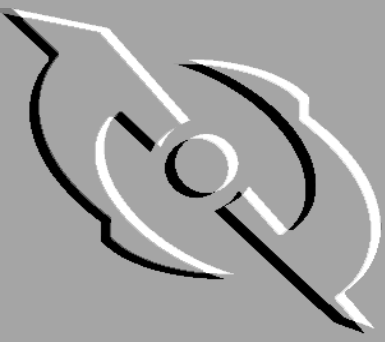


# VirusScan pour Windows NT

# Guide de l’utilisateur

**Network Associates France S.A.**
50 rue de Londres
75008 Paris
France

**Network Associates Canada**
139 Main Street
Suite 201
Unionville
Ontario L3R 2G9
Canada

**Network Associates Suisse AG**
Bäulerwisenstrasse 3
8152 Glattbrugg
Switzerland

**ACCORD DE LICENSE NETWORK ASSOCIATES**

A L'ATTENTION DE TOUS LES UTILISATEURS : VEUILLEZ LIRE ATTENTIVEMENT LES DISPOSITIONS CONTRACTUELLES SUIVANTES (« L'ACCORD »), CONCERNANT LA LICENCE CONCEDEE PAR LE DISTRIBUTEUR (« DISTRIBUTEUR ») POUR LE LOGICIEL SPECIFIE (« LOGICIEL ») DEVELOPPE PAR NETWORK ASSOCIATES, INC. (« NETWORK ASSOCIATES »). EN CLIQUANT SUR LE BOUTON D'ACCEPTATION OU EN INSTALLANT LE LOGICIEL, VOUS (EN TANT QU'INDIVIDU OU ENTITE) CONSENTEZ A ETRE LIE PAR CET ACCORD ET EN DEVENEZ PARTIE PRENANTE. SI VOUS N'ACCEPTEZ PAS TOUS LES TERMES DE CET ACCORD, CLIQUEZ SUR LE BOUTON INDIQUANT QUE VOUS N'ACCEPTEZ PAS LES TERMES DE L'ACCORD ET N'INSTALLEZ PAS LE LOGICIEL. (LE CAS ECHEANT, VOUS POUVEZ RETOURNER LE PRODUIT AU DISTRIBUTEUR AFIN D'EN OBTENIR LE REMBOURSEMENT.)

1. **Octroi de licence**. Sous réserve du paiement des droits de licence applicables, et sous réserve des conditions définies dans cet Accord, le Distributeur vous accorde par le présent contrat un droit incessible et non exclusif d'utiliser une copie de la version spécifiée du Logiciel et la documentation qui l'accompagne (la « Documentation »). Vous pouvez installer une copie du Logiciel sur un ordinateur, une station de travail, un assistant numérique personnel, un système d'appel, un « téléphone intelligent » ou tout autre dispositif électronique pour lequel le Logiciel a été conçu (« Dispositif Client »). Si le Logiciel est fourni sous licence dans le cadre d'une suite ou d'un groupe de programmes comprenant plusieurs produits Logiciels, cette licence s'applique à tous les produits Logiciels spécifiés, sous réserve de toutes restrictions ou conditions d'utilisation spécifiées dans le barême de prix applicable ou sur l'emballage du produit s'appliquant à ces produits Logiciels individuellement.

   a. Utilisation. Le Logiciel est cédé sous licence en tant que produit unique ; il ne peut pas être utilisé sur plusieurs Dispositifs Client ni par plusieurs utilisateurs à la fois, sauf comme stipulé dans cette section 1. Le Logiciel est considéré comme étant « utilisé » sur un Dispositif Client lorsqu'il est chargé en mémoire temporaire (mémoire RAM ou vive) ou installé sur la mémoire permanente (par exemple, disque dur, CD-ROM ou tout autre périphérique de stockage) de ce Dispositif Client. Cette licence vous autorise à effectuer une copie du Logiciel exclusivement à des fins de sauvegarde ou d'archivage, à condition que la copie réalisée contienne toutes les revendications de propriété du Logiciel.

   b. Mode Serveur. Vous ne pouvez utiliser le Logiciel sur un Dispositif Client comme serveur (« Serveur ») dans un environnement multi-utilisateurs ou de réseau (« Mode Serveur ») que si une telle utilisation est autorisée en vertu du barême de prix applicable ou de l'emballage du Logiciel. Une licence distincte est requise pour chaque Dispositif Client ou « poste » pouvant se connecter au Serveur à tout moment, que ces Dispositifs Client ou postes sous licence soient ou non connectés simultanément, qu'ils accèdent au Logiciel et qu'ils l'utilisent ou pas. L'utilisation de logiciels ou de

matériel réduisant le nombre de Dispositifs Client ou postes accédant directement au Logiciel ou l'utilisant (par exemple, logiciel ou matériel de « multiplexage » ou de « regroupement ») ne réduit pas le nombre de licences requis (le nombre de licences requis est égal au nombre d'entrées initiales distinctes dans le logiciel ou le matériel de multiplexage ou de regroupement). Si le nombre de Dispositifs Client ou de postes pouvant se connecter au Logiciel est susceptible de dépasser le nombre de licences obtenues, vous devez disposer d'un mécanisme adapté garantissant que votre utilisation du Logiciel ne dépasse pas les limites spécifiées pour la licence obtenue. Cette licence vous autorise à effectuer ou à télécharger une copie de la Documentation pour chaque Dispositif Client ou poste sous licence, à condition que ces copies contiennent toutes les revendications de propriété figurant dans la Documentation.

c. Licences de volume. Si le Logiciel fait l'objet d'une licence de volume, ainsi que cela est indiqué dans la facture concernée ou sur l'emballage du Logiciel, vous pouvez réaliser, utiliser et installer autant de copies supplémentaires du Logiciel sur des Dispositifs Client qu'il est permis conformément aux dispositions applicables. Vous devez disposer d'un mécanisme adapté garantissant que le nombre de Dispositifs Client sur lequel le Logiciel a été installé ne dépasse pas le nombre de licences obtenues. Cette licence vous autorise à effectuer ou à télécharger une copie de la Documentation pour chaque copie supplémentaire autorisée par la licence de volume, à condition que ces copies contiennent toutes les revendications de propriété figurant dans la Documentation.

2. **Durée.** Cet Accord restera en vigueur jusqu'à ce qu'il y soit mis fin conformément aux dispositions des présentes. Cet Accord cesse automatiquement si vous ne vous conformez pas aux limitations ou autres exigences qui y sont décrites. A la rupture ou à l'expiration de cet Accord, vous devez détruire toutes les copies du Logiciel et de la Documentation. Vous pouvez par ailleurs mettre fin à cet Accord à tout moment en détruisant toutes les copies du Logiciel et de la Documentation.

3. **Mises à jour**. Pendant la durée spécifiée dans le barème de prix applicable ou sur l'emballage du Logiciel, vous pouvez télécharger les révisions ou les mises à jour du Logiciel publiées par Network Associates via son serveur télématique, son site Web ou d'autres services en ligne. Pendant une période de quatre-vingt-dix (90) jours à compter de la date d'achat d'origine du Logiciel, vous pouvez télécharger une (1) révision ou mise à jour du Logiciel publiée par Network Associates via son serveur télématique, son site Web ou d'autres services en ligne. Après la durée spécifiée, vous n'avez plus le droit de recevoir des révisions ou mises à jour sans acheter une nouvelle licence du Logiciel.

4. **Droits de propriété**. Le Logiciel est protégé par les lois sur le droit d’auteur et le copyright, et par certains articles de traités internationaux. Network Associates et ses fournisseurs détiennent et conservent tout droit, titre et intérêt lié au Logiciel, y compris tous les droits d’auteur, brevets, droits de secret commercial, marques et autres droits de propriété intellectuelle s'y rattachant. La possession, l’installation ou l’utilisation du Logiciel ne vous transfère aucun titre de propriété intellectuelle sur le Logiciel et vous n'acquérez aucun droit sur le Logiciel, sauf stipulations expresses dans cet

Accord. Toutes les copies du Logiciel et de la Documentation réalisées dans le cadre de ce contrat doivent contenir les mêmes revendications de propriété que ceux apparaissant dans le Logiciel et la Documentation.

5. **Restrictions**. Vous ne pouvez pas louer, donner à bail, prêter, ni revendre le Logiciel. Vous ne pouvez pas autoriser des tiers à bénéficier de l'utilisation ou des fonctions du Logiciel via un bureau en temps partagé, un bureau de service ou tout autre arrangement, excepté dans la limite où cette utilisation est prévue dans le barême de prix applicable ou sur l'emballage du Logiciel. Vous ne pouvez transférer aucun des droits qui vous sont accordés dans le cadre de cet Accord. Vous ne pouvez pas effectuer de l'ingénierie inverse, décompiler, ni désassembler le Logiciel, sauf si la restriction qui précède est expressément interdite par la loi en vigueur. Vous ne pouvez pas modifier le Logiciel en totalité ou partiellement, ni créer d'oeuvres dérivées. Vous ne pouvez pas copier le Logiciel ni la Documentation sauf dans les conditions expresses visées à la section 1. Vous ne pouvez pas supprimer les revendications ou libellés relatifs à la propriété du Logiciel. Tous les droits non expressément stipulés dans ce contrat sont réservés par Network Associates. Sous réserve de respecter un préavis écrit, le Distributeur se réserve le droit de mener périodiquement des audits afin de vérifier la bonne application des termes de cet Accord.

6. **Garantie et exclusion**.

a. Garantie limitée. Le Distributeur garantit que pendant soixante (60) jours à compter de la date d'achat d'origine, les supports (tels que les disquettes) sur lesquels le Logiciel est enregistré seront exempts de défauts matériels et de fabrication.

b. Recours du client. La seule responsabilité du Distributeur, et votre recours exclusif, en cas de manquement à la garantie précitée seront, à la discrétion du Distributeur, (i) le remboursement du prix réglé pour la licence, le cas échéant, ou (ii) le remplacement des supports défectueux sur lesquels le Logiciel est enregistré. Vous devez renvoyer les supports défectueux au Distributeur à vos frais avec une copie de votre reçu. Cette garantie limitée n'est pas applicable si le défaut résulte d'un accident, d'un abus ou d'une mauvaise application. Tout support de remplacement sera garanti pour le restant de la période de garantie d'origine.

c. Exclusion de garantie. Excepté pour la garantie limitée stipulée dans ce document, LE LOGICIEL EST FOURNI « EN L'ETAT ». DANS TOUTE LA MESURE AUTORISEE PAR LA LOI APPLICABLE, LE DISTRIBUTEUR EXCLUT TOUTES GARANTIES, EXPRESSES OU IMPLICITES, Y COMPRIS, NOTAMMENT, LES GARANTIES IMPLICITES DE QUALITE MARCHANDE, DE CONVENANCE A UN USAGE PARTICULIER ET D'EVICTION, CONCERNANT LE LOGICIEL ET LA DOCUMENTATION QUI L'ACCOMPAGNE. VOUS ASSUMEZ LA RESPONSABILITE DU CHOIX DU LOGICIEL POUR ATTEINDRE LES RESULTATS ESCOMPTES, AINSI QUE DE L'INSTALLATION, DE L'UTILISATION ET DES RESULTATS OBTENUS A PARTIR DU LOGICIEL. SANS LIMITER LES DISPOSITIONS

PRECEDENTES, LE DISTRIBUTEUR N'OFFRE AUCUNE GARANTIE QUE LE LOGICIEL SERA EXEMPT D'ERREUR NI D'INTERRUPTIONS OU AUTRES DEFAILLANCES, OU QU'IL REPONDRA A VOS EXIGENCES. CERTAINS ETATS ET JURIDICTIONS N'AUTORISENT PAS LES LIMITATIONS DE GARANTIES IMPLICITES, DE SORTE QUE LA LIMITATION CI-DESSUS PEUT NE PAS S'APPLIQUER A VOUS. Les clauses qui précèdent seront exécutoires dans la limite maximale autorisée par la loi en vigueur.

7. **Limitation de responsabilité**. EN AUCUNE CIRCONSTANCE ET SOUS AUCUNE THEORIE JURIDIQUE, QU'IL S'AGISSE DE RESPONSABILITE CIVILE, CONTRACTUELLE OU AUTRE, LE DISTRIBUTEUR N'ENCOURRA UNE QUELCONQUE RESPONSABILITE ENVERS VOUS OU TOUTE AUTRE PERSONNE, A RAISON DES DOMMAGES INDIRECTS, SPECIAUX, ACCESSOIRES OU CONSECUTIFS DE TOUTE NATURE, Y COMPRIS NOTAMMENT, LES DOMMAGES LIES A TOUTE PERTE DE CLIENTELE, A DES ARRETS DE TRAVAIL, A UNE DEFAILLANCE OU A UN MAUVAIS FONCTIONNEMENT INFORMATIQUE, OU TOUT AUTRE DOMMAGE OU PERTE COMPARABLE OU DE MEME NATURE. EN AUCUN CAS LA RESPONSABILITE DU DISTRIBUTEUR A RAISON D'UN PREJUDICE REPARABLE QUELCONQUE NE POURRA EXCÉDER LE MONTANT FIGURANT AU BAREME DE PRIX POUR LA LICENCE DU LOGICIEL. CETTE LIMITATION DE RESPONSABILITE NE S'APPLIQUE PAS EN CAS DE DECES OU DE DOMMAGES CORPORELS DANS LA MESURE OU LA LOI APPLICABLE INTERDIT UNE TELLE LIMITATION. DE PLUS, CERTAINS ETATS ET JURIDICTIONS N'AUTORISENT PAS L'EXCLUSION OU LA LIMITATION DES DOMMAGES ACCESSOIRES OU CONSECUTIFS, DE SORTE QUE CES LIMITATIONS ET EXCLUSIONS PEUVENT NE PAS S'APPLIQUER A VOUS. Les clauses qui précèdent seront exécutoires dans la limite maximale autorisée par la loi applicable.

8. **Gouvernement des Etats-Unis**. Le Logiciel et la Documentation qui l'accompagne sont considérés respectivement comme « logiciel commercial » et « documentation du logiciel commercial », conformément aux sections DFAR 227.7202 et FAR 12.212 applicables. Toute utilisation, modification, reproduction, mise en circulation, exécution, présentation ou divulgation du Logiciel et de la Documentation qui l'accompagne par le Gouvernement des Etats-Unis est régie exclusivement par les termes de cet Accord et est interdite en dehors de la limite expressément autorisée par les termes du présent Accord.

9. **Contrôles des exportations**. Ni le Logiciel ni la Documentation et les informations ou la technologie sous-jacentes ne peuvent être téléchargés ni exportés ou ré-exportés de quelque autre manière (i) vers (ou vers un citoyen ou un résident de) Cuba, l'Iran, l'Irak, la Libye, la Corée du Nord, le Soudan, la Syrie ou tout autre pays à l'encontre duquel les Etats-Unis applique un embargo commercial ; ni (ii) vers tout membre figurant sur la liste des nations spécialement désignées par le Ministère des Finances des Etats-Unis ("Specially Designated Nations") ou dans le tableau des commandes interdites du Ministère du Commerce des Etats-Unis ("Table of Denial Orders"). En

téléchargeant ou en utilisant le Logiciel, vous acceptez ce qui précède et certifiez que vous ne vous trouvez pas dans un de ces pays ou sur une telle liste, ni sous leur contrôle, et que vous n'en êtes ni citoyen ni résident.

DE PLUS, VOUS DEVEZ CONNAITRE LES DISPOSITIONS SUIVANTES : L'EXPORTATION DU LOGICIEL PEUT FAIRE L'OBJET DE RESTRICTIONS CONFORMEMENT AUX REGLES ET REGLEMENTIONS PROMULGUEES PERIODIQUEMENT PAR LE BUREAU DE GESTION DES EXPORTATIONS DU MINISTERE DU COMMERCE DES ETATS-UNIS, QUI LIMITENT L'EXPORTATION ET LA RE-EXPORTATION DE CERTAINS PRODUITS ET DONNEES TECHNIQUES. SI L'EXPORTATION DU LOGICIEL EST REGIE PAR DE TELLES REGLES ET REGLEMENTATIONS, LE LOGICIEL NE DEVRA PAS ETRE EXPORTE NI RE-EXPORTE, DIRECTEMENT OU INDIRECTEMENT, (A) SANS TOUTES LES LICENCES D'EXPORTATION OU DE RE-EXPORTATION ET LES APPROBATIONS DES ETATS-UNIS OU D'AUTRES GOUVERNEMENTS REQUISES PAR TOUTE LOI APPLICABLE, OU (B) EN VIOLATION DE TOUTE INTERDICTION APPLICABLE A L'EXPORTATION OU LA RE-EXPORTATION DE TOUT ELEMENT DU LOGICIEL. CERTAINS PAYS APPLIQUENT DES RESTRICTIONS CONCERNANT L'UTILISATION DE LA CRYPTOLOGIE A L'INTERIEUR DE LEURS FRONTIERES, OU L'IMPORTATION OU L'EXPORTATION DE PRODUITS OU MOYENS DE CRYPTOLOGIE MEME DANS LE CADRE D'UNE UTILISATION PERSONNELLE OU PROFESSIONNELLE TEMPORAIRE. VOUS RECONNAISSEZ QUE LA MISE EN OEUVRE ET L'APPLICATION DE CES LOIS NE SONT PAS TOUJOURS COHERENTES A L'EGARD DE PAYS SPECIFIQUES. BIEN QUE LES PAYS SUIVANTS NE CONSTITUENT PAS UNE LISTE EXHAUSTIVE, IL PEUT EXISTER DES RESTRICTIONS SUR L'EXPORTATION OU L'IMPORTATION DE PRODUITS OU MOYENS DE CRYPTOLOGIE PAR : LA BELGIQUE, LA CHINE (Y COMPRIS HONG-KONG), LA FRANCE, L'INDE, L'INDONESIE, ISRAEL, LA RUSSIE, L'ARABIE SAOUDITE, SINGAPOUR ET LA COREE DU SUD. VOUS RECONNAISSEZ QU'IL EST DE VOTRE ULTIME RESPONSABILITE DE VOUS SOUMETTRE A TOUTES LOIS D'EXPORTATION GOUVERNEMENTALES ET AUTRES LOIS EN VIGUEUR ET QUE LE DISTRIBUTEUR N'A AUCUNE RESPONSABILITE SUPPLEMENTAIRE APRES LA VENTE INITIALE DANS LE PAYS DE VENTE D'ORIGINE.

10. **Activités à hauts risques**. Le Logiciel n'est pas exempt de défaillances et n'est pas conçu ni prévu pour être utilisé dans des environnements à risques nécessitant des performances à sécurité intégrée, y compris et sans s'y limiter dans l'exploitation d'installations nucléaires, la navigation ou les systèmes de communication aériens, le contrôle du trafic aérien, les systèmes d'armement, les machines d'assistance respiratoire directe, ou toute autre application pour laquelle la défaillance du Logiciel pourrait entraîner directement la mort, des dommages corporels, ou des dommages physiques ou matériels graves (désignés collectivement comme « Activités à hauts risques »). Le Distributeur exclut toute garantie expresse ou implicite d'adaptation à des Activités à hauts risques.

11. **Divers**. Cet Accord est régi par la loi française, à l'exclusion des principes de confllit de lois. L'application de la Convention des Nations Unies sur les contrats pour la vente internationale de biens est expressément exclue. Cet Accord stipule tous les droits de l'utilisateur du Logiciel et constitue l'intégralité de l'accord entre les parties. Il remplace toute autre communication concernant le Logiciel et la Documentation. Le présent contrat ne peut être modifié que par un avenant écrit, émanant d'un représentant dûment autorisé du Distributeur. Aucune de ses clauses ne pourra être considérée comme abandonnée à moins que cette renonciation ne soit écrite et signée par le Distributeur ou un représentant dûment autorisé du Distributeur. Si une ou plusieurs dispositions du présent Accord sont déclarées nulles, les autres dispositions conserveront leur plein effet. Les parties confirment qu'il est de leur souhait que cet Accord soit rédigé uniquement en langue française.

12. **SERVICE CLIENTELE DU DISTRIBUTEUR**. Si vous avez des questions concernant ces termes et conditions, ou si vous souhaitez contacter le Distributeur pour toute autre raison, appelez le +31 20 586 61 00, envoyez une télécopie au +31 20 586 61 01, ou écrivez à : Network Associates International B.V., P.O. Box 58326, 1044 HH Amsterdam, Pays-Bas.
http://www.nai.com

# Table des matières

# 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 ” virale, vous pouvez vous estimer heureux. Toutefois, étant donné qu’il circule plus de 40.000 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 se “reproduisent” automatiquement en s’attachant à des logiciels hôtes ou à des secteurs du disque de votre ordinateur, 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 programmeur 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 entraver 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 entraîne 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 1 milliard 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 baptisèrent ces programmes " vers ", après avoir remarqué des " trous " sur les impressions des cartes mémoire, 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'affectent pas le logiciel qui les abrite.

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 " sournois et les faisaient combattre entre eux pour déterminer le programme gagnant, celui qui aurait " 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 anciens 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 situent l'avènement des programmes virus en 1986, date de 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 relativement faciles à exploiter pour servir leurs propres desseins.

## Les virus du secteur d'amorçage

Par exemple, les premiers PC " amorçaient " ou chargeaient leur système 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 le secteur d'amorçage 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 secteurs d'amorçage d'autres disquettes ou disques durs. Ceux qui ont, sans le vouloir, chargé le virus Brain à partir d'une disquette infectée ont pu lire un pseudo " message publicitaire " 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 du secteur d'amorçage constituaient la menace la plus sérieuse pour les utilisateurs d'ordinateurs. Des formes variantes de virus du secteur d'amorçage peuvent aussi infecter le Master Boot Record (MBR), qui stocke les informations du secteur de partition dont votre ordinateur a besoin pour localiser chacune des parties de votre disque dur et le secteur d'amorçage lui-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 le secteur d'amorçage ou 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 anti-virus n'ait eu le temps de démarrer. De nombreux logiciels antivirus de Network Associates anticipent cette possibilité en vous permettant de créer un disque d'urgence que vous pouvez utiliser pour amorcer votre ordinateur et supprimer les infections.

Cependant, les virus du secteur d'amorçage et du MBR ont un point faible particulier: ils ont besoin de disquettes ou d'autres moyens mobiles pour se répandre, en se déplaçant dissimulés dans cette première piste de l'espace du disque. 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, d'autres types de virus ont récemment éclipsé la menace émanant du secteur d'amorçage. La popularité que connaissent les disquettes à grande capacité comme les disquettes Iomega Zip et d'autres disquettes identiques, pourrait cependant provoquer une résurgence de ces virus.

## Virus infectant les fichiers

À peu près à la même époque où les auteurs du virus Brain découvraient des points faibles dans le secteur d'amorçage de DOS, d'autres concepteurs de virus ont trouvé comment utiliser un logiciel existant 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 requêtes du logiciel légitime au système d'exploitation et lui 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 anti-virus 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 du secteur d'amorçage 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. Pour ce faire, ils ont imaginé une " signature " codée par laquelle le virus marquait les fichiers infectés, 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 des signatures codées elles-mêmes pour dénicher les virus.

La réponse des concepteurs de virus a été de trouver des méthodes pour dissimuler les signatures codées. Certains virus " mutaient " ou signaient avec un code différent à chaque nouvelle infection. D'autres cryptaient l'essentiel de la signature codée ou du virus lui-même, 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 logiciels 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 l’existence de virus préfabriqués en “ kit ” qui permettaient même à des non-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 l’année 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 concepteurs de virus considéraient les fichiers de données: textes, tableurs et dessins, crées par le logiciel que vous utilisez, comme étant immunisés contre une infection. 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 dans 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 documents capables de se mettre automatiquement au format et d’ajouter de nouvelles capacités aux documents crées avec Word et Excel. Les concepteurs de virus saisirent l’opportunité que cela représentait pour dissimuler et propager des virus dans des documents que vous, l’utilisateur, avez créés vous-même.

L’explosion du succès d’Internet et des logiciels de courrier électronique 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.

# Quelle sera leur prochaine cible?

Des logiciels nuisibles ont même déjà commencé à s'introduire dans des zones jusqu'alors considérées comme absolument 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 textes, 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.

Certains concepteurs de virus ne le font que pour se procurer des sensations, d'autres pour gagner une notoriété au sein de leurs pairs. Toutefois, certains cherchent à rendre la monnaie de leur pièce à des employeurs ou d'autres personnes dont ils considèrent avoir subi un préjudice. Quels que soient leurs motifs, ils ne cessent d'inventer de nouveaux moyens pour vous causer du tort.

# Comment vous protéger

Le logiciel antivirus de Network Associates 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 pour vous protéger. Un logiciel anti-virus 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 données (.DAT) permettant au logiciel de Network Associates 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. Toutefois, Network Associates a rassemblé dans la division McAfee Labs une des plus importante équipe de recherche anti-virus du monde (du point de vue du nombre de chercheurs et de l'expérience acquise) ; grâce à elle, les fichiers de mise à jour qui vous sont nécessaires pour combattre les nouveaux virus sont disponibles aussitôt que vous en avez besoin (et souvent avant).

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 anti-virus, 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. Les logiciels antivirus de Network Associates incluent l'utilitaire de vérification VALIDATE.EXE afin d'éviter ce genre de manipulation. Cependant, ni celui-là ni aucun logiciel antivirus ne peut détecter lorsque quelqu'un substitue un cheval de Troie ou un autre programme nuisible non encore identifié à l'un de vos utilitaires contributifs ou commerciaux favoris.

L'accès au Web et à Internet engendre ses propres risques. Cependant, il est indispensable de disposer d'un coupe-feu à toute épreuve pour protéger votre réseau et de mettre en œuvre d'autres mesures pour sa sécurité, dès lors que des attaquants sans scrupules peuvent le pénétrer 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 de Network Associates.

Network Associates est en mesure de vous procurer d'autres logiciels faisant partie de l'ensemble Total Virus Defense (TVD), la solution anti-virus la plus complète disponible, ainsi que le Total Network Security (TNS), l'ensemble le plus en pointe de l'industrie en matière de sécurité des réseaux. Network Associates les accompagne d'un support de haute qualité, d'une formation et d'un réseau mondial rassemblant des équipes de recherche et de développement. Contactez votre représentant Network Associates ou visitez le site web de Network Associates afin de savoir comment mettre la puissance de Total Virus Defense de votre côté.

# Comment contacter Network Associates

## Service Clients

Pour passer commande ou obtenir des informations complémentaires sur nos produits, appelez notre service Clients au (33 1) 44.69.98.00 ou contactez-nous à l'adresse suivante :

Network Associates International B.V.
P.O. Box 898
7301 BS Apeldoorn
Pays-Bas

# Support technique

Network Associates a toujours mis un point d'honneur à satisfaire ses clients. Nous continuons cette tradition en consentant des investissements considérables en temps et en efforts pour faire de notre site Web une source précieuse d'informations et de réponses aux questions des utilisateurs. Nous vous encourageons à visiter notre site Web sur lequel vous trouverez les réponses aux questions les plus courantes, les mises à jour des logiciels Network Associates et les dernières informations concernant Network Associates et les virus..

| | |
|---|---|
| World Wide Web | http://support.nai.com |

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

| | |
|---|---|
| Internet | tech-support-europe@nai.com |
| CompuServe | GO NAI |

Si les services automatisés ne suffisent pas à résoudre le problème, contactez Network Associates du lundi au vendredi, de 6h00 à 18h00, heure du Pacifique.

Pour les clients multi-licences:

| | |
|---|---|
| Téléphone | +31 20 586 61 00 |
| Fax | +31 20 586 61 01 |

Pour les clients mono-licences:

| | |
|---|---|
| Téléphone | 1 4993 9002 |
| Fax | +31 55 543 46 46 |

Pour permettre aux ingénieurs-techniciens de Network Associates de répondre le plus rapidement et le plus efficacement possible à vos questions, veillez à avoir sous la main les informations suivantes avant d'appeler :

- 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 des fichiers AUTOEXEC.BAT et CONFIG.SYS, et du script LOGIN ;
- Etapes spécifiques permettant de reproduire le problème.

## Formation Network Associates

Pour obtenir des informations sur les programmes de formation sur site pour les produits Network Associates, contactez notre service clientèle au +1 (800) 338-8754.

## Commentaires

Network Associates 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 anti-virus Network Associates à : Network Associates International B.V., P.O. Box 58326, 1040 HH Amsterdam, Pays-Bas. Vous pouvez également télécopier vos commentaires au (31) 20 586 6101 ou les envoyer par courrier électronique à tvd_documentation@nai.com.

## Rapporter les nouveaux virus à incorporer dans les mises à jour des fichiers de données anti-virus

Les logiciels antivirus Network Associates 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 Network Associates 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 Network Associates 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 :

| | |
|---|---|
| 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 des questions ou des échantillons de virus groupés avec le logiciel antivirus du Dr Solomon à nos bureaux au Royaume-Uni |

L'adresse électronique de notre bureau de recherche européen est la 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 |

Les adresses électroniques de nos bureaux de recherche au Japon et dans la zone Asie du Pacifique sont les 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 des questions ou des échantillons de virus à nos bureaux en Australie et en Asie du Sud-est |

# Informations concernant les contacts internationaux

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

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

**Network Associates Autriche**
Pulvermuehlstrasse 17
Linz, Autriche
Code postal : A-4040
Tél. : 43-732-757-244
Télécopie : 43-732-757-244-20

**Network Associates Belgique**
Bessenveldtstraat, 25a
Diegem
1831 - Belgique
Tél. : 32-2-716-4070
Télécopie : 32-2-716-4770

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

**Network Associates Canada**
139 Main Street, Suite 201
Unionville, Ontario
Canada L3R 2G6
Tél. : (905) 479-4189
Télécopie : (905) 479-4540

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

**NA Network Associates Oy**
Sinikalliontie 9, 3rd Floor
02630 Espoo
Finlande
Tél. : 358 9 5270 70
Télécopie : 358 9 5270 7100

**Network Associates France S.A.**
50 rue de Londres
75008 Paris
France
Tél. : 33 1 44 908 737
Télécopie : 33 1 45 227 554

**Network Associates Deutschland GmbH**
Ohmstraße 1
D-85716 Unterschleißheim
Allemagne
Tél. : 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
Tél. : 39 (0)2 9214 1555
Télécopie : 39 (0)2 9214 1644

**Network Associates Amérique latine**
150 S. Pine Island Road, Suite 205
Plantation, Floride 33324
États-Unis d'Amérique
Tél. : (954) 452-1731
Télécopie : (954) 236-8031

**Network Associates International B.V.**
Gatwickstraat 25
1043 GL Amsterdam
Pays-Bas
Tél. : 31 20 586 6100
Télécopie : 31 20 586 6101

**Network Associates Hong Kong**
19th Floor, Matheson Centre
3 Matheson Way
Causeway Bay
Hong Kong 63225
Tél. : 852-2832-9525
Télécopie : 852-2832-9530

**Network Associates Japan, Inc.**
Toranomon 33 Mori Bldg.
3-8-21 Toranomon Minato-Ku
Tokyo 105-0001
Tél. : 81 3 5408 0700
Télécopie : 81 3 5408 0780

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

**Network Associates Portugal**
Av. da Liberdade, 114
1269-046 Lisboa
Portugal
Tél. : 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
Tél. : 27 11 706-1629
Télécopie : 27 11 706-1569

**Network Associates Asie du Sud-est**

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

**Network Associates Espagne**

Orense 4, 4ª Planta.
Edificio Trieste
28020 Madrid
Espagne
Tél. : 34 91 598 18 00
Télécopie : 34 91 556 14 04

**Network Associates Suède**

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

**Network Associates AG**

Baeulerwisenstrasse 3
8152 Glattbrugg
Suisse
Tél. : 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
Tél. : 886-2-27-474-8800
Télécopie : 886-2-27-635-5864

**Network Associates International Ltd.**

Minton Place, Victoria Street
Windsor, Berkshire
SL4 1EG
Royaume-Uni
Tél. : 44 (0)1753 827 500
Télécopie : 44 (0)1753 827 520

# Introduction à VirusScan 1

## Qu’est-ce que VirusScan ?

VirusScan pour Windows NT est un élément clé de la gamme d'outils de sécurité Network Associates Total Virus Defense. La puissance des technologies d'analyse qu'il contient lui permet d'agir comme une sentinelle en ligne infatigable, protégeant vos postes de travail Windows NT des attaques virales et empêchant les dommages provoqués par d'autres logiciels nuisibles.

Dans la mesure où l'informatique en réseau et l'émergence des technologies collaboratives ont considérablement augmenté la vitesse de propagation des virus dans les entreprises, se prémunir contre les logiciels nuisibles n'est désormais 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 de virus. Comparez cela 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. L’analyse régulière de votre disque dur à l'aide de VirusScan réduit considérablement la vulnérabilité de votre machine face aux contaminations et vous permet de ne pas perdre de temps, d'argent et de données inutilement.

VirusScan vous offre les outils nécessaires à la bonne conservation et à la sécurité de votre système. Utilisé correctement comme programme de sécurité à part entière, comprenant des sauvegardes, des protections de mots de passe explicites, de la formation et une prise de conscience, VirusScan permet de préserver votre ordinateur de toute attaque affaiblissant ses performances et d'empêcher la propagation de logiciels nuisibles à travers votre réseau.

## Quels sont les composants fournis avec VirusScan ?

VirusScan comprend plusieurs jeux de composants. Il s'agit d'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 jeux de composants sont les suivants :

- **Composants communs.** Il s'agit des fichiers de données et des autres fichiers d'aide que se partagent de nombreux programmes de VirusScan. Ces fichiers comprennent les fichiers de définition de virus de VirusScan (.DAT), les fichiers de configuration par défaut, les fichiers de validation et d'autres types de fichier.

- **Console antivirus de VirusScan.** Ce composant constitue l'interface principale de VirusScan. Vous pouvez utiliser la console pour créer, configurer et planifier des tâches d'analyse, mettre à jour les fichiers de définition des virus et les programmes, et configurer l'analyse lors de l'accès par VirusScan. La console est fournie avec une série de tâches préconfigurées permettant de mettre à jour les fichiers de définition des virus et les programmes, et avec un dispositif de surveillance des tâches lors de l'accès qui vous permet de configurer la fonction d'analyse en arrière-plan de VirusScan. Vous avez la possibilité de créer de nouvelles tâches d'analyse, soit à l'aide de l'Assistant d'analyse, soit à l'aide d'un ensemble de pages de propriétés. Pour apprendre à démarrer et à utiliser la console, reportez-vous au chapitre 3, “Démarrage,”

- **Scanner à la demande de VirusScan (SCAN32.EXE).** Ce composant vous permet de déclencher une opération d'analyse urgente à tout moment ; cette fonction est qualifiée d'analyse “ à la demande ”. Vous pouvez l'exécuter indépendamment de la console antivirus et l'utiliser pour désigner des disques locaux et en réseau comme cibles d'analyse, choisir la réponse à appliquer aux contaminations détectées et consulter les rapports relatifs aux actions engagées. Lorsque vous planifiez une opération d'analyse à l'aide de la console antivirus, le gestionnaire des tâches de Network Associates lance ce composant pour exécuter l'analyse. Pour apprendre à configurer les analyses à la demande, reportez-vous au chapitre 6, “Planification et exécution des opérations d'analyse à la demande,”

- **Network Associates McShield.** Ce service Windows NT est le composant d'analyse lors de l'accès de VirusScan. Il travaille en arrière-plan et surveille l'activité sur votre poste de travail ou les lecteurs réseau que vous avez reliés à votre système. A chaque fois que vous ou un autre utilisateur ouvre, copie, enregistre ou utilise n'importe quel fichier de votre système, VirusScan l'analyse à la recherche de virus.

  Vous pouvez configurer ce service à partir du dispositif de surveillance lors de l'accès de VirusScan dans la console antivirus. Vous avez également la possibilité de l'activer et de le désactiver à partir du panneau de commandes de Windows NT Services. Network Associates recommande toutefois de gérer ce service à partir de la console antivirus à moins que des circonstances particulières n'exigent de le désactiver à partir du panneau de commandes.

- **Gestionnaire des tâches de Network Associates.** Ce service Windows NT exécute toute opération d'analyse que vous avez planifiée ultérieurement. A l'instar du service Network Associates McShield, il fonctionne en arrière-plan et vous évite de maintenir la console antivirus en fonctionnement afin d'exécuter les tâches planifiées.

  Ce service entre en activité dès que vous installez et redémarrez votre poste de travail. Vous avez la possibilité de l'activer et de le désactiver à partir du panneau de commandes de Windows NT Services, mais Network Associates conseille de le laisser activé, à moins que des circonstances particulières n'exigent de le contrôler à partir du panneau de commandes de Windows NT.

- **Gestionnaire d'alertes.** Ce service Windows NT reçoit et distribue les messages d'alerte qui vous avertissent vous ou d'autres utilisateurs de la détection d'un virus par VirusScan. Le gestionnaire d'alertes offre 10 possibilités différentes d'émettre des messages d'alerte et comprend un utilitaire de configuration souple qui vous permet de définir des options d'envoi. Comme tous les autres services de Network Associates, le gestionnaire d'alertes fonctionne en arrière-plan, et vous pouvez le contrôler depuis le panneau de commandes de Windows NT Services.

- **Utilitaire de copie de fichiers.** Cet utilitaire permet à l'utilitaire de mise à jour et de mise à niveau automatiques de VirusScan de se connecter et de récupérer les mises à jour de fichiers .DAT ainsi que les mises à niveau des programmes à partir des serveurs NetWare de votre réseau. Si vous utilisez un serveur NetWare comme point de distribution central pour les fichiers VirusScan, installez cet utilitaire comme élément d'une installation personnalisée ; l'utilitaire d'installation de VirusScan ne l'installe pas par défaut.

- **Documentation.** La documentation VirusScan se compose des éléments suivants :

  – Un *guide de démarrage* 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.

  – Ce guide de l'utilisateur est enregistré sur le CD-ROM de VirusScan ou installé sur votre disque dur, dans le format .PDF d'Adobe Acrobat. Le *guide de l'utilisateur* de VirusScan offre une description détaillée de l'utilisation de VirusScan, ainsi que d'autres informations utiles, sur les options de configuration avancées ou d'arrière-plan, par exemple. Les fichiers .PDF d'Acrobat sont des documents en ligne maniables contenant des hyperliens, des définitions et d'autres options qui facilitent la navigation au sein de ces documents, et donc l'accès à l'information.

Vous pouvez également télécharger le guide de l'utilisateur à partir du site Web de Network Associates à l'adresse suivante :

ftp://ftp.nai.com/pub/manuals/total_virus_defense/_english_us

– Un fichier d'aide en ligne. Ce fichier contient des astuces et conseils pour une meilleure utilisation de VirusScan. Pour ouvrir le fichier d'aide à partir de VirusScan ou du Planificateur VirusScan, choisissez **Rubriques d'aide** dans le menu **Aide**.

  VirusScan comporte également un système d'aide en ligne contextuel. Avec le bouton droit de la souris, cliquez sur les boutons, les listes ou les autres éléments des boîtes de dialogue pour afficher les rubriques d'aide. Pour ouvrir le fichier d'aide principal rattaché à une rubrique déterminée, cliquez sur les boutons **Aide** lorsque vous les voyez s'afficher.

– Un fichier README.1ST ou LICENSE.TXT. Ce fichier stipule les termes de la licence d'utilisation de VirusScan. Lisez-le avec attention car l'installation de VirusScan implique l'acceptation de ces termes.

– Un fichier WHATSNEW.TXT. Ce fichier présente les modifications et/ou les ajouts de dernière minute, énumère les aspects propres à la diffusion du produit, et décrit généralement les nouvelles fonctions incorporées dans la mise à jour du produit. Le fichier WHATSNEW.TXT réside au niveau de la racine dans la structure arborescente du CD-ROM de VirusScan, ou dans le dossier des programmes 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.

# Caractéristiques de VirusScan

- La technologie d'analyse nouvelle génération de Network Associates permet à VirusScan de détecter et d'éliminer plus de 40 000 virus connus de fichier, de macro, multipartites, furtifs, cryptés et polymorphes.
- Les détecteurs de virus de Network Associates offrent une protection à réaction rapide contre les nouveaux virus et les autres logiciels nuisibles. Un personnel de renommée mondiale, composé des anciennes équipes de McAfee et du Dr Solomon, développe et améliore chaque mise à jour des dispositifs d'analyse et chaque version des fichiers de définition des virus.
- La fonction d'analyse lors de l'accès déclenche la recherche de virus par VirusScan dès que vous créez, ouvrez, enregistrez, exécutez ou copiez des fichiers sur votre réseau.

- La puissance des modules d'analyse à la demande vous permet de lancer une opération d'analyse sur le champ ou de planifier des analyses régulières adaptées à votre flux de travail.
- La technologie avancée d'analyse heuristique détecte des virus de macro jusque-là non identifiés ou non répertoriés.
- Les méthodes d'alerte souples peuvent vous avertir automatiquement de la détection d'un virus par VirusScan, tout en offrant des réponses automatiques vous garantissant la désinfection, l'isolement ou la suppression du fichier infecté, puis l'enregistrement des résultats dans un fichier journal pour une consultation ultérieure.
- La création de tâches d'analyse est simple et rapide grâce à l'Assistant d'analyse intuitif de VirusScan.
- Les mises à jour de définition des virus et les mises à niveau de programmes automatiques et planifiées sont la garantie que VirusScan exploite instantanément la technologie d'analyse pour traiter les virus dès leur apparition. Procédez aux mises à jour à partir d'un site FTP ou d'un serveur désigné sur votre réseau pour assurer un contrôle total des mesures de sécurité antivirus.

# 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. 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 scanner lors de l'accès de VirusScan pour rechercher des virus dans la mémoire de votre ordinateur et pour maintenir un niveau constant de vigilance entre deux analyses. 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. VirusScan est doté d'une série de tâches d'analyse par défaut afin de vous aider à 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 vous connectez ou reliez une unité de réseau à votre système.

Cependant, si votre logiciel de détection n'est pas mis à jour, il se peut que certains nouveaux virus échappent même aux analyses les plus poussées. Avec l'achat de 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. Reportez-vous au chapitre 8, “Mise à jour et Mise à niveau de VirusScan,” pour apprendre à mettre à jour les fichiers de définition des virus et les programmes de VirusScan.

# Comment éliminer l’hypothèse de l’infection virale ?

Tout au long de leur courte existence, les ordinateurs particuliers 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 système VirusScan complète, toutes les variantes des virus connus susceptibles d'infecter votre ordinateur seront découvertes, quelques unes d'entre elles n'ayant 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 tel que McAfee Nuts & Bolts.

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, les brèches dans le système de protection permettant aux pirates informatiques d'empêcher l'accès au réseau et de mettre en panne les systèmes, 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 VirusScan ne détecte aucune infection virale, il est peu probable que votre panne provienne d'un virus - cherchez alors d'autres causes possibles à votre problème. De plus, dans le cas très rare où 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 Network Associates pour identifier, isoler et mettre à jour 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 “Rapporter les nouveaux virus à incorporer dans les mises à jour des fichiers de données anti-virus” à la page xxiii.

# Installation de VirusScan 2

## Présentation

Lors de l'installation, vous pouvez choisir d'installer VirusScan soit sur votre ordinateur local, soit sur d'autres ordinateurs du réseau. La première option copiera tous les fichiers programme de VirusScan sur le disque dur de votre ordinateur. La seconde copiera les composants sélectionnés sur le poste de travail cible.

## Avant de démarrer

Pour installer VirusScan, vous devez avoir les autorisations administratives requises pour le poste de travail local ou distant sur lequel vous envisagez d'installer le programme. Vous devez aussi être connecté correctement à ce système. Examinez la configuration requise indiquée ci-dessous pour déterminer si les postes de travail cibles peuvent exécuter VirusScan.

## Configuration requise

❑ **REMARQUE :** L'essentiel de VirusScan consiste en services Windows NT. Votre poste de travail n'a pas besoin de mémoire supplémentaire pour exécuter ces services, mais la quantité de ressources système qu'ils requièrent peut varier. Si vous indiquez une priorité d'analyse pour chaque tâche, vous pouvez déterminer les ressources système utilisées par le programme.

VirusScan pour Windows NT sera installé et fonctionnera sur un poste de travail local ou distant doté de :

- Un processeur Intel ou d'une architecture compatible, ou encore d'un processeur DEC Alpha
- Windows NT version 3.51 ou supérieure

**IMPORTANT :** N'essayez pas d'installer la version de VirusScan optimisée pour les postes de travail d'architecture Intel sur un système DEC Alpha. N'essayez pas non plus d'installer la version de VirusScan optimisée pour les postes de travail d'architecture Alpha sur des postes dotés d'un processeur Intel ou de processeurs compatibles.

- Windows NT v3.51 Service Pack 5 (requis) ou Windows NT v4.0 Service Pack 4 (recommandé)
- Au moins 6 Mo d'espace disque sur votre poste de travail local. Les postes distants nécessitent généralement moins d'espace disque.

# Installation de VirusScan sur un poste de travail local

Pour installer VirusScan sur votre poste de travail local, vous devez utiliser un compte Windows NT avec des droits d'administrateur. Connectez-vous d'abord à votre système, puis suivez la procédure d'installation présentée ci-après.

## Procédure d'installation

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 ou d'un autre service électronique de Network Associates, créez un répertoire sur votre disque, 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 à partir de 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.

- **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 McAfee VirusScan doit s'afficher automatiquement .

**Procédez comme suit :**

1. Dans le menu **Démarrer**, sélectionnez **Exécuter**.

   La boîte de dialogue Exécuter va apparaître (Figure 2-1 à la page 39).

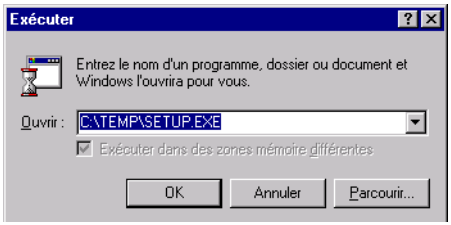



**Figure 2-1. Boîte de dialogue Exécuter**

2. 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 VirusScan Security Suite ou Total Virus Defense, vous devez également préciser le dossier qui contient VirusScan pour Windows NT. Pour savoir où trouver le dossier adéquat, lisez le fichier CONTENTS.TXT inclus dans ces deux CD-ROM.

---

Le programme d'installation se lance et affiche un écran d'accueil (Figure 2-2).

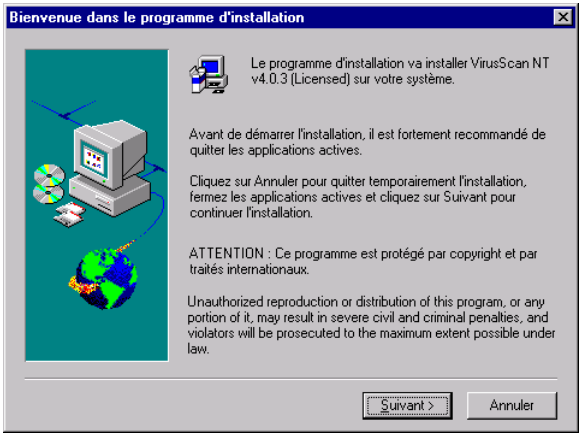



**Figure 2-2. Écran d'accueil de l'assistant Installation**

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

   L'écran suivant affiche le contrat de licence utilisateur final de VirusScan. Lisez ce document attentivement — si vous installez VirusScan, cela veut dire que vous acceptez les termes du contrat de licence.

4. Si vous n'acceptez pas les termes du contrat de licence, cliquez sur **Non**. Vous quitterez immédiatement le programme d'installation. Dans le cas contraire, cliquez sur **Oui** pour continuer.

5. Le programme d'installation vous demande si vous souhaitez installer VirusScan sur votre poste de travail local ou sur d'autres ordinateurs du réseau (référez-vous à la Figure 2-3). Cliquez sur **Installation locale**, puis sur **Suivant>**.

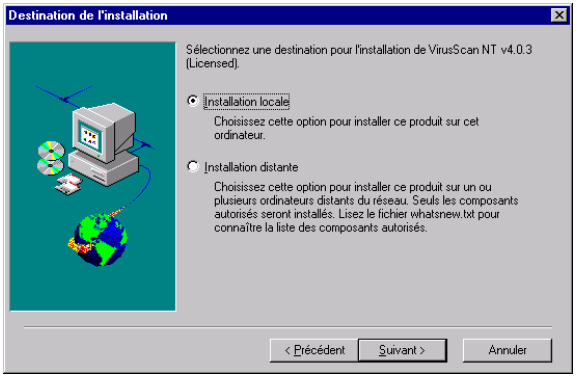



**Figure 2-3. Écran Destination de l'installation**

Si le programme d'installation détecte une version existante de VirusScan pour Windows NT, v3.1.4a ou supérieure, il propose de la supprimer complètement de votre ordinateur ou de supprimer le logiciel tout en conservant vos options de configuration (Figure 2-4 à la page 41).

Si le programme d'installation détecte une version existante de VirusScan pour Windows NT antérieure à v3.1.4a, ou une version existante de Dr Solomon Anti-Virus Toolkit, v7.74 ou supérieure, il propose uniquement de supprimer cette version de votre système.


**Figure 2-4. Écran Installation antérieure détectée**

6. Pour continuer, vous devez choisir l'une des options suivantes :

   - **Préserver**. Cette option indique au programme d'installation de remplacer les fichiers programme antérieurs par les fichiers actuels, mais de préserver les paramètres du programme de la version précédente, notamment les tâches que vous avez créées et toute autre option de configuration que vous avez choisie.
   - **Désinstaller.** Cette option indique au programme d'installation de supprimer la version existante du système, notamment tous les fichiers de configuration, avant de poursuivre l'installation. Vous devrez recréer toutes les tâches dont vous avez besoin et reconfigurer les autres paramètres du programme.

   Une fois que le programme d'installation a terminé de supprimer le logiciel précédent, il affiche l'écran Type d'installation (Figure 2-5).

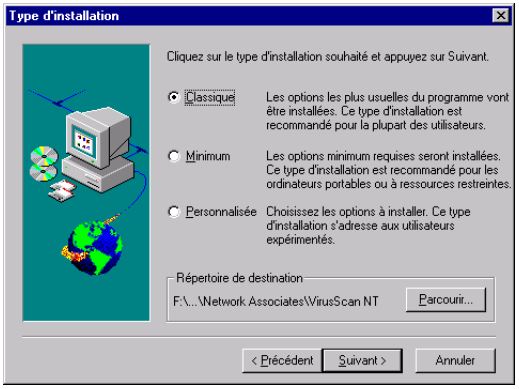



**Figure 2-5. Écran Type d'installation**

7. Sélectionnez les composants de VirusScan que vous souhaitez installer. Vous avez le choix entre les options suivantes :

   - **Par défaut.** Sélectionnez cette option pour installer la console antivirus de VirusScan, les scanners lors de l'accès et à la demande de VirusScan et les services Gestionnaire des tâches et Gestionnaire d'alertes de Network Associates. Ce jeu de composants répond aux besoins de la plupart des utilisateurs.

   - **Compacte.** Sélectionnez cette option pour installer la console antivirus et le service Gestionnaire des tâches de Network Associates. Cela vous permettra de planifier et de lancer des opérations d'analyse uniquement à la demande. Network Associates recommande cette option aux utilisateurs disposant uniquement de l'espace disque minimal requis ou dont le système présente d'autres limites de ce type.

   - **Personnalisée.** Sélectionnez cette option pour choisir les composants de VirusScan que vous souhaitez installer. Par défaut, l'option Personnalisée installe la plupart des composants inclus dans l'option Par défaut, mais vous pouvez également choisir d'installer un utilitaire de copie de fichiers qui fonctionne avec les utilitaires de mise à jour automatique des fichiers DAT et de mise à jour automatique des logiciels pour télécharger les fichiers à partir des serveurs NetWare.

     **IMPORTANT :** *N'installez* l'utilitaire de copie de fichiers sur votre système que si vous utilisez les serveurs NetWare pour distribuer les mises à jour de définition des virus et les mises à niveau du logiciel. Si vous ne disposez pas d'un environnement réseau doté de cette configuration, l'utilitaire de copie de fichiers peut mal orienter les utilitaires de mise à jour automatique des fichiers DAT et de mise à jour automatique des logiciels.

8. Cliquez sur **Parcourir** pour choisir le répertoire de destination des fichiers VirusScan. Par défaut, le programme d'installation installe VirusScan selon le chemin d'accès suivant :

   C:\Program Files\Network Associates\VirusScan NT

9. Après avoir choisi le jeu de composants à installer et spécifié un répertoire de destination, cliquez sur **Suivant>** pour continuer.

- **Si vous avez choisi l'option Par défaut ou Compacte**, le programme d'installation passe directement à l'écran Priorité du compte service. Lisez les informations qui s'affichent, cliquez sur **Suivant>** pour continuer, puis **passez à** étape 10 à la page 44.

- **Si vous avez choisi l'option Personnalisée**, le programme d'installation affiche la liste des composants disponibles pour l'installation (Figure 2-6). Sélectionnez les composants à installer et désélectionnez les cases correspondant aux composants que vous ne souhaitez pas installer.

  Lorsque vous sélectionnez un composant, une description apparaît dans la partie supérieure de l'écran. Une fois vos sélections spécifiées, cliquez sur **Suivant>**.

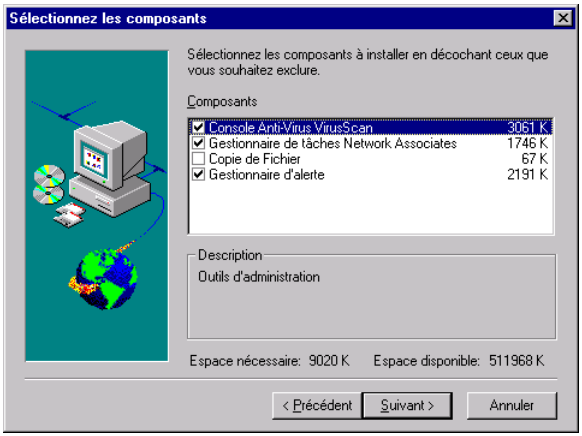



**Figure 2-6. Sélectionnez le panneau Composants**

Les trois écrans suivants vous demandent de choisir les options que vous souhaitez activer pour le service Gestionnaire des tâches, pour une analyse lors de l'accès et pour le Gestionnaire d'alertes.

Le service Gestionnaire des tâches peut ajouter une commande **Scan** qui apparaît chaque fois que vous cliquez avec le bouton droit de la souris sur un fichier ou un disque du bureau Windows ou dans l'Explorateur Windows. Cette commande effectue immédiatement une analyse à la demande sur cet objet à l'aide des options de configuration actives. Cochez la case pour activer cette fonction.

Le scanner lors de l'accès peut lancer des analyses dès que vous avez terminé l'installation et dès que vous démarrez votre poste de travail. Cochez chaque case pour activer ces fonctions.

Le service Gestionnaire d'alertes peut également démarrer dès que l'installation est terminée et chaque fois que vous allumez votre poste de travail. Cochez chacune des cases pour activer ces options.

Cliquez sur **Suivant>** en bas de chaque écran pour continuer. Après avoir choisi vos options, le programme d'installation affiche l'écran Priorité du compte service. Lisez les informations qui s'affichent, puis cliquez sur **Suivant>** pour continuer.

10. Dans l'écran Informations sur le compte du système, choisissez le type de compte qui sera utilisé par VirusScan pour activer ses services Windows NT (Figure 2-7).

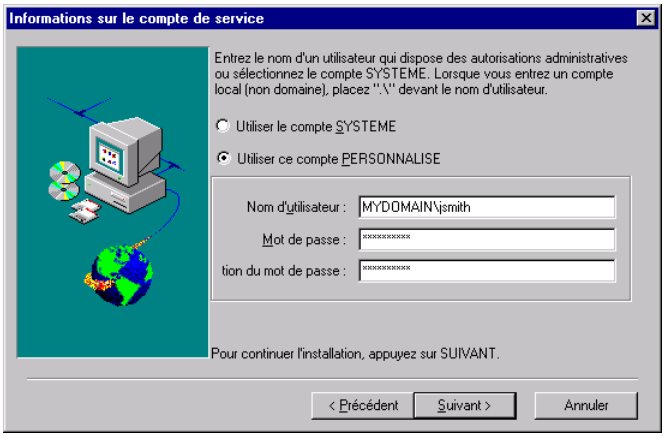



**Figure 2-7. Écran Informations sur le compte service**

11. Vous avez le choix entre les actions suivantes :

    - **Utiliser le compte du SYSTÈME.** Sélectionnez cette option uniquement si vous ne pouvez ou ne souhaitez pas utiliser un compte personnalisé ; le compte du système par défaut ne donne pas à VirusScan suffisamment de droit système pour activer certaines de ses fonctions.

      Par exemple, le Gestionnaire d'alertes ne transmettra pas les messages d'alerte aux serveurs Windows NT et ne les enverra pas vers les imprimantes. AutoUpdate ne pourra pas non plus récupérer les fichiers des partages de Windows NT au cours des tâches de mise à jour planifiées. En outre, VirusScan ne consignera pas les événements distants et n'exécutera pas les opérations d'analyse prévues sur les lecteurs du réseau.

- **Utiliser ce compte PERSONNALISÉ.** Sélectionnez cette option afin d'utiliser un compte valide pour ce poste de travail avec la totalité des droits d'administrateur. Cela permet à VirusScan d'activer tous ses services Windows NT.

  Ensuite, spécifiez le domaine de connexion, le cas échéant, et le nom d'utilisateur pour le compte dans la première zone de texte ci-dessous. N'oubliez pas d'insérer une barre oblique (\) avant le nom d'utilisateur, qu'elle soit précédée ou non d'un nom de domaine. Entrez le mot de passe du compte, puis confirmez-le dans les deux zones de texte suivantes.

  Une fois vos sélections spécifiées, cliquez sur **Suivant>**.

12. Dans l'écran suivant, le programme d'installation affiche un nom par défaut pour le dossier de programme qu'il va créer. Vous pouvez taper un nouveau nom ou en sélectionner un dans la liste Dossiers existants. Pour accepter le nom de dossier par défaut ou le nom que vous avez désigné, cliquez sur **Suivant>**.

    Dans l'écran suivant, le programme d'installation récapitule toutes les options que vous avez choisies. Si elles sont correctes, cliquez sur **Suivant>** pour commencer à copier les fichiers programme de VirusScan sur votre disque dur. Dans le cas contraire, cliquez sur **<Précédent** pour regagner les écrans précédents et modifier vos options.

    Une fois que les fichiers ont été copiés, le programme d'installation affiche le fichier WHATSNEW.TXT que vous devez lire. Cliquez sur **Oui** pour ouvrir le fichier. Il contient des ajouts de dernière minute relatifs aux fonctions, aux problèmes connus et d'autres informations importantes. Vous trouverez également une copie de ce fichier dans le répertoire du programme VirusScan.

13. Cliquez sur **Terminer** pour terminer l'installation de VirusScan.

# Installation de VirusScan sur un poste de travail distant

L'utilitaire d'installation de VirusScan vous permet d'installer le programme sur plusieurs autres postes de travail de votre réseau, à condition que vous disposiez d'un compte avec des droits d'administrateur sur chaque poste cible.

En outre, VirusScan est compatible avec Microsoft BackOffice et inclut un fichier pré-écrit (PDF) de définition du programme à utiliser avec System Management Server (SMS). Vous pouvez utiliser SMS pour installer le logiciel sur plusieurs postes de travail de votre réseau. Pour apprendre comment utiliser SMS pour déployer le programme d'installation VirusScan, consultez votre documentation Microsoft SMS.

## Procédure d'installation

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 ou d'un autre service électronique de Network Associates, créez un répertoire sur votre disque, 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 à partir de 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.

- **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 McAfee VirusScan doit s'afficher automatiquement.

**Procédez comme suit :**

1. Choisissez **Exécuter** depuis le **menu** Démarrer dans la barre des tâches de Windows.

   La boîte de dialogue Exécuter va apparaître (Figure 2-8).

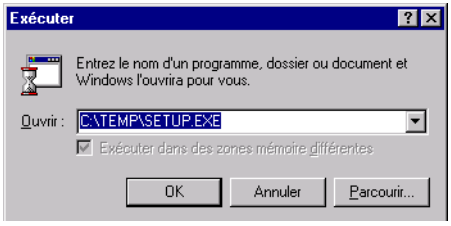



**Figure 2-8. Boîte de dialogue Exécuter**

2. 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 VirusScan Security Suite ou Total Virus Defense, vous devez également préciser le dossier qui contient VirusScan pour Windows NT. Pour savoir où trouver le dossier adéquat, lisez le fichier CONTENTS.TXT inclus dans ces deux CD-ROM.

   ---

   Le programme d'installation se lance et affiche un écran d'accueil (Figure 2-9).

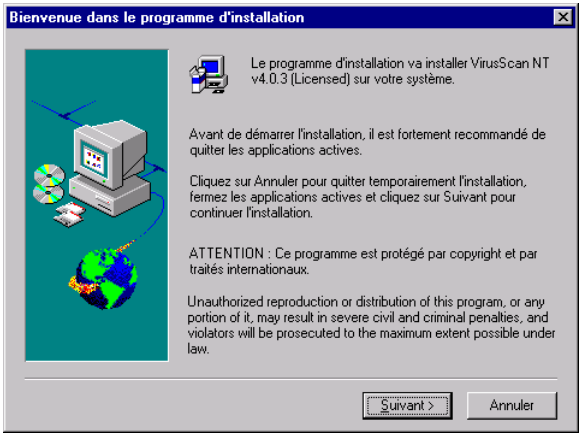



**Figure 2-9. Écran d'accueil de l'assistant Installation**

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

   L'écran suivant affiche le contrat de licence utilisateur final de VirusScan. Lisez ce document attentivement — si vous installez VirusScan, cela veut dire que vous acceptez les termes du contrat de licence.

4. Si vous n'acceptez pas les termes du contrat de licence, cliquez sur **Non**. Vous quitterez immédiatement le programme d'installation. Dans le cas contraire, cliquez sur **Oui** pour continuer.

5. Le programme d'installation vous demande si vous souhaitez installer VirusScan sur votre poste de travail local ou sur d'autres ordinateurs du réseau (voir Figure 2-3 à la page 40). Cliquez sur **Installation distante**, puis sur **Suivant>**.

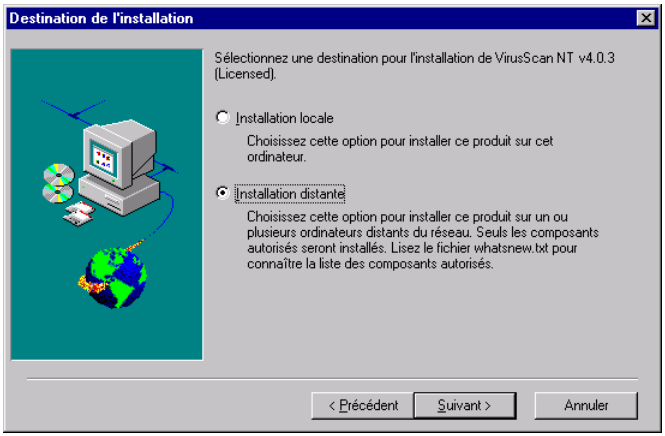



**Figure 2-10. Écran Destination de l'installation**

L'écran Sélectionner le serveur distant apparaît (Figure 2-11). Vous pouvez préciser les ordinateurs sur lesquels vous souhaitez installer VirusScan.

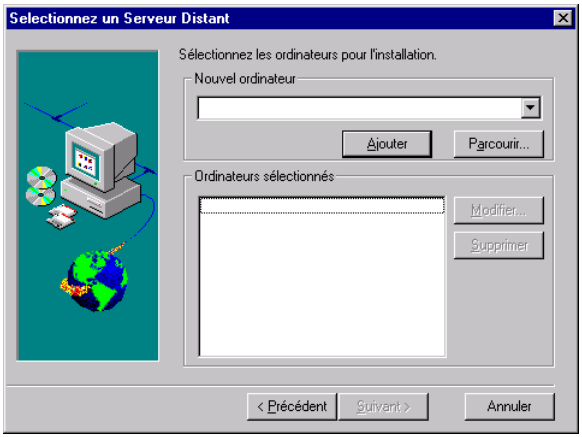



**Figure 2-11. Écran Sélectionner le serveur distant**

Procédez comme suit :

a. Cliquez sur **Parcourir** pour ouvrir la boîte de dialogue qui vous permet de localiser un ordinateur du réseau (Figure 2-12 à la page 49).

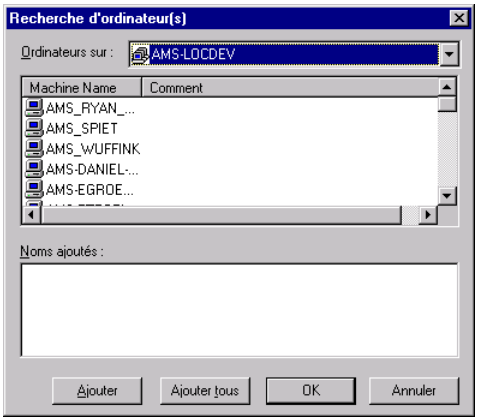



**Figure 2-12. Boîte de dialogue Recherche des ordinateurs**

b. Dans le menu **Afficher les machines à partir de**, choisissez le domaine dans lequel la recherche se fera. Le programme d'installation se connecte au réseau et affiche tous les ordinateurs accessibles dans ce domaine.

c. Sélectionnez-en un ou plusieurs dans la liste. Pour sélectionner plusieurs noms, appuyez sur la touche CTRL du clavier tout en cliquant sur chaque nom. Pour sélectionner une série continue de noms, cliquez sur le premier nom, puis appuyez sur la touche SHIFT du clavier tout en cliquant sur le dernier nom de la liste.

d. Cliquez sur **Ajouter** pour sélectionner les ordinateurs que vous avez choisis. Les noms apparaissent dans la liste en bas de la boîte de dialogue. Pour ajouter tous les ordinateurs du domaine, cliquez sur **Ajouter tout**. Puis, cliquez sur **OK** pour fermer la boîte de dialogue et retourner à l'écran Sélectionner le serveur distant.

6. Les ordinateurs que vous avez désignés s'affichent dans la zone de texte Nouvel ordinateur. Cliquez sur **Ajouter** pour ouvrir une boîte de dialogue où vous pouvez préciser le nom d'utilisateur et le mot de passe pour un compte avec des droits d'administrateur sur le poste de travail cible (Figure 2-13 à la page 50).

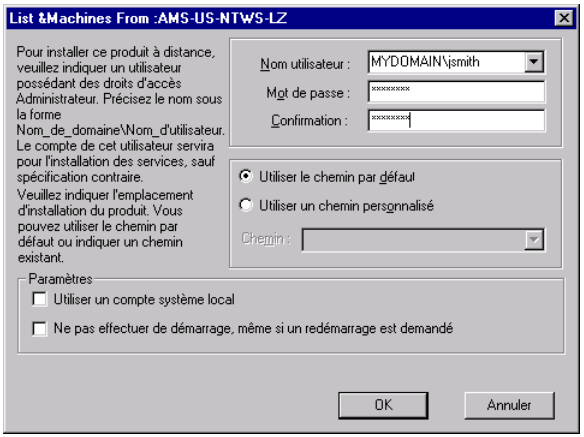



**Figure 2-13. Boîte de dialogue Installation distante**

7. Entrez un nom d'utilisateur dans la zone de texte à cet effet, ou bien choisissez l'un des comptes répertoriés dans la liste. N'oubliez pas d'insérer un nom de domaine et une barre oblique (\) avant le nom d'utilisateur. Ensuite, entrez un mot de passe et confirmez-le dans les deux zones de texte suivantes.

8. Au centre de la boîte de dialogue, précisez l'emplacement, sur le poste de travail, où seront installés les fichiers programme de VirusScan. Vous pouvez choisir d'installer VirusScan selon le chemin d'accès par défaut suivant :

   C:\Program Files\Network Associates\VirusScan NT

   ou désigner un chemin différent pour ce poste de travail. Vérifiez que le chemin que vous désirez utiliser existe bien sur le poste de travail cible car le programme d'installation ne va pas le créer.

9. Cochez la case **Utiliser un compte de système local,** pour indiquer à VirusScan d'activer ses services Windows NT par l'intermédiaire du compte du système par défaut sur le poste de travail cible. Si vous ne le faites pas, VirusScan utilisera le compte que vous avez spécifié en haut de la boîte de dialogue.

Sélectionnez l'option compte du système uniquement si vous ne pouvez ou ne souhaitez pas utiliser un compte personnalisé pour ce poste de travail. Le compte du système par défaut ne donne pas à VirusScan suffisamment de droits système pour activer certaines de ses fonctions. Par exemple, le Gestionnaire d'alertes ne transmettra pas les messages d'alerte aux serveurs Windows NT et ne les enverra vers les imprimantes. AutoUpdate ne pourra pas non plus récupérer les fichiers des partages de Windows NT au cours des tâches de mise à jour planifiées. En outre, VirusScan ne consignera pas les événements distants et n'exécutera pas les opérations d'analyse prévues sur les lecteurs du réseau.

10. Cochez la case **Ne pas redémarrer même si le redémarrage est nécessaire** pour empêcher le poste de travail cible de redémarrer après l'installation. Certains services VirusScan vous obligent à réamorcer le poste de travail avant d'être activés. Ces services restent inactifs jusqu'à ce que vous redémarriez ce poste de travail.

11. Cliquez sur **OK** pour fermer la boîte de dialogue. Le programme d'installation affiche la liste des serveurs que vous avez sélectionnés pour l'installation dans l'écran Confirmer les paramètres d'installation. Si ces paramètres sont corrects, cliquez sur **Suivant>** pour commencer à copier les fichiers sur les postes de travail cibles. Dans le cas contraire, cliquez sur **<Précédent** afin de modifier vos options.

    Le programme d'installation effectuera une installation silencieuse de VirusScan sur chaque poste de travail cible. Pendant l'installation, les utilisateurs ne verront qu'un bouton de programme minimisé dans la barre des tâches de Windows.

---

❑ **REMARQUE :** Si les utilisateurs travaillant sur l'ordinateur cible cliquent sur le bouton minimisé de l'installation silencieuse dans la barre des tâches, une petite boîte de dialogue décrivant l'état de l'installation s'ouvre. S'ils cliquent sur **OK** pour fermer la boîte de dialogue, la fenêtre se minimise une nouvelle fois. Mais s'ils cliquent sur la case de fermeture, l'installation s'arrête immédiatement.

---

# Procéder à une installation " silencieuse "

Si vous gérez un réseau et souhaitez déployer l'application antivirus VirusScan standard, vous pouvez utiliser l'option d'installation " silencieuse " de l'utilitaire d'installation pour mettre en place VirusScan sur chaque nœud du réseau avec peu ou pas d'interaction avec les utilisateurs finaux. Au cours d'une installation silencieuse, le programme d'installation n'affiche pas les écrans ou fenêtres habituels de l'assistant et l'utilisateur final n'a pas non plus accès aux options de configuration. C'est vous qui prédéfinissez ces choix et

exécutez le programme d'installation en tâche de fond sur chaque poste de travail cible. Si vous le souhaitez, vous pouvez même installer VirusScan sur un poste de travail qui fonctionne sans opérateur ou à l'insu de l'utilisateur final, à condition que vous disposiez de toutes les autorisations administratives requises.

Une installation silencieuse consiste en deux étapes principales. Vous devez d'abord installer sur votre ordinateur ou serveur administratif les mêmes composants VirusScan que vous souhaitez que le programme installe sur chaque poste de travail cible. Un mode spécial d'installation enregistre les choix que vous avez faits au cours de l'installation et les conserve dans un fichier de configuration appelé SETUP.ISS. Puis, vous devez utiliser un mode d'installation différent pour mettre en place une configuration de VirusScan identique sur chaque système cible. Le programme utilisera le fichier SETUP.ISS créé à la première étape pour vous guider à chaque installation ultérieure.

## Enregistrement de vos préférences

**Pour tester votre installation, exécutez la procédure suivante :**

1. Cherchez un fichier SETUP.ISS existant dans le dossier \WINDOWS sur votre ordinateur administratif. Si vous trouvez un fichier portant ce nom dans le dossier WINDOWS, renommez-le ou supprimez-le.

   Lors de l'enregistrement de vos préférences d'installation, le programme les sauvegarde dans un nouveau fichier SETUP.ISS situé dans le même dossier.

2. Choisissez **Exécuter** depuis le **menu** Démarrer dans la barre des tâches de Windows.

   La boîte de dialogue Exécuter va apparaître (Figure 2-14).

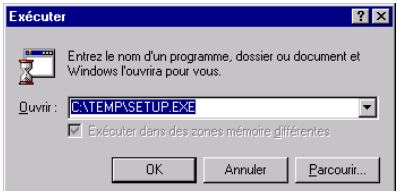



**Figure 2-14. Boîte de dialogue Exécuter**

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. La lettre -R demande au programme d'installation de s'exécuter en mode " enregistrement ".

   ---

   **REMARQUE :** Si vous disposez de VirusScan sur un CD-ROM VirusScan Security Suite ou Total Virus Defense, vous devez également préciser le dossier qui contient VirusScan pour Windows NT. Pour savoir où trouver le dossier adéquat, lisez le fichier CONTENTS.TXT inclus dans ces deux CD-ROM.

   ---

   Pour rechercher les fichiers sur le disque dur ou le CD-ROM, cliquez sur **Parcourir**. Ayez soin d'ajouter la lettre -R à la commande d'exécution si vous utilisez cette option.

4. Suivez les procédures d'installation qui figurent aux pages 38 à 45 pour choisir les composants et les paramètres que vous souhaitez appliquer à chaque poste de travail.

   Le programme d'installation note les choix que vous avez faits à chaque étape et les enregistre sous forme d'entrées dans le fichier SETUP.ISS.

   ---

   **IMPORTANT :** Prenez grand soin au cours de l'installation initiale de répondre à toutes les questions qui figurent sur les écrans de l'assistant et de respecter l'ordre proposé des étapes d'installation sinon l'installation silencieuse que vous lancerez ultérieurement échouera. Vous ne pouvez pas revenir en arrière pendant l'installation pour modifier vos paramètres.

   Pour spécifier des options différentes, vous devrez recommencer l'installation depuis le début afin que le programme sauvegarde vos choix correctement. Si vous envisagez d'installer VirusScan sur des postes de travail qui fonctionnent sans opérateur, ayez soin de préciser les options qui ne nécessitent pas d'interaction avec l'utilisateur.

   L'installation échouera également si VirusScan détecte un virus sur votre ordinateur.

   ---

5. A la fin de l'installation, cliquez sur **Terminer** pour quitter le programme d'installation.

## Édition d'un fichier SETUP.ISS pour spécifier un répertoire d'installation

Si vous souhaitez que le programme installe VirusScan dans un répertoire particulier, vous devrez éditer le fichier SETUP.ISS que vous avez créé lors de l'installation de VirusScan sur votre ordinateur administratif. Pour faciliter l'administration du réseau, vous pourriez notamment vouloir installer toutes les copies de VirusScan dans le même répertoire sur chaque nœud du réseau.

SETUP.ISS est un simple fichier texte avec un format spécial identique à des fichiers de configuration tels que WIN.INI ou SYSTEM.INI. Vous pouvez l'ouvrir avec tout éditeur de texte et modifier chacune de ses entrées pour qu'elles répondent à vos besoins.

---

❑ **REMARQUE :** Network Associates recommande que vous ne procédiez qu'à un nombre limité de modifications dans le fichier SETUP.ISS. Si vous souhaitez avoir un contrôle complet du processus d'installation, ou si vous voulez spécifier à l'avance les options de configuration pour chaque copie de VirusScan, vous pouvez utiliser ISeamless, un puissant outil de scripte conçu par Network Associates à cet effet. Contactez Network Associates Support technique pour plus de détails.

---

SETUP.ISS spécifie un répertoire d'installation sous la forme d'une valeur pour la variable **szDir,** qui figure sous l'en-tête **[SdSetupType-0]**. Par défaut cette entrée s'écrit :

```
SdSetupType-0]
szDir=C:\Program Files\Network Associates\VirusScan NT\
Result=401
```

Pour spécifier un autre répertoire d'installation, remplacez le chemin d'accès affiché par celui que vous souhaitez. Le répertoire d'installation que vous spécifiez à cet endroit remplacera le répertoire d'installation par défaut sur chaque système cible.

---

**IMPORTANT :** Le programme d'installation crée un unique fichier SETUP.ISS pour chaque produit de Network Associates sur chaque plate-forme. Vous devez utiliser le fichier correspondant au système d'exploitation exécuté sur le poste de travail cible. Vous ne devez pas notamment utiliser un fichier SETUP.ISS créé au cours d'une installation de VirusScan sous Windows 95 pour contrôler une installation de VirusScan sous Windows NT.

---

6. Enregistrez le fichier en format de texte, puis quittez votre éditeur de texte.

**IMPORTANT :** Network Associates recommande que vous utilisiez le fichier SETUP.ISS que vous avez créé pour effectuer un test d'installation sur un poste de travail unique avant de l'utiliser pour étendre VirusScan à l'ensemble de votre réseau.

## Exécuter une installation silencieuse

Une fois que vous disposez d'un fichier SETUP.ISS dans lequel figurent tous les composants et paramètres que vous souhaitez utiliser sur chaque poste de travail de votre réseau, vous pouvez recopier ces paramètres pour chaque copie de VirusScan installée. Voir "Enregistrement de vos préférences" à la page 52 pour savoir comment créer le fichier SETUP.ISS.

Vous pouvez exécuter une installation silencieuse de plusieurs manières et avec plusieurs niveaux d'interaction avec les utilisateurs du réseau. Vous pouvez notamment créer un scripte pour vos utilisateurs. Celui-ci exécute une installation silencieuse de VirusScan dès que les utilisateurs se connectent à un serveur d'identification sans autre interaction que celle qui est nécessaire à la connexion. Vous pouvez également demander à vos utilisateurs de lancer l'installation à partir d'un serveur désigné. D'autres options permettent encore de déployer VirusScan par le biais d'une application de gestion de réseau telle que Zero Administration Client (ZAC) ou Management Edition conçues par Network Associates, System Management Server (SMS) de Microsoft, ou d'autres programmes similaires.

Quelle que soit la méthode que vous choisissez, vous devez préparer le paquet VirusScan en vue de son installation, puis lancer le programme d'installation en mode silencieux.

**Procédez comme suit :**

1. Copiez les fichiers d'installation de VirusScan à partir du disque CD-ROM VirusScan ou du dossier sur votre ordinateur administratif dans lequel vous les stockez, dans un répertoire de VirusScan sur un serveur central. Vos utilisateurs ou l'application gérant votre réseau installeront VirusScan depuis ce serveur.
2. Localisez le fichier SETUP.ISS qui est stocké dans le répertoire de VirusScan sur le serveur central. Renommez-le ou supprimez-le.
3. Copiez le fichier SETUP.ISS que vous avez créé lors de l'exécution de l'installation enregistrée sur votre ordinateur administratif, dans le répertoire de VirusScan sur le serveur central. Vous trouverez le fichier que vous devez copier dans le répertoire WINDOWS de votre ordinateur administratif. Voir "Enregistrement de vos préférences" à la page 52 pour apprendre comment enregistrer votre installation.

Une fois cette étape achevée, vos utilisateurs ou l'application gérant votre réseau sont en mesure d'exécuter le programme d'installation en mode silencieux pour copier l'installation que vous avez enregistrée.

Pour exécuter le programme d'installation en mode silencieux, incluez la ligne de commande `<X>:\SETUP.EXE -S` dans tous les scriptes de connexion que vous rédigez ou dans toutes les instructions destinées à vos utilisateurs indiquant comment lancer le programme. Dans cette ligne, la lettre `<X>` représente le chemin d'accès au dossier du serveur contenant les fichiers d'installation de VirusScan et le fichier SETUP.ISS que vous avez créé. La lettre `-S` demande au programme d'installation de s'exécuter en mode silencieux. Par défaut, le programme redémarre le poste de travail lorsque qu'il a achevé l'installation des fichiers.

Si vous ne voulez pas que le programme d'installation réamorce chaque poste de travail cible, vous devez éditer le fichier SETUP.ISS que vous avez créé lors de l'installation enregistrée. Vous devrez changer la valeur de l'entrée **Option de réamorçage** de ce fichier sous l'en-tête **[sdFinishReboot - 0]** de sa valeur courante à zéro (0). Cette valeur indique au programme d'installation de ne pas forcer le poste de travail à se réamorcer.

Une étape supplémentaire dans la mise en place sur l'ensemble de votre réseau d'une politique de sécurité anti-virus efficace consiste aussi à copier un fichier de configuration contenant les options que vous souhaitez que vos serveurs possèdent dans le répertoire d'installation de chaque poste de travail. Pour apprendre comment sauvegarder vos paramètres dans un fichier de configuration, consultez la section "Utilisations des menus de VirusScan" à la page 133.

---

**REMARQUE :** Pour prédéfinir vos options de configuration afin que VirusScan s'installe avec celles déjà en place, utilisez l'utilitaire de scripte Iseamless de Network Associates. Cet utilitaire vous permet un contrôle total des options d'installation et de configuration. Contactez votre revendeur ou l'aide technique de Network Associates pour plus de détails.

---

# Validation des fichiers

Lorsque vous téléchargez ou copiez des fichiers à partir d'une source extérieure, vous exposez votre ordinateur à un risque d'infection virale, même si ce risque est peu élevé. Le téléchargement d'un logiciel antivirus n'échappe pas à cette règle. Network Associates a adopté des mesures de sécurité rigoureuses et étendues visant à garantir l'authenticité, la fiabilité et l'absence de virus dans les produits que vous pouvez acquérir ou télécharger à partir de son site Web ou de ses autres services électroniques. Cependant, les antivirus attirent tout particulièrement l'attention de certains auteurs de virus diffusant des copies infectées ou utilisant les mêmes noms de fichiers afin de camoufler leurs propres écrits.

Vous pouvez vous protéger contre cette éventualité et contre la corruption éventuelle des fichiers téléchargés en veillant à

- télécharger vos fichiers uniquement à partir du site Web de Network Associates; et à
- valider les fichiers téléchargés.

Network Associates fournit une copie de son utilitaire de validation VALIDATE.EXE avec chaque logiciel VirusScan.

---

**Pour valider vos fichiers, effectuez les opérations suivantes :**

1. Installez VirusScan en suivant les instructions de la "Procédure d'installation", pages 38 à 45.
2. Cliquez sur **Démarrer** dans la barre des tâches de Windows, pointez sur **Programmes** et sélectionnez **Invite de commande**.
3. Dans la fenêtre qui apparaît, modifiez l'invite de la ligne de commande pour qu'elle pointe sur le répertoire contenant les fichiers VirusScan que vous avez installés. Si vous avez choisi le répertoire de destination par défaut, le chemin d'accès aux fichiers sera le suivant :

   C:\Program Files\Network Associates\VirusScan NT

   Si vous avez installé VirusScan dans un autre répertoire, tapez son chemin d'accès.

4. Exécutez VALIDATE.EXE. Pour cela, tapez `validate *.*` à l'invite de la ligne de commande.

   VALIDATE.EXE analyse tous les fichiers placés dans le répertoire d'installation de VirusScan, puis génère une liste des fichiers comportant le nom des fichiers, leur taille en octets, la date et l'heure de leur création, ainsi que deux codes de validation dans des colonnes séparées.

   Si vous voulez que VALIDATE.EXE examine un fichier individuellement, tapez `validate` à l'invite, suivi du nom du fichier que vous souhaitez vérifier, ou utilisez les caractères génériques DOS ? et * pour spécifier une série de fichiers.

   ---

   ❑ **REMARQUE :** Afin d'en faciliter la lecture, Network Associates vous recommande de rediriger le fichier résultant de l'exécution de VALIDATE.EXE vers votre imprimante. Si la configuration de votre imprimante vous permet d'imprimer à partir de programmes MS-DOS, tapez simplement `validate * *>lpt1` à l'invite de la ligne de commande. Pour savoir comment paramétrer votre imprimante pour qu'elle puisse imprimer à partir de programmes MS-DOS, consultez votre documentation Windows.

   ---

   Pour vérifier que vous disposez exactement des mêmes fichiers que ceux utilisés par nos ingénieurs pour votre copie de VirusScan, vous devez comparer les codes de validation à la liste de distribution fournie avec le programme. La liste de distribution est un fichier texte contenant les codes de validation que les ingénieurs Network Associates ont générés à partir des procédures de contrôle de redondance cyclique (CRC) effectuées lors de la constitution du coffret VirusScan. Cette méthode garantit une sécurité élevée et prévient les risques de manipulation abusive.

5. Pour afficher la liste de distribution, tapez `type packing.lst` à l'invite de la ligne de commande, puis appuyez sur ENTRÉE.

   ---

   ❑ **REMARQUE :** Network Associates vous recommande également de rediriger le fichier résultant de l'exécution de PACKING.LST vers votre imprimante. Pour cela, tapez `type packing.lst>lpt1` à l'invite de la ligne de commande.

   ---

6. Comparez le fichier résultant de l'exécution de VALIDATE.EXE à celui résultant de l'exécution de PACKING.LST. Les tailles, les heures et les dates de création, ainsi que les codes de validation pour chaque nom de fichier—c'est à dire, ceux avec des extensions .EXE et .DLL —doivent correspondre exactement. Dans le cas contraire, supprimez immédiatement le fichier— vous ne devez *pas* ouvrir le fichier ni l'analyser avec un autre utilitaire, au risque de contracter un virus.

---

**IMPORTANT :** La vérification de vos fichiers VirusScan à l'aide de VALIDATE.EXE ne vous *garantit* pas que votre copie est exempte de défauts, d'erreurs de copie, d'infections virales ou de manipulations abusives. Cependant, les mesures de sécurité adoptées permettent de dire que, s'ils possèdent les bons codes de validation, il est fort peu probable que les fichiers aient fait l'objet de manipulations abusives. Reportez-vous aux fichiers LICENSE.TXT ou README.1ST fournis avec votre copie de VirusScan pour connaître les termes de la licence couvrant l'utilisation du logiciel.

Les codes de validation pour certains fichiers, notamment ceux ayant l'extension .INI et .VSC *peuvent ne pas correspondre à ceux* figurant dans PACKING.LST, car le programme d'installation est susceptible de procéder à des modifications sur ces fichiers pendant l'installation.

---

# 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, exécutez la procédure suivante :**

1. Ouvrez un éditeur de texte Windows standard, tel que Notepad, et tapez ensuite la ligne suivante :

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

**REMARQUE :** La chaîne de caractères ci-dessous doit constituer *une seule ligne* dans la fenêtre de votre éditeur de texte. Si vous consultez ce guide sur votre ordinateur, vous pouvez copier la ligne directement à partir du fichier Acrobat vers Notepad.

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.

# Démarrage 3

## Activation des composants de VirusScan

VirusScan pour Windows NT se compose d'une application, dite console antivirus, et d'un ensemble de services Windows NT offrant des fonctions d'action et de journalisation en plus des fonctions d'analyse. La console antivirus permet de configurer les tâches d'analyse, de définir des opérations d'analyse lors de l'accès et de choisir d'autres options du programme. Elle permet également d'afficher des statistiques d'analyse et de recevoir des messages d'alerte en cas d'infection.

Vous devez impérativement utiliser la console antivirus pour configurer les services. Toutefois, VirusScan pourra mener les analyses en arrière-plan et les autres tâches d'analyse planifiées même si la console est inactive. En revanche, ces opérations nécessitent de maintenir actifs les services Gestionnaire des tâches et McShield de Network Associates.

---

❑ **REMARQUE :** Il n'est *pas* nécessaire de lancer les services Windows NT de VirusScan séparément. En revanche, vous pouvez les activer ou les désactiver à partir du panneau de configuration des services Windows NT.

Dans la mesure où le programme ne peut pas toujours se procurer les informations nécessaires pour déterminer l'état de ces services, l'utilisation du panneau de configuration pour changer ses fonctions peut entraîner un comportement imprévisible de VirusScan, en particulier de son scanner lors de l'accès. C'est pourquoi Network Associates recommande de gérer les opérations du programme de préférence au moyen de la console antivirus .

---

## Démarrage de la console antivirus de VirusScan

Démarrer la console antivirus

- Lancez le gestionnaire de programmes de Windows NT 3.51, ouvrez le groupe de programmes VirusScan puis double-cliquez sur l'icône Console VirusScan.
- Dans Windows NT 4.0, Windows 95 et Windows 98, cliquez sur **Démarrer** dans la barre des tâches de Windows, pointez le curseur sur **VirusScan** dans le sous-menu **Programmes**, puis choisissez **Console VirusScan.**

La fenêtre de la console VirusScan s'affiche (voir la Figure 3-1).

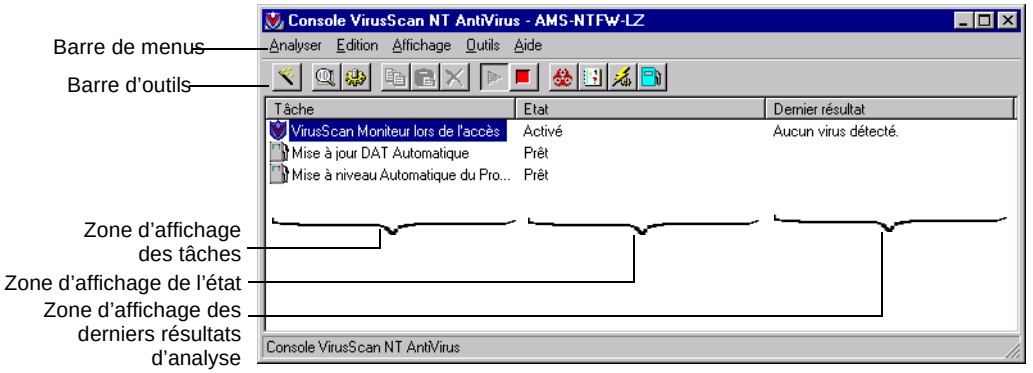



**Figure 3-1. Fenêtre de la console VirusScan**

La fenêtre de la console comprend un menu, une barre des tâches, une liste des tâches et une barre d'état. Chacun de ces outils fournit des informations ou propose des fonctions permettant de créer, de configurer, de modifier ou de supprimer des opérations d'analyse ainsi que d'autres tâches de VirusScan. Les sections suivantes proposent une description détaillée de chaque élément.

## Liste des tâches

Une tâche est un ensemble d'instructions destinées à exécuter un programme ou une analyse spécifique, dans une configuration donnée, à une heure donnée. VirusScan peut effectuer trois types de tâche : les tâches lors de l'accès, les tâches à la demande ou planifiées, et les mises à jour automatiques des fichiers DAT ou les mises à niveau automatiques des logiciels. La liste des tâches affiche une série de tâches définies par défaut qui permettent d'actualiser les fichiers de définition des virus et de mettre à niveau les fichiers programme. Elle comprend également le dispositif de surveillance lors de l'accès de VirusScan, un utilitaire permettant de configurer et contrôler le composant d'analyse lors de l'accès de VirusScan. La liste des tâches ne comprend aucune tâche à la demande ou planifiée par défaut ; vous pouvez les créer selon vos besoins.

### Dispositif de surveillance lors de l'accès de VirusScan

Le scanner lors de l'accès de VirusScan recherche les virus dans les fichiers que vous ouvrez, enregistrez ou copiez depuis et vers la station de travail. Le dispositif de surveillance des tâches lors de l'accès permet de spécifier les fichiers à analyser et les actions que VirusScan doit entreprendre s'il détecte des fichiers infectés. Pour savoir comment modifier les paramètres des tâches lors de l'accès, consultez la section "Configuration du scanner lors de l'accès" à la page 99

### Tâches à la demande et tâches planifiées

Les tâches à la demande permettent de déclencher une opération d'analyse instantanément. Vous pouvez désigner les volumes à analyser sur votre poste de travail, indiquer à VirusScan les actions à entreprendre s'il détecte un fichier infecté, choisir les options d'alerte et d'enregistrement, puis déclencher l'exécution du programme. Les tâches planifiées s'exécutent à des heures précises ou à intervalles périodiques, et peuvent comporter toutes les options disponibles pour l'analyse à la demande. VirusScan ne propose aucune tâche à la demande ou planifiée prédéfinie. Pour savoir comment configurer les tâches à la demande ou planifier les tâches d'analyse, reportez-vous au chapitre 6, "Planification et exécution des opérations d'analyse à la demande,"

### Tâches de mise à jour automatique des fichiers DAT et de mise à niveau automatique des logiciels

La mise à jour automatique des fichiers DAT permet de récupérer de nouveaux fichiers de définition des virus qui seront utilisés par VirusScan. La mise à niveau automatique des logiciels permet quant à elle de récupérer de nouveaux fichiers programme destinés à VirusScan lui-même, à partir d'un site FTP ou d'un serveur de réseau préalablement désigné comme site d'approvisionnement. La mise à jour automatique des fichiers DAT peut également acheminer les fichiers téléchargés vers un autre serveur d'approvisionnement à l'attention d'autres stations de travail. La mise à niveau automatique des logiciels récupère de nouveaux fichiers programme qui actualisent VirusScan. Pour apprendre comment créer et planifier les tâches de mise à jour automatique des fichiers DAT et de mise à niveau automatique, reportez-vous au chapitre 8, "Mise à jour et Mise à niveau de VirusScan,"

### Statistiques sur les tâches

Pour afficher les derniers résultats et informations disponibles pour une tâche d'analyse lors de l'accès ou à la demande, sélectionnez la tâche en question puis choisissez l'option **Statistiques** dans le menu **Analyser** pour ouvrir la boîte de dialogue Statistiques des tâches (Figure 3-2 à la page 64). Vous pouvez également afficher cette boîte de dialogue en double-cliquant sur l'une des

tâches de la liste. Les tâches de mise à jour automatique des fichiers DAT et de mise à niveau automatique des logiciels ne permettent pas d'accéder aux statistiques de cette façon.
Si vous double-cliquez sur une tâche de ce type, vous afficherez sa page de propriétés.

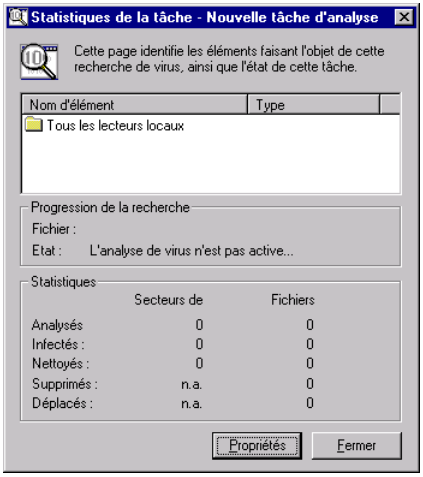



**Figure 3-2. Fenêtre Statistiques des tâches**

### Barre d'état

La barre d'état affiche successivement des informations sur les éléments que le curseur désigne tour à tour dans la fenêtre de la console VirusScan.

### Affichage des derniers résultats

La zone d'affichage des derniers résultats récapitule les derniers résultats d'une tâche donnée.

## Utilisation de la console antivirus

La console antivirus comprend une série de commandes permettant de créer, supprimer, configurer, exécuter, arrêter, importer, exporter et copier des tâches d'analyse selon vos exigences de sécurité.

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 . La plupart de ces mêmes commandes figurent également dans les menus placés dans le haut de cette fenêtre, ainsi que dans les menus contextuels qui apparaissent à l'écran lorsque vous cliquez avec le bouton droit de la souris sur une tâche de la liste.

Le Table 3-1 répertorie les boutons de la barre d'outils dans l'ordre où ils apparaissent sur la console antivirus. Il présente également la commande équivalente pour chaque bouton et décrit sa fonction. Le Table 3-2 à la page 70 fournit les mêmes informations, présentées selon l'ordre d'apparition des commandes dans les menus de la console.

**Table 3-1. Présentation des commandes de la console antivirus (par bouton de la barre d'outils)**

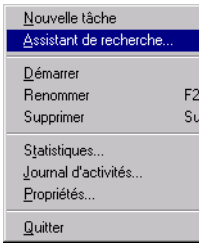
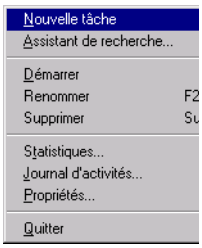
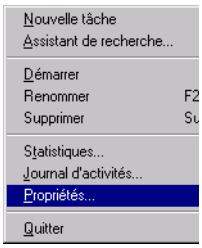
| Barre d'outils Bouton | Commande de menu équivalente | Description |
|---|---|---|
|  |  | Cliquez sur ce bouton dans la barre d'outils de la console, ou sélectionnez Assistant d'analyse dans le menu Analyser, pour lancer l'assistant d'analyse qui offre une méthode simple pour planifier ou configurer des tâches d'analyse à la demande. Lorsque le premier écran de l'assistant d'analyse s'affiche, suivez les instructions qui vous sont données.Voir "Création d'une tâche avec l'assistant d'analyse" à la page 81 |
|  |  | Pour créer une tâche, cliquez sur ce bouton dans la barre d'outils de la console ou sélectionnez Nouvelle tâche dans le menu **Analyser**. Une boîte de dialogue Propriétés des tâches s'affiche. Pour apprendre comment configurer une nouvelle tâche, reportez-vous au chapitre 6, "Planification et exécution des opérations d'analyse à la demande,". |
|  |  | Pour afficher la boîte de dialogue Propriétés des tâches, sélectionnez la tâche désirée dans la fenêtre de la console, puis cliquez sur ce bouton ou sélectionnez **Propriétés** dans le menu **Analyser**. Pour apprendre comment modifier la configuration d'une tâche, reportez-vous au chapitre 6, "Planification et exécution des opérations d'analyse à la demande," |

**Table 3-1. Présentation des commandes de la console antivirus (par bouton de la barre d'outils) (suite)**

| Barre d'outils Bouton | Commande de menu équivalente | Description |
|---|---|---|
|  |  | Pour copier une tâche dans le Presse-papiers de Windows, sélectionnez la tâche en question dans la fenêtre de la console, puis cliquez sur ce bouton ou sélectionnez **Copier** dans le menu **Analyser**. Cette fonction permet par exemple de copier les paramètres d'une tâche si vous souhaitez utiliser une analyse à la demande comme modèle pour créer d'autres tâches similaires. |
|  |  | Pour coller une tâche depuis le Presse-papiers de Windows vers la liste des tâches de la fenêtre de la console, cliquez sur ce bouton ou sélectionnez **Coller** dans le menu **Analyser**.<br><br>Lorsque vous collez la tâche dans la fenêtre de la console, VirusScan vous demande de la renommer. Tapez un nom puis appuyez sur **ENTREE**. La boîte de dialogue Propriétés des tâches s'affiche, et vous pouvez y modifier la tâche avant de l'enregistrer. Pour apprendre comment modifier les paramètres d'une tâche, reportez-vous à la section "Création d'une tâche à la demande dans la console antivirus" à la page 115. Une fois les paramètres de la tâche modifiés selon vos besoins, cliquez sur **OK** pour fermer la boîte de dialogue Propriétés des tâches. |

**Table 3-1. Présentation des commandes de la console antivirus (par bouton de la barre d'outils) (suite)**

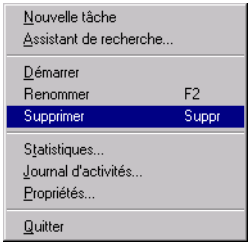
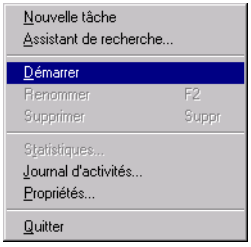
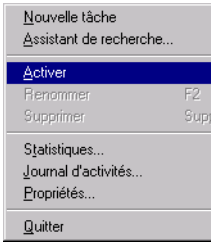
| Barre d'outils Bouton | Commande de menu équivalente | Description |
|---|---|---|
|  |  | Pour supprimer une tâche de la liste des tâches, sélectionnez la tâche en question dans la fenêtre de la console, puis cliquez sur ce bouton ou sélectionnez **Supprimer** dans le menu **Analyser**. VirusScan vous demande de confirmer la suppression de la tâche sélectionnée. Cliquez sur **Oui** pour la supprimer ou sur **Non** pour la conserver.<br><br>Seules les tâches que vous avez créées peuvent être supprimées. Il est impossible de supprimer les tâches prédéfinies liées au dispositif de surveillance lors de l'accès, à la mise à jour automatique des fichiers DAT ou à la mise à niveau automatique des logiciels. Vous pouvez cependant *désactiver* toute tâche que vous ne souhaitez pas exécuter. |
|  |  | Pour exécuter une tâche, sélectionnez la tâche en question dans la fenêtre de la console, puis cliquez sur ce bouton ou sélectionnez **Démarrer** dans le menu **Analyser**. La tâche s'exécute immédiatement avec les options que vous avez choisies.<br><br>  <br>Pour démarrer le scanner lors de l'accès, sélectionnez le dispositif de surveillance des tâches lors de l'accès dans la liste puis choisissez **Activer** dans le menu Analyser. Notez que la commande Démarrer du menu Analyser a été remplacée par la commande **Activer**. |

**Table 3-1. Présentation des commandes de la console antivirus (par bouton de la barre d'outils) (suite)**

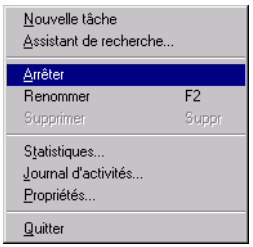
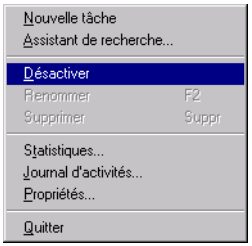
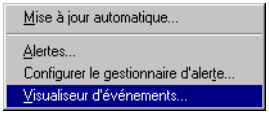
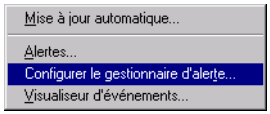
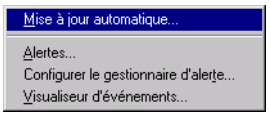
| Barre d'outils Bouton | Commande de menu équivalente | Description |
|---|---|---|
|  |  | Pour arrêter une tâche en cours, sélectionnez la tâche en question dans la fenêtre de la console, puis cliquez sur ce bouton ou sélectionnez **Arrêter** dans le menu **Analyser**.<br><br>Pour arrêter le scanner lors de l'accès, sélectionnez le dispositif de surveillance des tâches lors de l'accès dans la liste puis choisissez Désactiver dans le menu Analyser.<br>  <br>Notez que la commande Arrêter du menu Analyser a été remplacée par la commande Désactiver. |
|  |  | Pour vous connecter à la bibliothèque d'informations sur les virus, cliquez sur ce bouton ou sélectionnez **Bibliothèque d'informations sur les virus en ligne** dans le menu **Aide**. VirusScan démarre votre navigateur Web par défaut et se connecte au site web de Network Associates pour afficher la bibliothèque. |
|  |  | Pour afficher la visionneuse d'événements Windows NT, cliquez sur ce bouton ou sélectionnez **Visionneuse d'événements** dans le menu **Outils**. La visionneuse d'événements permet de contrôler l'état de la station de travail et notamment celui des services Windows NT de VirusScan.<br><br>Pour afficher la même boîte de dialogue, vous pouvez également cliquer sur le bouton **Démarrer**, pointer le curseur sur **Programmes**, sur **Outils de gestion (communs)** et choisir enfin **Visionneuse d'événements**. |

**Table 3-1. Présentation des commandes de la console antivirus (par bouton de la barre d'outils) (suite)**

| Barre d'outils Bouton | Commande de menu équivalente | Description |
|---|---|---|
|  |  | Pour afficher la boîte de dialogue Propriétés du gestionnaire d'alertes, cliquez sur ce bouton ou sélectionnez **Configurer le gestionnaire d'alertes** dans le menu **Outils**.Pour savoir comment définir une alerte en cas d'infection virale, reportez-vous au chapitre 7, "Transmission des messages d'alerte,". |
|  |  | Cliquez sur ce bouton ou sélectionnez **Mise à jour automatique** dans le menu **Outils** pour afficher la boîte de dialogue Propriétés de la mise à jour / mise à niveau automatique. Pour savoir comment configurer la mise à jour automatique des fichiers DAT ou la mise à niveau automatique des logiciels, reportez-vous au chapitre 8, "Mise à jour et Mise à niveau de VirusScan,". |

Le Table 3-2 répertorie les options de menu dans l'ordre où elles apparaissent dans la console antivirus. Il présente également les boutons de barre d'outils équivalents pour chaque option - s'il y en a - et décrit leur fonction. Le Table 3-1 à la page 65 fournit les mêmes informations, présentées selon l'ordre d'apparition des boutons dans la barre d'outils de la console.

**Table 3-2. Présentation des commandes de la console antivirus (par option)**

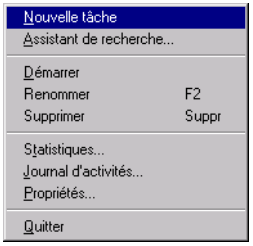
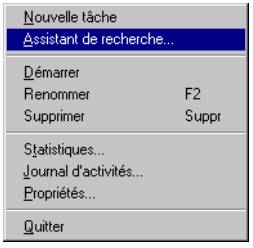
| Menu | Bouton de barre d'outils équivalent | Description |
|---|---|---|
|  |  | Pour créer une tâche, sélectionnez **Nouvelle tâche** dans le menu **Analyser**, ou cliquez sur ce bouton dans la barre d'outils de la console. Une boîte de dialogue Propriétés des tâches s'affiche. Reportez-vous au chapitre 6, "Planification et exécution des opérations d'analyse à la demande," pour apprendre comment configurer une nouvelle tâche. |
|  |  | Sélectionnez **Assistant d'analyse** dans le menu **Analyser** ou cliquez sur ce bouton dans la barre d'outils de la console pour démarrer l'assistant d'analyse qui offre une méthode simple pour planifier ou configurer des tâches d'analyse à la demande. Lorsque le premier écran de l'assistant d'analyse s'affiche, suivez les instructions qui vous sont données. pour de plus amples informations |

**Table 3-2. Présentation des commandes de la console antivirus (par option) (suite)**

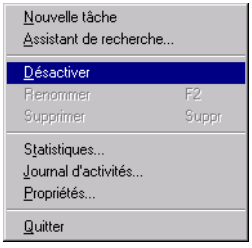
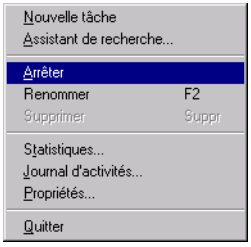
| Menu | Bouton de barre d'outils équivalent | Description |
|---|---|---|
|  |  | Pour arrêter le scanner lors de l'accès, sélectionnez le dispositif de surveillance des tâches lors de l'accès dans la liste puis choisissez **Désactiver** dans le menu **Analyser** ou cliquez sur le bouton de barre d'outils représenté.<br><br>  <br>Pour arrêter une tâche à la demande en cours, sélectionnez la tâche en question dans la fenêtre de la console, puis sélectionnez **Arrêter** dans le menu **Analyser**, ou cliquez sur ce bouton de barre d'outils. Notez que la commande **Désactiver** du menu **Analyser** est remplacée par la commande **Arrêter** lorsque vous sélectionnez une tâche à la demande active.. |

**Table 3-2. Présentation des commandes de la console antivirus (par option) (suite)**

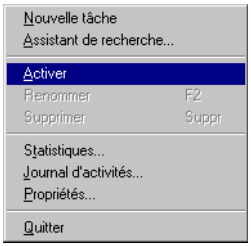
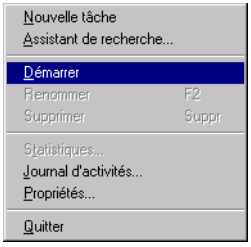
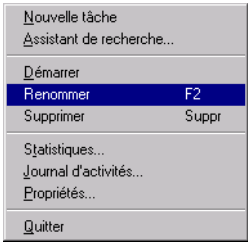
| Menu | Bouton de barre d'outils équivalent | Description |
|---|---|---|
|  |  | Pour démarrer le scanner lors de l'accès, sélectionnez le dispositif d'analyse des tâches lors de l'accès dans la liste puis choisissez Activer dans le menu Analyser ou cliquez sur le bouton de barre d'outils représenté. La tâche s'exécute avec les options que vous avez choisies.<br><br>  <br>Pour démarrer une tâche à la demande avec les options que vous avez définies, sélectionnez la tâche en question dans la fenêtre de la console, puis sélectionnez **Démarrer** dans le menu **Analyser**, ou cliquez sur ce bouton de barre d'outils. Notez que la commande **Activer** du menu **Analyser** est remplacée par la commande **Démarrer** lorsque vous sélectionnez une tâche à la demande.. |
|  | Aucune | Pour renommer une tâche dans la fenêtre de la console, sélectionnez une tâche à la demande que vous avez créée puis sélectionnez **Renommer** dans le menu **Analyser**. Tapez ensuite le nouveau nom de la tâche puis appuyez sur ENTREE.<br><br>Il est impossible de renommer les tâches liées au dispositif de surveillance lors de l'accès, à la mise à jour automatique des fichiers DAT ou à la mise à niveau automatique des logiciels. |

**Table 3-2. Présentation des commandes de la console antivirus (par option) (suite)**

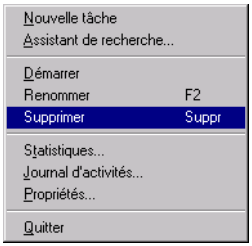
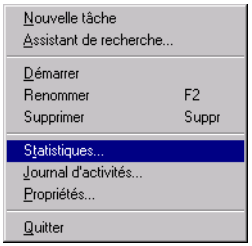
| Menu | Bouton de barre d'outils équivalent | Description |
|---|---|---|
|  |  | Pour supprimer une tâche de la liste des tâches, sélectionnez la tâche en question dans la fenêtre de la console, puis choisissez **Supprimer** dans le menu **Analyser**, ou cliquez sur ce bouton. VirusScan vous demande de confirmer la suppression de la tâche sélectionnée. Cliquez sur **Oui** pour la supprimer ou sur **Non** pour la conserver.<br><br>Seules les tâches que vous avez créées peuvent être supprimées. Il est impossible de supprimer les tâches prédéfinies liées au dispositif de surveillance lors de l'accès, à la mise à jour automatique des fichiers DAT ou à la mise à niveau automatique des logiciels. Vous pouvez cependant *désactiver* toute tâche que vous ne souhaitez pas exécuter. |
|  | Aucune | Pour afficher l'état et les résultats de la dernière analyse, sélectionnez la tâche correspondante dans la fenêtre de la console puis choisissez **Statistiques** dans le menu **Analyser**, ou double-cliquez sur la tâche. Si vous sélectionnez une tâche en cours, VirusScan actualise son état et ses résultats dynamiquement à mesure que l'analyse progresse.<br><br>Notez que cette méthode ne permet pas d'afficher de statistiques pour les tâches de mise à jour automatique des fichiers DAT ou de mise à niveau automatique des logiciels. |

**Table 3-2. Présentation des commandes de la console antivirus (par option) (suite)**

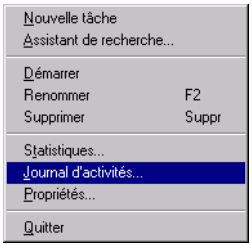
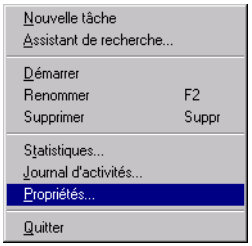
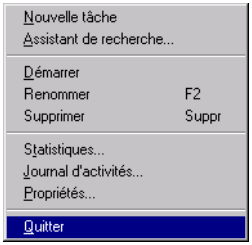
| Menu | Bouton de barre d'outils équivalent | Description |
|---|---|---|
|  | Aucune | Pour ouvrir le fichier journal dans lequel VirusScan enregistre les actions entreprises pendant les analyses, choisissez **Journal d'activité** dans le menu **Analyser**. Pour en savoir plus sur la création des fichiers journaux, consultez la section "Sélection des options de rapport" à la page 123. |
|  |  | Pour afficher la boîte de dialogue Propriétés des tâches, sélectionnez la tâche désirée dans la fenêtre de la console, puis choisissez **Propriétés** dans le menu **Analyser**, ou cliquez sur ce bouton. Pour apprendre comment modifier la configuration d'une tâche, reportez-vous au chapitre 6, "Planification et exécution des opérations d'analyse à la demande," |
|  | Aucune | Pour fermer la console antivirus, choisissez **Quitter** dans le menu **Analyser**. Notez que fermer la console antivirus n'interrompt pas les tâches d'analyse à la demande ou lors de l'accès en cours. Il n'est pas non plus nécessaire de garder ouverte la fenêtre de la console pour exécuter les opérations d'analyse planifiées. |
|  |  | Pour copier une tâche dans le Presse-papiers de Windows, sélectionnez la tâche en question dans la fenêtre de la console, puis choisissez **Copier** dans le menu **Edition**, ou cliquez sur ce bouton. Cette fonction permet par exemple de copier les paramètres d'une tâche si vous souhaitez utiliser une analyse à la demande comme modèle pour créer d'autres tâches similaires. |

**Table 3-2. Présentation des commandes de la console antivirus (par option) (suite)**

| Menu | Bouton de barre d'outils équivalent | Description |
|---|---|---|
|  |  | Sélectionnez **Coller** dans le menu **Edition**,ou cliquez sur ce bouton pour coller une tâche copiée dans le Presse-papiers de Windows dans la liste des tâches de la fenêtre de la console.<br><br>Lorsque vous collez la tâche dans la fenêtre de la console, VirusScan vous demande de la renommer. Tapez un nom puis appuyez sur **ENTREE**. La boîte de dialogue Propriétés des tâches s'affiche et vous pouvez y modifier la tâche avant de l'enregistrer. Pour apprendre comment modifier les paramètres d'une tâche, reportez-vous à la section "Création d'une tâche à la demande dans la console antivirus" à la page 115 Une fois les paramètres de la tâche modifiés selon vos besoins, cliquez sur **OK** pour fermer la boîte de dialogue Propriétés des tâches. |
|  | Aucune | Sélectionnez dans la fenêtre de la console une des tâches que vous avez créées, puis choisissez **Exporter** dans le menu **Edition**. Dans la boîte de dialogue Sélection des fichiers à exporter qui s'affiche, nommez le fichier, choisissez un emplacement pour l'enregistrer puis cliquez sur **Enregistrer**. VirusScan enregistre la tâche dans un fichier .VSC qui conserve toutes les options de tâche définies. Vous pouvez copier ce fichier sur une autre station de travail, l'envoyer par e-mail ou le distribuer afin qu'il soit utilisé sur d'autres installations de VirusScan. |

**Table 3-2. Présentation des commandes de la console antivirus (par option) (suite)**

| Menu | Bouton de barre d'outils équivalent | Description |
|---|---|---|
|  | Aucune | Sélectionnez **Importer** dans le menu **Edition**, puis recherchez un fichier doté de l'extension .VSC dans la boîte de dialogue Sélection des fichiers à importer qui s'affiche. Cliquez ensuite sur **OK** pour le faire apparaître dans la fenêtre de la console. VirusScan vous demande de nommer la tâche. Tapez un nom puis appuyez sur ENTREE.<br>La boîte de dialogue Propriétés des tâches s'affiche, et vous pouvez y modifier la tâche avant de l'enregistrer. Pour apprendre comment modifier les paramètres d'une tâche, reportez-vous à la section chapitre 6, "Planification et exécution des opérations d'analyse à la demande," Une fois les paramètres de la tâche modifiés, cliquez sur **OK** pour fermer la boîte de dialogue Propriétés des tâches. |
|  | Aucune | Pour afficher ou masquer les boutons de la barre d'outils de la fenêtre de la console, sélectionnez **Barre d'outils** dans le menu **Afficher**. La présence d'une coche en regard de l'élément indique que la barre d'outils est active. Aucune coche n'apparaît si la barre d'outils est masquée. |
|  | Aucune | Pour afficher ou masquer la barre d'état dans la partie inférieure de la fenêtre de la console, sélectionnez **Barre d'état** dans le menu **Afficher**. La présence d'une coche en regard de l'élément indique que la barre d'état est active. Aucune coche n'apparaît si la barre d'état est masquée. |

**Table 3-2. Présentation des commandes de la console antivirus (par option) (suite)**

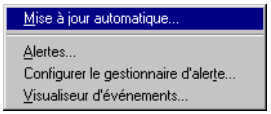
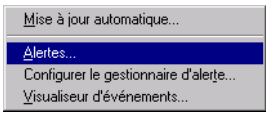
| Menu | Bouton de barre d'outils équivalent | Description |
|---|---|---|
|  | Aucune | Pour actualiser instantanément la liste des tâches, sélectionnez **Rafraîchir** dans le menu **Afficher**. |
|  | Aucune | Pour spécifier la fréquence de régénération automatique de la liste des tâches, sélectionnez **Options** dans le menu **Afficher**. Une boîte de dialogue prévue à cet effet apparaît. Par défaut, la fenêtre de la console se régénère toutes les 3 secondes. Entrez un intervalle dans la zone de texte **Fréquence de rafraîchissement** ou cliquez sur les flèches en regard de la zone de texte pour modifier la valeur affichée. Cliquez sur **OK** pour enregistrer vos paramètres et refermer la boîte de dialogue Options. |
|  |  | Sélectionnez **Mise à jour automatique** dans le menu **Outils**, ou cliquez sur ce bouton, pour afficher la boîte de dialogue Propriétés de la mise à jour / mise à niveau automatique. Pour savoir comment configurer la mise à jour automatique des fichiers DAT ou la mise à niveau automatique des logiciels, reportez-vous au chapitre 8, "Mise à jour et Mise à niveau de VirusScan,". |
|  | Aucune | Sélectionnez **Alertes** dans le menu **Outils** pour ouvrir la boîte de dialogue Propriétés d'alerte. Cette boîte de dialogue permet d'activer le gestionnaire d'alertes et de modifier le niveau de priorité et le contenu des messages d'alerte envoyés par VirusScan. Pour apprendre comment configurer et envoyer des messages d'alerte, reportez-vous au chapitre 7, "Transmission des messages d'alerte,". |

**Table 3-2. Présentation des commandes de la console antivirus (par option) (suite)**

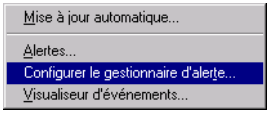
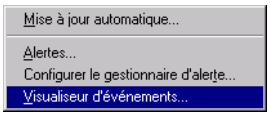
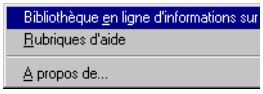
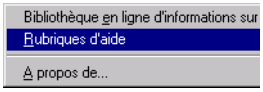
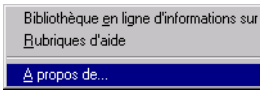
| Menu | Bouton de barre d'outils équivalent | Description |
|---|---|---|
|  |  | Pour afficher la boîte de dialogue Propriétés du gestionnaire d'alertes, sélectionnez **Configurer le gestionnaire d'alertes** dans le menu **Outils**, ou cliquez sur ce bouton. Pour savoir comment définir une alerte en cas d'infection, reportez-vous au chapitre 7, "Transmission des messages d'alerte,". |
|  |  | Pour afficher la visionneuse d'événements Windows NT, sélectionnez **Visionneuse d'événements** dans le menu **Outils**, ou cliquez sur ce bouton. La visionneuse d'événements permet de contrôler l'état du poste de travail et notamment celui des services Windows NT de VirusScan.<br>Pour afficher la même boîte de dialogue, vous pouvez également cliquer sur le bouton **Démarrer**, pointer le curseur sur **Programmes**, sur **Outils de gestion (communs)**, et choisir enfin **Visionneuse d'événements**. |
|  |  | Pour vous connecter à la bibliothèque d'informations sur les virus, sélectionnez **Bibliothèque d'informations sur les virus en ligne** dans le menu **Aide**, ou cliquez sur ce bouton.VirusScan démarre votre navigateur Web par défaut et se connecte au site web de Network Associates pour afficher la bibliothèque. |

**Table 3-2. Présentation des commandes de la console antivirus (par option) (suite)**

| Menu | Bouton de barre d'outils équivalent | Description |
|---|---|---|
|  | Aucune | Pour afficher le fichier d'aide en ligne de VirusScan, choisissez **Rubriques d'aide** dans le menu **Aide**. |
|  | Aucune | Pour afficher les informations relatives au copyright, les numéros de série, les numéros de version des fichiers de définition des virus ainsi que d'autres informations sur votre copie de VirusScan, sélectionnez **A propos de** dans le menu **Aide**. |

# Utilisation de l'icône VirusScan de la barre des tâches

Le scanner lors de l'accès de VirusScan s'installe et s'active lui-même par défaut lorsque vous procédez à une installation par défaut. Une fois lancé, le scanner affiche une icône en forme de bouclier dans la barre des tâches de Windows NT.

Double-cliquez sur cette icône pour afficher des informations sur l'état et les résultats de la dernière analyse lors de l'accès (Figure 3-3). La boîte de dialogue Statistiques affiche le nombre total de fichiers analysés, le nombre de fichiers infectés détectés et le nombre d'actions entreprises par le scanner.

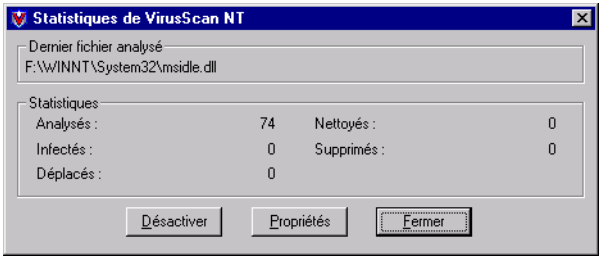



**Figure 3-3. Boîte de dialogue Statistiques de VirusScan NT**

Pour arrêter le service McShield, qui gère les analyses lors de l'accès de VirusScan, cliquez sur **Désactiver** dans cette boîte de dialogue. L'icône de la barre des tâches et l'icône en regard du dispositif de surveillance lors de l'accès de VirusScan dans la fenêtre de la console sont remplacées par , ce qui indique que le service n'est plus actif. Pour réactiver le service, cliquez sur **Activer** dans la boîte de dialogue Statistiques.

Pour ouvrir la boîte de dialogue Propriétés de VirusScan et configurer le scanner lors de l'accès, cliquez sur **Propriétés**. Cliquez sur **Fermer** pour fermer la boîte de dialogue.

L'icône VirusScan de la barre des tâches cache également un menu contextuel qui donne accès aux mêmes fonctions et à quelques autres. Pour afficher ce menu contextuel, cliquez sur l'icône avec le bouton droit de la souris puis sélectionnez la commande de votre choix. Sélectionnez au choix :

- **Statistiques.** Ouvre la boîte de dialogue Statistiques (Figure 3-3).
- **Désactiver.** Désactive le scanner lors de l'accès. Pour réactiver le scanner, sélectionnez **Activer** dans ce même menu.
- **Propriétés.** Ouvre la boîte de dialogue Propriétés de VirusScan.
- **Console.** Affiche la fenêtre de la console antivirus.

- **Alertes.** Ouvre la boîte de dialogue Propriétés du gestionnaire d'alertes.
- **A propos de.** Affiche les informations relatives au copyright, les numéros de série, les numéros de version des fichiers de définition des virus ainsi que d'autres informations sur votre copie de VirusScan.

# Création d'une tâche avec l'assistant d'analyse

VirusScan inclut un service Windows NT prédéfini qui lui permet de rechercher les virus dès son installation. Pour bénéficier d'une protection antivirus plus que minimale, vous devez configurer VirusScan selon vos besoins en définissant la tâche lors de l'accès et en créant une série de tâches à la demande ou planifiées afin de détecter au mieux les virus susceptibles d'infecter votre station de travail. L'assistant d'analyse de VirusScan peut vous aider à créer directement une première série de tâches à la demande. Par la suite, à mesure que vous connaîtrez mieux VirusScan et le degré de vulnérabilité de votre système, vous pourrez modifier ces tâches pour qu'elles fonctionnent au mieux dans votre environnement.

**Pour créer une tâche à l'aide de l'assistant d'analyse, procédez comme suit :**

1. Démarrez la console antivirus. Voir "Démarrage de la console antivirus de VirusScan" à la page 61 pour plus de détails.
2. Choisissez **Assistant d'analyse** dans le menu **Analyser**, ou cliquez sur  dans la barre d'outils de la console.

   Le premier écran de l'assistant d'analyse apparaît (Figure 3-4).


**Figure 3-4. Écran d'accueil de l'assistant d'analyse**

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

   L'assistant d'analyse affiche un écran qui permet de désigner les volumes dans lesquels VirusScan doit rechercher des virus (voir la Figure 3-5). Par défaut, VirusScan examine tous les volumes des disques durs du poste de travail et tous les sous-répertoires qu'ils contiennent. Une opération d'analyse aussi complète pouvant durer très longtemps, il se peut que vous souhaitiez limiter sa portée pour une utilisation régulière.


**Figure 3-5. Écran Sélection des cibles d'analyse**

4. Choisissez les cibles à analyser. Vous pouvez :

   - **Ajouter des cibles d'analyse à celles définies.** Pour cela, cliquez sur **Ajouter** afin d'ouvrir la boîte de dialogue Ajout d'un élément à analyser (Figure 3-6).

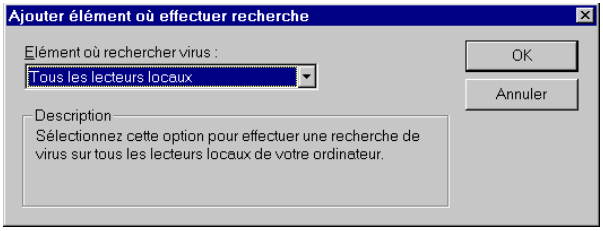



**Figure 3-6. Boîte de dialogue Ajout d'un élément à analyser**

Sélectionnez ensuite une cible à analyser dans la liste qui vous est proposée. Vous pouvez choisir d'analyser tous les lecteurs locaux, des lecteurs ou des dossiers spécifiques, ou encore des fichiers particuliers. Pour analyser un lecteur, un dossier ou un fichier, entrez le chemin de l'objet cible dans la zone de texte **Description**. Vous pouvez indiquer le chemin en respectant la notation de la convention d'affectation des noms (UNC) ou cliquer sur **Parcourir** pour localiser le fichier, le dossier ou le lecteur de votre choix. Lorsque vous avez terminé, cliquez sur **OK** pour refermer la boîte de dialogue.

- **Supprimer les cibles à analyser existantes.** Pour cela, sélectionnez une des cibles de la liste puis cliquez sur **Supprimer**.
- **Modifier ou limiter les cibles à analyser existantes.** Pour cela, sélectionnez l'une des cibles de la liste puis cliquez sur **Modifier** afin d'ouvrir la boîte de dialogue Modifier l'élément à analyser (Figure 3-7).

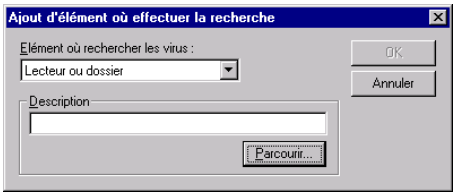



**Figure 3-7. Boîte de dialogue Modifier l'élément à analyser**

Choisissez ou entrez une nouvelle cible puis cliquez sur **OK** pour fermer la boîte de dialogue.

5. Une fois les cibles d'analyse définies, cliquez sur **Suivant>** pour continuer.

   L'assistant d'analyse affiche un écran qui permet de spécifier la manière dont VirusScan doit effectuer l'opération d'analyse (Figure 3-8).


**Figure 3-8. Écran Sélection des options d'analyse**

6. Choisissez les options d'analyse. Vous pouvez :

   - **Analyser les sous-dossiers du volume.** Par défaut, VirusScan analyse tous les sous-dossiers des volumes retenus pour l'analyse. Pour n'analyser que la racine des volumes choisis, désélectionnez la case **Inclure les sous-dossiers**.

   - **Analyser les fichiers compressés.** Par défaut, le scanner à la demande de VirusScan analyse les fichiers compressés dans les formats suivants : .??_, .CAB, LZEXE, LZH, PKLite, .TD0 et .ZIP. Pour empêcher VirusScan d'analyser ces fichiers, désélectionnez la case **Analyser les fichiers compressés**.

   - **Ne pas analyser le secteur d'amorçage.** Généralement, VirusScan analyse le secteur de partition et les blocs d'amorçage du disque dur à la recherche de virus dans le secteur d'amorçage. Bien que la majorité des nouveaux virus soit des virus de macro, les virus de secteur d'amorçage continuent à proliférer et peuvent endommager les systèmes. Network Associates recommande d'analyser régulièrement le secteur d'amorçage de votre ordinateur mais, si cette procédure gêne les opérations normales du système, vous pouvez cocher cette case pour désactiver ce type d'opération d'analyse.

- **Sélectionner les types de fichier à analyser.** D'ordinaire, les virus ne peuvent infecter les fichiers de données ou les fichiers qui ne contiennent pas de code exécutable. Vous pouvez donc sans risque limiter les opérations d'analyse aux fichiers les plus susceptibles d'être infectés par les virus pour les accélérer. Pour cela, cliquez sur le bouton **Fichiers programme uniquement**. Pour visualiser ou sélectionner les extensions des noms de fichier correspondantes, cliquez sur **Types de fichiers** pour afficher la boîte de dialogue Extensions des fichiers programme (Figure 3-9).


**Figure 3-9. Boîte de dialogue Extensions des fichiers programme**

Par défaut, VirusScan recherche les virus dans les fichiers portant les extensions .EXE, .COM, .DOC, .DOT, .XL?, .MD?, .VXD, .386, .SYS, .BIN, .RTF, .OBD, .DLL, .SCR, .OBT, .PP?, .POT, .OLE, .SHS, .MPP, .MPT, .XTP, .XLB, .CMD, .OVL et .DEV. Cette liste comprend presque tous les fichiers susceptibles d'être infectés par des virus de macro, y compris tous les types de fichiers de Microsoft Office. Le caractère générique ? permet à VirusScan d'analyser des fichiers du même type, tels que les fichiers documents et modèles.

  – Pour ajouter des types de fichier à la liste, cliquez sur **Ajouter**, puis entrez les extensions que VirusScan doit prendre en compte dans la boîte de dialogue qui s'affiche alors.

  – Pour supprimer une extension de la liste, sélectionnez-la, puis cliquez sur : **Supprimer**.

  – Cliquez sur **Par défaut** pour revenir à la liste originale.

Lorsque vous avez terminé, cliquez sur **OK** pour refermer la boîte de dialogue.

Pour demander à VirusScan d'analyser tous les volumes, dossiers et fichiers de votre poste de travail sélectionnez l'option **Analyser tous les fichiers**. Ceci ralentit notablement les opérations d'analyse mais garantit une protection totale pour le système.

7. Une fois les options d'analyse sélectionnées, cliquez sur **Suivant>** pour continuer. L'assistant d'analyse affiche un écran qui permet de sélectionner les options d'alertes et d'enregistrement (Figure 3-10).


**Figure 3-10. Écran Sélection des options d'alertes et d'enregistrement**

8. Cet écran permet d'activer les options d'alertes de votre choix et de définir l'emplacement du fichier journal qui consignera les actions réalisées par VirusScan. Vous pouvez :

   - **Envoyer des alertes par le biais du gestionnaire d'alertes.** Pour que le gestionnaire d'alertes de VirusScan envoie un message d'alerte en cas de détection d'un virus, sélectionnez la case **Avertir le gestionnaire d'alertes**. Le gestionnaire d'alertes enverra un message par le biais des canaux que vous aurez définis à cette fin. Pour apprendre comment configurer le gestionnaire d'alertes, reportez-vous à la section "Configuration du gestionnaire d'alertes" à la page 145

   - **Consigner les activités d'analyse dans un fichier journal.** Pour que VirusScan consigne les analyses dans un fichier texte que vous pourrez ouvrir et consulter, sélectionnez la case **Consigner dans un fichier**, puis entrez le nom du fichier texte dans lequel VirusScan enregistrera les actions réalisées. Par défaut, VirusScan consigne ses actions dans un fichier nommé SCAN ACTIVITY LOG.TXT. Si vous souhaitez utiliser un autre fichier texte, entrez son nom et son chemin d'accès dans la zone de texte prévue à cet effet ou cliquez sur **Parcourir** pour rechercher un fichier sur votre disque dur.

     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. VirusScan videra le contenu du fichier journal et y enregistrera les nouvelles données une fois la limite de capacité définie atteinte.

9. Une fois les options d'alertes et d'enregistrement définies, cliquez sur **Suivant>** pour continuer.

   L'assistant d'analyse affiche un écran qui permet de spécifier les actions que doit entreprendre VirusScan en cas de détection d'un virus (Figure 3-11).


**Figure 3-11. Écran Sélection des actions**

10. Choisissez l'une des actions proposées. Ces actions sont les suivantes :

    - **Poursuivre l'analyse.** VirusScan consigne la détection du virus puis continue l'analyse sans entreprendre aucune action. Si vous avez défini les options d'alertes et d'enregistrement, VirusScan vous avertira qu'il a trouvé un virus et consignera l'incident dans le fichier journal.

    - **Placer le fichiers infecté dans un dossier**. VirusScan déplace automatiquement tout fichier infecté dans un dossier de quarantaine. Par défaut, VirusScan enregistre le fichier dans un dossier nommé "Infected" à l'intérieur de son répertoire programme. Pour choisir un autre emplacement, entrez le chemin dans la zone de texte prévue à cet effet, ou bien cliquez sur **Parcourir** pour rechercher un dossier approprié.

    - **Nettoyer les fichiers infectés.** VirusScan tente de supprimer le virus des fichiers infectés et de restaurer celui-ci dans son état initial, avant infection. Les fichiers de données fournis avec VirusScan permettent de supprimer la plupart des types de virus. Cependant, il arrive qu'un virus ne puisse pas être supprimé. Dans ce cas, VirusScan signale l'incident par un message d'alerte approprié et le consigne dans le fichier journal, si vous avez sélectionné cette option, puis l'analyse reprend son cours.

- **Supprimer les fichier infectés.** VirusScan supprime instantanément tout fichier infecté décelé. Vous devrez ensuite restaurer le fichier supprimé à partir d'une copie de sauvegarde s'il vous est nécessaire.

11. Une fois l'action sélectionnée, cliquez sur **Suivant>** pour continuer.

    L'assistant d'analyse affiche le dernier écran qui permet d'exécuter instantanément la tâche que vous venez de créer, ou de l'enregistrer pour l'exécuter ou la planifier à un autre moment (Figure 3-12).


**Figure 3-12. Écran Exécution ou enregistrement de la tâche**

12. Indiquez ce que vous voulez faire de la tâche que vous venez de créer. Vous pouvez :

    - **Exécuter une tâche maintenant sans l'enregistrer.** VirusScan exécute la tâche une fois puis l'abandonne sans l'enregistrer.
    - **Enregistrer une tâche sans l'exécuter.** VirusScan enregistre la tâche en vue d'une exécution ultérieure. Vous pouvez alors choisir de l'exécuter en tant que tâche à la demande en la sélectionnant dans la liste des taches puis en choisissant **Démarrer** dans le menu **Analyser**. Voir Chapitre 6, "Planification et exécution des opérations d'analyse à la demande" pour plus de détails.

      Pour enregistrer la tâche dans la liste des tâches de la console antivirus, entrez son nom dans la zone de texte prévue à cet effet.
    - **Enregistrer et lancer une tâche maintenant.** VirusScan exécute la tâche instantanément et l'enregistre également en vue d'une exécution ultérieure. Pour enregistrer la tâche dans la liste des tâches de la console antivirus, entrez son nom dans la zone de texte prévue à cet effet.

13. Une fois l'option choisie, cliquez sur **Terminer** pour fermer l'écran de l'assistant.

    Si vous avez demandé l'exécution immédiate de la tâche, vous verrez apparaître la boîte de dialogue Nouvelle tâche d'analyse tandis que commencera l'analyse des volumes spécifiés (Figure 3-13). Vous pouvez réduire cette fenêtre pour exécuter l'analyse en arrière-plan.

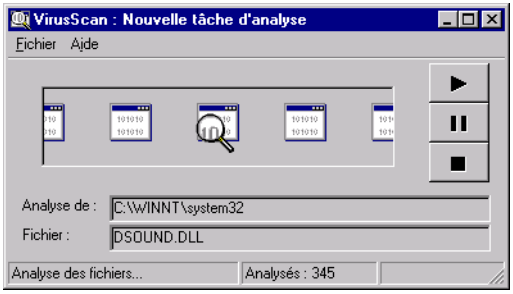



**Figure 3-13. Fenêtre Nouvelle tâche d'analyse**

Pour arrêter la procédure d'analyse, cliquez sur ■. Pour interrompre momentanément la procédure d'analyse, cliquez sur ❚❚. Pour redémarrer l'analyse après son interruption ou son arrêt, cliquez sur ▶.

# Suppression d'une infection dans votre système 4

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

Tout d'abord, ne paniquez pas ! Bien que *la plupart* des virus susceptibles d'infecter votre système ne soient pas inoffensifs, il est peu probable qu'ils détruisent des données, qu'ils vous jouent des tours ou qu'ils rendent votre station de travail inutilisable. Même les virus, relativement rares, programmés pour exécuter 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 fragments de code indésirables pouvant enrayer le fonctionnement normal du poste de travail, consommer des ressources système et réseau 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 situations vous font suspecter la présence d'un virus sur votre ordinateur, l'analyse du système ne produira peut-être pas les résultats escomptés. Cependant, elle vous permettra d'éliminer le virus comme cause possible du problème.

*La solution la plus sûre consiste à installer VirusScan et à exécuter une analyse complète du système.*

Avant de procéder à son installation, VirusScan examine la mémoire système et le secteur d'amorçage du disque dur pour vérifier l'absence de virus et éliminer tout risque d'infection de ses propres fichiers. Si VirusScan détecte un virus pendant son installation, il vous informera de cet incident, le consignera dans le journal des activités et interdira l'accès au fichier infecté. Faites une analyse à la demande dès que possible après l'installation de VirusScan, puis désinfectez, déplacez ou supprimez les fichiers infectés détectés. Voir la section "Options de réponse à un virus ou à un programme malveillant" à la page 93 pour plus de détails.

Vous pouvez également tenter de supprimer vous-même le virus du fichier infecté. Cette méthode n'est pas recommandée dans la mesure où elle induit un risque d'altération du fichier. Cependant, la bibliothèque d'informations sur les virus en ligne, disponible sur le site web de Network Associates, contient des informations facilitant ce type d'opération. Pour consulter ces informations, lancez le navigateur Web de votre choix, puis tapez l'adresse Web suivante :

http://vil.mcafee.com/vil/<numéro du document>.asp

Dans l'adresse indiquée ci-dessus, <numéro du document> fait référence à un document technique de la bibliothèque d'informations sur les virus. Remplacez <numéro du document> par l'un des numéros ci-dessous :

0118 0319 0322 0323 0327 1145

**REMARQUE :** Les numéros des documents peuvent changer. Consultez, au besoin, le sommaire de la bibliothèque d'informations sur les virus.

# Création d'une disquette de secours

Les modules du programme de VirusScan peuvent généralement détecter et supprimer un virus avant que celui-ci ne menace véritablement le système mais, dans certaines circonstances, vous devez initialiser le poste de travail avec une disquette puis conduire une analyse du système afin de supprimer les virus cachés en mémoire ou dissimulés dans les secteurs d'amorçage du disque dur. Si, par exemple, un virus est présent dans le système au moment de l'installation, certains fichiers programme de VirusScan peuvent se trouver infectés.

**Pour créer une disquette de secours, suivez les étapes ci-dessous :**

1. Pour ouvrir la fenêtre de l'invite de commande, cliquez sur **Démarrer**, pointez le curseur sur **Programmes**, puis sur **Invite de commande**.
2. Passez dans le répertoire \EDU, à l'intérieur du répertoire programme de VirusScan. Si vous avez installé VirusScan dans son répertoire par défaut, tapez la ligne suivante à l'invite de commande :

   ```
   cd \program files\network associates\virusscan nt\edu
   ```

3. Insérez une disquette vierge, *formatée* de 1,44 Mo dans le lecteur de disquette.

4. Tapez la ligne suivante à l'invite de commande :

   ```
   naidskim /wa /t144 /f<x>:\progra~1\networ~1\viruss~1
   \edu\edisk.img
   ```

   Prenez soin d'indiquer l'unité sur laquelle VirusScan a été installé à la place de la lettre <x> apparaissant dans cet exemple. Si vous avez installé le programme dans un autre répertoire, tapez son chemin d'accès à la place de celui indiqué ici.

   L'utilitaire de création de disquette d'urgence exécutera un fichier de traitement par lots qui copie les fichiers nécessaires depuis un fichier image vers le lecteur de disquette indiqué. Les options de l'exemple demandent l'écriture du fichier de traitement par lots sur l'unité A:, sur une disquette de 1,44 Mo, les fichiers à copier étant extraits du fichier EDISK.IMG du répertoire \EDU. Pour copier les fichiers sur une autre unité, ou depuis un autre chemin, remplacez les valeurs données en exemple par celles qui conviennent. Pour connaître la syntaxe exacte de l'utilitaire de copie, tapez `naidskim` sur la ligne de commande, sans aucune option.

5. Une fois la disquette de secours créée, étiquetez cette disquette, protégez-la en écriture, puis rangez-la en lieu sûr.

# Options de réponse à un virus ou à un programme malveillant

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 plus d'informations sur les autres actions possibles, reportez-vous au chapitre consacré à chaque composant.

## Options de réponses lorsque le scanner lors de l'accès détecte un virus

Le scanner lors de l'accès de VirusScan effectue 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 ou que vous laissez une disquette dans le lecteur à l'arrêt de la station de travail.

Après son installation, le scanner tente automatiquement de désinfecter les fichiers infectés qu'il détecte au cours de l'analyse. S'il n'y parvient pas, il ajoute au fichier infecté l'extension .VIR et en interdit l'accès. Pour apprendre à configurer le scanner avec d'autres actions, reportez-vous au chapitre 5, "Si vous utilisez Le scanner lors de l'accès,"

En cas de détection d'un virus, le scanner vous avertira également par le biais du gestionnaire d'alertes. Par défaut, le gestionnaire d'alertes n'envoie qu'un message d'alerte réseau Windows NT qui n'apparaît que sur votre poste de travail (Figure 4-1).

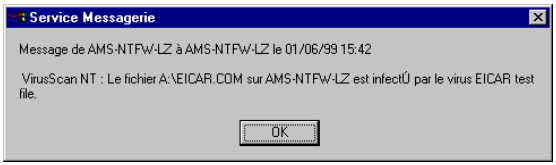



**Figure 4-1. Message d'alerte réseau**

Dans cet exemple, VirusScan a détecté le virus test EICAR, un virus non infectieux et non reproductible constitué d'un fichier texte, destiné à tester les logiciels antivirus. Cliquez sur **OK** pour abandonner le message de réseau.

Sauf si VirusScan ne parvient pas à éliminer le virus, comme dans l'exemple fourni, aucune action supplémentaire n'est nécessaire. VirusScan va également consigner l'incident dans le journal des activités. Vous pourrez y consulter les résultats des analyses à votre gré.

Si VirusScan ne parvient pas à éliminer le virus, vous pouvez supprimer le fichier puis le restaurer à partir d'une sauvegarde saine, l'isoler dans un dossier de quarantaine, ou l'envoyer à Network Associates pour analyse. Pour apprendre comment sélectionner d'autres options de réponse, reportez-vous au Chapitre 5. Pour apprendre comment envoyer des fichiers d'échantillon à Network Associates, reportez-vous à la section "Rapporter les nouveaux virus à incorporer dans les mises à jour des fichiers de données anti-virus" à la page xxiii.

## Options de réponse lorsque VirusScan détecte un virus

Lorsque vous lancez une analyse à la demande immédiatement après l'installation de VirusScan, le programme analyse tous les fichiers présents sur l'unité C: et susceptibles d'être infectés. Cela vous assure un niveau de protection minimal, que vous pouvez étendre et adapter à vos besoins propres en configurant VirusScan de manière plus personnelle.

Par défaut, VirusScan vous demande de choisir une action lorsqu'il découvre un virus (Figure 4-2).

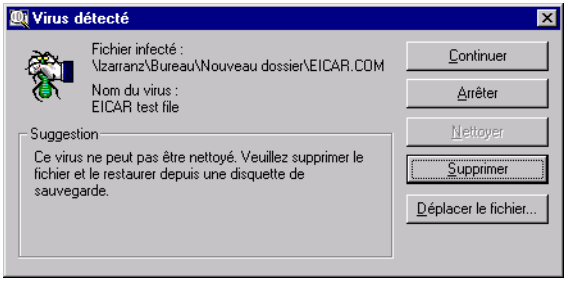



**Figure 4-2. Options de réponse de VirusScan**

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. VirusScan va afficher la liste des fichiers infectés dans la partie inférieure de la fenêtre principale (Figure 4-3) et consigner chaque détection dans son fichier journal. Aucune mesure corrective ne sera entreprise. A l'issue de l'examen du système, vous pouvez cliquer avec le bouton droit de la souris sur chacun des fichiers affichés dans la fenêtre principale et choisir l'action appropriée dans le menu contextuel qui apparaît.

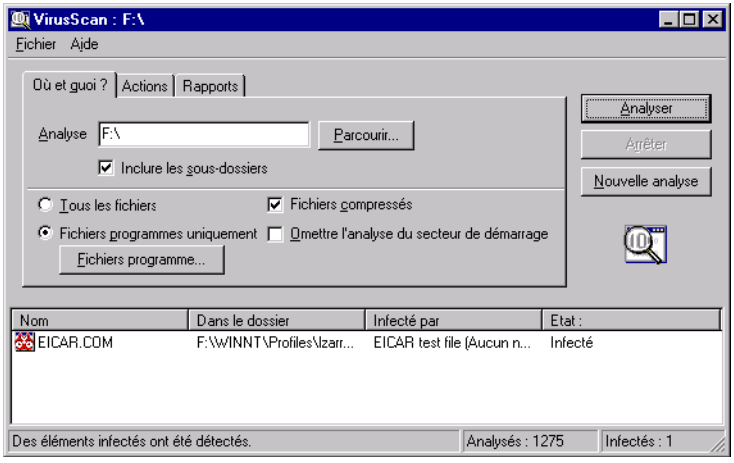



**Figure 4-3. Fenêtre principale de VirusScan**

- **Arrêter.** Cliquez sur ce bouton pour mettre fin immédiatement à l'opération d'analyse. VirusScan affiche la liste des fichiers infectés déjà détectés dans la partie inférieure de la fenêtre principale (voir la Figure 4-3 à la page 95) et consigne chaque détection dans son fichier journal. Il ne prend cependant aucune mesure corrective. Cliquez avec le bouton droit de la souris sur chaque fichier infecté répertorié dans la fenêtre principale puis choisissez une réponse individuelle dans le menu contextuel qui apparaît.
- **Désinfecter.** Cliquez sur ce bouton pour demander à VirusScan d'essayer de supprimer le code du 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 4-2 à la page 95, VirusScan n'a pas réussi à nettoyer le fichier infecté par le virus test EICAR. 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, VirusScan consigne le nom du fichier infecté dans le fichier journal pour vous permettre de le restaurer à partir d'une copie de sauvegarde.
- **Déplacer le fichier vers.** Cliquez sur ce bouton pour ouvrir une boîte de dialogue qui vous permettra 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.

---

**IMPORTANT :** Si vous *planifiez* une analyse à la demande, VirusScan ne vous demandera *pas* de choisir une action. Vous devez choisir une réponse automatique dans ce cas. Voir le chapitre 6, "Planification et exécution des opérations d'analyse à la demande," pour plus de détails.

Par défaut, VirusScan continue l'analyse et en consigne les résultats dans le journal des activités.

---

# 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 différents logiciels de détection de virus sur votre ordinateur. En effet, certains programmes antivirus n'appliquent aucune protection lorsqu'ils stockent les signatures codées utilisées pour la détection en 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 VirusScan a généré une fausse alerte (par exemple, un virus a été détecté dans un fichier que vous utilisez sans problème depuis de nombreuses années), consultez la liste ci-dessous pour connaître l'origine possible de cette fausse alerte avant de contacter Network Associates :

- **Vous utilisez simultanément plusieurs programmes antivirus.** VirusScan risque alors de détecter des signatures non protégées qu'un autre programme utilise 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 tous les codes des autres programmes anti-virus, puis rallumez l'ordinateur.

- **Vous avez une puce BIOS dotée de fonctions antivirus.** Certaines puces BIOS comprennent des fonctions antivirus qui peuvent entraîner de fausses alertes lorsque VirusScan fonctionne. Consultez le manuel d'utilisation de l'ordinateur pour vous familiariser avec cette fonction antivirus, et pour la désactiver, si nécessaire.

- **Votre ordinateur est un PC ancien de marque Hewlett-Packard ou Zenith.** Certains anciens modèles d'ordinateur de ces deux constructeurs modifient les secteurs d'amorçage de leur disque dur chaque fois que le système est réamorcé. VirusScan risque de détecter ces modifications comme une infection probable, même si aucun virus n'est présent sur le système. Consultez le guide d'utilisation 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 de la version ligne de commande de VirusScan. Cette méthode ne permet pas d'enregistrer les informations sur le secteur d'amorçage ou le secteur de partition.

- **Vous utilisez des logiciels protégés contre la copie.** Selon le type de protection anti-copie utilisé, VirusScan risque de détecter un virus dans le secteur d'amorçage ou dans le secteur de partition de certaines disquettes ou d'autres supports.

Si aucune de ces situations ne s'applique à votre cas, contactez le service d'assistance technique de Network Associates ou adressez un courrier électronique détaillant le problème rencontré à l'adresse : virus_research@nai.com.

# Si vous utilisez Le scanner lors de l'accès 5

## L’analyse sans interruption

Grâce à son élément d'analyse lors de l'accès, VirusScan vous propose une détection permanente de virus en temps réel et une action appropriée en cas d'infection sur votre poste de travail. Le scanner lors de l'accès vérifie l'absence d'infection chaque fois que vous ouvrez ou copiez un fichier, enregistrez un fichier ou utilisez n'importe quel fichier stocké sur votre poste de travail. Il se lance lorsque vous démarrez votre poste de travail et reste en mémoire jusqu'à ce que vous l'éteigniez. Vous pouvez utiliser le dispositif de surveillance lors de l’accès de VirusScan qui s'affiche dans la fenêtre de la console antivirus pour configurer ce scanner.

## Configuration du scanner lors de l'accès

Pour que VirusScan puisse garantir les meilleurs résultats sur votre ordinateur ou votre environnement réseau, il faut que vous lui indiquiez ce qu’il doit analyser, ce qu’il doit faire lorsqu’il trouve un virus et comment il doit vous informer de la détection d’un virus.

Par défaut, le scanner lors de l'accès recherche simplement les virus sur votre poste de travail et vous informe lorsqu'il en a trouvé un. Il enregistre également l'incident dans son fichier journal. Vous pouvez doter le scanner lors de l'accès d’options beaucoup plus énergiques qui protégeront automatiquement votre poste de travail.

---

**Pour configurer la tâche lors de l'accès, procédez comme suit :**

1. Lancez la console antivirus Reportez-vous à “Démarrage de la console antivirus de VirusScan” à la page 61 pour apprendre à le faire.
2. Le dispositif de surveillance lors de l'accès de VirusScan s'affiche dans la fenêtre de la console antivirus (Figure 5-1 à la page 100).

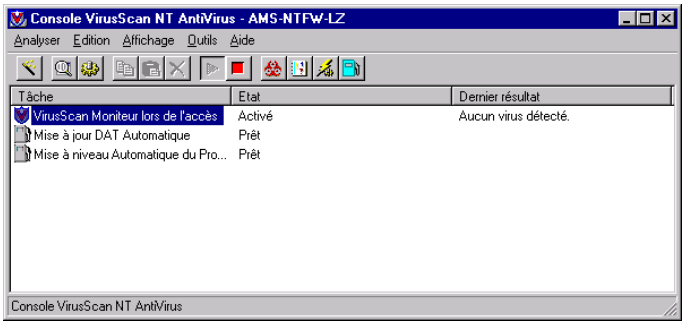



**Figure 5-1. Fenêtre de la console antivirus**

3. Sélectionnez le dispositif d'analyse lors de l'accès dans la fenêtre de la console, puis choisissez **Propriétés** dans le menu **Analyser** ou cliquez sur  dans la barre d'outils de la console.

4. La boîte de dialoguePropriétés de VirusScan s'affiche à l'écran (Figure 5-2).

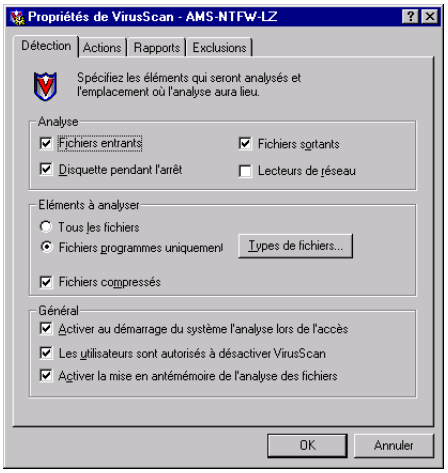



**Figure 5-2. Boîte de dialogue Propriétés deVirusScan - page Détection**

La boîte de dialogue Propriétés de VirusScan comprend quatre pages de propriétés ; chacune d'entre elles est chargée d'un aspect de l'opération d'analyse lors de l'accès. Cliquez sur chaque onglet pour afficher la page de propriétés correspondante et indiquer la façon dont vous souhaitez que VirusScan effectue l'opération. Lorsque vous avez terminé, cliquez sur **OK** pour enregistrer les modifications et refermer la boîte de dialogue. Votre tâche d'analyse commencera à s'exécuter immédiatement avec les options que vous avez sélectionnées.

Les sections suivantes présentent les options disponibles.

## Sélection des options de détection

Utilisez la page Détection (Figure 5-2 à la page 100) pour définir la portée de l'opération d'analyse lors de l'accès - dans quel chemin de fichier VirusScan doit rechercher des virus et quelles sont les extensions qui doivent être considérées comme susceptibles d'être infectées.

**Procédez comme suit :**

1. Dans la zone **Analyser**, sélectionnez quel chemin de fichier VirusScan doit analyser. Vous avez le choix entre les actions suivantes :

   - **Fichiers reçus.** Cochez cette case pour analyser tous les fichiers écrits ou modifiés sur votre poste de travail.
   - **Fichiers envoyés.** Cochez cette case pour analyser les fichiers lus à partir de votre poste de travail.
   - **Analyse de disquette lors de l'arrêt.** Cochez cette case pour analyser toute disquette laissée dans votre lecteur dès que vous éteignez votre poste de travail.
   - **Lecteurs réseau.** Cochez cette case pour analyser le lecteur réseau que vous avez lié à votre poste de travail. Cette option analysera également tout lecteur réseau actuellement ouvert sur votre poste de travail, que vous l'ayez mappé ou sélectionné selon le chemin de la convention d'affectation des noms (UNC).

2. Indiquez quels sont les fichiers de chaque fréquence de débit à analyser par VirusScan. Vous avez le choix entre les actions suivantes :

   - **Tous les fichiers.** Cette option indique à VirusScan qu'il doit analyser tous les fichiers stockés sur votre poste de travail. Elle vous offre la meilleure protection contre les virus mais peut ralentir l'opération d'analyse.

- **Fichiers programme uniquement.** D'ordinaire, les virus ne peuvent infecter les fichiers de données ou les fichiers qui ne contiennent pas de code exécutable. Vous pouvez donc sans risque limiter la portée de vos opérations d'analyse aux fichiers les plus susceptibles d'être infectés par les virus pour les accélérer. Pour ce faire, cliquez sur le bouton **Fichiers programme uniquement**. Pour voir ou sélectionner les extensions des noms de fichiers que VirusScan examinera, cliquez sur **Types de fichiers** pour ouvrir la boîte de dialogue Extensions des fichiers programme.

  La boîte de dialogue Extensions des fichiers programme s'affiche à l'écran (Figure 5-3).


**Figure 5-3. Boîte de dialogue Extensions des fichiers programme**

Par défaut, VirusScan recherche les virus dans les fichiers d'extension .EXE, .COM, .DOC, DOT,.XL?, MD?, .VXD, 386, SYS, BIN, RTF, OBD, DLL., SCR, OBT, PP? .POT, .OLE, .SHS, .MPP, .MPT, .XTP, .XLB, .CMD, .OVL et .DEV. Cette liste couvre presque tous les fichiers susceptibles d'être infectés par des virus, y compris la totalité des types de fichiers de Microsoft Office qui sont susceptibles de l'être par des virus de macros. Le caractère ? est un caractère générique qui permet à VirusScan d'examiner les fichier de même type, tels que les fichiers documents et modèles.

  – Pour ajouter des types de fichiers à la liste, cliquez sur **Ajouter**, puis entrez les extensions que VirusScan doit analyser dans la boîte de dialogue qui s'affiche alors.

  – Pour supprimer une extension de la liste, sélectionnez-la, puis cliquez sur : **Supprimer**.

  – Cliquez sur **Par défaut** pour revenir à la liste originale.

  Lorsque vous avez terminé, cliquez sur **OK** pour refermer la boîte de dialogue.

- **Fichiers compressés.** Cette option demande à VirusScan de rechercher des virus dans les fichiers compressés dans les formats suivants : LZEXE, PKLite, .TD0 et .ZIP. Bien qu'il offre une protection supplémentaire, l'examen des fichiers compressés peut ralentir l'opération d'analyse.

3. Sélectionnez les options générales qui gèrent le fonctionnement du scanner lors de l'accès. Vous avez le choix entre les actions suivantes :

   - **Activer l'analyse lors de l'accès au démarrage du système.** Cochez cette case pour commencer le service lors de l'accès chaque fois que vous démarrez votre poste de travail.

   - **Les utilisateurs sont autorisés à désactiver VirusScan.** Cochez cette case pour activer la commande **Désactiver** dans le menu raccourci du scanner lors de l'accès, le  bouton dans la barre d'outils de la fenêtre Console et le bouton **Désactiver** dans la boîte de dialogue Statistiques de VirusScan. Le fait de désélectionner cette case désactive tous ces boutons et commandes.

   - **Activer la mise en antémémoire de l'analyse des fichiers.** Cochez cette case pour que le scanner lors de l'accès examine chaque fichier de votre système une fois, lorsque vous démarrez pour la première fois votre système ou le service Network Associates McShield. Le scanner ignorera alors les fichiers qu'il a analysés au cours des dernières opérations d'analyse, à moins qu'ils n'aient été modifiés. Cette option peut accélérer considérablement les opérations d'analyse.

4. Cliquez sur l'onglet Actions pour sélectionner d'autres options de tâches lors de l'accès. Pour enregistrer vos modifications et revenir à la console antivirus, cliquez sur **OK**. Pour revenir à la console antivirus sans enregistrer vos modifications, cliquez sur **Annuler**.

## Sélection des options d'action

VirusScan peut empêcher la propagation d'une infection virale en désinfectant, supprimant, déplaçant ou refusant l'accès aux fichiers infectés automatiquement. Utilisez la page de propriétés Actions pour sélectionner l'action de VirusScan qui correspond à votre environnement de travail.

**Procédez comme suit :**

1. Dans la console antivirus, sélectionnez la tâche lors de l'accès dans la liste des tâches, puis sélectionnez **Propriétés** dans le menu **Analyser** ou cliquez  dans la barre d'outils de la console.

   La boîte de dialogue Propriétés de VirusScans'affiche à l'écran. Cliquez sur l'onglet Actions pour afficher la bonne page de propriétés (Figure 5-4).


**Figure 5-4. Boîte de dialogue Propriétés de VirusScan - page Actions**

2. Sélectionnez l'action que VirusScan entreprendra lorsqu'il trouvera un virus dans la liste **Lors de la détection d'un virus**. Vous avez le choix entre les actions suivantes :

   - **Refuser l'accès aux fichiers infectés et continuer.** Cette option demande à VirusScan d'interdire l'accès à tout fichier infecté trouvé dans le poste de travail aux utilisateurs du réseau. VirusScan ajoutera également l'extension .VIR aux noms des fichiers infectés. Veillez à activer la fonction d'enregistrement de VirusScan pour disposer d'une liste des fichiers infectés. Voir "Sélection des options de rapports" à la page 106 pour plus de détails.

**REMARQUE :** Étant donné que VirusScan arrête une opération de lecture ou de copie et modifie les permissions de tout fichier identifié comme infecté - sans attendre votre intervention -, Network Associates vous recommande cette option d'action si vous prévoyez de laisser votre poste de travail sans surveillance pendant de longues périodes. Vous pourrez vérifier plus tard l'infection, puis décider de désinfecter, supprimer ou restaurer le fichier à partir des copies de sauvegarde.

- **Déplacer les fichiers infectés dans un dossier**. Cette option demande à VirusScan de déplacer les fichiers infectés dans un dossier de “ quarantaine ”. Par défaut, VirusScan déplace ces fichiers dans le dossier “ Infectés ” de son répertoire programme. Vous pouvez indiquer un autre nom dans la zone de texte du **Dossier à déplacer** ou cliquez sur **Parcourir** pour trouver un dossier approprié sur le réseau.

  **REMARQUE :** Si VirusScan ne peut pas déplacer un fichier infecté ou ne peut y accéder pendant une opération d'analyse, il ajoutera une extension .VIR au nom du fichier et en interdira l'accès.

- **Nettoyer automatiquement les fichiers infectés.** Cette option demande à VirusScan d’essayer de supprimer le virus dans le fichier infecté.

  **REMARQUE :** Si VirusScan ne peut pas supprimer un virus dans un fichier infecté ou si le virus a endommagé irrémédiablement le fichier, VirusScan ajoutera une extension .VIR au nom du fichier et en interdira l'accès. Il est conseillé de supprimer un tel fichier et de le restaurer à partir des copies de sauvegarde. Veillez à activer l’option d'enregistrement de VirusScan pour disposer d'une liste des fichiers infectés Vous pouvez ensuite restaurer les fichiers endommagés à partir des copies de sauvegarde. Voir “Sélection des options de rapports” à la page 106 pour plus de détails.

- **Supprimer automatiquement les fichiers infectés.** Cette option demande à VirusScan de supprimer les fichiers infectés dès qu'il les détecte. Veillez à activer l’option d'enregistrement de VirusScan pour disposer de la liste des fichiers infectés.

3. Cliquez sur l'onglet Rapports pour choisir d'autres options de tâche lors de l'accès. Pour enregistrer vos modifications et revenir à la console antivirus, cliquez sur **OK**. Pour revenir à la console AntiVirus sans enregistrer vos modifications, cliquez sur **Annuler**.

## Sélection des options de rapports

VirusScan enregistre la liste des paramètres courants et récapitule toutes les actions qu'il entreprend durant ses opérations d'analyse dans un fichier journal nommé VIRUSSCAN ACTIVITY LOG.TXT. Vous pouvez soit demander à VirusScan de consigner son journal dans ce fichier, soit créer un fichier texte qu'utilisera VirusScan à l'aide d'un éditeur de texte. Vous pouvez ensuite ouvrir et imprimer le fichier journal pour une consultation ultérieure, depuis VirusScan ou depuis un éditeur de texte.

Le fichier journal de VirusScan peut être un outil de gestion précieux pour suivre les activités des virus dans votre réseau et noter quels paramètres vous avez utilisés pour détecter et remédier aux infections virales signalées par VirusScan. Vous pouvez également utiliser les rapports d'incidents enregistrés dans le fichier pour déterminer quels fichiers vous devez remplacer à partir des copies de sauvegarde, examiner en quarantaine ou supprimer de votre poste de travail.

**Procédez comme suit :**

1. Dans la console antivirus, sélectionnez la tâche lors de l'accès dans la liste des tâches, puis choisissez **Propriétés** dans le menu **Analyser**, ou cliquez  dans la barre d'outils de la console.

   La boîte de dialogue Propriétés de VirusScans'affiche à l'écran. Cliquez sur l'onglet Rapports pour afficher la bonne page de propriétés . (Figure 5-5 à la page 107).

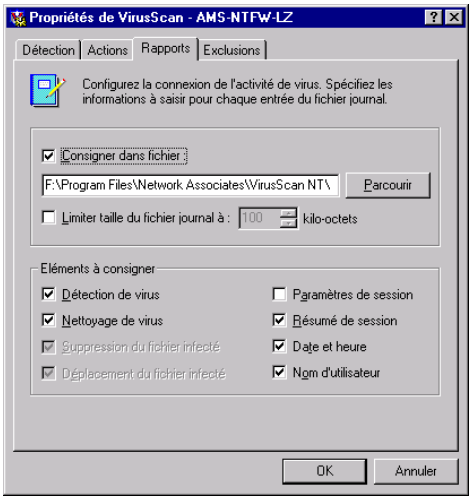



**Figure 5-5. boîte de dialogue Propriétés de VirusScan - page Rapports**

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

   Par défaut, VirusScan enregistre les informations consignées dans le fichier VIRUSSCAN ACTIVITY LOG.TXT du répertoire programme de VirusScan. Vous pouvez entrer un autre nom dans la zone de texte affichée, ou cliquer sur **Parcourir** pour trouver un fichier approprié sur votre poste de travail ou votre réseau.

3. Pour limiter la taille du fichier journal, cochez la case **Taille maximale du fichier journal**, puis saisissez cette taille, en Kilo-octets, dans la zone de texte prévue à cet effet.

   Saisissez une valeur comprise entre 10 Ko et 99 999 Ko(100 giga-octets). Par défaut, VirusScan ne limite pas du tout la taille du fichier. Si les données du fichier journal dépassent la taille définie pour le fichier, VirusScan efface le fichier journal existant et reprend au point où il s'était interrompu.

4. Cochez les cases correspondant aux informations que VirusScan doit enregistrer dans son fichier journal. Les options d'enregistrements disponibles dépendent des options que vous avez sélectionnées dans la page Actions. Voir "Sélection des options d'action" à la page 104 pour plus de détails.

Vous pouvez sélectionner l'enregistrement des informations suivantes :

- **Détection de virus.** Cochez cette case pour que VirusScan note le nombre de fichiers infectés détectés lors de cette session d'analyse.
- **Éliminer l'infection.** Cochez cette case pour que VirusScan note dans combien de fichiers il a supprimé le code du virus. Cette option ne sera pas disponible si vous ne sélectionnez pas **Nettoyer automatiquement les fichiers infectés** dans la page Actions.
- **Suppression des fichiers infectés.** Cochez cette case pour que VirusScan note le nombre de fichiers infectés qu'il a supprimés de votre système. Cette option ne sera pas disponible si vous ne sélectionnez pas **Supprimer automatiquement les fichiers infectés** dans la page Actions.
- **Déplacement des fichiers infectés.** Cochez cette case pour que VirusScan note le nombre de fichiers infectés qu'il a déplacés dans votre répertoire de quarantaine. Cette option ne sera pas disponible si vous ne sélectionnez pas **Placer le fichier infecté dans un dossier** dans la page Actions.
- **Paramètres de session.** Cochez cette case pour que VirusScan répertorie les options que vous choisissez dans la boîte de dialogue Propriétés de VirusScan pour chaque session d'analyse.
- **Résumé de la session.** Cochez cette case pour que VirusScan résume ses actions pour chaque session d'analyse. Ce résumé comporte entre autres informations le nombre de fichiers analysés, le nombre et le type des virus détectés, le nombre des fichiers déplacés ou supprimés. Une session d'analyse lors de l'accès représente la durée pendant laquelle VirusScan reste chargé en mémoire sur votre poste de travail. Elle s'achève lorsque vous déchargez VirusScan ou redémarrez votre poste de travail.
- **Date et heure.** Cochez cette case pour que VirusScan ajoute la date et l'heure à la fin de chaque entrée de journal qu'il enregistre.
- **Nom d'utilisateur.** Cochez cette case pour que VirusScan ajoute le nom de l'utilisateur connecté au poste de travail à l'heure où il enregistre chaque entrée de journal .

5. Cliquez sur l'onglet Exclusions pour sélectionner d'autres options de tâche lors de l'accès. Pour enregistrer vos modifications et revenir à la console antivirus, cliquez sur **OK**. Pour revenir à la console antivirus sans enregistrer vos modifications, cliquez sur **Annuler**.

## Sélection des options d'exclusion

Nombre de fichiers stockés sur votre poste de travail ne risquent pas d'être infectés par des virus ou ne sont jamais modifiés. Les opérations d'analyse lors de l'accès qui examinent ces fichiers peuvent être longues et ne donner que peu de résultats. Vous pouvez accélérer les opérations d'analyse en demandant à VirusScan de n'inspecter que les types de fichiers susceptibles d'être infectés (voir "Sélection des options de détection" à la page 101 pour plus de détails) ou d'ignorer des fichiers ou des dossiers complets dont vous savez qu'ils ne peuvent être infectés.

Au début, vous voudrez peut être effectuer une analyse complète à la demande pour vous assurer que votre système ne contient pas de fichiers infectés avant d'exclure des fichiers ou des dossiers de l'opération d'analyse lors de l'accès.

**Procédez comme suit :**

1. Dans la console antivirus, sélectionnez la tâche lors de l'accès dans la liste des tâches, puis choisissez **Propriétés** dans le menu **Analyser** ou cliquez  dans la barre d'outils de la console.

   La boîte de dialogue Propriétés de VirusScan s'affiche à l'écran. Cliquez sur l'onglet Exclusions pour afficher la bonne page de propriétés. (Figure 5-6).

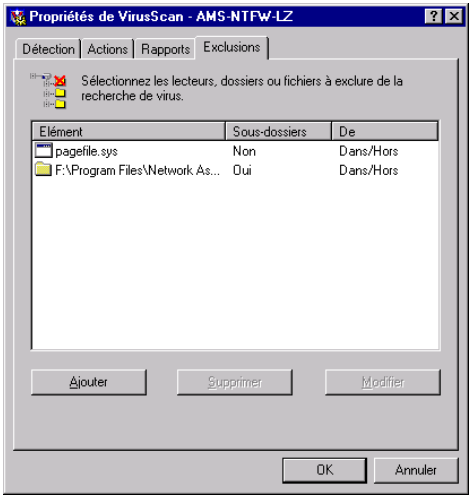



**Figure 5-6. boîte de dialogue Propriétés deVirusScan - page Exclusions**

La page Exclusions affiche d'abord un fichier base de données du système et le répertoire programme de VirusScan. VirusScan exclut ces fichiers des opérations d'analyse car ils ne sont pas susceptibles d'être infectés par des virus ou parce qu'ils sont constamment utilisés. La liste d'exclusion indique également si l'opération d'analyse est paramétrée pour ignorer tous les sous-dossiers de l'élément exclu et dans quelles circonstances VirusScan exclut celui-ci.

2. Indiquez les fichiers ou dossiers que vous voulez exclure des opérations d'analyse lors de l'accès. Vous pouvez ainsi :

   - **Ajouter des fichiers ou dossiers.** Cliquez sur **Ajouter** pour afficher la boîte de dialogue Ajouter un élément à exclure (Figure 5-7).

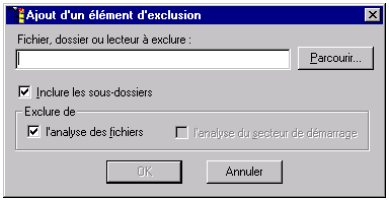



**Figure 5-7. Boîte de dialogue Ajouter un élément à exclure**

   a. Saisissez le nom du volume ou le chemin d'accès du fichier ou du dossier que vous voulez exclure de l'analyse, ou cliquez sur **Parcourir** pour localiser un fichier ou un dossier sur votre poste de travail.

      ❒ **REMARQUE :** Si vous avez configuré VirusScan pour placer automatiquement les fichiers infectés dans un dossier de quarantaine, le programme exclut ce dossier des opérations d'analyse.

   b. Cochez la case **Inclure les sous-dossiers** pour exclure tous les sous-dossiers du dossier que vous venez d'indiquer.

   c. Indiquez si VirusScan doit exclure le fichier ou le dossier que vous, ou d'autres utilisateurs, enregistrez ou copiez sur votre poste de travail, lisez à partir de votre poste de travail, ou les deux.

      – Cochez la case **Réception** pour enregistrer le fichier ou dossier sur votre poste de travail sans que VirusScan ne l'analyse.

– Cochez la case **Envoi** pour lire le fichier ou dossier à partir de votre poste de travail sans que VirusScan ne l'analyse.

d. Cliquez sur **OK** pour enregistrer vos modifications et fermer la boîte de dialogue.

Répétez les étapes a. à d. jusqu'à ce que vous ayez indiqué tous les fichiers et dossiers à exclure de l'analyse lors de l'accès.

- **Modifier la liste des exclusions.** Pour modifier les paramètres d'un élément à exclure, sélectionnez-le dans la liste des exclusions, puis cliquez sur **Modifier** pour ouvrir la boîte de dialogue Modification d'un élément à exclure. Effectuez les changements voulus, puis cliquez sur **OK** pour fermer la boîte de dialogue.
- Supprimer un élément de la liste. Pour supprimer un élément à exclure de la liste, sélectionnez-le, puis cliquez sur **Supprimer**. VirusScan analysera ce fichier ou dossier pendant la prochaine opération d'analyse lors de l'accès.

Pour enregistrer vos modifications et revenir à la console antivirus, cliquez sur **OK**. Pour revenir à la console antivirus sans enregistrer vos modifications, cliquez sur **Annuler**.

# Planification et exécution des opérations d'analyse à la demande 6

## Début des opérations d'analyse

Le composant d'analyse à la demande de VirusScan vous propose une méthode d'analyse pour tout ou partie de votre poste de travail, à l'heure qui vous convient ou à intervalles réguliers. Utilisez-la pour compléter la protection permanente dont vous bénéficiez avec le scanner lors de l'accès de VirusScan ou pour planifier des opérations d'analyse régulières lorsqu'elles ne vont pas gêner votre travail.

La console antivirus n'inclut pas de tâches d'analyse déjà planifiées car la diversité des configurations des postes de travail et des environnements réseau dans lesquels VirusScan est exécuté ne permet absolument pas de prévoir vos besoins. Vous pouvez cependant créer rapidement et facilement une tâche à la demande avec l'assistant d'analyse (voir "Création d'une tâche avec l'assistant d'analyse" à la page 81 pour apprendre à le faire), ou importer une définition de tâche d'un autre logiciel antivirus de Network Associates pour commencer (voir "Utilisation de la console antivirus" à la page 64 pour plus de détails).

Cependant, si vous démarrez le scanner autonome à la demande de VirusScan plutôt que d'exécuter une tâche à la demande à partir de la console antivirus, vous pouvez analyser immédiatement le lecteur C: de votre poste de travail. Cliquez simplement sur **Analyser maintenant** lorsque la fenêtre principale s'affiche à l'écran. Pour en savoir plus sur le scanner autonome, voir "Utilisation du scanner autonome à la demande" à la page 132.

## Pourquoi exécuter des opérations d'analyse à la demande ?

Puisque le scanner à la demande vous offre la protection d'une analyse en arrière plan sur votre poste de travail, l'exécution d'opérations d'analyse à la demande peut sembler superflue. 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 scanner lors de l'accès de VirusScan recherche des virus lors du lancement des fichiers exécutables ou lors de la lecture d'une disquette. Mais les opérations d'analyse à la demande peuvent vérifier les signatures codées dans les fichier stockés sur votre disque dur. Si vous exécutez rarement un fichier infecté, il se peut que le scanner lors de l'accès ne détecte pas le virus avant qu'il ait déjà fait beaucoup de dégâts. Cependant, une opération d'analyse à la demande peut détecter un virus qui attend une occasion 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 début de l'analyse lors de l'accès, en particulier si le programme n'est pas configuré pour analyser les disquettes. Une fois en mémoire, un virus puissant peut infecter pratiquement tous les programmes.

- **L'analyse lors de l'accès 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 et d'autres tâches. En fonction de vos besoins, vous pourriez plutôt consacrer ce moment à un travail important. Bien que les conséquences soient très peu importantes, vous pourriez être tenté de désactiver l'analyse lors de l'accès si vous avez besoin de chaque parcelle de la puissance disponible de votre système pour des tâches exigeantes. 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 que cette analyse n'est pas configurée 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.

# Création d'une tâche à la demande dans la console antivirus

La console antivirus répertorie chaque tâche à la demande dont vous avez planifié l'exécution sur votre poste de travail. Lorsque vous la démarrez pour la première fois, elle n'inclut aucune tâche à la demande préconfigurée. Pour créer une tâche à la demande entièrement nouvelle, procédez comme suit :

1. Démarrez la console antivirus (Figure 6-1). Voir "Démarrage de la console antivirus de VirusScan" à la page 61 pour apprendre à le faire.

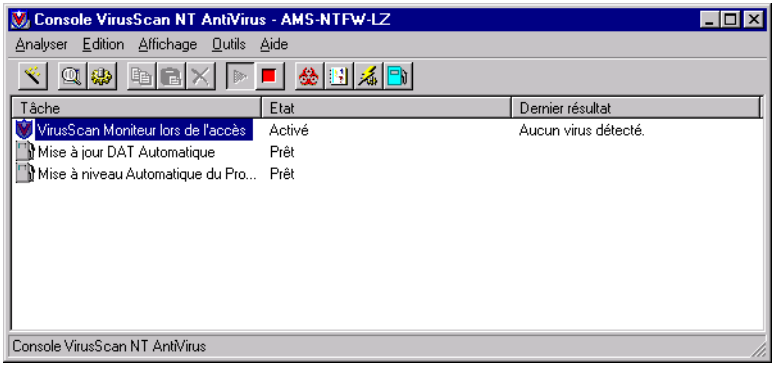



**Figure 6-1. Fenêtre de la console antivirus**

2. Choisissez **Nouvelle tâche** dans le menu **Analyser** ou cliquez dans la barre d'outils de la console.

   Une nouvelle tâche à la demande s'affiche en surbrillance dans la fenêtre des tâches de la console antivirus.

3. Entrez un nouveau nom pour votre tâche puis appuyez sur **ENTREE**.

   La console fait s'afficher la boîte de dialogue Propriétés de la tâche (Figure 6-2 à la page 116).

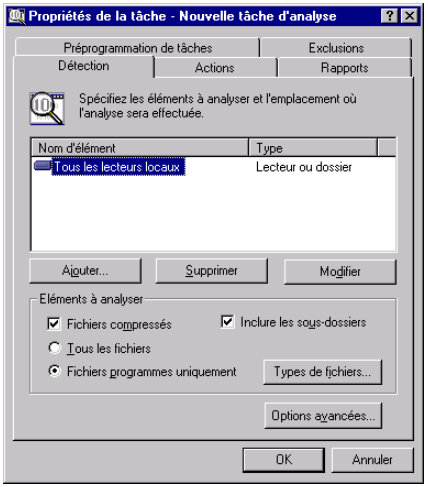



**Figure 6-2. Boîte de dialogue Propriétés de la tâche - page de Détection**

La boîte de dialogue Propriétés de la tâche comprend cinq pages de propriétés; chacune d'elles contrôle un aspect de l'opération d'analyse à la demande. Cliquez sur chaque onglet à tour de rôle pour afficher la page de propriétés correspondante et indiquer comment vous souhaitez que VirusScan effectue l'opération. Lorsque vous avez terminé, cliquez sur **OK** pour enregistrer vos modifications et fermer la boîte de dialogue.

Les sections suivantes présentent les options disponibles.

## Sélection des options de détection

Utilisez la page de Détection (Figure 6-2) pour définir la portée de l'opération d'analyse lors de l'accès - quels sont les lecteurs, fichiers ou dossiers que VirusScan doit analyser et quelles sont les extensions de noms de fichiers qu'il doit considérer comme susceptibles d'être infectées. Par défaut, VirusScan répertorie tous les lecteurs de votre poste de travail et tous les sous-dossiers qu'ils contiennent. Une opération d'analyse aussi complète pouvant prendre très longtemps, il se peut que vous souhaitiez limiter sa portée pour une utilisation régulière ultérieure.

1. Sélectionnez les cibles à analyser. Vous pouvez :

    - **Ajouter des cibles d'analyse à celles définies.** Cliquez sur **Ajouter** pour ouvrir la boîte de dialogue Ajout d'un élément à analyser (Figure 6-3 à la page 117).

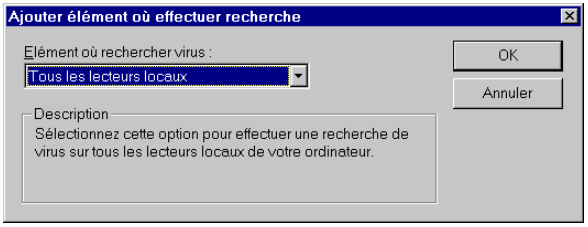



**Figure 6-3. Boîte de dialogue Ajout d'un élément à analyser**

Sélectionnez ensuite une cible à analyser dans la liste qui vous est proposée. Vous pouvez choisir d'analyser tous les lecteurs locaux, des lecteurs ou des dossiers spécifiques, ou encore des fichiers particuliers. Si vous choisissez d'analyser un lecteur, un dossier ou un fichier, entrez son chemin dans la boîte de dialogue **Description**. Vous pouvez indiquer le chemin selon la notation de la convention d'affectation des noms (UNC) ou cliquez sur **Parcourir** pour trouver le fichier ou le volume sur votre poste de travail. Lorsque vous avez terminé, cliquez sur **OK** pour refermer la boîte de dialogue.

- **Supprimer les cibles à analyser existantes.** Sélectionnez une cible dans la liste puis cliquez sur **Supprimer**.
- **Modifier ou limiter les cibles à analyser existantes.** Sélectionnez l'un des objets de la liste puis cliquez sur **Modifier** pour ouvrir la boîte de dialogue Modifier l'élément à analyser (Figure 6-4).

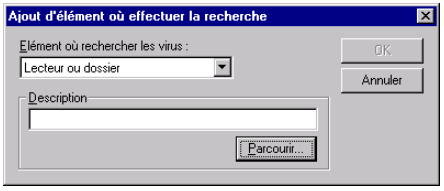



**Figure 6-4. Boîte de dialogue Modifier l'élément à analyser**

Choisissez ou entrez une nouvelle cible à analyser puis cliquez sur **OK** pour fermer la boîte de dialogue.

2. Indiquez comment vous souhaitez que VirusScan effectue l'analyse. Vous pouvez :
   - **Analyser les sous-dossiers du volume.** Par défaut, VirusScan analyse tous les sous-dossiers dans les volumes à analyser. Pour n'analyser que le niveau de la racine des volumes choisis, désélectionnez la case **Inclure les sous-dossiers**.

- **Analyser les fichiers compressés.** Par défaut, VirusScan analyse les fichiers compressés dans les formats suivants : .??_, .CAB, LZEXE, LZH, PKLite, .TD0 et .ZIP. Bien qu'il offre une protection supplémentaire, l'examen des fichiers compressés peut ralentir l'opération d'analyse. Vous pouvez empêcher VirusScan d'analyser ces fichiers en désélectionnant la case **Fichiers compressés**.

- **Sélectionner les types de fichiers à analyser.** D'ordinaire, les virus ne peuvent infecter les fichiers de données ou les fichiers qui ne contiennent pas de code exécutable. Vous pouvez donc sans risque limiter la portée de vos opérations d'analyse aux fichiers les plus susceptibles d'être infectés par les virus pour les accélérer. Pour ce faire, cochez la case **Fichiers programme uniquement**. Pour voir ou désigner les extensions des noms de fichiers que VirusScan doit analyser, cliquez sur **Types de fichiers** pour ouvrir la boîte de dialogue Extensions des fichiers programme (voir Figure 6-5).


**Figure 6-5. Boîte de dialogue Extensions des fichiers programme**

Par défaut, VirusScan recherche des virus dans les fichiers portant les extensions .EXE, .COM, .DOC, .DOT, .XL?, .MD ?, .VXD, .386, .SYS, .BIN, .RTF, .OBD, .DLL, .SCR, .OBT, .PP?. .POT, .OLE, .SHS, .MPP, .MPT, .XTP, .XLB, .CMD, .OVL et .DEV. Cette liste comprend presque tous les fichiers susceptibles d'être infectés par des virus de macro, y compris tous les types de fichiers de Microsoft Office. Le caractère ? est un caractère générique qui permet à VirusScan d'examiner les fichiers de même type, tels que les fichiers documents et modèles.

  – Pour ajouter des types de fichiers à la liste, cliquez sur **Ajouter** puis entrez les extensions que VirusScan doit analyser dans la boîte de dialogue qui s'affiche alors.

  – Pour supprimer une extension de la liste, sélectionnez-la, puis cliquez sur **Supprimer**.

  – Cliquez sur **Par défaut** pour revenir à la liste originale.

Lorsque vous avez terminé, cliquez sur **OK** pour refermer la boîte de dialogue.

Pour analyser tous les volumes, dossiers et fichiers de votre poste de travail, cochez la case **Tous les fichiers**. Ceci ralentira considérablement vos opérations d'analyse, mais vous garantira que votre système est exempt de tout virus.

3. Pour définir une priorité de votre tâche d'analyse par rapport aux autres opérations du poste de travail, cliquez sur **Avancés** pour afficher la boîte de dialogue Paramètres avancés du scanner (Figure 6-6).

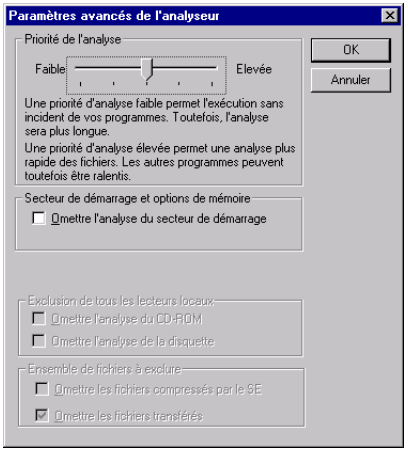



**Figure 6-6. Boîte de dialogue Paramètres avancés du scanner**

Les choix possibles sont :

- **Définir une priorité pour votre tâche d'analyse.** Faites glisser le curseur vers la gauche pour donner à la tache d'analyse une priorité inférieure par rapport aux autres tâches qui s'exécutent sur votre poste de travail. Vous serez certain qu'un autre logiciel en cours d'exécution ne ralentira pas pendant une opération d'analyse, mais l'opération d'analyse prendra plus de temps. Donner à la tâche d'analyse une priorité inférieure si vous prévoyez de l'exécuter pendant que vous travaillez.

  Faites glisser le curseur vers la droite pour donner à la tâche d'analyse une plus grande priorité par rapport aux autres tâches. Cela enlèvera du temps de traitement à un autre logiciel et ralentira d'autres applications, mais vous serez sûr que l'opération d'analyse s'effectuera plus vite. Donner plus de priorité à la tâche si vous prévoyez de l'exécuter lorsque vous n'êtes pas en train de travailler.

Par défaut, VirusScan essaie d'équilibrer la priorité de la tâche d'analyse selon les besoins d'autres services.

- **Ne pas analyser le secteur d'amorçage.** Normalement, VirusScan analysera votre secteur de partition et les blocs d'amorçage de votre disque dur pour rechercher des virus du secteur d'amorçage. Bien que la plupart des nouveaux virus soient des virus de macro, les virus du secteur d'amorçage continuent à s'étendre et peuvent endommager votre système. Network Associates vous recommande d'analyser régulièrement votre secteur d'amorçage, mais si cela perturbe les opérations du système, cochez la case pour éviter ce type d'opération d'analyse.
- **Exclure les CD-ROM de l'analyse.** Cette option n'est pas disponible dans VirusScan pour Windows NT.
- **Ignorer le balayage de la disquette.** Cette option n'est pas disponible dans VirusScan pour Windows NT.
- **Exclure les groupes de fichiers de l'analyse.** Cette option n'est pas disponible dans VirusScan pour Windows NT.
- **Ne pas analyser les fichiers transférés.** Cette option n'est pas disponible dans VirusScan pour Windows NT.

Lorsque vous avez fini de définir les priorités de cette tâche d'analyse, cliquez sur **OK** pour refermer la boîte de dialogue Paramètres avancés du Scanner.

4. Cliquez sur l'onglet Action pour sélectionner d'autres options de tâche à la demande Pour enregistrer vos modifications et revenir à la console antivirus, cliquez sur **OK**. Pour revenir à la console antivirus sans enregistrer vos modifications, cliquez sur **Annuler**.

## Sélection des options d'action

VirusScan peut empêcher la propagation d'une infection virale en désinfectant, supprimant, déplaçant ou refusant l'accès aux fichiers infectés automatiquement Utilisez la page de propriétés Action pour sélectionner l'action de VirusScan qui correspond à votre environnement de travail.

**Pour choisir les actions de VirusScan en cas d'infection, procédez comme suit :**

1. Dans la console antivirus, sélectionnez la tâche à la demande que vous avez créée dans la liste des tâches, puis sélectionnez **Propriétés** dans le menu **Analyser** ou cliquez  dans la barre d'outils de la console

La boîte de dialogue Propriétés de la tâche s'affiche à l'écran. Cliquez sur l'onglet Action pour afficher la bonne page de propriétés. (Figure 6-7).

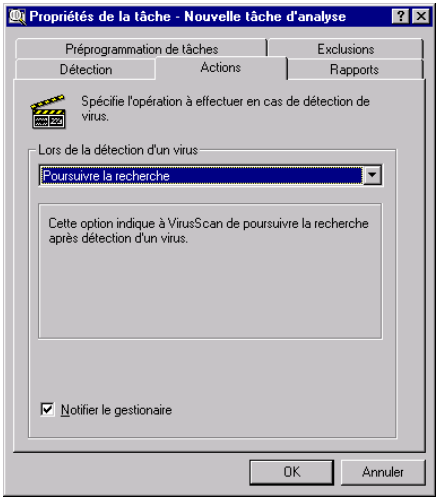



**Figure 6-7. boîte de dialogue Propriétés de la tâche - page d'Action**

2. Sélectionnez l'action que vous voulez que VirusScan entreprenne lorsqu'il détecte un virus. Vous avez le choix entre les actions suivantes :

   - **Poursuivre l'analyse.** Cette option demande à VirusScan de noter lorsqu'il détecte un virus, puis de continuer l'analyse sans entreprendre aucune autre action. Si vous avez activé les options d'alerte et d'enregistrement, VirusScan vous indiquera qu'il a trouvé un virus et enregistrera l'incident dans son journal d'activité. Voir "Sélection des options de rapport" à la page 123 pour plus de détails.

   - **Placer le fichier infecté dans un dossier.** Cette option demande à VirusScan de placer le fichier infecté dans un dossier de " quarantaine ". Par défaut, VirusScan place ces fichiers dans un dossier nommé Infected de son répertoire programme.

     Vous pouvez entrer un autre nom de dossier dans la zone de texte affichée ou cliquer sur **Parcourir** pour trouver un dossier approprié sur votre poste de travail ou sur le réseau.

> **REMARQUE :** Si VirusScan ne peut pas déplacer un fichier infecté pendant une opération d'analyse, il vous préviendra qu'il a détecté un virus - si vous avez activé son option d'alerte -, signalera qu'il n'a pu déplacer le fichier infecté et n'entreprendra aucune autre action. Si son option d'enregistrement est activée, VirusScan enregistrera cet incident dans son journal d'activité. Voir chapitre 7, "Transmission des messages d'alerte" et "Sélection des options de rapport" à la page 123 pour de plus amples informations.

- **Nettoyer les fichiers infectés.** Cette option demande à VirusScan d'essayer de supprimer le virus dans les fichiers infectés.

> **REMARQUE :** Si VirusScan ne peut pas supprimer un virus dans un fichier infecté ou si le virus a endommagé irrémédiablement le fichier, VirusScan vous préviendra qu'il a détecté un virus - si vous avez activé son option d'alerte -, signalera qu'il n'a pu nettoyer le fichier mais n'entreprendra aucune autre action Si son option d'enregistrement est activée, VirusScan enregistrera cet incident dans son journal d'activité. Voir chapitre 7, "Transmission des messages d'alerte" "Sélection des options de rapport" à la page 123pour de plus amples informations.

- **Supprimer les fichiers infectés.** Cette option demande à VirusScan de supprimer les fichiers infectés dès qu'il les détecte. Veillez à activer l'option d'enregistrement de VirusScan afin de disposer d'un enregistrement des fichiers que VirusScan a marqué comme étant infectés.

3. Pour que VirusScan vous avertisse lorsqu'il détecte un fichier infecté, cochez la case **Avertir le gestionnaire d'alertes**. Le gestionnaire d'alertes vous informe des infections virales en vous envoyant un message par toute une série de canaux. Voir chapitre 7, "Transmission des messages d'alerte," pour apprendre comment configurer le gestionnaire d'alertes.

4. Cliquez sur l'onglet Rapport pour choisir d'autres options de tâche à la demande. Pour enregistrer vos modifications et revenir à la console antivirus, cliquez sur **OK**. Pour revenir à la console antivirus sans enregistrer vos modifications, cliquez sur **Annuler.**

## Sélection des options de rapport

VirusScan enregistre la liste des paramètres courants et récapitule toutes les actions qu'il entreprend durant ses opérations d'analyse dans un fichier journal nommé SCAN ACTIVITY LOG.TXT. Vous pouvez soit demander à VirusScan de consigner son journal dans ce fichier, soit créer un fichier texte qu'utilisera VirusScan à l'aide d'un éditeur de texte. Vous pouvez par conséquent ouvrir et imprimer le fichier journal pour consultation ultérieure depuis VirusScan ou depuis un éditeur de texte.

Le fichier journal de VirusScan peut être un outil de gestion précieux pour suivre les activités des virus dans votre réseau et noter quels paramètres vous avez utilisés pour détecter et remédier aux infections virales signalées par VirusScan. Vous pouvez également utiliser les rapports d'incidents enregistrés dans le fichier pour déterminer quels fichiers vous devez remplacer à partir de vos copies de sauvegarde, examiner en quarantaine ou supprimer de votre poste de travail. Utilisez la page de propriétés Rapport pour déterminer les informations que vous souhaitez inclure dans le fichier journal de VirusScan.

**Pour indiquer à VirusScan ce qu'il doit enregistrer dans son fichier journal, procédez comme suit :**

1. Dans la console antivirus, sélectionnez la tâche à la demande que vous avez créée dans la liste des tâches, puis sélectionnez **Propriétés** dans le menu **Analyser** ou cliquez  dans la barre d'outils de la console.

   La boîte de dialogue Propriétés de la tâche s'affiche à l'écran Cliquez sur l'onglet Rapport pour afficher la bonne page de propriétés. (Figure 6-8 à la page 124).


**Figure 6-8. boîte de dialogue Propriétés de la tâche - page de Rapport**

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

   Par défaut, VirusScan enregistre les informations relatives au journal dans le fichier SCAN ACTIVITY LOG.TXT du répertoire programme VirusScan NT. Vous pouvez entrer un autre nom dans la zone de texte affichée ou cliquer sur **Parcourir** pour trouver un fichier approprié sur votre poste de travail ou sur votre réseau.

3. Pour limiter la taille du fichier journal, cochez la case **Taille maximale du fichier journal**, puis saisissez cette taille, en Kilo-octets, dans la zone de texte prévue à cet effet.

   Saisissez une valeur comprise entre 10 Ko et 99 999 Ko (100 Mo). Par défaut, VirusScan ne limite pas du tout la taille du fichier. Si les données du journal dépassent la taille allouée pour le fichier, VirusScan efface le fichier journal existant et le reprend au point où il s'était interrompu.

4. Cochez les cases correspondant aux informations que VirusScan doit enregistrer dans son fichier journal. Les options d'enregistrement disponibles dépendent des options que vous avez sélectionnées dans la page d'Action. Voir "Sélection des options d'action" à la page 120 pour plus de détails. Vous pouvez sélectionner l'enregistrement des informations suivantes :

   - **Détection des virus.** Cochez cette case pour que VirusScan note le nombre de fichiers infectés détectés lors de cette session d'analyse.

- **Élimination des virus.** Cochez cette case pour que VirusScan note dans combien de fichiers il a supprimé le code du virus. Cette option ne sera pas disponible si vous ne sélectionnez pas **Nettoyer les fichiers infectés** dans la page d'Action.
- **Suppression des fichiers infectés.** Cochez cette case pour que VirusScan note le nombre de fichiers infectés qu'il a supprimés de votre système. Cette option ne sera pas disponible si vous ne sélectionnez pas **Supprimer les fichiers infectés** dans la page d'Action.
- **Déplacement des fichiers infectés**. Cochez cette case pour que VirusScan note le nombre de fichiers infectés qu'il a placés dans votre répertoire de quarantaine. Cette option ne sera pas disponible si vous ne sélectionnez pas **Placer le fichier infecté dans un dossier** dans la page d'Action.
- **Paramètres de session.** Cochez cette case pour que VirusScan répertorie les options que vous choisissez dans la boîte de dialogue Propriétés de VirusScan pour chaque session d'analyse.
- **Résumé de session.** Cochez cette case pour que VirusScan résume ses actions pour chaque session d'analyse. Ce résumé comporte entre autres informations le nombre de fichiers analysés, le nombre et le type des virus détectés, le nombre des fichiers déplacés ou supprimés. Une session d'analyse lors de l'accès représente la durée pendant laquelle VirusScan reste chargé en mémoire sur votre poste de travail. Elle s'achève lorsque vous déchargez VirusScan ou redémarrez votre poste de travail.
- **Date et heure.** Cochez cette case pour que VirusScan ajoute la date et l'heure à la fin de chaque entrée de journal qu'il enregistre.
- **Nom de l'utilisateur.** Cochez cette case pour que VirusScan ajoute le nom de l'utilisateur travaillant sur votre poste de travail à l'heure où il enregistre chaque entrée de journal .

5. Cliquez sur l'onglet Planifier pour choisir des options supplémentaires de tâche à la demande. Pour enregistrer vos modifications et revenir à la console antivirus, cliquez sur **OK**. Pour revenir à la console antivirus sans enregistrer vos modifications, cliquez sur **Annuler.**

## Sélection des options de planification

VirusScan vous offre des outils pour planifier des opérations d'analyse à des dates et heures spécifiques ou à des intervalles particuliers. Vous pouvez planifier l'exécution d'une opération d'analyse par VirusScan en votre absence ou quand cela vous convient.

**Pour planifier cette tâche à la demande, procédez comme suit :**

1. Dans la console antivirus, sélectionnez la tâche à la demande que vous avez créée dans la liste des tâches, puis sélectionnez **Propriétés** dans le menu **Analyser** ou cliquez  dans la barre d'outils de la console.

   La boîte de dialogue Propriétés deVirusScan s'affiche à l'écran. Cliquez sur l'onglet Planifier pour afficher la bonne page de propriétés. (Figure 6-9).

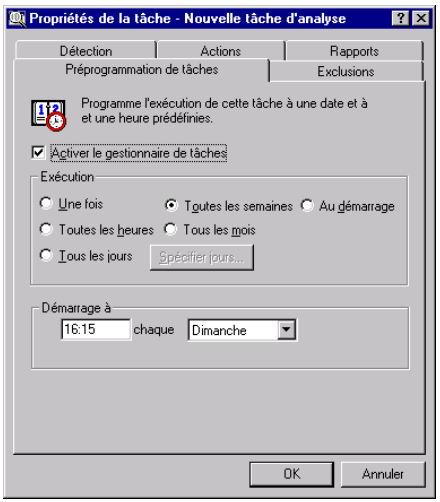



**Figure 6-9. boîte de dialogue Propriétés des tâches - page de Planification**

2. Cochez la case **Activer le planificateur**. Les options des zones **Exécuter** et **Démarrer à** deviennent actives.

3. Choisissez la fréquence d'exécution de la tâche dans la zone **Exécuter**, ou sélectionnez **Au démarrage** pour que votre tâche s'exécute dès que VirusScan est chargé. Selon la fréquence choisie, la zone **Démarrer à** vous propose des choix différents pour la planification de votre tâche. Vos choix sont :

   - **Une fois.** Cette option exécute votre tâche une seule fois à la date et à l'heure que vous spécifiez. Entrez l'heure dans la zone de texte à gauche de la zone **Démarrer à**, puis sélectionnez un mois et une date dans les listes de droite.

- **Toutes les heures.** Cette option exécute votre tâche toutes les heures tant que votre poste de travail est allumé et que VirusScan est en cours d'exécution. Spécifiez dans la zone de texte affichée la durée en minutes que VirusScan doit attendre après chaque heure pour exécuter votre tâche.
- **Tous les jours**. Cette option exécute votre tâche une fois, à l'heure et aux jours que vous spécifiez. Cliquez sur **Quel jour** pour sélectionner dans la boîte de dialogue qui s'affiche les jours d'exécution de votre tâche. Après l'avoir fait, cliquez sur **OK** pour fermer la boîte de dialogue puis entrez dans la zone de texte **Démarrer à** l'heure à laquelle la tâche s'exécutera chaque jour.
- **Toutes les semaines.** Cette option exécute 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.
- **Tous les mois.** Cette option exécute votre tâche une fois par mois au jour et à l'heure que vous spécifiez. Entrez l'heure dans la zone de texte à gauche, puis le jour du mois souhaité pour l'exécution de la tâche .

4. Cliquez sur l'onglet Planifier pour choisir des options supplémentaires de tâche à la demande. Pour enregistrer vos modifications et revenir à la console antivirus, cliquez sur **OK**. Pour revenir à la console antivirus sans enregistrer vos modifications, cliquez sur **Annuler.**

---

❑ **REMARQUE :** Pour que VirusScan exécute votre tâche, il faut que votre poste de travail soit allumé et que VirusScan soit en cours d'exécution. Si ces deux conditions ne sont pas remplies au moment où votre tâche devrait démarrer, cette tâche ne s'exécutera qu'à la prochaine date planifiée.

---

## Sélection des options d'exclusion

Nombre de fichiers stockés sur votre poste de travail ne risquent pas d'être infectés par des virus ou ne changent jamais. Les opérations d'analyse à la demande ou planifiées qui examinent ces fichiers peuvent être longues et ne donner que peu de résultats. Vous pouvez accélérer les opérations d'analyse en demandant à VirusScan de n'inspecter que les types de fichiers susceptibles d'être infectés (voir "Sélection des options de détection" à la page 116 pour plus de détails), 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 vous reposer sur le scanner lors de l'accès de VirusScan pour vous protéger entre deux opérations d'analyse planifiées ou à la demande. Cependant, la meilleure protection contre les virus demeure la régularité des opérations d'analyse examinant tous les secteurs de votre poste de travail.

**Pour exclure certains fichiers, dossiers ou volumes des opérations d'analyse à la demande, procédez comme suit :**

1. Dans la console antivirus, sélectionnez la tâche à la demande que vous avez créée dans la liste des tâches, puis sélectionnez **Propriétés** dans le menu **Analyser** ou cliquez  dans la barre d'outils de la console.

   La boîte de dialogue Propriétés deVirusScans'affiche à l'écran Cliquez sur l'onglet Exclusion pour afficher la bonne page de propriétés. (Figure 6-10).


**Figure 6-10. boîte de dialogue Propriétés des tâches - page d'Exclusion**

La page d'Exclusion affichera d'abord un fichier base de données du système et le répertoire programme de VirusScan. VirusScan exclut ces fichiers des opérations d'analyse car ils ne sont pas susceptibles d'être infectés par des virus ou parce qu'ils sont constamment utilisés. La liste d'exclusion indique également si l'opération d'analyse est configurée pour ignorer tous les sous-dossiers de l'élément exclu et dans quelles circonstances VirusScan exclut celui-ci.

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

   - **Ajouter des fichiers, des dossiers ou des volumes à la liste d'exclusion.** Cliquez sur **Ajouter** pour ouvrir la boîte de dialogue Ajout d'un élément à exclure (Figure 6-11).

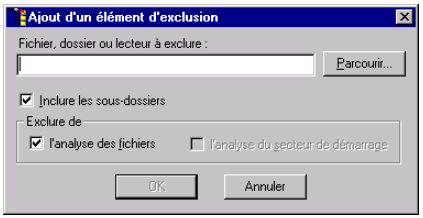



**Figure 6-11. Boîte de dialogue Ajout d'un élément à exclure**

   a. Saisissez le nom du volume ou le chemin d'accès au fichier ou au dossier que vous voulez exclure de l'analyse, ou cliquer sur **Parcourir** pour trouver un fichier ou un dossier sur votre poste de travail.

   ❑ **REMARQUE :** Si vous avez configuré VirusScan pour placer automatiquement les fichiers infectés dans un dossier de quarantaine, le programme exclut ce dossier des opérations d'analyse.

   b. Cochez la case **Inclure les sous-dossiers** pour exclure tous les sous-dossiers du dossier que vous venez d'indiquer.

   c. Vérifiez que VirusScan exclut le fichier ou le dossier de l'analyse de fichiers. Bien que vous ne puissiez analyser le secteur de partition de votre poste de travail ou les blocs d'amorçage pendant une opération d'analyse planifiée, vous pouvez configurer une tâche à la demande qui le fera avec le scanner autonome à la demande. Voir "Utilisation du scanner autonome à la demande" à la page 132 pour plus de détails.

   d. Cliquez sur **OK** pour sauvegarder vos modifications et fermer la boîte de dialogue.

   e. Répéter les étapes a. à d. jusqu'à ce que vous ayez listé tous les fichiers et dossiers que vous ne voulez pas voir analyser.

   - **Modifier la liste des exclusions.** Pour modifier les paramètres d'un élément à exclure, sélectionnez-le dans la liste des exclusions, puis cliquez sur **Modifier** pour ouvrir la boîte de dialogue Modifier l'élément à exclure. Faites les changements voulus, puis cliquez sur **OK** pour fermer la boîte de dialogue.

- **Supprimer un élément de la liste.** Pour supprimer un élément à exclure de la liste, sélectionnez-le, puis cliquez sur **Supprimer**. VirusScan analysera ce fichier ou dossier lors de la prochaine opération d'analyse à la demande.

3. Pour enregistrer vos modifications et revenir à la console antivirus, cliquez sur **OK**. Pour revenir à la console antivirus sans enregistrer vos modifications, cliquez sur **Annuler.**

# Exécution de votre tâche d'analyse

Une fois que vous avez configuré votre tâche avec les options d'analyse que vous voulez, vous pouvez fermer la console antivirus et laisser la tâche s'exécuter automatiquement. Si vous avez planifié votre tâche pour qu'elle s'exécute à une certaine heure, le service du Gestionnaire des tâches de Network Associates démarrera votre tâche à l'heure indiquée, sous réserve que votre poste de travail soit allumé et que VirusScan soit en cours d'exécution. Si vous n'avez pas planifié votre tâche mais prévoyez de l'exécuter immédiatement, il est préférable de laisser la console antivirus ouverte afin de pouvoir contrôler les progrès de l'opération d'analyse et répondre aux messages d'alerte que vous verrez.

**Pour démarrer immédiatement une tâche à la demande, procédez comme suit :**

1. Si elle n'est pas déjà en cours d'exécution, démarrez la console antivirus. Voir"Démarrage de la console antivirus de VirusScan" à la page 61 pour apprendre à le faire.

2. Sélectionnez votre tâche à la demande dans la liste des tâches (Figure 6-12), puis choisissez **Démarrer** dans le menu **Analyser**, ou cliquez  dans la barre d'outils de la console.




**Figure 6-12. fenêtre de la console antivirus**

Votre tâche d'analyse commencera. La console antivirus affichera sa progression dans la colonne **Etat** ainsi qu'un résumé des résultats d'analyse dans la colonne **Dernier résultat**.

# Visualisation des résultats d'analyse

Une fois votre opération d'analyse terminée, ou même pendant l'exécution de la tâche, vous pouvez voir un résumé statistique plus détaillé du nombre de fichiers analysés par VirusScan, ainsi que du nombre de virus trouvés et des actions entreprises.

**Pour voir les statistiques et les résultats de votre tâche, procédez comme suit :**

1. Si elle n'est pas déjà en cours d'exécution, démarrez la console antivirus. Voir "Démarrage de la console antivirus de VirusScan" à la page 61 pour apprendre à le faire.
2. Double-cliquez sur votre tâche à la demande dans la liste des tâches (voir Figure 6-12 à la page 130), ou sélectionnez **Statistiques** dans le menu **Analyser** pour ouvrir la boîte de dialogue Statistiques de la tâche (Figure 6-13).

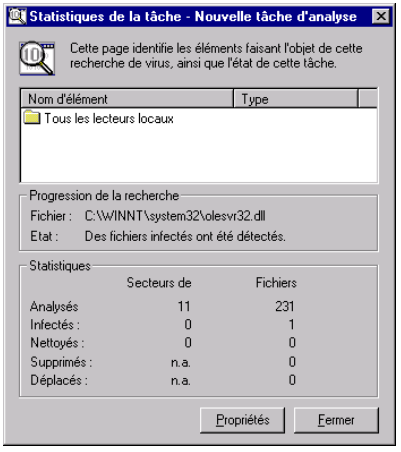



**Figure 6-13. boîte de dialogue Statistiques de la tâche**

La boîte de dialogue Statistiques de la tâche affiche chaque cible à analyser que vous avez choisie pour cette tâche en haut de l'écran ainsi qu'un résumé statistique en bas. Si votre tâche d'analyse est toujours en cours, elle affiche le fichier que VirusScan est en train d'analyser ainsi que l'état de l'opération d'analyse.

Vous pouvez aussi actualiser la configuration de la tâche de manière dynamique dans cette boîte de dialogue. Cliquez sur **Propriétés** pour ouvrir la boîte de dialogue Propriétés de la tâche, puis modifiez les options de la tâche que vous souhaitez changer. Voir pages 115 à 130 pour apprendre comment configurer une tâche à la demande. La tâche s'exécutera immédiatement avec vos nouveaux paramètres, mais la boîte de dialogue Statistiques de la tâche ne sera pas rafraîchie tant que vous ne l'aurez pas fermée puis ouverte à nouveau.

Lorsque vous aurez fini de modifier les statistiques de la tâche, cliquez sur **Fermer** pour revenir à la console antivirus.

# Utilisation du scanner autonome à la demande

Lorsque vous planifiez ou exécutez une opération d'analyse à la demande dans la console antivirus, le service de Gestionnaire des tâches de Network Associates démarre VirusScan (SCAN32.EXE) pour effectuer l'opération d'analyse. Vous pouvez ouvrir ce même programme comme un scanner autonome pour effectuer vos opérations d'analyse à la demande très rapidement, ou choisir des paramètres exportables que vous pourrez envoyer à d'autres stations de travail sur votre réseau.

Certaines options de configuration disponibles avec cette interface varient également de celles disponibles lorsque vous configurez une tâche d'analyse avec la console antivirus.

# Démarrage de VirusScan

**Pour démarrer VirusScan, vous pouvez :**

- Cliquez sur **Démarrer** dans la barre des tâches Windows, pointez sur **Programmes** et sélectionnez **Network Associates VirusScan NT**. Puis, choisissez **VirusScan** dans la liste qui s'affiche ; ou
- Cliquez sur **Démarrer**, puis choisissez **Exécuter** dans le menu qui apparaît. Entrez SCAN32.EXE dans la boîte de dialogue Exécuter, puis cliquez sur **OK**.

Ces deux méthodes ouvrent la fenêtre de VirusScan (Figure 6-14).

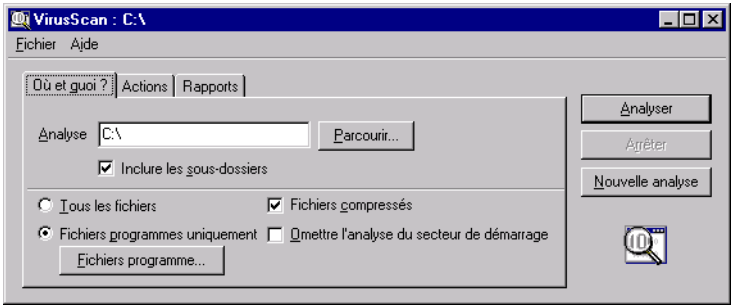



**Figure 6-14. Fenêtre principale de VirusScan**

Cliquez sur **Analyser maintenant** à droite de la fenêtre pour lancer immédiatement l'analyse par défaut ou configurez une tâche d'analyse qui convienne à vos besoins en cliquant sur les onglets en haut de la fenêtre afin de choisir les options appropriées sur chacune des pages de propriétés.

# Utilisations des menus de VirusScan

Les menus qui apparaissent le long du bord supérieur de la fenêtre de VirusScan vous permettent de modifier certains aspects du fonctionnement du programme. Vous pouvez ainsi :

- **Démarrer une opération d'analyse.** Choisissez **Démarrer** dans le menu **Fichier** pour exécuter une opération d'analyse immédiatement, quelles que soient les options de configuration que vous ayez définies à ce moment. Vous pouvez aussi cliquer sur **Analyser maintenant** pour démarrer une opération d'analyse de la même façon.
- **Enregistrer de nouveaux paramètres.** Par défaut, VirusScan recherchera la présence de virus dans les fichiers les plus susceptibles d'être infectés. Il analysera le secteur de partition et les blocs d'amorçage de votre ordinateur, examinera votre lecteur C: et tous ses sous-dossiers, puis enverra un message au gestionnaire d'alertes s'il détecte un virus. Dans sa configuration d'origine, il n'entreprendra aucune action contre les virus détectés, mais il enregistrera ses actions et résumera ses paramètres actuels dans un fichier journal que vous pourrez consulter plus tard.

Si vous souhaitez disposer de plusieurs configurations de VirusScan afin d'effectuer différents types d'opérations d'analyse ou que vous voulez exécuter une opération d'analyse avec une configuration identique sur plusieurs ordinateurs, vous pouvez enregistrer vos options de configuration sous forme d'un fichier .VSC avec son propre nom. Un fichier .VSC est un fichier texte qui enregistre les options de configuration de VirusScan, de façon analogue aux fichiers .INI de Windows qui enregistrent les options de démarrage des programmes.

Pour enregistrer vos paramètres, configurez tout d'abord VirusScan avec les options de votre choix, puis choisissez **Enregistrer les paramètres** dans le menu **Fichier**. Entrez un nom explicite dans la boîte de dialogue Enregistrer sous, choisissez un emplacement pour votre fichier sur votre disque dur, puis cliquez sur **Enregistrer**. Vous pouvez ensuite copier ce fichier sur tout ordinateur susceptible d'utiliser les mêmes paramètres. Pour plus d'informations, Voir "Configuration de VirusScan" à la page 136 ou .

Pour exécuter VirusScan avec ces paramètres, il vous suffit de rechercher le fichier .VSC que vous avez enregistré et de double-cliquer sur son nom. VirusScan démarre alors avec les paramètres chargés.

- **Ouvrir le fichier journal de VirusScan.** Pour ouvrir le fichier journal dans lequel VirusScan enregistre ses actions et ses paramètres, choisissez **Afficher le journal d'activité** dans le menu **Fichier**.

  Le fichier journal s'ouvre dans une fenêtre du Bloc-notes (voir Figure 6-15). Vous pouvez imprimer, éditer, copier ou manipuler ce fichier comme vous le feriez avec un fichier texte ordinaire. Pour en savoir davantage sur les informations enregistrées dans le fichier journal, voir "Sélection des options de rapport" à la page 141.

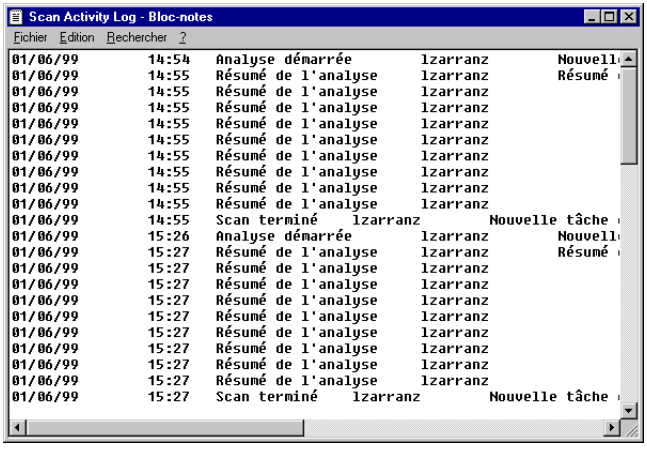



**Figure 6-15. Journal d'activité de VirusScan**

- **Quitter VirusScan.** Pour quitter VirusScan, choisissez **Fermer** dans le menu **Fichier**. Le fait de fermer VirusScan arrête toutes les opérations d'analyse actives mais n'affecte *pas* le Gestionnaires des tâches de Network Associates ni les tâches en arrière-plan permanentes du scanner lors de l'accès. À moins que vous ne les enregistriez, toutes les options de configuration que vous avez choisies disparaîtront également à la fermeture de VirusScan.

- **Connexion à la bibliothèque d'informations sur les virus en ligne.** Le fait de choisir **Bibliothèque d'informations sur les virus en ligne** dans le menu **Aide** vous connectera à la Bibliothèque d'informations sur les virus en ligne 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 6-16).

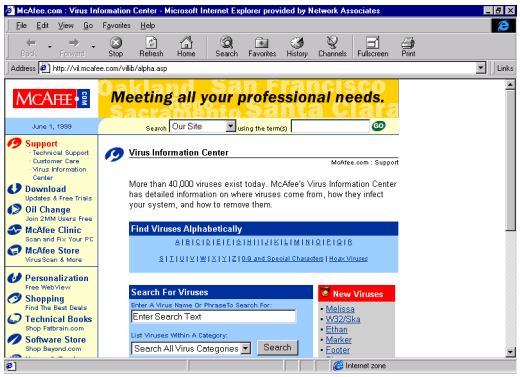



**Figure 6-16. Bibliothèque d'informations sur les virus en ligne**

La Bibliothèque d'informations sur les virus vous donne une description détaillée de chaque virus que VirusScan peut détecter ou nettoyer. Ces informations comprennent, entre autres, la façon dont le virus infecte et modifie les fichiers, le type d'armes qu'il déploie, comment reconnaître une infection, etc. La bibliothèque fournit également des conseils pour empêcher les infections virales et éradiquer les virus que VirusScan n'est pas en mesure de supprimer des fichiers infectés.

- **Ouverture du fichier d'aide en ligne.** Pour afficher la liste des rubriques d'aide de VirusScan, choisissez **Rubriques d'aide** dans le menu **Aide**. Pour faire apparaître une description contextuelle des boutons, des listes et des autres éléments de la fenêtre de 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 apparaît.

- **Voir le numéro de la version et d'autres informations.** Choisissez **A propos de** dans le menu **Aide** pour voir les informations relatives au copyright, les numéros de série, les numéros de version des fichiers de définition des virus, ainsi que d'autres informations sur votre copie de VirusScan.

# Configuration de VirusScan

Afin de pouvoir effectuer une opération d'analyse, VirusScan doit savoir ce que vous voulez qu'il analyse, ce que vous souhaitez qu'il fasse s'il détecte un virus et comment il doit vous en avertir. Vous pouvez également demander à VirusScan de tenir à jour l'enregistrement des actions qu'il effectue. Une série de pages de propriétés contrôle les options relatives à chaque tâche ; pour configurer VirusScan en fonction de votre tâche, cliquez sur les onglets correspondants dans la fenêtre VirusScan.

## Choix des options Où & Quoi

VirusScan suppose au départ que vous souhaitez analyser votre unité C: et tous ses sous-dossiers et restreindre les fichiers à analyser à ceux susceptibles d'être infectés par un virus (Figure 6-17).

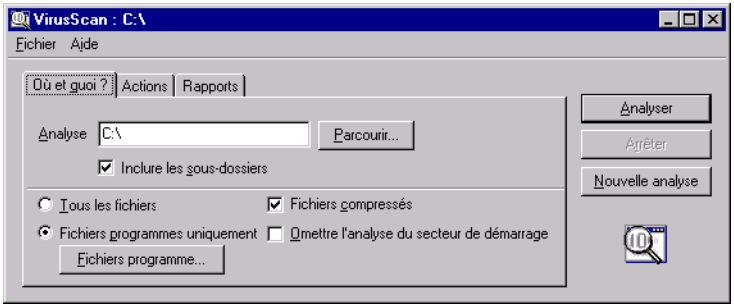



**Figure 6-17. Fenêtre principale de VirusScan - Page Où & Quoi**

**Pour modifier ces options, suivez cette procédure :**

1. Choisissez un volume ou un dossier de votre système ou de votre réseau que vous souhaitez faire analyser par VirusScan à la recherche de virus.

   Vous pouvez entrer le chemin du volume ou du dossier cible dans la zone de texte **Analyser dans** ou cliquer sur **Parcourir** pour ouvrir la boîte de dialogue Recherche d'un dossier (Figure 6-18).

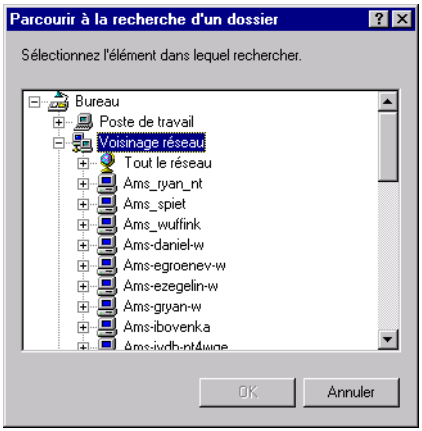



**Figure 6-18. Boîte de dialogue Recherche d'un dossier**

   Pour ouvrir la liste d'un élément figurant dans la boîte de dialogue, cliquez sur ⊞. Cliquez sur ⊟ pour réduire un élément Vous pouvez sélectionner comme cibles d'analyse 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 ou plusieurs volumes comme cibles d'analyse ; pour cela, vous devez créer une tâche d'analyse dans la console antivirus.

   Une fois que vous avez sélectionné votre cible d'analyse, cliquez sur **OK** pour revenir à la fenêtre VirusScan.

2. Cochez la case **Inclure les sous-dossiers** si vous souhaitez que VirusScan recherche les virus dans tous les dossiers contenus dans votre cible d'analyse.

3. Spécifier les types de fichier à faire analyser par VirusScan. Vous pouvez ainsi :

   - **Analyser les fichiers compressés.** Cochez la case **Fichiers compressés** pour que VirusScan analyse les fichiers compressés dans les formats suivants: .??_, .CAB, LZEXE, LZH, PKLite, .TD0, et .ZIP. Bien qu'il offre une protection supplémentaire, l'examen des fichiers compressés peut ralentir l'opération d'analyse. Vous pouvez empêcher VirusScan d'analyser ces fichiers en désélectionnant la case **Fichiers compressés**.

   - **Ne pas analyser le secteur d'amorçage.** Normalement, VirusScan analysera votre secteur de partition et les blocs d'amorçage de votre disque dur pour rechercher des virus de secteur d'amorçage. Bien que la plupart des nouveaux virus soient des virus de macro, les virus du secteur d'amorçage continuent à s'étendre et peuvent endommager votre système. Network Associates vous recommande d'analyser régulièrement votre secteur d'amorçage ; cependant, si cela perturbe les opérations du système, cochez la case pour éviter ce type d'opération d'analyse.

   - **Sélectionner les types de fichiers à analyser.** D'ordinaire, les virus ne peuvent infecter les fichiers de données ou les fichiers qui ne contiennent pas de code exécutable. Vous pouvez donc sans risque limiter la portée de vos opérations d'analyse aux fichiers les plus susceptibles d'être infectés par les virus pour les accélérer. Pour cela, cliquez sur le bouton **Fichiers programme uniquement**. Pour voir ou désigner les extensions des noms de fichiers que doit examiner VirusScan, cliquez sur **Types de fichiers** pour ouvrir la boîte de dialogue Extensions des fichiers programme (Figure 6-19).

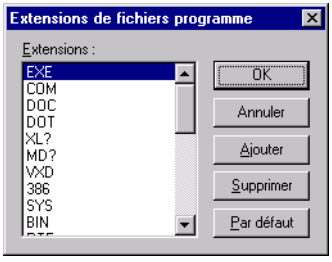



**Figure 6-19. Boîte de dialogue Extensions des fichiers programme**

Par défaut, VirusScan recherche les virus dans les fichiers portant les extensions .EXE, .COM, .DOC?, .DOT, .XL?, .MD?, .VXD, .386, .SYS, .BIN, .RTF, .OBD, .DLL, .SCR, .OBT, .PP .POT, .OLE, .SHS, .MPP, .MPT, .XTP, .XLB, .CMD, .OVL et .DEV. Cette liste comprend presque tous les fichiers susceptibles d'être infectés par des virus de macro, y compris tous les types de fichiers de Microsoft Office. Le caractère ? est un caractère générique qui permet à VirusScan d'examiner les fichiers de même type, tels que les fichiers documents et modèles.

- Pour ajouter des types de fichiers à la liste, cliquez sur **Ajouter**, puis entrez les extensions que VirusScan doit prendre en compte dans la boîte de dialogue qui s'affiche alors.
- Pour supprimer une extension de la liste, sélectionnez-la puis cliquez sur **Supprimer**.
- Cliquez sur **Par défaut** pour revenir à la liste originale.

Lorsque vous avez terminé, cliquez sur **OK** pour refermer la boîte de dialogue.

Pour demander à VirusScan d'examiner tous les fichiers de votre système, quelle que soit leur extension, sélectionnez le bouton **Tous les fichiers**. Ceci ralentit considérablement vos opérations d'analyse, mais vous garantit que votre système est exempt de tout virus.

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, 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 apparaît, puis cliquez sur **Enregistrer**.

## Sélection des options d'action

Lorsque 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 antérieurement. Utilisez la page de propriétés d'Action pour spécifier dans les options ce que VirusScan doit vous retourner lorsqu'il détecte un virus, ou quelles actions il doit mettre en œuvre automatiquement.

**Procédez comme suit :**

1. Cliquez sur l'onglet Action dans la fenêtre VirusScan pour afficher la bonne page de propriétés (Figure 6-20).

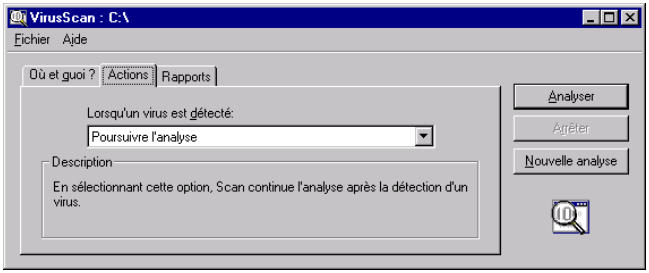



**Figure 6-20. fenêtre VirusScan - Page d'Action**

2. Sélectionnez une réponse dans la liste **Lors de la 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 actions suivantes :

   - **Continuer l'analyse.** N'utilisez cette option que si vous prévoyez d'être absent au moment où VirusScan recherchera les virus. Si vous activez également la fonction de rapport de VirusScan (voir "Sélection des options de rapport" à la page 141 pour plus de détails), le programme enregistrera le nom des virus détectés et le nom des fichiers infectés, pour vous permettre de les supprimer à une prochaine occasion.

   - **Demande d'action.** Utilisez cette option si vous pensez être auprès de votre ordinateur pendant que VirusScan analyse votre disque ; VirusScan affiche un message d'alerte lorsqu'il détecte un virus et vous propose la liste complète des réponses disponibles.

   - **Placer les fichiers infectés dans un dossier**. Utilisez cette option pour que VirusScan déplace les fichiers infectés dans un répertoire de quarantaine dès qu'il les détecte. Par défaut, VirusScan place ces fichiers dans un dossier nommé Infected de son répertoire programme.

     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 les fichiers infectés.** Permet de demander à VirusScan de supprimer le code du virus dans le fichier infecté dès sa détection. Si VirusScan ne parvient pas à supprimer le virus, il notera l'incident dans le fichier journal. Voir "Sélection des options de rapport" à la page 141 pour plus de détails.
- **Supprimer les fichiers infectés.** Utilisez cette option pour que VirusScan supprime tout fichier infecté dès sa détection. Veillez à activer la fonction de rapport pour disposer de la liste des fichiers supprimés par VirusScan. Consultez ensuite cette dernière pour connaître les fichiers supprimés à restaurer à partir des copies de sauvegarde. Si VirusScan ne parvient pas à supprimer un fichier infecté, il notera l'incident dans le fichier journal.

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, 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, VirusScan envoie un message de réseau Windows NT par l'intermédiaire du gestionnaire d'alertes lorsqu'il détecte un virus. Vous pouvez utiliser la page de Rapport pour activer ou désactiver cet envoi de message au gestionnaire d'alertes ou pour ajouter un message d'alerte dans la boîte de dialogue Virus détecté qui apparaît lorsque VirusScan 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 du réseau.

Cette même page permet de déterminer la taille et l'emplacement du fichier journal de VirusScan. Par défaut, le programme présente dans un fichier journal nommé SCANLOG.TXT la liste de ses paramètres en cours ainsi qu'un résumé des actions qu'il a entreprises pendant ses opérations d'analyse. Vous pouvez choisir que VirusScan enregistre ces informations dans ce fichier ou recourir à un éditeur de texte pour créer un fichier texte à cette intention. Vous pouvez par conséquent ouvrir et imprimer le fichier journal pour consultation ultérieure, soit depuis 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 de la fenêtre VirusScan pour afficher la bonne page de propriétés (Figure 6-21).

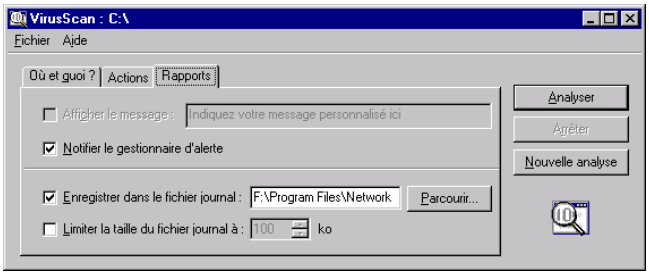



**Figure 6-21. Fenêtre principale de VirusScan - Page de Rapport**

2. Choisissez les méthodes d'alerte que vous souhaitez que VirusScan utilise lorsqu'il détecte un virus. Vous pouvez faire en sorte que VirusScan :

   - **Affiche un message personnalisé.** Cochez la case **Afficher un message personnalisé**, puis entrez dans la zone de texte prévue à cet effet le message que vous voulez voir apparaître. La longueur de votre message ne peut excéder 225 caractères.

     **REMARQUE :** Pour que VirusScan puisse afficher votre message, vous devez avoir sélectionné **Interroger l'utilisateur** comme réponse dans la page d'Action (voir "Sélection des options d'action" à la page 139 pour plus de détails).

   - **Envoyer des messages par l'intermédiaire du gestionnaire d'alertes.** Cochez la case **Avertir le gestionnaire d'alertes** pour que VirusScan envoie des informations au gestionnaire d'alertes qui les transmettra. Le gestionnaire d'alertes vous avertira en employant la méthode que vous lui aurez indiquée.

3. Cochez la case **Consigner dans un fichier**.

   Par défaut, VirusScan enregistre les informations relatives au journal dans le fichier SCANLOG.TXT du répertoire 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.

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.

   Saisissez une valeur comprise entre 10 Ko et 99 999 Ko (100 Mo). Par défaut, VirusScan ne limite pas du tout la taille du fichier. Si les données du journal dépassent la taille allouée pour le fichier, 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 de vos 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, 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**.

# Transmission des messages d'alerte 7

## Utilisation des fonctions d'alerte de VirusScan

Une fois configuré avec les options que vous souhaitez, vous pourrez laisser VirusScan détecter et supprimer automatiquement les virus de votre serveur à mesure qu'il les détectera et n'aurez pratiquement plus à intervenir. Lorsque le journal des activités est activé, il est également possible de voir les résultats de chaque opération d'analyse de VirusScan et de suivre, à votre gré, leur progression, ou bien d'afficher les résultats et les statistiques d'analyse à partir de la console antivirus au moment où vous vous connectez à votre serveur.

Si toutefois vous souhaitez que VirusScan vous informe immédiatement de la détection d'un virus afin de pouvoir prendre les mesures nécessaires, vous pouvez configurer le gestionnaire d'alertes intégré pour qu'il envoie un message d'alerte, à vous ou à d'autres utilisateurs. Vous avez le choix entre plusieurs types d'alerte. Voir "Configuration du gestionnaire d'alertes" ci-dessous pour apprendre comment configurer les types de méthodes d'alerte que vous souhaitez.

VirusScan vous donne par ailleurs un contrôle total sur le contenu de ses messages d'alerte et sur les priorités relatives que vous leur affectez par le biais de la console antivirus. Voir la section "Personnalisation des messages d'alerte" à la page 178 pour apprendre comment créer ou modifier les messages d'alerte afin qu'ils répondent à vos besoins.

## Configuration du gestionnaire d'alertes

VirusScan utilise l'utilitaire gestionnaire d'alertes de Network Associates pour vous avertir de la détection d'un virus sur votre poste de travail. Le gestionnaire d'alertes vous offre une grande variété d'options de notification qui peuvent être employées individuellement ou combinées entre elles pour répondre à vos besoins.

Si le gestionnaire d'alertes est installé sur d'autres ordinateurs ou serveurs de votre réseau, vous pouvez également transmettre les messages d'alerte à ces ordinateurs, qui, à leur tour, peuvent avertir d'autres ordinateurs en fonction de la configuration de votre réseau.

**Astuce:** Dans les grandes organisations, vous pouvez utiliser cette fonction de transmission pour envoyer des alertes à des systèmes de notification centralisée ou à des départements MIS afin de suivre les statistiques relatives aux virus ainsi que les domaines qui posent problème.

Bien que VirusScan soit en mesure d'envoyer des messages vers un système d'alerte centralisée, il ne peut *pas* recevoir ces alertes ni les traiter. Cependant, NetShield NT - le programme associé à VirusScan pour Windows NT Server - est capable d'effectuer ces opérations. Veuillez vous adresser à votre revendeur pour de plus amples informations.

**Pour activer et configurer le gestionnaire d'alertes, procédez comme suit :**

1. Lancez la console antivirus, puis choisissez **Alertes** dans le **menu** Outils. Pour apprendre comment lancer la console antivirus, voir "Démarrage de la console antivirus de VirusScan" à la page 61.

   La page Propriétés d'alerte s'affiche (Figure 7-1).

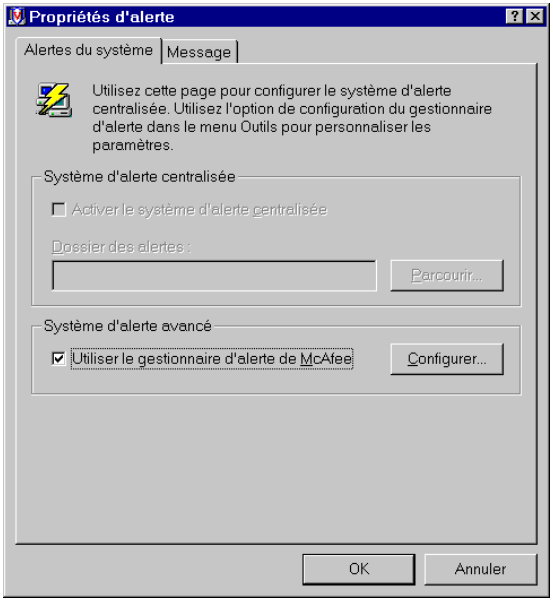



**Figure 7-1. Boîte de dialogue Propriétés d'alerte - Page Alertes système**

2. Vérifiez que la case **Utiliser le gestionnaire d'alertes** est cochée, puis cliquez sur **Configurer** afin d'ouvrir la boîte de dialogue Gestionnaire d'alertes (voir Figure 7-2 à la page 148).

**REMARQUE :** VirusScan ne prend pas en charge la fonction Alerte centralisée présentée ici. Cette fonction est disponible dans NetShield NT, le programme associé à VirusScan pour Windows NT Server.

3. La boîte de dialogue Gestionnaire d'alertes comprend 10 méthodes d'alerte différentes, chacune dotée d'options de configuration présentées dans des pages de propriétés séparées. Cliquez sur l'onglet qui correspond à la méthode d'alerte que vous souhaitez configurer pour afficher les options disponibles. Lorsque vous avez terminé de choisir vos options, cliquez sur **Appliquer** pour enregistrer vos modifications sans fermer la boîte de dialogue Gestionnaire d'alertes. Pour sauvegarder vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans sauvegarder vos modifications, cliquez sur **Annuler**.

   **REMARQUE :** Cliquer sur **Annuler** n'annulera pas les modifications déjà sauvegardées en cliquant sur **Appliquer**.

   Les sections suivantes présentent les options disponibles pour chaque méthode.

## Affichage de la page Résumé

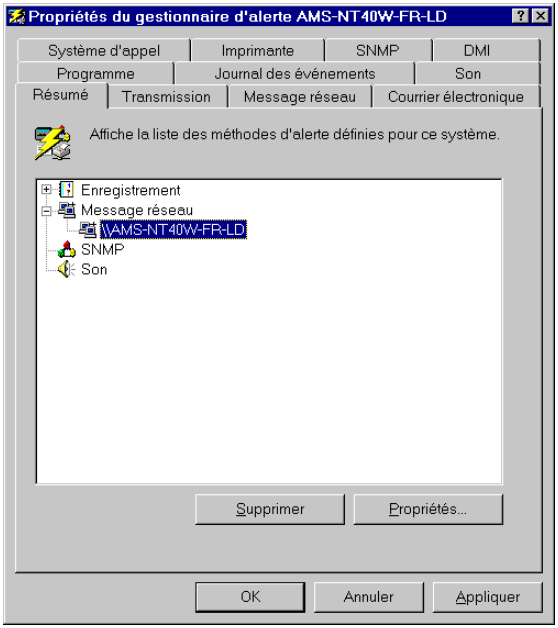



**Figure 7-2. Boîte de dialogue Propriétés du gestionnaire d'alertes - page Résumé**

La page Résumé répertorie l'ensemble des méthodes d'alerte pour l'usage desquelles VirusScan est configuré. Dans l'exemple fourni dans Figure 7-2 à la page 148, les 10 options d'alerte du gestionnaire d'alertes sont toutes configurées et prêtes à être utilisées. Si vous n'avez pas encore configuré le gestionnaire d'alertes, la page Résumé sera vide.

Cliquez sur ⊞ en regard de chaque méthode d'alerte dans la liste pour afficher les ordinateurs, imprimantes, numéros de téléphone, adresses de messagerie et autres méthodes par lesquelles vous recevrez les messages d'alerte de VirusScan. Pour supprimer une méthode d'alerte, sélectionnez-la puis cliquez sur **Supprimer.** Pour modifier les options de configuration d'une méthode répertoriée dans la liste, sélectionnez-la puis cliquez sur **Propriétés.** Le gestionnaire d'alertes ouvre la même page de propriétés que vous avez utilisée pour configurer les options de cette méthode d'alerte.

Reportez-vous aux sections suivantes pour apprendre comment choisir des options pour chaque méthode.

## Transmission des messages d'alerte à d'autres ordinateurs

Le gestionnaire d'alertes peut transmettre les messages d'alerte générés par VirusScan à d'autres ordinateurs de votre réseau. Si le gestionnaire d'alertes est installé sur chacun des ordinateurs destinataires, ces derniers peuvent à leur tour faire suivre les messages d'alerte aux destinataires figurant sur les pages Résumé de leur gestionnaire d'alertes. Il est possible d'utiliser cette fonction pour envoyer des messages d'alerte sur l'ensemble des domaines du réseau ou pour élaborer une hiérarchie gérant l'envoi des messages d'alerte.

### Pour configurer les options de transmission du gestionnaire d'alertes, procédez comme suit :

1. Ouvrez la boîte de dialogue Propriétés du gestionnaire d'alertes.
2. Cliquez sur l'onglet Transmettre.

   La page Transmettre (Figure 7-3 à la page 149) s'affiche et présente une liste de tous les ordinateurs que vous avez désignés pour recevoir les messages transmis. Si vous n'avez pas encore choisi les ordinateurs destinataires, cette liste sera vide.

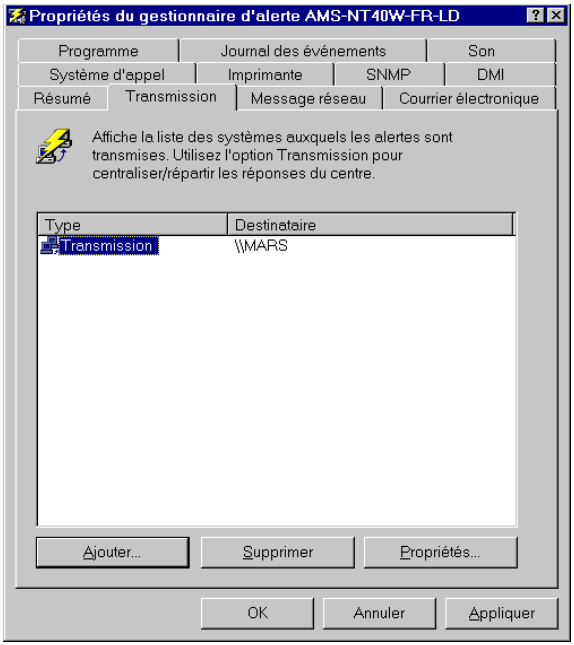



**Figure 7-3. Boîte de dialogue Propriétés du gestionnaire d'alertes - page Transmettre**

3. Pour mettre à jour cette liste, vous pouvez :

   - **Supprimer un ordinateur.** Sélectionnez un des ordinateurs destinataires de la lise, puis cliquez sur **Supprimer.**
   - **Ajouter un ordinateur.** Cliquez sur **Ajouter** pour ouvrir la boîte de dialogue Propriétés de transmission (Figure 7-4 à la page 150), puis saisissez le nom de l'ordinateur qui recevra les messages que vous transmettrez dans la zone de texte prévue à cet effet. Vous pouvez saisir le nom de l'ordinateur en respectant la notation de la convention d'affectation des noms (UNC), ou cliquer sur **Parcourir** pour localiser l'ordinateur sur votre réseau. Pour sélectionner des options supplémentaires, passez à Étape 4.
   - **Modifier les options de configuration.** Sélectionnez un des ordinateurs destinataires de la liste, puis cliquez sur **Propriétés.** Le gestionnaire d'alertes ouvre la boîte de dialogue Propriétés de transmission (voir Figure 7-4 à la page 150). Modifiez éventuellement des informations dans la zone de texte Ordinateur, puis passez à Étape 4 pour apprendre comment choisir des options de configuration nouvelles ou différentes.

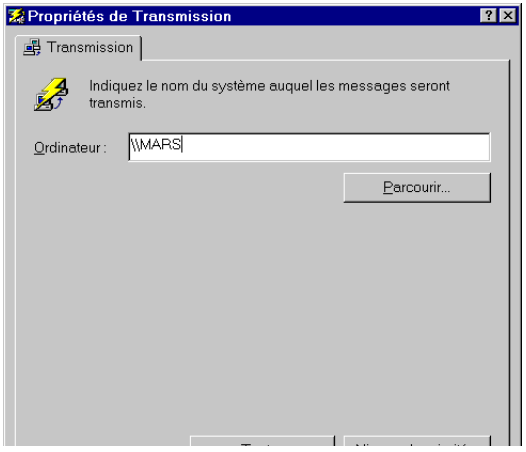



**Figure 7-4. Boîte de dialogue Propriétés de transmission**

4. Cliquez sur **Niveau de priorité** pour indiquer quels types de messages d'alerte l'ordinateur destinataire recevra.

Dans la boîte de dialogue Niveau de priorité qui s'affiche (Figure 7-5), faites glisser le curseur vers la droite afin d'envoyer à l'ordinateur destinataire un nombre de messages réduit mais dotés d'un niveau de priorité plus élevé. Faites glisser le curseur sur la gauche pour envoyer à l'ordinateur destinataire un nombre plus important de messages, y compris ceux dotés d'un niveau de priorité moins élevé. Cliquez sur **OK** pour enregistrer vos modifications et revenir à la boîte de dialogue Propriétés de transmission. Pour apprendre comment paramétrer les niveaux de priorité pour les différents types de message, voir "Personnalisation des messages d'alerte" à la page 178.

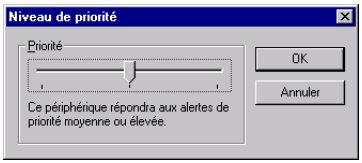



**Figure 7-5. Boîte de dialogue Niveau de priorité**

5. Cliquez sur **Tester** pour envoyer à l'ordinateur destinataire un message test. Ce message s'affichera instantanément dans une boîte de dialogue sur l'écran de l'ordinateur destinataire. Le destinataire devra cliquer sur **OK** pour accuser réception du message.

6. Cliquez sur **OK** pour revenir à la boîte de dialogue Gestionnaire d'alertes.

7. Pour configurer d'autres options de notification, cliquez sur un autre onglet. Pour enregistrer vos modifications sans fermer la boîte de dialogue Gestionnaire d'alertes, cliquez sur **Appliquer**. Pour sauvegarder vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans sauvegarder vos modifications, cliquez sur **Annuler**.

> **REMARQUE :** Cliquer sur **Annuler** n'annulera pas les modifications déjà sauvegardées en cliquant sur **Appliquer**.

## Envoi d'alertes comme messages de réseau

Le gestionnaire d'alertes peut envoyer les messages d'alerte générés par VirusScan à d'autres ordinateurs ou utilisateurs de votre réseau par le biais d'un message diffusé par le réseau Windows NT standard. Le message d'alerte s'affiche sur l'écran de l'ordinateur destinataire, et le destinataire doit en accuser réception.

Le service Windows NT Messenger doit être exécuté sur les ordinateurs destinataires afin de pouvoir recevoir les messages d'alerte. Ceux qui fonctionnent sous Windows 95 ou Windows 3.1x doivent également exécuter l'utilitaire WinPopup afin de recevoir les messages de réseau. WinPopup est inclus dans certaines versions de Windows. Consultez votre documentation Windows pour de plus amples informations.

**Pour transmettre des alertes sous forme de messages de réseau, procédez comme suit :**

1. Ouvrez la boîte de dialogue Propriétés du gestionnaire d'alertes.
2. Cliquez sur l'onglet Message de réseau.

La page Message de réseau s'affiche et présente la liste des ordinateurs ou des noms d'utilisateur que vous avez configurés pour recevoir des messages de réseau (Figure 7-6). Si vous n'avez pas encore choisi un ordinateur ou un utilisateur destinataire, cette liste sera vide.

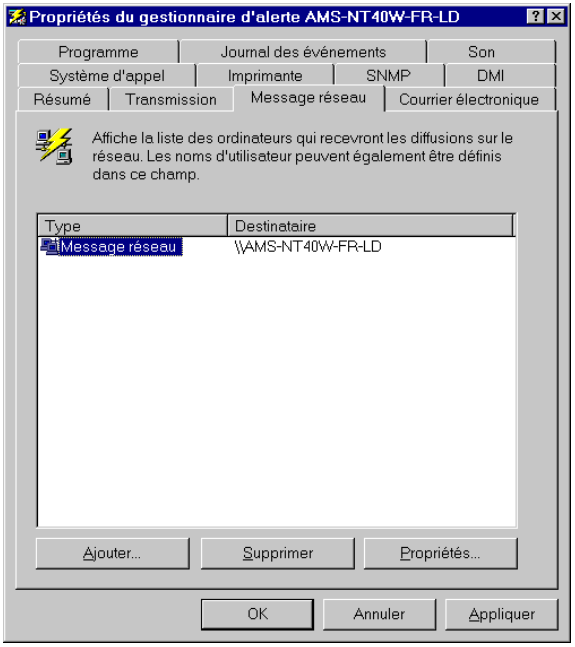



**Figure 7-6. Boîte de dialogue Propriétés du gestionnaire d'alertes - page Message de réseau**

3. Pour mettre à jour cette liste, vous pouvez :

   - **Supprimer un ordinateur ou un utilisateur**. Sélectionnez un des utilisateurs ou un des ordinateurs destinataires figurant sur la liste, puis cliquez sur **Supprimer**.

   - **Ajouter un ordinateur ou un utilisateur.** Cliquez sur **Ajouter** pour ouvrir la boîte de dialogue Propriétés des messages de réseau (Figure 7-7 à la page 154), puis saisissez le nom de l'utilisateur ou de l'ordinateur destinataire dans la zone de texte prévue à cet effet. Vous pouvez saisir le nom de l'ordinateur en respectant la notation de la convention d'affectation des noms (UNC), ou cliquez sur **Parcourir** pour localiser l'ordinateur sur le réseau. Pour sélectionner des options supplémentaires, passez à Étape 4.

> **REMARQUE :** Si la destination spécifiée est à la fois un nom d'utilisateur et un ordinateur, le gestionnaire d'alertes enverra le message à l'utilisateur.

- **Modifier les options de configuration.** Sélectionnez un des utilisateurs ou un des ordinateurs destinataires figurant dans la liste, puis cliquez sur **Propriétés**. Le gestionnaire d'alertes ouvre la boîte de dialogue Propriétés des messages de réseau (Figure 7-7). Modifiez éventuellement des informations dans la zone de texte Ordinateur, puis passez à Étape 4.

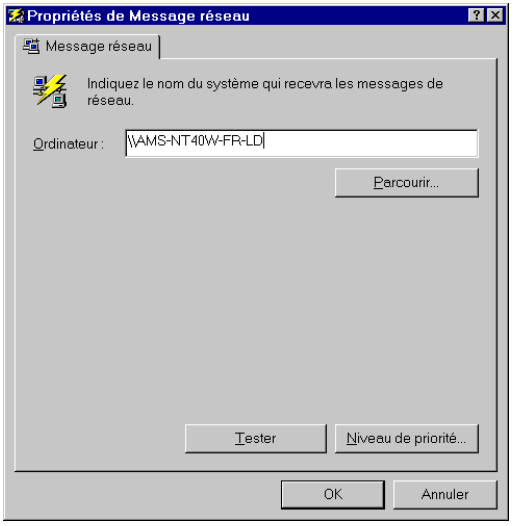



**Figure 7-7. Boîte de dialogue Propriétés des messages de réseau**

4. Cliquez sur **Niveau de priorité** afin de spécifier les types de messages d'alerte que l'utilisateur ou l'ordinateur destinataire recevra.

   Dans la boîte de dialogue Niveau de priorité (voir Figure 7-5 à la page 151), faites glisser le curseur vers la droite pour envoyer à l'ordinateur ou à l'utilisateur destinataire un nombre réduit de messages, mais dotés d'un niveau de priorité plus élevé. Faites glisser le curseur vers la gauche pour envoyer à l'ordinateur ou à l'utilisateur destinataire un nombre de messages plus important, y compris ceux dotés d'un niveau de priorité moins élevé. Cliquez sur **OK** pour enregistrer vos modifications et revenir à la boîte de dialogue Propriétés des messages de réseau.

Pour apprendre comment paramétrer les niveaux de priorité pour les différents types de messages, voir "Personnalisation des messages d'alerte" à la page 178.

5. Cliquez sur **Tester** pour envoyer à l'ordinateur ou à l'utilisateur destinataire un message test.

   Ce message s'affichera instantanément dans une boîte de dialogue sur l'écran de l'ordinateur destinataire. Le destinataire devra cliquer sur **OK** pour accuser réception du message. Si votre destinataire ne reçoit pas le message, vérifiez qu'un message d'erreur n'apparaisse pas sur la visionneuse d'événements de Windows NT.

6. Cliquez sur **OK** pour revenir à la boîte de dialogue Propriétés du gestionnaire d'alertes.

7. Pour configurer d'autres options de notification, cliquez sur un autre onglet. Pour enregistrer vos modifications sans fermer la boîte de dialogue Gestionnaire d'alertes, cliquez sur **Appliquer**. Pour sauvegarder vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans sauvegarder vos modifications, cliquez sur **Annuler**.

   ❑ **REMARQUE :** Cliquer sur **Annuler** n'annulera pas les modifications déjà sauvegardées en cliquant sur **Appliquer**.

## Envoi de messages d'alerte à des adresses de messagerie

Le gestionnaire d'alertes peut envoyer les messages d'alerte générés par VirusScan à l'adresse de messagerie d'un destinataire par le biais des services de messagerie standard, Simple Mail Transfer Protocol (SMTP). Les messages d'alerte apparaissent dans la boîte aux lettres électronique du destinataire. Si votre message est particulièrement urgent, il est préférable d'utiliser d'autres méthodes d'envoi en plus du courrier électronique afin d'être certain que votre destinataire voie l'alerte à temps et prenne les mesures qui s'imposent.

**Pour envoyer des alertes par courrier électronique, procédez comme suit :**

1. Ouvrez la boîte de dialogue Propriétés du gestionnaire d'alertes.
2. Cliquez sur l'onglet Courrier électronique.

La page Courrier électronique s'affiche et présente une liste des adresses de messagerie que vous avez choisies pour recevoir les messages d'alerte (Figure 7-8). Si vous n'avez pas encore choisi d'adresse de messagerie, cette liste sera vide.

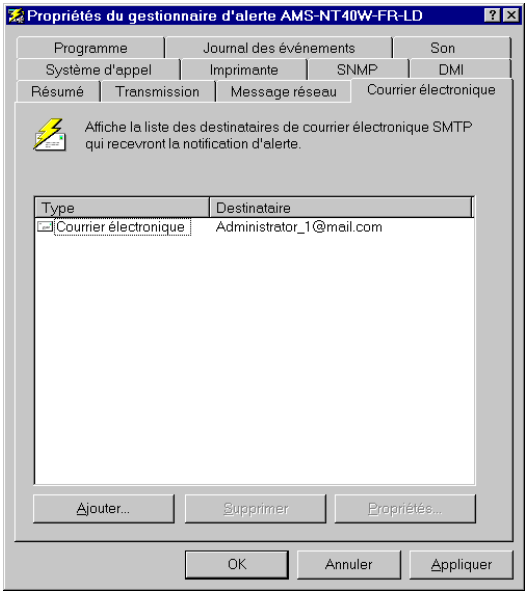



**Figure 7-8. Boîte de dialogue Propriétés du gestionnaire d'alertes - page Courrier électronique**

3. Pour mettre à jour cette liste, vous pouvez :

   - **Supprimer une adresse.** Sélectionnez une des adresses de messagerie figurant sur la liste, puis cliquez sur **Supprimer.**
   - **Ajouter une adresse de messagerie.** Cliquez sur **Ajouter** pour ouvrir la boîte de dialogue Propriétés du courrier électronique (Figure 7-9 à la page 157). Saisissez l'adresse de messagerie de votre destinataire dans la zone de texte Adresse, saisissez l'objet de votre message dans la zone de texte Sujet, puis saisissez votre adresse de messagerie dans la zone de texte Expéditeur. Utilisez le format d'adresse Internet standard <*nomdutilisateur*>@<*domaine*> (admin@mondomaine.com, par exemple). Pour sélectionner des options supplémentaires, passez à Étape 4.

- **Modifier les options de configuration.** Sélectionnez une des adresses de messagerie figurant dans la liste, puis cliquez sur **Propriétés.** Le gestionnaire d'alertes ouvre la boîte de dialogue Propriétés du courrier électronique (Figure 7-9 à la page 157). Modifiez éventuellement les informations dans les zones de texte prévues à cet effet, puis passez à Étape 4 pour apprendre comment choisir des options de configuration nouvelles ou différentes.

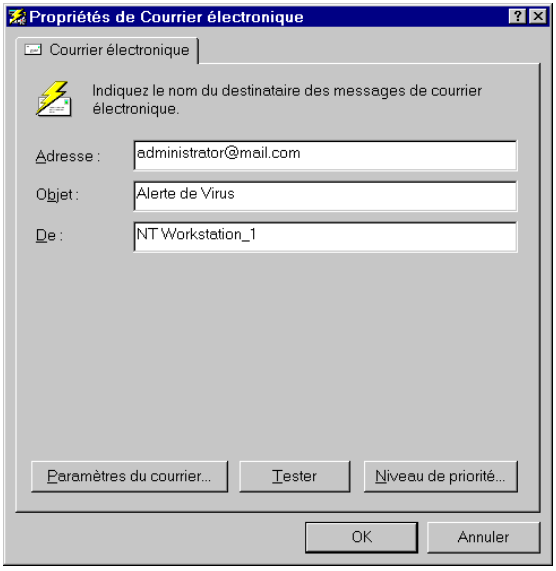



**Figure 7-9. Boîte de dialogue Propriétés du courrier électronique**

4. Cliquez sur **Niveau de priorité** pour spécifier quels types de messages d'alerte votre destinataire recevra.

   Dans la boîte de dialogue Niveau de priorité (voir Figure 7-5 à la page 151), faites glisser le curseur vers la droite afin d'envoyer au destinataire un nombre réduit de messages, mais dotés d'un niveau de priorité plus élevé. Faites glisser le curseur vers la gauche pour envoyer au destinataire un nombre de messages plus important, y compris ceux dotés d'un niveau de priorité moins élevé. Cliquez sur **OK** pour enregistrer vos modifications et revenir à la boîte de dialogue Propriétés du courrier électronique.

   Pour apprendre comment paramétrer les niveaux de priorité pour les différents types de messages, voir "Personnalisation des messages d'alerte" à la page 178.

5. Cliquez sur **Paramètres du courrier** pour spécifier le serveur SMTP que vous utilisez pour envoyer du courrier sur Internet. Dans la boîte de dialogue qui s'affiche (Figure 7-10 à la page 158), saisissez le nom du serveur dans la zone de texte Serveur et entrez dans la zone de texte Connexion un nom d'utilisateur correspondant à un compte de courrier actif que VirusScan peut utiliser pour se connecter au serveur.

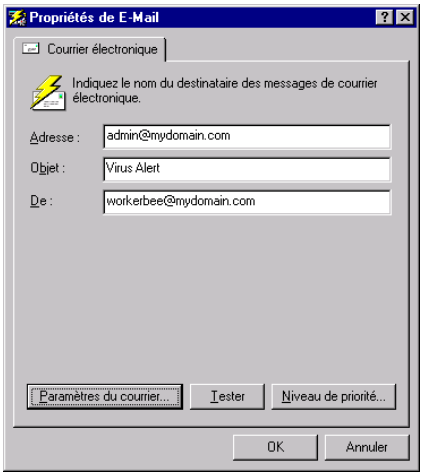



**Figure 7-10. Boîte de dialogue Paramètres de courrier**

Vous pouvez saisir le nom du serveur sous la forme d'une adresse Internet Protocol (IP), d'un nom reconnu par votre domaine local, ou en respectant la notation de la convention d'affectation des noms (UNC). Cliquez sur **OK** pour enregistrer vos modifications et revenir à la boîte de dialogue Propriétés du courrier électronique.

6. Cliquez sur **Tester** pour envoyer un message test à l'adresse de messagerie que vous avez saisie. Le message apparaîtra dans la boîte aux lettres de votre destinataire.

7. Cliquez sur **OK** pour revenir à la boîte de dialogue Propriétés du gestionnaire d'alertes.

8. Pour configurer d'autres options de notification, cliquez sur un autre onglet. Pour enregistrer vos modifications sans fermer la boîte de dialogue Gestionnaire d'alertes, cliquez sur **Appliquer**. Pour sauvegarder vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans sauvegarder vos modifications, cliquez sur **Annuler**.

---

**REMARQUE :** Cliquer sur **Annuler** n'annulera pas les modifications déjà sauvegardées en cliquant sur **Appliquer**.

---

## Envoi de messages d'alerte à des récepteurs d'appels

Le gestionnaire d'alertes peut envoyer les messages d'alerte générés par VirusScan sur le récepteur d'appels d'un destinataire, à condition que vous ayez un modem et une ligne téléphonique reliés à votre poste de travail. Le gestionnaire d'alertes prend en charge les récepteurs d'appels alphanumériques et ceux qui ne peuvent recevoir que des messages numériques. En fonction du mode de fonctionnement du service de réception d'appels de votre destinataire, il peut s'avérer indispensable de rédiger un script personnalisé pour composer et sélectionner les options de menu adéquates avant que VirusScan ne soit en mesure de transmettre son message.

**Pour envoyer des messages d'alerte à un récepteur d'appels, procédez comme suit :**

1. Ouvrez la boîte de dialogue Propriétés du gestionnaire d'alertes.
2. Cliquez sur l'onglet Récepteur d'appels.

   La page Récepteur d'appels (Figure 7-11) s'affiche et présente une liste des numéros des récepteurs d'appels que vous avez choisis pour recevoir les messages d'alerte. Si vous n'avez pas encore choisi un numéro de récepteur d'appels, cette liste sera vide.

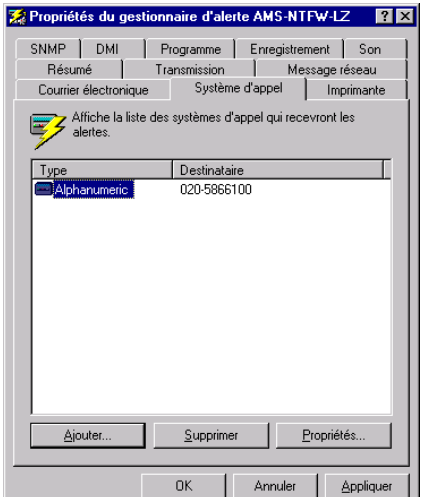



**Figure 7-11. Boîte de dialogue Propriétés du gestionnaire d'alertes - page Récepteur d'appels**

3. Pour mettre à jour cette liste, vous pouvez :

   - **Supprimer un numéro de récepteur d'appels.** Sélectionnez un des numéros de récepteur d'appels dans la liste, puis cliquez sur **Supprimer.**

   - **Ajouter un numéro de récepteur d'appels à la liste.** Cliquez sur **Ajouter** pour ouvrir la boîte de dialogue Propriétés du récepteur d'appels (voir Figure 7-12 à la page 161). Choisissez le type de récepteur d'appels utilisé par votre destinataire dans la liste qui se trouve en haut de la page, puis saisissez les informations le concernant dans les zones de texte prévues à cet effet.

     – Si votre destinataire utilise un récepteur d'appels alphanumérique, saisissez le numéro du récepteur d'appels et, le cas échéant, l'ID et le mot de passe du destinataire dans les zones de texte prévues à cet effet. Ensuite, sélectionnez le bouton **Utiliser le message d'alerte** pour envoyer le message d'alerte standard de VirusScan ou le bouton **Utiliser un message personnalisé** , puis saisissez votre message personnalisé dans la zone de texte figurant en-dessous.

     – Si votre destinataire utilise un récepteur d'appels numérique, saisissez le numéro du récepteur d'appels et le message numérique que vous souhaitez transmettre dans les zones de texte prévues à cet effet. Ensuite, saisissez la durée en secondes pendant laquelle le gestionnaire d'alertes doit attendre avant d'envoyer son message dans la case Retarder.

       Laissez au gestionnaire d'alertes suffisamment de temps pour permettre au service de réception d'appels d'achever d'afficher les messages de bienvenue et les autres messages préliminaires avant d'accepter les messages. Si le service requiert une numérotation au clavier pour activer les options de menu, il peut s'avérer indispensable de rédiger un script de connexion à utiliser avec votre modem.

     Pour sélectionner des options supplémentaires, passez à Étape 4.

   - **Modifier les options de configuration.** Sélectionnez un des numéros des récepteurs d'appel de la liste, puis cliquez sur **Propriétés.** Le gestionnaire d'alertes ouvre la boîte de dialogue Propriétés du récepteur d'appels (Figure 7-12 à la page 161). Modifiez éventuellement les informations dans les zones de texte prévues à cet effet, puis passez à Étape 4 pour apprendre comment choisir des options de configuration nouvelles ou différentes.

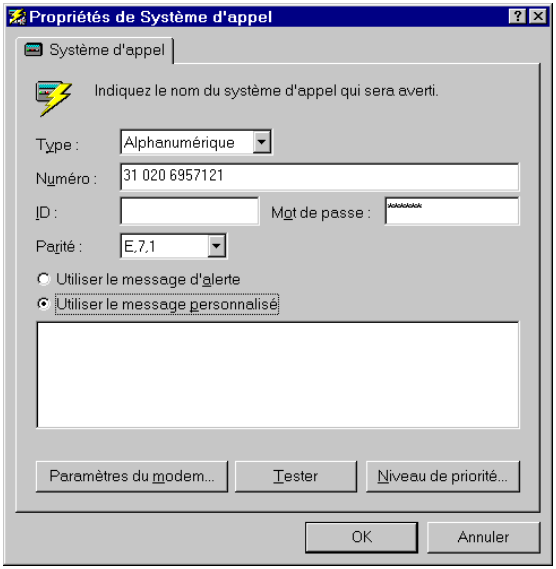



**Figure 7-12. boîte de dialogue Propriétés du récepteur d'appels**

4. Cliquez sur **Niveau de priorité** afin de spécifier quels types de messages d'alerte votre destinataire recevra.

   Dans la boîte de dialogue Niveau de priorité (voir Figure 7-5 à la page 151), faites glisser le curseur vers la droite afin d'envoyer au destinataire un nombre réduit de messages, mais dotés d'un niveau de priorité plus élevé. Faites glisser le curseur vers la gauche pour envoyer au destinataire un nombre de messages plus important, y compris ceux dotés d'un niveau de priorité moins élevé. Cliquez sur **OK** pour sauvegarder vos choix et revenir à la boîte de dialogue Propriétés du récepteur d'appels.

   Pour apprendre comment paramétrer les niveaux de priorité pour les différents types de messages, voir "Personnalisation des messages d'alerte" à la page 178.

5. Cliquez sur **Paramètres du modem** pour configurer votre modem afin qu'il envoie des messages à des récepteurs d'appels. Dans la boîte de dialogue qui s'affiche (Figure 7-13 à la page 162), choisissez le type de modem connecté à votre serveur dans la liste Modem, le port COM qu'il utilise dans la liste Port, et la vitesse à laquelle il peut transmettre les données dans la liste Baud. Puis, saisissez dans les zones de texte prévues à cet effet tous les préfixes ou suffixes de numérotation que le modem doit composer afin de se relier aux lignes extérieures, utiliser des porteuses longue-distance particulières, saisir des numéros d'identification ou effectuer des tâches similaires.

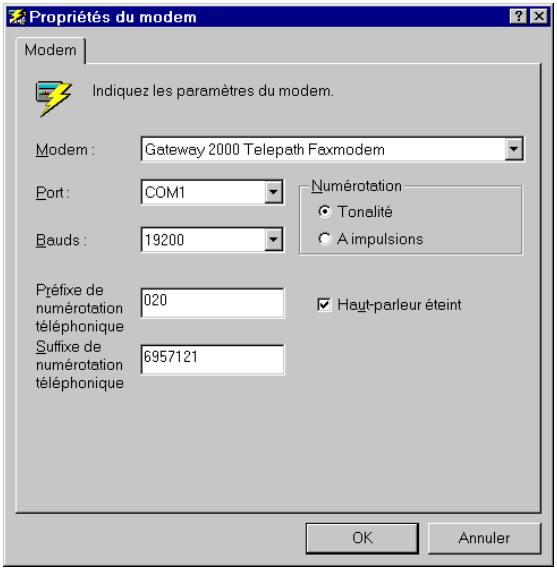



**Figure 7-13. Boîte de dialogue Propriétés du modem**

Choisissez la méthode de numérotation - **Par tonalité** ou **Par impulsion** - que vous souhaitez que le modem utilise et cochez la case **Haut-parleur éteint** afin que le modem compose un numéro et se connecte en silence. Cliquez sur **OK** pour sauvegarder vos modifications et revenir à la boîte de dialogue Propriétés du récepteur d'appels.

6. Cliquez sur **Tester** pour envoyer un message test au numéro de récepteur d'appels que vous avez saisi. Si votre destinataire utilise un récepteur d'appels alphanumérique, il recevra un message texte transmis par le gestionnaire d'alertes. Si votre destinataire utilise un récepteur d'appels numérique, il verra s'afficher le numéro de téléphone ou le message que vous aurez indiqué dans la boîte de dialogue Propriétés du récepteur d'appels.

7. Cliquez sur **OK** pour revenir à la boîte de dialogue Propriétés du gestionnaire d'alertes.

8. Pour configurer d'autres options de notification, cliquez sur un autre onglet. Pour enregistrer vos modifications sans fermer la boîte de dialogue Gestionnaire d'alertes, cliquez sur **Appliquer**. Pour sauvegarder vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans sauvegarder vos modifications, cliquez sur **Annuler**.

**REMARQUE :** Cliquer sur **Annuler** n'annulera pas les modifications déjà sauvegardées en cliquant sur **Appliquer**.

## Envoi de messages d'alerte à une imprimante

Le gestionnaire d'alertes peut envoyer les messages d'alerte générés par VirusScan sous la forme d'une tâche d'impression à effectuer par votre imprimante ou votre serveur d'impression. Pour utiliser cette option, vous devez d'abord configurer votre imprimante avec Windows NT et choisir le gestionnaire d'impression adapté à votre imprimante cible. Consultez votre documentation Windows NT pour de plus amples informations.

**Pour configurer le gestionnaire d'alertes afin qu'il envoie des messages à une imprimante, procédez comme suit :**

1. Ouvrez la boîte de dialogue Propriétés du gestionnaire d'alertes.
2. Cliquez sur l'onglet Imprimante.

   La page Imprimante (Figure 7-14) s'affiche et présente une liste de toutes les imprimantes que vous avez configurées pour recevoir des messages d'alerte. Si vous n'avez pas encore choisi d'imprimante, cette liste sera vide.

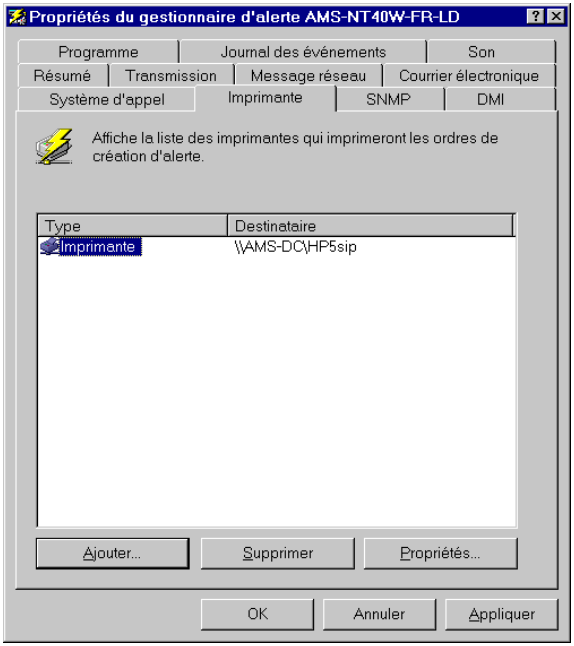



**Figure 7-14. Boîte de dialogue Propriétés du gestionnaire d'alertes - page Imprimante**

3. Pour mettre à jour cette liste, vous pouvez :

   - **Supprimer une imprimante.** Sélectionnez une des imprimantes de la liste, puis cliquez sur **Supprimer.**
   - **Ajouter une imprimante.** Cliquez sur **Ajouter** pour ouvrir la boîte de dialogue Propriétés de l'imprimante (voir Figure 7-15), puis saisissez le nom de l'imprimante cible dans la zone de texte prévue à cet effet ou cliquez sur **Parcourir** pour localiser l'imprimante sur le réseau. Pour choisir des options supplémentaires, passez à Étape 4.
   - **Modifier les options de configuration.** Sélectionnez une des files d'attente d'imprimante dans la liste, puis cliquez sur **Propriétés.** Le gestionnaire d'alertes ouvre la boîte de dialogue Propriétés de l'imprimante (Figure 7-15). Modifiez éventuellement les informations dans la zone de texte **Imprimante,** puis passez à Étape 4 pour apprendre comment choisir des options de configuration nouvelles ou différentes.

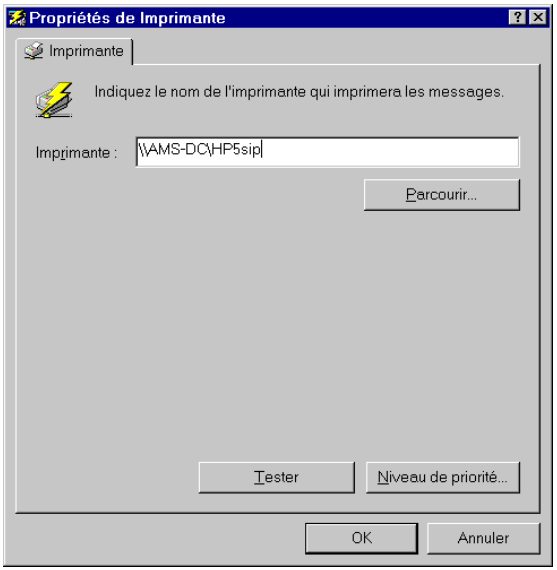



**Figure 7-15. Boîte de dialogue Propriétés de l'imprimante**

4. Cliquez sur **Niveau de priorité** afin de spécifier quels types de messages d'alerte l'imprimante destinataire recevra.

   Dans la boîte de dialogue Niveau de priorité (voir Figure 7-5 à la page 151), faites glisser le curseur vers la droite afin d'envoyer à l'imprimante destinataire un nombre réduit de messages, mais dotés d'un niveau de priorité plus élevé. Faites glisser le curseur vers la gauche pour envoyer à l'imprimante destinataire un nombre plus important de messages de réseau, y compris ceux dotés d'un niveau de priorité moins élevé. Cliquez sur **OK** pour sauvegarder vos modifications et revenir à la boîte de dialogue Propriétés de l'imprimante.

   Pour apprendre comment paramétrer les niveaux de priorité pour les différents types de messages, voir "Personnalisation des messages d'alerte" à la page 178.

5. Cliquez sur **Tester** pour envoyer un message test à l'imprimante destinataire. Ce message s'imprimera sous la forme d'une ligne de texte simple, sans mise en forme.

6. Cliquez sur **OK** pour revenir à la boîte de dialogue Propriétés du gestionnaire d'alertes.

7. Pour configurer d'autres options de notification, cliquez sur un autre onglet. Pour enregistrer vos modifications sans fermer la boîte de dialogue Propriétés du gestionnaire d'alertes, cliquez sur **Appliquer**. Pour sauvegarder vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans sauvegarder vos modifications, cliquez sur **Annuler**.

> ❑ **REMARQUE :** Cliquer sur **Annuler** n'annulera pas les modifications déjà sauvegardées en cliquant sur **Appliquer**.

## Envoi de messages d'alerte via le protocole SNMP

Le gestionnaire d'alertes peut envoyer les messages d'alerte générés par VirusScan à d'autres ordinateurs via le protocole SNMP. Pour visualiser les messages d'alerte envoyés par VirusScan, vous devez disposer d'un système de gestion SNMP configuré avec une visionneuse SNMP, tel que OpenView de Hewlett-Packard. Pour apprendre comment installer et configurer votre visionneuse SNMP, voir la documentation de votre logiciel de gestion.

**Pour configurer VirusScan afin qu'il envoie des messages d'alerte via SNMP, procédez comme suit :**

1. Ouvrez la boîte de dialogue Propriétés du gestionnaire d'alertes.
2. Cliquez sur l'onglet SNMP.

La page SNMP (Figure 7-16) s'affiche.

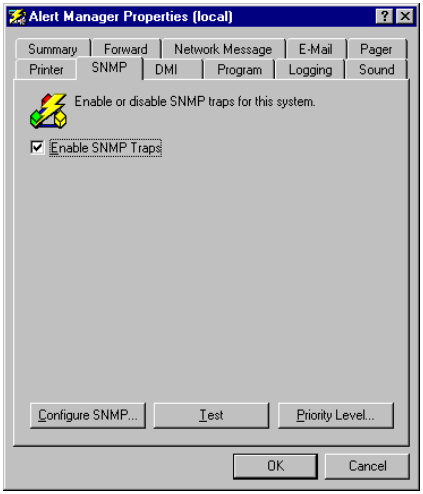



**Figure 7-16. Boîte de dialogue Propriétés du gestionnaire d'alertes - page SNMP**

3. Cochez la case **Activer les filtres SNMP**.

4. Cliquez sur **Niveau de priorité** afin de spécifier quels types de messages d'alerte votre ordinateur de gestion SNMP recevra.

   Dans la boîte de dialogue Niveau de priorité (voir Figure 7-5 à la page 151), faites glisser le curseur vers la droite pour envoyer à l'ordinateur SNMP un nombre réduit de messages, mais dotés d'un niveau de priorité plus élevé. Faites glisser le curseur vers la gauche pour envoyer à l'ordinateur SNMP un nombre plus important de messages, y compris ceux dotés d'un niveau de priorité moins élevé. Cliquez sur **OK** pour enregistrer vos modifications et revenir à la boîte de dialogue Propriétés du gestionnaire d'alertes.

   Pour apprendre comment paramétrer les niveaux de priorité pour les différents types de messages, voir "Personnalisation des messages d'alerte" à la page 178.

5. Pour activer l'alerte SNMP, vous devez installer et activer le protocole SNMP sur votre poste de travail. Si vous n'avez pas encore configuré ce service, cliquez sur **Configurer le SNMP** pour ouvrir le panneau de configuration réseau de Windows NT. Cliquez sur l'onglet Services, puis sur **Ajouter** pour ajouter le service SNMP. Consultez votre documentation Windows NT pour de plus amples informations concernant la configuration.

6. Cliquez sur **Tester** pour envoyer un message test à l'ordinateur SNMP.
7. Cliquez sur **OK** pour revenir à la boîte de dialogue Propriétés du gestionnaire d'alertes.
8. Pour configurer d'autres options de notification, cliquez sur un autre onglet. Pour enregistrer vos modifications sans fermer la boîte de dialogue Gestionnaire d'alertes, cliquez sur **Appliquer**. Pour sauvegarder vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans sauvegarder vos modifications, cliquez sur **Annuler**.

> ❑ **REMARQUE :** Cliquer sur **Annuler** n'annulera pas les modifications déjà sauvegardées en cliquant sur **Appliquer**.

## Envoyer des messages d'alerte via l'interface DMI

Le gestionnaire d'alertes peut envoyer les messages d'alerte générés par VirusScan à d'autres ordinateurs via l'interface DMI. L'interface DMI est une norme multi-plateforme de communication des requêtes d'administration et des informations d'alerte entre éléments matériels et logiciels connectés à ou stockés sur les ordinateurs individuels et les applications utilisées pour les gérer.

Pour utiliser cette méthode d'alerte, vous devez disposer d'un logiciel d'administration DMI installé et configuré sur votre réseau. Pour plus de détails, consultez la documentation de cet autre logiciel DMI.

> ❑ **REMARQUE :** Pour en savoir plus sur la norme DMI, consultez le site Web des spécialistes de la gestion des ordinateurs personnels à l'adresse http://www.dtmf.org

**Pour configurer VirusScan afin qu'il envoie des messages d'alerte via l'interface DMI, procédez comme suit :**

1. Ouvrez la boîte de dialogue Propriétés du gestionnaire d'alertes.
2. Cliquez sur l'onglet Interface DMI.

   La page Interface DMI (Figure 7-17) s'affiche.

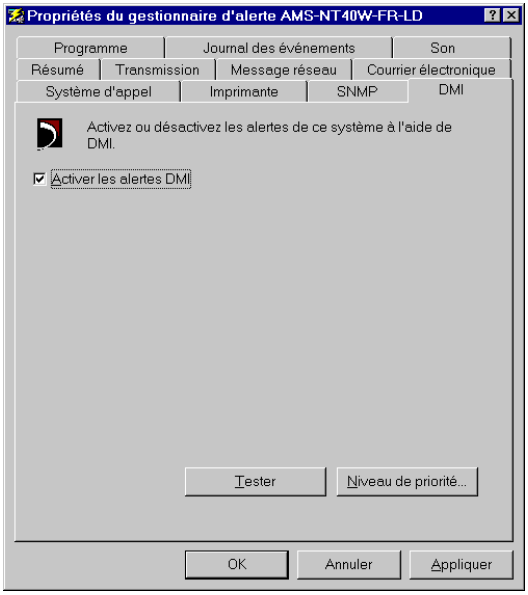



**Figure 7-17. Boîte de dialogue Propriétés du gestionnaire d'alertes - page Interface DMI**

3. Cochez la case **Activer les alertes DMI**.

4. Cliquez sur **Niveau de priorité** afin de spécifier quels types de messages d'alerte votre logiciel d'administration DMI recevra.

   Dans la boîte de dialogue Niveau de priorité (voir Figure 7-5 à la page 151), faites glisser le curseur vers la droite pour envoyer au logiciel DMI un nombre réduit de messages, mais dotés d'un niveau de priorité plus élevé. Faites glisser le curseur vers la gauche pour envoyer au logiciel DMI un nombre plus important de messages d'alerte, y compris ceux dotés d'un niveau de priorité moins élevé. Cliquez sur **OK** pour enregistrer vos modifications et revenir à la boîte de dialogue Gestionnaire d'alertes.

   Pour apprendre comment paramétrer les niveaux de priorité pour les différents types de messages, voir "Personnalisation des messages d'alerte" à la page 178.

5. Cliquez sur **Tester** pour envoyer un message test à votre logiciel DMI.

6. Cliquez sur **OK** pour revenir à la boîte de dialogue Propriétés du gestionnaire d'alertes.

7. Pour configurer d'autres options de notification, cliquez sur un autre onglet. Pour enregistrer vos modifications sans fermer la boîte de dialogue Gestionnaire d'alertes, cliquez sur **Appliquer**. Pour sauvegarder vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans sauvegarder vos modifications, cliquez sur **Annuler**.

> ❑ **REMARQUE :** Cliquer sur **Annuler** n'annulera pas les modifications déjà sauvegardées en cliquant sur **Appliquer**.

## Lancement d'un programme pour envoyer une alerte

Le gestionnaire d'alertes peut vous prévenir de la détection d'un virus lors du lancement d'un programme ou de l'exécution d'un fichier d'automatisation des tâches sur votre réseau. Par exemple, si votre entreprise utilise cc:Mail ou un programme de courrier spécial que VirusScan ne supporte pas directement, vous pouvez écrire un fichier d'automatisation des tâches qui enverra les messages d'alerte vers votre programme de courrier afin qu'il le délivre.

> ❑ **REMARQUE :** Tout programme lancé par le gestionnaire d'alertes s'exécutera en arrière-plan sans apparaître sur une interface utilisateur.

**Pour exécuter un programme lors de la détection d'un virus par VirusScan, procédez comme suit :**

1. Ouvrez la boîte de dialogue Propriétés du gestionnaire d'alertes.
2. Cliquez sur l'onglet Programme.

   La page Programme (Figure 7-18) s'affiche.

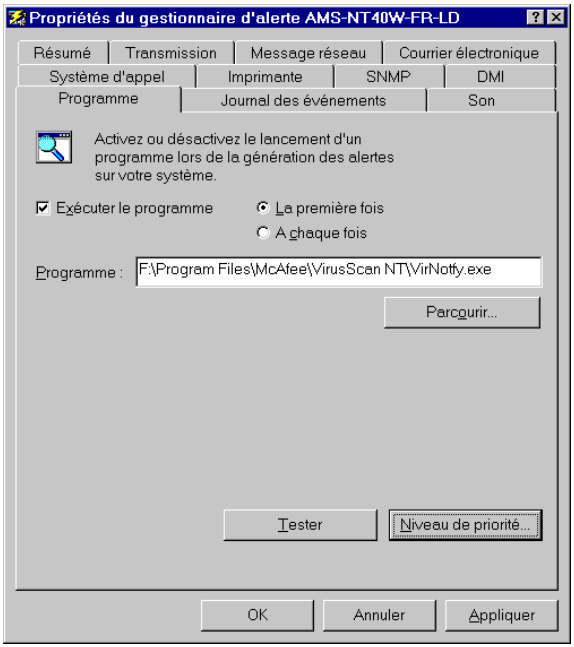



**Figure 7-18. Boîte de dialogue Propriétés du gestionnaire d'alertes - page Programme**

3. Saisissez le nom et le chemin d'accès du programme que VirusScan doit exécuter lorsqu'il détecte un virus, ou cliquez sur **Parcourir** pour localiser le fichier programme sur le réseau.

   Par défaut, le gestionnaire d'alertes exécute le programme VIRNOTFY.EXE depuis le répertoire de programme VirusScan. Ce programme s'exécute sans avoir recours à une interface, et ne reçoit des données qu'à partir de VirusScan par le biais de deux variables :

   - %DANSNOMFICHIER% - Cette variable identifie l'emplacement du fichier infecté, y compris le chemin pour y accéder.
   - %NOMVIRUS% - Cette variable identifie le virus responsable de l'infection.

   Puis, le programme affiche les informations fournies par VirusScan dans la boîte de dialogue Notification d'un virus qui apparaît sur l'écran de votre poste de travail. Vous devez cliquer sur **OK** pour fermer cette boîte de dialogue avant d'être en mesure de poursuivre votre travail.

**REMARQUE :** Si vous préférez un autre affichage pour la Notification d'un virus, vous pouvez écrire votre propre application d'affichage ou fichier d'automatisation des tâches incluant ces variables.

4. Pour que VirusScan lance le programme uniquement lors de la première détection d'un virus, sélectionnez le bouton **Première fois**. Pour lancer le programme à chaque détection d'un virus, sélectionnez le bouton **Chaque fois**.

   **IMPORTANT :** Si vous sélectionnez **Première fois**, VirusScan lancera le programme désigné la première fois qu'il rencontre un virus. S'il trouve plusieurs occurrences du même virus lorsqu'il analyse le même répertoire, il ne relancera pas le programme.

   Si toutefois il trouve une occurrence d'un virus, puis découvre un autre virus avant de trouver une autre copie du premier virus, VirusScan lancera le même programme trois fois de suite. Le fait de lancer plusieurs fois le même programme peut saturer la mémoire de votre poste de travail.

5. Cliquez sur **Niveau de priorité** pour spécifier quels types d'événements d'alerte déclencheront le lancement d'un programme.

6. Dans la boîte de dialogue Niveau de priorité (voir Figure 7-5 à la page 151), faites glisser le curseur vers la droite pour demander à VirusScan de lancer le programme pour répondre à un nombre réduit d'événements d'alerte, mais dotés d'un niveau de priorité plus élevé. Faites glisser le curseur vers la gauche pour que VirusScan lance le programme plus souvent, pour répondre à des événements d'alerte dotés d'un niveau de priorité moins élevé. Puis, cliquez sur **OK** pour enregistrer vos modifications et revenir à la boîte de dialogue Propriétés du gestionnaire d'alertes .

   Pour apprendre comment paramétrer les niveaux de priorité pour les différents types de messages, voir "Personnalisation des messages d'alerte" à la page 178.

7. Pour tester la capacité de VirusScan à lancer le programme, cliquez sur **Tester.**

8. Pour configurer d'autres options de notification, cliquez sur un autre onglet. Pour enregistrer vos modifications sans fermer la boîte de dialogue Gestionnaire d'alertes, cliquez sur **Appliquer**. Pour sauvegarder vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans sauvegarder vos modifications, cliquez sur **Annuler**.

> ❑ **REMARQUE :** Cliquer sur **Annuler** n'annulera pas les modifications déjà sauvegardées en cliquant sur **Appliquer**.

## Envoi de messages d'alerte aux journaux du système Windows NT

Le gestionnaire d'alertes peut envoyer les messages d'alerte générés par VirusScan au journal du système sur tous les postes de travail ou les serveurs qui exécutent Windows NT. Pour afficher les messages d'alerte transmis par cette méthode, vous devez ouvrir la visionneuse d'événements de Windows NT. Consultez votre documentation Windows NT pour de plus amples informations.

**Pour envoyer des messages d'alerte au journal du système Windows NT, procédez comme suit :**

1. Ouvrez la boîte de dialogue Propriétés du gestionnaire d'alertes.
2. Cliquez sur l'onglet Enregistrement.

   La page Enregistrement (Figure 7-19) s'affiche et présente une liste de tous les ordinateurs que vous avez configurés pour recevoir des messages d'alerte. Si vous n'avez pas encore configuré d'ordinateur pour recevoir des messages d'alerte, cette liste sera vide.

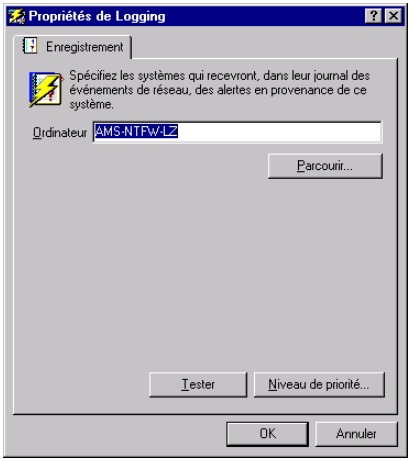



**Figure 7-19. Boîte de dialogue Propriétés du gestionnaire d'alertes - page Enregistrement**

3. Pour mettre à jour cette liste, vous pouvez :

   - **Supprimer un ordinateur.** Sélectionnez un des ordinateurs dans la liste, puis cliquez sur **Supprimer.**
   - **Ajouter un ordinateur.** Cliquez sur **Ajouter** pour ouvrir la boîte de dialogue Propriétés de l'enregistrement (voir Figure 7-20), puis saisissez le nom de l'ordinateur cible dans la zone de texte prévue à cet effet, ou cliquez sur **Parcourir** pour localiser l'ordinateur sur le réseau. Pour choisir des options supplémentaires, passez à Étape 4.

- **Modifier les options de configuration.** Sélectionnez un des ordinateurs de la liste, puis cliquez sur **Propriétés.** Le gestionnaire d'alertes ouvre la boîte de dialogue Propriétés de l'enregistrement (voir Figure 7-20). Modifiez éventuellement les informations dans la zone de texte **Imprimante,** puis passez à Étape 4 pour apprendre comment choisir des options de configuration nouvelles ou différentes.

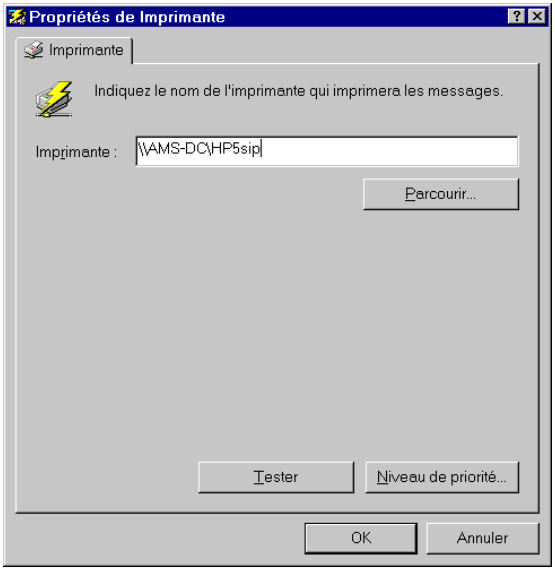



**Figure 7-20. boîte de dialogue Propriétés de l'enregistrement**

4. Cliquez sur **Niveau de priorité** afin de spécifier quels types de messages d'alerte l'ordinateur destinataire recevra.

   Dans la boîte de dialogue Niveau de priorité (voir Figure 7-5 à la page 151), faites glisser le curseur vers la droite pour envoyer à l'ordinateur destinataire un nombre réduit de messages, mais dotés d'un niveau de priorité plus élevé. Faites glisser le curseur vers la gauche pour envoyer à l'ordinateur destinataire un nombre plus important de messages de réseau, y compris ceux dotés d'un niveau de priorité moins élevé. Cliquez sur **OK** pour sauvegarder vos modifications et revenir à la boîte de dialogue Propriétés de l'enregistrement.

   Pour apprendre comment paramétrer les niveaux de priorité pour les différents types de messages, voir "Personnalisation des messages d'alerte" à la page 178.

5. Cliquez sur **Tester** pour envoyer un message test à l'ordinateur destinataire. Ce message s'affichera dans le journal système du système cible. Ouvrez la visionneuse d'événements de Windows NT pour visualiser le message.

6. Cliquez sur **OK** pour revenir à la boîte de dialogue Propriétés du gestionnaire d'alertes.

7. Pour configurer d'autres options de notification, cliquez sur un autre onglet. Pour enregistrer vos modifications sans fermer la boîte de dialogue Gestionnaire d'alertes, cliquez sur **Appliquer**. Pour sauvegarder vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans sauvegarder vos modifications, cliquez sur **Annuler**.

> ❑ **REMARQUE :** Cliquer sur **Annuler** n'annulera pas les modifications déjà sauvegardées en cliquant sur **Appliquer**.

## Envoi d'un message d'alerte en émettant un signal sonore

Le gestionnaire d'alertes peut faire entendre un signal sonore afin de vous avertir de la détection d'un virus. Vous pouvez choisir de faire entendre un signal sonore sous la forme d'un fichier au format .WAV, ou demander au gestionnaire d'alertes d'émettre un signal sonore d' " exclamation " par défaut.

**Pour que VirusScan fasse entendre un signal sonore lors de la détection d'un virus, procédez comme suit :**

1. Ouvrez la boîte de dialogue Propriétés du gestionnaire d'alertes.

2. Cliquez sur l'onglet Signal sonore.

   La page Signal sonore (Figure 7-21) s'affiche.

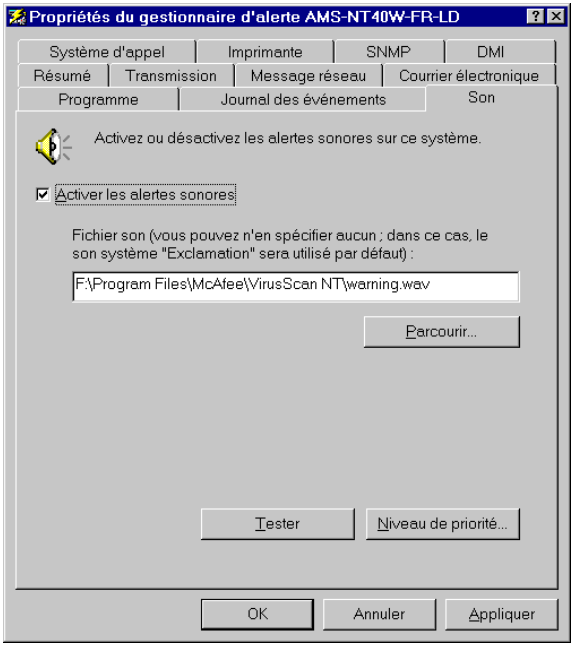



**Figure 7-21. Boîte de dialogue Propriétés du gestionnaire d'alertes - page Signal sonore**

3. Cochez la case **Activer les alertes sonores**.

4. Saisissez le nom et le chemin d'accès du fichier son que vous souhaitez que VirusScan exécute lors de la détection d'un virus, ou cliquez sur **Parcourir** pour localiser le fichier programme sur le disque dur.

   Par défaut, le gestionnaire d'alertes fait entendre le signal sonore du fichier WARNING.WAV depuis le répertoire de programme VirusScan.

5. Cliquez sur **Niveau de priorité** pour spécifier quels types d'événements d'alerte déclencheront le lancement d'un programme.

6. Dans la boîte de dialogue Niveau de priorité (voir Figure 7-5 à la page 151), faites glisser le curseur vers la droite pour demander à VirusScan de faire entendre un signal sonore en réponse à un nombre réduit d'événements d'alerte, mais dotés d'un niveau de priorité plus élevé. Faites glisser le curseur vers la gauche pour que VirusScan fasse entendre un message sonore plus souvent, en réponse à des événements d'alerte dotés d'un niveau de priorité moins élevé. Puis, cliquez sur **OK** pour enregistrer vos modifications et revenir à la boîte de dialogue Propriétés du gestionnaire d'alertes.

Pour apprendre comment paramétrer les niveaux de priorité pour les différents types de messages, voir "Personnalisation des messages d'alerte" à la page 178.

7. Pour tester la capacité de VirusScan à faire entendre le signal sonore de votre choix, cliquez sur **Tester.**

8. Pour configurer d'autres options de notification, cliquez sur un autre onglet. Pour enregistrer vos modifications sans fermer la boîte de dialogue Gestionnaire d'alertes, cliquez sur **Appliquer**. Pour sauvegarder vos modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour fermer la boîte de dialogue sans sauvegarder vos modifications, cliquez sur **Annuler**.

❑ **REMARQUE :** Cliquer sur **Annuler** n'annulera pas les modifications déjà sauvegardées en cliquant sur **Appliquer**.

# Personnalisation des messages d'alerte

VirusScan est fourni avec une large gamme de messages d'alerte conçus pour répondre à la plupart des situations que vous êtes susceptible de rencontrer lorsque le programme trouve un virus sur votre poste de travail ou ailleurs sur votre réseau. Ces messages d'alerte ont un niveau de priorité prédéterminé. Ils comprennent également des variables qui identifient le fichier et le système infectés, nomment le virus responsable de l'infection, et fournissent d'autres informations que vous pouvez utiliser pour avoir un aperçu bref mais exhaustif de la situation.

Vous pouvez cependant activer ou désactiver chaque message d'alerte ou modifier le contenu et le niveau de priorité d'un message pour qu'il corresponde à votre cas de figure. VirusScan continuera toutefois d'activer le message d'alerte en réponse à des événements déclencheurs spécifiques ; c'est pourquoi vous devez tenter de conserver le sens général des messages d'alerte que vous avez choisis de modifier.

## Activation et désactivation des messages d'alerte

Bien que VirusScan puisse vous avertir à chaque détection d'un virus et quasiment à chaque modification significative de son fonctionnement, il se peut que vous ne souhaitiez pas recevoir de messages d'alerte pour chacune de ces situations. Tous les messages d'alerte de VirusScan sont activés par défaut. Pour empêcher VirusScan d'envoyer des messages d'alerte spécifiques, désactivez ceux que vous ne souhaitez pas recevoir dans la boîte de dialogue Propriétés de l'alerte.

**Procédez comme suit :**

1. Lancez la console antivirus puis choisissez **Alertes** dans le **menu** Outils.

   La fenêtre Propriétés de l'alerte s'affiche (voir Figure 7-1 à la page 146). Cliquez sur l'onglet Messages pour afficher la bonne page de propriétés (Figure 7-22).

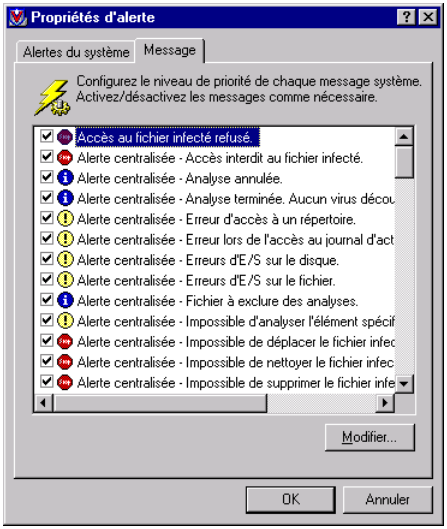



**Figure 7-22. Boîte de dialogue Propriétés de l'alerte - page Messages**

2. Consultez la liste des messages affichée. Pour désactiver les messages que vous ne souhaitez pas que VirusScan envoie, décochez la case de gauche. Laissez la coche dans la case située en regard des messages que vous *souhaitez* que VirusScan transmette.

3. Cliquez sur **OK** pour sauvegarder vos modifications et fermer la boîte de dialogue Propriétés de l'alerte. Pour fermer la boîte de dialogue sans sauvegarder vos modifications, cliquez sur **Annuler**.

## Modification des priorités des messages d'alerte

Certains situations rencontrées par VirusScan lors de l'analyse du système requerront davantage une attention immédiate que d'autres. Dans la plupart des cas, vous préférerez sans doute recevoir un message d'alerte lors de la détection d'un virus sur votre poste de travail plutôt que d'apprendre ultérieurement que la programme a exclu un fichier lors d'une opération d'analyse. Par défaut, VirusScan affecte un niveau de priorité à chacun des ses

messages d'alerte qui traduit l'urgence que la majorité des administrateurs système leur attribueraient. Vous pouvez réorganiser ces niveaux de priorité afin qu'ils répondent mieux à vos besoins et les utiliser pour filtrer les messages que vous recevez du gestionnaire d'alertes, de sorte que vous puissiez vous concentrer en priorité sur les messages les plus importants.

**Pour changer le niveau de priorité affecté à un message d'alerte, procédez comme suit :**

1. Lancez la console antivirus, puis choisissez **Alertes** dans le **menu** Outils.

   La fenêtre Propriétés de l'alerte s'affiche (voir Figure 7-1 à la page 146). Cliquez sur l'onglet Messages pour afficher la bonne page de propriétés (voir Figure 7-22 à la page 179).

2. Sélectionnez un des messages d'alerte de la liste, puis cliquez sur **Modifier.**

   La boîte de dialogue Configurer le message du système s'affiche (Figure 7-23).

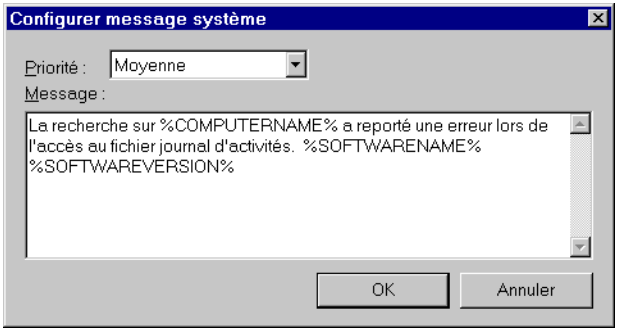



**Figure 7-23. Boîte de dialogue Configurer le message du système**

3. Choisissez un niveau de priorité dans la liste Priorité. Vous pouvez affecter à chaque message d'alerte un niveau de priorité **Haut**, **Moyen** ou **Bas**.

   Les icônes qui apparaissent en regard de chaque message vous indiquent le niveau de priorité désormais affecté au message : indique un message hautement prioritaire, indique un message moyennement prioritaire, et indique un message peu prioritaire.

   Lorsque vous changez la priorité affectée à un message, l'icône en regard de celui-ci se modifie pour afficher son nouvel état de priorité.

4. Cliquez sur **OK** pour sauvegarder vos modifications et fermer la boîte de dialogue Configurer le message du système.

5. Pour filtrer vos messages, configurez chaque méthode d'alerte paramétrée dans le gestionnaire d'alertes afin qu'il n'accepte de délivrer que les messages dotés d'un niveau de priorité donné.

   Par exemple, supposons que vous souhaitez que le gestionnaire d'alertes vous avertisse à chaque fois qu'un virus est détecté sur votre serveur, mais que vous ne voulez pas qu'il vous transmette les messages relatifs aux opérations de routine. Vous préférez que le gestionnaire d'alertes envoie les messages de routine par courrier électronique, ou d'autres moyens de transmission moins urgents.

   Pour ce faire, vous devez utiliser les pages Messages de la boîte de dialogue Propriétés de l'alerte afin d'affecter un haut niveau de priorité aux alertes virales, et un niveau intermédiaire ou faible pour les messages routiniers (voir Figure 7-22 à la page 179). Puis vous devez demander au gestionnaire d'alertes de n'envoyer que les messages dotés d'un niveau de priorité élevé à votre récepteur d'appels.

   Pour ce faire, revenez à la boîte de dialogue Gestionnaire d'alertes (voir Figure 7-2 à la page 148), puis cliquez sur l'onglet correspondant à la méthode d'alerte que vous souhaitez modifier. Reportez-vous à la section figurant précédemment dans le présent chapitre qui expose la méthode d'alerte que vous souhaitez changer, puis lisez les instructions concernant la boîte de dialogue Niveau de priorité (voir Figure 7-5 à la page 151).

## Personnalisation des messages d'alerte

Pour vous aider à réagir à une situation qui requiert votre attention, VirusScan inclut suffisamment d'informations dans ses messages d'alerte pour identifier la source du problème rencontré ainsi que des informations relatives aux circonstances durant lesquelles le problème est apparu. Vous pouvez ajouter des informations ou des commentaires à un message d'alerte qui rendent compte du problème de façon plus précise, répertorier les personnes à contacter pour le résoudre, ou aider le destinataire du message à comprendre comment réagir.

---

**IMPORTANT :** Bien que vous puissiez modifier le texte du message d'alerte pour qu'il dise ce que vous voulez lui faire dire, vous devez vous efforcer de conserver son contenu essentiel intact, car VirusScan n'envoie chaque message que lorsqu'il est confronté à certaines situations. Par exemple, il n'enverra le message d'alerte " tâche en cours " que lorsqu'il aura réellement démarré une tâche.

---

**Pour personnaliser le texte d'un message d'alerte, procédez comme suit :**

1. Lancez la console antivirus, puis choisissez **Alertes** dans le **menu** Outils.

   La boîte de dialogue Propriétés de l'alerte s'ouvre (voir Figure 7-1 à la page 146). Cliquez sur l'onglet Messages pour afficher la bonne page de propriétés (voir Figure 7-22 à la page 179).

2. Sélectionnez un des messages d'alerte de la liste, puis cliquez sur **Modifier.**

   La boîte de dialogue Configurer le message du système s'ouvre (voir Figure 7-23 à la page 180).

3. Modifiez ou ajoutez un commentaire au texte affiché. Le texte figurant entre deux signes de pourcentage, %NOMORDINATEUR%, par exemple, représente une variable que VirusScan complète avec un texte au moment où il crée le message d'alerte.

   VirusScan utilise ces variables dans les messages d'alerte :

   - %NOMFICHIER% - VirusScan remplace le nom de cette variable par celui d'un fichier. Ce nom peut être soit celui d'un fichier infecté qu'il a trouvé, soit celui d'un fichier qu'il a tenté d'exclure d'une opération d'analyse.
   - %NOMTACHE% - VirusScan remplace le nom de cette variable par celui d'une tâche active. Ce nom peut être soit celui de la tâche qui a découvert le virus, soit celui d'une tâche qui a rapporté une erreur au cours d'une opération d'analyse.
   - %NOMVIRUS% - VirusScan remplace le nom de cette variable par celui d'un virus responsable d'une infection.
   - %DATE% - VirusScan remplace le nom de cette variable par la date à laquelle il a effectué une opération d'analyse.
   - %HEURE% - VirusScan remplace le nom de cette variable par l'heure à laquelle il a effectué une option d'analyse.
   - %COMPUTERNAME% - VirusScan remplace le nom de cette variable par celui d'un ordinateur lorsqu'il apparaît sur le réseau. Ce nom peut être celui d'un ordinateur infecté, celui d'un ordinateur qui a rapporté une erreur dans le gestionnaire de périphérique, ou encore celui d'un autre ordinateur auquel VirusScan est connecté.

- %NOMLOGICIEL% - VirusScan remplace le nom de cette variable par celui d'un fichier exécutable. Ce nom peut être celui de l'application qui a détecté un virus, d'une application qui a signalé une erreur, ou de toute autre application avec laquelle VirusScan interagit.
- %VERSIONLOGICIEL% - VirusScan remplace le nom de cette variable par un numéro de version pris sur un progiciel actif. Ce numéro peut être celui de l'application qui a détecté un virus, d'une application qui a signalé une erreur, ou de toute autre application avec laquelle VirusScan interagit.
- %NOMDUTILISATEUR% - VirusScan remplace le nom de cette variable par le nom de l'utilisateur qui est actuellement connecté à votre poste de travail. Cette variable vous indique notamment si quelqu'un a annulé une opération d'analyse.

4. Cliquez sur **OK** pour enregistrer vos modifications et revenir à la boîte de dialogue Propriétés de l'alerte, puis cliquez à nouveau sur **OK** pour revenir à la console antivirus.

# Mise à jour et Mise à niveau de VirusScan

# 8

## Pourquoi effectuer des mises à jour et des mises à niveau ?

Pour que VirusScan fonctionne le mieux possible, on doit lui fournir régulièrement des fichiers de définition des nouveaux virus (fichiers .DAT), des perfectionnements de son dispositif d'analyse et d'autres améliorations techniques. Sans mise à jour de ses fichiers, VirusScan risque de ne pas détecter les attaques des nouveaux virus ou de ne pas répondre efficacement à la menace qui pèse sur votre système. Plus de 200 nouveaux virus apparaissent chaque mois partout dans le monde ; la mise à jour des fichiers de définition des virus constitue le minimum pour se préserver des surprises désagréables.

Network Associates publie chaque mois, par l'intermédiaire de sa division NAI Labs et de son équipe AVERT (Anti-Virus Emergency Response Team), de nouveaux fichiers .DAT pour contrer les attaques des nouveaux virus ; les fichiers réactualisés sont mis à disposition lorsque des modifications dans les caractéristiques des virus ou l'amélioration des produits justifient leur publication. Les utilitaires de mise à jour automatique des fichiers DAT et de mise à niveau automatique des logiciels fournis avec VirusScan facilitent l'utilisation de ce service. Vous pouvez également installer SecureCast, un service client de Network Associates, pour recevoir des “ annonces ” par le Web concernant la mise à disposition de nouveaux fichiers dès leur parution.

❑ **REMARQUE :** “ Mettre à jour ” VirusScan signifie télécharger et installer de nouvelles versions des fichiers .DAT ; “ mettre à niveau ” VirusScan signifie télécharger et installer des révisions de la version du produit, des programmes exécutables, et dans certains cas, des fichiers .DAT. Network Associates vous offre l’actualisation en ligne des fichiers .DAT, et ceci pendant toute la durée de vie de votre version de VirusScan. Toutefois, ceci n’offre pas la garantie que vos fichiers .DAT soient compatibles avec les versions précédentes du produit.

Votre droit de télécharger gratuitement des mises à niveau de VirusScan est prévu par les termes de votre licence ou par les termes du contrat de vente que vous avez acceptés au moment de l’acquisition du logiciel. Si vous avez des questions concernant ces termes, consultez les documents LICENSE.TXT ou README.1ST fournis avec la copie de VirusScan, ou consultez votre revendeur. Network Associates vous offre la possibilité de télécharger gratuitement les fichiers de mise à niveau à partir de ses services en ligne aussi longtemps que votre licence vous y autorise.

## Stratégies de mise à jour et de mise à niveau

La tâche de mise à jour automatique des fichiers DAT est fournie configurée par défaut pour télécharger les mises à jour les plus récentes des fichiers .DAT, directement d'un site FTP (File Transfer Protocol) 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 grand 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 noeud du réseau tente de mettre à jour ses fichiers .DAT en même temps.

Network Associates vous conseille plutôt d'utiliser les utilitaires de mise à jour automatique des fichiers DAT et de mise à niveau automatique des logiciels en association avec le service annexe SecureCast, pour une organisation “ symétrique ” efficace. Dès que vous avez installé le logiciel client sur un serveur d’administration, SecureCast est en mesure de vous envoyer ou d’expédier des fichiers actualisés de façon automatique dès que NAI Labs les a mis à disposition.

Si vous fournissez alors ces fichiers actualisés à un ou plusieurs serveurs centraux de votre réseau et configurez les noeuds de réseau restants pour qu’ils les chargent depuis ces serveurs, vous pouvez

- Planifier le retrait des fichiers .DAT et des mises à niveau de produit sur l'ensemble du réseau aux heures qui vous conviennent et avec une intervention minimale des administrateurs ou des utilisateurs du réseau. Vous pouvez configurer les tâches de mise à jour et de mise à niveau automatiques pour planifier l'heure à laquelle chaque noeud de réseau doit interroger le serveur pour recevoir les fichiers actualisés. Il serait judicieux, par exemple, d'échelonner vos tâches de mise à jour ou de définir votre programmation de sorte à introduire progressivement ou à alterner les mises à jour des fichiers .DAT et les mises à niveau du logiciel sur les différentes parties du réseau.
- 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. Maintenir en priorité le trafic de mise à jour et de mise à niveau à un niveau interne peut également limiter les possibilités de violation de la sécurité du réseau.
- Réduire l'attente éventuelle pour télécharger de nouveaux fichiers .DAT ou de mise à niveau. Le trafic sur les serveurs de Network Associates est susceptible d'augmenter considérablement aux dates habituelles de publication des fichiers .DAT et à la sortie des nouvelles versions de produit. Eviter la saturation de la bande passante du réseau vous permet d'utiliser votre nouveau logiciel avec un minimum d'interruptions.

D'autres options avancées de mise à jour vous permettent de sauvegarder les fichiers .DAT existants, d'installer la mise à jour des fichiers .DAT ou d'exécuter des programmes particuliers une fois les mises à jour achevées. Une série de pages de propriétés de mise à jour / mise à niveau automatique contrôlent les options de cette tâche ; voir "Configuration des options de mise à jour automatique des fichiers DAT" à la page 187 et "Configuration des options de mise à niveau automatique des logiciels" à la page 194 pour plus de détails.

# Configuration des options de mise à jour automatique des fichiers DAT

Les fichiers de définition des virus réactualisés apparaissent sur le site FTP de Network Associates sous forme de paquets de fichiers de données (.DAT). Un paquet .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. L'utilitaire de mise à jour automatique des fichiers DAT télécharge ces fichiers, interrompt temporairement le scanner lors de l'accès de VirusScan, installe les fichiers actualisés puis redémarre le scanner lors de l'accès. VirusScan peut alors utiliser immédiatement les fichiers actualisés.

**Pour configurer la tâche de mise à jour automatique des fichiers DAT, procédez comme suit :**

1. Lancez la console antivirus Voir “Démarrage de la console antivirus de VirusScan” à la page 61 pour savoir comment s'y prendre.

2. Sélectionnez la tâche de mise à jour automatique des fichiers DAT, puis cliquez sur  dans la barre d'outils Console pour ouvrir la boîte de dialogue Propriétés de mise à jour / mise à niveau automatique (Figure 8-1).

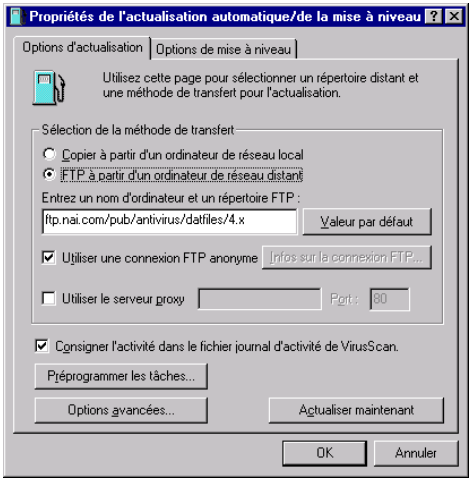



**Figure 8-1. Boîte de dialogue Mise à jour/mise à niveau automatique page Options de mise à jour**

3. Pour lancer une tâche de mise à jour immédiatement en utilisant les options de configuration par défaut déjà paramétrées pour cette tâche, cliquez simplement sur **Mettre à jour maintenant** en bas de la boîte de dialogue. Sinon, passez aux étapes suivantes pour modifier les configurations ou définir un calendrier de mise à jour.

4. Choisissez la méthode que vous souhaitez utiliser pour vous connecter au serveur de transfert. Vous avez le choix entre les actions suivantes :

   - **Copier à partir d’un ordinateur en réseau local**. Sélectionnez cette option pour un simple transfert des fichiers de mise à jour vers votre réseau par le biais de n’importe quel protocole réseau actif. Les paramètres de ce protocole contrôlent la méthode qu’utilise la tâche de mise à jour automatique des fichiers DAT pour tenter de se connecter et l'intervalle de temps qui doit s’écouler avant qu'elle ne cesse ses tentatives.

Saisissez le nom de l'ordinateur en respectant la notation de la convention d'affectation des noms (UNC) dans la zone de texte prévue à cet effet, ou cliquez sur **Parcourir** pour localiser l'ordinateur sur votre réseau. Les autres options de la zone Sélection d'un mode de transfert de la boîte de dialogue deviennent indisponibles.

---

**IMPORTANT :** La tâche de mise à jour automatique des fichiers DAT s'attend à trouver les nouveaux fichiers .DAT dans leurs archives .ZIP d'origine portant les noms de fichiers originaux. Si vous enregistrez ces nouveaux fichiers sur un serveur central pour que les autres postes de travail puissent les télécharger, assurez-vous de ne pas extraire les fichiers ou de ne pas les renommer.

Si vous enregistrez les fichiers sur un serveur Novell NetWare, vous devez installer et vous servir de l'utilitaire de copie de fichier en association avec l'utilitaire de mise à jour automatique des fichiers DAT. Pour savoir comment utiliser cet utilitaire, voir étape 7 à la page 42 dans le chapitre 2. Pour connaître le fonctionnement de cet utilitaire, voir "Mise à jour et mise à niveau à partir des serveurs NetWare" à la page 200.

---

- **FTP depuis un ordinateur en réseau distant**. Sélectionnez cette option pour le transfert des fichiers de mise à jour via le protocole de transfert de fichiers (FTP). Pour utiliser cette option, le serveur de transfert doit disposer d'un service FTP actif.

  La tâche de mise à jour automatique des fichiers DAT utilise sa propre implémentation FTP pour se connecter au serveur, mais la durée de l'intervalle de la tentative de connexion dépend de vos paramètres de protocole réseau.

  Ensuite, saisissez le nom du domaine du serveur cible ainsi que toutes les informations requises concernant le répertoire dans la zone de texte prévue à cet effet. Cliquer sur **Par défaut** saisit le serveur FTP de Network Associates.

  ftp:/ / ftp.nai.com / pub / antivirus / datfiles / 4.x

Si le serveur cible accepte les connexions FTP effectuées par un utilisateur anonyme, cochez **Utiliser un nom d'utilisateur FTP anonyme**. Si vous utilisez un compte FTP spécifique qui nécessite un nom et un mot de passe utilisateur, décochez la case et à la place cliquez sur **Informations de connexion FTP**. Ce bouton ouvre une boîte de dialogue dans laquelle vous pouvez saisir le nom et le mot de passe utilisateur appropriés. Saisissez à nouveau le mot de passe pour le confirmer, puis cliquez sur **OK** pour fermer la boîte de dialogue.

5. Si vous acheminez les requêtes FTP depuis un réseau au travers d'un serveur proxy, cochez **Utiliser un serveur proxy**, puis saisissez le nom de votre serveur proxy dans la zone de texte prévue 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. Puis, dans la zone de texte restante, saisissez le port logique du serveur proxy auquel vous souhaitez adresser vos requêtes FTP.

6. Pour enregistrer les résultats de la mise à jour, cochez la case **Enregistrer l'activité dans le fichier journal VirusScan**.

   Le fichier journal enregistre par défaut l'heure de début d'une tâche de mise à jour et la façon dont elle se termine. Pour ouvrir et consulter le journal d'activité, choisissez **Journal d'activité** dans le menu **Analyser** de la fenêtre de la console antivirus.

7. Cliquez sur **Planifier** pour ouvrir une boîte de dialogue où vous pouvez définir un calendrier ponctuel ou périodique pour votre tâche de mise à jour (voir Figure 8-2).


**Figure 8-2. Boîte de dialogue Planifier**

8. Cochez la case **Activer le planificateur**. Les options des zones Exécuter et Démarrer à deviennent actives.

9. Choisissez la fréquence à laquelle vous souhaitez exécuter la tâche dans la zone Exécuter ou sélectionnez **Au démarrage** pour l'exécuter dès que VirusScan se charge. Selon la fréquence choisie, la zone **Démarrer à** vous propose des choix différents pour le calendrier de votre tâche. Vos choix sont :

   - **Une fois.** Exécute votre tâche une seule fois à la date et à l'heure que vous spécifiez. Entrez l'heure dans la zone de texte à gauche de la zone **Démarrer à**, puis sélectionnez un mois et une date dans la liste de droite.
   - **Toutes les heures.** Exécute votre tâche toutes les heures tant que votre poste de travail est allumé et que VirusScan demeure activé. Spécifiez dans la zone de texte affichée la durée en minutes que doit attendre VirusScan après chaque heure pour exécuter votre tâche.
   - **Tous les jours.** Exécute votre tâche une fois, à l'heure et aux dates que vous spécifiez. Cliquez sur **Quel jour** pour ouvrir une boîte de dialogue dans laquelle vous pouvez sélectionner les jours auxquels vous souhaitez que la tâche s'exécute. Ensuite, cliquez sur **OK** pour fermer la boîte de dialogue et entrez l'heure à laquelle vous souhaitez exécuter la tâche dans la zone de texte Démarrer à.
   - **Toutes les semaines.** Exécute 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.
   - **Tous les mois.** Exécute 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 .

10. Pour enregistrer vos modifications et revenir à la boîte de dialogue Propriétés de mise à jour / mise à niveau automatique, cliquez sur **OK**. Pour revenir à la boîte de dialogue sans enregistrer vos modifications, cliquez sur **Annuler.**

---

❑ **REMARQUE :** Pour que VirusScan exécute la tâche, votre poste de travail doit être allumé et VirusScan doit être activé. Si ces deux conditions ne sont pas remplies au moment où votre tâche devrait démarrer, celle-ci ne s'exécutera qu'à la prochaine date planifiée.

---

11. Pour configurer des options supplémentaires, cliquez sur **Avancées**, et reportez-vous à "Configuration des options de mise à jour avancées" pour en savoir plus sur vos choix. Pour enregistrer vos modifications et revenir à la console antivirus, cliquez sur **OK**. Pour fermer la boîte de dialogue sans sauvegarder vos modifications, cliquez sur **Annuler**.

# Configuration des options de mise à jour avancées

Pour que votre tâche de mise à jour soit prête à être exécutée, vous n'avez qu'à saisir un serveur cible, un mode de connexion et toutes les informations nécessaires à la connexion. Puis, lorsque vous aurez planifié son exécution, l'utilitaire de mise à jour automatique des fichiers DAT 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 programme de VirusScan.

Pour effectuer un pré ou post traitement supplémentaire des fichiers, ou pour exécuter d'autres actions, cliquez sur **Avancées** afin d'ouvrir la boîte de dialogue Options de mise à jour avancées (voir Figure 8-3).

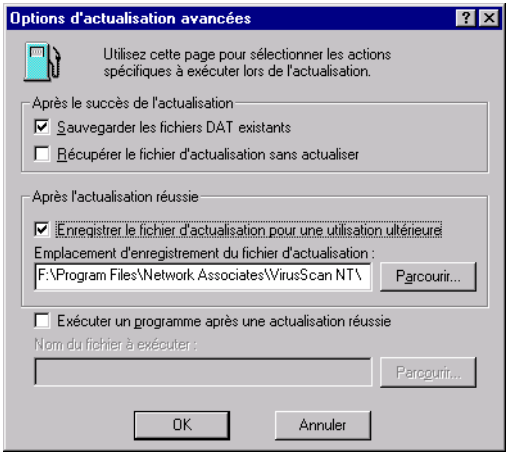



**Figure 8-3. Boîte de dialogue Options de mise à jour avancées**

**Procédez comme suit :**

1. Précisez à l'utilitaire de mise à jour automatique des fichiers DAT ce que vous souhaitez qu'il fasse avant ou pendant l'exécution d'une mise à jour. Les choix possibles sont :

   - **Sauvegarder les fichiers .DAT existants.** Cochez cette case pour que l'utilitaire 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.

- **Extraire le fichier de mise à jour mais sans mise à jour**. Cochez cette case pour que l'utilitaire télécharge le fichier d'archive .ZIP qui contient les nouveaux fichiers .DAT et le sauvegarde dans un emplacement que vous désignez au lieu de l'extraire et de l'installer.

  ---

  ↳ **Astuce:** Sélectionnez cette option si vous envisagez de configurer d'autres postes de travail sur votre réseau à mettre à jour à partir d'un serveur central.

  ---

  Cocher cette case active aussi la case **Enregistrer le fichier mis à jour pour une utilisation ultérieure** située dans la zone Après une mise à jour réussie. Pour indiquer à l'utilitaire où enregistrer le paquet de fichiers .DAT, entrez un chemin et un nom de dossier dans la zone de texte prévue à cet effet ou cliquez sur **Parcourir** pour trouver un dossier approprié.

2. Précisez à l'utilitaire de mise à jour automatique des fichiers DAT ce qu'il doit faire après un téléchargement, une extraction et une installation réussis de nouveaux fichiers .DAT. Les choix possibles sont :

   - **Enregistrer le fichier mis à jour pour un usage ultérieur.** Cochez cette case pour que l'utilitaire enregistre une copie non extraite du paquet de fichiers .DAT dans un emplacement que vous spécifiez. Après cette sauvegarde, l'utilitaire extrait les fichiers DAT du paquet de mise à jour et procède à l'installation sur le poste de travail local. Au contraire, l'option **Extraire le fichier de mise à jour mais sans mise à jour** enregistre le fichier non extrait, mais n'installe pas les nouveaux fichiers .DAT.

     ---

     ↳ **Astuce:** Sélectionnez cette option si vous envisagez de configurer d'autres postes de travail sur votre réseau à mettre à jour à partir d'un serveur central.

     ---

     Pour indiquer à l'utilitaire où enregistrer le paquet de fichiers .DAT, entrez un chemin et un nom de dossier dans la zone de texte prévue à cet effet ou cliquez sur **Parcourir** pour trouver un dossier approprié.

   - **Lancer un programme après une mise à jour réussie.** Cochez cette case pour indiquer à l'utilitaire de lancer un autre programme lorsque l'installation des nouveaux fichiers .DAT est achevée. Vous pourriez souhaitez utiliser cette option pour notamment démarrer un programme de courrier électronique client ou un utilitaire de messagerie réseau qui indique à un administrateur système que l'opération de mise à jour s'est déroulée normalement.

Puis, saisissez un chemin et un nom de fichier pour le 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 Mise à jour / mise à niveau automatique, cliquez sur **OK**. Pour fermer la boîte de dialogue sans sauvegarder vos modifications, cliquez sur **Annuler**.

# Configuration des options de mise à niveau automatique des logiciels

Network Associates révise VirusScan fréquemment afin de lui fournir de nouveaux outils de détection et de réparation, de nouvelles options pour une meilleure gestion et flexibilité, et d'autres améliorations pour qu'il soit un meilleur outil de protection contre les virus.

L'utilitaire de mise à niveau automatique des logiciels de VirusScan est conçu pour rechercher et télécharger ces nouvelles versions lorsqu'elles sont disponibles. Il se connecte automatiquement à un serveur central sur votre réseau ou à un site FTP désigné, télécharge les nouveaux fichiers, les extrait et les vérifie, effectue une copie de sauvegarde des fichiers existants puis commence l'installation des nouveaux fichiers. Une fois ce travail accompli, il redémarre tous les services VirusScan et reprend ses analyses.

Par défaut, l'utilitaire inclus dans VirusScan n'est pas configuré avec les informations relatives au site requises pour télécharger de nouvelles versions de VirusScan. Les utilisateurs consignés de VirusScan peuvent obtenir cette information de leur revendeur ou d'autres sources de Network Associates.

---

**Pour configurer la tâche de mise à niveau automatique des logiciels, procédez comme suit :**

1. Lancez la console antivirus Voir "Démarrage de la console antivirus de VirusScan" à la page 61 pour savoir comment s'y prendre.

2. Sélectionnez la tâche de mise à niveau automatique des logiciels, puis cliquez sur  dans la barre d'outils Console pour ouvrir la boîte de dialogue Propriétés de mise à jour / mise à niveau automatique (voir Figure 8-1 à la page 188).

3. Cliquez ensuite sur l'onglet Options de mise à niveau pour afficher la page de propriétés correspondante (Figure 8-4 à la page 195).

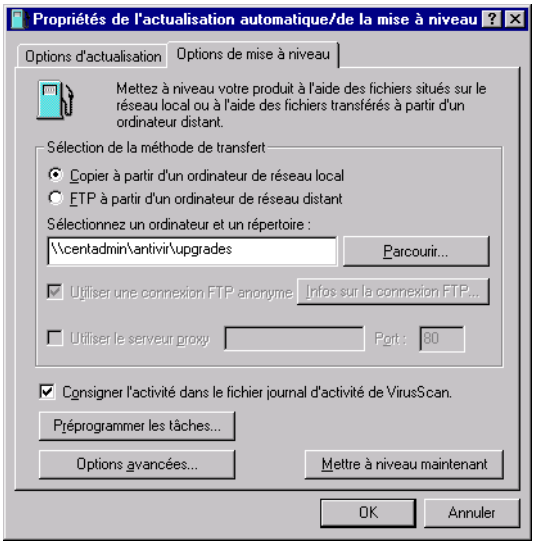



**Figure 8-4. Boîte de dialogue Mise à jour/mise à niveau automatique page Options de mise à niveau**

4. Pour lancer une tâche de mise à niveau immédiatement en utilisant les options de configuration par défaut définies pour cette tâche, cliquez sur **Mettre à niveau maintenant** en bas de la boîte de dialogue. Sinon, passez aux étapes suivantes pour modifier la configuration ou définir un calendrier de mise à jour.

5. Choisissez la méthode que vous souhaitez utiliser pour vous connecter au serveur de transfert. Vous avez le choix entre les actions suivantes :

   - **Copier à partir d'un ordinateur en réseau local**. Sélectionnez cette option pour un simple transfert des fichiers de mise à jour vers votre réseau par le biais de n'importe quel protocole réseau actif. Les paramètres de ce protocole contrôlent la façon dont la tâche de mise à niveau automatique des logiciels tente de se connecter et l'intervalle de temps qui doit s'écouler avant qu'elle ne cesse ses tentatives.

     Saisissez le nom de l'ordinateur en respectant la notation de la convention d'appellation universelle (UNC) dans la zone de texte fournie à cet effet, ou cliquez sur **Parcourir** pour localiser l'ordinateur sur votre réseau. Les autres options de la zone Sélection du mode de transfert de la boîte de dialogue deviennent indisponibles.

**IMPORTANT :** La tâche de mise à niveau automatique des logiciels s'attend à trouver une image disque *dézippée* des nouveaux fichiers de mise à niveau sur votre serveur. Ceci vous permet de personnaliser votre installation avant d'utiliser les nouveaux fichiers.

Si vous enregistrez vos fichiers actualisés sur un serveur Novell NetWare, vous devez installer et utiliser l'utilitaire de copie de fichier en association avec l'utilitaire de mise à niveau. Pour savoir comment installer cet utilitaire, voir étape 7 à la page 42 dans le chapitre 2. Pour connaître son fonctionnement, voir “Mise à jour et mise à niveau à partir des serveurs NetWare” à la page 200.

Si vous stockez des fichiers de mise à niveau sur un serveur qui utilise des noms de fichier prenant en compte la casse, vous devez renommer le fichier PKGDESC.INI, fourni avec les mises à niveau de VirusScan, afin qu’il ne comporte que des lettres de bas de casse. Sinon, l'utilitaire de mise à niveau sera incapable de trouver le fichier sur le serveur et n’installera donc pas la nouvelle version de VirusScan sur les ordinateurs client.

- **FTP depuis un ordinateur en réseau distant**. Sélectionnez cette option pour le transfert des fichiers de mise à jour via le protocole de transfert de fichiers (FTP). Pour utiliser cette option, le serveur de transfert doit disposer d'un service FTP actif.

  La tâche de mise à niveau automatique des logiciels utilise sa propre implémentation FTP pour se connecter au serveur, mais la durée de l'intervalle de la tentative de connexion dépend de vos paramètres de protocole réseau.

  Puis, saisissez le nom du domaine du serveur cible ainsi que toutes les informations requises concernant le répertoire dans la zone de texte prévue à cet effet.

  Si le serveur cible accepte les connexions FTP effectuées par un utilisateur anonyme, cochez **Utiliser un nom d’utilisateur FTP anonyme** . Si vous utilisez un compte FTP spécifique qui nécessite un nom et un mot de passe utilisateur, décochez la case et à la place cliquez sur **Informations de connexion FTP** . Ce bouton ouvre une boîte de dialogue dans laquelle vous pouvez saisir le nom et le mot de passe utilisateur appropriés. Saisissez à nouveau le mot de passe pour le confirmer, puis cliquez sur **OK** pour fermer la boîte de dialogue.

6. Si vous acheminez les requêtes FTP depuis un réseau au travers d'un serveur proxy, cochez **Utiliser un serveur proxy**, puis saisissez le nom de votre serveur proxy dans la zone de texte prévue 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. Puis, dans la zone de texte restante, entrez le port logique du serveur proxy auquel vous souhaitez adresser vos requêtes FTP.

7. Pour enregistrer les résultats d'une mise à niveau, cochez la case **Enregistrer l'activité dans le fichier journal VirusScan**.

   Par défaut, le fichier journal enregistre l'heure de début d'une tâche de mise à niveau et la façon dont elle se termine. Pour ouvrir et consulter le fichier journal, choisissez **Journal d'activité** dans le menu **Analyser** de la fenêtre de la console antivirus.

8. Cliquez sur **Planifier** pour ouvrir une boîte de dialogue où vous pouvez définir un calendrier ponctuel ou périodique pour votre tâche de mise à niveau (Figure 8-5).


**Figure 8-5. Boîte de dialogue Planifier**

9. Cochez la case **Activer le planificateur**. Les options des zones Exécuter et Démarrer à deviennent actives.

10. Choisissez la fréquence à laquelle vous souhaitez exécuter la tâche dans la zone Exécuter ou sélectionnez **Au démarrage** pour l'exécuter dès que VirusScan se charge. Selon la fréquence choisie, la zone **Démarrer à** vous propose des choix différents pour le calendrier de votre tâche. Vos choix sont :

    - **Une fois.** Exécute 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 à, puis sélectionnez un mois et une date dans la liste de droite.

- **Toutes les heures.** Exécute votre tâche toutes les heures tant que votre ordinateur est allumé et que VirusScan demeure activé. Spécifiez dans la zone de texte affichée combien de minutes après l'heure doit attendre VirusScan pour exécuter votre tâche.
- **Tous les jours.** Exécute votre tâche une fois, à l'heure et aux dates que vous spécifiez. Cliquez sur **Quel jour** pour ouvrir une boîte de dialogue où vous pouvez sélectionner les jours auxquels vous souhaitez que la tâche s'exécute. Ensuite, cliquez sur **OK** pour fermer la boîte de dialogue, puis entrez l'heure à laquelle vous souhaitez que la tâche s'exécute dans la zone de texte Démarrer à.
- **Toutes les semaines.** Exécute 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.
- **Tous les mois.** Exécute 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 .

11. Pour enregistrer vos modifications et revenir à la boîte de dialogue Propriétés de mise à jour / mise à niveau automatique, cliquez sur **OK**. Pour revenir à la boîte de dialogue sans enregistrer vos modifications, cliquez sur **Annuler.**

> ❑ **REMARQUE :** Pour que VirusScan puisse exécuter votre tâche, votre poste de travail doit être allumé et VirusScan doit être activé. Si ces deux conditions ne sont pas remplies au moment où votre tâche devrait démarrer, celle-ci ne s'exécutera qu'à la prochaine date planifiée.

12. Pour configurer des options supplémentaires, cliquez sur **Avancées**, et reportez-vous à "Configuration des options avancées de mise à niveau" pour en savoir plus sur vos choix. Pour enregistrer vos modifications et revenir à la console antivirus, cliquez sur **OK**. Pour fermer la boîte de dialogue sans sauvegarder vos modifications, cliquez sur **Annuler**.

# Configuration des options avancées de mise à niveau

Pour que votre tâche soit prête à être exécutée, vous n'avez qu'à saisir un serveur cible, un mode de connexion et toutes les informations nécessaires à la connexion. Puis, lorsque vous aurez planifié son exécution, l'utilitaire de mise à jour automatique des fichiers .DAT 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 programme de VirusScan.

Pour effectuer un pré ou post traitement des fichiers ou pour exécuter d'autres actions, cliquez sur **Avancées** pour ouvrir la boîte de dialogue Options de mise à niveau avancées (Figure 8-6).

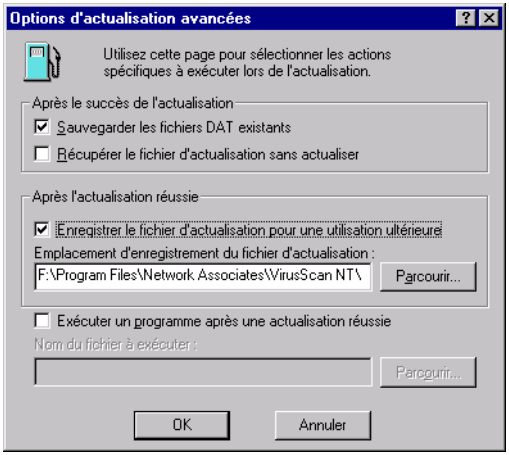



**Figure 8-6. Boîte de dialogue Options de mise à niveau avancées**

**Procédez comme suit :**

1. Cochez la case **Extraire les fichiers de mise à niveau mais sans mise à niveau** pour que l'utilitaire télécharge l'archive .ZIP qui contient les nouveaux fichiers de mise à niveau, extrait ces derniers et les enregistre dans un emplacement que vous spécifiez au lieu de les installer.

   Cocher cette case sélectionne également la case **Enregistrer les fichiers mis à niveau pour une utilisation ultérieure**. Pour indiquer à l'utilitaire où il doit enregistrer les nouveaux fichiers, entrez un chemin d'accès et un nom de dossier dans la zone de texte affichée ou cliquez sur **Parcourir** pour localiser un dossier approprié.

2. Pour enregistrer vos modifications et revenir à la boîte de dialogue Propriétés de mise à jour / mise à niveau automatique, cliquez sur **OK**. Pour fermer la boîte de dialogue sans sauvegarder vos modifications, cliquez sur **Annuler**.

# Mise à jour et mise à niveau à partir des serveurs NetWare

Si vous stockez vos fichiers .DAT et fichiers de mise à niveau pour les extraire à partir des serveurs Novell NetWare, vous devez installer et activer l'utilitaire de copie de fichier fourni avec le programme VirusScan. Cet utilitaire s'exécute automatiquement, sans interface utilisateur, dès l'instant où vous ouvrez une session sur votre poste Windows NT. Sinon, il fonctionne directement avec les utilitaires de mise à jour automatique des fichiers DAT et de mise à niveau automatique des logiciels pour naviguer sur le Web et télécharger des fichiers à partir des serveurs NetWare que vous désignez dans la boîte de dialogue Mise à jour / mise à niveau automatique.

Pour pouvoir vous servir de l'utilitaire, vous devez l'installer comme élément à part entière d'une installation personnalisée lorsque vous installez VirusScan pour la première fois. Le chapitre 2, étape 7 à la page 42 décrit la procédure d'installation.

---

**IMPORTANT :** N'installez *pas* l'utilitaire de copie de fichiers sur votre système à moins que vous n'utilisiez les serveurs NetWare pour distribuer les mises à jour de définition des virus et les mises à niveau des logiciels. Si vous ne disposez pas d'un environnement réseau doté de cette configuration, l'utilitaire de copie de fichiers risque de mal orienter les utilitaires de mise à jour automatique des fichiers DAT et de mise à niveau automatique des logiciels.

---

Cet utilitaire nécessite également que vous exécutiez l'application Client 32 de Novell à partir du poste de travail Windows NT et que vous ayiez installé NetWare v4.11 sur le serveur NetWare.

Une fois installé, l'utilitaire de copie de fichier se connecte à votre gisement de données NetWare, puis télécharge les fichiers .DAT existants ou les fichiers de mise à niveau dans un répertoire temporaire sur le poste de travail locale. Le possesseur de l'ordinateur qui exécute l'utilitaire doit avoir les autorisations nécessaires pour se connecter au serveur NetWare afin que l'utilitaire de copie de fichier puisse réaliser cette opération.

Lorsque la mise à jour ou la mise à niveau planifiée doit démarrer, l'utilitaire de copie de fichier dirige les utilitaires de mise à niveau et de mise à jour pour extraire les nouveaux fichiers du répertoire temporaire local au lieu de les extraire du serveur NetWare. Cette opération se déroule sans aucune intervention de l'utilisateur. Si elle échoue pour quelque raison que ce soit, l'utilitaire de copie de fichier enregistre un message d'erreur dans le fichier du journal d'activité de VirusScan.

**IMPORTANT :** Comme l'utilitaire de copie de fichier ne commence à s'exécuter que lorsque vous allumez votre ordinateur, vous devez vous assurer de l'allumer au moins une fois pendant la période entre la dernière mise à jour ou mise à niveau effectuée et la prochaine opération planifiée.

# Mise à jour des fichiers .DAT sans mise à jour automatique des fichiers DAT

Network Associates vous conseille d'utiliser l'utilitaire de mise à jour automatique des fichiers DAT fourni avec VirusScan pour installer les nouvelles versions des fichiers .DAT. Ces utilitaires constituent un moyen simple et infaillible de mettre à jour correctement des fichiers .DAT. Toutefois, si vous souhaitez installer vous-même des fichiers .DAT, vous pouvez télécharger :

- **les fichiers .DAT habituels.** Network Associates stocke ces fichiers sur son site FTP sous forme d'archives .ZIP portant le nom DAT-XXXX.ZIP. Le XXXX du nom de fichier est un numéro de série qui change à chaque création de fichiers .DAT. Pour télécharger ces fichiers, utilisez un navigateur ou un client FTP permettant de se connecter à :

  ftp://ftp.nai.com/pub/antivirus/datfiles/4.x

- **des fichiers .EXE installables.** Network Associates stocke ces fichiers sur son site Web sous la forme d'un fichier d'installation auto-exécutable nommé XXXXUPDT.EXE. Ici également, le XXXX est un numéro de série qui change à chaque création de fichiers de définition de virus. Pour télécharger ces fichiers, utilisez un navigateur Web pour vous connecter à :

  http://download.mcafee.com/updates/4x.asp

Les deux fichiers contiennent exactement les mêmes fichiers de définition de virus. La différence entre les eux réside dans la façon dont vous les utilisez pour mettre à jour votre copie de VirusScan.

En résumé, pour utiliser l'archive DAT-XXXX.ZIP, vous devez télécharger le fichier, l'extraire de son archive, interrompre le scanner lors de l'accès de VirusScan , copier les fichiers dans le répertoire programme de VirusScan, puis relancer le scanner lors de l'accès de VirusScan. Voir “Mise à jour à partir des archives de fichiers .DAT” pour plus de détails.

Pour installer les fichiers .DAT livrés avec leur propre utilitaire d'installation, il suffit de les télécharger dans un répertoire temporaire sur votre disque dur, puis d'exécuter ou de double-cliquer sur le fichier XXXXUPDT.EXE. L'utilitaire d'installation interrompt le scanner lors de l'accès, copie les fichiers dans le bon répertoire, puis relance le scanner lors de l'accès.

**IMPORTANT :** Ces deux méthodes de mise à jour nécessitent que vous bénéficiiez des droits d'administrateur pour l'ordinateur que vous souhaitez mettre à jour. Vous devez vous connecter correctement au poste de travail cible avant de mettre à jour vos fichiers.

Une fois mis à jour, VirusScan utilise immédiatement les nouveaux fichiers .DAT : il ne vous est pas nécessaire de redémarrer votre poste de travail.

## Mise à jour à partir des archives de fichiers .DAT

Pour installer les mises à jour des fichiers .DAT directement à partir d'une archive .ZIP SANS utiliser la mise à jour automatique, procédez comme suit.

**REMARQUE :** Network Associates ne recommande pas d'utiliser cette méthode pour mettre à jour vos fichiers .DAT.

1. Créez un répertoire temporaire sur votre disque dur, puis copiez l'archive .ZIP contenant les fichiers .DAT que vous avez téléchargée dans ce répertoire.
2. Effectuez une copie de sauvegarde ou renommez les fichiers .DAT existants stockés dans le répertoire programme :
   - CLEAN.DAT
   - LICENSE.DAT
   - MESSAGES.DAT
   - NAMES.DAT
   - SCAN.DAT
   - SHLDMSG.DAT
3. Servez-vous de WinZip, de PKUnzip ou d'un utilitaire similaire pour ouvrir l'archive .ZIP et extraire les fichiers .DAT actualisés.
4. Connectez-vous au poste de travail que vous souhaitez mettre à jour. Vous devez bénéficier des droits d'administrateur pour l'ordinateur cible.
5. Cliquez sur **Démarrer**, pointer le curseur sur **Paramètres**, puis choisissez **Panneau de commandes** pour ouvrir la fenêtre Panneau de commandes. Ensuite, localisez et double-cliquez sur le panneau de commandes Services pour l'ouvrir.

Si l'ordinateur fonctionne sous Windows NT 3.51, lancez le Gestionnaire de programmes puis localisez le groupe de programmes Panneaux de commandes. Double-cliquez sur le groupe de programmes pour l'ouvrir, puis localisez le panneau de commandes Services et double-cliquez dessus.

6. Sélectionnez le service Network Associates McShield , puis cliquez sur **Arrêter**.
7. Copiez les fichiers .DAT que vous avez extraits de l'archive .zip dans le répertoire programme de VirusScan. Si vous avez installé VirusScan dans son répertoire programme par défaut, copiez-y les fichiers :

   C:\Program Files\Network Associates\VirusScan NT

8. Revenez au panneau de commandes Services, sélectionnez le service McShield, puis cliquez sur **Démarrer**.
9. Fermez le panneau de commandes Services.

VirusScan utilise immédiatement les fichiers .DAT pour ses analyses.

# Utilisation des utilitaires de gestion de VirusScan A

## Paramétrage des références de l'utilisateur sur les stations de travail

La plupart des fonctions essentielles de VirusScan fonctionnent comme des services Windows NT. Tous ces services requièrent un compte d'utilisateur sur la station de travail locale afin d'obtenir les droits indispensables pour planifier et exécuter les opérations d'analyse. D'ordinaire, vous paramétrez le compte d'utilisateur utilisé par ces services lorsque vous l'installez sur l'ordinateur cible (voir étape 10 à la page 44 ou Étape 6 par Étape 9 aux pages 49 à 50 pour plus de détails).

Si vous souhaitez toutefois affecter les services de Network Associates sur un autre compte utilisateur, vous pouvez le faire à l'aide de SVCPWD.EXE, un utilitaire exécutable fourni avec le programme. SVCPWD s'exécute à partir de la ligne de commande de Windows NT et nécessite un fichier texte en entrée que vous pouvez créer à l'aide d'un éditeur de texte comme Notepad, par exemple.

Dans ce fichier texte, vous devez dresser la liste de tous les ordinateurs dont vous souhaitez changer le compte utilisé par ces services. Indiquez le nom de chaque ordinateur selon la convention d'affectation des noms (UNC). Pour changer les comptes d'un ordinateur nommé CentAdmin et d'un autre nommé AVClient, par exemple, tapez les lignes suivantes dans un fichier texte :

```
\\centadmin

\\avclient
```

Ensuite, enregistrez le fichier dans le répertoire programme de VirusScan ou dans tout autre répertoire approprié.

SVCPWD ne crée *pas* de nouveau compte sur les stations de travail cibles ; le compte que vous adoptez doit déjà exister sur chaque ordinateur et doit bénéficier de droits administratifs. De même, les services Network Associates doivent être paramétrés pour se connecter au titre de LocalSystem.

**Pour exécuter SVCPWD, procédez comme suit :**

1. Cliquez sur **Démarrer**, pointez le curseur sur **Programmes**, puis sur **Invite de commande**.
2. A l'invite de commande, remplacez le répertoire indiqué par le répertoire programme de VirusScan.
3. Tapez cette ligne à l'invite :

   ```
   svcpwd <TEXTFILE.TXT>
   ```

   L'utilitaire vous demande alors d'entrer le nom d'utilisateur du compte que vous souhaitez voir utilisé par les services Network Associates.
4. Tapez un nom de compte ou appuyez sur ENTREE sans indiquer de nom pour utiliser le compte système existant sur l'ordinateur cible. Si vous tapez un nom d'utilisateur, assurez-vous de le faire précéder d'un nom de domaine.

   Pour utiliser le compte Client du domaine Mondomaine, par exemple, tapez `mondomaine\client`, puis appuyez sur ENTREE.

   **IMPORTANT :** SVCPWD indiquera aux services Network Associates sur chacun des ordinateurs que vous avez répertoriés dans le fichier texte d'utiliser les informations du compte que vous avez spécifié ici. Si le compte n'existe pas sur le serveur cible, SVCPWD interrompra l'exécution.
5. Si vous avez indiqué un nom d'utilisateur pour le compte, l'utilitaire vous invitera à entrer un mot de passe pour ce compte lorsqu'il se connectera à chacun des ordinateurs répertoriés dans le fichier texte. Si vous avez précisé d'utiliser le compte du système, l'utilitaire passera à l'étape suivante. A l'invite, entrez le mot de passe du compte d'utilisateur que vous souhaitez utiliser puis appuyez sur ENTREE.

   Lorsqu'il contactera chaque ordinateur répertorié, l'utilitaire cherchera les services Network Associates installés, puis les paramètrera tous pour utiliser le compte que vous avez spécifié.

   **AVERTISSEMENT :** N'exécutez *pas* SVCPWD au cours d'une opération d'analyse à la demande. Vous risqueriez d'entraver le fonctionnement du gestionnaire des tâches de Network Associates.

# “ Diffusion ” de tâches à la demande vers les postes de travail

Une fois que vous avez créé une tâche d'analyse à la demande sur votre propre ordinateur, vous pouvez enregistrer ses paramètres sous forme de fichier .VSC, puis envoyer la tâche vers d'autres postes de travail afin qu'ils les exécutent (voir “Utilisations des menus de VirusScan” à la page 133 pour plus de détails). Les utilisateurs de ces postes de travail n'ont qu'à double-cliquer sur le fichier .VSC que vous avez envoyé pour ouvrir VirusScan, préchargé avec les paramètres que vous avez enregistrés. Bien qu'il soit possible de transférer des fichiers .VSC par presque tous les moyens habituels - sous forme de pièces jointes aux courriers électroniques, ou en copiant le fichier directement dans le système cible -, cette procédure nécessite généralement la coopération de l'autre utilisateur.

VirusScan comprend également un autre utilitaire conçu expressément à cet effet : vous pouvez utiliser IMPTASK.EXE pour demander à l'autre poste de travail d'importer les paramètres de la tâche que vous avez enregistrés directement à partir de votre propre ordinateur. IMPTASK s'exécute à partir de la ligne de commande de Windows NT et nécessite un fichier .VSC en entrée que vous avez créé depuis le scanner autonome à la demande de VirusScan.

---

**Pour exécuter SVCPWD, procédez comme suit :**

1. Cliquez sur **Démarrer**, pointez le curseur sur **Programmes**, puis sur **Invite de commande**.

2. A l'invite de commande, remplacez le répertoire existant par le répertoire programme de VirusScan.

3. Tapez cette ligne à l'invite :

   ```
   imptask /file <SETTINGS.VSC>
   ```

   Celle-ci indique à la copie de VirusScan figurant sur votre poste de travail local d'importer les paramètres du fichier SETTINGS.VSC, ou de n'importe quel autre fichier .VSC que vous désignez.

   Pour demander à un autre ordinateur situé ailleurs sur le réseau d'importer le même fichier de paramètres, tapez cette ligne à l'invite :

   ```
   imptask /file <SETTINGS.VSC> /server \\<NOMORDINATEUR>
   ```

   En ajoutant l'option /SERVER, vous indiquez à IMPTASK de copier le fichier de paramètres sur l'ordinateur désigné sur la même ligne selon la convention d'affectation des noms.

# Network Associates Services de support

# B

## Améliorer la performance de votre produit Network Associates

Choisir les produits anti-virus et les logiciels de sécurité de Network Associates permet d'assurer 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 quatre niveaux de supports étendus dans le programme PrimeSupport* entreprise de Network Associates. Si vous êtes un particulier, vous avez la possibilité de choisir un plan adapté à vos besoins dans le programme PrimeSupport destiné aux particuliers.

## Options PrimeSupport destinées aux clients d'entreprise

Le programme PrimeSupport entreprise offre quatre plans de support:

- Le plan PrimeSupport KnowledgeCenter
- Le plan PrimeSupport Connect
- Le plan PrimeSupport Connect 24/7
- Le plan PrimeSupport Entreprise

Chaque plan 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.

## Le plan PrimeSupport KnowledgeCenter

Le plan PrimeSupport KnowledgeCenter vous donne accès à une gamme étendue d'informations regardant le support technique via une base de connaissances Network Associates en ligne, et vous fournit la possibilité de télécharger les mises à niveau des produits depuis 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, comme composante du package, aussi longtemps que durera votre abonnement.

Si vous l'avez acheté accompagné d'une licence définitive, vous pourrez acheter un plan PrimeSupport KnowledgeCenter moyennant une cotisation annuelle.

Pour recevoir votre mot de passe pour KnowledgeCenter ou pour faire enregistrer votre accord de licence PrimeSupport auprès de Network Associates, rendez-vous à:

http://knowledge.nai.com/

Votre formulaire complété sera transmis au centre du service clientèle de Network Associates. Vous devez soumettre ce formulaire avant de vous connecter au site PrimeSupport KnowledgeCenter.

Avec le plan PrimeSupport KnowledgeCenter, vous obtenez:

- Un accès illimité en ligne 24 heures sur 24 aux solutions techniques depuis une base de connaissance consultable sur le site web de Network Associates.
- Présentation de l'incident électronique et demande d'information
- Documents techniques, y compris les guides de l'utilisateur, les listes de FAQs, et les indications concernant la version
- Mises à jour en ligne des fichiers de données et mises à niveau en ligne des produits

## Le plan PrimeSupport Connect

Le plan PrimeSupport Connect vous fournit une assistance téléphonique aux principaux produits par l'intermédiaire de l'équipe expérimentée du support technique. Avec ce plan, vous obtenez:

- En Amérique du Nord, une assistance téléphonique fournie par le support technique du lundi au vendredi, de 08 heures à 20 heures (Heure du Centre des Etats-Unis) ;

- En Europe, Au Moyen-Orient, et en Afrique, une assistance téléphonique fournie par le support technique du lundi au vendredi, de 09 heures à 18 heures (heure locale), au tarif longue distance standard ou tarif international.
- Dans la région Asie Pacique, une assistance téléphonique fournie par le support technique du lundi au vendredi, de 08 heures à 18 heures AEST
- En Amérique Latine, une assistance téléphonique fournie par le support technique du lundi au vendredi, de 09 heures à 17 heures, heure du centre des Etats-Unis.
- Un accès illimité en ligne 24 heures sur 24 aux solutions techniques depuis une base de connaissance consultable sur le site web de Network Associates.
- Présentation de l'incident électronique et demande d'information
- Documents techniques, y compris les guides de l'utilisateur, les listes de FAQs, et les indications concernant la version
- Mise à jour des fichiers de données et mise à niveau des produits via le site Web de Network Associates ;

## Le plan PrimeSupport Connect 24/7

Le plan PrimeSupport Connect 24/7 vous fournit une assistance téléphonique 24 heures sur 24 aux principaux produits par l'intermédiaire de l'équipe expérimentée du support technique. Il vous est possible de vous abonner annuellement à PrimeSupport Connect 24/7 que vous achetiez un produit de Network Associates accompagné d'une licence d'abonnement ou d'une licence valable 1 an.

Le plan PrimeSupport Connect 24/7 dispose des caractéristiques suivantes:

- En Amérique du Nord, une assistance téléphonique fournie par le support technique du lundi au vendredi, de 08 heures à 20 heures (Heure du Centre des Etats-Unis) ;
- En Europe, Au Moyen-Orient, et en Afrique, une assistance téléphonique fournie par le support technique du lundi au vendredi, de 09 heures à 18 heures, au tarif longue distance standard ou tarif international.
- Dans la région Asie Pacifique, une assistance téléphonique fournie par le support technique du lundi au vendredi, de 08 heures à 18 heures AEST
- En Amérique Latine, une assistance téléphonique fournie par le support technique du lundi au vendredi, de 09 heures à 17 heures, heure du centre des Etats-Unis.

- Accès prioritaire au personnel du support technique pendant les heures ouvrables habituelles
- Réponses dans l'heure pour les problèmes urgents ayant lieu en dehors des heures ouvrables, y compris durant les week-ends et les périodes de vacances locales.
- Un accès illimité en ligne 24 heures sur 24 aux solutions techniques depuis une base de connaissance consultable sur le site web de Network Associates.
- Présentation de l'incident électronique et demande d'information
- Documents techniques, y compris les guides de l'utilisateur, les listes de FAQs, et les indications concernant la version
- Mise à jour des fichiers de données et mise à niveau des produits via le site Web de Network Associates ;

## Le plan PrimeSupport Entreprise

Le plan PrimeSupport Entreprise vous offre un support 24 heures sur 24, pro-actif et personnalisé par l'intermédiaire d'un ingénieur du support technique. 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 Entreprise vous aidera à mieux les prévenir. Toutefois, en cas d'urgence, PrimeSupport Entreprise vous indiquera le délai de réponse nécessaire avant l'arrivée prévue de l'aide. Il vous est possible de vous abonner annuellement à PrimeSupport Entreprise que vous achetiez un produit de Network Associates accompagné d'une licence d'abonnement ou d'une licence d'un an.

Avec le plan PrimeSupport Entreprise, vous obtenez:

- Un accès téléphonique illimité à un ingénieur technique assigné, 24 heures sur 24, 7 jours par semaine, y compris durant les week-ends et les périodes de vacances locales.

  - **REMARQUE :** La disponibilité du support varie selon les régions et n'existe pas dans certaines régions d'Europe, du Moyen-Orient, d'Afrique et d'Amérique Latine.

- Assistance téléphonique ou électronique pro-active fournie par un ingénieur assigné, aux intervalles de votre choix
- L'ingénieur du support technique répondra dans la demi-heure qui suit aux radiomessages, dans un délai d'une heure aux messages vocaux et dans un délai de 4 heures aux messages électroniques
- La possibilité d'assigner des contacts clients qui vous permet de désigner cinq personnes au sein de votre organisation qui pourront être contactées dans le cas de votre absence
- Le statut du site bêta en option qui vous donne accès aux tout nouveaux produits et technologie de Network Associates.
- Un accès illimité en ligne 24 heures sur 24 aux solutions techniques depuis une base de connaissance consultable sur le site web de Network Associates.
- Présentation de l'incident électronique et demande d'information
- Documents techniques, y compris les guides de l'utilisateur, les listes de FAQs, et les indications concernant la version
- Mises à jour en ligne des fichiers de données et mises à niveau en ligne des produits

## Commander le plan PrimeSupport pour l'entreprise

Pour commander un plan PrimeSupport, contacter votre agent commercial, ou

- En Amérique du Nord, appeler Network Associates au (408) 988-3832, du lundi au vendredi de 8:00 à 19:00 Heure du Centre des Etats-Unis. Appuyez sur la touche 3 de votre téléphone pour l'assistance commerciale.
- En Europe, au Moyen-Orient, en Afrique, contactez votre représentant local Network Associates. Les coordonnées des contacts figurent au début de ce manuel.

**Table B-1. Le plan PrimeSupport pour l'entreprise en un coup d'oeil**

| Plan Caractéristique | Knowledge Center | Connect | Connect 24/7 | Entreprise |
|---|---|---|---|---|
| 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<br>Amérique du Nord: 8:00-20:00 CT<br>Europe, Moyen-Orient, Afrique: 9h00-18h00 Heure locale<br>Asie-Pacifique: 8:00-18:00 AEST<br>Amérique latine: 9:00-17:00 CT | Du lundi au Vendredi, accès d'urgence hors horaires<br>Amérique du Nord: 8:00-20:00 CT<br>Europe, Moyen-Orient, Afrique: 9h00-18h00 Heure locale<br>Asie-Pacifique: 8:00-18:00 AEST<br>Amérique latine: 9:00-17:00 CT | Du lundi au Vendredi, accès d'urgence hors horaires<br>Amérique du Nord: 8:00-20:00 CT<br>Europe, Moyen-Orient, Afrique: 9h00-18h00 Heure locale<br>Asie-Pacifique: 8:00-18:00 AEST<br>Amérique Latine: 9:00-17:00 CT |
| Service téléphonique prioritaire | — | — | oui | oui |
| Support hors horaires | — | — | oui | oui |
| Ingénieur de support assigné | — | — | — | oui |
| Support pro-actif | — | — | — | oui |

**Table B-1. Le plan PrimeSupport pour l'entreprise en un coup d'oeil**

| Plan Caractéristique | Knowledge Center | Connect | Connect 24/7 | Entreprise |
|---|---|---|---|---|
| Contacts désignés | — | — | — | Au moins 5 |
| Charte de temps de réponse | Courrier électronique dans la journée (ouvrable) | Les appels aboutissent dans les 3mn, réponse dans la journée (ouvrable) | En une heure pour les problèmes urgents hors horaires | Radio-messagerie hors horaires: 30 minutes<br>Messagerie vocale : 1 heure<br>Messagerie électronique : 4 heures |

Les options PrimeSupport décrites dans le reste de ce chapitre ne sont disponibles qu'en Amérique du Nord. Pour obtenir plus d'informations sur les options PrimeSupport de formations et de conseils disponibles en dehors du continent nord-américain, consultez votre revendeur le plus proche. Les coordonnées des contacts figurent au début de ce manuel.

# Les options PrimeSupport pour les particuliers

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 spécifique de support inclus dépend du produit acheté. Les services inclus comprennent:

- Pour les logiciels anti-virus, des mises à jour gratuites de vos données de fichiers pendant la durée de vie de votre produit via le site Web de Network Associates, la fonction Mise à jour automatique de votre produit ou le service SecureCast. Vous pouvez également effectuer la mise à niveau de votre logiciel en utilisant votre navigateur Web pour visiter le site à l'adresse :

  http://www.nai.com/download/updates/updates.asp

- Des programmes (fichiers exécutables) de mises à niveau gratuites valables un an via le site web de Network Associates. Si vous avez acheté une version élaborée d'un produit Network Associates, vous recevrez des mises à jour 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 :

  http://www.nai.com/download/upgrades/upgrades.asp.

- Accès libre 24 heures sur 24, sept jours sur sept à un support en ligne ou électronique par le système de messagerie vocale et de télécopie de Network Associates, par le site Web de Network Associates et par d'autres services électroniques tels que America Online et CompuServe.

  Pour contacter les services électroniques de Network Associates

  - Appelez le système répondeur automatisé voix/fax 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 au service PrimeSupport KnowledgeBase: accès en ligne aux solutions techniques depuis une base de connaissance consultable, via la soumission des incidents électroniques et les documents techniques tels que les guides utilisateurs, les FAQs et les indications concernant la version. Visitez la KnowledgeBase à:

  http://knowledge.nai.com

- Trente jours supplémentaires de support technique dispensé par un technicien de Network Associates du lundi au vendredi, de 9 heures à 17 heures (Heure du Centre des Etats-Unis). La période de 30 jours dont vous disposez débute à la date de votre premier contact téléphonique avec le service support pour tous les produits Network Associates. Pour contacter le service support, appelez

  (972) 855-7044

  Si vous avez besoin d'un service support supplémentaire, Network Associates offre un choix de plans de support que vous pouvez acheter soit avec votre produit Network Associates soit après l'expiration des 30 jours de support supplémentaires. Ce sont :

  - **REMARQUE :** Les plans de support décrits ici ne sont disponibles qu'en Amérique du Nord. Contactez votre agent commercial local pour vous informer des options de support local.

- **Plan annuel Small Office/Home Office.** Ce plan vous donne un accès illimité au support technique durant les heures ouvrables habituelles, du lundi au vendredi de 9 heures à 17 heures, Heure du Centre des Etats-Unis.
- **Plan de paiement par incident.** Ce plan vous donne accès au support technique dès qu'un incident se produit, durant les heures ouvrables habituelles, du lundi au vendredi de 9 heures à 20 heures, Heure du Centre des Etats-Unis. Vous pouvez appeler un numéro gratuit, utiliser une carte de crédit pour la transaction, et voir votre appel transféré à l'équipe du support technique en quelques minutes.

  | | |
  |---|---|
  | Pour les logiciels VirusScan, Nuts & Bolts, Hurricane, Safe & Sound, ou 2000 Toolbox | (888) 847-8766 |
  | Pour les logiciels Dr Solomon et Virex | (800) 950-1165 |

- **Plan de paiement par minute.** Ce plan vous permet d'accéder au service support selon le besoin. Vous disposez de numéros d'accès gratuits au personnel du support technique sur une base prioritaire afin de minimiser votre temps d'attente. Vos deux premières minutes sont gratuites.

| | |
|---|---|
| Tous les produits excepté le logiciel de cryptage PGP | (900) 225-5624 |

- **Plan de Mises à niveau en ligne.** Ce plan vous offre la facilité d'accéder automatiquement aux mises à niveau des produits via les services en ligne ou électroniques de Network Associates
- **Plan du Disque/CD trimestriel.** Ce plan vous permet de recevoir des disques ou des CDs de mises à niveau sur une base trimestrielle, pour le cas où vous ne pouvez pas obtenir en ligne les mises à niveau des produits. Ce service est disponible uniquement pour les logiels McAfee VirusScan et NetShield.

## Comment joindre le support international destiné aux particuliers

Le tableau suivant présente la liste des numéros de téléphone du support technique présent internationalement. Les coûts spécifiques, la disponibilité du service, les horaires ouvrables et les détails du plan peuvent varier selon le pays. Consultez votre agent commercial ou un bureau régional de Network Associates pour plus de détails.

| Pays ou Région | Numéro de téléphone* | Panneau d'affichage 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 |
| Latin America | +55-11-5505-1009 | +55-11-5506-9100 |

* des coûts longue distance peuvent s'appliquer dans ce cas

## Commander un plan PrimeSupport pour les particuliers

Pour commander un plan annuel PrimeSupport Small Office / Home Office, un plan de paiement par incident, un plan de paiement par minute, un plan de mises à niveau en ligne, ou un plan comprenant un disque ou CD trimestriel pour vos produits Network Associates:

- En Amérique du Nord, appelez le Service Clientèle de Network Associates au (972) 278-6100
- Hors des Etats-Unis, contactez le centre de support technique régional de Network Associates le plus proche de votre emplacement pour plus d'informations. Certaines options de support peuvent n'être pas disponibles dans des régions déterminées.

# Conseils et formations de Network Associates

Le programme Total Service Solutions de Network Associates vous fournit des conseils d'experts ainsi qu'une formation complète susceptible d'accroître la sécurité et les performances de votre réseau. Le programme Total Service Solutions de Network Associates inclut la branche Network Associates Professional Consulting et le programme Total Education Services.

## Services Professionnels

Le programme des 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 son implémentation. 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.

### Les services Jumpstart

Pour une aide spécialisée dans la solution de problèmes spécifiques ou les questions de mise en application de logiciels, Network Associates offre un service Jumpstart qui vous fournit les outils dont vous avez besoin pour gérer votre environnement. Ce service peut inclure ces éléments:

- **Installation et optimisation.** Ce service comprend l'installation, la configuration et l'optimisation sur site de votre produit Network Associates par un consultant Network Associates, ainsi qu'une formation opérationnelle de base pour votre équipe concernant le fonctionnement du produit.
- **Selfstart knowledge.** Ce service comprend la venue sur site d'un consultant Network Associates pour vous aider dans la mise en application du nouveau produit et, dans certains cas, pour procéder à l'installation.
- **Proposal Development.** Ce service vous aide à évaluer quels sont les traitements, les procédures, le matériel, le logiciel dont vous avez besoin avant le lancement ou la mise à niveau des produits Network Associates afin qu'ensuite un consultant Network Associates élabore un projet dédié à votre environnement.

## Services de conseil Network

Les consultants Network Associates offrent leur expertise en analyse des protocoles, ainsi qu'une perspective désintéressée pour vous recommander des solutions appropriées au dépannage et à l'optimisation de votre réseau. Les consultants peuvent aussi contribuer leur compréhension intime des meilleures méthodes de gestion des réseaux et leurs relations dans le domaine pour accélérer l'évaluation des problèmes ainsi que leur solution via le support revendeur.

Vous avez aussi la possibilité de commander un service conseil personnalisé pour vous aider à planifier, concevoir, mettre en œuvre et gérer votre réseau. Ce qui pourra vous permettre d'évaluer l'impact du lancement de nouvelles applications, de systèmes d'exploitation réseaux, ou de supports d'interconnexion de réseaux.

Pour plus d'informations sur celles-ci, contactez le service Conseils de Network Associates au 1-800-395-3151 ou visitez le site Web de Network Associates à l'adresse suivante :

http://www.nai.com/services/consulting/consulting.asp

## Services Total Education

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 d'en enseigner les procédés 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 réseaux agréés.

Contactez votre agent commercial pour en apprendre plus sur ces programmes, appelez Network Associates Total Education Services au 1-800-395-3151, ou visitez le site web de Network Associates à:

http://www.nai.com/services/education/

# Utilisation de SecureCast C

## Introduction à 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.

Pour utiliser cette option, les utilisateurs (particuliers et entreprises) doivent installer le logiciel client BackWeb. Ensuite, les particuliers doivent s'abonner au canal SecureCast Home (également appelé canal SecureCast VirusScan). Les entreprises doivent s'abonner au canal Enterprise SecureCast.

---

❑ **REMARQUE :** Si vous êtes une entreprise, vous devez d'abord disposer d'un numéro de licence (numéro de série du produit) pour pouvoir vous abonner à Enterprise SecureCast.

Si vous n'avez pas ce numéro, veuillez contacter votre revendeur, votre distributeur ou le service clientèle de Network Associates au (+1) 408 988- 3832.

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/products/securecast/esc/grantreq.asp

OU BIEN

Envoyez un courrier électronique à l'adresse appropriée :

ESCRegistration@nai.com (Etats-Unis)

ESC-Registration-Europe@nai.com (Europe)

ESC-Registration-Asia@nai.com (Asie)

Que vous soyez un particulier ou une entreprise, BackWeb présente une gamme d'options permettant d'adapter le mode de liaison de BackWeb au canal SecureCast. L'aide en ligne concernant la configuration de BackWeb est disponible à l'adresse suivante :

http://www.backweb.com/doc/version30/Client/

**REMARQUE :** Si vous êtes une entreprise (mais non l'administrateur du réseau), renseignez-vous auprès de votre administrateur pour savoir à quel endroit effectuer la mise à jour de vos fichiers ou utilisez la fonction de mise à jour automatique des fichiers DAT de VirusScan. Reportez-vous au paragraphe “Configuration des options de mise à jour automatique des fichiers DAT” à la page 187 pour de plus amples informations.

# 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, Network Associates publie de nouveaux fichiers .DAT toutes les 4 à 6 semaines. 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 poursuit 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 SecureCast, vous recevrez automatiquement des téléchargements de ces fichiers de données communs :

- NAMES.DAT : comprend les noms de virus et autres informations dont l'utilisateur peut prendre connaissance en affichant la liste des virus.
- SCAN.DAT : comprend les données des chaînes de détection de tous les virus détectés.
- CLEAN.DAT : comprend les données des chaînes de suppression de tous les virus nettoyés.

En complément des fichiers .DAT communs cités ci-dessus, il vous est également possible de recevoir des fichiers supplémentaires, selon les antivirus ou les programmes de protection que vous utilisez :

- WEBSCANX.DAT ou INTERNET.DAT : comprend les données des chaînes de détection des applets Java hostiles et des contrôles ActiveX. WebShieldX et VirusScan utilisent ces fichiers.
- MCALYZE.DAT : comprend les données des chaînes de détection concernant la détection des virus polymorphes complexes. Les produits 32 bits de Network Associates associés aux versions 3.0.0 à 3.1.4 utilisent ce fichier.
- POLYSCAN.DAT : comprend les données des chaînes de détection concernant la détection des virus polymorphes complexes. Les produits 32 bits de Network Associates associés aux versions 3.1.5 et supérieures utilisent ce fichier.

# Configuration requise

- Windows 95 ou supérieure, ou Windows NT
- 100 Mo minimum d'espace libre sur le disque dur. Home SecureCast (client et chaîne) 7Mo, plus 3 à 6Mo par téléchargement. Enterprise SecureCast (client et canal) 15Mo, plus 6 à 6,5Mo par téléchargement.
- Une connexion active à Internet, en accès direct ou distant, pour un minimum d'une heure par semaine.

# Fonctions de SecureCast

- SecureCast utilise un logiciel client développé avec les technologies BackWeb.
- SecureCast supprime le besoin de télécharger des fichiers de mise à jour à partir des services électroniques de Network Associates.
- SecureCast fonctionne de manière invisible en arrière-plan ; il permet ainsi à d'autres applications d'avoir la priorité en n'utilisant votre connexion Internet que lorsqu'elle est libre. Cependant, vous pouvez configurer votre ordinateur de bureau client pour que les téléchargements de SecureCast disposent d'une priorité supérieure.
- SecureCast fonctionne avec la plupart des systèmes firewall d'entreprise.
- SecureCast prend en charge les connexions TCP/IP 32 bits des abonnés aux canaux Enterprise SecureCast et Home SecureCast, et propose des connexions autres qu'Internet aux particuliers utilisant un accès distant asynchrone par modem.
- SecureCast livre des fichiers .ZIP, .EXE et .DAT à votre ordinateur de bureau sous la forme de InfoPaks BackWeb.

## Services gratuits

- Livraison automatique de fichiers .DAT, généralement disponibles vers le milieu du mois.
- Alertes contre les derniers virus dangereux identifiés.
- Annonces des dernières versions de logiciel et produits associés.

# Chaîne VirusScan SecureCast

SecureCast peut être installé à partir de nombreux CD-ROM de Network Associates. Si votre logiciel n'inclut pas SecureCast, vous pouvez le télécharger sur le Web.

- si vous êtes un particulier, allez à l'adresse suivante :

  http://download.mcafee.com/securecast/scast.asp

- si vous êtes une entreprise, allez à l'adresse suivante :

  http://www.nai.com/products/securecast/esc/default.asp

# Installation de BackWeb Client et SecureCast

Paramétrage de SecureCast et de BackWeb Client en trois phases :

- Télécharger et installer BackWeb (Étape 1 à Étape 12).
- Configurer BackWeb (Étape 13 à Étape 19).
- S'enregistrer pour recevoir SecureCast InfoPaks via BackWeb (Étape 20 à Étape 29).

## Phase 1 : Télécharger et installer BackWeb

1. Sélectionnez SecureCast parmi les choix du CD-ROM d'installation ou localisez le fichier que vous avez téléchargé sur le Web et double-cliquez sur son icône :
   - La version destinée aux particuliers s'appelle VS_BWClient.EXE.
   - La version destinée aux entreprises s'appelle ESC_BWClient.EXE.
2. Une boîte de dialogue vous avertit que vous êtes sur le point d'installer BackWeb (Figure C-1).

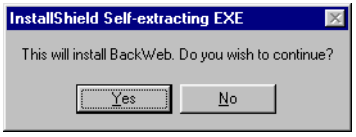



**Figure C-1. Boîte de dialogue du fichier InstallShield Self-extracting**

Cliquez sur **Oui** pour procéder à l'installation. La fenêtre de progression d'Install Shield Self-extracting EXE apparaît (Figure C-2).

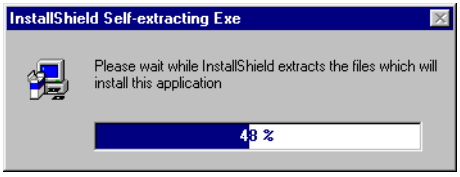



**Figure C-2. Fenêtre de progression d'InstallShield Self-extracting Exe**

Dès que les fichiers d'installation nécessaires ont été extraits, l'écran de **bienvenue** d'InstallShield pour BackWeb s'affiche (Figure C-3 à la page 228).

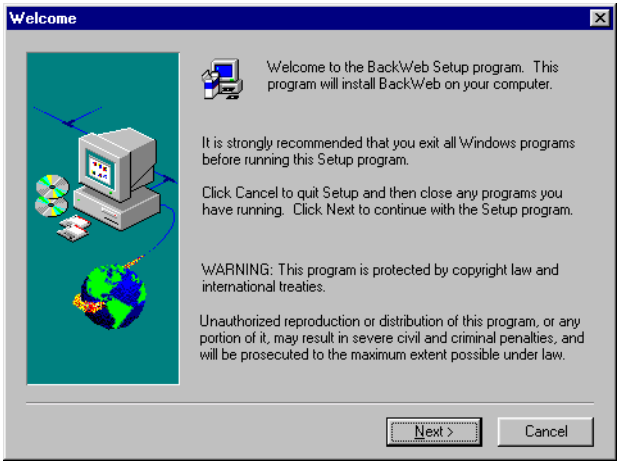



**Figure C-3. Écran de bienvenue d'InstallShield**

3. Lisez les instructions et les avertissements affichés. Cliquez sur **Suivant**. L'accord de licence BackWeb apparaît (Figure C-4).

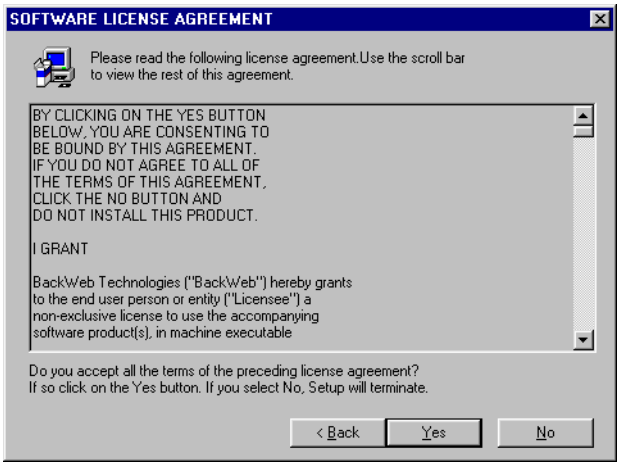



**Figure C-4. Écran Accord de licence du logiciel BackWeb**

Si vous acceptez les termes et conditions de l'accord de licence, cliquez sur **Oui** pour continuer. L'écran **Choisir l'emplacement de destination** s'affiche (Figure C-5).

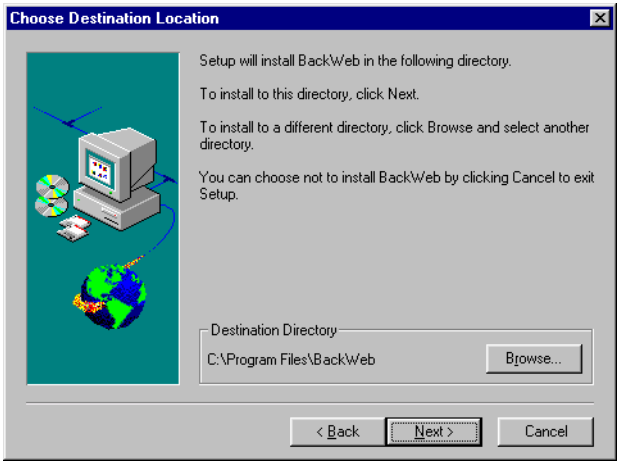



**Figure C-5. Écran Répertoire de destination BackWeb**

4. Notez l'emplacement où le programme va être installé. Cliquez sur **Suivant** pour accepter l'emplacement par défaut ou sur **Parcourir** pour sélectionner un emplacement différent pour les fichiers programme. Après avoir choisi un autre répertoire de destination, vous revenez à l'écran **Choisir l'emplacement de destination** . Si ce dernier vous convient, cliquez sur **Suivant**. InstallShield affiche un compteur de progression de l'installation de BackWeb (Figure C-6).

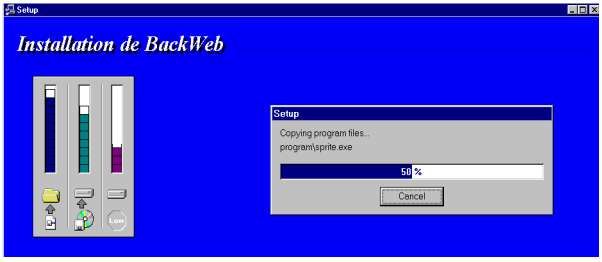



**Figure C-6. Fenêtre de progression de l'installation de BackWeb**

Une fois l'installation terminée, l'écran **Type de connexion** d'InstallShield apparaît (Figure C-7 à la page 230).

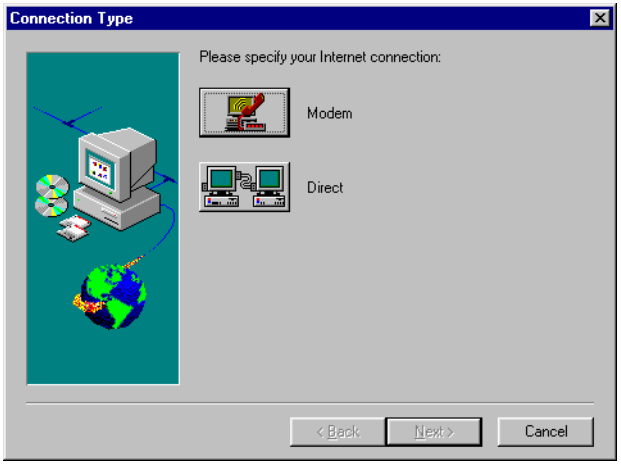



**Figure C-7. Écran Type de connexion d'InstallShield**

5. Cliquez soit sur le bouton **Modem**, soit sur le bouton **Direct** (c'est-à-dire une connexion en réseau local) pour spécifier le type de connexion Internet que vous utilisez.

   - Si vous sélectionnez **Modem**, passez à l'étape 10.
   - Si vous sélectionnez **Direct**, l'écran **Mode de communication** apparaît (Figure C-8). Passez à l'étape 6.

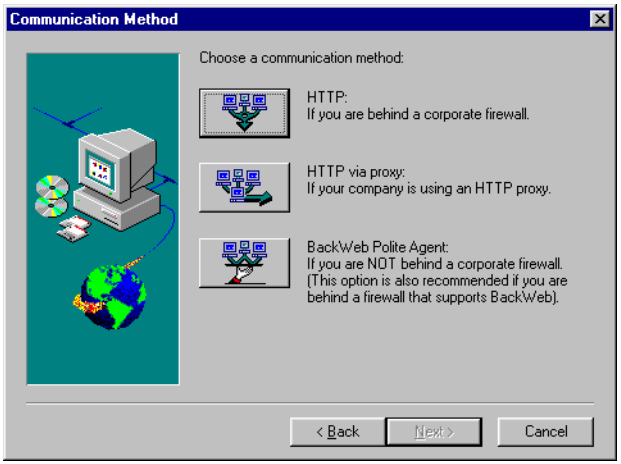



**Figure C-8. Écran Mode de communication d'InstallShield**

6. Cliquez sur le bouton symbolisant le mode de communication qu'utilise votre ordinateur pour Internet.

   - Si vous sélectionnez **HTTP**, c'est-à-dire si votre société n'utilise pas de serveur proxy pour se connecter à Internet, passez à l'étape 10.
   - Si vous sélectionnez **HTTP via proxy**, passez à l'étape 7.
   - Si vous sélectionnez **BackWeb Polite Agent**, passez à l'étape 10.

   ---

   ☐ **REMARQUE :** Le BackWeb Polite Agent vous permet de contrôler la façon dont BackWeb est relié à d'autres applications susceptibles de s'exécuter lorsque des InfoPaks arrivent sur votre bureau. Pour de plus amples informations, consultez l'aide en ligne de BackWeb à l'adresse suivante :

   http://www.backweb.com/doc/version30/Client/

   Reportez-vous en particulier à Application Politeness, sous Personnalisation de BackWeb, dans la section Premiers pas.

   ---

7. Si vous avez sélectionné **HTTP via proxy**, l'écran **Installation du proxy HTTP** apparaît (Figure C-9).

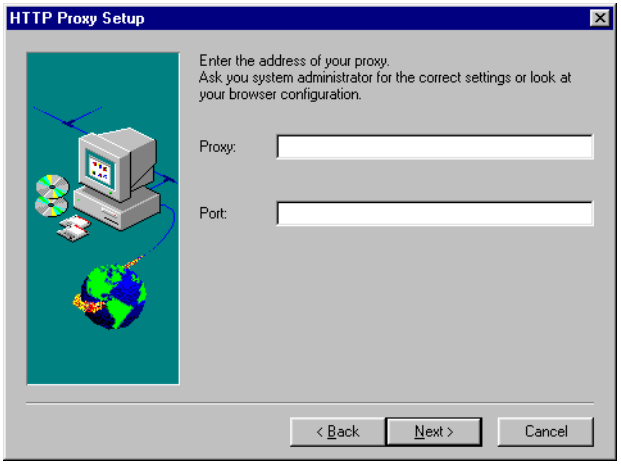



**Figure C-9. Écran Installation du proxy HTTP d'InstallShield**

8. Entrez l'identification du proxy et son port. Cliquez sur **Suivant** L'écran **Authentification du proxy** apparaît (Figure C-10 à la page 232).

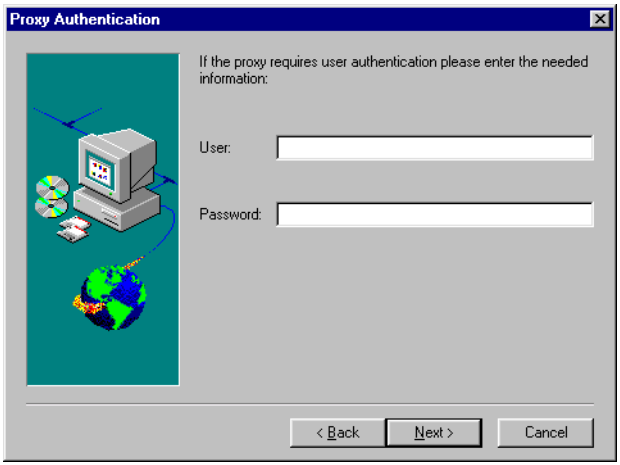



**Figure C-10. Écran Authentification du proxy d'InstallShield**

9. Si le serveur proxy requiert l'authentification de l'identité de l'utilisateur, entrez le nom d'utilisateur et le mot de passe autorisant l'accès. Puis cliquez sur **Suivant**.

10. L'écran **Installation terminée** d'InstallShield apparaît (Figure C-11).

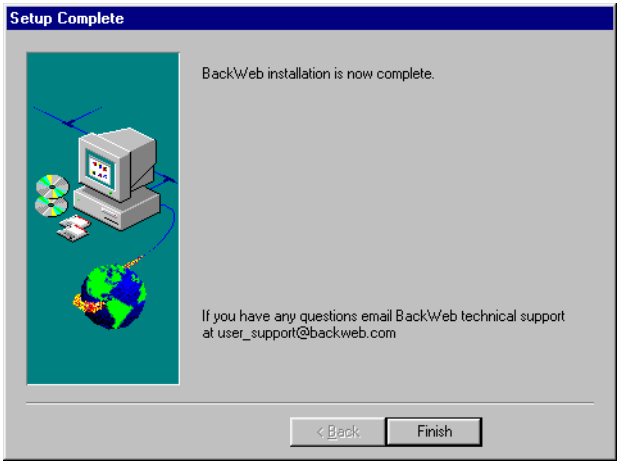



**Figure C-11. Écran Installation terminée d'InstallShield**

11. Cliquez sur **Terminer** pour mettre fin à la première phase du processus d'installation. Un message indiquant que BackWeb est prêt à recevoir des InfoPaks s'affiche (Figure C-12). Il s'agit des paquets d'informations comprenant les fichiers .DAT mis à jour, les alertes concernant les nouveaux virus et les autres messages importants envoyés par Network Associates.

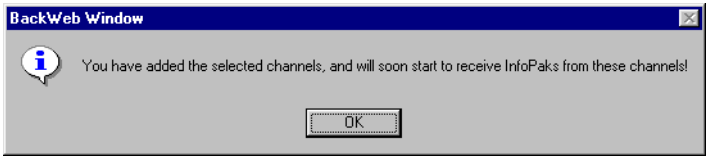



**Figure C-12. Message Installation terminée de BackWeb**

**REMARQUE :** Le message présenté ici s'affiche pendant l'installation de la version de SecureCast à utiliser avec les produits Network Associates destinés au particuliers. Un message légèrement différent s'affiche au cours de l'installation de la version de SecureCast à utiliser avec un logiciel bénéficiant d'une licence pour les environnements d'entreprise.

12. Cliquez sur **OK** et passez à la deuxième phase du processus d'installation de SecureCast.

## Phase 2 : Configurer BackWeb

13. L'écran **BackWeb Installation rapide** apparaît (Figure C-13).


**Figure C-13. Écran BackWeb Installation rapide**

14. Cliquez sur **Suivant**. L'écran **BackWeb InfoPaks** apparaît (Figure C-14).

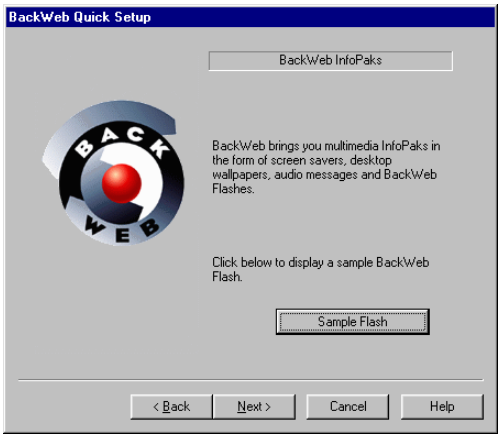



**Figure C-14. Écran BackWeb Installation rapide InfoPaks**

15. Cliquez sur **Sample Flash** pour obtenir une démonstration des différents styles de messages InfoPak. Une fois la démonstration terminée, cliquez sur **Suivant**. L'écran **BackWeb Auto-player** apparaît (Figure C-15).

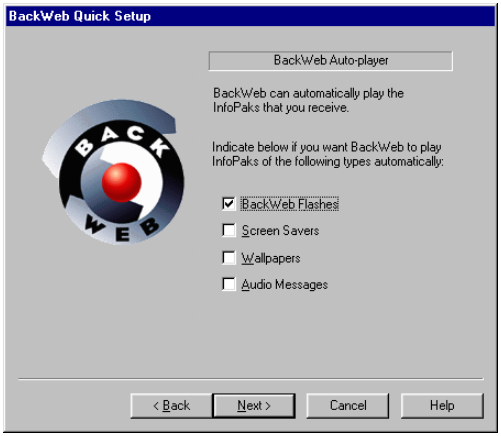



**Figure C-15. Écran BackWeb Installation rapide Auto-player**

16. Sélectionnez les types de messages InfoPak que vous souhaitez voir afficher par BackWeb. Les types disponibles sont : **BackWeb Flashes**, **Économiseurs d'écran**, **Fond d'écran** et **Messages sonores**. Après avoir effectué votre choix, cliquez sur **Suivant**. L'écran **Canaux BackWeb** apparaît (Figure C-16).


**Figure C-16. Écran BackWeb Installation rapide Canaux**

17. Cliquez sur **Répertoire des canaux** si vous souhaitez vous abonner à d'autres canaux BackWeb, en plus de SecureCast. Une fois vos sélections spécifiées, cliquez sur **Suivant**. L'écran **BackWeb Disk Space** apparaît (Figure C-17).


**Figure C-17. Écran BackWeb Disk Space**

18. Servez-vous des boutons pour indiquer le volume d'espace disque de votre ordinateur que vous souhaitez affecter aux InfoPaks que livre BackWeb. Une fois vos sélections spécifiées, cliquez sur **Suivant**. L'écran **BackWeb Installation réussie** apparaît (Figure C-18).

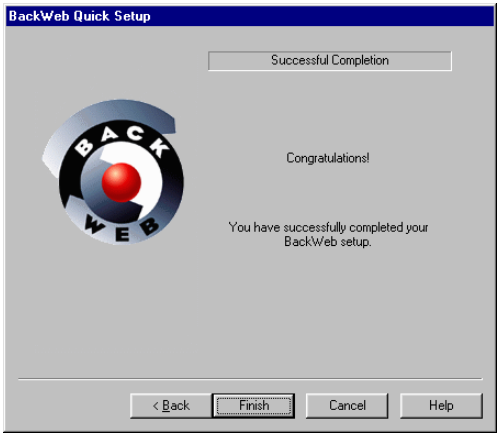



**Figure C-18. Écran BackWeb Installation réussie**

19. Cliquez sur **Terminer** pour passer à la troisième phase du processus d'installation de SecureCast.

## Phase 3 : Enregistrez-vous pour recevoir les InfoPaks de SecureCast via BackWeb.

20. L'interface BackWeb est désormais intégralement visible (Figure C-19 à la page 237). Le premier InfoPak que livre BackWeb est le formulaire d'enregistrement à SecureCast.

---

**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. Poursuivez à l'étape 21.

Si vous êtes un particulier et disposez d'une connexion moyennement rapide ou si le trafic est particulièrement dense sur le site de SecureCast site ou le vôtre, il est possible que la fenêtre n'affiche aucun InfoPaks. Dans ce cas, réduisez ou fermez la fenêtre BackWeb. Après un laps de temps, vous recevrez un message clignotant. Cliquez sur ce dernier et poursuivez à l'étape 22.

---

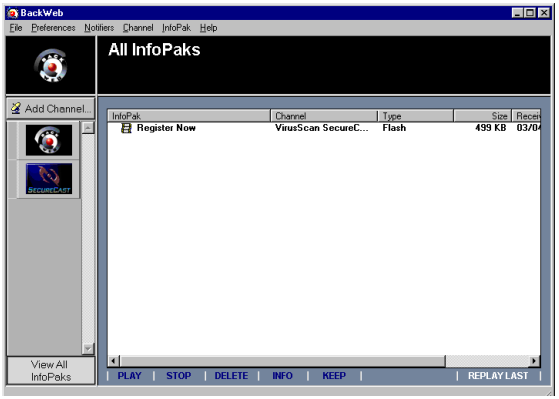



**Figure C-19. Interface utilisateur BackWeb**

21. Lorsque la mention **Enregistrer maintenant** apparaît dans la fenêtre, double-cliquez dessus. Le drapeau SecureCast Flash apparaît (Figure C-20).


**Figure C-20. Drapeau SecureCast Flash**

22. Cliquez sur le drapeau. L'écran de **bienvenue de Network Associates** apparaît (Figure C-21).

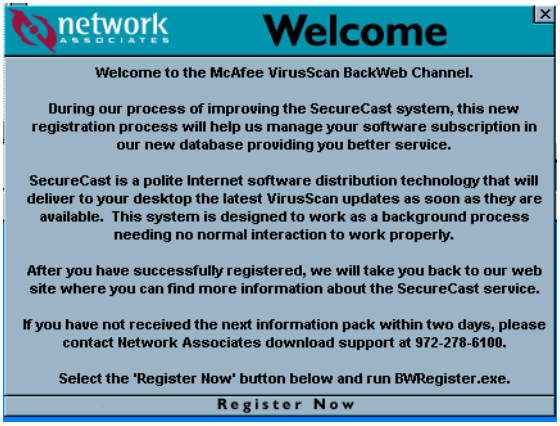



**Figure C-21. Écran de bienvenue de Network Associates**

23. Lisez les informations. Puis cliquez sur **Enregistrer maintenant** dans le bas de l'écran. Le dossier **Boîte aux lettres** que BackWeb a créé au cours de l'installation apparaît ; il contient l'icône de **BW Register.** (Figure C-22).

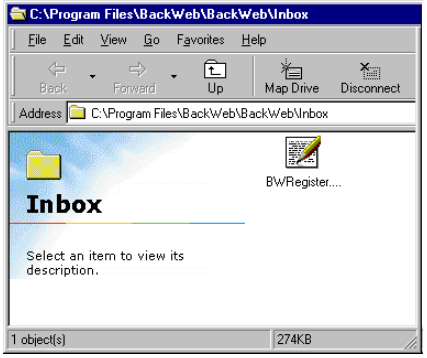
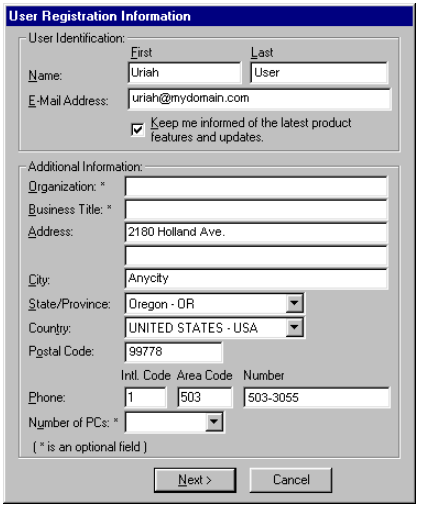
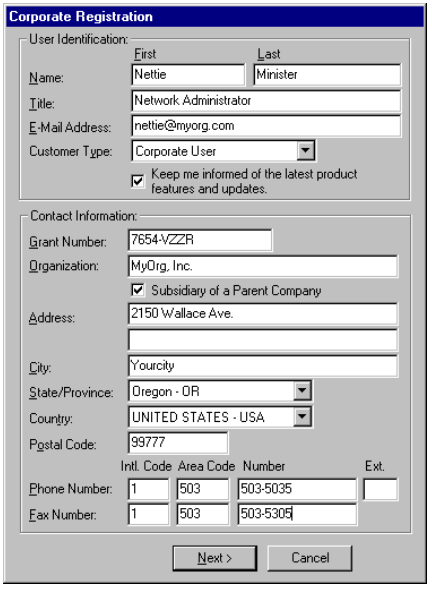



**Figure C-22. Dossier Boîte aux lettres BackWeb**

24. Double-cliquez sur l'icône **BW Register. . .** Un formulaire d'enregistrement s'affiche. Le formulaire destiné aux particuliers est différent de celui destiné aux entreprises (Figure C-23).




Formulaire d'enregistrement pour les particuliers




Formulaire d'enregistrement pour les entreprises

**Figure C-23. Formulaire d'enregistrement pour les utilisateurs de SecureCast**

25. Fournissez les informations demandées. Une fois vos sélections spécifiées, cliquez sur **Suivant**.

---

**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.

---

- Si vous ne le faites pas, la boîte de dialogue **Informations sur la société mère** apparaît (Figure C-24). Passez à l'étape 26.
- Si vous avez décoché la case **Filiale d'une société mère**, passez à l'étape 27.

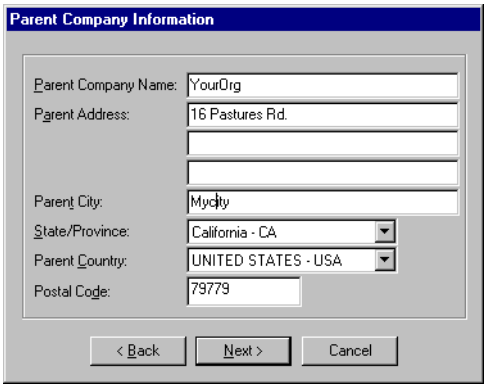



**Figure C-24. Formulaire d'informations sur la société mère SecureCast**

26. Si votre entreprise est une filiale d'une autre entreprise, des informations concernant cette dernière vous sont demandées. Une fois vos sélections spécifiées, cliquez sur **Suivant**. La boîte de dialogue **Configuration de communication du proxy** apparaît (Figure C-25 à la page 240).

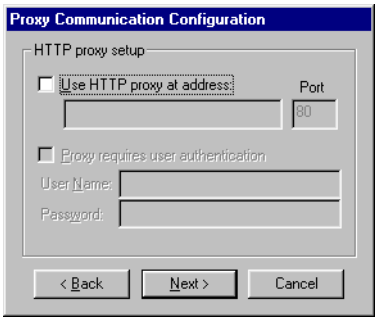



**Figure C-25. Configuration de communication du proxy SecureCast**

27. Si vous utilisez un proxy HTTP, veuillez fournir les informations demandées :

    - Cochez la case **Utiliser un proxy HTTP à l'adresse**.
    - Entrez l'adresse du proxy HTTP et confirmez que c'est le bon port qui est affiché.
    - Sélectionnez **Le proxy exige l'authentification des utilisateurs** le cas échéant, et entrez vos nom d'utilisateur et mot de passe.

28. Une fois vos sélections spécifiées, cliquez sur **Suivant**. L'écran **État des activités en ligne** apparaît, montrant la progression du processus d'enregistrement (Figure C-26).

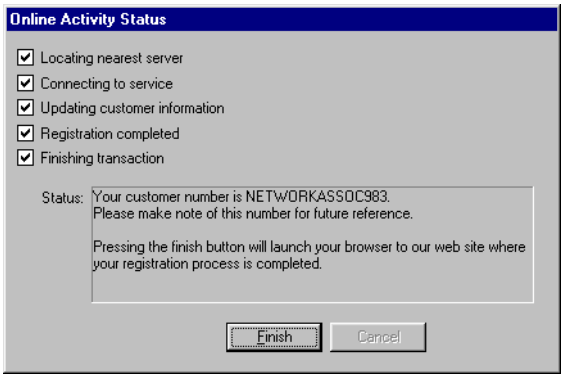



**Figure C-26. Écran État des activités en ligne de SecureCast**

29. 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-27 :

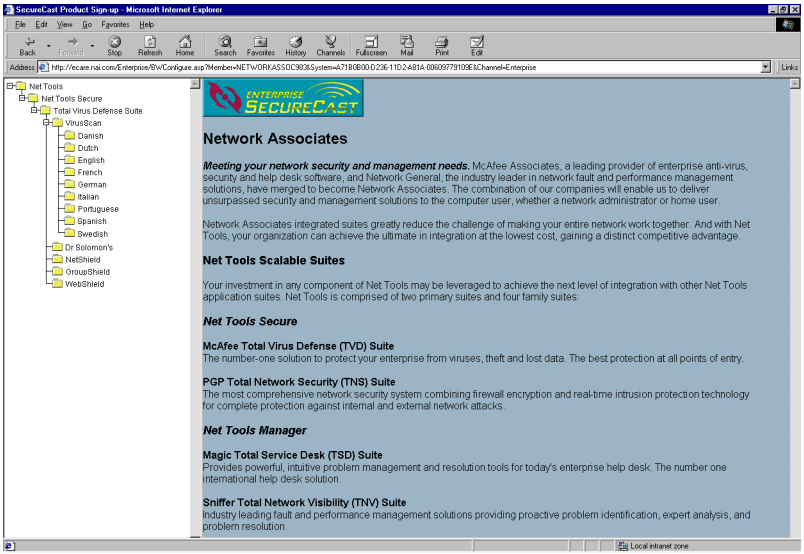



**Figure C-27. Service électronique de clientèle d'entreprise de SecureCast**

Si vous utilisez un produit destiné aux particuliers, la fenêtre ressemble à celle représentée dans la Figure C-28 à la page 242.

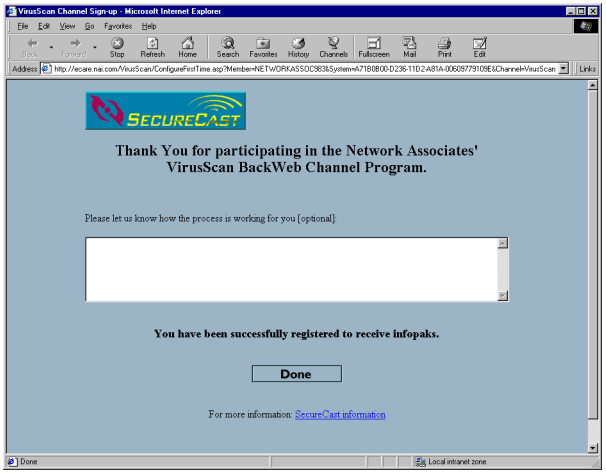



**Figure C-28. Service électronique de clientèle particuliers de SecureCast**

# Dépannage d'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 " or " Erreur de la base de données : Impossible de se connecter à la source de données " s'affichent, cela signifie que le serveur SecureCast rencontre un problème de base de données. Essayez de renvoyer votre formulaire ou de renouveler l'opération ultérieurement. Si ces problèmes persistent, veuillez contacter le service de téléchargement de Network Associates (du lundi au vendredi, de 8 HEURES à 20HEURES (heure du Centre des États-Unis) au (+1) 972 278-6100.

# Suspension de l'abonnement à SecureCast

**Suivez les étapes suivantes pour suspendre ce service à tout moment :**

1. Dans la zone de liste figurant à gauche de l'interface BackWeb, sélectionnez le service SecureCast auquel vous êtes abonné (Enterprise SecureCast ou VirusScan SecureCast).

2. Cliquez avec le bouton droit de la souris et sélectionnez **Suspension de l'abonnement**. Tous les InfoPaks répertoriés dans la fenêtre SecureCast seront supprimés et vous ne les recevrez plus.

# Ressources de prise en charge

## SecureCast

Si vous avez des questions supplémentaires sur SecureCast, consultez le Forum Aux Questions SecureCast à l'adresse suivante :

http://www.nai.com/products/securecast/esc/enterprise_faq.asp

## BackWeb

- Pour une description générale de BackWeb et des InfoPaks, reportez-vous à l'aperçu BackWeb :

  http://www.nai.com/products/securecast/anchor.asp

- Pour obtenir un guide complet sur BackWeb (comprenant des conseils de dépannage supplémentaires), cliquez sur le signet du manuel de l'utilisateur BackWeb :

  http://www.backweb.com/doc/version30/

- Pour résoudre les problèmes notoires conséquents à l'exploitation de BackWeb, veuillez contacter le service de téléchargement de Network Associates (du lundi au vendredi, de 8 HEURES à 20 HEURES au (+1) 972 278-6100.

# Index

## A

## B

## C

## D

## E

## F

## G



## H



## I

## N



## O

## P

## Q



## R

## S

## T

## U



## V

## W



## Z