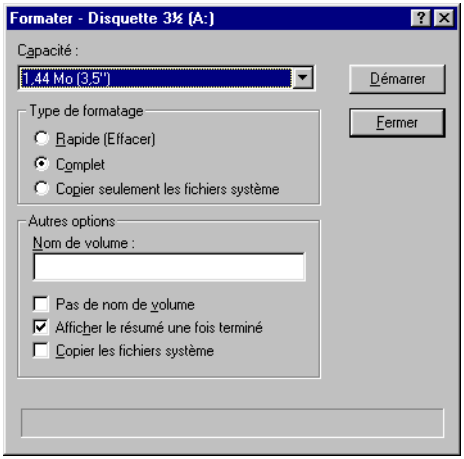

Figure 2-17. Boîte de dialogue de formatage Windows

d. Assurez-vous que la case **Complet** est cochée dans la zone Type de format, de même que la case **Copier les fichiers système** dans la zone Autres options. Cliquez ensuite sur **Démarrer**.

   Windows formate la disquette et y copie les fichiers système nécessaires au démarrage de l'ordinateur.

e. Cliquez sur **Fermer** lorsque Windows a terminé de formater votre disquette, puis cliquez à nouveau sur **Fermer** pour revenir à l'écran Disquette de secours.

3. Cliquez sur **Suivant>** pour continuer. Le programme d'installation analyse la disquette que vous venez de formater à la recherche d'éventuels virus(Figure 2-18).

Figure 2-18. Analyse de la disquette de secours

Si VirusScan ne détecte aucun virus lors de l'analyse, le programme d'installation copie immédiatement le fichier BOOTSCAN.EXE et ses fichiers de support sur la disquette que vous avez créée. Si VirusScan *détecte* un virus, quittez immédiatement le programme d'installation. Reportez-vous à la section voir « Si vous suspectez la présence d'un virus... » à la page 71 pour connaître la démarche à suivre.

4. Lorsque l'Assistant termine de copier les fichiers de la disquette de secours, il affiche son écran final (Figure 2-19).

Figure 2-19. Écran final de l'Assistant de la disquette de secours

5. Cliquez sur **Terminer** pour fermer l'Assistant. Retirez ensuite la nouvelle disquette de secours de votre lecteur, collez-lui une étiquette, verrouillez-la et placez-la en lieu sûr.

> **REMARQUE :** Une disquette verrouillée ou protégée en écriture présente deux orifices près du bord situé à l'opposé de la partie métallique de la disquette. Si les deux orifices ne sont pas visibles, recherchez un taquet en plastique dans l'un des coins de la disquette et faites-le glisser jusqu'à ce qu'il soit verrouillé laissant l'orifice ouvert.

Circonstances qui exigent le redémarrage de votre ordinateur

Dans certains cas, vous pouvez installer et utiliser cette version de VirusScan immédiatement, sans avoir à redémarrer votre ordinateur. Dans d'autres cas, Microsoft Installer (MSI) doit parfois remplacer ou initialiser certains fichiers, ou vous pouvez être amené à supprimer certains fichiers des anciennes installations de McAfee pour que le logiciel VirusScan puisse fonctionner correctement. Ces conditions peuvent également varier selon la plate-forme Windows prise en charge.

Dans ces cas, vous devez redémarrer votre ordinateur au cours de l'installation, souvent pour installer les fichiers MSI, ou une fois l'installation terminée.

Pour savoir dans quelles circonstances vous devez redémarrer votre ordinateur, reportez-vous au Table 2-1.

Table 2-1. Circonstances qui exigent le redémarrage du système

Circonstance	Windows 95 et Windows 98	Windows NT et Windows 2000
Installation sur un ordinateur ne possédant pas de version antérieure de VirusScan ni de logiciel incompatible	Redémarrage non requis, sauf si vous avez installé Novell Client32 pour NetWare, auquel cas le redémarrage devient obligatoire	Redémarrage requis
Installation sur un ordinateur possédant une version antérieure de VirusScan	Redémarrage requis	Redémarrage requis

Table 2-1. Circonstances qui exigent le redémarrage du système

Circonstance	Windows 95 et Windows 98	Windows NT et Windows 2000
Installation sur un ordinateur possédant un logiciel incompatible	Redémarrage non requis, mais le programme d'installation vous demande si vous souhaitez redémarrer votre ordinateur. Vous pouvez cliquer sur **Non** en toute sécurité.	Redémarrage non requis, mais le programme d'installation vous demande si vous souhaitez redémarrer votre ordinateur. Vous pouvez cliquer sur **Non** en toute sécurité.
Installation sur un ordinateur possédant Microsoft Installer (MSI) v1.0 **REMARQUE** : Microsoft Office 2000 installe cette version de MSI	Redémarrage requis après l'installation des fichiers MSI et avant la poursuite de l'installation	Redémarrage requis après l'installation des fichiers MSI et avant la poursuite de l'installation
Installation sur un ordinateur possédant Microsoft Installer v1.1	Redémarrage non requis, sauf pour les systèmes Windows 98 Second Edition, ou en cas d'utilisation de certains pilotes ou fichiers .DLL	Redémarrage non requis
Mises à jour des fichiers .DAT	Redémarrage non requis	Redémarrage non requis
Mise à jour du moteur d'analyse via l'utilitaire SuperDAT de McAfee	Redémarrage non requis	Redémarrage non requis

Test de votre installation

Une fois installé, VirusScan peut rechercher les fichiers infectés dans votre système. Vous pouvez vérifier que VirusScan est correctement installé et que le logiciel est en mesure de détecter des virus en appliquant le test EICAR, fruit de la volonté des principaux fabricants d'antivirus en Europe d'offrir à leurs clients la possibilité de tester n'importe quelle installation antivirus.

Pour tester votre installation, procédez comme suit :

1. Ouvrez un éditeur de texte Windows standard, tel que le Bloc-notes, et tapez le texte suivant, sur *une seule ligne, sans espaces et sans retours à la ligne* :

   ```
   X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
   ```

REMARQUE : La chaîne de caractères ci-dessus doit constituer *une seule ligne* dans la fenêtre de votre éditeur de texte; veillez donc à maximiser la fenêtre et à supprimer les retours à la ligne. Aussi, vérifiez que vous avez bien tapé la lettre O et non le chiffre 0, dans la chaîne « X5O... », au début du message test.

Si vous consultez ce guide sur votre ordinateur, vous pouvez copier la ligne directement à partir du fichier .PDF Acrobat vers le Bloc-notes. Vous pouvez également copier cette chaîne de texte directement à partir de la section « Test de votre installation » du fichier README.TXT, qui se trouve dans le répertoire du programme VirusScan. Si vous copiez la ligne à partir de l'une de ces sources, pensez à supprimer les retours à la ligne et les espaces.

2. Enregistrez le fichier sous le nom EICAR.COM. Sa taille sera de 69 ou 70 octets.
3. Lancez VirusScan et demandez-lui d'analyser le répertoire contenant le fichier EICAR.COM. Lorsque VirusScan analysera ce fichier, il indiquera qu'il a détecté le virus EICAR-STANDARD-AV-TEST-FILE.

IMPORTANT : Ce fichier *n'est pas un virus*. Il ne peut en aucun cas se propager ou infecter d'autres fichiers, ni endommager votre système de quelque façon que ce soit. Lorsque vous aurez terminé votre test, supprimez ce fichier afin que les utilisateurs non avertis n'en soient pas inutilement alarmés.

Modification ou suppression de VirusScan

La version de Microsoft Windows Installer utilisée par le logiciel VirusScan inclut également une méthode standard de modification et de suppression de votre installation de VirusScan.

Pour modifier ou supprimer le logiciel VirusScan, procédez comme suit :

1. Cliquez sur **Démarrer** dans la barre des tâches Windows, pointez sur **Paramètres**, puis choisissez **Panneau de configuration**.
2. Double-cliquez sur l'icône **Ajout/Suppression de programmes** du Panneau de configuration.
3. Dans la boîte de dialogue Ajout / Suppression de programmes, choisissez **McAfee VirusScan v4.5.0** dans la liste, puis cliquez sur **Ajouter/ Supprimer**.

Le programme d'installation démarre et affiche le premier écran de l'assistant de Maintenance (Figure 2-20 à la page 69).

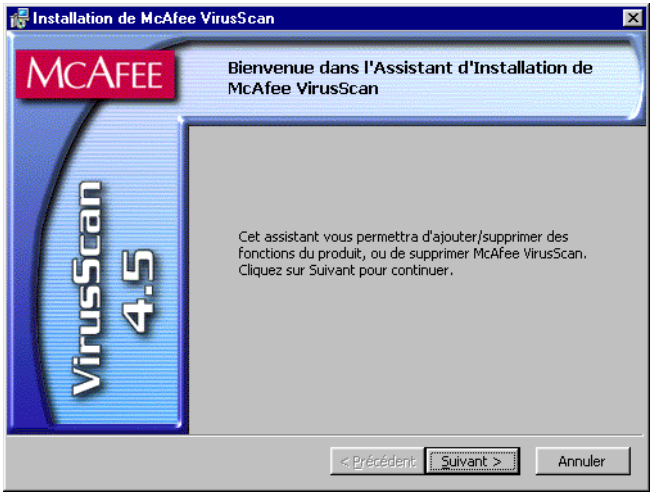

Figure 2-20. Premier écran de maintenance

4. Cliquez sur **Suivant>** pour continuer.

   Le programme d'installation affiche l'écran Maintenance du programme.

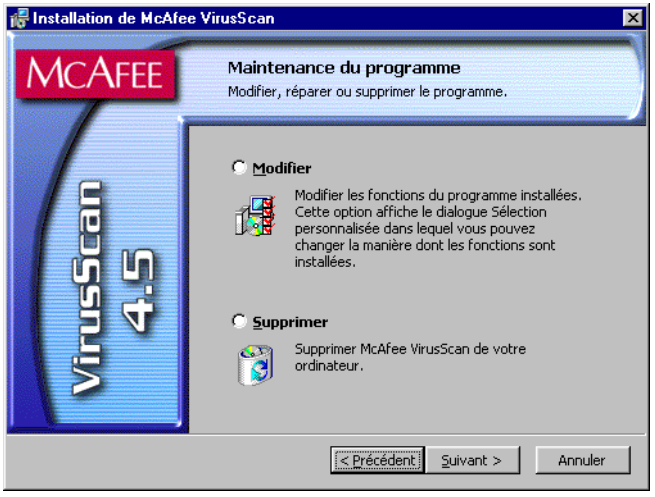

Figure 2-21. Écran Maintenance du programme

5. Vous pouvez modifier les composants VirusScan ou supprimer complètement le logiciel VirusScan de votre système. Vous avez le choix entre les options suivantes :

   - **Modifier.** Sélectionnez cette option pour ajouter ou supprimer des composants VirusScan individuels. Le programme d'installation affiche l'écran Personnalisé (Figure 2-7 à la page 52). Commencez par l'Étape 11 à la page 52 pour choisir les composants que vous souhaitez ajouter ou supprimer.

     ☐ **REMARQUE :** Cet écran diffère de celui qui apparaît à la page 52: Il ne vous permet pas de changer le répertoire du programme VirusScan et n'affiche pas non plus les statistiques sur l'utilisation du disque. Pour installer VirusScan dans un répertoire différent ou sur un autre lecteur, vous devez d'abord supprimer le logiciel, puis le réinstaller.

   - **Supprimer.** Sélectionnez cette option pour supprimer complètement le logiciel VirusScan de votre ordinateur. Le programme d'installation vous demande de confirmer la suppression du logiciel de votre ordinateur (Figure 2-22).

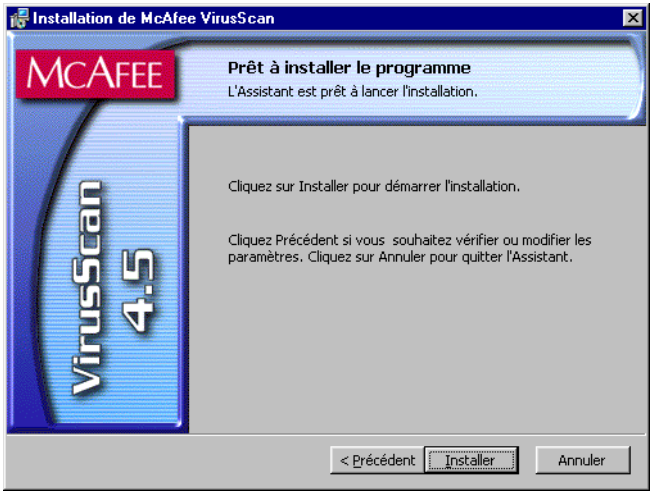

Figure 2-22. Écran Supprimer le programme

Cliquez sur **Supprimer**. Pendant qu'il supprime VirusScan de votre système, le programme d'installation affiche des informations sur la progression de la tâche. Une fois la suppression terminée, cliquez sur **Terminer** pour fermer l'écran de l'Assistant.

Suppression d'une infection dans votre système 3

Si vous suspectez la présence d'un virus...

Tout d'abord, ne paniquez pas ! Bien que *la plupart* des virus susceptibles d'infecter votre machine ne soient pas inoffensifs, il est peu probable qu'ils détruisent des données, qu'ils vous jouent des tours ou qu'ils rendent votre ordinateur inutilisable. Même les virus relativement rares programmés pour réaliser une fonction dommageable ne se déclenchent qu'en réponse à un événement particulier. Dans la plupart des cas, et à moins que vous n'ayez la preuve du déclenchement d'une fonction malveillante, vous avez le temps de prendre les mesures qui s'imposent. Toutefois, la seule présence de ces petits fragments de codes indésirables pouvant enrayer le fonctionnement normal de l'ordinateur, consommer des ressources système ou avoir d'autres effets importuns, il est essentiel de les supprimer dès que vous détectez leur présence.

Par ailleurs, il est important de garder à l'esprit qu'un fonctionnement inhabituel de l'ordinateur, un blocage système inexpliqué ou d'autres événements imprévisibles peuvent avoir d'autres causes que l'infection virale. Si de telles occurrences vous font suspecter la présence d'un virus sur votre ordinateur, l'analyse du système ne produira peut-être pas les résultats escomptés. Cependant, il vous permettra d'éliminer le virus comme cause possible du problème.

La solution la plus sûre consiste à installer le logiciel VirusScan et à exécuter l'analyse complète du système.

Lors de l'installation de VirusScan, le programme d'installation démarre l'application VirusScan et examine la mémoire système et la zone système du disque dur pour vérifier l'absence de virus et éliminer tout risque d'infection de ses propres fichiers. Si l'application ne détecte pas de virus, continuez l'installation, puis exécutez une analyse complète du système dès le redémarrage de l'ordinateur. Les virus responsables de l'infection des fichiers, qui ne se chargent pas dans la mémoire de votre ordinateur ou qui ne se cachent pas dans les zones système de votre disque dur, peuvent toujours se cacher ailleurs dans votre système. Pour plus d'informations sur l'analyse du système pendant la procédure d'installation, reportez-vous au Chapitre 2, « Installation du logiciel VirusScan »,. Pour en savoir plus sur la procédure d'analyse système, reportez-vous au Chapitre 5, « Utilisation de l'application VirusScan »,.

Si l'application VirusScan détecte un virus pendant son installation, vous devez le supprimer avant de poursuivre la procédure. Pour ce faire, suivez les instructions présentées à la page 72.

IMPORTANT : Afin de garantir la sécurité maximale du système, vous suivrez également ces mêmes instructions en cas de détection d'un virus dans la mémoire de l'ordinateur, après l'installation de VirusScan.

Si le logiciel VirusScan a découvert une infection durant l'installation, procédez comme suit :

1. Quittez immédiatement le programme d'installation et éteignez l'ordinateur.

   Veillez à mettre l'ordinateur entièrement hors tension. Ne réamorcez *pas* le système à l'aide des touches CTRL+ALT+SUPPR ou du bouton de réinitialisation (Reset) de votre ordinateur ; certains virus risquent en effet de ne pas être affectés par ce type de démarrage à chaud.

2. Si vous avez créé une disquette de secours VirusScan au cours de l'installation ou si elle a été livrée avec votre exemplaire de VirusScan, verrouillez la disquette et insérez-la dans le lecteur.

   REMARQUE : Si votre exemplaire de VirusScan ne comporte pas de disquette de secours ou si vous n'avez pas réussi à la créer au cours de l'installation, vous devez en créer une sur un ordinateur *non infecté*. Passez sur un poste sain et suivez les instructions présentées dans la section « Utilisation de l'utilitaire de création d'une disquette de secours » à la page 59.

   ---

3. Attendez au moins 15 secondes, puis redémarrez votre ordinateur.

   REMARQUE : Si le BIOS de votre ordinateur est configuré pour rechercher son code d'amorçage d'abord sur le lecteur C:, vous devez modifier les paramètres du BIOS afin que l'ordinateur commence la recherche par le lecteur A: ou le lecteur B: Pour en savoir plus sur la configuration des paramètres du BIOS, consultez la documentation de votre matériel.

   Après avoir démarré votre ordinateur, la disquette de secours exécute un fichier de commande qui vous guide à travers une procédure d'analyse d'urgence. Le fichier de commande vous demande si vous avez mis votre ordinateur hors tension.

4. Tapez y pour continuer, puis passez à l'Étape 7. Dans le cas contraire, tapez n, mettez l'ordinateur hors tension, puis recommencez la procédure.

   Le fichier de commande vous informe qu'il va démarrer une opération d'analyse.

5. Lisez les informations qui s'affichent à l'écran, puis appuyez sur une touche quelconque de votre clavier pour continuer.

   La disquette de secours chargera les fichiers requis pour analyser la mémoire de votre ordinateur. Si votre ordinateur dispose d'une mémoire étendue, la disquette de secours y chargera ses fichiers de base de données afin d'accélérer l'analyse.

   BOOTSCAN.EXE, le moteur d'analyse de ligne de commande livré avec la disquette de secours, effectuera quatre opérations d'analyse afin d'examiner les zones système du disque dur, la partition d'amorçage (MBR), les répertoires système, les fichiers programme et d'autres éventuels points d'infection, et ceci sur chaque disque dur de votre ordinateur local.

   ❑ **REMARQUE :** McAfee vous recommande vivement de ne pas interrompre le moteur d'analyse BOOTSCAN.EXE pendant l'analyse. La disquette de secours ne détecte pas les virus de macro, les virus de script, ni les programmes de cheval de Troie, mais détecte les virus de fichier et de zone système courants.

   Si BOOTSCAN.EXE détecte un virus, il tentera de nettoyer le fichier infecté. S'il n'y parvient pas, il refusera l'accès au fichier et continuera l'opération d'analyse. Une fois les analyses terminées, BOOTSCAN.EXE affiche un résumé des actions effectuées sur chaque disque dur. Ce rapport comporte les informations suivantes :

   - Nombre de fichiers analysés
   - Nombre de fichiers nettoyés ou non infectés sur le total de fichiers analysés
   - Nombre de fichiers susceptibles d'être infectés
   - Nombre de fichiers nettoyés sur le total de fichiers susceptibles d'être infectés
   - Nombre de fichiers de zone système et MBR analysés
   - Nombre de fichiers de zone système et MBR susceptibles d'être infectés

   En cas d'infection, le moteur d'analyse émet un signal sonore et affiche le nom et l'emplacement du virus.

6. Une fois l'analyse du disque dur terminée, retirez la disquette de secours du lecteur et mettez à nouveau l'ordinateur hors tension.

7. Au terme de l'analyse du système effectuée par BOOTSCAN.EXE, deux solutions s'offrent à vous :

   - **Reprendre votre travail.** Si BOOTSCAN.EXE n'a pas détecté de virus ou s'il a nettoyé tous les fichiers infectés qu'il a détectés, retirez la disquette de secours du lecteur et redémarrez normalement l'ordinateur. Si vous avez interrompu l'installation du logiciel VirusScan suite à la découverte d'une infection, vous pouvez à présent la reprendre.

   - **Tenter de nettoyer ou de supprimer manuellement les fichiers infectés.** Si BOOTSCAN.EXE ne parvient pas à supprimer un virus détecté, il identifiera les fichiers infectés et vous dira qu'il est incapable de les nettoyer ou qu'il ne dispose pas d'un outil de suppression à jour pour ce virus.

   L'étape suivante consiste à localiser et à supprimer manuellement le ou les fichiers infectés. Vous devrez ensuite restaurer les fichiers supprimés à partir d'une sauvegarde. Veillez à analyser également vos fichiers de sauvegarde pour vous assurer qu'ils sont sains. Pensez également à utiliser l'application VirusScan dès que possible pour effectuer une analyse complète du système afin de vous assurer qu'il est exempt de tout virus.

Quand faut-il lancer une recherche de virus ?

Si vous souhaitez conserver un environnement informatique sûr, il faut rechercher les virus éventuels régulièrement. Une analyse « régulière » peut tout aussi bien signifier une fois par mois comme plusieurs fois par jour. Tout dépend de la fréquence des échanges de disquettes entre utilisateurs, du partage de fichiers sur votre réseau local ou de l'interaction avec d'autres ordinateurs via Internet. D'autres bonnes habitudes sont à adopter, comme une analyse juste avant la sauvegarde des données, avant l'installation d'un nouveau logiciel ou d'un logiciel amélioré - notamment les logiciels téléchargés depuis d'autres ordinateurs - et lors du démarrage ou de la fermeture de votre ordinateur tous les jours. Utilisez le moteur d'analyse VShield pour examiner la mémoire de votre ordinateur et conservez un niveau de vigilance permanent entre chaque analyse. Ces précautions protégeront l'intégrité de votre système dans la plupart des cas.

Si vous vous connectez fréquemment à Internet ou téléchargez souvent des fichiers, il est souhaitable d'effectuer des analyses supplémentaires lors d'événements particuliers. Utilisez la console VirusScan pour planifier une série de tâches d'analyse afin de vérifier votre système dès qu'il est susceptible d'être infecté par un virus, notamment

- lors de chaque insertion d'une disquette dans votre lecteur de disquettes
- lors de chaque démarrage d'une application ou ouverture d'un fichier
- lorsque vous connectez ou reliez une unité de réseau à votre système

Cependant, si vos fichiers de définition de virus (.DAT) ne sont pas à jour, il se peut que certains nouveaux virus échappent même aux analyses les plus poussées. Avec l'achat du logiciel VirusScan sont fournies gratuitement des mises à jour de virus pendant la durée de vie du produit, de façon à pouvoir effectuer de fréquentes mises à jour pour être au point. La console VirusScan inclut les tâches de mise à jour automatique et de mise à niveau automatique, vous permettant de mettre à jour les fichiers .DAT et le moteur d'analyse VirusScan. Pour en savoir plus sur la mise à jour du logiciel, reportez-vous au Chapitre 7, « Mise à jour et mise à niveau du logiciel VirusScan »..

Comment éliminer l'hypothèse de l'infection virale ?

Tout au long de leur courte existence, les ordinateurs individuels ont évolué pour devenir des machines hautement perfectionnées en mesure d'exécuter des logiciels toujours plus complexes. Même les défenseurs les plus perspicaces des premiers PC n'auraient jamais pu imaginer le travail accompli par les techniciens, les scientifiques et autres chercheurs grâce à la vitesse, la flexibilité et la puissance du PC moderne. Mais cette puissance a un prix : les conflits entre matériel et logiciel se multiplient, les systèmes d'exploitation et d'application tombent en panne et des centaines d'autres problèmes peuvent surgir là où on les attend le moins. Dans certains cas, ces incidents s'assimilent un peu aux effets provoqués lors d'une infection virale à capacité destructrice. D'autres incidents semblent défier toute explication ou diagnostic, et les utilisateurs frustrés s'en prennent alors aux virus, peut-être en dernier recours.

Les virus laissent des traces, c'est pourquoi vous pouvez rapidement et facilement éliminer l'hypothèse de l'infection virale comme cause de la panne de votre ordinateur. Si vous exécutez une analyse VirusScan complète, toutes les variantes des virus connus susceptibles d'infecter votre ordinateur seront découvertes, ainsi que de nombreuses autres qui n'ont pas de noms connus ou de comportement spécifique. Cela ne vous aidera pas à résoudre votre problème s'il est réellement dû à un conflit d'interruption, mais vous permettra d'éliminer l'une des causes possibles. Sachant cela, vous pouvez tenter de dépanner votre système à l'aide d'un utilitaire de diagnostic de système complet.

En revanche, les programmes semblables à des virus, les canulars et les véritables infractions de sécurité entraînent une confusion encore plus grande. Les logiciels antivirus ne sont tout simplement pas en mesure de détecter ou de combattre les agents destructeurs tels que les programmes Cheval de Troie, qui ne s'étaient jamais manifestés auparavant, ou encore l'impression qu'il existe un virus alors que ce n'est pas le cas.

Le meilleur moyen de savoir si votre panne est due à une attaque virale est d'effectuer une analyse complète et d'en examiner les résultats. Si l'application VirusScan ne détecte aucune infection virale, il est peu probable que votre panne provienne d'un virus - cherchez alors d'autres causes possibles aux symptômes que vous avez identifiés. De plus, dans le cas très rare où l'application VirusScan n'est pas en mesure d'identifier un virus de macro ou tout autre type de virus infiltré dans votre système, les risques de voir cette infection affecter gravement votre système sont relativement faibles. Vous pouvez cependant vous fier aux chercheurs de McAfee pour identifier et isoler le virus, puis mettre à jour le logiciel VirusScan immédiatement afin de détecter et si possible supprimer le virus la prochaine fois que vous le rencontrerez. Pour savoir comment permettre aux chercheurs de vous aider, reportez-vous à la section « Signalement de nouveaux virus à incorporer dans les mises à jour de fichiers de données antivirus » à la page xxiii.

Mieux comprendre les fausses alertes

On appelle fausse alerte la détection d'un virus dans un fichier ou dans la mémoire quand bien même ce virus n'a aucune réalité physique. Les fausses alertes ont d'autant plus de chance de se produire que vous avez installé plusieurs logiciels de détection de virus sur votre ordinateur. En effet, certains programmes antivirus n'appliquent aucune protection lorsqu'ils stockent les signatures codées dans la mémoire.

Tout virus détecté par VirusScan doit toujours être considéré comme réel et dangereux, et il convient de prendre les mesures nécessaires pour le supprimer du système. Si, néanmoins, vous pensez que le composant VirusScan a généré une fausse alerte—un virus a été détecté dans un fichier que vous utilisez sans problème depuis de nombreuses années, par exemple—consultez la liste ci-dessous pour connaître l'origine possible de cette fausse alerte avant de contacter le support technique de Network Associates :

- **Plusieurs programmes antivirus sont exécutés simultanément.** Les composants de VirusScan risquent alors de détecter des signatures codées non protégées utilisées par un autre programme et de les signaler comme virus. Pour éviter ce type de situation, configurez l'ordinateur pour qu'un seul de ces programmes soit exécuté, puis arrêtez l'ordinateur et mettez-le hors tension. Patientez quelques secondes pour laisser le temps au système de supprimer de la mémoire toutes les signatures codées des autres programmes antivirus, puis rallumez l'ordinateur.

- **Votre ordinateur est doté d'une puce BIOS avec une fonction antivirus.** Certaines puces BIOS comportent une fonction antivirus pouvant provoquer une fausse alerte lors de l'exécution du logiciel VirusScan. Consultez le guide d'utilisateur de l'ordinateur pour vous familiariser avec cette fonction antivirus, et pour la désactiver, si nécessaire.
- **Vous possédez un ancien ordinateur de la marque Hewlett-Packard ou Zenith PC.** Certains anciens modèles d'ordinateur de ces deux constructeurs modifient la zone système chaque fois que le système est amorcé. Les composants de VirusScan risquent de détecter ces modifications comme une infection probable, même si aucun virus n'est présent sur le système. Consultez le guide d'utilisateur de votre ordinateur pour savoir s'il dispose d'un code d'amorçage qui s'auto-modifie. Pour résoudre ce problème, ajoutez aux fichiers de démarrage les informations de validation par le biais du moteur d'analyse de ligne de commande de VirusScan. Cette méthode ne permet pas d'enregistrer les informations sur la zone système ou la partition d'amorçage (MBR).
- **Vous possédez un logiciel protégé en copie.** Selon le type de protection en copie utilisé, les composants de VirusScan risquent de détecter un virus dans la zone système ou dans la partition d'amorçage de certaines disquettes ou d'autres supports.

Si aucune de ces situations ne s'applique à votre cas, contactez le support technique de Network Associates ou adressez un courrier électronique détaillant le problème rencontré à virus_research_europe@nai.com.

Options de réponse à un virus ou à un programme malveillant

Le logiciel VirusScan étant constitué de plusieurs composants, les actions possibles en réponse à une infection virale ou à la présence d'un programme malveillant sur l'ordinateur dépendent du composant VirusScan qui a détecté l'objet nuisible, de la configuration de ce composant, ainsi que d'autres conditions. Les sections qui suivent présentent les actions par défaut associées à chaque composant de VirusScan. Pour en savoir plus sur les autres actions possibles, reportez-vous au chapitre consacré à chaque composant.

Options de réponse lorsque le moteur d'analyse VShield détecte un programme malicieux

Le moteur d'analyse VShield se compose de quatre modules connexes qui analysent le système en permanence et en arrière-plan, le protégeant contre les virus, les objets Java et ActiveX nocifs et les sites Web dangereux. Un cinquième module contrôle les paramètres de sécurité des quatre premiers. Vous pouvez configurer et activer chaque module séparément ou conjointement. Dans ce dernier cas, vous assurez une protection maximale.

Pour en savoir plus sur la configuration de chaque module, reportez-vous au Chapitre 4, « Utilisation du moteur d'analyse VShield »,. Chaque module possède un ensemble propre d'actions par défaut, adaptées aux objets qu'il détecte et aux points d'entrée de virus qu'il analyse.

Options de réponse lorsque le module Analyse système détecte un virus

Le comportement de ce module face à la détection d'un virus dépend du système d'exploitation utilisé par votre ordinateur et, sur les systèmes Windows 95 et Windows 98, du type réponse choisi dans la page Action du module Analyse système. Pour en savoir plus sur ces options, reportez-vous à la section « Sélection des options d'action » à la page 124.

Sur Windows 95 et Windows 98, ce module d'analyse effectue implicitement une recherche de virus chaque fois que vous exécutez, copiez, créez ou renommez un fichier sur le système, et chaque fois que vous effectuez une lecture sur disquette. Sur Windows NT Workstation v4.0 et Windows 2000 Professionnel, le module Analyse système effectue une recherche de virus chaque fois que votre système ou un autre ordinateur lit ou écrit des fichiers sur votre disque dur ou sur disquette.

Parce qu'il procède de la sorte, le module Analyse système peut faire office de sauvegarde au cas où un autre module VShield ne détecterait pas un virus qui infecte pour la première fois votre système. Dans sa configuration initiale, le module refuse l'accès à tout fichier infecté détecté, quelle que soit la version de Windows utilisée par votre ordinateur. Il affiche également un message d'alerte vous demandant la démarche à suivre vis-à-vis du virus (voir Figure 3-11 à la page 90). Les options de réponse qui apparaissent dans cette boîte de dialogue proviennent des choix par défaut ou des choix que vous avez faits dans la page Action du module Analyse système.

Pendant que cette boîte de dialogue attend votre réponse, votre ordinateur continue à traiter en arrière-plan toutes les autres tâches en cours d'exécution.

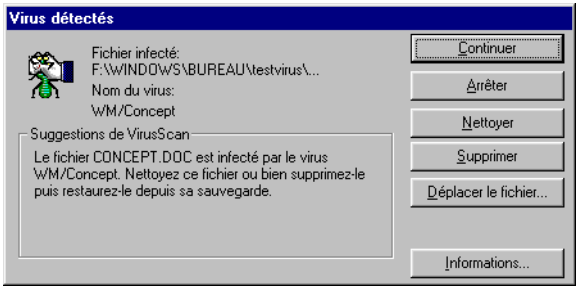

Figure 3-1. Options de réponse initiales du module Analyse système

Si votre ordinateur utilise Windows 95 ou Windows 98, vous pouvez choisir un message d'alerte différent. Si vous avez coché la case **BIOS** dans la zone Type d'invite de la page Action du module Analyse système, vous verrez apparaître un avertissement en mode plein écran vous offrant diverses options de réponse (Figure 3-2).

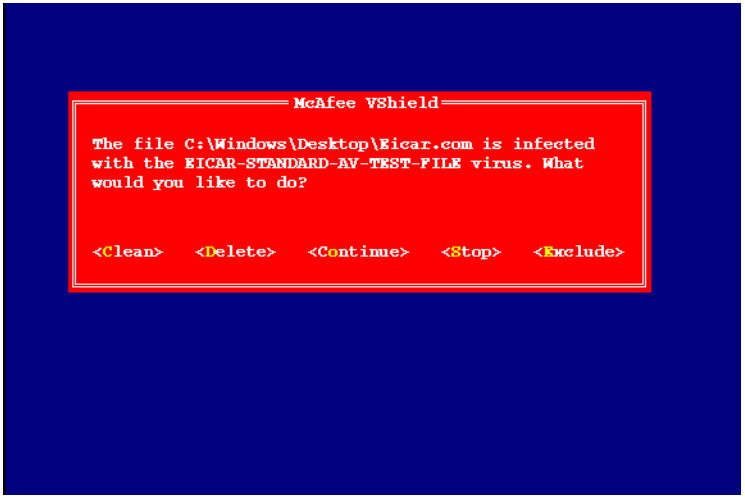

Figure 3-2. Options de réponse de l'avertissement en mode plein écran du module Analyse système

Dans l'attente de votre réponse, ce message d'alerte bloque complètement le fonctionnement de votre système. Aucun autre programme ou système d'exploitation ne fonctionne sur votre ordinateur tant que vous n'avez pas choisi une option de réponse.

Le type d'invite BIOS vous permet également de remplacer l'option **Déplacer le fichier** par l'option **Continuer**. Pour ce faire, cochez la case **Continuer l'accès** dans la page Action du module Analyse système.

REMARQUE : La case à cocher Continuer l'accès n'est pas accessible si votre ordinateur utilise Windows NT Workstation v4.0 ou Windows 2000 ou si vous choisissez **GUI** comme type d'invite sur les systèmes Windows 95 et Windows 98.

Pour exécuter l'une des actions proposées dans le message d'alerte, cliquez sur un bouton de la boîte de dialogue Accès au fichier interdit ou entrez la lettre en surbrillance (jaune) lorsque le système affiche l'avertissement. Si vous souhaitez appliquer la même action pour tous les fichiers infectés détectés par le module Analyse système lors de cette session d'analyse, cochez la case **Appliquer à tous les éléments** dans cette boîte de dialogue. Cette option n'est pas disponible dans le message d'alerte en mode plein écran.

Les options de réponse sont les suivantes :

- **Nettoyer le fichier.** Cliquez sur **Nettoyer** dans la boîte de dialogue ou tapez N lorsque le système affiche l'avertissement en mode plein écran. En procédant de la sorte, le module Analyse système tentera de supprimer le code de virus du fichier infecté. Si le module parvient à supprimer l'infection, il restaure le fichier dans son état d'origine et consigne le résultat dans son fichier journal.

  Si le module n'est pas en mesure de nettoyer le fichier (soit qu'il ne possède pas le programme de désinfection correspondant, soit que le virus ait irrémédiablement endommagé le fichier), il consigne ce résultat dans son fichier journal et n'entreprend aucune autre action. Dans la plupart des cas, il est préférable de supprimer ces fichiers et de les restaurer à partir d'une sauvegarde récente.

- **Supprimer le fichier.** Cliquez sur **Supprimer** dans la boîte de dialogue ou tapez S lorsque le système affiche l'avertissement en mode plein écran pour indiquer au module Analyse système de supprimer immédiatement le fichier infecté. Par défaut, le module note le nom du fichier infecté dans son fichier journal afin que vous disposiez d'un enregistrement des fichiers marqués comme infectés. Consultez ce dernier pour connaître les fichiers supprimés à restaurer à partir d'une précédente sauvegarde.

- **Déplacer le fichier.** Cliquez sur **Déplacer le fichier** dans la boîte de dialogue. Vous accédez alors à une fenêtre de consultation vous permettant de localiser votre dossier de quarantaine ou tout autre dossier que vous souhaitez utiliser pour isoler les fichiers infectés. Aussitôt le dossier sélectionné, le module Analyse système y transfère le fichier infecté. Cette option n'apparaît pas dans le message d'alerte en mode plein écran.

- **Continuer à travailler. Lorsque le système affiche l'avertissement en mode plein écran,** tapez O pour demander au module Analyse système de vous laisser poursuivre avec le fichier et de ne prendre aucune autre mesure. Vous recourrez généralement à cette option pour contourner les fichiers que vous savez exempts de tout virus. Si l'option de rapport est activée, le module notera chaque incident dans son fichier journal. Cette option n'est pas disponible dans la boîte de dialogue Accès au fichier interdit.

- **Arrêter l'analyse.** Cliquez sur **Arrêter** dans la boîte de dialogue ou tapez A lorsque le système affiche l'avertissement en mode plein écran. En procédant de la sorte, le module Analyse système empêche tout accès au fichier mais ne prend aucune autre mesure. Interdire l'accès au fichier empêche tout utilisateur de l'ouvrir, de l'enregistrer, de le copier ou de le renommer. Pour continuer, vous devez cliquer sur **OK**. Si l'option de rapport est activée, le module notera chaque incident dans son fichier journal.

- **Exclure le fichier des opérations d'analyse.** Cliquez sur **Exclure** dans la boîte de dialogue ou tapez E lorsque le système affiche l'avertissement en mode plein écran. En procédant de la sorte, vous indiquez au module Analyse système d'exclure ce fichier des futures opérations d'analyse. Vous recourrez généralement à cette option pour contourner les fichiers que vous savez exempts de tout virus.

Options de réponse lorsque le module Analyse E-Mail détecte un virus

Ce module recherche les virus dans les messages électroniques que vous recevez par l'intermédiaire d'un système de messagerie commerciale, tel que cc:Mail ou Microsoft Exchange. Dans sa configuration initiale, le module vous invite à choisir une action parmi cinq, chaque fois qu'il détecte un virus (Figure 3-3).

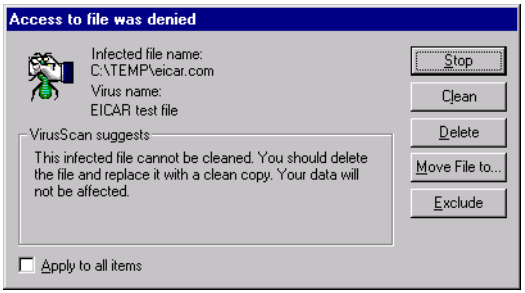

Figure 3-3. Options de réponses du module Analyse E-Mail

Cliquez sur le bouton qui correspond à la réponse souhaitée. Vous avez le choix entre les options suivantes :

- **Arrêter.** Cliquez sur ce bouton pour mettre fin immédiatement à l'opération d'analyse. Le module Analyse E-Mail consignera chaque détection dans son fichier journal, mais ne prendra aucune autre mesure corrective à l'encontre du virus.

- **Nettoyer.** Cliquez sur ce bouton pour demander au module Analyse E-Mail d'essayer de supprimer le code de virus dans le fichier infecté. Si VirusScan n'est pas en mesure de nettoyer le fichier (soit qu'il ne possède pas le programme de désinfection correspondant, soit que le virus ait irrémédiablement endommagé le fichier), il consigne ce résultat dans le fichier journal et suggère une autre action. Dans l'exemple illustré par la Figure 3-3, le module n'a pas été en mesure de nettoyer le fichier test EICAR—un simulacre de « virus » écrit spécifiquement pour tester l'installation d'un programme antivirus. Ici, **Nettoyer** n'est pas une action disponible. Dans la plupart des cas, il est préférable de supprimer ces fichiers et de les restaurer à partir d'une sauvegarde récente.

- **Supprimer.** Cliquez sur ce bouton pour supprimer immédiatement le fichier infecté du système. Par défaut, le module Analyse E-Mail note le nom du fichier infecté dans son fichier journal pour vous permettre de le restaurer à partir d'une copie de sauvegarde.
- **Déplacer le fichier.** Cliquez sur ce bouton pour ouvrir une boîte de dialogue vous permettant de rechercher votre dossier de quarantaine ou un autre dossier approprié. Lorsque vous avez choisi le dossier approprié, cliquez sur **OK** pour transférer le fichier à cet emplacement.
- **Exclure.** Cliquez sur ce bouton pour éviter que le module Analyse E-Mail identifie ce fichier comme un virus dans les futures opérations d'analyse. Si vous copiez ce fichier sur votre disque dur, cette option empêche également que le module Analyse système identifie ce fichier comme un virus.

Le module Analyse E-Mail applique immédiatement l'action que vous avez choisie et ajoute une note en haut du message électronique contenant le document attaché infecté. Cette note fournit le nom de fichier du document infecté, identifie le nom du virus et décrit la mesure corrective prise par le module.

Si vous souhaitez appliquer la même action pour tous les fichiers infectés détectés par le module Analyse E-Mail lors de cette session d'analyse, cochez la case **Appliquer à tous les éléments** dans cette boîte de dialogue.

Options de réponse lorsque le module Analyse au téléchargement détecte un virus

Ce module recherche les virus dans les messages électroniques et autres fichiers que vous recevez sur Internet par l'intermédiaire de navigateurs Web ou de tout programme de messagerie client tel que Eudora Light, Netscape Mail ou Outlook Express. Il ne détectera *pas* les fichiers que vous téléchargez au moyen d'applications FTP clientes, d'applications de terminal ou de méthodes similaires. Dans sa configuration initiale, le module vous invite à choisir une action parmi trois, chaque fois qu'il détecte un virus (Figure 3-4). Une quatrième option vous donne des informations supplémentaires.

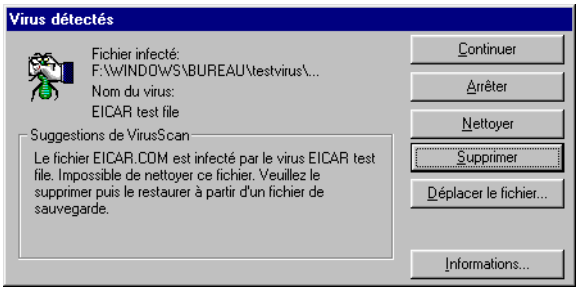

Figure 3-4. Options de réponse du module Analyse au téléchargement

Cliquez sur le bouton qui correspond à la réponse souhaitée. Vous avez le choix entre les options suivantes :

- **Continuer.** Cliquez sur ce bouton pour indiquer au module Analyse au téléchargement de ne prendre aucune mesure et de poursuivre l'analyse. Le module continuera jusqu'à ce qu'il détecte un autre virus sur votre système ou termine l'opération d'analyse. Vous utilisez généralement cette option pour contourner les fichiers que vous savez exempts de tout virus ou si vous envisagez de laisser votre ordinateur sans surveillance pendant le téléchargement du courrier électronique ou d'autres fichiers. Le module notera chaque incident dans son fichier journal.
- **Supprimer.** Cliquez ici pour indiquer au module Analyse au téléchargement de supprimer le fichier infecté ou le document attaché au courrier électronique que vous avez reçu. Par défaut, le module consigne le nom du fichier infecté dans son fichier journal.
- **Déplacer.** Cliquez ici pour indiquer au module Analyse au téléchargement de déplacer le fichier vers le répertoire de quarantaine que vous avez choisi dans la page de propriétés Action du module.

Le module Analyse au téléchargement applique immédiatement l'action que vous avez choisie et ajoute une note en haut du message e-mail contenant le document attaché infecté. Cette note fournit le nom de fichier du document infecté, identifie le nom du virus et décrit la mesure corrective prise par le module.

Options de réponses lorsque le Filtre Internet détecte un virus

Ce module recherche les classes Java et les contrôles ActiveX hostiles, chaque fois que vous accédez à un site Web ou que vous téléchargez un fichier à partir d'Internet. Vous pouvez également configurer ce module de façon à bloquer l'accès de votre navigateur aux sites Internet dangereux. Dans sa configuration initiale, le module vous laisse le choix, chaque fois qu'il décèle un objet potentiellement nuisible, de **Refuser** à l'objet l'accès à votre système, ou de **Continuer** en autorisant l'accès. Le module vous propose également ces deux options lors de toute tentative de connexion à un site Web potentiellement dangereux (Figure 3-5).

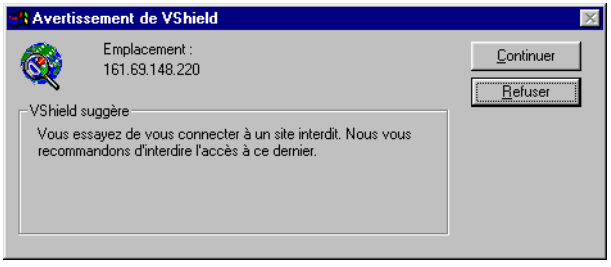

Figure 3-5. Options de réponse du module Filtre Internet

Options de réponse lorsque l'application VirusScan détecte un virus

Lorsque vous lancez une opération d'analyse pour la première fois à l'aide de l'application VirusScan, cette dernière analysera tous les fichiers présents sur l'unité C: susceptibles d'être infectés par un virus. Cela vous assure un niveau de protection de base, que vous pouvez étendre et adapter à vos besoins propres en configurant le logiciel VirusScan.

Dans sa configuration initiale, le programme vous invite à choisir une action lorsqu'il détecte un virus (Figure 3-6).

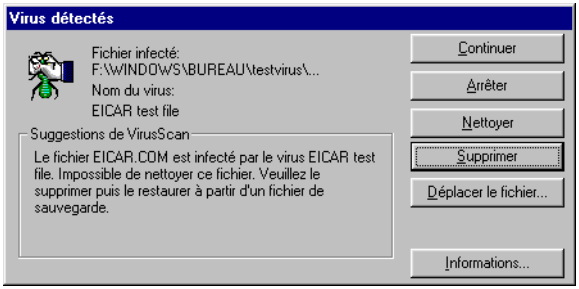

Figure 3-6. Options de réponse de VirusScan

Pour répondre à l'infection, cliquez sur l'un des boutons présentés. Vous avez le choix entre les actions suivantes :

- **Continuer.** Cliquez sur ce bouton pour continuer l'opération d'analyse et demander à l'application de dresser la liste des fichiers infectés dans la partie inférieure de sa fenêtre principale (Figure 3-7 à la page 85) et de consigner chaque détection dans son fichier journal, mais de ne prendre aucune mesure corrective à l'encontre du virus. À l'issue de l'examen du système, vous pouvez faire un clic droit sur chacun des fichiers énumérés dans la fenêtre principale, et choisir l'action appropriée dans le menu contextuel qui s'affiche.

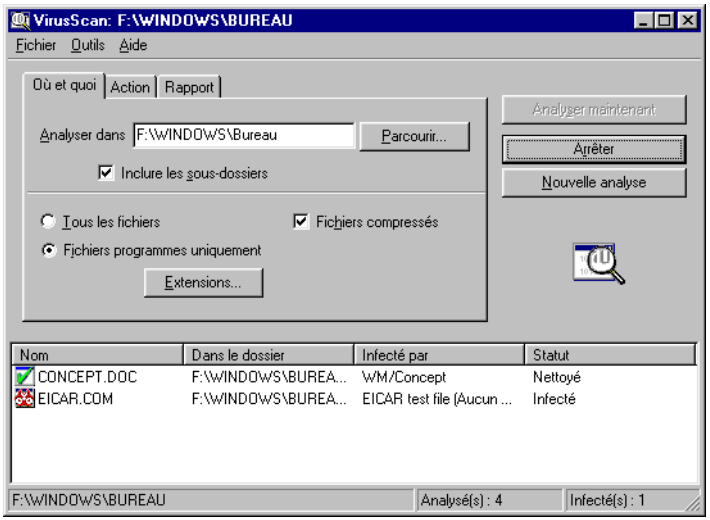

Figure 3-7. Fenêtre principale de VirusScan

- **Arrêter.** Cliquez sur ce bouton pour mettre fin immédiatement à l'opération d'analyse. L'application VirusScan affiche la liste des fichiers infectés dans la partie inférieure de la fenêtre principale (Figure 3-7) et consigne chaque détection dans son fichier journal, mais ne prend aucune mesure corrective à l'encontre du virus. Cliquez avec le bouton droit sur chaque fichier infecté répertorié dans la fenêtre principale, puis choisissez une réponse individuelle dans le menu contextuel qui s'affiche.
- **Nettoyer.** Cliquez sur ce bouton pour demander à l'application VirusScan d'essayer de supprimer le code de virus dans le fichier infecté. Si VirusScan n'est pas en mesure de nettoyer le fichier (soit qu'il ne possède pas le programme de désinfection correspondant, soit que le virus ait irrémédiablement endommagé le fichier), il consigne ce résultat dans le fichier journal et suggère une autre action.

  Dans l'exemple illustré par la Figure 3-6 à la page 84, VirusScan n'a pas été en mesure de nettoyer le virus test EICAR—un simulacre de « virus » écrit spécifiquement pour tester l'installation d'un programme antivirus. Ici, **Nettoyer** n'est pas une action disponible. Dans la plupart des cas, il est préférable de supprimer ces fichiers et de les restaurer à partir d'une sauvegarde récente.
- **Supprimer.** Cliquez sur ce bouton pour supprimer immédiatement le fichier infecté du système. Par défaut, l'application VirusScan note le nom du fichier infecté dans son fichier journal pour vous permettre de le restaurer à partir d'une copie de sauvegarde.

- **Déplacer le fichier.** Cliquez sur ce bouton pour ouvrir une boîte de dialogue vous permettant de rechercher votre dossier de quarantaine ou un autre dossier approprié. Lorsque vous avez choisi le dossier approprié, cliquez sur **OK** pour transférer le fichier à cet emplacement.
- **Informations.** Cliquez ici pour vous connecter à la Bibliothèque d'informations sur les virus de Network Associates. Cette option ne prend aucune mesure corrective à l'encontre du virus détecté par VirusScan. Pour plus de détails, reportez-vous à la section Voir « Affichage des informations sur les virus » à la page 88.

Options de réponse lorsque l'extension Analyse E-Mail détecte un virus

Au besoin, le module Analyse E-Mail, inclus dans le logiciel VirusScan, vous permet d'analyser les messages électroniques que vous recevez via Microsoft Exchange ou Microsoft Outlook. Vous pouvez le démarrer depuis l'un de ces programmes de messagerie clients ; il viendra compléter l'analyse en tâche de fond du courrier électronique reçu exécutée par le module Analyse E-Mail de VShield. Le module Analyse E-Mail vous permet également de nettoyer les pièces jointes infectées et d'arrêter l'analyse, fonctions qui complètent la surveillance continue assurée par ce module. Dans sa configuration initiale, l'extension Analyse E-Mail vous invite à choisir une action chaque fois qu'elle détecte un virus (Figure 3-8).

Figure 3-8. Options de réponse du module Analyse E-Mail

Pour répondre à l'infection, cliquez sur l'un des boutons présentés. Vous avez le choix entre les actions suivantes :

- **Continuer.** Cliquez sur ce bouton pour demander à l'extension Analyse E-Mail de poursuive son analyse, d'afficher la liste des fichiers infectés dans la partie inférieure de sa fenêtre principale (Figure 3-9 à la page 87) et de consigner chaque détection dans son fichier journal, mais de ne prendre aucune mesure corrective à l'encontre du virus. L'extension continuera l'analyse jusqu'à ce qu'elle détecte un autre virus sur votre système ou termine l'opération. À l'issue de l'examen du système, vous pouvez faire un clic droit sur chacun des fichiers répertoriés dans la fenêtre principale, et choisir l'action appropriée dans le menu contextuel qui s'affiche.

- **Arrêter.** Cliquez sur ce bouton pour mettre fin immédiatement à l'opération d'analyse. L'extension Analyse E-Mail affiche la liste des fichiers infectés décelés avant l'interruption dans la partie inférieure de la fenêtre principale (Figure 3-9) et note chaque détection dans son fichier journal, mais ne prend aucune mesure corrective. Cliquez avec le bouton droit sur chaque fichier infecté répertorié dans la fenêtre principale, puis choisissez une réponse individuelle dans le menu contextuel qui s'affiche.

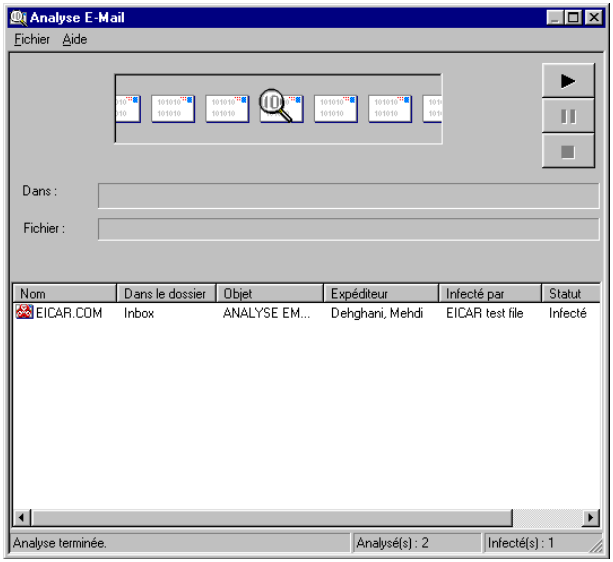

Figure 3-9. Fenêtre de l'extension Analyse E-Mail

- **Nettoyer.** Cliquez sur ce bouton pour supprimer le code de virus dans le fichier infecté. Si l'extension Analyse E-Mail n'est pas en mesure de nettoyer le fichier (soit qu'elle ne possède pas le programme de désinfection correspondant, soit que le virus ait irrémédiablement endommagé le fichier), elle consigne ce résultat dans le fichier journal et suggère une autre action. Dans l'exemple illustré par la Figure 3-8 à la page 86, **Nettoyer** n'est pas une action disponible. Dans la plupart des cas, il est préférable de supprimer ces fichiers et de les restaurer à partir d'une sauvegarde récente.

- **Supprimer.** Cliquez sur ce bouton pour supprimer le fichier infecté du système. Par défaut, l'extension Analyse E-Mail note le nom du fichier infecté dans son fichier journal pour vous permettre de le restaurer à partir d'une copie de sauvegarde.
- **Déplacer.** Cliquez sur ce bouton pour ouvrir une boîte de dialogue vous permettant de rechercher votre dossier de quarantaine ou un autre dossier approprié. Lorsque vous avez choisi le dossier approprié, cliquez sur **OK** pour transférer le fichier à cet emplacement.
- **Informations.** Cliquez ici pour vous connecter à la Bibliothèque d'informations sur les virus de Network Associates. Cette option ne prend aucune mesure corrective contre le virus détecté par l'extension Analyse E-Mail. Pour plus de détails, reportez-vous à la section "Affichage des informations sur les virus".

Affichage des informations sur les virus

Le fait de cliquer sur l'option **Informations** dans n'importe quelle boîte de dialogue de mesure corrective vous connectera à la Bibliothèque en ligne d'informations sur les virus de Network Associates, à condition que vous disposiez d'un accès à Internet et que votre ordinateur soit équipé d'un logiciel de navigation Web (Figure 3-10).

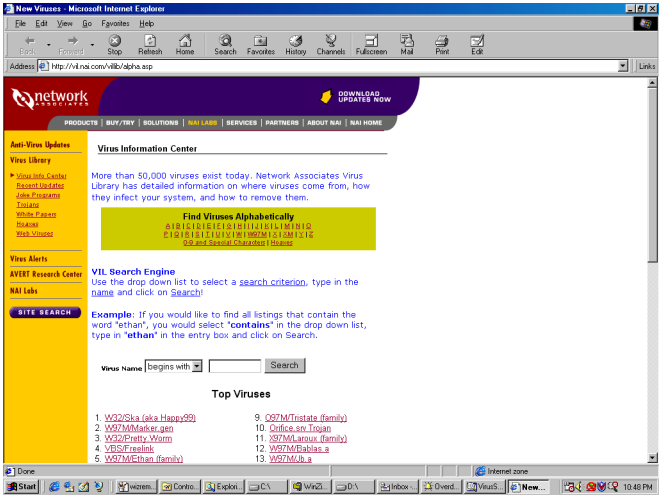

Figure 3-10. Page Bibliothèque d'informations sur les virus de Network Associates

La Bibliothèque d'informations sur les virus regroupe des documents qui offrent une description détaillée de chaque virus que le logiciel VirusScan est en mesure d'identifier et de nettoyer, ainsi que des informations sur la façon dont le virus infecte et modifie les fichiers, et les types de dégâts qu'il provoque. Le site dresse une liste des virus les plus répandus ou les plus dangereux, fournit un moteur de recherche vous permettant d'obtenir la description d'un virus spécifique, par ordre alphabétique ou par nom de virus, présente des tables de fréquence, des documents techniques et des papiers blancs, et met à votre disposition des données techniques que vous pouvez utiliser pour supprimer des virus de votre système.

Pour vous connecter directement à la Bibliothèque, visitez le site à l'adresse suivante :

http://vil.nai.com/villib/alpha.asp

Vous pouvez également vous connecter directement à la Bibliothèque depuis la console VirusScan. Pour ce faire, choisissez **Liste des virus** dans le menu **Affichage** de la fenêtre de la console. Pour en savoir plus sur la console, reportez-vous au Chapitre 6, « Création et configuration des tâches planifiées ».

La Bibliothèque fait partie du site AVERT de McAfee, que vous pouvez visiter à l'adresse suivante :

http://www.nai.com/asp_set/anti_virus/avert/intro.asp

Le site Web AVERT constitue une source inépuisable de logiciels et d'informations sur le virus.

Vous y trouverez par exemple :

- Des informations actualisées et des évaluations sur les dangers des nouveaux virus et des virus connus
- Des logiciels que vous pouvez utiliser pour étendre ou compléter les fonctionnalités de votre logiciel antivirus McAfee
- Des adresses des contacts et autres informations que vous pouvez utiliser pour soumettre des questions, des exemples de virus et autres données utiles
- Des mises à jour des fichiers de définition de virus, y compris des mises à journalières du fichier .DAT bêta, des fichiers EXTRA.DAT, des fichiers .DAT de secours à jour, des versions actualisées du moteur d'analyse, des mises à jour hebdomadaires des fichiers .DAT et de l'utilitaire SuperDAT, et de nouveaux fichiers de définition de virus incrémentiels (.UPD)
- Des logiciels en version bêta et en « version préliminaire »

Affichage des informations sur un fichier

Si vous cliquez avec le bouton droit de la souris sur un fichier répertorié dans la fenêtre principale de VirusScan ou dans la fenêtre du module Analyse E-Mail (voir Figure 3-9 à la page 87), et que vous sélectionnez ensuite **Infos sur le fichier** dans le menu contextuel qui s'affiche, le logiciel VirusScan ouvre une boîte de dialogue intitulée Informations sur les éléments infectés, dans laquelle seront indiqués le nom, le type et la taille (en octets) du fichier. Vous y trouverez également les dates de modification et de création du fichier, ainsi qu'une description de ses attributs (Figure 3-11 à la page 90).

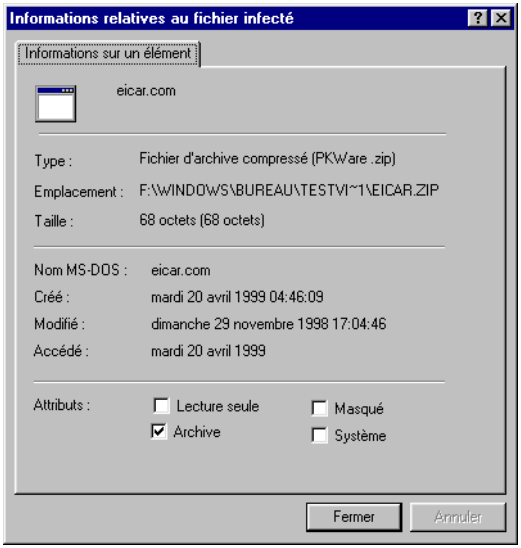

Figure 3-11. Page de propriétés Informations relatives au fichier infecté

Envoi d'un exemple de virus

Si vous suspectez la présence d'un virus dans un fichier ou si votre système présente des signes caractéristiques d'une infection virale, mais que VirusScan n'a détecté aucun virus, McAfee vous recommande d'envoyer un exemple à son équipe de recherche antivirus pour analyse. Pour ce faire, assurez-vous de démarrer votre système tel quel (sans supprimer l'éventuel virus) ; ne le démarrez pas à l'aide d'une disquette saine.

Il existe plusieurs méthodes de capture et d'envoi des exemples de virus. La section suivante décrit ces méthodes, adaptées à des conditions spécifiques.

Utilisation de l'utilitaire SendVirus pour soumettre un exemple de fichier

Dans la mesure où la plupart des virus de dernière génération ont tendance à infecter des fichiers document et des fichiers exécutables, le logiciel VirusScan est livré avec SENDVIR.EXE, qui est un utilitaire qui vous permet d'envoyer facilement un exemple de fichier infecté aux chercheurs de McAfee en vue d'une analyse.

Pour soumettre un exemple de fichier infecté, procédez comme suit :

1. Si vous devez vous connecter à votre réseau ou au fournisseur des services Internet pour envoyer un courrier électronique, commencez par effectuer cette opération. Si vous disposez d'une connexion permanente à votre réseau ou au fournisseur des services Internet, ignorez cette étape et passez à l'Étape 2.
2. Localisez le fichier SENDVIR.EXE dans le répertoire du programme VirusScan. Si vous avez installé le logiciel VirusScan avec les options par défaut, le chemin d'accès au fichier est le suivant :

   C:\Program Files\Network Associates\VirusScan
3. Double-cliquez sur le fichier pour afficher le premier écran de l'Assistant du centre de recherche antivirus (AVERT) (Figure 3-12).

Figure 3-12. Premier écran SENDVIR.EXE

4. Lisez le message d'accueil, puis cliquez sur **Suivant>** pour continuer.

   L'écran Informations pour vous contacter s'affiche.

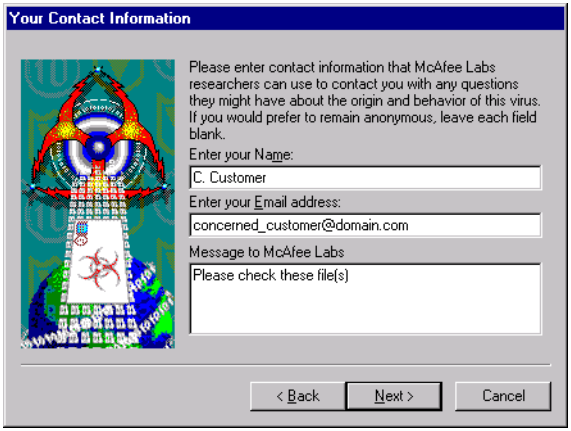

Figure 3-13. Écran Informations pour vous contacter

5. Si vous souhaitez que les chercheurs de l'équipe AVERT prennent contact avec vous pour vous communiquer leurs résultats sur le fichier que vous envoyez, entrez votre nom, votre adresse électronique et, si vous le souhaitez, un commentaire, dans les zones de texte prévues à cet effet, puis cliquez sur **Suivant>** pour continuer.

REMARQUE : Si vous le souhaitez, vous pouvez soumettre des fichiers en conservant l'anonymat. Il suffit pour cela de laisser les zones de texte de cet écran vides. Aucune information demandée dans cet écran n'est obligatoire.

L'écran Choix des fichiers à envoyer s'affiche (Figure 3-14).

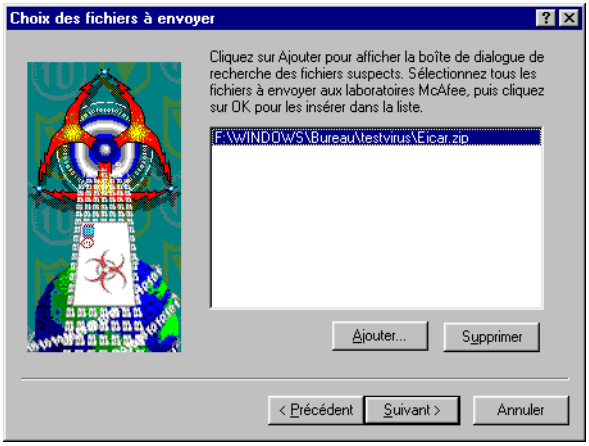

Figure 3-14. Écran Choix des fichiers à envoyer

6. Cliquez sur **Ajouter** pour ouvrir une boîte de dialogue vous permettant de localiser les fichiers pour lesquels vous suspectez la présence d'un virus.

   Choisissez tous les fichiers que vous souhaitez envoyer pour analyse. Pour supprimer un fichier inclus dans la liste d'envoi, sélectionnez-le, puis cliquez sur **Supprimer**. Après avoir sélectionné tous les fichiers à envoyer, cliquez sur **Suivant>** pour continuer.

   L'écran Options d'envoi s'affiche (Figure 3-15).

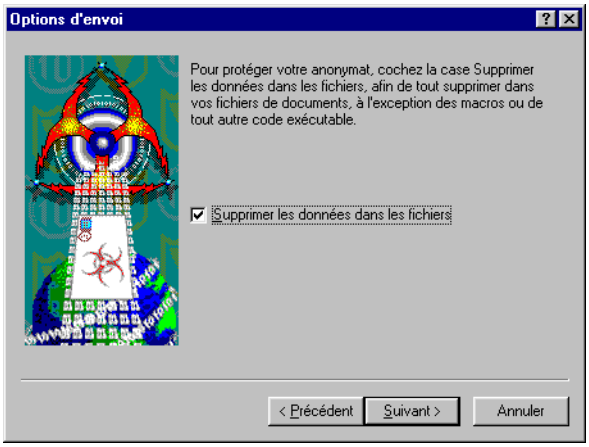

Figure 3-15. Écran Options d'envoi

   Si le fichier que vous souhaitez envoyer est un document Microsoft Office ou un autre type de fichier contenant des informations confidentielles, cochez la case **Supprimer les données dans les fichiers**, puis cliquez sur **Suivant>** pour continuer. Vous demandez ainsi à l'utilitaire SENDVIR.EXE de supprimer le contenu du fichier, à l'exception des macros ou du code exécutable.

   L'écran Choix du service E-mail s'affiche (Figure 3-16 à la page 94).

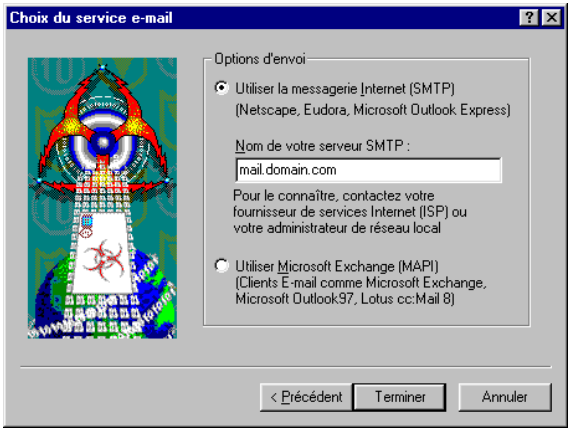

Figure 3-16. Écran Choix du service E-mail

7. Sélectionnez le type d'application cliente e-mail installée sur votre ordinateur. Vous avez le choix entre les options suivantes :

   - **Utiliser la messagerie Internet (SMTP)**. Cliquez sur ce bouton pour envoyer votre exemple de virus via un client de messagerie SMTP, tel que Eudora, NetScape Mail, ou Microsoft Outlook Express. Tapez ensuite le nom de votre serveur de courrier sortant ; mail.domain.com par exemple.

   - **Utiliser Microsoft Exchange (MAPI)**. Cliquez sur ce bouton pour envoyer votre exemple de virus via un système de messagerie commerciale. Vous ne pouvez utiliser cette option que si votre système de messagerie électronique prend en charge l'interface MAPI (Messaging Application Programming Interface). C'est le cas par exemple de Microsoft Exchange, Microsoft Outlook, et des versions 8.0 et suivantes de Lotus cc:Mail.

8. Cliquez sur **Terminer** pour envoyer votre exemple de virus.

REMARQUE : Même si les chercheurs de McAfee apprécient la réception d'exemples de virus, l'envoi de votre message ne les oblige en aucun cas à entreprendre une action, fournir une solution, ou vous adresser une réponse.

SENDVIR.EXE utilisera le client de messagerie électronique que vous avez spécifié pour envoyer votre exemple. Pour y parvenir, vous devez être connecté à votre réseau ou à votre fournisseur des services Internet.

Capture des virus de zone système, de fichier et de macro

Si vous suspectez une infection de votre système, vous pouvez capturer un exemple du virus, puis en créer une image sur disquette pour l'envoyer par courrier électronique, ou envoyer directement cette disquette aux chercheurs de McAfee. Il est également conseillé d'envoyer aux chercheurs des exemples de vos fichiers système courants sur une autre disquette.

Capture des virus de zone système

Les virus de zone système se cachent généralement dans les zones de votre disque dur ou des disquette auxquelles vous n'avez pas accès en lecture ni en écriture. Vous pouvez toutefois capturer un exemple de virus de zone système en infectant délibérément une disquette avec ce virus.

Pour y parvenir, procédez comme suit :

1. Insérez une disquette vierge non formatée dans votre lecteur de disquette.
2. Cliquez sur **Démarrer** dans la barre des tâches Windows, pointez sur **Programmes**, puis choisissez **MS-DOS** si votre ordinateur utilise Windows 95 ou Windows 98, ou **Invite de commande**, si votre ordinateur utilise Windows NT Workstation v4.0 ou Windows 2000 Professionnel.
3. Tapez la ligne suivante à l'invite de commande :

   ```
   format a: /s
   ```

   Si votre système s'arrête pendant le formatage de la disquette, retirez celle-ci du lecteur. Préparez une étiquette intitulée « Endommagée au cours du formatage infecté en tant que disquette d'amorçage », collez-la sur la disquette et mettez cette dernière de côté.
4. Insérez une nouvelle disquette formatée dans votre lecteur de disquette.
5. Copiez vos fichiers système courants sur la disquette. Dans la plupart des versions de DOS, les fichiers système sont les suivants :

   - IO.SYS
   - MSDOS.SYS
   - COMMAND.COM

   Pour les systèmes Windows, copiez les fichiers suivants sur la même disquette pré-formatée.

   - GDI.EXE
   - KRNL286.EXE ou KRNL386.EXE
   - PROGMAN.EXE

6. Préparez une étiquette intitulée « Contient des fichiers infectés », collez-la sur la disquette et mettez cette dernière de côté.

Capture des virus de fichier ou de macro

Si vous pensez qu'un virus de fichier ou un virus de macro a infecté un ou plusieurs fichiers Microsoft Word, Excel, ou PowerPoint, envoyez ces fichiers aux chercheurs de McAfee, soit par courrier électronique, à l'aide de l'utilitaire SENDVIR.EXE, sous forme d'images de disquette, soit par la poste, en copiant ces fichiers sur une disquette :

- Si vous pensez qu'un virus a infecté des fichiers exécutables dans votre système, copiez le fichier COMMAND.COM sur une disquette formatée, puis remplacez son extension par une extension de fichier non exécutable.
- Si vous pensez qu'un virus de macro a infecté vos fichiers Microsoft Word, copiez le fichier NORMAL.DOT et tous les fichiers du dossier Startup de Microsoft Office sur la disquette. Si vous avez installé Microsoft Office dans l'emplacement par défaut, le chemin d'accès aux fichiers de démarrage est le suivant :

  C:\Program Files\Microsoft Office\Office\Startup
- Si vous pensez qu'un virus de macro a infecté vos fichiers Microsoft Excel, copiez tous les fichiers du répertoire C:\Program Files\Microsoft Office\Office\XLSTART sur la disquette. Incluez tous les fichiers que vous avez installés dans d'autres répertoires destinés aux fichiers de démarrage.
- Si vous pensez qu'un virus de macro a infecté vos fichiers PowerPoint, copiez le fichier BLANKPRESENTATION.POT, situé dans C:\Program Files\Microsoft Office\Templates, sur la disquette.

Création d'une image de disquette

Pour envoyer les fichiers stockés sur les disquettes que vous avez créées, vous pouvez utiliser RWFLOPPY.EXE, un outil mis au point par le centre de recherche antivirus (AVERT) McAfee, pour créer une image de disquette qui encapsule l'infection. L'outil RWFLOPPY.EXE n'est pas inclus dans votre logiciel VirusScan, mais vous pouvez le télécharger à l'adresse suivante :

http://www.nai.com/asp_set/anti_virus/avert/tools.asp

Le site AVERT stocke l'outil sous la forme d'un fichier .ZIP compressé. Téléchargez le fichier sur votre ordinateur, puis décompressez-le dans un dossier temporaire du disque dur. Le fichier .ZIP inclut un petit fichier texte qui explique la syntaxe à utiliser pour l'utilitaire RWFLOPPY.EXE.

REMARQUE : Si vous pensez que votre système est infecté par un virus d'amorçage, vous devez utiliser RWFLOPPY pour envoyer vos exemples par courrier électronique ; sinon, vous pouvez les envoyer par la poste, sur disquette. Si vous envoyez vos exemples par courrier électronique sans utiliser RWFLOPPY, ils seront incomplets ou inutilisables, car les virus d'amorçage se cachent souvent derrière les dernier secteurs d'une disquette, et les autres programmes de création d'images de disquette ne sont pas en mesure d'obtenir ces données.

Une fois que vous avez créé les images de disquette que vous souhaitez envoyer, vous pouvez les envoyer en tant que pièces jointes, par courrier électronique, aux chercheurs de McAfee.

Préparation des fichiers d'archives à envoyer

Essayez de stocker le maximum d'exemples de virus en une seule disquette. Pour ce faire, compressez les exemples que vous avez capturés sur disquette dans un seul fichier .ZIP, avec une protection par mot de passe. Voici un exemple de procédure de compression à l'aide de l'utilitaire WinZip :

1. Démarrez WinZip.
2. Appuyez sur CTRL+N pour créer un nouveau fichier d'archives.

   La boîte de dialogue Nouveau fichier d'archives s'affiche.
3. Entrez un nom pour le fichier d'archives, puis cliquez sur **OK**.
4. Appuyez sur CTRL+A pour ajouter des fichiers dans le fichier d'archives.

   La boîte de dialogue Ajouter s'affiche.
5. Cliquez sur **Mot de passe** pour afficher la boîte de dialogue Mot de passe.
6. Tapez INFECTÉ dans la zone de texte Mot de passe, puis cliquez sur **OK**.
7. Lorsque vous y êtes invité, tapez à nouveau votre mot de passe pour vérifier son exactitude, puis cliquez sur **OK**.

   La boîte de dialogue Ajouter avec mot de passe s'affiche.
8. Sélectionnez vos fichiers exemple, puis cliquez sur **OK**.

   WinZip applique le mot de passe que vous avez saisi à tous les fichiers que vous ajoutez ou retirez du fichier d'archives. Vous pouvez identifier facilement les fichiers protégés par mot de passe dans une liste de fichier d'archives, car leurs noms sont suivis du signe plus (+) .

REMARQUE : Si vous ne protégez pas vos exemples avec le mot de passe `INFECTÉ`, les moteurs d'analyse antivirus de McAfee peuvent les détecter et les nettoyer avant même qu'ils n'arrivent à destination.

9. Attachez le fichier .ZIP que vous avez créé à un message électronique.

Envoi d'exemples par e-mail

Une fois que vous avez créé des images de disquette ou un fichier d'archives pour vos exemples, envoyez-les aux chercheurs de McAfee à l'une des adresses électroniques suivantes :

Aux États-Unis	virus_research@nai.com
Au Royaume-Uni	vsample@nai.com
En Allemagne	virus_research_de@nai.com
Au Japon	virus_research_japan@nai.com
En Australie	virus_research_apac@nai.com
Au Pays-Bas	virus_research_europe@nai.com

Votre message doit contenir les informations suivantes :

- Les symptômes qui vous amènent à penser que votre ordinateur est infecté
- Le cas échéant, le nom et le numéro de version du produit qui a détecté le virus, ainsi que les résultats
- Les numéros de version du logiciel VirusScan et du fichier .DAT
- Des informations détaillées sur votre système permettant de reproduire l'environnement dans lequel vous avez détecté le virus
- Si possible, votre nom, le nom de votre entreprise, votre numéro de téléphone et votre adresse électronique
- La liste de tous les éléments inclus dans le lot que vous envoyez

Envoi des disquettes infectées

Vous pouvez également envoyer par courrier les disquettes que vous avez créées directement aux chercheurs de McAfee. McAfee vous recommande de créer un fichier texte ou d'écrire un message sur papier avec les mêmes informations que pour l'envoi d'une image de disquette électronique et de le joindre à la ou les disquettes que vous envoyez. Envoyez votre exemple à une seule adresse de centre de recherche afin de recevoir une réponse dans les meilleurs délais. Utilisez les adresses suivantes :

Aux États-Unis :
Network Associates, Inc.
Virus Research
20460 NW Von Neumann Drive
Beaverton, OR 97006

Au Royaume-Uni :
Network Associates, Inc.
Virus Research
Gatehouse Way
Aylesbury, Bucks HP19 3XU
UK

En Allemagne :
Network Associates, Inc.
Virus Research
Luisenweg 40
20537 Hamburg
Allemagne

Au Japon :
Network Associates, Inc.
Virus Research
9F Toranomon Mori-bldg. 33
3-8-21 Toranomon, Minato-Ku
Tokyo
Japon 105-0001

En Australie :
Network Associates, Inc.
Virus Research
Level 1, 500 Pacific Highway
St. Leonards, NSW
Sydney
Australie 2065

En Europe :
Network Associates, Inc.
Virus Research
Gatwickstraat 25
1043 GL Amsterdam
Pays-Bas

REMARQUE : Le centre de recherche antivirus AVERT de McAfee conserve tous les exemples reçus, mais il ne peut en aucun cas vous les renvoyer. AVERT n'accepte ni ne traite pas les cartouches Iomega Ditto ou Jazz, les disques zip Iomega ou tout autre type de support amovible.

Utilisation du moteur d'analyse VShield 4

Que fait le moteur d'analyse VShield ?

Les produits antivirus de bureau McAfee utilisent deux méthodes générales pour protéger votre système. La première, l'analyse à l'arrière plan, fonctionne en permanence à la recherche de virus dans votre ordinateur, pendant l'exécution de vos tâches quotidiennes. Dans le produit VirusScan, c'est le moteur d'analyse VShield qui assure cette fonction. La deuxième vous permet de lancer vos propres opérations d'analyse. En règle générale, c'est l'application VirusScan qui gère ces tâches. Pour en savoir plus sur l'application, reportez-vous au Chapitre 5, « Utilisation de l'application VirusScan ».

Selon la façon dont vous le configurez, le moteur d'analyse VShield peut contrôler tout fichier que vous recevez ou envoyez, que ce soit sur disquette, sur le réseau, en tant que pièce jointe d'un message électronique ou sur Internet. Le moteur d'analyse recherche des virus à chaque fois que vous ouvrez, enregistrez, copiez, renommez ou modifiez vos fichiers de quelque façon que ce soit, et examine la mémoire de votre ordinateur pendant toute opération effectuée sur des fichiers. VShield est lancé lorsque vous démarrez votre ordinateur et reste en mémoire jusqu'à ce que vous l'arrêtiez ou jusqu'à ce que vous éteigniez votre système. VShield dispose également de fonctions de protection optionnelles contre les applets Java et les contrôles ActiveX nuisibles. Ces technologies évitent également que votre ordinateur ne se connecte à des sites Internet dangereux pour sa sécurité.

Le moteur d'analyse VShield se compose de cinq modules associés, chacun avec une fonction spécialisée. Vous pouvez configurer les paramètres pour l'ensemble de ces modules dans la boîte de dialogue Propriétés de VShield. Ces modules sont les suivants :

- **Analyse système.** Ce module recherche des virus sur votre disque dur pendant que vous travaillez sur votre ordinateur. Il analyse les fichiers chaque fois que votre système ou d'autres ordinateurs effectuent des opérations de lecture ou d'écriture sur votre disque dur. Il peut également analyser les disquettes et les lecteurs réseau mappés sur votre système.
- **Analyse E-Mail.** Ce module analyse les messages e-mail et les pièces jointes que vous recevez via un système de messagerie interne ou via Internet. Le module Analyse E-Mail examine votre boîte aux lettres Microsoft Exchange ou Outlook sur votre serveur Microsoft Exchange et les anciens systèmes de messagerie cc:Mail.

Il travaille conjointement avec le module Analyse au téléchargement pour examiner le courrier Internet que vous recevez par le biais du protocole SMTP (Simple Mail Transfer Protocol) ou POP-3 (Post Office Protocol).

- **Analyse au téléchargement**. Ce module analyse les fichiers que vous téléchargez sur votre système depuis Internet. Si vous avez activé l'option de messagerie Internet dans le module Analyse E-Mail, ce dernier inclut le courrier électronique et les pièces jointes qui arrivent sur votre ordinateur à l'aide des systèmes SMTP ou POP-3, notamment les programmes clients de messagerie tels que Eudora Pro, Microsoft Outlook Express, NetScape Mail et America Online Mail.
- **Filtre Internet**. Ce module recherche les objets Java et les contrôles ActiveX nocifs et empêche leur téléchargement et leur exécution sur votre système lorsque vous visitez des sites Internet. Il peut également empêcher la connexion de votre navigateur à des sites Internet potentiellement dangereux qui abritent des logiciels nocifs.

IMPORTANT : Pour utiliser les modules Analyse E-Mail, Analyse au téléchargement ou Filtre Internet, vous devez les installer en sélectionnant l'option Personnalisée lors de l'installation de VirusScan. Pour en savoir plus sur cette procédure, reportez-vous au Chapitre 2, « Installation du logiciel VirusScan ».

- **Sécurité**. Ce module fournit une protection par mot de passe pour les modules VShield restants. Vous pouvez protéger une ou plusieurs pages de propriétés de module et définir un mot de passe pour éviter toute modification non autorisée.

REMARQUE : Le moteur d'analyse VShield fonctionnant en permanence, vous devez installer et exécuter un seul moteur d'analyse VShield par station de travail. Dans le cas contraire, vous pouvez provoquer des interférences dans le fonctionnement des moteurs d'analyse.

Pourquoi utiliser le moteur d'analyse VShield ?

Le moteur d'analyse VShield dispose de fonctionnalités uniques qui en font un élément à part entière du progiciel de protection antivirus global de VirusScan. Ces fonctionnalités sont les suivantes :

- **Analyse lors de l'accès**. Le moteur d'analyse recherche la présence de virus éventuels dans les fichiers que vous ouvrez, copiez, enregistrez ou modifiez par toute autre méthode ainsi que dans les fichiers que vous lisez ou enregistrez sur des disquettes et sur des lecteurs réseau. Il peut ainsi détecter et arrêter les virus dès qu'ils apparaissent dans votre système, y compris ceux qui arrivent par courrier électronique ou en tant que téléchargements via Internet. Cela signifie que le moteur d'analyse VShield peut protéger votre ordinateur contre les attaques virales sur tous les fronts, même entre deux opérations d'analyse. VShield détecte les virus aussi bien dans la mémoire que lorsqu'ils tentent de s'exécuter à partir de fichiers infectés.
- **Détection et interception des objets destructeurs**. Le moteur d'analyse VShield peut empêcher les objets ActiveX et Java destructeurs d'accéder à votre système avant même qu'ils constituent un danger pour lui. Il y parvient en analysant les centaines d'objets que vous téléchargez quand vous êtes connecté au Web ou à d'autres sites Internet, ainsi que les fichiers joints aux courriers électroniques que vous recevez. Il compare ces éléments à une liste d'objets dangereux qu'il maintient à jour et intercepte ceux qui pourraient poser des problèmes.
- **Filtrage des sites Internet**. Le moteur d'analyse VShield dispose d'une liste de sites Internet qui présentent un danger pour votre système, en général parce qu'ils contiennent des logiciels destructeurs pouvant être téléchargés. Vous pouvez y ajouter tout autre site auquel vous voulez éviter toute connexion, en saisissant soit son adresse IP, soit son nom de domaine.
- **Analyse automatique**. Le moteur d'analyse VShield inclut un large éventail de logiciels de navigation et d'applications de messagerie clientes. Ceci lui permet de se connecter à votre boîte aux lettres sur le serveur qui l'abrite et d'analyser les pièces jointes qui vous sont envoyées, avant même qu'elles n'arrivent sur votre ordinateur.

Si vous vous connectez à Internet ou si vous êtes relié à un réseau, le fait d'avoir ce composant activé en permanence peut améliorer considérablement vos capacités de détection et d'élimination des logiciels nuisibles avant qu'ils n'endommagent votre système.

Prise en charge de navigateurs et de clients de messagerie

Le moteur d'analyse VShield fonctionne sans problème avec la plupart des navigateurs Web et des logiciels clients de messagerie disponibles pour la plate-forme Windows. Il n'est pas nécessaire d'effectuer de configuration particulière pour que le moteur d'analyse fonctionne avec votre navigateur ; la configuration de votre ordinateur pour une connexion à Internet suffit. Vous devez toutefois configurer VShield pour qu'il fonctionne correctement avec votre logiciel de messagerie client. Pour savoir comment effectuer la configuration requise, reportez-vous à la section voir « Utilisation de l'Assistant de configuration VShield » à la page 110 ou à la section « Paramétrage des propriétés du moteur d'analyse VShield » à la page 116.

Les navigateurs Web testés par McAfee et reconnus comme fonctionnant correctement avec le moteur d'analyse VShield sont :

- Netscape Navigator v3.x
- Netscape Navigator v4.0.x (sauf la version 4.0.6)
- Microsoft Internet Explorer v3.x
- Microsoft Internet Explorer v4.x

Les clients e-mail testés par McAfee et reconnus comme fonctionnant correctement avec le module Analyse au téléchargement de VShield sont :

- Microsoft Outlook Express
- Qualcomm Eudora v3.x et v4.x
- Netscape Mail (livré avec la plupart des versions de Netscape Navigator et de Netscape Communicator)
- America Online mail v3.0 et v4.0

Pour pouvoir travailler avec le module Analyse E-Mail de VShield, votre système de messagerie commerciale doit utiliser le client Lotus cc:Mail, Microsoft Exchange, ou Microsoft Outlook. Les clients e-mail testés par McAfee et reconnus comme fonctionnant correctement avec le module Analyse E-Mail sont :

- Microsoft Exchange v4.0, v5.0 et v5.5
- Microsoft Outlook 97 et Microsoft Outlook 98
- Lotus cc:Mail v6.x, v7.x et v8.x (non conformes à la norme MAPI)

McAfee ne garantit pas la compatibilité du logiciel VShield avec des logiciels clients non listés ci-dessus.

Activation ou démarrage du moteur d'analyse VShield

À la fin de l'installation de VirusScan, le programme d'installation vous demande si vous souhaitez activer immédiatement le moteur d'analyse VShield. Si vous répondez par oui, le moteur d'analyse VShield se charge immédiatement en mémoire et commence à fonctionner avec un jeu d'options par défaut qui vous offre une protection antivirus de base. Dans le cas contraire, le moteur d'analyse VShield se chargera automatiquement lors du prochain démarrage de votre ordinateur.

Lors du démarrage du moteur d'analyse VShield, ce dernier affiche une icône dans la barre d'état système Windows pour indiquer les modules en cours d'exécution. Pour en savoir plus sur la signification des différents états d'une icône, reportez-vous à la section « Description de chaque état d'une icône de la barre d'état système VShield » à la page 109.

Le moteur d'analyse commence par activer uniquement son module Analyse système, qui recherche les virus qui arrivent sur votre système par le biais de disquettes ou de tout autre support amovible, de connexions à un réseau local ou de tout autre moyen similaire. Le module Analyse système vérifie également les fichiers qui arrivent via le système de messagerie et via Internet, mais pour ce faire, il doit travailler conjointement avec les autres modules VShield : Analyse E-Mail, Analyse au téléchargement, et Filtre Internet.

IMPORTANT : Pour utiliser les modules Analyse E-Mail, Analyse au téléchargement ou Filtre Internet, vous devez les installer en sélectionnant l'option Personnalisée lors de l'installation de VirusScan. Pour en savoir plus sur cette procédure, reportez-vous au Chapitre 2, « Installation du logiciel VirusScan ».

Si votre ordinateur fonctionne avec Windows NT Workstation v4.0 ou Windows 2000 Professionnel, le moteur d'analyse VShield s'exécute en tant que service Windows NT, appelé McShield, et apparaît dans le panneau de configuration des services Windows.

REMARQUE : McAfee vous recommande de ne pas démarrer ou arrêter le service McShield depuis le panneau de configuration Windows. Il est préférable d'arrêter et de démarrer le moteur d'analyse depuis le panneau de configuration VirusScan. Pour en savoir plus sur l'utilisation du panneau de configuration VirusScan, reportez-vous à la section « Présentation du Panneau de configuration VirusScan » à la page 333

Si votre ordinateur utilise Windows 95 ou Windows 98, le moteur d'analyse s'exécute de la même façon qu'un service Windows chargé dans une plate-forme Windows. Ce service n'est pas disponible dans l'interface utilisateur Windows.

Démarrage automatique du moteur d'analyse

Si le moteur d'analyse VShield ne démarre pas automatiquement, vous pouvez configurer ce type de démarrage dans le panneau de configuration VirusScan.

Procédez comme suit :

1. Cliquez sur **Démarrer** dans la barre des tâches Windows, pointez sur **Paramètres**, puis choisissez **Panneau de configuration**.
2. 

Localisez et double-cliquez sur le panneau de configuration VirusScan pour l'ouvrir.
3. Cliquez sur l'onglet Composants (Figure 4-1).

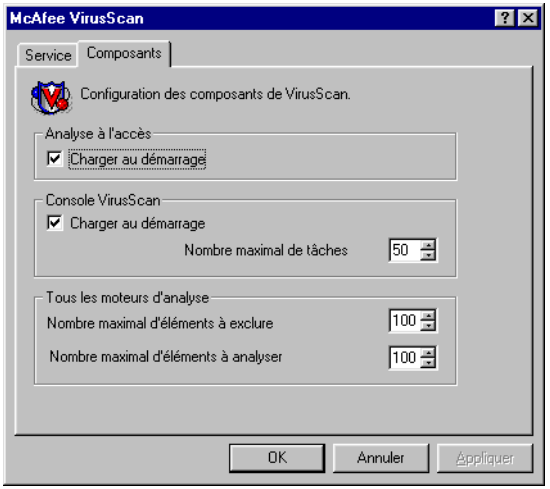

Figure 4-1. Panneau de configuration VirusScan – page Composants

4. Cochez la case **Charger VShield au démarrage** dans la partie supérieure de la page de propriétés Composants.
5. Cliquez sur **OK** pour fermer le panneau de configuration.

Activation du moteur d'analyse VShield et de ses modules

Une fois que vous avez installé tous les composants de VShield, vous pouvez utiliser l'une des quatre méthodes d'activation proposées, appliquant des combinaisons diverses.

REMARQUE : Activer un module signifie également le charger dans la mémoire de l'ordinateur pour être utilisé. Le moteur d'analyse VShield peut démarrer et rester actif dans la mémoire même si l'un de ses modules est inactif.

Méthode 1 : Utiliser le menu contextuel de VShield

Procédez comme suit :

1. Dans la barre d'état système Windows, cliquez avec le bouton droit sur l'icône VShield pour afficher son menu contextuel.
2. Pointez sur **Activation rapide**.
3. Choisissez l'un des noms de module non cochés. Les noms de module cochés sont déjà actifs. Les autres sont inactifs. Si vous utilisez cette méthode pour activer un module, ce dernier reste actif tant que vous ne redémarrez pas votre logiciel VirusScan ou votre ordinateur. À ce stade, l'état affiché par le module dépend du fait que vous l'ayez activé ou désactivé dans la boîte de dialogue Propriétés VirusScan.

L'icône VShield affichera un état différent en fonction de la combinaison de modules que vous activez. Pour en savoir plus sur la signification des différents états d'une icône, reportez-vous à la section « Description de chaque état d'une icône de la barre d'état système VShield » à la page 109.

Méthode 2 : Utiliser la boîte de dialogue État de l'Analyse système

Procédez comme suit :

1. Double-cliquez sur l'icône VShield dans la barre d'état système Windows pour ouvrir la boîte de dialogue État de l'Analyse système (Figure 4-1).

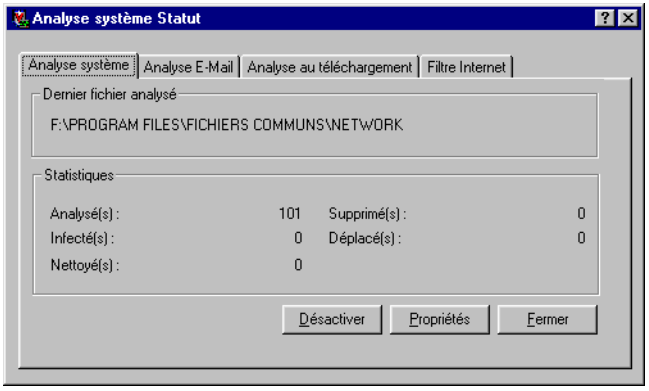

Figure 4-1. Boîte de dialogue État de l'Analyse système

2. Pour chacun des modules que vous souhaitez activer, cliquez sur l'onglet correspondant, puis cliquez sur **Activer**. Dans la page de propriétés de chaque module actif, ce même bouton portera le nom **Désactiver**.
3. Cliquez sur **Fermer** pour fermer la boîte de dialogue.

L'icône VShield affichera un état différent en fonction de la combinaison de modules que vous activez.

Méthode 3 : Utiliser la boîte de dialogue Propriétés de VShield.

Procédez comme suit :

1. Cliquez avec le bouton droit sur l'icône VShield située dans la barre d'état système Windows pour afficher le menu contextuel de VShield, pointez sur **Propriétés**, puis cliquez sur **Analyse système** pour ouvrir la boîte de dialogue Propriétés de VShield.

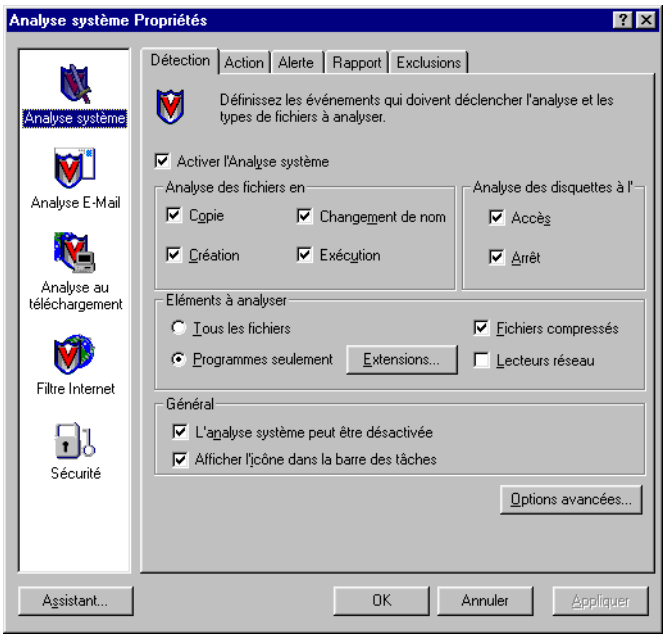

Figure 4-2. Boîte de dialogue Propriétés de VShield

2. Pour chacun des modules que vous souhaitez activer, cliquez sur l'icône correspondante, à gauche de la boîte de dialogue, puis cliquez sur l'onglet Détection.
3. Cochez ensuite la case **Activer** en haut de chaque page.

Le moteur d'analyse active ainsi chacun des modules choisis. L'icône VShield affichera un état différent en fonction de la combinaison de modules que vous activez.

Si vous activez tous les modules, VShield s'affichera dans la barre d'état système Windows, sauf si vous avez décoché la case **Afficher l'icône dans la barre des tâches** dans la page de propriétés Détection de l'Analyse système.

Méthode 4 : Utiliser la console VirusScan

Procédez comme suit :

1. Double-cliquez sur l'icône Console VirusScan dans la barre d'état système Windows pour amener la fenêtre de la console au premier plan.
2. Sélectionnez VShield dans la liste des tâches, puis choisissez **Activer** dans le menu **Tâche**.

   La console active le module Analyse système et tout autre module activé précédemment. Vous ne pouvez pas utiliser cette méthode pour activer des modules individuels, à l'exception du module Analyse système.
3. Cliquez sur le bouton Réduire ou Fermer, dans le coin supérieur droit de la fenêtre de la console, pour afficher à nouveau la console sous forme d'icône dans la barre d'état système.

> **REMARQUE :** *Ne* choisissez pas **Quitter** dans le menu **Tâche**. Ceci provoquerait la fermeture de la console et son retrait de la mémoire. Si vous souhaitez exécuter des tâches planifiées, elle doit être activée.

Description de chaque état d'une icône de la barre d'état système VShield

Le moteur d'analyse VShield affiche quatre états d'icône différents dans la barre d'état système Windows pour indiquer les modules en cours d'exécution. Un module actif est un module activé ou chargé dans la mémoire par le moteur d'analyse VShield et qui est prêt pour analyser des fichiers entrants et sortants. Un module inactif est un module désactivé par le moteur d'analyse VShield. De tels modules n'exécutent aucune opération d'analyse sur les fichiers.

Le tableau suivant présente une description détaillée de chaque état d'une icône :

	Cette icône indique que le moteur d'analyse VShield a démarré et que tous les modules VShield sont actifs
	Cette icône indique que le module Analyse système est actif, mais un ou plusieurs autres modules VShield sont inactifs
	Cette icône indique que le module Analyse système est inactif, mais un ou plusieurs autres modules VShield sont actifs
	Cette icône indique que tous les modules VShield sont inactifs

Utilisation de l'Assistant de configuration VShield

Une fois que vous avez installé le logiciel VirusScan et redémarré votre ordinateur, le moteur d'analyse VShield se charge immédiatement en mémoire et commence à fonctionner avec un jeu d'options par défaut qui vous offre une protection antivirus de base. À moins que vous ne désactiviez VShield ou l'un de ses modules, ou que vous ne l'arrêtiez complètement, vous n'aurez jamais à vous soucier de lancer le moteur d'analyse ou de planifier ses analyses.

Toutefois, pour jouir d'un niveau de sécurité supérieur, vous devez configurer le moteur d'analyse pour qu'il fonctionne avec votre logiciel client e-mail et qu'il puisse analyser soigneusement votre trafic Internet pour y découvrir d'éventuels virus et logiciels destructeurs. L'Assistant de configuration VShield peut vous aider à mettre en œuvre nombre de ces options tout de suite. Par la suite, au fur et à mesure que vous vous familiariserez avec le moteur d'analyse et avec le degré de vulnérabilité de votre système aux logiciels dangereux, vous pourrez personnaliser le programme pour qu'il fonctionne au mieux dans votre environnement.

Pour démarrer l'Assistant de configuration VShield :

1. Cliquez avec le bouton droit sur l'icône VShield  , située dans la barre d'état système Windows, pour afficher le menu contextuel de VShield, pointez sur **Propriétés**, puis cliquez sur **Analyse système** pour ouvrir la boîte de dialogue Propriétés de VShield (voir Figure 4-2 à la page 108).
2. Cliquez sur **Assistant** dans le coin inférieur gauche de la boîte de dialogue pour afficher l'écran d'accueil de l'Assistant de configuration (Figure 4-3 à la page 111).

Figure 4-3. Assistant de configuration VShield – écran d'accueil

3. Cliquez sur **Suivant>** pour afficher l'écran de configuration de l'Analyse système (voir Figure 4-4).

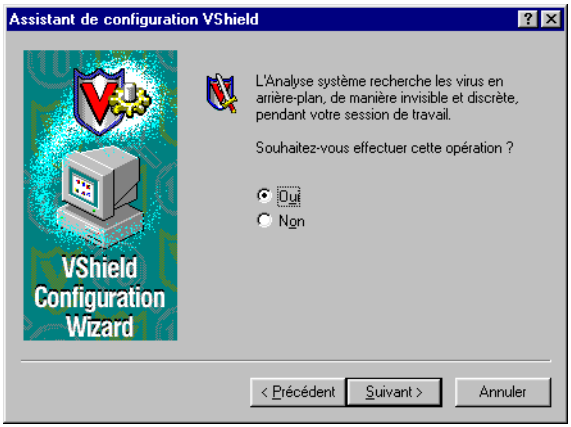

Figure 4-4. Assistant de configuration VShield – écran Analyse système

C'est ici que vous pouvez demander au moteur d'analyse VShield de rechercher d'éventuels virus dans les fichiers susceptibles d'être infectés, à chaque fois que vous les ouvrez, lancez, copiez, enregistrez ou modifiez de toute autre façon. Parmi les fichiers susceptibles d'être infectés figurent différents types de fichiers exécutables et de fichiers document comportant des macros, comme les fichiers Microsoft Office. Le module Analyse système analysera également les fichiers stockés sur disquette à chaque fois que vous y effectuerez une opération de lecture ou d'écriture ou bien lorsque vous éteindrez votre ordinateur.

S'il trouve un virus, le module Analyse système déclenchera une alerte sonore et vous demandera quoi faire. Le module enregistrera également ses actions et fournira un résumé de ses paramètres en cours dans un fichier journal que vous pourrez visualiser ultérieurement.

4. Pour activer ces fonctions, cliquez sur **Oui**, puis sur **Suivant>**. Sinon, cliquez sur **Non**, puis sur **Suivant>** pour continuer.

   L'écran de l'Assistant Analyse E-Mail s'affiche (Figure 4-5).

Figure 4-5. Assistant de configuration VShield – écran Analyse E-Mail

5. Cochez la case **Activer l'Analyse E-Mail**, puis cochez la case correspondant au type de client e-mail que vous utilisez. Vous avez le choix entre les options suivantes :

   - **Clients de messagerie Internet.** Cochez cette case si vous utilisez un client e-mail exploitant le protocole POP-3 (Post Office Protocol) ou le protocole SMTP (Simple Mail Transfer Protocol) qui envoie et reçoit du courrier électronique Internet classique directement ou via une connexion par modem. Si vous utilisez le courrier électronique chez vous avec Netscape Mail, America Online, ou des clients largement répandus comme Eudora de Qualcomm ou Outlook Express de Microsoft, c'est cette option qu'il vous faut choisir.
   - **Activer la messagerie commerciale.** Cochez cette case si vous utilisez un système e-mail propriétaire au travail ou dans un environnement réseau. La plupart de ces systèmes utilisent un serveur de réseau central pour recevoir et distribuer le courrier que les utilisateurs individuels s'envoient entre eux à partir d'applications clientes. De tels systèmes peuvent envoyer et recevoir du courrier de l'extérieur du réseau ou depuis Internet, mais ils le font en général en passant par une application « passerelle » exécutée sur le serveur.

Le module Analyse E-Mail prend en charge les systèmes de messagerie commerciale qui appartiennent aux deux catégories suivantes :

- **Lotus cc:Mail.** Cliquez sur ce bouton si vous utilisez une version 6.x ou ultérieure de cc:Mail ; ces versions utilisent un protocole propriétaire de Lotus pour l'envoi et la réception du courrier électronique.
- **Client e-mail conforme à la norme MAPI**. Cliquez sur ce bouton si vous utilisez Microsoft Exchange ou Microsoft Outlook comme système de messagerie commerciale.

Spécifiez le système e-mail que vous utilisez, puis cliquez sur **Suivant>** pour continuer.

❑ **REMARQUE :** Si vous utilisez les deux systèmes e-mail, cochez les deux cases. Notez cependant que le module Analyse E-Mail ne prend en charge qu'un seul type de système de messagerie*commerciale* à la fois. Si vous avez besoin de vérifier quel système e-mail est utilisé par votre entreprise, posez la question à l'administrateur de votre réseau.

Ne confondez pas Microsoft Outlook et Microsoft Outlook Express. Même si les deux programmes portent des noms similaires, Outlook 97 et Outlook 98 sont des systèmes de messagerie commerciale conformes à la norme MAPI, alors que Outlook Express utilise les protocoles POP-3 et SMTP pour l'envoi et la réception du courrier. Pour en savoir plus sur ces programmes, consultez votre documentation Microsoft.

L'écran suivant de l'Assistant de configuration permet de définir les options du module Analyse au téléchargement de VShield (Figure 4-6).

Figure 4-6. Assistant de configuration VShield – écran Analyse au téléchargement

6. Pour que le module Analyse au téléchargement recherche la présence de virus éventuels dans chacun des fichiers que vous téléchargez sur Internet, cochez la case **Oui, analyser les fichiers téléchargés**, puis cliquez sur **Suivant>** pour continuer.

   Ce module recherchera les virus éventuels dans les fichiers les plus susceptibles d'être infectés et analysera les fichiers compressés au fur et à mesure de leur réception.

   Sinon, cochez la case **Non, ne pas analyser les fichiers téléchargés**, puis cliquez sur **Suivant>** pour continuer.

   Le panneau suivant de l'Assistant de configuration permet de sélectionner les options concernant le module Filtre Internet de VShield (Figure 4-7).

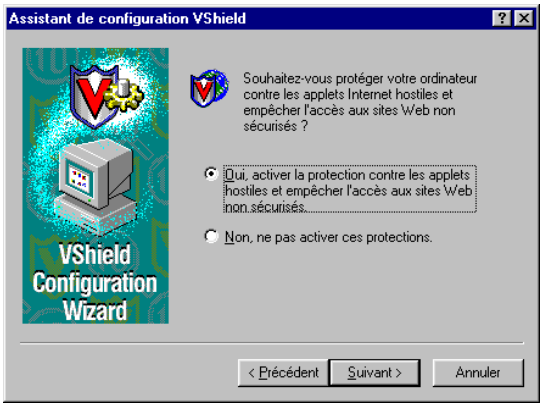

Figure 4-7. Assistant de configuration VShield – écran Filtre Internet

7. Sélectionnez **Oui, activer la protection contre les applets hostiles et empêcher l'accès aux sites Web non sécurisés**, puis cliquez sur **Suivant>** pour que le module Filtre Internet intercepte les objets Java et ActiveX dangereux et bloque l'accès aux sites Internet susceptibles d'endommager votre système.

   Le module Filtre Internet gère une liste d'objets et de sites dangereux qu'il utilise pour vérifier les sites que vous visitez et les objets que vous rencontrez. S'il trouve une correspondance, il peut soit bloquer l'accès automatiquement, soit vous proposer de l'autoriser ou de l'interdire vous-même.

   Pour désactiver cette fonction, sélectionnez **Non, ne pas activer ces protections**, puis cliquez sur **Suivant>** pour continuer.

   Le dernier écran de l'Assistant récapitule les options que vous avez sélectionnées (Figure 4-8).

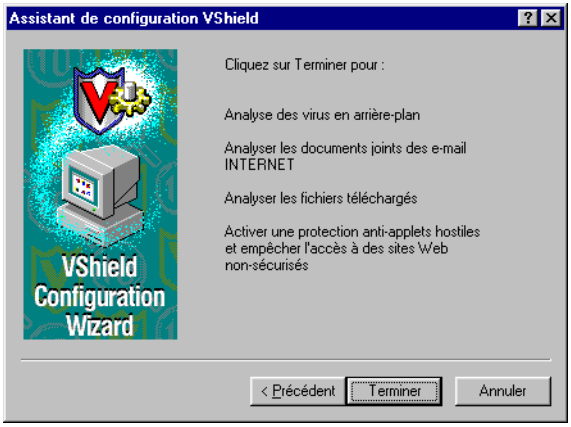

Figure 4-8. Assistant de configuration VShield – écran récapitulatif

8. Si la liste récapitulative reprend correctement vos choix, cliquez sur **Terminer** pour enregistrer vos modifications et revenir à la boîte de dialogue Propriétés de VShield. Sinon, cliquez sur **<Précédent** pour modifier les options choisies, ou sur **Annuler** pour revenir à la boîte de dialogue Propriétés de VShield sans enregistrer vos modifications.

Paramétrage des propriétés du moteur d'analyse VShield

Pour que le moteur d'analyse VShield puisse vous assurer une performance optimale sur votre ordinateur ou votre environnement réseau, il faut que vous lui indiquiez ce que vous voulez qu'il analyse, ce qu'il doit ignorer, ce qu'il doit faire en cas de détection d'un virus ou d'un autre logiciel destructeur et comment il doit vous en avertir. Vous pouvez utiliser l'Assistant de configuration pour activer la plupart des options de protection du moteur d'analyse, mais si vous voulez avoir la maîtrise des performances du programme et de sa capacité à s'adapter à vos besoins, y compris la possibilité de protéger vos paramètres par un mot de passe, sélectionnez les options qui vous intéressent dans la boîte de dialogue Propriétés de VShield.

La boîte de dialogue Propriétés de VShield se compose d'une série de pages de propriétés qui contrôlent le paramétrage de chaque module du programme. Pour sélectionner les options qui vous intéressent, cliquez sur l'icône du module approprié, puis cliquez tour à tour sur chaque onglet de la boîte de dialogue Propriétés de VShield.

Pour ouvrir la boîte de dialogue Propriétés de VShield, cliquez avec le bouton droit sur l'icône VShield, située dans la barre d'état système Windows, pour afficher le menu contextuel de VShield, pointez sur **Propriétés**, puis cliquez sur **Analyse système**.

La boîte de dialogue s'affiche avec l'icône Analyse système sélectionnée (Figure 4-9).

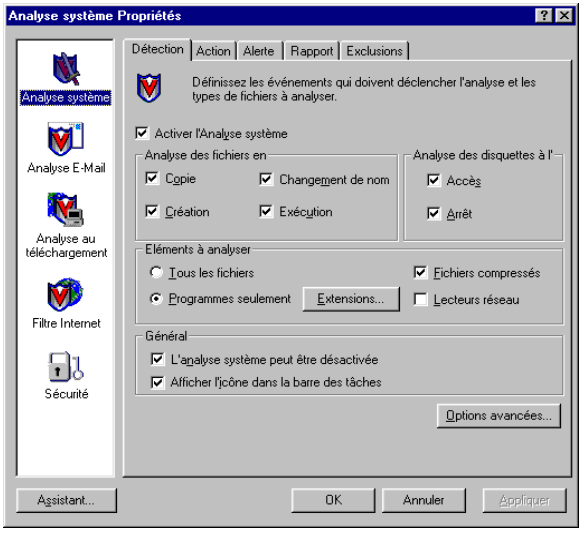

Figure 4-9. Boîte de dialogue Propriétés de l'analyse du système – page Détection

Configuration du module Analyse système

Le module Analyse système de VShield se trouve au cœur du moteur d'analyse VShield. Il analyse les fichiers provenant de différentes sources, y compris ceux qui lui sont envoyés par les autres modules VShield, tels que les fichiers téléchargés depuis un site Internet et les messages électroniques. Le module Analyse système peut rechercher la présence éventuelle de virus dans votre système à chaque fois que vous ouvrez, lancez, copiez, enregistrez, renommez ou modifiez des fichiers sur votre disque dur de quelque façon que ce soit, et ceci sur tout support amovible relié à votre ordinateur, ou sur des lecteurs réseau mappés sur votre système. Il peut également détecter des virus à chaque fois que vous effectuez une opération de lecture ou d'écriture sur une disquette. Le module Analyse système met également à votre disposition une option avancée, l'analyse heuristique, que vous pouvez activer afin que le moteur d'analyse puisse détecter des virus non identifiés ou non classés.

Le module peut exécuter différentes opérations automatiques en cas de détection d'un virus et indiquer l'action entreprise en réponse à cette infection, soit par un message d'alerte, qu'il émet au moment d'appliquer la mesure corrective, soit dans un fichier journal que vous pouvez consulter à tout moment. Vous pouvez également le configurer pour qu'il vous demande l'action à entreprendre en cas de détection d'un virus.

Le module Analyse système inclut également des options que vous pouvez sélectionner pour indiquer au moteur d'analyse VShield d'afficher une icône d'état dans la barre des tâches Windows ; vous saurez ainsi d'un simple coup d'œil quels sont les modules VShield actifs. Il existe par ailleurs une autre option qui vous permet de désactiver le module Analyse système. Il se peut que cette option ne soit pas disponible si vous exécutez le logiciel VirusScan en mode sécurisé.

Pour sélectionner les options qui vous intéressent, cliquez sur l'icône Analyse système, située à gauche de la boîte de dialogue Propriétés de l'analyse du système, pour afficher les pages de propriétés de ce module. Les sections suivantes présentent une description des différentes options de configuration disponibles dans ce module.

Sélection des options de détection

Lorsque vous l'activez pour la première fois, le module Analyse système prend comme hypothèse de départ que vous souhaitez qu'il détecte les virus éventuels à chaque fois que vous travaillez avec un fichier susceptible d'être infecté, que ce soit sur le disque dur ou sur disquette et que ce soit une opération de lecture ou d'écriture sur le disque dur. Le module Analyse système examinera également les fichiers compressés par défaut mais, à moins que vous n'ayez activé cette option, il n'appliquera pas l'analyse heuristique.

REMARQUE : La présentation et les options proposées dans cette page de propriétés peuvent varier en fonction du système d'exploitation utilisé par votre ordinateur.

Pour modifier ces options, procédez comme suit :

1. Assurez-vous que la case **Activer l'Analyse système** est cochée.

   Le fait de cocher cette case active toutes les autres options de cette page de propriétés. Décochez cette case pour désactiver toutes les options de configuration de cette page de propriétés et éviter que le module Analyse système examine votre système.

2. Indiquez au module le moment et l'endroit où il doit rechercher d'éventuels virus. Vous pouvez lui demander d'

   - **analyser les fichiers lorsqu'ils sont utilisés**. À chaque fois que vous ouvrez, copiez, enregistrez, renommez ou utilisez de toute autre façon des fichiers sur votre disque dur, le code d'un virus peut s'exécuter et contaminer d'autres fichiers.

     Pour éviter ce risque sur les ordinateurs qui exécutent Windows NT Workstation v4.0 ou Windows 2000 Professionnel, cochez à la fois les cases **Fichiers entrants** et **Fichiers sortants**. Sur les ordinateurs qui exécutent Windows 95 ou Windows 98, cochez les cases **Exécution**, **Copie**, **Création** et **Changement de nom** pour une protection totale.

     Les fichiers « entrants » sont des fichiers que votre ordinateur ou un autre système du réseau enregistre ou écrit sur des disques durs locaux reliés à votre ordinateur ou sur des disques durs du réseau que vous avez mappés sur votre système. Pour inclure dans l'analyse des lecteurs réseau mappés sur votre système, cochez également la case **Lecteurs réseau**.

     Votre système peut recevoir des données provenant de la mémoire de l'ordinateur, d'une disquette insérée dans le lecteur de disquette, d'autres systèmes, du courrier électronique ou de toute autre source, puis écrire ces données sur un fichier de votre disque dur. Le moteur d'analyse VShield traite toutes ces informations comme des données « entrantes »

     Les fichiers « sortants » sont des fichiers que votre ordinateur ou un autre système du réseau lit à partir de disques durs locaux reliés à votre ordinateur ou à partir de disques réseau mappés sur votre système. Pour inclure dans l'analyse des lecteurs réseau mappés sur votre système, cochez également la case **Lecteurs réseau**.

À chaque fois que votre ordinateur ou un autre système lit des données à partir d'un fichier stocké sur un disque dur local relié à votre système ou à partir d'un disque réseau mappé sur votre système, le module Analyse système traite ces informations comme des données « sortantes ».

❑ **REMARQUE :** Si vous disposez de lecteurs réseau mappés sur votre ordinateur et à partir desquels vous copiez des fichiers, ou si d'autres utilisateurs du réseau copient des fichiers à partir de votre ordinateur, McAfee vous recommande vivement d'installer le moteur d'analyse VShield à la fois sur votre ordinateur et sur celui qui « possède » le lecteur réseau. Vous devez également cocher toutes les cases de la zone Analyser, dans la page Détection, plus la case **Lecteurs réseau** dans la zone Éléments à analyser.

Votre exemplaire du module Analyse système examinera ensuite les fichiers à chaque opération de lecture effectuée sur votre disque dur, puis à chaque opération d'écriture effectuée sur le disque dur de l'ordinateur de destination. Si le module Analyse système est activé sur l'ordinateur de destination, il analysera également le fichier à chaque opération d'écriture sur le lecteur réseau, à condition que la case **Fichiers entrants** soit cochée dans ce module.

Si vous avez tendance à copier des fichiers à partir d'un serveur et que ce serveur ne copie pas des fichiers à partir de votre ordinateur, et s'il en va de même pour d'autres utilisateurs du réseau, il est préférable de configurer vos ordinateurs pour analyser uniquement les fichiers qu'ils écrivent ou qu'ils lisent sur leurs disques durs afin d'éviter qu'un même fichier soit analysé par deux ordinateurs. Pour y parvenir, vous devez configurer les ordinateurs de façon identique. Sinon, un ordinateur qui analyse uniquement les fichiers sortants pourrait copier un fichier infecté à partir d'un serveur qui n'analyse que les fichiers sortants.

- **Analyser les fichiers sur disquette**. Les virus de zone système peuvent se dissimuler dans les zones système de toute disquette formatée, puis se charger en mémoire dès que votre ordinateur accède au lecteur de disquette. Cochez la case **Accès** pour que le module Analyse système examine les disquettes à chaque fois que votre ordinateur y accède, que ce soit en lecture ou en écriture. Cochez la case **Arrêt** pour que le module analyse toute disquette présente dans votre lecteur au moment ou vous éteignez votre ordinateur.

Cela permet d'éviter qu'un virus ne soit chargé au moment où votre ordinateur accède au lecteur de disquette au cours de sa phase de démarrage.

3. Spécifiez les types de fichiers que le module Analyse système doit examiner. Vous pouvez :

   - **Analyser les fichiers compressés.** Cochez la case **Fichiers compressés** pour que le module recherche les virus éventuels dans les fichiers compressés ou dans les fichiers d'archives. Cette option permet d'éviter que les virus ne se propagent à partir de fichiers compressés, car le module décompresse les fichiers avant de les analyser. L'activation de cette option peut augmenter le délai requis pour l'analyse d'un jeu de fichiers spécifique pendant que vous travaillez sur votre ordinateur.

     REMARQUE : Lorsque le module Analyse système examine un fichier d'archives, il analyse uniquement le fichier d'archives lui-même et non les fichiers compressés qu'il contient. Pour savoir quels sont les fichiers et les archives examinés par le module, reportez-vous à la section « Liste en cours des fichiers compressés analysés » à la page 352.

   - **Sélectionner les types de fichiers à analyser.** D'ordinaire, les virus ne peuvent infecter les fichiers qui ne contiennent pas de code exécutable, que ce soit du code de script, de macro ou binaire. C'est pourquoi vous pouvez sans risque réduire la portée des opérations d'analyse afin que le module ne vérifie que les fichiers les plus susceptibles d'être infectées. Pour ce faire, cliquez sur le bouton **Fichiers programme uniquement**.

     Pour afficher ou désigner les extensions de fichier que le module Analyse système doit examiner, cliquez sur **Extensions** pour ouvrir la boîte de dialogue Extensions de fichiers programme (Figure 4-10).

Figure 4-10. Boîte de dialogue Extensions de fichiers programme

Reportez-vous aux sections voir « Ajout d'extensions de fichier pour analyse » à la page 345 et « Liste en cours des extensions de noms de fichiers vulnérables » à la page 346 pour connaître les extensions de nom de fichier pouvant être analysées par défaut par le module Analyse système et ajouter ou modifier des éléments dans cette liste.

- **Analyser tous les fichiers.** Cliquez sur le bouton **Tous les fichiers** pour que le module Analyse système examine tous les fichiers, quelle que soit leur extension, à chaque fois que vous ou un processus système y apporte une modification.
- **Analyser les lecteurs réseau.** Cochez la case **Lecteurs réseau** si vous souhaitez que le module Analyse système recherche des virus sur les lecteurs mappés sur votre système.

REMARQUE : Si votre système comporte des disques réseau, le module Analyse système traite tout fichier écrit sur ces lecteurs comme des fichiers « entrants » et tout fichier lu à partir de ces lecteurs comme des fichiers « sortants ». Pour garantir une protection maximale, cochez ces deux cases dans la zone Analyse lorsque vous activez l'option **Lecteurs réseau**.

---

4. Sélection des options de gestion du logiciel VShield. Ces options vous permettent de contrôler vos échanges avec le moteur d'analyse VShield. Vous pouvez :
   - **Désactiver le module Analyse système à volonté.** Cochez la case **L'Analyse système peut être désactivée** pour avoir la possibilité de désactiver ce module. Notez que McAfee vous recommande de laisser le module Analyse système activé pour une protection maximale. Lorsque vous décochez cette case, les options **Quitter** et **Analyse système** disparaissent du menu contextuel de VShield, de même que le bouton **Désactiver** de la boîte de dialogue État de VShield.

ASTUCE : Pour être sûr que personne d'autre que vous ne puisse désactiver le moteur d'analyse VShield, ou pour imposer une stratégie de sécurité antivirus parmi les utilisateurs de VirusScan sur votre réseau, décochez cette case, puis protégez vos paramètres avec un mot de passe. Ceci empêchera d'autres utilisateurs de désactiver le moteur d'analyse à partir de la console VirusScan ou de la boîte de dialogue Propriétés de VShield. Pour plus de détails, reportez-vous à la section voir « Configuration du module Sécurité » à la page 181.

Vous pouvez également exécuter la totalité du produit VirusScan en mode sécurisé, ce qui désactive l'accès à toutes les options configurables. Pour en savoir plus sur l'installation du logiciel VirusScan en mode sécurisé, reportez-vous à la section voir « Procédure d'installation » à la page 45.

- **Afficher l'icône VShield dans la barre d'état système Windows.** Cochez la case **Afficher l'icône dans la Barre des tâches** pour que le moteur d'analyse VShield affiche l'icône dans la barre d'état système. L'état de l'icône dans la barre d'état système dépend des modules VShield que vous avez activés. Pour plus de détails, reportez-vous à la section « Description de chaque état d'une icône de la barre d'état système VShield » à la page 109.

  Un double clic sur l'icône provoque l'affichage de la boîte de dialogue État de VShield. Un clic droit sur l'icône provoque l'affichage d'un menu contextuel. Pour plus de détails, reportez-vous aux sections voir « Utilisation du menu contextuel de VShield » à la page 185 et « Recherche des informations d'état du logiciel VShield » à la page 193.

5. activer l'analyse heuristique. Sélectionnez l'option **Options avancées** pour ouvrir la boîte de dialogue Paramètres d'analyse avancés (Figure 4-11).

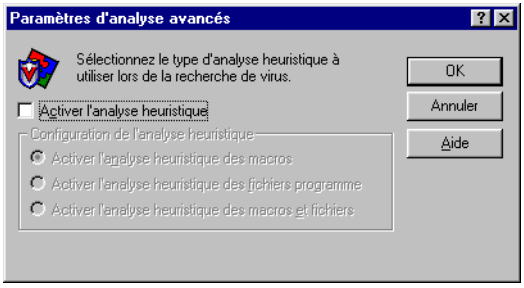

Figure 4-11. Boîte de dialogue Paramètres d'analyse avancés

La technologie d'analyse heuristique permet au module Analyse système de reconnaître les nouveaux virus à partir de leur ressemblance avec des virus semblables déjà identifiés. Pour ce faire, le programme recherche des caractéristiques propres aux virus dans les fichiers que vous lui avez demandé d'analyser. S'il détecte un nombre suffisant de caractéristiques dans un fichier, le module identifie le fichier comme étant potentiellement infecté par un nouveau virus ou un virus non identifié.

Le module Analyse système recherche en même temps des caractéristiques de fichier excluant la possibilité d'une infection par un virus, c'est pourquoi il ne vous donnera que rarement des indications erronées sur la présence d'un virus. À moins d'être certain que votre fichier ne contient *pas* de virus, vous devez apporter aux infections « probables » les mêmes précautions que vous apportez aux infections confirmées.

Lorsque vous démarrez le module Analyse système, aucune option d'analyse heuristique n'est activée par défaut. Pour activer l'analyse heuristique, procédez comme suit :

a. Cochez la case **Activer l'analyse heuristique**. Les options proposées dans le reste de la boîte de dialogue deviennent accessibles.

b. Sélectionnez les types d'analyses heuristiques que vous souhaitez utiliser. Vous avez le choix entre les options suivantes :

   – **Activer l'analyse heuristique des macros.** Sélectionnez cette option pour que le module Analyse système identifie d'abord tous les fichiers Microsoft Word, Microsoft Excel et autres fichiers Microsoft Office incorporant des macros et compare ensuite le code de la macro avec sa base de données de définitions de virus. Si la correspondance est exacte, le module identifie le nom du virus ; pour les signatures codées qui ressemblent à celles des virus existants, il vous informe qu'il a détecté un virus de macro « probable ».

   – **Activer l'analyse heuristique des fichiers programme.** Sélectionnez cette option si vous souhaitez que le module Analyse système localise de nouveaux virus dans les fichiers programme en examinant les caractéristiques des fichiers et en les comparant avec celles figurant sur une liste de virus connus. Lorsqu'il détecte un fichier ayant un certain nombre de caractéristiques, le module l'identifie comme étant potentiellement infecté.

   – **Activer l'analyse heuristique des macros et fichiers programme.** Sélectionnez cette option si vous souhaitez que le module utilise les deux types d'analyse heuristique. McAfee vous recommande d'utiliser cette option pour une protection antivirus optimale.

> **REMARQUE :** Le module Analyse système n'utilise les techniques d'analyse heuristique que sur les types de fichiers que vous désignez dans la boîte de dialogue Extensions de fichiers programme. Si vous décidez d'analyser **Tous les fichiers**, le module appliquera l'analysera heuristique à tous les types de fichiers.

c. Cliquez sur **OK** pour enregistrer vos paramètres et revenir à la boîte de dialogue Propriétés de VShield.

6. Cliquez sur l'onglet Action pour sélectionner d'autres options du module Analyse système. Pour enregistrer vos modifications sans fermer la boîte de dialogue Propriétés de l'analyse du système, cliquez sur **Appliquer**. Pour enregistrer vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans enregistrer vos modifications, cliquez sur **Annuler**.

> **REMARQUE :** Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

Sélection des options d'action

Lorsque le module Analyse système détecte un virus, deux cas de figure se présentent : soit il vous demande comment traiter le fichier infecté, soit il exécute automatiquement une action que vous avez définie précédemment. Utilisez la page de propriétés Action pour spécifier les actions que le module doit vous proposer en cas de détection d'un virus et celles qu'il doit mettre en œuvre automatiquement.

> **REMARQUE :** La présentation et les options proposées dans cette page de propriétés peuvent varier en fonction du système d'exploitation utilisé par votre ordinateur.

Procédez comme suit :

1. Cliquez sur l'onglet Action dans le module Analyse système pour afficher la page de propriétés correspondante (Figure 4-12 à la page 125).

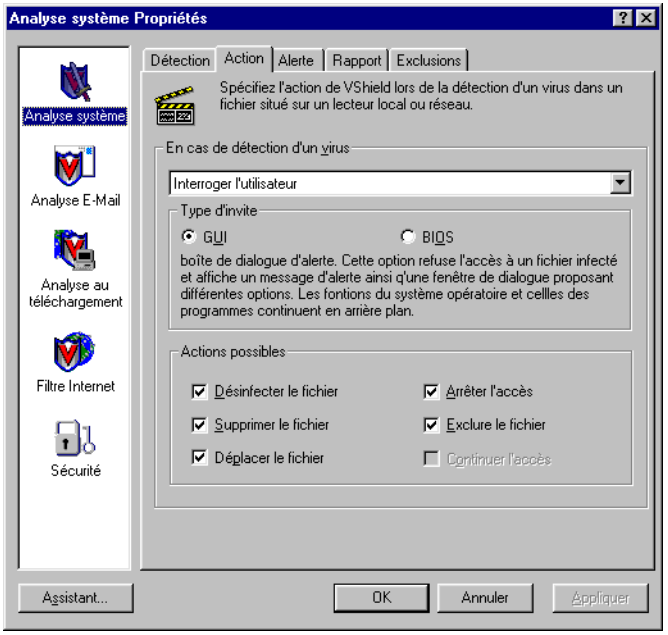

Figure 4-12. Boîte de dialogue Propriétés de l'Analyse du système – page Action

2. Sélectionnez une réponse dans la liste *En cas de détection d'un virus*. La zone située immédiatement sous la liste changera pour vous proposer des options supplémentaires.

❑ **REMARQUE :** Si vous sélectionnez **Interroger l'utilisateur** dans la liste, cliquez sur l'onglet Alerte pour préciser si le module Analyse système doit utiliser un message, un signal sonore ou les deux à la fois pour vous avertir en cas d'infection. Pour plus de détails, reportez-vous à la section voir « Sélection des options d'alerte » à la page 128. Pour en savoir plus sur les options de réponse en cas d'infection, reportez-vous à la section « Options de réponse lorsque le moteur d'analyse VShield détecte un programme malicieux » à la page 77.

---

3. La liste vous propose les options suivantes :

   - **Interroger l'utilisateur.** Sélectionnez cette option si vous souhaitez que le module Analyse système vous demande quoi faire lorsqu'il détecte un virus — le module affichera alors un message d'alerte et vous proposera plusieurs actions possibles.

Si votre ordinateur utilise Windows 95 ou Windows 98 et que vous sélectionnez cette option, le système affiche l'option Type d'invite (Figure 4-13 à la page 126). Choisissez les méthodes d'alerte que le module Analyse système doit utiliser en cas de détection d'un virus.

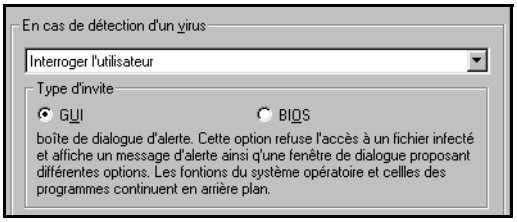

Figure 4-13. zone Type d'invite

Vous avez le choix entre les options suivantes :

- **BIOS.** Cliquez sur ce bouton pour afficher un message d'alerte en mode plein écran comportant plusieurs options de réponse, y compris la possibilité de continuer sans prendre aucune mesure corrective à l'encontre du virus. Dans l'attente de votre réponse, ce mode bloque complètement le fonctionnement de votre système.
- **GUI.** Cliquez sur ce bouton pour afficher un message d'alerte graphique standard incluant plusieurs options de réponse. Ce message d'alerte n'inclut pas l'option Continuer l'accès. Pendant que vous sélectionnez vos options, le système continue à exécuter normalement ses tâches en arrière-plan.

Dans la zone Actions possibles, située en bas de la page de propriétés, sélectionnez les options de réponse à afficher dans ce message d'alerte. Pour chaque case que vous cochez dans cette zone, un bouton d'option apparaîtra dans le message d'alerte que le module affichera en cas de détection d'un virus. Ainsi, si vous cochez par exemple la case **Supprimer le fichier**, le message d'alerte comportera un bouton d'option **Supprimer**. Vous avez le choix entre les options suivantes :

- **Désinfecter le fichier.** Cette option demande au module d'essayer de supprimer le code de virus dans le fichier infecté. Si vous avez activé la fonction de rapport, le module enregistrera l'événement dans un journal à chaque fois qu'il parviendra ou non à nettoyer un fichier infecté.
- **Supprimer le fichier.** Cette option demande au module de supprimer immédiatement le fichier infecté.

- **Déplacer le fichier.** Cette option demande au module de placer le fichier infecté dans un dossier de quarantaine. La version GUI du message d'alerte affichera un bouton **Déplacer le fichier** pour vous permettre de localiser le dossier de quarantaine à utiliser.
- **Arrêter l'accès.** Cette option demande au module d'empêcher l'accès au fichier à l'utilisateur qui a tenté de le modifier, y compris vous.
- **Exclure le fichier.** Cette option demande au module d'ignorer ce fichier dans l'analyse en cours et dans les opérations d'analyse à venir.
- **Continuer l'accès.** Cette option laisse le fichier intact et dans son emplacement d'origine sur votre ordinateur et vous autorise à l'ouvrir, le copier, le renommer ou le modifier de quelque façon que ce soit par la suite. Utilisez cette option uniquement si vous êtes certain que le fichier signalé par le module Analyse système n'est pas infecté. Pour conserver les fichiers infectés comme des exemples de virus, McAfee vous recommande plutôt de les placer dans un dossier de quarantaine.

  ❑ **REMARQUE :** L'option n'est disponible que sur les ordinateur qui utilisent Windows 95 ou Windows 98 et à condition que vous choisissiez **BIOS** comme mode d'invite.

- **Déplacer automatiquement les fichiers infectés**. Sélectionnez cette option pour que le module déplace les fichiers infectés vers un dossier de quarantaine dès leur détection.

  Par défaut, le module place ces fichiers dans un dossier nommé Infecté, situé dans le répertoire du programme VirusScan. Vous pouvez entrer un autre nom de dossier dans la zone de texte affichée ou cliquer sur **Parcourir** pour retrouver le fichier voulu sur votre disque dur.

- **Nettoyer automatiquement les fichiers infectés.** Sélectionnez cette option de réponse pour que le module supprime le code de virus dans le fichier infecté dès sa détection. Si le module ne parvient pas à supprimer le virus, il interdira l'accès au fichier et notera l'incident dans son fichier journal. Pour plus de détails, reportez-vous à la section « Sélection des options de rapport » à la page 130.

- **Supprimer automatiquement les fichiers infectés.** Sélectionnez cette option pour que le module supprime immédiatement tout fichier infecté détecté. Assurez-vous d'avoir activé la fonction de rapport afin de disposer d'une liste des fichiers supprimés par le module. Consultez ensuite cette dernière pour connaître les fichiers supprimés à restaurer à partir des copies de sauvegarde. Si le module ne parvient pas à supprimer un fichier infecté, il notera l'incident dans son fichier journal.
- **Refuser l'accès aux fichiers infectés et continuer.** Sélectionnez cette option pour que le module étiquette le fichier « accès interdit » et continue ses opérations d'analyse. N'utilisez cette option que si vous prévoyez de laisser votre ordinateur sans surveillance pendant des périodes prolongées.

  Si vous activez parallèlement la fonction de rapport du module Analyse système (voir « Sélection des options de rapport » à la page 130), le programme enregistrera les noms de tous les virus détectés, ainsi que les noms des fichiers infectés, que vous pourrez ainsi supprimer dès que vous en aurez l'occasion.

4. Cliquez sur l'onglet Alerte pour sélectionner d'autres options du module Analyse système. Pour enregistrer vos modifications sans fermer la boîte de dialogue Propriétés de l'analyse du système, cliquez sur **Appliquer**. Pour enregistrer vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans enregistrer vos modifications, cliquez sur **Annuler**.

REMARQUE : Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

Sélection des options d'alerte

Une fois que vous l'avez configuré avec les options de réponse qui vous intéressent dans la page Action, vous pouvez laisser le module Analyse système rechercher et éliminer automatiquement les virus de votre système au fur et à mesure qu'il les trouve, pratiquement sans aucune autre intervention de votre part. Si, toutefois, vous souhaitez que le module vous informe dès qu'il détecte un virus afin que vous puissiez prendre les mesures adéquates, vous devez le configurer de telle sorte qu'il envoie un message d'alerte à vous ou aux autres utilisateurs.

Procédez comme suit :

1. Cliquez sur l'onglet Alerte dans le module Analyse système pour afficher la page de propriétés correspondante (Figure 4-14 à la page 129).

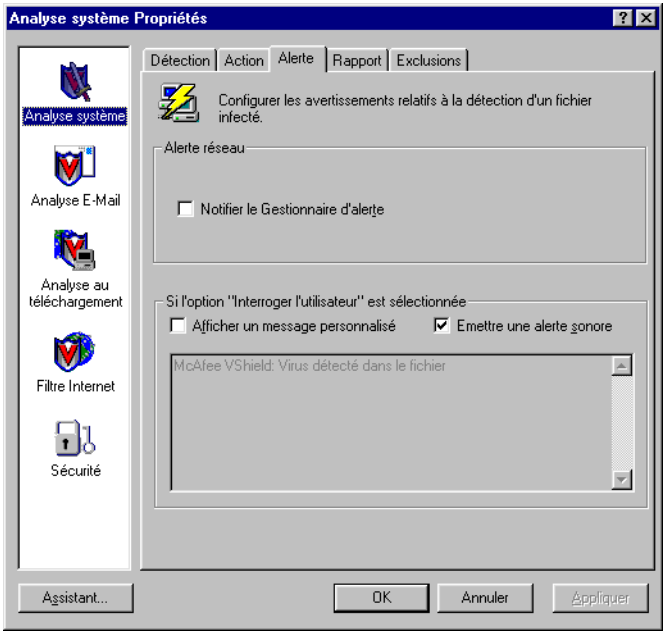

Figure 4-14. Boîte de dialogue Propriétés de l'analyse du système – page Alerte

2. Cochez la case **Notifier le Gestionnaire d'alerte** pour que le module envoie des messages d'alerte au Gestionnaire d'alerte qui les transmettra.

   Le Gestionnaire d'alerte est un composant indépendant du logiciel McAfee qui regroupe des messages d'alerte et utilise diverses méthodes pour les envoyer aux destinataires que vous désignez. Le module Analyse système enverra ces messages d'alerte avec succès uniquement si vous avez installé l'utilitaire de configuration cliente du Gestionnaire d'alerte. Pour plus de détails, reportez-vous à la section voir « Utilisation de l'utilitaire de Configuration cliente du Gestionnaire d'alerte » à la page 338.

   Vous pouvez transmettre des messages d'alerte directement à un serveur du Gestionnaire d'alerte. Sinon, vous pouvez les envoyer en tant que fichiers texte (.ALR) à un répertoire d'alerte centralisée que le serveur du Gestionnaire d'alerte interroge régulièrement.

   ❑ **REMARQUE :** Si vous décochez cette case, le module Analyse système n'enverra pas des messages d'alerte via le Gestionnaire d'alerte, mais tous les autres messages d'alerte que vous configurez dans cette page de propriétés resteront intacts.

   ---

3. Cochez la case **Émettre une alerte sonore** pour que le module envoie un signal sonore à chaque fois qu'il trouve un fichier infecté.

   Vous pouvez modifier le paramétrage de cette option à condition d'avoir sélectionné **Interroger l'utilisateur** dans la page de propriétés Action. Sinon, la case à cocher Émettre une alerte sonore affichera et utilisera le paramètre que vous lui avez attribué la dernière fois que vous avez sélectionné l'option **Interroger l'utilisateur**. Le module émettra le signal sonore standard du système ou exécutera le fichier .WAV que vous avez configuré sur votre ordinateur.

4. Cochez la case **Afficher un message personnalisé** pour que le module ajoute un message personnalisé au texte du message qu'il affiche lorsqu'il trouve un fichier infecté.

   À l'égard de l'alerte sonore, vous pouvez modifier le paramétrage de cette option à condition d'avoir sélectionné **Interroger l'utilisateur** dans la page de propriétés Action. Si vous ne sélectionnez pas cette option dans la page Action, aucun message d'alerte ou message personnalisé ne s'affichera même si vous avez coché la case Afficher un message personnalisé.

5. Entrez le message que le module doit afficher dans la zone de texte. Vous pouvez entrer 250 caractères maximum.

6. Cliquez sur l'onglet Rapport pour sélectionner d'autres options du module Analyse système. Pour enregistrer vos modifications sans fermer la boîte de dialogue Propriétés de l'analyse du système, cliquez sur **Appliquer**. Pour enregistrer vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans enregistrer vos modifications, cliquez sur **Annuler**.

   ❑ **REMARQUE :** Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

Sélection des options de rapport

Le module Analyse système liste ses paramètres courants et récapitule toutes les actions qu'il effectue au cours de ses opérations d'analyse dans un fichier journal appelé VSHLOG.TXT. Ce rapport peut à votre convenance figurer dans ce fichier ou dans un fichier texte que vous aurez créé dans un éditeur de texte quelconque à l'intention du module. Vous pourrez ensuite ouvrir et imprimer le fichier journal à partir de n'importe quel éditeur de texte pour le consulter ultérieurement.

Le fichier VSHLOG.TXT constitue un outil de gestion essentiel pour garder la trace de l'activité virale sur votre système et pour noter les paramétrages que vous utilisez pour détecter et traiter les infections identifiées par le module Analyse système. Vous pouvez également utiliser les rapports d'incidents enregistrés dans le fichier pour déterminer quels fichiers vous devez remplacer à partir de vos sauvegardes, examiner en quarantaine ou supprimer de votre système. Utilisez la page de propriétés Rapport pour déterminer les informations à inclure dans le fichier journal du module.

Pour configurer le module Analyse système de sorte qu'il consigne ses actions dans un fichier journal, procédez comme suit :

1. Cliquez sur l'onglet Rapport dans le module Analyse système pour afficher la page de propriétés correspondante (Figure 4-15).

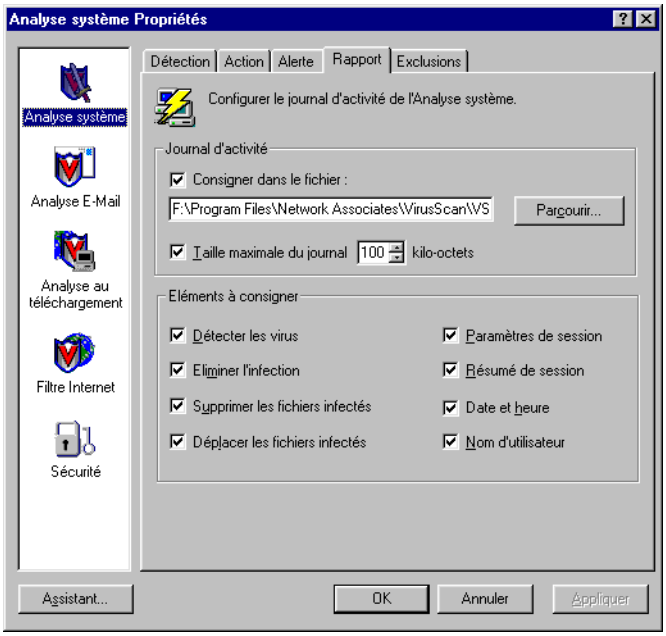

Figure 4-15. Boîte de dialogue Propriétés de l'analyse du système – page Rapport

2. Cochez la case **Consigner dans le fichier**.

   Par défaut, le module Analyse système enregistre les informations de journal dans le fichier VSHLOG.TXT, situé dans le répertoire du programme VirusScan.

Vous pouvez saisir un chemin d'accès et un nom de fichier différents dans la zone de texte prévue à cet effet, ou bien cliquer sur **Parcourir** pour localiser un fichier approprié sur votre disque dur ou sur votre réseau. Vous pouvez utiliser un fichier différent, mais celui-ci doit être déjà créé. Le module ne crée pas de fichier.

3. Pour limiter la taille du fichier journal, cochez la case **Taille maximale du journal**, puis spécifiez cette taille, en Kilo-octets, dans la zone de texte prévue à cet effet. Si vous ne cochez pas cette case, le fichier journal peut voir sa taille augmenter et atteindre une limite déterminée par votre espace disque ou votre système de fichiers.

   Saisissez une valeur comprise entre 10 Ko et 999 Ko. Par défaut, le module Analyse système limite la taille du fichier à 100Ko. Si les données du journal dépassent la taille allouée pour le fichier, le module efface le journal existant et le reprend au point où il s'était interrompu.

4. Cochez les cases correspondant aux informations que vous souhaitez que le module enregistre dans son fichier journal. En général, le module enregistre les données à la fin de la session d'analyse ou lorsque vous arrêtez le système.

   Vous pouvez choisir d'enregistrer les informations suivantes :

   - **Détecter les virus.** Cochez cette case pour que le fichier journal enregistre le nombre de virus trouvés par le module dans chaque session d'analyse. Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.
   - **Éliminer l'infection.** Cochez cette case pour que le fichier journal enregistre le nombre de fichiers infectés que le module a nettoyé ou tenté de nettoyer dans chaque session d'analyse. Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.
   - **Supprimer les fichiers infectés.** Cochez cette case pour que le fichier journal enregistre le nombre de virus supprimés par le module dans chaque session d'analyse. Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.
   - **Déplacer les fichiers infectés.** Cochez cette case pour que le fichier journal enregistre le nombre de virus que le module a placé dans un dossier de quarantaine dans chaque session d'analyse. Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.

- **Paramètres de session.** Cochez cette case pour que le fichier journal enregistre les paramètres de configuration que vous avez utilisés pour le module dans chaque session d'analyse. Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.
- **Résumé de session.** Cochez cette case pour que le fichier journal récapitule les actions effectuées par le module dans chaque session d'analyse.

  Si vous activez cette option, le journal enregistrera les informations suivantes :

  – Nombre de fichiers analysés par le module.

  – Nombre de fichiers infectés nettoyés par le module.

  – Nombre de fichiers infectés supprimés par le module.

  – Nombre de fichiers infectés que le module a placé dans un dossier de quarantaine.

  – Paramètres que vous avez attribués au module Analyse système.

  Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.

5. **Date et heure.** Cochez cette case pour que le fichier journal enregistre la date et l'heure de début de chaque session d'analyse. Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.
6. **Nom d'utilisateur.** Cochez cette case pour que le fichier journal enregistre le nom de l'utilisateur connecté à la station de travail lorsque le module démarre chaque session d'analyse. Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.
7. Cliquez sur l'onglet Exclusions pour sélectionner d'autres options du module Analyse système. Pour enregistrer vos modifications sans fermer la boîte de dialogue Propriétés de l'analyse du système, cliquez sur **Appliquer**. Pour enregistrer vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans enregistrer vos modifications, cliquez sur **Annuler**.

❑ **REMARQUE :** Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

Sélection des options d'exclusion

Nombre des fichiers stockés sur votre ordinateur ne risquent pas d'être infectés par des virus. L'examen de ces fichiers par le module Analyse système peut prendre beaucoup de temps pour un résultat insignifiant. Vous pouvez réduire le temps d'analyse consacré à chaque fichier modifié par le module Analyse système en lui demandant d'examiner uniquement les fichiers vulnérables. Vous pouvez également lui demander d'ignorer des fichiers ou des dossiers entiers pour lesquels tout risque d'infection est nul.

La liste des exclusions répertorie les disques, les dossiers ou les fichiers individuels que vous souhaitez exclure des sessions d'analyse de VShield. Par défaut, le module Analyse système n'examine pas la Corbeille, car Windows n'exécute pas les éléments qu'elle contient. L'élément exclu apparaît dans la liste la première fois que vous ouvrez la fenêtre.

Chaque entrée de la liste des exclusions affiche le chemin d'accès de l'élément exclu, indique si le module va exclure également les sous-dossiers contenus dans le dossier de l'élément et précise si l'application va exclure l'élément lors de l'analyse des fichiers, ou lors de l'analyse de la zone système de votre disque dur, ou les deux à la fois.

Une fois que vous avez utilisé le logiciel VirusScan pour analyser complètement votre système, vous pouvez demander au module Analyse système d'ignorer les fichiers et les dossiers qui ne sont jamais modifiés ou qui ne sont normalement pas susceptibles d'être infectés.

Pour sélectionner vos options, procédez comme suit :

1. Cliquez sur l'onglet Exclusions dans le module Analyse système pour afficher la page de propriétés correspondante (Figure 4-16 à la page 135).

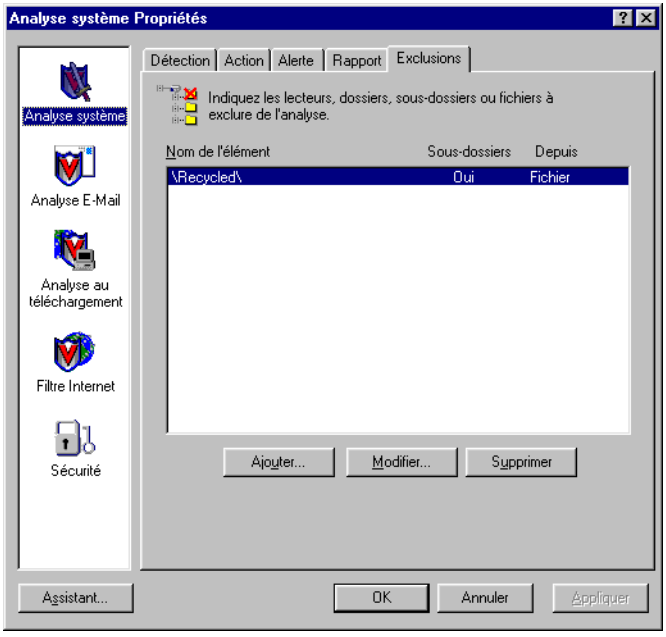

Figure 4-16. Boîte de dialogue Propriétés de l'analyse du système – page Exclusions

2. Spécifiez les éléments que vous voulez exclure. Vous pouvez :

   - **Ajouter des fichiers, des dossiers ou des volumes à la liste des exclusions.** Cliquez sur **Ajouter** pour ouvrir la boîte de dialogue Ajout d'un élément à exclure (Figure 4-17).

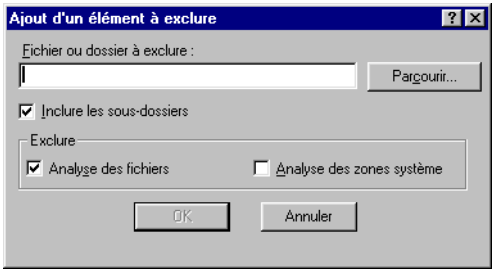

Figure 4-17. Boîte de dialogue Ajout d'un élément à exclure

Pour ajouter un élément à la liste des exclusions, procédez comme suit :

a. Entrez un chemin d'accès à un dossier ou un nom de fichier dans la zone de texte affichée ou cliquez sur **Parcourir** pour trouver l'élément que vous souhaitez exclure de l'analyse.

> **REMARQUE :** Si vous avez choisi de déplacer automatiquement tout fichier infecté vers un dossier de quarantaine, le module exclut ce dossier des opérations d'analyse.

b. Cochez la case **Inclure les sous-dossiers** pour que le module ignore les fichiers stockés dans les sous-dossiers du dossier que vous avez spécifié dans l'Étape a.

> **REMARQUE :** Lorsque vous sélectionnez l'option **Inclure les sous-dossiers**, le module n'exclut de l'analyse que les fichiers stockés dans les sous-dossiers. Cela veut dire qu'il analysera tous les fichiers stockés à la racine du dossier que vous désignez. Pour exclure de l'analyse les fichiers situés à la racine du dossier, décochez la case **Inclure les sous-dossiers**.

c. Cochez la case **Analyse des fichiers** pour exclure l'élément que vous avez spécifié dans la première étape lorsque le module recherche des virus infectant des fichiers. Ces virus apparaissent généralement dans des fichiers stockés dans les parties visibles de votre disque dur.

d. Cochez la case **Analyse des zones système** pour exclure l'élément que vous avez spécifié dans la première étape lorsque le module recherche des virus infectant des fichiers.

Ces virus résident souvent dans la mémoire ou dans des fichiers stockés dans la zone système ou dans la partition d'amorçage (MBR) de votre disque dur. Utilisez cette option pour exclure des opérations d'analyse des fichiers système comme COMMAND.COM.

> **AVERTISSEMENT :** McAffe vous recommande de *ne pas* exclure vos fichiers système des opérations d'analyse.

e. Répétez les étapes Étape a. à Étape d. jusqu'à ce que vous ayez listé tous les fichiers et dossiers que vous souhaitez exclure de l'analyse.

- **Modifier la liste des exclusions.** Pour modifier les paramètres d'un élément exclu, sélectionnez-le dans la liste Exclusions, puis cliquez sur **Edition** pour ouvrir la boîte de dialogue Edition d'élément à exclure. Effectuez les modifications voulues, puis cliquez sur **OK** pour fermer la boîte de dialogue.

- **Supprimer un élément de la liste.** Pour supprimer un élément de la liste, sélectionnez-le, puis cliquez sur **Supprimer**. Cela signifie que le module Analyse système *n'examinera pas* ce fichier ou dossier au cours de cette session d'analyse.

3. Cliquez sur un autre onglet pour modifier l'un ou l'autre des paramètres du module Analyse système, ou bien cliquez sur l'une des icônes situées le long de la boîte de dialogue Propriétés de l'analyse du système pour sélectionner les options d'un autre module.

   Pour enregistrer les modifications effectuées dans le module Analyse système sans fermer la boîte de dialogue, cliquez sur **Appliquer**. Pour enregistrer vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans enregistrer vos modifications, cliquez sur **Annuler**.

❑ **REMARQUE :** Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

Configuration du module Analyse E-Mail

Le module Analyse E-Mail de VShield recherche des virus dans les pièces jointes des messages électroniques que vous recevez par le biais de systèmes de messagerie commerciale utilisant la norme MAPI (Messaging Application Programming Interface). C'est le cas par exemple de Microsoft Exchange et Outlook, et des versions ultérieures de Lotus cc:Mail. Ce module inclut également un mode d'analyse spécial conçu pour rechercher des virus dans les versions antérieures de cc:Mail.

Ce module peut travailler conjointement avec le module Analyse au téléchargement pour examiner les messages que vous recevez par le biais de programmes clients e-mail POP-3 ou SMTP, tels que Eudora, Netscape Mail, ou Outlook Express. Le module est particulièrement vigilant avec les pièces jointes que vous recevez par e-mail ; ces dernières étant la principale source potentielle d'infection virale. Dans la mesure où il analyse le courrier électronique dès qu'il arrive sur votre ordinateur, le module Analyse E-Mail peut intercepter les virus avant même qu'ils n'aient la possibilité de contaminer d'autres fichiers.

À chaque fois qu'il trouve un virus, le module peut vous demander l'action à entreprendre, ou exécuter automatiquement plusieurs actions correctives en réponse à cette infection. Le module peut vous informer sur les actions menées en réponse à l'infection, soit par un message d'alerte, qu'il émet au moment d'appliquer la mesure corrective, soit dans un fichier journal que vous pouvez consulter à tout moment. Il peut même adresser un message à la personne qui vous a envoyé le courrier infecté, ce qui facilite énormément l'identification des sources d'infection.

❑ **REMARQUE :** Le module Analyse E-Mail n'apparaît pas dans la boîte de dialogue Propriétés de VShield, sauf si vous avez installé le logiciel VirusScan à l'aide de l'option Installation personnalisée et que vous avez choisi d'installer le module Analyse E-Mail.

Par défaut, le moteur d'analyse VShield *n'active pas* le module Analyse E-Mail lors du premier démarrage. Pour l'activer, vous devez d'abord indiquer au module les systèmes e-mail que vous utilisez.

Sélection des options de détection

Le moteur d'analyse VShield n'active pas le module Analyse E-Mail par défaut, car il doit connaître au préalable les systèmes e-mail que vous utilisez. Une fois que vous l'avez configuré pour utiliser votre client e-mail courant, le module utilisera votre profil MAPI, ou vos nom d'utilisateur et mot de passe cc:Mail pour ouvrir une session sur votre compte de messagerie à chaque opération d'analyse.

Si vous êtes déjà connecté à votre système e-mail, le module travaillera à l'intérieur de la session que vous avez créée. Toutefois, si vous n'êtes pas encore connecté à votre système e-mail, le module vous demandera de choisir un profil ou d'entrer des informations de compte dès le démarrage de la session d'analyse, même si vous n'êtes pas encore connecté. Ceci peut également se produire lorsque vous démarrez votre ordinateur et que vous n'avez pas configuré votre programme client e-mail pour être chargé au démarrage.

Si vous utilisez plusieurs profils ou si vous ouvrez une session sur un compte différent, dans un autre domaine par exemple, le module vous demande de choisir le profil à utiliser ou de fournir un nouveau nom d'utilisateur et un nouveau mot de passe pour vous connecter au système e-mail.

Pour sélectionner les options de configuration pour cette page, procédez comme suit :

1. Cochez la case **Activer l'analyse des documents joints**.

   Les options proposées dans le reste de la page de propriétés deviennent accessibles (Figure 4-18).

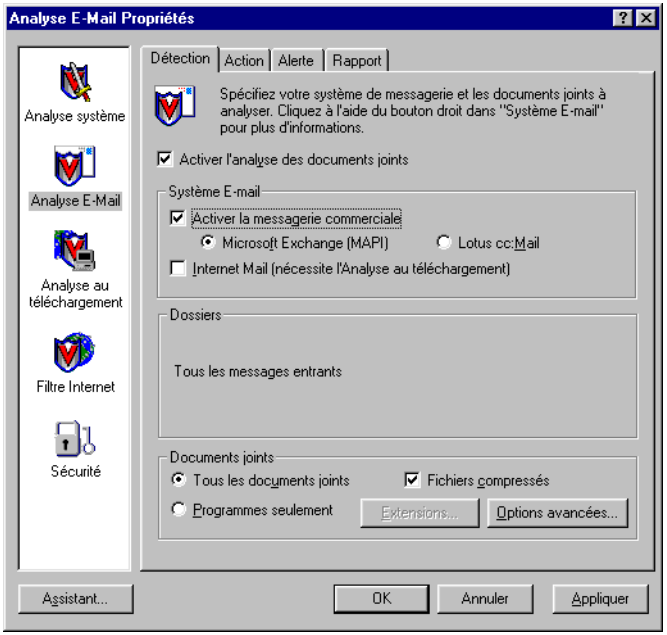

Figure 4-18. Boîte de dialogue Propriétés de l'Analyse E-Mail – page Détection

2. Sélectionnez le type de système e-mail que vous utilisez. Vous avez le choix entre les options suivantes :

   - **Activer la messagerie commerciale.** Cochez cette case pour que le module Analyse E-Mail examine les pièces jointes que vous recevez via un système e-mail fonctionnant sur le réseau interne de votre entreprise. En général de tels systèmes utilisent un protocole de messagerie propriétaire et disposent d'un serveur de messagerie central auquel vous envoyez vos courriers pour expédition. Il est fréquent que ces systèmes envoient et reçoivent du courrier électronique Internet, mais ils le font en général grâce à une application passerelle. Le module Analyse E-Mail prend en charge deux types de systèmes de messagerie commerciale :

– **Microsoft Exchange (MAPI).** Cliquez sur ce bouton si vous utilisez un système e-mail qui envoie et reçoit du courrier via l'interface MAPI de Microsoft, qui est un protocole de messagerie de Windows. Microsoft Exchange, Microsoft Outlook 97 et Outlook 98 en sont des exemples.

– **Lotus cc:Mail.** Cliquez sur ce bouton si vous utilisez cc:Mail 6.x ou 7.x. Ces systèmes utilisent un protocole propriétaire de Lotus pour envoyer et recevoir du courrier électronique. Si vous le désirez, vous avez la possibilité d'installer cc:Mail version 8.0 de façon à ce qu'il utilise le même protocole que les versions précédentes. Pour vérifier quel système vous utilisez, consultez votre administrateur réseau.

❑ **REMARQUE :** Vous ne pouvez sélectionner qu'un seul système de messagerie*commerciale* à la fois. Cependant, si vous utilisez en parallèle un système de messagerie commerciale et un système de messagerie Internet, le module Analyse E-Mail peut examiner toutes les pièces jointes qui vous sont envoyées.

• **Internet Mail (nécessite l'Analyse au téléchargement).** Cochez cette case pour que le module Analyse E-Mail examine les fichiers joints au courrier Internet que vous envoyez et recevez via le protocole POP-3 (Post Office Protocol) ou le protocole SMTP (Simple Mail Transfer Protocol). Sélectionnez cette option si vous vous connectez par modem à un fournisseur de services Internet avec un logiciel comme Eudora Pro de Qualcomm, Outlook Express de Microsoft, ou Netscape Mail (c'est souvent le cas chez vous et cela peut être le cas à votre travail).

IMPORTANT : Dans la mesure où vous recevez le courrier électronique Internet et les autres fichiers que vous téléchargez (depuis des sites Web ou d'autres sources) via le même « canal », le module Analyse E-Mail utilise les options de détection, d'action, d'alerte et de rapport que vous avez choisies au niveau du module Analyse au téléchargement pour déterminer sa façon de réagir face au courrier électronique Internet entrant. C'est pourquoi, pour analyser les fichiers joints au courrier électronique Internet, vous devez activer également le module Analyse au téléchargement et utiliser les différentes pages de propriétés pour sélectionner les options qui vous intéressent.

---

3. Indiquez au module Analyse E-Mail les sources de messagerie qu'il doit contrôler.

   - Si vous choisissez **Microsoft Exchange (MAPI)** comme système de messagerie commerciale, la zone Dossiers affiche **Tous les messages entrants**, ce qui signifie que le module cherchera les virus dans les fichiers joints aux messages électroniques dès qu'ils arriveront à votre boîte aux lettres MAPI ou via d'autres services MAPI.

   - Si vous choisissez **Lotus cc:Mail** comme système de messagerie commerciale, vous devrez indiquer au module la fréquence d'analyse de la boîte aux lettres cc:Mail (Figure 4-19).

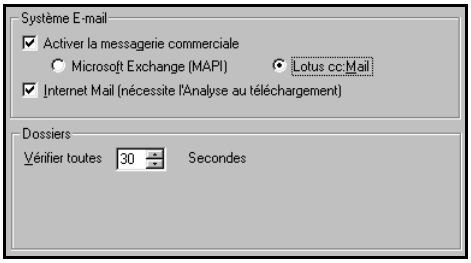

Figure 4-19. Page Détection avec option cc:Mail sélectionnée

   Dans la zone Dossiers, entrez le nombre de secondes que le module Analyse E-Mail doit attendre avant de vérifier l'arrivée de nouveaux messages dans votre boîte aux lettres cc:Mail. Par défaut, le module vérifie vos boîtes toutes les minutes. Prenez soin d'indiquer un intervalle plus court que celui que vous avez fixé pour la récupération de votre courrier, de façon à ce que le module puisse détecter les virus avant qu'ils n'atteignent votre ordinateur.

4. Spécifiez les types de pièces jointes que le module Analyse E-Mail doit examiner. Vous pouvez :

   - **Analyser les fichiers compressés.** Cochez la case **Fichiers compressés** pour que le module recherche les virus éventuels dans les fichiers compressés ou dans les fichiers d'archives. Cette option permet d'éviter que les virus ne se propagent à partir de fichiers compressés, car le module décompresse les fichiers avant de les analyser. L'activation de cette option peut augmenter le délai requis pour l'analyse d'un jeu de fichiers spécifique pendant que vous travaillez sur votre ordinateur.

REMARQUE : Lorsque le module Analyse E-Mail examine un fichier d'archives, il analyse uniquement le fichier d'archives lui-même et non les fichiers compressés qu'il contient. Pour savoir quels sont les fichiers et les archives examinés par le module, reportez-vous à la section « Liste en cours des fichiers compressés analysés » à la page 352.

- **Sélectionner les types de fichiers à analyser.** D'ordinaire, les virus ne peuvent infecter les fichiers qui ne contiennent pas de code exécutable, que ce soit du code de script, de macro ou binaire. C'est pourquoi vous pouvez sans risque réduire la portée des opérations d'analyse afin que le module ne vérifie que les fichiers les plus susceptibles d'être infectées. Pour ce faire, cliquez sur le bouton **Fichiers programme uniquement**.

  Pour afficher ou désigner les extensions de fichier que le module Analyse E-Mail doit examiner, cliquez sur **Extensions** pour ouvrir la boîte de dialogue Extensions de fichiers programme (Figure 4-10).

Figure 4-20. Boîte de dialogue Extensions de fichiers programme

  Reportez-vous aux sections voir « Ajout d'extensions de fichier pour analyse » à la page 345 et « Liste en cours des extensions de noms de fichiers vulnérables » à la page 346 pour connaître les extensions de nom de fichier pouvant être analysées par défaut par le module Analyse E-Mail et ajouter ou modifier des éléments dans cette liste.

- **Analyser tous les fichiers.** Cliquez sur le bouton **Tous les fichiers** pour que le module Analyse E-Mail examine tous les fichiers, quelle que soit leur extension, à chaque fois que vous ou un processus système y apporte une modification.

5. Activer l'analyse heuristique. Cliquez sur **Options avancées** pour ouvrir la boîte de dialogue Paramètres d'analyse avancés (Figure 4-11).

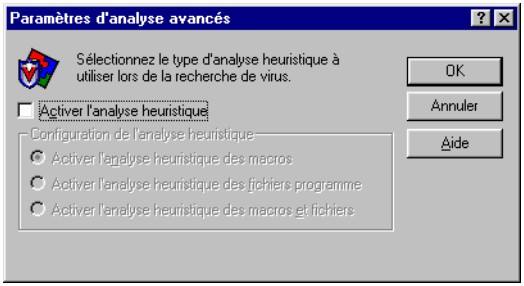

Figure 4-21. Boîte de dialogue Paramètres d'analyse avancés

La technologie d'analyse heuristique permet au module Analyse E-Mail de reconnaître les nouveaux virus à partir de leur ressemblance avec des virus semblables déjà identifiés.

Pour ce faire, le programme recherche des caractéristiques propres aux virus dans les fichiers que vous lui avez demandé d'analyser. S'il détecte un nombre suffisant de caractéristiques dans un fichier, le module identifie le fichier comme étant potentiellement infecté par un nouveau virus ou un virus non identifié.

Le module Analyse E-Mail recherche en même temps des caractéristiques de fichier excluant la possibilité d'une infection par un virus, c'est pourquoi il ne vous donnera que rarement des indications erronées sur la présence d'un virus. À moins d'être certain que votre fichier ne contient *pas* de virus, vous devez apporter aux infections « probables » les mêmes précautions que vous apportez aux infections confirmées.

Lorsque vous démarrez le module Analyse E-Mail, aucune option d'analyse heuristique n'est activée par défaut. Pour activer l'analyse heuristique, procédez comme suit :

a. Cochez la case **Activer l'analyse heuristique**. Les options proposées dans le reste de la boîte de dialogue deviennent accessibles.

b. Sélectionnez les types d'analyses heuristiques que vous souhaitez utiliser. Vous avez le choix entre les options suivantes :

- **Activer l'analyse heuristique des macros.** Sélectionnez cette option pour que le module Analyse E-Mail identifie d'abord tous les fichiers Microsoft Word, Microsoft Excel et autres fichiers Microsoft Office incorporant des macros et compare ensuite le code de la macro avec sa base de données de définitions de virus. Si la correspondance est exacte, le module identifie le nom du virus ; pour les signatures codées qui ressemblent à celles des virus existants, il vous informe qu'il a détecté un virus de macro « probable ».
- **Activer l'analyse heuristique des fichiers programme.** Sélectionnez cette option si vous souhaitez que le module Analyse E-Mail localise de nouveaux virus dans les fichiers programme en examinant les caractéristiques des fichiers et en les comparant avec celles figurant sur une liste de virus connus. Lorsqu'il détecte un fichier ayant un certain nombre de caractéristiques, le module l'identifie comme étant potentiellement infecté.
- **Activer l'analyse heuristique des macros et fichiers programme.** Sélectionnez cette option si vous souhaitez que le module utilise les deux types d'analyse heuristique. McAffe vous recommande d'utiliser cette option pour une protection antivirus optimale.

> **REMARQUE :** Le module Analyse E-Mail n'utilise les techniques d'analyse heuristique que sur les types de fichiers que vous désignez dans la boîte de dialogue Extensions de fichiers programme. Si vous décidez d'analyser **Tous les fichiers**, le module appliquera l'analysera heuristique à tous les types de fichiers.

6. Cliquez sur l'onglet Action pour sélectionner d'autres options du module Analyse E-Mail. Pour enregistrer vos modifications sans fermer la boîte de dialogue Propriétés de l'Analyse E-Mail, cliquez sur **Appliquer**. Pour enregistrer vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans enregistrer vos modifications, cliquez sur **Annuler**.

> **REMARQUE :** Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

Sélection des options d'action

Lorsque le module Analyse E-Mail détecte un virus dans un document joint à un courrier électronique, il peut réagir soit en vous demandant quoi faire avec le fichier infecté, soit en prenant automatiquement les mesures que vous aurez déterminées à l'avance. Utilisez la page de propriétés Action pour spécifier les actions que le module doit vous proposer en cas de détection d'un virus et celles qu'il doit mettre en œuvre automatiquement.

REMARQUE : Pour que le module Analyse E-Mail puisse réagir face à une infection virale, vous devez sélectionner un système de messagerie commerciale à examiner. Si vous ne sélectionnez que Internet Mail, les options décrites ici ne seront pas disponibles. Si vous recevez du courrier électronique via Internet Mail uniquement, vous devez sélectionner vos réponses dans la page de propriétés Action du module Analyse au téléchargement.

Procédez comme suit :

1. Cliquez sur l'onglet Action dans le module Analyse E-Mail pour afficher la page de propriétés correspondante (Figure 4-22).

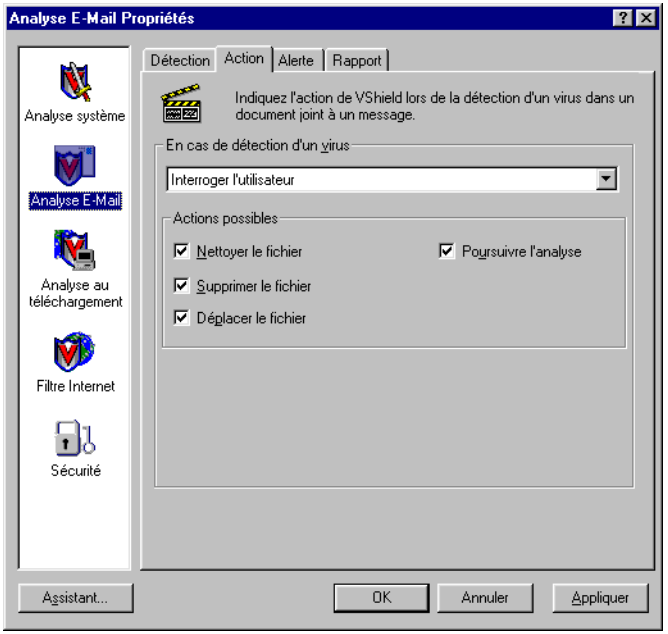

Figure 4-22. Boîte de dialogue Propriétés de l'Analyse E-Mail – page Action

2. Sélectionnez une réponse dans la liste **En cas de détection d'un virus**. La zone située au-dessous de la liste se modifie pour vous proposer des options supplémentaires adaptées à chacun de vos choix. Vous avez le choix entre les options suivantes :

   - **Interroger l'utilisateur.** Sélectionnez cette option si vous souhaitez que le module Analyse E-Mail vous demande quoi faire lorsqu'il détecte un virus — le module affichera alors un message d'alerte et vous proposera plusieurs actions possibles.

     ❑ **REMARQUE :** Si vous sélectionnez **Interroger l'utilisateur** dans la liste, cliquez sur l'onglet Alerte pour préciser si le module Analyse E-Mail doit utiliser un message, un signal sonore ou les deux à la fois pour vous avertir en cas d'infection.

     Sélectionnez les options à afficher dans le message d'alerte : Pour chaque case que vous cochez dans cette zone, un bouton d'option apparaîtra dans le message d'alerte que le module affichera en cas de détection d'un virus. Ainsi, si vous cochez par exemple la case **Supprimer le fichier**, le message d'alerte comportera un bouton **Supprimer**.

     Vous avez le choix entre les options suivantes :

     – **Désinfecter le fichier.** Cette option demande au module d'essayer de supprimer le code de virus dans le fichier infecté. Si vous avez activé la fonction de rapport, le module enregistrera l'événement dans un journal à chaque fois qu'il parviendra ou non à nettoyer un fichier infecté.

       ❑ **REMARQUE :** Le module Analyse E-Mail *ne prend pas* en charge cette option pour les systèmes e-mail Lotus cc:Mail v7.x et versions antérieures. Si vous avez sélectionné Lotus cc:Mail dans la page Détection du module Analyse E-Mail, l'option Désinfecter le fichier n'apparaîtra pas ici.

     – **Supprimer le fichier.** Cette option demande au module de supprimer immédiatement la pièce jointe infectée. Toutefois, le module ne touchera pas au message proprement dit.

     – **Déplacer le fichier.** Cette option demande au module de placer le fichier infecté dans un dossier de quarantaine. Le message d'alerte affichera un bouton **Déplacer le fichier** pour vous permettre de localiser le dossier de quarantaine à utiliser.

  - **Poursuivre l'analyse.** Cette option indique au module de continuer son analyse sans prendre d'autres mesures. Si vous avez activé ses options de rapport, le module Analyse E-Mail enregistre l'incident dans son fichier journal.

- **Déplacer les fichiers infectés vers un dossier.** Sélectionnez cette option de réponse pour que le module déplace les fichiers infectés vers un dossier de quarantaine dès leur détection. Le module place ces fichiers dans un dossier nommé Infecté, situé dans le répertoire du programme VirusScan.

  Vous pouvez modifier le nom et l'emplacement du dossier dans lequel le module place le courrier Internet infecté, mais pour ce faire vous devez d'abord passer dans le module Analyse au téléchargement, puis cliquer sur l'onglet Action. Pour plus de détails, reportez-vous à la section voir « Sélection des options d'action » à la page 161.

- **Nettoyer les fichiers infectés.** Sélectionnez cette réponse pour que le module supprime le code de virus dans le fichier infecté dès sa détection. Si le module ne parvient pas à supprimer le virus, il notera l'incident dans son fichier journal.

  ❑ **REMARQUE :** Le module Analyse E-Mail *ne prend pas* en charge cette option pour les systèmes e-mail Lotus cc:Mail v7.x et versions antérieures. Si vous avez sélectionné Lotus cc:Mail dans la page Détection du module Analyse E-Mail, l'option Désinfecter le fichier n'apparaîtra pas ici.

- **Supprimer les fichiers infectés.** Sélectionnez cette option de réponse pour que le module Analyse E-Mail supprime immédiatement tout fichier infecté détecté. Assurez-vous d'avoir activé la fonction de rapport, afin de disposer d'une liste des fichiers supprimés par le module. Consultez ensuite cette dernière pour connaître les fichiers supprimés à restaurer à partir des copies de sauvegarde. Pour plus de détails, reportez-vous à la section « Sélection des options de rapport » à la page 153.

- **Poursuivre l'analyse.** Sélectionnez cette option de réponse pour que le module continue l'analyse sans prendre de mesures à l'encontre du virus détecté. Si vous activez également la fonction de rapport du module Analyse E-Mail (voir « Sélection des options de rapport » à la page 153), le programme consignera les noms des virus qu'il détecte, ainsi que les noms des fichiers infectés. Cela vous permettra de les supprimer dès que l'occasion se présente.

  N'utilisez cette option que si vous prévoyez d'être absent au moment où le module recherchera les virus.

3. Cliquez sur l'onglet Alerte afin de sélectionner d'autres options du module Analyse E-Mail. Pour enregistrer vos modifications sans fermer la boîte de dialogue Propriétés de l'Analyse E-Mail, cliquez sur **Appliquer**. Pour enregistrer vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans enregistrer vos modifications, cliquez sur **Annuler**.

REMARQUE : Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

Sélection des options d'alerte

Une fois que vous l'avez configuré avec les options de réponse qui vous intéressent dans la page Action, vous pouvez laisser le module Analyse E-Mail rechercher et éliminer automatiquement les virus de votre système au fur et à mesure qu'il les trouve, pratiquement sans aucune autre intervention de votre part. Si, toutefois, vous souhaitez que le module vous informe dès qu'il détecte un virus afin que vous puissiez prendre les mesures adéquates, vous devez le configurer de telle sorte qu'il envoie un message d'alerte à vous ou aux autres utilisateurs.

Procédez comme suit :

1. Cliquez sur l'onglet Alerte dans le module Analyse E-Mail pour afficher la page de propriétés correspondante (Figure 4-23).

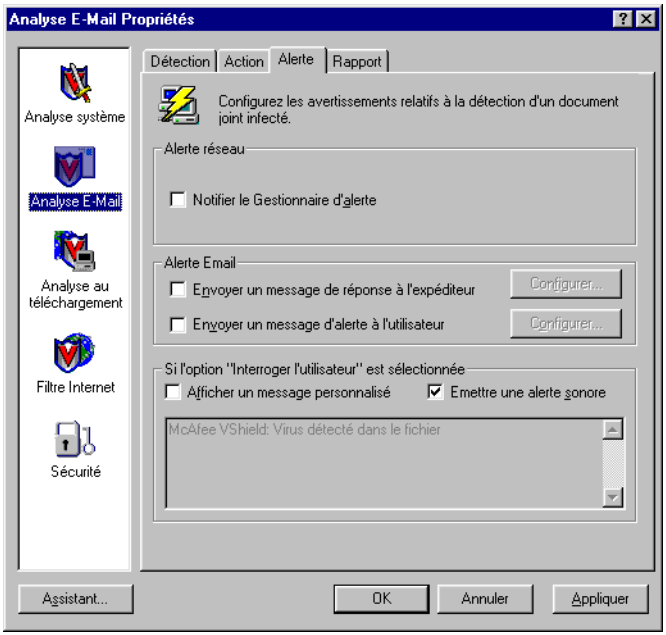

Figure 4-23. Boîte de dialogue Propriétés de l'Analyse E-Mail – page Alerte

2. Cochez la case **Notifier le Gestionnaire d'alerte** pour que le module envoie des messages d'alerte au Gestionnaire d'alerte qui les transmettra.

Le Gestionnaire d'alerte est un composant indépendant du logiciel McAfee qui regroupe des messages d'alerte et utilise diverses méthodes pour les envoyer aux destinataires que vous désignez. Le module Analyse E-Mail enverra ces messages d'alerte avec succès uniquement si vous avez installé l'utilitaire de configuration cliente du Gestionnaire d'alerte. Pour plus de détails, reportez-vous à la section voir « Utilisation de l'utilitaire de Configuration cliente du Gestionnaire d'alerte » à la page 338.

Vous pouvez transmettre des messages d'alerte directement à un serveur du Gestionnaire d'alerte. Sinon, vous pouvez les envoyer en tant que fichiers texte (.ALR) à un répertoire d'alerte centralisée que le serveur du Gestionnaire d'alerte interroge régulièrement.

❑ **REMARQUE :** Si vous décochez cette case, le module Analyse E-Mail n'enverra pas des messages d'alerte via le Gestionnaire d'alerte, mais tous les autres messages d'alerte que vous configurez dans cette page de propriétés resteront intacts.

En tant que partie intégrante de votre système d'alerte antivirus, le module Analyse E-Mail peut répondre directement par un message d'alerte à l'utilisateur qui vous a envoyé le message ou le document joint infecté. Vous pouvez envoyer une copie de ce message à d'autres destinataires, que ce soit à l'intérieur ou à l'extérieur de votre entreprise. Si vous préférez ne pas envoyer de réponse, vous pouvez configurer le module pour envoyer une notification par e-mail à l'administrateur système par exemple, à chaque fois qu'il détecte un virus.

L'envoi de messages de réponse facilite l'identification des sources des virus et de leurs points d'entrée dans votre réseau, alors que les copies de ces messages envoyées aux administrateurs système leur permettent plutôt d'identifier la méthode de propagation utilisée par les virus.

Vous avez également la possibilité d'envoyer un message à n'importe quel destinataire sans répondre à l'émetteur de la pièce jointe infectée. Le module Analyse E-Mail peut extraire les destinataires directement de votre carnet d'adresses Microsoft Exchange, Microsoft Outlook, ou de tout autre carnet d'adresses conforme à la norme MAPI, ou d'un annuaire Lotus cc:Mail équivalent. Sinon, vous pouvez entrer les adresses des destinataires directement.

Le message que vous créez pour une réponse est un modèle ; le module l'enverra automatiquement à chacun des destinataires que vous désignez.

C'est pourquoi McAfee vous recommande de créer un message pouvant être lu et compris par tous les destinataires. À l'exception de la rédaction du modèle de message, le module ne vous permettra pas de modifier le message avant de l'envoyer.

Vous pouvez envoyer un message pour répondre à l'émetteur du message infecté et un message différent pour les autres destinataires, mais vous ne pouvez pas créer un même message pour des destinataires différents.

3. Pour créer vos modèles de message, procédez comme suit :

   a. Cochez la case **Envoyer un message de réponse à l'expéditeur** dans la page de propriétés Alerte, puis cliquez sur **Configurer** pour ouvrir un formulaire de message électronique standard.

      Dans la mesure où le module enverra ce message directement à l'émetteur du message électronique infecté, le bouton **A:** et la zone de texte correspondante ne sont pas disponibles.

   b. Pour envoyer une copie de ce message à quelqu'un d'autre, entrez une adresse électronique dans la zone de texte intitulée Copie à: ou cliquez sur **Copie à:** pour choisir un destinataire dans l'annuaire d'utilisateurs ou le carnet d'adresses de votre système e-mail.

      ❑ **REMARQUE :** Pour retrouver une adresse électronique dans l'annuaire d'utilisateurs de votre système e-mail, vous devez stocker les adresses dans un annuaire d'utilisateurs, une base de données ou un carnet d'adresses compatible MAPI, ou dans un annuaire Lotus cc:Mail équivalent. Si vous n'êtes pas encore connecté à votre système e-mail, le module Analyse E-Mail tente d'utiliser votre profil MAPI par défaut pour se connecter à des systèmes e-mail compatibles MAPI. Sinon, il vous invite à saisir un nom d'utilisateur, un mot de passe et un chemin d'accès à votre boîte aux lettres Lotus cc:Mail. Entrez les informations nécessaires au module, puis cliquez sur **OK** pour continuer.

      ---

   c. Indiquez un objet qui laisse apparaître le caractère urgent de votre message, puis ajoutez vos commentaires dans le corps du message, sous un avis d'infection standard qui sera fourni par l'Analyse E-Mail. Vous pouvez ajouter jusqu'à 1 024 caractères de texte.

d. Cliquez sur **OK** pour enregistrer le message.

À chaque fois qu'il détectera un virus, le module enverra une copie de ce message à la personne qui vous a envoyé le courrier électronique comportant la pièce jointe infectée. Il remplira l'adresse du destinataire avec les informations de l'en-tête du message d'origine, et identifiera le virus et le fichier infecté dans la zone située immédiatement après la ligne Objet. De plus, si vous avez activé sa fonction de rapport, le module y mentionnera tout message d'alerte qu'il aura envoyé.

e. Pour envoyer un message d'alerte à d'autres utilisateurs, un administrateur réseau par exemple, à propos d'une pièce jointe infectée, cochez la case **Envoyer un message d'alerte à l'utilisateur** dans la page de propriétés Alerte. Vous pouvez ensuite créer une réponse standard, tel que vous l'avez fait dans les étapes Étape a à Étape d ci-dessus. Dans ce cas, vous pouvez remplir les zones de texte A: et Copie à:

Dès qu'il détectera un virus, le module Analyse E-Mail enverra une copie de ce message à toutes les adresses que vous avez spécifiées dans ce message.

4. Cochez la case**Émettre une alerte sonore** pour que le module envoie un signal sonore à chaque fois qu'il trouve un fichier infecté.

   Vous pouvez modifier le paramétrage de cette option à condition d'avoir sélectionné **Interroger l'utilisateur** dans la page de propriétés Action. Sinon, la case à cocher Émettre une alerte sonore affichera et utilisera le paramètre que vous lui avez attribué la dernière fois que vous avez sélectionné l'option **Interroger l'utilisateur**.

   Le module émettra le signal sonore standard du système ou exécutera le fichier .WAV que vous avez configuré sur votre ordinateur.

5. Cochez la case **Afficher un message personnalisé** pour que le module ajoute un message personnalisé au texte du message qu'il affiche lorsqu'il trouve un fichier infecté.

   À l'égard de l'alerte sonore, vous pouvez modifier le paramétrage de cette option à condition d'avoir sélectionné **Interroger l'utilisateur** dans la page de propriétés Action. Si vous ne sélectionnez pas cette option dans la page Action, aucun message d'alerte ou message personnalisé ne s'affichera même si vous avez coché la case Afficher un message personnalisé.

6. Entrez le message que le module doit afficher dans la zone de texte. Vous pouvez entrer 250 caractères maximum.

7. Cliquez sur l'onglet Rapport pour sélectionner d'autres options du module Analyse E-Mail. Pour enregistrer vos modifications sans fermer la boîte de dialogue Propriétés de l'Analyse E-Mail, cliquez sur **Appliquer**. Pour enregistrer vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans enregistrer vos modifications, cliquez sur **Annuler**.

❑ **REMARQUE :** Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

Sélection des options de rapport

Le module Analyse E-Mail liste ses paramètres courants et récapitule toutes les actions qu'il effectue au cours de ses opérations d'analyse dans un fichier journal appelé WEBEMAIL.TXT. Ce rapport peut à votre convenance figurer dans ce fichier ou dans un fichier texte que vous aurez créé dans un éditeur de texte quelconque à l'usage du module. Vous pourrez ensuite ouvrir et imprimer le fichier journal à partir de n'importe quel éditeur de texte pour le consulter ultérieurement.

Le fichier WEBEMAIL.TXT constitue un outil de gestion essentiel pour garder la trace de l'activité virale sur votre système et pour noter les paramètres que vous utilisez pour détecter et pour traiter les infections trouvées par le module. Vous pouvez également utiliser les rapports d'incidents enregistrés dans le fichier pour déterminer quels fichiers vous devez remplacer à partir de vos sauvegardes, examiner en quarantaine ou supprimer de votre système. Utilisez la page de propriétés Rapport pour déterminer les informations à inclure dans le fichier journal du module.

Pour configurer le module Analyse E-Mail de sorte qu'il consigne ses actions dans un fichier journal, procédez comme suit :

1. Cliquez sur l'onglet Rapport dans le module Analyse E-Mail pour afficher la page de propriétés correspondante (voir Figure 4-24 à la page 154).

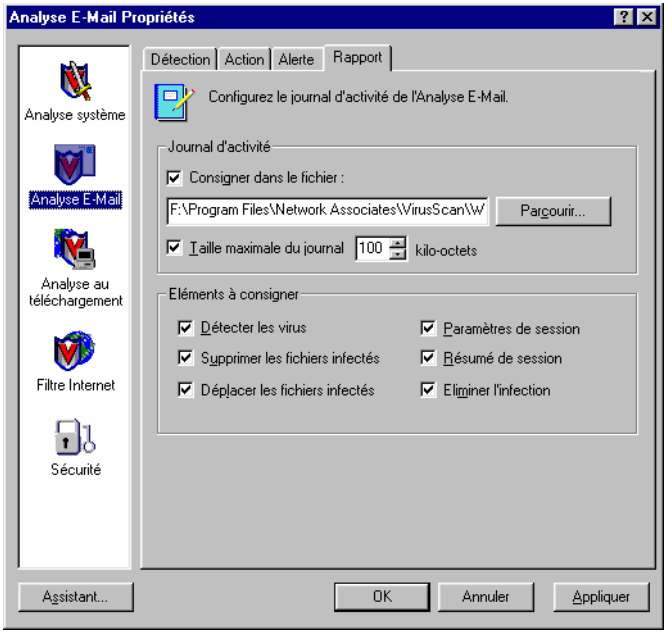

Figure 4-24. Boîte de dialogue Propriétés de l'Analyse E-Mail – page Rapport

2. Cochez la case **Consigner dans le fichier**.

   Par défaut, le module enregistre les données de son rapport dans le fichier WEBEMAIL.TXT, situé dans le répertoire du programme VirusScan. Vous pouvez saisir un chemin d'accès et un nom de fichier différents dans la zone de texte prévue à cet effet, ou bien cliquer sur **Parcourir** pour localiser un fichier approprié sur votre disque dur ou sur votre réseau.

3. Pour limiter la taille du fichier journal, cochez la case **Taille maximale du journal**, puis spécifiez cette taille, en Kilo-octets, dans la zone de texte prévue à cet effet. Si vous ne cochez pas cette case, le fichier journal peut voir sa taille augmenter et atteindre une limite déterminée par votre espace disque ou votre système de fichiers.

   Entrez une valeur comprise entre 10 Ko et 999 Ko. Par défaut, le module Analyse système limite la taille du fichier à 100 Ko. Si les données du journal dépassent la taille allouée pour le fichier, le module efface le journal existant et le reprend au point où il s'était interrompu.

4. Cochez les cases correspondant aux informations que vous souhaitez que le module enregistre dans son fichier journal. En général, le module enregistre les données à la fin de la session d'analyse ou lorsque vous arrêtez le système.

Vous pouvez choisir d'enregistrer les informations suivantes :

- **Détecter les virus.** Cochez cette case pour que le fichier journal enregistre le nombre de virus trouvés par le module dans chaque session d'analyse. Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.
- **Supprimer les fichiers infectés.** Cochez cette case pour que le fichier journal enregistre le nombre de virus supprimés par le module dans chaque session d'analyse. Décochez cette case pour exclure ces informations.
- **Déplacer les fichiers infectés.** Cochez cette case pour que le fichier journal enregistre le nombre de virus que le module a placé dans un dossier de quarantaine dans chaque session d'analyse. Décochez cette case pour exclure ces informations.
- **Paramètres de session.** Cochez cette case pour que le fichier journal enregistre les paramètres de configuration que vous avez utilisés pour le module dans chaque session d'analyse. Décochez cette case pour exclure ces informations.
- **Résumé de session.** Cochez cette case pour que le fichier journal récapitule les actions effectuées par le module dans chaque session d'analyse. Le journal enregistrera les informations suivantes :
  - Nombre de fichiers analysés par le module.
  - Nombre de fichiers infectés nettoyés par le module (systèmes e-mail MAPI uniquement).
  - Nombre de fichiers infectés supprimés par le module.
  - Nombre de fichiers infectés que le module a placé dans un dossier de quarantaine.
  - Paramètres que vous avez attribués au module Analyse E-Mail

  Décochez la case pour exclure ces informations.
- **Éliminer l'infection.** Cochez cette case pour que le fichier journal enregistre le nombre de fichiers infectés que le module a nettoyé ou tenté de nettoyer dans chaque session d'analyse. Décochez cette case pour exclure ces informations.

❑ **REMARQUE :** Le module Analyse E-Mail *ne prend pas* en charge cette option pour les systèmes e-mail Lotus cc:Mail v7.x et versions antérieures. Si vous avez sélectionné Lotus cc:Mail dans la page Détection du module Analyse E-Mail, l'option Désinfecter le fichier n'apparaîtra pas ici.

---

5. Cliquez sur un autre onglet pour modifier l'un ou l'autre des paramètres du module Analyse E-Mail, ou bien cliquez sur l'une des icônes situées le long de la boîte de dialogue Propriétés de l'Analyse E-Mail pour sélectionner les options d'un autre module.

   Pour enregistrer les modifications effectuées dans le module Analyse E-Mail sans fermer la boîte de dialogue, cliquez sur **Appliquer**. Pour enregistrer vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans enregistrer vos modifications, cliquez sur **Annuler**.

   ❑ **REMARQUE :** Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

Configuration du module Analyse au téléchargement

Le module Analyse au téléchargement peut vérifier les fichiers que vous téléchargez depuis Internet lorsque vous visitez des sites Web, des sites FTP et d'autres sites Internet. C'est aussi le module dans lequel vous sélectionnez les options de réponse à utiliser en cas de réception de pièces jointes infectées via les programmes clients e-mail conformes à la norme POP-3 et SMTP comme Eudora, Netscape Mail, ou Microsoft Outlook Express. Pour activer cette fonction, vous devez également sélectionner un système e-mail approprié dans la page Détection du module Analyse E-Mail. Pour plus de détails, reportez-vous à la section voir « Sélection des options de détection » à la page 138.

À chaque fois qu'il trouve un virus, le module peut vous demander l'action à entreprendre, ou exécuter automatiquement plusieurs actions correctives en réponse à cette infection. Le module peut vous informer sur les actions menées en réponse à l'infection, soit par un message d'alerte, qu'il émet au moment d'appliquer la mesure corrective, soit dans un fichier journal que vous pouvez consulter à tout moment. Il peut même adresser un message à la personne qui vous a envoyé le courrier infecté, ce qui facilite énormément l'identification des sources d'infection.

❑ **REMARQUE :** Le module Analyse au téléchargement *n'apparaît pas* dans la boîte de dialogue Propriétés de VShield, sauf si vous avez installé le logiciel VirusScan à l'aide de l'option Installation personnalisée et que vous avez choisi d'installer le composant Analyse Internet.

Sélection des options de détection

Le module Analyse au téléchargement prend comme hypothèse de départ que vous souhaitez qu'il détecte les virus éventuels à chaque fois que vous téléchargez depuis Internet un fichier susceptible d'être infecté (Figure 4-25 à la page 157). Ces options par défaut offrent un excellent niveau de sécurité, mais votre environnement peut exiger un paramétrage différent.

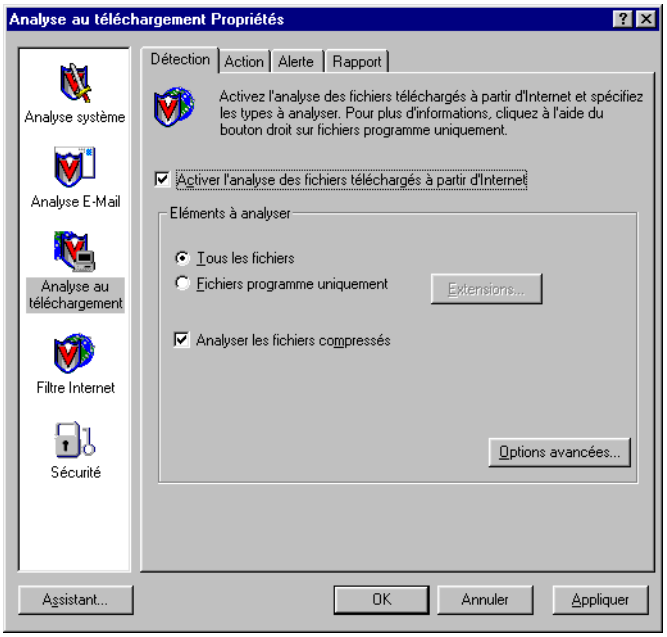

Figure 4-25. Boîte de dialogue Propriétés de l'Analyse au téléchargement – page Détection

Pour modifier les paramètres de cette page de propriétés, procédez comme suit :

1. Cochez la case **Activer l'analyse des fichiers téléchargés à partir d'Internet**.

   Les options proposées dans le reste de la page de propriétés deviennent accessibles.

2. Spécifiez les types de fichiers que le module Analyse au téléchargement doit examiner. Vous pouvez :

- **Sélectionner les types de fichiers à analyser.** D'ordinaire, les virus ne peuvent infecter les fichiers qui ne contiennent pas de code exécutable, que ce soit du code de script, de macro ou binaire. C'est pourquoi vous pouvez sans risque réduire la portée des opérations d'analyse afin que le module ne vérifie que les fichiers les plus susceptibles d'être infectées. Pour ce faire, cliquez sur le bouton **Fichiers programme uniquement**.

  Pour afficher ou désigner les extensions de fichier que le module Analyse au téléchargement doit examiner, cliquez sur **Extensions** pour ouvrir la boîte de dialogue Extensions de fichiers programme (Figure 4-10 à la page 120).

Figure 4-26. Boîte de dialogue Extensions de fichiers programme

  Reportez-vous aux sections voir « Ajout d'extensions de fichier pour analyse » à la page 345 et « Liste en cours des extensions de noms de fichiers vulnérables » à la page 346 pour connaître les extensions de nom de fichier pouvant être analysées par défaut par le module Analyse au téléchargement et ajouter ou modifier des éléments dans cette liste.

- **Analyser tous les fichiers.** Cliquez sur le bouton **Tous les fichiers** pour que le module Analyse au téléchargement examine tous les fichiers, quelle que soit leur extension, à chaque fois que vous ou un processus système y apporte une modification.

- **Analyser les fichiers compressés.** Cochez la case **Fichiers compressés** pour que le module recherche les virus éventuels dans les fichiers compressés ou dans les fichiers d'archives.

Cette option permet d'éviter que les virus ne se propagent à partir de fichiers compressés, car le module décompresse les fichiers avant de les analyser. L'activation de cette option peut augmenter le délai requis pour l'analyse d'un jeu de fichiers spécifique pendant que vous travaillez sur votre ordinateur.

REMARQUE : Lorsque le module Analyse au téléchargement examine un fichier d'archives, il analyse uniquement le fichier d'archives lui-même et non les fichiers compressés qu'il contient. Pour savoir quels sont les fichiers et les archives examinés par le module, reportez-vous à la section « Liste en cours des fichiers compressés analysés » à la page 352.

---

3. Activer l'analyse heuristique. Cliquez sur **Options avancées** pour ouvrir la boîte de dialogue Paramètres d'analyse avancés (Figure 4-11 à la page 122).

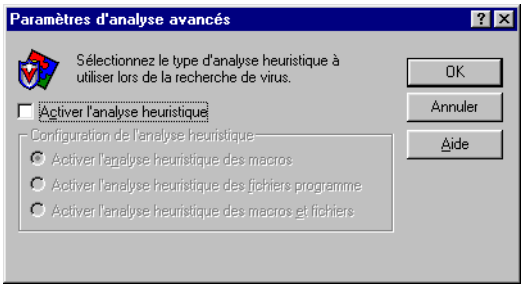

Figure 4-27. Boîte de dialogue Paramètres d'analyse avancés

La technologie d'analyse heuristique permet au module Analyse au téléchargement de reconnaître les nouveaux virus à partir de leur ressemblance avec des virus semblables déjà identifiés. Pour ce faire, le programme recherche des caractéristiques propres aux virus dans les fichiers que vous lui avez demandé d'analyser. S'il détecte un nombre suffisant de caractéristiques dans un fichier, le module identifie le fichier comme étant potentiellement infecté par un nouveau virus ou un virus non identifié.

Le module Analyse au téléchargement recherche en même temps des caractéristiques de fichier excluant la possibilité d'une infection par un virus, c'est pourquoi il ne vous donnera que rarement des indications erronées sur la présence d'un virus. À moins d'être certain que votre fichier ne contient *pas* de virus, vous devez apporter aux infections « probables » les mêmes précautions que vous apportez aux infections confirmées.

Lorsque vous démarrez le module Analyse au téléchargement, aucune option d'analyse heuristique n'est activée par défaut. Pour activer l'analyse heuristique, procédez comme suit :

a. Cochez la case **Activer l'analyse heuristique**. Les options proposées dans le reste de la boîte de dialogue deviennent accessibles.

b. Sélectionnez les types d'analyses heuristiques que vous souhaitez utiliser. Vous avez le choix entre les options suivantes :

- **Activer l'analyse heuristique des macros**. Sélectionnez cette option pour que le module Analyse au téléchargement identifie d'abord tous les fichiers Microsoft Word, Microsoft Excel et autres fichiers Microsoft Office incorporant des macros et compare ensuite le code de la macro avec sa base de données de définitions de virus. Si la correspondance est exacte, le module identifie le nom du virus ; pour les signatures codées qui ressemblent à celles des virus existants, il vous informe qu'il a détecté un virus de macro « probable ».
- **Activer l'analyse heuristique des fichiers programme.** Sélectionnez cette option si vous souhaitez que le module Analyse au téléchargement localise de nouveaux virus dans les fichiers programme en examinant les caractéristiques des fichiers et en les comparant avec celles figurant sur une liste de virus connus. Lorsqu'il détecte un fichier ayant un certain nombre de caractéristiques, le module l'identifie comme étant potentiellement infecté.
- **Activer l'analyse heuristique des macros et fichiers programme.** Sélectionnez cette option si vous souhaitez que le module utilise les deux types d'analyse heuristique. McAffe vous recommande d'utiliser cette option pour une protection antivirus optimale.

> **REMARQUE :** Le module Analyse au téléchargement n'utilise les techniques d'analyse heuristique que sur les types de fichiers que vous désignez dans la boîte de dialogue Extensions de fichiers programme. Si vous décidez d'analyser **Tous les fichiers**, le module appliquera l'analysera heuristique à tous les types de fichiers.

c. Cliquez sur **OK** pour enregistrer vos paramètres et revenir à la boîte de dialogue Propriétés de VShield.

4. Cliquez sur l'onglet Action pour sélectionner d'autres options du module Analyse au téléchargement. Pour enregistrer vos modifications sans fermer la boîte de dialogue Propriétés de l'Analyse au téléchargement, cliquez sur **Appliquer**. Pour enregistrer vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans enregistrer vos modifications, cliquez sur **Annuler**.

> **REMARQUE :** Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

Sélection des options d'action

Lorsque le module Analyse au téléchargement détecte un virus, deux cas de figure se présentent : soit il vous demande comment traiter le fichier infecté, soit il exécute automatiquement une action que vous avez définie précédemment. Utilisez la page de propriétés Action pour spécifier les actions que le module doit vous proposer en cas de détection d'un virus et celles qu'il doit mettre en œuvre automatiquement.

Procédez comme suit :

1. Cliquez sur l'onglet Action dans le module Analyse au téléchargement pour afficher la page de propriétés correspondante (Figure 4-28).

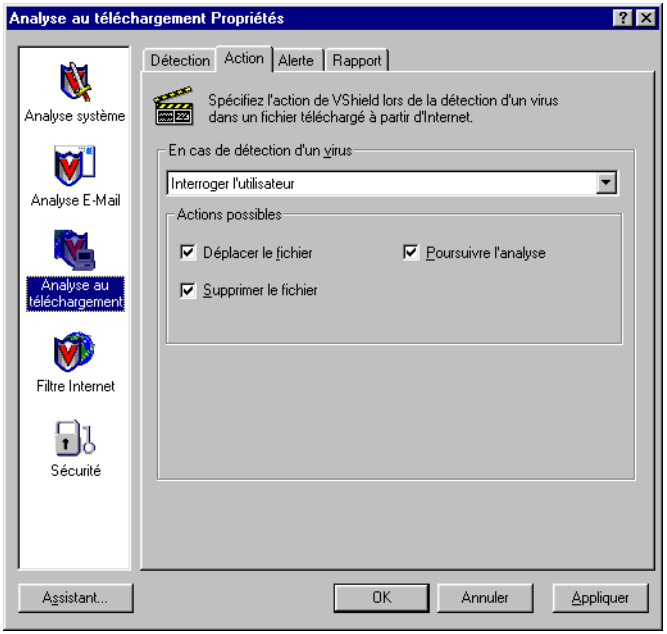

Figure 4-28. Boîte de dialogue Propriétés de l'Analyse au téléchargement – page Action

2. Sélectionnez une réponse dans la liste **En cas de détection d'un virus**. La zone située immédiatement sous la liste changera pour vous proposer des options supplémentaires. Vous avez le choix entre les options suivantes :

   - **Interroger l'utilisateur.** Sélectionnez cette option si vous souhaitez que le module Analyse au téléchargement vous demande quoi faire lorsqu'il détecte un virus — le module affichera alors un message d'alerte et vous proposera plusieurs actions possibles.

REMARQUE : Si vous sélectionnez **Interroger l'utilisateur** dans la liste, cliquez sur l'onglet Alerte pour préciser si le module Analyse au téléchargement doit utiliser un message, un signal sonore ou les deux à la fois pour vous avertir en cas d'infection.

Sélectionnez les options à afficher dans le message d'alerte : Pour chaque case que vous cochez dans cette zone, un bouton d'option apparaîtra dans le message d'alerte que le module affichera en cas de détection d'un virus. Ainsi, si vous cochez par exemple la case **Supprimer le fichier**, le message d'alerte comportera un bouton **Supprimer**.

Vous avez le choix entre les options suivantes :

- **Supprimer le fichier.** Cette option demande au module de supprimer immédiatement la pièce jointe infectée. Toutefois, le module ne touchera pas au message proprement dit.
- **Déplacer le fichier.** Cette option demande au module de placer le fichier infecté dans un dossier de quarantaine. Le message d'alerte affichera un bouton **Déplacer** pour indiquer au module de déplacer le fichier infecté vers un dossier de quarantaine présélectionné. Par défaut, le fichier est stocké dans le dossier intitulé Infecté, situé dans le répertoire du programme VirusScan.
- **Poursuivre l'analyse.** Cette option demande au module de poursuivre son analyse sans prendre d'autres mesures. Si vous avez activé ses options de rapport, le module Analyse au téléchargement enregistre l'incident dans son fichier journal.

- **Déplacer les fichiers infectés vers un dossier.** Sélectionnez cette option de réponse pour que le module déplace les fichiers infectés vers un dossier de quarantaine dès leur détection. Le module place ces fichiers dans un dossier nommé Infecté, situé dans le répertoire du programme VirusScan.
- **Supprimer les fichiers infectés.** Sélectionnez cette option de réponse pour que le module Analyse au téléchargement supprime immédiatement tout fichier infecté détecté. Assurez-vous d'avoir activé la fonction de rapport, afin de disposer d'une liste des fichiers supprimés par le module. Consultez ensuite cette dernière pour connaître les fichiers supprimés à restaurer à partir des copies de sauvegarde. Pour plus de détails, reportez-vous à la section « Sélection des options de rapport » à la page 167.
- **Poursuivre l'analyse.** Sélectionnez cette option de réponse pour que le module continue l'analyse sans prendre de mesures à l'encontre du virus détecté. Si vous activez également la fonction de rapport du module Analyse au téléchargement (voir « Sélection des options de rapport » à la page 167), le programme enregistrera les noms des virus détectés et les noms des fichiers infectés, pour vous permettre de les supprimer à une prochaine occasion.

N'utilisez cette option que si vous prévoyez d'être absent au moment où le module recherchera les virus.

3. Cliquez sur l'onglet Alerte pour sélectionner d'autres options du module Analyse au téléchargement. Pour enregistrer vos modifications sans fermer la boîte de dialogue Propriétés de l'Analyse au téléchargement, cliquez sur **Appliquer**. Pour enregistrer vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans enregistrer vos modifications, cliquez sur **Annuler**.

❑ **REMARQUE :** Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

Sélection des options d'alerte

Une fois que vous l'avez configuré avec les options de réponse qui vous intéressent dans la page Action, vous pouvez laisser le module Analyse au téléchargement rechercher et éliminer automatiquement les virus de votre système au fur et à mesure qu'il les trouve, pratiquement sans aucune autre intervention de votre part. Si, toutefois, vous souhaitez que le module vous informe dès qu'il détecte un virus afin que vous puissiez prendre les mesures adéquates, vous devez le configurer de telle sorte qu'il envoie un message d'alerte à vous ou aux autres utilisateurs.

Procédez comme suit :

1. Cliquez sur l'onglet Alerte dans le module Analyse au téléchargement pour afficher la page de propriétés correspondante (voir Figure 4-29).

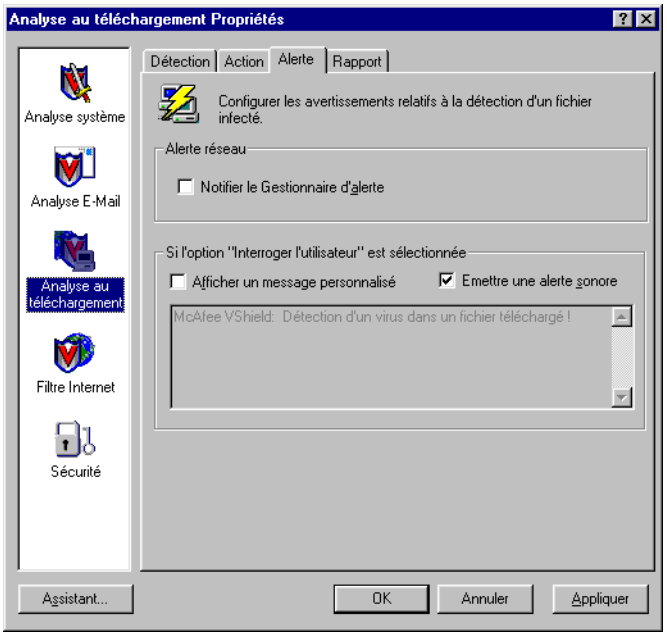

Figure 4-29. Boîte de dialogue Propriétés de l'Analyse au téléchargement – page Alerte

2. Cochez la case **Notifier le Gestionnaire d'alerte** pour que le module envoie des messages d'alerte au Gestionnaire d'alerte qui les transmettra.

   Le Gestionnaire d'alerte est un composant indépendant du logiciel McAfee qui regroupe des messages d'alerte et utilise diverses méthodes pour les envoyer aux destinataires que vous désignez. Le module Analyse au téléchargement enverra ces messages d'alerte avec succès uniquement si vous avez installé l'utilitaire de configuration cliente du Gestionnaire d'alerte. Pour plus de détails, reportez-vous à la section voir « Utilisation de l'utilitaire de Configuration cliente du Gestionnaire d'alerte » à la page 338.

   Vous pouvez transmettre des messages d'alerte directement à un serveur du Gestionnaire d'alerte. Sinon, vous pouvez les envoyer en tant que fichiers texte (.ALR) à un répertoire d'alerte centralisée que le serveur du Gestionnaire d'alerte interroge régulièrement.

REMARQUE : Si vous décochez cette case, le module Analyse au téléchargement n'enverra pas des messages d'alerte via le Gestionnaire d'alerte, mais tous les autres messages d'alerte que vous configurez dans cette page de propriétés resteront intacts.

3. Cochez la case **Émettre une alerte sonore** pour que le module envoie un signal sonore à chaque fois qu'il trouve un fichier infecté.

   Vous pouvez modifier le paramétrage de cette option à condition d'avoir sélectionné **Interroger l'utilisateur** dans la page de propriétés Action. Sinon, la case à cocher Émettre une alerte sonore affichera et utilisera le paramètre que vous lui avez attribué la dernière fois que vous avez sélectionné l'option **Interroger l'utilisateur**. Le module émettra le signal sonore standard du système ou exécutera le fichier .WAV que vous avez configuré sur votre ordinateur.

4. Cochez la case **Afficher un message personnalisé** pour que le module ajoute un message personnalisé au texte du message qu'il affiche lorsqu'il trouve un fichier infecté.

   À l'égard de l'alerte sonore, vous pouvez modifier le paramétrage de cette option à condition d'avoir sélectionné **Interroger l'utilisateur** dans la page de propriétés Action. Si vous ne sélectionnez pas cette option dans la page Action, aucun message d'alerte ou message personnalisé ne s'affichera même si vous avez coché la case Afficher un message personnalisé.

5. Entrez le message que le module doit afficher dans la zone de texte. Vous pouvez entrer 250 caractères maximum.

6. Cliquez sur l'onglet Rapport pour sélectionner d'autres options du module Analyse au téléchargement. Pour enregistrer vos modifications sans fermer la boîte de dialogue Propriétés de l'Analyse au téléchargement, cliquez sur **Appliquer**. Pour enregistrer vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans enregistrer vos modifications, cliquez sur **Annuler**.

REMARQUE : Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

Sélection des options de rapport

Le module Analyse au téléchargement liste ses paramètres courants et récapitule toutes les actions qu'il effectue au cours de ses opérations d'analyse dans un fichier journal appelé WEBINET.TXT. Ce rapport peut à votre convenance figurer dans ce fichier ou dans un fichier texte que vous aurez créé dans un éditeur de texte quelconque à l'intention du module. Vous pourrez ensuite ouvrir et imprimer le fichier journal à partir de n'importe quel éditeur de texte pour le consulter ultérieurement. Utilisez la page de propriétés Rapport pour déterminer les informations à inclure dans le fichier journal du module.

Le fichier WEBINET.TXT constitue un outil de gestion essentiel pour garder la trace de l'activité virale sur votre système et pour noter les paramétrages que vous utilisez pour détecter et traiter les infections identifiées par le module Analyse au téléchargement. Vous pouvez également utiliser les rapports d'incidents enregistrés dans le fichier pour déterminer quels fichiers vous devez remplacer à partir de vos sauvegardes, examiner en quarantaine ou supprimer de votre système.

Pour configurer le module Analyse au téléchargement de sorte qu'il consigne ses actions dans un fichier journal, procédez comme suit :

1. Cliquez sur l'onglet Rapport dans le module Analyse au téléchargement pour afficher la page de propriétés correspondante (Figure 4-30).

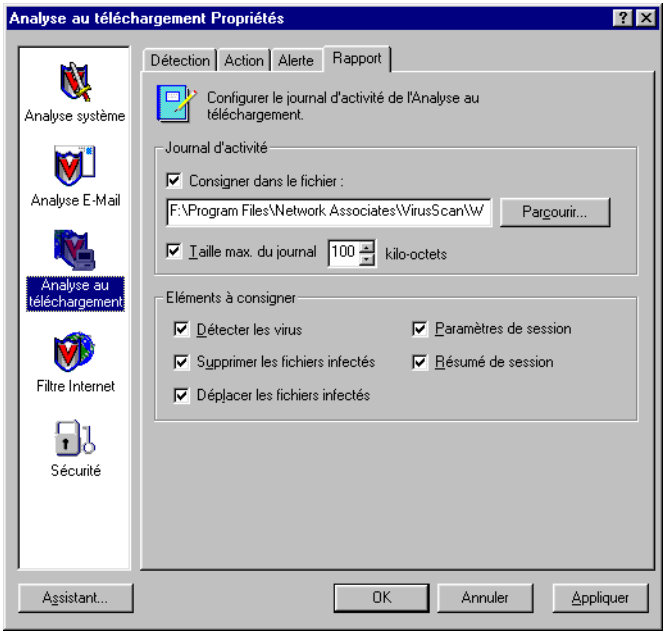

Figure 4-30. Boîte de dialogue Propriétés de l'Analyse au téléchargement – page Rapport

2. Cochez la case **Consigner dans le fichier**.

   Par défaut, le module Analyse au téléchargement enregistre les informations de journal dans le fichier WEBINET.TXT, situé dans le répertoire du programme VirusScan.

   Vous pouvez saisir un chemin d'accès et un nom de fichier différents dans la zone de texte prévue à cet effet, ou bien cliquer sur **Parcourir** pour localiser un fichier approprié sur votre disque dur ou sur votre réseau. Vous pouvez utiliser un fichier différent, mais le fichier texte doit être déjà créé. Le module ne crée pas de fichier.

3. Pour limiter la taille du fichier journal, cochez la case **Taille maximale du journal**, puis spécifiez cette taille, en Kilo-octets, dans la zone de texte prévue à cet effet. Si vous ne cochez pas cette case, le fichier journal peut voir sa taille augmenter et atteindre une limite déterminée par votre espace disque ou votre système de fichiers.

   Entrez une valeur comprise entre 10 Ko et 999 Ko. Par défaut, le module Analyse au téléchargement limite la taille du fichier à 100 Ko. Si les données du journal dépassent la taille allouée pour le fichier, le module efface le journal existant et le reprend au point où il s'était interrompu.

4. Cochez les cases correspondant aux informations que vous souhaitez que le module enregistre dans son fichier journal. En général, le module enregistre les données à la fin de la session d'analyse ou lorsque vous arrêtez le système.

   Vous pouvez choisir d'enregistrer les informations suivantes :

   - **Détecter les virus**. Cochez cette case pour que le fichier journal enregistre le nombre de virus trouvés par le module dans chaque session d'analyse. Décochez la case pour exclure ces informations.
   - **Supprimer les fichiers infectés**. Cochez cette case pour que le fichier journal enregistre le nombre de virus supprimés par le module dans chaque session d'analyse. Décochez cette case pour exclure ces informations.
   - **Déplacer les fichiers infectés**. Cochez cette case pour que le fichier journal enregistre le nombre de virus que le module a placé dans un dossier de quarantaine dans chaque session d'analyse. Décochez cette case pour exclure ces informations.
   - **Paramètres de session**. Cochez cette case pour que le fichier journal enregistre les paramètres de configuration que vous avez utilisés pour le module dans chaque session d'analyse. Décochez cette case pour exclure ces informations.
   - **Résumé de session**. Cochez cette case pour que le fichier journal récapitule les actions effectuées par le module dans chaque session d'analyse.

     Si vous activez cette option, le journal enregistrera les informations suivantes :

     – Nombre de fichiers analysés par le module.

     – Nombre de fichiers infectés nettoyés par le module.

     – Nombre de fichiers infectés supprimés par le module.

     – Nombre de fichiers infectés que le module a placé dans un dossier de quarantaine.

     – Paramètres que vous avez attribués au module Analyse au téléchargement.

     Décochez la case pour exclure ces informations.

5. Cliquez sur un autre onglet pour modifier l'un ou l'autre des paramètres du module Analyse au téléchargement, ou bien cliquez sur l'une des icônes situées le long de la boîte de dialogue Propriétés de l'Analyse au téléchargement pour sélectionner les options d'un autre module.

Pour enregistrer vos modifications sans fermer la boîte de dialogue Propriétés de l'Analyse au téléchargement, cliquez sur **Appliquer**. Pour enregistrer vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans enregistrer vos modifications, cliquez sur **Annuler**..

❑ **REMARQUE :** Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

Configuration du module Filtre Internet

Bien que les objets Java et ActiveX comportent des sécurités destinées à protéger les systèmes informatiques, des programmeurs déterminés à nuire ont développé des objets qui exploitent des fonctionnalités Java ou ActiveX peu connues pour commettre différentes agressions sur ces systèmes.

Ces objets dangereux sont souvent tapis à l'abri des sites Web jusqu'à ce que vous les consultiez et que vous les téléchargiez dans votre système, souvent sans vous douter de leur présence. La plupart des navigateurs offrent la possibilité de bloquer complètement les applets Java ou les contrôles ActiveX, ou d'activer des fonctions de sécurité qui authentifient les objets avant de les télécharger sur votre système. Mais ces approches risquent de vous priver des bénéfices de l'interactivité de certains sites que vous visitez en bloquant sans discrimination tous les objets, qu'ils soient dangereux ou non.

Le module Filtre Internet propose une approche plus judicieuse. Il utilise une base de données à jour d'objets connus pour attaquer les classes écran de Java et les contrôles ActiveX que vous rencontrez en surfant.

À chaque fois qu'il trouve un virus, le module peut vous demander l'action à entreprendre, ou bloquer automatiquement l'objet ou le site dangereux. Le module peut vous informer sur les actions menées en réponse à l'infection, soit par un message d'alerte, qu'il émet au moment d'appliquer la mesure corrective, soit dans un fichier journal que vous pouvez consulter à tout moment.

Pour sélectionner les options qui vous intéressent, cliquez sur l'icône Filtre Internet, située à gauche de la boîte de dialogue Propriétés de VShield, pour afficher les pages de propriétés de ce module.

❑ **REMARQUE :** L'icône Filtre Internet n'apparaît pas ici, sauf si vous avez installé le logiciel VirusScan à l'aide de l'option Installation personnalisée et que vous avez choisi d'installer le composant Analyse Internet.

Sélection des options de détection

Par défaut, le module Filtre Internet prend comme hypothèse de départ que vous souhaitez bloquer tous les objets et tous les sites nocifs listés dans sa base de données pour vous éviter de les charger accidentellement (Figure 4-31 à la page 171). Cette option vous offre le niveau de sécurité le plus étroit vis-à-vis des objets nuisibles, mais vous permet d'utiliser les autres objets présents dans les sites Internet que vous visitez.

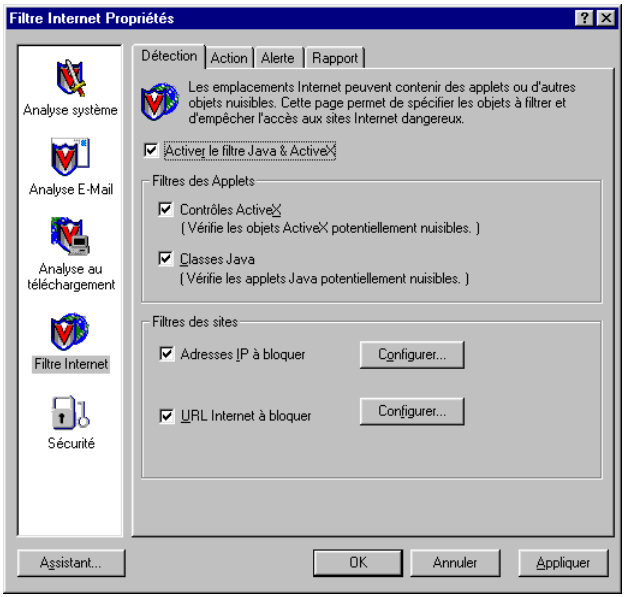

Figure 4-31. Propriétés du Filtre Internet – page Détection

Pour modifier les options de configuration, procédez comme suit :

1. Vérifiez que la case Activer le filtre Java & ActiveX est cochée.

   Les options proposées dans le reste de la page de propriétés deviennent accessibles.

2. Spécifiez les objets que le module Filtre Internet doit examiner. Vous avez le choix entre les options suivantes :

   - **Contrôles ActiveX**. Cochez cette case pour que le module recherche et bloque les contrôles ActiveX ou .OCX dangereux.
   - **Classes Java**. Cochez cette case pour que le module recherche et bloque les classes Java ou les applets écrits en Java susceptibles d'endommager votre système.

Le module Filtre Internet comparera les objets que vous rencontrerez en visitant des sites Internet avec une base de données interne listant les caractéristiques des objets connus comme nocifs. Lorsqu'il trouve une correspondance, le module peut soit vous alerter et vous laisser décider quoi faire, soit empêcher automatiquement le téléchargement des objets concernés. Pour plus de détails, reportez-vous à la section voir « Sélection des options d'action » à la page 175.

3. Indiquez au module les sites à filtrer. Le programme dispose d'une liste de sites Internet dangereux, qu'il utilise pour sélectionner les sites auxquels il empêchera votre navigateur d'accéder. Vous pouvez activer cette fonction et faire des ajouts à la liste des sites « interdits » de deux façons différentes :

   - **Adresses IP à bloquer.** Cochez cette case pour demander au module d'identifier les sites Internet dangereux à l'aide de leurs adresses IP (Internet Protocol). Pour visualiser ou indiquer les adresses des sites dont l'accès doit être interdit, cliquez sur **Configurer** pour afficher la boîte de dialogue Adresses IP interdites (Figure 4-32).

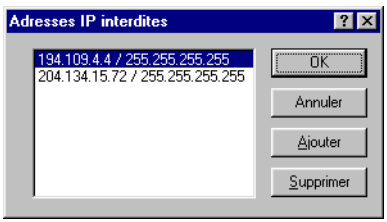

Figure 4-32. Boîte de dialogue Adresses IP interdites

La boîte de dialogue Adresses IP interdites identifie les adresses IP que le module Filtre Internet doit bloquer à chaque fois que vous ou un autre utilisateur tente de s'y connecter.

Par défaut, la liste inclut deux sites qui téléchargent des objets Java ou ActiveX nuisibles pour votre ordinateur dès votre connexion. Vous pouvez ajouter d'autres sites, puis protéger vos paramètres par un mot de passe afin qu'aucun autre utilisateur ne puisse les supprimer.

Une adresse IP (Internet Protocol) se compose de quatre groupes de trois chiffres. En voici un exemple :

123.123.123.123

Le module Filtre Internet peut utiliser cette séquence pour identifier un ordinateur ou un réseau d'ordinateurs spécifique sur Internet et empêcher votre navigateur de s'y connecter. Chaque série de chiffres peut aller de zéro à 255. La première série de chiffres correspond à l'adresse de domaine du site interdit, c'est-à-dire, le numéro que vous utilisez pour le retrouver sur Internet, et la deuxième série correspond à un « masque de sous-réseau ».

Un masque de sous-réseau est un moyen de « réaffecter » une suite d'adresses d'ordinateurs au sein d'un réseau interne. Le module affiche 255.255.255.255 comme masque de sous-réseau par défaut. Dans la plupart des cas, vous n'aurez pas à modifier cette séquence, mais si vous savez qu'un nœud de réseau particulier accessible à partir du site que vous visitez est une source de danger, vous pouvez essayer de saisir un masque de sous-réseau pour éviter d'accéder à d'autres machines en réseau avec le serveur en question.

Pour modifier la liste, vous avez le choix entre les options suivantes :

– Cliquez sur **Ajouter** pour ouvrir la boîte de dialogue Ajouter une adresse IP (Figure 4-33).

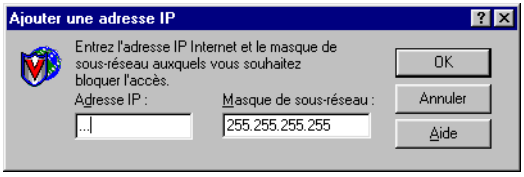

Figure 4-33. Boîte de dialogue Ajouter une adresse IP

Ensuite, procédez comme suit :

a. Tapez l'adresse IP que vous souhaitez ajouter à la liste des adresses IP interdites dans la zone de texte de gauche. Faites bien attention à saisir l'adresse correctement, en séparant chaque série de chiffres par un point.

b. Si vous connaissez sa valeur exacte, tapez le masque de sous-réseau associé à l'adresse IP que vous souhaitez ajouter à la liste des adresses IP interdites dans la zone de texte de droite. Sinon, ne touchez pas à la valeur par défaut.

c. Cliquez sur **OK** pour revenir à la boîte de dialogue Adresses IP interdites.

– Sélectionnez un élément dans la liste, puis cliquez sur **Supprimer** pour l'effacer.

Une fois que vous avez terminé d'ajouter à la liste les adresses que vous souhaitez bloquer, cliquez sur **OK** pour revenir à la boîte de dialogue Propriétés du Filtre Internet.

- **URL Internet à bloquer.** Cochez cette case pour demander au module d'identifier les sites Internet dangereux à l'aide de leurs URL (Uniform Resource Locator). Pour visualiser ou sélectionner les adresses que le module doit interdire, cliquez sur **Configurer** pour ouvrir la boîte de dialogue URL interdites (Figure 4-34).

Figure 4-34. Boîte de dialogue URL interdites

La boîte de dialogue URL interdites identifie les URL que le module Filtre Internet doit bloquer à chaque fois que vous ou un autre utilisateur tente de s'y connecter.

Par défaut, la liste inclut deux noms de domaine qui téléchargent des objets Java ou ActiveX nuisibles pour votre ordinateur dès votre connexion. Vous pouvez ajouter d'autres noms de domaine, puis protéger vos paramètres par un mot de passe afin qu'aucun autre utilisateur ne puisse les supprimer.

Une URL indique le nom de domaine et l'emplacement d'un ordinateur sur Internet. Cette adresse est souvent accompagnée du « protocole de transport » que vous souhaitez utiliser pour demander une ressource à cet ordinateur. Voici un exemple d'URL complète de site Web :

http://www.domain.com

L'URL complète indique à votre navigateur de demander la ressource en utilisant le protocole HTTP (HyperText Transport Protocol) — « http:// » — à un ordinateur appelé « www » sur un domaine de réseau appelé « domaine.com ». Parmi les autres protocoles figurent le FTP — « ftp:// » — et le GOPHER — « gopher:// ». Le système de nom de domaine (DNS) d'Internet traduit les URL en adresses IP à partir de bases de données centralisées, tenues à jour et communiquant entre elles.

Pour ajouter un site dans cette liste, vous devez entrer le nom de domaine, car le module part du principe que vous utiliserez le protocole HTTP (Hyper Text Transport Protocol). Pour modifier la liste, vous avez le choix entre les options suivantes :

– Cliquez sur **Ajouter** pour ouvrir la boîte de dialogue Ajouter une URL. Tapez ensuite l'URL que vous souhaitez ajouter à la liste des URL interdites dans la boîte de dialogue qui s'affiche (Figure 4-35). Cliquez sur **OK** pour revenir à la boîte de dialogue Adresses IP interdites.

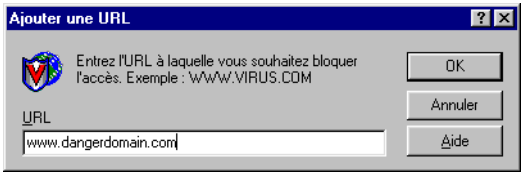

Figure 4-35. Boîte de dialogue Ajouter une URL

– Sélectionnez un élément dans la liste, puis cliquez sur **Supprimer** pour l'effacer.

Une fois que vous avez terminé d'ajouter à la liste les adresses que vous souhaitez bloquer, cliquez sur **OK** pour revenir à la boîte de dialogue Propriétés du Filtre Internet.

4. Cliquez sur l'onglet Action pour sélectionner d'autres options du module Filtre Internet. Pour enregistrer vos modifications sans fermer la boîte de dialogue Propriétés du Filtre Internet, cliquez sur **Appliquer**. Pour enregistrer vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans enregistrer vos modifications, cliquez sur **Annuler**.

❑ **REMARQUE :** Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

Sélection des options d'action

Lorsque le module Filtre Internet rencontre un objet dangereux ou un site interdit, il peut réagir soit en vous demandant si vous désirez qu'il le bloque, soit en le bloquant automatiquement. Utilisez la page de propriétés Action pour indiquer au module la solution à adopter.

Par défaut, le module vous laisse décider quoi faire (Figure 4-36 à la page 176).

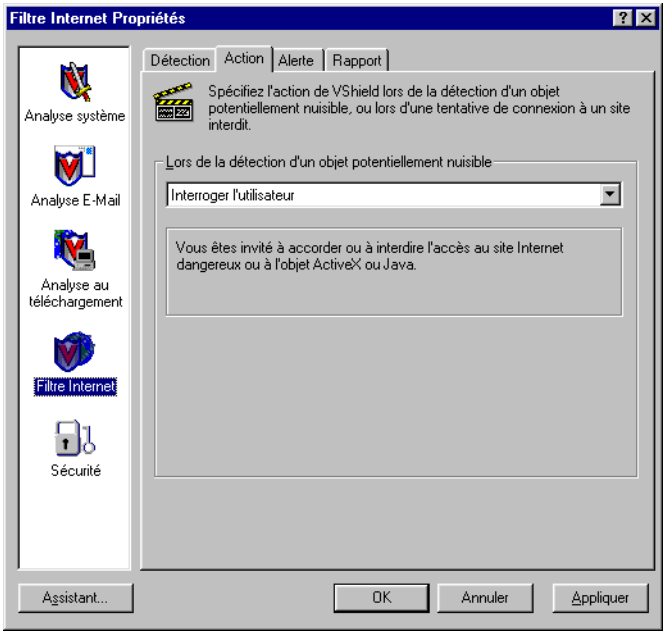

Figure 4-36. Boîte de dialogue Propriétés du Filtre Internet – page Action

Sélectionnez une action dans la liste **Lors de la détection d'un objet potentiellement nuisible**. Vous avez le choix entre les options suivantes :

- **Interroger l'utilisateur.** Sélectionnez cette option de réponse pour que le module vous demande s'il doit bloquer l'objet ou le site dangereux, ou s'il doit en autoriser l'accès.

  REMARQUE : Si vous sélectionnez **Interroger l'utilisateur** dans la liste, cliquez sur l'onglet Alerte pour préciser si le module Filtre Internet doit utiliser un message, un signal sonore ou les deux à la fois pour vous avertir en cas de détection d'un objet potentiellement nuisible.

- **Interdire l'accès aux objets.** Sélectionnez cette option de réponse si vous souhaitez que le module bloque automatiquement les objets et les sites dangereux. Le programme le fera en fonction du contenu de sa propre base de données, ainsi que des informations concernant les sites que vous aurez vous-même ajoutés. Pour plus de détails, reportez-vous à la section voir « Sélection des options de détection » à la page 171.

Cliquez sur l'onglet Alerte pour sélectionner d'autres options du module Filtre Internet. Pour enregistrer vos modifications sans fermer la boîte de dialogue Propriétés du Filtre Internet, cliquez sur **Appliquer**. Pour enregistrer vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans enregistrer vos modifications, cliquez sur **Annuler**.

❑ **REMARQUE :** Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

Sélection des options d'alerte

Une fois que vous l'avez configuré avec les options de réponse qui vous intéressent dans la page Action, vous pouvez laisser le module Filtre Internet rechercher et bloquer automatiquement les objets nuisibles ou les sites Internet dangereux de votre système au fur et à mesure qu'il les trouve, pratiquement sans aucune autre intervention de votre part. Si, toutefois, vous souhaitez que le module vous informe dès qu'il détecte un objet nuisible afin que vous puissiez prendre les mesures adéquates, vous devez le configurer de telle sorte qu'il envoie un message d'alerte à vous ou aux autres utilisateurs.

Procédez comme suit :

1. Cliquez sur l'onglet Alerte dans le module Filtre Internet pour afficher la page de propriétés correspondante (Figure 4-37).

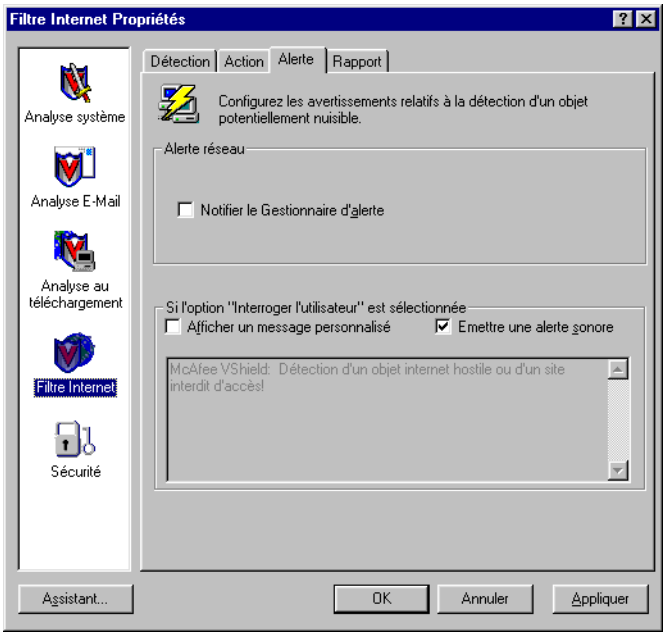

Figure 4-37. Boîte de dialogue Propriétés du Filtre Internet – page Alerte

2. Cochez la case **Notifier le Gestionnaire d'alerte** pour que le module envoie des messages d'alerte au Gestionnaire d'alerte qui les transmettra.

   Le Gestionnaire d'alerte est un composant indépendant du logiciel McAfee qui regroupe des messages d'alerte et utilise diverses méthodes pour les envoyer aux destinataires que vous désignez. Le module Filtre Internet enverra ces messages d'alerte avec succès uniquement si vous avez installé l'utilitaire de configuration cliente du Gestionnaire d'alerte. Pour plus de détails, reportez-vous à la section voir « Utilisation de l'utilitaire de Configuration cliente du Gestionnaire d'alerte » à la page 338.

   Vous pouvez transmettre des messages d'alerte directement à un serveur du Gestionnaire d'alerte. Sinon, vous pouvez les envoyer en tant que fichiers texte (.ALR) à un répertoire d'alerte centralisée que le serveur du Gestionnaire d'alerte interroge régulièrement.

   REMARQUE : Si vous décochez cette case, le module Filtre Internet n'enverra pas des messages d'alerte via le gestionnaire d'alerte, mais tous les autres messages d'alerte que vous configurez dans cette page de propriétés resteront intacts.

3. Cochez la case **Émettre une alerte sonore** pour que le module envoie un signal sonore à chaque fois qu'il trouve un fichier infecté.

   Vous pouvez modifier le paramétrage de cette option à condition d'avoir sélectionné **Interroger l'utilisateur** dans la page de propriétés Action. Sinon, la case à cocher Émettre une alerte sonore affichera et utilisera le paramètre que vous lui avez attribué la dernière fois que vous avez sélectionné l'option **Interroger l'utilisateur**. Le module émettra le signal sonore standard du système ou exécutera le fichier .WAV que vous avez configuré sur votre ordinateur.

4. Cochez la case **Afficher un message personnalisé** pour que le module ajoute un message personnalisé au texte du message qu'il affiche lorsqu'il trouve un fichier infecté.

   À l'égard de l'alerte sonore, vous pouvez modifier le paramétrage de cette option à condition d'avoir sélectionné **Interroger l'utilisateur** dans la page de propriétés Action. Si vous ne sélectionnez pas cette option dans la page Action, aucun message d'alerte ou message personnalisé ne s'affichera même si vous avez coché la case Afficher un message personnalisé.

5. Entrez le message que le module doit afficher dans la zone de texte. Vous pouvez entrer 250 caractères maximum.

6. Cliquez sur l'onglet Rapport pour sélectionner d'autres options du module Filtre Internet. Pour enregistrer vos modifications sans fermer la boîte de dialogue Propriétés du Filtre Internet, cliquez sur **Appliquer**. Pour enregistrer vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans enregistrer vos modifications, cliquez sur **Annuler**.

   ❑ **REMARQUE :** Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

Sélection des options de rapport

Le module Filtre Internet enregistre le nombre d'objets Java et ActiveX analysés et le nombre d'objets bloqués dans un fichier appelé WEBFLTR.TXT. C'est également dans ce fichier qu'il consigne le nombre de sites Internet que vous avez visités pendant que le module était actif et le nombre de sites dangereux auxquels il a empêché votre navigateur de se connecter.

Ce rapport peut à votre convenance figurer dans ce fichier ou dans un fichier texte que vous aurez créé dans un éditeur de texte quelconque à l'intention du module. Vous pourrez ensuite ouvrir et imprimer le fichier journal à partir de n'importe quel éditeur de texte pour le consulter ultérieurement. Utilisez la page de propriétés Rapport pour désigner le fichier qui servira de journal du module Filtre Internet et pour spécifier la taille maximale de ce fichier.

Le fichier WEBFLTR.TXT constitue un outil de gestion essentiel pour garder la trace de l'activité des logiciels nuisibles sur votre système et pour noter les paramétrages que vous utilisez pour détecter et bloquer les objets ou les sites dangereux identifiés par le module.

Pour configurer le module Filtre Internet de sorte qu'il consigne ses actions dans un fichier journal, procédez comme suit :

1. Cliquez sur l'onglet Rapport dans le module Filtre Internet pour afficher la page de propriétés correspondante (Figure 4-38 à la page 180).

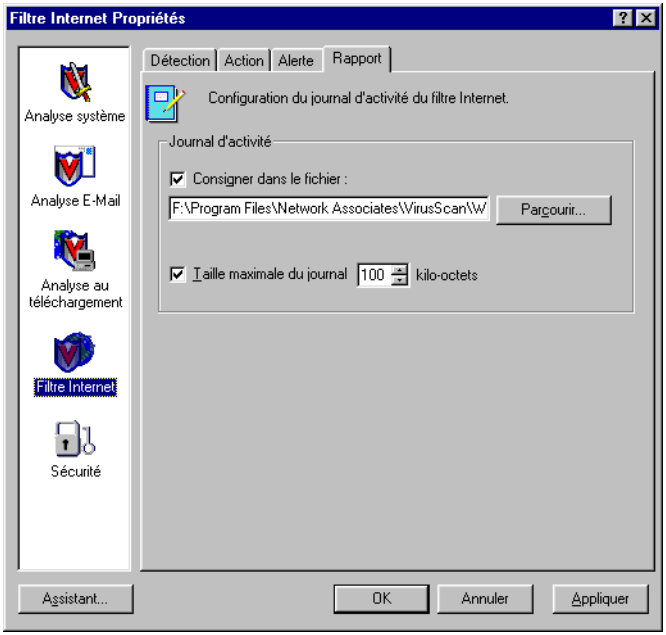

Figure 4-38. Boîte de dialogue Propriétés du Filtre Internet – page Rapport

2. Cochez la case **Consigner dans le fichier**.

Par défaut, le module enregistre les données de son rapport dans le fichier WEBFLTR.TXT, situé dans le répertoire du programme de VirusScan. Vous pouvez saisir un chemin d'accès et un nom de fichier différents dans la zone de texte prévue à cet effet, ou bien cliquer sur **Parcourir** pour localiser un fichier approprié sur votre disque dur ou sur votre réseau.

3. Pour limiter la taille du fichier journal, cochez la case **Taille limite du fichier journal**, puis saisissez cette taille, en Kilo-octets, dans la zone de texte prévue à cet effet.

   Entrez une valeur comprise entre 10 Ko et 999 Ko. Par défaut, le module limite la taille du fichier à 100 Ko. Si les données du journal dépassent la taille allouée pour le fichier, le module efface le journal existant et le reprend au point où il s'était interrompu.

4. Cliquez sur un autre onglet pour modifier l'un ou l'autre des paramètres du module Filtre Internet, ou bien cliquez sur l'une des icônes situées le long de la boîte de dialogue Propriétés du Filtre Internet pour sélectionner les options d'un autre module.

   Pour enregistrer vos modifications dans le module Filtre Internet sans fermer la boîte de dialogue, cliquez sur **Appliquer**. Pour enregistrer vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans enregistrer vos modifications, cliquez sur **Annuler**.

❑ **REMARQUE :** Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

Configuration du module Sécurité

Pour éviter que quelqu'un puisse modifier vos paramétrages des modules VShield sans votre accord, vous pouvez protéger l'accès aux pages de propriétés de l'un ou de plusieurs de vos modules avec un mot de passe. Les administrateurs système peuvent interdire aux utilisateurs du réseau de désactiver le moteur d'analyse VShield (voir Étape 4 à la page 121 pour plus de détails), puis protéger ce paramètre avec un mot de passe afin d'imposer une politique antivirus stricte à tous les utilisateurs du réseau et ce, facilement et efficacement.

Utilisez le module Sécurité pour attribuer un mot de passe et choisir les pages de propriétés que vous souhaitez protéger.

Activation de la protection par mot de passe

VShield n'active pas le module Sécurité par défaut, car il lui faut connaître le mot de passe que vous souhaitez attribuer à vos paramétrages.

Pour activer et configurer la protection par mot de passe du module Sécurité, procédez comme suit :

1. Cochez la case **Activer la protection par mot de passe**.

   Les options proposées dans le reste de la page de propriétés deviennent accessibles (Figure 4-39 à la page 182).

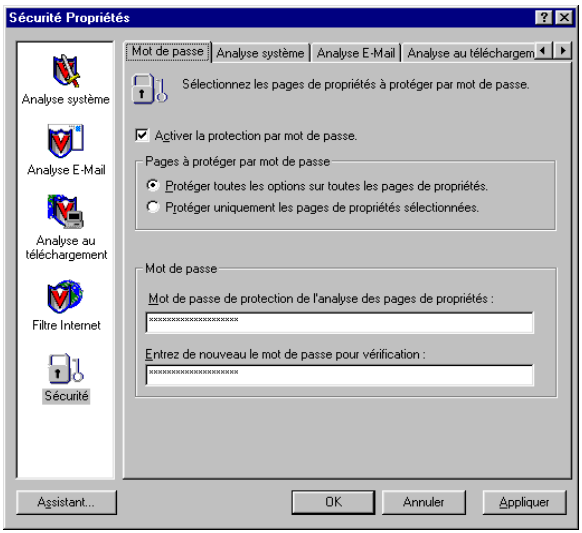

Figure 4-39. Boîte de dialogue Propriétés de la Sécurité – page Mot de passe

2. Décidez si vous voulez protéger les pages de propriétés de tous les modules VShield, ou seulement certaines de ces pages. Vous avez le choix entre les options suivantes :

   - **Protéger toutes les options sur toutes les pages de propriétés.** Cliquez sur ce bouton pour tout verrouiller en une seule fois.
   - **Protéger uniquement les pages de propriétés sélectionnées.** Cliquez sur ce bouton pour sélectionner les pages de propriétés que vous souhaitez verrouiller. Les autres onglets de la boîte de dialogue Propriétés de la Sécurité vous permettent de choisir les pages une par une.

3. Saisissez un mot de passe qui servira à verrouiller vos paramétrages. Tapez une combinaison de 20 caractères maximum dans la zone de texte supérieure de la partie Mot de passe, puis tapez à nouveau la même combinaison dans la zone de texte située dessous pour confirmer votre mot de passe.

IMPORTANT : La protection par mot de passe dans le moteur d'analyse VShield est différente de celle que vous pouvez attribuer aux tâches dans la console VirusScan, ou aux paramètres dans l'application VirusScan. Le mot de passe que vous choisissez pour l'un de ces éléments n'est pas automatiquement assigné à l'autre. Vous devez choisir les mots de passe indépendamment l'un de l'autre.

---

4. Cliquez sur n'importe lequel des autres onglets du module Sécurité pour protéger les pages de propriétés individuellement. Pour enregistrer votre mot de passe sans fermer la boîte de dialogue Propriétés de la Sécurité, cliquez sur **Appliquer**. Si vous choisissez de protéger toutes les pages de propriétés de tous les modules et que vous voulez fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans enregistrer vos modifications, cliquez sur **Annuler**.

REMARQUE : Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

Saisie de votre mot de passe pour protéger les paramètres de configuration

Une fois vos paramétrages protégés par un mot de passe, le module Sécurité vous demandera de saisir ce mot de passe à chaque fois que vous ouvrirez la boîte de dialogue Propriétés de VShield (Figure 4-40).

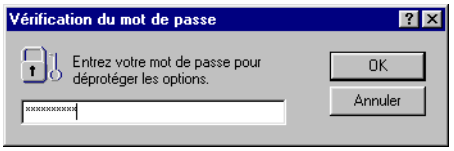

Figure 4-40. Boîte de dialogue Vérification du mot de passe

Tapez votre mot de passe dans la zone de texte prévue à cet effet, puis cliquez sur **OK** pour accéder à la boîte de dialogue Propriétés de VShield.

Protection individuelle des pages de propriétés

Si vous avez sélectionnez l'option **Protéger uniquement les pages de propriétés sélectionnées** dans la page Mot de passe du module Sécurité, vous pouvez sélectionner les options de configuration que vous souhaitez verrouiller dans chaque module.

Procédez comme suit :

1. Cliquez l'onglet du *module* dont vous souhaitez protéger le paramétrage. Si vous ne voyez pas l'onglet qui vous intéresse, cliquez sur ◀ ou sur ▶ pour l'afficher. La Figure 4-41 à la page 184 montre exemple de cette page.

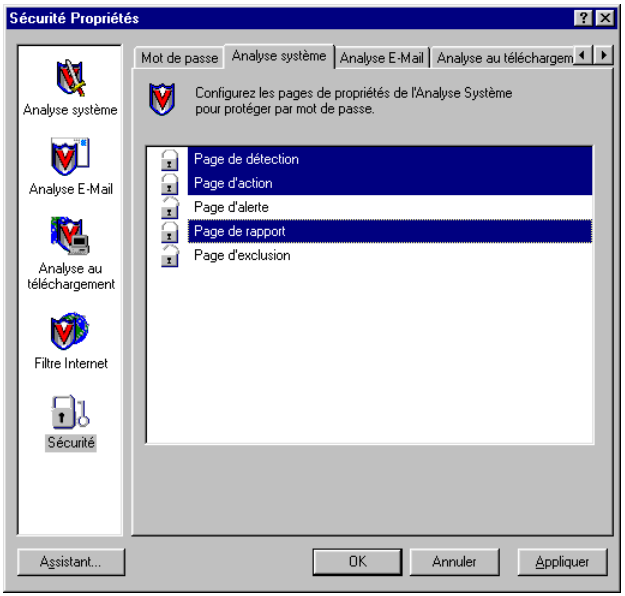

Figure 4-41. Boîte de dialogue Propriétés de la Sécurité – page Analyse système

2. Sélectionnez les paramètres que vous souhaitez protéger dans la liste affichée.

   Vous pouvez protéger les pages de propriétés d'un module individuellement ou dans leur ensemble. Dans la liste de sécurité illustrée par la Figure 4-41, les noms des pages de propriétés verrouillées sont assortis d'une icône représentant un verrou fermé. Pour désactiver la protection d'une page de propriétés, cliquez sur le verrou fermé pour qu'il s'ouvre.

3. Sélectionnez toutes les pages de propriétés que vous souhaitez protéger dans chaque module.

4. Pour enregistrer votre mot de passe sans fermer la boîte de dialogue Propriétés de la Sécurité, cliquez sur **Appliquer**. Pour enregistrer vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans enregistrer vos modifications, cliquez sur **Annuler**.

❑ **REMARQUE :** Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

Utilisation du menu contextuel de VShield

Le moteur d'analyse VShield regroupe plusieurs de ses commandes les plus courantes dans un menu contextuel associé à son icône de la barre d'état système  . Double-cliquez sur cette icône pour afficher la boîte de dialogue État de VShield. Cliquez avec le bouton droit sur l'icône pour afficher les commandes suivantes :

- **État.** Choisissez cette commande pour ouvrir la boîte de dialogue État de VShield.
- **Propriétés.** Pointez sur cette option, puis choisissez l'un des modules listés pour ouvrir la boîte de dialogue Propriétés de VShield sur la page de propriétés du module sélectionné.
- **Activer.** Pointez sur cette option, puis choisissez l'un des modules VShield listés pour l'activer ou le désactiver. Les modules cochés dans le menu sont activés, les autres ne le sont pas. Si vous utilisez cette méthode pour désactiver un module, il reste désactivé jusqu'au redémarrage de votre ordinateur.
- **À propos de.** Choisissez cette option pour afficher le numéro de version et le numéro de série du moteur d'analyse VShield, le numéro de version et la date de création des fichiers .DAT courants, et la mention des droits d'auteur de Network Associates.
- **Quitter.** Choisissez cette option pour arrêter tous les modules VShield et pour vider le moteur d'analyse de la mémoire de l'ordinateur.

Désactivation ou arrêt du moteur d'analyse VShield

À la fin de l'installation de VirusScan, le programme d'installation vous demande si vous souhaitez activer immédiatement le moteur d'analyse VShield. Si vous répondez par oui, le moteur d'analyse VShield se charge immédiatement en mémoire et commence à fonctionner avec un jeu d'options par défaut qui vous offre une protection antivirus de base. Dans le cas contraire, le moteur d'analyse VShield se chargera automatiquement lors du prochain démarrage de votre ordinateur.

Lors du démarrage du moteur d'analyse VShield, ce dernier affiche une icône dans la barre d'état système Windows pour indiquer les modules en cours d'exécution. Pour en savoir plus sur la signification des différents états d'une icône, reportez-vous à la section « Description de chaque état d'une icône de la barre d'état système VShield » à la page 109.

Vous pouvez arrêter complètement le moteur d'analyse, ce qui implique la désactivation de tous les modules VShield et la suppression du moteur d'analyse de la mémoire de l'ordinateur. L'icône VShield disparaît de la barre d'état système. À ce stade, vous ne pouvez redémarrer le moteur d'analyse qu'à partir du panneau de configuration VirusScan, de la console VirusScan, ou en redémarrant votre ordinateur, à condition d'avoir configuré VShield pour être chargé au démarrage.

Cette procédure diffère de la désactivation du moteur d'analyse, qui implique la désactivation de l'un ou de plusieurs de ses modules afin d'éviter qu'ils soient exécutés au cours d'une session d'analyse. Dans ce cas, le moteur d'analyse n'est pas arrêté ni déchargé de la mémoire de votre ordinateur. Le moteur d'analyse VShield peut demeurer actif dans la mémoire même si aucun de ses modules n'est actif. Dans cet état, le moteur d'analyse affiche toujours une icône dans la barre d'état système Windows, sur laquelle vous pouvez cliquer pour le réactiver.

Annulation du démarrage automatique du moteur d'analyse

Si vous ne souhaitez pas que le moteur d'analyse VShield démarre automatiquement, vous pouvez interdire ce type de démarrage dans le panneau de configuration VirusScan.

Procédez comme suit :

1. Cliquez sur **Démarrer** dans la barre des tâches Windows, pointez sur **Paramètres**, puis choisissez **Panneau de configuration**.
2. Localisez et double-cliquez sur le panneau de configuration VirusScan pour l'ouvrir.

3. Cliquez sur l'onglet Composants.
4. Décochez la case **Charger VShield au démarrage** dans la partie supérieure de la page de propriétés Composants.
5. Cliquez sur **OK** pour fermer le panneau de configuration.

Le moteur d'analyse VShield ne sera pas arrêté ni déchargé à ce stade, mais il ne sera pas chargé lors du prochain démarrage de votre ordinateur.

Arrêt complet du moteur d'analyse VShield

Vous pouvez arrêter complètement le moteur d'analyse VShield, c'est-à-dire, le désactiver et le supprimer de la mémoire de l'ordinateur en utilisant l'une des trois méthodes proposées ci-dessous. Une fois que vous avez arrêté le moteur d'analyse, vous pouvez le réactiver uniquement en le redémarrant ou en réamorçant votre ordinateur. Pour en savoir plus sur le démarrage et le redémarrage du moteur d'analyse, reportez-vous à la section « Activation ou démarrage du moteur d'analyse VShield » à la page 105.

Méthode 1 : Utiliser le menu contextuel de VShield

Procédez comme suit :

1. Dans la barre d'état système Windows, cliquez avec le bouton droit sur l'icône VShield pour afficher son menu contextuel.
2. Cliquez sur **Quitter**.

   Le moteur d'analyse VShield est fermé et retiré de la mémoire. L'icône VShield disparaît de la barre des tâches Windows.

Méthode 2 : Utiliser la console VirusScan

Procédez comme suit :

1. Double-cliquez sur l'icône Console VirusScan dans la barre d'état système Windows pour amener la fenêtre de la console au premier plan (Figure 4-42).

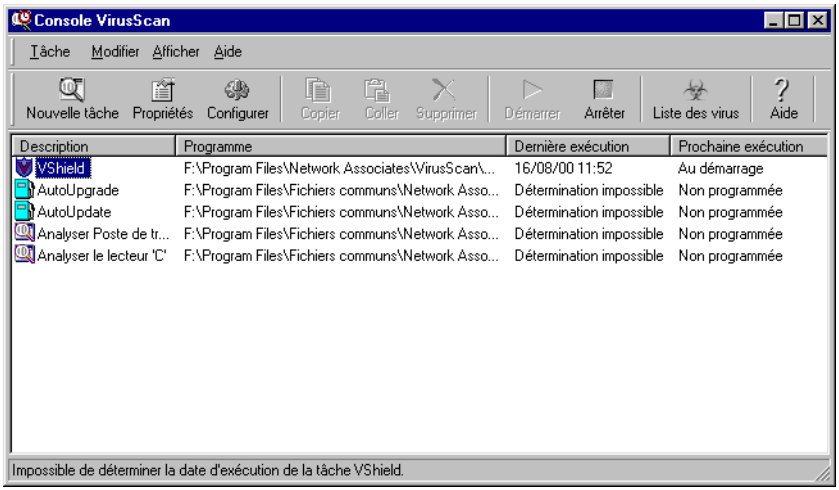

Figure 4-42. Fenêtre de la console VirusScan

2. Sélectionnez VShield dans la liste des tâches, puis choisissez **Désactiver** dans le menu **Tâche**.

   La console arrête le moteur d'analyse VShield et tous ses modules et les vide de la mémoire de l'ordinateur. L'icône VShield disparaît de la barre des tâches Windows.

3. Cliquez sur le bouton Réduire ou Fermer, dans le coin supérieur droit de la fenêtre de la console, pour l'afficher à nouveau sous forme d'icône dans la barre d'état système.

❑ **REMARQUE :** Ne choisissez pas **Quitter** dans le menu **Tâche**. Ceci provoquerait l'arrêt de la console et son retrait de la mémoire de l'ordinateur. La console doit être activée pour pouvoir exécuter vos tâches planifiées.

Méthode 3 : Utiliser le panneau de configuration VirusScan

Procédez comme suit :

1. Cliquez sur **Démarrer** dans la barre des tâches Windows, pointez sur **Paramètres**, puis choisissez **Panneau de configuration**.

2. Localisez et double-cliquez sur le panneau de configuration VirusScan  pour l'ouvrir (Figure 4-43).

VirusScan

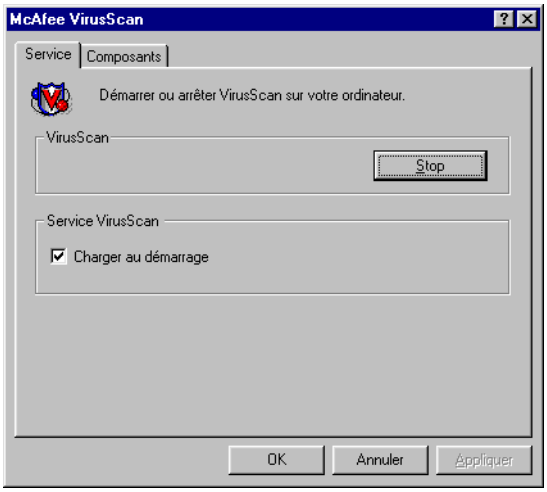

Figure 4-43. Panneau de configuration VirusScan – page Service

3. Dans la page Service, cliquez sur **Arrêter**.

   Tous les composants VirusScan actifs s'arrêtent, toutes les fenêtres ou boîtes de dialogue ouvertes, sont fermées, les icônes VirusScan sont supprimées de la barre d'état système Windows et tous les composants sont retirés de la mémoire.

4. Cliquez sur **OK** pour fermer le panneau de configuration.

Désactivation du moteur d'analyse VShield et de ses modules

Vous pouvez utiliser l'une des trois méthodes proposées ci-dessous pour désactiver un ou plusieurs modules VShield, sans supprimer le moteur d'analyse de la mémoire. Une fois que vous avez désactivé un module, vous pouvez le réactiver en suivant la même procédure. Pour en savoir plus sur l'activation des modules, reportez-vous à la section « Activation ou démarrage du moteur d'analyse VShield » à la page 105.

Méthode 1 : Utiliser le menu contextuel de VShield

Procédez comme suit :

1. Dans la barre d'état système Windows, cliquez avec le bouton droit sur l'icône VShield  pour afficher son menu contextuel.

2. Pointez sur **Activer**.

3. Choisissez l'un des noms de module cochés pour le désactiver. Les noms de module cochés sont déjà actifs. Les autres sont inactifs. Cette méthode désactive un module uniquement pour la durée d'une session d'analyse, ou jusqu'à ce que vous le réactiviez. Le module sera réactivé lors du redémarrage de votre ordinateur.

   L'icône VShield affichera un état différent en fonction de la combinaison de modules que vous activez. Pour en savoir plus sur la signification des différents états d'une icône, reportez-vous à la section « Description de chaque état d'une icône de la barre d'état système VShield » à la page 109.

Méthode 2 : Utiliser la boîte de dialogue État de l'Analyse système

Procédez comme suit :

1. Double-cliquez sur l'icône VShield dans la barre d'état système Windows pour ouvrir la boîte de dialogue État de l'Analyse système (Figure 4-44).

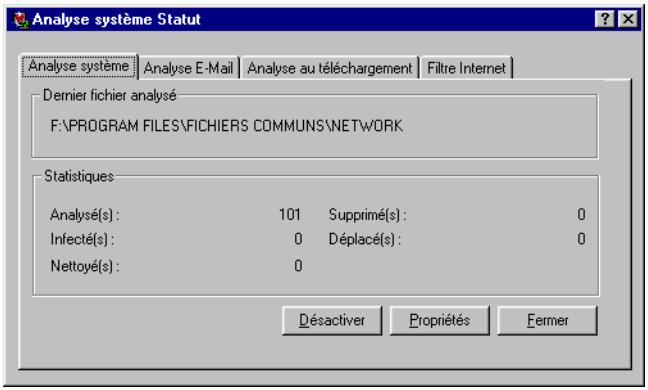

Figure 4-44. Boîte de dialogue État de l'Analyse système de VShield

2. Pour chacun des modules que vous voulez désactiver, cliquez sur l'onglet correspondant, puis cliquez sur **Désactiver**. Dans la page de propriétés de chaque module inactif, ce même bouton portera le nom **Activer**.
3. Cliquez sur **Fermer** pour fermer la boîte de dialogue.

   L'icône VShield affichera un état différent en fonction de la combinaison de modules que vous activez. Pour en savoir plus sur la signification des différents états d'une icône, reportez-vous à la section « Description de chaque état d'une icône de la barre d'état système VShield » à la page 109.

Méthode 3 : Utiliser la boîte de dialogue Propriétés de VShield.

Procédez comme suit :

1. Dans la barre d'état système Windows, cliquez avec le bouton droit sur l'icône VShield pour afficher son menu contextuel.
2. Pointez sur **Propriétés**, puis choisissez un nom de module pour ouvrir la boîte de dialogue Propriétés de VShield (Figure 4-45 à la page 192).

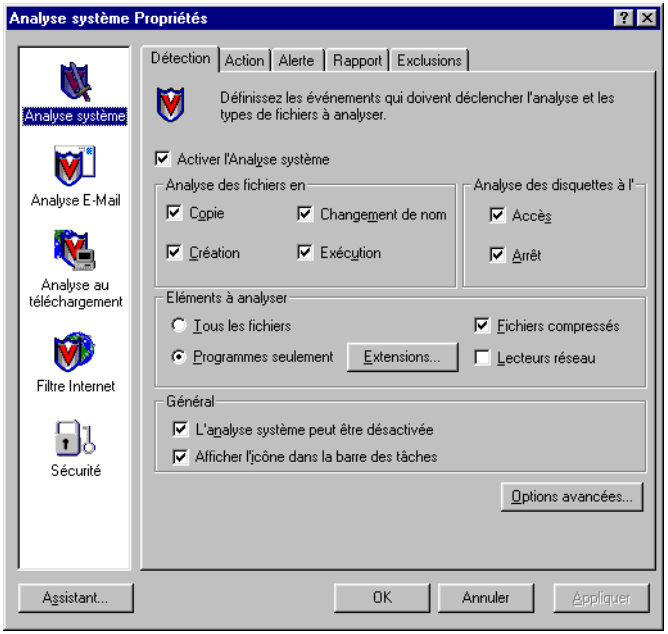

Figure 4-45. Boîte de dialogue Propriétés de VShield

3. Pour chacun des modules que vous voulez désactiver, cliquez sur l'icône correspondante à gauche de la boîte de dialogue, puis cliquez sur l'onglet Détection.

4. Décochez ensuite la case **Activer** en haut de la page de chaque module.

   Lorsque vous décochez cette case, le moteur d'analyse désactive le module correspondant et les options de configuration de cette page deviennent inaccessibles. L'icône VShield affichera un état différent en fonction des modules que vous désactivez.

   Si vous désactivez tous les modules, VShield s'affichera dans la barre d'état système Windows, sauf si vous avez décoché la case **Afficher l'icône dans la barre des tâches** dans la page de propriétés Détection de l'Analyse système. Dans ce cas, VShield n'affichera pas d'icône dans la barre d'état système.

   L'utilisation de cette méthode pour désactiver le module provoque l'application de l'état désactivé comme état « par défaut » du module. Si vous utilisez ensuite le menu contextuel pour activer le module, ce dernier restera actif tant que vous ne redémarrerez pas votre logiciel VirusScan ou votre ordinateur.

Recherche des informations d'état du logiciel VShield

Une fois activé et configuré, VShield opère en permanence en tâche de fond, surveillant et analysant le courrier entrant, les fichiers exécutés ou téléchargés et les objets Java et ActiveX rencontrés.

Pour visualiser un résumé de la progression en temps réel :

1. Double-cliquez sur l'icône VShield  dans la barre d'état système pour ouvrir la boîte de dialogue État.
2. Cliquez sur l'onglet du module dont vous souhaitez vérifier la progression.

   Chaque module fournit les informations suivantes :

   - **Analyse système**. Ce module indique le nombre de fichiers analysés, le nombre de fichiers infectés détectés et le nombre de fichiers désinfectés, déplacés ou supprimés.
   - **Analyse E-Mail**. Ce module indique le nombre de fichiers analysés, le nombre de fichiers infectés détectés et le nombre de fichiers déplacés ou supprimés.
   - **Analyse au téléchargement**. Ce module indique le nombre de fichiers analysés, le nombre de fichiers infectés détectés et le nombre de fichiers déplacés ou supprimés.
   - **Filtre Internet**. Ce module indique le nombre d'objets Java et ActiveX ou de sites Internet analysés et précise combien ont été « interdits », ou combien il vous a empêché d'atteindre.

   Pour afficher une brève description de chacun des éléments présentés dans cette page, cliquez avec le bouton droit sur une image ou un label, puis cliquez sur **Qu'est-ce que c'est ?** dans le menu contextuel qui s'affiche, ou cliquez sur le bouton **?** dans le coin supérieur droit de la boîte de dialogue, puis cliquez sur l'élément dont vous souhaitez obtenir une description.

   Si vous avez activé la fonction de rapport, le moteur d'analyse VShield enregistre également ces données dans le fichier journal de chaque module.

Les autres fonctions disponibles dans cette boîte de dialogue sont :

- **Activer ou désactiver les modules**. Cliquez sur l'onglet correspondant au composant logiciel que vous souhaitez activer ou désactiver, puis cliquez sur **Activer** pour démarrer ce composant. Cliquez sur **Désactiver** pour le désactiver.
- **Ouvrir la boîte de dialogue Propriétés de VShield**. Cliquez sur l'onglet correspondant au composant logiciel que vous souhaitez configurer, puis cliquez sur **Propriétés** pour ouvrir la boîte de dialogue Propriétés de VShield pour ce module.

Afficher des informations sur les tâches exécutées par VShield

Vous pouvez également afficher des informations statistiques sur chacun des modules de VShield dans la boîte de dialogue Propriétés des tâches.

Pour afficher ces informations, procédez comme suit :

1. Double-cliquez sur l'icône Console VirusScan dans la barre d'état système Windows pour amener la fenêtre de la console au premier plan (voir Figure 4-42 à la page 188).
2. Double-cliquez dans la liste des tâches sur la tâche VShield de McAfee pour afficher la boîte de dialogue Propriétés des tâches, illustrée dans la Figure 4-46.

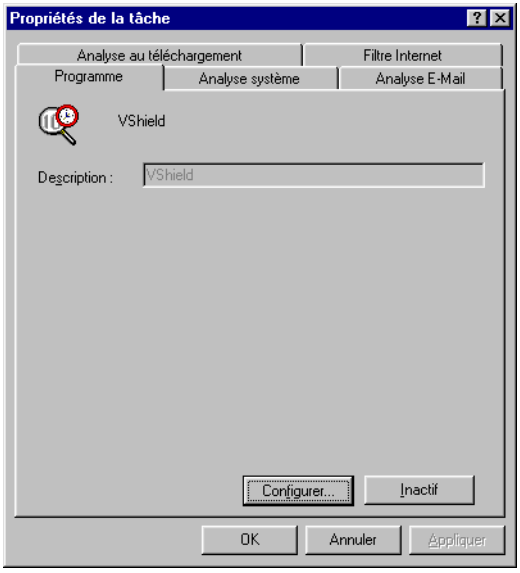

Figure 4-46. Boîte de dialogue Propriétés des tâches VShield

3. Cliquez sur l'onglet correspondant au composant logiciel que vous voulez activer ou désactiver, ou dont vous souhaitez voir la progression.

   La page État affiche la liste des résultats de la dernière opération d'analyse exécutée par la tâche ainsi que le nom du dernier fichier analysé. Pour afficher une brève description de chacun des éléments présentés dans cette page, cliquez avec le bouton droit sur une image ou un label, puis cliquez sur **Qu'est-ce que c'est ?** dans le menu contextuel qui s'affiche, ou cliquez sur le bouton **?** dans le coin supérieur droit de la boîte de dialogue, puis cliquez sur l'élément dont vous souhaitez obtenir une description. Ces affichages *ne seront pas* mis à jour en temps réel.

   Si vous avez activé la fonction de rapport, le moteur d'analyse VShield enregistre également ces données dans le fichier journal de chaque module.

Utilisation de l'application VirusScan 5

Qu'est-ce que l'application VirusScan ?

Les produits antivirus de bureau McAfee utilisent deux méthodes générales pour protéger votre système. La première, l'analyse en arrière-plan, fonctionne en permanence à la recherche de virus dans votre ordinateur, pendant l'exécution de vos tâches quotidiennes. Dans le produit VirusScan, c'est le moteur d'analyse VShield qui assure cette fonction. Pour en savoir plus sur le moteur d'analyse VShield, reportez-vous au Chapitre 4, « Utilisation du moteur d'analyse VShield ».

La seconde méthode requiert votre intervention. C'est vous qui décidez quand le logiciel doit exécuter une opération d'analyse et sur quelle cible doit être effectuée cette recherche, puis vous personnalisez et exécutez ces opérations en fonction de vos besoins. Vous pouvez exécuter des analyses successives ou simultanées, créer des paramètres différents, spécifier plusieurs cibles d'analyse pour chaque opération et enregistrer vos paramètres dans des fichiers d'exportation pour une utilisation ultérieure.

D'autres matériels appellent cette deuxième méthode « analyse à la demande ». L'expression « à la demande » signifie que c'est vous, en tant qu'utilisateur, qui décidez quand VirusScan doit commencer et finir une opération d'analyse, sur quelle cible doit porter cette opération, quelles sont les opérations à entreprendre en cas de détection de virus et comment gérer tous les autres aspects de l'opération d'analyse. Les autres composants de VirusScan, quant à eux, fonctionnent automatiquement ou selon un calendrier que vous avez défini.

L'appellation VirusScan recouvre à la fois l'ensemble des programmes de protection antivirus pour ordinateur personnel décrits dans le présent *Guide d'utilisateur*, ainsi qu'un composant en particulier de cet ensemble : SCAN32.EXE, ou l'application VirusScan. L'application VirusScan fonctionne selon deux modes :

- **L'interface VirusScan « Classique »**. Ce mode vous permet d'être opérationnel rapidement, avec un minimum d'options de configuration mais avec toute la puissance du moteur d'analyse antivirus de VirusScan.
- **L'interface VirusScan Avancée**. Ce mode offre davantage de souplesse pour les options de configuration du programme, ainsi que la possibilité d'exécuter simultanément plusieurs opérations d'analyse.

Le présent chapitre traite de l'utilisation du logiciel VirusScan en mode Classique et en mode Avancé.

Pourquoi utiliser l'application VirusScan ?

Si vous souhaitez conserver un environnement informatique sûr, il faut rechercher les virus éventuels régulièrement. Une analyse « régulière » peut tout aussi bien signifier une fois par mois comme plusieurs fois par jour. Tout dépend de la fréquence des échanges de disquettes entre utilisateurs, du partage de fichiers sur votre réseau local ou de l'interaction avec d'autres ordinateurs via Internet. Prenez aussi l'habitude de faire une analyse avant de sauvegarder des données, avant d'installer un nouveau logiciel ou une mise à niveau, en particulier pour les logiciels téléchargés depuis d'autres ordinateurs, et avant d'allumer ou d'éteindre votre ordinateur chaque jour.

Utilisez le moteur d'analyse VShield pour examiner la mémoire de votre ordinateur et conservez un niveau de vigilance permanent entre chaque analyse. Dans la majorité des cas, cela devrait protéger l'intégrité de votre système. Cependant, une protection antivirus efficace repose sur une analyse complète et régulière du système, et ce pour plusieurs raisons :

- **L'analyse en arrière-plan porte sur les fichiers au moment de leur exécution**. Le moteur d'analyse VShield recherche le code viral lors du lancement d'un fichier exécutable ou de la lecture d'une disquette, alors que l'application VirusScan est capable de contrôler les signatures de code dans les fichiers stockés sur votre disque dur. Si vous exécutez rarement un fichier infecté, il se peut que le moteur d'analyse VShield ne détecte pas le virus avant qu'il ait déjà répandu ses dégâts. L'application VirusScan, en revanche, peut détecter un virus qui attend encore l'opportunité de s'exécuter.

- **Les virus sont vicieux**. Il suffit que vous laissiez par inadvertance une disquette dans le lecteur lors du démarrage de votre ordinateur pour qu'un virus puisse se charger en mémoire avant même le chargement du moteur d'analyse VShield, en particulier si le moteur d'analyse n'est pas configuré pour analyser les disquettes. Une fois en mémoire, un virus peut infecter pratiquement tout programme, y compris le moteur d'analyse VShield.

- **L'exécution du moteur d'analyse VShield demande du temps et des ressources**. La recherche de virus lors de l'exécution, la copie ou l'enregistrement des fichiers est susceptible de retarder très légèrement les heures de lancement d'un logiciel ou d'autres tâches. En fonction de vos besoins, vous pourriez consacrer ce moment à des opérations d'analyse importantes. Même si cet impact est minime, vous pourriez être tenté de désactiver le moteur d'analyse VShield afin que les tâches les plus lourdes puissent exploiter toute la puissance disponible. Dans ce cas, le fait d'effectuer des opérations d'analyse régulières pendant les périodes d'inactivité du système peut protéger celui-ci contre une éventuelle infection sans nuire à ses performances.

- **En matière de sécurité, deux précautions valent mieux qu'une**. Dans l'univers de réseaux largement ouvert sur le Web qui est celui de la plupart des utilisateurs d'ordinateur aujourd'hui, il suffit d'un instant pour télécharger un virus d'une source que l'on n'est même pas conscient d'avoir consultée. Si, à cet instant, un conflit logiciel a désactivé, l'analyse en arrière-plan ou si vous n'avez pas configuré cette analyse pour surveiller un point d'entrée vulnérable, vous pourriez bien être atteint par un virus. Des opérations d'analyse régulières peuvent souvent détecter une infection avant qu'elle n'ait eu le temps de s'étendre ou de commettre des dégâts.

Si vous vous connectez à Internet ou téléchargez des fichiers fréquemment, vous pouvez planifier des opérations d'analyse régulières afin de balayer votre système à des intervalles prédéfinis. Ainsi, vous n'aurez même pas à vous soucier de lancer l'application VirusScan. La console VirusScan fournit un jeu d'option très flexible permettant de planifier vos analyses. Pour en savoir plus sur la planification des tâches dans l'application VirusScan, reportez-vous à la section « Création de nouvelles tâches » à la page 243.

Démarrage de l'application VirusScan

Vous pouvez démarrer l'application VirusScan dans sa propre fenêtre ou en tant que partie intégrante d'une tâche d'analyse programmée. La méthode que vous choisissez dépend du type d'analyse que vous souhaitez exécuter. La première fois que vous démarrez VirusScan, la fenêtre de l'application s'ouvre pour vous permettre de modifier sa configuration. Vous devez cliquer sur **Analyser maintenant** ou sur **Exécuter** dans une autre étape pour démarrer une opération d'analyse réelle.

Il existe quatre méthodes différentes pour démarrer l'application VirusScan ; la quatrième implique l'exécution de l'application à partir de la ligne de commande. Le *Guide de l'administrateur* VirusScan liste les options de ligne de commande pour cette méthode.

Les sections suivantes présentent une description de chaque méthode.

Méthode 1 : Affichage de la fenêtre principal de l'application VirusScan

Procédez comme suit :

1. Cliquez sur **Démarrer** dans la barre des tâches Windows, pointez sur **Programmes**, puis sur Network Associates. Choisissez ensuite **McAfee VirusScan**.

   La fenêtre principale de VirusScan classique s'affiche (Figure 5-1 on page 200).

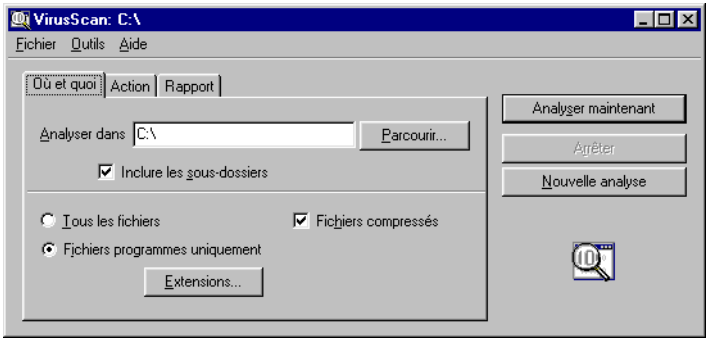

Figure 5-1. fenêtre VirusScan Classique

À partir d'ici, vous pouvez :

- **Lancer immédiatement l'analyse** Cliquez sur **Analyser maintenant** pour que l'application analyse votre système en utilisant les dernières options de configuration que vous avez définies, ou en intégrant les options par défaut.

- **Basculer entre les interfaces Classique et Avancée**. Utilisez l'interface Classique pour exécuter des analyses simples et rapides avec des paramètres par défaut ou restreints. Pour passer de VirusScan Classique à VirusScan Avancé, choisissez **Options avancées** dans le menu **Outils**. Utilisez l'interface Avancée pour contrôler presque tous les aspects de votre opération d'analyse. Pour revenir à l'interface Classique, choisissez **Classique** dans le menu **Outils**.

- **Configurer de nouvelles options d'analyse**. Spécifiez les fichiers à analyser, puis choisissez vos options de réponse, de rapport, d'alerte et d'exclusion dans chaque page de propriétés à onglets. Pour en savoir plus sur les options avancées, reportez-vous à la section « Configuration de l'interface VirusScan Avancé » à la page 213.

  Cliquez ensuite sur le bouton **Nouvelle analyse**, à droite de la fenêtre, ou choisissez **Enregistrer comme valeur par défaut** dans le menu **Fichier** pour enregistrer vos choix comme options par défaut. Les nouveaux paramètres seront utilisés par la suite pour toutes les opérations d'analyse que vous exécuterez. Vous pouvez modifier vos options aussi souvent que vous le souhaitez et les enregistrer ensuite suivant la même procédure pour remplacer les anciennes options.

Choisissez **Enregistrer les paramètres** dans le menu **Fichier** pour enregistrer vos options dans un fichier de paramètres. Vous pouvez utiliser ce fichier pour les futures opérations d'analyse ou l'envoyer à d'autres ordinateurs afin de contrôler leurs opérations d'analyse.

- **Afficher le journal d'activité de l'application VirusScan**. Choisissez **Afficher le journal d'activité** dans le menu **Fichier** pour ouvrir le fichier VSCLOG.TXT dans une fenêtre du Bloc-notes.

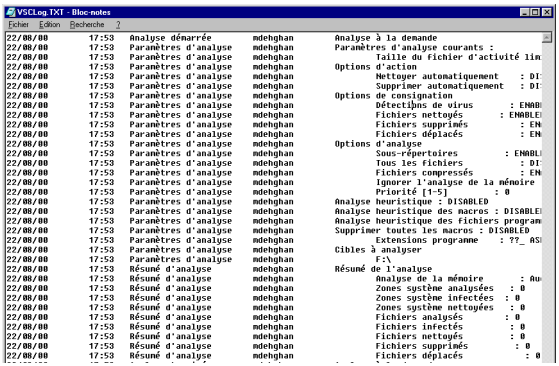

Figure 5-2. Journal d'activité de VirusScan

- **Protéger vos paramètres avec un mot de passe**. Choisissez **Protéger par mot de passe** dans le menu **Outils** pour ouvrir une boîte de dialogue vous permettant de verrouiller n'importe quelle page de propriétés de l'application VirusScan.

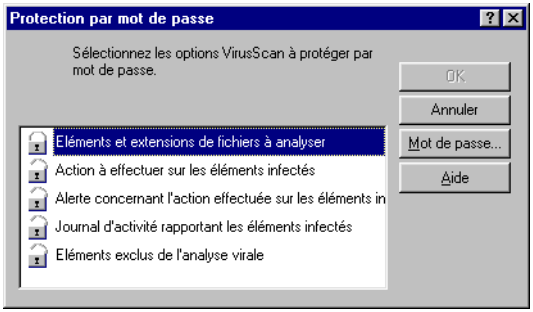

Figure 5-3. Boîte de dialogue Protection par mot de passe

Sélectionnez les pages de propriétés que vous souhaitez protéger, puis cliquez sur le bouton à droite, **Mot de passe**, pour attribuer un mot de passe.

- **Ouvrir le fichier d'aide en ligne.** Pour afficher la liste des rubriques d'aide de VirusScan, choisissez **Rubriques d'aide** dans le menu **Aide**. Pour afficher une description contextuelle des boutons, des listes et des autres éléments de la fenêtre VirusScan, choisissez **Qu'est-ce que c'est ?** dans le menu **Aide**, puis cliquez sur l'élément de votre choix avec le bouton gauche de la souris lorsque votre curseur prend la forme d'un ?. Vous pouvez accéder à ces mêmes rubriques d'aide en cliquant avec le bouton droit de la souris sur un élément de la fenêtre de VirusScan, puis en choisissant **Qu'est-ce que c'est ?** dans le menu qui s'affiche.

2. Pour quitter l'application, choisissez **Quitter** dans le menu **Fichier**.

Méthode 2 : Exécution d'une opération d'analyse à partir de la console VirusScan

Procédez comme suit :

1. Double-cliquez sur l'icône Console VirusScan dans la barre d'état système Windows pour amener la fenêtre de la console au premier plan.

   Si l'icône n'apparaît pas dans la barre d'état système, cliquez sur **Démarrer** dans la barre des tâches Windows, pointez sur **Programmes**, puis sur **Network Associates**. Choisissez ensuite **Console VirusScan**.

   La Console inclut deux tâches prédéfinies utilisant l'application VirusScan pour exécuter les opérations Analyser le poste de travail et Analyser le lecteur 'C'. Pour en savoir plus sur la configuration et l'exécution des tâches d'analyse, reportez-vous à la section « Création de nouvelles tâches » à la page 243.

   Vous pouvez :

   - **Démarrer l'une des tâches prédéfinies dans sa configuration par défaut**. Sélectionnez une tâche dans la liste, puis cliquez sur dans la barre d'outils de la Console. Si la tâche d'analyse est configurée pour démarrer automatiquement, la fenêtre de l'application VirusScan s'ouvre et la tâche est exécutée immédiatement. Sinon, la fenêtre s'ouvre, mais vous devez cliquer sur **Analyser maintenant** pour démarrer l'opération.

- **Créer et planifier les tâches par vous-même**. Cliquez sur dans la barre d'outils de la Console pour ouvrir la boîte de dialogue Propriétés des tâches. Nommez la tâche, choisissez ses options de sécurité, spécifiez la façon dont elle doit apparaître lors de son exécution et ce qu'elle doit faire une fois terminée. Pour définir les options de configuration pour la tâche, cliquez sur le bouton **Configurer**, en bas de la page de propriétés. Pour en savoir plus sur la configuration d'une tâche d'analyse, reportez-vous à la section « Configuration des options de l'application VirusScan » à la page 252.

2. Cliquez sur l'onglet Planification pour indiquer à quel moment la tâche doit être exécutée. Cochez la case **Activer la tâche** pour activer la tâche en vue de son exécution à l'heure prévue. Pour en savoir plus sur la planification d'une tâche, reportez-vous à la section « Activation des tâches » à la page 247.

Méthode 3 : Exécution d'une opération d'analyse à partir d'un fichier de paramètres

Vous pouvez utiliser n'importe quel fichier de paramètres, que vous avez enregistré avec vos propres options de configuration, pour démarrer l'application VirusScan.

Procédez comme suit :

1. Localisez et double-cliquez sur un fichier de paramètres que vous avez enregistré à partir de la fenêtre de l'application VirusScan.

   La fenêtre de l'application VirusScan s'ouvre à nouveau et charge les options de configuration que vous avez enregistrées (Figure 5-4).

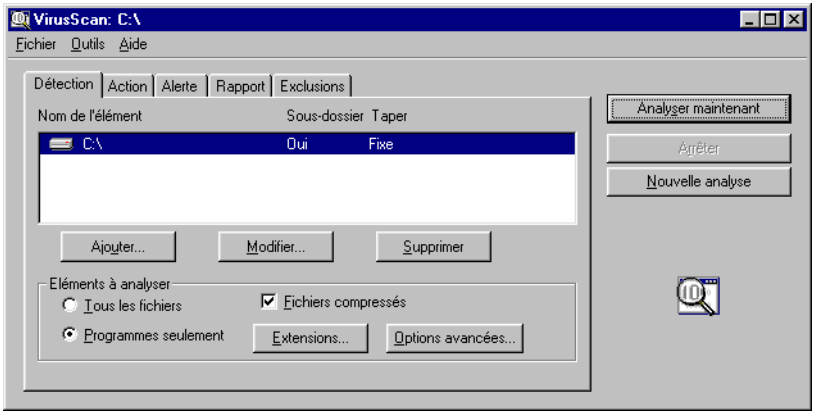

Figure 5-4. fenêtre VirusScan Avancé

Vous pouvez également ouvrir cette fenêtre et charger vos paramètres en cliquant avec le bouton droit sur le fichier de paramètres et en choisissant **Démarrer** dans le menu contextuel qui s'affiche.

D'ordinaire, vous trouverez vos fichiers de paramètres dans le répertoire du programme VirusScan, mais vous pouvez les enregistrer n'importe où sur votre disque dur. Les fichiers de paramètres VirusScan portent l'extension .VSC.

2. Cliquez sur **Analyser maintenant** pour démarrer une opération d'analyse avec les paramètres spécifiés.

Vous pouvez aussi modifier rapidement ces paramètres avant de lancer l'analyse. Pour ce faire, procédez de l'une des façons suivantes :

- Suivez les étapes Étape 1 et Étape 2, décrites ci-dessus, pour ouvrir la fenêtre de l'application VirusScan, puis modifiez vos options de configuration dans chaque page de propriétés ; ou
- Cliquez avec le bouton droit sur le fichier de paramètres .VSC, puis choisissez **Propriétés** dans le menu contextuel qui s'affiche.

  La boîte de dialogue Propriétés s'affiche avec des onglets configuration similaires aux onglets disponibles lors de la configuration de l'application VirusScan à partir de la console VirusScan (Figure 5-5).

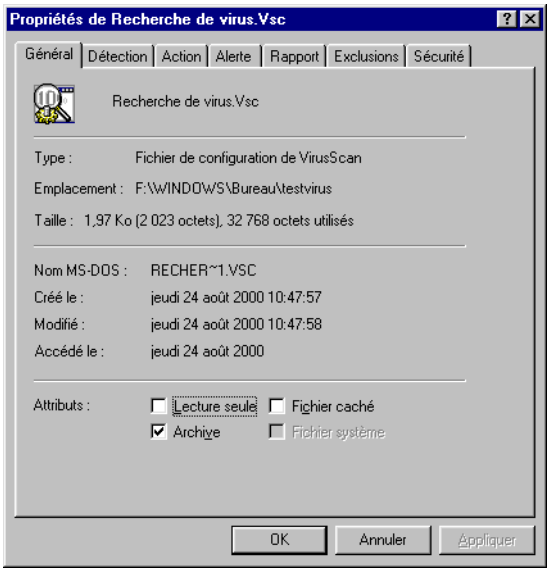

Figure 5-5. Exemple de boîte de dialogue Propriétés de .VSC

Pour en savoir plus sur la configuration des options de cette page de propriétés, reportez-vous à la section « Configuration des options de l'application VirusScan » à la page 252.

Méthode 4 : Démarrage de l'application à partir de la ligne de commande

Procédez comme suit :

1. Cliquez sur **Démarrer** dans la barre des tâches Windows, pointez sur **Programmes**, puis choisissez **Invite MS-DOS** si votre ordinateur utilise Windows 95 ou Windows 98. Si votre ordinateur fonctionne avec Windows NT Workstation v4.0 ou Windows 2000 Professionnel, choisissez plutôt **Invite de commande**.

   Windows affiche une fenêtre d'invite de commande Si vous avez installé le logiciel VirusScan dans le répertoire par défaut, placez-vous à l'emplacement suivant :

   C:\Program Files\Common Files\Network Associates\Moteur d'analyse à la demande\Scan32

2. Tapez la ligne suivante à l'invite de commande :

   ```
   scan32.exe <cible à analyser> /<options de configuration>
   ```

   Ici, la `<cible à analyser>` désigne le lecteur, le chemin d'accès de répertoire ou le nom de fichier que l'application doit examiner. Spécifiez les lecteurs avec des noms au format DOS—C: ou D:, par exemple—et indiquez les chemins d'accès complets aux répertoires selon les conventions applicables à votre système d'exploitation.

   Vous pouvez utiliser des noms longs sur les systèmes Windows NT Workstation v4.0 et Windows 2000 Professionnel, mais les noms tronqués sont obligatoires sur les systèmes Windows 95 et Windows 98.

3. Indiquez ensuite la cible à analyser avec le jeu d'options de configuration, le cas échéant, que cette opération d'analyse doit utiliser lors de son exécution. Pour une obtenir une liste complète des options de configuration disponibles, consultez le *Guide de l'administrateur* VirusScan.

   Faites précéder chaque option d'une `/`. Même si l'application vous autorise à spécifier certaines options sans la `/`, le fait d'omettre ce paramètre pour les autres options provoquera une erreur. Vous pouvez spécifier tous les paramètres requis pour vos options sans une méthode de notation particulière.

En fonction des options de ligne de commande que vous choisissez, le fait de démarrer l'application de cette façon peut déclencher l'exécution d'une opération d'analyse ou l'affichage de la fenêtre de l'application VirusScan, où vous pouvez choisir des options de configuration pour l'analyse.

Configuration de l'interface VirusScan Classique

Pour que l'application VirusScan puisse protéger votre système, vous devez lui fournir les informations suivantes :

- ce qu'elle doit analyser
- ce qu'elle doit faire en cas de détection d'un virus
- comment elle doit vous informer en cas de détection d'un virus
- si vous souhaitez conserver une trace de ses actions

Une série de pages de propriétés, située dans la fenêtre VirusScan, contrôle les opérations relatives à chaque tâche ; pour configurer l'application en fonction de votre tâche, cliquez sur les onglets correspondants. Pour obtenir d'autres options de configuration, passez à l'interface VirusScan Avancé. Choisissez **Options avancées** dans le menu **Outils** de la fenêtre VirusScan Classique.

Vous pouvez à tout moment lancer une opération d'analyse avec les options que vous avez choisies, il vous suffit de cliquer sur **Analyser maintenant**. Pour enregistrer vos modifications comme options d'analyse par défaut, choisissez **Enregistrer comme valeur par défaut** dans le menu **Fichier** ou cliquez sur **Nouvelle analyse**. Pour enregistrer vos paramètres dans un nouveau fichier, choisissez **Enregistrer les paramètres** dans le menu **Fichier**, donnez un nom à votre fichier dans la boîte de dialogue qui s'affiche, puis cliquez sur **Enregistrer**.

Le fichier de paramètres que vous enregistrez portera l'extension .VSC. Pour en savoir plus sur l'utilisation de ce fichier pour démarrer une opération d'analyse VirusScan, reportez-vous à la section « Méthode 3 : Exécution d'une opération d'analyse à partir d'un fichier de paramètres » à la page 203.

Sélection des options Où et Quoi

Le logiciel VirusScan suppose au départ que vous souhaitez analyser votre lecteur C: et tous ses sous-dossiers et restreindre les fichiers à analyser à ceux susceptibles d'être infectés par un virus (Figure 5-6).

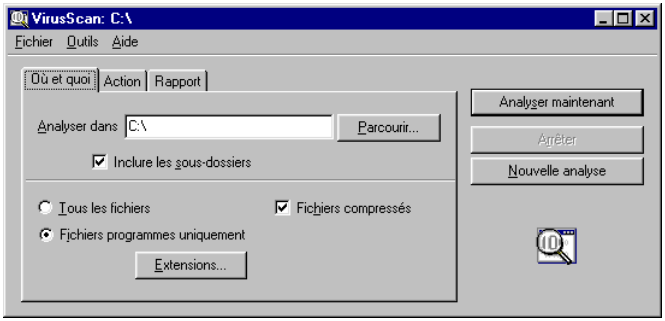

Figure 5-6. Fenêtre VirusScan Classique – page Où et Quoi

Pour modifier ces options, procédez comme suit :

1. Choisissez le volume ou le dossier de votre système ou de votre réseau que VirusScan doit analyser à la recherche de virus.

   Tapez le chemin du volume ou du dossier cible dans la zone de texte prévue à cet effet ou cliquez sur **Parcourir** pour ouvrir la boîte de dialogue Recherche de dossier (Figure 5-7).

Figure 5-7. Boîte de dialogue Recherche de dossier

Pour développer une liste de la boîte de dialogue, cliquez sur ⊞. Cliquez sur ⊟ pour réduire cette liste. Vous pouvez sélectionner comme cible à analyser des disques durs, des dossiers ou des fichiers qui se trouvent sur votre système ou sur d'autres ordinateurs de votre réseau. Vous ne pouvez pas sélectionner le Poste de travail, le Voisinage réseau ni plusieurs volumes comme cible à analyser à partir de VirusScan Classique ; pour ce faire, vous devez passer à VirusScan Avancé.

Une fois que vous avez sélectionné votre cible à analyser, cliquez sur **OK** pour revenir à la fenêtre VirusScan Classique.

2. Cochez la case **Inclure les sous-dossiers** si vous souhaitez que l'application recherche les virus dans les dossiers contenus dans votre cible à analyser.

   REMARQUE : Si vous sélectionnez **Inclure les sous-dossiers**, l'application analyse uniquement les fichiers stockés dans les sous-dossiers eux-mêmes. Elle n'analyse pas les fichiers stockés à la racine du dossier que vous spécifiez. Pour analyser ces fichiers, décochez la case **Inclure les sous-dossiers**.

3. Spécifiez les types de fichiers que le logiciel VirusScan doit examiner. Vous pouvez :

   - **Analyser les fichiers compressés.** Cochez la **case Fichiers compressés** pour que le logiciel VirusScan recherche les virus éventuels dans les fichiers compressés ou dans les fichiers d'archives. Bien qu'il offre une protection supplémentaire, l'examen des fichiers compressés peut ralentir l'opération d'analyse.

     Pour afficher la liste des types de fichiers et d'archives que l'application analyse, reportez-vous à la section « Liste en cours des fichiers compressés analysés » à la page 352.

   - **Analyser tous les fichiers**. Cochez la case **Tous les fichiers** pour que l'application analyse tous les fichiers contenus dans la cible que vous avez spécifiée, quelle qu'en soit l'extension.

     REMARQUE : McAfee recommande de sélectionner cette option pour votre première opération d'analyse, ou à intervalles réguliers par la suite, de manière à garantir que votre système est exempt de tout virus. Vous pouvez ensuite limiter la portée des opérations d'analyse ultérieures.

   - **Choisir les types de fichiers**. D'ordinaire, les virus ne peuvent infecter les fichiers qui ne contiennent pas de code exécutable, que ce soit du code de script, de macro ou binaire. Vous pouvez par conséquent limiter en toute sécurité la portée de vos opérations d'analyse aux fichiers les plus susceptibles d'être infectés par des virus. Pour ce faire, cliquez sur le bouton **Fichiers programme uniquement**.

Pour afficher ou spécifier les extensions de nom de fichier que l'application doit examiner, cliquez sur **Extensions**. La boîte de dialogue Extensions de fichiers programme s'affiche. Pour en savoir plus sur la modification des fichiers répertoriés à cet endroit, reportez-vous à la section « Ajout d'extensions de fichier pour analyse » à la page 345.

4. Cliquez sur l'onglet Action pour choisir d'autres options de VirusScan.

   Pour démarrer immédiatement une opération d'analyse selon les options que vous avez choisies, cliquez sur **Analyser maintenant**. Pour enregistrer vos modifications comme options d'analyse par défaut, choisissez **Enregistrer comme valeur par défaut** dans le menu **Fichier** ou cliquez sur **Nouvelle analyse**.

   Pour enregistrer vos paramètres dans un nouveau fichier, choisissez **Enregistrer les paramètres** dans le menu **Fichier**, donnez un nom à votre fichier dans la boîte de dialogue qui s'affiche, puis cliquez sur **Enregistrer**.

Sélection des options d'action

Lorsque le logiciel VirusScan détecte un virus, il réagit soit en vous demandant ce qu'il doit faire du fichier infecté, soit en lançant automatiquement une action que vous avez déterminée au préalable. Utilisez la page de propriétés Action pour spécifier les actions que le logiciel VirusScan doit vous proposer en cas de détection d'un virus et celles qu'il doit mettre en œuvre automatiquement.

Procédez comme suit :

1. Cliquez sur l'onglet Action dans la fenêtre VirusScan Classique pour afficher la page de propriétés correspondante (Figure 5-8).

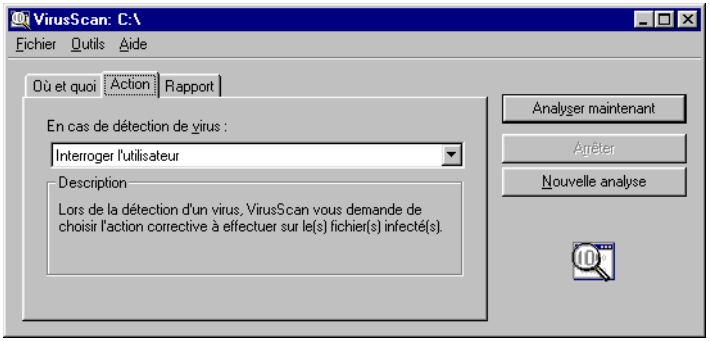

Figure 5-8. Fenêtre VirusScan Classique – page Action

2. Sélectionnez une réponse dans la liste **En cas de détection d'un virus**. La zone située juste au-dessous de la liste se modifiera pour vous proposer d'autres options pour chacun de vos choix. Vous avez le choix entre les options suivantes :

   - **Interroger l'utilisateur.** Utilisez cette option si vous pensez être auprès de votre ordinateur pendant que l'application VirusScan analyse votre disque ; l'application affiche un message d'alerte lorsqu'il détecte un virus et vous propose la liste complète des réponses disponibles.
   - **Déplacer automatiquement les fichiers infectés.** Sélectionnez cette option de réponse pour que l'application déplace les fichiers infectés vers un dossier de quarantaine dès leur détection.

     Par défaut, l'application place ces fichiers dans un dossier nommé Infecté, situé dans le répertoire du programme VirusScan. Vous pouvez entrer un autre nom de dossier dans la zone de texte affichée ou cliquer sur **Parcourir** pour retrouver le dossier voulu sur votre disque dur.
   - **Nettoyer automatiquement les fichiers infectés.** Sélectionnez cette option de réponse pour que l'application VirusScan supprime le code de virus dans le fichier infecté dès sa détection. Si l'application ne parvient pas à supprimer le virus, elle notera l'incident dans le fichier journal. Pour plus de détails, reportez-vous à la section « Sélection des options de rapport » à la page 223.
   - **Supprimer automatiquement les fichiers infectés.** Utilisez cette option pour demander à l'application VirusScan de supprimer tout fichier infecté dès sa détection. Assurez-vous d'avoir activé la fonction de rapport, afin de disposer d'une liste des fichiers supprimés par l'application. Consultez ensuite cette dernière pour connaître les fichiers supprimés à restaurer à partir des copies de sauvegarde. Si l'application ne parvient pas à supprimer un fichier infecté, elle notera l'incident dans son fichier journal.
   - **Poursuivre l'analyse.** N'utilisez cette option que si vous prévoyez d'être absent au moment où l'application VirusScan recherchera les virus. Si vous activez également la fonction de rapport de VirusScan (voir « Sélection des options de rapport » à la page 223), le programme enregistrera le nom des virus détectés et le nom des fichiers infectés, pour vous permettre de les supprimer à une prochaine occasion.

3. Cliquez sur l'onglet Rapport pour choisir d'autres options de VirusScan.

Pour démarrer immédiatement une opération d'analyse selon les options que vous avez choisies, cliquez sur **Analyser maintenant**. Pour enregistrer vos modifications comme options d'analyse par défaut, choisissez **Enregistrer comme valeur par défaut** dans le menu **Fichier** ou cliquez sur **Nouvelle analyse**. Pour enregistrer vos paramètres dans un nouveau fichier, choisissez **Enregistrer les paramètres** dans le menu **Fichier**, donnez un nom à votre fichier dans la boîte de dialogue qui s'affiche, puis cliquez sur **Enregistrer**.

Sélection des options de rapport

Par défaut, l'application VirusScan émet un signal sonore pour vous avertir lorsqu'il détecte un virus. Vous pouvez utiliser la page Rapport pour activer ou désactiver cette alerte ou pour ajouter un message dans la boîte de dialogue Virus détecté, qui s'affiche lorsque l'application détecte un fichier infecté. Ce message d'alerte peut contenir des informations quelconques, d'un simple avertissement à des instructions sur la façon de signaler l'incident à l'administrateur réseau.

Cette page vous permet également de définir la taille et l'emplacement du fichier journal de VirusScan. Par défaut, l'application présente la liste de ses paramètres en cours ainsi qu'un résumé des actions qu'elle a entreprises pendant ses opérations d'analyse dans un fichier journal nommé VSCLOG.TXT. Vous pouvez conserver ce fichier comme fichier journal ou spécifier un autre fichier texte existant qui sera utilisé par l'application. L'application ne crée pas de fichier texte.

Vous pouvez ensuite ouvrir et imprimer le fichier journal pour consultation ultérieure, soit depuis l'application VirusScan, soit depuis un éditeur de texte.

Pour choisir les options d'alerte et de journal de VirusScan, procédez comme suit :

1. Cliquez sur l'onglet Rapport dans la fenêtre VirusScan Classique pour afficher la page de propriétés correspondante (Figure 5-9).

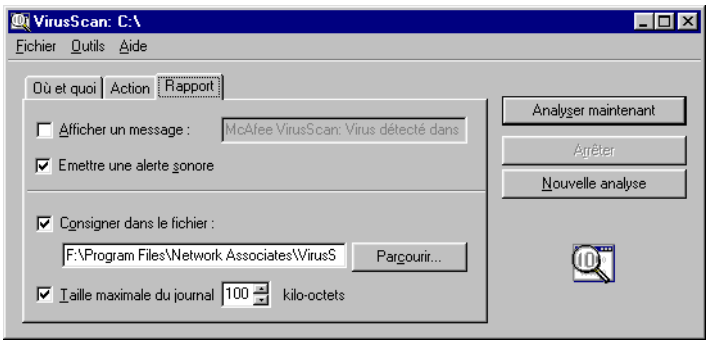

Figure 5-9. Fenêtre VirusScan Classique – page Rapport

2. Choisissez les méthodes d'alerte que l'application VirusScan doit utiliser en cas de détection d'un virus. Vous pouvez lui demander d'effectuer les opérations suivantes :

   - **Afficher un message personnalisé.** Cochez la case **Afficher un message**, puis entrez dans la zone de texte prévue à cet effet le message que vous voulez afficher. La longueur de votre message ne peut excéder 225 caractères.

     ❑ **REMARQUE :** Pour que l'application VirusScan puisse afficher votre message, vous devez d'abord sélectionner **Interroger l'utilisateur** comme option de réponse dans la page Action (pour plus de détails, reportez-vous à la section « Sélection des options d'action » à la page 219).

   - **Émettre un signal sonore.** Cochez la case **Émettre une alerte sonore**.

3. Cochez la case **Consigner dans le fichier**.

   Par défaut, le logiciel VirusScan enregistre les informations de journal dans le fichier VSCLOG.TXT, situé dans le répertoire du programme VirusScan. Pour spécifier un fichier journal autre que VSCLOG.TXT, entrez un chemin d'accès et un nom de fichier dans la zone de texte prévue à cet effet, ou bien cliquez sur **Parcourir** pour localiser un fichier approprié sur votre disque dur ou sur votre réseau.

4. Pour limiter la taille du fichier journal, cochez la case **Taille limite du fichier journal**, puis saisissez cette taille, en Kilo-octets, dans la zone de texte prévue à cet effet.

   Entrez une valeur comprise entre 10 Ko et 999 Ko. Par défaut, le logiciel VirusScan limite la taille du fichier à 100 Ko. Si les données du journal dépassent la taille allouée pour le fichier, le logiciel VirusScan efface le fichier existant et le reprend au point où il s'était interrompu.

5. Cliquez sur un autre onglet pour modifier l'un ou l'autre des paramètres de VirusScan.

   Pour démarrer immédiatement une opération d'analyse selon les options que vous avez choisies, cliquez sur **Analyser maintenant**. Pour enregistrer vos modifications comme options d'analyse par défaut, choisissez **Enregistrer comme valeur par défaut** dans le menu **Fichier** ou cliquez sur **Nouvelle analyse**. Pour enregistrer vos paramètres dans un nouveau fichier, choisissez **Enregistrer les paramètres** dans le menu **Fichier**, donnez un nom à votre fichier dans la boîte de dialogue qui s'affiche, puis cliquez sur **Enregistrer**.

Configuration de l'interface VirusScan Avancé

L'interface VirusScan Avancé vous offre davantage de souplesse que l'interface VirusScan Classique en ce qui concerne les options de configuration, avec entre autres la possibilité d'exécuter simultanément plusieurs opérations d'analyse, d'exclure certains éléments des opérations d'analyse ou encore d'activer la détection heuristique de VirusScan.

Pour que l'application VirusScan puisse protéger votre système, vous devez lui fournir les informations suivantes :

- ce qu'elle doit analyser
- ce qu'elle doit faire en cas de détection d'un virus
- comment elle doit vous informer en cas de détection d'un virus
- si vous souhaitez conserver une trace de ses actions
- les éléments qu'elle doit exclure de la recherche de virus.

Une série de pages de propriétés, située dans la fenêtre VirusScan, contrôle les opérations relatives à chaque tâche ; pour configurer l'application en fonction de votre tâche, cliquez sur les onglets correspondants. Pour faire votre choix à partir d'un jeu d'options de configuration plus simple, passez à l'interface VirusScan Classique. Choisissez **Classique** dans le menu **Outils** de la fenêtre VirusScan Avancé.

Pour protéger vos paramètres contre toute modification non autorisée, choisissez **Protection par mot de passe** dans le menu **Outils** pour ouvrir la boîte de dialogue Protection par mot de passe. Pour en savoir plus sur la configuration des paramètres de cette boîte de dialogue, reportez-vous à la section « Activation de la protection par mot de passe » à la page 229.

Vous pouvez à tout moment lancer une opération d'analyse avec les options que vous avez choisies ; il vous suffit simplement de cliquer sur **Analyser maintenant**. Pour enregistrer vos modifications comme options d'analyse par défaut, choisissez **Enregistrer comme valeur par défaut** dans le menu **Fichier** ou cliquez sur **Nouvelle analyse**. Pour enregistrer vos paramètres dans un nouveau fichier, choisissez **Enregistrer les paramètres** dans le menu **Fichier**, donnez un nom à votre fichier dans la boîte de dialogue qui s'affiche, puis cliquez sur **Enregistrer**.

Sélection des options de détection

Le logiciel VirusScan prend comme hypothèse de départ que vous souhaitez analyser tous les disques durs de votre ordinateur, y compris ceux affectés à partir de lecteurs réseau, et restreindre l'analyse aux seuls fichiers susceptibles d'être infectés par un virus (Figure 5-10 on page 214).

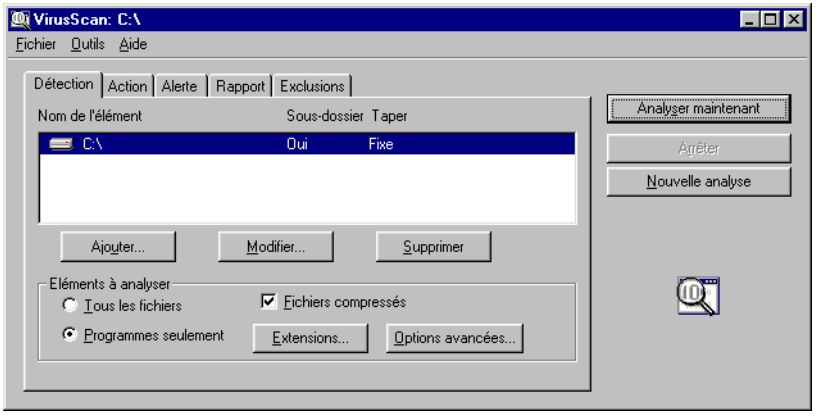

Figure 5-10. Fenêtre VirusScan Avancé – page Détection

Pour modifier ces options ou en ajouter d'autres, procédez comme suit :

1. Choisissez les éléments de votre système ou de votre réseau que le logiciel VirusScan doit analyser. Vous pouvez :

   - **Ajouter des cibles à analyser.** Cliquez sur **Ajouter** pour ouvrir la boîte de dialogue Ajout d'un élément à analyser (Figure 5-11).

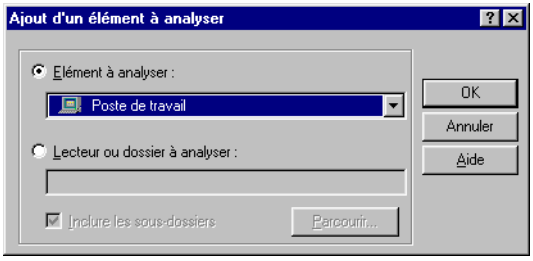

Figure 5-11. Boîte de dialogue Ajout d'un élément à analyser

Pour analyser tout votre ordinateur ou un sous-ensemble d'unités de votre système ou de votre réseau, cliquez sur le bouton **Sélection de l'élément à analyser**, puis

a. choisissez une cible à analyser dans la liste qui vous est proposée. Vous avez le choix entre les options suivantes :

   – **Poste de travail.** Cette option demande à l'application d'analyser tous les lecteurs physiquement connectés à votre ordinateur ou logiquement associés à une lettre de lecteur de votre ordinateur par l'intermédiaire de l'explorateur Windows.

- **Tous les supports amovibles.** Cette option demande à l'application d'analyser uniquement les disquettes, les CD-ROM, les disques ZIP Iomega ou des supports de stockage similaires physiquement connectés à votre ordinateur.
- **Tous les lecteurs fixes.** Cette option demande à l'application d'analyser les disques durs physiquement connectés à votre ordinateur.
- **Tous les lecteurs réseau**. Cette option demande à l'application d'analyser toutes les unités logiquement associées à une lettre de lecteur de votre ordinateur par l'intermédiaire de l'explorateur Windows.

b. Lorsque vous avez choisi votre cible, cliquez sur **OK** pour fermer la boîte de dialogue.

Pour examiner un disque ou un dossier spécifique de votre système, cliquez sur le bouton **Lecteur ou dossier à analyser**, puis

a. entrez, dans la zone de texte prévue à cet effet, la lettre du lecteur ou le chemin d'accès au dossier que vous souhaitez analyser. Vous pouvez également cliquer sur **Parcourir** pour rechercher la cible à analyser sur votre ordinateur.

❑ **REMARQUE :** Vous ne pouvez pas utiliser la notation de la convention d'affectation des noms (UNC) pour spécifier un disque réseau comme cible à analyser pour les tâches planifiées. L'utilisation de ce type de notation génère l'erreur « chemin non valide ». Vous pouvez utiliser la notation de la convention d'affectation des noms (UNC) pour spécifier des cibles d'analyse pour les opérations que vous exécutez directement avec l'application VirusScan.

---

b. Cochez la case **Inclure les sous-dossiers** pour que l'application VirusScan recherche les virus dans tous les dossiers contenus dans votre cible à analyser.

❑ **REMARQUE :** Si vous sélectionnez **Inclure les sous-dossiers**, l'application analyse uniquement les fichiers stockés dans les sous-dossiers eux-mêmes. Elle n'analyse pas les fichiers stockés à la racine du dossier que vous spécifiez. Pour analyser ces fichiers, décochez la case **Inclure les sous-dossiers**.

---

c. Cliquez sur **OK** pour fermer la boîte de dialogue.

- **Modifier une cible à analyser.** Sélectionnez l'une des cibles de la liste, puis cliquez sur **Edition** pour ouvrir la boîte de dialogue Modifier l'élément à analyser (Figure 5-12).

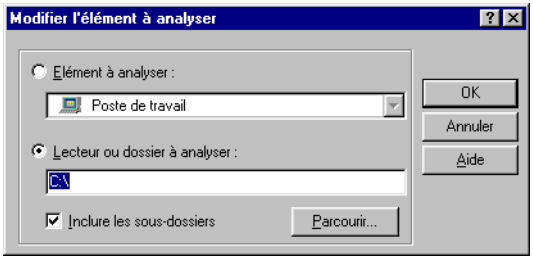

Figure 5-12. Boîte de dialogue Modifier l'élément à analyser

La boîte de dialogue s'affiche avec les cibles d'analyse actuellement spécifiées. Choisissez une cible à analyser ou tapez-en une, puis cliquez sur **OK** pour fermer la boîte de dialogue.

- **Supprimer des cibles à analyser.** Sélectionnez l'une des cibles de la liste, puis cliquez sur **Supprimer** pour l'effacer.

2. Spécifiez les types de fichiers que l'application VirusScan doit examiner. Vous pouvez :

   - **Analyser les fichiers compressés.** Cochez la **case Fichiers compressés** pour que l'application VirusScan recherche les virus éventuels dans les fichiers compressés ou dans les fichiers d'archives. Bien qu'il offre une protection supplémentaire, l'examen des fichiers compressés peut ralentir l'opération d'analyse.

     Pour afficher la liste des types de fichiers et d'archives que l'application analyse, reportez-vous à la section « Liste en cours des fichiers compressés analysés » à la page 352.

   - **Analyser tous les fichiers**. Cochez la case **Tous les fichiers** pour que l'application analyse tous les fichiers contenus dans la cible que vous avez spécifiée, quelle qu'en soit l'extension.

     REMARQUE : McAfee recommande de sélectionner cette option pour votre première opération d'analyse, ou à intervalles réguliers par la suite, de manière à garantir que votre système est exempt de tout virus. Vous pouvez ensuite limiter la portée des opérations d'analyse ultérieures.

- **Choisir les types de fichiers**. D'ordinaire, les virus ne peuvent infecter les fichiers qui ne contiennent pas de code exécutable, que ce soit du code de script, de macro ou binaire. Vous pouvez par conséquent limiter en toute sécurité la portée de vos opérations d'analyse aux fichiers les plus susceptibles d'être infectés par des virus. Pour ce faire, cliquez sur le bouton **Fichiers programme uniquement**.

  Pour afficher ou spécifier les extensions de nom de fichier que l'application doit examiner, cliquez sur **Extensions**. La boîte de dialogue Extensions de fichiers programme s'affiche. Pour en savoir plus sur la modification des fichiers répertoriés à cet endroit, reportez-vous à la section « Ajout d'extensions de fichier pour analyse » à la page 345.

3. Activer l'analyse heuristique. Cliquez sur **Options avancées** pour ouvrir la boîte de dialogue Paramètres d'analyse avancés (Figure 5-13).

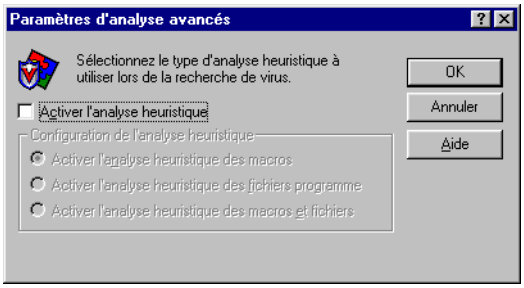

Figure 5-13. Boîte de dialogue Paramètres d'analyse avancés

La technologie d'analyse heuristique permet à l'application VirusScan de reconnaître les nouveaux virus en fonction de leur ressemblance avec des virus similaires déjà identifiés. Pour ce faire, l'application recherche des caractéristiques propres aux virus dans les fichiers que vous lui avez demandé d'analyser. Si elle détecte un nombre suffisant de caractéristiques dans un fichier, l'application identifie le fichier comme étant potentiellement infecté par un nouveau virus ou un virus non identifié.

L'application recherche en même temps des caractéristiques qui dénotent de l'absence de virus, c'est pourquoi elle ne se trompe que rarement en vous signalant une infection. À moins d'être certain que votre fichier ne contient *pas* de virus, vous devez apporter aux infections « probables » les mêmes précautions que vous apportez aux infections confirmées.

Lorsque vous démarrez l'application VirusScan, aucune option d'analyse heuristique n'est activée par défaut. Pour activer l'analyse heuristique, procédez comme suit :

a. Cochez la case **Activer l'analyse heuristique**. Les options proposées dans le reste de la boîte de dialogue deviennent accessibles.

b. Sélectionnez les types d'analyses heuristiques que l'application VirusScan doit utiliser. Vous avez le choix entre les options suivantes :

   – **Activer l'analyse heuristique des macros.** Sélectionnez cette option pour que l'application identifie d'abord tous les fichiers Microsoft Word, Microsoft Excel et autres fichiers Microsoft Office incorporant des macros et compare ensuite le code de la macro avec sa base de données de définitions de virus. Si la correspondance est exacte, l'application identifie le nom du virus ; pour les chaînes de signature qui ressemblent à celles de virus existants, elle vous informe qu'elle a détecté un virus de macro « probable ».

   – **Activer l'analyse heuristique des fichiers programme.** Sélectionnez cette option si vous souhaitez que l'application VirusScan localise de nouveaux virus dans les fichiers programme en examinant les caractéristiques des fichiers et en les comparant avec celles figurant sur une liste de virus connus. Lorsqu'elle détecte un fichier ayant un certain nombre de caractéristiques, l'application l'identifie comme étant potentiellement infecté.

   – **Activer l'analyse heuristique des macros et fichiers programme.** Sélectionnez cette option si vous souhaitez que l'application utilise les deux types d'analyse heuristique. McAfee vous recommande d'utiliser cette option pour une protection antivirus optimale.

   REMARQUE : L'application n'utilise les techniques d'analyse heuristique que sur les types de fichiers que vous désignez dans la boîte de dialogue Extensions de fichiers programme. Si vous décidez d'analyser **Tous les fichiers**, elle appliquera l'analysera heuristique à tous les types de fichiers.

   ---

c. Cliquez sur **OK** pour enregistrer vos paramètres et revenir à la boîte de dialogue Propriétés de VShield.

4. Cliquez sur l'onglet Action pour choisir d'autres options de l'application VirusScan.

   Pour démarrer immédiatement une opération d'analyse selon les options que vous avez choisies, cliquez sur **Analyser maintenant**. Pour enregistrer vos modifications comme options d'analyse par défaut, choisissez **Enregistrer comme valeur par défaut** dans le menu **Fichier** ou cliquez sur **Nouvelle analyse**. Pour enregistrer vos paramètres dans un nouveau fichier, choisissez **Enregistrer les paramètres** dans le menu **Fichier**, donnez un nom à votre fichier dans la boîte de dialogue qui s'affiche, puis cliquez sur **Enregistrer**.

Sélection des options d'action

Lorsque le logiciel VirusScan détecte un virus, il réagit soit en vous demandant ce qu'il doit faire du fichier infecté, soit en lançant automatiquement une action que vous avez déterminée au préalable. Utilisez la page de propriétés Action pour spécifier les actions que le logiciel VirusScan doit vous proposer en cas de détection d'un virus et celles qu'il doit mettre en œuvre automatiquement.

Procédez comme suit :

1. Cliquez sur l'onglet Action dans la fenêtre VirusScan Avancé pour afficher la page de propriétés correspondante (Figure 5-14).

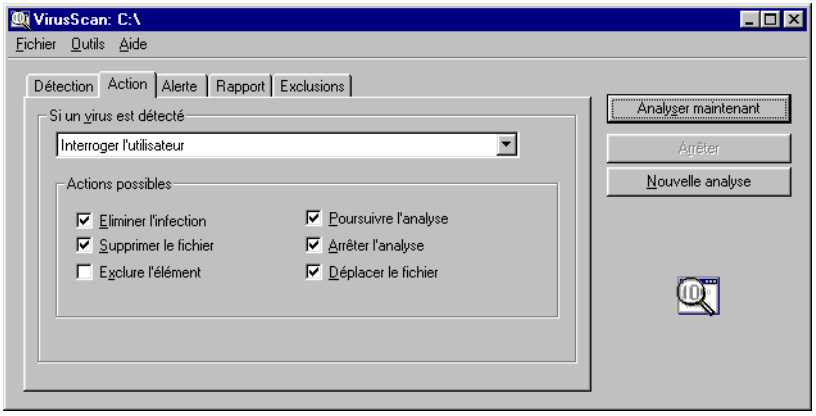

Figure 5-14. VirusScan Avancé – page Action

2. Sélectionnez une réponse dans la liste **En cas de détection d'un virus**. La zone située juste au-dessous de la liste se modifiera pour vous proposer d'autres options pour chacun de vos choix. Vous avez le choix entre les options suivantes :

- **Interroger l'utilisateur.** Utilisez cette option si vous pensez être auprès de votre ordinateur pendant que l'application VirusScan analyse votre disque ; VirusScan affiche un message d'alerte lorsqu'il détecte un virus et vous propose une liste des réponses possibles.

  Pour chaque case que vous cochez dans la page Action, un bouton d'option apparaîtra dans le message d'alerte que l'application affichera en cas de détection d'un virus. Ainsi, si vous cochez par exemple la case **Supprimer le fichier**, le message d'alerte comportera un bouton **Supprimer**.

  Vous avez le choix entre les options suivantes :

  – **Éliminer l'infection**. Cette option demande à l'application d'essayer de supprimer le code de virus dans le fichier infecté. Si vous avez activé la fonction de rapport, l'application enregistrera l'événement dans un journal à chaque fois qu'elle parviendra ou non à nettoyer un fichier infecté.

  – **Supprimer le fichier**. Cette option demande à l'application de supprimer immédiatement le fichier infecté.

  – **Exclure l'élément**. Cette option demande à l'application d'ignorer ce fichier lors des opérations d'analyse à venir. C'est la seule option qui ne soit pas sélectionnée par défaut.

  – **Poursuivre l'analyse**. Cette option demande à l'application de poursuivre son analyse sans prendre d'autres mesures. Si vous avez activé ses options de rapport, l'application enregistre l'incident dans son fichier journal.

  – **Arrêter l'analyse**. Cette option demande à l'application de cesser immédiatement l'opération d'analyse. Pour continuer, vous devez cliquer sur **Analyser maintenant** afin de relancer l'opération.

  – **Déplacer le fichier**. Cette option demande à l'application de placer le fichier infecté dans un dossier de quarantaine. Le message d'alerte affichera un bouton **Déplacer le fichier** pour vous permettre de localiser le dossier de quarantaine à utiliser.

- **Déplacer automatiquement les fichiers infectés.** Cette option demande à l'application de placer les fichiers infectés dans un dossier de quarantaine.

  Par défaut, l'application place ces fichiers dans un dossier nommé Infecté, situé dans le répertoire du programme VirusScan. Vous pouvez entrer un autre nom de dossier dans la zone de texte affichée ou cliquer sur **Parcourir** pour retrouver le dossier voulu sur votre disque dur.

- **Nettoyer automatiquement les fichiers infectés.** Sélectionnez cette option cette réponse pour que l'application supprime le code de virus dans le fichier infecté dès sa détection. Si l'application ne parvient pas à supprimer le virus, elle notera l'incident dans son fichier journal.
- **Supprimer les fichiers infectés automatiquement.** Sélectionnez cette option pour que l'application supprime immédiatement tout fichier infecté détecté. Assurez-vous d'avoir activé la fonction de rapport afin de disposer d'une liste des fichiers supprimés par l'application. Consultez ensuite cette dernière pour connaître les fichiers supprimés à restaurer à partir des copies de sauvegarde. Si l'application ne parvient pas à supprimer un fichier infecté, elle notera l'incident dans son fichier journal.
- **Poursuivre l'analyse.** N'utilisez cette option que si vous prévoyez d'être absent au moment où l'application recherchera les virus. Si vous activez également la fonction de rapport, l'application enregistrera le nom des virus détectés et le nom des fichiers infectés, pour vous permettre de les supprimer à une prochaine occasion.

3. Cliquez sur l'onglet Alerte pour choisir d'autres options de configuration de VirusScan.

   Pour démarrer immédiatement une opération d'analyse selon les options que vous avez choisies, cliquez sur **Analyser maintenant**. Pour enregistrer vos modifications comme options d'analyse par défaut, choisissez **Enregistrer comme valeur par défaut** dans le menu **Fichier** ou cliquez sur **Nouvelle analyse**. Pour enregistrer vos paramètres dans un nouveau fichier, choisissez **Enregistrer les paramètres** dans le menu **Fichier**, donnez un nom à votre fichier dans la boîte de dialogue qui s'affiche, puis cliquez sur **Enregistrer**.

Sélection des options d'alerte

Lorsque vous avez configuré vos options de réponse, vous pouvez laisser l'application VirusScan rechercher et supprimer automatiquement les virus de votre système au fur et à mesure qu'elle les détecte, pratiquement sans aucune autre intervention de votre part. Toutefois, pour que l'application vous informe immédiatement de la détection d'un virus de sorte que vous puissiez entreprendre l'action appropriée, vous devez la configurer pour qu'elle vous envoie un message d'alerte.

Procédez comme suit :

1. Cliquez sur l'onglet Alerte de la fenêtre VirusScan Avancé pour afficher la page de propriétés correspondante (Figure 5-15).

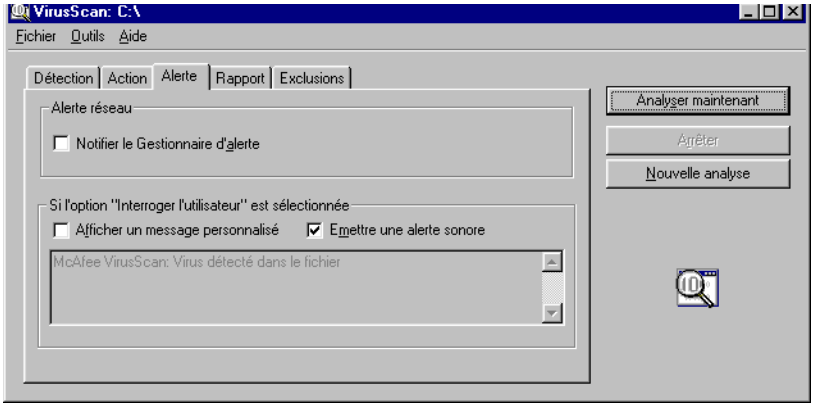

Figure 5-15. VirusScan Avancé – page Alerte

2. Cochez la case **Notifier le Gestionnaire d'alerte** pour que l'application VirusScan envoie des messages d'alerte au Gestionnaire d'alerte qui les transmettra.

   Le Gestionnaire d'alerte est un composant indépendant du logiciel McAfee qui regroupe des messages d'alerte et utilise diverses méthodes pour les envoyer aux destinataires que vous désignez. L'application VirusScan enverra ces messages d'alerte avec succès uniquement si vous avez installé l'utilitaire de Configuration cliente du Gestionnaire d'alerte. Pour plus de détails, reportez-vous à la section voir « Utilisation de l'utilitaire de Configuration cliente du Gestionnaire d'alerte » à la page 338.

   Vous pouvez transmettre des messages d'alerte directement à un serveur du Gestionnaire d'alerte. Sinon, vous pouvez les envoyer en tant que fichiers texte (.ALR) à un répertoire d'alerte centralisée que le serveur du Gestionnaire d'alerte interroge régulièrement.

   REMARQUE : Si vous décochez cette case, l'application VirusScan n'enverra pas des messages d'alerte via le Gestionnaire d'alerte, mais tous les autres messages d'alerte que vous configurez dans cette page de propriétés resteront intacts.

3. Cochez la case **Émettre une alerte sonore** pour que l'application envoie un signal sonore à chaque fois qu'elle trouve un fichier infecté.

Vous pouvez modifier le paramétrage de cette option à condition d'avoir sélectionné **Interroger l'utilisateur** dans la page de propriétés Action. Sinon, la case à cocher Émettre une alerte sonore affichera et utilisera le paramètre que vous lui avez attribué la dernière fois que vous avez sélectionné l'option **Interroger l'utilisateur**. L'application émettra le signal sonore standard du système ou exécutera le fichier .WAV que vous avez configuré sur votre ordinateur.

4. Cochez la case **Afficher un message personnalisé** pour que l'application ajoute un message personnalisé au texte du message qu'elle affiche lorsqu'elle trouve un fichier infecté.

   À l'égard de l'alerte sonore, vous pouvez modifier le paramétrage de cette option à condition d'avoir sélectionné **Interroger l'utilisateur** dans la page de propriétés Action. Si vous ne sélectionnez pas cette option dans la page Action, aucun message d'alerte ou message personnalisé ne s'affichera même si vous avez coché la case Afficher un message personnalisé.

5. Entrez le message que l'application doit afficher dans la zone de texte. Vous pouvez entrer 250 caractères maximum.

6. Cliquez sur l'onglet Rapport pour choisir d'autres options de configuration de VirusScan.

   Pour démarrer immédiatement une opération d'analyse selon les options que vous avez choisies, cliquez sur **Analyser maintenant**. Pour enregistrer vos modifications comme options d'analyse par défaut, choisissez **Enregistrer comme valeur par défaut** dans le menu **Fichier** ou cliquez sur **Nouvelle analyse**. Pour enregistrer vos paramètres dans un nouveau fichier, choisissez **Enregistrer les paramètres** dans le menu **Fichier**, donnez un nom à votre fichier dans la boîte de dialogue qui s'affiche, puis cliquez sur **Enregistrer**.

Sélection des options de rapport

L'application VirusScan liste ses paramètres courants et récapitule toutes les actions qu'elle effectue au cours de ses opérations d'analyse dans un fichier journal appelé VSCLOG.TXT. Ce rapport peut à votre convenance figurer dans ce fichier ou dans un fichier texte que vous aurez créé dans un éditeur de texte quelconque à l'intention de l'application. Vous pouvez ensuite ouvrir et imprimer le fichier journal pour consultation ultérieure, soit depuis l'application VirusScan, soit depuis un éditeur de texte.

Le fichier VSCLOG.TXT est un outil de gestion essentiel pour garder la trace de l'activité virale sur votre système et pour noter les paramétrages que vous utilisez pour détecter et traiter les infections signalées par l'application VirusScan. Vous pouvez également utiliser les rapports d'incidents enregistrés dans le fichier pour déterminer quels fichiers vous devez remplacer à partir de vos sauvegardes, examiner en quarantaine ou supprimer de votre système. Utilisez la page de propriétés Rapport pour déterminer les informations à inclure dans le fichier journal de l'application.

Pour afficher le contenu du fichier journal, démarrez l'application VirusScan, puis choisissez **Afficher le journal d'activité** dans le menu **Fichier**.

Pour configurer le logiciel VirusScan de sorte qu'il enregistre ses actions dans un fichier journal, procédez comme suit :

1. Cliquez sur l'onglet Rapport de la fenêtre VirusScan Avancé pour afficher la page de propriétés correspondante (Figure 5-16).

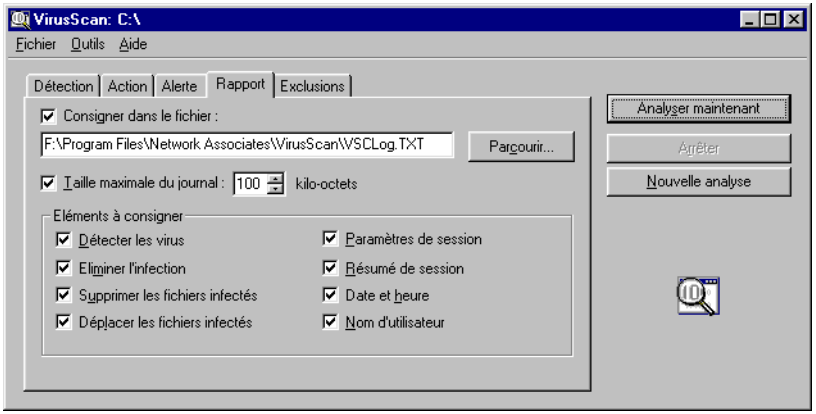

Figure 5-16. VirusScan Avancé – page Rapport

2. Cochez la case **Consigner dans le fichier**.

   Par défaut, l'application VirusScan enregistre les informations de journal dans le fichier VSCLOG.TXT, situé dans le répertoire du programme VirusScan. Vous pouvez entrer un autre nom de fichier dans la zone de texte affichée, ou cliquer sur **Parcourir** pour trouver un fichier approprié sur votre disque dur ou votre réseau. Vous pouvez utiliser un fichier différent, mais le fichier texte doit être déjà créé. L'application ne crée pas de fichier.

3. Pour limiter la taille du fichier journal, cochez la case **Taille limite du fichier journal**, puis saisissez cette taille, en Kilo-octets, dans la zone de texte prévue à cet effet. Si vous ne cochez pas cette case, le fichier journal peut voir sa taille augmenter et atteindre une limite déterminée par votre espace disque.

   Entrez une valeur comprise entre 10 Ko et 999 Ko. Par défaut, l'application limite la taille du fichier à 100 Ko. Si les données du journal dépassent la taille allouée pour le fichier, l'application efface le journal existant et le reprend au point où il s'était interrompu.

4. Cochez les cases correspondant aux informations que l'application doit enregistrer dans son fichier journal. Chaque case cochée génère l'enregistrement par l'application de l'information correspondante, généralement à la fin de l'opération d'analyse ou lorsque vous arrêtez votre système :

   - **Détecter les virus**. Cochez cette case pour que le fichier journal enregistre le nombre de virus trouvés par l'application dans chaque opération d'analyse. Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.
   - **Éliminer l'infection**. Cochez cette case pour que le fichier journal enregistre le nombre de fichiers infectés que l'application nettoie (ou tente de nettoyer) au cours de chaque opération d'analyse. Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.
   - **Suppression des fichiers infectés**. Cochez cette case pour que le fichier journal enregistre le nombre de virus supprimés par l'application dans chaque opération d'analyse. Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.
   - **Déplacement des fichiers infectés**. Cochez cette case pour que le fichier journal enregistre le nombre de virus que l'application a placé dans un dossier de quarantaine dans chaque opération d'analyse. Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.
   - **Paramètres de session**. Cochez cette case pour que le fichier journal enregistre les paramètres de configuration que vous avez utilisés pour l'application dans chaque opération d'analyse. Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.
   - **Résumé de session**. Cochez cette case pour que le fichier journal récapitule les actions effectuées par l'application dans chaque opération d'analyse. Le journal enregistrera les informations suivantes :

- Nombre de fichiers analysés par l'application.
- Nombre de fichiers infectés nettoyés par l'application.
- Nombre de fichiers infectés supprimés par l'application.
- Nombre de fichiers infectés que l'application a placé dans un dossier de quarantaine.
- Paramètres que vous avez attribués à l'application.

Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.

- **Date et heure**. Cochez cette case pour que le fichier journal enregistre la date et l'heure de début de chaque session d'analyse. Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.
- **Nom d'utilisateur**. Cochez cette case pour que le fichier journal enregistre le nom de l'utilisateur connecté à la station de travail lorsque le logiciel démarre chaque opération d'analyse. Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.

5. Cliquez sur l'onglet Exclusion pour choisir d'autres options de configuration de VirusScan.

   Pour démarrer immédiatement une opération d'analyse selon les options que vous avez choisies, cliquez sur **Analyser maintenant**. Pour enregistrer vos modifications comme options d'analyse par défaut, choisissez **Enregistrer comme valeur par défaut** dans le menu **Fichier** ou cliquez sur **Nouvelle analyse**. Pour enregistrer vos paramètres dans un nouveau fichier, choisissez **Enregistrer les paramètres** dans le menu **Fichier**, donnez un nom à votre fichier dans la boîte de dialogue qui s'affiche, puis cliquez sur **Enregistrer**.

Sélection des options d'exclusion

Nombre des fichiers stockés sur votre ordinateur ne risquent pas d'être infectés par des virus. Les opérations d'analyse qui examinent ces fichiers peuvent être longues et ne donner que peu de résultats. Vous pouvez accélérer les opérations d'analyse en demandant à l'application VirusScan de n'inspecter que les types de fichiers susceptibles d'être infectés (voir « Sélection des options de détection » à la page 213), d'ignorer des fichiers ou des dossiers complets dont vous savez qu'ils ne peuvent être infectés.

Après avoir analysé à fond votre système, vous pouvez exclure les fichiers et les dossiers qui ne se modifient jamais ou ne sont pas normalement vulnérables aux infections virales. Vous pouvez aussi compter sur le moteur d'analyse VShield pour vous protéger entre les opérations d'analyse planifiées. Cependant, la meilleure protection contre les virus demeure la régularité des opérations d'analyse examinant tous les secteurs de votre système.

Pour éviter que l'application examine des fichiers qui ne sont pas infectés, vous pouvez indiquer les disques, les dossiers ou les fichiers que vous souhaitez exclure des opérations d'analyse dans une liste d'exclusions Par défaut, l'application VirusScan n'examine pas la Corbeille, car Windows n'exécute pas les éléments qu'elle contient. Par conséquent, cet élément apparaît dans la liste des exclusions la première fois que vous ouvrez la fenêtre.

Chaque entrée de la liste des exclusions affiche le chemin d'accès de l'élément exclu, indique si l'application va exclure également les sous-dossiers contenus dans le dossier de l'élément et précise si l'application va exclure l'élément lors de l'analyse des fichiers, ou lors de l'analyse de la zone système de votre disque dur, ou les deux à la fois.

Par défaut, vous pouvez exclure jusqu'à 100 cibles à analyser uniques. Pour modifier ce chiffre, ouvrez le panneau de configuration VirusScan, cliquez sur l'onglet Composants, puis entrez un nouveau chiffre dans la zone de texte **Nombre maximal d'éléments à exclure**. Pour en savoir plus sur l'utilisation du panneau de configuration VirusScan, reportez-vous à la section « Présentation du Panneau de configuration VirusScan » à la page 333.

Pour exclure des opérations d'analyse certains fichiers ou dossiers, procédez comme suit :

1. Cliquez sur l'onglet Exclusion dans la fenêtre VirusScan Avancé pour afficher la page de propriétés correspondante (Figure 5-17).

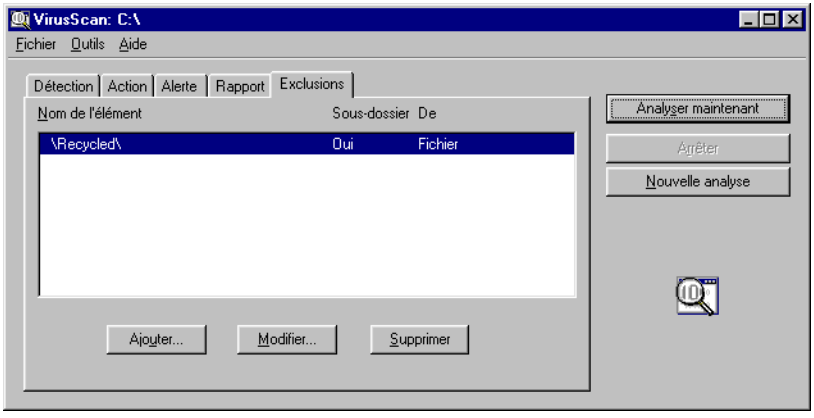

Figure 5-17. Fenêtre VirusScan Avancé – page Exclusion

2. Spécifiez les éléments que vous souhaitez exclure. Vous pouvez :

   - **Ajouter des fichiers, des dossiers ou des volumes à la liste des exclusions.** Cliquez sur **Ajouter** pour afficher la boîte de dialogue Ajout d'un élément à exclure (Figure 5-18 on page 228).

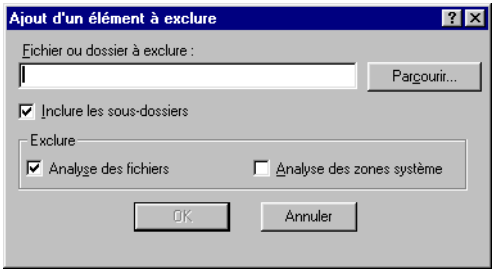

Figure 5-18. Boîte de dialogue Ajout d'un élément à exclure

Pour ajouter un élément à la liste des exclusions, procédez comme suit :

a. Entrez un chemin d'accès à un dossier ou un nom de fichier dans la zone de texte affichée ou cliquez sur **Parcourir** pour trouver l'élément que vous souhaitez exclure de l'analyse.

REMARQUE : Si vous avez choisi de déplacer automatiquement tout fichier infecté vers un dossier de quarantaine, l'application exclut ce dossier des opérations d'analyse.

---

b. Cochez la case **Inclure les sous-dossiers** pour que l'application ignore les fichiers stockés dans les sous-dossiers du dossier que vous avez spécifié dans l'Étape a.

REMARQUE : Lorsque vous sélectionnez l'option **Inclure les sous-dossiers**, l'application n'exclut de l'analyse que les fichiers stockés dans les sous-dossiers. Elle analysera les fichiers stockés à la racine du dossier que vous spécifiez. Pour exclure de l'analyse les fichiers situés à la racine du dossier, décochez la case **Inclure les sous-dossiers**.

---

c. Cochez la case **Analyse des fichiers** pour exclure l'élément que vous avez spécifié dans la première étape lorsque l'application recherche des virus infectant des fichiers. Ces virus apparaissent généralement dans des fichiers stockés dans les parties visibles de votre disque dur.

d. Cochez la case **Analyse de la zone système** pour exclure l'élément que vous avez spécifié dans la première étape lorsque le module recherche des virus infectant la zone système.

Ces virus résident souvent dans la mémoire ou dans des fichiers stockés dans la zone système ou dans la partition d'amorçage (MBR) de votre disque dur. Utilisez cette option pour exclure des opérations d'analyse des fichiers système comme COMMAND.COM.

AVERTISSEMENT : McAfee vous recommande de *ne pas* exclure vos fichiers système des opérations d'analyse.

e. Répétez les étapes Étape a. à Étape d. jusqu'à ce que vous ayez listé tous les fichiers et dossiers que vous souhaitez exclure de l'analyse.

- **Modifier la liste des exclusions.** Pour modifier les paramètres d'un élément exclu, sélectionnez-le dans la liste Exclusions, puis cliquez sur **Edition** pour ouvrir la boîte de dialogue Edition d'élément à exclure. Effectuez les modifications voulues, puis cliquez sur **OK** pour fermer la boîte de dialogue.
- **Supprimer un élément de la liste.** Pour supprimer un élément de la liste, sélectionnez-le, puis cliquez sur **Supprimer**. Cela signifie que l'application VirusScan *examinera* ce fichier ou dossier au cours de la prochaine session d'analyse.

3. Cliquez sur un autre onglet pour modifier l'un ou l'autre des paramètres de VirusScan.

Pour démarrer immédiatement une opération d'analyse selon les options que vous avez choisies, cliquez sur **Analyser maintenant**. Pour enregistrer vos modifications comme options d'analyse par défaut, choisissez **Enregistrer comme valeur par défaut** dans le menu **Fichier** ou cliquez sur **Nouvelle analyse**. Pour enregistrer vos paramètres dans un nouveau fichier, choisissez **Enregistrer les paramètres** dans le menu **Fichier**, donnez un nom à votre fichier dans la boîte de dialogue qui s'affiche, puis cliquez sur **Enregistrer**.

Activation de la protection par mot de passe

Le logiciel VirusScan vous permet de définir un mot de passe pour protéger les paramètres de chaque page de propriétés contre toute modification non autorisée. Cette fonction se révèle particulièrement utile pour les administrateurs système qui doivent empêcher les utilisateurs de tricher avec les mesures de sécurité en modifiant les paramètres de VirusScan. Utilisez la page de propriétés Sécurité pour verrouiller vos paramètres.

Pour activer la protection par mot de passe pour VirusScan Avancé, procédez comme suit :

1. Choisissez **Protection par mot de passe** dans le menu **Outils** de la fenêtre VirusScan Avancé pour ouvrir la boîte de dialogue Protection par mot de passe (Figure 5-19).

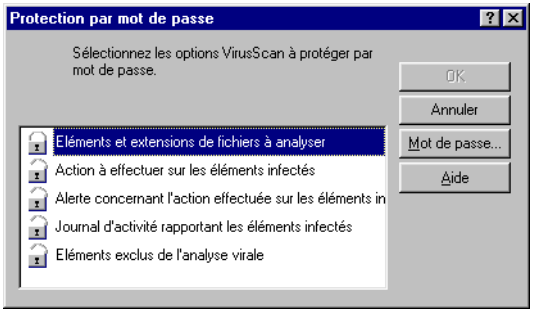

Figure 5-19. Boîte de dialogue Protection par mot de passe

2. Sélectionnez les paramètres que vous souhaitez protéger dans la liste affichée.

   Vous pouvez protéger les pages de propriétés de VirusScan individuellement ou dans leur ensemble. Dans la liste illustrée par la Figure 5-19, les noms des pages de propriétés verrouillées sont assortis d'une icône représentant un verrou fermé . Pour désactiver la protection d'une page de propriétés, cliquez sur le verrou fermé pour qu'il s'ouvre .

3. Cliquez sur **Mot de passe** pour ouvrir la boîte de dialogue Spécification du mot de passe (Figure 5-20).

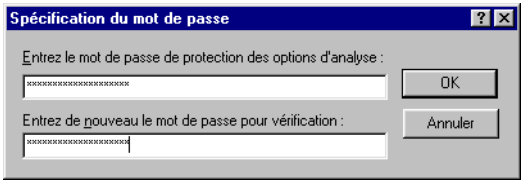

Figure 5-20. Boîte de dialogue Spécification du mot de passe

   a. Entrez un mot de passe dans la première zone de texte affichée, puis entrez-le de nouveau dans la zone de texte située au-dessous pour le confirmer.

   b. Cliquez sur **OK** pour fermer la boîte de dialogue Spécification du mot de passe.

4. Cliquez sur **OK** pour revenir à la fenêtre VirusScan Options avancées.

Création et configuration des tâches planifiées 6

Quel est le rôle de la console VirusScan ?

La principale fonction de la console VirusScan consiste à exécuter des opérations d'analyse et d'autres tâches aux dates et heures que vous souhaitez ou selon une périodicité que vous déterminez. Ayez recours à la console pour exécuter une opération d'analyse en votre absence, au moment où elle gênera le moins votre travail, dans un ensemble de tâches automatisées, ou selon tout autre mode adapté à vos besoins. La console VirusScan peut devenir le pilier de votre stratégie antivirus si vous la configurez pour exécuter un certain nombre de tâches interdépendantes ou associées qui garantissent la protection de votre système pendant les périodes d'inactivité. Par exemple, des tâches différentes à l'intérieur de cycles individuels peuvent analyser différentes parties de votre système ou garantir une protection maximale lors de l'exécution de tâches régulières ou planifiées.

La console vous permet également de démarrer et d'arrêter d'autres opérations importantes de VirusScan, notamment les sessions d'analyse de VShield et les opérations de mise à jour automatique et de mise à niveau automatique. Vous pouvez vous connecter au site Web AVERT de McAfee et obtenir des informations sur les virus, ouvrir et consulter des fichiers journaux et copier et coller des définitions de tâche à l'intérieur de la fenêtre de la console. Pour obtenir une présentation détaillée des fonctions disponibles à partir de la fenêtre de la console, reportez-vous à la section « Utilisation de la fenêtre de la console » à la page 235.

Pourquoi planifier les opérations d'analyse ?

Le logiciel VirusScan recherche les virus en permanence ou vous permet d'analyser votre système chaque fois que vous le souhaitez. Cependant, vous avez aussi la possibilité de planifier des opérations d'analyse régulières ainsi que d'autres tâches logicielles pour :

- **Déterminer une périodicité pour l'analyse de votre système**. Si vous souhaitez prévenir dans votre système ou votre réseau l'activité de virus récurrents, planifiez une opération d'analyse complète de votre système à intervalles réguliers. Les fonctions de rapport du logiciel VirusScan vous fournissent un rapport complet indiquant le nombre, le type, la taille et les autres caractéristiques de tout virus détecté.

- **Compléter ou remplacer l'analyse lors de l'accès**. McAfee vous recommande d'utiliser le logiciel VShield pour rechercher les virus en permanence, mais, si votre environnement ne vous le permet pas ou si vous vous préoccupez des performances de votre système, planifiez des opérations d'analyse fréquentes pour prévenir toute infection. Même si vous utilisez le logiciel VShield, planifiez régulièrement des opérations d'analyse complètes pour réduire le risque que des fichiers infestés puissent échapper à la détection.
- **Choisir entre différentes opérations d'analyse**. La planification vous offre le choix entre différentes opérations d'analyse pour des usages et des moments différents. Si, par exemple, vous souhaitez recourir au logiciel VShield pour analyser votre propre système en permanence et analyser moins souvent les unités de réseau associées, vous pouvez planifier une tâche à cet effet.

La console est livrée avec un ensemble de tâches par défaut déjà configurées mais pas encore planifiées. Cet ensemble inclut des tâches qui lancent le moteur d'analyse VShield lorsque vous allumez votre ordinateur, analysent tous les lecteurs, y compris le groupe Poste de travail et le lecteur C:, et mettent à jour les fichiers de données et les composants de programme du logiciel VirusScan. Vous pouvez activer l'une des tâches par défaut pour la lancer, ou bien créer vos propres tâches en fonction de vos habitudes de travail.

Démarrage de la console VirusScan

Vous devez activer la console VirusScan pour pouvoir exécuter n'importe quelle tâche planifiée. McAfee vous recommande de configurer la console de sorte qu'elle démarre automatiquement, dès l'amorçage de votre système.

Pour y parvenir, procédez comme suit :

1. Cliquez sur **Démarrer** dans la barre des tâches Windows, pointez sur **Paramètres**, puis choisissez **Panneau de configuration**.
2. Localisez et double-cliquez sur le panneau de configuration VirusScan  pour l'ouvrir.
3. Cliquez sur l'onglet Composants (Figure 6-1 à la page 233).

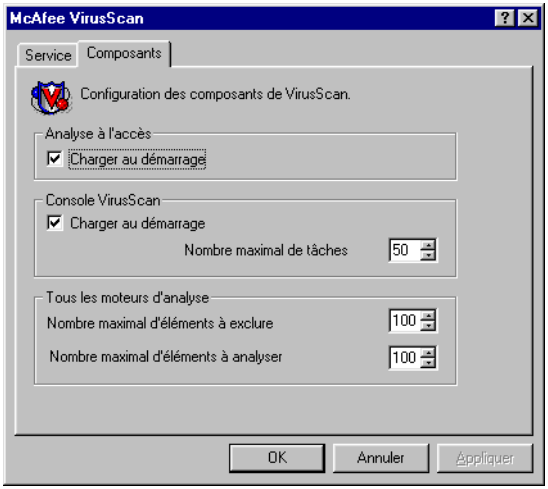

Figure 6-1. Panneau de configuration VirusScan – page Composants

4. Cochez la case **Charger au démarrage** dans la zone Console VirusScan de la page de propriétés Composants.

5. Cliquez sur **OK** pour fermer le panneau de configuration.

Lors du prochain démarrage de votre ordinateur, la console sera lancée mais restera sous forme d'icône dans la barre d'état système Windows. Double-cliquez sur cette icône pour amener la fenêtre de la console au premier plan (Figure 6-2).

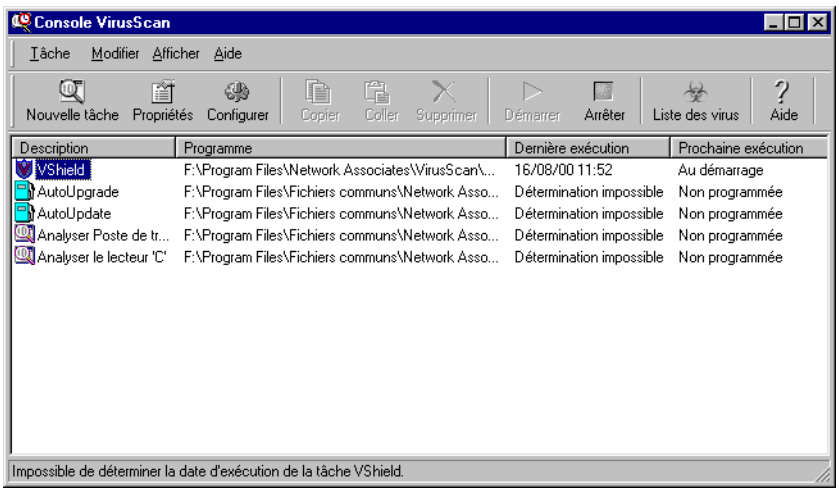

Figure 6-2. Fenêtre de la console VirusScan

Si l'icône ne s'affiche pas dans la barre d'état système Windows :

1. Cliquez sur **Démarrer** dans la barre des tâches Windows, pointez sur **Programmes**, puis sur **Network Associates**.
2. Choisissez **Console VirusScan** pour afficher la fenêtre de la console.

Une fois la fenêtre de la console affichée, vous pouvez la configurer pour qu'elle se charge automatiquement au démarrage. Pour ce faire, choisissez **Charger au démarrage** dans le menu **Affichage**.

La fenêtre de la console affiche au démarrage une liste de tâches par défaut, pré-configurées dans la console et prêtes à s'exécuter. Le terme « tâche » désigne un ensemble d'instructions destinées à exécuter un programme spécifique, dans une configuration particulière et à une heure donnée. La fenêtre de la console affiche non seulement le nom de chaque tâche, mais aussi le chemin d'accès et le nom de fichier du programme que la tâche exécutera à l'heure planifiée. Les tâches que vous créez exécutent toujours l'application VirusScan. Les dernières tâches créées s'affichent en bas de la fenêtre de la console. Cette dernière affiche également la date et l'heure de la dernière exécution de chaque tâche, ainsi que la date et l'heure de sa prochaine exécution.

La barre d'outils, située dans la partie supérieure de la fenêtre de la console, permet d'accéder rapidement aux commandes du programme les plus courantes. Pour que cette barre d'outils n'affiche que ses boutons de commande, cliquez sur **Affichage**, pointez sur **Barre d'outils**, puis choisissez **Boutons standard**.

Pour ajouter une légende aux boutons, cliquez sur **Affichage**, pointez sur **Barre d'outils**, puis choisissez **Étiquettes**. Vous pouvez activer les deux options simultanément—une coche en regard de l'élément de menu vous indique quel affichage est actif. La plupart de ces commandes figurent également dans les menus placés dans le haut de la fenêtre de la console, ainsi que dans les menus contextuels qui s'affichent lorsque vous cliquez sur une tâche de la liste à l'aide du bouton droit.

Une barre d'état située dans le bas de la fenêtre de la console affiche le nombre de tâches de la liste. Lorsque vous sélectionnez une tâche dans la liste, cette barre d'état vous indique la date de sa dernière exécution. Elle affiche également une brève description de chaque bouton de la barre d'outils lorsque vous placez dessus le curseur de la souris. Choisissez **Barre de titre** ou **Barre d'état** dans le menu **Affichage** pour afficher chaque élément de la fenêtre.

Utilisation de la fenêtre de la console

Depuis la fenêtre de la console, vous pouvez :

- **Créer une tâche.** Choisissez **Nouvelle tâche** dans le menu **Tâche** ou cliquez sur  dans la barre d'outils de la console. La boîte de dialogue Propriétés des tâches s'affiche. Pour en savoir plus sur l'attribution d'un nom à une tâche et la configuration d'autres propriétés, reportez-vous à la section « Création de nouvelles tâches » à la page 243.
- **Planifier et activer une tâche.** Sélectionnez une tâche dans la liste de la fenêtre de la console, puis choisissez **Propriétés** dans le menu **Tâche** ou cliquez sur  dans la barre d'outils de la console. La boîte de dialogue Propriétés des tâches s'affiche. Pour en savoir plus sur la planification et l'activation d'une tâche, reportez-vous à la section « Activation des tâches » à la page 247.
- **Configurer une tâche.** Sélectionnez une tâche dans la liste de la fenêtre de la console, puis cliquez sur  dans la barre d'outils de la console pour afficher une page de propriétés pour le composant VirusScan chargé d'exécuter la tâche. L'aspect de cette page de propriétés dépend du composant VirusScan que vous exécutez. Pour en savoir plus sur le paramétrage de l'application VirusScan, reportez-vous à la section « Configuration des options de l'application VirusScan » à la page 252.
- **Copier une tâche.** Sélectionnez une tâche dans la liste de la fenêtre de la console, puis choisissez **Copier** dans le menu **Edition** ou cliquez sur  dans la barre d'outils de la console. La tâche est copiée dans le Presse-papiers de Windows. Ensuite, cliquez dans la fenêtre de la console, puis choisissez **Coller** dans le menu **Edition** ou cliquez sur  dans la barre d'outils de la console pour coller la copie de la tâche dans la liste de la console. Utilisez cette fonction pour copier des paramètres de tâche afin de les réutiliser comme modèles dans d'autres tâches similaires.
- **Supprimer une tâche.** Sélectionnez une tâche dans la fenêtre de la console, puis choisissez **Supprimer** dans le menu **Tâche** ou cliquez sur  dans la barre d'outils de la console.

> **REMARQUE :** Vous ne pouvez supprimer que les tâches que vous avez créées, à l'exclusion de celles de l'ensemble par défaut prédéfini dans la console. Vous pouvez cependant désactiver toute tâche par défaut que vous ne souhaitez pas exécuter. Pour plus de détails, reportez-vous à la section « Activation des tâches » à la page 247.

- **Démarrer une tâche.** Sélectionnez une tâche dans la fenêtre de la console, puis choisissez **Démarrer** dans le menu **Tâche** ou cliquez sur  dans la barre d'outils de la console. La tâche sélectionnée démarre immédiatement et s'exécute avec les options que vous avez choisies. Pour activer le moteur d'analyse VShield, sélectionnez la tâche VShield, puis choisissez **Activer** dans le menu **Tâche**. Pour démarrer le moteur d'analyse et le charger en mémoire, sélectionnez la tâche VShield, puis cliquez sur  dans la barre d'outils de la console.

- **Arrêter une tâche.** Sélectionnez une tâche dans la fenêtre de la console, puis choisissez **Stop now** dans le menu **Tâche** ou cliquez sur  dans la barre d'outils de la console. Pour arrêter le moteur d'analyse VShield, sélectionnez la tâche VShield, puis cliquez sur  dans la barre d'outils de la console ou choisissez **Désactiver** dans le menu **Tâche**. Pour en savoir plus sur l'arrêt et la désactivation du moteur d'analyse VShield, reportez-vous à la section « Désactivation ou arrêt du moteur d'analyse VShield » à la page 186.

- **Vous connecter à la bibliothèque d'informations sur les virus McAfee.** Choisissez **Liste de virus** dans le menu **Affichage** ou cliquez sur  dans la barre d'outils de la console. La console lance votre navigateur préféré et se connecte au site Web AVERT. Pour en savoir plus sur les informations disponibles dans cette bibliothèque, reportez-vous à la section « Affichage des informations sur les virus » à la page 88.

  REMARQUE : Pour vous connecter au site d'information sur les virus, vous devez disposer d'une connexion à Internet et d'un logiciel de navigation résidant sur votre ordinateur.

- **Ouvrir le fichier d'aide en ligne.** Choisissez **Rubriques d'aide** dans le menu **Aide** ou cliquez sur  dans la barre d'outils de la console pour afficher la liste des rubriques d'aide du logiciel VirusScan. Vous pouvez également cliquer avec le bouton droit sur la plupart des boutons, listes, menus et autres éléments de boîte de dialogue pour afficher les rubriques d'aide contextuelles. Choisissez l'élément **Qu'est-ce que c'est ?**, qui apparaît lorsque vous cliquez avec le bouton droit dans une boîte de dialogue, pour afficher la rubrique d'aide correspondante. Pour en savoir plus sur la documentation VirusScan, reportez-vous à la section « Composants fournis avec VirusScan » à la page 34.

- **Afficher le journal d'activité.** Sélectionnez une des tâches dans la liste de la fenêtre de la console, puis choisissez **Afficher le journal d'activité** dans le menu **Tâche**. Toutes les tâches ne sont pas associées à un fichier journal, mais le logiciel VirusScan ouvre le fichier journal pour celles qui le sont dans une fenêtre du Bloc-notes. Vous pouvez imprimer, éditer, copier ou manipuler ce fichier comme vous le feriez avec un fichier texte ordinaire. Pour en savoir plus sur les informations enregistrées dans le fichier journal, reportez-vous aux chapitres Chapitre 4, « Utilisation du moteur d'analyse VShield », et Chapitre 5, « Utilisation de l'application VirusScan ».

- **Protéger les tâches avec un mot de passe**. Sélectionnez une tâche dans la liste de la fenêtre de la console, à l'exception de la tâche VShield, puis choisissez **Tâche de protection du mot de passe** dans le menu **Tâche** pour ouvrir la boîte de dialogue Spécification du mot de passe. Entrez un mot de passe de 20 caractères maximum dans la première zone de texte affichée, puis entrez-le de nouveau dans la zone de texte située au-dessous pour le confirmer. Cliquez sur **OK** pour fermer la boîte de dialogue.

  Chaque fois que vous ou quelqu'un d'autre tenterez de configurer les propriétés de la tâche que vous avez protégée, la console demandera de saisir le mot de passe que vous avez spécifié. Le fait de choisir cette option équivaut à cocher la case **Protéger de cette tâche par mot de passe** dans la boîte de dialogue Propriétés des tâches.

- **Démarrer la console VirusScan automatiquement.** Choisissez **Charger au démarrage** dans le menu **Affichage** pour que la console VirusScan soit lancée à chaque démarrage de l'ordinateur. Cette option est activée par défaut dans la console. Vous devez activer la console pour pouvoir exécuter les tâches planifiées, c'est pourquoi vous devez choisir l'option de démarrage automatique afin que les tâches planifiées s'exécutent aux heures indiquées.

  Vous pouvez également contrôler cette option depuis le panneau de configuration VirusScan. Pour en savoir plus sur l'utilisation du panneau de configuration, reportez-vous à la section « Présentation du Panneau de configuration VirusScan » à la page 333.

- **Afficher l'icône de la console dans la barre d'état système**. Choisissez **Afficher la barre des tâches** dans le menu **Affichage** pour que la console affiche cette icône  dans la barre d'état système Windows. Double-cliquez sur cette icône pour amener la fenêtre de la console au premier plan. Cliquez avec le bouton droit sur l'icône pour afficher un menu contextuel.

- **Quitter la console VirusScan.** Pour quitter la console, choisissez **Quitter** dans le menu **Tâche**. Si des tâches sont en attente d'exécution, vous devez réduire la fenêtre de la console mais vous ne devez pas la fermer. Pour en savoir plus sur le redémarrage de la console, reportez-vous à la section « Démarrage de la console VirusScan » à la page 232.

Exécution des tâches par défaut

Dès que vous avez installé le logiciel VirusScan et que vous redémarrez votre ordinateur, le logiciel VShield commence immédiatement à analyser votre système, en utilisant une configuration par défaut qui offre une protection de base à votre système. Les autres tâches de la liste de la fenêtre de la console ont elles aussi une configuration par défaut, mais elles demeurent en sommeil tant que vous ne les activez pas. Pour plus de détails, reportez-vous à la section « Activation des tâches » à la page 247.

La console est livrée avec cinq tâches par défaut. Ces tâches sont les suivantes :

- **VShield**. Cette tâche exécute le moteur d'analyse VShield. Par défaut, elle s'exécute automatiquement dès que vous démarrez votre ordinateur. Vous ne pouvez pas modifier le moment d'exécution du moteur d'analyse VShield, mais vous avez le choix entre plusieurs options d'analyse. Vous ne pouvez pas renommer ou supprimer cette tâche, mais vous pouvez afficher des statistiques de ses dernières sessions d'analyse, vous pouvez activer et désactiver la tâche et ouvrir la boîte de dialogue Propriétés de VShield pour la configurer.

  Pour en savoir plus sur les options disponibles, reportez-vous à la section Voir « Paramétrage des propriétés du moteur d'analyse VShield » à la page 116.

- **AutoUpgrade**. Cette tâche vous permet de planifier des mises à niveau automatiques du logiciel VirusScan. Ces mises à niveau peuvent s'appliquer aux fichiers du moteur d'analyse ou à d'autres types de fichiers. Pour mettre à niveau vos fichiers, vous devez configurer cette tâche pour se connecter à un serveur de réseau local ou à un site FTP que vous désignez, puis vous devez planifier la tâche et l'activer. Vous ne pouvez pas renommer ou supprimer cette tâche, mais vous pouvez l'activer et la désactiver, la planifier, la configurer et protéger ses paramètres par mot de passe.

  Pour en savoir plus sur la planification et l'activation de cette tâche, reportez-vous à la section « Activation des tâches » à la page 247. Pour en savoir plus sur la configuration de cette tâche en fonction de vos besoins, reportez-vous à la section Chapitre 7, « Mise à jour et mise à niveau du logiciel VirusScan ».

- **AutoUpdate**. Cette tâche vous permet de planifier la mise à jour automatique des fichiers de définition de virus (.DAT). Pour ce faire, vous devez configurer cette tâche pour se connecter à un serveur ou à un site FTP que vous désignez. La tâche est pré-configurée pour se connecter à un serveur McAfee, mais vous pouvez également la paramétrer pour télécharger des fichiers en interne. Vous pouvez aussi planifier et activer la tâche pour qu'elle exécute la mise à jour de vos fichiers. Pour le reste, cette tâche ressemble beaucoup à la tâche AutoUpgrade.

  Pour en savoir plus sur la planification et l'activation de cette tâche, reportez-vous à la section « Activation des tâches » à la page 247. Pour en savoir plus sur la configuration de cette tâche en fonction de vos besoins, reportez-vous à la section Chapitre 7, « Mise à jour et mise à niveau du logiciel VirusScan »..

- **Analyser le Poste de travail**. Cette tâche exécute une analyse de base de tous les disques durs et de tous les lecteurs connectés à votre ordinateur, ainsi que de la mémoire vive et des zones système du disque dur ou des disquettes. Vous ne pouvez pas renommer ou supprimer cette tâche, mais vous pouvez modifier sa configuration, la planifier, afficher les statistiques de sa dernière opération d'analyse et protéger ses paramètres par mot de passe. Pour exécuter cette tâche, vous devez d'abord l'activer, mais vous pouvez utiliser sa configuration par défaut pour obtenir une protection appropriée.

- **Analyser le lecteur 'C'**. Cette tâche exécute une opération d'analyse de base sur le lecteur C: de votre ordinateur. Pour le reste, cette tâche ressemble beaucoup à la tâche Analyser le Poste de travail.

Les tâches Analyser le poste de travail et Analyser le lecteur 'C' nécessitent toutes deux l'exécution de l'application VirusScan. Pour en savoir plus sur la configuration de l'application pour utiliser la console VirusScan, reportez-vous à la section « Configuration des options de l'application VirusScan » à la page 252.

Exécution de la tâche VShield

La tâche VShield s'affiche à l'origine dans la fenêtre de la console pour vous permettre de gérer son fonctionnement. Vous pouvez l'activer et la désactiver directement depuis la fenêtre de la console ou double-cliquer sur la tâche pour ouvrir la boîte de dialogue Propriétés des tâches (Figure 6-3).

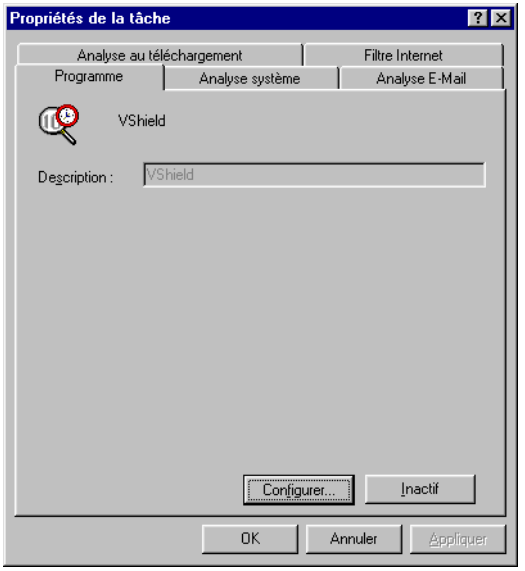

Figure 6-3. Boîte de dialogue Propriétés des tâches du moteur d'analyse VShield

Dans cette boîte de dialogue, vous pouvez :

- **Activer ou désactiver la tâche**. Cliquez sur le bouton **Désactiver**, situé en bas de la boîte de dialogue Propriétés des tâches. Si le moteur d'analyse n'est pas actif, ce même bouton affiche la mention **Activer**.
- **Ouvrir les pages de propriétés de configuration de VShield**. Cliquez sur **Propriétés** pour ouvrir la boîte de dialogue Analyse système, où vous trouverez toutes les options de configuration disponibles pour le moteur d'analyse VShield. Pour en savoir plus sur la configuration du moteur d'analyse, reportez-vous à la section « Paramétrage des propriétés du moteur d'analyse VShield » à la page 116.
- **Afficher les statistiques sur les modules VShield**. Toutes les autres pages de propriétés de la boîte de dialogue Propriétés des tâches affichent chacune des statistiques de la dernière opération d'analyse effectuée. Cliquez sur un autre onglet pour les afficher. Pour en savoir plus sur l'affichage d'une mise à jour en temps réel des statistiques, reportez-vous à la section « Recherche des informations d'état du logiciel VShield » à la page 193.

Exécution des tâches AutoUpgrade et AutoUpdate

La tâche de mise à niveau automatique vous permet de télécharger et d'installer de nouveaux fichiers programme pour votre logiciel VirusScan selon un calendrier que vous avez défini à l'avance. La tâche de mise à jour automatique vous permet de télécharger et d'installer de nouveaux fichiers de définition de virus (.DAT). Vous ne pouvez pas renommer, supprimer ou créer d'autres copies de ces tâches, mais vous pouvez les configurer, les protéger par un mot de passe ou les exécuter immédiatement depuis la boîte de dialogue Propriétés des tâches.

Pour exécuter l'une ou l'autre de ces tâches, ouvrez la fenêtre de la console et procédez comme suit :

1. Double-cliquez sur la tâche AutoUpgrade ou AutoUpdate dans la fenêtre de la console.

   La boîte de dialogue Propriétés des tâches s'affiche (Figure 6-4).

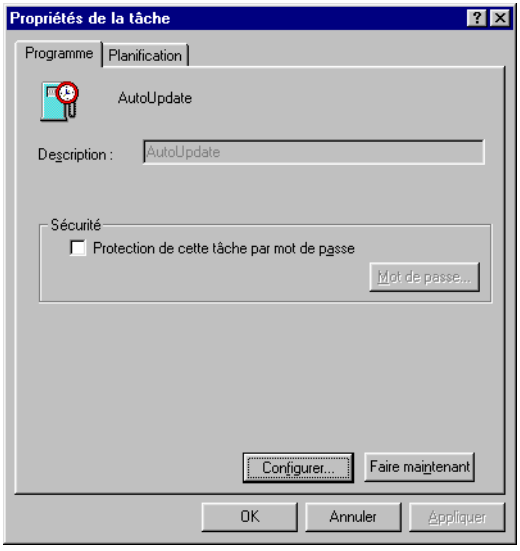

Figure 6-4. Boîte de dialogue Propriétés des tâches de l'utilitaire AutoUpdate

   Dans la mesure où vous ne pouvez pas renommer la tâche AutoUpgrade ou AutoUpdate, la zone de texte Description n'est pas accessible.

2. Définissez un mot de passe pour protéger cette tâche et empêcher toute modification des paramètres attribués AutoUpdate et AutoUpgrade. Pour définir le mot de passe, procédez comme suit :

a. Cochez la case **Protéger cette tâche par mot de passe**, puis cliquez sur **Mot de passe** pour ouvrir la boîte de dialogue Spécification du mot de passe.

b. Entrez un mot de passe unique dans la zone de texte prévue à cet effet.

   Vous pouvez entrer jusqu'à 20 caractères de toute sorte. Assurez-vous de choisir un mot de passe facile à retenir.

c. Tapez à nouveau le mot de passe, tel que vous l'avez fait dans la zone de texte précédente.

d. Cliquez sur **OK** pour fermer la boîte de dialogue Spécification du mot de passe.

   La console demandera ce mot de passe à chaque fois qu'un utilisateur tentera d'ouvrir la boîte de dialogue Propriétés des tâches pour cette tâche.

3. Ensuite, vous pouvez :

   - **Exécuter cette tâche avec les options de configuration existantes**. Cliquez sur **Exécuter maintenant** pour lancer immédiatement une opération de mise à niveau automatique ou de mise à jour automatique.
   - **Configurer la tâche AutoUpgrade ou AutoUpdate**. Cliquez sur **Configurer** pour ouvrir la boîte de dialogue Mise à niveau automatique ou Mise à jour automatique. Pour en savoir plus sur la configuration de l'utilitaire AutoUpgrade, reportez-vous à la section « Configuration de l'utilitaire AutoUpgrade » à la page 290. Pour en savoir plus sur la configuration de la tâche de mise à jour automatique, reportez-vous à la section « Description de l'utilitaire AutoUpdate » à la page 277.
   - Cliquez sur **Appliquer** pour enregistrer vos modifications sans fermer la boîte de dialogue Propriétés des tâches, puis cliquez sur l'onglet Planification. Pour en savoir plus sur la définition d'un calendrier d'exécution pour une tâche, reportez-vous à la section « Activation des tâches » à la page 247.
   - Cliquer sur **OK** pour enregistrer vos modifications et revenir à la fenêtre de la console VirusScan. Vous devrez ultérieurement définir un calendrier d'exécution pour cette tâche.

     Pour ce faire, sélectionnez la tâche dans la liste de la fenêtre de la console, puis cliquez sur  pour ouvrir la boîte de dialogue Propriétés des tâches.
   - Cliquez sur **Annuler** pour fermer la boîte de dialogue sans créer de tâche.

Création de nouvelles tâches

Les tâches définies par défaut assurent à votre système une protection appropriée ; néanmoins vous souhaiterez probablement créer et exécuter vos propres tâches lorsque vous aurez acquis l'expérience de VirusScan et que vous saurez quoi analyser et quand.

Vous pouvez modifier certains aspects des tâches par défaut fournies avec la console VirusScan, mais vous ne pouvez pas supprimer, renommer ou, à l'exception des tâches Analyser le Poste de travail et Analyser le lecteur 'C', créer de nouvelles instances de ces tâches. Vous pouvez copier les options de configuration prédéfinies des tâches Analyser le Poste de travail et Analyser le lecteur 'C' afin de les utiliser comme modèle de paramétrage pour vous nouvelles tâches.

La console vous permet toutefois de créer jusqu'à 50 nouvelles tâches pour répondre à vos besoins spécifiques. Vous pouvez modifier cette limite dans le panneau de configuration VirusScan. Pour en savoir plus sur cette procédure, reportez-vous à la section « Présentation du Panneau de configuration VirusScan » à la page 333.

Pour créer une tâche, procédez comme suit :

1. Choisissez **Nouvelle tâche** dans le menu **Tâche** de la fenêtre de la console ou cliquez sur  dans la barre d'outils de la console.

   La boîte de dialogue Propriétés des tâches s'affiche (Figure 6-5).

Figure 6-5. Boîte de dialogue Propriétés des tâches – page Programme

2. Entrez un nom pour cette tâche dans la zone de texte Description.

   Veillez à ce que ce nom décrive la tâche pour que vous puissiez la distinguer des autres tâches dans la fenêtre de la console et que vous sachiez immédiatement ce qu'elle fait.

3. Définissez un mot de passe pour protéger cette tâche et empêcher toute modification de ses paramètres. Pour définir le mot de passe, procédez comme suit :

   a. Cochez la case **Protection de cette tâche par mot de passe**, puis cliquez sur **Mot de passe** pour ouvrir la boîte de dialogue Spécification du mot de passe.

   b. Entrez un mot de passe unique dans la zone de texte prévue à cet effet.

      Vous pouvez entrer jusqu'à 20 caractères de toute sorte. Assurez-vous de choisir un mot de passe facile à retenir.

   c. Tapez à nouveau le mot de passe, tel que vous l'avez fait dans la zone de texte précédente.

   d. Cochez la case **Protéger toutes les options** pour protéger toutes les options définies pour cette tâche.

      Toutes les pages de propriétés relatives à cette tâche sont immédiatement verrouillées dans la page Sécurité de la boîte de dialogue Propriétés VirusScan. Si cette case n'est pas cochée, vous pouvez choisir des paramètres de sécurité différents pour chacune des pages dans la page de propriétés Sécurité. Pour en savoir plus sur la sélection de ces options, reportez-vous à la section « Sélection des options de sécurité » à la page 270.

   e. Cliquez sur **OK** pour fermer la boîte de dialogue Spécification du mot de passe.

      La console demandera ce mot de passe à chaque fois qu'un utilisateur tentera d'ouvrir la boîte de dialogue Propriétés des tâches pour cette tâche.

4. Spécifiez la façon dont l'interface de la tâche doit s'afficher et le degré de contrôle que vous souhaitez avoir sur cette tâche lors de son exécution. Vous avez le choix entre les options suivantes :

- **Normal scan mode**. Ce mode affiche la fenêtre principale de l'application VirusScan pendant les opérations d'analyse. Ceci permet à l'utilisateur situé devant l'ordinateur qui exécute la tâche d'afficher, mais pas de modifier, les options de configuration utilisées par la tâche lors de son exécution, de consulter les résultats de l'opération d'analyse et d'arrêter à tout moment l'exécution de la tâche. Toutes les commandes sont disponibles depuis les menus de la fenêtre principale.

  Cochez la case **Exécuter en réduction** pour afficher la fenêtre sous forme de bouton dans la barre des tâches Windows.

- **Scan only Mode**. Cette option affiche une fenêtre réduite qui indique que la tâche est en cours d'exécution. Vous pouvez à tout moment arrêter, suspendre ou reprendre l'exécution de la tâche.

  Cochez la case **Exécuter en réduction** pour afficher la fenêtre sous forme de bouton dans la barre des tâches Windows.

- **Hidden mode**. Ce mode n'affiche pas d'interface pendant l'exécution de la tâche. Vous ne pouvez pas suspendre ou arrêter l'exécution de la tâche, sauf si vous avez activé la console VirusScan ou la boîte de dialogue Propriétés des tâches. L'application VirusScan vous avertira en cas de détection de virus, si vous avez configuré l'une des options d'alerte locales pour la tâche. Une fois exécutée, cette tâche quitte toujours l'application.

5. Indiquez ce que la tâche doit faire une fois exécutée. Vous avez le choix entre les options suivantes :

   - **Toujours fermer**. Cliquez sur ce bouton pour demander à l'application VirusScan de toujours quitter immédiatement une fois la tâche d'analyse achevée. Si vous choisissez **Hidden mode** dans la liste Type d'interface, celle-ci est la seule option disponible.

   - **Auto-fermeture**. Cliquez sur ce bouton pour demander à l'application VirusScan de quitter immédiatement si elle ne trouve pas de virus au cours de cette tâche d'analyse. En l'absence de virus, l'application reste ouverte pour afficher les résultats de l'analyse.

     Si vous exécutez la tâche en mode analyse normale, l'application vous permet également de supprimer les virus détectés si vous ne l'avez pas encore configurée pour le faire automatiquement.

   - **Ne jamais fermer**. Cliquez sur ce bouton pour demander à l'application VirusScan de toujours rester ouverte une fois la tâche d'analyse achevée.

Si vous exécutez la tâche en mode analyse normale, l'application affiche les résultats de l'opération d'analyse et vous permet de supprimer les virus détectés si vous ne l'avez pas encore configurée pour le faire automatiquement. Si vous le souhaitez, vous pouvez relancer immédiatement la tâche d'analyse.

6. Vous avez maintenant entré suffisamment d'informations pour créer votre tâche, mais vous n'avez pas encore fixé sa date d'exécution ni choisi d'options de programme. Vous pouvez :

   - Cliquer sur **Configurer** pour définir les propriétés de cette tâche.

     La boîte de dialogue Propriétés VirusScan s'affiche. Cette boîte de dialogue vous permet d'indiquer à l'application VirusScan l'emplacement et la cible d'analyse, la façon dont elle doit réagir en cas de détection de virus, la méthode à utiliser pour vous en avertir, les informations qu'elle doit consigner dans son journal d'activité, les éléments qu'elle doit exclure des tâches d'analyse et si elle doit ou non protéger les options de configuration que vous avez définies pour la tâche.

     Pour en savoir plus sur la configuration de ces options, reportez-vous à la section « Configuration des options de l'application VirusScan » à la page 252.

   - Cliquez sur **Exécuter maintenant** pour exécuter immédiatement cette tâche. La tâche s'exécute avec les options de configuration par défaut ou avec celles que vous avez choisies. Qu'est-ce qui se passe lorsque vous cliquez sur le bouton ?

     – Si vous avez configuré la tâche pour un démarrage automatique, elle sera exécutée immédiatement. Ceci est possible à condition d'avoir coché la case **Démarrer automatiquement** dans la boîte de dialogue Propriétés VirusScan. Pour afficher cette case à cocher, cliquez à gauche sur **Configurer**, puis localisez-la dans la zone Eléments à analyser de la page de propriétés Détection.

     – Si vous choisissez d'analyser une tâche non configurée pour un démarrage automatique, la fenêtre de l'application VirusScan s'affiche. Cliquez dans cette fenêtre sur **Analyser maintenant** pour exécuter la tâche.

   - Cliquez sur **Appliquer** pour enregistrer vos modifications sans fermer la boîte de dialogue Propriétés des tâches, puis cliquez sur l'onglet Planification. Pour en savoir plus sur la définition d'un calendrier d'exécution pour une tâche, reportez-vous à la section « Activation des tâches » à la page 247.

- Cliquer sur **OK** pour enregistrer vos modifications et revenir à la fenêtre de la console VirusScan. Vous devrez ultérieurement définir un calendrier d'exécution pour cette tâche.

  Pour ce faire, sélectionnez la tâche dans la liste de la fenêtre de la console, puis cliquez sur  pour ouvrir la boîte de dialogue Propriétés des tâches.

- Cliquez sur **Annuler** pour fermer la boîte de dialogue sans créer de tâche.

Activation des tâches

Activer une tâche c'est choisir pour elle un calendrier et activer ce calendrier afin qu'elle s'exécute au moment où vous le souhaitez. Vous pouvez planifier l'exécution de toutes les tâches listées dans la fenêtre de la console VirusScan, à l'exception de la tâche VShield qui s'exécute en permanence dès que vous démarrez votre ordinateur ou dès que vous exécutez la tâche par vous-même.

Une tâche ne peut être exécutée que si la console VirusScan est active au moment prévu pour son exécution. Pour en savoir plus sur le démarrage de la console, reportez-vous à la section « Démarrage de la console VirusScan » à la page 232.

Pour exécuter une tâche d'analyse qui utilise l'application VirusScan, cette opération doit être configurée pour démarrer automatiquement. Ceci ne s'applique pas aux autres tâches par défaut. Pour plus de détails, reportez-vous à l'Étape 5 à la page 258.

Pour activer une tâche, procédez comme suit :

1. Si la boîte de dialogue Propriétés des tâches n'est pas déjà ouverte, double-cliquez sur une tâche dans la liste de la fenêtre de la console ou sélectionnez une tâche, puis cliquez sur  dans la barre d'outils de la console.

   La boîte de dialogue Propriétés des tâches s'affiche (voir Figure 6-5 à la page 243). Si vous choisissez VShield, AutoUpdate ou AutoUpgrade dans la liste des tâches de la console, la boîte de dialogue Propriétés des tâches n'aura pas la même apparence que celle illustrée dans la Figure 6-5.

2. Cliquez sur l'onglet Planification pour afficher la page de propriétés correspondante (voir Figure 6-6 à la page 248).

REMARQUE : La boîte de dialogue Propriétés des tâches du moteur d'analyse VShield n'inclura pas de page de propriétés Planification mais des pages d'état pour chacun de ses modules. Les boîtes de dialogue Propriétés des tâches pour les tâches AutoUpdate et AutoUpgrade quant à elles n'incluront pas de pages d'état.

Figure 6-6. Boîte de dialogue Propriétés des tâches – page Planification

3. Cochez la case **Activer**. Les options des zones Exécuter et Démarrer deviennent accessibles.

4. Choisissez la fréquence d'exécution de la tâche dans la zone Exécuter. Selon la fréquence choisie, la zone Démarrer vous propose des choix différents pour le calendrier d'exécution de votre tâche. Vous avez le choix entre les options suivantes :

   - **Une fois**. Cochez cette case pour exécuter votre tâche une seule fois à la date et à l'heure que vous spécifiez. Entrez l'heure dans la zone de texte de gauche de la zone Démarrer, puis sélectionnez un mois dans la liste de droite. Entrez ensuite la date et l'année dans les zones de texte affichées.
   - **Tous les jours**. Cochez cette case pour exécuter votre tâche une fois, à l'heure et aux dates que vous spécifiez. Entrez l'heure dans la zone de texte affichée puis cochez les cases de la zone Démarrer pour chacun des jours où vous souhaitez exécuter cette tâche.

- **Au démarrage**. Cochez cette case pour exécuter votre tâche une fois à chaque fois que vous démarrez votre ordinateur et la console VirusScan. Indiquez en heures et en minutes le délai que la console doit respecter avant d'exécuter la tâche une fois l'ordinateur démarré. Vous *ne pouvez pas* randomiser ce calendrier.
- **Toutes les semaines**. Cochez cette case pour exécuter votre tâche une fois par semaine au jour et à l'heure que vous spécifiez. Entrez l'heure dans la zone de texte affichée puis choisissez un jour dans la liste de droite.
- **Toutes les heures**. Cochez cette case pour exécuter votre tâche toutes les heures tant que votre ordinateur est allumé et que la console demeure activée. Spécifiez dans la zone de texte affichée le délai en minutes que la console doit respecter après chaque heure avant d'exécuter votre tâche.
- **Tous les mois**. Cochez cette case pour exécuter votre tâche une fois par mois au jour et à l'heure que vous spécifiez. Entrez l'heure dans la zone de texte de gauche, puis le jour souhaité pour l'exécution de la tâche.

❑ **REMARQUE :** Toutes les heures planifiées, à l'exception de l'intervalle horaire, doivent être spécifiées au format 24 heures. Si par exemple vous souhaitez exécuter une tâche le soir à 9h 30, entrez 21:30.

---

5. Pour exécuter cette tâche dans un intervalle randomisé à partir de l'heure que vous définissez, cochez la case **Activer la randomisation**, puis entrez un délai de huit heures maximum dans la zone de texte Randomiser la fenêtre temporelle.

   Sauf si vous avez configuré cette tâche pour être exécutée au démarrage, vous pouvez utiliser cette fonction pour réduire le trafic réseau et autres charges du système qui résultent de l'exécution simultanée d'opérations d'analyse ou de mise à jour par différents ordinateurs. La tâche s'exécutera à un moment aléatoire compris dans la « fenêtre » de temps que vous spécifiez.

   La fenêtre prend comme point central l'heure prévue pour l'exécution de la tâche. Par exemple, si vous configurez cette tâche pour être exécutée tous les jours à 15:00 et que vous sélectionnez ensuite **Activer la randomisation** en spécifiant une fenêtre de temps d'une heure, la tâche sera exécutée à n'importe quelle heure dans un intervalle compris entre 14:30 et 15:30. Vous pouvez définir une fenêtre de 480 minutes ou huit heures maximum.

6. Vous avez défini un calendrier pour votre tâche et vous l'avez activée pour qu'elle s'exécute au moment prévu. Cliquez sur **OK** pour fermer la boîte de dialogue Propriétés des tâches ou sur **Appliquer** pour enregistrer vos paramètres sans fermer la boîte de dialogue. Cliquez sur **Annuler** pour fermer la boîte de dialogue sans enregistrer vos modifications.

REMARQUE : Pour démarrer votre tâche, votre ordinateur doit être allumé et la console VirusScan doit être en cours d'exécution. Si ces deux conditions ne sont pas remplies au moment où votre tâche devrait démarrer, elle ne s'exécutera qu'à la prochaine date planifiée. Vous pouvez réduire la fenêtre de la console de telle sorte qu'elle n'apparaisse que sous forme d'icône dans la barre des tâches Windows.

Si vous souhaitez que VirusScan exécute une tâche d'analyse sur un ordinateur fonctionnant sans opérateur, vous devez également configurer le programme pour qu'il lance automatiquement l'opération d'analyse. Pour plus de détails, reportez-vous à la section Étape 5 à la page 258.

Consultation de l'état d'une tâche

La fenêtre de la console VirusScan indique l'heure et le jour de la dernière exécution des tâches et de leur prochain démarrage ; cette information est affichée à droite de chaque tâche répertoriée dans la liste. Vous pouvez également afficher un résumé du nombre de fichiers analysé par chaque tâche, savoir si des agents nuisibles ont été détectés et connaître les mesures appliquées.

Pour afficher les résultats d'une tâche, procédez comme suit :

1. Si la boîte de dialogue Propriétés des tâches n'est pas déjà ouverte, double-cliquez sur une tâche dans la liste de la fenêtre de la console ou sélectionnez une tâche, puis cliquez sur  dans la barre d'outils de la console.

2. La boîte de dialogue Propriétés des tâches s'affiche (voir Figure 6-5 à la page 243). Cliquez sur l'onglet État pour afficher la page de propriétés correspondante (Figure 6-7 à la page 251).

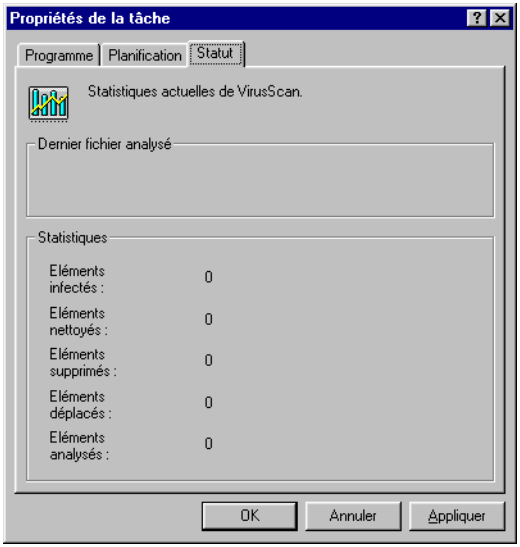

Figure 6-7. Boîte de dialogue Propriétés des tâches – page État

La page État affiche la liste des résultats de la dernière opération d'analyse exécutée par la tâche ainsi que le nom du dernier fichier analysé. Pour afficher une brève description de chacun des éléments présentés dans cette page, cliquez avec le bouton droit sur une image ou un label, puis cliquez sur **Qu'est-ce que c'est ?** dans le menu contextuel qui s'affiche, ou cliquez sur le bouton **?** dans le coin supérieur droit de la boîte de dialogue, puis cliquez sur l'élément dont vous souhaitez obtenir une description. Ces affichages *ne seront pas* mis à jour en temps réel.

REMARQUE : La boite de dialogue Propriétés des tâches de VShield inclut des pages d'état pour tous les modules VShield. La boîte de dialogue Propriétés des tâches pour AutoUpdate et AutoUpgrade n'inclut pas de page d'état. Pour en savoir plus sur la recherche d'informations sur l'état du moteur d'analyse VShield, reportez-vous à la section « Recherche des informations d'état du logiciel VShield » à la page 193.

Configuration des options de l'application VirusScan

Pour configurer une tâche d'analyse VirusScan de sorte qu'elle soit exécutée à l'heure que vous désignez, vous devez fournir à l'application les informations suivantes :

- à quel moment elle doit exécuter l'analyse
- ce qu'elle doit analyser
- ce qu'elle doit faire en cas de détection d'un virus
- comment elle doit vous informer en cas de détection d'un virus
- si vous souhaitez conserver une trace de ses actions
- les éléments qu'elle doit exclure de la recherche de virus
- si vous souhaitez protéger les paramètres que vous choisissez contre toute modification non autorisée

La console VirusScan inclut un ensemble de pages de propriétés que vous pouvez utiliser pour définir votre tâche. Ces pages de propriétés reproduisent une grande partie des options qui figurent dans la fenêtre principale de l'application VirusScan et en ajoutent d'autres afin de vous aider à définir une tâche qui sera exécutée régulièrement et à plusieurs reprises.

Pour configurer l'application VirusScan afin d'exécuter une tâche d'analyse, sélectionnez une tâche dans la liste de la fenêtre de la console—y compris les tâches que vous avez créées vous-même—puis cliquez sur  dans la barre d'outils de la console.

La boîte de dialogue Propriétés VirusScan s'affiche (Figure 6-8).

Figure 6-8. Boîte de dialogue Propriétés VirusScan – page Détection

Sélection des options de détection

Si vous choisissez de configurer une tâche que vous venez de créer, l'application VirusScan suppose à priori que vous souhaitez analyser le lecteur C: et la mémoire de votre ordinateur, rechercher des virus dans les secteurs d'amorçage et limiter l'analyse aux fichiers susceptibles d'avoir été infectés par un virus. Si vous choisissez de configurer l'une des tâches par défaut, vos options initiales varient.

Pour modifier les options de tâche initiales, procédez comme suit :

1. Choisissez les éléments de votre système ou de votre réseau que l'application VirusScan doit analyser. Vous pouvez :

   - **Ajouter des cibles à analyser.** Cliquez sur **Ajouter** pour ouvrir la boîte de dialogue Ajout d'un élément à analyser (Figure 6-9 à la page 254).

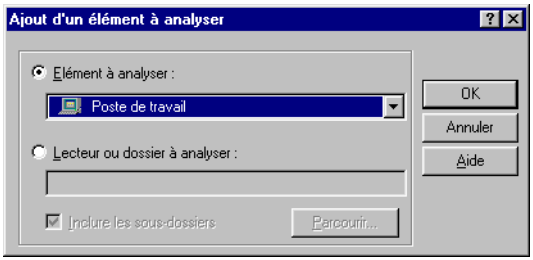

Figure 6-9. Boîte de dialogue Ajout d'un élément à analyser

Pour analyser tout votre ordinateur ou un sous-ensemble d'unités de votre système ou de votre réseau, cliquez sur le bouton **Sélection de l'élément à analyser**, puis

a. choisissez une cible à analyser dans la liste qui vous est proposée. Vous avez le choix entre les options suivantes :

   – **Poste de travail**. Cette option demande à l'application d'analyser tous les lecteurs physiquement connectés à votre ordinateur ou logiquement associés à une lettre de lecteur de votre ordinateur par l'intermédiaire de l'explorateur Windows.

   – **Tous les supports amovibles**. Cette option demande à l'application d'analyser uniquement les disquettes, les CD-ROM, les disques ZIP Iomega ou des supports de stockage similaires physiquement connectés à votre ordinateur.

   – **Tous les lecteurs fixes**. Cette option demande à l'application d'analyser les disques durs physiquement connectés à votre ordinateur.

   – **Tous les lecteurs réseau**. Cette option demande à l'application d'analyser toutes les unités logiquement associées à une lettre de lecteur de votre ordinateur par l'intermédiaire de l'explorateur Windows.

b. Cliquez sur **OK** pour fermer la boîte de dialogue.

Pour examiner un disque ou un dossier spécifique de votre système, cliquez sur le bouton **Lecteur ou dossier à analyser**, puis

a. entrez, dans la zone de texte prévue à cet effet, la lettre du lecteur ou le chemin d'accès au dossier que vous souhaitez analyser. Vous pouvez également cliquer sur **Parcourir** pour rechercher la cible à analyser sur votre ordinateur.

REMARQUE : Vous ne pouvez pas utiliser la notation de la convention d'affectation des noms (UNC) pour spécifier un disque réseau comme cible à analyser pour les tâches planifiées. L'utilisation de ce type de notation génère l'erreur « chemin non valide ». Vous pouvez utiliser la notation de la convention d'affectation des noms (UNC) pour spécifier des cibles à analyser pour les opérations que vous exécutez directement avec l'application VirusScan.

b. Cochez la case **Inclure les sous-dossiers** si vous souhaitez que l'application VirusScan recherche les virus dans les dossiers contenus dans votre cible d'analyse.

REMARQUE : Si vous sélectionnez **Inclure les sous-dossiers**, l'application analyse uniquement les fichiers stockés dans les sous-dossiers eux-mêmes. Elle n'analyse pas les fichiers stockés à la racine du dossier que vous spécifiez. Pour analyser ces fichiers, décochez la case **Inclure les sous-dossiers**.

c. Cliquez sur **OK** pour fermer la boîte de dialogue.

- **Modifier une cible à analyser.** Sélectionnez l'une des cibles de la liste puis cliquez sur **Modifier** pour ouvrir la boîte de dialogue Modifier l'élément à analyser (Figure 6-10).

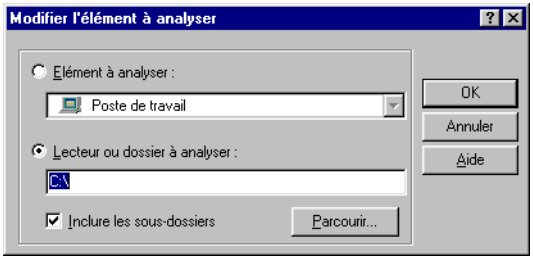

Figure 6-10. Boîte de dialogue Modifier l'élément à analyser

La boîte de dialogue s'affiche avec les cibles à analyser actuellement spécifiées. Choisissez une cible à analyser ou tapez-en une, puis cliquez sur **OK** pour fermer la boîte de dialogue.

- **Supprimer les cibles à analyser.** Sélectionnez l'une des cibles de la liste, puis cliquez sur **Supprimer** pour l'effacer.

2. Spécifiez les types de fichiers que l'application VirusScan doit examiner. Vous pouvez :

   - **Analyser les fichiers compressés.** Cochez la **case Fichiers compressés** pour que l'application VirusScan recherche les virus éventuels dans les fichiers compressés ou dans les fichiers d'archives. Bien qu'il offre une protection supplémentaire, l'examen des fichiers compressés peut ralentir l'opération d'analyse.

     Pour afficher la liste des types de fichiers et d'archives que l'application analyse, reportez-vous à la section « Liste en cours des fichiers compressés analysés » à la page 352.

   - **Analyser tous les fichiers**. Cochez la case **Tous les fichiers** pour que l'application analyse tous les fichiers contenus dans la cible que vous avez spécifiée, quelle qu'en soit l'extension.

     ❑ **REMARQUE :** McAfee recommande de sélectionner cette option pour votre première opération d'analyse, ou à intervalles réguliers par la suite, de manière à garantir que votre système est exempt de tout virus. Vous pouvez ensuite limiter la portée des opérations d'analyse ultérieures.

   - **Choisir les types de fichiers**. D'ordinaire, les virus ne peuvent infecter les fichiers qui ne contiennent pas de code exécutable, que ce soit du code de script, de macro ou binaire. Vous pouvez par conséquent limiter en toute sécurité la portée de vos opérations d'analyse aux fichiers les plus susceptibles d'être infectés par des virus. Pour ce faire, cliquez sur le bouton **Fichiers programme uniquement**.

     Pour afficher ou spécifier les extensions de nom de fichier que l'application doit examiner, cliquez sur **Extensions**. La boîte de dialogue Extensions de fichiers programme s'affiche. Pour en savoir plus sur la modification des fichiers répertoriés à cet endroit, reportez-vous à la section « Ajout d'extensions de fichier pour analyse » à la page 345.

3. Activer l'analyse heuristique. Cliquez sur **Options avancées** pour ouvrir la boîte de dialogue Paramètres d'analyse avancés (Figure 6-11 à la page 257).

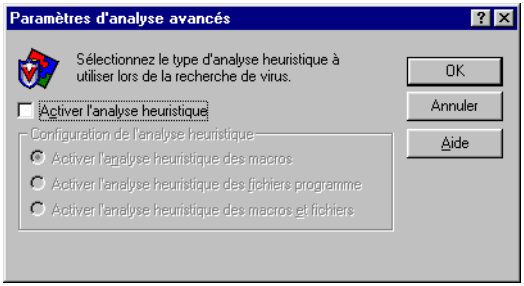

Figure 6-11. Boîte de dialogue Paramètres d'analyse avancés

La technologie d'analyse heuristique permet à l'application VirusScan de reconnaître les nouveaux virus en fonction de leur ressemblance avec des virus similaires déjà identifiés. Pour ce faire, l'application recherche des caractéristiques propres aux virus dans les fichiers que vous lui avez demandé d'analyser. Si elle détecte un nombre suffisant de caractéristiques dans un fichier, l'application identifie le fichier comme étant potentiellement infecté par un nouveau virus ou un virus non identifié.

L'application recherche en même temps des caractéristiques qui dénotent de l'absence de virus, c'est pourquoi elle ne se trompe que rarement en vous signalant une infection. À moins d'être certain que votre fichier ne contient *pas* de virus, vous devez apporter aux infections « probables » les mêmes précautions que vous apportez aux infections confirmées.

Lorsque vous démarrez l'application VirusScan, aucune option d'analyse heuristique n'est activée par défaut. Pour activer l'analyse heuristique, procédez comme suit :

a. Cochez la case **Activer l'analyse heuristique**. Les options proposées dans le reste de la boîte de dialogue deviennent accessibles.

b. Sélectionnez les types d'analyses heuristiques que l'application VirusScan doit utiliser. Vous avez le choix entre les options suivantes :

   – **Activer l'analyse heuristique des macros**. Sélectionnez cette option pour que l'application identifie d'abord tous les fichiers Microsoft Word, Microsoft Excel et autres fichiers Microsoft Office incorporant des macros et compare ensuite le code de la macro avec sa base de données de définitions de virus. Si la correspondance est exacte, l'application identifie le nom du virus ; pour les chaînes de signature qui ressemblent à celles de virus existants, elle vous informe qu'elle a détecté un virus de macro « probable ».

- **Activer l'analyse heuristique des fichiers programme.** Sélectionnez cette option si vous souhaitez que l'application VirusScan localise de nouveaux virus dans les fichiers programme en examinant les caractéristiques des fichiers et en les comparant avec celles figurant sur une liste de virus connus. Lorsqu'elle détecte un fichier ayant un certain nombre de caractéristiques, l'application l'identifie comme étant potentiellement infecté.
- **Activer l'analyse heuristique des macros et fichiers programme.** Sélectionnez cette option si vous souhaitez que l'application utilise les deux types d'analyse heuristique. McAfee vous recommande d'utiliser cette option pour une protection antivirus optimale.

> **REMARQUE :** L'application n'utilise les techniques d'analyse heuristique que sur les types de fichiers que vous désignez dans la boîte de dialogue Extensions de fichiers programme. Si vous décidez d'analyser **Tous les fichiers**, elle appliquera l'analysera heuristique à tous les types de fichiers.

c. Cliquez sur **OK** pour enregistrer vos paramètres et revenir à la boîte de dialogue Propriétés VirusScan.

4. Sélectionner des options d'analyse spéciales.

   Les virus des zones système se chargent dans la mémoire de votre ordinateur et se tapissent dans les secteurs d'amorçage ou dans la partition d'amorçage de votre disque dur. Pour utiliser cette tâche d'analyse pour détecter ces types de virus, cochez les cases **Analyser la mémoire** et **Analyser les zones système**.

5. Si vous avez planifié l'exécution d'opérations d'analyse en votre absence, cochez la case **Démarrer automatiquement** pour demander à l'application VirusScan de commencer l'analyse dès son démarrage.

   Si vous ne cochez pas cette case, la console démarrera le logiciel VirusScan, mais celui-ci attendra que vous cliquiez sur **Démarrer maintenant** pour commencer l'analyse. En laissant cette case décochée, vous aurez la possibilité d'annuler l'opération d'analyse si elle gêne votre travail.

6. Cliquez sur l'onglet Action pour choisir d'autres options de VirusScan. Pour enregistrer vos modifications sans fermer la boîte de dialogue Propriétés VirusScan, cliquez sur **Appliquer**. Pour enregistrer vos modifications et revenir à la fenêtre de la console, cliquez sur **OK**. Pour revenir à la fenêtre de la console sans enregistrer vos modifications, cliquez sur **Annuler**.

REMARQUE : Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

Sélection des options d'action

Lorsque l'application VirusScan détecte un virus, elle réagit soit en vous demandant ce qu'elle doit faire du fichier infecté, soit en lançant automatiquement une action que vous avez déterminée auparavant. Utilisez la page de propriétés Action pour spécifier les actions que le logiciel VirusScan doit vous proposer en cas de détection d'un virus et celles qu'il doit mettre en œuvre automatiquement.

Procédez comme suit :

1. Pour démarrer depuis la fenêtre de la console, sélectionnez la tâche que vous avez créée dans la liste des tâches, puis cliquez sur dans la barre d'outils de la console.

2. La boîte de dialogue Propriétés VirusScan s'affiche (voir Figure 6-8 à la page 253). Cliquez sur l'onglet Action pour afficher la page de propriétés correspondante (voir Figure 6-12 à la page 259).

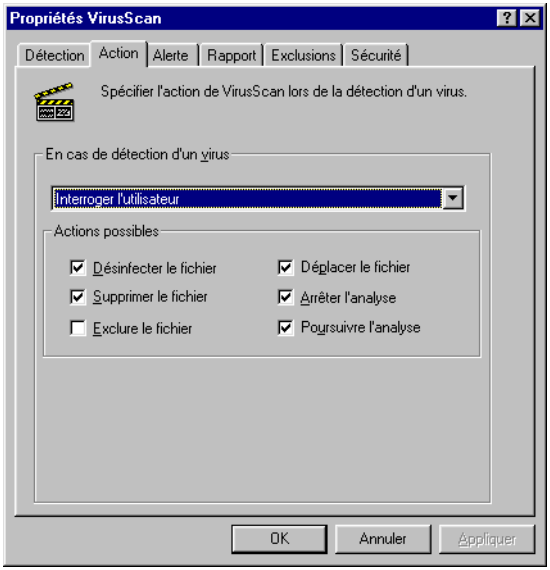

Figure 6-12. Boîte de dialogue Propriétés VirusScan – page Action

3. Sélectionnez une réponse dans la liste **En cas de détection d'un virus**. La zone située juste au-dessous de la liste se modifiera pour vous proposer d'autres options pour chacun de vos choix. Vous avez le choix entre les options suivantes :

   - **Interroger l'utilisateur.** Choisissez cette option de réponse si vous pensez être auprès de votre ordinateur pendant que l'application VirusScan analyse votre disque ; VirusScan affiche un message d'alerte lorsqu'il détecte un virus et vous propose une liste des réponses possibles.

     Pour chaque case que vous cochez dans la page Action, un bouton d'option apparaîtra dans le message d'alerte que l'application affichera en cas de détection d'un virus. Ainsi, si vous cochez par exemple la case **Supprimer le fichier**, le message d'alerte comportera un bouton **Supprimer**. Pour en savoir plus sur les options de réponse en cas d'infection, reportez-vous à la section « Options de réponse lorsque l'application VirusScan détecte un virus » à la page 84.

     Vous avez le choix entre les options suivantes :

     – **Nettoyer le fichier**. Cette option demande à l'application d'essayer de supprimer le code de virus dans le fichier infecté. Si vous avez activé la fonction de rapport, l'application enregistrera l'événement dans un journal à chaque fois qu'elle parviendra ou non à nettoyer un fichier infecté.

     – **Supprimer le fichier**. Cette option demande à l'application de supprimer immédiatement le fichier infecté.

     – **Exclure le fichier**. Cette option demande à l'application d'ignorer ce fichier lors des opérations d'analyse à venir. C'est la seule option qui ne soit pas sélectionnée par défaut.

     – **Poursuivre l'analyse**. Cette option demande à l'application de poursuivre son analyse sans prendre d'autres mesures. Si vous avez activé ses options de rapport, l'application enregistre l'incident dans son fichier journal.

     – **Arrêter l'analyse**. Cette option demande à l'application de cesser immédiatement l'opération d'analyse. Pour continuer, vous devez cliquez sur **Analyser maintenant** afin de relancer l'opération.

     – **Déplacer le fichier**. Cette option demande à l'application de placer le fichier infecté dans un dossier de quarantaine. Le message d'alerte affichera un bouton **Déplacer le fichier** pour vous permettre de localiser le dossier de quarantaine à utiliser.

- **Déplacer automatiquement les fichiers infectés**. Cette option demande à l'application de placer les fichiers infectés dans un dossier de quarantaine.

  Par défaut, l'application place ces fichiers dans un dossier nommé Infecté, situé dans le répertoire du programme VirusScan. Vous pouvez entrer un autre nom de dossier dans la zone de texte affichée ou cliquer sur **Parcourir** pour retrouver le dossier voulu sur votre disque dur.

- **Nettoyer automatiquement les fichiers infectés**. Sélectionnez cette option cette réponse pour que l'application supprime le code de virus dans le fichier infecté dès sa détection. Si l'application ne parvient pas à supprimer le virus, elle notera l'incident dans son fichier journal.

- **Supprimer automatiquement les fichiers infectés** . Sélectionnez cette option pour que l'application supprime immédiatement tout fichier infecté détecté. Assurez-vous d'avoir activé la fonction de rapport afin de disposer d'une liste des fichiers supprimés par l'application. Consultez ensuite cette dernière pour connaître les fichiers supprimés à restaurer à partir des copies de sauvegarde. Si l'application ne parvient pas à supprimer un fichier infecté, elle notera l'incident dans son fichier journal.

- **Poursuivre l'analyse**. N'utilisez cette option que si vous prévoyez d'être absent au moment où l'application recherchera les virus. Si vous activez également la fonction de rapport, l'application enregistrera le nom des virus détectés et le nom des fichiers infectés, pour vous permettre de les supprimer à une prochaine occasion.

4. Cliquez sur l'onglet Alerte pour choisir d'autres options de VirusScan. Pour enregistrer vos modifications sans fermer la boîte de dialogue Propriétés VirusScan, cliquez sur **Appliquer**. Pour enregistrer vos modifications et revenir à la fenêtre de la console, cliquez sur **OK**. Pour revenir à la fenêtre de la console sans enregistrer vos modifications, cliquez sur **Annuler**.

❑ **REMARQUE :** Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

Sélection des options d'alerte

Lorsque vous avez configuré vos options de réponse, vous pouvez laisser l'application VirusScan rechercher et supprimer automatiquement les virus de votre système au fur et à mesure qu'elle les détecte, pratiquement sans aucune autre intervention de votre part. Toutefois, pour que l'application vous informe immédiatement de la détection d'un virus de sorte que vous puissiez entreprendre l'action appropriée, vous devez la configurer pour qu'elle vous envoie un message d'alerte.

Procédez comme suit :

1. Pour démarrer depuis la fenêtre de la console, sélectionnez la tâche que vous avez créée dans la liste des tâches, puis cliquez sur  dans la barre d'outils de la console.

2. La boîte de dialogue Propriétés VirusScan s'affiche (voir Figure 6-8 à la page 253). Cliquez sur l'onglet Alerte pour afficher la page de propriétés correspondante (Figure 6-13).

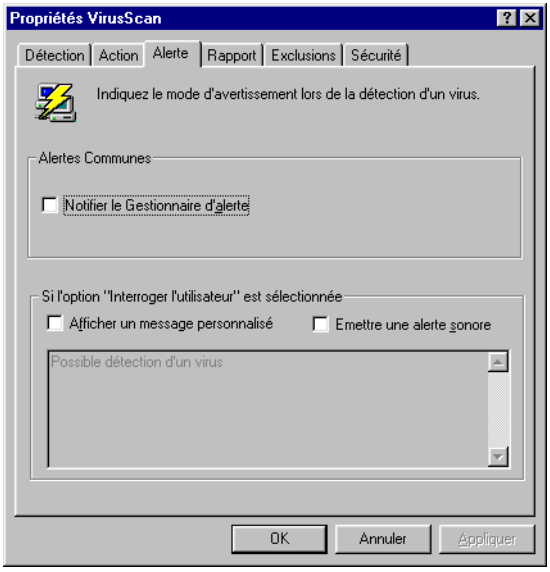

Figure 6-13. Boîte de dialogue Propriétés VirusScan – page Alerte

3. Cochez la case **Notifier le Gestionnaire d'alerte** pour que l'application VirusScan envoie des messages d'alerte au Gestionnaire d'alerte qui les transmettra.

Le Gestionnaire d'alerte est un composant indépendant du logiciel McAfee qui regroupe des messages d'alerte et utilise diverses méthodes pour les envoyer aux destinataires que vous désignez. L'application VirusScan enverra ces messages d'alerte avec succès uniquement si vous avez installé l'utilitaire de Configuration cliente du Gestionnaire d'alerte. Pour plus de détails, reportez-vous à la section Voir « Utilisation de l'utilitaire de Configuration cliente du Gestionnaire d'alerte » à la page 338.

Vous pouvez transmettre des messages d'alerte directement à un serveur du Gestionnaire d'alerte. Sinon, vous pouvez les envoyer en tant que fichiers texte (.ALR) à un répertoire d'alerte centralisée que le serveur du Gestionnaire d'alerte interroge régulièrement.

❑ **REMARQUE :** Si vous décochez cette case, l'application VirusScan n'enverra pas des messages d'alerte via le Gestionnaire d'alerte, mais tous les autres messages d'alerte que vous configurez dans cette page de propriétés resteront intacts.

---

4. Cochez la case **Émettre une alerte sonore** pour que l'application envoie un signal sonore à chaque fois qu'elle trouve un fichier infecté.

   Vous pouvez modifier le paramétrage de cette option à condition d'avoir sélectionné **Interroger l'utilisateur** dans la page de propriétés Action. Sinon, la case à cocher Émettre une alerte sonore affichera et utilisera le paramètre que vous lui avez attribué la dernière fois que vous avez sélectionné l'option **Interroger l'utilisateur**. L'application émettra le signal sonore standard du système ou exécutera le fichier .WAV que vous avez configuré sur votre ordinateur.

5. Cochez la case **Afficher un message personnalisé** pour que l'application ajoute un message personnalisé au texte du message qu'elle affiche lorsqu'elle trouve un fichier infecté.

   À l'égard de l'alerte sonore, vous pouvez modifier le paramétrage de cette option à condition d'avoir sélectionné **Interroger l'utilisateur** dans la page de propriétés Action. Si vous ne sélectionnez pas cette option dans la page Action, aucun message d'alerte ou message personnalisé ne s'affichera même si vous avez coché la case Afficher un message personnalisé.

6. Entrez le message que l'application doit afficher dans la zone de texte. Vous pouvez entrer 250 caractères maximum.

7. Cliquez sur l'onglet Rapport pour choisir d'autres options de VirusScan. Pour enregistrer vos modifications sans fermer la boîte de dialogue Propriétés VirusScan, cliquez sur **Appliquer**. Pour enregistrer vos modifications et revenir à la fenêtre de la console, cliquez sur **OK**. Pour revenir à la fenêtre de la console sans enregistrer vos modifications, cliquez sur **Annuler**.

❑ **REMARQUE :** Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

Sélection des options de rapport

L'application VirusScan liste ses paramètres courants et récapitule toutes les actions qu'elle effectue au cours de ses opérations d'analyse dans un fichier journal appelé VSCLOG.TXT. Ce rapport peut à votre convenance figurer dans ce fichier ou dans un fichier texte que vous aurez créé dans un éditeur de texte quelconque à l'intention de l'application. Vous pouvez ensuite ouvrir et imprimer le fichier journal pour consultation ultérieure, soit depuis l'application VirusScan, soit depuis un éditeur de texte.

Le fichier VSCLOG.TXT est un outil de gestion essentiel pour garder la trace de l'activité virale sur votre système et pour noter les paramétrages que vous utilisez pour détecter et traiter les infections signalées par l'application VirusScan. Vous pouvez également utiliser les rapports d'incidents enregistrés dans le fichier pour déterminer quels fichiers vous devez remplacer à partir de vos sauvegardes, examiner en quarantaine ou supprimer de votre système. Utilisez la page de propriétés Rapport pour déterminer les informations que vous souhaitez inclure dans le fichier journal du logiciel VirusScan.

Pour sélectionner les données que l'application doit enregistrer et définir la taille du fichier journal, procédez comme suit :

1. Pour démarrer depuis la fenêtre de la console, sélectionnez la tâche que vous avez créée dans la liste des tâches, puis cliquez sur  dans la barre d'outils de la console.

2. La boîte de dialogue Propriétés VirusScan s'affiche (voir Figure 6-8 à la page 253). Cliquez sur l'onglet Rapport pour afficher la page de propriétés correspondante (Figure 6-14 à la page 265).

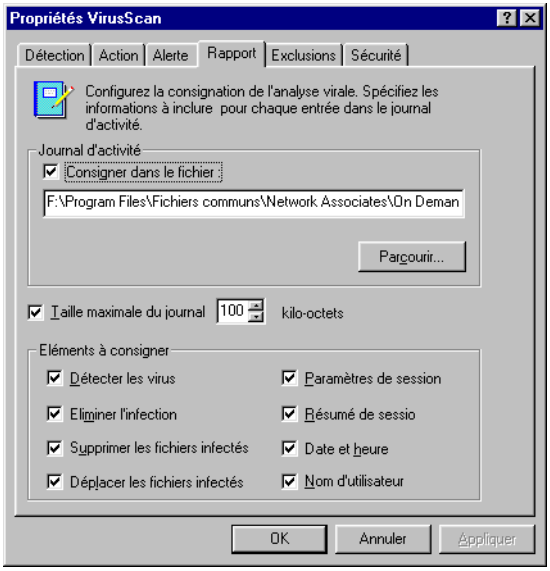

Figure 6-14. Propriétés VirusScan – page Rapport

3. Cochez la case **Consigner dans le fichier**.

   Par défaut, l'application VirusScan enregistre les informations de journal dans le fichier VSCLOG.TXT, situé dans le répertoire du programme VirusScan. Vous pouvez entrer un autre nom de fichier dans la zone de texte affichée, ou cliquer sur **Parcourir** pour trouver un fichier approprié sur votre disque dur ou votre réseau. Vous pouvez utiliser un fichier différent, mais le fichier texte doit être déjà créé. L'application ne crée pas de fichier.

4. Pour limiter la taille du fichier journal, cochez la case **Taille limite du fichier journal**, puis saisissez cette taille, en Kilo-octets, dans la zone de texte prévue à cet effet. Si vous ne cochez pas cette case, le fichier journal peut voir sa taille augmenter et atteindre une limite déterminée par votre espace disque.

   Entrez une valeur comprise entre 10 Ko et 999 Ko. Par défaut, l'application limite la taille du fichier à 100 Ko. Si les données du journal dépassent la taille allouée pour le fichier, l'application efface le journal existant et le reprend au point où il s'était interrompu.

5. Cochez les cases correspondant aux informations que l'application doit enregistrer dans son fichier journal. Chaque case cochée génère l'enregistrement par l'application de l'information correspondante, généralement à la fin de l'opération d'analyse ou lorsque vous arrêtez votre système :

- **Détecter les virus**. Cochez cette case pour que le fichier journal enregistre le nombre de virus trouvés par l'application dans chaque opération d'analyse. Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.
- **Éliminer l'infection**. Cochez cette case pour que le fichier journal enregistre le nombre de fichiers infectés que l'application nettoie (ou tente de nettoyer) au cours de chaque opération d'analyse. Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.
- **Supprimer les fichiers infectés**. Cochez cette case pour que le fichier journal enregistre le nombre de virus supprimés par l'application dans chaque opération d'analyse. Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.
- **Déplacer les fichiers infectés**. Cochez cette case pour que le fichier journal enregistre le nombre de virus que l'application a placé dans un dossier de quarantaine dans chaque opération d'analyse. Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.
- **Paramètres de session**. Cochez cette case pour que le fichier journal enregistre les paramètres de configuration que vous avez utilisés pour l'application dans chaque opération d'analyse. Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.
- **Résumé de session**. Cochez cette case pour que le fichier journal récapitule les actions effectuées par l'application dans chaque opération d'analyse. Le journal enregistrera les informations suivantes :
  - Nombre de fichiers analysés par l'application.
  - Nombre de fichiers infectés nettoyés par l'application.
  - Nombre de fichiers infectés supprimés par l'application.
  - Nombre de fichiers infectés que l'application a placé dans un dossier de quarantaine.
  - Paramètres que vous avez attribués à l'application.

  Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.
- **Date et heure**. Cochez cette case pour que le fichier journal enregistre la date et l'heure de début de chaque session d'analyse. Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.

- **Nom d'utilisateur**. Cochez cette case pour que le fichier journal enregistre le nom de l'utilisateur connecté à la station de travail lorsque le logiciel démarre chaque opération d'analyse. Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.

Pour afficher le contenu du fichier journal depuis la console VirusScan, sélectionnez la tâche que vous avez créée dans la liste des tâches, puis choisissez **Afficher le journal d'activité** dans le menu **Tâche**. Vous pouvez aussi lancer l'application VirusScan et choisir **Afficher le journal d'activité** dans le menu **Fichier**.

6. Cliquez sur l'onglet Exclusion pour choisir d'autres options de VirusScan. Pour enregistrer vos modifications sans fermer la boîte de dialogue Propriétés VirusScan, cliquez sur **Appliquer**. Pour enregistrer vos modifications et revenir à la fenêtre de la console, cliquez sur **OK**. Pour revenir à la fenêtre de la console sans enregistrer vos modifications, cliquez sur **Annuler**.

REMARQUE : Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

Sélection des options d'exclusion

Nombre des fichiers stockés sur votre ordinateur ne risquent pas d'être infectés par des virus. Les opérations d'analyse qui examinent ces fichiers peuvent être longues et ne donner que peu de résultats. Vous pouvez accélérer les opérations d'analyse en demandant à l'application VirusScan de n'inspecter que les types de fichiers susceptibles d'être infectés (voir « Sélection des options de détection » à la page 253), d'ignorer des fichiers ou des dossiers complets dont vous savez qu'ils ne peuvent être infectés.

Après avoir analysé à fond votre système, vous pouvez exclure les fichiers et les dossiers qui ne se modifient jamais ou ne sont pas normalement vulnérables aux infections virales. Vous pouvez aussi compter sur le moteur d'analyse VShield pour vous protéger entre les opérations d'analyse planifiées. Cependant, la meilleure protection contre les virus demeure la régularité des opérations d'analyse examinant tous les secteurs de votre système.

Pour éviter que l'application examine des fichiers qui ne sont pas infectés, vous pouvez indiquer les disques, les dossiers ou les fichiers que vous souhaitez exclure des opérations d'analyse dans une liste d'exclusions Par défaut, l'application VirusScan n'examine pas la Corbeille, car Windows n'exécute pas les éléments qu'elle contient. Par conséquent, cet élément apparaît dans la liste des exclusions la première fois que vous ouvrez la fenêtre.

Chaque entrée de la liste des exclusions affiche le chemin d'accès de l'élément exclu, indique si l'application va exclure également les sous-dossiers contenus dans le dossier de l'élément et précise si l'application va exclure l'élément lors de l'analyse des fichiers, ou lors de l'analyse des zones système de votre disque dur, ou les deux à la fois.

Par défaut, vous pouvez exclure jusqu'à 100 cibles à analyser uniques. Pour modifier ce chiffre, ouvrez le panneau de configuration VirusScan, cliquez sur l'onglet Composants, puis entrez un nouveau chiffre dans la zone de texte **Nombre maximal d'éléments à exclure**. Pour en savoir plus sur l'utilisation du panneau de configuration VirusScan, reportez-vous à la section « Présentation du Panneau de configuration VirusScan » à la page 333.

Pour exclure des opérations d'analyse certains fichiers ou dossiers, procédez comme suit :

1. Pour démarrer depuis la fenêtre de la console, sélectionnez la tâche que vous avez créée dans la liste des tâches, puis cliquez sur  dans la barre d'outils de la console.

2. La boîte de dialogue Propriétés VirusScan s'affiche (voir Figure 6-8 à la page 253). Cliquez sur l'onglet Exclusion pour afficher la page de propriétés correspondante. (Figure 6-15).

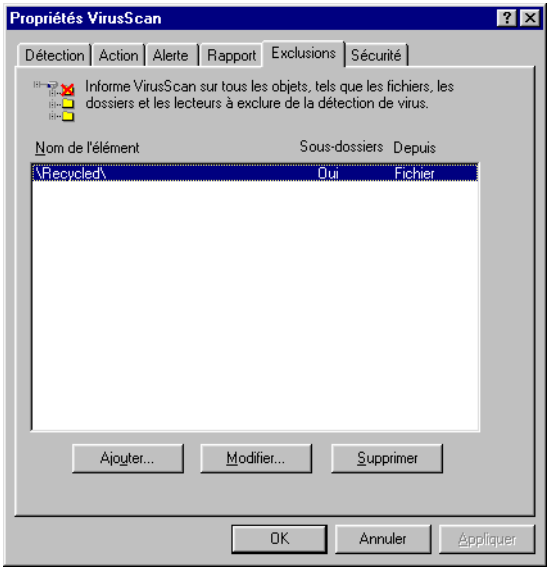

Figure 6-15. Boîte de dialogue Propriétés VirusScan – page Exclusion

3. Spécifiez les éléments que vous souhaitez exclure. Vous pouvez :

   - **Ajouter des fichiers, des dossiers ou des volumes à la liste des exclusions.** Cliquez sur **Ajouter** pour afficher la boîte de dialogue Ajout d'un élément à exclure (Figure 6-16).

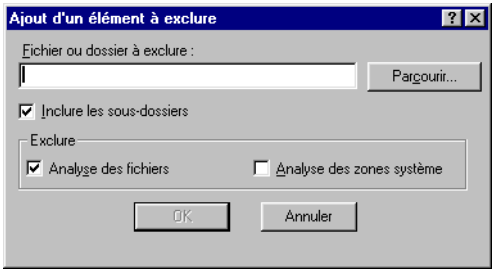

Figure 6-16. Boîte de dialogue Ajout d'un élément à exclure

Pour ajouter un élément à la liste des exclusions, procédez comme suit :

a. Entrez un chemin d'accès à un dossier ou un nom de fichier dans la zone de texte affichée ou cliquez sur **Parcourir** pour trouver l'élément que vous souhaitez exclure de l'analyse.

REMARQUE : Si vous avez choisi de déplacer automatiquement tout fichier infecté vers un dossier de quarantaine, l'application exclut ce dossier des opérations d'analyse.

---

b. Cochez la case **Inclure les sous-dossiers** pour que l'application ignore les fichiers stockés dans les sous-dossiers du dossier que vous avez spécifié dans l'Étape a.

REMARQUE : Lorsque vous sélectionnez l'option **Inclure les sous-dossiers**, l'application n'exclut de l'analyse que les fichiers stockés dans les sous-dossiers. Elle analysera les fichiers stockés à la racine du dossier que vous spécifiez. Pour exclure de l'analyse les fichiers situés à la racine du dossier, décochez la case **Inclure les sous-dossiers**.

---

c. Cochez la case **Analyse des fichiers** pour exclure l'élément que vous avez spécifié dans la première étape lorsque l'application recherche des virus infectant des fichiers. Ces virus apparaissent généralement dans des fichiers stockés dans les parties visibles de votre disque dur.

d. Cochez la case **Analyse des zones système** pour exclure l'élément que vous avez spécifié dans la première étape lorsque le module recherche des virus infectant la zone système.

Ces virus résident souvent dans la mémoire ou dans des fichiers stockés dans la zone système ou dans la partition d'amorçage (MBR) de votre disque dur. Utilisez cette option pour exclure des opérations d'analyse des fichiers système comme COMMAND.COM.

AVERTISSEMENT : McAfee vous recommande de *ne pas* exclure vos fichiers système des opérations d'analyse.

e. Répétez les étapes Étape a. à Étape d. jusqu'à ce que vous ayez listé tous les fichiers et dossiers que vous souhaitez exclure de l'analyse.

- **Modifier la liste des exclusions.** Pour modifier les paramètres d'un élément exclu, sélectionnez-le dans la liste Exclusions, puis cliquez sur **Edition** pour ouvrir la boîte de dialogue Edition d'élément à exclure. Effectuez les modifications voulues, puis cliquez sur **OK** pour fermer la boîte de dialogue.
- **Supprimer un élément de la liste.** Pour supprimer un élément de la liste, sélectionnez-le, puis cliquez sur **Supprimer**. Cela signifie que l'application VirusScan *examinera* ce fichier ou dossier au cours de la prochaine session d'analyse.

4. Cliquez sur l'onglet Sécurité pour choisir d'autres options de VirusScan. Pour enregistrer vos modifications sans fermer la boîte de dialogue Propriétés VirusScan, cliquez sur **Appliquer**. Pour enregistrer vos modifications et revenir à la fenêtre de la console, cliquez sur **OK**. Pour revenir à la fenêtre de la console sans enregistrer vos modifications, cliquez sur **Annuler**.

REMARQUE : Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

Sélection des options de sécurité

Le logiciel VirusScan vous permet de définir un mot de passe pour protéger les paramètres de chaque page de propriétés contre toute modification non autorisée. Cette fonction se révèle particulièrement utile pour les administrateurs système qui doivent empêcher les utilisateurs de tricher avec les mesures de sécurité en modifiant les paramètres de VirusScan. Utilisez la page de propriétés Sécurité pour verrouiller vos paramètres.

Vous pouvez aussi protéger simultanément tous les paramètres de cette tâche sans avoir à sélectionner les pages individuellement. Pour ce faire, sélectionnez la tâche dans la fenêtre de la console, puis choisissez **Tâche de protection du mot de passe** dans le menu **Tâche**.

Vous pouvez également double-cliquer sur la tâche pour ouvrir la boîte de dialogue Propriétés des tâches. Vous pouvez ensuite cocher la case **Protection de cette tâche par mot de passe**, puis cliquer sur **Mot de passe** pour attribuer un mot de passe. Entrez le mot de passe, puis cochez la case **Protéger toutes les options** pour protéger simultanément toutes les pages de propriétés de l'application VirusScan.

Pour protéger individuellement les paramètres de la tâche, procédez comme suit :

1. Pour démarrer depuis la fenêtre de la console, sélectionnez la tâche que vous avez créée dans la liste des tâches, puis cliquez sur  dans la barre d'outils de la console.

2. La boîte de dialogue Propriétés VirusScan s'affiche (voir Figure 6-8 à la page 253). Cliquez sur l'onglet Sécurité pour afficher la page de propriétés correspondante. (voir Figure 6-17 à la page 271).

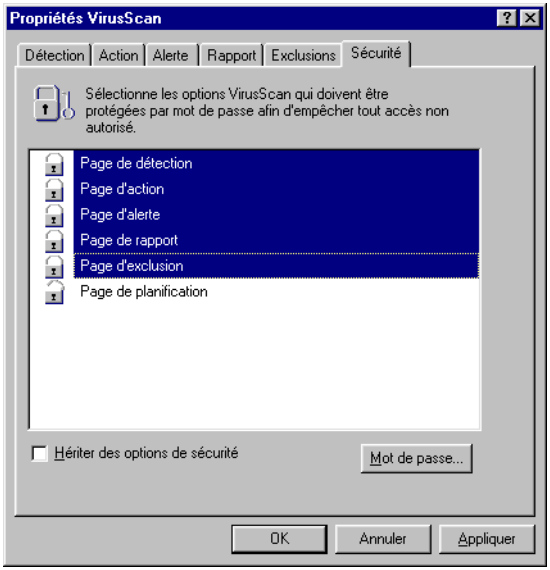

Figure 6-17. Boîte de dialogue Propriétés VirusScan – page Sécurité

3. Sélectionnez les paramètres que vous souhaitez protéger dans la liste affichée.

Vous pouvez protéger les pages de propriétés de VirusScan individuellement ou dans leur ensemble. Dans la liste illustrée par la Figure 6-17 à la page 271, les noms des pages de propriétés verrouillées sont assortis d'une icône représentant un verrou fermé . Pour désactiver la protection d'une page de propriétés, cliquez sur le verrou fermé pour qu'il s'ouvre .

4. Cliquez sur **Mot de passe** pour ouvrir la boîte de dialogue Spécification du mot de passe (Figure 6-18).

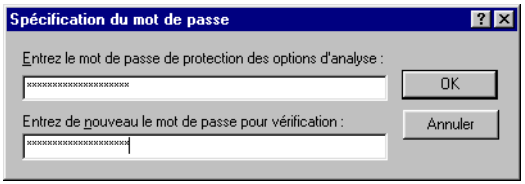

Figure 6-18. Boîte de dialogue Spécification du mot de passe

   a. Entrez un mot de passe dans la première zone de texte affichée, puis entrez-le de nouveau dans la zone de texte située au-dessous pour le confirmer.

   b. Cliquez sur **OK** pour fermer la boîte de dialogue Spécification du mot de passe.

5. Pour vous assurer que vos paramètres de sécurité se recopieront par défaut dans toute nouvelle tâche que vous créez en copiant cette tâche (voir « Utilisation de la fenêtre de la console » à la page 235), cochez la case **Hériter des options de sécurité**.

6. Cliquez sur un autre onglet pour modifier l'un ou l'autre des paramètres de VirusScan. Pour enregistrer vos modifications sans fermer la boîte de dialogue Propriétés VirusScan, cliquez sur **Appliquer**. Pour enregistrer vos modifications et revenir à la fenêtre de la console, cliquez sur **OK**. Pour revenir à la fenêtre de la console sans enregistrer vos modifications, cliquez sur **Annuler**.

❑ **REMARQUE :** Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

Mise à jour et mise à niveau du logiciel VirusScan 7

Développement d'une stratégie de mise à jour

Même s'ils sont qualifiés de vandales électroniques, certains concepteurs de virus effectuent des recherches approfondies et exécutent un travail « soigné ». Ils cherchent à introduire de nouvelles difficultés techniques ou des stratégies d'attaque innovatrices dans leurs créations et son très fiers de leur succès. Malheureusement, ce succès se traduit souvent par la perte de données, par l'instabilité du système ou par d'autres effets néfastes pour vous. Pour contrer ces menaces, les chercheurs du groupe AVERT (Anti-Virus Emergency Response Team) de McAfee éditent régulièrement des mises à jour de la base de données de définitions de virus et des améliorations ou des mises à niveau du moteur d'analyse utilisé par le logiciel VirusScan. Sans ces mises à jour, le logiciel VirusScan risque de ne pas reconnaître de nouvelles formes de logiciels nocifs ou de ne pas détecter de nouvelles souches de virus lorsqu'il est en leur présence.

Qu'est-ce qu'un fichier .DAT ?

Les fichiers de définition de virus, ou fichiers .DAT, contiennent des signatures de virus actualisées et autres informations utilisées par les produits antivirus McAfee pour protéger votre ordinateur contre les milliers de virus informatiques qui circulent actuellement. McAfee publie de nouveaux fichiers .DAT chaque semaine afin de vous garantir une protection optimale contre 300 nouveaux virus environ qui apparaissent chaque mois.

Avec cette version de VirusScan, McAfee a introduit une nouvelle technologie incrémentielle (.DAT ou iDAT) basée sur de petits kits contenant uniquement les définitions de virus qui ont été modifiées entre les versions de fichier .DAT hebdomadaires et *non* la totalité du jeu de fichiers .DAT. Grâce à cette innovation, vous pouvez télécharger des mises à jour des fichiers .DAT à une vitesse beaucoup plus élevée et au moindre coût en matière de bande passante. Pour en savoir plus sur cette nouvelle technologie, reportez-vous à l'Annexe D, « Description de la technologie iDAT ».

Qu'est-ce que le moteur d'analyse ?

Le moteur d'analyse Olympus est situé au cœur du logiciel antivirus McAfee. Le moteur contient la logique du programme requise pour analyser les fichiers à des endroits spécifiques, traiter et comparer les définitions de virus avec les données de vos fichiers, décrypter et exécuter le code de virus dans un environnement similaire, appliquer des techniques heuristiques pour reconnaître les nouveaux virus et supprimer le code infectieux de vos fichiers.

Les autres composants du kit VirusScan fournissent des fichiers au moteur pour traitement, se greffent dans différentes parties du système d'exploitation de votre ordinateur afin d'intercepter les fichiers lors de leur exécution ou de leur utilisation, et fournissent une interface qui vous permet de configurer divers paramètres d'analyse.

Méthodes de mise à jour et de mise à niveau

Les fichiers .DAT et les fichiers programme actualisés étant la clé d'une protection antivirus totale, McAfee a incorporé diverses options de mise à jour dans le kit du produit VirusScan. Ce sont :

- **Diffusions du service SecureCast.** Le service SecureCast de McAfee utilise la technologie « push » BackWeb pour envoyer automatiquement des mises à jour de fichier .DAT, des mises à niveau du produit, des alertes au virus et autres éléments utiles aux abonnés. McAfee recommande d'utiliser conjointement ce service et le mécanisme fourni dans le logiciel VirusScan pour effectuer la mise à jour et la mise à niveau du logiciel. Pour en savoir plus sur le service SecureCast, reportez-vous à l'Annexe C, « Utilisation du service SecureCast pour obtenir de nouveaux fichiers de données ».
- **Opérations d'actualisation et de mise à niveau automatiques planifiées**. Le logiciel VirusScan inclut deux utilitaires qui vous permettent de planifier régulièrement des mises à jour de fichier .DAT et des mises à niveau du produit directement depuis la console VirusScan : AutoUpdate et AutoUpgrade. McAfee vous recommande d'utiliser ces utilitaires en priorité pour mettre à jour ou mettre à niveau votre logiciel sur les stations de travail de votre réseau. Pour ce faire, vous devez auparavant télécharger vos fichiers depuis le site Web de McAfee ou vous le procurer par le biais du service SecureCast. Pour en savoir plus sur ces utilitaires, reportez-vous aux sections « Description de l'utilitaire AutoUpdate » à la page 277 et « Description de l'utilitaire AutoUpgrade » à la page 289.
- **Mises à jour incrémentielles des fichiers .DAT**. La nouvelle technologie iDAT de McAfee fonctionne de manière transparente avec la version de AutoUpdate fournie. Les nouveaux fichiers iDAT se composent de kits .UPD et d'un fichier DELTA.INI qui identifie les modifications intervenues entre deux versions de fichier .DAT hebdomadaires. L'utilitaire AutoUpdate utilise le fichier DELTA.INI pour déterminer les fichiers à télécharger et à installer.

Par défaut, l'utilitaire AutoUpdate téléchargera les fichiers iDAT, sauf si les fichiers .DAT ou le moteur d'analyse installés sur votre ordinateur sont trop anciens. Dans ce cas, l'utilitaire télécharge et installe automatiquement la totalité du kit .DAT. Vous n'avez pas besoin de configurer l'utilitaire à cet effet, car il est capable d'identifier la route la plus appropriée en fonction des éléments installés sur votre ordinateur. Pour en savoir plus sur le fonctionnement des fichiers iDAT, reportez-vous à l'Annexe D, « Description de la technologie iDAT ».

- **Moteur d'analyse SuperDAT et mises à jour du fichier .DAT**. McAfee publie un kit SuperDAT hebdomadaire avec des mises à jour du fichier .DAT et un moteur d'analyse Olympus actualisés, accompagnés d'une fonction d'installation très rapide.

  Grâce à l'utilitaire SuperDAT, vous n'avez plus besoin de déployer des logiciels complexes à chaque fois que vous recevez des composants de mise à niveau. SuperDAT commence par arrêter toute opération d'analyse, tout service ou tout autre composant logiciel résidant en mémoire en cours d'exécution et susceptible d'interférer avec vos opérations de mise à jour, puis il copie les nouveaux fichiers aux emplacements adéquats et les met immédiatement à la disposition du logiciel.

  La version actuelle de VirusScan peut télécharger et installer de nouveaux fichiers .DAT et de nouveaux fichiers de moteur d'analyse depuis un kit SuperDAT. Vous pouvez les installer sur n'importe quelle plate-forme Windows prise en charge et sans avoir à redémarrer votre ordinateur. Vous pouvez télécharger et exécuter les kits SuperDAT séparément pour mettre à jour et mettre à niveau votre logiciel ou vous pouvez utiliser l'utilitaire SuperDAT en association avec l'utilitaire AutoUpgrade pour accroître le degré d'automatisation de vos mises à jour. Pour en savoir plus sur la façon de combiner les deux utilitaires, reportez-vous à la section « Utilisation conjointe des utilitaires AutoUpgrade et SuperDAT » à la page 300.

  En plus du kit SuperDAT hebdomadaire contenant à la fois des fichiers .DAT courants et un moteur d'analyse Olympus actualisé, McAfee mettra à votre disposition un kit SuperDAT qui contiendra uniquement des fichiers .DAT. Grâce à ce fichier exécutable, vous n'aurez plus besoin de gérer de près les mises à jour des fichiers .DAT. Il commence par arrêter toute opération d'analyse, tout service et tout composant logiciel résident en mémoire en cours d'exécution, susceptible d'interférer avec vos opérations de mise à jour. Puis, il copie les nouveaux fichiers aux emplacements adéquats et met immédiatement les fichiers à la disposition du logiciel.

- **Kits de mise à jour des fichiers .DAT**. McAfee publie également un kit de fichiers .DAT autonome hebdomadaire, que vous pouvez télécharger, extraire et copier sur le répertoire de votre logiciel. Un kit .DAT est composé d'un fichier d'archives .ZIP nommé DAT-XXXX.ZIP. Le XXXX dans le nom de fichier est un numéro de série qui change à chaque création d'un fichier .DAT. McAfee vous recommande de ne pas utiliser cette méthode pour mettre à jour votre logiciel, mais vous pouvez le faire, si nécessaire. Pour en savoir plus sur l'utilisation de ces kits pour vos mises à jour, lisez le fichier README.TXT qui accompagne chaque kit hebdomadaire.

- **Fichiers EXTRA.DAT**. Les mises à jour régulières du fichier de définition de virus (.DAT) fournies par Network Associates vous offrent une protection optimale contre les nouveaux codes nuisibles et contre ceux qui ont été déjà identifiés. Même les versions hebdomadaires du fichier .DAT ne peuvent pas toujours vous protéger contre une attaque virale rapide, notamment dans le cas d'un virus de messagerie électronique, tel que le virus W97M / MELISSA.

  Le logiciel antivirus de Network Associates anticipe ce type de situation. Il vous permet de profiter des capacités du moteur d'analyse Olympus pour déployer un petit fichier de définition de virus supplémentaire entre deux versions du fichier .DAT. Ce petit fichier EXTRA.DAT contient les toutes dernières signatures de virus disponibles pour les virus qualifiés par les chercheurs du centre AVERT de Network Associates comme des agents contaminants à haut risque.

  Ce fichier peut vous aider à identifier plusieurs virus simultanément mais, dans la mesure où les chercheurs du centre AVERT publient généralement un fichier EXTRA.DAT dès qu'ils identifient un virus à haut risque, ce fichier cible souvent un ou deux agents les plus courants. Si une série de virus à haut risque apparaît entre deux versions de fichier.DAT, les chercheurs du centre AVERT peuvent publier la série de fichiers EXTRA.DAT correspondante.

- **Fichiers .DAT de secours**. Le logiciel VirusScan inclut l'utilitaire Disquette de secours qui vous permet de créer une disquette amorçable pour démarrer votre ordinateur dans un environnement exempt de virus. La disquette de secours que vous créez utilise des fichiers .DAT spécialisés destinés spécifiquement aux virus de la zone système et aux virus résidant en mémoire, car ils représentent la plus grande menace d'infection lorsqu'ils parviennent à s'activer avant l'exécution de votre logiciel antivirus. Vous pouvez télécharger des mises à jour de ces fichiers directement du site Web du centre AVERT à l'adresse suivante :

  http://www.nai.com/asp_set/anti_virus/updates/virus_4e.asp

McAfee vous recommande de télécharger ces fichiers directement sur un ordinateur exempt de virus, puis de les extraire dans une disquette de secours que vous venez de créer. Pour en savoir plus sur la création d'une disquette de secours, reportez-vous à la section « Utilisation de l'utilitaire de création d'une disquette de secours » à la page 59. Pour en savoir plus sur l'utilisation de la disquette de secours pour analyser votre système, reportez-vous à la section « Si vous suspectez la présence d'un virus... » à la page 71.

Description de l'utilitaire AutoUpdate

L'utilitaire AutoUpdate est la principale méthode recommandée par McAfee pour mettre à jour vos fichiers .DAT. L'utilitaire s'exécute exclusivement en tant que tâche depuis la console VirusScan. Pour mettre à jour votre logiciel VirusScan à l'aide de l'utilitaire, vous devez :

- Définir un calendrier pour la tâche AutoUpdate et l'activer en vue de son exécution
- Définir un mot de passe pour protéger vos paramètres de configuration (facultatif)
- Configurer la tâche pour télécharger les nouveaux fichiers depuis un emplacement spécifique de votre réseau, ou sur Internet

Par défaut, la tâche AutoUpdate incluse dans la console VirusScan est fournie configurée pour télécharger les mises à jour les plus récentes des fichiers .DAT directement depuis le site FTP de Network Associates. Cette configuration rend l'administration plus simple et directe pour les petits réseaux ou les installations individuelles de VirusScan. Cependant, si vous disposez d'un réseau de grande envergure, elle peut affecter de façon significative la bande passante extérieure de votre système si, comme cela arrivera en laissant active la configuration par défaut, chaque nœud du réseau tente de mettre à jour ses fichiers .DAT en même temps.

À la place, McAfee vous recommande d'utiliser AutoUpdate avec Enterprise SecureCast, son canal associé, dans un montage symétrique « push-pull » efficace. Une fois que vous aurez installé le logiciel client sur le serveur d'administration, le service SecureCast sera en mesure de vous envoyer ou d'expédier des fichiers actualisés de façon automatique dès que McAfee les aura mis à la disposition des utilisateurs sur ses serveurs Pour en savoir plus sur le service SecureCast, reportez-vous à l'Annexe C, « Utilisation du service SecureCast pour obtenir de nouveaux fichiers de données ». ou visitez le site Web de Network Associates à l'adresse suivante :

http://www.nai.com/asp_set/anti_virus/alerts/enterprise.asp

Si vous fournissez alors ces fichiers actualisés à un ou plusieurs serveurs centraux de votre réseau et configurez les nœuds de réseau restants pour qu'ils les chargent depuis ces serveurs, vous pouvez

- Planifier le retrait des fichiers .DAT sur l'ensemble du réseau aux heures qui vous conviennent et avec une intervention minimale des administrateurs ou des utilisateurs du réseau. Utilisez la boîte de dialogue Propriétés de la tâche AutoUpdate pour déterminer le moment où chaque nœud de réseau consultera le serveur pour charger des fichiers actualisés.

  Spécifier par exemple une heure de mise à jour qui vous convienne la première fois que vous utilisez le logiciel VirusScan, mais paramétrer l'utilitaire AutoUpdate pour qu'il se déclenche à n'importe quel moment dans l'intervalle de 60 minutes qui suit, ou fixer un calendrier prévoyant que les différents éléments du réseau chargent les mises à jours des fichiers .DAT en même temps ou à tour de rôle. Pour en savoir plus sur la planification de la tâche AutoUpdate ou des autres tâches, reportez-vous à la section « Activation des tâches » à la page 247.
- Partager les devoirs d'administration des retraits entre différents serveurs ou contrôleurs de domaine, entre différentes zones des réseaux étendus ou entre d'autres parties de réseau. Conserver en priorité à un niveau interne le trafic de mise à jour peut également limiter les possibilités de violation de la sécurité du réseau.
- Réduire l'attente éventuelle pour télécharger de nouveaux fichiers .DAT. Le trafic sur les serveurs McAfee est susceptible d'augmenter considérablement aux dates régulières de publication des fichiers .DAT. Éviter la saturation de la bande passante du réseau vous permet d'utiliser votre mise à jour avec un minimum d'interruptions.

D'autres options avancées de AutoUpdate vous permettent de sauvegarder les fichiers .DAT existants, d'installer la mise à jour des fichiers .DAT, de redémarrer le cas échéant le système mis à jour ou d'exécuter des programmes particuliers une fois les mises à jour achevées.

Configuration de l'utilitaire AutoUpdate

Pour configurer l'utilitaire AutoUpdate de sorte qu'il exécute correctement une tâche depuis la console VirusScan, vous devez lui fournir les informations suivantes :

- les sites de mise à jour qui possèdent les nouveaux fichiers que vous souhaitez télécharger ;
- la méthode de transfert que vous souhaitez utiliser pour le téléchargement ;
- si vous utilisez un serveur proxy et, le cas échéant, le port que vous lui avez attribué ;
- si vous souhaitez qu'il sauvegarde vos fichiers .DAT existants ;
- ce qu'il doit faire avec les fichiers téléchargés ; les installer, les enregistrer pour une utilisation ultérieure ou les deux à la fois ;

- ce qu'il doit faire après avoir téléchargé les fichiers ; forcer une mise à jour, réinitialiser le système ou exécuter un programme après une mise à jour ;
- si vous souhaitez conserver une trace de ses actions dans un fichier journal.

Les pages de propriétés de la boîte de dialogue Propriétés de la mise à jour automatique contrôlent les options de votre tâche de mise à jour. Vous pouvez alors cliquer sur chacun des onglets pour configurer cette tâche.

Pour afficher la boîte de dialogue Actualisation automatique, procédez comme suit :

1. Double-cliquez sur la tâche **AutoUpdate** dans la liste des tâches de la console pour ouvrir la boîte de dialogue Propriétés des tâches (voir Figure 6-4 à la page 241).

   Pour en savoir plus sur la définition d'un mot de passe pour cette tâche, reportez-vous à la section « Exécution des tâches AutoUpgrade et AutoUpdate » à la page 241. Pour en savoir plus sur la planification d'une tâche, reportez-vous à la section « Activation des tâches » à la page 247.

2. Cliquez sur **Configurer**.

   La boîte de dialogue Actualisation automatique s'affiche avec la page de propriétés Sites de mise à jour sélectionnée (voir Figure 7-1 à la page 279).

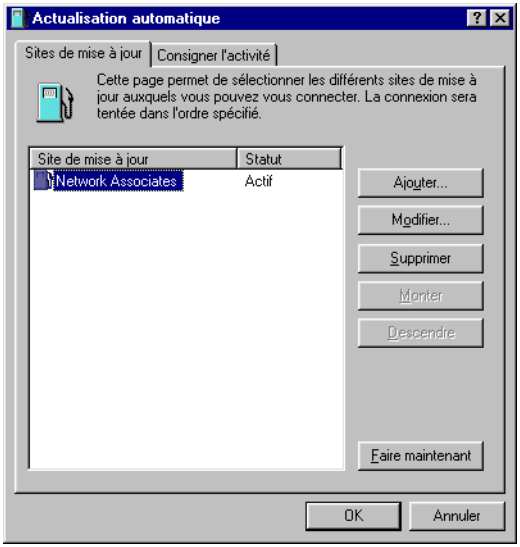

Figure 7-1. Boîte de dialogue Actualisation automatique – page Sites de mise à jour

L'utilitaire AutoUpdate répertorie dans cette boîte de dialogue les sites à partir desquels il téléchargera les nouveaux fichiers .DAT. Il indique également l'état actuel de chaque site par la mention Activé ou Désactivé. Un site est activé si vous avez coché la case **Activé** dans la boîte de dialogue Propriétés de la mise à jour automatique. Il est désactivé si la case n'est pas cochée. Cette désignation n'a aucune influence sur les possibilités de l'utilitaire AutoUpdate de se connecter au site.

L'utilitaire AutoUpdate est fourni au départ avec une configuration qui ne lui permet de se connecter qu'au site FTP de Network Associates. Vous pouvez, à partir de la boîte de dialogue, ajouter autant de sites qui vous sont nécessaires et modifier l'ordre suivant lequel AutoUpdate tente de s'y connecter. L'utilitaire tentera de se connecter successivement à chaque site, en commençant par le début de la liste et jusqu'à ce qu'il parvienne à télécharger les nouveaux fichiers avec succès ou à déterminer qu'il n'y a aucun nouveau fichier disponible.

3. À partir d'ici, vous pouvez :

   - Ajouter un nouveau site. Cliquez sur **Ajouter** pour ouvrir la boîte de dialogue Propriétés de la mise à jour automatique (Figure 7-2 à la page 280). Pour en savoir plus sur la spécification des options pour votre site, reportez-vous à la section « Configuration des options de mise à jour » à la page 283.

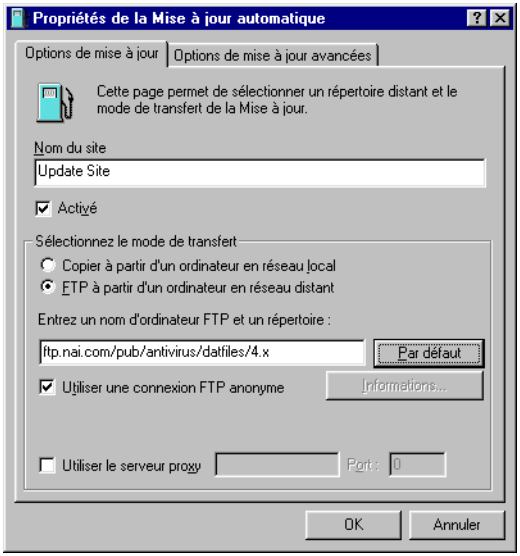

Figure 7-2. Boîte de dialogue Propriétés de la mise à jour automatique – page Options de mise à jour

- Modifier les options définies pour un site de mise à jour existant. Sélectionnez un site dans la liste des sites de mise à jour, puis cliquez sur **Edition** pour ouvrir la boîte de dialogue Propriétés de la mise à jour automatique (Figure 7-2). Procédez à vos modifications, puis cliquez sur **OK** pour les enregistrer et revenir à cette boîte de dialogue. Pour consulter des descriptions et des instructions concernant la configuration des options disponibles, reportez-vous à la section « Configuration des options de mise à jour » à la page 283.

- Supprimer un site existant de la liste des sites de mise à jour. Sélectionnez un site dans la liste des sites de mise à jour, puis cliquez sur **Supprimer**.

- Spécifier l'ordre suivant lequel l'utilitaire AutoUpdate doit se connecter aux sites répertoriés. Pour faire monter un site dans la liste, sélectionnez-le et cliquez sur **Monter**. Pour faire descendre un site dans la liste, sélectionnez-le et cliquez sur **Descendre**.

- Mettre immédiatement à jour vos fichiers à partir des sites répertoriés dans la liste de mise à jour, en utilisant les options de configuration par défaut ou les options que vous avez choisies pour cette tâche. Cliquez sur **Mettre à jour maintenant**.

  Pour utiliser cette fonction, vous devez configurer un nombre suffisant d'options nécessaires à l'utilitaire AutoUpdate pour localiser le site répertorié et, le cas échéant, s'y connecter. Pour en savoir plus sur la spécification des options dont vous avez besoin, reportez-vous à la section « Configuration des options de mise à jour » à la page 283.

  Si au bout de trois tentatives l'utilitaire AutoUpdate n'est pas en mesure de se connecter au site de la liste, ou s'il ne trouve pas de nouveaux fichiers .DAT, il se connecte à chacun des autres sites de la liste jusqu'à ce qu'il localise les fichiers .DAT les plus récents.

  Si vous avez sélectionné l'option **Forcer la mise à jour**, l'utilitaire AutoUpdate télécharge tous les fichiers .DAT qu'il trouve sur le premier site auquel il est parvenu à se connecter. Pour plus de détails, reportez-vous à la section « Configuration des options de mise à jour avancées » à la page 286.

4. Cliquez sur l'onglet Consigner l'activité pour afficher la prochaine page des propriétés (Figure 7-3 à la page 282).

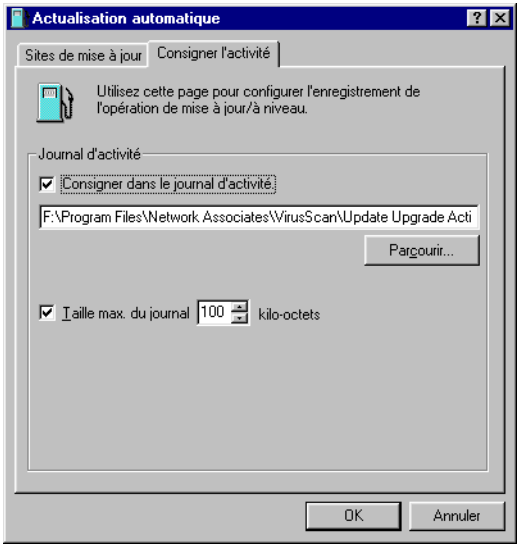

Figure 7-3. Boîte de dialogue Actualisation automatique – page Consigner l'activité

5. Cochez la case **Consigner les activités dans le journal d'activité**.

   Par défaut, l'utilitaire AutoUpdate enregistre les événements qui se sont déroulés lors des tentatives de mise à jour et les enregistre dans le fichier UPDATE UPGRADE ACTIVITY LOG.TXT, situé dans le répertoire du programme VirusScan, à chaque fois que vous arrêtez la tâche ou l'ordinateur.

   Si vous préférez enregistrer ces données dans un fichier texte différent, entrez son chemin d'accès et son nom dans la zone de texte prévue à cet effet ou cliquez sur **Parcourir** pour localiser le fichier. L'utilitaire AutoUpdate ne génère pas de fichier texte, il peut uniquement écrire dans un fichier existant.

6. Pour réduire la taille du fichier journal, cochez la case **Taille maximale du journal**. Cliquez ensuite sur pour définir une taille ou entrez une valeur comprise entre 10 Ko et 999 Ko. Par défaut, l'utilitaire AutoUpdate limite la taille du fichier à 100 Ko.

   Si vous décochez cette case, le fichier journal peut voir sa taille augmenter jusqu'à une limite déterminée par l'espace disque ou par le système de fichiers. Si le fichier atteint la taille maximale allouée, l'utilitaire AutoUpdate efface ce fichier et démarre le journal au point où il s'était interrompu.

Pour afficher le contenu du fichier journal depuis la console VirusScan, sélectionnez la tâche AutoUpdate dans la liste des tâches, puis choisissez **Afficher le journal d'activité** dans le menu **Tâche**.

7. Cliquez sur **OK** pour enregistrer vos modifications et fermer la boîte de dialogue Actualisation automatique. Cliquez sur **Annuler** pour fermer la boîte de dialogue sans enregistrer vos modifications.

Configuration des options de mise à jour

Pour créer un nouveau site de mise à jour ou changer les paramètres d'un site existant, cliquez sur **Ajouter** dans la boîte de dialogue Actualisation automatique (voir Figure 7-1 à la page 279), ou sélectionnez un site de la liste, puis cliquez sur **Edition**. Les deux méthodes affichent la boîte de dialogue Propriétés de la mise à jour automatique (Figure 7-4).

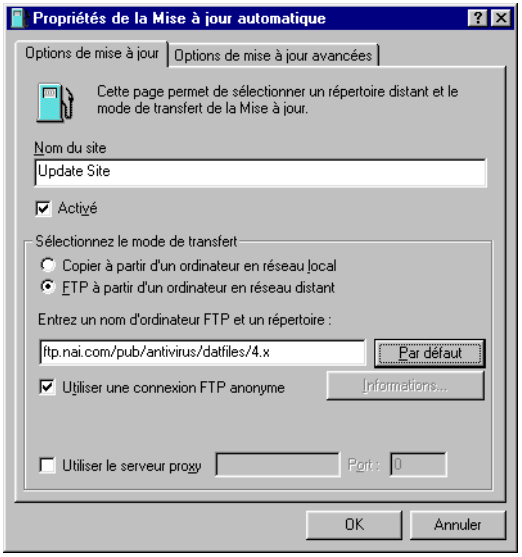

Figure 7-4. Boîte de dialogue Propriétés de la mise à jour automatique – page Options de mise à jour

Ensuite, procédez comme suit :

1. Entrez un nom descriptif permettant d'identifier clairement le site dans la zone de texte Nom du site.

   Tapez par exemple `Site de mise à jour interne du fichier DAT`.

2. Cochez la case **Activé** pour que le site puisse être utilisé par l'utilitaire AutoUpdate.

Si vous décochez cette case, vous conservez les options choisies, mais l'utilitaire ignorera ce site lorsqu'il tentera de télécharger les nouveaux fichiers .DAT.

L'utilitaire AutoUpdate fera trois tentatives de connexion au maximum au cours de chaque opération de mise à jour planifiée. Lorsqu'il parvient à se connecter et à télécharger le nouveau kit de fichiers .DAT, l'utilitaire procède également à l'extraction des fichiers et à leur installation dans le répertoire approprié.

3. Spécifiez la méthode de transfert que vous souhaitez utiliser pour télécharger les nouveaux fichiers. Vous avez le choix entre les options suivantes :

   - **Copier à partir d'un ordinateur en réseau local**. Cliquez sur ce bouton si vous souhaitez que l'utilitaire AutoUpdate utilise une configuration de réseau standard pour rechercher les nouveaux fichiers sur votre ordinateur local ou sur un autre ordinateur du réseau. Vos paramètres de réseau contrôlent la façon dont l'utilitaire tente de se connecter et l'intervalle de temps qui doit s'écouler avant qu'il ne cesse ses tentatives.

     Utilisez ensuite la notation de la convention d'affectation des noms (UNC) pour spécifier, dans la zone de texte Sélectionnez un ordinateur et un répertoire, le chemin d'accès de l'ordinateur qui héberge les nouveaux fichiers que vous souhaitez télécharger. Vous pouvez également cliquer sur **Parcourir** pour localiser le répertoire approprié.

     Pour utiliser la notation UNC, vous devez, soit utiliser le même compte que vous avez utilisé pour ouvrir une session sur le réseau, soit spécifier un nom d'utilisateur et un mot de passe pour vous y connecter. Pour utiliser le compte courant, cochez la case **Utiliser un compte connecté**.

     REMARQUE : Le fait d'activer cette option peut avoir des effets légèrement différents selon que vous utilisiez le système Windows NT Workstation v4.0 ou le système Windows 2000 Professionnel. Si vous avez planifié la mise à jour de vos fichiers, l'utilitaire AutoUpdate utilisera son propre compte de service pour se connecter au serveur de mise à niveau et télécharger les nouveaux fichiers. Si vous cliquez sur **Mettre à jour maintenant**, l'utilitaire AutoUpdate utilisera le même compte que vous avez utilisé pour vous ouvrir une session sur le réseau et vous connecter au serveur de mise à niveau.

Pour utiliser un compte personnalisé, décochez la case **Utiliser un compte connecté** et cliquez sur **Informations sur la connexion UNC** pour entrer un nom d'utilisateur et un mot de passe pour un compte disposant de droits d'accès pour ce serveur cible.

- **FTP depuis un ordinateur en réseau distant**. Cliquez sur ce bouton si vous souhaitez que l'utilitaire AutoUpdate recherche les nouveaux fichiers sur un site FTP que vous désignez. Pour utiliser cette option, le serveur cible doit posséder un service FTP actif.

  Par défaut, l'utilitaire télécharge les nouveaux fichiers depuis le site FTP de Network Associates, qui accepte les connexions FTP anonymes. Vous pouvez cliquer sur **Par défaut** pour spécifier ce site à tout moment.

  L'utilitaire AutoUpdate utilise sa propre implémentation FTP pour se connecter au serveur, cependant l'intervalle de temps après lequel les tentatives seront abandonnées dépendra de vos paramètres de protocole réseau existants.

  Pour utiliser un autre site FTP, entrez l'URL du site que vous souhaitez utiliser dans la zone de texte Entrez un nom d'ordinateur FTP et un répertoire. Vous devez vous connecter à un site configuré pour les connexions FTP anonymes ou désigner le nom d'utilisateur et le mot de passe d'un compte existant sur le site.

  Pour que l'utilitaire utilise une connexion anonyme, cochez la case **Utiliser une connexion FTP anonyme**.

  Pour spécifier un compte, décochez la case **Utiliser une connexion FTP anonyme** et cliquez sur **Informations…** pour entrer un nom d'utilisateur et un mot de passe pour un compte disposant de droits d'accès pour ce serveur cible.

  Si votre serveur utilise un serveur proxy, cochez la case **Utiliser le serveur proxy**, puis entrez le nom du serveur et le port logique qu'il utilise dans les zones de texte fournies à cet effet. Vous pouvez saisir le nom avec la notation UNC ou sous la forme d'un nom de domaine, en fonction de ce qui est adapté à votre environnement.

REMARQUE : L'utilitaire AutoUpdate n'autorise pas les connexions à un serveur proxy qui nécessitent une authentification de proxy de stimulation / réponse.

Configuration des options de mise à jour avancées

Pour exécuter votre tâche AutoUpdate, vous ne devez saisir qu'un serveur cible, une méthode de connexion et toutes les informations nécessaires à la connexion. Puis, lorsque vous aurez activé la tâche et fixé un calendrier pour son exécution, l'utilitaire AutoUpdate procédera pour vous au téléchargement des fichiers appropriés depuis le serveur cible, à leur extraction des archives .ZIP et à leur installation dans le répertoire du programme VirusScan.

Pour que l'utilitaire AutoUpdate effectue des opérations supplémentaires postérieures ou antérieures sur les fichiers, ou pour qu'il procède à d'autres actions, cliquez sur l'onglet Options de mise à jour avancées pour afficher la page de propriétés illustrée dans la (Figure 7-5).

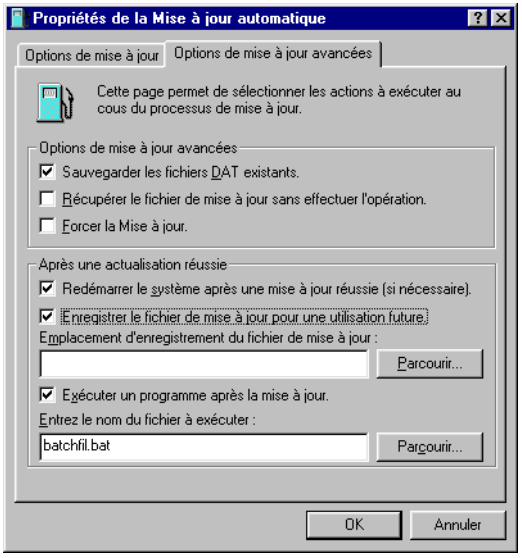

Figure 7-5. Boîte de dialogue Propriétés de la mise à jour automatique – page Options de mise à jour avancées

---

Ensuite, procédez comme suit :

1. Précisez à l'utilitaire AutoUpdate ce que vous souhaitez qu'il fasse avant ou pendant l'exécution d'une mise à jour. Vous avez le choix entre les options suivantes :

   - **Sauvegarder les fichiers .DAT existants.** Cochez cette case pour que l'utilitaire AutoUpdate attribue un nouveau nom aux fichiers .DAT de VirusScan existants avant l'installation des nouveaux fichiers. Pour renommer chaque fichier, l'utilitaire ajoute l'extension .SAV au nom et à l'extension des fichiers existants. CLEAN.DAT, par exemple, devient CLEAN.DAT.SAV.

- **Récupérer le fichier d'actualisation, sans effectuer l'opération**. Cochez cette case pour que l'utilitaire télécharge le fichier d'archives .ZIP qui contient les nouveaux fichiers .DAT et l'enregistre dans un emplacement que vous désignez au lieu de l'extraire et de l'installer.

  En cochant cette case, vous activez aussi la case **Enregistrer le fichier de mise à jour pour une utilisation future**, située dans la zone Après une actualisation réussie. Pour indiquer à l'utilitaire AutoUpdate l'emplacement où il doit enregistrer la kit de fichiers .DAT, entrez un chemin d'accès et un nom de dossier dans la zone de texte située au-dessous cette case ou cliquez sur **Parcourir** pour trouver un dossier approprié.

  En cochant cette case, vous désactivez aussi les cases **Sauvegarder les fichiers .DAT existants**, **Forcer la mise à jour** et **Redémarrer le système après une mise à jour réussie (si nécessaire)**.

  Vous pouvez utiliser cette option si vous téléchargez de nouveaux fichiers .DAT vers un serveur central de votre réseau et souhaitez que les ordinateurs clients individuels téléchargent, extraient et installent ces fichiers au niveau local.

- **Forcer la mise à jour.** Cochez cette case pour demander à l'utilitaire AutoUpdate de télécharger et d'installer tout kit de fichiers .DAT qu'il trouve sur le serveur cible, qu'il soit ou non postérieur à vos fichiers .DAT existants.

  Vous pourriez utiliser cette option pour « actualiser » régulièrement les fichiers .DAT stockés dans le répertoire du programme VirusScan, au cas où ils auraient été corrompus. Cette option évitera également tout message d'erreur que VirusScan pourrait retourner s'il ne trouve pas de nouveaux fichiers sur le serveur cible à l'heure que vous avez fixée pour l'exécution de la tâche de mise à jour.

  AVERTISSEMENT : Network Associates vous recommande d'utiliser cette option avec la plus grande prudence. Si vous avez configuré la tâche AutoUpdate pour se connecter à un serveur qui stocke des versions plus anciennes de fichiers .DAT, vous risquez de réduire l'efficacité de VirusScan et d'exposer votre ordinateur ou votre réseau à l'infection de nouveaux virus et autres logiciels nocifs. Les mises à niveau des composants du programme VirusScan peuvent aussi provoquer des incompatibilités avec des versions de fichiers .DAT plus anciennes. Ces incompatibilités sont susceptibles à leur tour de provoquer un comportement imprévisible du logiciel VirusScan.

2. Précisez à l'utilitaire AutoUpdate ce qu'il doit faire après un téléchargement, une extraction et une installation réussis des nouveaux fichiers .DAT. Vous avez le choix entre les options suivantes :

   - **Redémarrer le système après une mise à jour réussie (si nécessaire)**. Cochez cette case pour que l'utilitaire AutoUpdate relance votre système après l'installation de nouveaux fichiers .DAT.

     En règle générale vous n'avez pas besoin de redémarrer l'ordinateur pour que le logiciel VirusScan puisse utiliser les nouveaux fichiers .DAT, mais certains systèmes doivent être réinitialisés pour activer les nouveaux fichiers. Si vous préférez attendre un moment plus approprié pour le redémarrage, décochez cette case. Si vous envisagez d'exécuter un programme après la mise à jour des fichiers .DAT, laissez cette case décochée.

   - **Enregistrer le fichier de mise à jour pour une utilisation future.** Cochez cette case pour que l'utilitaire AutoUpdate enregistre une copie non extraite du kit de fichiers .DAT dans un emplacement que vous spécifiez. L'utilitaire procède alors à l'extraction des fichiers .DAT à partir du kit de mise à jour et reprend l'installation.

     En revanche, l'option **Récupérer le fichier de mise à jour, sans effectuer l'opération** enregistre le fichier non extrait, mais n'installe pas les nouveaux fichiers .DAT.

     Pour demander à l'utilitaire AutoUpdate d'enregistrer la kit de fichiers .DAT, entrez un chemin d'accès et un nom de dossier dans la zone de texte située au-dessous cette case ou cliquez sur **Parcourir** pour trouver un dossier approprié.

   - **Exécuter un programme après la mise à jour.** Cochez cette case pour indiquer à l'utilitaire de lancer un autre programme une fois l'installation des nouveaux fichiers .DAT achevée. Vous pourriez utiliser cette option notamment pour démarrer un programme client e-mail ou un utilitaire de messagerie réseau qui indique à un administrateur système que l'opération de mise à jour s'est déroulée comme prévu.

     Tapez ensuite le chemin d'accès et le nom de fichier du programme que vous souhaitez exécuter ou cliquez sur **Parcourir** pour localiser le programme sur votre disque dur.

3. Pour enregistrer vos modifications et revenir à la boîte de dialogue Actualisation automatique, cliquez sur **OK**. Pour fermer la boîte de dialogue sans enregistrer vos modifications, cliquez sur **Annuler**.

Description de l'utilitaire AutoUpgrade

Network Associates révise fréquemment le logiciel VirusScan et le moteur d'analyse Olympus afin d'ajouter de nouveaux outils de détection et de réparation, de nouvelles fonctions qui renforcent la flexibilité et la facilité de gestion du logiciel et d'autres améliorations permettant d'accroître ses capacités de protection contre les virus. L'utilitaire AutoUpgrade de VirusScan est conçu pour rechercher et télécharger ces nouvelles versions lorsqu'elles sont disponibles. Vous pouvez utiliser cet utilitaire en association avec l'utilitaire SuperDAT pour automatiser les mises à niveau du moteur d'analyse. Pour en savoir plus sur cette procédure, reportez-vous à la section « Utilisation conjointe des utilitaires AutoUpgrade et SuperDAT » à la page 300.

L'utilitaire AutoUpgrade s'exécute exclusivement en tant que tâche depuis la console VirusScan. Pour mettre à niveau votre logiciel VirusScan à l'aide de l'utilitaire, vous devez :

- Définir un calendrier pour la tâche AutoUpgrade et l'activer en vue de son exécution
- Définir un mot de passe pour protéger vos paramètres de configuration (facultatif)
- Configurer la tâche pour télécharger les nouveaux fichiers depuis un emplacement spécifique de votre réseau, ou sur Internet

Par défaut, la tâche AutoUpgrade incluse dans la console VirusScan n'est pas configurée pour utiliser un site de mise à niveau par défaut. McAfee vous recommande plutôt d'utiliser d'autres mécanismes, tels que le service Enterprise SecureCast, pour recevoir de nouveaux fichiers SuperDAT ou de nouveaux fichiers programme et de placer ensuite ces fichiers sur un serveur central de votre réseau. Vous pouvez ensuite configurer l'utilitaire AutoUpgrade sur chaque station de travail du réseau pour extraire les nouveaux fichiers depuis l'emplacement que vous spécifiez. Pour en savoir plus sur le service SecureCast, reportez-vous à l'Annexe C, « Utilisation du service SecureCast pour obtenir de nouveaux fichiers de données ». ou visitez le site Web de Network Associates à l'adresse suivante :

http://www.nai.com/asp_set/anti_virus/alerts/enterprise.asp

Le fait de placer les nouveaux fichiers sur un ou plusieurs serveurs centraux de votre réseau vous permet de :

- Planifier le retrait des fichiers programme sur l'ensemble du réseau aux heures qui vous conviennent et avec une intervention minimale des administrateurs ou des utilisateurs du réseau. Utilisez la boîte de dialogue Propriétés de la tâche AutoUpgrade pour déterminer le moment où chaque nœud de réseau consultera le serveur pour charger des fichiers actualisés.

Vous pourriez notamment spécifier une heure de mise à jour qui vous convienne la première fois que vous utilisez le logiciel VirusScan, mais paramétrer l'utilitaire AutoUpgrade pour qu'il se déclenche à n'importe quel moment dans l'intervalle de 60 minutes qui suit, ou fixer un calendrier prévoyant que les différents éléments du réseau chargent les mises à niveau des fichiers programme en même temps ou à tour de rôle. Pour en savoir plus sur la planification de la tâche AutoUpdate ou des autres tâches, reportez-vous à la section « Activation des tâches » à la page 247.

- Partager les devoirs d'administration des retraits entre différents serveurs ou contrôleurs de domaine, entre différentes zones des réseaux étendus ou entre d'autres parties de réseau. Conserver en priorité à un niveau interne le trafic de mise à jour, peut également limiter les possibilités de violation de la sécurité du réseau.
- Réduire les attentes éventuelles pour télécharger les nouvelles versions des fichiers programme. Le trafic sur les serveurs McAfee est susceptible d'augmenter considérablement aux dates de publication des nouveaux fichiers programme. Éviter la saturation de la bande passante du réseau vous permet d'utiliser votre mise à jour avec un minimum d'interruptions.

Configuration de l'utilitaire AutoUpgrade

Pour mettre à jour les fichiers programme pour votre logiciel VirusScan, vous devez indiquer à l'utilitaire AutoUpgrade :

- les sites de mise à jour qui possèdent les nouveaux fichiers que vous souhaitez télécharger ;
- la méthode de transfert que vous souhaitez utiliser pour le téléchargement ;
- si vous utilisez un serveur proxy et, le cas échéant, le port que vous lui avez attribué ;
- ce qu'il doit faire avec les fichiers téléchargés ; les installer, les enregistrer pour une utilisation ultérieure ou les deux à la fois ;
- si vous souhaitez réamorcer le système une fois la mise à niveau terminée ;
- si vous souhaitez conserver une trace de ses actions dans un fichier journal.

Les pages de propriétés de la boîte de dialogue Propriétés de la mise à niveau automatique contrôlent les options de votre tâche de mise à niveau. Vous pouvez alors cliquer sur chacun des onglets pour configurer cette tâche.

Pour afficher la boîte de dialogue Mise à niveau automatique, procédez comme suit :

1. Double-cliquez sur la tâche AutoUpgrade dans la liste des tâches de la console pour ouvrir la boîte de dialogue Propriétés des tâches (voir Figure 7-6).

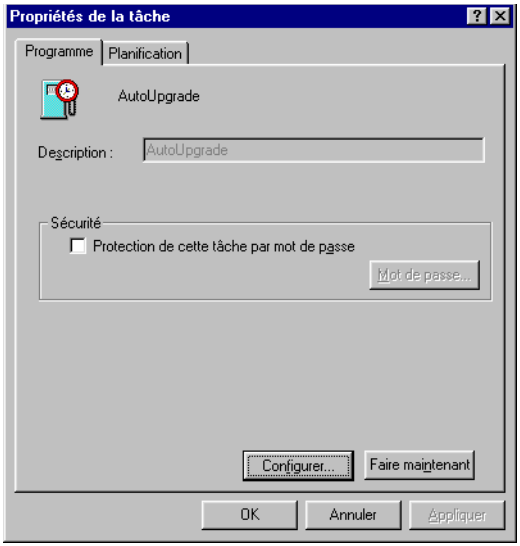

Figure 7-6. Boîte de dialogue Propriétés de la tâche Mise à niveau automatique

Pour en savoir plus sur la définition d'un mot de passe pour cette tâche, reportez-vous à la section « Exécution des tâches AutoUpgrade et AutoUpdate » à la page 241. Pour en savoir plus sur la planification d'une tâche, reportez-vous à la section « Activation des tâches » à la page 247.

2. Cliquez sur **Configurer**.

   La boîte de dialogue Mise à niveau automatique s'affiche avec la page de propriétés Sites de mise à niveau sélectionnée (voir Figure 7-7 à la page 292).

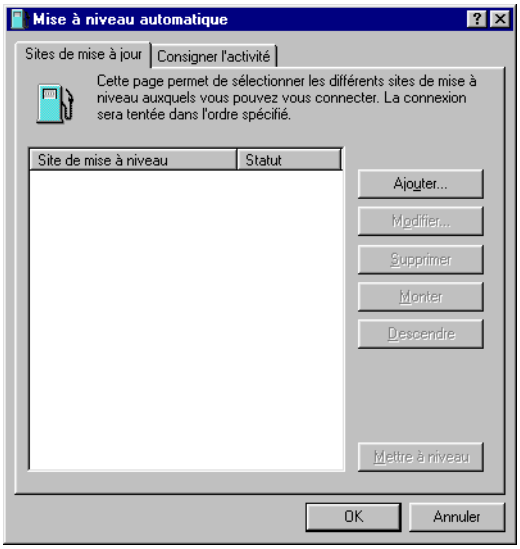

Figure 7-7. Boîte de dialogue Mise à niveau automatique – page Sites de mise à niveau

L'utilitaire AutoUpgrade répertorie dans cette boîte de dialogue les sites à partir desquels il téléchargera les nouveaux fichiers programme de VirusScan. Il indique également l'état actuel de chaque site par la mention Activé ou Désactivé. Un site est activé si vous avez coché la case **Activé** dans la boîte de dialogue Propriétés de la mise à niveau automatique. Il est désactivé si la case n'est pas cochée. Cette désignation n'a aucune influence sur les possibilités de l'utilitaire AutoUpgrade de se connecter au site.

Aucun site ne figurera dans la liste de départ car l'utilitaire AutoUpgrade n'est pas configuré pour se connecter à un site de mise à niveau spécifique. Vous devez ajouter les sites dont vous avez besoin en vous référant aux informations que vous avez reçues lors de l'acquisition de VirusScan. L'utilitaire AutoUpgrade peut télécharger de nouveaux fichiers programme à partir de n'importe quel partage réseau ou site FTP que vous spécifiez.

Vous pouvez ajouter autant de sites qui vous sont nécessaires et modifier l'ordre suivant lequel l'utilitaire tente de s'y connecter. L'utilitaire tentera de se connecter successivement à chaque site, en commençant par le début de la liste et jusqu'à ce qu'il parvienne à télécharger les nouveaux fichiers avec succès ou à déterminer qu'il n'y a aucun nouveau fichier disponible.

3. Dans cette boîte de dialogue, vous pouvez :

   - Ajouter un nouveau site. Cliquez sur **Ajouter** pour ouvrir la boîte de dialogue Propriétés de la mise à niveau automatique (Figure 7-2 à la page 280). Pour en savoir plus sur la spécification des options pour votre site, reportez-vous à la section « Configuration des options de mise à niveau » à la page 295.

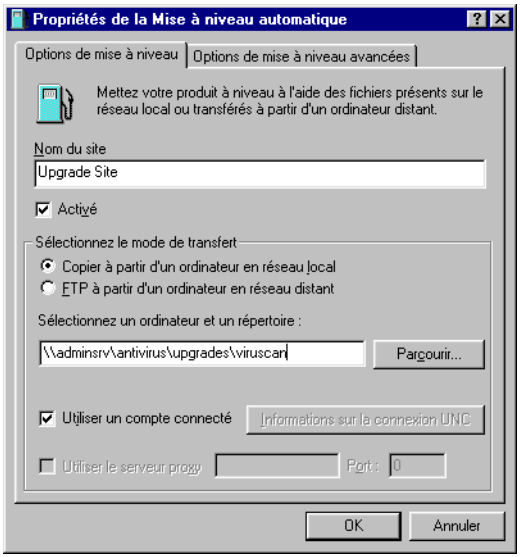

Figure 7-8. Boîte de dialogue Propriétés de la mise à niveau automatique – page Options de mise à niveau

   - Modifier les options définies pour un site de mise à niveau existant. Sélectionnez un site dans la liste des sites de mise à niveau, puis cliquez sur **Edition** pour ouvrir la boîte de dialogue Propriétés de la mise à niveau automatique (Figure 7-8). Procédez à vos modifications, puis cliquez sur **OK** pour les enregistrer et revenir à cette boîte de dialogue. Pour consulter des descriptions et des instructions concernant la configuration des options disponibles, reportez-vous à la section « Configuration des options de mise à niveau » à la page 295.

   - Supprimer un site existant de la liste des sites de mise à niveau. Sélectionnez un site dans la liste des sites de mise à niveau, puis cliquez sur **Supprimer**.

   - Spécifiez l'ordre suivant lequel l'utilitaire AutoUpgrade doit se connecter aux sites répertoriés. Pour faire monter un site dans la liste, sélectionnez-le et cliquez sur **Monter**. Pour faire descendre un site dans la liste, sélectionnez-le et cliquez sur **Descendre**.

- Mettez immédiatement à jour vos fichiers à partir des sites répertoriés dans la liste de mise à jour, en utilisant les options de configuration par défaut ou les options que vous avez choisies pour cette tâche. Cliquez sur **Mettre à niveau**.

  Pour utiliser cette fonction, vous devez configurer un nombre suffisant d'options nécessaires à l'utilitaire AutoUpgrade pour localiser le site répertorié et, le cas échéant, s'y connecter. Pour en savoir plus sur la spécification des options dont vous avez besoin, reportez-vous à la section « Configuration des options de mise à niveau » à la page 295.

  Si le programme AutoUpgrade ne parvient pas à se connecter à un site de la liste au bout de trois tentatives ou s'il ne trouve pas de nouveaux fichiers programme, il se connecte à chacun des autres sites répertoriés jusqu'à ce qu'il trouve la version la plus récente des fichiers programme disponible.

4. Cliquez sur l'onglet Consigner l'activité pour afficher la prochaine page des propriétés (Figure 7-9).

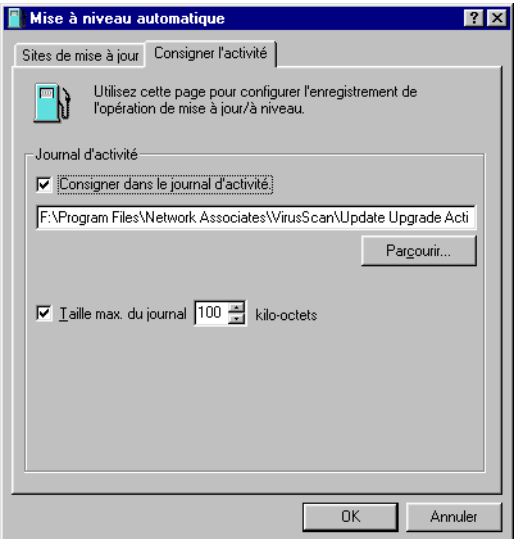

Figure 7-9. Boîte de dialogue Mise à niveau automatique – page Consigner l'activité

5. Cochez la case **Consigner les activités dans le journal d'activité**.

   Par défaut, l'utilitaire AutoUpgrade enregistre les événements qui se sont déroulés lors des tentatives de mise à jour et les enregistre dans le fichier UPDATE UPGRADE ACTIVITY LOG.TXT, situé dans le répertoire du programme VirusScan, à chaque fois que vous arrêtez la tâche ou l'ordinateur.

   Si vous préférez enregistrer ces données dans un fichier texte différent, entrez son chemin d'accès et son nom dans la zone de texte prévue à cet effet ou cliquez sur **Parcourir** pour localiser le fichier. L'utilitaire AutoUpgrade ne génère pas de fichier texte, il peut uniquement écrire dans un fichier existant.

6. Pour réduire la taille du fichier journal, cochez la case **Taille maximale du journal**. Cliquez ensuite sur pour définir une taille ou entrez une valeur comprise entre 10 Ko et 999 Ko. Par défaut, l'utilitaire AutoUpgrade limite la taille du fichier à 100 Ko.

   Si vous décochez cette case, le fichier journal peut voir sa taille augmenter jusqu'à une limite déterminée par l'espace disque ou par le système de fichiers. Si le fichier atteint la taille maximale allouée, l'utilitaire AutoUpgrade efface ce fichier et démarre le journal au point où il s'était interrompu.

   Pour afficher le contenu du fichier journal depuis la console VirusScan, sélectionnez la tâche AutoUpgrade dans la liste des tâches, puis choisissez **Afficher le journal d'activité** dans le menu **Tâche**.

7. Cliquez sur **OK** pour enregistrer vos modifications et fermer la boîte de dialogue Mise à niveau automatique. Cliquez sur **Annuler** pour fermer la boîte de dialogue sans enregistrer vos modifications.

Configuration des options de mise à niveau

Pour créer un nouveau site de mise à jour ou changer les paramètres d'un site existant, cliquez sur **Ajouter** dans la boîte de dialogue Mise à niveau automatique (voir Figure 7-7 à la page 292), ou sélectionnez un site de la liste, puis cliquez sur **Edition**. Les deux méthodes affichent la boîte de dialogue Propriétés de la Mise à niveau automatique (Figure 7-10 à la page 296).

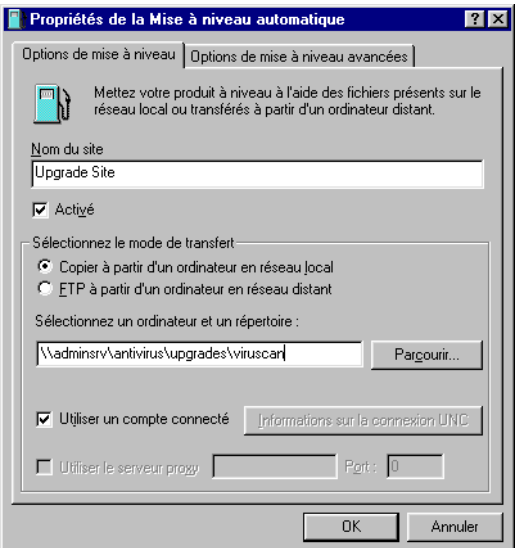

Figure 7-10. Boîte de dialogue Propriétés de la Mise à niveau automatique – page Options de mise à niveau

Ensuite, procédez comme suit :

1. Entrez un nom descriptif permettant d'identifier clairement le site dans la zone de texte Nom du site.

   Tapez par exemple `Site de mise à niveau interne des fichiers programme`.

2. Cochez la case **Activé** pour que le site puisse être utilisé par l'utilitaire AutoUpgrade.

   Si vous décochez cette case, vous conservez les options choisies, mais l'utilitaire ignorera ce site lorsqu'il tentera de télécharger les nouveaux fichiers .DAT.

   L'utilitaire AutoUpgrade fera trois tentatives de connexion au maximum au cours de chaque opération de mise à jour planifiée. Lorsqu'il parvient à se connecter et à télécharger les nouveaux fichiers programme, l'utilitaire procède également à l'extraction des fichiers et à leur installation dans le répertoire approprié.

3. Spécifiez la méthode de transfert que vous souhaitez utiliser pour télécharger les nouveaux fichiers. Vous avez le choix entre les options suivantes :

- **Copier à partir d'un ordinateur en réseau local**. Cliquez sur ce bouton si vous souhaitez que l'utilitaire AutoUpgrade utilise une configuration de réseau standard pour rechercher les nouveaux fichiers sur votre ordinateur local ou sur un autre ordinateur du réseau. Vos paramètres réseau contrôlent la façon dont l'utilitaire tente de se connecter et l'intervalle de temps qui doit s'écouler avant qu'il ne cesse ses tentatives.

  Utilisez ensuite la notation de la convention d'affectation des noms (UNC) pour spécifier, dans la zone de texte Sélectionnez un ordinateur et un répertoire, le chemin d'accès de l'ordinateur qui héberge les nouveaux fichiers que vous souhaitez télécharger. Vous pouvez également cliquer sur **Parcourir** pour localiser le répertoire approprié.

  Pour utiliser la notation UNC, vous devez, soit utiliser le même compte que vous avez utilisé pour ouvrir une session sur le réseau, soit spécifier un nom d'utilisateur et un mot de passe pour vous y connecter. Pour utiliser le compte courant, cochez la case **Utiliser un compte connecté**.

  REMARQUE : Le fait d'activer cette option peut avoir des effets légèrement différents selon que vous utilisiez le système Windows NT Workstation v4.0 ou le système Windows 2000 Professionnel. Si vous avez *planifié* la mise à jour de vos fichiers, l'utilitaire AutoUpgrade utilisera son propre compte de service pour se connecter au serveur de mise à niveau et télécharger les nouveaux fichiers. Si vous cliquez sur **Mettre à jour maintenant**, l'utilitaire AutoUpgrade utilisera le même compte que vous avez utilisé pour vous ouvrir une session sur le réseau et vous connecter au serveur de mise à niveau.

  Pour installer un nouveau moteur d'analyse ou de nouveaux fichiers programme qui remplacent les services VirusScan existants, le compte doit avoir des droits d'administration sur votre réseau local ; en d'autres termes, il doit faire partie du groupe Administrateurs locaux.

  Pour utiliser un compte personnalisé, décochez la case **Utiliser un compte connecté** et cliquez sur **Informations sur la connexion UNC** pour entrer un nom d'utilisateur et un mot de passe pour un compte disposant de droits d'accès pour ce serveur cible.

- **FTP depuis un ordinateur en réseau distant**. Cliquez sur ce bouton si vous souhaitez que l'utilitaire AutoUpgrade recherche les nouveaux fichiers sur un site FTP que vous désignez. Pour utiliser cette option, le serveur cible doit posséder un service FTP actif.

  L'utilitaire AutoUpgrade utilise sa propre implémentation FTP pour se connecter au serveur, cependant l'intervalle de temps après lequel les tentatives seront abandonnées dépendra de vos paramètres de protocole réseau existants.

  Pour utiliser un autre site FTP, entrez l'URL du site que vous souhaitez utiliser dans la zone de texte Entrez un nom d'ordinateur FTP et un répertoire. Vous devez vous connecter à un site configuré pour les connexions FTP anonymes ou désigner le nom d'utilisateur et le mot de passe d'un compte existant sur le site.

  Pour que l'utilitaire utilise une connexion anonyme, cochez la case **Utiliser une connexion FTP anonyme**.

  Pour spécifier un compte, décochez la case **Utiliser une connexion FTP anonyme** et cliquez sur **Informations…** pour entrer un nom d'utilisateur et un mot de passe pour un compte disposant de droits d'accès pour ce serveur cible.

  Si votre serveur utilise un serveur proxy, cochez la case **Utiliser le serveur proxy**, puis entrez le nom du serveur et le port logique qu'il utilise dans les zones de texte fournies à cet effet. Vous pouvez saisir le nom avec la notation UNC ou sous la forme d'un nom de domaine, en fonction de ce qui est adapté à votre environnement.

  ❑ **REMARQUE :** L'utilitaire AutoUpgrade n'autorise pas les connexions à un serveur proxy qui nécessitent une authentification de proxy de stimulation / réponse.

Configuration des options avancées de mise à niveau

Pour exécuter votre tâche AutoUpgrade, vous devez entrer un serveur cible, une méthode de connexion et toutes les informations nécessaires à la connexion. Puis, lorsque vous aurez activé la tâche et défini un calendrier pour son exécution, l'utilitaire AutoUpgrade procédera pour vous au téléchargement des fichiers appropriés depuis le serveur cible, à leur extraction et à leur installation dans le répertoire du programme VirusScan.

Pour que l'utilitaire AutoUpgrade effectue des opérations supplémentaires postérieures ou antérieures sur les fichiers, ou pour qu'il procède à d'autres actions, cliquez sur l'onglet Options de mise à niveau avancées pour afficher la page de propriétés illustrée dans la (Figure 7-5 à la page 286).

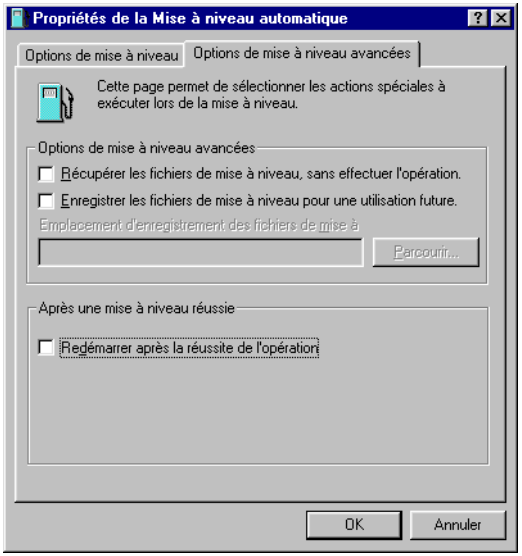

Figure 7-11. Boîte de dialogue Propriétés de la mise à jour automatique – page Options de mise à jour avancées

Ensuite, procédez comme suit :

1. Précisez à l'utilitaire AutoUpgrade ce que vous souhaitez qu'il fasse avant ou pendant l'exécution d'une mise à jour. Vous avez le choix entre les options suivantes :

   - **Récupérer les fichiers de mise à niveau, sans effectuer l'opération**. Cochez cette case pour que l'utilitaire télécharge le fichier d'archives .ZIP qui contient les nouveaux fichiers programme et l'enregistre dans un emplacement que vous désignez au lieu de l'extraire et de l'installer.

     En cochant cette case, vous activez aussi la case **Enregistrer les fichiers de mise à niveau pour une utilisation future**. Pour indiquer à l'utilitaire AutoUpgrade l'emplacement où il doit enregistrer le fichier d'archives contenant les fichiers programme, entrez un chemin d'accès et un nom de dossier dans la zone de texte située au-dessous de cette case ou cliquez sur **Parcourir** pour localiser un dossier approprié.

     Vous pouvez utiliser cette option si vous téléchargez de nouveaux fichiers programme vers un serveur central de votre réseau et souhaitez que les ordinateurs clients individuels téléchargent, extraient et installent ces nouveaux fichiers au niveau local.

2. Précisez à l'utilitaire AutoUpgrade ce qu'il doit faire après un téléchargement, une extraction et une installation réussis des nouveaux fichiers .DAT. Vous avez le choix entre les options suivantes :

   - **Redémarrer le système après une mise à jour réussie (si nécessaire)**. Cochez cette case pour que l'utilitaire AutoUpgrade relance votre système après l'installation de nouveaux fichiers programme.

     En règle générale vous n'avez pas besoin de redémarrer l'ordinateur pour que le logiciel VirusScan puisse utiliser les nouveaux fichiers programme, mais certains systèmes doivent être réinitialisés pour activer les nouveaux fichiers. Si vous préférez attendre un moment plus approprié pour le redémarrage, décochez cette case.

3. Pour enregistrer vos modifications et revenir à la boîte de dialogue Mise à niveau automatique, cliquez sur **OK**. Pour fermer la boîte de dialogue sans enregistrer vos modifications, cliquez sur **Annuler**.

Utilisation conjointe des utilitaires AutoUpgrade et SuperDAT

Dans la version actuelle, vous devez modifier le kit SuperDAT que vous téléchargez à partir du site Web de McAfee pour pouvoir l'utiliser en association avec l'utilitaire AutoUpgrade.

REMARQUE : Le logiciel VirusScan v4.5 et versions ultérieures requiert l'utilisation de l'utilitaire SuperDAT v1.2 ou versions ultérieures.

Pour modifier le kit SuperDAT, procédez comme suit :

1. Renommez le fichier SDATXXXX.EXE en le remplaçant par SETUP.EXE. Ici, XXXX désigne le numéro de version de l'utilitaire SuperDAT en tant que partie du nom du fichier.

2. Téléchargez le fichier AUTOUPG.ZIP, que vous trouverez sur le site FTP de Network Associates, à l'adresse suivante :

   ftp://<nomd'utilisateur>:<motdepasse>@ftp.nai.com/licensed/antivirus/superdat/tools/

REMARQUE : Ici, <nomd'utilisateur> correspond à votre nom d'utilisateur permettant d'accéder au site d'entreprise de Network Associates et <motdepasse> désigne votre mot de passe permettant d'accéder au site d'entreprise. Pour télécharger ces fichiers, vous devez avoir accès au site en tant que client détenteur d'une licence McAfee.

AUTOUPG.ZIP contient le fichier PKGDESC.INI. Procédez à l'extraction du fichier PKGDESC.INI à partir du fichier .ZIP, puis copiez à la fois le fichier extrait et le kit renommé SETUP.EXE sur le serveur à partir duquel les autres ordinateurs du réseau doivent télécharger les fichiers actualisés. Les fichiers PKGDESC.INI et SETUP.EXE doivent être présents pour que l'utilitaire AutoUpgrade puisse télécharger correctement les fichiers de mise à jour.

REMARQUE : Si votre serveur de mise à niveau exécute UNIX ou un autre système d'exploitation respectant les caractères majuscules / minuscules, vérifiez que vous avez renommé le fichier PKGDESC.INI correctement. Dans la version actuelle de l'utilitaire AutoUpdate, fourni avec le logiciel antivirus VirusScan, ce nom de fichier doit apparaître tout en minuscules : pkgdesc.ini.

3. Si vous le souhaitez, vous pouvez créer et copier un fichier SETUP.ISS dans le répertoire à partir duquel l'utilitaire AutoUpgrade doit télécharger les nouveaux fichiers.

   SETUP.ISS est un fichier texte simple qui contrôle la façon dont l'utilitaire AutoUpgrade met à niveau votre logiciel. Vous pouvez utiliser n'importe quel éditeur de texte standard pour créer et enregistrer ce fichier.

   Pour spécifier des options de configuration dans votre fichier SETUP.ISS, utilisez l'exemple ci-dessous pour connaître les options disponibles. Vous pouvez couper et coller cet exemple directement sur un fichier texte, puis le modifier et l'enregistrer en tant que fichier SETUP.ISS.

```
[SuperDATOptions]

bReboot=1

bPrompt=1

szLogFile=C:\temp\mylog.txt
```

Voici une description du rôle de chaque instruction du fichier :

- bReboot=1

  Cette instruction demande à l'utilitaire SuperDAT de redémarrer l'ordinateur cible, s'il le faut, afin de terminer la mise à jour ou la mise à niveau de votre logiciel antivirus. Si vous ne souhaitez pas redémarrer l'ordinateur cible après la mise à jour de vos fichiers, attribuez au paramètre `bReboot=` la valeur zéro ou supprimez l'instruction du fichier SETUP.ISS.

  Si vous ne demandez pas à l'utilitaire SuperDAT de redémarrer l'ordinateur cible, en incluant cette instruction dans le fichier SETUP.ISS, ou partir de la ligne de commande, ou dans un script de mise à jour, il *ne le fera en aucun cas*. Le logiciel VirusScan ne requiert pas le redémarrage du système après la mise à niveau des fichiers du moteur d'analyse ou de la mise à jour des fichiers .DAT.

- bPrompt=1

  Cette instruction demande à l'utilitaire SuperDAT d'afficher uniquement la boîte de dialogue Arrêter de Windows après la mise à jour ou la mise à niveau de votre logiciel.

- szLogFile=<CHEMIND'ACCES\NOMDEFICHIER>

  Cette option demande à l'utilitaire SuperDAT d'enregistrer un fichier journal sous le nom et à l'emplacement que vous avez spécifiés. Par défaut, l'utilitaire SuperDAT crée un fichier journal dans le répertoire de travail en cours.

Une fois que vous avez placé le fichier PKGDESC.INI, le fichier SETUP.EXE et tout fichier SETUP.ISS que vous souhaitez utiliser sur un serveur central, configurez les exemplaires de l'utilitaire AutoUpgrade installés sur les stations de travail pour télécharger de nouveaux fichiers depuis le partage que vous avez créé sur ce serveur central. Les utilitaires AutoUpgrade téléchargeront et installeront les nouveaux fichiers à partir de ce kit.

Pour en savoir plus sur le fonctionnement de l'utilitaire SuperDAT, téléchargez le *Guide d'utilisateur* SuperDAT depuis le site Web de McAfee, à l'adresse suivante :

http://www.nai.com/asp_set/download/upgrade/login.asp

Sinon, consultez le fichier README.TXT fourni avec chaque version hebdomadaire de l'utilitaire SuperDAT.

Utilisation des outils d'analyse spécialisés 8

Analyse des systèmes de messagerie Microsoft Exchange et Outlook

Le logiciel VirusScan vous propose deux méthodes supplémentaires pour assurer la protection de vos systèmes de messagerie Microsoft Exchange ou Outlook :

- Le moteur d'analyse VShield inclut un module Analyse E-Mail qui effectue des opérations d'analyse en arrière-plan permanentes sur les messages e-mail, à mesure qu'ils arrivent sur votre serveur.
- L'extension Analyse E-Mail vous permet d'analyser votre boîte aux lettres située sur le serveur Exchange de votre propre initiative et aux moments qui vous conviennent.

Une architecture de plug-in discrète vous permet d'accéder à l'extension Analyse E-Mail directement à partir de votre application cliente Exchange ou Outlook.

À quel moment utiliser l'extension Analyse E-Mail et pourquoi

La majorité des virus à expansion rapide, des vers et des autres agents nocifs qui sont apparus ces dernières années se sont propagés par l'intermédiaire du courrier électronique. Le courrier électronique constitue un moyen rapide et omniprésent pour les auteurs de virus de diffuser des documents joints infectés, qu'ils parviennent souvent à faire ouvrir et activer par les utilisateurs. Les virus de la dernière génération, comme l'a montré le virus VBS/BUBBLEBOY, peuvent même fonctionner sans que les utilisateurs ouvrent ou lisent le message e-mail en soi.

Les clients e-mail Microsoft Exchange et Outlook sont particulièrement exposés aux infections de ce type en raison des capacités puissantes d'interprétation de macro et de script dont ils sont dotés. À l'instar de l'ensemble d'applications Microsoft Office, le logiciel client Exchange utilise beaucoup les macros, le texte à balises, les commandes de script et des fonctions similaires qui l'exposent aux attaques des virus.

Utilisez le module Analyse E-Mail de VShield pour effectuer des opérations d'analyse en arrière-plan sur votre système e-mail et pour maintenir un niveau constant de vigilance entre les opérations d'analyse que vous exécutez à l'aide de l'extension Analyse E-Mail. Dans la majorité des cas, cela devrait protéger l'intégrité de votre système.

Si votre serveur contient une importante accumulation de messages que vous n'avez pas encore analysés, si vous fermez la session de votre serveur Exchange ou si vous arrêtez le module Analyse E-Mail à un point quelconque, vous devez utiliser l'extension Analyse E-Mail pour analyser votre boîte aux lettres de manière à assurer l'intégrité du système. Les virus peuvent facilement demeurer dans des messages e-mail anciens stockés sur votre serveur ou dans des messages e-mail arrivant à des instants où aucune session de votre système e-mail n'est ouverte.

Cependant, une protection antivirus efficace repose sur une analyse complète et régulière de votre boîte aux lettres, et ce pour les raisons suivantes :

- **En matière de sécurité, deux précautions valent mieux qu'une**. Le module Analyse E-Mail de VShield recherche du code viral à mesure que les messages e-mail arrivent sur votre serveur ou lorsque des pièces jointes exécutables sont exécutées après un téléchargement sur votre système. L'extension Analyse E-Mail peut analyser les anciens messages e-mail stockés sur le serveur que le module Analyse E-Mail ne verra pas, rechercher des virus dans les messages e-mail arrivant entre deux intervalles de connexion au serveur Exchange ou encore analyser votre boîte aux lettres si vous avez désactivé temporairement le module Analyse E-Mail de VShield.
- **Une maintenance préventive est synonyme de sécurité**. Avec les connexions rapides aux messageries e-mail, effectuées entre logiciels clients puissants, dotés de capacités Web et de script, il suffit de quelques secondes pour être infecté par un virus, parfois avant même d'ouvrir vos messages. Des opérations d'analyse régulières peuvent souvent détecter une infection avant qu'elle n'ait eu le temps de s'étendre ou de commettre des dégâts.

Utilisation de l'extension Analyse E-Mail

Pour pouvoir utiliser l'extension Analyse E-Mail, vous devez installer le logiciel VirusScan en sélectionnant l'installation Personnalisée et choisir d'installer le composant Analyse E-Mail (pour plus de détails, reportez-vous à la section « Procédure d'installation » à la page 45). Pour utiliser le composant E-Mail Scan avec les paramètres par défaut, démarrez votre logiciel client Microsoft Exchange ou Microsoft Outlook.

Ensuite, procédez comme suit :

1. Connectez-vous à votre serveur e-mail en suivant la procédure habituelle.
2. Sélectionnez l'option **Recherche de virus** dans le menu **Outils** ou cliquez sur  dans la barre d'outils Exchange ou Outlook.

> **REMARQUE :** Si vous utilisez Microsoft Exchange 5.0, les boutons correspondant à l'extension Analyse E-Mail ne peuvent pas s'afficher immédiatement, en raison d'une limitation dans la façon dont le programme met à jour sa barre d'outils. Pour ajouter le bouton Recherche de virus à la barre d'outils, sélectionnez **Personnaliser la barre d'outils** dans le menu **Outils**, puis ajoutez les boutons correspondant à l'extension Analyse E-Mail à partir de la liste des boutons disponibles figurant dans la boîte de dialogue Personnaliser la barre d'outils.

Une fois que vous l'avez démarrée, l'extension Analyse E-Mail commence immédiatement à analyser votre boîte aux lettres Exchange ou Outlook à la recherche de virus (voir Figure 8-1 à la page 306).

Par défaut, l'extension Analyse E-Mail examine *tous* les messages électroniques stockés dans votre boîte aux lettres sur le serveur e-mail Exchange et y recherche des messages et des pièces jointes susceptibles d'être infectés par des virus. Si votre boîte aux lettres sur le serveur contient un grand nombre de messages que vous n'avez pas encore téléchargés, cette opération d'analyse peut prendre un certain temps.

Pour interrompre l'opération d'analyse, cliquez sur  . Pour y mettre fin, cliquez sur  . Pour reprendre l'analyse, cliquez sur  .

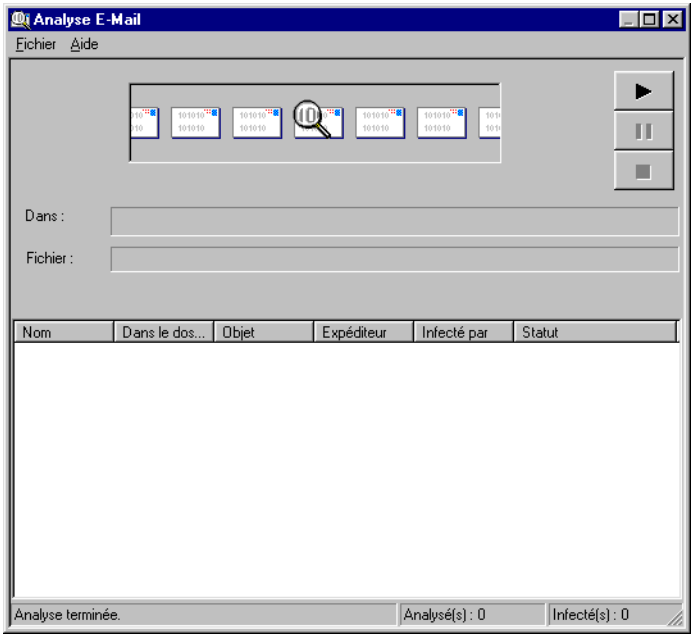

Figure 8-1. L'extension Analyse E-Mail en action

Si elle trouve un fichier infecté, l'extension Analyse E-Mail vous demande comment vous souhaitez réagir à cette infection. Pour plus de détails, reportez-vous à la section Voir « Options de réponse lorsque l'extension Analyse E-Mail détecte un virus » à la page 86.

Configuration de l'extension Analyse E-Mail

L'extension Analyse E-Mail est livrée avec un paramétrage prévu pour protéger votre système dans la majorité des situations et contre les agents nocifs les plus probables qui arrivent via la messagerie électronique. Vous pouvez toutefois modifier les options de configuration de l'extension afin de les adapter à votre environnement de travail. Pour modifier les paramètres, vous devez indiquer à l'extension Analyse E-Mail les éléments suivants :

- ce qu'elle doit analyser
- ce qu'elle doit faire en cas de détection d'un virus
- comment elle doit vous informer en cas de détection d'un virus
- si vous souhaitez conserver une trace de ses actions.

Une série de pages de propriétés contenues dans la boîte de dialogue Propriétés de l'Analyse E-Mail déterminent les options pour chacune des opérations d'analyse que vous exécutez. Vous pouvez cliquer sur chacun des onglets afin de choisir les options que l'extension doit utiliser pour l'analyse de vos messages e-mail.

Pour afficher cette boîte de dialogue, procédez comme suit :

1. Démarrez votre client Microsoft Exchange ou Outlook et connectez-vous à votre serveur e-mail.

   REMARQUE : Si vous êtes déjà connecté au domaine réseau qui héberge votre serveur e-mail, il n'est pas nécessaire de vous connecter directement à votre serveur e-mail ; il vous suffit simplement de démarrer Exchange ou Outlook. Contactez votre administrateur réseau afin de connaître les exigences de connexion au niveau de votre serveur.

2. Sélectionnez **Propriétés de l'Analyse E-Mail** dans le menu **Outils** ou cliquez sur dans la barre d'outils de l'application cliente.

   La boîte de dialogue Propriétés de l'Analyse E-Mail s'affiche (Figure 8-2).

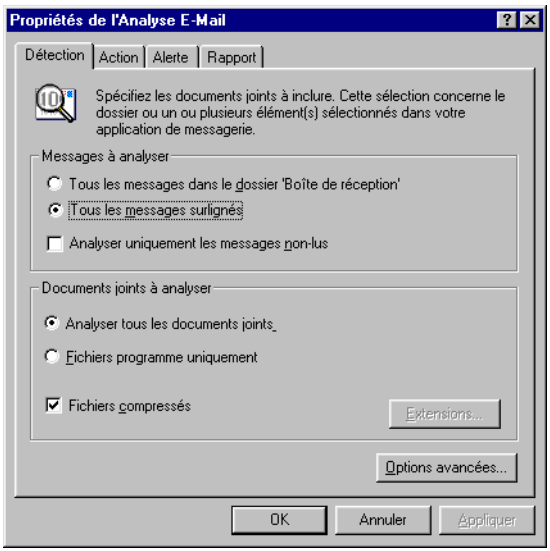

Figure 8-2. Boîte de dialogue Propriétés de l'Analyse E-Mail – page Détection

Sélection des options de détection

Lorsque vous ouvrez pour la première fois la boîte de dialogue Propriétés de l'Analyse E-Mail pour configurer une opération d'analyse, l'extension Analyse E-Mail suppose qu'elle doit analyser tous les messages contenus dans votre boîte de réception, toutes les pièces jointes des messages, tous les fichiers compressés et uniquement les fichiers susceptibles de contenir une infection par un virus.

L'extension Analyse E-Mail effectue en fait une analyse des messages électroniques eux-mêmes, dans la mesure où les fichiers Microsoft Exchange peuvent contenir des macros incorporées, des balises HTML (Hyper Text Markup Language) et des applets VBScript, qui peuvent à leur tour héberger des virus spécialisés, des vers ou des programmes de type Cheval de Troie.

REMARQUE : L'extension Analyse E-Mail se connecte directement à votre boîte aux lettres sur votre serveur e-mail Microsoft Exchange pour y exécuter ses opérations d'analyse. Vous pouvez également analyser les dossiers publics auxquels vous avez accès, mais l'extension n'analyse pas les messages stockés dans les dossiers personnels Microsoft Outlook (fichiers .PST) ou les éléments archivés. D'autres composants VirusScan analyseront toutefois les fichiers .PST dans le cadre de leurs opérations d'analyse régulières, sauf si vous les excluez de manière spécifique.

Pour modifier ces paramètres, procédez comme suit :

1. Sélectionnez les messages e-mail dans lesquels l'extension Analyse E-Mail doit rechercher des virus. Vous pouvez analyser :

   - **Tous les messages dans le dossier 'Boîte de réception'.** Cliquez sur ce bouton pour que l'extension recherche les virus dans l'intégralité des messages électroniques stockés dans votre boîte de réception Microsoft Exchange ou Microsoft Outlook, que vous ayez ou non lu ces messages.

     Si votre boîte de réception contient un grand nombre de messages, cette opération d'analyse peut prendre un certain temps. Cependant, si vous avez installé l'extension Analyse E-Mail après avoir installé et utilisé un certain nombre de fois votre système de messagerie, McAfee vous recommande d'effectuer au moins une fois cette opération d'analyse, de manière à vous assurer que vos anciens messages électroniques ne contiennent pas de virus.

REMARQUE : Une fois que vous avez téléchargé un message sur votre ordinateur, le logiciel VirusScan traite votre dossier personnel ou fichier d'archives comme tout autre fichier, à moins que vous ne l'ayez exclu explicitement des opérations d'analyse. Cette fonctionnalité vous assure un niveau de protection supérieur contre les virus.

- **Tous les messages surlignés.** Cliquez sur ce bouton pour que l'extension recherche les virus uniquement dans les messages électroniques que vous sélectionnez parmi les messages stockés dans votre boîte de réception Microsoft Exchange ou Microsoft Outlook.

2. Pour limiter cette opération d'analyse de sorte que seuls les messages non lus soient examinés, cochez la case **Analyser uniquement les messages non lus**. Selon l'option que vous sélectionnez à l'Étape 1, cela signifie que l'extension analysera tous les messages non lus contenus dans votre boîte aux lettres ou dans les dossiers publics accessibles, ou elle analysera tous les messages non lus compris dans la plage sélectionnée.
3. Spécifiez les types de fichiers que l'extension doit examiner. Vous pouvez :
   - **Analyser les fichiers compressés.** Cochez la case **Fichiers compressés** pour que l'extension Analyse E-Mail recherche les virus dans les fichiers compressés et dans les fichiers d'archives. Bien qu'il offre une protection supplémentaire, l'examen des fichiers compressés peut ralentir l'opération d'analyse.

     L'extension analyse les mêmes types de fichiers compressés et d'archives que l'application VirusScan. Pour afficher la liste de ces fichiers et archives, reportez-vous à la section « Liste en cours des fichiers compressés analysés » à la page 352.
   - **Analyser tous les fichiers**. Cochez la case **Tous les fichiers** pour que l'extension Analyse E-Mail analyse tous les types de fichiers contenus dans votre boîte aux lettres, quelles que soient les extensions de nom de fichier.

     REMARQUE : McAfee recommande de sélectionner cette option pour votre première opération d'analyse, ou à intervalles réguliers par la suite, de manière à garantir que votre boîte aux lettres est exempte de tout virus. Vous pouvez ensuite limiter la portée des opérations d'analyse ultérieures.

- **Choisir les types de fichiers**. D'ordinaire, les virus ne peuvent infecter les fichiers qui ne contiennent pas de code exécutable, que ce soit du code de script, de macro ou binaire. Vous pouvez par conséquent limiter en toute sécurité la portée de vos opérations d'analyse aux fichiers les plus susceptibles d'être infectés par des virus. Pour ce faire, cliquez sur le bouton **Fichiers programme uniquement**.

  Pour afficher ou désigner les types de fichiers que le module Analyse E-Mail doit examiner, cliquez sur **Extensions**. Ceci ouvre la boîte de dialogue Extensions de fichiers programme. Pour en savoir plus sur la modification des fichiers répertoriés à cet endroit, reportez-vous à la section « Ajout d'extensions de fichier pour analyse » à la page 345.

4. Activer l'analyse heuristique. Cliquez sur **Options avancées** pour ouvrir la boîte de dialogue Paramètres d'analyse avancés (Figure 8-3).

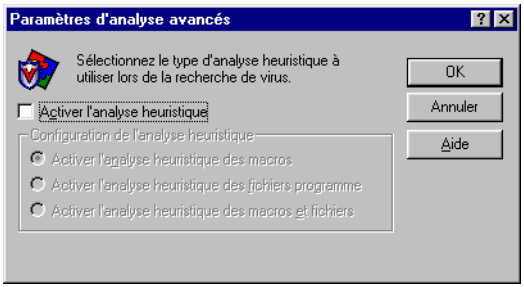

Figure 8-3. Boîte de dialogue Paramètres d'analyse avancés

La technologie d'analyse heuristique permet à l'extension Analyse E-Mail de reconnaître les nouveaux virus à partir de leur ressemblance avec des virus semblables déjà identifiés. Pour ce faire, l'extension recherche des caractéristiques propres aux virus dans les fichiers que vous lui avez demandé d'analyser. Si elle détecte un nombre suffisant de caractéristiques dans un fichier, l'extension identifie le fichier comme étant potentiellement infecté par un nouveau virus ou un virus non identifié.

L'extension recherche en même temps des caractéristiques qui dénotent de l'absence de virus, c'est pourquoi il ne se trompe que rarement en vous signalant une infection. À moins d'être certain que votre fichier ne contient *pas* de virus, vous devez apporter aux infections « probables » les mêmes précautions que vous apportez aux infections confirmées.

Lorsque vous démarrez l'extension Analyse E-Mail, aucune option d'analyse heuristique n'est activée par défaut. Pour activer l'analyse heuristique, procédez comme suit :

a. Cochez la case **Activer l'analyse heuristique**. Les options proposées dans le reste de la boîte de dialogue deviennent accessibles.

b. Sélectionnez les types d'analyses heuristiques que l'extension Analyse E-Mail doit utiliser. Vous avez le choix entre les options suivantes :

- **Activer l'analyse heuristique des macros.** Sélectionnez cette option pour que l'extension identifie d'abord tous les fichiers Microsoft Word, Microsoft Excel et autres fichiers Microsoft Office incorporant des macros et compare ensuite le code de la macro avec sa base de données de définitions de virus. Si la correspondance est exacte, l'extension identifie le nom du virus ; pour les chaînes de signature qui ressemblent à celles de virus existants, elle vous informe qu'elle a détecté un virus de macro « probable ».
- **Activer l'analyse heuristique des fichiers programme.** Sélectionnez cette option si vous souhaitez que l'extension Analyse E-Mail localise de nouveaux virus dans les fichiers programme en examinant les caractéristiques des fichiers et en les comparant avec celles figurant sur une liste de virus connus. Lorsqu'elle détecte un fichier ayant un certain nombre de caractéristiques, l'extension l'identifie comme étant potentiellement infecté.
- **Activer l'analyse heuristique des macros et fichiers programme.** Sélectionnez cette option si vous souhaitez que l'extension utilise les deux types d'analyse heuristique. McAfee vous recommande d'utiliser cette option pour une protection antivirus optimale.

❑ **REMARQUE :** L'extension n'utilise les techniques d'analyse heuristique que sur les types de fichiers que vous désignez dans la boîte de dialogue Extensions de fichiers programme. Si vous décidez d'analyser **Tous les fichiers**, elle appliquera l'analysera heuristique à tous les types de fichiers.

---

c. Cliquez sur **OK** pour enregistrer vos paramètres et revenir à la boîte de dialogue Propriétés de l'Analyse E-Mail.

5. Cliquez sur l'onglet Action pour sélectionner d'autres options de l'extension Analyse E-Mail. Pour enregistrer vos modifications sans fermer la boîte de dialogue Propriétés de l'Analyse E-Mail, cliquez sur **Appliquer**. Pour enregistrer vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans enregistrer vos modifications, cliquez sur **Annuler**.

> **REMARQUE :** Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

Sélection des options d'action

Lorsque l'extension Analyse E-Mail détecte un virus, deux cas de figure se présentent : soit elle vous demande comment traiter du fichier infecté, soit elle exécute automatiquement une action que vous avez définie précédemment. Utilisez la page de propriétés Action pour spécifier les actions que l'extension doit vous proposer en cas de détection d'un virus et celles qu'elle doit mettre en œuvre automatiquement.

Procédez comme suit :

1. Cliquez sur l'onglet Action dans la boîte de dialogue Propriétés de l'Analyse E-Mail pour afficher la page de propriétés correspondante (Figure 8-4).

Figure 8-4. Boîte de dialogue Propriétés de l'Analyse E-Mail – page Action

2. Sélectionnez une réponse dans la liste **En cas de détection d'un virus**. La zone située juste au-dessous de la liste se modifiera pour vous proposer d'autres options pour chacun de vos choix.

   Vous avez le choix entre les options suivantes :

   - **Interroger l'utilisateur.** Sélectionnez cette option si vous pensez que vous serez auprès de votre ordinateur lorsque l'extension Analyse E-Mail examinera votre boîte aux lettres. Le cas échéant, le programme affichera un message d'alerte s'il détecte un virus et vous proposera plusieurs actions possibles.

     Pour chaque case que vous cochez dans la page Action, un bouton d'option apparaîtra dans le message d'alerte que l'extension affichera en cas de détection d'un virus. Ainsi, si vous cochez par exemple la case **Supprimer le fichier**, le message d'alerte comportera un bouton **Supprimer**.

     Vous avez le choix entre les options suivantes :

     – **Nettoyer le fichier.** Cette option demande à l'extension d'essayer de supprimer le code de virus dans le fichier infecté. Si vous avez activé la fonction de rapport, l'application enregistrera l'événement dans un journal à chaque fois qu'elle parviendra ou non à nettoyer un fichier infecté.

  - **Supprimer le fichier.** Cette option demande à l'extension de supprimer immédiatement le fichier infecté.
  - **Déplacer le fichier.** Cette option demande à l'extension de placer le fichier infecté dans un dossier de quarantaine. Le message d'alerte affichera un bouton **Déplacer le fichier** pour vous permettre de placer l'élément infecté dans le dossier de quarantaine, situé sur votre serveur Microsoft Exchange. Vous pouvez déplacer les éléments infectés vers n'importe quel autre dossier créé dans votre boîte aux lettres Exchange ou Outlook ou les déplacer vers n'importe quel dossier public auquel vous avez accès sur le serveur Exchange. L'élément demeure sur le serveur Exchange jusqu'à ce que vous le supprimiez (il n'est pas téléchargé sur votre ordinateur).
  - **Poursuivre l'analyse.** Cette option demande à l'extension de poursuivre son analyse sans prendre d'autres mesures. Si vous avez activé ses options de rapport, l'extension enregistre l'incident dans son fichier journal.
  - **Arrêter l'analyse.** Cette option demande à l'extension d'interrompre immédiatement l'opération d'analyse. Pour continuer, vous devez à nouveau cliquer sur  dans votre barre d'outils Exchange ou Outlook, ou sélectionner **Recherche de virus** dans le menu **Outils** pour redémarrer l'opération.

- **Déplacer automatiquement les fichiers infectés.** Sélectionnez cette option de réponse pour que l'extension déplace les fichiers infectés vers un dossier de quarantaine situé sur votre serveur Microsoft Exchange, dès leur détection. L'extension place ces fichiers dans un dossier nommé Infecté, situé sur le serveur Microsoft Exchange.
- **Nettoyer automatiquement les fichiers infectés.** Sélectionnez cette option cette réponse pour que l'extension supprime le code de virus dans la pièce jointe infectée dès sa détection. Si l'extension ne parvient pas à supprimer le virus, elle notera l'incident dans son fichier journal.
- **Supprimer les fichiers infectés automatiquement.** Sélectionnez cette option pour que l'extension supprime immédiatement toute pièce jointe infectée détectée. Assurez-vous d'avoir activé la fonction de rapport, afin de disposer d'une liste des fichiers supprimés par l'extension. Si l'extension ne parvient pas à supprimer un fichier infecté, elle notera l'incident dans son fichier journal.

- **Poursuivre l'analyse.** N'utilisez cette option que si vous prévoyez d'être absent au moment où l'application recherchera les virus. Si vous activez également la fonction de rapport, l'application enregistrera le nom des virus détectés et le nom des fichiers infectés, pour vous permettre de les supprimer à une prochaine occasion.

AVERTISSEMENT : L'extension Analyse E-Mail *ne* tente pas de décrypter les messages cryptés pour les analyser. Si une pièce jointe infectée contient une signature numérique, l'extension *supprime* la signature numérique pour pouvoir nettoyer ou supprimer le fichier infecté.

3. Cliquez sur l'onglet Alerte pour sélectionner d'autres options de l'extension Analyse E-Mail. Pour enregistrer vos modifications sans fermer la boîte de dialogue Propriétés de l'Analyse E-Mail, cliquez sur **Appliquer**. Pour enregistrer vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans enregistrer vos modifications, cliquez sur **Annuler**.

REMARQUE : Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

Sélection des options d'alerte

Une fois que vous avez configuré l'extension Analyse E-Mail avec les options de réponses voulues, vous pouvez la laisser rechercher les virus et les supprimer automatiquement de votre boîte aux lettres Exchange dès qu'elle en trouve, sans presque nécessiter d'autres interventions de votre part. Toutefois, pour que l'extension vous informe immédiatement de la détection d'un virus de sorte que vous puissiez entreprendre l'action appropriée, vous devez la configurer pour qu'elle vous envoie un message d'alerte.

Procédez comme suit :

1. Cliquez sur l'onglet Alerte de la boîte de dialogue Propriétés de l'Analyse E-Mail pour afficher la page de propriétés correspondante (Figure 8-5).

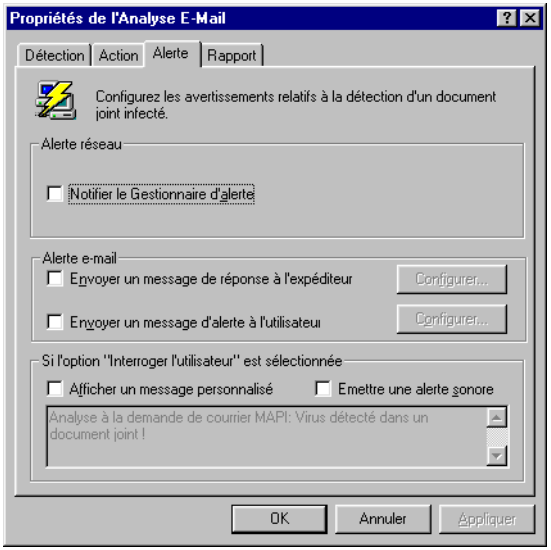

Figure 8-5. Boîte de dialogue Propriétés de l'Analyse E-Mail – page Alerte

2. Cochez la case **Notifier le Gestionnaire d'alerte**pour que l'extension Analyse E-Mail envoie des messages d'alerte au Gestionnaire d'alerte qui les transmettra.

   Le Gestionnaire d'alerte est un composant indépendant du logiciel McAfee qui regroupe des messages d'alerte et utilise diverses méthodes pour les envoyer aux destinataires que vous désignez. L'extension enverra ces messages d'alerte avec succès uniquement si vous avez installé l'utilitaire de Configuration cliente du Gestionnaire d'alerte. Pour plus de détails, reportez-vous à la section Voir « Utilisation de l'utilitaire de Configuration cliente du Gestionnaire d'alerte » à la page 338.

   Vous pouvez transmettre des messages d'alerte directement à un serveur du Gestionnaire d'alerte. Sinon, vous pouvez les envoyer en tant que fichiers texte (.ALR) à un répertoire d'alerte centralisée que le serveur du Gestionnaire d'alerte interroge régulièrement.

   ☐ **REMARQUE :** Si vous décochez cette case, l'extension Analyse E-Mail n'enverra pas des messages d'alerte via le Gestionnaire d'alerte, mais tous les autres messages d'alerte que vous configurez dans cette page de propriétés resteront intacts.

En tant que partie intégrante de votre système d'alerte antivirus, l'extension Analyse E-Mail peut répondre directement par un message d'alerte à l'utilisateur qui vous a envoyé le message ou le document joint infecté. Vous pouvez envoyer une copie de ce message à d'autres destinataires, que ce soit à l'intérieur ou à l'extérieur de votre entreprise.

Si vous préférez ne pas envoyer de réponse, vous pouvez configurer l'extension pour envoyer une notification par e-mail à l'administrateur système par exemple, à chaque fois qu'elle détecte un virus.

L'envoi de messages de réponse facilite l'identification des sources des virus et de leurs points d'entrée dans votre réseau, alors que les copies de ces messages envoyées aux administrateurs système leur permettent plutôt d'identifier la méthode de propagation utilisée par les virus.

Vous avez également la possibilité d'envoyer un message à n'importe quel destinataire sans répondre à l'émetteur du document joint infecté. L'extension Analyse E-Mail peut extraire les destinataires directement de votre carnet d'adresses Microsoft Exchange, Microsoft Outlook, ou de tout autre carnet d'adresses conforme à la norme MAPI, ou d'un annuaire Lotus cc:Mail équivalent. Sinon, vous pouvez entrer les adresses des destinataires directement.

Le message que vous créez pour une réponse est un modèle ; l'extension Analyse E-Mail l'enverra automatiquement à chacun des destinataires que vous désignez. C'est pourquoi McAfee vous recommande de créer un message pouvant être lu et compris par tous les destinataires. À l'exception de la rédaction du modèle de message, l'extension ne vous permettra pas de modifier le message avant de l'envoyer.

Vous pouvez envoyer un message pour répondre à l'émetteur du message infecté et un message différent pour les autres destinataires, mais vous ne pouvez pas créer un même message pour des destinataires différents.

3. Pour créer vos modèles de message, procédez comme suit :

   a. Cochez la case **Envoyer un message de réponse à l'expéditeur** dans la page de propriétés Alerte, puis cliquez sur **Configurer** pour ouvrir un formulaire de message e-mail standard.

      Dans la mesure où l'extension Analyse E-Mail enverra ce message directement à l'émetteur du message e-mail infecté, le bouton **A:** et la zone de texte correspondante ne sont pas disponibles.

   b. Pour envoyer une copie de ce message à quelqu'un d'autre, entrez une adresse électronique dans la zone de texte intitulée Copie à: ou cliquez sur **Copie à:** pour choisir un destinataire dans l'annuaire d'utilisateurs ou le carnet d'adresses de votre système e-mail.

> **REMARQUE :** Pour retrouver une adresse électronique dans l'annuaire d'utilisateurs de votre système e-mail, vous devez stocker les adresses dans un annuaire d'utilisateurs, une base de données ou un carnet d'adresses compatible MAPI, ou dans un annuaire Lotus cc:Mail équivalent. Si vous n'êtes pas encore connecté à votre système e-mail, l'extension module Analyse E-Mail tente d'utiliser votre profil MAPI par défaut pour se connecter à des systèmes e-mail compatibles MAPI. Sinon, il vous invite à saisir un nom d'utilisateur, un mot de passe et un chemin d'accès à votre boîte aux lettres Lotus cc:Mail. Entrez les informations nécessaires à l'extension, puis cliquez sur **OK** pour continuer.

c. Indiquez un objet qui laisse apparaître le caractère urgent de votre message, puis ajoutez vos commentaires dans le corps du message, sous un avis d'infection standard qui sera fourni par l'extension. Vous pouvez ajouter jusqu'à 1 024 caractères de texte.

d. Cliquez sur **OK** pour enregistrer le message.

   À chaque fois qu'elle détectera un virus, l'extension enverra une copie de ce message à la personne qui vous a envoyé le courrier électronique comportant un document joint infecté. Elle remplira l'adresse du destinataire avec les informations de l'en-tête du message d'origine, et identifiera le virus et le fichier infecté dans la zone située immédiatement après la ligne Objet. De plus, si vous avez activé sa fonction de rapport, l'extension y mentionnera tout message d'alerte qu'elle aura envoyé.

e. Pour envoyer un message d'alerte à d'autres utilisateurs, un administrateur réseau par exemple, à propos d'un document joint infecté, cochez la case **Envoyer un message d'alerte à l'utilisateur** dans la page de propriétés Alerte. Vous pouvez ensuite créer une réponse standard, tel que vous l'avez fait dans les étapes Étape a à Étape d ci-dessus. Dans ce cas, vous pouvez remplir les zones de texte A: et Copie à:

   Dès qu'elle détectera un virus, l'extension Analyse E-Mail enverra une copie de ce message à toutes les adresses que vous avez spécifiées dans ce message.

4. Cochez la case**Émettre une alerte sonore** pour que l'extension envoie un signal sonore à chaque fois qu'elle trouve un fichier infecté.

Vous pouvez modifier le paramétrage de cette option à condition d'avoir sélectionné **Interroger l'utilisateur** dans la page de propriétés Action. Sinon, la case à cocher Émettre une alerte sonore affichera et utilisera le paramètre que vous lui avez attribué la dernière fois que vous avez sélectionné l'option **Interroger l'utilisateur**.

L'extension émettra le signal sonore standard du système ou exécutera le fichier .WAV que vous avez configuré sur votre ordinateur.

5. Cochez la case **Afficher un message personnalisé** pour que l'extension ajoute un message personnalisé au texte du message qu'elle affiche lorsqu'elle trouve un fichier infecté.

   À l'égard de l'alerte sonore, vous pouvez modifier le paramétrage de cette option à condition d'avoir sélectionné **Interroger l'utilisateur** dans la page de propriétés Action. Si vous ne sélectionnez pas cette option dans la page Action, aucun message d'alerte ou message personnalisé ne s'affichera même si vous avez coché la case Afficher un message personnalisé.

6. Entrez le message que l'extension doit afficher dans la zone de texte. Vous pouvez entrer 250 caractères maximum.

7. Cliquez sur l'onglet Rapport pour sélectionner d'autres options de l'extension Analyse E-Mail. Pour enregistrer vos modifications sans fermer la boîte de dialogue Propriétés de l'Analyse E-Mail, cliquez sur **Appliquer**. Pour enregistrer vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans enregistrer vos modifications, cliquez sur **Annuler**.

   REMARQUE : Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

Sélection des options de rapport

L'Analyse E-Mail répertorie ses paramètres actuels et résume toutes les actions entreprises au cours de ses opérations d'analyse dans un fichier journal nommé MAILSCAN.TXT. Vous pouvez faire en sorte que l'Analyse E-Mail écrive son journal dans ce fichier ou vous pouvez utiliser n'importe quel éditeur de texte pour créer un fichier texte destiné à être utilisé par l'Analyse E-Mail. Vous pouvez ensuite ouvrir et imprimer le fichier journal, à partir de l'Analyse E-Mail ou d'un éditeur de texte, pour effectuer des vérifications ultérieures.

Vous pouvez utiliser le fichier MAILSCAN.TXT pour suivre l'activité des virus sur votre système et pour noter les paramètres que l'extension a utilisé pour détecter les infections et répondre à celles trouvées. Vous pouvez également utiliser les rapports d'incidents enregistrés dans le fichier pour déterminer quels fichiers vous devez examiner en quarantaine ou supprimer de votre système.

Pour configurer l'extension Analyse E-Mail de sorte qu'elle enregistre ses actions dans un fichier journal, procédez comme suit :

1. Cliquez sur l'onglet Rapport de la boîte de dialogue Propriétés de l'Analyse E-Mail pour afficher la page de propriétés correspondante (Figure 8-6).

Figure 8-6. Boîte de dialogue Propriétés de l'Analyse E-Mail – page Rapport

2. Cochez la case **Consigner dans le fichier**.

   Par défaut, l'extension Analyse E-Mail consigne les informations de journal dans le fichier MAILSCAN.TXT, situé dans le répertoire du programme VirusScan. Vous pouvez entrer un autre nom dans la zone de texte affichée ou cliquer sur **Parcourir** pour trouver un fichier approprié sur votre disque dur ou votre réseau. Vous pouvez utiliser un fichier différent, mais le fichier texte doit être déjà créé. L'extension ne créera pas un nouveau fichier.

REMARQUE : Si vous choisissez un emplacement différent pour votre fichier journal sur un système exécutant Windows NT Workstation version 4.0 ou Windows 2000 Professionnel, vérifiez que vous bénéficiez d'un accès de niveau utilisateur à cet emplacement. Étant donné que l'extension Analyse E-Mail est exécutée avec les mêmes droits d'accès que ceux utilisés par votre programme client e-mail, elle ne peut pas écrire correctement dans ce fichier journal si le fichier se situe à un emplacement nécessitant des droits d'accès de niveau administrateur et si vous vous êtes connecté en tant qu'utilisateur pour exécuter votre programme client e-mail. Dans ce cas, l'extension Analyse E-Mail génère un message « Erreur d'accès au journal d'activité » en cas de détection d'un virus.

3. Pour limiter la taille du fichier journal, cochez la case **Taille limite du fichier journal**, puis saisissez cette taille, en Kilo-octets, dans la zone de texte prévue à cet effet. Si vous ne cochez pas cette case, le fichier journal peut voir sa taille augmenter et atteindre une limite déterminée par votre espace disque.

   Entrez une valeur comprise entre 10 Ko et 999 Ko. Par défaut, l'extension limite la taille du fichier à 100 Ko. Si les données du journal dépassent la taille allouée pour le fichier, le moteur d'analyse efface le journal existant et le reprend au point où il s'était interrompu.

4. Cochez les cases correspondant aux informations que l'extension doit enregistrer dans son fichier journal. Chaque case cochée génère l'enregistrement par l'extension de l'information correspondante, généralement à la fin de l'opération d'analyse ou lorsque vous fermez votre système :

   - **Détecter les virus.** Cochez cette case pour que le fichier journal enregistre le nombre de virus trouvés par l'extension dans chaque opération d'analyse. Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.
   - **Éliminer les virus.** Cochez cette case pour que le fichier journal enregistre le nombre de fichiers infectés que l'extension nettoie (ou tente de nettoyer) au cours de chaque opération d'analyse. Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.
   - **Supprimer les fichiers infectés.** Cochez cette case pour que le fichier journal enregistre le nombre de virus supprimés par l'extension dans chaque opération d'analyse. Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.

- **Déplacer les fichiers infectés.** Cochez cette case pour que le fichier journal enregistre le nombre de virus que l'extension a placé dans un dossier de quarantaine dans chaque opération d'analyse. Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.
- **Paramètres de session.** Cochez cette case pour que le fichier journal enregistre les paramètres de configuration que vous avez utilisés pour l'extension dans chaque opération d'analyse. Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.
- **Résumé de session.** Cochez cette case pour que le fichier journal récapitule les actions effectuées par l'extension dans chaque opération d'analyse. Le journal enregistrera les informations suivantes :
  - Nombre de fichiers analysés par l'extension.
  - Nombre de fichiers infectés nettoyés par l'extension.
  - Nombre de fichiers infectés supprimés par l'extension.
  - Nombre de fichiers infectés que l'extension a placé dans un dossier de quarantaine.
  - Paramètres de l'extension.

  Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.
- **Date et heure.** Cochez cette case pour que le fichier journal enregistre la date et l'heure de début de votre opération d'analyse. Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.
- **Nom d'utilisateur.** Cochez cette case pour que le fichier journal enregistre le nom de l'utilisateur connecté à la station de travail lorsque l'extension démarre chaque opération d'analyse. Ne cochez pas cette case si vous souhaitez exclure ces informations du fichier journal.

5. Cliquez sur un autre onglet pour modifier des paramètres quelconques de l'extension Analyse E-Mail. Pour enregistrer vos modifications sans fermer la boîte de dialogue Propriétés de l'Analyse E-Mail, cliquez sur **Appliquer**. Pour enregistrer vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans enregistrer vos modifications, cliquez sur **Annuler**.

REMARQUE : Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

Analyse de cc:Mail

Le logiciel VirusScan inclut une prise en charge native pour les clients Microsoft Exchange et Outlook, ainsi que pour Lotus cc:Mail version 6.0, version 7.0 et version 8.0. Les clients cc:Mail utilisent un système e-mail qui leur est propre et que l'extension Analyse E-Mail ne prend pas directement en charge. À la place, le logiciel VirusScan inclut une extension spécialisée pour cc:Mail qui se greffe au logiciel VShield, ouvre une session de votre système cc:Mail, puis fonctionne de manière discrète en arrière-plan, en interrogeant votre boîte de réception cc:Mail pour y vérifier l'arrivée de nouveaux messages. Lorsqu'un nouveau message arrive, le moteur d'analyse cc:Mail l'examine pour y détecter d'éventuelles pièces jointes infectées avant que le logiciel client ne le télécharge sur votre ordinateur.

Le choix du système de messagerie commerciale que le moteur d'analyse VShield doit examiner pour y détecter des virus constitue la seule véritable interaction que vous avez avec cc:Mail Scan. Pour en savoir plus sur la spécification de cc:Mail en tant que système de messagerie commerciale, reportez-vous à la section « Sélection des options de détection » à la page 138.

Si vous vous connectez à votre serveur cc:Mail pour la première fois, le moteur d'analyse cc:Mail peut également vous demander d'entrer votre nom d'utilisateur et un mot de passe dans un écran de connexion de sorte qu'il puisse accéder à votre serveur cc:Mail et analyser votre boîte de réception. Entrez votre nom d'utilisateur et votre mot de passe cc:Mail, comme si vous vous connectiez normalement à cc:Mail, puis cliquez sur **OK** pour continuer. Ensuite, démarrez votre application cliente cc:Mail et définissez un intervalle supérieur à cinq minutes pour l'interrogation de votre serveur cc:Mail par le client. Ceci permet au logiciel VShield d'examiner votre courrier avant que le logiciel client ne le récupère.

Le composant cc:Mail se déconnecte automatiquement de votre serveur e-mail lorsque vous quittez le logiciel client.

Utilisation de l'utilitaire ScreenScan

L'utilitaire ScreenScan analyse votre système en arrière-plan au moment où votre écran de veille est en exécution. Ce procédé permet à votre système de tirer parti des périodes d'inactivité pour veiller à sa propre sécurité. Lorsqu'il détecte un virus, ScreenScan se contente d'en prendre note dans le fichier journal afin que vous puissiez le consulter quand vous en aurez le loisir.

REMARQUE : Pour pouvoir utiliser ScreenScan, vous devez sélectionner l'option d'installation Personnalisée au cours de l'installation (l'utilitaire d'installation n'installe pas ce composant par défaut). Pour plus de détails, reportez-vous à la section Voir « Procédure d'installation » à la page 45.

Une fois installé, ScreenScan affiche une page de propriétés dans la boîte de dialogue Propriétés d'affichage de Windows. Cette page vous permet de sélectionner les options de détection et de rapport que ScreenScan doit utiliser.

À condition d'avoir configuré et activé l'utilitaire, il démarre au démarrage de l'écran de veille de votre ordinateur et s'arrête lorsque vous déplacez la souris, appuyez sur une touche du clavier ou effectuez une autre action interrompant votre écran de veille.

Pour configurer ScreenScan, procédez comme suit :

1. Cliquez sur **Démarrer** dans la barre des tâches Windows, pointez sur **Paramètres**, puis choisissez **Panneau de configuration**.
2. Localisez dans la fenêtre qui s'affiche l'icône Affichage du panneau de configuration et double-cliquez dessus pour ouvrir la boîte de dialogue Propriétés de l'affichage. Ensuite, cliquez sur l'onglet ScreenScan (Figure 8-7 à la page 325).

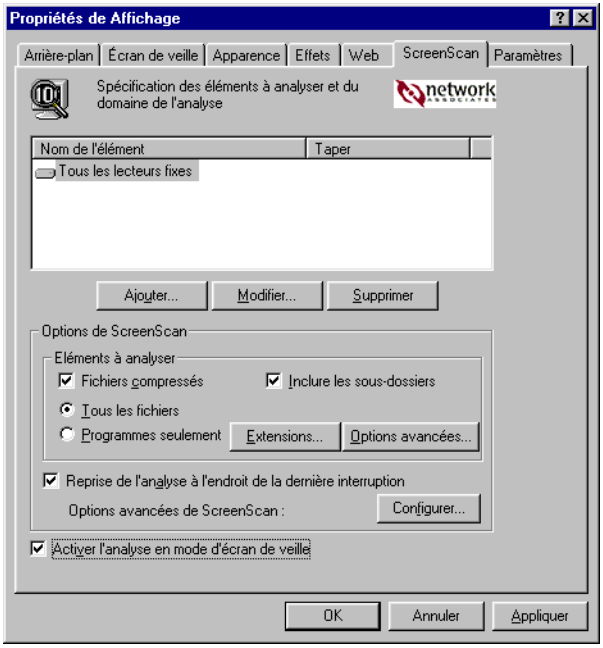

Figure 8-7. Boîte de dialogue Propriétés de l'affichage – page ScreenScan

3. Cochez la case **Activer l'analyse en mode écran de veille** pour activer les autres options de la page de propriétés.

4. Sélectionnez les parties de votre système que l'utilitaire ScreenScan doit analyser. Vous pouvez :

   - **Ajouter des cibles à analyser.** Cliquez sur **Ajouter** pour ouvrir la boîte de dialogue Ajout d'un élément à analyser (voir Figure 8-8 à la page 325).

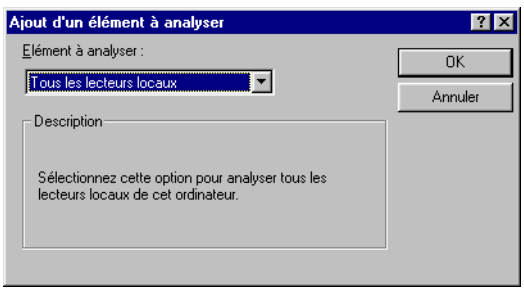

Figure 8-8. Boîte de dialogue Ajout d'un élément à analyser

Sélectionnez ensuite la cible à analyser dans la liste qui vous est proposée. Vous avez le choix entre les options suivantes :

- **Tous les lecteurs locaux.** Ceci indique à l'utilitaire d'analyser tous les lecteurs attachés physiquement à votre ordinateur, y compris les lecteurs médias amovibles.
- **Lecteur ou dossier.** Ceci indique à l'utilitaire d'analyser des fichiers ou dossiers donnés de votre système. Entrez, dans la zone de texte prévue à cet effet, la lettre du lecteur ou le chemin d'accès au dossier que vous souhaitez analyser. Vous pouvez également cliquer sur **Parcourir** pour rechercher la cible d'analyse sur votre ordinateur.
- **Tous les lecteurs fixes.** Ceci indique à l'utilitaire d'analyser les disques durs physiquement connectés à votre ordinateur.

Lorsque vous avez choisi votre cible, cliquez sur **OK** pour fermer la boîte de dialogue.

- **Modifier les cibles à analyser.** Sélectionnez une des cibles à analyser répertoriées, puis cliquez sur **Modifier** pour ouvrir la boîte de dialogue Modifier l'élément à analyser (Figure 8-9).

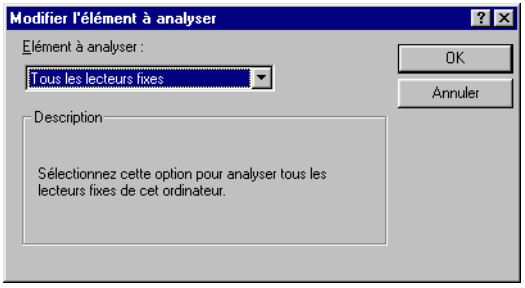

Figure 8-9. Boîte de dialogue Modifier l'élément à analyser

La boîte de dialogue s'affiche avec les cibles à analyser actuellement spécifiées. Choisissez ou entrez une nouvelle cible puis cliquez sur **OK** pour fermer la boîte de dialogue.

- **Supprimer les cibles à analyser.** Sélectionnez l'une des cibles de la liste, puis cliquez sur **Supprimer** pour l'effacer.

5. Spécifiez les types de fichiers que l'utilitaire ScreenScan doit examiner. Vous pouvez :

- **Analyser les fichiers compressés**. Cochez la case **Fichiers compressés** pour que l'utilitaire recherche les virus éventuels dans les fichiers compressés ou dans les fichiers d'archives. Pour afficher la liste des types de fichiers et d'archives que l'application analyse, reportez-vous à la section « Liste en cours des fichiers compressés analysés » à la page 352.

- **Analyser les sous-dossiers contenus dans la cible spécifiée**. Cochez la case **Inclure les sous-dossiers** si vous souhaitez que l'utilitaire recherche les virus dans les dossiers contenus dans votre cible à analyser.

  REMARQUE : Si vous sélectionnez **Inclure les sous-dossiers**, l'utilitaire analyse uniquement les fichiers stockés dans les sous-dossiers eux-mêmes. Il n'analyse pas les fichiers stockés à la racine du dossier que vous spécifiez. Pour analyser ces fichiers, décochez la case **Inclure les sous-dossiers**.

- **Analyser tous les fichiers**. Cochez la case **Tous les fichiers** pour que l'utilitaire analyse tous les fichiers contenus dans la boîte aux lettres ou le dossier public que vous spécifiez, quelle qu'en soit l'extension.

  REMARQUE : McAfee recommande de sélectionner cette option pour votre première opération d'analyse, ou à intervalles réguliers par la suite, de manière à garantir que votre système est exempt de tout virus. Vous pouvez ensuite limiter la portée des opérations d'analyse ultérieures.

- **Choisir les types de fichiers**. D'ordinaire, les virus ne peuvent infecter les fichiers qui ne contiennent pas de code exécutable, que ce soit du code de script, de macro ou binaire. Vous pouvez par conséquent limiter en toute sécurité la portée de vos opérations d'analyse aux fichiers les plus susceptibles d'être infectés par des virus. Pour ce faire, cliquez sur le bouton **Fichiers programme uniquement**.

  Pour afficher ou spécifier les extensions de nom de fichier que l'utilitaire ScreenScan doit examiner, cliquez sur **Extensions**. Ceci ouvre la boîte de dialogue Extensions de fichiers programme. Pour en savoir plus sur la modification des fichiers répertoriés à cet endroit, reportez-vous à la section « Ajout d'extensions de fichier pour analyse » à la page 345.

6. Activer l'analyse heuristique. Cliquez sur **Options avancées** pour ouvrir la boîte de dialogue Paramètres d'analyse avancés (voir Figure 8-10 à la page 328).

   La technologie d'analyse heuristique permet à l'utilitaire ScreenScan de reconnaître les nouveaux virus en fonction de leur ressemblance avec des virus similaires déjà identifiés. Pour ce faire, l'utilitaire recherche des caractéristiques propres aux virus dans les fichiers que vous lui avez demandé d'analyser.

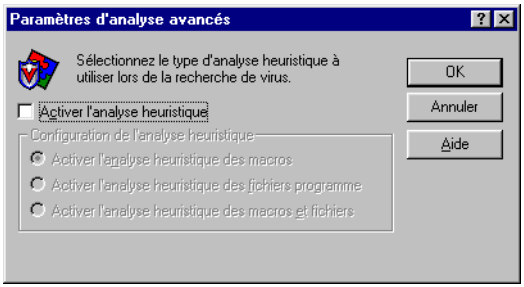

Figure 8-10. Boîte de dialogue Paramètres d'analyse avancés

   S'il détecte un nombre suffisant de caractéristiques dans un fichier, l'utilitaire identifie le fichier comme étant potentiellement infecté par un nouveau virus ou un virus non identifié.

   L'utilitaire recherche en même temps des caractéristiques qui dénotent de l'absence de virus, c'est pourquoi il ne se trompe que rarement en vous signalant une infection. À moins d'être certain que votre fichier ne contient *pas* de virus, vous devez apporter aux infections « probables » les mêmes précautions que vous apportez aux infections confirmées.

   Lorsque vous démarrez l'utilitaire ScreenScan, aucune option d'analyse heuristique n'est activée par défaut. Pour activer l'analyse heuristique, procédez comme suit :

   a. Cochez la case **Activer l'analyse heuristique**. Les options proposées dans le reste de la boîte de dialogue deviennent accessibles.

   b. Sélectionnez les types d'analyses heuristiques que l'utilitaire ScreenScan doit utiliser. Vous avez le choix entre les options suivantes :

- **Activer l'analyse heuristique des macros**. Sélectionnez cette option pour que l'utilitaire identifie d'abord tous les fichiers Microsoft Word, Microsoft Excel et autres fichiers Microsoft Office incorporant des macros et compare ensuite le code de la macro avec sa base de données de définitions de virus. Si la correspondance est exacte, l'utilitaire identifie le nom du virus ; pour les chaînes de signature qui ressemblent à celles de virus existants, il vous informe qu'il a détecté un virus de macro « probable ».
- **Activer l'analyse heuristique des fichiers programme.** Sélectionnez cette option si vous souhaitez que l'utilitaire ScreenScan localise de nouveaux virus dans les fichiers programme en examinant les caractéristiques des fichiers et en les comparant avec celles figurant sur une liste de virus connus. Lorsqu'il détecte un fichier ayant un certain nombre de caractéristiques, l'utilitaire l'identifie comme étant potentiellement infecté.
- **Activer l'analyse heuristique des macros et fichiers programme.** Sélectionnez cette option si vous souhaitez que l'utilitaire utilise les deux types d'analyse heuristique. McAfee vous recommande d'utiliser cette option pour une protection antivirus optimale.

> **REMARQUE :** L'utilitaire n'utilise les techniques d'analyse heuristique que sur les types de fichiers que vous désignez dans la boîte de dialogue Extensions de fichiers programme. Si vous décidez d'analyser **Tous les fichiers**, il appliquera l'analysera heuristique à tous les types de fichiers.

7. Configurez l'utilitaire ScreenScan pour qu'il reprenne les opérations d'analyse qui ont été interrompues au point où elles se sont arrêtées. Sélectionnez **Reprendre l'analyse là où ScreenScan s'est arrêté**.

   Si vous ne cochez pas cette case, l'utilitaire commence à nouveau l'opération d'analyse à partir de la racine du premier lecteur spécifié en tant que cible à analyser, ce chaque fois que l'exécution de l'écran de veille commence. Ceci signifie que l'utilitaire peut analyser à plusieurs reprises certaines parties du système, en omettant totalement d'autres parties.

8. Définissez les options avancées de ScreenScan. Cliquez sur **Configurer** pour ouvrir la boîte de dialogue Options d'analyse avancées (Figure 8-11).

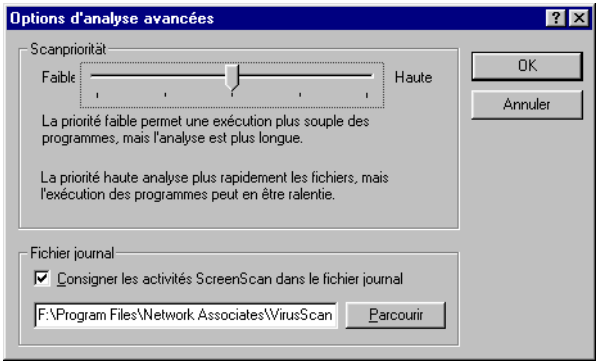

Figure 8-11. Boîte de dialogue Options d'analyse avancées

Vous avez le choix entre les options suivantes :

- **Définir une priorité d'exécution pour les tâches de ScreenScan**. Faites glisser le curseur de la priorité d'analyse vers **Haute** pour attribuer une priorité plus élevée aux ressources systèmes et au temps alloué à l'utilitaire ScreenScan qu'aux autres activités en arrière-plan, telles que les opérations de défragmentation du disque, qui sont effectuées pendant les périodes d'inactivité de votre ordinateur. Ceci ralentit l'exécution des autres activités.

  Faites glisser le curseur vers **Basse** pour attribuer une priorité plus élevée aux autres tâches d'arrière-plan qu'à l'utilitaire ScreenScan. Ceci ralentit l'exécution de l'utilitaire ScreenScan.

- **Indiquer à l'utilitaire d'enregistrer ses actions**. Cochez la case **Consigner les activités ScreenScan dans le fichier journal** pour que l'utilitaire ScreenScan résume les actions qu'il a entreprises au moment de son exécution dans le fichier SCREENSCAN ACTIVITY LOG.TXT.

  L'utilitaire enregistrera ses actions lorsque vous arrêterez la tâche ou le système. Si vous préférez enregistrer ces données dans un fichier texte différent, entrez son chemin d'accès et son nom dans la zone de texte pourvue à cet effet ou cliquez sur **Parcourir** pour localiser le fichier. L'utilitaire ScreenScan ne génère pas de fichier texte, il peut uniquement écrire dans un fichier existant.

9. Cliquez sur **Appliquer** pour enregistrer vos modifications sans fermer la boîte de dialogue Propriétés de l'affichage. Pour enregistrer vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans enregistrer vos modifications, cliquez sur **Annuler**.

> **REMARQUE :** Notez que le fait de cliquer sur **Annuler** n'annule aucune des modifications enregistrées précédemment au moyen du bouton **Appliquer**.

L'utilitaire ScreenScan sera exécuté à la prochaine exécution de votre écran de veille actuel. Si vous changez les écrans de veille, vous devez aussi reconfigurer les options d'utilitaire ScreenScan.

Utilisations des utilitaires VirusScan 9

Présentation du Panneau de configuration VirusScan

Le Panneau de configuration VirusScan sert d'interface graphique au service de gestion VirusScan, qui permet de démarrer et de contrôler l'ensemble des processus des composants de niveau supérieur, notamment l'application VirusScan, la console et le moteur d'analyse VShield. Le service de gestion VirusScan propose également une structure de mémoire commune pour l'intégralité des composants VirusScan, ce qui leur permet de partager des données ainsi que d'agir sur celles-ci.

En pratique, le panneau de configuration vous permet d'effectuer les opérations suivantes :

- démarrer et arrêter tous les composants VirusScan en utilisant un seul bouton ;
- demander le chargement du moteur d'analyse VShield et de la console VirusScan au démarrage de l'ordinateur ;
- définir un plafond pour le nombre de cibles à analyser que l'application VirusScan peut examiner ou exclure lors d'une session d'analyse ;
- limiter le nombre de tâches d'analyse que vous pouvez créer, configurer et exécuter à partir de la console VirusScan.

Vous pouvez en outre définir le chargement du service de gestion VirusScan au démarrage de votre ordinateur.

❑ **REMARQUE :** McAfee vous recommande vivement de définir le chargement du service de gestion VirusScan au démarrage de l'ordinateur. Si vous ne le faites pas, vous pouvez vous trouver dans l'impossibilité de démarrer certains composants VirusScan et vous ne bénéficierez pas du partage des données entre les différents composants.

Ouverture du panneau de configuration VirusScan

Le panneau de configuration VirusScan fonctionne de la même manière qu'un panneau de configuration Windows standard.

Pour ouvrir le panneau de configuration, procédez comme suit :

1. Cliquez sur **Démarrer** dans la barre des tâches Windows, pointez sur **Paramètres**, puis choisissez **Panneau de configuration**.
2. Localisez et double-cliquez sur l'icône du panneau de configuration VirusScan  pour l'ouvrir (voir Figure 9-1 à la page. 334).

Figure 9-1. Panneau de configuration VirusScan – page Service

Sélection des options du panneau de configuration VirusScan

Le Panneau de configuration se compose de deux pages de propriétés contenant plusieurs onglets, qui permettent de définir ses options.

Pour sélectionner vos options, procédez comme suit :

1. Ouvrez le panneau de configuration, puis cliquez sur l'onglet Service.
2. Pour arrêter tous les composants VirusScan actifs, cliquez sur **Arrêter**.

   Si tous les composants VirusScan qui se chargent habituellement dans la mémoire (normalement la console et le moteur d'analyse VShield) sont inactifs, ce bouton se présente sous la forme **Démarrer**. Cliquez dessus pour charger à nouveau les composants VirusScan inactifs.

   Vous pouvez également redémarrer indépendamment l'application VirusScan et la console à partir du menu **Démarrer** de Windows.
3. Cochez la case **Charger au démarrage** dans la zone Service VirusScan pour démarrer le service de gestion VirusScan (AVSYNMGR.EXE) au démarrage de votre ordinateur.

   Le service de gestion contrôle toutes les communications entre les composants de programme VirusScan, détermine les composants qui doivent être chargés pour effectuer les tâches de programme et vous permet de démarrer ou d'arrêter simultanément tous les composants de programme.

   Si votre ordinateur utilise Windows NT Workstation version 4.0 ou Windows 2000 Professionnel, ce service apparaît dans la boîte de dialogue Services en tant que Gestionnaire AvSync. Si votre ordinateur utilise Windows 95 ou Windows 98, ce service n'est pas directement accessible.

   ❑ **REMARQUE :** McAfee vous recommande vivement de définir le chargement du service de gestion VirusScan au démarrage de l'ordinateur. Si vous ne le faites pas, vous pouvez vous trouver dans l'impossibilité de démarrer certains composants VirusScan et vous ne bénéficierez pas du partage des données entre les différents composants.
4. Cliquez sur l'onglet Composants pour continuer (Figure 9-2 à la page. 336).

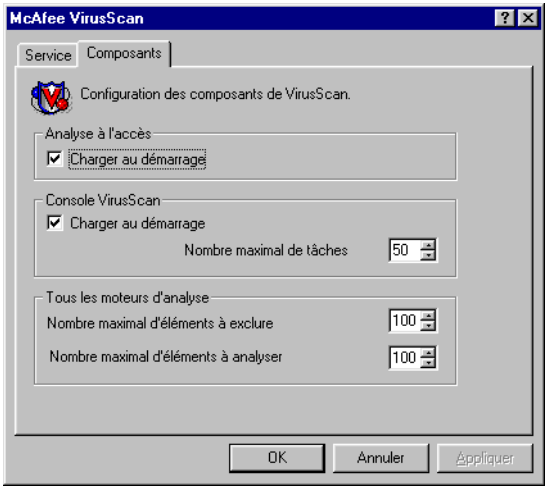

Figure 9-2. Panneau de configuration VirusScan – page Composants

5. Pour que le moteur d'analyse VShield se charge au démarrage de votre ordinateur, cochez la case **Charger VShield au démarrage**. Ce même paramètre apparaît dans la page Détection du module Analyse système. L'un ou l'autre paramètre chargera le moteur d'analyse au démarrage de votre ordinateur.

REMARQUE : McAfee recommande de laisser cette case cochée. Le moteur d'analyse VShield constitue votre meilleure protection permanente contre les infections par des virus.

---

6. Cliquez sur ou entrez un chiffre dans la zone de texte Éléments à exclure pour spécifier le nombre d'éléments qui peuvent figurer dans la liste des exclusions du module Analyse système de VShield. Ce paramètre détermine également le nombre d'éléments qui peuvent figurer dans la liste des exclusions pour toute tâche d'analyse effectuée par l'application VirusScan ou pour toute tâche d'analyse que vous configurez dans la console VirusScan..

   Par défaut, 100 éléments peuvent figurer dans la liste. Vous ne pouvez pas définir une valeur inférieure à cinq éléments pour ce paramètre.

7. Cliquez sur ou entrez un chiffre dans la zone de texte Éléments à analyser pour spécifier le nombre de cibles que l'application VirusScan peut examiner simultanément.

Ce paramètre définit un nombre maximal d'éléments qui peuvent figurer en tant que cibles à analyser pour toute tâche d'analyse par défaut ou pour toute tâche que vous configurez dans la console VirusScan. Par défaut, 100 éléments peuvent figurer dans la liste. Si vous ajoutez plus de 100 éléments uniques à la liste des exclusions, l'application VirusScan peut affecter les performances du système. Vous ne pouvez pas définir une valeur inférieure à cinq éléments pour ce paramètre.

8. Cochez la case **Charger au démarrage** dans la zone Console pour que la console VirusScan démarre au démarrage de votre ordinateur.

   La console doit être en cours d'exécution pour pouvoir effectuer toute tâche planifiée, notamment les tâches d'analyse, les tâches AutoUpgrade et les tâches AutoUpdate. Il n'est toutefois pas nécessaire de démarrer la console pour pouvoir démarrer le moteur d'analyse VShield.

9. Cliquez sur  ou entrez un chiffre dans la zone de texte Nombre maximal de tâches pour définir le nombre de tâches d'analyse qui peuvent figurer dans la fenêtre de la console VirusScan.

   Par défaut, 50 éléments peuvent figurer dans la liste. Si vous ajoutez plus de 50 éléments, l'exécution des tâches peut affecter les performances du système. Vous ne pouvez pas définir une valeur inférieure à cinq éléments pour ce paramètre.

10. Cliquez sur **Appliquer** pour enregistrer les modifications apportées aux paramètres sans fermer le panneau de configuration. Cliquez sur **OK** pour enregistrer vos modifications et fermer le panneau de configuration. Cliquez sur **Annuler** pour fermer le panneau de configuration sans enregistrer vos modifications.

REMARQUE : Le service de gestion VirusScan et tous les composants actifs VirusScan doivent redémarrer pour que les modifications apportées soient prises en compte.

Utilisation de l'utilitaire de Configuration cliente du Gestionnaire d'alerte

L'ensemble des logiciels antivirus McAfee incluent une grande variété de méthodes permettant de vous avertir lorsqu'un virus ou un autre logiciel nuisible a été détecté. Ces méthodes incluent notamment :

- des avertissements graphiques et en plein écran s'affichant sur votre ordinateur local, souvent accompagnés d'options de réponse ;
- des signaux sonores système et des messages personnalisés que vous pouvez composer ;
- des messages e-mail envoyés en tant que réponses aux personnes qui ont envoyé les éléments infectés ou des messages e-mail envoyés en tant qu'avertissements destinés à d'autres personnes pour les prévenir que vous avez reçu un élément infecté ;
- des fichiers journaux consignant les actions des composants VirusScan, y compris les événements de détection de virus et de réponse ;
- des affichages de statistiques de synthèse et en temps réel mettant à jour les événements de détection et de réponse.

Nombre de ces méthodes vous avertissent uniquement si vous vous trouvez devant votre ordinateur et que vous surveillez l'exécution des opérations d'analyse. Cependant, si vous gérez un réseau de stations de travail que vous souhaitez sécuriser, vous avez souvent besoin d'une méthode qui permette de vous avertir d'une infection, que vous vous trouviez devant une autre station de travail de votre réseau ou que vous ne soyez pas du tout connecté au réseau. Vous avez également besoin d'une méthode permettant de rassembler et de gérer dans un emplacement central les messages d'alerte provenant de l'ensemble du réseau, de sorte que vous puissiez répondre lorsque n'importe quelle station de travail détecte un fichier infecté.

McAfee propose le logiciel serveur du Gestionnaire d'alerte pour répondre précisément à ce besoin. Le logiciel vous permet de centraliser le rassemblement et le traitement des messages d'alerte, d'attribuer des désignations de priorité et des messages personnalisés à ces messages d'alerte, ainsi que de définir n'importe laquelle des 11 méthodes différentes permettant de les diffuser à vous-même ou à d'autres personnes. Avec les gammes de produits antivirus version 4.5, le serveur du Gestionnaire d'alerte est à présent livré en tant que programme indépendant fourni avec le logiciel antivirus NetShield de McAfee. Vous pouvez installer ce nouveau serveur du Gestionnaire d'alerte en association avec le logiciel NetShield ou vous pouvez l'installer isolément sur un ordinateur que vous souhaitez utiliser comme point de rassemblement des alertes.

Vous pouvez installer plusieurs serveurs du gestionnaire d'alerte, un serveur par domaine, ou un serveur sur chacune des machines d'un serveur en cluster. Dans le cas d'une telle installation, vous avez également la possibilité de transférer les messages d'alerte aux différents serveurs du gestionnaire d'alerte ; vous pouvez par conséquent les transférer aux autres ordinateurs de votre réseau ou à des systèmes centralisés de notification. Cette fonction peut permettre aux départements des systèmes de gestion de l'information de suivre de près les statistiques concernant les virus et les zones à problèmes.

Pour en savoir plus sur l'installation et la configuration de l'utilitaire Gestionnaire d'alerte, consultez le *Guide de l'administrateur* NetShield.

Logiciel VirusScan en tant que client du Gestionnaire d'alerte

Le logiciel VirusScan fonctionne en tant que programme client vis-à-vis du logiciel NetShield et d'un serveur du Gestionnaire d'alerte. Il peut envoyer à n'importe quel serveur du Gestionnaire d'alerte que vous spécifiez des « événements » d'alerte lorsqu'il détecte un virus ou un logiciel nuisible. Le serveur du Gestionnaire d'alerte effectue ensuite le relais de ces événements (et de tous les autres événements qu'il reçoit des autres stations de travail) en tant que messages d'alerte, en utilisant les méthodes que vous ou votre administrateur système avez définies pour la diffusion des alertes.

Le logiciel VirusScan peut aussi envoyer ces mêmes messages d'alerte sous la forme de fichiers texte (.ALR) vers un répertoire d'alerte centralisée accessible par le serveur du Gestionnaire d'alerte. Le serveur du Gestionnaire d'alerte vérifie régulièrement la présence de nouveaux fichiers .ALR dans le répertoire d'alerte centralisée et diffuse les messages d'alerte extraits des fichiers qu'il trouve.

❑ **REMARQUE :** McAfee recommande d'envoyer les événements d'alerte directement à un serveur du Gestionnaire d'alerte plutôt que par l'intermédiaire du système d'alerte centralisée, sauf si votre configuration réseau ne vous permet pas d'utiliser les serveurs du Gestionnaires d'alerte. Le serveur du Gestionnaire d'alerte peut fonctionner conjointement avec le logiciel Event Orchestrator de Network Associates pour associer les messages d'alerte à l'application Magic HelpDesk de Network Associates pour la génération de tickets de dépannage et d'autres fonctions.

Les messages du Gestionnaire d'alerte contiennent en outre des données plus élaborées que celles envoyées par l'intermédiaire du système d'alerte centralisée. L'activation des interruptions SNMP pour le Gestionnaire d'alerte permet de rassembler de nombreuses informations concernant l'ordinateur qui génère le message d'alerte et sa configuration logicielle.

Le client VirusScan peut fournir l'une ou l'autre méthode avec les alertes DMI pour permettre le fonctionnement du logiciel de gestion réseau, tel que le programme OpenView de Hewlett-Packard.

Configuration de l'utilitaire client du Gestionnaire d'alerte

Le logiciel VirusScan comprend un utilitaire de configuration client simple qui vous permet de choisir le serveur du Gestionnaire d'alerte destiné à recevoir les événements d'alerte, de désigner un répertoire d'alerte centralisée destiné à recevoir les messages d'alerte et de spécifier la valeur numérique des messages d'alerte DMI que vous souhaitez envoyer.

La configuration d'un système d'alerte complet est un processus se déroulant en deux étapes : Vous devez d'abord activer l'utilitaire de Configuration client du Gestionnaire d'alerte et le faire pointer vers le serveur du Gestionnaire d'alerte ou l'emplacement du système d'alerte centralisée adéquat. Vous devez ensuite vérifier que vous avez coché la case **Notifier le Gestionnaire d'alerte** dans la page de propriétés Alerte avancée VirusScan, située dans la page Alerte pour l'extension Analyse E-Mail et dans les pages Alerte de chacun des modules VShield que vous avez activés.

Ceci indique à chaque composant VirusScan d'envoyer un événement d'alerte à l'utilitaire client du Gestionnaire d'alerte à chaque fois qu'il détecte un virus ou un objet nuisible. L'utilitaire client transmet, à son tour, le message d'alerte au serveur du Gestionnaire d'alerte que vous indiquez. Si vous ne configurez pas au préalable votre logiciel de sorte qu'il génère des messages d'alerte, l'utilitaire client n'aura rien à transmettre au serveur du Gestionnaire d'alerte en vue d'une diffusion.

Pour démarrer et configurer l'utilitaire Gestionnaire d'alerte, procédez comme suit :

1. Cliquez sur **Démarrer** dans la barre des tâches Windows, pointez sur **Programmes**, puis sur **Network Associates**. Sélectionnez ensuite **Configuration de l'alerte VirusScan**.

   La page Configuration cliente du Gestionnaire d'alerte s'affiche (Figure 9-3 à la page. 341).

Figure 9-3. Boîte de dialogue Configuration cliente du Gestionnaire d'alerte

2. Vérifiez que la case **Désactiver la fonction d'alerte** n'est pas cochée. Cette opération active toutes les autres options de cette boîte de dialogue.

   Cochez cette case uniquement si vous voulez que l'utilitaire de Configuration cliente du Gestionnaire d'alerte *ne* transmette pas les messages d'alerte de votre logiciel antivirus au serveur du Gestionnaire d'alerte ou à votre logiciel d'administration DMI. Par défaut, cette case n'est pas cochée. McAfee recommande de la laisser non cochée, de sorte que le client puisse envoyer des messages d'alerte à l'extérieur.

   ☐ **REMARQUE :** Si vous utilisez le logiciel ePolicy Orchestrator de McAfee dans votre environnement réseau, le logiciel VirusScan continue d'envoyer des messages d'alerte au composant de création de rapports ePolicy Orchestrator, que vous activiez ou désactiviez l'alerte à cet endroit.

   ---

3. Sélectionnez la méthode d'alerte à utiliser. Vous avez le choix entre les options suivantes :

   - **Fonction d'alerte du Gestionnaire d'alerte**. Cliquez sur ce bouton pour envoyer des événements d'alerte à un serveur du Gestionnaire d'alerte situé à un endroit de votre réseau. Le choix de cette option empêche l'envoi d'événements d'alerte vers un répertoire d'alerte centralisée.

     Pour sélectionner un serveur de destination, cliquez sur **Configurer** pour ouvrir la boîte de dialogue Sélection du serveur du Gestionnaire d'alerte (Figure 9-4 à la page. 342).

Figure 9-4. Boîte de dialogue Sélection du serveur du Gestionnaire d'alerte

Entrez ensuite le chemin d'accès au répertoire qui héberge le serveur du Gestionnaire d'alerte que vous souhaitez utiliser ou cliquez sur **Parcourir** pour localiser le serveur sur votre réseau.

Vous pouvez utiliser la notation de la convention d'affectation des noms (UNC) dans la zone de texte pour spécifier l'ordinateur qui héberge le serveur du Gestionnaire d'alerte ou vous pouvez entrer seulement le nom de l'ordinateur. L'utilitaire de Configuration cliente du Gestionnaire d'alerte validera la forme du nom entrée à cet endroit, mais il ne vérifiera pas que le serveur du Gestionnaire d'alerte existe sur l'ordinateur cible. Ceci permet aux ordinateurs portables et aux autres utilisateurs distants de spécifier un serveur du Gestionnaire d'alerte même lorsqu'ils ne sont pas connectés à votre réseau.

Si les services Active Directory sont installés sur votre ordinateur, le fait de cliquer sur Parcourir génère l'affichage d'une liste des noms de serveurs du Gestionnaire d'alerte logiques. Si les services Active Directory ne sont pas installés, l'affichage présente votre arborescence complète. Dans ce cas, contactez votre administrateur système pour savoir quel ordinateur héberge le serveur du Gestionnaire d'alerte à utiliser.

Par défaut, l'utilitaire client utilise la recherche Active Directory pour localiser un serveur du Gestionnaire d'alerte publié, à condition que les services Active Directory soient installés sur cet ordinateur et exécutés sur votre réseau. Pour empêcher l'utilitaire client de procéder de la sorte, cochez la case **Désactiver la recherche du répertoire actif** à son affichage.

Lorsque vous avez choisi une destination pour vos messages d'alerte, cliquez sur **OK** pour fermer la boîte de dialogue.

- **Alerte centralisée**. Cliquez sur ce bouton pour que les composants VirusScan envoient des messages d'alerte vers un répertoire d'alerte centralisée situé à un endroit de votre réseau. Le choix de cette option empêche l'envoi d'événements d'alerte à un serveur du Gestionnaire d'alerte.

  Pour sélectionner un répertoire de destination, cliquez sur **Configurer** pour ouvrir la boîte de dialogue Configuration de l'alerte centralisée (Figure 9-5).

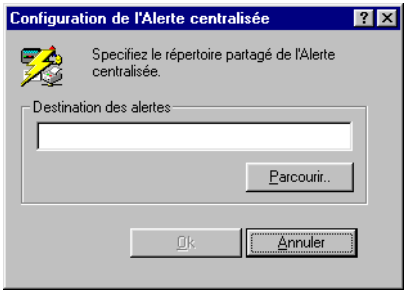

Figure 9-5. Boîte de dialogue Configuration de l'alerte centralisée

Entrez ensuite le chemin d'accès au répertoire d'alerte centralisée que vous souhaitez utiliser ou cliquez sur **Parcourir** pour localiser le répertoire sur votre réseau. Lorsque vous avez choisi une destination, cliquez sur **OK** pour fermer la boîte de dialogue.

Vous pouvez indiquer n'importe quel répertoire situé sur votre réseau en tant que destination pour les messages du système d'alerte centralisée, mais le répertoire doit contenir une copie du fichier CENTALRT.TXT pour que le serveur du Gestionnaire d'alerte puisse relayer les messages d'alerte que vous envoyez à cet endroit.

Si vous activez le système d'alerte centralisée, le logiciel VirusScan envoie au répertoire cible les messages d'alerte sous la forme de fichiers texte portant l'extension .ALR.

Vous pouvez ensuite faire pointer un serveur du Gestionnaire d'alerte désigné vers le répertoire, s'il contient le fichier CENTALRT.TXT, pour qu'il vérifie régulièrement la présence de fichiers .ALR. S'il en trouve un fichier, il extrait le contenu du message d'alerte du fichier, diffuse le message en utilisant une de ses méthodes de notification préconfigurées, puis supprime le fichier .ALR. Il augmente ensuite la fréquence de vérification dans le répertoire d'alerte centralisée pour capturer tout autre message d'alerte qui arrive.

- **Activer aussi les alertes DMI**. Cochez cette case pour proposer une des autres méthodes d'alerte. Cliquez ensuite sur **Configurer** pour ouvrir la boîte de dialogue Configuration DMI, dans laquelle vous pouvez entrer le numéro d'identification que votre application cliente DMI a attribué à votre logiciel VirusScan lors de son installation (Figure 9-6).

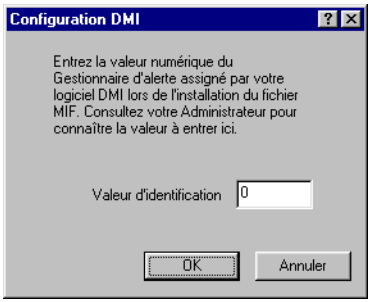

Figure 9-6. Boîte de dialogue Configuration DMI

Pour utiliser cette option, une application cliente DMI, telle que le programme OpenView de Hewlett-Packard, doit déjà être installée sur votre ordinateur local et un logiciel d'administration DMI doit être exécuté à un endroit de votre réseau.

Le logiciel VirusScan est livré avec un fichier MIF (Management Information File) (AMG.MIF) qui identifie les attributs d'alerte VirusScan auprès de votre application cliente DMI. L'application cliente DMI, à son tour, attribue un numéro d'identification au logiciel VirusScan, de sorte qu'il puisse rassembler les événements d'alerte VirusScan et les envoyer à une application d'administration DMI.

Pour que le logiciel VirusScan envoie les messages d'alerte avec un numéro d'identification que l'application d'administration peut reconnaître et traiter, vous devez entrer le numéro d'identification adéquat à cet endroit. Contactez votre administrateur système pour obtenir des détails spécifiques s'appliquant à votre logiciel DMI.

Lorsque vous avez entré un numéro, cliquez sur **OK** pour fermer la boîte de dialogue.

4. Cliquez sur **OK** pour enregistrer les modifications apportées et fermer la boîte de dialogue Configuration cliente du Gestionnaire d'alerte..

Extensions de fichiers vulnérables et compressés par défaut A

Ajout d'extensions de fichier pour analyse

Dans la mesure où les virus ne peuvent pas infecter les fichiers qui ne contiennent pas de code exécutable, le logiciel VirusScan limite d'abord l'analyse aux fichiers susceptibles d'être infectés par des virus. Le logiciel utilise une liste d'extensions de nom de fichier pour garder une trace des fichiers vulnérables. Cette liste apparaît dans la boîte de dialogue Extensions programme et vous pouvez la modifier en fonction de vos besoins.

Pour changer les extensions affichées dans la boîte de dialogue Extensions programme, procédez comme suit :

1. Cliquez sur **Extensions** dans la page de propriétés Détection pour chacun des composants VirusScan que vous configurez.
2. La boîte de dialogue Extensions des fichiers programme s'affiche.

Figure A-1. Boîte de dialogue Extensions des fichiers programme

3. Vous pouvez :
   - cliquer sur **Ajouter** pour ajouter une nouvelle extension.

Cette option ouvre la boîte de dialogue Ajout d'une extension de fichier programme. Tapez l'extension à trois caractères que vous souhaitez ajouter dans la zone de texte prévue à cet effet. N'incluez pas le point qui précède normalement une extension de fichier. Cliquez ensuite sur **OK** pour revenir à la boîte de dialogue Extensions des fichiers programme.

Vous pouvez ajouter autant d'extensions uniques que vous le souhaitez.

- sélectionner une extension dans la liste, puis cliquer sur **Modifier** pour modifier sa définition.
- sélectionner une extension dans la liste, puis cliquer sur **Supprimer** pour l'effacer.
- cliquer sur **Par défaut** pour restaurer la liste d'extensions d'origine. Les extensions ajoutées à la liste seront supprimées.

4. Une fois la liste modifiée, cliquez sur OK pour enregistrer vos modifications et fermer la boîte de dialogue. Cliquez sur Annuler pour fermer la boîte de dialogue sans enregistrer vos modifications.

Liste en cours des extensions de noms de fichiers vulnérables

Dans cette liste, les symboles ? représentent des caractères génériques ; le logiciel VirusScan remplace le ? par n'importe quel caractère afin d'analyser plusieurs types de fichiers possédant des extensions similaires. Le logiciel utilisera par exemple le caractère générique .XL? pour rechercher des virus dans les feuilles de calcul (.XLS) et les modèles (.XLT) Microsoft Excel.

REMARQUE : McAfee recommande d'examiner minutieusement votre système lors de la première opération d'analyse ou d'effectuer des analyses régulières par la suite, sans limiter l'étendue de l'analyse à ces types de fichiers. Ceci vous garantit qu'aucun virus ne sévit à l'intérieur de votre système. Vous pouvez ensuite utiliser cette liste d'extensions pour limiter l'étendue des prochaines analyses.

Table A-1. Extensions de noms de fichiers vulnérables

Extension	Type de fichier	Description du fichier
<VIDE>	Indifféremment	Fichiers sans extension.
.??_	Compressés	Fichiers compressés Windows.
.ARC	Macro/script	Fichiers ARC LH, version antérieure
.ARJ	Archive	Fichiers d'archive compressés .ARJ Robert Jung.
.ASP	Macro/script	Fichiers Microsoft Active Server Pages. Ces fichiers contiennent des commandes de script à utiliser avec Microsoft Internet Information Server.
.BAT	Programme	Fichiers de commandes DOS.
.CAB	Compressés	Fichiers .CAB (Compressed Application Binary) Windows ou fichiers « cabinet ».
.CDR	Macro	Fichier document Corel Draw. Les versions ultérieures de Corel Draw incluent un langage de script pouvant générer des virus de macro.
.CLA	Programme	Fichiers de classe Java (tronqué à partir de .CLASS)
.COM	Programme	Fichiers de comamnde/fichiers image binaires. Ces fichiers courants s'exécutent en tant que programmes exécutables susceptibles d'être infectés par un virus. Les fichiers système DOS et Windows utilisent régulièrement cette extension.
.CSC	Script/macro	Fichiers script Corel. Les fichiers script peuvent inclure des virus ou générer des virus de macro.
.DL?	Programme	Fichier DDL (Dynamic Link Library) ; fichiers script de boîte de dialogue C++. Les fichiers DDL sont des fichiers de ressources liés à des fichiers programme exécutables. Les fichiers exécutables peuvent charger en mémoire les virus qui les ont infectés et les exécuter en tant que partie intégrante de leur code natif.
.DOC	Macro	Fichiers document Microsoft Word. Ces fichiers peuvent contenir des macros Word Basic et, par conséquent, des virus de macro

Table A-1. Extensions de noms de fichiers vulnérables

Extension	Type de fichier	Description du fichier
.DOT	Macro	Fichiers modèle de document Microsoft Word. Ces fichiers peuvent contenir des macros Word Basic et des virus de macro
.EXE	Programme	Fichiers exécutables. La plupart des logiciels utilisent cette extension pour identifier des fichiers qui démarrent son shell de commande ou le noyau du programme.
.GMS	Macro	Fichiers Global Macro Storage Corel.
.GZ?	Compressés	Fichiers compressés Gzip GNU UNIX.
.HLP	Macro	Fichiers d'aide Windows. Ces fichiers peuvent contenir des exécutables Word Basic ou d'autres codes de macro.
.HT?	Script/macro	Fichiers HTML (Hyper Text Markup Language) et fichiers associés, ainsi que des fichiers modèle Microsoft Hyper Text. Bien qu'ils soient théoriquement en texte brut, ces fichiers peuvent contenir des fonctions de script puissantes qui agissent par le biais d'un logiciel de navigation.
.ICE	Compressés	Fichiers compressés ICE.
.IM?	Programme	Fichiers image pour la création d'images du disque.
.INI	Programme	Fichiers d'initialisation Windows. Bien que ces fichiers soient souvent des fichiers texte, des fichiers .INI infectés peuvent forcer les clients mIRC à effectuer des actions non voulues.
.JS?	Script	Fichiers source JavaScript. Les fichiers JavaScript peuvent contenir du code virus qui agit directement sur les navigateurs Web.
.LZH	Compressés	Fichiers LHARC compressés
.MD?	Macro	Base de données Microsoft Access, macro complémentaire et fichiers associés. Ces fichiers peuvent contenir des macros Visual Basic pour Applications susceptibles d'être infectées par un virus.

Table A-1. Extensions de noms de fichiers vulnérables

Extension	Type de fichier	Description du fichier
.MPP	Macro	Fichiers Microsoft Project. Ces fichiers peuvent contenir des macros Visual Basic pour Applications susceptibles d'être infectées par un virus.
.MPT	Macro	Fichiers modèle Microsoft Project. Ces fichiers peuvent contenir des macros Visual Basic pour Applications susceptibles d'être infectées par un virus.
.MSG	Macro	Fichiers de messages Microsoft Mail, Exchange et Outlook. Ces fichiers peuvent contenir des commandes de script susceptibles d'introduire des virus.
.MSO	Macro	Fichiers Microsoft Office 2000.
.OCX	Programme	Contrôles personnalisés Microsoft OLE (Object Linking and Embedding). Ces fichiers sont similaires aux contrôles ActiveX et, en cas d'infection, peuvent être néfastes pour votre ordinateur.
.OLE	Programme	Fichiers objet Microsoft OLE (Object Linking and Embedding). Ces fichiers sont similaires aux contrôles ActiveX. Ils sont créés dans une application afin d'être imbriqués dans une autre application.
.OV?	Programme	Fichiers de recouvrement.
.POT	Macro	Fichiers modèle Microsoft PowerPoint. Ces fichiers peuvent contenir des macros Visual Basic pour Applications susceptibles d'être infectées par un virus.
.PP?	Macro	Fichiers document et diaporama Microsoft PowerPoint. Ces fichiers peuvent contenir des macros Visual Basic pour Applications susceptibles d'être infectées par un virus.
.RAR	Archive	Archives compressés RAR.
.RTF	Macro	Fichiers RTF (Rich Text Format). Ces fichiers servent de fichier texte commun à plusieurs fichiers document.
.SCR	Programme	Fichiers écran de veille Windows.

Table A-1. Extensions de noms de fichiers vulnérables

Extension	Type de fichier	Description du fichier
.SHS	Programme	Fichiers de script du shell (objet bribes) Windows. Ces fichiers peuvent introduire descommandes qui génèrent un comportement inattendu sur l'ordinateur hôte.
.SMM	Macro	Fichiers feuille de calcul Lotus AmiPro. Ces fichiers peuvent contenir des macros.
.SYS	Programme	Fichiers système et pilotes de périphérique DOS ou Windows. Ces fichiers exécutables démarrent généralement soit lors de l'exécution d'un programme, soit en tant que partie intégrante du programme.
.TAR	Archive	Fichiers Tape Archive UNIX.
.VBS	Script	Fichiers script Visual Basic et fichiers VBScript. VBScript est une implémentation du langage de programmation Microsoft Visual Basic. Il contrôle des fonctions spécifiques sur différentes pages Web et peut gérer directement un grand nombre de fonctions à l'intérieur de Microsoft Outlook et d'autres logiciels.
.VS?	Macro	Fichiers de dessin et fichiers associés Visio. Des versions plus récentes de Visio incluent des extensions de script susceptibles d'être infectées par un virus.
.VXD	Programme	Pilotes de périphérique virtuels Windows. Fichiers exécutables qui résident généralement dans la mémoire.
.WBK	Macro	Fichiers de sauvegarde Microsoft Word.
.WPD	Macro	Fichiers document Corel WordPerfect.
.XL?	Macro	Fichiers de feuille de calcul, de macro complémentaire, de barre d'outils, de graphique, de boîte de dialogue, de sauvegarde, de macro, d'espace de travail, de module Visual Basic et fichiers modèle Microsoft Excel. Ces fichiers peuvent contenir des macros Visual Basic pour Applications susceptibles d'être infectées par un virus.

Table A-1. Extensions de noms de fichiers vulnérables

Extension	Type de fichier	Description du fichier
.XML	Script/macro	Fichiers XML (Extensible Markup Language). Bien qu'ils soient théoriquement en texte brut, ces fichiers peuvent contenir des fonctions de script puissantes qui agissent par le biais d'un logiciel de navigation.
.ZIP	Archive	Fichiers d'archives compressés WinZip et PKZip.

Liste en cours des fichiers compressés analysés

L'application VirusScan et le moteur d'analyse VShield recherchent des virus dans une gamme de formats de fichier compressés et archivés. Pour y parvenir, chaque composant utilise toutefois des technologies légèrement différentes et, par conséquent, traite différemment chaque type de fichier.

Pour les besoins de cette description, un fichier « compressé » désigne un fichier unique. Les utilitaires de compression tels que PKLite, LZEXE et d'autres réduisent la taille de ces fichiers en combinant ou en éliminant les données redondantes qu'ils contiennent. Un « fichier d'archives » désigne un fichier qui agit en tant qu'« empaqueteur », ou une enveloppe qui renferme d'autres fichiers. Les fichiers contenus dans l'empaqueteur peuvent ou non être compressés. Les fichiers WinZip, .TAR et .ARC sont des exemples de ces types de fichiers. La plupart des fichiers WinZip compressent d'autres fichiers et les empaquettent dans un seul fichier d'archives.

Ce tableau résume le comportement de chaque composant VirusScan en fonction du type de fichier :

Table A-2. Opération d'analyse appliquée aux fichiers et aux archives compressés

Composant VirusScan	Fichier archivé	Fichier compressé
Application VirusScan	• Cochez la case **Fichiers compressés** pour l'activer. • Ouvre les archives et analyse les fichiers qu'elles contiennent. • Spécifiez **Tous les fichiers** comme cibles à analyser ou ajoutez l'extension du nom du fichier d'archives dans la boîte de dialogue Extensions programme pour que l'application analyse les archives en tant que fichiers.	• Cochez la case **Fichiers compressés** pour l'activer. • Analyse le fichier compressé si vous spécifiez **Tous les fichiers** comme cibles à analyser ou si vous ajoutez l'extension du fichier compressé dans la boîte de dialogue Extensions programme.
Moteur d'analyse VShield	• Le moteur d'analyse n'ouvrira pas les archives pour analyser les fichiers qu'ils contiennent. • Spécifiez **Tous les fichiers** comme cibles à analyser ou ajoutez l'extension du nom du fichier d'archives dans la boîte de dialogue Extensions programme pour que l'application analyse les archives en tant que fichiers.	• Cochez la case **Fichiers compressés** pour l'activer. • Spécifiez **Tous les fichiers** comme cibles à analyser ou ajoutez l'extension du nom du fichier compressé dans la boîte de dialogue Extensions programme pour que l'application recherche les virus dans le fichier compressé.

Les deux composants VirusScan incluent la prise en charge intégrée de certains formats de fichier compressés et archivés. Le tableau ci-dessous répertorie les formats et décrit la façon dont ils sont analysés par chaque composant lorsque vous cochez la case Fichiers compressés. Vous ne pouvez ni modifier ni ajouter des éléments dans cette liste.

Table A-3. Opération d'analyse appliquée par le logiciel VirusScan à chaque type de fichier

Format	Description	Prise en charge de l'application VirusScan ?	VShield prise en charge du moteur d'analyse ?
.??_	Fichier compressé Windows	• Analyse le fichier compressé s'il s'affiche dans la boîte de dialogue Extensions programme	• Analyse le fichier compressé s'il s'affiche dans la boîte de dialogue Extensions programme
.GZ?	Fichier compressé Gzip GNU UNIX	• Analyse le fichier compressé s'il s'affiche dans la boîte de dialogue Extensions programme	• Analyse le fichier compressé s'il s'affiche dans la boîte de dialogue Extensions programme
.TD0	Fichier compressé Teledisk	• Analyse le fichier compressé s'il s'affiche dans la boîte de dialogue Extensions programme	• Analyse le fichier compressé s'il s'affiche dans la boîte de dialogue Extensions programme
.ARC	Fichier ARC LH, version antérieure	• Analyse l'archive • Analyse les fichiers contenus dans les archives	• Analyse les archives en tant que fichiers s'ils s'affichent dans la boîte de dialogue Extensions programme • N'analyse pas les fichiers contenus dans les archives
.ARJ	Fichier compressé .ARJ Robert Jung	• Analyse l'archive • Analyse les fichiers compressés contenus dans les archives	• Analyse les archives en tant que fichiers s'ils s'affichent dans la boîte de dialogue Extensions programme • N'analyse pas les fichiers compressés contenus dans les archives

Table A-3. Opération d'analyse appliquée par le logiciel VirusScan à chaque type de fichier

Format	Description	Prise en charge de l'application VirusScan ?	VShield prise en charge du moteur d'analyse ?
.CAB	Fichier .CAB (Compressed Application Binary) Windows ou fichier « cabinet »	• Analyse l'archive • Analyse les fichiers compressés contenus dans les archives	• Analyse les archives en tant que fichiers s'ils s'affichent dans la boîte de dialogue Extensions programme • N'analyse pas les fichiers compressés contenus dans les archives
.ICE	Fichier compressé ICE	• Analyse le fichier compressé s'il s'affiche dans la boîte de dialogue Extensions programme	• Analyse le fichier compressé s'il s'affiche dans la boîte de dialogue Extensions programme
.LZH	Fichier compressé LHARC	• Analyse le fichier compressé s'il s'affiche dans la boîte de dialogue Extensions programme	• Analyse le fichier compressé s'il s'affiche dans la boîte de dialogue Extensions programme
.RAR	Archive compressé RAR	• Analyse l'archive • Analyse les fichiers contenus dans les archives	• Analyse les archives en tant que fichiers s'ils s'affichent dans la boîte de dialogue Extensions programme • N'analyse pas les fichiers contenus dans les archives

Table A-3. Opération d'analyse appliquée par le logiciel VirusScan à chaque type de fichier

Format	Description	Prise en charge de l'application VirusScan ?	VShield prise en charge du moteur d'analyse ?
.TAR	Fichier Tape Archive UNIX	• Analyse l'archive • Analyse les fichiers contenus dans les archives	• Analyse les archives en tant que fichiers s'ils s'affichent dans la boîte de dialogue Extensions programme • N'analyse pas les fichiers contenus dans les archives
.ZIP	Fichier PKZip ou WinZip	• Analyse l'archive • Analyse les fichiers compressés contenus dans les archives	• Analyse l'archive en tant que fichiers s'ils s'affichent dans la boîte de dialogue Extensions programme • N'analyse pas les fichiers compressés contenus dans les archives

Network Associates Support technique

B

Valeur ajoutée de votre produit McAfee

En choisissant les produits antivirus McAfee, la gestion des réseaux Sniffer Technologies et le logiciel de sécurité PGP, vous assurez un fonctionnement aisé et efficace de la technologie informatique que vous utilisez. L'utilisation du plan de support de Network Associates accroît la protection fournie par votre logiciel en vous donnant accès aux connaissances requises pour installer, surveiller, assurer la maintenance et effectuer la mise à niveau de votre système avec la technologie de Network Associates la plus récente. Grâce à un plan de support répondant à vos besoins, votre système ou votre réseau peut fonctionner, dans votre environnement informatique, pendant des années de manière fiable.

Les plans de support de Network Associates se répartissent en deux catégories. Si vous êtes une entreprise, vous pouvez choisir parmi 4 niveaux de support étendu dans le cadre du programme Corporate PrimeSupport* de Network Associates. Si vous êtes un utilisateur à domicile, vous pouvez choisir un plan adapté à vos besoins dans le cadre du programme Home User PrimeSupport.

Options PrimeSupport destinées aux clients d'entreprise

Le programme Corporate PrimeSupport offre les quatre plans de support technique suivants :

- Plan PrimeSupport KnowledgeCenter
- Plan PrimeSupport Connect
- Plan PrimeSupport Priority
- Plan PrimeSupport Enterprise

Chaque option présente une gamme de fonctions vous fournissant un support rentable et adapté à vos besoins. Les paragraphes suivants offrent une description détaillée de chaque plan.

Plan PrimeSupport KnowledgeCenter

PrimeSupport KnowledgeCenter vous donne accès à un large éventail d'informations sur le support technique via une base de connaissances en ligne de Network Associates, en plus des mises à niveau de logiciel disponibles sur le site Web de Network Associates. Si vous avez acheté votre produit Network Associates avec une licence d'abonnement, vous recevrez le plan PrimeSupport KnowledgeCenter en tant que partie intégrante du paquet, pendant toute la durée de votre abonnement.

Si vous l'avez acheté accompagné d'une licence définitive, vous pourrez renouveler votre plan PrimeSupport KnowledgeCenter moyennant une cotisation annuelle.

Pour recevoir votre mot de passe KnowledgeCenter ou pour enregistrer votre accord PrimeSupport auprès de Network Associates, visitez le site :

http://www.nai.com/asp_set/support/introduction/default.asp

Le formulaire rempli par vos soins sera transmis au service clientèle de Network Associates. Vous devez envoyer ce formulaire avant de vous connecter au site de PrimeSupport KnowledgeCenter.

Le plan PrimeSupport KnowledgeCenter vous offre les avantages suivants :

- Accès illimité 24 heures sur 24 aux solutions techniques en ligne, à partir d'une base de connaissances que vous pouvez interroger sur le site Web de Network Associates
- Accès au service technique par voie électronique pour soumettre vos questions et incidents
- Documents techniques, y compris des guides d'utilisateur, des listes de Forums aux Questions et des notes de mise à jour
- Mises à jour des fichiers et mises à niveau du produit en ligne

Plan PrimeSupport Connect

PrimeSupport Connect vous fournit une assistance téléphonique pour les principaux produits par l'intermédiaire de l'équipe expérimentée du support technique. Le plan PrimeSupport Connect vous offre les avantages suivants :

- En Amérique du Nord, accès illimité par un numéro vert au support technique du lundi au vendredi, de 8 heures à 20 heures (heure du centre des États-Unis)
- En Europe, au Moyen Orient et en Afrique, accès illimité au support technique par téléphone pour le prix d'un appel longue distance ou international standard, du lundi au vendredi, de 9 heures à 18 heures (heure locale)
- Dans la région Asie-Pacifique, accès illimité par un numéro vert au support technique du lundi au vendredi, de 8 heures à 18 heures (heure de l'Asie du Sud-Est)
- En Amérique Latine, accès illimité au support technique par téléphone pour le prix d'un appel longue distance ou international standard, du lundi au vendredi, de 9 heures à 17 heures (heure du centre des États-Unis)
- Accès illimité 24 heures sur 24 aux solutions techniques en ligne, à partir d'une base de connaissances que vous pouvez interroger sur le site Web de Network Associates
- Accès au service technique par voie électronique pour soumettre vos questions et incidents
- Documents techniques, y compris des guides d'utilisateur, des listes de Forums aux Questions et des notes de mise à jour
- Mises à jour des fichiers de données et mises à niveau des produits via le site Web de Network Associates

Plan PrimeSupport Priority

PrimeSupport Priority vous fournit une assistance téléphonique à toute heure pour les principaux produits par l'intermédiaire de l'équipe expérimentée du support technique de Network Associates. Il est possible de souscrire un abonnement annuel à PrimeSupport Priority lorsque vous achetez un produit Network Associates accompagné d'une licence d'abonnement ou d'une licence d'un an.

Le plan PrimeSupport Priority vous offre les avantages suivants :

- En Amérique du Nord, accès illimité par un numéro vert au support technique du lundi au vendredi, de 8 heures à 20 heures (heure du centre des États-Unis)
- En Europe, au Moyen Orient et en Afrique, accès illimité au support technique par téléphone pour le prix d'un appel longue distance ou international standard, du lundi au vendredi, de 9 heures à 18 heures (heure locale)
- Dans la région Asie-Pacifique, accès illimité par un numéro vert au support technique du lundi au vendredi, de 8 heures à 18 heures (heure de l'Asie du Sud-Est)
- En Amérique Latine, accès illimité au support technique par téléphone pour le prix d'un appel longue distance ou international standard, du lundi au vendredi, de 9 heures à 17 heures (heure du centre des États-Unis)
- Accès prioritaire au support technique pendant les heures ouvrables normales
- Réponse dans l'heure pour les problèmes urgents survenus en dehors des heures ouvrables normales, y compris pendant les week-ends et les jours fériés locaux
- Accès illimité 24 heures sur 24 aux solutions techniques en ligne, à partir d'une base de connaissances que vous pouvez interroger sur le site Web de Network Associates
- Accès au service technique par voie électronique pour soumettre vos questions et incidents
- Documents techniques, y compris des guides d'utilisateur, des listes de Forums aux Questions et des notes de mise à jour
- Mises à jour des fichiers de données et mises à niveau des produits via le site Web de Network Associates

Plan PrimeSupport Enterprise

PrimeSupport Enterprise vous fournit à toute heure une assistance proactive et personnalisée, par l'intermédiaire de l'ingénieur du support technique qui vous est assigné. Vous aurez toutes les raisons d'apprécier les services d'un professionnel de l'assistance, connaissant l'historique de l'installation et du support technique du produit Network Associates que vous avez acquis, et qui vous contactera, comme vous en aurez convenu avec lui, afin de vérifier que vous possédez les connaissances nécessaires pour utiliser et effectuer la maintenance des produits de Network Associates.

En vous appelant avant que les problèmes ne surviennent, le représentant de PrimeSupport Enterprise vous aidera à mieux les éviter. Toutefois, en cas d'urgence, PrimeSupport Enterprise vous indiquera le délai de réponse notifié avant l'arrivée de l'aide. Il est possible de souscrire un abonnement annuel à PrimeSupport Enterprise lorsque vous achetez un produit Network Associates accompagné d'une licence d'abonnement ou d'une licence d'un an.

Le plan PrimeSupport Enterprise vous offre les avantages suivants :

- Accès illimité par un numéro vert à un ingénieur du support technique assigné, 24 heures sur 24 et 7 jours sur 7, y compris pendant les week-ends et les jours fériés.

  REMARQUE : La disponibilité du support technique par numéro vert varie d'une région à l'autre et n'existe pas partout en Europe, au Moyen Orient, en Afrique ou en Amérique Latine.

- Assistance téléphonique ou électronique proactive fournie par un ingénieur assigné, aux intervalles de votre choix
- Délai de réponse nécessaire notifié par votre ingénieur assigné, qui répondra au récepteur d'appels dans la demi-heure, à la messagerie vocale dans l'heure et au courrier électronique dans les quatre heures
- Sélection de cinq contacts au sein de votre entreprise, auxquels votre ingénieur assigné pourra s'adresser pendant votre absence
- Statut facultatif de site bêta, vous permettant d'accéder aux technologies et aux produits Network Associates les plus récents
- Accès illimité 24 heures sur 24 aux solutions techniques en ligne, à partir d'une base de connaissances que vous pouvez interroger sur le site Web de Network Associates

- Accès au service technique par voie électronique pour soumettre vos questions et incidents
- Documents techniques, y compris des guides d'utilisateur, des listes de Forums aux Questions et des notes de mise à jour
- Mises à jour des fichiers et mises à niveau du produit en ligne

Commande de PrimeSupport pour les entreprises

Pour commander un plan PrimeSupport, contactez votre revendeur, ou

- En Amérique du Nord, appelez les services de Network Associates au (972) 308-9960, du lundi au vendredi de 8 heures à 19 heures (heure du centre des États-Unis). Appuyez sur le 3 à l'aide du clavier téléphonique pour obtenir le service des ventes.
- En Europe, appelez les services de Network Associates au 00-31-20-586-6100 et au Moyen Orient et en Afrique, contactez notre représentant local. Les coordonnées des contacts figurent au début de ce manuel.

Table B-1. Aperçu de PrimeSupport pour les entreprises

Plan Caractéristique	Knowledge Center	Connect	Priority	Enterprise
Support technique via le site Web	oui	oui	oui	oui
Mises à jour du logiciel	oui	oui	oui	oui
Support technique par téléphone	—	Du lundi au vendredi Amérique du Nord : De 8 heures à 20 heures, heure du centre des États-Unis Europe, Moyen Orient, Afrique : De 9 heures à 18 heures, heure locale Asie-Pacifique : De 8 heures à 18 heures, heures de l'Asie du Sud-Est Amérique latine : De 9 a heures à 17 heures, heure du centre des États-Unis	Accès après les heures ouvrables, en cas d'urgence, du lundi au vendredi Amérique du Nord : De 8 heures à 20 heures, heure du centre des États-Unis Europe, Moyen Orient, Afrique : De 9 heures à 18 heures, heure locale Asie-Pacifique : De 8 heures à 18 heures, heures de l'Asie du Sud-Est Amérique latine : De 9 a heures à 17 heures, heure du centre des États-Unis	Accès après les heures ouvrables, en cas d'urgence, du lundi au vendredi Amérique du Nord : De 8 heures à 20 heures, heure du centre des États-Unis Europe, Moyen Orient, Afrique : De 9 heures à 18 heures, heure locale Asie-Pacifique : De 8 heures à 18 heures, heure de l'Asie du Sud-Est Amérique latine : De 9 a heures à 17 heures, heure du centre des États-Unis
Traitement des appels prioritaires	—	—	oui	oui
Support en dehors des heures ouvrables	—	—	oui	oui
Ingénieur de support assigné	—	—	—	oui
Support proactif	—	—	—	oui

Table B-1. Aperçu de PrimeSupport pour les entreprises

Plan Caractéristique	Knowledge Center	Connect	Priority	Enterprise
Contacts client assignés	—	—	—	Au moins 5
Délai de réponse	Un jour ouvrable pour le courrier électronique	Au maximum 3 minutes d'attente pour les appels et un jour ouvrable pour la réponse	Dans l'heure pour les problèmes urgents en dehors des heures ouvrables	Pager en dehors des heures ouvrables : 30 minutes Messagerie vocale : 1 heure E-Mail : 4 heures

Les options PrimeSupport décrites ci-dessous ne sont disponibles qu'en Amérique du Nord. Pour obtenir des informations sur les options PrimeSupport, Formation et Conseil, disponibles en dehors du continent nord-américain, consultez votre revendeur le plus proche. Les coordonnées des contacts figurent au début de ce manuel.

Options PrimeSupport pour les utilisateurs à domicile

Si vous avez acheté votre produit Network Associates auprès d'un revendeur ou via le site Web de Network Associates, vous recevrez également des services de support comme partie intégrante de votre achat. Le niveau de support inclus dépend du produit acheté. Parmi les services dont vous pouvez bénéficier figurent :

- Pour les logiciels antivirus, des mises à jour gratuites de vos données de fichiers (.DAT) pendant la durée de vie de votre produit via le site Web de Network Associates, la fonction de mise à jour automatique de votre produit ou le service SecureCast. Vous pouvez également effectuer la mise à jour de vos fichiers de données en utilisant votre navigateur Web pour visiter le site à l'adresse suivante :

  http://www.nai.com/asp_set/download/dats/find.asp

- Des mises à niveau gratuites de votre programme (fichier exécutable) pendant une année via le site Web de Network Associates. Si vous avez acheté une version élaborée d'un produit Network Associates, vous recevrez des mises à niveau gratuites du programme pendant deux ans. Vous pouvez également effectuer la mise à niveau de votre logiciel en utilisant votre navigateur Web pour visiter le site à l'adresse suivante :

  http://www.nai.com/asp_set/download/upgrade/login.asp

- Accès gratuit 24 heures sur 24, 7 jours sur 7, à un support en ligne ou électronique par l'intermédiaire du système de messagerie vocale et de télécopie de Network Associates, via le site Web de Network Associates et par l'intermédiaire d'autres services électroniques tels que America Online et CompuServe.

  Pour contacter les services électroniques de Network Associates

  - Appelez le service de messagerie vocale et de télécopie automatique au (408) 346-3414
  - Visitez le site Web de Network Associates à l'adresse http://support.nai.com
  - Visitez le forum CompuServe de Network Associates à GO NAI
  - Visitez Network Associates sur America Online : Mot clé MCAFEE

- Accès gratuit à PrimeSupport KnowledgeBase : Accès en ligne aux solutions techniques dans une base de connaissances consultable, à la présentation des incidents électroniques et à la documentation technique, comme les guides d'utilisateur, le Forum Aux Questions et les notes de mise à jour. Visitez KnowledgeBase à l'adresse suivante :

  http://www.nai.com/asp_set/support/technical/intro.asp

- Trente jours supplémentaires de support technique dispensé par un technicien de Network Associates du lundi au vendredi, de 9 heures à 17 heures 30 (heure du centre des États-Unis). Cette période de trente jours démarre à la date de votre premier appel téléphonique au support technique et s'applique à tous les produits Network Associates. Pour contacter le support technique, composez le

  00 31 20 586 6100

  Si vous avez besoin d'autres supports, Network Associates offre plusieurs autres plans de support que vous pouvez acheter avec votre produit Network Associates ou après l'expiration du délai supplémentaire de 30 jours. Ce sont :

> **REMARQUE :** Les plans de support décrits ici ne sont disponibles qu'en Amérique du Nord. Pour obtenir des informations sur les options de support locales, contactez votre revendeur local.

- **Plan annuel Small Office/Home Office.** Ce plan vous offre un accès illimité par un numéro vert au support technique pendant les heures ouvrables habituelles, du lundi au vendredi de 9 heures à 17 heures (heure du centre des États-Unis).
- **Plan de paiement par incident.** Ce plan vous offre un accès payant au support technique par incident pendant les heures ouvrables habituelles, du lundi au vendredi de 7 heures à 18 heures (heure du Pacifique). Vous composez un numéro vert, vous payez l'accès au service par carte bancaire, puis vous entrez en contact avec l'équipe du support technique en quelques minutes. Le coût par incident est de 35 $.

Tous les produits McAfee	(800) 950-1165

- **Plan de paiement par minute.** Ce plan vous donne droit à une assistance uniquement lorsque vous en avez besoin. Le numéro 900 vous donne accès au support technique et votre appel est traité en priorité afin de minimiser votre temps d'attente. Les deux premières minutes sont gratuites.

Tous les produits à l'exception du logiciel de cryptage PGP	(900) 225-5624

- **Plan de mises à niveau en ligne.** Ce plan vous offre l'avantage d'accéder automatiquement aux mises à niveau de votre produit via les services en ligne ou électroniques de Network Associates.
- **Plan trimestriel Disquettes/CD.** Ce plan propose la livraison automatique tous les trimestres de CD ou de disquettes de mise à niveau si vous ne pouvez pas accéder aux mises à niveau des produits en ligne. Ce service n'est disponible que pour McAfee VirusScan et NetShield.

Comment accéder à l'assistance internationale pour les utilisateurs à domicile

Le tableau suivant liste les numéros de téléphone du support technique au niveau international. Les coûts, la disponibilité, les heures ouvrables et le contenu des plans peuvent varier d'un endroit à l'autre. Contactez votre revendeur ou l'agence régionale de Network Associates pour plus de détails.

Pays ou région	*Téléphone	Forum électronique (BBS)
Allemagne	+49 (0)69 21901 300	+49 89 894 28 999
France	+33 (0)1 4993 9002	+33 (0)1 4522 7601
Royaume-Uni	+44 (0)171 5126099	+44 1344-306890
Italie	+31 (0)55 538 4228	+31 (0)20 586 6128
Pays-Bas	+31 (0)55 538 4228	+31 (0)20 586 6128
Europe	+31 (0)55 538 4228	+31 (0)20 688 5521
Amérique latine	+55-11-3794-0125	+55-11-5506-9100

* des frais peuvent s'appliquer pour les appels longue distance

Commande d'un plan PrimeSupport pour les utilisateurs à domicile

Pour commander le plan annuel PrimeSupport Small Office / Home Office, le plan de paiement par incident, le plan de paiement par minute, le plan de mises à niveau en ligne ou le plan trimestriel Disquettes / CD pour vos produits Network Associates :

- En Amérique du Nord, appelez le service clientèle de Network Associates au (972) 855-7044
- Pour les autres pays, contactez le centre de support technique de Network Associates le plus proche de chez vous pour plus d'informations. Il est probable que certaines options de support ne soient pas disponibles partout.

Conseil et formation proposés par Network Associates

Le programme Total Service Solutions de Network Associates fournit des conseils d'experts et une formation complète susceptible d'accroître la sécurité et les performances de votre réseau. Ce programme inclut le volet Conseils professionnels de Network Associates et le programme Total Education Services.

Services professionnels

Le programme Services professionnels de Network Associates peut vous aider à tous les niveaux de croissance de votre réseau, depuis sa planification et sa conception jusqu'à sa gestion en passant par sa mise en œuvre. Les consultants de Network Associates constituent une ressource de spécialistes supplémentaire et apportent une perspective indépendante pour résoudre vos problèmes. Vous obtiendrez de l'aide pour intégrer les produits Network Associates à votre environnement, qu'il s'agisse de l'assistance dépannage ou de conseils pour optimiser les performances de votre réseau. Les consultants de Network Associates développent et proposent aussi des solutions personnalisées pour vous permettre de réaliser vos projets : depuis la résolution de petits problèmes jusqu'aux longues implémentations à grande échelle.

Services Jumpstart

Pour des problèmes spécifiques ou pour des questions liées à la mise en œuvre des logiciels, Network Associates propose le service Jumpstart qui met à votre disposition les outils nécessaires à la gestion adéquate de votre environnement. Ce service peut inclure les éléments suivants :

- **Installation et optimisation.** Avec ce service, un conseiller de Network Associates se déplace sur le site pour installer, configurer et optimiser votre produit Network Associates, mais aussi pour former votre équipe aux principes de fonctionnement du produit.
- **Selfstart.** Avec ce service, un conseiller de Network Associates se déplace sur le site et vous aide à vous préparer pour réaliser tout seul l'implémentation de votre nouveau produit et, dans certains cas, installe le produit.
- **Proposal Development.** Ce service vous aide à évaluer les processus, les procédures, le matériel et logiciel requis avant de mettre en œuvre ou mettre à niveau vos produits Network Associates, puis un conseiller de Network Associates prépare une proposition personnalisée pour votre environnement.

Network Consulting

Les conseillers de Network Associates apportent leurs compétences en analyse de protocole et un point de vue objectif, source de solutions impartiales en cas de panne et de conseils pour optimiser votre réseau. De même, leur compréhension approfondie des meilleures pratiques de gestion de réseau et des relations industrielles accélère la résolution des problèmes par l'intermédiaire du support du vendeur.

Vous pouvez demander un conseil personnalisé pour vous aider à planifier, concevoir, mettre en œuvre et gérer votre réseau afin de déterminer l'impact de l'implémentation de nouvelles applications, de nouveaux systèmes d'exploitation réseau, ou de nouveaux périphériques d'interconnexion réseau.

Pour en savoir plus sur les options disponibles :

- Contactez votre revendeur local.
- En Amérique du Nord, appelez les services de Network Associates au (972) 308-9960, du lundi au vendredi de 8 heures à 19 heures (heure du centre des États-Unis).
- Visitez le site Web de Network Associates à l'adresse suivante :

  http://www.nai.com/asp_set/services/introduction/default.asp

Total Education Services

Total Education Services de Network Associates permet de concevoir et d'améliorer les tâches de tous les professionnels de réseau grâce à des instructions pratiques applicables sur-le-champ. La formation technologique de Total Education Services porte plus particulièrement sur la gestion des performances et les problèmes de réseau, et permet de résoudre ces derniers à tous les niveaux. Network Associates propose également des formations par module afin que vous compreniez les fonctions et fonctionnalités de votre nouveau logiciel.

Vous pouvez vous inscrire aux cours du programme Total Education Services tout au long de l'année dans les centres de formation de Network Associates ou suivre des cours personnalisés se déroulant sur votre site. Tous les cours répondent à des étapes de formation menant à une connaissance et à une maîtrise parfaites de nos produits. Network Associates est membre fondateur du Certified Network Expert (CNX), un consortium d'experts de réseau agréés. Pour en savoir plus sur ces programmes :

- Contactez votre revendeur local.
- Contactez Total Education Services de Network Associates au (800) 395-3151 poste 2670 (pour planifier les cours privés) ou au (888) 624-8724 (pour planifier les cours publics).
- Visitez le site Web de Network Associates à l'adresse suivante :

  http://www.nai.com/services/education/

Utilisation du service SecureCast pour obtenir de nouveaux fichiers de données

C

Présentation du service SecureCast

Le service SecureCast de Network Associates constitue une solution pratique vous permettant de recevoir automatiquement les dernières mises à jour des fichiers de données (.DAT) dès qu'elles sont disponibles. Le service SecureCast utilise la technologie « push » BackWeb pour envoyer de nouveaux fichiers, des messages d'alerte et d'autres informations en utilisant le canal Enterprise SecureCast, auquel vous pouvez vous abonner lors de votre inscription auprès de Network Associates.

Pour utiliser cette option, vous devez télécharger le logiciel BackWeb, disponible à partir du site Web de Network Associates à l'adresse suivante :

http://www.nai.com/asp_set/anti_virus/alerts/register.asp

REMARQUE : Si vous êtes une entreprise, vous devez d'abord disposer d'un numéro de licence ou d'un numéro de série du produit pour pouvoir vous abonner au canal Enterprise SecureCast.

Si vous n'avez pas ces informations, veuillez contacter votre revendeur, votre distributeur ou le service clientèle de Network Associates au 00800-122-55-624.

Si vous êtes déjà un client enregistré de Network Associates et que vous ne connaissez pas votre numéro de licence, remplissez le questionnaire s'y rapportant sur le site dont l'adresse suit :

http://www.nai.com/asp_set/anti_virus/alerts/grantreq.asp

OU BIEN

Envoyez un message e-mail à l'adresse appropriée :

entsecast@nai.com (États-Unis)

esc_registration_Europe@nai.com (Europe)

esc_registration_asia@nai.com (Asie)

Network Associates met à votre disposition une large section Forum aux Questions où vous pouvez trouver la plupart des réponses à vos questions relatives au téléchargement et à la configuration de SecureCast. Pour consulter ce Forum aux Questions, visitez le site Web de Network Associates à l'adresse suivante :

http://www.nai.com/asp_set/anti_virus/alerts/faq.asp

Pourquoi dois-je mettre à jour mes fichiers de données ?

Votre logiciel s'appuie sur les informations que contiennent ses fichiers de définition des virus (fichiers .DAT) pour identifier les virus. Mais plus de 200 nouveaux virus apparaissent chaque mois et les anciens fichiers .DAT risquent de ne pas les reconnaître. En guise de parade, McAfee publie de nouveaux fichiers .DAT chaque semaine. Vous êtes autorisé à vous procurer ces mises à jour gratuites des fichiers de données pour les utiliser avec votre version du logiciel. Si vous n'utilisez pas les fichiers .DAT en cours, vous risquez de compromettre l'efficacité de la protection antivirale de votre programme. Pour une protection maximale, Network Associates vous recommande expressément de mettre régulièrement à jour vos fichiers .DAT.

IMPORTANT : L'utilisation de fichiers à jour d'identification des virus ne constitue pas l'essentiel d'un programme de protection. Il est tout aussi important de recourir à un dispositif d'analyse qui intègre les dernières découvertes en matière de détection virale et de désinfection. Network Associates publie régulièrement une mise à niveau de son dispositif d'analyse qui comprend ces avancées.

Les fichiers .DAT antérieurs, toutefois, risquent de ne pas fonctionner correctement avec les dispositifs d'analyse les plus récents. Une fois l'ancien dispositif devenu obsolète, Network Associates arrête le développement de fichiers .DAT compatibles avec lui. Il est conseillé de mettre à niveau le logiciel avant que la version en cours ne devienne obsolète.

Quels fichiers de données SecureCast livre-t-il ?

Avec le service SecureCast, vous recevrez automatiquement des téléchargements des fichiers suivants :

- **Nouvelles mises à jour du produit**. Les mises à jour du produit que vous recevrez via SecureCast dépendent des termes de votre contrat de licence.
- **Mises à jour du fichier de définition des virus**. Vous recevrez chaque semaine des mises à jour du fichier .DAT pour la version de votre produit.
- **Mises à jour du paquet SuperDAT**. Les paquets SuperDAT incluent des mises à jour du fichier .DAT (exactement les mêmes mises à jour que vous recevez via votre paquet hebdomadaire) et des mises à niveau du dispositif d'analyse, dès qu'ils sont disponibles. L'utilitaire SuperDAT comporte également une architecture d'installation facile à utiliser pour la mise à jour et la mise à niveau rapides du fichier .DAT et du dispositif d'analyse.

- **Messages d'alerte au virus**. Les chercheurs du centre de recherche AVERT McAfee publient des messages d'alerte aux virus pour avertir les clients sur toute menace potentielle de virus à haut risque. Ces messages vous connectent directement au site Web AVERT, où vous pouvez télécharger des fichiers EXTRA.DAT, si disponibles, afin de neutraliser la menace et connaître les caractéristiques du nouveau virus.

Installation du client BackWeb et du service SecureCast

Paramétrage du service SecureCast et du client BackWeb en deux phases :

1. Téléchargez et installez le client BackWeb
2. Enregistrez-vous pour recevoir les InfoPaks du service SecureCast

Pour vous initier au service SecureCast, consultez la configuration système requise ci-dessous, puis suivez la procédure décrite dans chaque section.

Configuration système requise

Le logiciel client BackWeb peut être installé et exécuté sur n'importe quel ordinateur personnel équipé des éléments suivants :

- Processeur Intel ou architecture compatible
- Système d'exploitation Windows 95, 98, NT ou 2000
- 10Mo minimum d'espace disponible sur le disque dur, plus de l'espace suffisant pour le produit et autres téléchargements
- Connexion active à Internet, en accès direct ou distant, pour un minimum d'une heure par semaine.

Phase 1 : Télécharger et installer BackWeb

1. Pour télécharger le logiciel client BackWeb, connectez-vous au site Web de Network Associates à l'adresse suivante :

   http://www.nai.com/asp_set/anti_virus/alerts/register.asp

   Téléchargez ensuite le fichier ESC_501.EXE dans un répertoire temporaire du disque dur.

   Si votre produit a été livré sur CD-ROM, sélectionnez le service SecureCast dans les choix proposés par le CD-ROM d'installation, ou recherchez le fichier ESC_501.EXE sur votre CD-ROM.

2. Double-cliquez sur l'icône du programme pour démarrer.

Dès que les fichiers d'installation nécessaires ont été extraits, le premier écran d'installation de BackWeb s'affiche (voir Figure C-1).

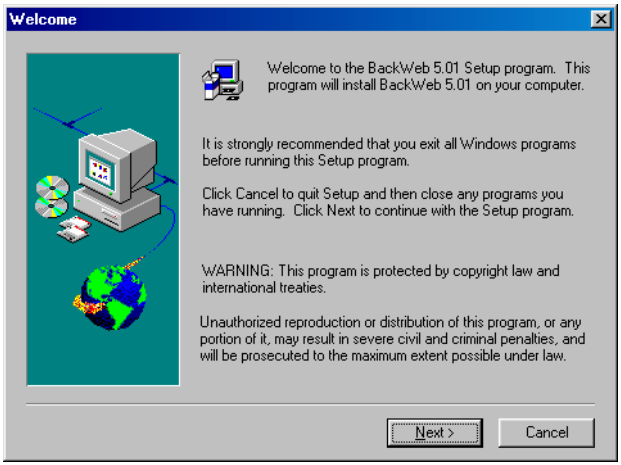

Figure C-1. Écran d'accueil du client BackWeb

3. Lisez les instructions et les avertissements affichés, puis cliquez sur **Suivant>** pour continuer.
4. L'accord de licence de BackWeb s'affiche (Figure C-2).

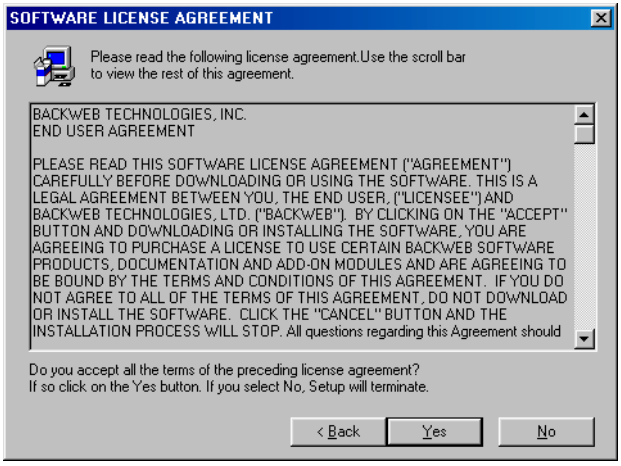

Figure C-2. Écran Accord de licence du logiciel BackWeb

5. Cliquez sur **Oui** pour continuer.
6. L'écran Choisir l'emplacement de destination s'affiche (Figure C-3 à la page 375).

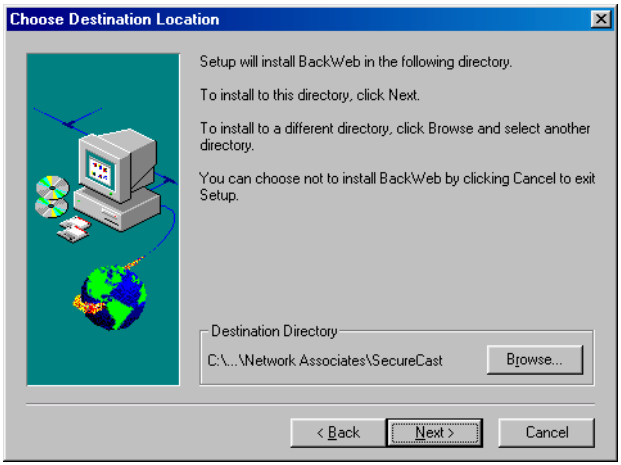

Figure C-3. Écran Choisir l'emplacement de destination

7. Si vous le souhaitez, spécifiez un nouvel emplacement pour installer le logiciel client, ou cliquez sur **Parcourir** pour rechercher un dossier approprié. Cliquez sur **Suivant>** pour continuer.

   Le programme d'installation commencera alors à copier les fichiers programme BackWeb sur votre ordinateur. Pendant la copie des fichiers, il affiche leur progression. Une fois les fichiers copiés, le programme d'installation affiche l'écran Type de connexion (Figure C-4).

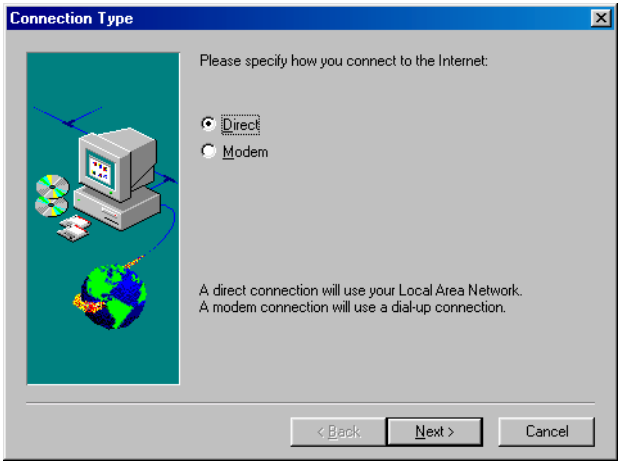

Figure C-4. Écran Type de connexion

8. Spécifiez le type de connexion à Internet utilisé par votre ordinateur. Vous avez le choix entre les options suivantes :

   - **Directe**. Choisissez cette option si vous vous connectez à Internet via un réseau local, une connexion avec une bande passante élevée telle qu'un modem câble, ou une connexion à une ligne d'abonnement numérique (DSL). Passez à l'Étape 9.
   - **Modem**. Choisissez cette option si vous composez un numéro pour vous connecter à un fournisseur de services Internet, ou à votre réseau d'entreprise. Passez à l'Étape 13.

   L'écran Méthode de communication s'affiche (Figure C-5).

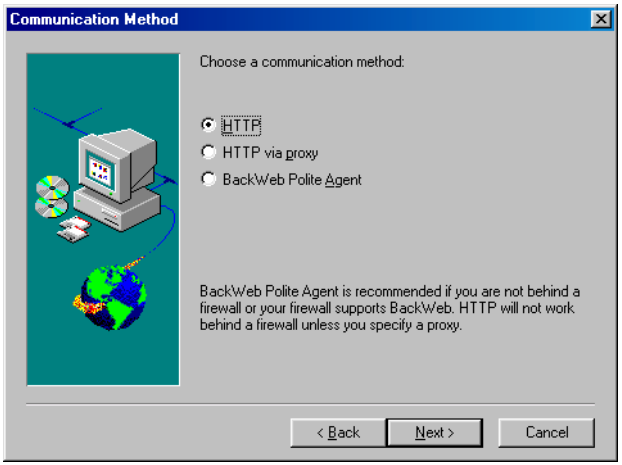

Figure C-5. Écran Méthode de communication

9. Choisissez une méthode de communication. Vous avez le choix entre les options suivantes :

   - **HTTP**. Choisissez cette option si vous pouvez vous connecter directement à Internet sans passer par un serveur proxy. Passez à l'Étape 13.
   - **HTTP via proxy**. Choisissez cette option si vous vous connectez à Internet via un serveur proxy de votre réseau Passez à l'Étape 10.
   - **BackWeb Polite Agent**. Choisissez cette option pour vous connecter à Internet par le biais d'une connexion UDP (Universal Datagram Protocol). Le BackWeb Polite Agent vous permet de contrôler la façon dont le client BackWeb interagit avec d'autres applications susceptibles de s'exécuter lorsque des InfoPaks SecureCast arrivent sur votre bureau. Pour de plus amples informations, consultez l'aide en ligne de BackWeb à l'adresse suivante :http://www.backweb.com/.

     Passez à l'Étape 13.

10. Si vous avez sélectionné **HTTP via proxy** comme méthode de connexion, l'écran Installation du proxy HTTP s'affiche (Figure C-6).

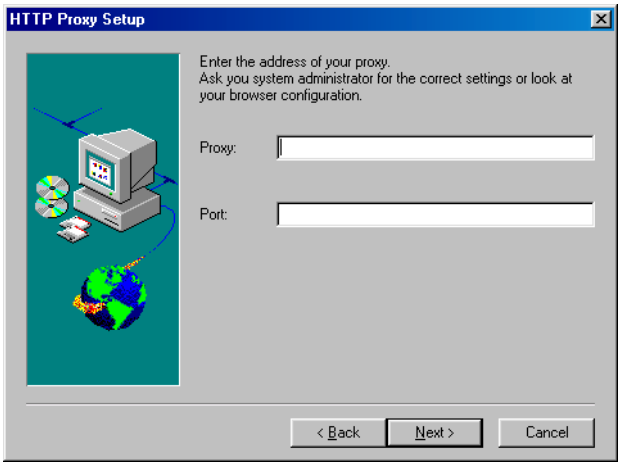

Figure C-6. Écran Installation du proxy HTTP

11. Tapez le nom de votre serveur proxy dans la zone de texte Proxy, puis tapez le numéro de port utilisé par le serveur dans la zone de texte Port.

    Une fois vos sélections spécifiées, cliquez sur **Suivant>** pour continuer. L'écran Authentification du proxy s'affiche (Figure C-7).

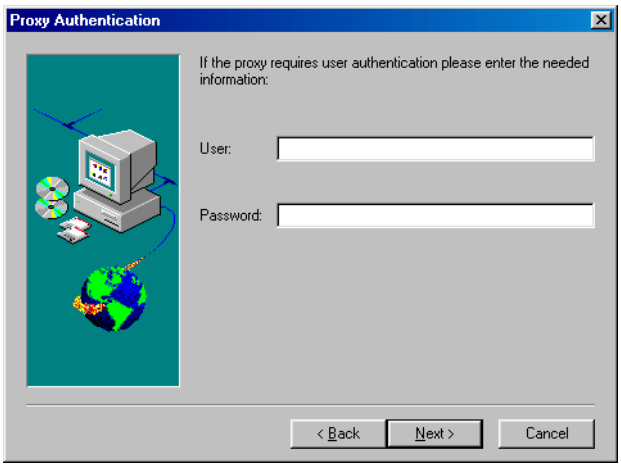

Figure C-7. Écran Authentification du proxy

12. Si le serveur proxy nécessite l'authentification de l'utilisateur, tapez dans les zones de textes prévues à cet effet un nom d'utilisateur et un mot de passe avec des droits suffisants pour permettre la connexion, puis cliquez sur **Suivant**> pour continuer.

L'écran Installation terminée s'affiche (Figure C-8).

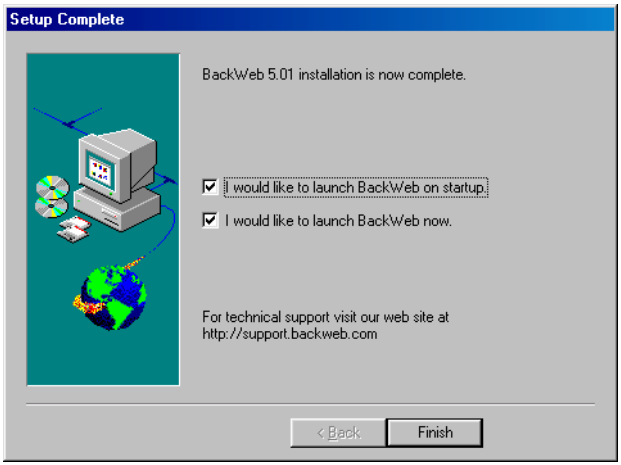

Figure C-8. Écran Installation terminée

13. Pour démarrer immédiatement, laissez les deux cases cochées dans cet écran, puis cliquez sur **Terminer** pour terminer votre installation.

Phase 2 : S'inscrire auprès du service Enterprise SecureCast

Une fois que vous avez installé et démarré le client BackWeb, le service SecureCast ouvre immédiatement l'application cliente et envoie son premier InfoPak : les formulaires d'enregistrement de SecureCast (Figure C-9).

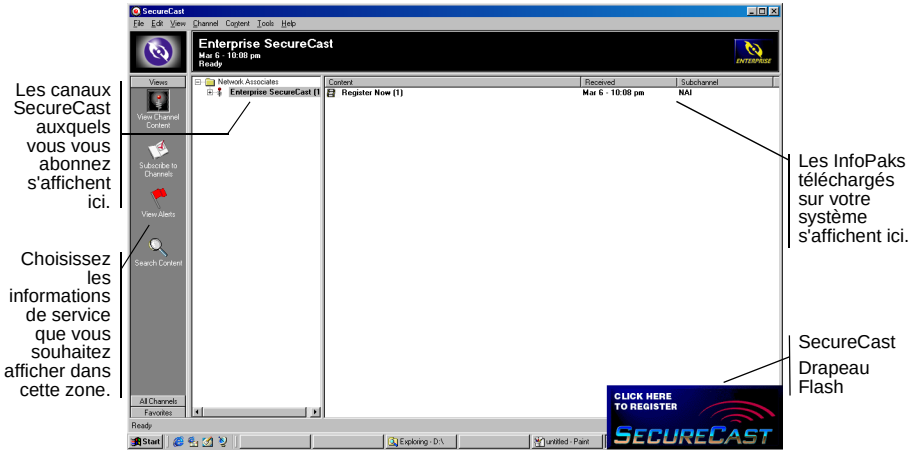

Figure C-9. Fenêtre du client Enterprise SecureCast

Le service SecureCast vous avertit qu'un InfoPak est arrivé avec le message clignotant qui apparaît à l'angle inférieur droit de la Figure C-9.

IMPORTANT : Si vous êtes une entreprise et disposez d'une connexion à Internet grande vitesse, il est possible que la fenêtre affiche **Enregistrer maintenant** puisqu'un InfoPak a déjà été livré. Passez à l'Étape 1.

Si vous disposez d'une connexion moyennement rapide ou si le trafic est particulièrement dense sur le site de SecureCast ou le vôtre, il est possible que la fenêtre n'affiche aucun InfoPak. Dans ce cas, réduisez ou fermez la fenêtre BackWeb. Après un laps de temps, vous recevrez un message clignotant. Cliquez sur ce dernier et passez à l'Étape 2.

Suivez les étapes suivantes pour vous abonner au canal Enterprise SecureCast :

1. Lorsque la mention **Enregistrer maintenant** apparaît dans la fenêtre, double-cliquez dessus. Le drapeau SecureCast Flash apparaît (Figure C-10).

Figure C-10. Drapeau Flash SecureCast

2. Cliquez sur le drapeau. L'écran d'accueil de Network Associates s'affiche (Figure C-11).

Figure C-11. Écran d'accueil de Network Associates

3. Lisez les informations qui s'affichent, puis cliquez sur **Enregistrer maintenant** en bas de l'écran.

4. Double-cliquez sur l'icône **BW Enregistrer** 

dans la fenêtre qui s'ouvre ensuite. Un formulaire d'enregistrement s'affiche (Figure C-12).

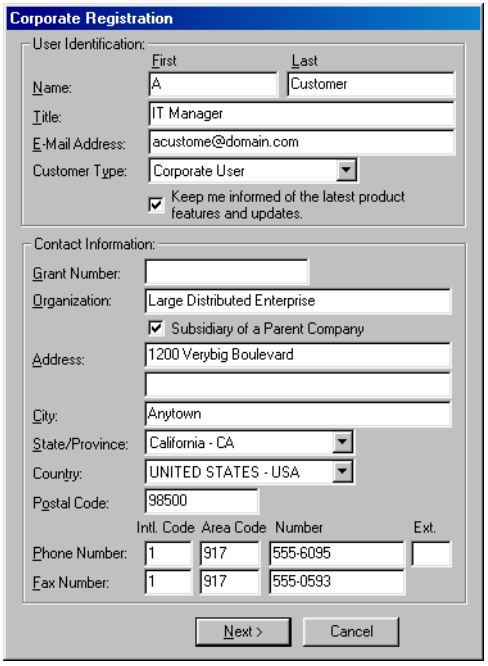

Figure C-12. Formulaire d'enregistrement pour les utilisateurs SecureCast

5. Tapez votre nom, votre fonction et le nom de votre entreprise dans les zones de texte prévues à cet effet. Vous devez également taper le numéro de licence que vous avez reçu lors de l'achat du logiciel, ou qui vous a été attribué par le service clients de Network Associates.

REMARQUE : Si vous êtes une entreprise et que celle-ci n'est pas une filiale d'une autre entreprise, décochez la case **Filiale d'une société mère** avant de poursuivre.

Une fois les informations saisies, cliquez sur **Suivant>** pour continuer.

- Si vous n'avez pas décoché la case **Filiale d'une société mère**, la boîte de dialogue **Informations sur la société mère** s'affiche (voir Figure C-13 à la page 381). Passez à l'Étape 7 à la page 381.

- Si vous avez décoché la case **Filiale d'une société mère**, passez à l'Étape 6.

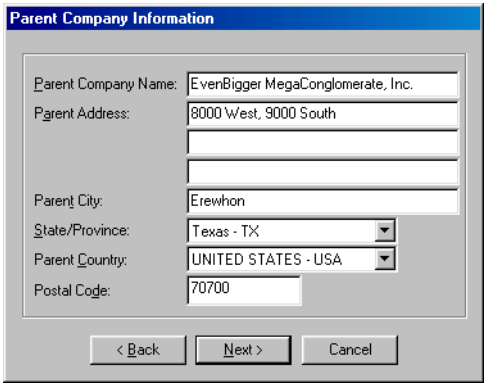

Figure C-13. Formulaire d'informations sur la société mère de SecureCast

6. Si votre société est une filiale d'une autre société, tapez les informations de contact pour votre société mère dans les zones de texte prévues à cet effet.

   Une fois les informations saisies, cliquez sur **Suivant>**. La boîte de dialogue **Configuration de communication du proxy** s'affiche (Figure C-14).

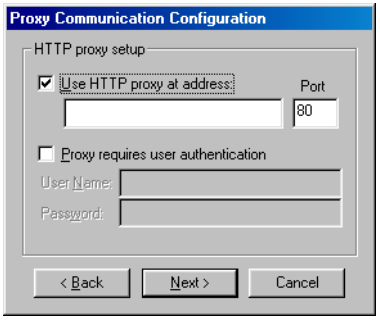

Figure C-14. Configuration de communication du proxy SecureCast

7. Si vous vous connectez à Internet par le biais d'un serveur proxy, cochez la case Utiliser un proxy HTTP à l'adresse, puis tapez le nom du serveur ou son adresse IP dans la zone de texte prévue à cet effet. Vérifiez ensuite que le numéro de port qui s'affiche dans la zone de texte Port est correct ou entrez le numéro de port approprié.

   Si le serveur proxy nécessite l'authentification de l'utilisateur, cochez la case **Le proxy requiert l'authentification de l'utilisateur**, puis tapez un nom d'utilisateur et un mot de passe avec des droits suffisants.

8. Une fois les informations saisies, cliquez sur **Suivant>**. L'écran**État des activités en ligne** s'affiche, montrant la progression du processus d'enregistrement (Figure C-15).

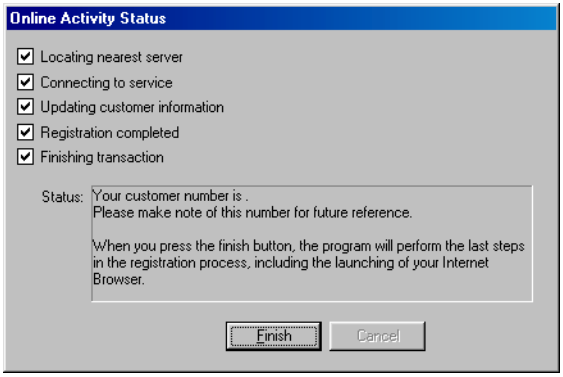

Figure C-15. Écran État des activités en ligne de SecureCast

9. Cliquez sur **Terminer** une fois que toutes les cases sont cochées.

   Le processus d'installation est achevé. Votre navigateur Web s'ouvrira à la page du service clientèle électronique SecureCast de Network Associates. Si vous êtes une entreprise, la fenêtre ressemble à celle présentée dans la Figure C-16 :

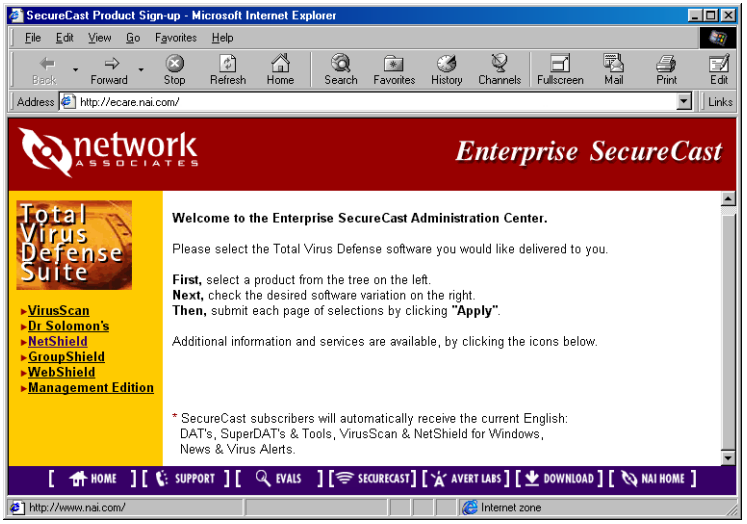

Figure C-16. Service électronique de clientèle d'entreprise de SecureCast

Vous pouvez utiliser cette page pour télécharger des mises à jour et des mises à niveau du produit, pour contacter le support technique et obtenir d'autres informations directement auprès de Network Associates. Les informations qui s'affichent ici et les éléments que vous pouvez télécharger sont déterminés par les termes de votre contrat de licence.

Dépannage du service Enterprise SecureCast

Problèmes relatifs à l'abonnement

Si vous essayez de vous abonner à une heure de grande affluence sur le Web, vous risquez d'attendre avant que le serveur ne réponde à votre demande. Si les messages d'erreur « Erreur 1105 » ou « Erreur de la base de données : Impossible de se connecter à la source de données » s'affichent, cela signifie que le serveur rencontre un problème de base de données. Essayez de renvoyer votre formulaire ou de renouveler l'opération ultérieurement. Si vous ne réussissez pas à vous abonner au canal Enterprise SecureCast, contactez le support de téléchargement de Network Associates (du lundi au vendredi de 8 HEURES à 20 HEURES (heure du centre des États-Unis) au (801) 492-2650.

Suspension de l'abonnement au service SecureCast

Vous pouvez à tout moment suspendre la livraison d'InfoPaks par le service SecureCast. Pour cela, cliquez avec le bouton droit sur l'icône BackWeb dans la barre d'état Windows, puis choisissez **Démarrer SecureCast** dans le menu contextuel qui s'affiche.

Ensuite, procédez comme suit :

1. Dans la zone de liste figurant à gauche de la fenêtre du client BackWeb (voir Figure C-9 à la page 378), recherchez puis sélectionnez la liste qui correspond au canal SecureCast auquel vous êtes abonné.

2. Cliquez avec le bouton droit sur l'icône du canal, puis choisissez **Suspendre l'abonnement** dans le menu contextuel qui s'affiche.

   Tous les InfoPaks listés dans la fenêtre du service SecureCast disparaissent. Le service SecureCast ne livrera plus d'InfoPaks à partir de ce canal.

Ressources de support

service SecureCast

Si vous avez des questions supplémentaires sur le service SecureCast, consultez le Forum Aux Questions SecureCast sur le site Web de Network Associates, à l'adresse suivante :

http://www.nai.com/asp_set/anti_virus/alerts/faq.asp

client BackWeb

- Pour obtenir un guide complet sur BackWeb (comprenant des conseils de dépannage supplémentaires), consultez le guide d'utilisateur BackWeb en ligne à l'adresse suivante :

  http://www.backweb.com/

Description de la technologie iDAT D

Description des fichiers .DAT incrémentiels

Pour que VirusScan fonctionne de manière efficace, vous devez lui fournir régulièrement des fichiers de données de définition des nouveaux virus (fichiers .DAT). Sans fichiers .DAT à jour, le logiciel risque de ne pas détecter les attaques des nouveaux virus ou de ne pas répondre efficacement à la menace qui pèse sur votre système. Dans les versions antérieures de l'utilitaire AutoUpdate, vous deviez télécharger et installer la totalité du kit de définition de virus chaque semaine. Avec l'ajout de nouvelles définitions de virus, ce kit est devenu très volumineux et compte à ce jour plus de 50 000 définitions de virus.

Avec cette version de VirusScan, McAfee a introduit une nouvelle technologie de définition de virus incrémentielle (.DAT ou iDAT) basée sur de petits kits contenant uniquement les définitions de virus qui ont été modifiées entre les versions de fichier .DAT hebdomadaires et *non* la totalité du jeu de fichiers .DAT. Plutôt que de télécharger chaque semaine une mise à jour de fichier .DAT de 3Mo ou plus, vous pouvez maintenant télécharger des kits iDAT dont la taille varie entre 100Ko et 110Ko, en fonction du nombre de définitions de virus incluses. Grâce à cette innovation, vous pouvez télécharger des mises à jour de fichier .DAT à une vitesse beaucoup plus élevée et au moindre coût en matière de bande passante.

Mieux encore, l'utilitaire AutoUpdate rend ce processus entièrement transparent—il téléchargera tous les fichiers .DAT dont il a besoin pour mettre à jour votre logiciel. Si vos fichiers .DAT sont plus anciens que la sélection de kits iDAT disponible, ou si un téléchargement iDAT échoue pour une raison quelconque, l'utilitaire téléchargera la totalité du kit de fichiers .DAT courant. Dans tous les cas, l'utilitaire AutoUpdate garantit la protection permanente de votre système par l'utilisation de fichiers .DAT actualisés, sans avoir à vous soucier du choix des fichiers à télécharger. Il suffit de spécifier la source de mise à jour dans l'utilitaire, de programmer l'heure d'exécution de AutoUpdate et l'utilitaire se charge du reste.

IMPORTANT : Les mises à jour incrémentielles s'appliquent uniquement aux fichiers .DAT. McAfee ne fournit pas des mises à jour incrémentielles pour les fichiers du moteur d'analyse. Pour mettre à jour les fichiers du moteur d'analyse, utilisez l'utilitaire SuperDAT. L'utilitaire SuperDAT téléchargera et installera uniquement des mises à jour complètes de fichiers .DAT.

Configuration requise pour l'installation du produit

Pour télécharger et installer les kits iDAT, vous devez posséder le logiciel antivirus VirusScan v4.5 ou version ultérieure et l'utilitaire AutoUpdate correspondant, et vous devez avoir mis à niveau votre moteur d'analyse Olympus vers la version v4.0.50 ou version ultérieure. Les fichiers .DAT incrémentiels ne fonctionnent pas avec des versions antérieures du produit ou du moteur d'analyse.

Principe de fonctionnement de la mise à jour des fichiers iDAT

L'utilitaire AutoUpdate télécharge deux types de fichiers lorsqu'il se connecte au site de mise à jour que vous avez spécifié.

- **fichiers .UPD**. Ces fichiers de mise à jour contiennent uniquement les modifications de définition de virus intervenues dans une version de fichier .DAT d'une semaine à l'autre. Les noms des fichiers .UPD se composent du numéro de version d'un fichier .DAT, par exemple 4053, et du numéro de version du fichier .DAT suivant, 4054 dans ce cas précis. Ainsi, le nom de fichier complet de ce fichier .UPD sera 40534054.UPD.

  Si vous avez mis à jour vos fichiers .DAT chaque semaine, l'utilitaire AutoUpdate téléchargera simplement le fichier hebdomadaire, puis l'installera pour mettre à jour vos fichiers .DAT. Si vous n'avez pas mis à jour votre logiciel pendant trois ou quatre semaines, l'utilitaire AutoUpdate devra alors télécharger un certain nombre de kits .UPD afin d'extraire et d'installer tous les fichiers de définition de virus dont il a besoin pour mettre à jour vos fichiers .DAT existants. Toutes les informations dont l'utilitaire a besoin pour choisir les kits à télécharger se trouvent dans le fichier DELTA.INI.

- **Fichiers DELTA.INI**. Ce sont des fichiers texte qui décrivent les fichiers .UPD hebdomadaires que l'utilitaire AutoUpdate doit télécharger pour mettre à jour vos fichiers .DAT. Le fichier DELTA.INI contient des entrées qui répertorient un certain nombre de versions de fichier .DAT précédentes, ainsi que le nombre de fichiers .UPD hebdomadaires correspondants qu'il doit télécharger à partir d'un numéro de version de fichier .DAT donné pour posséder toutes les définitions de virus répertoriées par la version courante du fichier .DAT. Les entrées du fichier ont le format suivant :

```
[Table des patchs multiples]

4053=10

4054=11

4055=12

[Résolveur incrémentiel]

10=40534054.UPD

11=40544055.UPD

12=40554056.UPD
```

Dans cet exemple, imaginons que le fichier .DAT version 4053 est installé sur votre ordinateur et que la version actuelle du fichier .DAT est la 4056. Après une analyse du fichier DELTA.INI, l'utilitaire AutoUpdate sait qu'il doit télécharger les 10ème, 11ème et 12ème versions du fichier .UPD pour obtenir toutes les définitions de virus répertoriées par la version courante du fichier .DAT.

Entre-temps, les entrées de la table du résolveur incrémentiel traduisent les numéros séquentiels de la table des patchs multiples en noms de fichier réels pouvant être téléchargés par l'utilitaire AutoUpdate.

Le fichier DELTA.INI contient également le total de contrôle et d'autres informations pouvant être utilisées par l'utilitaire AutoUpdate pour vérifier que les fichiers téléchargés n'ont pas été modifiés ou corrompus.

❑ **REMARQUE :** Si le téléchargement d'un fichier iDAT échoue pour une raison quelconque, l'utilitaire AutoUpdate télécharge et installe une mise à jour complète de fichier .DAT.

Après avoir téléchargé le fichier .UPD approprié, l'utilitaire AutoUpdate décode les fichiers .DAT existants, applique les fichiers iDAT téléchargés aux fichiers .DAT existants, valide les données, puis code les fichiers .DAT actualisés afin de les utiliser avec votre logiciel.

❑ **REMARQUE :** Dans la mesure où les fichiers iDAT corrigent les fichiers .DAT existants, il est préférable de ne pas télécharger les fichiers iDAT à l'aide de l'utilitaire AutoUpdate et d'utiliser l'utilitaire pour enregistrer ces fichiers pour des mises à jour ultérieures. Vous pouvez toutefois télécharger les kits .UPD à partir du site FTP de McAfee et enregistrer ces fichiers pour une distribution ultérieure. Pour plus de détails, reportez-vous à la section “Conseils pratiques”.

Éléments publiés par McAfee chaque semaine

McAfee publie chaque semaine une mise à jour complète du fichier .DAT, une mise à jour hebdomadaire du fichier iDAT et un nouveau fichier DELTA.INI avec des entrées actualisées pour la table des patchs multiples et le résolveur incrémentiel. Vous pouvez télécharger ces fichiers sans passer par l'utilitaire de mise à jour automatique et les publier sur vos serveurs internes en vous connectant directement au site FTP de McAfee à l'adresse :

ftp://ftp.nai.com/licensed/antivirus/datfiles/4.x/

IMPORTANT : Pour vous connecter à ce site, vous devez posséder un nom d'utilisateur et un mot de passe et être titulaire d'une licence d'utilisation. Le site FTP n'accepte pas les connexions anonymes.

Voici une liste de fichiers type :

```
00_index.txt
40534054.UPD
40544055.UPD
40554056.UPD
dat-4056.zip
dat-4056.tar
DELTA.INI
README.TXT
```

Conseils pratiques

Les sections suivantes présentent quelques conseils d'utilisation des fichiers iDAT téléchargés dans le cadre de votre stratégie de mise à jour.

Mise à jour en trois étapes

Si vous devez mettre en œuvre de nouvelles définitions de virus sur plusieurs stations de travail de votre réseau, McAfee recommande une stratégie de mise à jour en trois étapes permettant d'économiser votre bande passante, de minimiser les risques liés à la sécurité et de renforcer le contrôle de votre stratégie de mise à jour interne :

1. Si les fichiers .DAT installés sur votre ordinateur sont très anciens, utilisez un navigateur Web ou un logiciel client FTP pour télécharger une mise à jour complète du fichier .DAT ou pour télécharger l'utilitaire SuperDAT sur un serveur central de votre réseau, puis configurez les copies de mise à jour automatique sur les ordinateurs du réseau afin de télécharger et d'installer la mise à jour complète du fichier .DAT et le moteur d'analyse courant.

   Cette procédure met votre réseau dans un état de protection optimal. Vous pouvez ensuite télécharger et installer les fichiers iDAT pour actualiser vos fichiers de définition de virus.

2. À partir de l'état de protection optimal, utilisez un navigateur Web ou un logiciel client FTP chaque semaine pour télécharger les nouveaux fichiers .UPD directement du site FTP de McAfee sur un serveur central de votre réseau.

   Si vous démarrez à partir de l'état de protection optimal décrit dans l'Étape 1, il suffit de télécharger le fichier .UPD le plus récent publié sur le site FTP de McAfee. Si vous n'avez pas mis à jour votre fichier de définition de virus depuis deux semaines, ouvrez le fichier DELTA.INI en ligne et observez les entrées qui figurent dans la table des patchs multiples et la table du résolveur incrémentiel afin d'identifier les fichiers .UPD que vous devez télécharger pour mettre à jour les fichiers .DAT installés sur votre réseau, puis téléchargez les fichiers requis, *y compris* le fichier DELTA.INI.

3. Installez tous les fichiers .UPD et le fichier DELTA.INI que vous avez téléchargés sur un serveur central de votre réseau, puis configurez les copies de AutoUpdate sur les ordinateurs de votre réseau afin de télécharger et d'installer l'ensemble iDAT. Ne marquez pas ces fichiers en lecture seule, car l'ordinateur cible pourrait renvoyer un message d'erreur lors de la prochaine tentative de suppression des anciens fichiers.

   L'utilitaire AutoUpdate téléchargera chaque fichier requis, l'un après l'autre, afin d'actualiser les fichiers .DAT installés sur l'ordinateur hôte. À partir de ce moment-là, les ordinateurs du réseau installeront les fichiers iDAT, réduisant ainsi le temps de mise à jour et les besoins en matière de bande passante.

Planification des mises à jour internes du fichier .DAT

L'utilitaire AutoUpdate inclut une fonction de planification intégrée qui vous permet d'automatiser tout le processus de mise à jour. Vous pouvez programmer les mises à jour afin qu'elles soient exécutées tard dans la nuit ou lorsque la demande de bande passante diminue ou à d'autres moments plus appropriés. La fonction de planification vous permet également de définir une

« fenêtre de randomisation » centrée sur l'heure à laquelle vous avez programmé votre mise à jour. Vous pouvez utiliser cette fonction pour envoyer une configuration AutoUpdate standard, avec un planning de mise à jour standard, tout en évitant la saturation du trafic réseau qui survient lorsque tous les ordinateurs du réseau essaient de mettre à jour simultanément leurs fichiers .DAT.

Si certains de vos ordinateurs clients sont inactifs ou si la console VirusScan n'est pas activée, l'utilitaire AutoUpdate reprendra la tâche planifiée lors du prochain démarrage de l'ordinateur ou de la console VirusScan.

Pour plus d'informations sur l'utilisation de cette fonction, consultez la section « Activation des tâches » à la page 247.

❑ **REMARQUE :** Pensez à programmer les mises à jour de vos ordinateurs clients à une heure où vous aurez déjà téléchargé et installé les fichiers de mise à jour sur votre serveur central. Si vous configurez vos ordinateurs pour télécharger des fichiers iDAT directement du site Web de McAfee, veillez à programmer vos mises à jour à une heure où les fichiers .DAT hebdomadaires seront déjà publiés.

Forum aux questions

Problèmes relatifs à la connectivité

Q: Que se passe-t-il si mon ordinateur est éteint au moment de l'exécution d'une mise à jour planifiée ?

R: Si l'utilitaire AutoUpdate n'exécute pas une tâche planifiée parce que votre ordinateur ou la console VirusScan étaient inactifs à l'heure prévue pour son exécution, l'utilitaire exécutera la tâche lors du prochain démarrage de l'ordinateur ou de la console.

Q: Que se passe-t-il si ma connexion Internet ou ma connexion réseau sont interrompues au cours d'une mise à jour ?

R: Si l'utilitaire AutoUpdate a téléchargé un ou plusieurs fichiers iDAT avant l'interruption de la connexion, il installera ces fichiers sur vos fichiers .DAT existants et consignera l'absence de téléchargement des fichiers iDAT restants dans son journal d'activité.

Données corrompues

Q: Que se passe-t-il si l'un des fichiers iDAT est corrompu au cours du téléchargement ?

R: Avant d'installer un fichier iDAT quelconque, l'utilitaire AutoUpdate compare le fichier avec un total de contrôle de vérification enregistré dans le fichier DELTA.INI. Si les totaux de contrôle ne sont pas identiques, l'utilitaire n'installe pas le fichier iDAT ni les autres fichiers téléchargés au cours de cette session. L'utilitaire affiche plutôt un message d'erreur, puis télécharge un jeu de fichiers .DAT complet pour mettre à jour votre logiciel.

Mise à jour incrémentielle ou complète des fichiers .DAT

Q: Que se passe-t-il si mes fichiers .DAT existants sont très anciens ? La mise à jour incrémentielle des fichiers .DAT fonctionnera quand même ?

R: L'utilitaire AutoUpdate choisit le processus à utiliser. Il télécharge des fichiers iDAT uniquement si votre jeu de fichiers .DAT existant date de moins de 15 semaines. Au-delà de ce délai, il téléchargera un jeu de fichiers .DAT complet.

Problèmes relatifs à la configuration du réseau

Q: Tous les ordinateurs que je souhaite mettre à jour doivent-ils être en mesure de se connecter à Internet ?

R: Non. Vous pouvez configurer un ordinateur de votre réseau pour télécharger les fichiers iDAT à partir d'Internet, puis les autres ordinateurs du réseau pourront télécharger leurs fichiers à partir de cet ordinateur. Pour plus d'informations, consultez la section « Mise à jour en trois étapes » à la page 388.

Q: Comment puis-je éviter la saturation du réseau lors de la mise à jour de nombreuses stations de travail ?

R: La boîte de dialogue Propriétés de la tâche AutoUpdate inclut une fonction de randomisation que vous pouvez utiliser pour répartir la charge du réseau. Pour plus d'informations sur l'utilisation de cette fonction, consultez la section « Activation des tâches » à la page 247.

Problèmes relatifs à la planification

Q: Quelle est la fréquence conseillée pour vérifier l'arrivée des fichiers de mises à jour ?

R: En général, McAfee publie les fichiers .DAT actualisés chaque semaine. Vous pouvez toutefois vérifier l'arrivée des mises à jour plus ou moins souvent en fonction des besoins de sécurité de votre réseau. Gardez à l'esprit que le risque d'infection est multiplié lorsque les téléchargements des mises jour des fichiers de données sont moins réguliers.

Index

A

B

C

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W