eTrust™ Antivirus

Manuel de l'administrateur

7.1

Computer Associates®

G00417-2F

Table des matières

Chapitre 1: A propos des virus

Chapitre 2: Pour obtenir les mises à jour de signatures

Chapitre 3: Utilisation des options d'analyse et de sélection

Chapitre 4: Utilisation de l'analyseur local

Chapitre 5: Utilisation du moniteur temps réel

Chapitre 6: Planification de jobs d'analyse

Chapitre 7: Affichage et gestion des journaux

Chapitre 8: Utilisation de l'affichage de l'administrateur

Chapitre 9: Utilisation de l'utilitaire d'installation à distance

Chapitre 10: Utilisation de disquettes de secours pour Windows 9x

Chapitre 11: Utilisation du gestionnaire Alert

Chapitre 12: Intégration avec Unicenter

Annexe A: Installation du logiciel antivirus pour UNIX

Annexe B: Installation et démarrage de eTrust Antivirus pour Macintosh OS X

Annexe C: Installation du logiciel antivirus pour NetWare

Annexe D: Utilisation du programme de console ETRUSTAV

Annexe E: Utilisation du fichier de commande de l'installation

Annexe F: Fichier InoDist.ini

Annexe G: Installation de la connexion à la source de données ODBC

Annexe H: Installation et utilisation de l'analyseur eTrust Antivirus pour un système de fichiers NetApp

Annexe I: Installation automatique de eTrust Antivirus

Index

Chapitre

1

A propos des virus

Les menaces d'infection par un virus constituent le principal problème de sécurité pour toute personne utilisant un ordinateur. Un virus ou une infection informatique est un programme informatique pouvant détruire des informations sur votre poste de travail. Semblable à un virus biologique, un virus informatique peut se reproduire en se nichant dans d'autres fichiers, en général des programmes exécutables. Lorsqu'ils sont isolés (non exécutés comme par exemple dans un fichier compressé), les virus informatiques ne sont pas dangereux, mais dès qu'ils sont ouverts, ils peuvent occasionner d'importants dommages.

Pour être classé comme virus, un fichier suspect doit pouvoir :

- se répliquer,
- se nicher dans d'autres exécutables.

Il existe de nombreux types d'infections, notamment les infections de fichiers, les virus de macro, les vers et les chevaux de Troie

Infection par un virus

Les infections peuvent se propager par l'intermédiaire de messages électroniques ou de téléchargements à partir d'Internet, de disquettes ou de connexions à des réseaux. Elles sont parfois transmises accidentellement dans les progiciels. Les virus ne peuvent pas se développer tout seuls ; ils doivent être exécutés pour pouvoir causer des dommages. Les virus de secteur d'amorçage se multiplient lorsqu'un utilisateur amorce par inadvertance un poste de travail avec une disquette infectée. Les virus de macro peuvent se propager simplement par l'ouverture d'un document infecté.

Des ordinateurs non protégés connectés à Internet, au Web et à des systèmes de messagerie peuvent être infectés et propager rapidement des infections. Des fichiers malveillants joints dans des courriers non sollicités sont capables de se multiplier très vite et de paralyser votre réseau.

Symptômes d'infection informatique

Les symptômes d'infection varient en fonction du virus spécifique infectant votre système. La liste suivante contient les symptômes que vous risquez de rencontrer le plus souvent.

- Votre écran affiche un message tel que « Votre PC est lent comme une tortue ! »
- Votre écran affiche des motifs graphiques étranges tels que des balles rebondissantes.
- La taille des fichiers augmente. Les changements sont parfois tellement importants qu'il devient impossible de charger ces fichiers dans la mémoire. Mais le plus souvent, le changement de taille est peu important.
- Le tampon horodateur d'un fichier est modifié. Il est possible que vous trouviez un fichier *.com ou *.exe comportant un tampon horodateur plus récent que le moment où vous l'avez chargé.
- Vous recevez un message d'erreur concernant l'écriture d'un disque protégé même si votre application n'est pas en train d'essayer d'effectuer une opération en écriture.
- Le chargement des programmes prend plus de temps bien que la configuration de votre ordinateur n'ait pas été modifiée.
- Votre ordinateur s'exécute apparemment beaucoup plus lentement qu'il n'est normal.
- Votre ordinateur dispose de moins de mémoire disponible qu'il n'est normal.
- Les mêmes problèmes surgissent sur plusieurs ordinateurs.
- Vous recevez un message d'erreur « Commande ou nom de fichier incorrect » alors que vous êtes sûr que le fichier est sur le disque.
- Vous ne pouvez pas accéder à une unité qui existe pourtant.
- CHKDSK découvre soudain des secteurs endommagés sur plusieurs ordinateurs.
- Des problèmes persistants se produisent sur votre ordinateur, comme par exemple des difficultés à copier des fichiers.
- Votre ordinateur se bloque souvent.

Si votre ordinateur présente un ou plusieurs de ces symptômes, il est possible qu'il soit infecté. Etant donné qu'il est difficile de déterminer si ces symptômes sont liés à une infection, le logiciel antivirus de Computer Associates vous permet de confirmer si votre poste de travail est infecté.

Conséquences d'une infection informatique

Toutes les infections n'endommagent pas votre ordinateur. Certaines sont simplement gênantes car elles se reproduisent sans arrêt ou affichent d'étranges graphiques ou messages sur votre écran. La plupart des virus sont furtifs et demeurent cachés jusqu'à leur exécution.

Si une infection cause des dommages, ces derniers varient en fonction du type d'infection contaminant votre système. En général, les virus peuvent agir sur votre ordinateur de la façon suivante :

- Bloquer votre ordinateur
- Effacer, modifier ou masquer des fichiers
- Brouiller les données de votre disque dur
- Attaquer et brouiller la table d'allocation de fichier (FAT)
- Attaquer et brouiller la table des partitions
- Formater votre disque dur

Types de virus

Les virus sont classés selon leur mode de propagation et d'infection de l'ordinateur.

Voici une liste des types de virus les plus répandus et de leurs effets.

Nom du virus	Description
virus de secteur d'amorçage	Ces virus remplacent le secteur d'amorçage initial du disque (contenant le code exécuté lors de l'amorçage du système) par leur propre code, si bien que le virus est toujours chargé dans la mémoire avant toute autre programme. Cela signifie que le virus s'exécute à chaque fois que vous démarrez votre ordinateur. Une fois dans la mémoire, le virus peut rendre votre disque de démarrage inutilisable ou contaminer d'autres disques.
virus de secteur d'amorçage maître	Ces virus écrasent le secteur d'amorçage maître du disque (table des partitions). Ces virus sont difficiles à détecter car de nombreux outils d'examen du disque ne vous permettent pas de voir le secteur de partition qui est le premier secteur de votre disque dur.

Nom du virus	Description
virus de macro	Ces virus sont écrits dans le langage macro de programmes informatiques spécifiques tels que les logiciels de traitement de texte ou les tableurs. Les virus de macros infectent les fichiers (et non le secteur d'amorçage ou la table des partitions) et peuvent résider dans la mémoire lors de leur exécution. Ils peuvent être exécutés lorsque vous accédez au document d'un programme ou être déclenchés par des actions d'utilisateurs telles que certaines frappes au clavier ou des sélections de menus. Les virus de macros peuvent être stockés dans n'importe quel type de fichier et sont propagés par des transferts de fichiers ou des courriers électroniques.
virus de fichiers	Ces virus infectent d'autres programmes lorsqu'un programme infecté est exécuté. Ils ne demeurent pas dans la mémoire si bien qu'ils n'infectent pas le système. Tout comme les virus résidant dans la mémoire, les virus non-résidents se joignent à des fichiers exécutables. Ces virus modifient souvent les informations concernant les attributs des fichiers, ainsi que la taille, l'heure et la date du fichier.
virus multipartie	Ces virus combinent les caractéristiques des virus résidant dans la mémoire, des virus de fichiers et des virus de secteur d'amorçage.

D'autres types d'infections et d'attaques existent, comme les vers et les attaques par saturation (dénis de service – DDOS). Les vers sont similaires aux virus dans la mesure où ils réalisent des copies d'eux-mêmes. Lorsqu'un ver est exécuté, il cherche à infecter d'autres systèmes, plutôt que des parties de système. Les attaques par saturation installent des fichiers cachés sur des systèmes à leur insu. Les fichiers cachés sont ensuite activés ultérieurement afin d'effectuer des opérations malveillantes sur un autre système.

Caractéristiques des virus

Les différents types de virus peuvent présenter différentes caractéristiques de comportement basées sur leur fonctionnement.

Type de virus	Comportement
virus résidant en mémoire	Ces virus se chargent eux-mêmes dans la mémoire et prennent le contrôle du système d'exploitation. Les virus résidant dans la mémoire se joignent aux fichiers exécutables (tels que les fichiers *.exe, *.com et *.sys). Ces virus modifient souvent les informations concernant les attributs des fichiers, ainsi que la taille, l'heure et la date du fichier.

Type de virus	Comportement
virus furtifs	Ces virus dissimulent leur présence. Tous les virus s'efforcent de se dissimuler d'une certaine manière, mais les virus furtifs s'y efforcent encore davantage. Par exemple, un virus furtif peut infecter un programme en ajoutant des octets au fichier infecté. Ensuite, dans l'entrée du répertoire du fichier infecté, il soustrait le même nombre d'octets pour donner l'impression que la taille du fichier n'a pas changé.
virus polymorphes	Ces virus modifient régulièrement leur apparence et leur signature (leur code identifiable). Par exemple, ils peuvent insérer un code parasite au milieu de l'exécution du fichier ou modifier l'ordre d'exécution. Ceci permet au virus d'éviter les méthodes de détection par analyse des signatures.

Solution antivirus de Computer Associates

Le logiciel antivirus de Computer Associates est une solution antivirus performante pour le réseau de votre entreprise ou votre poste de travail individuel. Il peut protéger vos postes de travail fonctionnant sous Windows, UNIX, Macintosh OS X et NetWare. Ce logiciel est certifié par l'ICSA (International Computer Security Association) capable de détecter 100% des virus qui existent « dans la nature ». Ses fonctionnalités comprennent une interface utilisateur de style Windows, l'intégration avec l'Explorateur Windows et des mises à jour mensuelles et gratuites de signatures de virus proposées par Computer Associates. Des options sont disponibles pour la protection des systèmes de messagerie Lotus Notes et Microsoft Exchange. Des versions sont également disponibles pour Novell NetWare, Linux, Solaris, HP-UX et Macintosh OS X.

Références des plates-formes

Le terme Windows se réfère au système d'exploitation Windows de Microsoft, notamment Windows 95, Windows 98, Windows NT, Windows 2000, Windows 2003 et Windows XP. Sauf indication contraire, Windows se réfère à tout système d'exploitation Windows de Microsoft pris en charge par le logiciel antivirus de Computer Associates. Linux se réfère à Linux sur les machines Intel et System 390, Solaris se réfère uniquement à Solaris sur les machines Sun Sparc et HP-UX se réfère uniquement à HP-UX sur les machines HP PA-RISC.

Automatisez votre protection antivirus

Une fois que la solution logicielle antivirus de Computer Associates est configurée pour votre système ou réseau, vous pouvez automatiser votre protection antivirus. Toutes les opérations de mise à jour des signatures, de distribution, de surveillance, de configuration des paramètres d'analyse et d'analyse peuvent être configurées pour s'exécuter sans intervention. Les mises à jour des signatures peuvent être collectées de manière planifiée et distribuées à tous les ordinateurs de votre réseau antivirus sans qu'un administrateur n'ait besoin de gérer chaque ordinateur individuellement et sans temps d'arrêt des postes de travail.

Pourquoi avez-vous besoin d'une protection antivirus ?

Les infections informatiques sont devenues un problème majeur pour la gestion de la sécurité des réseaux et pour les utilisateurs individuels. Le coût des données perdues et le temps nécessaire à la restauration des ordinateurs infectés sont considérables dans le cas où un virus infecte votre réseau ou votre ordinateur.

Etant donné que les unités et répertoires partagés fournissent un accès aux applications et aux informations pour tous les utilisateurs d'un réseau, un fichier infecté sur un ordinateur peut se propager rapidement dans l'ensemble du réseau. C'est pourquoi il est essentiel que tous les ordinateurs soient protégés contre une infection.

Mode de fonctionnement du logiciel antivirus de Computer Associates

Le logiciel antivirus de Computer Associates utilise un détecteur de virus à base de règles, polymorphe et analytique pour détecter les virus connus. En outre, le moniteur temps réel vous offre une protection antivirus continue pendant que vous travaillez. Le moniteur temps réel est un pilote de périphérique virtuel (VxD) fournissant une protection antivirus spécifique aux systèmes basés sur Windows.

En ce qui concerne les systèmes basés sur UNIX, le moniteur temps réel utilise l'Event Notification Facility de Computer Associates (CAIENF) pour leur fournir une protection antivirus.

Sous NetWare, le moniteur temps réel utilise le sous-système NetWare FSHOOKS.

Sous OS X, le moniteur temps réel utilise une extension du noyau (KEXT).

Architecture	Dans un environnement en réseau utilisant une architecture client/serveur, un ou plusieurs serveurs centralisés permettent de garder une trace des informations concernant les ordinateurs de votre réseau antivirus et peuvent servir de points de distribution pour les mises à jour des signatures et des configurations. Un ordinateur local peut exécuter des analyses ou bien un administrateur autorisé peut gérer les ordinateurs à distance.
Découverte	Toutes les instances du logiciel antivirus de Computer Associates en cours d'exécution au sein de votre réseau peuvent être découvertes automatiquement.
Analyseur	Un moteur d'analyse à base de règles détecte les virus connus. Les virus inconnus sont détectés grâce à l'option Analyseur heuristique.
Notification	De nombreuses fonctionnalités de notification sont intégrées à ce produit. Microsoft Mail, les récepteurs d'appels alphanumériques et numériques, le protocole SMTP, le protocole SNMP, les rapports d'incidents (file d'impression) et les messages de diffusion réseau sont tous disponibles sur une plate-forme Windows pour assurer que vous soyez alerté en cas de détection d'un virus. La fonction de notification pour UNIX et OS X permet d'envoyer des messages au syslog. Il est possible d'appeler un script défini par l'utilisateur afin de fournir des messages de notification d'alerte personnalisés.
Rapport	Un mécanisme de rapport sophistiqué consigne toutes les opérations d'analyse qui peuvent être passées en revue à des fins de suivi et d'étude.
Traitement	Vous pouvez décider de la façon de traiter un fichier infecté avant sa découverte ou après une analyse.
Mises à jour des signatures	Les mises à jour des signatures sont régulièrement disponibles chez Computer Associates. Vous pouvez automatiser le processus de mise à jour des ordinateurs de votre réseau antivirus. Le poste de travail ne connaît pas de temps d'arrêt lors de la mise à jour.
Propagation et application des règles	Les administrateurs autorisés peuvent définir des options de règles antivirus, les propager dans le réseau et surveiller les paramètres des règles.

Méthodes de protection

Le logiciel antivirus de Computer Associates offre un ensemble de techniques de détection des infections informatiques. Un grand nombre de ces techniques sont transparentes pour l'utilisateur.

- La *vérification d'intégrité* détermine si la taille du fichier d'un programme a augmenté parce qu'un virus s'y serait joint. Cette méthode est utilisée en premier lieu pour vérifier l'intégrité des informations de la zone critique de disque.
- La *détection polymorphe à base de règles* observe les actions des programmes telles que les fonctions d'appel afin de détecter le comportement suspect d'un programme.
- La *surveillance des interruptions* observe tous les appels système des programmes (par exemple, DOS ou Macintosh) pour essayer d'arrêter la séquence d'appels qui pourrait indiquer les actions d'un virus.
- L'*analyse des signatures* recherche un ensemble unique de code hexadécimal, c'est-à-dire la signature du virus déposée par ce dernier dans un fichier infecté. En effectuant une recherche à l'aide de ces codes dans les fichiers programme, l'analyseur des signatures peut détecter ce virus connu.

Protection de vos ordinateurs contre les infections

Vous pouvez *simplement* vous contenter de détecter et de désinfecter vos ordinateurs. Toutefois, le meilleur moyen d'éviter ce type de problème est d'abord d'empêcher les infections d'atteindre votre ordinateur. Le logiciel antivirus de Computer Associates constitue une barrière efficace contre les infections.

Le *moniteur temps réel* analyse les fichiers lorsqu'ils entrent ou sortent de votre poste de travail en provenance ou vers d'autres ordinateurs de votre réseau. La protection temps réel inclut l'analyse des fichiers de votre poste de travail à chaque exécution, accès ou ouverture de fichier afin de détecter les éventuels virus qu'ils peuvent contenir.

La *protection de la zone de disque critique* (pour Windows 95 et Windows 98) protège le disque dur de votre poste de travail. La zone de disque critique comprend le secteur d'amorçage maître, la table des partitions, des informations concernant la mémoire CMOS (RAM) et des fichiers système. La fonctionnalité Disquette de secours vous permet de créer une disquette de sauvegarde des fichiers de la zone de disque critique.

Suggestions permettant de préserver vos ordinateurs de toute infection

Voici quelques suggestions d'ordre général afin d'éviter que votre ordinateur ne soit infecté.

- Définissez tous vos fichiers exécutables comme fichiers en lecture seule. Ceci réduit les risques d'infection des fichiers exécutables.
- Analysez les disquettes avant de copier des fichiers à partir de celles-ci.
- Utilisez un outil de sauvegarde tel que BrightStor afin de sauvegarder votre poste de travail après une analyse antivirus réussie. Si un fichier avec une infection ne pouvant être désinfectée est détecté, vous pouvez ainsi restaurer une version de sauvegarde de ce fichier.
- Installez les dernières mises à jour de signatures de virus pour assurer une protection optimale de votre environnement.
- Gérez vos répertoires partagés en définissant des droits d'accès de telle sorte que les utilisateurs aient le niveau d'autorité appropriée pour le répertoire, tel que la lecture seule au lieu du contrôle total.
- Dans les systèmes Windows, UNIX et OS X, si le moteur de l'analyseur heuristique détecte un fichier que vous pensez être infecté et que vous souhaitez l'envoyer à Computer Associates pour qu'il soit analysé, utilisez la fonctionnalité automatisée Envoyer pour analyse. En cas de traitement manuel du fichier, renommez-le toujours avec une extension AVB et utilisez un utilitaire de compression avant de l'envoyer par courrier électronique ou de l'enregistrer sur une disquette.

Composants du produit

Le logiciel antivirus de Computer Associates dispose d'un jeu complet de composants fournissant une protection maximale à tous les environnements informatiques : de ceux composés d'un seul ordinateur aux plus vastes.

Les principaux composants sont brièvement décrits ci-dessous.

Interface utilisateur graphique – L'interface utilisateur graphique fournit une interface familière de type Explorateur/Finder qui permet la gestion de tous les aspects de la protection antivirus. Les différents affichages et les différentes options vous permettent d'afficher et de contrôler tous les types d'activité d'analyse.

Interface utilisateur basée sur le Web – L'accès au logiciel antivirus de Computer Associates est possible par Internet via un navigateur. Utilisez l'interface comme vous le feriez avec celle de Windows, étant donné que leurs styles et leurs structures sont identiques.

Analyseur local – L'analyseur local vous permet de gérer les options d'analyse d'un ordinateur local.

Moniteur temps réel – Les options d'analyse en temps réel vous permettent de détecter les infections dans les fichiers de votre poste de travail à chaque exécution, accès ou ouverture de fichier. Vous pouvez surveiller un poste de travail à la recherche de comportements viraux, tels que le formatage non autorisé d'un disque dur. Les utilisateurs peuvent configurer le moniteur temps réel afin de détecter les infections connues et inconnues et de spécifier les actions à entreprendre si une infection est détectée. Les administrateurs peuvent transmettre des paramètres temps réel dans l'ensemble du réseau et surveiller les règles de cette option. Si un fichier infecté est détecté, une fenêtre contenant le nom du fichier infecté et celui du virus s'affiche.

Analyseur planifié – Les options de planification du job d'analyse vous permettent d'automatiser l'analyse sur les ordinateurs distants et locaux. L'analyse est alors effectuée à une date et une heure données et, si vous le souhaitez, à intervalles réguliers.

Extension Shell – L'option Extension Shell est intégrée à votre système d'exploitation Windows. Elle vous permet de cliquer avec le bouton droit de la souris sur tout élément du Bureau ou de l'Explorateur et d'effectuer une analyse grâce à l'analyseur du shell.

Affichage de l'administrateur – Les options de l'affichage de l'administrateur permettent d'effectuer une gestion administrative de tous les ordinateurs de votre réseau antivirus. Ces options permettent d'effectuer une gestion à distance, de transmettre les configurations, ainsi que de définir et de faire appliquer les règles antivirus de l'entreprise.

Serveur Admin – Le serveur Admin garde une trace de toutes les instances du produit antivirus exécutées sur votre réseau. Les utilisateurs autorisés peuvent effectuer des fonctions de gestion à distance basées sur les informations de découverte automatique fournies par le serveur Admin.

Agents Client – Des agents Client sont disponibles pour la plupart des systèmes d'exploitation, incluant Windows 3.x.

Journaux – La visionneuse du journal vous permet de consulter et de gérer les journaux de chaque type d'opération d'analyse, de visualiser les informations du journal de mise à jour des signatures ainsi que d'afficher et de modifier les options d'analyse planifiée. Les journaux sont compatibles avec les outils de base de données standard et peuvent être utilisés pour analyser l'impact des infections sur votre entreprise.

Utilitaire d'installation à distance – Les administrateurs peuvent utiliser cette interface utilisateur graphique pour installer le produit sur les ordinateurs Windows NT, Windows 2000 et Windows XP de l'entreprise.

Installation à distance pour Windows 9.x – Un programme d'installation (Setup.exe) est fourni afin de mettre à jour les ordinateurs Windows 9.x grâce à un script de connexion lorsqu'ils se connectent à un domaine.

Alert – Composant commun pour les systèmes Windows permettant d'envoyer des messages du logiciel antivirus de Computer Associates et d'autres produits de Computer Associates aux membres de votre organisation en utilisant différentes méthodes de communication. Des messages avec plusieurs niveaux d'alerte (état, avertissement et erreur) peuvent être envoyés à l'administrateur du système, à un technicien ou à toute autre personne située à l'intérieur ou à l'extérieur des bureaux. Une personne ou des groupes de personnes situés dans différents segments du réseau peuvent ainsi être informés. Pour de plus amples informations, consultez l'aide Alert. Vous pouvez également gérer les informations de notification pour Alert à partir des paramètres Alert intégrés à l'interface graphique utilisateur du logiciel antivirus de Computer Associates.

Remarque : Bien que le composant Alert ne soit pas disponible dans les systèmes basés sur UNIX et OS X, le logiciel antivirus de Computer Associates se lie à des scripts définis par l'utilisateur et à syslog, fournissant ainsi un niveau de souplesse de notification équivalent.

Inocmd32 – L'interface de l'analyseur en mode commande pouvant être utilisée par tous les systèmes d'exploitation.

Inocucmd – L'analyseur en mode commande pouvant être utilisé uniquement pour l'utilisation avec la fonctionnalité Disquette de secours de Windows 98/95.

Examine – Utilitaire de récupération à utiliser avec Windows 98/95.

ETRUSTAV – Programme sous NetWare seulement, à partir duquel vous pouvez contrôler un grand nombre des opérations eTrust Antivirus depuis une console de serveur NetWare.

Utilisation des affichages de fenêtre

L'interface utilisateur graphique fournit différents affichages pour gérer l'activité d'analyse. Les options du menu Affichage vous permettent de faire apparaître les affichages disponibles.

Analyseur local – Cet affichage permet de visualiser la fenêtre de l'analyseur local et de gérer les options d'analyse locale.

Visionneuse du journal – Cet affichage permet de consulter et de gérer les informations du journal.

Affichage de l'administrateur – Un administrateur autorisé peut utiliser cet affichage pour gérer à distance tous les aspects du réseau antivirus.

Gestionnaire de domaines pour NetWare – Cet affichage permet de gérer les domaines antivirus NetWare.

Remarque : Les affichages disponibles varient selon les options installées.

Options

Les options du produit disponibles comprennent :

Option Microsoft Exchange – Fournit une protection intégrée contre les infections contenues dans les documents et fichiers joints à des messages et les dossiers du courrier électronique.

Option Lotus Notes – Fournit une protection intégrée contre les infections contenues dans les documents et les fichiers joints à des messages électroniques et les bases de données Lotus Notes.

Gestion de domaine NetWare

Remarque : L'option de gestion de domaine NetWare ne concerne pas les machines exécutant eTrust Antivirus 7.0 ou 7.1 pour NetWare.

L'option de domaine NetWare ne concerne que les composants nécessaires à la connexion et à la gestion des machines exécutant InoculateIT 4.5 pour NetWare. Lors de l'exécution d'InoculateIT 4.5 pour NetWare, ceci permet de gérer votre logiciel antivirus Computer Associates pour les domaines NetWare par l'intermédiaire de la console Windows NT, Windows 2000 ou Windows Server 2003.

Analyse d'infections inconnues

L'option Analyseur heuristique vous permet d'analyser les infections inconnues. Même si les mises à jour des signatures les plus récentes analysent tous les virus isolés et classés par l'ICSA (International Computer Security Association), il est toutefois possible d'être infecté par un virus inconnu.

Vous pouvez utiliser à la fois la reconnaissance des signatures et l'analyseur heuristique pour détecter les infections avant qu'elles n'attaquent votre réseau. Si une infection inconnue est détectée, vous pouvez utiliser l'option Envoyer pour analyse pour compresser automatiquement le fichier et l'envoyer pour analyse à Computer Associates.

Analyse heuristique

L'option Analyseur heuristique exécute une analyse heuristique, technique d'intelligence artificielle utilisée pour détecter dans des fichiers des virus dont les signatures n'ont pas encore été isolées ni documentées. Plutôt que d'utiliser un algorithme fixe pour détecter les signatures de virus spécifiques, l'analyse heuristique utilise des méthodes alternatives pour détecter des modèles de comportements similaires à ceux de virus.

Etant donné la prolifération croissante de nouveaux virus, il peut être utile de maintenir l'option Analyseur heuristique activée à chaque analyse et également lors de l'utilisation du moniteur temps réel.

Mises à jour des signatures les plus récentes

Les mises à jour de signatures les plus récentes sont disponibles sur le site d'assistance Internet de Computer Associates à l'adresse suivante :

`http://esupport.ca.com/public/antivirus/infodocs/virussig.asp`

Dans la bataille constante contre les infections destructrices et malveillantes, nous effectuons continuellement une mise à jour des fichiers de signatures. Votre environnement doit déjà être défini pour pouvoir recevoir les mises à jour les plus récentes en fonction d'une planification déterminée par votre administrateur antivirus.

Cependant, des infections nouvelles et auparavant inconnues peuvent apparaître soudainement et sans avertissement. Nous vous recommandons de consulter régulièrement le site d'assistance pour obtenir les mises à jour de signatures les plus récentes, en particulier lorsque vous entendez parler d'infections et d'attaques nouvelles. Pour protéger votre environnement de traitement, assurez-vous d'être constamment à jour des signatures les plus récentes de Computer Associates.

Pour votre sécurité, Computer Associates n'utilise pas de pièces jointes électroniques comme moyen standard de distribution de la maintenance ou des mises à jour des produits. Computer Associates n'envoie pas de mises à jour non sollicitées par fichiers exécutables. Nous envoyons des messages d'alerte contenant des liens vers Computer Associates que vous pouvez utiliser pour effectuer une demande de mise à jour. Ceci évite que des virus se dissimulent sous la forme de mises à jour antivirus.

En cas d'infection

Si vous détectez une infection, des informations supplémentaires concernant les virus, vers et chevaux de Troie sont disponibles sur le Web au Centre d'informations sur les virus de Computer Associates à l'adresse suivante :

`http://www.ca.com/virusinfo/`

Des informations détaillées sur les infections les plus récentes ainsi que des instructions de suppression spécifiques sont disponibles sur le Web à l'adresse suivante :

`http://www.ca.com/virusinfo/virusalert.htm`

Chapitre 2

Pour obtenir les mises à jour de signatures

Ce chapitre contient des informations sur l'utilisation des options de mise à jour des signatures en vue d'obtenir les mises à jour de signatures les plus récentes pour les appliquer à votre système. Il aborde également la gestion des mises à jour de signatures dans un réseau antivirus.

Présentation des mises à jour de signatures

Les mises à jour de signatures contiennent les dernières versions des fichiers de signatures qui reconnaissent et neutralisent les infections les plus récentes. En outre, elles contiennent les versions de moteurs les plus récentes qui recherchent les infections éventuelles dans le système, ainsi que des mises à jour de programmes.

Lorsque vous configurez une mise à jour de signatures, vous devez spécifier le moment auquel elle doit être exécutée et comment la télécharger. Vous avez différentes méthodes à votre disposition pour obtenir des mises à jour de signatures, à savoir, via un serveur de redistribution désigné, le protocole de transfert de fichier (FTP), le chemin UNC (Universal Naming Convention) et un chemin de l'ordinateur local.

Computer Associates met à votre disposition des mises à jour de signatures régulièrement. Vous disposez de plusieurs méthodes pour obtenir les mises à jour, comme décrit dans ce chapitre.

Les mises à jour sont cumulatives

Les mises à jour de signatures sont disponibles pour toutes les versions et plates-formes prises en charge. Ces mises à jour sont cumulées et contiennent toutes les mises à jour de fichiers précédentes, ainsi que les dernières informations sur les infections les plus récentes. Si vous avez manqué une récente mise à jour, il vous suffit de télécharger le dernier fichier de signatures pour obtenir la protection la plus à jour. Les mises à jour de signatures adaptées à votre configuration sont disponibles par défaut.

Pour les utilisateurs individuels

Si vous êtes un utilisateur individuel, vous pouvez obtenir les fichiers de signatures de Computer Associates en utilisant une des méthodes source disponibles, puis mettre votre ordinateur à jour.

Pour les administrateurs antivirus

Si vous êtes l'administrateur antivirus d'une entreprise, quelle que soit sa taille, depuis le petit bureau jusqu'au plus grand groupe, nous vous recommandons de télécharger les mises à jour de Computer Associates en utilisant une des méthodes source disponibles et les options de mise à jour des signatures pour appliquer les mises à jour disponibles à votre réseau. Vous pouvez désigner les ordinateurs sélectionnés pour être des serveurs de redistribution de signatures. En outre, vous pouvez utiliser l'affichage de l'administrateur pour définir des options de règles pour les mises à jour de signatures.

Automatiser votre distribution

Vous pouvez définir que la collecte et la distribution se fassent automatiquement, de sorte que chaque ordinateur de votre réseau antivirus obtienne à temps les mises à jour de signatures les plus récentes sans qu'une intervention de l'utilisateur soit nécessaire. L'automatisation et les règles d'administration permettant de surveiller les normes d'utilisation de la protection antivirus constituent l'une des méthodes les plus puissantes pour protéger votre environnement de réseau contre les infections.

Remarque : De nouveaux virus apparaissent régulièrement. Utilisez toujours les fichiers de signatures les plus récents.

Visitez le site Internet d'assistance de Computer Associates à l'adresse http://esupport.ca.com pour obtenir la dernière version des mises à jour de signatures, une liste des virus détectés depuis la dernière mise à jour et d'autres informations importantes pour la protection de votre environnement. Vous pouvez également vous inscrire sur la liste de diffusion de notre bulletin d'information et être informé gratuitement par courrier électronique des nouvelles signatures.

Nous vous recommandons d'automatiser votre configuration pour obtenir régulièrement des mises à jour de signatures. Nous fournissons une fois par mois des mises à jour de signatures régulières et plus souvent lorsque le besoin s'en fait sentir. L'équipe antivirus de Computer Associates met à disposition des mises à jour dès que des infections suffisamment menaçantes apparaissent. Ces mises à jour fournissent les fonctions de détection et de désinfection les plus récentes.

Remarque : Il existe une différence entre la détection et la désinfection. Certaines infections peuvent être détectées, mais non éradiquées. Pour les infections ne pouvant être désinfectées, une fonction de détection est fournie. Des informations supplémentaires sur la détection et la protection antivirus sont mises à votre disposition sur le site d'assistance de Computer Associates. A mesure que les nouveaux traitements sont découverts, ils sont ajoutés aux mises à jour.

Aucun temps d'arrêt pour les mises à jour

Lorsque vous effectuez une mise à jour des signatures, le poste de travail n'interrompt pas son activité. La mise à jour des signatures est transparente et n'interfère pas avec votre travail.

Utilisation des options de mise à jour des signatures

Les options de mise à jour des signatures permettent d'indiquer comment et quand les mises à jour des signatures sont collectées à partir d'une source de distribution. Elles vous permettent de définir depuis où et à quel moment effectuer les téléchargements des mises à jour de signatures, ainsi que les versions de moteurs et les plates-formes nécessaires.

Important ! Pour distribuer automatiquement les mises à jour de signatures sur un ordinateur, vous devez utiliser l'option Activer le téléchargement planifié dans l'onglet Planification.

Remarque : Reportez-vous à l'aide en ligne pour obtenir des informations détaillées sur l'utilisation de toutes les options de mise à jour des signatures.

Sur les systèmes Windows, au cours de la mise à jour des signatures, une icône d'état du téléchargement est affichée dans la barre des tâches et vous pouvez afficher des informations sur la progression du téléchargement.

Options de mise à jour des signatures

Utilisez les onglets suivants pour configurer les options de mise à jour des signatures.

- Planification
- Entrée
- Sortie

Pour accéder à ces options depuis la fenêtre de l'analyseur local, cliquez sur le bouton Options de mise à jour des signatures pour afficher la boîte de dialogue des options de mise à jour des signatures ou utilisez le menu Analyseur pour sélectionner les Options de mise à jour des signatures.

Remarque : La fenêtre Analyseur local n'est pas disponible sous NetWare. La configuration de la mise à jour des signatures sur une machine NetWare s'effectue par l'intermédiaire de l'affichage de l'administrateur. Pour en savoir plus sur l'affichage de l'administrateur, reportez-vous au chapitre « Utilisation de l'affichage de l'administrateur ».

Les mises à jour de signatures adaptées à votre configuration sont disponibles par défaut. Pour la mise à jour d'un ordinateur local, vous devez uniquement indiquer où obtenir les mises à jour à l'aide de l'onglet Entrée. Vous pouvez ensuite utiliser l'onglet Planification pour définir une heure pour le job de mise à jour des signatures. Vous pouvez également obtenir les signatures immédiatement.

Les options de mise à jour des signatures sont utilisées à différents niveaux de la collecte et de la distribution par les différents types d'utilisateurs.

- En tant qu'utilisateur individuel, vous pouvez définir ces options pour collecter les mises à jour de signatures de Computer Associates et les mettre à disposition pour la mise à jour de votre ordinateur local.
- Un administrateur antivirus utilise ces options pour collecter les mises à jour de signatures auprès de Computer Associates et les mettre à disposition des ordinateurs définis comme serveurs de redistribution de signatures.
- Les administrateurs autorisés peuvent utiliser ces options pour collecter les mises à jour de signatures auprès des serveurs de redistribution de signatures et mettre ces mises à jour à disposition des autres ordinateurs du réseau.
- Ce processus de distribution peut être automatisé.
- Les administrateurs autorisés peuvent définir des règles pour ces options.

Reportez-vous au chapitre « Utilisation de l'affichage de l'administrateur » pour obtenir plus d'informations sur la définition des options de règles.

Utilisation des options de planification

L'onglet Planification vous permet d'activer les téléchargements planifiés et de déterminer la date, l'heure et la fréquence de mise à jour des signatures.

Vous pouvez planifier un job de mise à jour de signatures pour qu'il s'exécute de différentes manières.

- Télécharger la mise à jour des signatures immédiatement.
- Planifier une seule exécution du job de mise à jour des signatures.
- Planifier le job de mise à jour des signatures pour qu'il soit répété suivant la fréquence indiquée.

Remarque : Les options que vous spécifiez dans l'onglet Planification s'appliquent uniquement au job de mise à jour des signatures. Elles sont différentes des options de l'onglet Planification qui est utilisé pour planifier un job d'analyse sur un ordinateur local.

Télécharger maintenant

Utilisez le bouton Télécharger pour exécuter immédiatement un job de mise à jour des signatures. Les paramètres de l'onglet Entrée sont utilisés pour ce job. Les versions appropriées des signatures sont disponibles par défaut. Elles sont destinées à la mise à jour de signatures sur l'ordinateur local.

Reportez-vous à la section « Distribution de signatures avec Télécharger » du chapitre « Utilisation de l'affichage de l'administrateur » pour obtenir plus d'informations sur l'utilisation du téléchargement immédiat dans un environnement de réseau.

Pour l'installation à distance sur des systèmes Windows et NetWare, le fichier de configuration INOC6.ICF peut être utilisé pour programmer l'exécution de l'option Télécharger après l'installation.

Activer le téléchargement planifié

L'option Activer le téléchargement planifié vous permet d'indiquer que des téléchargements automatiques planifiés vont être effectués. Pour obtenir une distribution automatique des mises à jour de signatures sur un ordinateur, vous devez utiliser cette option. Lorsque cette option n'est pas activée, le téléchargement planifié est désactivé.

Nous vous conseillons d'utiliser cette option pour garantir une mise à jour régulière de vos fichiers de signatures.

Date et heure de téléchargement

L'option Date vous permet d'indiquer le jour, le mois et l'année du job. La flèche vers le bas permet d'afficher un calendrier pratique pour sélectionner une date. L'option Heure vous permet d'indiquer l'heure du job en heures et minutes.

L'interface graphique utilisateur du navigateur Web et l'interface OS X n'affichent aucun calendrier. Utilisez les flèches vers le haut ou vers le bas pour modifier la date ou l'heure.

Options Répéter

Utilisez les options Répéter pour indiquer la fréquence d'exécution d'un job régulier de mise à jour des signatures. Vous pouvez planifier l'exécution répétée d'un job de mise à jour des signatures en mois, jours, heures ou minutes.

Remarque : Les paramètres des options Date et Heure déterminent la première occurrence de la mise à jour répétée de signatures.

Utilisation des options Entrée

L'onglet Entrée vous permet d'afficher la liste des sources de téléchargement et d'indiquer comment et à partir d'où télécharger les mises à jour. Utilisez le bouton Ajouter pour afficher la boîte de dialogue Sélectionner une source et ajouter à la liste une méthode de téléchargement et une source pour la mise à jour. Vous pouvez créer des sources multiples de téléchargement si nécessaire.

Effectuer un téléchargement rapide

L'option Effectuer un téléchargement rapide vous permet de mettre à jour vos signatures sans télécharger les informations dont vous disposez déjà.

Lorsque cette option est sélectionnée, le processus de téléchargement analyse les informations de vos signatures actuelles pour déterminer le type de mise à jour dont vous avez besoin. Si seule une mise à jour incrémentielle des fichiers de données est nécessaire, les fichiers appropriés sont alors téléchargés et mis à jour automatiquement. Si une mise à jour incrémentielle n'est pas appropriée et qu'une mise à jour complète est nécessaire, tous les fichiers de signatures et de moteurs sont téléchargés et mis à jour.

Cette méthode se caractérise par des temps de téléchargement plus courts car elle permet de télécharger uniquement les données dont vous avez besoin. Vous n'avez pas besoin de télécharger l'ensemble de la mise à jour des signatures si vous avez réactualisé vos signatures récemment. Le résultat final de la mise à jour incrémentielle ou de la mise à jour complète fournit la même protection de votre ordinateur contre les virus.

Cette option est utile pour les mises à jour cumulées mineures, par exemple pour les signatures *nn*.01 à *nn*.04. Toutefois, si vous effectuez une mise à jour majeure, par exemple des signatures 1.01 à 2.01, le téléchargement fournit la mise à jour complète de la signature, même si cette option est sélectionnée. Ainsi, vous obtenez toujours la mise à jour de signatures adaptée à vos besoins.

Liste des sources de téléchargement

La liste des sources de téléchargement est une liste de sites à partir desquels vous pouvez télécharger des signatures. Elle fournit des informations sur la méthode et la source utilisées par le job de téléchargement. Vous pouvez ajouter des éléments à la liste et les supprimer. Cette liste doit vous permettre de télécharger les mises à jour de signatures de plusieurs sources.

Les mises à jour des signatures sont téléchargées à partir des sources selon l'ordre dans lequel elles sont affichées dans la liste, du haut vers le bas. Pour modifier cet ordre, mettez une méthode en surbrillance dans la liste et utilisez les boutons fléchés pour déplacer l'élément vers le haut ou le bas de la liste.

Utilisation des options de sélection de la source

La boîte de dialogue Sélectionner une source permet de spécifier la méthode de téléchargement ainsi que d'autres informations pour la connexion à la source de téléchargement.

Remarque : Les options de la boîte de dialogue Sélectionner une source changent en fonction de l'option Méthode sélectionnée.

Sélection d'une méthode

Il existe différentes méthodes pour la connexion à une source de téléchargement. Utilisez la méthode adaptée à votre configuration.

Les méthodes disponibles sont les suivantes :

- Serveur de redistribution
- FTP
- UNC
- Chemin local

Remarque : Un serveur NetWare peut obtenir des mises à jour de signatures à partir d'un autre ordinateur en utilisant uniquement les méthodes FTP ou UNC.

Utilisation d'un serveur de redistribution

Utilisez un serveur de redistribution pour télécharger des mises à jour des signatures à partir d'un serveur de redistribution défini dans le réseau.

Avec cette méthode, vous indiquez un serveur de redistribution dans votre réseau à partir duquel les mises à jour des signatures peuvent être collectées. Cet ordinateur vous permet d'accéder aux mises à jour les plus récentes une fois qu'elles ont été téléchargées du site de Computer Associates. C'est la méthode conseillée pour la plupart des utilisateurs dans un environnement d'entreprise. Reportez-vous à la section « Utilisation des options de sortie » pour obtenir de plus amples informations sur la définition d'un serveur de redistribution.

Notes pour l'utilisation du serveur de redistribution sous UNIX

Pour utiliser la méthode du serveur de redistribution pour le téléchargement des mises à jour des signatures d'un système Windows ou UNIX vers un autre système UNIX, le logiciel Samba doit être installé sur votre ordinateur cible UNIX. Samba est un progiciel tiers gratuit qui permet aux systèmes UNIX d'interagir avec des systèmes Windows et UNIX en utilisant la méthode UNC. Il est distribué avec certaines versions d'UNIX et peut aussi être obtenu à l'adresse www.samba.org. Pour télécharger des mises à jour d'un serveur de redistribution Windows, vous devez utiliser la version 2.0.7 ou supérieure de Samba.

En outre, un système UNIX peut servir de serveur de redistribution pour d'autres systèmes UNIX comme pour des systèmes Windows. Pour cela, Samba doit être installé sur le système UNIX. Le démon Samba (smbd) doit être en cours d'exécution et INOUPD$ doit être défini comme un partage dans le fichier de configuration de Samba (smb.conf). INOUPD$ ne peut pas être protégé par mot de passe. A partir de l'interface utilisateur graphique, spécifiez l'ordinateur UNIX comme Nom de l'ordinateur dans la boîte de dialogue Sélectionner une source de l'onglet Entrée situé dans la boîte de dialogue Options de mise à jour des signatures.

Notes pour l'utilisation du serveur de redistribution sous OS X

Pour utiliser la méthode du serveur de redistribution pour le téléchargement des mises à jour des signatures d'un système Windows ou UNIX vers un système OS X, le logiciel Samba doit être installé sur votre ordinateur cible UNIX.

En outre, un système OS X peut servir de serveur de redistribution pour des systèmes OS X, UNIX et Windows. INOUPD$ doit être défini comme un partage dans le fichier de configuration de samba (/etc/smb.conf). INOUPD$ ne peut pas être protégé par mot de passe. Voici un exemple d'entrée :

```
[INOUPD$]
path = /Library/Application Support/eTrustAntivirus/ino/Outgoing
guest ok = yes
browseable = no
read only = yes
```

Remarque : Il y a un espace entre les mots Application et Support.

Utilisation de FTP (Windows, NetWare, UNIX et OS X)

La méthode FTP permet de télécharger les mises à jour des signatures à partir d'un site FTP.

Nous vous recommandons d'utiliser la méthode FTP pour télécharger des mises à jour des signatures de Computer Associates.

Option	Description
Méthode	FTP
Nom de l'hôte	Nom du site FTP qui est la source de la mise à jour. Il s'agit par défaut du serveur FTP de Computer Associates où se trouvent les mises à jour des signatures.
Nom d'utilisateur	Nom d'utilisateur pour la connexion à l'ordinateur source. **anonymous** est la méthode utilisée par défaut pour le téléchargement par FTP des mises à jour des signatures du site de Computer Associates. Ce compte dispose de tous les droits et privilèges requis pour se connecter et télécharger les mises à jour.
Mot de passe	Mot de passe associé au nom de l'utilisateur sur l'ordinateur source. Pour télécharger des mises à jour des signatures de Computer Associates, entrez votre adresse électronique dans ce champ. Par exemple, *dupont@societex.com.*

Option	Description
Nom proxy	Nom de l'ordinateur proxy. Si votre société utilise un serveur proxy, entrez l'adresse du serveur proxy et le numéro de port utilisé. Par exemple, *un_proxy.unesociété.com:80.* Ce serveur doit être un simple serveur proxy pass-through. N'utilisez pas un serveur proxy basé FTP ou un serveur nécessitant un identifiant de connexion.
Chemin distant	Chemin FTP pour la localisation des fichiers source de mise à jour des signatures que vous souhaitez télécharger. Il s'agit par défaut du serveur FTP de Computer Associates où se trouvent les mises à jour des signatures.

Configuration d'un serveur NetWare pour la distribution des signatures

Vous trouverez ci-après un résumé de la procédure permettant de configurer un serveur NetWare agissant comme serveur de distribution des signatures pour les serveurs NetWare et les autres types d'ordinateurs.

1. Installez la fonction de serveur FTP sur votre serveur NetWare.
2. Exécutez un utilitaire FTP, par exemple *Nwtftp-A* pour NetWare Version 6.x, pour créer un utilisateur anonymous FTP, s'il n'en existe pas.
3. Modifiez le fichier de configuration FTP du serveur NetWare, par exemple, le fichier ftpserv.cfg se trouvant sous le répertoire sys:system\etc pour NetWare Version 6.x, afin de permettre l'accès anonyme au serveur FTP.
4. En utilisant le serveur Admin, à partir de l'onglet Entrée de la fenêtre Options de mise à jour des signatures, sélectionnez FTP comme méthode de la source de distribution de signatures. Pour en savoir plus sur l'utilisation du serveur Admin, reportez-vous au chapitre « Utilisation de l'affichage de l'administrateur ».
5. Dans la boîte de dialogue Sélectionner une source, saisissez le nom de votre serveur NetWare comme nom d'hôte, « anonymous » comme nom d'utilisateur, et saisissez un mot de passe.

   Remarque : Assurez-vous que le mot de passe est une adresse électronique au bon format. La plupart des serveurs FTP exigent une adresse électronique comme mot de passe lorsque vous utilisez une connexion FTP anonyme.
6. Dans la même boîte de dialogue, saisissez le chemin distant comme le chemin complet de l'emplacement à partir duquel le téléchargement des mises à jour de signatures doit s'effectuer. Ceci peut être spécifié dans le format NetWare ou UNIX standard. Par exemple :

   sys:/etrustav/ino/Outgoing

   ou

   /sys/etrustav/ino/Outgoing

7. Dans la même boîte de dialogue, laissez vide le champ Nom proxy.
8. Dans la même boîte de dialogue, cliquez sur OK pour terminer la configuration.

Une autre méthode de téléchargement de signatures sur un serveur NetWare pour d'autres types d'ordinateurs consiste à identifier le serveur, le volume et le chemin d'accès du serveur NetWare qui contient les signatures et à mapper un lecteur sur ce serveur.

Par exemple, si le chemin d'accès complet de l'emplacement depuis lequel les signatures peuvent être téléchargées est sys:etrustav/ino/Outgoing sur le serveur NetWare nommé SERVEUR1, vous pouvez mapper un lecteur sur sys:etrust/ino/Outgoing sur SERVEUR1 en utilisant la commande MAP du DOS ou l'option Connecter un lecteur réseau du menu Outils de l'Explorateur Windows.

Utilisation d'UNC

La méthode UNC (Universal Naming Convention : Convention universelle de désignation de noms) permet de télécharger les mises à jour des signatures d'un ordinateur en réseau.

Un ordinateur du réseau peut être utilisé pour obtenir les mises à jour à partir d'un répertoire partagé sur le réseau en indiquant le chemin UNC vers ce partage. Cette méthode est adéquate pour les ordinateurs d'un même réseau, notamment ceux configurés comme serveur de redistribution de signatures.

Option	Description
Méthode	UNC
Chemin	Nom du chemin du partage où se trouvent les fichiers de mise à jour de signatures, sous la forme *nom_ordinateur**nom_partage*.

Considérations relatives à UNC

Lorsque vous utilisez la méthode chemin UNC pour obtenir des mises à jour de signatures, certaines considérations doivent être prises en compte.

Pour la famille de systèmes d'exploitation Windows 9x, des restrictions du mode utilisateur sont imposées aux mises à jour automatisées des signatures. Lorsqu'un ordinateur exécutant un logiciel antivirus de Computer Associates est configuré comme serveur de redistribution de signatures, un nom de partage INOUPD$ est créé sur l'ordinateur local. Ce partage est créé avec les droits d'accès de système d'exploitation suivants :

- L'accès en lecture au partage est conféré au groupe Everyone.
- Le partage est ajouté à la liste NullSessionShares.

Pour utiliser la méthode de chemin UNC pour le téléchargement des mises à jour des signatures d'un système Windows ou UNIX vers un autre système UNIX, le logiciel Samba doit être installé sur votre ordinateur cible UNIX. Samba est un progiciel tiers gratuit qui permet aux systèmes UNIX d'interagir avec des systèmes Windows et UNIX en utilisant la méthode UNC. Il est distribué avec certaines versions d'UNIX et peut aussi être obtenu à l'adresse www.samba.org. Pour télécharger des mises à jour d'un système Windows, vous devez utiliser la version 2.0.7 ou supérieure de Samba.

Pour utiliser la méthode du chemin d'accès UNC pour le téléchargement des mises à jour des signatures d'un système Windows ou UNIX vers un système OS X, utilisez le logiciel Samba (SMB) fourni avec OS X. Aucune configuration particulière n'est requise.

En outre, un ordinateur Windows peut également télécharger des signatures en utilisant UNC depuis un ordinateur UNIX où le logiciel Samba est installé. Le démon du logiciel Samba (smbd) doit être en cours d'exécution et un partage approprié doit être défini dans le fichier de configuration de Samba (smb.conf). Le partage ne peut pas être protégé par mot de passe. A partir de l'interface graphique utilisateur de l'ordinateur Windows, indiquez le partage sur l'ordinateur UNIX dans la boîte de dialogue Sélectionner une source de l'onglet Entrée de la boîte de dialogue Options de mise à jour des signatures, à l'aide de la même syntaxe utilisée pour spécifier un partage sur un ordinateur Windows.

Un système OS X peut aussi fournir des signatures via UNC pour d'autres systèmes OS X, UNIX et Windows. Pour cela, un partage doit être défini dans le fichier de configuration de samba (/etc/smb.conf). Le partage ne peut pas être protégé par mot de passe. Reportez-vous à la section sur les serveurs de redistribution pour un exemple de l'entrée smb.conf.

Notez les considérations suivantes pour l'utilisation d'un répertoire partagé :

Dans ce cas	Notez ce qui suit

Ordinateurs Windows NT, Windows 2000 et Windows Server 2003	Sur les ordinateurs Windows NT, Windows 2000 et Windows Server 2003, le serveur de job du logiciel antivirus de Computer Associates lance la mise à jour des signatures pendant l'exécution depuis le compte du système local. Lorsque le mécanisme de mise à jour des signatures tente une connexion au répertoire partagé, le serveur ne peut pas authentifier l'utilisateur. Ceci arrive lorsqu'un processus exécuté sous un compte de système local n'a aucun utilisateur qui lui est associé.
	Pour permettre aux processus exécutés avec le compte du système local d'accéder à un répertoire partagé, le serveur doit ajouter le partage à la liste de partages de sessions vides. Cette liste est maintenue dans la valeur suivante de registre :
	Ruche :
	`HKEY_LOCAL_MACHINE`
	Sous-clé :
	`\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters`
	Valeur :
	`NullSessionShares`
	Remarque : Lorsqu'un ordinateur est configuré pour fonctionner comme un serveur de redistribution de signatures, le partage INOUPD$ est ajouté automatiquement à cette valeur de registre.

Dans ce cas	Notez ce qui suit
Lorsque le processus de mise à jour de signatures est exécuté en mode utilisateur	Le processus de mise à jour de signatures est exécuté en mode utilisateur dans les circonstances suivantes : ■ Sur les ordinateurs Windows 9x, toujours. ■ Sur les ordinateurs Windows NT, Windows 2000 et Windows 2003, lors de l'exécution à partir d'un script de connexion en utilisant un planificateur tiers Dans ces conditions, le processus de mise à jour de signatures est exécuté dans le contexte de sécurité de l'utilisateur actuellement connecté. C'est pourquoi il est soumis aux règles de contrôle d'accès des répertoires partagés Microsoft et **une** des conditions suivantes est nécessaire pour garantir la bonne exécution du processus : ■ L'utilisateur doit avoir accès au partage avec le compte qu'il a utilisé pour se connecter. ■ Le compte GUEST du serveur doit être activé et il ne doit utiliser aucun mot de passe.

Dans le cas de NetWare, les partages ne sont pas accessibles. La méthode UNC pour NetWare ne peut servir qu'au téléchargement de mises à jour depuis un serveur NetWare vers un autre, et la convention UNC sert à indiquer l'emplacement des mises à jour sur le serveur source. Par exemple, vous trouverez ci-dessous le résumé de la procédure de téléchargement des mises à jour de signatures à partir d'un serveur NetWare vers un autre serveur NetWare en utilisant UNC :

1. A partir de l'arborescence de l'organisation dans l'affichage de l'administrateur du serveur Admin qui gère l'ordinateur NetWare, sélectionnez l'ordinateur vers lequel vous voulez télécharger des mises à jour de signatures.
2. Cliquez avec le bouton droit et sélectionnez l'option Configurer paramètres de distribution.
3. Dans l'onglet Entrée de la boîte de dialogue Options de mise à jour des signatures, cliquez sur Ajouter.
4. Sélectionnez la méthode UNC dans la boîte de dialogue Sélectionner une source et saisissez le chemin du serveur à partir duquel vous voulez effectuer le téléchargement dans le format UNC. Par exemple, pour obtenir les mises à jour à partir de SYS:ETRUSTAV\INO\OUTGOING sur le serveur SERVER1, indiquez \\SERVER1\SYS\ETRUSTAV\INO\OUTGOING comme chemin du serveur source.

Remarque : Le serveur NetWare vers lequel le téléchargement des mises à jour de signatures va s'effectuer doit se trouver dans la même arborescence que le serveur source. En outre, si le serveur vers lequel les mises à jour sont téléchargées se trouve dans un contexte différent de celui du serveur source, ce dernier doit être spécifié en utilisant son nom qualifié complet, par exemple, server1.xxx.yyy, ou cn=server1.ouxxx.o=yyy.

5. Créez un nom d'utilisateur nommé **inosigdown** dans le contexte du serveur source (SERVER1 dans notre exemple). Ce nom d'utilisateur doit avoir un accès en lecture seule et en analyse au répertoire à partir duquel les mises à jour doivent être obtenues et ne doit avoir accès à aucun autre répertoire ou fichier se trouvant ailleurs sur le serveur source ou dans son contexte. L'identité de l'utilisateur inosigdown **ne** doit **pas** avoir de mot de passe. Du fait que l'utilisateur ne peut voir que les fichiers qui sont déjà des informations publiques, l'absence de mot de passe ne présente aucun risque en matière de sécurité d'accès.

Utilisation du chemin local

Utilisez cette méthode lorsque les mises à jour des signatures se trouvent sur votre ordinateur ou dans une unité mappée et que vous souhaitez mettre à jour les fichiers de signatures sur votre ordinateur. Vous avez la possibilité de parcourir et de sélectionner un chemin de répertoire sur l'ordinateur local ou une unité mappée.

Option	Description
Méthode	Chemin local
Chemin	Nom du répertoire où résident les mises à jour des signatures. Sous Windows, la lettre du lecteur y est incluse.

Considérations relatives à l'utilisation du chemin local

Outre le téléchargement de mises à jour des signatures d'un autre système UNIX utilisant Samba, un ordinateur UNIX peut également utiliser une des méthodes ci-dessous pour effectuer le téléchargement de mises à jour des signatures d'un autre ordinateur UNIX.

- Montez le serveur de signatures UNIX comme NFS. A partir de l'interface utilisateur, utilisez la méthode de téléchargement **Chemin local** dans la boîte de dialogue Sélectionner une source de l'onglet Entrée de la boîte de dialogue Options de mise à jour des signatures et entrez le point de montage spécifié dans la commande **smbmount** en tant que Chemin.
- Exécutez le démon **smb** sur le serveur de signatures UNIX et définissez un partage dans **smb.conf** pour l'emplacement des mises à jour. La commande **smbmount** sur l'ordinateur client vous permet de monter le partage. A partir de l'interface graphique utilisateur, utilisez la méthode de téléchargement **Chemin local** dans la boîte de dialogue Sélectionner une source, dans l'onglet Entrée de la boîte de dialogue Options de mise à jour des signatures et entrez le point de montage comme Chemin.

Les systèmes OS X peuvent télécharger des mises à jour de signatures depuis un système Windows, UNIX ou OS X en utilisant un chemin d'accès local qui est un point de montage de serveur NFS ou SMB.

- Montez le serveur de signatures en utilisant la commande mount_nfs ou mount_smbfs depuis une fenêtre de terminal. Depuis l'interface graphique de eTrust Antivirus, utilisez la méthode de téléchargement de chemn d'accès local et utilisez le point de montage comme chemin d'accès.
- Montez le serveur de signatures en utilisant le Finder. Depuis l'interface graphique de eTrust Antivirus, utilisez la méthode de téléchargement de chemn d'accès local et utilisez le point de montage comme chemin d'accès. Vous trouverez le point de montage sous le répertoire /Volumes.

Utilisation des options de sortie

L'onglet Sortie vous permet d'afficher et de configurer les options de redistribution et de définir un ordinateur comme serveur de redistribution, ainsi que de gérer les signatures à télécharger en vue de la redistribution.

Remarque : Les ordinateurs NetWare ne peuvent pas être utilisés comme serveurs de redistribution.

Utilisation des options de redistribution

Les options de redistribution vous permettent de désigner un ordinateur comme serveur de redistribution de signatures et de mettre les mises à jour à disposition des autres ordinateurs.

Serveur de redistribution des signatures

Si l'option de distribution des mises à jour de signatures vers d'autres ordinateurs est cochée, l'ordinateur local est désigné comme un serveur de redistribution de signatures. Cet ordinateur peut ensuite mettre les mises à jour à disposition des autres ordinateurs.

Si cette option n'est pas sélectionnée, les options de redistribution ne sont pas disponibles. Lorsque cette option est sélectionnée, le répertoire Sortie où sont stockées les mises à jour est accessible comme répertoire partagé. La plupart des ordinateurs client ne jouent pas le rôle de serveur de redistribution.

Remarque : L'ordinateur rendant les mises à jour accessibles à d'autres ordinateurs doit exécuter la version serveur du logiciel antivirus de Computer Associates.

Temps d'attente avant la redistribution

L'option de temps d'attente vous permet d'indiquer le nombre d'heures que vous souhaitez attendre avant que les mises à jour soient disponibles pour être redistribuées aux autres ordinateurs.

Signatures à télécharger pour la redistribution

La liste de signatures à télécharger en vue de la redistribution fournit des informations sur les versions de moteur et plate-forme collectées par les jobs de mise à jour de signatures. Les versions de signatures mises à disposition doivent être appropriées à votre configuration.

Si nécessaire, vous pouvez cliquer dans la case en regard d'un élément pour inclure ou exclure celui-ci de la liste de signatures à télécharger. Vous pouvez également utiliser les boutons Sélectionner tout et Effacer tout, selon vos besoins.

Les informations suivantes sont affichées dans la liste des signatures à télécharger :

Champ	Description
Moteur	Type de moteur antivirus à télécharger. **Remarque :** Le processus d'installation sélectionne automatiquement le moteur d'analyse adapté à votre configuration. La plupart des utilisateurs n'ont pas besoin de modifier la sélection.
Plate-forme	Version de la plate-forme à télécharger.

Reportez-vous à l'aide en ligne pour des informations détaillées sur la définition des jobs de téléchargement pour la mise à jour de signatures.

Considérations relatives à l'utilisation de systèmes UNIX et OS X comme serveurs de redistribution

Un système UNIX peut servir de serveur de redistribution aussi bien pour d'autres systèmes UNIX que pour des systèmes Windows. Pour cela, **Samba** doit être installé sur le système UNIX. (Samba est un progiciel tiers gratuit qui permet aux systèmes UNIX d'interagir avec des systèmes Windows utilisant la méthode UNC. Il est distribué avec certaines versions d'UNIX et peut aussi être obtenu à l'adresse www.samba.org.) Le démon du logiciel **Samba** (smbd) doit être en cours d'exécution et INOUPD$ doit être défini comme un partage dans le fichier de configuration de **Samba** (smb.conf).

Un système OS X peut servir de serveur de redistribution pour des systèmes OS X, UNIX et Windows. Pour cela, un partage nommé INOUPD$ doit être défini dans le fichier de configuration de samba (/etc/smb.conf). INOUPD$ ne peut pas être protégé par mot de passe. Voici un exemple d'entrée :

```
[INOUPD$]
path = /Library/Application Support/eTrustAntivirus/ino/Outgoing
guest ok = yes
browseable = no
read only = yes
```

Notez qu'il y a un espace entre les mots Application et Support.

Gestion des mises à jour de signatures

Chaque ordinateur peut être configuré pour télécharger des mises à jour de signatures à partir d'une source particulière, pour une configuration spécifique et à un moment donné.

Lorsque vous spécifiez comment télécharger les mises à jour, vous créez la liste des sources de téléchargement, qui contient les sites à partir desquels les signatures peuvent être téléchargées. Vous pouvez indiquer plus d'une méthode à utiliser et plus d'un emplacement d'où télécharger les mises à jour. Lorsque vous vous connectez à la première source de la liste, la mise à jour des signatures est téléchargée. Si pour une raison quelconque, le téléchargement échoue ou est impossible, la source suivante de la liste est automatiquement contactée et ainsi de suite jusqu'à ce que tous les fichiers de mise à jour soient téléchargés.

Remarque : A chaque tentative, les éléments appropriés sont téléchargés pour votre configuration, telle que la version du système d'exploitation de la signature.

Distribution signatures

Vous pouvez définir votre réseau pour télécharger et distribuer efficacement les mises à jour des signatures. Chaque ordinateur qui permet d'accéder aux mises à jour de signatures est un serveur de redistribution de signatures. Vous pouvez définir plusieurs ordinateurs de redistribution de signatures.

Par exemple, un ordinateur de votre réseau peut télécharger les mises à jour du site FTP de Computer Associates. D'autres ordinateurs situés à des emplacements différents de votre réseau peuvent se connecter à cet ordinateur pour obtenir les dernières mises à jour. Ces ordinateurs peuvent à leur tour mettre à disposition les mises à jour pour les autres ordinateurs de leurs sous-réseaux.

Remarque : Le serveur de redistribution de signatures a un rôle différent du serveur proxy de configuration. Le serveur de redistribution des signatures permet de mettre les fichiers de mises à jour de signatures à disposition d'autres ordinateurs. Le serveur proxy de configuration est utilisé pour distribuer les paramètres des règles à travers le réseau.

Fonctionnement du processus de téléchargement

Cette section décrit comment le job de mise à jour de signatures utilise la liste des sources de téléchargement et la liste de signatures à télécharger en vue de la redistribution pour obtenir les mises à jour de signatures dont vous avez besoin.

Un job de mise à jour de signatures comprend les étapes suivantes :

- Définir la planification – moment du téléchargement
- Spécifier la source – emplacement du téléchargement
- Spécifier les signatures – éléments à télécharger

Le job de mise à jour de signatures utilise les informations de la liste des sources de téléchargement et de la liste de signatures à télécharger pour répondre à votre demande de mise à jour des signatures.

Fonctionnement de la liste des sources de téléchargement

La liste des sources de téléchargement indique où obtenir les mises à jour de signatures. Le job de mise à jour de signatures peut se connecter à plusieurs emplacements de sources. A l'heure planifiée pour le job, votre système utilise la première méthode et la première source de la liste pour la connexion à la source. Si pour une raison quelconque, la connexion ne peut pas être établie (exemple : trafic intense dans le réseau, échec de connexion ou délai d'attente dépassé), votre système passe à la méthode et à la source suivantes de la liste.

Par exemple, après le téléchargement des mises à jour des signatures de Computer Associates, vous pouvez les mettre à disposition d'un ou plusieurs serveurs de redistribution. Un utilisateur de votre réseau peut ensuite se connecter à ces sources pour obtenir les mises à jour. La première source de la liste de sources peut être un serveur de réseau de département, indiqué par la méthode de serveur de redistribution. La seconde source peut être un serveur dans un département différent, également indiqué par la méthode de serveur de redistribution. La troisième source de la liste peut être un site FTP interne de la société. Chaque ordinateur source doit être défini comme serveur de redistribution de signatures.

Si la première source n'est pas disponible, votre système tente automatiquement de se connecter à la source suivante de la liste. Ce processus se poursuit jusqu'à ce que toutes les signatures spécifiées aient été téléchargées. La liste des sources de téléchargement fonctionne avec la liste de signatures à télécharger pour obtenir toutes les signatures spécifiées.

Fonctionnement de la liste de signatures à télécharger

La liste de signatures à télécharger indique les versions de mises à jour de signatures à télécharger. Les versions appropriées des signatures sont disponibles par défaut. Vous pouvez sélectionner une entrée de la liste pour chaque version de moteur et plate-forme dont vous avez besoin ou annuler la sélection de signatures qui ne répondent pas aux besoins de votre entreprise.

Lors de l'exécution du job de mise à jour de signatures, votre système se connecte à la première source de la liste des sources de téléchargement. Le job parcourt ensuite les entrées de la liste de signatures à télécharger et tente de télécharger depuis cette source les versions de tous les moteurs et plates-formes qui ont été demandées.

Le job télécharge toutes les versions de signatures demandées qui sont disponibles dans la première source avant de se connecter à une autre source. Si toutes les signatures demandées sont téléchargées de la première source, le job est terminé.

Si vous demandez une version de mise à jour de signatures qui n'est pas disponible dans la première source de la liste des sources de téléchargement, votre système demande à la source suivante de cette liste la version requise. Ce processus se poursuit jusqu'à ce que toutes les demandes soient satisfaites pour les différentes versions de mises à jour de signatures spécifiées dans la liste de signatures à télécharger.

Surveillance des téléchargements de signatures

Sur les systèmes Windows, au cours du téléchargement d'une mise à jour de signatures, une icône d'état du téléchargement de la signature est affichée dans la barre des tâches, à côté de l'icône Temps réel. Au cours du téléchargement, vous pouvez cliquer avec le bouton droit de la souris pour afficher l'état du job.

Options de surveillance

Les options suivantes de surveillance sont disponibles lorsque l'icône d'état du téléchargement de la signature est affichée.

Option	Description
Afficher l'état entrant	Affiche le moniteur de téléchargement de l'antivirus qui indique l'état du job. Lors de l'exécution du moniteur temps réel, le moniteur de téléchargement de l'antivirus est affiché automatiquement lorsque vous sélectionnez Télécharger. L'interface graphique utilisateur du navigateur Web n'affiche pas le moniteur de téléchargement de l'antivirus.
Annuler le téléchargement	Annule le job de téléchargement de signatures. Vous pouvez également utiliser le bouton Annuler dans la boîte de dialogue Moniteur de téléchargement de l'antivirus pour annuler le job de téléchargement des signatures.

Moniteur de téléchargement de l'antivirus

Le moniteur de téléchargement de l'antivirus affiche les informations relatives à l'état du job de téléchargement des signatures. Ceci inclut les messages sur les connexions et les indications sur la progression du téléchargement. Lorsqu'un téléchargement s'est terminé avec succès, un message s'affiche pour l'indiquer. En outre, lorsque les signatures sont mises à jour sur l'ordinateur local, un message contextuel s'affiche indiquant que la mise à jour des fichiers des signatures et des moteurs a réussi.

Reportez-vous aux journaux d'événements généraux et d'événements de distribution pour connaître les autres messages de téléchargement de signatures.

Tentatives répétées de téléchargements

Si un job de téléchargement de signatures est incapable de télécharger l'ensemble des fichiers de signatures, plusieurs tentatives de téléchargement ont lieu pour répondre à la demande. Si la tentative échoue, le téléchargement a lieu lors du prochain téléchargement planifié.

Chapitre

3

Utilisation des options d'analyse et de sélection

Ce chapitre décrit les options d'analyse et de sélection disponibles dans l'interface utilisateur pour les différentes méthodes d'analyse mentionnées ci-dessous.

- Analyse locale
- Analyse planifiée
- Analyse en temps réel
- Pour les administrateurs définissant les options de règles via l'affichage de l'administrateur

Ce chapitre comporte également des informations sur l'utilisation de l'analyseur en mode commande, Inocmd32.

Utilisation des options d'analyse communes

Lorsque vous spécifiez des options pour une analyse, vous devez indiquer comment elle doit être exécutée et comment agir en cas d'infection. Que vous effectuiez une analyse locale, planifiée ou en temps réel, vous pouvez sélectionner différents paramètres pour chaque type d'opération. Par exemple, les options d'action sur fichiers contrôlent les actions en cas de découverte d'une infection. Lors d'une analyse locale, vous pouvez avoir l'action sur fichiers définie sur l'option Rapport seulement. Lorsque vous définissez les options d'une analyse planifiée, vous pouvez définir l'action sur fichiers sur Désinfecter le fichier.

Remarque : Il ne faut pas oublier que lorsque vous définissez une option d'analyse, elle s'applique au type spécifique d'opération d'analyse que vous définissez.

Les options décrites dans ce chapitre sont communes à tous les types d'analyse, c'est pourquoi elles sont décrites ici par souci de commodité. Consultez l'aide en ligne pour obtenir de plus amples informations sur les options d'analyse.

Remarque : Etant donné que certaines options s'appliquent seulement à une méthode d'analyse et pas aux autres, ces exceptions sont indiquées lorsqu'il y a lieu. Reportez-vous à Utilisation du moniteur temps réel pour obtenir des informations sur les options disponibles exclusivement pour le moniteur temps réel. Reportez-vous à Planification des jobs d'analyse pour obtenir des informations sur les options disponibles pour les analyses planifiées.

Utilisation des options d'analyse

Les options d'analyse sont affichées dans l'onglet Analyse. Ces options vous permettent de modifier le niveau d'analyse, le moteur d'analyse, les options de détection et de contrôler comment traiter une infection dans le cas d'une détection. Ces options peuvent être utilisées pour une analyse locale, une analyse planifiée ou une analyse en temps réel.

Options de l'onglet Analyse

Les options disponibles dans l'onglet Analyse sont décrites ci-dessous.

Direction

L'option Direction est uniquement disponible pour l'analyse en temps réel. Reportez-vous au chapitre « Utilisation du moniteur temps réel » pour obtenir des informations sur les options de direction d'analyse.

Niveau de sécurité de l'analyse

Vous pouvez définir le niveau de sécurité de l'analyse en mode Sécurisée ou Approfondie. Utilisez le mode Sécurisée comme méthode standard pour une analyse complète des fichiers.

Si vous pensez qu'une infection n'a pas été détectée par le mode Sécurisée, vous pouvez utiliser le mode Approfondie. Le mode Approfondie peut être utilisé pour détecter des virus qui ne sont pas actifs ou qui ont été délibérément modifiés, comme cela peut être le cas dans un laboratoire qui teste les virus. En outre, le mode Approfondie s'exécute nettement plus lentement que le mode Sécurisée.

Remarque : Le mode Approfondie peut, dans certains cas, générer une fausse alerte. Par conséquent, si vous utilisez ce mode comme option d'analyse standard, utilisez-le avec l'option Rapport seulement.

Moteur d'analyse

Dans le groupe de détection, l'option Moteur d'analyse vous permet de modifier le moteur d'analyse si une sélection est possible. Le moteur d'analyse est le processeur spécialisé recherchant les infections. Le processus d'installation sélectionne automatiquement le moteur d'analyse adapté à votre configuration. La plupart des utilisateurs n'ont pas besoin de modifier cette option. Elle est essentiellement destinée aux utilisateurs confirmés des grandes entreprises.

Options de détection avancées

Vous pouvez afficher des options de détection supplémentaires en cliquant sur le bouton Avancées. La boîte de dialogue Options de détection avancées vous permet de sélectionner des options d'analyse pour le moteur de l'analyseur heuristique et des options pour analyser les systèmes de fichiers NTFS et HFS+.

Le moteur de l'analyseur heuristique détecte les virus dont les signatures n'ont pas encore été isolées ni documentées.

L'option Analyser les flux de données secondaires vous permet de détecter des virus dans les flux de données secondaires des systèmes NTFS et HFS+.

Remarque : Pour le moniteur temps réel, vous pouvez accéder à l'option Moteur d'analyse ainsi qu'aux autres options de détection à partir de l'onglet Sélection.

Options de traitement de l'infection

Les options de traitement de l'infection déterminent comment traiter l'infection après sa découverte. Vous pouvez définir des actions sur fichiers et des actions sur secteur d'amorçage.

Pour une analyse locale, vous pouvez définir ces options avant ou après l'analyse. Si vous souhaitez avoir connaissance des éventuels fichiers infectés avant de procéder à leur traitement, sélectionnez Rapport seulement. En cas de détection d'une infection, vous pouvez alors sélectionner l'une des autres actions.

Actions sur fichiers

Vous pouvez traiter une infection en définissant une action sur fichiers. Les actions sur fichiers disponibles sont les suivantes :

Action sur fichiers	Description
Rapport seulement	Effectue un rapport en cas de détection d'infection. En cas de détection de virus, vous pouvez décider du traitement à appliquer au fichier infecté.
Supprimer le fichier	Supprime un fichier infecté.
Renommer le fichier	Si un fichier infecté est détecté, il est renommé avec une extension AVB. Des extensions incrémentielles sous la forme *numéro.AVB* (par exemple, *FICHIER.0.AVB, FICHIER.1.AVB*, etc.) sont attribuées aux fichiers infectés portant le même nom. Un fichier renommé avec un type d'extension AVB n'est pas analysé de nouveau par la suite.
Déplacer le fichier	Déplace un fichier infecté de son répertoire actuel vers le dossier de déplacement.
Désinfecter le fichier	Essaie de désinfecter automatiquement le fichier infecté. Cliquez sur le bouton Options de fichier pour afficher les options de l'action de désinfection afin de spécifier la façon d'exécuter l'option Désinfecter le fichier. Même si le fichier infecté est désinfecté, nous vous recommandons de le supprimer et de restaurer le fichier original à partir d'une sauvegarde. Si le fichier infecté provient d'un progiciel, restaurez les fichiers à partir des disquettes d'installation du produit.

Actions sur secteur d'amorçage

Sur les systèmes Windows, les actions sur secteur d'amorçage déterminent comment agir en cas de détection d'une infection dans le secteur d'amorçage d'un disque dur ou d'une disquette. Les actions disponibles sont Rapport seulement et Désinfection du secteur d'amorçage.

Utilisation des options de l'action de désinfection

Les options de l'action de désinfection déterminent la manière de traiter les virus de macro et les chevaux de Troie, ainsi que les actions à effectuer avant ou après une tentative de désinfection.

Les options suivantes sont disponibles dans la boîte de dialogue Options de l'action de désinfection.

Options de l'action de désinfection	Description
Action à exécuter avant la désinfection	Copie le fichier dans le répertoire de déplacement avant toute tentative de désinfection.
Action à exécuter en cas d'échec de la désinfection	En cas d'échec de la désinfection, le fichier infecté peut être soit déplacé vers le répertoire de déplacement, soit renommé avec une extension AVB ou encore laissé tel quel si l'option Aucune action a été activée.
Traitement des chevaux de Troie et des vers	Si une infection par ver ou par cheval de Troie est détectée, le fichier infecté peut être supprimé. Cette option est désormais disponible si le paramètre Désinfection du système est activé.
Traitement des virus de macros	Vous pouvez choisir de supprimer seulement les macros infectées ou toutes les macros du fichier.
Désinfection du système	Utilisez l'option Désinfection du système pour nettoyer le système après avoir traité certains virus malveillants tels que les chevaux de Troie ou les vers. Certains virus peuvent endommager, modifier ou ajouter des fichiers système. Dans le cas de virus connus, cette option répare les dommages causés au système. Par exemple, elle permet de supprimer des entrées de registre, des clés et des fichiers malveillants. Elle peut également détecter et supprimer des fichiers insérés dans un système par un cheval de Troie. Ainsi, il n'est plus nécessaire d'utiliser des utilitaires distincts pour nettoyer un système infecté. Cette option minimise également le temps de nettoyage manuel du système. Dans certains cas, cette option peut exiger un redémarrage de l'ordinateur. (Cette option ne s'applique pas aux systèmes UNIX, OS X et NetWare. Cependant, elle est disponible dans l'interface graphique utilisateur du navigateur Web lorsque vous créez des règles devant être appliquées ou lorsque vous gérez un ordinateur Windows dans l'affichage de l'administrateur.)

Utilisation des options de sélection

Utilisez les options de sélection pour choisir les types d'objets à analyser, les types d'extensions de fichiers à inclure ou à exclure d'une analyse ainsi que les types de fichiers compressés à analyser.

Options de l'onglet Sélection

Les options disponibles dans l'onglet Sélection sont décrites ci-dessous.

Objets à analyser

Vous pouvez choisir d'effectuer une analyse antivirus de la mémoire, d'analyser le secteur d'amorçage du disque dur ou d'une disquette et d'analyser les fichiers. Lors de l'analyse de fichiers, les types de fichiers analysés sont déterminés par les types d'extensions que vous avez inclus ou exclus comme indiqué dans les options Fichiers ordinaires et Analyser les fichiers compressés.

Remarque : Pour une analyse temps réel, l'option Objets à analyser n'est pas disponible. Dans le cadre d'une analyse planifiée, cette option est définie pour analyser les fichiers et ne peut pas être modifiée.

Fichiers ordinaires

Vous pouvez choisir d'analyser tous les fichiers ou de sélectionner des types particuliers d'extensions à inclure ou à exclure.

Analyse des fichiers compressés

Si vous souhaitez analyser des fichiers compressés, vous devez sélectionner l'option Analyser les fichiers compressés et indiquer les extensions des types de fichiers compressés.

Types de fichiers compressés pris en charge

Les types de fichiers compressés actuellement pris en charge et pouvant être analysés sont les suivants :

- ARJ
- GZIP
- Archives ZIP/JAVA
- LHA

- CAB
- MIME
- RAR
- TAR
- Fichier compressé UNIX (.Z)
- Fichiers messages électroniques TNEF encapsulés

Options d'analyse de fichiers compressés

Des options supplémentaires sont disponibles pour la gestion des fichiers compressés. Elles peuvent être utilisées pour améliorer les performances d'analyse. Cliquez sur le bouton Options dans le groupe Analyser les fichiers compressés pour afficher ces options.

Les options de fichiers compressés suivantes sont disponibles :

- Appliquer le filtre d'extensions aux fichiers contenus dans les archives, pour analyser les fichiers compressés selon la liste des fichiers ordinaires sélectionnés dans l'onglet Sélection.
- Arrêter l'analyse d'archives de fichiers compressés lorsqu'un fichier infecté y est détecté.
- Appliquer des actions liées aux virus à un fichier archive (excepté l'action de désinfection)
- Analyser les fichiers compressés en les reconnaissant grâce à leur extension, ce qui est plus rapide que de les analyser en fonction du contenu de leurs archives.
- Analyser les fichiers compressés en analysant leur contenu, ce qui est plus lent que de les reconnaître par leur extension.

Ne pas analyser les fichiers migrés

Sur les systèmes Windows et NetWare, vous pouvez analyser les fichiers qui ont été migrés vers un stockage externe. Lorsque cette option est activée, les fichiers qui ont été sauvegardés **ne** sont **pas** analysés. Si cette option est activée et qu'une entrée existe dans un répertoire pour un fichier ayant été sauvegardé et déplacé d'une unité locale, le fichier n'est pas analysé. Si vous souhaitez analyser des fichiers migrés, assurez-vous que cette option n'est pas activée afin que les fichiers ayant été sauvegardés soient restaurés dans l'unité locale puis analysés.

Utilisation de l'analyseur en mode commande Inocmd32

Sur les systèmes Windows, l'analyseur en mode commande INOCMD32.EXE vous permet d'effectuer des analyses à partir de la ligne de commande. Les résultats sont affichés à l'écran pendant l'analyse ; ils sont également enregistrés dans le journal d'analyse pour consultation ou impression ultérieure.

Sur les systèmes UNIX, sensibles à la casse, et les systèmes OS X, utilisez la commande inocmd32.

Remarque : Sous eTrust Antivirus 7.0 ou 7.1 pour NetWare, utilisez l'application de console ETRUSTAV pour effectuer l'analyse. Pour plus d'informations, reportez-vous à l'annexe « Utilisation du programme de console ETRUSTAV » de ce guide.

La syntaxe de commande pour INOCMD32 est la suivante :

```
inocmd32 [-options] fichier|répertoire|unité
```

Chaque option est précédée d'un tiret –. Des choix d'actions sont associés à certaines options.

Spécifiez au moins un fichier ou un répertoire à analyser. Sur les systèmes Windows, vous pouvez spécifier une unité à analyser.

Exemples

```
inocmd32 -ACT cure -SCA mf -LIS:myscan.txt c:\temp
```

Cette commande permet d'appeler l'analyseur en mode commande INOCMD32 pour analyser l'unité et le répertoire c:\temp, de configurer l'action sur fichiers ACT sur Désinfecter, de configurer l'action de désinfection spéciale SCA sur Déplacer le fichier en cas d'échec de la désinfection et d'envoyer les résultats de l'analyse vers le fichier myscan.txt.

```
inocmd32 -NEX -ARC /home/myfiles
```

Cette commande permet d'appeler inocmd32 pour analyser le répertoire UNIX /home/myfiles et tous les sous-répertoires. Les fichiers d'archives seront analysés et identifiés par leur contenu et non par leur nom.

Options de l'analyseur pour Inocmd32

Option	Description
ENG *moteur*	Type de moteur à utiliser. **Ino** – Le moteur Antivirus. **Vet** – Le moteur Vet.

Option	Description
MOD *mod*	Mode d'analyse. MOD vous permet de définir le niveau de sécurité de l'analyse. **Sécurisée** – Utilisez le mode Sécurisée comme méthode standard pour analyser entièrement les fichiers. **Approfondie** – Si vous pensez qu'une infection n'a pas été détectée par le mode Sécurisée, vous pouvez utiliser le mode Approfondie. **Mode par défaut** – Sécurisée
ACT *action*	Action sur fichier infecté. Spécifiez les actions à entreprendre sur un fichier infecté. Utilisez l'une des options d'*action* suivantes. **Désinfecter** – Tente de désinfecter automatiquement le fichier infecté. Même si le fichier infecté est désinfecté, nous vous recommandons de le supprimer et de restaurer le fichier original à partir d'une sauvegarde. **Renommer** – Renomme automatiquement le fichier infecté. Cette option permet de renommer le fichier infecté avec une extension AVB. Les fichiers infectés portant le même nom se voient attribuer des extensions incrémentielles de type *AVNuméro*. Par exemple, *FICHIER.AV0, FICHIER.AV1*, et ainsi de suite. Un fichier renommé avec un type d'extension AVB n'est pas analysé de nouveau par la suite. **Supprimer** – Supprime le fichier infecté. **Déplacer** – Déplace le fichier infecté de son répertoire actuel vers le dossier de déplacement. **Configuration par défaut** – Rapport seulement

Option	Description
EXE	Analyse uniquement les fichiers spécifiés. La liste des extensions de fichier dans l'option Uniquement les extensions spécifiées pour les fichiers ordinaires de l'interface graphique détermine les fichiers qui seront analysés.
EXC	Exclut des fichiers de l'analyse. La liste des extensions de fichiers dans l'option Toutes les extensions sauf celles spécifiées détermine les fichiers qui seront exclus de l'analyse parmi les fichiers ordinaires de l'interface graphique utilisateur.
ARC	Analyse des fichiers d'archives. Cette option vous permet d'analyser des fichiers compressés.
NEX	Détecte les fichiers compressés d'après leur contenu et non d'après leur extension.
NOS	Permet d'exclure les sous-répertoires. Cette option vous permet d'exclure les sous-répertoires du répertoire spécifié de l'analyse.
FIL:*modèle*	Analyse uniquement les fichiers qui correspondent au *modèle*. Les modèles de caractère générique du shell vous permettent de sélectionner les fichiers à analyser. **Exemple** Le modèle *.*doc* n'analysera que les fichiers avec une extension *.doc*.

Option	Description
SCA *action*	Action de désinfection spéciale. Utilisez cette option lorsque l'*action* ACT est configurée sur Désinfecter. Utilisez l'une des options d'action SCA suivantes. **CB** – Copier avant. Une copie du fichier d'origine est effectuée et la copie est déplacée vers le dossier de déplacement avant la tentative de désinfection. **RF** – Renommer si la désinfection échoue. Si un fichier ne peut pas être désinfecté, il est renommé avec une extension AVB. **MF** – Déplacer si la désinfection échoue. Si la désinfection échoue, le fichier infecté est transféré de son répertoire actuel vers le dossier de déplacement.
MCA *action*	Action de désinfection de macro. Utilisez l'une des options d'action suivantes. **RA** – Supprimer tout. Toutes les macros sont supprimées du fichier infecté. **RI** – Supprimer les macros infectées. Seules les macros contenant un code infecté sont supprimées du fichier infecté.
SPM *mode*	Mode spécial. Cette option vous permet d'exécuter une analyse avec le moteur heuristique, pour rechercher des virus inconnus. La seule option disponible pour le *mode* est **H**, pour Heuristique.
SFI	S'arrête à la première infection détectée dans l'archive. Si cette option est activée et qu'un fichier infecté est détecté au moment où les fichiers sont extraits d'un fichier compressé, aucun fichier supplémentaire de l'archive ne sera analysé.

Option	Description
SMF	Analyse les fichiers migrés sur les systèmes Windows et NetWare. Cette option vous permet d'analyser des fichiers qui ont été migrés vers un stockage externe. Lorsque cette option est activée, les fichiers ayant été sauvegardés sont restaurés sur l'unité locale, puis analysés. Si cette option n'est pas activée et qu'il existe une entrée de répertoire pour un fichier ayant été sauvegardé et déplacé d'une unité locale, le fichier n'est pas analysé.
SRF	Permet d'ignorer l'analyse régulière des fichiers d'archives. Si vous utilisez cette option, les fichiers compressés **ne** sont **pas** analysés.
BOO (Boot Sector Scan)	Analyse le secteur d'amorçage du système Windows. La configuration par défaut est Rapport seulement. L'option ACT vous permet de configurer cette option afin de désinfecter les infections au niveau du secteur d'amorçage.
MEM	Sur les systèmes Windows, analyse la mémoire. Recherche des infections dans les programmes actuellement exécutés dans la mémoire.
LIS:*fichier*	Utilisez cette option lorsque vous exécutez une analyse et que vous envoyez la liste des résultats de l'analyse vers un *fichier* spécifié.
APP:*fichier*	Permet d'ajouter le rapport d'analyse au *fichier*. Utilisez cette option lorsque vous exécutez une analyse et que vous ajoutez la liste des résultats de l'analyse à un *fichier* existant spécifié.

Option	Description
SYS	Sur les systèmes Windows, activez la désinfection du système. Cette option permet d'utiliser le dispositif de désinfection du système pour tout fichier infecté détecté et auquel une désinfection du système est associée. Veuillez vous référer à l'encyclopédie sur les virus que vous trouverez sur le site Web de Computer Associates pour plus d'informations sur les virus et sur les moyens de désinfection du système qui leur sont associés. Notez que dans certains cas, il vous faudra redémarrer l'ordinateur pour que la désinfection du système prenne effet.
VER	Mode détaillé. Cette option permet d'afficher des informations détaillées sur l'analyse.
COU (Counter)	Active le compteur de fichiers. Cette option vous permet d'envoyer un message après l'analyse de 1000 fichiers. Ce message est répété chaque fois que 1000 fichiers ont été analysés.
COU:*numéro*	Active le compteur de fichiers et le définit sur la valeur indiquée. Cette option vous permet d'envoyer un message lorsque le nombre de fichiers indiqué a été analysé. Ce message est répété chaque fois que le nombre de fichiers indiqué a été analysé.
SIG	Signature. Cette option vous permet d'afficher les numéros de version des signatures.
SIG:*rép*	Répertoire des signatures. Cette option vous permet d'afficher les numéros de version des signatures des moteurs dans le répertoire spécifié.
HEL ou ?	Affiche l'aide (Help) du mode commande.

Chapitre

4

Utilisation de l'analyseur local

L'analyseur local offre une protection antivirus complète pour un poste de travail en vous permettant d'effectuer des analyses d'infection à la demande. Ce chapitre décrit brièvement les fonctionnalités principales de l'analyseur local. Reportez-vous à l'aide en ligne pour une description détaillée de toutes les options de l'analyseur local et des procédures d'utilisation de celles-ci.

Remarque : La fenêtre de l'analyseur local n'est pas disponible sous NetWare. Utilisez l'application de console ETRUSTAV pour effectuer des analyses locales sur des ordinateurs NetWare. Pour en savoir plus sur l'application de console ETRUSTAV, reportez-vous l'annexe « Utilisation du programme de console ETRUSTAV ».

Fonctionnalités de l'analyseur local

Vous pouvez utiliser l'analyseur local sur un ordinateur local à tout moment pour vérifier si les unités, répertoires, fichiers ou disques ne sont pas infectés. Avant d'exécuter une analyse antivirus, vous pouvez définir des options de gestion d'un fichier infecté de sorte que lorsque vous lancez l'analyse, aucune action supplémentaire n'est nécessaire. Vous pouvez également définir des options pour générer uniquement un rapport en cas d'infection. Ceci vous permet de décider de l'action à entreprendre après la détection d'une infection.

Accès à d'autres options depuis la fenêtre de l'analyseur local

La fenêtre de l'analyseur local est également le point de départ pour accéder aux options des différents types d'analyse et aux autres actions. Vous pouvez accéder aux options suivantes depuis la fenêtre de l'analyseur local.

- Options de l'analyseur local
- Options de planification de jobs
- Options du moniteur temps réel
- Options de mise à jour des signatures
- Options de contact
- Paramètres Alert

Différentes options d'affichage sont également disponibles. Vous pouvez permuter les différents affichages en les sélectionnant dans le menu Affichage.

Options de l'analyseur local

Utilisez les onglets suivants pour configurer les options de l'analyseur local.

- Analyse
- Sélection
- Afficher
- Répertoire
- Journal

Les options d'analyse et de sélection sont communes aux différents types de méthodes d'analyse. Elles sont décrites au chapitre « Utilisation des options d'analyse et de sélection ». Toutefois, l'onglet Répertoire et l'onglet Journal sont uniquement disponibles depuis la fenêtre de l'analyseur local. Veuillez vous reporter au chapitre « Affichage et gestion des journaux » pour obtenir des informations sur la définition des options du journal.

Remarque : L'utilisation de l'analyseur local pour analyser une unité de réseau n'est pas la manière la plus efficace d'exploiter les ressources du réseau. Veuillez vous reporter à la section « Considérations relatives à l'analyse d'unités de réseau » du chapitre« Utilisation de l'affichage de l'administrateur » pour plus d'informations sur ce sujet.

Fenêtre de l'analyseur local

La fenêtre de l'analyseur local affiche à gauche une liste des éléments disponibles pour l'analyse et à droite le contenu de l'élément sélectionné. Vous pouvez définir des options relatives aux éléments affichés et à la façon de gérer l'analyse sur l'ordinateur local.

Vous pouvez modifier les options d'une analyse locale en sélectionnant les options de l'analyseur local dans le menu Analyseur ou en cliquant sur le bouton Options de l'analyseur local dans la barre d'outils de l'analyseur local. Après avoir indiqué les options appropriées et avoir sélectionné le ou les éléments que vous souhaitez analyser, lancez l'analyse en cliquant sur le bouton Démarrer l'analyse.

Barre d'outils de l'analyseur local

La barre d'outils de l'analyseur local comporte des boutons pour démarrer, arrêter, planifier une analyse, modifier les options de l'analyseur local ainsi que du moniteur temps réel. Vous pouvez également accéder aux options de mise à jour des signatures, aux options de contact et aux paramètres d'Alert.

Remarque : Veuillez vous reporter à la section « Utilisation d'Alert avec le logiciel antivirus » du chapitre « Utilisation du gestionnaire Alert » pour obtenir des informations sur les paramètres Alert.

Barre d'état

La barre d'état dans la partie inférieure de la fenêtre de l'analyseur local affiche des informations sur l'analyse, comprenant le nom du fichier analysé, le moteur utilisé, le nombre de répertoires et de fichiers analysés, le nombre de fichiers infectés détectés et le temps écoulé pour l'analyse.

Liste des résultats de l'analyse

Après avoir exécuté une analyse locale, la partie inférieure de la fenêtre de l'analyseur local affiche la liste des résultats de l'analyse.

Cette liste affiche le nom du fichier infecté ainsi que l'unité, le répertoire, les sous-répertoires et le nom de l'infection. La liste indique également l'état qui montre le type d'action effectué sur un fichier. Sont également affichés l'objet infecté, le type d'infection, la méthode de détection et le moteur utilisé.

Après l'exécution d'une analyse avec les actions sur fichiers configurées sur Rapport seulement, vous pouvez cliquer avec le bouton droit de la souris sur un fichier de la liste de résultats et sélectionner une autre action telle que Supprimer, Renommer, Déplacer ou Désinfecter. Vous pouvez également afficher des informations détaillées sur l'analyse. En outre, lorsque l'option Analyseur heuristique détecte une infection inconnue, vous pouvez utiliser l'option Envoyer pour transmettre le fichier à Computer Associates pour analyse.

Veuillez vous reporter à la section « Envoi d'un fichier pour analyse » pour obtenir plus d'informations sur l'utilisation de l'option Envoyer.

Affichage du résumé du résultat de l'analyse

Le bouton Afficher le résumé de la dernière analyse de la barre d'outils permet d'afficher le résumé du résultat de l'analyse la plus récente. Les statistiques de l'analyse sont affichées.

Vous pouvez afficher ce résumé automatiquement après chaque analyse en sélectionnant l'option Afficher la boîte de dialogue Résumé après chaque analyse dans l'onglet Afficher les options de l'analyseur local.

Effacer le dernier résultat d'analyse

Le bouton Effacer le dernier résultat d'analyse de la barre d'outils vous permet d'effacer la liste des résultats d'analyse affichée dans la partie inférieure de la fenêtre de l'analyseur.

Mes dossiers

La catégorie Mes dossiers permet de classer les dossiers et les fichiers que vous analysez fréquemment. La création d'une liste personnalisée de favoris vous permet de ne sélectionner que le groupe d'éléments que vous souhaitez analyser. Vous pouvez ajouter des dossiers de la liste principale en sélectionnant chaque élément et en cliquant dessus avec le bouton droit de la souris. Sur les systèmes Windows, vous pouvez également sélectionner un dossier dans la partie droite de la fenêtre de l'analyseur local et le faire glisser-déplacer jusqu'à la catégorie Mes dossiers. Certains dossiers sont affichés par défaut.

Dossier de déplacement

Après une analyse, vous pouvez mettre en surbrillance la catégorie Dossier de déplacement pour que les informations concernant les fichiers situés dans le Répertoire de déplacement s'affichent dans le côté droit de la fenêtre. Si vous devez gérer un fichier déplacé, vous pouvez le faire à partir de la fenêtre de l'analyseur local sans devoir accéder directement au fichier. Vous pouvez cliquer avec le bouton droit de la souris sur un élément et le restaurer à son emplacement d'origine ou à un emplacement différent sous un autre nom ou le supprimer.

Ces options de restauration vous permettent de restaurer des informations si nécessaire. Vous pouvez renommer un fichier et l'isoler en toute sécurité dans un endroit différent. Vous pouvez utiliser ces options, par exemple, si vous n'avez pas d'autre source pour ces données et que vous devez consulter ce fichier. Ou si vous avez un fichier que vous souhaitez analyser.

Lorsqu'un fichier est déplacé vers le dossier de déplacement, un nom unique lui est affecté afin de l'identifier. Ainsi, si vous avez eu des fichiers infectés portant les mêmes noms qui ont été stockés dans des répertoires différents, ils restent distincts lorsqu'ils sont déplacés.

L'option Restaurer et désinfecter vous permet de restaurer l'élément sélectionné dans son dossier d'origine et de le désinfecter. Cette option est utile si vous mettez les fichiers de signatures à jour après que des éléments aient été placés dans le dossier de déplacement. Si un traitement de désinfection est fourni alors que vous ne l'aviez pas à votre disposition, vous pouvez obtenir la dernière mise à jour de signatures et utiliser cette option pour restaurer et désinfecter l'élément infecté.

Jobs d'analyse planifiés

La catégorie Jobs d'analyse planifiés permet d'accéder aux options de Job d'analyse planifié. Veuillez vous reporter au chapitre « **Planification de jobs d'analyse** » pour plus d'information sur la planification.

Utilisation des options d'affichage

Vous pouvez utiliser les options d'affichage pour définir les types d'unités et de fichiers à afficher dans la fenêtre de l'analyseur local. Grâce à ces options vous pouvez personnaliser l'affichage d'objets pour ne voir que les types que vous souhaitez analyser.

Options de l'onglet Afficher

Les options disponibles dans l'onglet Afficher sont décrites ci-dessous.

Unités et systèmes de fichiers

Vous pouvez afficher différents types d'unités (ou de systèmes de fichiers sous UNIX) dans la fenêtre de l'analyseur local.

- Disque dur local (toujours sélectionné)
- Lecteur de CD-ROM
- Unité réseau
- Unité de disquette
- Unité amovible

Si vous sélectionnez toutes ces options, toutes les unités et les systèmes de fichiers connectés, montés à distance ou mappés sur l'ordinateur sont affichés dans la liste de l'analyseur local. Vous pouvez limiter les types d'unités ou les systèmes de fichiers selon vos besoins. Par exemple, si votre poste de travail est en réseau, vous pouvez être connecté à différents ordinateurs mais souhaiter n'effectuer des analyses locales que des fichiers se trouvant sur votre disque dur. Si vous ne sélectionnez pas l'option Unités réseau, les ordinateurs en réseau ne sont pas affichés dans la fenêtre Analyseur local.

Fichiers

Vous pouvez choisir de n'afficher que les types de fichiers que vous souhaitez voir dans la fenêtre Analyseur local. Vous pouvez afficher tous les fichiers ou masquer les fichiers selon les extensions que vous définissez en utilisant les filtres de sélection de l'onglet Sélection.

Remarque : Vous pouvez spécifier les types d'extensions de fichier que vous souhaitez inclure dans une analyse en utilisant l'option Fichiers ordinaires dans l'onglet Sélection. Ensuite, dans l'onglet Afficher, vous pouvez masquer tous les types de fichiers qui ne seront pas analysés, au lieu d'afficher tous les fichiers.

Afficher la boîte de dialogue Résumé d'analyse

Pour une analyse locale, si vous sélectionnez Afficher le résumé à la fin de l'analyse, la boîte de dialogue Résumé du résultat de l'analyse est affichée automatiquement une fois l'analyse terminée. Ce résumé comprend des informations sur l'heure de début et de fin de l'analyse, le nombre de fichiers analysés, le nombre d'infections trouvées, le nombre d'infections désinfectées et d'autres statistiques sur les actions effectuées sur les fichiers.

Utilisation des options de répertoire

Les options Répertoire affichent les emplacements des répertoires utilisés par le logiciel antivirus de Computer Associates. En outre, Renommer avec l'extension est affiché. Les emplacements des répertoires sont listés dans l'onglet Répertoire.

Remarque : L'onglet Répertoire est uniquement affiché pour l'analyseur local.

Répertoires d'installation des versions précédentes

Les versions précédentes du logiciel antivirus de Computer Associates utilisaient des répertoires d'installation par défaut différents. Sur un système Windows, si vous mettez une version antérieure à niveau, vous avez peut être un répertoire d'installation Inoculan.

Emplacements de répertoire affichés

L'information affichée dans l'onglet Répertoire est décrite ci-dessous.

Répertoires affichés

Les emplacements des répertoires suivants sont affichés dans l'onglet Répertoire.

Répertoire	Description
Répertoire d'installation	Répertoire dans lequel le logiciel antivirus de Computer Associates est installé.
Répertoire du moteur	Répertoire où se trouve le moteur.
Répertoire des journaux	Répertoire où sont stockés les fichiers journaux.
Répertoire de déplacement	Répertoire vers lequel les fichiers infectés sont déplacés.

Renommer extension

L'onglet Répertoire affiche l'extension qui est utilisée pour remplacer l'extension d'origine lorsqu'un fichier infecté est renommé. Cette fonctionnalité est utilisée lorsque l'action sur fichier est Renommer le fichier.

Par défaut : AVB

Des extensions incrémentielles sous la forme *numéro.AVB* (par exemple, *FICHIER.0.AVB*, *FICHIER.1.AVB*, etc.) sont attribuées aux fichiers infectés portant le même nom. Un fichier renommé avec un type d'extension AVB n'est pas analysé de nouveau par la suite.

Envoi d'un fichier pour analyse

Vous pouvez utiliser la fonction Envoyer les informations pour l'analyse pour envoyer des fichiers infectés à votre administrateur d'antivirus ou à Computer Associates en vue d'une analyse plus approfondie. Ces informations comprennent les coordonnées de contact et d'autres informations sur le système infecté qui peuvent s'avérer utiles pour le diagnostic et la désinfection. Cette option est uniquement disponible lorsque l'option Analyseur heuristique est sélectionnée et qu'une infection inconnue a été découverte.

Les fichiers de signatures peuvent reconnaître des milliers d'infections, mais vous pouvez en découvrir une nouvelle ou rencontrer un fichier problématique demandant une investigation.

Utilisation des options Envoyer les informations pour l'analyse

Si une infection inconnue est détectée par l'analyseur heuristique, vous pouvez cliquer avec le bouton droit de la souris dans la liste des résultats de l'analyse, et sélectionner l'option Envoyer pour afficher la boîte de dialogue Envoyer les informations pour l'analyse.

Cette boîte de dialogue automatise le processus d'envoi en compressant les fichiers infectés et en les envoyant pour analyse avec les coordonnées de contact en supplément. Un formulaire qui contient des informations sur l'ordinateur local est aussi soumis car il pourrait être utile pour l'analyse du fichier problématique. Les informations concernant la personne à qui envoyer les fichiers et celle à contacter se trouvent sous l'option Contact.

Utilisation de l'option Contact

L'option Contact permet de spécifier les informations relatives au contact qui sont automatiquement envoyées lorsque vous envoyez un fichier pour analyse. Vous pouvez consulter ces informations dans les options Envoyer les informations pour l'analyse. Un administrateur de virus autorisé peut définir les règles sur les coordonnées à inclure ou à modifier.

Remarque : Cette option permet de déterminer à qui sont envoyés les fichiers à analyser.

Vous pouvez accéder à cette option à partir de la barre d'outil Analyseur local en cliquant sur le bouton Options contact.

Informations sur la personne à contacter pour l'analyse de virus

La boîte de dialogue Options Contact contient les options suivantes.

Option	Description
Adresse électronique d'envoi	Adresse électronique où envoyer les fichiers infectés. Il s'agit de l'adresse électronique du service antivirus de Computer Associates à laquelle envoyer les fichiers qui doivent être analysés. Vous pouvez modifier cette adresse pour que les informations d'analyse soient envoyées à une adresse spécifique de votre société.
Objet	L'objet ou le titre du courrier électronique.
Adresse électronique de réponse	Adresse électronique pour répondre au message envoyé.
Nom de la société	Nom de la société qui envoie les fichiers infectés.
Adresse de la société	Adresse de la société qui envoie les fichiers infectés.
Nom de la personne à contacter	Nom de la personne à contacter dans la société au sujet des fichiers infectés.
Téléphone	Numéro de téléphone de la personne à contacter dans la société au sujet de cette infection.
ID du site	ID du site de l'entreprise.

Option	Description
Serveur SMTP	(Facultatif pour les environnements Intranet) Nom du serveur SMTP que votre réseau utilise pour envoyer des messages électroniques. Dans certains environnements, le nom du serveur de messagerie peut être déterminé automatiquement à partir du serveur DNS. Si vous utilisez un service de connexion pour les messages électroniques, par exemple, vous devez définir le serveur SMTP.

Gestion des infections à analyser

Un administrateur autorisé peut modifier l'emplacement par défaut pour qu'un fichier infecté soit soumis à une adresse interne dans votre entreprise au lieu qu'il soit envoyé à Computer Associates.

Par exemple, plusieurs infections du même type peuvent frapper une grande entreprise. En envoyant chaque fichier suspect à un administrateur interne, vous pouvez surveiller les occurrences des infections. Si l'administrateur a déjà une solution fournie par Computer Associates, le fichier n'aura pas à être envoyé pour analyse. L'administrateur peut étudier le problème et déterminer s'il doit être transmis à Computer Associates.

Utilisation du gestionnaire de services

Le gestionnaire de services est un moyen pratique pour accéder aux services antivirus de Computer Associates s'exécutant sur l'ordinateur local. Il ressemble à la fonctionnalité Services de Windows NT. Cette option peut être utilisée pour gérer des processus en arrière plan sur un système d'exploitation Windows 9x ou pour gérer les démons sous UNIX.

Cliquez sur le bouton Gestionnaire de services sur la barre d'outils pour afficher la boîte de dialogue correspondante. A partir de cette boîte de dialogue, vous pouvez démarrer ou arrêter les services et afficher leur état.

Remarque : Dans des circonstances normales, vous n'avez pas besoin d'arrêter ou de démarrer ces services.

Services

Les services suivants sont exécutés sur l'ordinateur local. Les services disponibles varient selon les composants installés.

Remarque : Les exécutables UNIX et OS X ne comprennent pas l'extension .exe, mais les noms restent les mêmes.

Service	Description
Serveur Admin	Agent du serveur Admin, InoNmSrv.exe.
Serveur RPC	Agent de gestion à distance, InoRpc.exe. Lorsque vous accédez à cette boîte de dialogue par le biais de l'affichage de l'administrateur, ce service n'est pas affiché dans la liste. Lors d'une utilisation avec l'affichage de l'administrateur, il doit toujours être en cours d'exécution car il assure la communication entre les ordinateurs situés dans le réseau antivirus.
Serveur temps réel	Agent d'analyse en temps réel, InoRT.exe. Sous Windows 9x, il s'agit de InoRT9x.exe.
Serveur de jobs	Agent de planification des jobs d'analyse et de planification de la mise à jour des signatures, InoTask.exe.
Serveur Web	Agent qui fournit l'accès au logiciel antivirus Computer Associates via un navigateur Web et l'interface native sous OS X, inoweb.

Chapitre

5

Utilisation du moniteur temps réel

Le moniteur temps réel offre un barrage automatique et permanent contre les infections en les stoppant avant qu'elles ne puissent se propager. Une gamme de composants temps réel protège l'ensemble des points d'entrée dans le réseau antivirus de Computer Associates ou d'un poste de travail individuel.

Le moniteur temps réel analyse les programmes d'un poste de travail ou d'un serveur à chaque exécution, accès ou ouverture de fichier. Sur les systèmes Windows, le moniteur temps réel est un pilote de périphérique virtuel (VxD) ; sur les systèmes UNIX, le moniteur temps réel utilise la fonction Event Notification Facility de Computer Associates ; sur les systèmes NetWare, il utilise le sous-système NetWare FSHOOKS ; sur les systèmes OS X, c'est une extension du noyau. Il surveille également les comportements de type viral de votre ordinateur tels que le formatage non autorisé d'un disque dur. Vous pouvez surveiller les virus connus et inconnus, spécifier les méthodes de détection et gérer les fichiers infectés. Sur les systèmes Windows et OS X, si une infection est détectée, une fenêtre contenant le nom du fichier infecté et celui de l'infection s'affiche.

Les administrateurs peuvent diffuser des configurations pour de multiples ordinateurs lors de l'installation du produit dans l'entreprise ; en outre, ils peuvent définir et faire appliquer les règles temps réel. Pour de plus amples informations sur la gestion des règles temps réel, reportez-vous au chapitre « Utilisation de l'affichage de l'administrateur ».

Fonctionnalités du moniteur temps réel

Les options de l'analyse en temps réel sont semblables aux options de l'analyse locale ou de l'analyse planifiée. Outre les options communes à toutes les méthodes d'analyse, le moniteur temps réel vous permet d'effectuer les actions suivantes :

- Définir la direction de l'analyse.
- Exclure des processus de l'analyse en temps réel (non disponible pour Windows 9x).
- Exclure des répertoires et fichiers de l'analyse en temps réel.
- Bloquer tous les accès aux extensions spécifiées de fichiers sans les analyser.
- Définir les options de protection avancée.
- Spécifier les options de quarantaine sur les systèmes Windows.

Remarque : N'oubliez pas que les paramètres que vous choisissez pour le moniteur temps réel ne s'appliquent qu'à l'analyse en temps réel et non pas à l'analyse locale.

Les fonctionnalités du moniteur temps réel comprennent :

- **Mode d'analyse en temps réel** – Les infections sont recherchées dans tous les fichiers entrants et sortants d'une unité locale, notamment dans les fichiers compressés. Lorsque l'analyse en temps réel est en fonction, les infections ne se propagent pas dans votre réseau. Vous pouvez également utiliser les fonctions de l'analyseur heuristique avec l'analyse en temps réel.
- **Quarantaine** – Sur les systèmes Windows, les utilisateurs qui essaient de copier des fichiers infectés sur un serveur sont automatiquement privés de l'accès à l'ordinateur afin d'isoler l'infection avant qu'elle ne puisse se propager.
- **Protection Internet** – La source la plus récente d'infections est Internet. Etant donné que les utilisateurs disposent d'un accès pratiquement illimité aux ordinateurs dans le monde entier, les risques de télécharger des fichiers infectés augmentent de manière exponentielle. Lorsque la protection en temps réel est activée, tous les téléchargements de fichiers, notamment de fichiers compressés, sont automatiquement analysés avant qu'ils puissent infecter un ordinateur. Cette fonctionnalité est compatible avec les navigateurs Netscape et Microsoft.
- **Options antivirus pour les messageries de groupe** – Les entreprises communiquent plus que jamais par le biais du courrier électronique. Etant donné le volume croissant des échanges de données, la propagation de virus dissimulés dans des pièces jointes et des fichiers de base de données augmente. Des options de messagerie disponibles peuvent protéger vos systèmes de messagerie Lotus Note ou Microsoft Exchange. Les fichiers zip joints sont également analysés.
- **Option Désinfection temps réel** –Désinfecte un fichier infecté et vous permet de faire une copie du fichier avant de le désinfecter.
- **Options Blocage pré-analyse** – Cette option permet de bloquer tous les accès aux extensions de fichiers spécifiées pour que des fichiers ou extensions potentiellement dangereux ne puissent pas être ouverts, copiés ou exécutés par les utilisateurs ou le système.

Chargement automatique du moniteur temps réel

Une fois le moniteur temps réel configuré, il sera chargé à chaque démarrage du poste de travail sur les systèmes Windows. L'icône du moniteur temps réel est affichée dans la barre des tâches de Windows, dans le coin inférieur droit de votre écran.

Sur les systèmes UNIX et NetWare, au cours de l'installation du logiciel antivirus, vous pouvez déterminer si vous souhaitez que le moniteur temps réel se charge automatiquement lors du démarrage du système. Il n'existe pas de barre des tâches permettant d'afficher une icône sur les systèmes UNIX ou NetWare.

Sur les systèmes OS X, au cours de l'installation du logiciel antivirus, vous pouvez déterminer si vous souhaitez que le moniteur temps réel se charge automatiquement lors du démarrage du système. La boîte de dialogue Options du moniteur temps réel permet de désactiver le moniteur temps réel. Il n'y a pas d'icône indiquant l'état du moniteur temps réel.

Remarque : Sur les systèmes Windows, si l'icône du moniteur temps réel n'est pas affichée, vous pouvez activer le moniteur temps réel à partir du menu Démarrer.

Options disponibles à partir de l'icône du moniteur temps réel

Sur les systèmes Windows, vous pouvez avoir accès à toutes les options du moniteur temps réel à partir de l'icône du moniteur temps réel dans la barre des tâches et gérer la surveillance des fichiers. En outre, les options suivantes sont disponibles :

- **Désactiver temps réel** – Permet de désactiver l'interface de la surveillance en temps réel. L'analyse reste néanmoins activée.
- **Contrôler les fichiers sortants, Contrôler les fichiers entrants et sortants** – Permet de configurer le moniteur temps réel de manière à ce qu'il recherche des virus dans les fichiers lorsqu'ils sont fermés ou lorsqu'ils sont ouverts et refermés.
- **Veille** – Permet de désactiver provisoirement le moniteur temps réel pour un nombre donné de minutes.
- **Icône animée** – Permet d'afficher ou de masquer l'animation de l'icône du moniteur temps réel dans la barre des tâches.
- **Lancer l'antivirus** – Permet de lancer le logiciel antivirus de Computer Associates.
- **Télécharger les signatures maintenant** – Permet d'effectuer une mise à jour de signatures pour l'ordinateur local.
- **A propos de** – Vous permet d'obtenir des informations sur la version installée du logiciel eTrust Antivirus.
- **Quitter** – Permet de supprimer l'icône Moniteur temps réel de la barre des tâches (le moniteur temps réel reste actif).

Messagerie temps réel

Sur les systèmes Windows, si les options Alert sont configurées et activées, des messages peuvent être envoyés par diffusion, Microsoft Mail, Microsoft Exchange, SMTP et SNMP, rapport d'incidents et récepteurs d'appels à chaque action entreprise. Les messages s'affichent également dans le journal d'analyse en temps réel et dans le journal d'événements Windows NT ou la visionneuse des événements Windows 2000. Pour de plus amples informations, consultez l'aide Alert.

Des messages peuvent également être envoyés lorsque l'option Quarantaine est exécutée.

Sur les systèmes UNIX et OS X, vous pouvez envoyer des informations vers un script Shell que vous écrivez vous-même. Le script peut exécuter n'importe quelle action, telle que l'envoi d'un message électronique à une adresse spécifiée lorsqu'un virus est détecté. En outre, sous UNIX et OS X, un événement provoquera l'affichage d'un message dans les fichiers syslog, comme indiqué dans /etc/syslog.conf. Pour plus d'informations concernant le script UNIX, reportez-vous à la section « Utilisation du gestionnaire Alert dans les systèmes UNIX » , au chapitre « Utilisation du gestionnaire Alert » .

Utilisation des options temps réel

Les options du moniteur temps réel permettent de définir les options d'analyse afin de détecter les infections sur votre poste de travail à chaque exécution, accès ou ouverture de fichier.

Remarque : Les options du moniteur temps réel communes à tous les types d'analyse sont décrites dans le chapitre « Utilisation des options d'analyse et de sélection ».

Gestion des paramètres temps réel

Un administrateur autorisé peut configurer et diffuser les paramètres du moniteur temps réel et faire appliquer les règles de ces paramètres. Reportez-vous au chapitre « Utilisation de l'affichage de l'administrateur » pour obtenir plus d'informations sur ce sujet.

Définition de la direction d'analyse

Utilisez les options suivantes pour configurer la direction d'analyse en temps réel pour surveiller les fichiers. Cliquez avec le bouton droit sur l'icône Moniteur temps réel dans la barre des tâches pour accéder à ces options. Ces options de direction sont également disponibles lorsque vous sélectionnez le bouton Temps réel dans la barre d'outils de l'analyseur local.

Option	Description
Fichiers sortants	Surveille les fichiers sortants d'une unité locale. Les fichiers sortants sont les fichiers copiés à partir d'une unité locale et ceux exécutés à partir d'une unité locale. Un fichier sortant est analysé lors de son ouverture. En cas d'infection du fichier, l'accès vous est refusé.
Fichiers entrants et sortants	Surveille à la fois les fichiers entrants et sortants. Un fichier entrant est analysé lors de sa fermeture.

Utilisation des options de sélection temps réel

La plupart des options de sélection temps réel sont communes à tous les types d'analyse. L'option Sélectionner le moteur d'analyse, d'autres options de détection, les options Fichiers ordinaires et Analyser les fichiers compressés sont décrites dans le chapitre « Utilisation des options d'analyse et de sélection ».

Utilisation des options de filtres temps réel

Les options Filtres temps réel vous permettent de spécifier les types de fichiers et de processus que vous souhaitez surveiller.

Exclusion de processus et de répertoires

Vous pouvez utiliser les options d'exclusion pour spécifier les processus (programmes exécutables exécutés sur l'ordinateur) et répertoires dont vous ne souhaitez pas l'analyse par le moniteur temps réel.

Remarque : Lorsque vous saisissez un nom d'un processus à exclure du temps réel sur un ordinateur UNIX ou OS X, ce processus doit comporter le nom complet du chemin.

Remarque : Sur les systèmes NetWare, l'option d'exclusion de processus ne permet que d'indiquer les threads à exclure, et non des NLM individuels.

Vous pouvez ajouter et supprimer ces exclusions selon vos besoins. Dans l'onglet Filtres, cliquez sur les boutons Processus ou Répertoire pour modifier ces options d'exclusion.

- Lorsque vous excluez un processus, tous les fichiers auquel le programme exécutable de l'ordinateur a accès **ne** sont **pas** analysés. (non disponible pour Windows 9x).
- Lorsque vous excluez un répertoire, tous les sous-répertoires et fichiers de ce répertoire **ne** sont **pas** analysés. Vous pouvez également indiquer des fichiers particuliers à exclure.

Lorsqu'un élément est inscrit dans la liste d'exclusion, il n'est pas analysé par le moniteur temps réel. Ces paramètres n'ont pas d'incidence sur les autres types d'analyse.

Utilisation des options Blocage pré-analyse

L'option Blocage pré-analyse permet de bloquer l'accès aux extensions de fichiers spécifiées. Lorsqu'une extension de fichier figure dans la liste des extensions bloquées, tout fichier avec cette extension n'est pas analysé et tout accès à ce fichier est refusé. Ni l'utilisateur ni le système ne peuvent utiliser ce fichier, c'est-à-dire qu'ils ne peuvent pas l'ouvrir, le copier ou l'exécuter.

Cette fonctionnalité peut s'avérer utile lorsqu'un virus a pour cible un certain type d'extension de fichier. Par exemple, en cas de prolifération soudaine d'un nouveau virus attaquant les fichiers .VBS, vous pouvez bloquer l'ensemble des accès à ce type de fichier afin de limiter les risques d'infection.

Pour spécifier les extensions de fichiers à bloquer, cliquez sur le bouton Bloquer. La liste des extensions bloquées s'affiche. Vous pouvez y ajouter toutes les extensions de fichiers à bloquer. Par exemple, VBS bloque l'accès à tous les fichiers .VBS.

Si vous trouvez que le fait de bloquer tous les accès à un certain type de fichier n'est pas concevable, utilisez la fonctionnalité Exempter du blocage pour autoriser l'accès aux fichiers spécifiés. Vous pouvez exempter des fichiers du blocage en cliquant sur le bouton Exempter. La boîte de dialogue Exempter du blocage s'affiche. Utilisez cette fonctionnalité pour inclure un fichier dans une analyse en temps réel même si l'extension du fichier est bloquée par la Liste des extensions bloquées. Ainsi, si un fichier figure dans la liste d'exemptions, il est traité comme un fichier normal et il **est** analysé par le moniteur temps réel.

Remarque : Les fichiers et types de fichiers disponibles que vous pouvez utiliser avec les fonctionnalités Blocage pré-analyse dépendent des paramètres activés dans l'onglet Sélection pour les types d'extensions de fichiers à analyser.

Utilisation des options temps réel avancées

L'onglet Options avancées temps réel permet de gérer les paramètres temps réel des zones protégées et des options de protection avancées.

Zones protégées

Le moniteur temps réel fournit des options de protection avancées et souples pour différents types d'unités. Sur les systèmes Windows, vous pouvez spécifier les zones d'unités protégées à surveiller. Cette option ne s'applique pas aux ordinateurs UNIX. Sur les systèmes UNIX, tous les types d'unités sont toujours protégés.

Protection des unités de disquettes

Les disquettes sont des sources communes d'infection. L'option Protéger les unités de disquettes permet d'analyser une disquette dès qu'elle est accédée. Lorsqu'un fichier est ouvert ou copié à partir d'une disquette, le fichier est analysé avant d'être déplacé vers le disque dur.

Protection des unités du réseau

Copier des fichiers d'une unité mappée vers une autre est également un moyen commun de propager des infections, mais il n'est pas toujours bien compris. Tous les fichiers déplacés entre les unités mappées peuvent être analysés même si aucun fichier ne passe par le disque dur de l'ordinateur local.

Protection de CD-ROM

Vous pouvez surveiller en temps réel les fichiers des CD-ROM.

Options de protection avancées

Les options de protection avancées offrent des fonctions de protection uniques pour l'analyse en temps réel.

Analyser la disquette à l'arrêt

Utilisez l'option Analyser la disquette à l'arrêt pour détecter les éventuelles infections lors de l'arrêt d'un ordinateur.

Lorsque vous redémarrez un ordinateur contenant une disquette dans le lecteur, le secteur d'amorçage de la disquette est utilisé. En cas de contamination de la disquette, elle est susceptible de contaminer tout votre système. Lorsque l'option est activée, le secteur d'amorçage de la disquette est analysé avant l'arrêt de l'ordinateur. Ceci vous évite de redémarrer l'ordinateur avec une disquette comportant un secteur d'amorçage infecté.

Utilisation de l'option Permettre la sauvegarde rapide

L'option Permettre la sauvegarde rapide vous permet de copier les fichiers à enregistrer sur bande lors d'une session de sauvegarde sans que le moniteur temps réel ne les analyse. Par exemple, si vous analysez régulièrement les fichiers d'un disque dur avant de les sauvegarder, vous ne devez pas analyser de nouveau les mêmes fichiers.

Si cette option n'est pas activée, le moniteur temps réel analyse tous les fichiers qui sont copiés sur la bande, ce qui ralentit la sauvegarde. Si vous analysez des fichiers avant l'exécution d'une sauvegarde, vous ne devez pas répéter l'analyse pendant la sauvegarde. Lorsque cette option est activée, le moniteur temps réel ignore les fichiers ouverts par le logiciel de sauvegarde. Ceci améliore les performances de sauvegarde.

Limitation des messages contextuels

L'option Messages contextuels temps réel permet que des messages contextuels s'affichent lorsque le moniteur temps réel détecte plusieurs infections pendant une opération d'analyse. Si cette option n'est pas sélectionnée, aucun message contextuel ne s'affiche. Vous pouvez limiter le nombre de messages contextuels qui s'affichent. Lorsque la limite est atteinte, un message s'affiche vous invitant à vous reporter au journal d'analyse en temps réel pour de plus amples informations. Cette option concerne également NetWare et OS X.

Par exemple, si le moniteur temps réel analyse un fichier compressé contenant dix fichiers infectés, dix messages s'affichent sur votre écran. Si vous fixez la limite à 3, seulement trois messages correspondant aux trois premières infections s'affichent.

Utilisation de l'option Quarantaine

L'option Quarantaine empêche un utilisateur d'exécuter des actions aux conséquences potentiellement désastreuses avec un fichier infecté. Ainsi, une infection n'a pas la possibilité de se propager vers ou à partir d'un serveur avant le nettoyage du poste de travail infecté. Cliquez sur l'onglet Quarantaine pour afficher ces options.

Remarque : L'option Quarantaine est gérée à partir d'ordinateurs Windows NT et Windows 2000. Cette option ne peut pas être gérée à partir d'ordinateurs Windows 9x. Cette option ne s'applique pas aux systèmes UNIX, OS X et NetWare. Cependant, elle est disponible dans l'interface graphique utilisateur du navigateur Web lorsque vous créez des règles devant être appliquées ou gérez un ordinateur Windows dans l'affichage de l'administrateur.

Lorsqu'elle est activée, l'option Quarantaine empêche un utilisateur de déplacer un fichier infecté vers un serveur ou d'exécuter un fichier infecté sur une console de serveur. L'utilisateur ne peut plus accéder au serveur pour la durée spécifiée par le Temps de quarantaine. Un utilisateur peut être mis en quarantaine pour une durée maximale de 24 heures. Pendant la quarantaine, vous pouvez déterminer quel est le fichier posant problème, l'isoler et nettoyer l'ordinateur infecté.

Un message mentionnant le nom de l'utilisateur ayant essayé de déplacer un fichier infecté peut être envoyé pour que les administrateurs compétents puissent être informés.

Le nom d'un utilisateur mis en quarantaine est mentionné dans l'onglet Quarantaine des options du moniteur temps réel lorsqu'un ordinateur particulier est sélectionné dans la liste des ordinateurs. L'administrateur peut accorder de nouveau l'accès à l'utilisateur mis en quarantaine en supprimant son nom de l'écran Quarantaine.

Remarque : Le compte administrateur sur un ordinateur Windows NT ou Windows 2000 ne peut pas être mis en quarantaine. Cependant, un utilisateur disposant de droits d'administrateurs peut être mis en quarantaine si nécessaire.

Messages contextuels de quarantaine

Pour qu'un ordinateur Windows 9x reçoive des messages de quarantaine provenant d'un serveur NT, WinPopup doit être en cours d'exécution. Pour exécuter WinPopup, ouvrez la boîte Exécuter et entrez WinPopup. Vous pouvez également ajouter WinPopup à votre groupe de démarrage si vous utilisez la quarantaine. (WinPopup est aussi compatible avec les postes de travail Windows 3.x.)

Noms d'utilisateurs en double

La quarantaine affecte tout utilisateur ayant le même nom car elle bloque l'accès au serveur sur la base des noms. C'est particulièrement important si un réseau compte plusieurs personnes partageant le même nom d'utilisateur, comme INVITE. Si un utilisateur est connecté en tant qu'INVITE et qu'il est mis en quarantaine alors qu'il tentait de copier un fichier infecté, tous les autres utilisateurs du nom d'INVITE seront aussi mis en quarantaine.

Statistiques du moniteur temps réel

A partir des Options du moniteur temps réel, vous pouvez afficher les statistiques du moniteur temps réel en cliquant sur l'onglet Statistiques.

Elles vous fournissent des informations cumulées sur l'activité du moniteur temps réel, comme le nombre d'infections trouvées, le nombre de fichiers analysés et les actions entreprises.

Etat du pilote temps réel

Sous Windows, outre le résumé des statistiques, l'état des pilotes temps réel est affiché pour indiquer s'ils sont chargés ou non. Ces indicateurs peuvent être utiles pour les diagnostics. De surcroît, le nom du pilote et la version sont indiqués dans la boîte de dialogue des informations de version.

Sous UNIX, le statut ENF s'affiche. Cependant, aucune statistique ne s'affiche, uniquement le statut.

Sous OS X, le statut KEXT s'affiche avec les statistiques.

Pilote de filtres

Le pilote de filtres fournit des services en temps réel pour surveiller les fichiers. L'état de ce pilote doit toujours être indiqué comme étant chargé.

Pilote de disquette

Le pilote de disquette permet de surveiller en temps réel toutes les unités, notamment les lecteurs de disquettes et les unités réseau. Si ce pilote est chargé, toute activité de fichier est protégée en temps réel.

Pour une protection complète en temps réel, redémarrez l'ordinateur pour charger ce pilote. Faites-le après l'installation, après des mises à niveau majeures du produit ou si une mise à jour du pilote est intervenue. Néanmoins, le redémarrage n'est pas nécessaire après l'installation. Si vous ne redémarrez pas après l'installation, le pilote ne sera pas chargé. Vous bénéficiez toujours de la protection en temps réel, mais pas de la protection en temps réel complète. Par exemple, si le pilote de disquette n'est pas chargé, vous ne bénéficiez pas de protection en temps réel lorsque vous copiez des fichiers d'une unité mappée vers le disque dur. Ce pilote doit être chargé pour une protection complète.

Chapitre

6

Planification de jobs d'analyse

Ce chapitre présente les options de planification des jobs d'analyse. Consultez l'aide en ligne pour obtenir de plus amples informations sur l'utilisation de ces options.

Remarque : Du fait qu'il n'existe pas d'affichage de l'analyse locale sous NetWare, les jobs d'analyse planifiés le sont à partir du serveur Admin. Pour plus d'informations sur le serveur Admin, reportez-vous au chapitre « Utilisation de l'affichage de l'administrateur ».

Options de planification des jobs d'analyse

Utilisez les options de planification des jobs d'analyse pour planifier un job et spécifier les options d'analyse que le job devra utiliser.

Les onglets suivants vous permettent de configurer les options de planification des jobs d'analyse :

- Description
- Analyse
- Sélection
- Planification
- Répertoires
- Exclure répertoires

Les options d'analyse et de sélection sont communes aux différents types de méthodes d'analyse. Elles sont décrites au chapitre « **Utilisation des options d'analyse et de sélection** ».

Remarque : Pour afficher les options de planification de jobs d'analyse à partir de la fenêtre de l'analyseur local, vous devez tout d'abord sélectionner un ou plusieurs éléments à analyser en cochant la ou les cases correspondantes dans la liste des éléments située dans la partie gauche de la fenêtre. Ensuite, cliquez sur le bouton de la barre d'outils Planification des jobs d'analyse pour en afficher les options.

Vous pouvez planifier un job d'analyse quels que soient les ordinateurs, catégories et dossiers sélectionnés. Un administrateur autorisé peut définir des règles et planifier des jobs sur des ordinateurs distants. Reportez-vous au chapitre « **Utilisation de l'affichage de l'administrateur** » pour obtenir de plus amples informations sur la définition de règles et sur l'analyse des unités du réseau.

Option de description des jobs d'analyse

L'onglet Description vous permet de fournir une description du job d'analyse. Cette description permet d'identifier le job d'analyse dans la liste Analyseur planifié qui apparaît dans la fenêtre Visionneuse du journal. Cette option est disponible dans l'onglet Règles pour l'administrateur qui utilise l'affichage de l'administrateur afin de créer des règles de planification.

Utilisation des options de planification

L'onglet Planification vous permet de spécifier la date et l'heure d'une analyse et de définir l'intervalle de répétition pour les analyses régulières.

Vous pouvez planifier des jobs d'analyse pour qu'ils s'exécutent de différentes manières.

- Planifier un job d'analyse pour qu'il soit exécuté au démarrage de l'ordinateur
- Planifier un job d'analyse pour qu'il soit exécuté une seule fois
- Planifier un job d'analyse pour qu'il soit répété à intervalles réguliers

Planifier au démarrage

L'option Planifier au démarrage vous permet d'exécuter une analyse au moment du démarrage de votre ordinateur. Lorsque cette option est sélectionnée, les autres options de l'onglet Planification ne sont pas disponibles.

Date et heure

L'option Date vous permet d'indiquer le jour, le mois et l'année du job. La flèche pointant vers le bas permet d'afficher un calendrier pratique pour sélectionner une date. L'option Heure vous permet d'indiquer l'heure du job en heures et minutes.

Options Répéter

Les options Répéter vous permettent d'indiquer la fréquence d'exécution d'un job d'analyse régulier.

Vous pouvez planifier un job d'analyse afin qu'il soit exécuté à intervalles réguliers spécifié par : mois, jours, heures ou minutes. Les administrateurs peuvent utiliser l'affichage de l'administrateur pour créer différentes règles de planification des jobs afin qu'ils soient exécutés une fois par semaine sur certains ordinateurs et une fois par jour sur d'autres ordinateurs. Vous pouvez également planifier des analyses fréquentes pour les unités et les répertoires qui ont un nombre important d'entrées et de sorties. En outre, les circonstances peuvent exiger que des fichiers suspects soient vérifiés rapidement et que vous décidiez de les analyser toutes les dix minutes.

Remarque : Les paramètres des options Date et Heure déterminent la première occurrence de l'analyse à répéter.

Niveau d'utilisation de l'UC

Sur les systèmes Windows, vous pouvez spécifier le niveau d'utilisation de l'UC pour un job d'analyse planifié en indiquant une utilisation de niveau faible, moyen ou élevé. Pendant les périodes de grande production, vous souhaiterez sûrement un faible niveau d'utilisation de l'UC pour une analyse. Pendant les périodes de faible production, vous opterez vraisemblablement pour un niveau plus élevé.

Utilisation de l'option Répertoires

L'onglet Répertoires vous permet de spécifier les répertoires que le job planifié doit analyser. Vous pouvez ajouter ou supprimer des répertoires de la liste.

Lorsque vous établissez une planification en sélectionnant un objet dans la liste de la fenêtre de l'analyseur local et en spécifiant les options d'analyse planifiée, l'emplacement du répertoire contenant l'objet sélectionné apparaît dans la liste des répertoires. L'onglet Répertoires vous permet d'ajouter ou de supprimer des objets dans la liste des répertoires. Vous pouvez également le faire lorsque vous modifiez un job d'analyse planifié.

Utilisation de l'option Exclure répertoires

L'onglet Exclure répertoires vous permet de spécifier les répertoires que le job planifié **ne** devra **pas** analyser. Vous pouvez ajouter des répertoires à la liste ou en supprimer.

Comme pour l'onglet Répertoires, vous pouvez accéder à cette option lorsque vous établissez une planification à partir de l'analyseur local et que vous modifiez une analyse planifiée.

Remarque : Si vous souhaitez analyser l'ensemble de votre disque dur, à l'exception d'un répertoire, sélectionnez l'analyse du lecteur C:\ dans la liste de la fenêtre de l'analyseur local ou le répertoire racine sur un système UNIX, puis spécifiez les options pour l'analyse planifiée. Ensuite, vous pouvez utiliser l'option Exclure répertoires pour n'exclure que le répertoire que vous ne souhaitez pas analyser.

Gestion des jobs d'analyse planifiés

Lorsque les options sont spécifiées pour un job d'analyse planifié, les jobs d'analyse planifiés disponibles s'affichent dans la fenêtre de l'analyseur local. Sélectionnez la catégorie Jobs d'analyse planifiés dans la liste de gauche afin d'afficher à droite la liste récapitulative des jobs planifiés.

Chaque job apparaît dans la liste avec des indications (état, numéro identificateur, type, description, date planifiée pour l'exécution et action sur fichier spécifiée). Les jobs planifiés à distance ne sont pas affichés.

Modification des options de planification de jobs

Vous pouvez modifier les options des jobs d'analyse planifiés – par exemple la date d'exécution du job, ce qu'il analyse, etc.

Lorsque vous créez un nouveau job planifié, les options sont affichées dans la boîte de dialogue Planifier un nouveau job d'analyse. Si vous souhaitez modifier les options pour un job existant, utilisez la fenêtre de l'analyseur local pour y accéder. Pour cela, sélectionnez la catégorie Jobs d'analyse planifiés dans la liste de gauche afin d'afficher à droite la liste récapitulative des jobs planifiés. Ensuite, cliquez avec le bouton droit de la souris sur un job et choisissez Options. Les options sont alors affichées dans la boîte de dialogue Modifier les options du job.

Arrêt d'un job

Pour arrêter un job planifié en cours d'exécution, sélectionnez la catégorie Jobs d'analyse planifiés afin d'afficher à droite leur liste récapitulative. Ensuite, cliquez avec le bouton droit de la souris sur un job et sélectionnez Arrêter.

Suppression d'un job

Pour supprimer un job planifié, sélectionnez la catégorie Jobs d'analyse planifiés afin d'afficher à droite leur liste récapitulative. Ensuite, cliquez avec le bouton droit de la souris sur un job et sélectionnez Supprimer.

Affichage des propriétés du job

Après l'exécution d'un job planifié, vous pouvez afficher les propriétés de ce job à partir de la fenêtre Visionneuse du journal.

Affichage des résultats d'une analyse planifiée

La fenêtre de la visionneuse du journal vous permet d'afficher les résultats d'une analyse planifiée. Veuillez vous reporter au chapitre « **Affichage et gestion des journaux** » pour obtenir de plus amples informations sur l'affichage des résultats du journal.

Grâce à l'affichage de l'administrateur, les administrateurs autorisés peuvent afficher les résultats des analyses planifiées à distance.

Statistiques du job pour une analyse planifiée en cours

Pendant l'exécution d'un job d'analyse planifié, vous pouvez consulter les statistiques du job dans la boîte de dialogue Statistiques du job planifié. Pour cela, cliquez sur le bouton de la barre d'outils Statistiques du job, dans la fenêtre de l'analyseur local. Vous pouvez également sélectionner Job d'analyse planifié dans le menu Analyseur, puis cliquer sur Statistiques.

La boîte de dialogue Statistiques du job planifié affiche le répertoire qui est en train d'être analysé et l'ID du job planifié en cours d'exécution. Le résumé des statistiques s'affiche, indiquant le nombre total d'infections détectées (fichiers désinfectés, supprimés, déplacés et renommés) ainsi que le nombre de fichiers analysés. Ces informations sont identiques à celles contenues dans le Résumé du résultat de l'analyse, que vous pouvez afficher après une analyse locale. Si un job d'analyse planifié n'est pas exécuté, aucune statistique ne s'affiche dans la boîte de dialogue. A la fin d'une analyse planifiée, utilisez la Visionneuse du journal pour afficher les informations sur le job.

Chapitre

7

Affichage et gestion des journaux

NetWare ne dispose pas de visionneuse du journal. Les journaux des ordinateurs NetWare peuvent être consultés à partir de la vue Admin du serveur Admin. Pour plus d'informations sur le serveur Admin, reportez-vous au chapitre « Utilisation de l'affichage de l'administrateur ».

Ce chapitre vous indique comment utiliser la fenêtre Visionneuse du journal pour gérer et afficher les différents types de journaux d'analyse pour l'ordinateur local. Vous pouvez visualiser les résultats de tous les types d'analyse et afficher le résumé et les informations détaillées qui résultent de chaque analyse, notamment les analyses exécutées à distance par un administrateur, à partir de la fenêtre Affichage de l'administrateur. Consultez l'aide en ligne pour obtenir de plus amples informations sur la visionneuse du journal.

En outre, ce chapitre décrit comment spécifier les options du journal pour une analyse. Il contient également des informations sur l'utilisation de journaux dans le cadre d'un format de base de données standard et sur la collecte d'informations relatives aux performances du système.

Remarques :

- L'affichage de l'administrateur est doté de fonctionnalités particulières pour afficher les informations du journal à partir d'ordinateurs distants. Pour en savoir plus, reportez-vous au chapitre « Utilisation de la fenêtre Affichage de l'administrateur ».

- Les termes « branche » et « conteneur » sont synonymes.

Utilisation de la fenêtre Visionneuse du journal

La fenêtre Visionneuse du journal permet de sélectionner, d'afficher et de gérer les journaux d'activité d'analyse.

La fenêtre Visionneuse du journal affiche à gauche une liste des différentes catégories de journaux. Surlignez la catégorie souhaitée pour afficher à droite la liste sommaire des journaux disponibles. Pour chaque catégorie, les journaux sont classés suivant la date et l'heure de leur création.

Lorsque vous sélectionnez un élément dans la visionneuse du journal et que vous cliquez dessus avec le bouton droit de la souris, différentes options sont disponibles pour supprimer, imprimer, afficher les propriétés ou actualiser l'affichage des informations du journal. Vous pouvez également utiliser les options du menu et les boutons de la barre d'outils pour accéder à ces options.

Remarque : Pour consulter les informations les plus récentes concernant un job d'analyse, utilisez l'option Actualiser afin de mettre à jour l'affichage de l'élément sélectionné dans la visionneuse du journal.

Liste de la visionneuse du journal

La liste de la visionneuse du journal peut inclure des journaux pour les types de jobs d'analyse suivants :

- Analyseur local
- Analyseur en temps réel
- Analyseur planifié
- Evénements généraux
- Evénements de distribution

Analyseur local

La catégorie Analyseur local contient une liste des journaux contenant les résultats des jobs d'analyse exécutés sur votre ordinateur local.

Analyseur en temps réel

La catégorie Analyseur en temps réel contient le journal d'analyse du moniteur temps réel pour l'ordinateur local. Les informations concernant l'analyse en temps réel sont jointes au journal existant ; il y a donc une seule entrée de journal par jour.

Analyseur planifié

La catégorie Analyseur planifié contient une liste des jobs d'analyse planifiés. Chaque job donne lieu à la création d'un journal d'analyse contenant les résultats de chacune des exécutions du job, classés suivant la date et l'heure planifiées. Si un job n'est exécuté qu'une fois, un seul journal de résultats est généré. Si un job est exécuté périodiquement, un seul journal de résultats est créé pour chaque job d'analyse.

L'utilisateur d'un ordinateur local peut visualiser les journaux d'analyse planifiée pour cet ordinateur local, qu'il s'agisse d'analyses exécutées localement ou à distance. Un administrateur autorisé peut visualiser les journaux d'analyse planifiée pour plusieurs ordinateurs, à partir de la fenêtre d'affichage de l'administrateur.

Evénements généraux

La catégorie Evénements généraux contient les journaux des événements généraux qui ont lieu chaque jour. Les codes d'erreurs du système d'exploitation peuvent également y apparaître. Les types de messages suivants peuvent s'afficher :

Message critique – Il s'agit d'un message de la plus haute importance. Le message nécessite une attention immédiate une fois enregistré. Ce message peut signifier qu'un virus a été détecté ou qu'un problème a été identifié au niveau du service, tel qu'une erreur lors du chargement d'un moteur.

Message d'avertissement – Ce second niveau de messages vous avertit en cas de problème non critique.

Message d'information – Ce type de messages fournit des informations sur les événements, notamment lorsque le service démarre ou s'arrête et si aucun virus n'a été détecté.

Evénements de distribution

La catégorie Evénements de distribution contient les journaux des événements de distribution des mises à jour de signatures qui ont lieu chaque jour. Les événements sont enregistrés pour toute action se produisant pendant la mise à jour des signatures ou pendant la distribution. Ceci inclut les détails concernant la connexion à une source de distribution de signatures, le démarrage et l'arrêt d'un téléchargement ainsi que les informations sur l'état du téléchargement des fichiers de signatures.

Affichage de l'administrateur des journaux

Dans un environnement en réseau, les administrateurs peuvent afficher tous les types de journaux (exécutés localement ou à distance) pour plusieurs ordinateurs, en utilisant la fenêtre Affichage de l'administrateur.

Pour l'administrateur, les journaux sont listés sous chaque ordinateur dans un conteneur de l'arborescence de l'organisation situé dans la fenêtre Affichage de l'administrateur. Il existe également des journaux récapitulatifs pour chaque instance de règle du job d'analyse, avec les résultats pour chacun des ordinateurs qui appliquent ces règles.

Affichage du résumé et des informations détaillées du journal

Lorsque vous sélectionnez une catégorie de journal dans la liste de gauche, les informations sommaires du journal s'affichent à droite de l'écran.

Les informations sommaires relatives aux analyses incluent la date et l'heure d'exécution de l'analyse, le nombre de fichiers analysés, le nombre de fichiers infectés, le nombre d'infections détectées, le nombre d'erreurs d'analyse et l'action appliquée à l'analyse.

Lorsque vous sélectionnez un journal dans la liste de droite, les informations détaillées du journal s'affichent dans le volet inférieur droit. Parmi ces détails figurent les résultats pour chaque fichier analysé.

Chaque type de job d'analyse possède une icône d'identification. Consultez l'aide en ligne pour plus d'informations sur les journaux.

Gestion des journaux

Vous pouvez gérer le type d'informations figurant dans les fichiers journaux, collecter les données historiques et les utiliser pour analyser l'impact de l'activité d'analyse.

Spécification des options du journal pour une analyse

Utilisez les options du journal afin de spécifier les options pour la gestion des journaux d'analyse. Un journal de résultats est créé pour chaque analyse effectuée. Ces fonctions vous permettent de recueillir le niveau d'enregistrement historique de l'activité d'analyse requis par votre organisation. Pour accéder aux options du journal, à partir de la fenêtre de l'analyseur local, affichez les options correspondantes et cliquez sur l'onglet Journal.

Filtrage des informations fichiers pour les journaux

Vous pouvez spécifier les types d'événements devant figurer dans un journal. Utilisez les options de filtres pour indiquer si les informations relatives à un fichier doivent être comprises dans la liste du journal ou non. Ces options vous permettent de concevoir vos journaux d'analyse en fonction du type d'informations dont vous avez besoin. Vous pouvez enregistrer les informations qui concernent

- Les fichiers infectés
- Les fichiers propres dont l'examen a révélé l'absence de virus
- Les fichiers ignorés et exclus de l'analyse

Cochez l'option Fichiers propres afin d'inclure dans le journal les informations relatives aux fichiers qui sont analysés et qui ne sont pas infectés. Cochez l'option Fichiers infectés afin d'inclure dans le journal les informations relatives aux fichiers qui sont infectés. Cochez l'option Fichiers ignorés afin d'inclure dans le journal les informations relatives aux fichiers qui ont été exclus de l'analyse.

La majorité des utilisateurs souhaitent uniquement enregistrer les fichiers infectés qui ont été détectés. Cependant, il se peut que votre entreprise ait besoin de conserver des enregistrements plus détaillés de l'activité d'analyse. Par exemple, il vous faudra peut-être un enregistrement vous permettant de savoir si un fichier a été analysé ou non. Si vous sélectionnez l'option Fichiers propres, tous les fichiers analysés par le détecteur de virus et ne présentant aucune infection sont répertoriés dans le journal. En consignant les informations relatives aux fichiers propres, vous disposez non seulement d'un enregistrement des fichiers infectés mais également d'un enregistrement indiquant qu'un fichier particulier a été examiné et qu'il ne présente aucune infection. De même, l'option Fichiers ignorés génère un enregistrement des fichiers qui ne sont pas examinés dans une analyse, notamment lorsque votre analyse est configurée pour ignorer un type spécifique d'extension de fichier.

Par ailleurs, les informations collectées dans les journaux peuvent être utilisées pour évaluer les résultats et l'activité d'analyse à l'échelle de l'entreprise. Pour de plus amples informations sur ce sujet, reportez-vous au chapitre « Collecte d'informations sur les performances du système ».

Conservation des fichiers journaux

Les options de purge du journal vous permettent de déterminer combien de jours vos fichiers journaux sont conservés et affichés dans la fenêtre Affichage du journal. Dans la barre d'outils de la visionneuse du journal, cliquez sur le bouton Option de purge des journaux, sélectionnez l'option Supprimer tous les fichiers journaux datant de plus de et utilisez le champ Jours pour indiquer combien de jours vos fichiers journaux doivent être conservés. Lorsque le nombre de jours indiqué est écoulé, les fichiers journaux sont supprimés. Les administrateurs peuvent également disposer de cette option à partir de la fenêtre Affichage de l'administrateur.

Impression et suppression de journaux

Vous pouvez imprimer ou supprimer les journaux au moyen des options de la fenêtre Visionneuse du journal.

- Pour imprimer un journal de la liste, cliquez dessus avec le bouton droit de la souris puis sélectionnez l'option Imprimer le journal. L'interface graphique utilisateur du navigateur Web ne prend pas en charge l'option permettant d'imprimer les journaux.
- Pour supprimer un journal de la liste, cliquez dessus avec le bouton droit de la souris, puis sélectionnez l'option Supprimer.
- Pour supprimer tous les journaux d'une catégorie, cliquez avec le bouton droit sur la catégorie dans la liste de gauche et sélectionnez l'option Supprimer tout.

Journaux dans un format de base de données standard

Toutes les informations du journal sont stockées dans un répertoire DB, dans un format de fichier accessible par des outils de base de données standard, en utilisant les normes ODBC (Open DataBase Connectivity). Ce type de fichier journal est nommé selon le mois, le jour, l'année et l'heure de sa création, et il porte l'extension .DBF(.dbf dans les systèmes UNIX et OS X).

Identification de l'emplacement du répertoire des journaux

Pour rechercher le chemin et le nom du répertoire des journaux, démarrez eTrust Antivirus, dans le menu Analyseur, sélectionnez Options de l'analyseur local… et cliquez sur l'onglet Répertoire.

Collecte d'informations sur les performances du système

Sur les systèmes Windows, les fonctionnalités de mesure de performances informatiques vous permettent de collecter des informations sur l'activité antivirus afin d'analyser l'impact de cette activité au sein de votre entreprise. Vous pouvez utiliser les méthodes et fonctionnalités de collecte suivantes :

- Collecte de journaux d'analyse au moyen de jobs planifiés
- Utilitaire en mode commande pour les planificateurs ou scripts de connexion
- Intégration de l'option TNG Data Transport
- Accès aux informations des fichiers journaux en utilisant des bases de données standard
- Surveillance des statistiques temps réel au moyen du moniteur des performances
- Purge des enregistrements collectés

Vous pouvez créer des jobs planifiés en vue de collecter les journaux d'analyse à partir d'ordinateurs personnels ou de groupes d'ordinateurs appartenant au réseau. Les informations des journaux peuvent être collectées de façon globale ou incrémentielle. Ces données sont ensuite stockées dans un emplacement centralisé. En outre, vous pouvez utiliser l'option TNG Data Transport pour planifier et collecter les informations du journal.

Toutes les informations du journal sont stockées dans un format de fichier accessible par les outils de base de données standard grâce à l'interface standardisée ODBC (Open DataBase Connectivity).

Surveillance de l'activité temps réel

Grâce à l'application standard PERFMON (moniteur des performances) sur Windows NT, Windows 2000 et Windows Server 2003, il vous est possible de surveiller l'activité antivirus temps réel.

Les activités temps réel suivantes peuvent être contrôlées par le Moniteur des performances au moyen de compteurs :

- Infections par virus d'amorçage
- Erreurs de désinfection
- Virus d'amorçage désinfectés
- Fichiers désinfectés
- Fichiers supprimés
- Virus détecté
- Fichiers infectés
- Fichiers déplacés
- Fichiers renommés
- Erreur d'analyse
- Ordinateur analysé
- Fichiers analysés
- Fichiers analysés dans les archives

Pour de plus amples informations sur la surveillance de l'activité, reportez-vous à la documentation Windows consacrée au Moniteur de performances.

Chapitre

8

Utilisation de l'affichage de l'administrateur

Un administrateur antivirus autorisé peut utiliser l'affichage de l'administrateur pour la gestion à distance de tous les aspects de eTrust Antivirus. Ce chapitre décrit l'utilisation de la fenêtre Affichage de l'administrateur et d'autres éléments pour l'administration de votre réseau antivirus.

Vous pouvez effectuer les opérations suivantes à partir de l'affichage de l'administrateur :

- Gestion de l'organisation logique des ordinateurs et de leur accès par les utilisateurs
- Utilisation des fonctionnalités de sécurité pour contrôler l'accès aux fonctionnalités de gestion à distance de l'affichage de l'administrateur
- Gestion des options de messagerie grâce aux options Temps réel de messagerie
- Configuration et surveillance des règles sur l'ensemble du système
- Gestion et diffusion des configurations à travers le réseau
- Gestion de la découverte d'ordinateurs dans votre réseau antivirus
- Configuration des ordinateurs proxy de distribution
- Affichage des rapports

Les fonctionnalités de l'affichage de l'administrateur (serveur Admin, client administrateur) ne sont pas disponibles depuis des ordinateurs Windows 9x.

Utilisation de la fenêtre Affichage de l'administrateur

La fenêtre Affichage de l'administrateur fournit une interface de type Explorateur pour la gestion à distance des paramètres de configuration et des ordinateurs de votre réseau antivirus.

En tant qu'administrateur antivirus autorisé, vous contrôlez l'affichage de cette fenêtre. Seul un utilisateur autorisé peut accéder à cette fenêtre. Un utilisateur exécutant des analyses sur un ordinateur local n'a pas besoin de cette fenêtre. C'est pourquoi l'accès à cette option peut être limité et donc impossible pour la plupart des utilisateurs.

Pour les utilisateurs autorisés à accéder à l'affichage de l'administrateur, vous pouvez utiliser les droits d'accès pour définir le niveau de contrôle autorisé pour les utilisateurs.

La fenêtre Affichage de l'administrateur vous permet de gérer l'organisation, ou la configuration logique, de tous les ordinateurs de votre réseau qui exécutent des instances du logiciel antivirus de Computer Associates. Ceci vous permet de gérer les ordinateurs, de diffuser des règles et d'imposer des paramètres dans l'ensemble du réseau de façon efficace.

Utilisation du serveur Admin

Le serveur Admin garde une trace de toutes les instances du logiciel antivirus de Computer Associates exécutées sur des ordinateurs de votre réseau. Il stocke cette liste d'ordinateurs basée sur les sous-réseaux qu'il doit interroger. Il garde également une trace de l'état des comptes d'utilisateurs et de leurs droits d'accès. Grâce au processus de découverte, il surveille la présence d'ordinateurs et toute modification effectuée dans les paramètres de règles. L'ensemble de ces informations est ensuite rendu disponible via l'affichage de l'administrateur.

Considérations relatives à l'installation du serveur Admin

Pour donner à un ordinateur le statut de serveur Admin sous Windows, sélectionnez l'option serveur Admin. Sous UNIX, répondez par « o » lorsque que le système vous demande si vous souhaitez exécuter le serveur d'administration sur votre ordinateur. Sous OS X, sélectionnez Personnaliser dans la boîte de dialogue Easy Install et cochez Serveur administrative dans la boîte de dialogue Installation personnalisée.

Conservation des données du serveur Admin

Si vous réinstallez le serveur Admin, vous pouvez conserver les paramètres de configuration des règles et les informations du conteneur de l'arborescence de l'organisation stockés dans le serveur Admin.

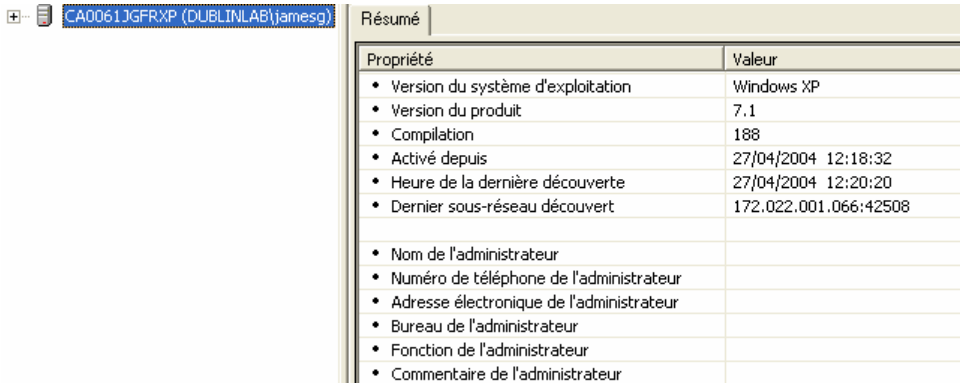
Connexion au serveur Admin

Lorsque vous affichez la fenêtre Affichage de l'administrateur pour la première fois au cours d'une session, il vous est demandé de vous connecter à un serveur Admin. Vous devez indiquer le nom du serveur ainsi qu'un nom d'utilisateur et un mot de passe valides. Après la connexion, le serveur Admin est affiché dans la fenêtre Affichage de l'administrateur comme élément racine de la liste située sur le côté gauche de la fenêtre. Reportez-vous à la section « Utilisation des droits d'accès » pour plus d'informations sur les comptes d'utilisateurs.

Vous pouvez également utiliser le bouton Connexion au serveur Admin dans la barre d'outils de l'affichage de l'administrateur pour vous connecter à un serveur.

Remarque : Lorsque vous n'êtes pas connecté à un serveur Admin, rien n'est affiché dans la fenêtre Affichage de l'administrateur.

La figure suivante montre un exemple du serveur Admin sélectionné, avec des informations sommaires sur le serveur Admin à droite.



Vous pouvez personnaliser les informations concernant l'administrateur en sélectionnant le bouton Gestionnaire du serveur Admin dans la barre d'outils.

Vous pouvez vous connecter à plusieurs serveurs Admin ; cependant l'arborescence de chaque serveur Admin est gérée séparément. Vous ne pouvez pas appliquer de paramètre de règles défini pour un serveur Admin à un ordinateur contrôlé par un autre serveur Admin.

Lorsque vous configurez votre réseau antivirus et vous connectez au serveur Admin pour la première fois, vous devez spécifier les sous-réseaux de votre réseau antivirus que le serveur Admin doit découvrir. Reportez-vous à la section « Utilisation des sous-réseaux » pour en savoir plus. Une fois les options de découverte du sous-réseau spécifiées, vous ou un utilisateur autorisé pouvez organiser les ordinateurs dans votre réseau antivirus.

Serveur Admin étendu

Lorsque vous vous connectez à un serveur Admin et que vous le développez, le côté gauche de la fenêtre Affichage de l'administrateur affiche les catégories suivantes :

- Serveur Admin (catégorie racine)
- Paramètres de configuration
- Domaines hérités
- Conteneur de l'arborescence de l'organisation

La figure suivante montre un exemple de catégorie racine du serveur Admin étendu.

Un utilisateur autorisé peut utiliser ces catégories pour configurer les paramètres des règles, gérer les ordinateurs hérités, créer des groupes logiques d'ordinateurs, ajouter et retirer des ordinateurs de l'arborescence de l'organisation et définir les droits d'accès.

Vous pouvez afficher les options disponibles en développant une catégorie de la liste à gauche de la fenêtre, en mettant en surbrillance un élément de la liste et en cliquant dessus avec le bouton droit de la souris. En outre, des informations relatives aux éléments de la liste sont affichées à droite. La barre d'outils et la barre de menus permettent également d'accéder aux options.

Considérations relatives au serveur Admin

Veuillez tenir compte des points suivants lors de l'utilisation du serveur Admin.

- L'ordinateur sur lequel est installé le serveur Admin doit exécuter la version serveur du logiciel antivirus de Computer Associates. Sur les systèmes Unix et OS X vous devez avoir choisi d'installer le logiciel de serveur administratif. Sur les systèmes NetWare, le serveur Admin n'est pas disponible.
- Un même réseau peut compter plusieurs serveurs Admin.
- Vous devez utiliser un compte de système d'exploitation valide sur l'ordinateur où réside le serveur Admin pour vous connecter à ce dernier et accéder à l'affichage de l'administrateur afin de gérer les ordinateurs et paramètres de règles.
- Le composant permettant d'utiliser l'affichage de l'administrateur est installé lorsque vous sélectionnez l'option Client administrateur lors de l'installation. Sur les systèmes OS X, l'affichage de l'administrateur est activé quand vous choisissez d'installer le logiciel de serveur administratif.
- Pour gérer des ordinateurs à distance avec l'affichage de l'administrateur , TCP/IP doit être installé et configuré correctement sur le réseau et les ordinateurs concernés.
- L'accès aux fonctions que l'utilisateur peut exécuter dans l'affichage de l'administrateur est contrôlé par un administrateur autorisé.
- Vous devez posséder un compte avec droits d'accès administrateur pour le système d'exploitation sur tous les ordinateurs que vous souhaitez ajouter à un conteneur de l'arborescence de l'organisation.
- Les fonctionnalités Serveur Admin et Client administrateur ne sont pas disponibles depuis des ordinateurs Windows 9x.
- Sur les systèmes OS X, l'utilisateur root doit être activé avant d'utiliser le serveur administratif pour la première fois. Consultez le gestionnaire Apple Netinfo pour activer l'utilisateur root.

Reportez-vous à la section « Utilisation des droits d'accès » pour plus d'informations sur la gestion de l'accès au serveur Admin.

Spécification d'un serveur Admin lors de l'installation

Vous avez la possibilité de vous connecter à un serveur Admin au moment de l'installation. Si vous indiquez un serveur Admin au moment de l'installation, une relation de confiance est établie de sorte que les ordinateurs sont ajoutés à la catégorie racine de l'arborescence de l'organisation automatiquement sans que l'administrateur n'ait à spécifier un nom d'utilisateur et un mot de passe pour chaque ordinateur.

Lors de l'installation de systèmes UNIX, une relation de confiance est établie par l'intermédiaire de l'utilisateur root. Sous OS X, une relation de confiance est établie en demandant que l'utilisateur installant le logiciel ait des droits administratifs. L'installation se poursuit sans qu'il soit nécessaire de sélectionner un serveur Admin.

Rôle du serveur Admin

Les étapes suivantes résument l'utilisation du serveur Admin pour collecter et configurer une liste d'ordinateurs. La plupart des étapes décrites sont transparentes pour l'utilisateur.

1. Installez le composant Serveur Admin.
2. Indiquez un sous-réseau dans le réseau interrogé par le serveur Admin, pour initier le processus de découverte.
3. Un ordinateur sélectionné dans le sous-réseau renvoie au serveur Admin les informations relatives à tous les ordinateurs du sous-réseau qui exécutent le logiciel antivirus de Computer Associates.
4. Le serveur Admin affiche l'instance du sous-réseau avec une liste des ordinateurs disponibles dans l'affichage de l'administrateur.
5. Un administrateur autorisé utilise ensuite cette liste pour créer une configuration logique organisée d'ordinateurs dans le réseau, en utilisant la catégorie Arborescence de l'organisation pour répondre aux besoins de l'entreprise.

Découverte des ordinateurs par le serveur Admin

Un administrateur autorisé indique les sous-réseaux que le serveur Admin doit interroger en utilisant la catégorie Sous-réseaux dans les paramètres de configuration. Ensuite, grâce à un processus de sélection transparent pour l'utilisateur, un ordinateur de ce sous-réseau est sélectionné pour répondre au serveur Admin.

L'ordinateur sélectionné répond au serveur Admin par des informations relatives aux ordinateurs du sous-réseau qui exécutent le logiciel antivirus de Computer Associates. Chaque instance du logiciel antivirus reçoit sur un port spécifié et des informations sur chaque ordinateur sont renvoyées au serveur Admin, avec les mises à jour pour chaque modification depuis la découverte précédente.

Les informations découvertes sont réactualisées à intervalle régulier, spécifié dans le cadre des propriétés de l'instance de sous-réseau. Les utilisateurs disposent également des options de réactualisation pour mettre l'affichage à jour.

Les informations comprennent des données sur la version du programme exécutée par un ordinateur, telles que le niveau de version, le nom de l'ordinateur, les paramètres en temps réel, les paramètres des règles et autres données générales. A partir de ces informations, le serveur Admin crée une liste des ordinateurs disponibles dans le réseau antivirus. Cette liste est utilisée pour compléter de manière dynamique la liste des ordinateurs apparaissant dans l'affichage de l'administrateur lorsque vous mettez en surbrillance une instance d'un sous-réseau. Des informations supplémentaires relatives aux ordinateurs apparaissent également dans l'affichage de l'administrateur telles que les droits d'accès et les paramètres de règles. Ce processus conserve des informations courantes sur l'ordinateur après son association avec un conteneur de l'arborescence de l'organisation.

Reportez-vous à la section « Utilisation des sous-réseaux » pour en savoir plus sur la définition des options de découverte et de sélection de sous-réseaux.

Prise en charge LDAP

Sur les systèmes Windows, vous pouvez accéder au serveur Admin par l'intermédiaire du protocole LDAP (Lightweight Directory Access Protocol). Le serveur OpenLDAP de Computer Associates vous permet d'afficher des informations du serveur Admin en mode de lecture seule, en utilisant le navigateur activé de la version 2 LDAP. Avec le serveur LDAP installé, vous pouvez vous connecter au serveur Admin pour afficher les ordinateurs dans les conteneurs que surveille le serveur Admin, notamment les règles appliquées aux branches de l'arborescence de l'organisation, aux données de sous-réseau et aux domaines hérités.

Considérations LDAP

Les conditions et considérations suivantes doivent être prises en compte lors de l'utilisation du serveur LDAP.

- Le serveur LDAP doit être installé sur le même ordinateur que le serveur Admin.
- Aucun autre programme ne peut utiliser le port 389 (exemple : serveurs de certification).
- Pour installer le serveur LDAP du dossier …/bin/support/ldap.x86 vers la source de distribution, veuillez exécuter setup.exe.
- Vous devez ouvrir le serveur OpenLDAP de CA sur le serveur Admin que vous souhaitez afficher.
- Avec l'explorateur LDAP, naviguez jusqu'au serveur Admin que vous souhaitez afficher et définissez le nom distinct de base (DN : Distinguished Name) en tant que branche=*admin_server* ; ce dernier étant le nom du serveur Admin.

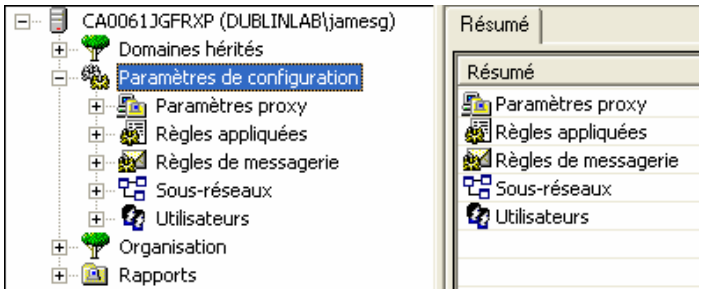
Gestion des paramètres de configuration

Utilisez la catégorie des paramètres de configuration pour configurer votre réseau antivirus Computer Associates et définir les paramètres de règles à appliquer aux conteneurs des ordinateurs pouvant être sélectionnés dans l'arborescence de l'organisation de l'affichage de l'administrateur.

Les paramètres de configuration regroupent les catégories suivantes :

- Règles de messagerie
- Règles appliquées
- Paramètres proxy
- Sous-réseaux
- Utilisateurs

La figure suivante illustre la catégorie des paramètres de configuration étendue.



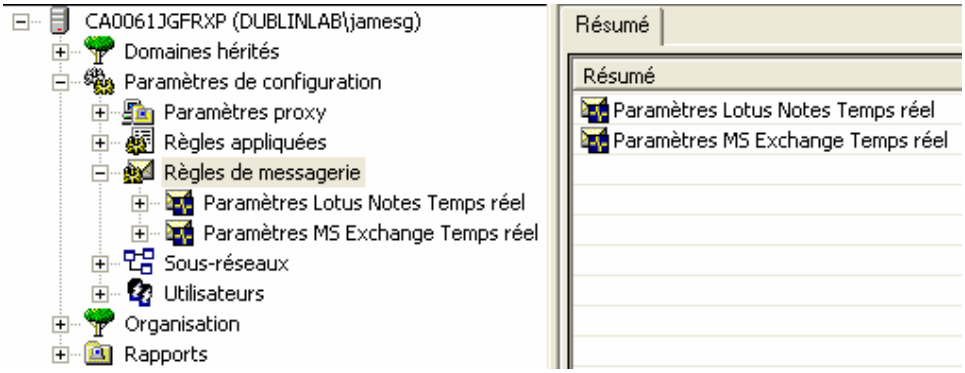
Lorsque vous sélectionnez une catégorie dans la liste située dans la partie gauche de la fenêtre Affichage de l'administrateur, des informations résumées s'affichent dans la partie droite de la fenêtre.

Utilisation des règles de messagerie

La catégorie Règles de messagerie permet de créer des paramètres de règles pour les analyses de messages en temps réel sur votre serveur de messagerie Lotus Note ou Microsoft Exchange.

En utilisant ces fonctions, vous pouvez mettre en vigueur les paramètres définis par l'administrateur concernant les analyses de virus sur vos serveurs de messagerie.

La figure suivante illustre la catégorie de règles de messagerie.



Utilisation des paramètres de la messagerie électronique en temps réel

Les paramètres de la messagerie électronique en temps réel permettent de créer des paramètres de règles pour les analyses de messages en temps réel sur votre serveur de messagerie. Vous pouvez définir de nombreuses options différentes pour l'analyse.

Règles – L'onglet Règles vous permet de libeller l'instance de règle et de verrouiller les paramètres pour les ordinateurs distants si vous le souhaitez. Lorsque vous verrouillez les paramètres, vous empêchez les utilisateurs de modifier les paramètres transmis aux ordinateurs distants. Lorsque les paramètres des règles sont appliqués, ils ont priorité sur les paramètres de l'ordinateur distant.

Analyse – L'onglet Analyse vous permet de modifier le niveau d'analyse, le moteur d'analyse et les options de détection, ainsi que de contrôler comment traiter l'infection si elle est détectée.

Sélection – L'onglet Sélection vous permet de choisir les types d'extensions de fichiers à inclure ou à exclure de l'analyse et les types de fichiers compressés à analyser. Vous pouvez également utiliser les options de blocage pré-analyse pour verrouiller le transfert de pièces jointes contenues dans les courriers électroniques selon une terminaison du fichier (pour Microsoft Exchange) ou extension (pour Lotus Notes Domino) spécifique.

Notification – Pour l'option Temps réel de messagerie Lotus Notes Domino, vous pouvez configurer des options de notification spécifiques pour alerter le propriétaire de la boîte aux lettres, l'expéditeur du message ou l'administrateur système lorsqu'une infection est détectée dans le système de messagerie.

Options – L'onglet Options vous permet de sélectionner les paramètres personnalisés pour l'analyse des messages électroniques de votre serveur Microsoft Exchange 2000. Vous pouvez choisir parmi les options disponibles pour affiner les performances de votre logiciel antivirus sur votre serveur Microsoft Exchange 2000.

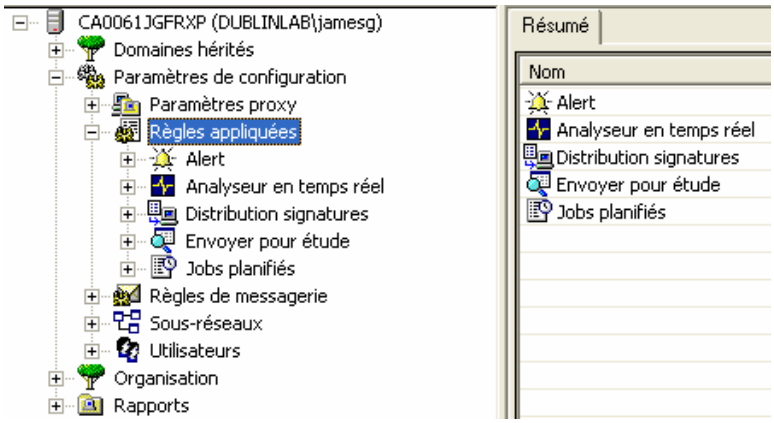
Divers – L'onglet Divers vous permet de spécifier les diverses options disponibles pour les analyses de courrier Microsoft Exchange. Vous pouvez spécifier la taille du journal, le nombre d'anciens journaux à conserver et le niveau de détail du journal. Vous pouvez également activer le journal d'événements système, spécifier la durée de l'attente et activer l'analyse antivirus d'arrière-plan.

Utilisation des règles appliquées

La catégorie Règles appliquées vous permet de créer des paramètres de règles qui s'appliquent aux conteneurs et à leurs ordinateurs dans l'arborescence de l'organisation :

- Alert
- Analyseur en temps réel
- Jobs planifiés
- Envoyer pour analyse
- Distribution signatures

La figure suivante illustre la catégorie de règles appliquées étendue.



Utilisation des fonctionnalités Règles appliquées

Les fonctionnalités Règles appliquées permettent de définir les paramètres de configuration des ordinateurs de votre réseau antivirus afin que les utilisateurs ne puissent pas modifier les paramètres s'ils n'en ont pas la permission. L'application des règles est une fonctionnalité puissante que les administrateurs peuvent utiliser pour surveiller les paramètres du logiciel antivirus de Computer Associates dans l'entreprise ou pour des conteneurs d'ordinateurs sélectionnés. Grâce à cette fonctionnalité, vous êtes assuré que les options d'analyse appropriées sont exécutées sur les ordinateurs des utilisateurs et que ces derniers ne modifient pas d'options importantes. Vous pouvez définir des règles pour chaque option pouvant être configurée à distance.

Application des règles

Vous pouvez surveiller les règles en appliquant un paramètre de règles à un conteneur.

Lors de la découverte de sous-réseaux, le serveur Admin reçoit des informations concernant chaque ordinateur et les paramètres des règles activés pour le conteneur dans lequel se trouve cet ordinateur. Si le serveur Admin rencontre une configuration ayant été modifiée, il force la configuration des options correctes.

Les paramètres des règles sont prioritaires par rapport aux paramètres de l'ordinateur local. C'est-à-dire, si des règles sont appliquées à un conteneur, les paramètres de ces règles remplacent les paramètres que l'utilisateur a définis sur l'ordinateur local.

Verrouillage des paramètres sur un ordinateur

L'option Verrouillage des paramètres vous permet de contrôler les règles de manière à ce que l'utilisateur ne puisse pas modifier les paramètres de règles sur l'ordinateur sur lequel la règle est appliquée.

L'option Verrouillage des paramètres est décrite dans le tableau suivant.

Verrouillage des paramètres	Description
Cochée (Règles verrouillées)	Si l'option Verrouillage des paramètres est activée pour une instance de règle, la règle est appliquée au conteneur de l'ordinateur pendant le processus de découverte et les paramètres sont verrouillés sur l'ordinateur local. L'utilisateur n'est pas habilité à modifier les paramètres de cette règle.
Non cochée (Règles non verrouillées)	Si l'option Verrouillage des paramètres n'est pas activée pour une instance de règle, la règle est appliquée au conteneur de l'ordinateur mais l'utilisateur peut modifier les paramètres de cette règle sur l'ordinateur local. Si l'utilisateur modifie les paramètres, la prochaine fois que le processus de découverte met à jour les informations pour l'ordinateur, les paramètres sont automatiquement redémarrés pour reprendre les valeurs de l'instance de règle.

Définition des règles

Chaque catégorie de règle dispose des options pour les mêmes paramètres que les options disponibles pour l'utilisateur de la fenêtre Analyseur local.

Pour accéder à ces options, cliquez avec le bouton droit sur une catégorie et sélectionnez Nouveau pour afficher la boîte de dialogue Options des règles. Il existe un onglet de règles pour chaque type de catégorie ainsi qu'un onglet d'options disponible pour la catégorie.

Lorsque vous créez une instance de règle, vous utilisez les options d'onglets disponibles de la même manière qu'un utilisateur spécifie les options d'analyse. La différence est que les options que vous spécifiez dans l'affichage de l'administrateur peuvent s'appliquer à tous les ordinateurs dans les conteneurs de l'arborescence de l'organisation et que vous pouvez contrôler si l'utilisateur final peut modifier les options ou pas.

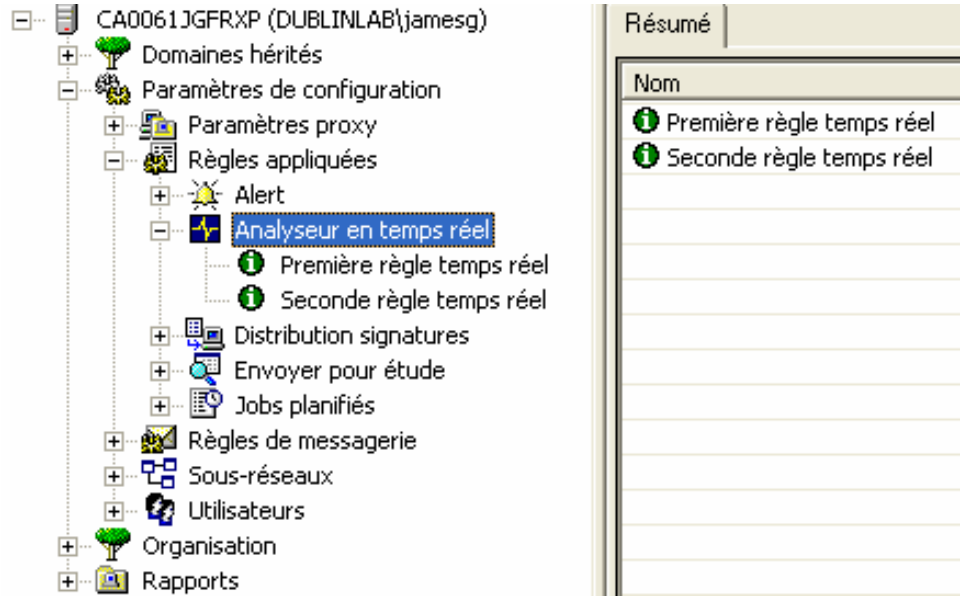
Une fois que vous avez spécifié les paramètres de règles, l'instance de la règle est répertoriée sous la catégorie, dans la fenêtre de gauche. Vous pouvez développer la catégorie pour afficher toutes les instances de la règle dans la liste. Lorsque vous sélectionnez l'instance de la règle dans la liste de gauche, différents onglets de résumé et d'informations indiquant les options activées pour cette règle s'affichent sur la droite. Vous avez également la possibilité d'éditer vos paramètres de règles.

Consultez l'aide en ligne ainsi que les autres chapitres de ce manuel pour obtenir de plus amples informations sur les options d'analyse. Veuillez vous reporter à la section « Utilisation d'Alert avec le logiciel antivirus » du chapitre « Utilisation du gestionnaire Alert » pour obtenir des informations sur les paramètres Alert.

Gestion des règles

Une fois que vous avez créé les paramètres des options de règles, vous pouvez appliquer les instances de règles à un conteneur de l'arborescence de l'organisation et utiliser les options du bouton droit de la souris pour gérer ces instances de règles. Vous pouvez appliquer des règles soit en utilisant la fonction Glisser-déplacer, soit en spécifiant une branche. Vous pouvez également accéder aux options de paramètres de règles en mettant une branche en surbrillance dans l'arborescence de l'organisation puis en sélectionnant une option dans la barre d'outils, le menu Administration, ou en utilisant les options du bouton droit de la souris (le « glisser-déplacer » n'est pas disponible dans OS X ni dans l'interface graphique du navigateur)..

La figure suivante donne un exemple de la catégorie Analyseur en temps réel sélectionnée avec deux instances de règles en temps réel disponibles.



Lorsque vous appliquez une instance de règle à une branche ou à un conteneur, la règle s'applique à tous les sous-conteneurs dans ce conteneur et à tous les ordinateurs dans le conteneur. Reportez-vous à la section « Priorité des règles » pour en savoir plus.

Remarque : Un conteneur est une branche de l'arborescence de l'organisation.

Options du bouton droit pour les règles

Les options du bouton droit sont disponibles lorsque vous sélectionnez une instance de règle. Lorsque vous cliquez avec le bouton droit de la souris sur une instance de règle et sélectionnez l'option Branche, vous pouvez alors affecter une instance de règle à une branche en utilisant l'option Affecter à la branche. Pour supprimer une règle de la branche, utilisez l'option Supprimer de la branche.

D'autres options vous permettent de créer une nouvelle règle, d'éditer une règle existante, de mettre à jour l'affichage et de supprimer une instance de règle.

En outre, lorsque vous sélectionnez un conteneur dans l'arborescence de l'organisation, vous pouvez gérer une instance de règle en cliquant sur un onglet de règle disponible dans la partie droite de la fenêtre puis en cliquant avec le bouton droit de la souris sur les paramètres affichés. Les options s'appliquent à l'instance de règle et au conteneur sélectionné.

Glisser-déplacer les règles vers les conteneurs

Si vous sélectionnez la catégorie de règles dans la liste de gauche, la liste des instances de règles s'affiche à droite. Vous pouvez, avec la fonction Glisser-déplacer, soit déplacer une instance de la liste située sur le côté droit de la fenêtre vers un conteneur de la liste située sur le côté gauche de la fenêtre, soit utiliser les options du bouton droit pour affecter l'instance de règle à une branche de l'arborescence de l'organisation.

L'interface utilisateur graphique du navigateur Web et d'OS X ne prennent pas en charge la fonctionnalité glisser-déplacer.

Reportez-vous à l'aide en ligne pour obtenir des informations détaillées sur les paramètres des options de règles et sur les procédures permettant de les gérer.

Priorité des règles

Vous pouvez appliquer des règles à tous les conteneurs dans l'arborescence de l'organisation. L'arborescence de l'organisation est constituée d'une liste hiérarchique de conteneurs ; chaque conteneur possède des conteneurs inférieurs. Une règle possède l'une des deux caractéristiques prioritaires suivantes :

- Hérité
- Spécifié

Un conteneur hérite des règles de celui dans lequel il se trouve. Ainsi les règles s'appliquant à un conteneur s'appliquent-elles également à tous les conteneurs qui s'y trouvent, et à tous les ordinateurs de ce conteneur. Cependant, lorsque vous appliquez une règle à un conteneur spécifique, celle-ci remplace la règle héritée. Ce type de règle est spécifié ou spécifique au conteneur sélectionné.

Remarque : Une règle spécifiée remplace une règle héritée.

Lorsque le serveur Admin effectue la découverte, il commence par analyser le niveau le plus bas du conteneur (un conteneur ne possédant pas d'autre conteneur) pour vérifier quelle règle lui est appliquée. Si une règle est associée au conteneur, elle est gardée et n'est pas modifiée par une règle appliquée à un conteneur supérieur. Le processus de découverte se poursuit alors le long de l'arborescence de l'organisation avec le prochain conteneur supérieur. Par exemple, si aucune règle n'est appliquée au prochain niveau de conteneur, le serveur Admin utilise la règle appliquée au conteneur ou à la branche au niveau du conteneur supérieur.

Affichage de l'application des règles

Pour afficher les instances de règles appliquées à un conteneur ou à une branche, mettez en surbrillance l'instance de règle et cliquez sur l'onglet Informations situé dans la partie droite de la fenêtre. Une liste, répertoriant tous les conteneurs et branches dans lesquels la règle sélectionnée est appliquée, s'affiche.

Si la règle s'applique au niveau de la branche, le nom de la branche est répertorié. Si la règle s'applique à une branche ou à un conteneur au sein de la branche, mais pas à la branche elle-même, le chemin de la branche et du conteneur est listé sous la forme *branche/conteneur*.

Utilisation de sous-réseaux

Utilisez la catégorie Sous-réseaux pour indiquer au serveur Admin quel(s) sous-réseau(x) vous souhaitez découvrir et gérer. Lorsque vous spécifiez un sous-réseau, le serveur Admin recherche toutes les instances du logiciel antivirus de Computer Associates exécutées dans ce sous-réseau et affiche les ordinateurs disponibles dans l'affichage de l'administrateur. Vous pouvez créer plusieurs instances de sous-réseaux.

Remarque : Les sous-réseaux peuvent être affichés dans les instances de sous-réseaux de l'affichage de l'administrateur par un administrateur de réseau possédant un accès valide à la catégorie Sous-réseaux et utilisant les options de découverte décrites ci-dessous. Une fois qu'une instance de sous-réseau est découverte, il n'est pas nécessaire de configurer à nouveau les options de sous-réseau étant donné que les informations sont remises à jour sur la base des options Répéter du processus de Découverte. Les utilisateurs autorisés de l'affichage de l'administrateur peuvent alors gérer les ordinateurs découverts et les placer dans les conteneurs de l'arborescence de l'organisation.

Options de sous-réseau

Les options de sous-réseau permettent de découvrir et de gérer un sous-réseau.

Définition des sous-réseaux

Pour définir les sous-réseaux souhaités, développez, dans la fenêtre de l'affichage de l'administrateur, la liste de gauche pour afficher les paramètres de configuration et cliquez avec le bouton droit de la souris sur la catégorie Sous-réseaux puis sélectionnez Nouveau. Dans la boîte de dialogue Sous-réseaux, indiquez le sous-réseau et le masque de sous-réseau appropriés. Un supplément d'information s'affiche.

Le libellé ou la description par défaut d'un sous-réseau est constitué de l'adresse IP suivie du numéro de port utilisé lors de la découverte. Vous pouvez utiliser l'option de bouton droit Editer pour modifier la description.

Remarque : Si vous utilisez l'affichage de l'administrateur de l'ordinateur sur lequel est situé le serveur Admin, le sous-réseau de ce dernier s'affiche automatiquement dans la catégorie de sous-réseaux.

Organisation par défaut pour la découverte de sous-réseaux

Lorsque le serveur Admin découvre des ordinateurs et trouve un serveur approuvé pour un ordinateur, l'ordinateur découvert est ajouté à la catégorie dans l'arborescence de l'organisation spécifiée dans l'option Organisation par défaut.

L'organisation par défaut correspond au nom d'un conteneur existant dans l'arborescence de l'organisation à laquelle un ordinateur découvert peut être affecté si un serveur approuvé est spécifié pour l'ordinateur au moment de l'installation. Si vous utilisez l'utilitaire d'installation à distance et le fichier de configuration INOC6.ICF pour installer le logiciel antivirus de Computer Associates, il vous est alors possible de spécifier un serveur approuvé pour l'ordinateur local.

En utilisant cette méthode, l'ordinateur découvert est placé dans le conteneur indiqué par l'option Organisation par défaut. Il n'est pas nécessaire de déplacer un ordinateur de la liste des ordinateurs du sous-réseau vers une catégorie de l'arborescence de l'organisation. Si aucun serveur approuvé n'est spécifié pour un ordinateur, ce dernier est disponible dans la liste des ordinateurs pour le sous-réseau mais doit être déplacé manuellement vers un conteneur.

Le bouton Modifier permet de changer le conteneur dans l'arborescence de l'organisation qui est spécifiée dans l'option Organisation par défaut.

Sur les systèmes UNIX et OS X, il n'existe pas d'utilitaire d'installation à distance. Vous pouvez utiliser le script InoSetApproved situé dans le répertoire $CAIGLBL0000/ino/scripts pour spécifier un serveur approuvé. Pour ce faire, indiquez l'adresse IP ou les adresses des serveurs approuvés comme arguments pour le script, comme par exemple InoSetApproved 123.123.123.123 234.234.234.234.

Sur les systèmes OS X, vous pouvez également approuver les serveurs Admin dans l'écran des préférences de eTrust Antivirus, disponible sous l'écran des préférences système.

Sous NetWare, vous pouvez définir un serveur Admin approuvé en utilisant ETRUSTAV. En outre, l'installation de NetWare utilise inoc6.icf qui peut être prédéfini pour utiliser un serveur Admin approuvé, comme sous Windows.

Informations de la découverte

Le champ Dernière découverte indique quand le sous-réseau a été découvert pour la dernière fois. Elle affiche quand les dernières informations relatives à l'état d'un ordinateur ont été fournies au serveur Admin. Ces informations indiquent également si l'ordinateur est toujours en service sur le réseau et quels paramètres de règles ont été appliqués au conteneur qui l'héberge. Si vous avez modifié la structure ou les paramètres de règles du conteneur depuis la dernière fois que le sous-réseau a été découvert, vous pouvez utiliser les options d'actualisation pour mettre à jour les informations qui sont listées dans l'affichage de l'administrateur.

Conflit d'adresse IP du serveur Admin

Si une adresse IP est affichée dans le champ Conflit d'adresse IP du serveur Admin, cela signifie qu'un autre serveur Admin a découvert le même sous-réseau que celui que vous avez spécifié. L'adresse IP affichée indique où réside le serveur Admin en conflit. Cette information est également consignée dans le journal d'événements. Veuillez contacter l'administrateur de ce sous-réseau pour éviter des conflits de paramètres de règles.

Il est préférable d'éviter que deux serveurs Admin gèrent le même sous-réseau. La découverte d'un même sous-réseau par deux serveurs différents entraîne des conflits de paramètres de règles. Si, par exemple, un serveur Admin découvre le sous-réseau, les informations apparaissant dans l'affichage de l'administrateur reflèteront l'organisation des conteneurs et les paramètres de règles appliqués sous ce serveur Admin. Si un autre serveur Admin découvre le même sous-réseau, il lui appliquera ses propres configurations et paramètres de règles. Ainsi, la prochaine fois que le premier serveur fait une découverte, il appliquera ses propres paramètres et ainsi de suite. Non seulement cela causera un trafic réseau inutile, mais cela empêchera également la création et la conservation de règles antivirus de réseau cohérentes.

Découverte de sous-réseaux

L'onglet Découverte de sous-réseaux permet de gérer le processus de découverte de sous-réseaux. Vous pouvez choisir de découvrir le sous-réseau tout de suite ou utiliser les options Répéter pour définir la fréquence de découverte à laquelle le serveur Admin mettra la liste des ordinateurs à jour.

L'onglet Découverte comprend les options de règles de découverte suivantes :

Option	Description
Numéro de port	Port utilisé par les ordinateurs sur lesquels le logiciel antivirus de Computer Associates est installé pour communiquer avec le serveur Admin. Il s'agit du port UDP (User Datagram Protocol) ouvert sur l'ordinateur client pour la découverte dirigée par le protocole IP à partir du serveur Admin. Le numéro de port utilisé pour le processus de découverte peut être configuré au moment de l'installation et doit posséder la même valeur dans l'ensemble de l'environnement. La valeur par défaut est le port UDP 42508. Sur les systèmes OS X, le numéro de port par défaut peut être défini dans l'écran des préférences de eTrust Antivirus, disponible sous l'écran des préférences système.
Maximum de découvertes non abouties	Permet de spécifier le nombre maximum de fois auquel un ordinateur n'est pas découvert avant d'être supprimé de la liste des ordinateurs découverts du sous-réseau et de l'arborescence de l'organisation. Ainsi, un ordinateur temporairement indisponible continue d'être affiché en tant que partie intégrante du réseau antivirus. Si, lors d'un processus de découverte d'un ordinateur, la requête reste toujours sans réponse après le nombre maximal spécifié de découvertes non abouties, l'ordinateur est alors supprimé de la liste des ordinateurs du sous-réseau et de l'arborescence de l'organisation. Si cette option est configurée sur zéro, l'ordinateur n'est jamais supprimé. Si un ordinateur est supprimé puis redécouvert, il sera de nouveau affiché à la place qu'il occupait auparavant dans l'arborescence de l'organisation.
Délai expiré après	Permet de définir en secondes un délai limite pour la découverte. Si la requête de découverte reste sans réponse du réseau dans le délai imparti, le processus de découverte s'arrête. Cette option s'applique au processus de découverte dans son ensemble et non au temps de réponse d'un ordinateur spécifique. Par exemple, si l'option est définie sur 180 secondes et que la recherche, dans le sous-réseau spécifié, d'une instance du logiciel antivirus de Computer Associates reste sans réponse, le processus de découverte s'arrête.

Options Répéter

Les options Répéter permettent de spécifier la fréquence de découverte du sous-réseau.

Options Méthode de sélection

Les options Méthode de sélection permettent de sélectionner différentes techniques de sélection pour la découverte. La méthode par défaut est Sélection libre. Le serveur Admin utilise la méthode de sélection choisie pour envoyer des messages de diffusion vers le sous-réseau spécifié dans l'onglet Sous-réseau. Le processus de découverte permet de trouver dans le sous-réseau spécifié les ordinateurs exécutant le logiciel antivirus de Computer Associates. Le processus de découverte est conçu pour être efficace et est optimisé pour réduire le trafic réseau.

Important ! *Les options Méthode de sélection sont conçues pour s'adapter aux différentes configurations de réseau. Le fonctionnement de chaque méthode dépend de la configuration réseau de votre environnement. Vous devez sélectionner une méthode qui soit adaptée à votre réseau et, si nécessaire, effectuer des modifications.*

Les méthodes de sélection suivantes sont disponibles :

Option	Description
Sélection libre	Sélection libre est la méthode de sélection par défaut. Avec cette méthode, vous ne devez pas nécessairement connaître la configuration des ordinateurs découverts dans le sous-réseau. Le serveur Admin envoie au sous-réseau un message dirigé par le protocole IP. De ce fait, une sélection s'effectue parmi les ordinateurs exécutant le logiciel antivirus de Computer Associates. L'ordinateur sélectionné répond au serveur Admin en lui faisant parvenir la liste des ordinateurs présents dans le sous-réseau. Si le serveur Admin n'est pas situé dans le sous-réseau en train d'être découvert, le message diffusé par le protocole IP peut être bloqué par un composant matériel du réseau. Si tel est le cas, vous devez reconfigurer le matériel réseau de manière à ouvrir le port de découverte. Cette fonction ne nécessite pas l'installation du logiciel antivirus de Computer Associates sur l'ordinateur spécifié dans l'option d'adresse IP de l'onglet Sous-réseau. Toutefois, si le logiciel antivirus est exécuté sur l'ordinateur spécifié, vous pouvez utiliser le bouton Test pour vérifier si les messages dirigés par le protocole IP sont bloqués.

Option	Description
Sélection variable	Utilisez la méthode Sélection variable si vous préférez obtenir une réponse d'un ordinateur spécifique qui n'est pas toujours disponible. La sélection variable utilise un message dirigé par le protocole IP pour tenter de découvrir cet ordinateur et pour en faire l'ordinateur sélectionné. Si cette adresse n'est pas disponible, la méthode Sélection libre est utilisée.
Sélection définie	La méthode Sélection définie permet d'effectuer des découvertes avec un ordinateur dont vous savez qu'il exécute le logiciel antivirus de Computer Associates. Indiquez l'ordinateur que vous souhaitez utiliser dans l'option d'adresse IP de l'onglet Sous-réseau. Avec cette méthode, l'option de diffusion par protocole IP de la sélection libre est supprimée et n'est pas utilisée. A la place, le serveur Admin communique directement avec l'ordinateur spécifié. Ce dernier répond au serveur Admin en lui faisant parvenir la liste des ordinateurs présents dans le sous-réseau. Cette option nécessite que le logiciel antivirus de Computer Associates soit exécuté sur l'ordinateur spécifié.

Option	Description
Sélection de la détection	La méthode Sélection de la détection permet d'effectuer la découverte en contactant chaque adresse IP individuelle du sous-réseau. Les ordinateurs spécifiques contactés sont déterminés par l'adresse IP et le masque spécifié dans l'onglet Sous-réseau. Cette méthode est conçue pour être utilisée lorsque aucune autre méthode ne convient. Ce peut être le cas, par exemple, lorsque des ordinateurs clients sont connectés au réseau par l'intermédiaire d'une connexion VPN ou PPP. En outre, la Sélection libre n'est pas possible si la diffusion dirigée par le protocole IP n'est pas autorisée vers le sous-réseau cible. Et la Sélection définie n'est pas possible si l'on ne peut pas être sûr que l'ordinateur spécifié fonctionne. De surcroît, la Sélection de la détection doit être utilisée pour découvrir les sous-réseaux sur un ordinateur sous Linux pour système 390 dans lesquels des ordinateurs Linux virtuels sont connectés au réseau par une connexion point à point au mainframe, plutôt que par une connexion Ethernet directe. Si l'une des autres méthodes de sélection convient pour un sous-réseau, il est préférable de ne pas utiliser la Sélection de la détection. La Sélection de la détection se traduira par un niveau plus élevé d'interrogations non abouties, et elle fait peser une charge plus importante sur le serveur Admin.

Remarque : L'ordinateur sélectionné pour répondre au serveur Admin apparaît en caractères gras dans la liste des ordinateurs du sous-réseau.

Découverte d'ordinateurs hors du sous-réseau local

Si vous lancez un processus de découverte et qu'il ne détecte pas les ordinateurs exécutant des instances du logiciel antivirus de Computer Associates, il est possible que vous ayez à modifier la configuration du routeur de réseau.

Lors du processus de découverte utilisant le paramètre par défaut Sélection libre, le serveur Admin envoie un message de diffusion dirigé par le protocole IP au sous-réseau découvert. Si les routeurs du réseau empêchent le passage de ces paquets, le processus de découverte échoue.

La procédure suivante vous permet de résoudre ce problème :

- Substituez la méthode Sélection définie à la méthode Sélection libre.
- Configurez les routeurs du réseau pour permettre l'acheminement de messages de diffusion dirigés par le protocole IP via un port UDP 42508.

Options du bouton droit du sous-réseau

Lorsque vous cliquez avec le bouton droit sur les catégories ou instances de sous-réseaux, vous pouvez créer une nouvelle instance de sous-réseau, éditer les options d'une instance existante, supprimer une instance, mettre à jour la découverte et actualiser l'affichage. Il vous est possible d'affecter un ordinateur à une branche en cliquant dessus avec le bouton droit de la souris dans la liste de sous-réseaux.

Informations sommaires du sous-réseau

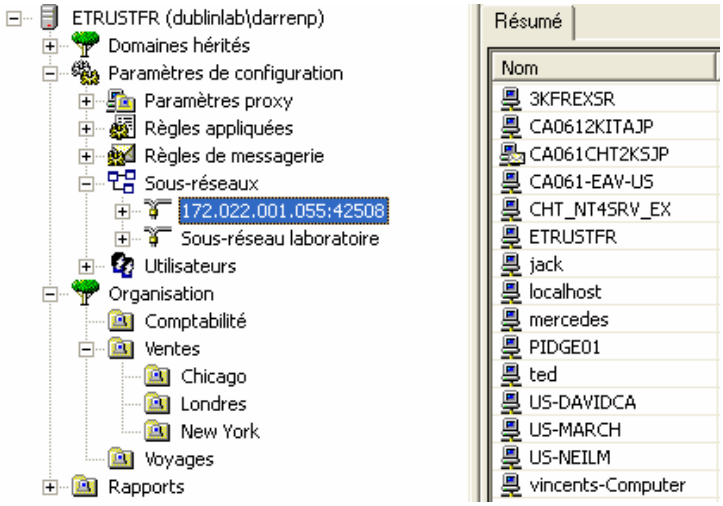
Lorsque la catégorie de sous-réseau, une instance de sous-réseau ou un ordinateur dans un sous-réseau est mis(e) en surbrillance, des informations résumées relatives à cet élément s'affichent dans le côté droit de la fenêtre Affichage de l'administrateur.

Ces informations portent également sur les versions du produit et des signatures exécutées sur les ordinateurs, du système d'exploitation et sur la date de la dernière découverte d'un ordinateur.

Affichage des ordinateurs découverts

Une fois les ordinateurs découverts, mettez en surbrillance l'instance du sous-réseau à gauche de la fenêtre Affichage de l'administrateur pour afficher à droite la liste des ordinateurs découverts.

La figure suivante représente une instance de sous-réseau sélectionnée avec les ordinateurs découverts.



Reportez-vous à la section « Création de configurations d'ordinateurs logiques » pour en savoir plus sur la manière d'associer un ordinateur à un conteneur.

Contrôle de l'accès aux options de sous-réseau

L'administrateur autorisé du logiciel antivirus peut garantir l'accès aux sous-réseaux et leurs options en définissant des droits d'accès dans la catégorie Utilisateurs. Les utilisateurs autorisés peuvent modifier la fréquence des découvertes ainsi que d'autres options. Reportez-vous à la section « Utilisation des droits d'accès » pour plus d'informations sur la configuration des droits d'utilisateurs.

Le processus de découverte est indépendant des paramètres de règles. De même, vous n'avez pas besoin de droit d'accès spécial pour découvrir des ordinateurs. Un utilisateur n'a pas besoin de disposer d'un compte de système d'exploitation sur les ordinateurs découverts et affichés. Toutefois, pour placer un ordinateur découvert dans un conteneur de l'arborescence de l'organisation, vous devez bénéficier des droits d'accès administrateur pour le système d'exploitation de l'ordinateur que vous souhaitez placer dans le conteneur.

Une fois qu'un ordinateur est placé dans un conteneur, les administrateurs autorisés peuvent le déplacer vers un autre conteneur sans nécessiter de droit d'administrateur pour l'ordinateur. Les droits d'accès accordés aux utilisateurs permettent de contrôler la possibilité de déplacer un ordinateur.

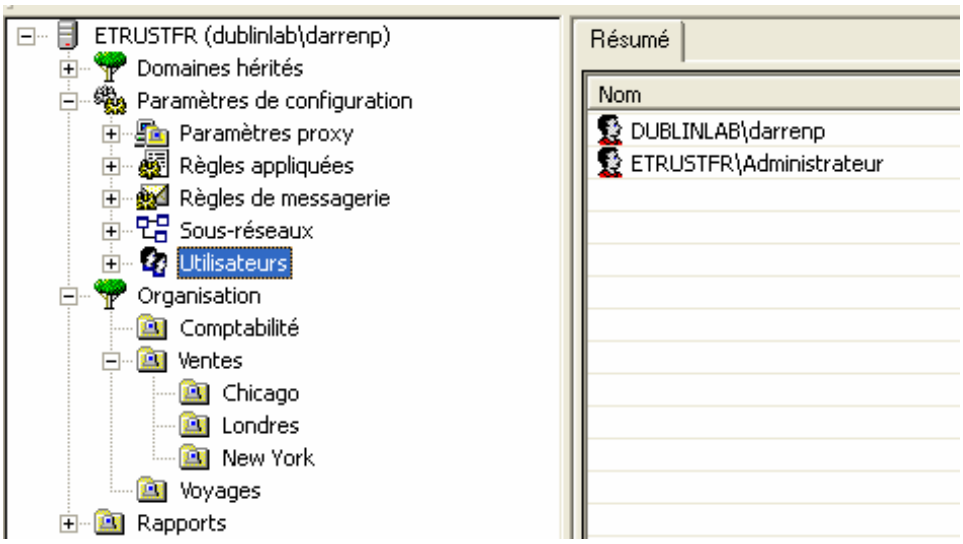
La fréquence de découverte peut être définie afin de mettre à jour périodiquement et sur une base régulière les informations relatives aux ordinateurs découverts. Une fois ces options configurées, elles ne devront pas être modifiées par la plupart des utilisateurs de l'affichage de l'administrateur.

A propos de la catégorie Utilisateurs

La catégorie Utilisateurs dans l'affichage de l'administrateur contient une liste des utilisateurs auxquels le droit d'accès aux conteneurs dans l'arborescence de l'organisation a été accordé. Utilisez cette catégorie pour définir les droits d'accès des utilisateurs et pour afficher clairement le type d'accès dont bénéficie chaque utilisateur. Lorsque vous sélectionnez la catégorie Utilisateurs, la liste de ces derniers est affichée sur la droite.

Sélection de la catégorie Utilisateurs

La figure suivante montre la catégorie Utilisateurs sélectionnée avec, à droite, un exemple de liste d'utilisateurs.



Remarque : Seuls les utilisateurs possédant des droits d'accès sont affichés dans cette liste. Sous Windows, le compte administrateur du système d'exploitation et le compte utilisé pour installer le serveur Admin sont affichés automatiquement. Sur les systèmes UNIX et OS X, l'utilisateur root est affiché automatiquement.

Sélection d'un utilisateur

Lorsque vous développez la catégorie Utilisateurs et sélectionnez un utilisateur dans la liste de gauche, des informations sommaires concernant cet utilisateur s'affichent à droite de l'écran. Les droits d'accès et autorisations permettant à l'utilisateur de modifier les configurations du logiciel antivirus de Computer Associates sont affichés.

Remarque : Vous pouvez également afficher des informations relatives à l'utilisateur en mettant en surbrillance soit la catégorie Arborescence de l'organisation, soit un conteneur s'y trouvant et en cliquant sur l'onglet Droits situé à droite de la fenêtre. Ce faisant, vous affichez une liste des utilisateurs ainsi que les paramètres pour les droits des utilisateurs.

Reportez-vous à la section « Utilisation des droits d'accès » pour plus d'informations sur la configuration des droits d'utilisateurs.

Gestion de domaines hérités

La catégorie Domaines hérités vous permet de gérer les noms de domaines existants créés pour votre réseau antivirus dans des versions 4.x du logiciel antivirus de Computer Associates.

Remarque : Sous UNIX et OS X, si un domaine hérité existe, il s'affiche au même niveau dans le volet de gauche de l'arborescence de l'organisation. La gestion des domaines hérités n'est toutefois pas prise en charge par l'interface graphique utilisateur du navigateur Web ou par le serveur Admin basé UNIX.

Le serveur Admin affiche la catégorie Domaines hérités avec la liste des noms de domaines existants et des ordinateurs exécutant des instances de versions 4.x du produit. Vous avez la possibilité de gérer ces ordinateurs en utilisant les anciens noms de domaines tout en tenant compte du fait que seules les options de la version de produit précédemment installée sont disponibles. Les différents ordinateurs qui n'ont pas été définis dans un domaine sont répertoriés dans la catégorie Serveur unique. Pour gérer des options sur un ordinateur, vous avez besoin d'un ID utilisateur et d'un mot de passe valides pour cet ordinateur.

Gestion des ordinateurs avec l'arborescence de l'organisation

La catégorie Arborescence de l'organisation permet de créer dans votre réseau un affichage organisé de l'arborescence des conteneurs d'ordinateurs qui exécutent des instances du logiciel antivirus de Computer Associates. Ensuite, vous pouvez appliquer les paramètres de règles aux conteneurs.

Utilisation de l'arborescence de l'organisation

Une fois que le serveur Admin a affiché la liste des ordinateurs disponibles dans la catégorie Sous-réseaux, un administrateur autorisé peut utiliser l'arborescence de l'organisation pour créer une configuration logique des ordinateurs dans le réseau. Vous pouvez créer une hiérarchie très souple et adaptée à votre environnement. Chaque conteneur ou branche dans la liste possède une structure identique à la liste des répertoires ou dossiers possédant des sous-répertoires ou sous-dossiers contenant eux-mêmes des ordinateurs.

Vous pouvez créer n'importe quelles catégories logiques de conteneurs nécessaires à votre organisation. Par exemple, vous pouvez soit définir une configuration qui reflète les emplacements physiques des ordinateurs, soit classer les ordinateurs en de nombreuses catégories, par département, fonction, type d'utilisateur ou autres catégories nécessaires. Un ordinateur peut être membre d'un seul conteneur à la fois.

Accès à l'arborescence de l'organisation et aux conteneurs

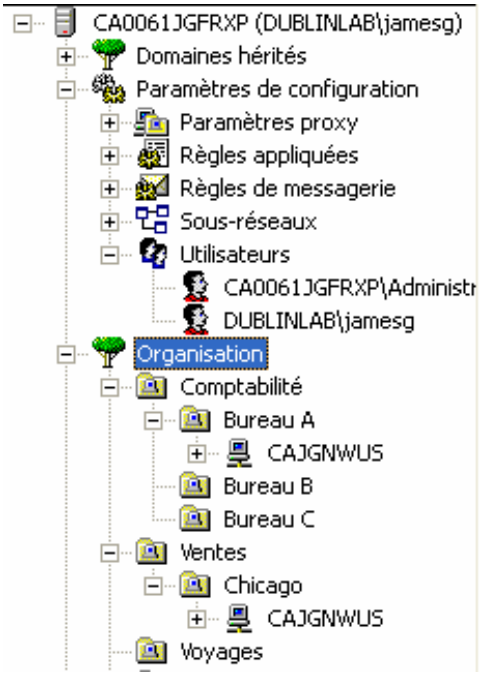
Vous pouvez contrôler l'accès aux conteneurs dans l'arborescence de l'organisation pour d'autres utilisateurs autorisés en affectant des droits d'accès.

Si vous possédez des droits d'accès pour un contrôle absolu mais pas de compte d'utilisateur pour les ordinateurs dans la branche, vous gardez le contrôle des paramètres de règles du logiciel antivirus de ces ordinateurs même si vous n'y possédez aucun compte de système d'exploitation. Toutefois, si vous supprimez un ordinateur de la branche et souhaitez le replacer dans un conteneur, vous avez besoin d'un compte de système d'exploitation avec des droits d'administrateur sur cet ordinateur. Reportez-vous à la section « Utilisation des droits d'accès » pour plus d'informations sur la configuration des droits d'utilisateurs.

Exemple d'arborescence de l'organisation

Comme exemple d'arborescence de l'organisation, nous pouvons créer une branche ou un conteneur appelé Comptabilité. Sous ce conteneur, vous pouvez créer des conteneurs pour chaque bureau ayant un service de comptabilité tel que Bureau A, Bureau B et ainsi de suite. Sous chaque bureau vous pouvez alors placer les ordinateurs de chacun de ces services de comptabilité.

La figure suivante est un exemple d'arborescence de l'organisation développée avec conteneurs et ordinateurs.



Remarque : Ces conteneurs correspondent au concept de domaine utilisé dans les versions 4.x du logiciel antivirus de Computer Associates.

Création de configurations d'ordinateurs logiques

Avant de pouvoir gérer un ordinateur, vous devez le placer dans une catégorie logique, c'est-à-dire dans un conteneur de l'arborescence de l'organisation. Pour ce faire, sélectionnez un ordinateur dans la liste des ordinateurs de l'instance de sous-réseau et associez-le à un conteneur.

Remarque : Vous devez posséder des droits d'administrateur pour le système d'exploitation de l'ordinateur que vous souhaitez placer dans un conteneur dans l'arborescence de l'organisation.

Pour créer un conteneur pour la première fois, cliquez avec le bouton droit de la souris sur la catégorie Arborescence de l'organisation. Vous pouvez alors ajouter autant de conteneurs et sous-conteneurs que nécessaires. Les conteneurs dans la liste constituent en quelque sorte une liste de répertoires ou de dossiers. Vous pouvez créer le nombre de conteneurs et sous-conteneurs que vous souhaitez, dans la hiérarchie, et organiser comme bon vous semble les ordinateurs dans les conteneurs.

Glisser-déplacer les ordinateurs vers les conteneurs

Pour associer un ordinateur à un conteneur, mettez en surbrillance l'instance du sous-réseau dans la partie gauche de la fenêtre Affichage de l'administrateur, sélectionnez un ordinateur dans la partie droite de la fenêtre et, à l'aide de la fonction Glisser-déplacer, placez-le dans le conteneur dans l'arborescence de l'organisation située dans la partie gauche de la fenêtre. Il vous est également possible de cliquer avec le bouton droit de la souris sur un ordinateur dans la partie gauche de la fenêtre et de l'affecter à une branche.

L'interface utilisateur graphique du navigateur Web et d'OS X ne prennent pas en charge la fonctionnalité glisser-déplacer.

Octroi de droits d'administrateur à l'installation

Si vous souhaitez gérer des ordinateurs dans un grand réseau, vous devrez, dans certains cas, octroyer des droits d'administrateur pour de nombreux ordinateurs à l'administrateur du serveur Admin. Il est possible d'accorder l'accès à un ordinateur client à un administrateur de serveur Admin si l'adresse IP du serveur Admin est spécifiée via le fichier de configuration INOC6.ICF sur l'ordinateur client lors de l'installation. Une relation de confiance est ainsi créée, permettant à l'administrateur de placer des ordinateurs dans des conteneurs sans avoir besoin, pour chaque ordinateur, d'informations relatives à la connexion et au mot de passe. Pour de plus amples informations, reportez-vous au chapitre « Utilisation de l'utilitaire d'installation à distance » et référez-vous au fichier exemple INOC6.ICF fourni avec le produit.

Sur les systèmes UNIX et OS X, vous pouvez utiliser le script InoSetApproved situé dans le répertoire $CAIGLBL0000/ino/scripts pour spécifier un serveur approuvé quand le logiciel antivirus a été installé. Pour ce faire, indiquez l'adresse IP ou les adresses des serveurs approuvés comme arguments pour le script, comme par exemple InoSetApproved 123.123.123.123 234.234.234.234.

Sur les systèmes OS X, vous pouvez également approuver les serveurs Admin dans l'écran des préférences de eTrust Antivirus, disponible sous l'écran des préférences système.

Sous NetWare, vous pouvez définir un serveur Admin approuvé en utilisant ETRUSTAV. En outre, l'installation de NetWare utilise inoc6.icf qui peut être prédéfini pour utiliser un serveur Admin approuvé, comme sous Windows.

Méthode de sécurité pour accéder à des ordinateurs Windows 9x

Une fois des ordinateurs Windows 9x découverts, une méthode de sécurité est fournie pour y accéder lorsque vous souhaitez les ajouter à des conteneurs dans l'arborescence de l'organisation. Utilisez simplement cette méthode pour affecter l'ordinateur à une branche de l'arborescence. Ensuite, le niveau de sécurité dépend des droits définis pour la branche.

Concernant les ordinateurs Windows 9x, le logiciel antivirus de Computer Associates n'est pas en mesure de contrôler les comptes d'utilisateur gérés par le système d'exploitation. C'est pourquoi un fichier d'authentification, Ino.sam, est stocké sur l'ordinateur Windows 9x. Ce fichier contient une liste de couples de hachage Nom d'utilisateur/mot de passe. Lors d'une authentification sur un ordinateur Windows 9x, l'utilisateur saisit son mot de passe et une valeur de hachage unidirectionnelle est générée. Si la valeur de hachage générée correspond à celle du fichier d'authentification, l'accès est alors accordé. Un programme utilitaire appelé InoPW.exe est fourni pour créer et gérer les fichiers d'authentification. Après avoir été modifié, le fichier d'authentification peut être copié manuellement dans le répertoire d'installation de l'antivirus sur des ordinateurs Windows 9x ou déplacé vers un répertoire contenant une copie de l'image d'installation. S'il est déplacé vers le répertoire image, le programme d'installation copie automatiquement le fichier sur les ordinateurs Windows 9x.

Gestion des ordinateurs et des conteneurs

Remarque : Les termes de conteneur et branche sont utilisés comme synonymes.

Lorsque, dans votre réseau, vous avez des ordinateurs rangés logiquement dans l'arborescence de l'organisation, vous pouvez les gérer et surveiller les paramètres de règles de configuration de manière efficace. Dans une hiérarchie de conteneurs, vous pouvez appliquer facilement des paramètres de règles à d'importants groupes d'ordinateurs.

Lorsque vous avez des conteneurs avec des ordinateurs, vous pouvez cliquer dessus avec le bouton droit de la souris pour accéder aux options de gestion supplémentaires telles que la création d'ordinateurs de serveur proxy.

D'autres options vous permettent de rechercher un ordinateur dans un conteneur, de créer de nouveaux conteneurs, de les renommer et de les supprimer. Vous pouvez également définir des règles pour un conteneur sélectionné, affecter un conteneur à une branche ou le supprimer et actualiser l'affichage.

Couper-coller des conteneurs

Vous pouvez utiliser la fonctionnalité Couper-coller pour déplacer un conteneur d'une branche vers une autre. Les ordinateurs et règles associés au conteneur sont également déplacés. Vous pouvez cliquer avec le bouton droit de la souris pour sélectionner et couper un conteneur dans la partie droite de la fenêtre, puis mettre en surbrillance un conteneur sur la gauche à l'emplacement où vous souhaitez le coller.

Options du bouton droit pour les ordinateurs

Les options du bouton droit sont disponibles lorsque vous sélectionnez un ordinateur dans un conteneur. Elles vous permettent d'affecter l'ordinateur à une branche, de le supprimer de la branche et de gérer les services du logiciel antivirus de Computer Associates sur l'ordinateur sélectionné.

Configuration point à point

Il existe également des options de bouton droit qui vous permettent de configurer des paramètres d'analyse sur un ordinateur sélectionné. Toutefois, l'utilisation de ces options de bouton droit ne vous permet pas de créer des paramètres de règles.

Lorsque vous mettez en surbrillance un ordinateur et accédez à ces paramètres de configuration, ces options de bouton droit s'appliquent uniquement à l'ordinateur sélectionné. Cela vous permet de gérer les paramètres de l'ordinateur sur une base point à point en définissant les options disponibles pour un utilisateur à partir de la fenêtre Analyseur local.

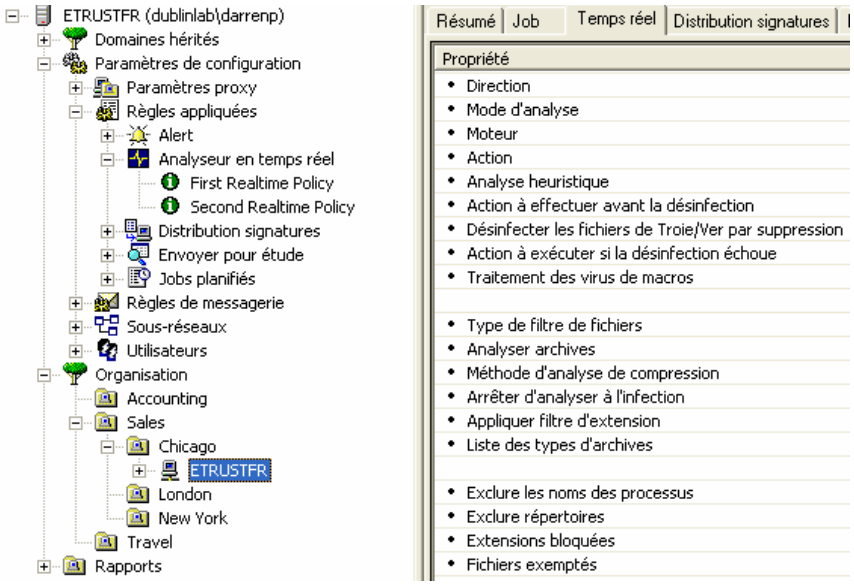
Consultez l'aide en ligne pour obtenir de plus amples informations sur la gestion des ordinateurs et conteneurs.

Affichage d'une règle sur un ordinateur ou conteneur

Remarque : Les termes de conteneur et branche sont utilisés comme synonymes.

Une fois que des instances de règles ont été appliquées à un conteneur ou à un ordinateur, vous pouvez sélectionner l'élément dans l'arborescence de l'organisation et afficher les paramètres de règles. Pour chaque type de paramètre de règles appliqué à l'élément, il vous est possible de cliquer sur un onglet dans la zone droite de la fenêtre pour afficher des informations détaillées sur les paramètres de règles.

La figure suivante montre un exemple d'ordinateur sélectionné dans un conteneur avec les onglets indiquant les paramètres de règles appliqués à l'ordinateur. Dans cet exemple, où l'onglet Temps réel est sélectionné, les informations sur les paramètres de règles temps réel qui sont appliqués au conteneur listant l'ordinateur sélectionné sont affichées.



Affichage des journaux sur les ordinateurs distants

Vous pouvez afficher les informations du journal relatives aux ordinateurs distants en développant une entrée d'un ordinateur. Les types de journaux sont répertoriés sous chaque ordinateur. Sélectionnez sur la gauche un type de journal pour afficher sur la droite un récapitulatif du journal pour cet ordinateur. Pour de plus amples informations, cliquez sur l'élément journal dans le coin supérieur droit de la fenêtre pour afficher les informations détaillées dans le volet inférieur droit.

Affichage des journaux par ordinateur

La figure suivante montre un exemple d'un conteneur et d'un ordinateur développé dans l'arborescence de l'organisation ainsi que les catégories de journaux pour cet ordinateur.

Vous pouvez afficher les informations du journal pour les jobs et événements exécutés localement et à distance.

Affichage des journaux des règles de jobs planifiés

Les administrateurs peuvent également afficher les statistiques du journal des résultats pour les jobs planifiés gérés par une série de règles. Les informations du journal s'affichent lorsque vous sélectionnez une instance de règle de job planifié et cliquez sur l'onglet journal situé dans la partie droite de la fenêtre. Il existe une entrée de journal pour l'heure d'exécution de chaque lancement de job, avec des statistiques sommaires sur le nombre d'ordinateurs sur lesquels le job a été exécuté ainsi que des statistiques de succès et d'échecs. Des informations détaillées sont également disponibles pour chaque ordinateur sur lequel le job a été exécuté. Les statistiques sur les analyses effectuées sur chaque ordinateur contiennent le nombre total de fichiers analysés, de fichiers infectés et de fichiers désinfectés.

Gestion des jobs planifiés avec un ordinateur sélectionné

Lorsque vous mettez en surbrillance un ordinateur dans l'arborescence de l'organisation puis cliquez sur l'onglet Job dans la partie droite de la fenêtre, il vous est alors possible de gérer les jobs planifiés qui sont répertoriés pour cet ordinateur. Vous pouvez gérer des jobs exécutés localement ainsi que des jobs planifiés à distance pour l'ordinateur sélectionné. Il vous est possible de modifier les propriétés d'un job, de l'interrompre et de le supprimer en le sélectionnant dans l'onglet Job et en cliquant dessus avec le bouton droit de la souris.

Utilisation des droits d'accès

Les droits d'accès permettent de spécifier les utilisateurs de l'Affichage de l'administrateur autorisés à contrôler les paramètres de règles du logiciel antivirus de Computer Associates exécuté sur des ordinateurs dans l'arborescence de l'organisation et à gérer les options de sous-réseaux. Cette section traite des différentes méthodes permettant d'utiliser les fonctionnalités de sécurité pour contrôler l'accès au serveur Admin et les fonctions de paramètres de règles pour habiliter les utilisateurs autorisés à gérer à distance des ordinateurs du réseau antivirus.

Les droits d'accès s'appliquent aux éléments suivants :

- Sous-réseaux
- Conteneurs

Les droits d'accès octroyés à un utilisateur s'appliquent à la catégorie Sous-réseaux et à l'arborescence de l'organisation.

Considérations concernant l'accès au serveur Admin

En utilisant des comptes d'utilisateurs sur l'ordinateur contenant le serveur Admin et des comptes disponibles sur le réseau, les administrateurs et utilisateurs peuvent bénéficier du droit d'accès au serveur Admin ainsi qu'à l'Affichage de l'administrateur.

Remarque : Ces droits d'accès s'appliquent au logiciel antivirus de Computer Associates et non à la gestion du système d'exploitation de l'ordinateur sur lequel réside le serveur Admin.

Les comptes avec des accès au serveur Admin sont considérés comme faisant partie des catégories de base décrites ci-dessous.

- Administrateur de système d'exploitation ou compte racine de l'ordinateur hébergeant le serveur Admin.
- Compte utilisé pour installer le serveur Admin (utilisateur root sur les systèmes UNIX, utilisateur dote de droits d'administrateur sur OS X)
- Comptes administrateur autorisé

Ces fonctionnalités de sécurité vous permettent de disposer du contrôle nécessaire pour gérer comme souhaité le logiciel antivirus dans votre réseau ; elles vous permettent également d'utiliser un compte invité générique sans pour autant compromettre la sécurité du système d'exploitation. Les droits d'accès aux comptes administrateur autorisés pour le logiciel antivirus ne dépendent pas du droit octroyé au compte par le système d'exploitation. Il est possible d'accéder à l'Affichage de l'administrateur pour gérer le logiciel antivirus à partir de n'importe quel compte valide désigné grâce aux droits dont il dispose. Ces comptes administrateur autorisés peuvent pour leur part octroyer des droits à d'autres comptes.

L'administrateur autorisé décide de ce qu'un utilisateur peut faire dans l'affichage de l'administrateur en définissant les droits d'accès qui sont appliqués aux sous-réseaux et aux conteneurs dans l'arborescence de l'organisation. Ces droits d'accès sont stockés dans une table de sécurité à laquelle le serveur Admin se réfère pour contrôler les droits d'accès et les compétences des utilisateurs en matière de paramètres de règles. Ainsi, lorsqu'un utilisateur se connecte au serveur Admin, celui-ci connaît le nom de l'utilisateur, ses droits d'accès et les actions qu'il a le droit d'effectuer.

Grâce à la table de sécurité du produit, le système reconnaît qu'un utilisateur est autorisé à se connecter au serveur Admin lorsque :

- L'utilisateur est connu de l'ordinateur hébergeant le serveur Admin étant donné que l'utilisateur possède un compte de système d'exploitation valide sur cet ordinateur.
- Les informations sont collectées et transmises au serveur lorsque le processus de découverte met périodiquement à jour les informations relatives aux ordinateurs dans les sous-réseaux qui exécutent les instances du logiciel antivirus de Computer Associates.

Compte administrateur du système d'exploitation

Le compte administrateur du système d'exploitation ou compte racine sur l'ordinateur hébergeant le serveur Admin dispose automatiquement du contrôle absolu des catégories racine des sous-réseaux et de l'arborescence de l'organisation. Ce compte possède ainsi à la fois le contrôle administratif de l'ordinateur du serveur Admin et des fonctionnalités disponibles dans l'affichage de l'administrateur. Pour Windows, il s'agit du compte administrateur. Pour les systèmes UNIX et OS X, il s'agit d'un compte administrateur avec des privilèges racine. Ce compte administrateur sur le serveur Admin peut, pour sa part, affecter un utilisateur possédant un compte valide sur le serveur Admin à un compte administrateur autorisé.

Compte d'installation du serveur Admin

Le compte utilisé pour installer le serveur Admin contrôle automatiquement et totalement les catégories racine des sous-réseaux et de l'arborescence de l'organisation. Il s'apparente donc au compte administrateur du système d'exploitation. Etant donné que ce compte confère des droits pour installer un logiciel, il confère également des droits d'administrateur du système d'exploitation.

Si le compte utilisé pour installer le serveur Admin est différent du compte administrateur du système d'exploitation, ce compte apparaîtra également dans la liste des comptes d'utilisateurs lorsque vous afficherez les droits d'accès. Si vous utilisez le compte administrateur du système d'exploitation pour installer le serveur Admin, aucun compte d'installation supplémentaire ne sera créé.

Remarque : Les systèmes UNIX n'utilisent pas de compte séparé pour installer le logiciel antivirus. C'est l'utilisateur root qui installe le produit.

Accès administrateur autorisé

Le compte administrateur peut accorder des droits d'accès à des comptes du réseau ou à des comptes ayant des comptes de système d'exploitation valides sur l'ordinateur où le serveur Admin se trouve. Ces comptes peuvent être qualifiés d'administrateurs autorisés pour le réseau antivirus.

La connexion au serveur Admin implique que l'utilisateur dispose d'un compte valide sur l'ordinateur qui héberge le serveur Admin. Pour qu'un utilisateur soit en mesure de gérer les règles sur les ordinateurs situés dans les conteneurs de l'arborescence de l'organisation, un administrateur autorisé doit définir les droits d'accès pour le compte concerné.

Le compte que vous utilisez pour vous connecter au serveur Admin peut être n'importe quel compte valide de cet ordinateur ou du réseau. Dans le cas d'un utilisateur autorisé souhaitant gérer et appliquer les paramètres des règles dans l'affichage de l'administrateur, aucun droit administrateur n'est requis pour l'ordinateur qui héberge le serveur Admin. Les droits d'accès que l'administrateur attribue à un compte utilisateur détermine les capacités de l'utilisateur à modifier les paramètres des règles. Toutefois, si vous souhaitez ajouter un ordinateur à un conteneur de la liste d'ordinateurs dans l'instance de sous-réseau, vous devez bénéficier de droits d'accès administrateur pour l'ordinateur que vous souhaitez ajouter.

Sur le système d'exploitation hébergeant le serveur Admin, ces comptes sont dépourvus de tout droit spécial. En vue de la gestion des paramètres des règles dans le logiciel antivirus, les administrateurs autorisés peuvent se voir attribuer des droits d'accès de différents niveaux, allant de droits d'accès illimités à toutes les fonctionnalités de l'affichage de l'administrateur en passant par la lecture seule, selon les besoins de l'entreprise. Un administrateur autorisé est relativement libre de choisir à qui attribuer ces droits d'accès.

Lorsqu'un utilisateur se connecte à l'ordinateur hébergeant le serveur Admin, le système vérifie d'abord que l'utilisateur a un compte valide sur cet ordinateur. Si son compte est valide, l'utilisateur peut alors accéder aux fonctions de l'affichage de l'administrateur selon les droits d'accès qui ont été définis pour cet utilisateur par l'administrateur autorisé.

Création d'un compte utilisateur

Vous pouvez créer un compte sur le serveur Admin pouvant agir comme un compte invité pour permettre à d'autres utilisateurs de se connecter au serveur Admin et d'utiliser l'affichage de l'administrateur. Pour que les utilisateurs de votre choix bénéficient d'un accès illimité à l'affichage de l'administrateur, vous pouvez leur accorder un contrôle absolu. Cependant, ce compte ne doit pas dépendre d'un compte ayant des droits d'administrateur sur le système d'exploitation qui héberge le serveur Admin.

Sur Windows NT ou Windows 2000, par exemple, vous pouvez utiliser le compte invité sur l'ordinateur hébergeant le serveur Admin afin de créer un compte à l'intention des utilisateurs autorisés pour qu'ils puissent se connecter au serveur Admin. Vous pouvez copier le compte invité vers un nouveau compte en lui donnant le nom suivant : *InoAdmin*. Utilisez ensuite les options de droits d'accès de l'affichage de l'administrateur pour accorder un contrôle absolu à ce nouveau compte. Quand les utilisateurs se connectent au serveur Admin via ce compte, ils bénéficient alors d'un contrôle absolu sur l'affichage de l'administrateur et sur ses fonctionnalités ; toutefois, ils ne peuvent accéder au système d'exploitation que de façon limitée.

Remarque : Quel que soit le modèle de compte utilisé pour créer un compte invité, les droits d'accès au système d'exploitation acquis sont conservés.

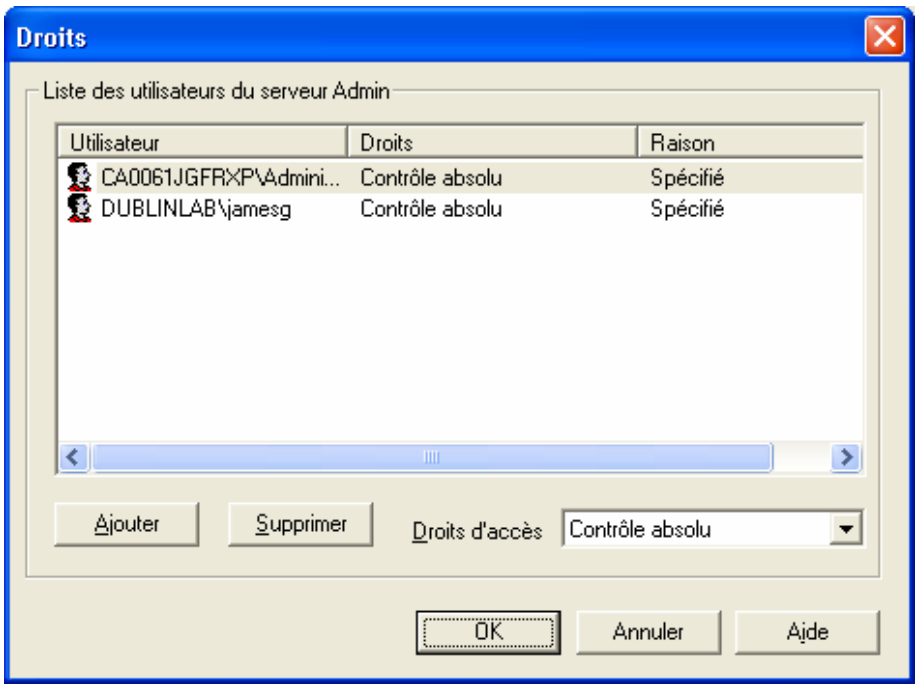
Cette méthode d'utilisation d'un compte invité permet de fournir un accès à l'affichage de l'administrateur sans qu'il soit nécessaire de créer un compte séparé pour chaque administrateur distant souhaitant accéder au serveur Admin. Vous pouvez même créer différents types de comptes génériques avec différents niveaux d'accès et une disponibilité adaptée aux besoins des administrateurs.

Configuration des droits d'accès

Les droits d'accès à un compte déterminent la capacité de l'utilisateur à accéder à l'arborescence de l'organisation ainsi qu'à apporter des modifications aux règles et aux options de sous-réseau.

Avec le bouton droit de la souris, cliquez sur la catégorie Utilisateurs puis sélectionnez Droits d'accès pour afficher la boîte de dialogue Droits. La boîte de dialogue Droits affiche la liste des utilisateurs existants.

L'illustration ci-dessous représente la boîte de dialogue Droits avec le compte administrateur de l'ordinateur hébergeant le serveur Admin.



Le compte administrateur qui apparaît dans l'illustration bénéficie de droits d'accès illimités. Reportez-vous à l'aide en ligne pour une description de la procédure permettant de créer des comptes avec un accès illimité à l'affichage de l'administrateur.

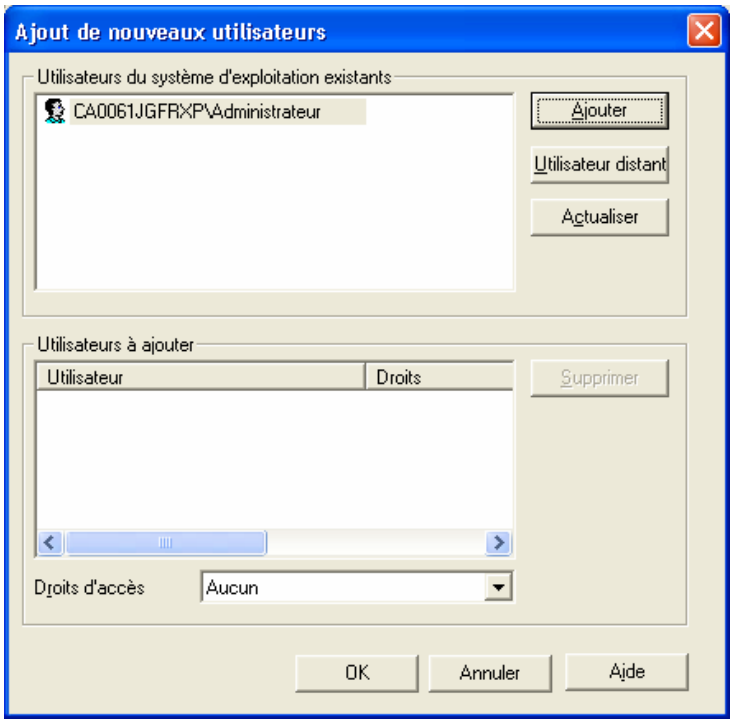
Remarque : Les droits d'accès s'appliquent au compte utilisateur. Ainsi, l'utilisateur est autorisé à accéder aux conteneurs de l'arborescence de l'organisation et aux options de sous-réseau.

Application des droits

La boîte de dialogue Droits permet d'ajouter des utilisateurs et de les supprimer, ainsi que de spécifier les droits d'accès de l'utilisateur sélectionné de l'affichage de l'administrateur. Vous pouvez également sélectionner un utilisateur existant et changer ses droits d'accès.

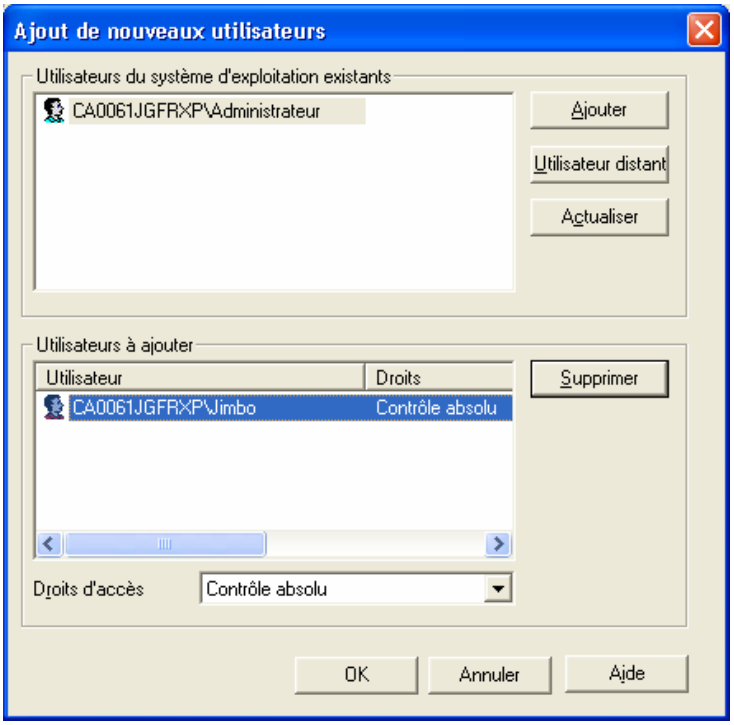
Pour ajouter un nouvel utilisateur à la liste des utilisateurs, cliquez sur le bouton Ajouter puis sélectionnez un utilisateur à partir de la boîte de dialogue Ajouter de nouveaux utilisateurs. Cette boîte de dialogue renferme une liste des comptes d'utilisateurs situés sur le système d'exploitation de l'ordinateur hébergeant le serveur Admin. En outre, vous pouvez ajouter des utilisateurs depuis le réseau en cliquant sur le bouton Simple ajout et en spécifiant l'utilisateur.

L'illustration suivante représente la boîte de dialogue Ajouter de nouveaux utilisateurs.



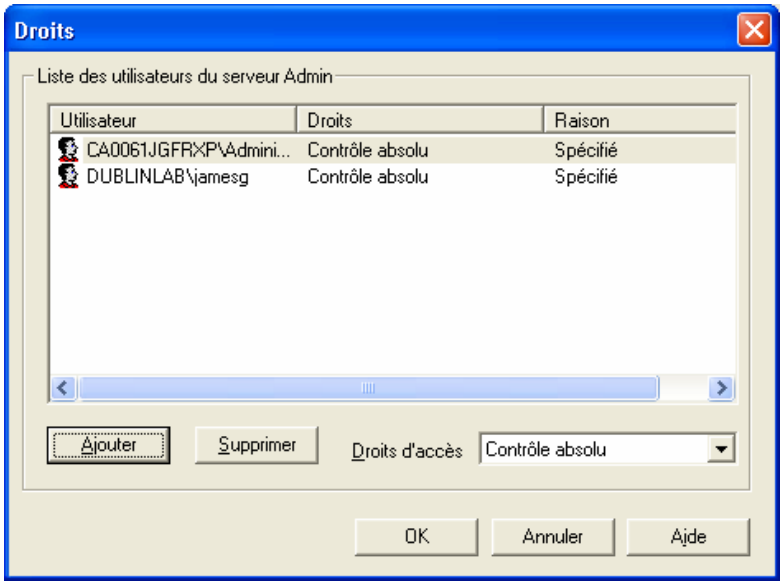
Dans la liste qui apparaît dans la partie supérieure de la fenêtre, vous pouvez sélectionner un utilisateur et cliquer sur Ajouter pour l'ajouter à la liste qui apparaît dans la partie inférieure de la boîte de dialogue. Lorsque l'utilisateur s'affiche dans la partie inférieure de la boîte de dialogue, mettez-le en surbrillance et attribuez-lui des droits d'accès à partir de la liste déroulante. Répétez cette procédure pour chaque utilisateur que vous souhaitez ajouter.

L'illustration suivante représente la boîte de dialogue qui apparaît après l'ajout d'un utilisateur et l'attribution de droits, avec l'utilisateur répertorié dans la partie inférieure de la boîte de dialogue. Cet utilisateur bénéficie de droits d'accès illimités.



Lorsque vous fermez la boîte de dialogue Ajouter de nouveaux utilisateurs, le nouvel utilisateur figure dans la liste de la boîte de dialogue Droits.

L'illustration suivante représente la boîte de dialogue Droits avec le nouvel utilisateur qui a été ajouté à la liste des comptes utilisateur et qui bénéficie de droits d'accès illimités.



Affichage des droits

Vous pouvez rapidement voir quels utilisateurs bénéficient de droits d'accès et de quel niveau sont ces droits d'accès.

Pour cela, développez l'arborescence de l'organisation pour afficher le conteneur que vous souhaitez analyser puis mettez ce conteneur en surbrillance. Ensuite, sélectionnez l'onglet Droits dans la zone droite de la fenêtre. L'onglet Droits affiche une liste des utilisateurs existants ainsi que les droits dont bénéficie actuellement chacun de ces utilisateurs. Une autre méthode pour obtenir ces informations consiste à mettre en surbrillance la catégorie Arborescence de l'organisation, puis à sélectionner l'onglet Droits.

Vous pouvez également vérifier les droits d'utilisateur en mettant un utilisateur en surbrillance dans la catégorie Utilisateurs.

Types d'accès

Les droits d'accès concernent les conteneurs de l'arborescence de l'organisation et les sous-réseaux. Le tableau ci-dessous répertorie les différents types d'accès et les droits associés.

Type d'accès	Droits
Aucun	Aucun accès pour l'utilisateur sélectionné. Lorsque vous ne bénéficiez d'aucun droit d'accès, vous ne voyez pas les conteneurs et les ordinateurs de l'arborescence de l'organisation.
Lire	L'utilisateur sélectionné bénéficie d'un accès en lecture limité à l'arborescence de l'organisation et à la catégorie Sous-réseaux. Il peut visualiser un objet de la liste ainsi que ses propriétés mais il n'est pas autorisé à faire des modifications ni à déplacer un ordinateur vers une autre catégorie.
Modifier	L'utilisateur sélectionné est autorisé à apporter des modifications à l'arborescence de l'organisation et à la catégorie Sous-réseaux. Il peut visualiser un objet et ses propriétés dans la liste, modifier les paramètres des règles appliquées à un conteneur et déplacer un ordinateur vers un autre conteneur.
Supprimer	L'utilisateur sélectionné bénéficie de droits d'accès lui permettant de supprimer l'objet sélectionné. Il est également autorisé à faire des changements. Il ne peut pas ajouter de nouveaux utilisateurs.
Contrôle absolu	L'utilisateur sélectionné bénéficie d'un contrôle absolu. Il peut ajouter de nouveaux utilisateurs et accorder un accès pour gérer les droits d'accès à d'autres comptes.

Caractéristiques des droits d'utilisateur

Après l'attribution de droits d'accès à un utilisateur, ces droits ont les caractéristiques suivantes :

Utilisateur – Indique un utilisateur pouvant accéder au conteneur sélectionné, avec le domaine où se trouve l'utilisateur.

Droits – Indique les droits d'accès dont l'utilisateur bénéficie pour ce conteneur.

Raison – Les droits d'utilisateur peuvent être hérités ou spécifiés.

Hérité – Indique que les droits d'utilisateur appliqués à ce conteneur sont hérités des droits d'utilisateur appliqués à un plus haut niveau de la hiérarchie, tel que la racine de l'arborescence de l'organisation.

Spécifié – Indique que les droits d'utilisateur appliqués au conteneur sont appliqués à un niveau particulier de la hiérarchie, tel que la racine de l'arborescence de l'organisation.

Affichage des droits d'utilisateur

Lorsque les droits sont définis et que vous mettez un conteneur en surbrillance dans la liste de gauche, vous pouvez alors cliquer sur l'onglet Droits dans la zone droite de la fenêtre pour afficher une liste d'utilisateurs avec les droits qui leur ont été octroyés. Les caractéristiques des droits d'utilisateur figurent dans cette liste. Ces caractéristiques s'affichent également lors de l'attribution de droits d'accès.

Affichage des droits d'utilisateur à partir de la catégorie Utilisateurs

Vous pouvez visualiser les droits d'utilisateur à partir de la catégorie Utilisateurs de la liste située à gauche de l'affichage de l'administrateur. Lorsque vous développez la catégorie Utilisateurs et sélectionnez un utilisateur dans la liste de gauche, les caractéristiques des droits d'utilisateur s'affichent dans la zone droite de la fenêtre.

Exemple d'accès pour différents comptes

Dans l'exemple suivant, il s'agit de montrer comment des droits d'accès de diverses natures peuvent être attribués à différents comptes.

L'illustration ci-dessous représente une arborescence de l'organisation avec trois conteneurs pour la Comptabilité, les Ventes et les Voyages.

Le tableau suivant décrit les possibilités pour attribuer différents droits d'accès à différents comptes.

Conteneur	Administrateur autorisé	Utilisateur 1	Utilisateur 2
Arborescence de l'organisation (objet racine)	Contrôle absolu	Modifier	Lire
Comptabilité	Contrôle absolu	Modifier	Lire
Ventes	Contrôle absolu	Modifier	Lire
Voyages	Contrôle absolu	Modifier	Lire

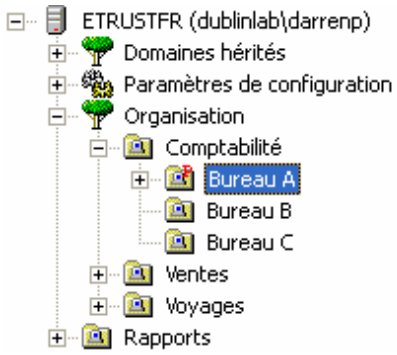
Tous les comptes de l'exemple ont accès à l'arborescence de l'organisation. L'administrateur autorisé bénéficie d'un contrôle absolu. Ce compte peut gérer l'ensemble des conteneurs de l'arborescence et définir des règles pour tous les ordinateurs situés dans les conteneurs. L'Utilisateur 1 est autorisé à faire des changements tandis que l'Utilisateur 2 ne bénéficie que d'un accès en lecture. Notez que l'accès à la catégorie Sous-réseaux et l'accès à l'arborescence de l'organisation sont de même niveau.

Création et utilisation des ordinateurs de configuration proxy

Utilisez l'option de configuration proxy pour indiquer les serveurs proxy que vous pouvez utiliser pour gérer efficacement les modifications de configuration dans votre réseau antivirus. Cette option vous permet de définir et d'appliquer les règles de configuration dans l'ensemble du réseau, selon une méthode hiérarchique. En désignant un ordinateur comme serveur proxy, vous créez un mécanisme de distribution efficace sur l'ensemble du réseau et réduisez ainsi la duplication du trafic.

Un administrateur autorisé peut désigner un ordinateur comme serveur proxy à partir de la liste des ordinateurs disponibles dans un conteneur de l'arborescence de l'organisation. Ce serveur proxy sert ensuite de point de distribution, transmettant les modifications de configuration aux ordinateurs de son conteneur et aux sous-conteneurs, en fonction des paramètres des règles.

Une fois que le serveur proxy est désigné, un indicateur s'affiche dans les icônes pour le conteneur et l'ordinateur.



Considérations relatives au serveur proxy

Veuillez noter les remarques suivantes sur les serveurs proxy.

- Tout ordinateur situé dans un conteneur de l'arborescence de l'organisation peut être utilisé comme serveur proxy, à l'exception des ordinateurs Windows 95 ou Windows 98.
- Vous pouvez désigner autant d'ordinateurs que vous le souhaitez comme serveurs proxy.

Grâce aux serveurs proxy, vous pouvez appliquer les paramètres de configuration au niveau racine de la liste des ordinateurs exécutant le logiciel antivirus ou à tout niveau de sous-conteneur de la liste. Les paramètres modifiés sont répartis efficacement dans le réseau si bien que le serveur Admin n'a plus besoin de transférer individuellement les commandes à chaque ordinateur.

Le serveur de redistribution de signatures a un rôle différent du serveur proxy de configuration. Le serveur de redistribution des signatures permet de rendre disponibles les fichiers de mises à jour de signatures à d'autres ordinateurs. Le serveur proxy de configuration est utilisé pour distribuer les paramètres des règles à travers le réseau.

Remarque : Le serveur proxy dont il est ici question se distingue d'un serveur proxy Internet.

Option de remplacement du proxy

Lorsque vous désignez un ordinateur comme serveur proxy, utilisez l'option de remplacement pour contrôler la transmission des règles à l'ensemble de la hiérarchie dans le cas où le serveur proxy pour une branche ne serait pas disponible.

Option	Description
Remplacement activé.	Lorsque le serveur proxy n'est pas disponible, le serveur proxy situé au niveau immédiatement supérieur dans la hiérarchie transmet les paramètres des règles aux ordinateurs servis de manière régulière.
Remplacement désactivé.	Lorsque le serveur proxy n'est pas disponible, le serveur proxy situé au niveau immédiatement supérieur dans la hiérarchie **ne** transmet **pas** les paramètres des règles aux ordinateurs servis de manière régulière.

Fonctionnement d'un serveur proxy

En parcourant la liste des ordinateurs, le serveur Admin trouve le proxy et transfère à cet ordinateur les commandes permettant de modifier la configuration. Puisque le proxy communique les modifications aux autres ordinateurs de son conteneur, le serveur Admin peut ignorer le reste des ordinateurs de ce conteneur et poursuivre en recherchant le prochain ordinateur qui recevra ces commandes. Il trouve le serveur proxy suivant et lui confère les commandes, et ainsi de suite.

Par exemple, s'il y a dix ordinateurs dans un conteneur et qu'un seul ordinateur est désigné comme serveur proxy, le serveur Admin envoie les informations une seule fois-à ce serveur proxy uniquement. Le proxy communique alors ces informations aux neuf ordinateurs restants dans son groupe de conteneurs. Comme le serveur Admin n'envoie pas les commandes à tous les ordinateurs, ses performances et celles du réseau en général s'en trouvent améliorées.

Ordinateurs sous-proxy

Le serveur proxy applique les paramètres aux ordinateurs de son conteneur. Si le conteneur comprend des sous-conteneurs, le serveur proxy applique les paramètres aux ordinateurs de ces sous-conteneurs. Cependant, si le sous-conteneur comprend un serveur proxy, le serveur proxy supérieur transmet les informations au serveur proxy du sous-conteneur et ignore le reste des ordinateurs et conteneurs de ce sous-conteneur.

Distribution de signatures avec l'option Télécharger

Vous pouvez utiliser l'option Télécharger pour une distribution de signatures dans l'affichage de l'administrateur afin d'obtenir des mises à jour de signatures sur demande et d'appliquer ces mises à jour à l'ensemble du réseau antivirus. Cette section décrit les modalités d'utilisation de l'option Télécharger dans un environnement de réseau.

Utilisation de l'option Télécharger dans l'affichage de l'administrateur

Pour les utilisateurs de l'Affichage de l'administrateur dans des environnements de réseau, l'option Télécharger est accessible de différentes façons.

Important ! *Lorsque vous utilisez l'option Télécharger dans un environnement de réseau, vous devez vous assurer que chaque serveur de redistribution est prêt à être utilisé comme source des mises à jour des signatures. Les mises à jour des signatures sur un serveur de redistribution doivent être à jour et disponibles pour la redistribution.*

Lorsque vous utilisez l'option Télécharger dans l'Affichage de l'administrateur, la mise à jour est effectuée sur plusieurs ordinateurs. Son action dépend du contexte dans lequel elle est utilisée. Reportez-vous à la section Priorité des règles pour de plus amples informations sur la manière dont les règles deviennent prioritaires dans une hiérarchie de conteneurs.

Vous pouvez utiliser comme suit l'option Télécharger dans l'Affichage de l'administrateur :

- En sélectionnant une règle de distribution des signatures
- En sélectionnant un conteneur dans l'arborescence de l'organisation
- En sélectionnant un ordinateur particulier dans une branche

Remarque : Le bouton Télécharger n'est pas disponible dans la boîte de dialogue Règles de mise à jour des signatures si les règles ne s'appliquent à aucune branche. Par exemple, il n'est pas disponible lorsque vous créez une nouvelle règle.

Utilisation de la fonction Télécharger avec une règle de distribution de signatures

Sélectionnez une instance de règles de distribution des signatures dans la catégorie Distribution des signatures, puis cliquez dessus avec le bouton droit et sélectionnez Editer. Si la règle sélectionnée est affectée à une branche dans l'arborescence de l'organisation, la boîte de dialogue Règles s'affiche et l'option Télécharger devient disponible. Lorsque vous cliquez sur Télécharger, la mise à jour des signatures est effectuée sur tous les ordinateurs des branches dans lesquelles la règle est appliquée. Les options activées pour l'instance de règle sélectionnée sont utilisées.

Utilisation de la fonction Télécharger avec un conteneur dans l'arborescence de l'organisation

Sélectionnez un conteneur ou une branche dans l'arborescence de l'organisation, cliquez dessus avec le bouton droit de la souris, sélectionnez Règles puis Distribution. La boîte de dialogue Règles de mise à jour des signatures s'affiche. Si des règles sont appliquées à la branche sélectionnée, les options pour ces règles s'affichent et le bouton Télécharger est disponible. Lorsque vous cliquez sur Télécharger, la mise à jour est effectuée sur tous les ordinateurs des branches dans lesquelles les règles sont appliquées.

Remarques sur les règles de la branche

Vous pouvez appliquer l'option Télécharger à une branche contenant des sous-branches. Il peut exister dans la branche sélectionnée des sous-branches soumises à différentes règles. Un ordinateur dans une sous-branche possédant des règles différentes ne sera pas mis à jour.

Utilisation de l'option Télécharger avec un ordinateur dans une branche

Lorsque vous sélectionnez un ordinateur dans une branche, cliquez dessus avec le bouton droit de la souris et sélectionnez Configurer paramètres de distribution ; les options de mise à jour des signatures pour cet ordinateur s'affichent. Si vous cliquez sur Télécharger, les paramètres activés pour cet ordinateur ne s'appliquent qu'à cet ordinateur. Il ne s'agit pas d'un paramètre de règles.

Utilisation de l'option Télécharger avec des serveurs de redistribution

Lorsque vous utilisez l'option Télécharger dans un environnement de réseau, vous devez vous assurer que les mises à jour des signatures sont disponibles via une source contenant les mises à jour les plus récentes. Vous pouvez utiliser la fonction Télécharger sur une branche possédant de nombreuses sous-branches. Il peut y avoir plusieurs ordinateurs qui agissent comme une source pour les mises à jour des signatures dans ces sous-branches. Par ailleurs, les options de mise à jour des signatures peuvent être configurées différemment pour chaque branche. Les sous-branches peuvent utiliser des listes de sources différentes. Chaque branche peut obtenir des mises à jour provenant d'un serveur de redistribution différent.

Lorsque vous utilisez l'option Télécharger, chaque serveur de redistribution doit déjà disposer des mises à jour les plus récentes. En outre, le temps d'attente doit être réglé sur une valeur permettant d'obtenir les mises à jour en temps utile.

Remarque : Vous pouvez organiser les ordinateurs qui agissent comme serveurs de redistribution dans un conteneur unique. Ceci permet de gérer plusieurs serveurs de redistribution de manière efficace. Vous pouvez ensuite appliquer des règles et des paramètres aux serveurs de redistribution en tant que groupe.

Lorsque vous utilisez l'option Télécharger, le téléchargement des signatures s'effectue sur tous les ordinateurs de la branche. Ceci comprend tout ordinateur qui agit en tant que serveur de redistribution dans cette branche. Si le serveur de redistribution possède déjà les mises à jour les plus récentes, le processus de téléchargement « reconnaît » que le serveur ne doit pas être mis à jour. Si la valeur du temps d'attente sur ce serveur est de zéro, les ordinateurs qui dépendent de ce serveur de redistribution pourront recevoir le téléchargement de signatures sans délai. En mettant les serveurs de redistribution à jour avant d'utiliser l'option Télécharger, vous êtes assurés que ce sont les signatures les plus récentes qui seront distribuées à votre réseau antivirus.

Remarques concernant l'analyse des unités du réseau

Un utilisateur peut se relier à une unité réseau à partir d'un ordinateur local et effectuer une analyse. De même, sous UNIX et OS X, un système de fichier distant peut être monté et analysé. Cela peut être utile pour analyser un fichier spécifique, mais cette méthode n'est pas la meilleure pour gérer des unités du réseau. Lorsqu'un ordinateur local analyse l'unité réseau, un trafic réseau important apparaît dû aux paquets de données diffusés entre les deux ordinateurs.

La méthode préférée de l'administrateur distant pour analyser une unité réseau est de planifier un job d'analyse sur un ordinateur en réseau en utilisant les fonctionnalités de l'affichage de l'administrateur. L'ordinateur à analyser doit posséder une instance de logiciel antivirus de Computer Associates. Vous pouvez ensuite planifier l'analyse à distance, qui sera exécutée localement sur l'ordinateur en réseau. Cette méthode est plus efficace et nécessite moins de ressources du réseau que lors d'une analyse locale exécutée sur l'ensemble du réseau.

Personnalisation des messages

Sous Windows, le logiciel antivirus de Computer Associates affiche des messages qui utilisent des codes d'événements Windows. Vous pouvez personnaliser les messages pour ajouter des informations supplémentaires. Vous pouvez utiliser cette fonctionnalité lorsqu'une infection est détectée ou lorsque des fichiers de signatures ne sont plus à jour et si vous souhaitez que l'utilisateur effectue une mise à jour. Par exemple, lorsqu'un message indiquant une infection apparaît, vous pouvez le personnaliser en y ajoutant des instructions qui permettront d'appeler l'administrateur antivirus et d'afficher le nom et le numéro de téléphone de la personne à contacter.

Remarque : L'utilitaire Nethelp de Windows vous permettra d'afficher les messages.

Génération et affichage de rapports

La catégorie Rapports vous permet d'afficher des rapports d'antivirus à partir d'ordinateur découverts par le serveur Admin.

Remarque : Les rapports ne sont pas disponibles dans l'interface utilisateur graphique du navigateur Web et d'OS X.

Génération de rapports

Les rapports sont générés sur le serveur Admin et affichés sur la console de ce serveur. Les rapports de détection de virus sont basés sur les données collectées sur les ordinateurs clients. Pour collecter ces données sur les ordinateurs clients, vous pouvez configurer ceux-ci de la manière suivante :

- **Retransmission des journaux des clients au serveur Admin –** Sur un ordinateur client, configurez les options Alert pour faire suivre les journaux au serveur Admin (ou au serveur proxy eTrust Antivirus si le réseau est configuré pour retransmettre selon une hiérarchie d'escalade). Pour générer des rapports basés sur les virus découverts, veillez à retransmettre les journaux au serveur Admin et à configurer le module de notification personnalisée sur la catégorie Rapport de virus de l'onglet de filtre Alert. En outre, sélectionnez le module de service depuis lequel vous voulez signaler des messages spécifiques.
- **Retransmission de journaux d'un serveur Amin à un autre –** Sur un ordinateur jouant le rôle d'un serveur Admin, configurez les options Alert pour qu'il se retransmette les journaux à lui-même. Pour générer des rapports basés sur les virus découverts, veillez à retransmettre les journaux au serveur Admin et à configurer le module de notification personnalisée sur la catégorie Rapport de virus de l'onglet de filtre Alert. En outre, sélectionnez le module de service depuis lequel vous voulez signaler des messages spécifiques.

  Pour planifier l'intervalle entre les générations de rapports, utilisez le programme *cfgReport.exe*. Pour plus d'informations sur le programme *cfgReport.exe*, consultez la section « Planification de la génération de rapports ».

Veuillez vous reporter à la section « Utilisation des options de rapport Alert » du chapitre « Utilisation du gestionnaire Alert » pour obtenir des informations sur la configuration des paramètres de rapport Alert.

Affichage des rapports

Les rapports peuvent être consultés dans l'affichage de l'administrateur. Vous pouvez choisir deux types de rapports :

- **Rapports eTrust Antivirus –** Pour les ordinateurs de votre réseau qui ont été découverts par le serveur Admin et sur lesquels eTrust Antivirus est installé.
- **Rapports de domaine –** Pour les ordinateurs de votre réseau groupés dans des domaines qui ont été découverts par le serveur Admin et sur lesquels eTrust Antivirus est ou non installé.

Vous pouvez afficher les types de rapports eTrust Antivirus suivants :

- **Détections de Virus –** Résumé des dix principaux virus et liste de tous les virus détectés, regroupés par plage horaire.
- **Ordinateurs infectés –** Résumé des dix principaux ordinateurs et liste de tous les ordinateurs dans lesquels un virus a été détecté, regroupés par plage horaire.
- **Utilisateurs infectés –** Résumé des dix principaux utilisateurs et liste de tous les utilisateurs ayant accédé à un fichier infecté, regroupés par plage horaire.
- **Déploiement –** Liste de toutes les installations de eTrust Antivirus regroupées par système d'exploitation.
- **Charge par serveur –** Affichage de la charge placée sur les signatures eTrust Antivirus ayant été affectée à ce serveur. Le rapport prend en compte le nombre d'ordinateurs dont chaque serveur est répertorié comme source de distribution principale ou comme source de distribution secondaire.
- **Charge par règle –** Affichage de la charge placée sur les signatures eTrust Antivirus ayant été affectée à une règle. Le rapport montre le nombre d'ordinateurs où apparaît chaque règle.
- **Signatures –** Affichage du nombre d'ordinateurs sur lesquels chaque moteur antivirus est installé, ainsi que le nom du moteur et le nombre d'ordinateurs sur lesquels ce type de moteur est installé, et le nombre de versions de signature détecté dans les sous-réseaux.
- **Exception de signature –** Affichage d'informations de type résumé sur les trois versions de signature les moins périmées, par comparaison avec la version de signature du serveur Admin, pour chaque moteur.
- **Exception de signature –** Affichage d'informations détaillées sur les ordinateurs contenant les trois versions de signature les moins périmées, par comparaison avec la version de signature du serveur Admin, pour chaque moteur.

- **Rapports par virus –** La catégorie Rapports par virus affiche les informations suivantes de type de résumé pour chaque virus trouvé :

  Par sous-réseau – Affichage des informations détaillées concernant le virus détecté en utilisant la catégorie de sous-réseau.

  Par branche – Affichage des informations détaillées concernant le virus détecté en utilisant la catégorie de branche.

  Par utilisateur – Affichage des informations détaillées concernant le virus détecté en utilisant la catégorie d'utilisateur.

  Par ordinateur – Affichage des informations détaillées concernant le virus détecté en utilisant la catégorie d'ordinateur.

  Par action – Affichage des informations détaillées concernant le virus détecté en utilisant la catégorie d'action.

- **Rapports par ordinateur –** La catégorie Rapports par ordinateur affiche les informations de type de résumé pour chaque virus trouvé regroupés par nom d'ordinateur.
- **Rapports par utilisateur –** La catégorie Rapports par utilisateur affiche les informations de type de résumé pour chaque virus trouvé regroupés par nom d'utilisateur.

Vous pouvez afficher les types de rapports de domaine suivants :

- **Rapports des ordinateurs protégés –** La catégorie Rapports des ordinateurs protégés affiche les informations suivantes de type de résumé pour chaque ordinateur découvert dans votre réseau Microsoft :

  - **Résumé de domaine –** Affichage des informations de type de résumé concernant tous les ordinateurs découverts avec les détails incluant le nom de domaine, les ordinateurs protégés et les ordinateurs non protégés.

  - **Total des ordinateurs protégés –** Affichage des informations concernant les ordinateurs sur lesquels eTrust Antivirus est installé avec des détails incluant le nom de domaine, l'adresse IP, le nom de la branche, et la version de l'antivirus.

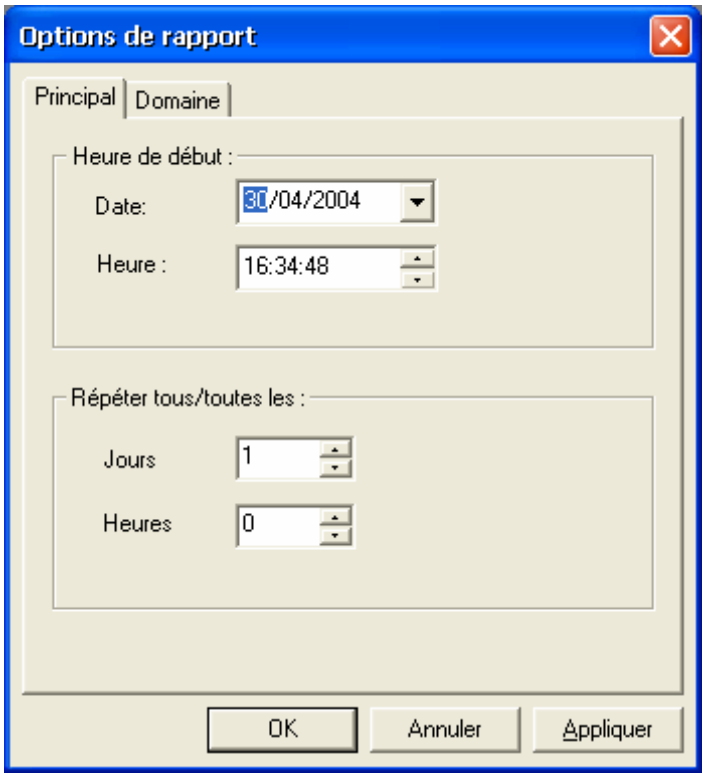
  - **Total des ordinateurs non protégés –** Affichage des informations concernant les ordinateurs sur lesquels eTrust Antivirus n'est pas installé avec des détails incluant le nom de l'ordinateur associé et le nom de domaine.

  - **Réseau Microsoft Windows –** Affichage de la liste des ordinateurs, par nom de domaine, qui sont protégés et de ceux qui ne sont pas protégés par eTrust Antivirus.

Planification de la génération des rapports

Vous pouvez configurer de façon indépendante l'heure et l'intervalle pour que le serveur Admin planifie la génération des rapports d'antivirus et de domaine. Pour planifier les heures, exécutez manuellement le programme *cfgReport.exe*. Il se trouve dans le chemin d'accès \CA\eTrust Antivirus sous le répertoire dans lequel vous avez installé eTrust Antivirus.

La figure suivante montre un exemple de catégorie de la boîte de dialogue Option de rapports après l'exécution de *cfgReport.exe* :



Vous pouvez définir l'heure à laquelle les rapports peuvent être générés dans le champ Heure de début, ainsi que la fréquence de génération des rapports dans le champ Répéter. Utilisez l'onglet Principal pour planifier les rapports de type antivirus. Utilisez l'onglet Domaine pour planifier les rapports de type domaine.

Chapitre

9

Utilisation de l'utilitaire d'installation à distance

Ce chapitre présente l'utilitaire d'installation à distance. Cet utilitaire vous permet d'installer le logiciel antivirus Computer Associates et le logiciel de licence dans l'entreprise sur des systèmes Windows NT, Windows 2000 et Windows XP uniquement.

Remarque : Reportez-vous à « **Installation à distance sur un ordinateur Windows 9x** » pour plus d'informations sur l'installation à distance sur Windows 9x.

L'installation à distance peut être divisée en différentes étapes :

- Première installation de l'utilitaire
- Configuration des fichiers ICF pour le logiciel avec les options d'installation souhaitées (si vous souhaitez modifier les options par défaut)
- Indication des cibles de l'installation et des informations administratives sur le compte pour chaque cible
- Lancement du processus d'installation du logiciel antivirus sur les ordinateurs cible

Exécution de l'utilitaire

Remarque : Cette version de l'utilitaire d'installation à distance ne peut être installée que sur des systèmes Windows NT, Windows 2000, Windows 2003 ou Windows XP fonctionnant sur un processeur Intel x86, IA64, AMD64 ou compatible.

La première fois que vous utilisez l'utilitaire d'installation à distance, vous pouvez le lancer à partir du CD produit ou de l'explorateur du produit. L'assistant est démarré et installe l'utilitaire sur l'ordinateur local. Nous entendons par « ordinateur local » l'ordinateur sur lequel l'utilitaire d'installation à distance est exécuté.

Conditions requises pour l'ordinateur local

Vous trouverez ci-dessous les conditions requises pour l'ordinateur local.

- Microsoft Windows NT, Windows 2000, Windows Server 2003 ou Windows XP.

  L'utilitaire d'installation à distance doit être exécuté sur un ordinateur disposant du système d'exploitation Microsoft Windows NT, Windows 2000, Windows Server 2003, Windows XP et basé sur les processeurs 64 bits.

- Le service du serveur doit être activé.

  L'utilitaire d'installation à distance distribue le logiciel dans les répertoires partagés de l'ordinateur local. L'ordinateur local doit donc être en mesure de partager des répertoires en tant que ressources du réseau.

- L'utilisateur connecté à l'ordinateur local doit disposer des droits d'accès d'administrateur.

  L'utilitaire d'installation à distance doit modifier les valeurs de registre et créer des ressources partagées pour les répertoires contenant les fichiers source d'installation.

  Remarque : Si votre ordinateur local fonctionne sous Windows XP, vous devez désactiver l'option Partage de fichiers simple pour que l'utilitaire d'installation à distance fonctionne convenablement. Vous pouvez désactiver l'option Partage de fichiers simple depuis la fenêtre Microsoft Explorer. Dans le menu Outils, sélectionnez Options des dossiers, puis cliquez sur l'onglet Affichage. Dans le volet Paramètres avancés, désélectionnez la case Utiliser le partage de fichiers simple (recommandé).

A propos de l'assistant d'installation

L'assistant d'installation installe automatiquement l'utilitaire sur l'ordinateur local et définit les répertoires et les fichiers source que vous pouvez utiliser pour effectuer une installation distante du logiciel antivirus.

Vous pouvez ré-exécuter l'installation sur un ordinateur sur lequel l'utilitaire d'installation à distance est déjà installé pour ajouter de nouvelles images source.

Source d'installation automatiquement créée

L'assistant copie automatiquement le CD sur le disque dur local. Il crée également une configuration d'installation par défaut pour le serveur Windows NT et le poste de travail Windows NT. En ce qui concerne les informations sur la licence, il est possible que vous ayez à configurer le répertoire de licence.

Vous pouvez modifier les emplacements de l'utilitaire et des fichiers source lors de l'installation ; cependant, la plupart des utilisateurs n'ont pas besoin de modifier la configuration par défaut.

Reportez-vous à la section « Configuration de la source d'installation

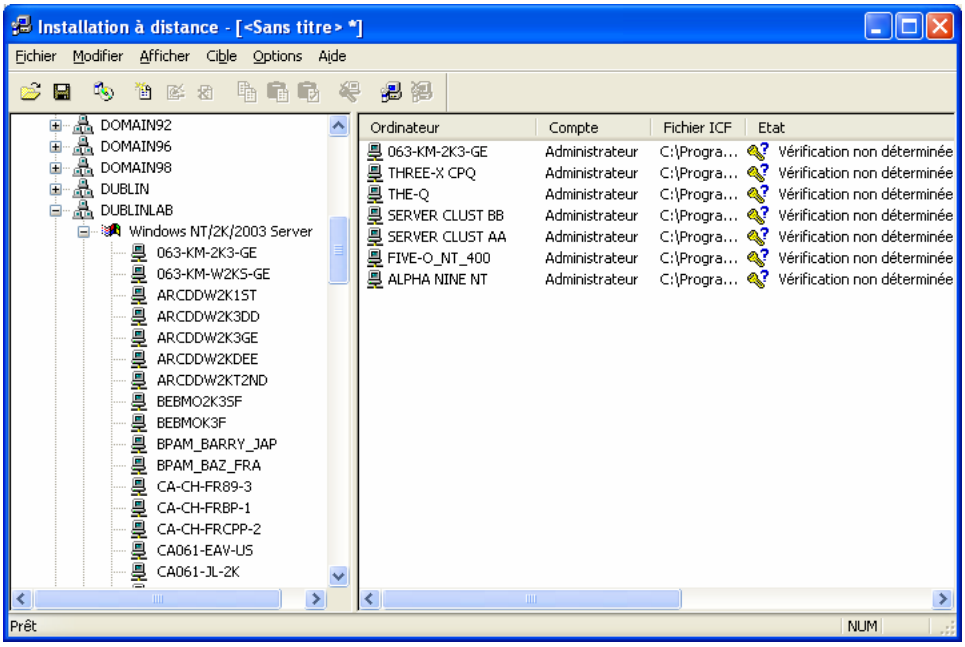
» pour plus d'informations sur les répertoires source et les licences.

Utilisation de l'interface d'installation à distance

Cette section décrit l'interface graphique de l'utilitaire d'installation à distance. Cette interface vous permet de définir les cibles de l'installation, d'ouvrir et de fermer des sessions d'installation, d'éditer les propriétés de la source d'installation et de modifier la configuration par défaut du logiciel qui sera installé sur les ordinateurs distants.

Lancement de l'interface d'installation à distance

Après avoir installé l'utilitaire pour la première fois, vous pouvez le lancer à partir du menu Démarrer. L'utilitaire d'installation à distance est composé de deux sections : un explorateur de réseau sur la gauche et une liste des cibles d'installation sur la droite, comme vous pouvez le voir ci-dessous.



Dans l'exemple, un ordinateur doté d'un serveur Windows NT a été sélectionné dans la liste de gauche. Une liste de cibles d'installation est affichée à droite. La liste est vide si aucun ordinateur n'est spécifié comme cible.

Recherche dans le réseau pour sélectionner les cibles d'installation

L'explorateur de réseau permet de sélectionner les cibles d'installation dans le réseau. Lorsque vous explorez les domaines et groupes de travail de Windows NT, Windows 2000, Windows 2003 ou Windows XP , les ordinateurs sont regroupés par système d'exploitation. Cela facilite la sélection des cibles d'installation valides. Affichez l'arborescence d'un domaine ou d'un groupe de travail, puis l'arborescence d'une catégorie de système d'exploitation pour sélectionner l'ordinateur approprié. Si vous connaissez le nom de l'ordinateur cible, vous pouvez le saisir manuellement, sans avoir à parcourir le réseau.

Reportez-vous à la section « Définition des cibles pour l'installation » pour plus d'informations sur les cibles d'installation.

A propos de la liste des cibles d'installation

Dans la partie droite de la fenêtre, une liste affiche les ordinateurs cibles spécifiés. La liste des cibles d'installation affiche les ordinateurs candidats à l'installation, ainsi que leur statut courant. Si aucun ordinateur n'a été spécifié comme cible, rien ne s'affiche dans la liste.

Informations sur la cible d'installation

Les informations suivantes sont affichées dans la liste des cibles d'installation pour chaque cible d'installation.

Colonne	Description
Ordinateur	Le nom de l'ordinateur sur lequel le logiciel antivirus sera installé. Chaque ordinateur ne peut figurer qu'une seule fois dans la liste d'installation.
Compte	Le compte permet de se connecter à l'ordinateur cible de l'installation. Le compte doit bénéficier des droits d'administrateur.
Fichier ICF	Le fichier de réponse automatique contient les options d'installation souhaitées. Un exemple de fichier ICF nommé INOC6.ICF est fourni sur le CD. Veuillez consulter ce fichier pour une description de la configuration et des options disponibles. Vous pouvez également éditer ce fichier dans l'utilitaire.
Etat	Etat actuel de la cible d'installation.
Progression de l'installation	Au cours de l'installation, ce champ affiche la fonction actuellement exécutée et son évolution.

Informations sur l'état de la cible

L'état de l'installation pour chaque cible d'installation est affiché dans la colonne d'état. Ces valeurs d'état sont décrites dans le tableau suivant.

Icône	Message	Description
	Installation	L'installation est en cours d'exécution. La colonne Progression de l'installation contient des informations détaillées sur l'état actuel.
	Installation en attente	Cette cible a été sélectionnée pour l'installation. L'installation commencera lorsqu'une cible en cours d'installation sera terminée ou interrompue manuellement.
	Installation réussie	L'installation s'est terminée avec succès.
	Echec de l'installation [###]	L'installation a échoué et a renvoyé le code d'erreur ###.
	Installation interrompue par l'utilisateur	L'installation a été interrompue manuellement.
	Vérification achevée avec succès	Une ouverture de session test a été effectuée avec succès avec les informations spécifiées sur le compte.
	Vérification non déterminée	Les informations spécifiées sur le compte n'ont pas été vérifiées par un test.
	Echec de la vérification [###]	Une connexion test a échoué avec les informations spécifiées sur le compte, en renvoyant le code erreur ###.

Remarque : Pour obtenir des informations supplémentaires sur les codes d'erreur, utilisez la commande Windows NET HELPMSG.

Utilisation de la barre d'outils

La barre d'outils permet d'accéder aux commandes et fonctionnalités les plus courantes. Les boutons de la barre d'outils sont activés ou désactivés en fonction des éléments sélectionnés dans l'explorateur de réseau et dans la liste des cibles d'installation. C'est pourquoi il est possible que certaines options ne soient pas disponibles, en fonction de votre sélection.

Le tableau suivant récapitule les différents boutons de la barre d'outils et leur correspondance dans les menus avec une description de ce qui se passe lorsqu'un bouton ou une option est sélectionné(e).

Bouton	Commande	Description
	Fichier, Ouvrir	Permet d'ouvrir une liste de cibles enregistrée antérieurement ou d'importer une liste de cibles générée dans une autre application.
	Fichier, Enregistrer	Permet d'enregistrer une liste de cibles sous forme de fichier.
	Options, Source d'installation	Permet de configurer les fichiers source d'installation.
	Cible, Ajouter	Permet d'ajouter une nouvelle cible d'installation à la liste.
	Cible, Editer	Permet d'éditer les cibles d'installation sélectionnées.
	Cible, Supprimer	Permet de supprimer les cibles d'installation sélectionnées.
	Edition, Copier	Permet de copier la cible d'installation sélectionnée dans le Presse-papiers.
	Edition, Coller	Permet d'appliquer tous les paramètres du Presse-papiers dans les cibles sélectionnées.
	Edition, Collage spécial	Permet d'appliquer à partir du Presse-papiers différents paramètres aux cibles sélectionnées.
	Cible, Vérifier le compte	Permet de vérifier les informations spécifiées sur le compte pour les cibles sélectionnées.

Bouton	Commande	Description
	Cible, Lancer l'installation	Permet de lancer la session d'installation pour les cibles sélectionnées.
	Cible, Arrêter l'installation	Permet d'arrêter l'installation ou d'annuler l'installation en attente pour les cibles sélectionnées.

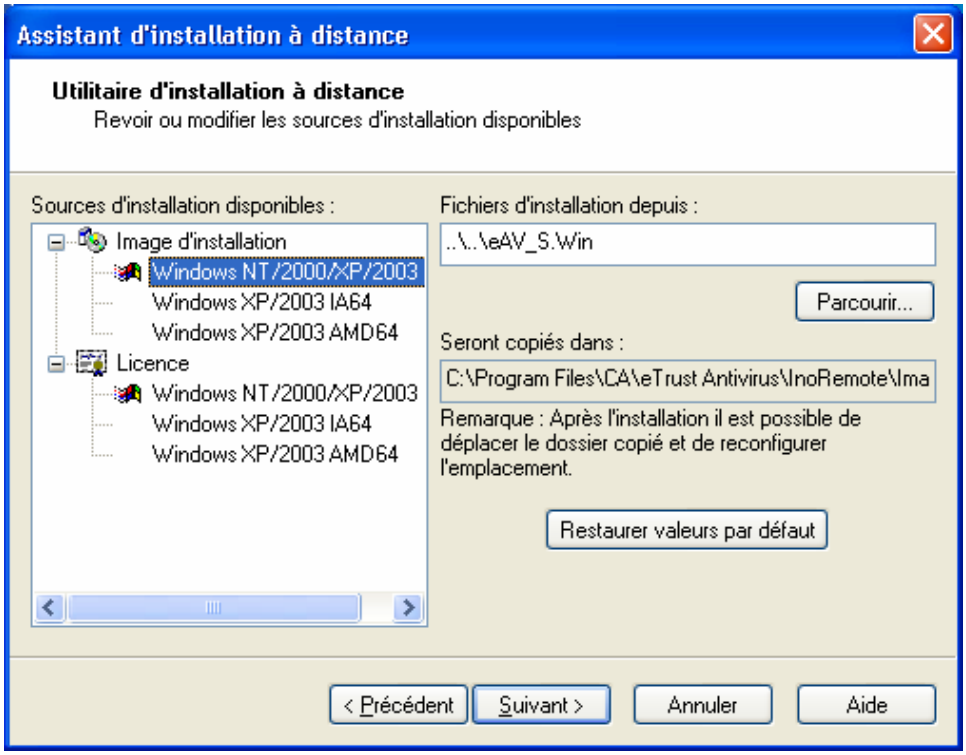
Configuration de la source d'installation

Cette section décrit les répertoires et fichiers de la source d'installation utilisés par l'utilitaire pour les installations à distance. La plupart des utilisateurs n'auront pas besoin de modifier la configuration par défaut des propriétés de la source d'installation. Le fichier exécutable d'installation est SETUP.EXE. Le fichier exécutable d'installation de licence est SILENT.BAT.

Configuration des propriétés de la source d'installation

Le logiciel antivirus de Computer Associates est distribué aux cibles d'installation depuis des répertoires partagés de l'ordinateur local. Vous pouvez modifier les propriétés de la source d'installation à l'aide de l'application d'installation, une fois que l'utilitaire est installé sur l'ordinateur local.

Dans la barre de menus Utilitaire d'installation à distance, sélectionnez Options, puis l'option ou le bouton de barre d'outils Source d'installation pour afficher la boîte de dialogue Assistant d'installation, comme dans l'exemple ci-dessous.



Pour éditer les propriétés de la source d'installation, sélectionnez un élément dans la liste des sources d'installation disponibles, puis cliquez sur le bouton Suivant.

Propriétés de la source d'installation

Toutes les propriétés de la source d'installation sont obligatoires, sauf mention contraire, et sont décrites dans le tableau suivant.

Propriété	Description
Nom de partage	Nom utilisé lors de la création du partage en lecture seule contenant les fichiers source d'installation. L'utilitaire crée le partage lorsqu'une installation est lancée et peut facultativement le supprimer lorsqu'il s'arrête. **Remarque :** Ce partage est ajouté à la liste de partages de sessions vides (NullSessionShares). Les processus peuvent ainsi se dérouler sous le compte du système local des ordinateurs distants pour accéder au partage sans qu'une connexion ne soit établie. Cet accès est limité à la lecture seule.
Chemin de partage	Chemin complet du répertoire partagé.

Propriété	Description
Sous-répertoire	Répertoire situé sous le partage abritant les fichiers source. Cette propriété est facultative si le chemin de partage contient l'image d'installation.
Nom exe	Nom de l'exécutable utilisé pour installer le logiciel antivirus.

Configuration des propriétés de la source de licence

Il est possible que vous ayez à modifier les propriétés de la source de licence. Vous trouverez ci-dessous un exemple de configuration de la source Windows NT (x86).

Propriété	Valeur
Nom de partage	INOREMOTE$
Chemin de partage	C:\PROGRAMMES\COMPUTER ASSOCIATES\INOREMOTE
Sous-répertoire	\LICENSE
Nom exe	SILENT.BAT

Suppression des partages de source d'installation

Au moment du lancement de la session d'installation, les répertoires source d'installation sont automatiquement spécifiés comme répertoires partagés. Lorsque vous avez terminé la session d'installation et quittez l'utilitaire, la désignation de ces répertoires en tant que partage est supprimée. Si vous préférez conserver la disponibilité des partages, cette fonction peut être désélectionnée dans la barre de menus, en choisissant Options et en sélectionnant l'option de menu Supprimer les partages en quittant. Une coche devant cette option indique qu'elle est activée et que les partages seront supprimés.

Remarque : Les partages créés par l'utilitaire d'installation à distance sont ajoutés à la liste des partages de sessions vides (NullSessionShares). Les processus peuvent ainsi se dérouler sous le compte du système local des ordinateurs distants pour accéder au partage sans qu'une connexion ne soit établie. Cet accès est limité à la lecture seule ; nous vous recommandons cependant de laisser cette fonctionnalité activée.

Définition des cibles pour l'installation

L'interface d'installation à distance vous permet de spécifier les cibles d'installation. Il s'agit des ordinateurs sur lesquels vous souhaitez installer le logiciel antivirus.

Conditions requises pour la cible d'installation

Vous trouverez ci-dessous les conditions requises pour l'ordinateur cible d'installation.

- Microsoft Windows NT (x86)

  Les cibles d'installation à distance doivent disposer des systèmes d'exploitation Microsoft Windows NT, Windows 2000, Windows Server 2003 ou Windows XP sur un processeur Intel x86 ou compatible.

- Création de partages d'unités masquées

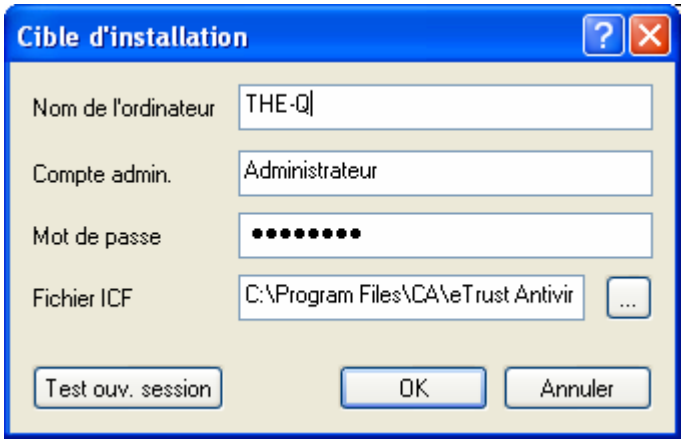
  L'utilitaire d'installation à distance accède au partage ADMIN$ de l'ordinateur cible d'installation. Vous devez donc avoir configuré les règles système pour qu'elles créent automatiquement le partage ADMIN$ au démarrage du système. Cette règle sera activée dans une installation par défaut de Windows NT, Windows 2000, Windows Server 2003 ou Windows XP.

Ajout de nouvelles cibles

La boîte de dialogue Cible d'installation vous permet d'indiquer l'ordinateur, le mot de passe et les informations concernant le fichier ICF pour la nouvelle cible. Cette boîte de dialogue est accessible de différentes manières.

- Depuis la barre de menus, sélectionnez Cible, puis l'option Ajouter ou cliquez sur le bouton Ajouter cible de la barre d'outils.
- Appuyez sur la touche Insérer de votre clavier.
- Double-cliquez sur un ordinateur valide dans l'arborescence de l'explorateur de réseau située dans la partie gauche de la fenêtre de l'explorateur de l'installation à distance. Affichez l'arborescence de la liste d'ordinateurs.

La boîte de dialogue Cible d'installation s'affiche, comme le montre l'exemple ci-dessous.



Dans cet exemple, l'ordinateur *THE-Q* est la cible de l'installation et le compte *Administrateur* est utilisé pour se connecter à celui-ci. Le processus d'installation aura recours à un fichier ICF nommé *NUMBER.ICF*.

Remarque : Si une entrée de la liste de cibles est sélectionnée, la nouvelle cible héritera automatiquement des paramètres de l'élément sélectionné.

Propriétés de la cible d'installation

Les propriétés de la cible d'installation sont décrites dans le tableau ci-dessous.

Propriété	Description
Nom de l'ordinateur	Le nom de l'ordinateur sur lequel le logiciel sera installé. Chaque ordinateur ne peut figurer qu'une seule fois dans la liste d'installation.
Compte admin.	Le compte utilisé pour accéder à l'ordinateur cible. Le compte doit bénéficier des droits d'administrateur. Cette valeur peut avoir la forme *NOM D'UTILISATEUR*, *DOMAINE\NOM D'UTILISATEUR* ou *ORDINATEUR\NOM D'UTILISATEUR*.

Propriété	Description
Mot de passe admin.	Le mot de passe pour le compte spécifié.
Fichier ICF	Le fichier de réponse automatique contient les options d'installation souhaitées. Un exemple de fichier ICF nommé INOC6.ICF est fourni sur le CD. Reportez-vous à l'annexe B de ce manuel de l'administrateur pour obtenir une description détaillée de la configuration et des options disponibles. Cliquez sur le bouton '...' pour rechercher le fichier. Vous pouvez cliquer sur le bouton Créer nouveau pour afficher une boîte de dialogue de configuration qui vous permettra d'éditer le fichier ICF depuis l'utilitaire.

Vous pouvez vérifier les informations sur le compte à ce moment-là en cliquant sur le bouton Test connexion. Les résultats du test de connexion sont stockés et affichés dans la colonne Etat de la liste des cibles d'installation.

Edition des cibles existantes

Vous pouvez modifier des cibles d'installation existantes à l'aide de la boîte de dialogue Cible d'installation. Pour cela, vous avez différentes possibilités.

- Sélectionnez l'élément dans la liste. Dans la barre de menus, sélectionnez ensuite l'option Cible, puis l'option Edition ou cliquez sur le bouton Editer la cible de la barre d'outils.
- Double-cliquez sur l'élément souhaité dans la liste des cibles d'installation.

La boîte de dialogue Cible d'installation s'affiche ; elle vous permet d'éditer les propriétés.

Vous pouvez sélectionner plusieurs éléments dans la liste ; cependant, la fonction d'édition ne peut être utilisée que sur un seul élément sélectionné. Pour modifier une sélection de plusieurs éléments, utilisez les commandes Coller et Collage spécial pour appliquer les propriétés d'une cible d'installation aux autres.

Suppression des cibles existantes

Vous pouvez supprimer les cibles d'installation de différentes manières.

- Sélectionnez les éléments dans la liste et cliquez sur la commande Cible, puis Supprimer ou utilisez le bouton Supprimer cible de la barre d'outils.
- Sélectionnez les éléments dans la liste et appuyez sur la touche Suppression.

Chacune de ces actions affiche une boîte de dialogue vous demandant de confirmer la suppression de l'élément.

Copie des informations sur la cible

Il est souvent nécessaire de saisir les mêmes informations pour différentes cibles. Vous pouvez copier les propriétés communes d'une cible d'installation à une autre grâce au Presse-papiers.

Pour cela, sélectionnez la cible d'installation contenant la configuration souhaitée et sélectionnez le menu Edition puis Copier ou cliquez sur le bouton Copier de la barre d'outils. L'élément sélectionné restera dans le Presse-papiers jusqu'à ce qu'un autre élément y soit copié ou jusqu'à ce que l'élément soit supprimé.

Utilisation de Coller et Collage spécial

Pour appliquer la configuration d'un élément du Presse-papiers à d'autres éléments, sélectionnez les éléments dans la liste et sélectionnez la commande Edition, puis Coller ou cliquez sur le bouton Collage spécial de la barre d'outils.

Toutes les propriétés de l'élément du Presse-papiers seront appliquées à la sélection de la liste.

Il est parfois recommandé de n'appliquer que certaines propriétés du Presse-papiers aux cibles sélectionnées. Sélectionnez le menu Edition, puis Collage spécial ou cliquez sur le bouton Collage spécial de la barre d'outils pour afficher une fenêtre Collage spécial dans laquelle vous pourrez sélectionner et appliquer les différentes propriétés.

Remarque : Les commandes Supprimer, Coller et Collage spécial **ne peuvent pas** être annulées. Vérifiez votre sélection avant de continuer.

Vérification des informations sur le compte

Les nouvelles cibles d'installation et les cibles d'installation dont les informations sur le compte ont été modifiées auront l'état 'Vérification non déterminée'. Pour que l'installation s'effectue sur toutes les cibles souhaitées, vous devez effectuer une vérification des informations sur le compte avant de lancer la session d'installation.

Pour vérifier les informations sur le compte, sélectionnez les éléments dans la liste, puis choisissez le menu Cible et l'option Vérifier le compte ou appuyez sur le bouton Vérifier de la barre d'outils. Pour chaque élément sélectionné, l'utilitaire d'installation à distance se connecte au partage ADMIN$ de la cible et vérifie l'accès administrateur à l'ordinateur.

Si une connexion existe avec un autre compte que celui spécifié, la vérification échouera à cause d'un conflit de caractéristiques (erreur 1219). Fermez la connexion et lancez la vérification à nouveau.

Importation et exportation de la liste de cibles

Vous pouvez enregistrer la liste de cibles pour une utilisation ultérieure. Les fichiers sont stockés dans un format natif et toutes les informations sont chiffrées. Le stockage des informations importantes est ainsi sécurisé pour chaque cible.

Outre le format de fichier sécurisé utilisé à l'origine par l'utilitaire, vous pouvez importer la liste de cibles d'installation d'un fichier texte ASCII délimité par une virgule. Pour créer ces fichiers, utilisez le format suivant :

Ordinateur,compte,mot de passe,ICF <nouvelle ligne>

Ce format permet de créer des fichiers dans un logiciel adapté à la création de listes très longues (tel que Microsoft Excel). Lorsque vous générez des fichiers dans un autre éditeur, les valeurs vides pour les propriétés de Compte, Mot de passe et ICF doivent être enregistrées sous forme de doubles guillemets (“”).

Remarque : Les fichiers texte ASCII stockent le mot de passe « en clair ». Cela signifie qu'il peut être retrouvé à l'aide de n'importe quel éditeur, tel que Notepad. Nous vous recommandons donc de supprimer les fichiers ASCII après leur importation dans l'utilitaire et de stocker la liste de cibles en format de fichier natif.

Configuration du fichier de contrôle de l'installation

Vous pouvez modifier les paramètres du fichier de contrôle de l'installation (ICF) pour adapter la configuration à votre entreprise. La boîte de dialogue de configuration ICF dans l'interface d'installation à distance vous permet d'éditer l'exemple de fichier ICF, INOC6.ICF. Vous pouvez également éditer ce fichier dans un éditeur de texte.

Il existe différents moyens d'accéder au fichier ICF.

- Dans la boîte de dialogue Cible d'installation, cliquez sur le bouton '...' pour rechercher le fichier et ouvrez-le.
- Dans la barre de menus, sélectionnez Créer un fichier ICF.
- Pour modifier un fichier existant, cliquez dans la barre de menus sur Modifier un fichier ICF, sélectionnez un fichier et ouvrez-le.

La boîte de dialogue de configuration ICF s'affiche.

A propos de la boîte de dialogue de configuration ICF

La boîte de dialogue de configuration ICF affiche une liste de groupes et d'éléments dans sa partie gauche. Lorsque vous sélectionnez un groupe, une description s'affiche dans la partie droite. Pour apporter des modifications, affichez l'arborescence d'un groupe et sélectionnez un élément. Dans la partie droite de la boîte de dialogue, vous trouverez une explication sur l'élément. En dessous, vous trouverez les options que vous pouvez sélectionner pour modifier la valeur de l'élément sélectionné. Une fois les modifications effectuées, enregistrez le fichier ICF.

Exécution de sessions d'installation

Cette section décrit la session d'installation, fournissant notamment les informations sur la connexion, sur le démarrage et l'arrêt d'une session.

A propos des sessions d'installation

Une fois les cibles d'installation identifiées et les sources d'installation configurées, vous pouvez lancer une session d'installation pour chaque cible. Vous trouverez des informations sur la session d'installation dans la colonne Progression de l'installation de la liste des ordinateurs cibles, dans la partie droite de la fenêtre Installation à distance.

La session d'installation passe par les étapes suivantes :

- Vérification des informations sur le compte et connexion à l'ordinateur cible.
- Copie d'un service d'aide à l'installation dans le partage ADMIN$ de la cible.
- Installation et lancement du service d'aide.
- Recherche d'une unité locale contenant assez d'espace disque pour stocker les images de l'installation.
- Copie des images de l'installation pour le logiciel antivirus et les licences vers la cible.
- Copie des fichiers de réponse automatique (fichiers ICF) vers la cible.
- Installation du logiciel des licences à l'aide de la copie locale de l'image de l'installation.
- Installation du logiciel antivirus à l'aide de la copie locale de l'image de l'installation.
- Suppression des images de l'installation de l'ordinateur cible.
- Arrêt et désinstallation du service d'aide à l'installation.
- Suppression de l'aide à l'installation du partage ADMIN$ de la cible.
- Déconnexion de l'ordinateur cible.

Pour une meilleure performance, l'installation distante a été limitée à cinq sessions simultanées. Si vous avez sélectionné plus de cinq cibles, les sessions d'installation seront lancées pour les cinq premières cibles et les cibles restantes seront affichées avec un rappel d'état d'installation en attente. Au fur et à mesure que les sessions d'installation sont terminées, les cibles suivantes en attente sont identifiées et une nouvelle session est lancée.

Adaptation du nombre de sessions simultanées

Les utilisateurs confirmés peuvent adapter le nombre de sessions simultanées en indiquant une valeur de configuration du registre MaxConcurrentInstalls entre 1 et 10.

Vous trouverez la valeur de registre sous les clés de registre suivantes :

```
HKEY_LOCAL_MACHINE
SOFTWARE\ComputerAssociates\Antivirus\RemoteInstall
\CurrentVersion\Settings
```

Remarque : Si vous modifiez la clé de registre, vous risquez d'amoindrir la performance de l'ordinateur local et du réseau. Ne modifiez cette valeur que si vous disposez de suffisamment de mémoire, d'un processeur assez puissant et d'une bande passante de réseau adéquate.

Enregistrement dans le journal de sessions d'installation

En cas d'erreur inattendue, il est recommandé de déterminer l'opération qui était en cours au moment de l'erreur. L'utilitaire d'installation à distance peut générer des journaux détaillés du processus d'installation.

Pour activer les journaux d'installation, sélectionnez le menu Options, puis Activer la journalisation. Lorsque cette option est activée, un répertoire nommé LOG est créé sous le répertoire dans lequel l'utilitaire est exécuté.

Lorsque l'installation est en cours, un fichier est créé pour chaque cible d'installation. Chaque nom de fichier journal est composé du *nom_de_l'ordinateur* de la cible et d'une extension *.log*. Ces fichiers journaux contiennent les informations détaillées sur les opérations en cours sur l'ordinateur local ainsi que les opérations effectuées par le service d'aide à l'installation à distance.

Lancement des sessions d'installation

Vous pouvez effectuer une installation sur certaines ou sur toutes les cibles de la liste. Pour lancer des sessions d'installation, sélectionnez les éléments dans la liste, puis choisissez le menu Cible et l'option Lancer l'installation ou appuyez sur le bouton Installer vers les cibles de la barre d'outils.

L'utilitaire d'installation à distance vérifie les informations sur les comptes. Lorsque la vérification est réussie, il modifie l'état de chaque cible en Installation en attente. Une fois les informations sur le compte vérifiées, l'installation est lancée pour les cinq premières cibles en attente (leur état passe à Installation).

Pendant l'installation, la colonne Progression de l'installation affiche l'état actuel de l'installation.

Lorsque l'installation a réussi, la colonne d'état affiche Installation réussie. Si l'installation échoue, la colonne d'état indique 'Echec de l'installation [###]', ### étant le code de l'erreur.

Remarque : Pour obtenir des informations supplémentaires sur les codes d'erreur, utilisez la commande Windows NET HELPMSG.

Arrêt de sessions d'installation

Vous pouvez arrêter les sessions des cibles dont l'état est Installation ou Installation en attente avant qu'elles ne soient terminées. Pour arrêter des sessions d'installation, sélectionnez les éléments dans la liste, puis choisissez le menu Cible et l'option Arrêter l'installation ou appuyez sur le bouton Arrêter l'installation de la barre d'outils.

Les éléments en attente verront leur état passer à Vérification achevée avec succès et l'installation n'aura pas lieu.

Les éléments en cours d'installation verront leur état passer à Installation interrompue par l'utilisateur, ce qui signifie que l'installation a été arrêtée manuellement. Le processus d'installation peut être interrompu jusqu'au moment où le programme d'installation est démarré sur la cible.

Remarque : Les requêtes Arrêter l'installation pour les ordinateurs ayant l'état Installation ne peuvent être traitées immédiatement. La session sera interrompue lorsqu'elle atteindra un état lui permettant d'effectuer un arrêt.

Désinstallation de l'utilitaire d'installation à distance

Vous pouvez supprimer l'utilitaire d'installation à distance du panneau de configuration à l'aide de l'option Ajout/Suppression de programmes. En outre, vous disposez d'une option vous permettant de désinstaller également le logiciel antivirus.

Installation à distance sur un ordinateur Windows 9x

Vous pouvez installer à distance le logiciel antivirus de Computer Associates sur des ordinateurs Windows 9x en utilisant l'utilitaire setup.exe dans un script de connexion. L'utilitaire vérifie que le logiciel est installé sur l'ordinateur.

Utilisation de Setup.exe pour Windows 9x

Pour effectuer une installation à distance sur un ordinateur Windows 9x, insérez setup.exe dans le script de connexion à l'aide d'une des commandes suivantes (setup.exe est situé dans …/bin/eav_s.win) :

Option	Description
/N	Vérifie si une version du programme est déjà installée sur l'ordinateur. Si la version sur l'ordinateur est supérieure ou égale à la version actuelle que vous souhaitez installer, le programme ne sera pas réinstallé.
/N-	Le programme que vous souhaitez installer le sera, quelle que soit la version installée sur l'ordinateur.

Exemples

La commande suivante vérifie la version installée sur l'ordinateur.

setup.exe /N

La commande suivante installe la version souhaitée.

setup.exe /N-

Chapitre 10

Utilisation de disquettes de secours pour Windows 9x

Ce chapitre fournit des informations sur l'utilisation de la fonction Disquette de secours pour récupérer d'une infection sur des stations de travail Windows 9x. La plupart des infections peuvent être gérées en utilisant l'analyseur local. Cependant, si un ordinateur Windows 9x est infecté au niveau du secteur d'amorçage ou si l'infection a endommagé les fichiers de la zone de disque critique, utilisez la fonctionnalité Disquette de secours.

Utilisation de la fonctionnalité Disquette de secours

La fonctionnalité Disquette de secours vous permet d'effectuer une sauvegarde rapide des zones critiques du disque d'un poste de travail Windows 9x. Lorsque les fichiers critiques situés sur le disque dur du poste de travail sont corrompus par une infection, vous pouvez utiliser la disquette de secours pour remettre l'ordinateur dans son état d'origine et restaurer ces fichiers.

Informations sur la disquette de secours

La disquette de secours protège les zones critiques du disque d'un poste de travail dans la mesure où elle sauvegarde les fichiers système importants.

Utilisation de différents moteurs pour la disquette de secours

Lorsque vous créez une disquette de secours, vous pouvez choisir parmi les différents moteurs disponibles. Les fonctionnalités disponibles sur la disquette de secours dépendent du moteur utilisé pour créer la disquette. Ainsi, une disquette de secours créée pour le moteur Antivirus n'a pas les mêmes fonctionnalités qu'une disquette de secours créée pour un moteur Vet.

Quelle que soit l'option de moteur utilisée, la disquette fournit les informations de sauvegarde et de récupération dont vous avez besoin.

Disquette de secours avec un moteur Antivirus

Une disquette de secours créée pour le moteur Antivirus garantit la protection des zones critiques du disque. Cette protection couvre :

- l'enregistrement d'amorçage principal,
- Secteur d'amorçage
- la table des partitions,
- les paramètres CMOS,
- le fichier système E/S,
- Fichier système Windows 9x
- Fichier shell Windows 9x (COMMAND.COM).

Cette disquette de secours est amorçable et contient une copie de INOCUCMD.EXE, l'analyseur en mode commande.

Disquette de secours avec un moteur Vet

Une disquette de secours créée pour le moteur Vet contient une copie de vos modèles d'unités ainsi que d'autres informations concernant le système. Elle inclut RESCUE.EXE qui contient une fonctionnalité de récupération à utiliser avec le moteur Vet. Dans la version 7.0 ou supérieure, cette disquette de secours est amorçable.

Utilisez le programme RESCUE.EXE uniquement si vous démarrez votre ordinateur en mode DOS. Ne le lancez pas à partir de Windows ni à partir d'une invite de Windows. Si vous êtes dans Windows, sélectionnez Démarrer, puis Arrêter. Sélectionnez ensuite l'option Redémarrer l'ordinateur en mode MS-DOS.

Conception et maintenance d'une disquette de secours

Vous pouvez créer une disquette de secours seulement après avoir installé le logiciel antivirus de Computer Associates et redémarré votre ordinateur afin que les modifications soient prises en compte.

Création d'une disquette de secours

Pour lancer l'assistant de disquette de secours, cliquez sur le bouton Disquette de secours dans la barre d'outils de l'analyseur local. Utilisez l'option Créer nouvelle disquette de secours pour formater la disquette et enregistrer les informations importantes du disque du poste de travail.

Important ! *Nous vous recommandons vivement de créer une disquette de secours. En cas de détection d'une infection, cette précaution supplémentaire peut être essentielle pour le processus de récupération. Une fois qu'une disquette de secours est créée, indiquez clairement le poste de travail auquel elle se rapporte, puis rangez-la dans un endroit sûr.*

Options de mise à jour et de vérification

Lorsque vous avez créé une disquette de secours, vous pouvez utiliser les options de vérification et de mise à jour de l'assistant de disquette de secours afin d'actualiser les informations du disque pour le poste de travail concerné. Si vous disposez déjà d'une disquette de secours, vous pouvez utiliser l'option Mettre à jour. Cette option est plus rapide que l'option Créer car elle permet de mettre la disquette à jour sans qu'un reformatage soit nécessaire. L'option Vérifier vous permet de déterminer si des modifications ont été apportées aux informations de la disquette.

Mise à jour de la disquette de secours

Il est primordial que vous disposiez d'une disquette de secours à jour pour votre poste de travail. Cette mesure préventive doit être appliquée régulièrement.

Vous devez créer une disquette de secours ou mettre à jour votre disquette dans les cas suivants :

- Lorsque vous modifiez vos informations CMOS (moteur Antivirus uniquement).
- Lorsque vous modifiez la configuration de votre matériel.
- Lorsque vous modifiez vos fichiers système, notamment si vous ajoutez de nouvelles lignes à AUTOEXEC.BAT lors de l'installation d'un produit (moteur Antivirus uniquement).
- Lorsque vous mettez à niveau votre système d'exploitation.

Contenu de la disquette de secours pour un moteur Antivirus

La création d'une disquette de secours pour le moteur Antivirus a les répercussions suivantes :

- La disquette de secours est formatée et rendue amorçable.
- Une copie des fichiers INOCUCMD.EXE et VIRSIG.DAT est effectuée.
- Le fichier HIMEM.SYS est copié.
- Un fichier CONFIG.SYS est généré avec les deux lignes suivantes :
  - FILES=40
  - DEVICE=HIMEM.SYS
- AUTOEXEC.BAT est créé pour invoquer INOCUCMD.EXE.
- Une étiquette sur laquelle est inscrit le volume est collée sur la disquette de secours.
- Les informations de la zone de disque critique sont sauvegardées.

Lorsque la disquette de secours est créée, les informations de la zone de disque critique suivantes sont enregistrées sur la disquette.

Fichier	Informations relatives à la zone de disque critique
AUTOEXEC.SIG	Fichier AUTOEXEC.BAT
BIOS.SIG	Fichier système BIOS
BOOTSECT.SIG	Secteur d'amorçage
CMOS.SIG	Paramètres CMOS
CONFIG.SIG	Fichier CONFIG.SYS
DOS.SIG	Fichier système Windows 9x
INFO.SIG	Informations concernant ces fichiers et leur emplacement sur le disque dur
PARTSECT.SIG	Table des partitions
SHELL.SIG	Fichier shell Windows 9x (COMMAND.COM).

Remarque : Cette liste vous donne une idée du type d'information sauvegardée. D'autres fichiers associés ne figurant pas dans la liste sont enregistrés sur la disquette de secours.

Récupération à la suite d'un virus informatique

Si une infection est détectée dans la mémoire ou si le programme vous invite à redémarrer le système, utilisez la disquette de secours.

Utilisation des options de la disquette de secours

Utilisez les options suivantes avec une disquette de secours créée pour le moteur Antivirus. Si vous avez besoin de la disquette de secours pour réinitialiser votre ordinateur, les options disponibles sont décrites ci-dessous. Une fois que vous avez choisi une option, suivez les instructions s'affichant à l'écran.

Analyser le secteur d'amorçage et supprimer tout virus détecté

L'option Analyser le secteur d'amorçage et supprimer tout virus détecté vous permet de déterminer si des fichiers du secteur d'amorçage sont endommagés et, le cas échéant, de les restaurer à partir de la disquette de secours.

Comparer/restaurer le secteur d'amorçage

L'option Comparer/Restaurer le secteur d'amorçage vous permet de déterminer si des fichiers de la zone de disque critique du disque dur ont été altérés par une infection et, le cas échéant, de les restaurer à partir de la disquette de secours.

Remarque : Après avoir utilisé la disquette de secours pour restaurer un poste de travail, utilisez l'analyseur local pour vérifier s'il n'y a plus d'infection.

Consultez l'aide en ligne pour en savoir plus sur les procédures d'utilisation de la disquette de secours.

Des informations spécialisées sur la suppression d'infections sont disponibles sur le site du Centre d'information sur les virus de Computer Associates à l'adresse suivante :

`http://www.ca.com/virusinfo/`

Chapitre

11 Utilisation du gestionnaire Alert

Ce chapitre décrit l'utilisation du composant Gestionnaire Alert. Il contient des informations sur les paramètres Alert intégrés à l'interface graphique utilisateur du logiciel antivirus de Computer Associates. Alert fonctionne sous Windows NT, Windows XP, Windows 2000 et Windows 2003. Ce chapitre décrit également l'utilisation du Gestionnaire Alert local sous UNIX et OS X.

Introduction à Alert

Alert est un système de notification qui envoie des messages à des personnes de votre organisation par différents moyens de communication. Des messages peuvent être envoyés à l'administrateur du système, à un technicien ou à toute autre personne située à l'intérieur ou à l'extérieur des bureaux. Une personne ou des groupes de personnes dans différents segments du réseau peuvent ainsi être informés.

Pour créer des messages d'alerte, vous devez indiquer à Alert quelles sont les informations à communiquer. Par exemple, si vous utilisez le système de récepteur d'appels, vous devez indiquer à Alert quel numéro de récepteur d'appel appeler et vous devez fournir des informations sur votre modem. Toutes ces informations doivent être configurées dans le programme Alert de votre serveur.

Alert ne crée pas ses propres messages. Il achemine tous les messages, les avertissements et toutes les erreurs qu'il reçoit de différentes sources, notamment du logiciel antivirus de Computer Associates et distribue ces messages d'alerte vers des destinations spécifiques. Par exemple, le logiciel antivirus de Computer Associates génère des messages d'avertissement lorsqu'un virus est détecté. Ces messages d'avertissements sont transmis à Alert qui envoie alors une notification.

Les alertes peuvent être envoyées selon les méthodes suivantes.

- Diffusions
  Des diffusions d'alerte peuvent être envoyées à des ordinateurs définis.
- Récepteur d'appels
  Numérique et alphanumérique.

- Messagerie
  Microsoft Exchange ou Lotus Notes

  Remarque : Pour configurer la messagerie MS Exchange, vous pouvez utiliser soit le programme d'installation Alert, soit l'option de configuration de la messagerie Exchange dans le menu du gestionnaire Alert pour son utilisation avec Alert.
- Rapport d'incidents
  Une alerte peut être imprimée par le biais d'une file d'attente d'imprimante sur votre réseau.
- SMTP (Simple Mail Transfer Protocol)
  Pour l'envoi de messages électroniques via Internet.
- Gestionnaires SNMP (Simple Network Management Protocol)
  Exemple : NetWare Management System (NMS) et HP OpenView.
- Notification locale et distante du journal d'événements Windows NT et Windows 2000.
- Option Unicenter TNG
  Envoyer un message à la console TNG et/ou au référentiel WorldView lorsqu'une alerte est générée.
- eTrust Audit
  Envoyer un message à eTrust Audit Viewer ou Security Monitor lorsqu'une alerte est générée.

Composants de base

Les composants de base d'Alert sont brièvement décrits ci-dessous.

- Service Alert
  Service responsable de la réception, du traitement et de la distribution des messages Alert.
- ALBUILD.DLL
  Fichier .DLL qui agit en tant que canal entre Alert et d'autres applications. Il doit être situé dans le répertoire d'installation où le logiciel antivirus de Computer Associates est installé.
- Gestionnaire Alert
  Vous permet de configurer l'envoi des messages Alert.

Fonctions d'Alert

Les fonctionnalités Alert vous permettent d'accéder aux informations les plus récentes sur vos systèmes et de recevoir des messages des clients.

- Gestion à distance et configuration du service Alert.
- Les alertes des clients peuvent être envoyées en utilisant l'IP en plus du protocole IPX standard.
- Messages contenant le chemin complet de tout fichier contenant un virus.

Exécution du gestionnaire Alert

Vous pouvez exécuter Alert à partir du groupe de programmes du logiciel antivirus de Computer Associates en sélectionnant le Gestionnaire Alert. Ce dernier vous permet de sélectionner un ordinateur distant afin de gérer les messages d'Alert. Avant de démarrer Alert, vous devez établir une connexion de compte de service et sélectionner un ordinateur distant.

Configuration d'Alert

Alert vous permet de configurer des paramètres par défaut utilisés par toutes les applications utilisant le service Alert. Vous pouvez également saisir des informations de configuration spécifiques pour une application individuelle, qui remplacent la configuration Alert par défaut. Chaque application qui utilise Alert est affichée en tant qu'élément de l'arborescence des fonctions dans la partie gauche.

Création et édition des configurations de port

L'objet Ports, situé sous l'objet Configuration, contient des profils de port de communication. Les configurations de ports suivants sont utilisées par le récepteur d'appel et par n'importe quelle fonction utilisant un accès port série :

- Port
  Nom du port de communication à partir duquel le message du récepteur d'appels doit être diffusé.
- Vitesse de transmission
  Vitesse de transmission utilisée par votre modem.
- Parité
  Paramètre de la parité, paire ou impaire de votre modem.
- Bits de données
  Nombre de bits de données que votre modem utilise (7 ou 8).
- Bits d'arrêt
  Nombre de bits de données que votre modem utilise (1 ou 2).

Utilisation de l'option de diffusion d'Alert

Les diffusions Alert peuvent être envoyées à des utilisateurs de réseau ou des groupes. Pour en savoir plus sur l'ajout de destinataires de diffusion, reportez-vous à l'aide en ligne Alert.

Utilisation du récepteur d'appels

L'option récepteur d'appels permet d'envoyer un message numérique ou alphanumérique. Lorsque vous sélectionnez l'option récepteur d'appels, la liste actuelle des destinataires s'affiche. Pour en savoir plus sur l'ajout de destinataires au récepteur d'appels, reportez-vous à l'aide en ligne d'Alert.

Remarque : Vous devez configurer vos ports de communication avant de pouvoir ajouter des destinataires au récepteur d'appels.

Remarque : Lors de l'envoi d'une page alphanumérique, veuillez consulter le manuel de votre récepteur d'appels pour connaître les paramètres de modem corrects.

Interprétation du message du récepteur d'appels

Il existe plusieurs messages semblables à ceux ci-dessous pouvant être envoyés à un récepteur d'appels alphanumérique. Les mots qui s'affichent en italique seront remplis par le nom de l'utilisateur, l'adresse de la station de travail, le nom du chemin et du fichier, celui du virus ou celui du serveur.

- Virus d'amorçage détecté (*nom d'utilisateur* à *l'adresse du poste de travail*)
- Le gestionnaire a détecté un virus [*nom du virus*] dans [*chemin*] (*nom d'utilisateur* à *l'adresse du poste de travail*)
- Fichier infecté [*nom du serveur/chemin*] détecté
- Fichier infecté [*chemin*] accédé par *nom d'utilisateur* à *l'adresse du poste de travail*

Utilisation de l'option SMTP

L'option SMTP vous permet de fournir des informations afin qu'Alert envoie des messages en utilisant SMTP (Simple Mail Transfer Protocol). Vous pouvez entrer une adresse électronique pour un destinataire et envoyer le message via Internet.

Utilisation de l'option SNMP

L'option SNMP vous permet d'envoyer une « interruption » SNMP (message) à un gestionnaire SNMP. NetWare Management System (NMS), HP OpenView et IBM Netview sont des exemples de gestionnaires SNMP.

L'aide en ligne d'Alert décrit les zones SNMP de l'écran de configuration SNMP et explique comment les utiliser.

Utilisation du ticket d'incident

Les tickets d'incident sont utilisés pour alerter les utilisateurs par le biais d'un document imprimé.

Utilisation de la messagerie électronique

L'option Messagerie est utilisée pour envoyer des messages électroniques à des utilisateurs définis.

Important ! *Microsoft Exchange ou Lotus Notes Client doit être installé sur votre ordinateur pour pouvoir envoyer des messages ou pour entrer des données de configuration sur cet écran. Consultez la documentation Windows correspondante pour obtenir plus de détails sur l'installation de votre compte de messagerie électronique.*

Utilisation de l'option Unicenter TNG

L'option Unicenter TNG vous permet d'envoyer un message à la console Unicenter TNG et au référentiel WorldView lorsqu'une alerte est générée.

Remarque : L'application Alert doit fonctionner sur l'ordinateur du gestionnaire d'événements ainsi que sur celui où se trouve WorldView.

Reportez-vous à l'aide en ligne d'Alert pour plus d'informations sur la façon d'envoyer un message à la console Unicenter TNG et/ou au référentiel WorldView.

Utilisation de l'option eTrust Audit

L'option eTrust Audit permet d'envoyer un message à la visionneuse eTrust Audit ou au système de surveillance lorsqu'une alerte est générée. Utilisez la boîte de dialogue Destinataires (Routeurs) pour ajouter un domaine ou un serveur individuel à la liste de destinataires.

Priorité de l'événement d'application

Toutes les applications appelant Alert déterminent l'une des priorités d'événement ci-dessous :

- Critique
- Avertissement
- Information

Exemples de scénarios TNG Alert

Des exemples de personnalisation des messages Alert envoyés à la console Unicenter TNG sont présentés ci-dessous.

Exemple 1

Si vous souhaitez envoyer des alertes pour information à la console Unicenter TNG en utilisant un texte bleu, par exemple, configurez le destinataire comme suit :

Option	Paramètre
Priorité de l'événement d'application	Information (affichage uniquement)
Gravité	Information
Couleur	Bleu
Envoyer à la console	Sélectionné
Dans le groupe TNG WorldView :	
Mettre à jour l'état de l'objet dans le référentiel WorldView	Sélectionné

Exemple 2

Si vous souhaitez envoyer des alertes d'erreur à la console Unicenter TNG en utilisant un texte rouge et mettre à jour l'état de l'objet dans le référentiel WorldView, configurez le destinataire comme suit :

Priorité de l'événement	Description
Priorité de l'événement d'application	Critique (affichage uniquement)
Gravité	Erreur
Couleur	Rouge
Envoyer à la console	Sélectionné
Dans le groupe TNG WorldView :	
Mettre à jour l'état de l'objet dans le référentiel WorldView	Sélectionné

Test des destinataires

Le bouton Test de la barre d'outils vous permet de tester n'importe quelle fonction de messagerie d'Alert sans condition d'« alarme » réelle. Consultez l'aide en ligne d'Alert pour obtenir des informations sur ces tests.

Remarque : Vous devez tester toutes les fonctionnalités à la fin de la configuration. Pensez à avertir les destinataires d'Alert qu'un test va avoir lieu.

Activité Alert et journaux d'événements

Si le statut actuel d'Alert s'affiche lorsque le résumé Alert est sélectionné dans le groupe Activité, une liste historique est stockée dans le journal d'activité. De même, chaque message généré par Alert est stocké dans le journal des événements. Vous pouvez afficher, imprimer ou effacer ces journaux. Reportez-vous à l'aide en ligne Alert pour plus d'informations.

Destination du journal d'événements

Vous pouvez configurer la destination du journal d'événements pour qu'Alert mette l'événement d'un serveur défini dans le journal d'événements de cet ordinateur.

Utilisation d'Alert avec le logiciel antivirus

Cette section décrit les options intégrées à l'interface graphique utilisateur du logiciel antivirus de Computer Associates qui vous permet de définir les options pour la gestion des informations qui sont transmises au gestionnaire Alert sur un ordinateur local. Utilisez ces options conjointement avec Alert.

Ces options vous permettent de personnaliser les informations de notification fournies avec Alert, pour réduire le trafic de messages et la distribution de notifications qui ne sont pas importantes.

Les options Alert définies sur l'ordinateur local s'appliquent à cet ordinateur. Les administrateurs peuvent définir les règles Alert pour plusieurs ordinateurs grâce à l'affichage de l'administrateur.

Les onglets suivants sont disponibles pour les boîtes de dialogue Paramètres d'Alert :

- Règles (uniquement pour les utilisateurs ayant accès à l'affichage de l'administrateur)
- Rapport
- Filtre

Accès aux options Paramètres Alert

Vous pouvez accéder aux options Paramètres Alert à partir de la barre d'outils de l'analyseur local en cliquant sur le bouton Paramètres Alert.

Utilisation des options de rapports Alert

Les options de rapports Alert vous permettent de spécifier où envoyer les informations de notification et de gérer la fréquence d'envoi des messages.

Utilisation des options Rapport destiné à

Les options Rapport destiné à vous permettent de définir l'endroit où envoyer les informations de rapport Alert.

Gestionnaire Alert local	Permet d'envoyer les informations de notification au composant du gestionnaire Alert sur l'ordinateur local.
Journal d'événements	Envoie des notifications au journal d'événements système de l'ordinateur local.

Transmettre à

Utilisez cette option pour envoyer une notification à un nom d'ordinateur déterminé sur lequel le logiciel antivirus de Computer Associates est installé. Lorsque l'ordinateur spécifié a reçu la notification, l'information est gérée selon les paramètres Alert de cet ordinateur. L'ordinateur auquel la notification est transmise peut alors distribuer des messages à d'autres ordinateurs.

Cette option peut être utilisée pour transmettre l'information selon une hiérarchie, par exemple, ou pour envoyer des informations à des personnes clés.

Nom de l'ordinateur

Définit le nom de l'ordinateur auquel vous souhaitez transmettre les informations de notification. Le logiciel antivirus de Computer Associates doit être installé sur cet ordinateur.

Gestion des critères du rapport

Les options Critères du rapport vous permettent de gérer la fréquence de rapport des messages du journal d'événements généraux, selon les paramètres de l'option Rapport destiné à. Les options File d'attente et Délai expiré après fonctionnent conjointement. Le rapport des messages se fait en vertu du premier des délais atteint.

Enregistrements en file d'attente

L'option File d'attente permet de définir un nombre d'enregistrements de messages à rassembler dans le journal d'événements généraux. Lorsque les limites sont atteintes, l'information est rapportée comme défini sous Rapport destiné à.

Délai expiré après

Une fois écoulé, le nombre de minutes spécifié, les informations du journal d'événements généraux font l'objet d'un rapport selon les paramètres définis sous Rapport destiné à, même si le nombre de messages n'a pas atteint le nombre défini pour la file d'attente.

Ignorer les enregistrements datant de plus de

Tout enregistrement dans le journal d'événements généraux plus ancien que le nombre de jours défini n'est pas inclus dans un rapport.

Utilisation des options du filtre Alert

Les options du filtre Alert permet de gérer les niveaux de gravité de la notification et de personnaliser des jeux de messages de notification à rapporter selon les différents composants de service de l'antivirus de Computer Associates. Ces options vous permettent de déterminer les types de messages qui doivent être transmis au gestionnaire Alert. Vous pouvez utiliser Notification par niveau de gravité ou Notification personnalisée.

Notification par niveau de gravité

Vous pouvez choisir d'envoyer des notifications en fonction de leur niveau de gravité :

Informatif – Ce type de messages fournit des informations sur les événements, par exemple, si le service a démarré ou est arrêté et si aucune infection n'a été détectée.

Avertissement – Ce message de seconde priorité fournit des informations d'avertissement non cruciales.

Critique – Message de priorité la plus élevée. Le message nécessite une attention immédiate une fois enregistré. Le message peut signifier qu'une infection a été détectée ou qu'un problème a été identifié au niveau du service, par exemple, qu'une erreur s'est produite lors du chargement d'un moteur.

Notification personnalisée

L'option de notification personnalisée permet de personnaliser les messages de notification de différents services.

Sélectionnez un des modules de service disponibles et sélectionnez un des messages de notification associés d'une liste. Ces options vous permettent de définir les messages que vous souhaitez envoyer en tant que notifications. Ceci permet de limiter les messages qui sont rapportés par Alert sur les systèmes Windows ou par le script défini par l'utilisateur sur des systèmes UNIX ou OS X. Pour chaque module de service, vous pouvez sélectionner les messages spécifiques qui doivent être envoyés.

Les modules de service suivants sont disponibles :

- **Analyseur local –** Pour les analyses locales.
- **Serveur temps réel –** Pour le moniteur temps réel.
- **Serveur de jobs –** Pour le job d'analyse planifié et l'agent planifiant la mise à jour des signatures.
- **Serveur Admin –** Pour l'agent du serveur Admin.
- **Rapport de virus –** Pour les rapports d'antivirus et de domaines à partir d'ordinateur découverts par le serveur Admin.

Liste des messages de notification

Une liste de messages différente est disponible pour chaque service sélectionné. Le niveau de gravité de chaque message est répertorié avec le texte du message.

Vous pouvez utiliser cette liste pour sélectionner uniquement les messages que vous souhaitez transmettre à Alert et qui doivent être rapportés par différents moyens de communication définis dans les options de configuration d'Alert. En sélectionnant les types de messages, vous pouvez réduire le trafic de messages superflus dans le réseau. Seuls les messages que vous définissez comme importants et qui nécessitent une notification seront transmis.

Utilisation des règles Alert dans l'affichage de l'administrateur

Les mêmes options Paramètres Alert disponibles à partir de l'analyseur local le sont aussi pour des utilisateurs ayant les droits d'accès nécessaires pour l'affichage de l'administrateur.

Dans cet affichage, sous Paramètres de configuration et Règles appliquées, vous pouvez sélectionner la catégorie Alert pour qu'elle affiche les options des règles Alert.

Utilisez les options de règles Alert de la même façon que vous le feriez avec les paramètres d'autres options de règle dans l'affichage de l'administrateur. Créez les paramètres que vous souhaitez utiliser et appliquez-les aux conteneurs dans l'arborescence de l'organisation. Reportez-vous au chapitre « **Utilisation de l'affichage de l'administrateur** » pour obtenir plus d'informations sur la gestion des options de règles.

Gestionnaire Alert local sur les systèmes UNIX et OS X

Sous Unix et OS X, vous pouvez utiliser le paramètre Gestionnaire Alert local pour envoyer des informations de notification à un script shell que vous pouvez écrire vous-même. Le script peut alors effectuer les actions que vous aurez précisées, comme envoyer un courrier électronique à une adresse définie lorsque le logiciel antivirus de Computer Associates détecte un virus.

Le script **InoSetAlert** vous permet de définir le nom du script que vous souhaitez exécuter lorsqu'une alerte est générée. Par exemple, la commande ci-dessous permet d'utiliser **/home/myfiles/myscript** en tant que script d'alerte :

```
InoSetAlert /home/myfiles/myscript
```

La commande suivante arrête cette fonctionnalité :

```
InoSetAlert
```

Sur les systèmes OS X, vous pouvez indiquer un script à exécuter dans l'écran des préférences de eTrust Antivirus, disponible sous l'écran des préférences système.

Le logiciel antivirus de Computer Associates envoie alors des informations spécifiques au script qui les reçoit sous forme d'argument de script standard, par exemple, $1, $2, etc. Ces arguments sont, dans l'ordre :

1. Heure de l'événement (une chaîne, telle que « 10:15:20 22 jan. 2001 »).
2. Numéro de code de l'événement. Le numéro pour une détection antivirus en temps réel est 26.
3. Gravité de l'événement : (1 = Information, 2 = Avertissement, 3 = Erreur).
4. Nom du nœud où l'événement est survenu.
5. Texte du message généré par le logiciel antivirus de Computer Associates.

Chapitre

12

Intégration avec Unicenter

Ce chapitre décrit comment le logiciel antivirus de Computer Associates intègre Unicenter TNG aux plates-formes Windows NT, Windows 2000 ou Windows 2003 et quelles sont les options d'analyse disponibles pour gérer un ordinateur à partir de Business Process View dans WorldView.

En tant qu'option Unicenter TNG, le logiciel antivirus de Computer Associates est compatible avec Unicenter TNG sur les serveurs d'entreprise, locaux et de groupes de travail. La plate-forme Unicenter TNG requise est déterminée par le système d'exploitation du serveur.

- Vous devez avoir installé Unicenter TNG pour Windows NT, 2000 ou 2003 sur tous les serveurs d'entreprise, locaux et de groupes de travail Windows NT ou 2000.
- La version d'Unicenter TNG qui correspond au matériel et au système d'exploitation des serveurs d'entreprise, locaux ou de groupes de travail UNIX doit être installé sur ces serveurs.

Utilisation de WorldView

Avec Unicenter TNG vous pouvez utiliser WorldView pour afficher, organiser et gérer les ordinateurs dans votre réseau antivirus.

WorldView est composé de plusieurs outils qui vous aideront à gérer vos ressources informatiques. WorldView offre également le service Auto Discovery (Auto-découverte), le référentiel d'objets (Common Object Repository), l'assistant des classes, l'interface utilisateur graphique 3D monde réel (Real World), l'interface utilisateur graphique carte 2D (cartographie), des vues métier (Business Process Views ou BPV) et plusieurs outils de navigation.

Fonction Auto Discovery

La fonction Auto Discovery (découverte automatique) détecte automatiquement tous les périphériques de votre réseau, les identifie et les ajoute au référentiel d'objets (Common Object Repository) d'Unicenter TNG comme des objets gérés.

Une fois définis, ils sont affichés comme faisant partie de votre configuration de réseau. Vous pouvez les afficher et les contrôler avec l'interface 3D monde réel, la carte 2D et d'autres interfaces.

Interface monde réel (Real World)

L'interface monde réel (Real World) offre un plan en 3 dimensions permettant de visualiser les ressources distribuées dans votre système. Grâce à une animation en trois dimensions, vous pouvez afficher des objets qui apparaissent de façon plus réaliste et qui sont plus faciles à gérer. C'est une manière simple et intuitive de personnaliser l'affichage de votre réseau antivirus.

Carte 2D

La carte 2D est un affichage graphique en deux dimensions de la structure logique de votre entreprise. Cette interface vous permet de positionner des objets sur des plans géographiquement complets. Vous serez en mesure de placer vos ressources dans une hiérarchie logique de réseaux, de sous-réseaux et de segments basés sur leur relation réciproque.

Vues métier (BPV)

Les vues métier (Business Process Views ou BPV) d'Unicenter TNG permettent d'afficher de manière simple et concise le groupage logique d'objets gérés qui correspondent à un processus spécifique. Cet outil vous permet de créer un affichage de toutes vos ressources antivirus de la manière la plus adaptée à votre site. Vous pouvez surveiller la condition et l'état d'objets, définir des déclencheurs et des seuils et intercepter des messages. Ces affichages peuvent vous aider à détecter et à prévenir des problèmes et fournissent un affichage graphique immédiat de la source de tout problème.

Assistant des classes

L'assistant des classes dans WorldView d'Unicenter TNG est une fonction conviviale qui vous permet de créer ou de modifier des classes sans avoir à écrire de code. L'assistant des classes vous guide à travers le processus de définition de propriétés, de création de menus contextuels pour lancer des applications ou de définition de l'apparence d'objets en deux ou en trois dimensions.

Explorateurs WorldView

Unicenter TNG permet d'afficher de différentes manières les informations stockées dans le référentiel d'objets (Common Object Repository). Les explorateurs mis à votre disposition sont : l'explorateur des classes, l'explorateur des objets, l'explorateur Topologie et ObjectView. Vous pouvez personnaliser n'importe quel affichage de votre entreprise selon sa structure logique. Vous pouvez les visualiser sous forme d'icônes en deux ou en trois dimensions ou sous forme de texte grâce à l'un de ces navigateurs.

Pour plus d'informations sur WorldView, reportez-vous à la documentation relative à Unicenter TNG.

Préparation de l'intégration TNG

Pour utiliser le logiciel antivirus de Computer Associates avec Unicenter TNG, vous devez importer les informations de classes appropriées dans le référentiel Unicenter TNG. Procédez à l'importation après avoir exécuté Auto Discovery (Auto-découverte) sur votre réseau. Ensuite, vous pouvez utiliser l'utilitaire InoUpTNG pour effectuer l'affichage d'une vue métier (BPV) sur votre réseau antivirus.

Utilisation de TRIX pour l'importation dans le référentiel

Le programme d'importation/exportation du référentiel (TRIX) vous permet d'utiliser le script d'importation fourni avec l'antivirus de Computer Associates. Une classe Antivirus est ainsi créée.

Vous pouvez accéder au programme TRIX à partir du menu Démarrer et du groupe de programmes WorldView d'Unicenter TNG. Sélectionnez l'option d'importation/d'exportation du référentiel pour lancer l'interface TRIX. Ensuite, utilisez TRIX pour ouvrir le fichier script TRIX0.TNG et l'importer dans le référentiel. Ce fichier script d'importation est situé dans le répertoire où se trouve le logiciel antivirus de Computer Associates.

Vous devez connaître le nom du référentiel auquel vous souhaitez vous connecter et utiliser un ID utilisateur et un mot de passe valides pour pouvoir y accéder.

Vous pouvez également utiliser TRIX en entrant la commande suivante lorsque l'invite apparaît :

```
trix
```

TRIX.EXE est alors lancé.

Pour plus d'informations sur TRIX, reportez-vous à la documentation d'Unicenter TNG.

Utilisation de InoUpTNG pour effectuer un affichage

Lorsque l'importation a été effectuée dans le référentiel, lancez l'utilitaire InoUpTNG pour créer la BPVantivirus et la peupler avec des ordinateurs de votre réseau antivirus.

InoUpTNG découvre les ordinateurs de votre réseau en se basant sur les informations relatives aux ordinateurs contenues dans la base de données TNG et les informations de découverte de sous-réseaux contenues dans la base de données du serveur Admin. L'utilitaire utilise les informations de ces deux sources pour alimenter le référentiel WorldView.

Le réseau TNG doit avoir été découvert et un ordinateur doit déjà exister dans le référentiel TNG avant d'exécuter InoUpTNG. La découverte du sous-réseau du serveur Admin doit également avoir été effectuée. En se basant sur les informations relatives à l'ordinateur de la base de données du serveur Admin, InoUpTNG parcourt le référentiel TNG à la recherche d'ordinateurs correspondants.

Si InoUpTNG trouve un ordinateur correspondant dans la base de données TNG, il crée un objet Antivirus et le relie à l'ordinateur. Ensuite l'objet apparaît dans la BPV (Business Process View). Cet affichage permet de visualiser tous les ordinateurs qui exécutent des instances du logiciel antivirus de Computer Associates dans votre réseau. Si votre réseau comprend plusieurs serveurs Admin, l'utilitaire les découvrira.

Inversement, si l'ordinateur ne se trouve pas encore dans la base de données TNG, alors aucun objet ne sera créé pour ce dernier et il n'apparaîtra pas dans la vue.

Reportez-vous à la section « **Utilisation de sous-réseaux** » du chapitre « **Utilisation de l'affichage de l'administrateur** » pour plus d'informations sur la découverte de sous-réseaux.

Gestion des options antivirus dans WorldView

Après avoir créé une BPV (Business Process View) de votre réseau antivirus, vous pouvez gérer les options d'analyse pour les ordinateurs de cette vue.

Intégration avec WorldView

Lorsque vous cliquez avec le bouton droit de la souris sur un ordinateur figurant dans la vue, les options standard Unicenter pour la gestion d'objets deviennent disponibles. De plus, vous avez le choix entre les options ci-dessous pour gérer le logiciel antivirus sur les ordinateurs de l'affichage.

- Configurer en temps réel
- Configurer la distribution
- Planifier un job
- Afficher les journaux
- Configurer le contact
- Afficher le résumé (pour les ordinateurs hérités)
- Configuration de la diffusion (pour les ordinateurs hérités)
- Configurer le service (pour les ordinateurs hérités)

Ces options vous permettent de définir des options d'analyse pour l'ordinateur sélectionné de la même manière que les utilisateurs définissent les options sur un ordinateur local.

Pour afficher et modifier les options sur un ordinateur, votre ID Utilisateur doit être valide, ainsi que votre mot de passe pour le serveur Admin qui gère votre ordinateur.

Gestion d'ordinateurs hérités

Lorsque vous sélectionnez un ordinateur hérité et cliquez dessus avec le bouton droit de la souris, vous pouvez sélectionner des options héritées pour gérer cet ordinateur. Ces options permettent d'afficher les boîtes de dialogue pour les versions antérieures du produit. Pour gérer des options sur un ordinateur, vous avez besoin d'un ID utilisateur et d'un mot de passe valides pour cet ordinateur.

Configurer en temps réel

L'option Configurer en temps réel vous permet de définir les options du moniteur temps réel pour l'ordinateur sélectionné. S'affichent alors les mêmes options que celles disponibles pour la gestion du moniteur temps réel sur un ordinateur local.

Reportez-vous au chapitre « **Utilisation du moniteur temps réel** » pour obtenir des informations sur les options du moniteur temps réel.

Configurer la distribution

L'option Configurer la distribution vous permet de définir les options de mise à jour des signatures pour l'ordinateur sélectionné. S'affichent alors les mêmes options que celles disponibles pour la gestion de mise à jour des signatures sur un ordinateur local.

Reportez-vous au chapitre « **Pour obtenir les mises à jour de signatures** » pour obtenir des informations sur les options de mise à jour des signatures.

Planifier un job

L'option Planifier un job vous permet de définir les options de planification de jobs d'analyse. L'affichage de l'analyse à distance apparaît alors, permettant d'accéder aux même options que celles disponibles pour la gestion des jobs d'analyse planifiés sur un ordinateur local. Vous pouvez créer un nouveau job d'analyse planifié ou modifier un job existant.

Utilisation de l'affichage de l'analyse à distance

A partir de l'affichage de l'analyse à distance, vous pouvez ajouter un nouveau job d'analyse planifié, éditer un job existant ou supprimer un job sélectionné. Ce sont les mêmes options que celles disponibles également pour la gestion des jobs d'analyse planifiés sur un ordinateur local.

Ces options sont disponibles à partir du menu Options et des boutons de la barre d'outils. Vous pouvez également accéder à ces options en cliquant avec le bouton droit de la souris dans la liste à gauche. Par ailleurs, lorsque vous mettez un job en surbrillance dans la liste située à gauche, vous pouvez cliquer avec le bouton droit de la souris à n'importe quel endroit du résumé sur la droite pour afficher les options disponibles.

L'affichage de l'analyse à distance indique l'ordinateur sélectionné à gauche de l'écran. Vous pouvez développer l'ordinateur pour afficher des jobs qui sont planifiés pour être exécutés sur l'ordinateur, le cas échéant.

Lorsque vous sélectionnez un job dans la liste située à gauche de la fenêtre, des informations relatives au résumé s'affichent sur la droite. S'affichent alors les propriétés utilisées pour le job.

Reportez-vous au chapitre « **Planification de jobs d'analyse** » pour plus d'informations sur l'utilisation des options de planification des jobs d'analyse.

Afficher les journaux

L'option Afficher les journaux vous permet d'afficher et de gérer les informations des journaux relatives à l'ordinateur sélectionné. Le même affichage et les mêmes options que celles disponibles dans la visionneuse du journal sur un ordinateur local apparaissent alors.

Veuillez vous reporter au chapitre « **Affichage et gestion des journaux** » pour obtenir plus d'informations sur l'utilisation de la visionneuse du journal.

Configurer le contact

L'option Configurer le contact vous permet de définir les options Contact pour l'ordinateur sélectionné. S'affichent alors les mêmes options que celles disponibles également pour la gestion du contact sur un ordinateur local.

Reportez-vous à la section « **Utilisation de l'option Contact** » du chapitre « **Utilisation de l'analyseur local** » pour plus d'informations sur l'utilisation des options Contact.

Afficher le résumé

Disponible uniquement pour les ordinateurs hérités. L'option Afficher le résumé permet d'afficher les informations relatives au résumé pour un ordinateur sélectionné utilisant la version 4.x du logiciel antivirus de Computer Associates.

Configuration de la diffusion

Disponible uniquement pour les ordinateurs hérités. L'option Configuration de la diffusion permet de gérer les informations relatives à la configuration pour un ordinateur sélectionné utilisant la version 4.x du logiciel antivirus de Computer Associates.

Configurer le service

Disponible uniquement pour les ordinateurs hérités. L'option Configurer le service permet de gérer les services antivirus pour un ordinateur sélectionné utilisant la version 4.x du logiciel antivirus de Computer Associates.

Annexe

A

Installation du logiciel antivirus pour UNIX

Les procédures décrites dans ce chapitre permettent d'installer le logiciel eTrust Antivirus sur les systèmes UNIX. Evaluez la configuration requise pour votre système, puis exécutez les étapes décrites pour installer le produit.

Reportez-vous à l'annexe B pour l'installation du logiciel eTrust Antivirus pour Macintosh OS X.

Avant l'installation

Avant d'installer le logiciel eTrust Antivirus pour UNIX, nous vous recommandons d'évaluer les besoins matériels et logiciels ci-dessous afin de vous assurer que votre site répond bien à la configuration minimale requise à l'installation du produit.

Navigateur Web

Pour utiliser l'interface graphique utilisateur sur les systèmes UNIX :

- Un serveur HTTP doit être installé et doit fonctionner sur le système où le logiciel eTrust Antivirus est installé afin de pouvoir utiliser le navigateur Web de l'interface graphique utilisateur.
- Pour accéder à l'interface graphique utilisateur, utilisez de préférence l'un des deux navigateurs Internet suivants :
  - Internet Explorer version 5 ou supérieure
  - Netscape Navigator version 4.5 ou supérieure

  Le navigateur peut être installé sur le système sur lequel eTrust Antivirus est également installé ou sur un système distant.

Configuration minimale du réseau

Pour pouvoir utiliser le logiciel eTrust Antivirus, un réseau TCP/IP doit avoir été installé correctement sur votre système.

Configuration minimale du matériel

Votre serveur d'administration UNIX doit posséder au moins 150 mégaoctets d'espace disque disponible.

Votre navigateur Web doit être installé sur un ordinateur avec un écran couleur SVGA offrant une résolution de 800 x 600, au minimum 16 couleurs et 256 couleurs de préférence.

Systèmes d'exploitation pris en charge

Veuillez-vous reporter au fichier README de votre CD d'installation pour obtenir une liste mise à jour des systèmes d'exploitation pris en charge. Les systèmes d'exploitation pris en charge sont :

- **Linux (Intel) –** Red Hat 7.2, 7.3, 8.0, Enterprise Linux 2.1 et 3.0 ; SuSE 7.2, 7.3, 8.0, 9.0 Professional, Desktop Linux 1.0, et SLES 7.0 et 8.0
- **Linux (S390) –** Red Hat 7.2 ; SuSE 7.0, 7.2 et SLES 8.1
- **Solaris pour Sparc –** 2.6, 7, 8 et 9
- **HP-UX pour PA-RISC –** 11 et 11i

Remarque : Sur un système Red Hat Linux, vous devez reformer le noyau Linux pour pouvoir exécuter le moniteur temps réel. Pour ce faire, vous devez télécharger et installer le code source associé à votre noyau.

Installation du logiciel antivirus pour UNIX

Procédez comme suit pour installer le logiciel eTrust Antivirus pour UNIX :

Procédure d'installation

Vous devez être un superutilisateur pour installer le logiciel eTrust Antivirus.

1. Sur une machine cible, créez un répertoire à partir duquel vous exécuterez le programme d'installation, et effectuez un cd vers ce répertoire.
2. Insérez le CD-ROM du logiciel eTrust Antivirus pour UNIX dans le lecteur de votre ordinateur.
3. Copiez le fichier setup et le fichier TAR compressé correspondant à votre système dans le répertoire.
4. Vérifiez que l'installation est exécutable. Par exemple :

   chmod +x setup

5. Exécutez le script d'installation. Par exemple :

   ./setup

6. La procédure d'installation débutera et vous devrez alors répondre à quelques questions.

   Si l'installation peut identifier l'emplacement d'une installation antérieure de eTrust Antivirus ou d'un autre produit qui s'installe dans la même arborescence de répertoire, elle vous demandera de confirmer que vous voulez poursuivre l'installation au même emplacement. Sans désinstaller l'installation précédente, vous n'avez pas la possibilité d'effectuer l'installation à un nouvel emplacement.

   Si l'installation ne trouve pas d'installation précédente de eTrust Antivirus ou d'un produit associé, elle vous demande où vous souhaitez installer le produit.

   Le système peut vous demander si vous souhaitez exécuter le serveur d'administration sur ce système. Répondez Oui si ce système est destiné à être un serveur d'administration. Sinon, répondez Non.

   Vous serez également invité à lire et à accepter les termes du contrat de licence, si vous souhaitez que le produit se lance automatiquement au démarrage, et si vous souhaitez installer ENF afin de bénéficier de la fonctionnalité d'analyse en temps réel de eTrust Antivirus. Répondez Oui ou Non selon vos besoins.

7. Sur le système Red Hat Linux, l'installation d'ENF implique le remodelage du noyau Linux à partir du code source, ce qui peut prendre un certain temps. De plus, pour ce faire, il faut impérativement que le code source pour le noyau soit installé et disponible. L'installation peut être effectuée à partir du CD-ROM d'installation original de Linux ou téléchargée sur le Web.

   Sur un système SuSE Linux ou UNIX, l'installation ENF prend moins de temps et ne nécessite pas de remodelage du noyau.

8. Lorsque l'installation est terminée, vous pouvez afficher le fichier README. Répondez par Oui ou par Non.

Configuration de la langue

eTrust Antivirus pour UNIX prend en charge cinq langues différentes. anglais, allemand, espagnol, français et italien. Par défaut, la langue définie par la variable d'environnement LANG est installée. Si cette variable n'est pas définie ou correspond à une langue non prise en charge par eTrust Antivirus, la langue par défaut est l'anglais.

Le choix de la langue peut également être contrôlé par l'option –lang de la commande setup. (Reportez-vous à la section « Utilisation des paramètres d'installation » pour des informations détaillées.) Le paramètre utilisé avec –lang remplace la variable $LANG.

Quand eTrust Antivirus pour UNIX a été installé, la langue peut être modifiée en utilisant la commande :

InoSetLang <XX>

où XX peut être EN(anglais), DE (allemand), ES (espagnol), FR (français) ou IT (italien). Pour utiliser cette commande, vous devez arrêter tous les services eTrust Antivirus.

Utilisation de fixhttpd

La procédure d'installation configure automatiquement votre serveur HTTP. Cependant, si vous installez un serveur HTTP après avoir installé le logiciel eTrust Antivirus, vous pourrez encore profiter de la configuration automatique sans avoir à répéter la procédure d'installation. Pour ce faire, utilisez la commande fixhttpd.

Démarrage et arrêt des services

Entrez la commande suivante pour démarrer les services eTrust Antivirus.

InoStart

Pour arrêter les services, saisissez :

InoStop

Utilisation du navigateur Web

Procédez comme suit pour accéder au logiciel eTrust Antivirus sur votre serveur à partir du navigateur Web.

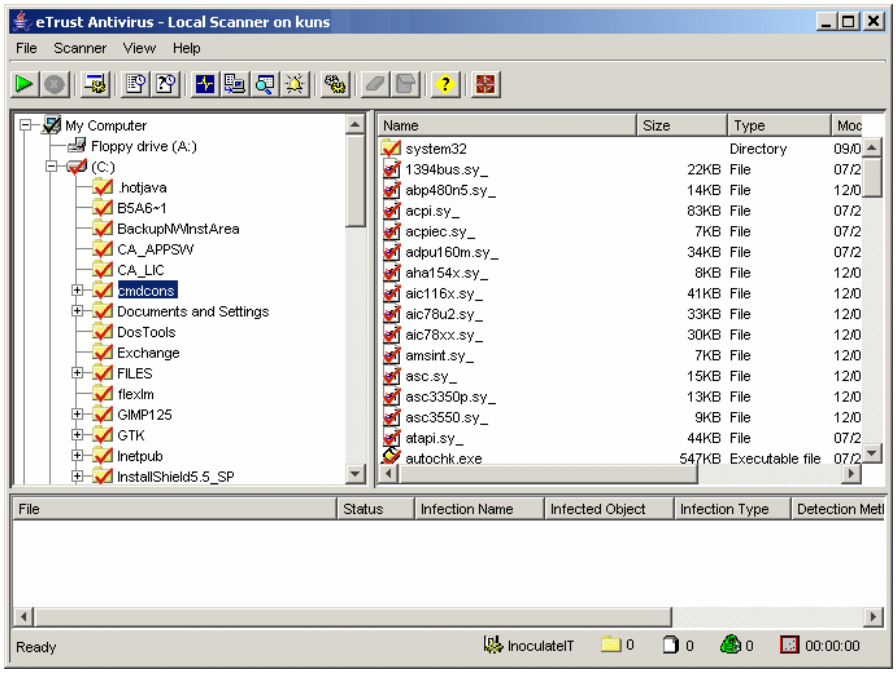
Remarque : Si votre interface graphique utilisateur se comporte bizarrement, le problème peut être lié au navigateur Web. Reportez-vous aux remarques concernant l'utilisation du plug-in de Java™ ci-dessous.

1. Démarrez votre navigateur Web.
2. Entrez l'URL suivant dans l'espace prévu pour l'adresse, puis cliquez sur OK :

   http://<nodename>/ino/
3. L'écran du produit s'affiche et le produit est alors chargé.

4. Lorsque la boîte de dialogue de connexion s'affiche comme ci-dessous, entrez votre nom d'utilisateur et votre mot de passe dans les champs correspondants.

5. L'interface graphique utilisateur de l'antivirus s'affiche dans la fenêtre de l'analyseur local, comme ci-dessous.



Utilisation d'un plug-in Java™

Il est possible que l'interface graphique utilisateur se comporte bizarrement. Si le navigateur est exécuté à partir d'un système d'exploitation Windows, vous pouvez corriger cela en installant un plug-in Java™ sur votre Internet Explorer, si cela n'a pas déjà été fait antérieurement. Vous pouvez obtenir un plug-in Java™ à l'URL http://java.sun.com/products/plugin. eTrust Antivirus prend en charge les versions de plug-in 1.3.1 à 1.4.2.

Si vous installez un plug-in, vous pouvez accéder à l'interface graphique utilisateur du navigateur Web de eTrust Antivirus en utilisant l'URL http://<nom de nœud>/ino/inoplug.html, plutôt que l'URL indiquée à la section Utilisation du navigateur Web.

Suppression du logiciel eTrust Antivirus

Avant de supprimer le logiciel eTrust Antivirus :

- Vous devez être un superutilisateur
- Tous les services antivirus doivent être arrêtés

1. Pour arrêter les services, saisissez la commande suivante :

   InoStop

Supprimer uniquement le logiciel antivirus

2. Pour supprimer uniquement le produit antivirus lorsque vous disposez d'un autre logiciel de Computer Associates, tel que CA-Unicenter TNG, installé sous $CAIGLBL0000, saisissez la commande suivante :

   InoDeinstall

3. Le script InoDeinstall est exécuté. Lorsque le script prend fin, il vous indique comment supprimer tous les fichiers restants du produit. Entrez la commande conformément aux instructions.

   Remarque : Cette commande ne supprime pas CAIENF s'il est installé sur votre système. CAIENF peut être requis par d'autres composants sous $CAIGLBL0000.

Suppression de tous les logiciels situés sous $CAIGLBL0000

4. Si aucun autre logiciel de CA n'est installé sous $CAIGLBL0000 ou si c'est le cas, mais que vous souhaitez désinstaller TOUS les logiciels situés dans ce répertoire, saisissez la commande suivante :

   $CAIGLBL0000/scripts/deinstall.

   Suivez les instructions qui s'affichent à l'écran.

   Remarque : Ce script supprime CAIENF.

Utilisation des paramètres d'installation

Si le script d'installation s'exécute normalement de façon interactive en utilisant uniquement la commande ./setup et en répondant aux questions, il possède également un certain nombre de paramètres de ligne de commande et d'arguments. Ceux-ci permettent d'indiquer au préalable un certain nombre d'options d'installation et/ou autorisent une installation automatique.

En dehors de ces paramètres, l'installation accepte un argument unique, l'emplacement dans lequel eTrust Antivirus doit être installé.

Les paramètres disponibles sont décrits dans le tableau suivant :

Paramètre d'installation	Description
-install	Exécute l'installation de eTrust Antivirus (par défaut).
-deinstall	Exécute la désinstallation de eTrust Antivirus. Identique à l'exécution de $CAIGLBL0000/ino/scripts/InoDeinstall.
-admin	Installe le serveur Admin.
-noadmin	N'installe pas le serveur Admin (par défaut).
-enf	Installe ENF (par défaut).
-noenf	N'installe pas ENF.
-autostart	Configure eTrust Antivirus pour être lancé automatiquement au démarrage (par défaut).
-noautostart	Configure eTrust Antivirus pour ne pas être lancé automatiquement au démarrage.
-acceptloc	Si l'installation détermine qu'il existe déjà une version de eTrust Antivirus ou d'un produit associé sur le système, ou si la variable d'environnement CAIGLBL0000 est déjà définie, poursuit automatiquement l'installation à cet emplacement, même si un emplacement différent a été indiqué dans la ligne de commande de l'installation.
-allowctrl	Si les services eTrust Antivirus fonctionnent, les ferme automatiquement et poursuit l'installation, plutôt que de quitter.

Paramètre d'installation	Description
-express	Exécute une installation « express » , en acceptant les paramètres par défaut pour toutes les options.
-lang	Détermine la langue à installer pour eTrust Antivirus. Les choix disponibles sont EN(anglais), DE (allemand), ES (espagnol), FR (français) ou IT (italien). Si -lang n'est pas spécifié, eTrust Antivirus utilise la valeur de la variable d'environnement LANG ou prend l'anglais par défaut si la variable n'est pas définie.

Annexe

B

Installation et démarrage de eTrust Antivirus pour Macintosh OS X

Les procédures décrites dans ce chapitre permettent d'installer le logiciel eTrust Antivirus sur les systèmes Macintosh OS X. Evaluez la configuration requise pour votre système, puis exécutez les étapes décrites pour installer le produit.

Avant l'installation

Avant d'installer le logiciel eTrust Antivirus pour OS X, nous vous recommandons d'évaluer les besoins matériels et logiciels ci-dessous afin de vous assurer que votre site répond bien à la configuration minimale requise à l'installation du produit.

Configuration minimale du réseau

Pour pouvoir utiliser le logiciel eTrust Antivirus, un réseau TCP/IP doit avoir été installé correctement sur votre système.

Configuration minimale du matériel

Votre serveur d'administration OS X doit posséder au moins 150 mégaoctets d'espace disque disponible.

Systèmes d'exploitation pris en charge

Veuillez-vous reporter au fichier README de votre CD d'installation pour obtenir une liste mise à jour des systèmes d'exploitation pris en charge. Les modèles de Macintosh et les systèmes d'exploitation pris en charge sont :

- OS X version 10.2 et 10.3 sur iBook G4, PowerBook G4, iMac, eMac et PowerPC G4
- OS X version 10.3 sur PowerPC G5

Installation du logiciel eTrust Antivirus pour OS X

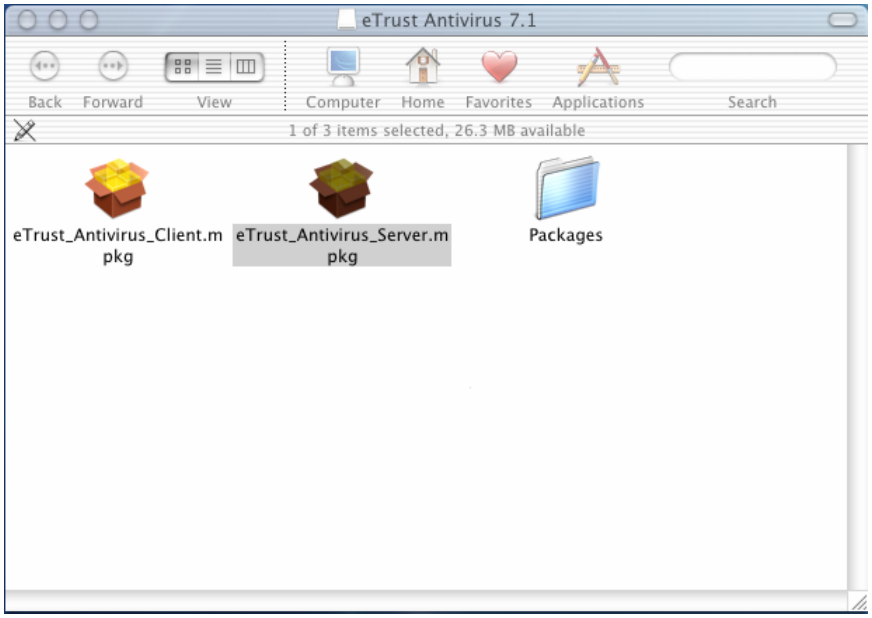
Procédez comme suit pour installer le logiciel eTrust Antivirus pour OS X :

Procédure d'installation

Vous devez être administrateur pour installer le logiciel eTrust Antivirus.

1. Insérez le CD-ROM du logiciel eTrust Antivirus pour OS X dans le lecteur de la machine cible.
2. Utilisez le Finder du système OS X pour localiser les paquets d'installation.

   Par exemple, pour installer la version client seul, sélectionnez Trust_Antivirus_Client.mpkg. Pour installer les versions client et serveur administratif, sélectionnez eTrust_Antivirus_Server.mpkg.

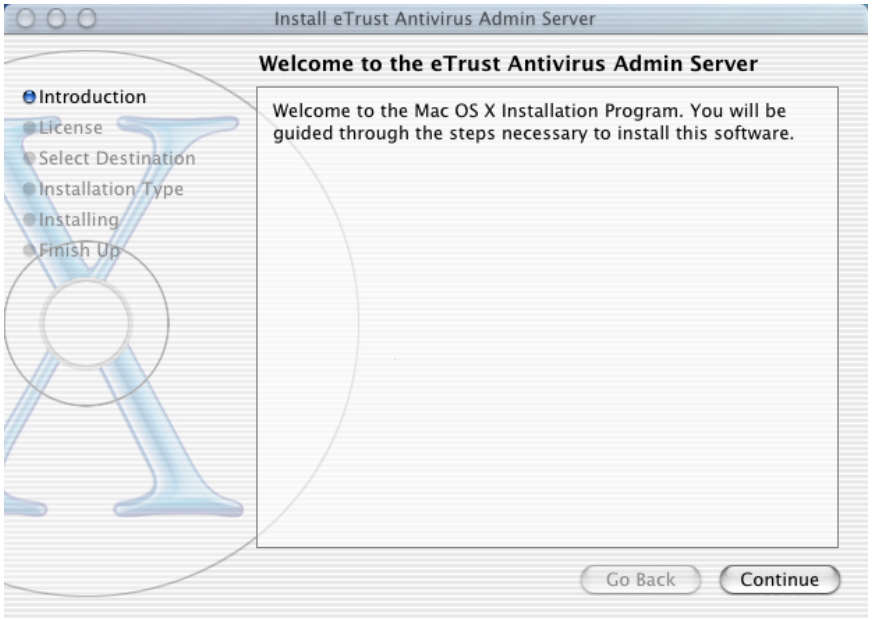


   Le paquet d'installation est un exécutable auto-extractible, qui s'exécute quand il est sélectionné dans le Finder OS X.
3. Double-cliquez sur l'icône du paquet d'installation.

La procédure d'installation débute et vous devrez alors répondre à quelques questions. La boîte de dialogue d'authentification s'affiche dans un premier temps.

4. Dans cette boîte de dialogue, saisissez le nom d'utilisateur et le mot de passe dotés de droits d'administrateur et cliquez sur OK.

   L'écran de bienvenue s'affiche.

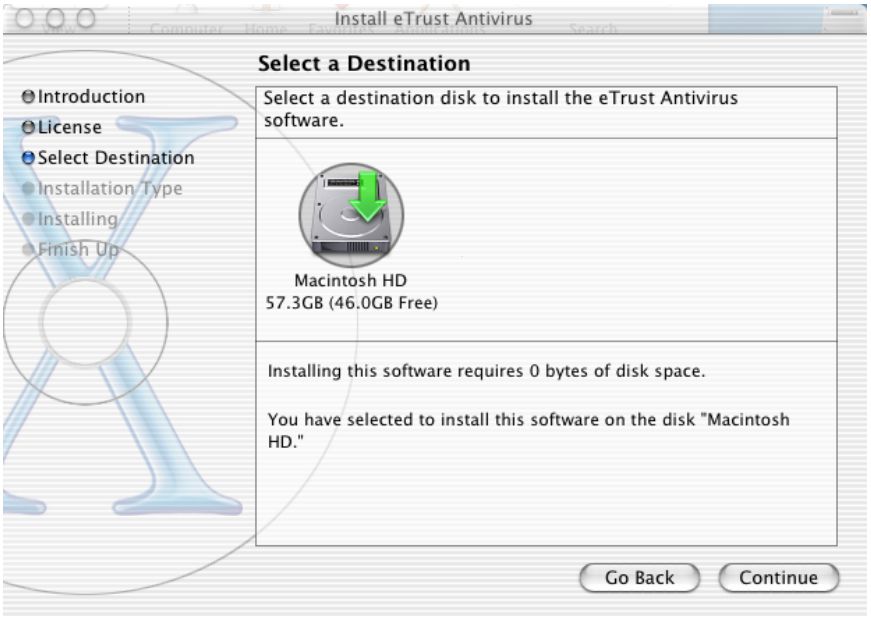


5. Cliquez sur Continuer.

   La boîte de dialogue du Contrat de licence du logiciel s'affiche.

6. Cliquez sur Continuer. Si vous acceptez les termes du contrat de licence, cliquez sur J'accepte.

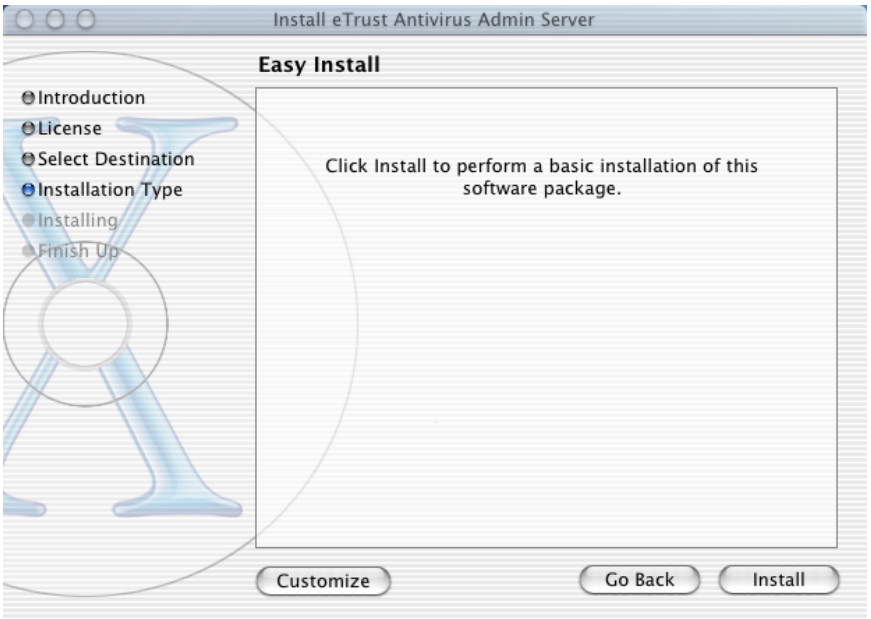
La boîte de dialogue de sélection de destination s'affiche.



7. Sélectionnez une destination pour installer le logiciel eTrust Antivirus et cliquez sur Continuer.

   Remarque : La destination doit être située sur le disque « root » par défaut.

   La boîte de dialogue d'installation simplifiée s'affiche.



8. Cliquez sur Installer.

   La boîte de dialogue de progression de l'installation s'affiche.

9. Un message vous demande si vous souhaitez exécuter eTrust Antivirus au démarrage d'OS X.

   Répondez par Oui ou par Non et cliquez sur Continuer.

   Une boîte de dialogue de progression s'affiche et vous devez fournir le numéro de votre licence.

10. Sélectionnez Version d'essai ou indiquez la clé de votre logiciel et cliquez sur Suivant.

    Remarque : La version d'essai ne peut pas être choisie pour le serveur administratif.

   Une boîte de dialogue de confirmation s'affiche.

11. Cliquez sur Terminé.

    Une boîte de dialogue de progression de l'installation s'affiche.

12. Lorsque l'installation est terminée, cliquez sur Fermer.

Services d'installation à distance

Pour distribuer et installer à distance le logiciel eTrust Antivirus sur d'autres ordinateurs Macintosh du réseau sous OS X, procédez comme suit :

1. L'image de l'installation doit être transmise à l'ordinateur cible.
2. Un fichier repère nommé unattended.marker doit être créé dans le répertoire où le métapaquet (pas le dmg) est copié. Cette étape est requise pour interdire au logiciel d'installation de eTrust Antivirus de demander des informations de licence.
3. L'utilitaire qui installe le paquet sur l'ordinateur cible doit être exécuté.
4. La licence devra ultérieurement être activée en exécutant AVLicense. Cet utilitaire est situé dans le répertoire Applications du dossier CA/eTrust Antivirus.

Vous pouvez créer et personnaliser des scripts pour effectuer une installation compose des deux étapes ci-dessus. Les deux exemples de script suivants assurent ces fonctions.

Exemples de script

Le premier exemple de script, nommé RemoteInst.sh, est exécuté depuis l'ordinateur source et prend le nom de l'ordinateur cible comme paramètre. Il copie le second script ClientInst.sh et l'image d'installation. Il exécute ensuite le second script pour terminer l'installation:

Exemple de script RemoteInst.sh

```
#!/bin/sh
#
# vérifie qu'un nom d'ordinateur cible a été fourni
#
if [ $# != 1 ]; then
    echo "usage :"
    echo "remoteInst.sh <ordinateur_cible>"
    exit
fi
```

```
TARGET=$1
#
# copie notre script d'installation de client
# et l'image de l'installation elle-même
#
scp clientInst.sh root@$TARGET:clientInst.sh
scp eTrust_Antivirus.dmg root@$TARGET:eTrust_Antivirus.dmg
#
# execute maintenant le script d'installation
#
ssh root@$TARGET ./clientInst.sh
```

Exemple de script ClientInst.sh

```
#!/bin/sh
#
#  récupère le nom de l'unité pour utilisation ultérieure et l'éjecte
#
DISKDEV=`hdid -nomount eTrust_Antivirus.dmg`
hdiutil eject $DISKDEV

#
#  monte l'unité et enregistre le nom du paquet d'installation
#  copie le paquet dans le répertoire courant et éjecte de nouveau l'unité
#
MOUNT_POINT=`hdid eTrust_Antivirus.dmg | awk 'BEGIN { FS = "\t" } { print $NF }'`
echo copying "$MOUNT_POINT"/eTrust_Antivirus_Client.mpkg
cp -R "$MOUNT_POINT"/eTrust_Antivirus_Client.mpkg .
cp -R "$MOUNT_POINT"/Packages .
hdiutil eject $DISKDEV

#
#  Touchez le fichier repère et exécutez l'installation
#
echo Démarrage de l'installation de eTrust_Antivirus_Client.mpkg
touchez unattended.marker
installer -pkg eTrust_Antivirus_Client.mpkg -target /
echo Installation de eTrust_Antivirus_Client.mpkg terminée

#
```

```
#  nettoyage (remarque : ce script est assez petit pour s'auto-détruire)
#
rm -rf Packages
rm -rf eTrust_Antivirus_Client.mpkg
rm -f eTrust_Antivirus.dmg
rm -f unattended.marker
rm -f clientInst.sh
```

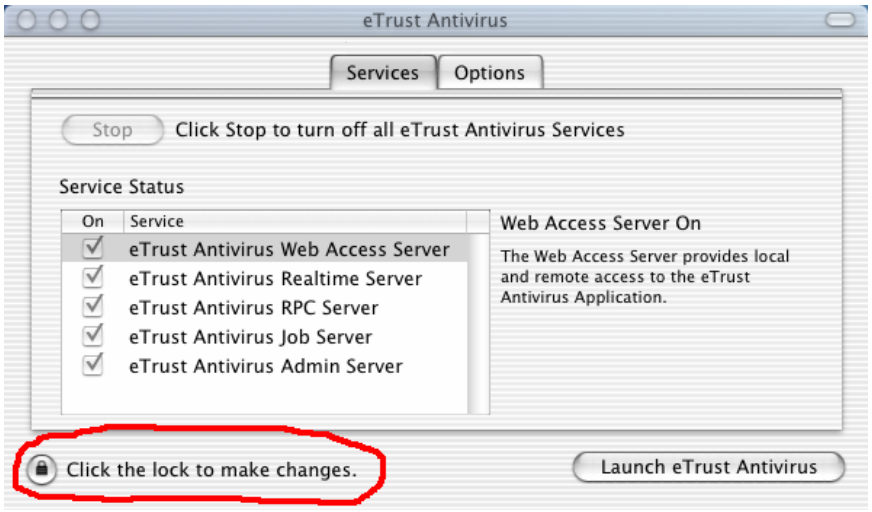
Remarque : Ces exemples de script fonctionneront pour installer une version client seulement de eTrust Antivirus. Pour installer la version Serveur Admin, utilisez eTrust_Antivirus_Server.mpkg au lieu de eTrust_Antivirus_Client.mpkg

Démarrage des services eTrust Antivirus

Vous pouvez démarrer et arrêter les services eTrust Antivirus depuis l'écran Préférences système en procédant comme suit :

1. Ouvrez les Préférences système et cliquez sur l'icône eTrust Antivirus dans la section « Autre ».

   L'écran de eTrust Antivirus s'affiche.



   L'écran eTrust Antivirus comporte deux onglets, Services et Options.

   Remarque : Pour effectuer des modifications dans un onglet, vous devez disposer de droits administratifs pour le déverrouiller.

Onglet Services

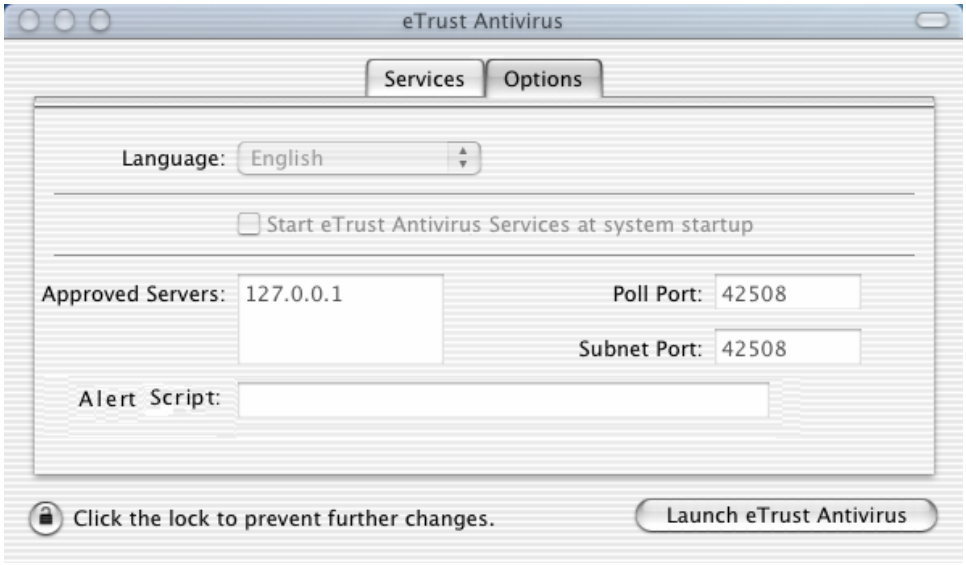
Les services et l'état de eTrust Antivirus sont affichés dans la fenêtre Etat des services. Les services sont activés ou désactivés.

Vous pouvez démarrer et arrêter les services eTrust Antivirus et lancer eTrust Antivirus depuis l'onglet Services. Pour modifier les services eTrust, par exemple pour les arrêter, déverrouillez d'abord l'onglet en procédant comme suit :

1. Sélectionnez le verrou, saisissez votre nom d'administrateur et votre mot de passe dans la boîte de dialogue d'authentification et cliquez sur OK.
2. Lorsque vous avez terminé, cliquez de nouveau sur le verrou pour verrouiller de nouveau l'onglet.

Onglet Options

Depuis l'onglet Options, vous pouvez modifier la langue par défaut, définir des serveurs Admin approuvés, spécifier les ports administrateur utilisés par la procédure de découverte et lancer eTrust Antivirus :



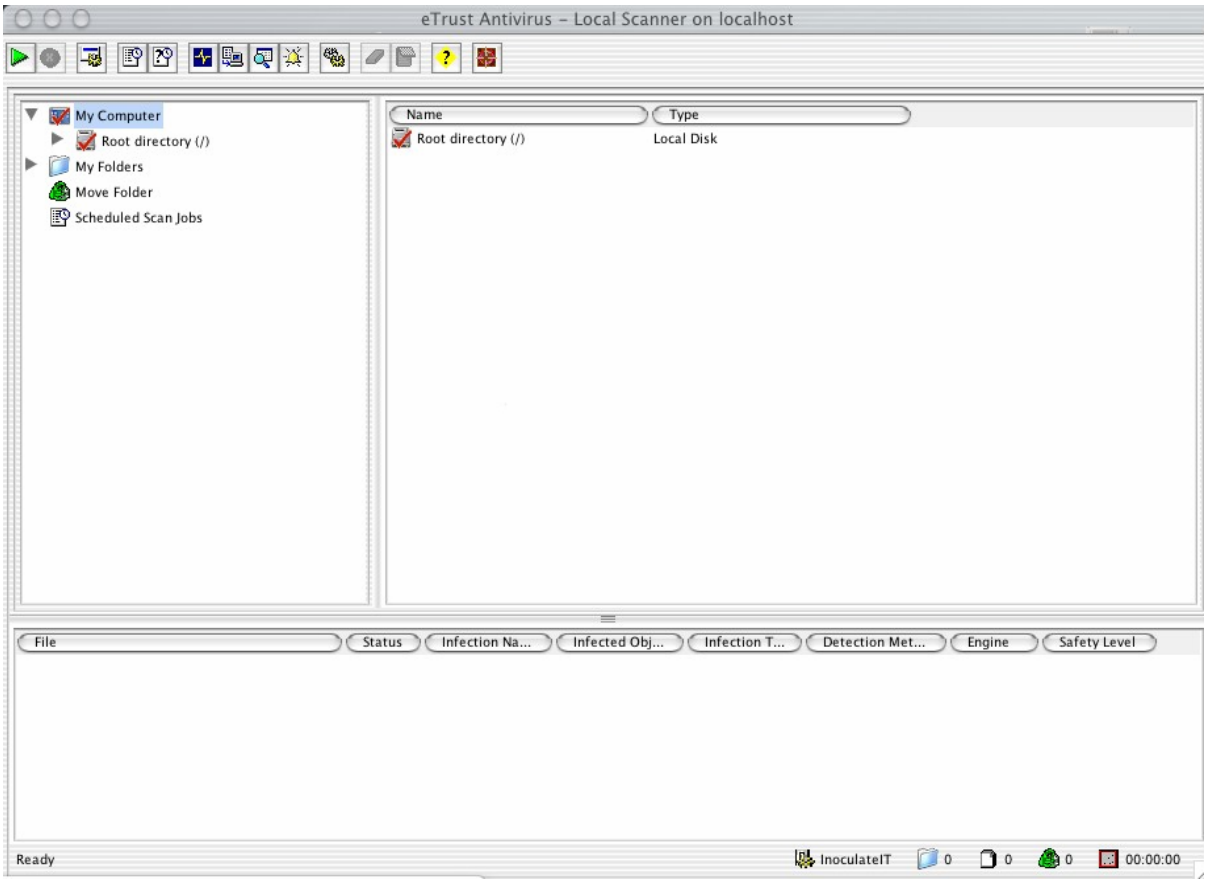
Remarque : Pour pouvoir changer de langue sur l'onglet Options, les services doivent être arrêtés.

Lancement de eTrust Antivirus

Pour utiliser le logiciel eTrust Antivirus, procédez comme suit :

1. Dans une fenêtre du Finder, ouvre le répertoire /Applications/CA/eTrust Antivirus.
2. Cliquez sur l'icône de l'application eTrust Antivirus.

   L'interface graphique utilisateur de l'antivirus s'affiche dans la fenêtre de l'analyseur local, comme ci-dessous.



Pour obtenir des informations sur eTrust Antivirus et la configuration des options, cliquez sur  dans la barre d'outil pour afficher l'aide en ligne.

Suppression du logiciel eTrust Antivirus

Pour supprimer le logiciel eTrust Antivirus, utilisez l'application Terminal puis exécutez le script de désinstallation depuis la ligne de commande du terminal. Le script de désinstallation est situé dans le répertoire /Library/Application Support/eTrustAntivirus/scripts/deinstall. Il doit être exécuté en utilisant sudo ou en étant connecté en tant que root.

Annexe

C

Installation du logiciel antivirus pour NetWare

Les procédures décrites dans ce chapitre permettent d'installer le logiciel eTrust Antivirus sur les systèmes NetWare®. Evaluez la configuration requise pour votre système, puis exécutez les étapes décrites pour installer le produit.

Avant l'installation

Avant d'installer eTrust Antivirus pour NetWare, il est conseillé de prendre en compte les éléments suivants pour éviter tout problème d'installation :

- Le produit prend en charge les versions de NetWare 4.2, 5.0, 5.1, 6.0 et 6.5. Pour les serveurs NetWare exécutant les versions 4.2, vous devez également installer NetWare Service Pack 9.
- Lorsque vous indiquez les emplacements par défaut d'installation des composants de eTrust AV, il est recommandé de placer les options HOME et ENG Path sur le même volume. Néanmoins, ceci n'est pas obligatoire. En outre, le(s) volume(s) utilisé(s) pour HOME et ENG doivent avoir l'espace de noms LONG. Pour vérifier si l'espace de noms LONG existe sur un volume, saisissez la commande VOLUMES sur la console du système. Si l'espace de noms LONG existe, il est inclus à la liste des espaces de noms de chaque volume que vous installez. Pour ajouter l'espace de noms :

  1. Vérifiez que LONG.NAM fonctionne. Saisissez la commande LOAD LONG.NAME sur la console du système.
  2. Sur la console du système, saisissez la commande ADD NAMESPACE LONG TO VOLUME <VOLUME>, où <VOLUME> désigne le volume dans lequel vous effectuez l'installation.

  Remarque : Pour détecter le changement d'espace de nom si vous avez ajouté l'espace de nom LONG à un volume, déconnectez toute connexion existante au serveur NetWare à partir des ordinateurs Windows sur lesquels l'installation a démarré.
- Les serveurs NetWare doivent exécuter IP (Internet Protocol). Le protocole de réseau IPX (Internet Packet Exchange) n'est pas pris en charge.
- Pour gérer un serveur NetWare exécutant eTrust Antivirus 7.1, vous devez avoir un serveur d'administration eTrust Antivirus 7.0 ou 7.1 disponible sur un système Windows ou UNIX.

- Le programme d'installation de eTrust Antivirus pour NetWare s'exécute sur un ordinateur Windows. Vous devez installer le client Novell NetWare sur l'ordinateur Windows avant d'installer eTrust Antivirus.
- Vous devez disposer des droits d'administrateur sur votre serveur NetWare.
- Au moment de l'installation, il n'est pas nécessaire que le client Novell NetWare soit connecté au serveur NetWare, mais les serveurs cibles doivent être accessibles sur le réseau à partir du système Windows.
- Si InoculateIT ou Inoculan 4.x se trouvent sur le serveur NetWare cible, vous pouvez en définir la désinstallation automatique par l'installation. L'option par défaut est de ne pas effectuer la désinstallation. De plus, l'installation de la version 7.1 fait migrer tous les paramètres de configuration correspondants à partir de 4.x. Vous pouvez modifier le fichier inoc6_nw.icf pour qu'il contrôle les détails de l'installation sur chaque serveur NetWare cible. Pour plus d'informations concernant le fichier inoc6_nw.icf, reportez-vous au chapitre « Utilisation du fichier de commande de l'installation » .
- Si InoculateIT ou Inoculan 4.x se trouvent sur le serveur NetWare cible, ne les exécutez pas en même temps qu'eTrust Antivirus 7.1. L'installation de eTrust Antivirus 7.1 arrête automatiquement 4.x, mais si des instructions d'autoexec.ncf déclenchent le lancement de 4.x au démarrage, retirez ces instructions après avoir installé eTrust Antivirus 7.1, et avant de redémarrer votre serveur.

Utilisation du programme d'installation

Les informations suivantes vous aident à démarrer votre installation de eTrust Antivirus pour NetWare.

Remarque : Pour garantir le succès de l'installation, les serveurs NetWare cibles doivent être accessibles sur le système Windows à partir duquel vous procédez à l'installation.

eTrust Antivirus pour NetWare utilise un assistant d'installation qui vous guide tout au long de la procédure et facilite l'installation. Le programme d'installation vous permet :

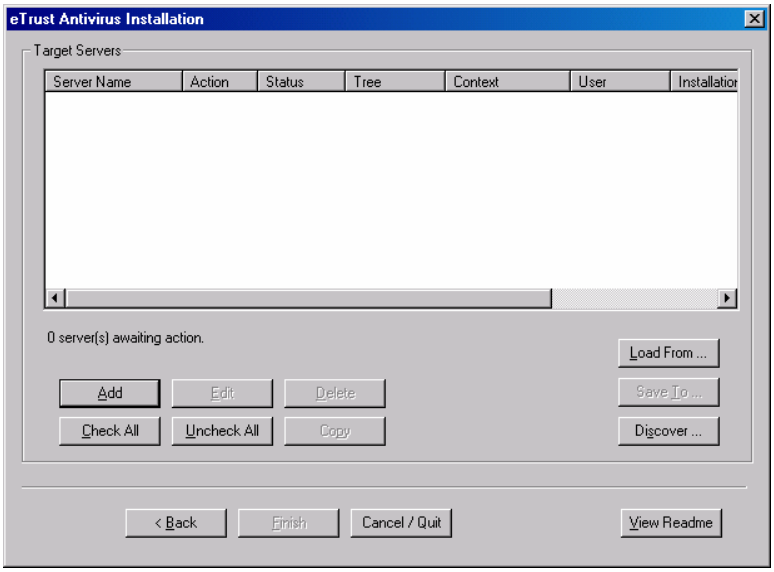
- d'installer eTrust Antivirus pour NetWare sur les serveurs NetWare
- de supprimer eTrust Antivirus des serveurs NetWare

Installation de eTrust Antivirus pour NetWare

Pour installer eTrust Antivirus pour NetWare :

1. Insérez le CD dans le lecteur de votre ordinateur Windows. Le processus d'installation démarre automatiquement.

2. Sélectionnez l'option eTrust Antivirus 7.1 pour NetWare.
3. Le chargement du programme d'installation démarre. Cliquez sur Suivant dans la boîte de dialogue Bienvenue. La boîte de dialogue Licence apparaît.
4. Dans la boîte de dialogue Licence, cliquez sur J'accepte. La boîte de dialogue Installation de eTrust AV s'affiche.



Remarque : Si vous avez la liste des serveurs enregistrés au cours d'une installation précédente, vous pouvez utiliser le bouton Charger depuis pour les charger en tant que serveurs cibles. Par exemple, si votre liste de serveurs NetWare cibles enregistrés se nomme C:\domain01.ini, cliquez sur Charger depuis pour charger automatiquement la liste à partir du fichier C:\domain01.ini.

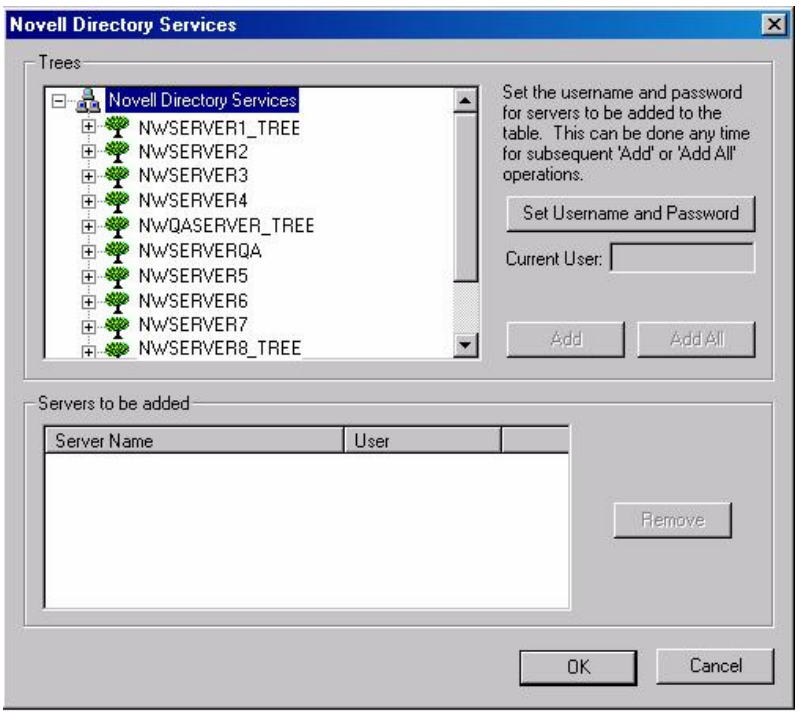
Le fichier Lisez-moi contient des informations à jour sur eTrust AV pour NetWare. Cliquez sur Afficher le fichier Lisez-moi pour consulter ces informations.

Utilisez le bouton Découvrir ou Ajouter pour créer une nouvelle liste de serveurs NetWare cibles. Le bouton Découvrir permet de rechercher vos serveurs NetWare sur le réseau. Par exemple, si vous ne savez pas quels serveurs NetWare vous voulez installer et si vous souhaitez rechercher quelles possibilités sont à votre disposition sur le réseau, cliquez sur Découvrir. En revanche, si vous connaissez déjà les informations de noms de vos serveurs NetWare, d'arborescence et de contexte, cliquez sur Ajouter pour les identifier. Si vous utilisez la fonction Ajouter, passez à l'étape 8.

Remarque : La méthode de découverte est utilisée pour la procédure d'installation de eTrust Antivirus pour NetWare. Ce mécanisme de découverte n'a rien à voir avec la découverte des clients eTrust Antivirus par le serveur Admin.

Utilisation de la fonction de découverte pour créer la liste des serveurs cibles

5. Cliquez sur Découvrir pour effectuer une recherche sur le réseau et créer une nouvelle liste de serveurs NetWare cibles. La boîte de dialogue Services d'annuaire Novell s'affiche :

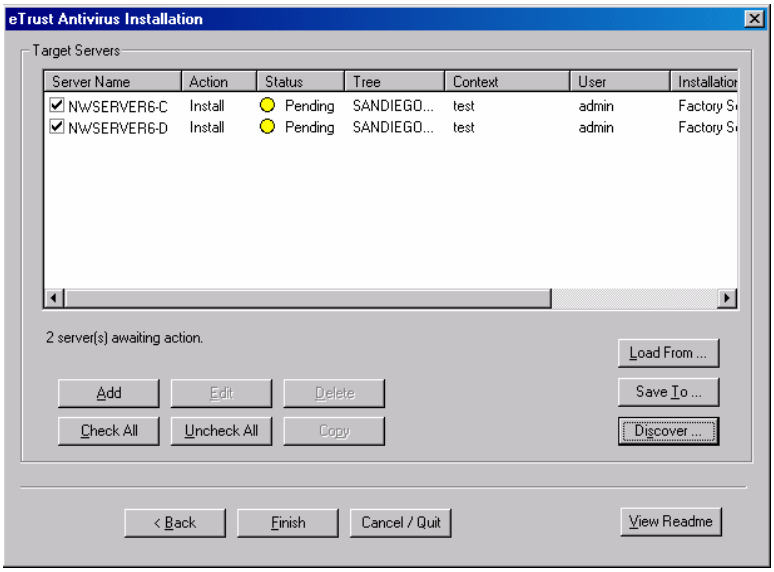


6. Dans la boîte de dialogue Services d'annuaire Novell, les arborescences NetWare de votre réseau s'affichent dans la zone de liste Arborescences sous le nœud d'arborescence Services d'annuaire Novell. Vous pouvez développer la liste Arborescences pour afficher les informations de noms de vos serveurs NetWare, d'arborescence et de contexte. Sélectionnez et saisissez les nouveaux serveurs NetWare et utilisez les contrôles décrits dans le tableau suivant :

Champ/Contrôle	Description
Zone de liste Arborescences	Développez la liste pour découvrir et sélectionner les serveurs NetWare cibles.
Bouton Définir nom d'utilisateur et mot de passe	Sélectionnez le nom et le mot de passe pour prédéfinir le nom d'utilisateur et le mot de passe qui seront utilisés pour plusieurs ou pour un grand nombre de serveurs partageant l'espace de noms de l'utilisateur sans avoir à ressaisir ces informations pour chaque serveur. Lorsque vous définissez le nom d'utilisateur et le mot de passe, ils seront utilisés pour tous les serveurs ultérieurs que vous placerez dans la liste des serveurs à ajouter.
Bouton Définir nom d'utilisateur et mot de passe (suite)	Vous pouvez modifier le nom d'utilisateur et le mot de passe à tout moment. Les nouveaux paramètres seront utilisés pour tous les serveurs que vous ajouterez à la liste à partir de ce moment. Si vous ne prédéfinissez pas le nom d'utilisateur et le mot de passe, vous serez invité à en fournir un chaque fois que vous sélectionnerez un serveur. Dans la boîte de dialogue Accès au serveur, saisissez le nom d'utilisateur et le mot de passe dans les champs respectifs. Vous devez confirmer votre mot de passe. **Remarque :** Le nom d'utilisateur que vous utilisez pour le serveur doit posséder des droits d'administrateur NetWare sur ce serveur afin de pouvoir mener à bien l'installation. **Remarque :** Le nom d'utilisateur et le mot de passe que vous saisissez seront utilisés par la suite dans la procédure d'installation ou de désinstallation. Aucune connexion n'existe réellement au serveur NetWare lorsque vous effectuez la saisie dans cette boîte de dialogue.

Champ/Contrôle	Description
Boutons Ajouter, Ajouter tout	Sélectionnez Ajouter pour placer le serveur sélectionné dans la liste des serveurs à ajouter. Sélectionnez Ajouter tout pour ajouter tous les serveurs sous un contexte sélectionné d'une arborescence dans la liste des serveurs à ajouter. **Remarque :** Les fonctions Ajouter et Ajouter tout ne placent que les serveurs que vous sélectionnez dans la liste Arborescences dans la zone de liste des serveurs à ajouter. Ces serveurs ne sont pas prêts à être ajoutés en tant que serveurs cibles jusqu'à ce que vous cliquiez sur OK et sont ensuite placés dans la boîte de dialogue Installation de eTrust Antivirus.
Zone de liste Serveurs à ajouter	Affiche la liste des serveurs que vous avez sélectionnés dans la liste Arborescences. Après avoir cliqué sur OK, ces serveurs sont placés dans la boîte de dialogue Installation deeTrust Antivirus.
Bouton Supprimer	Sélectionnez un serveur dans la liste des serveurs à ajouter et cliquez sur Supprimer pour supprimer le serveur de la liste.

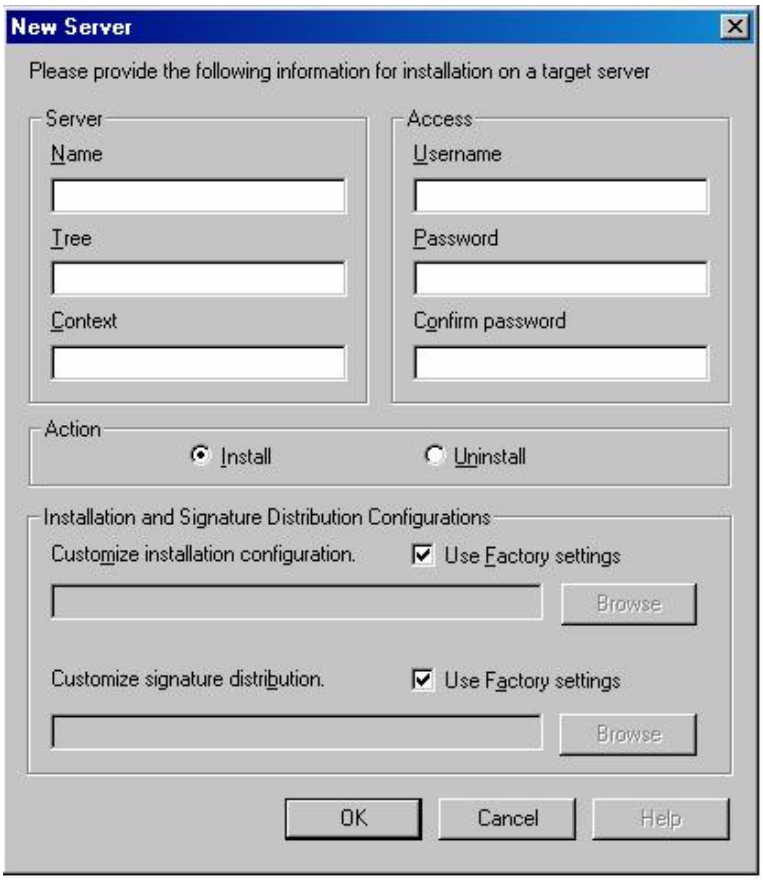
7. Lorsque vous avez terminé la sélection et la saisie de vos informations, cliquez sur OK. Le(s) serveur(s) NetWare s'affiche(nt) dans la liste des serveurs cibles.



Remarque : Vous pouvez enregistrer la liste des serveurs dans un fichier en cliquant sur Enregistrer vers. L'enregistrement de la liste vous permet de la récupérer plus tard et d'ajouter des serveurs NetWare ou de modifier l'installation sans avoir à ressaisir les informations.

Utilisation de la fonction d'ajout pour créer des serveurs cibles

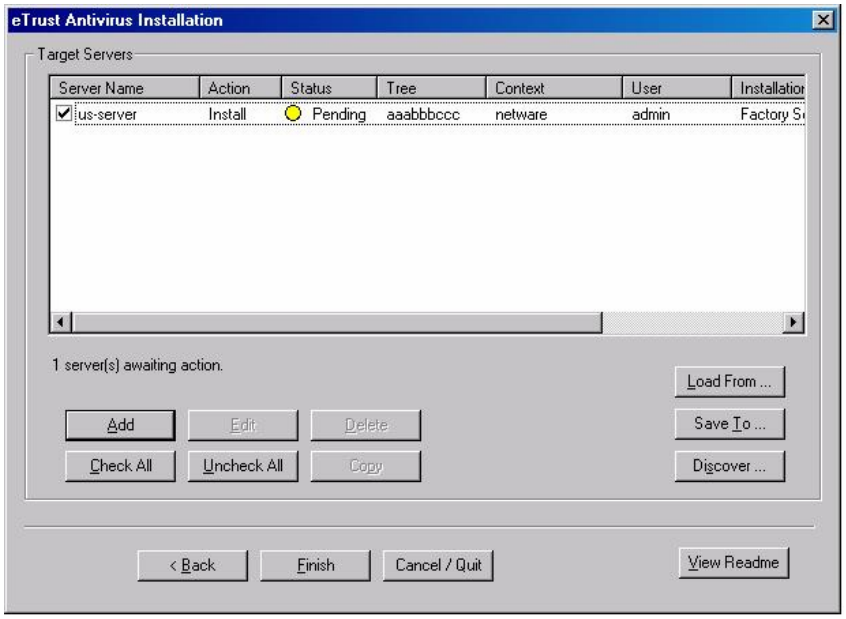
8. Cliquez sur Ajouter pour ajouter un serveur NetWare cible individuel. La boîte de dialogue Nouveau serveur s'affiche :



9. Dans la boîte de dialogue Nouveau serveur, saisissez les informations du nouveau serveur NetWare cible dans les champs correspondants et utilisez les contrôles décrits dans le tableau suivant :

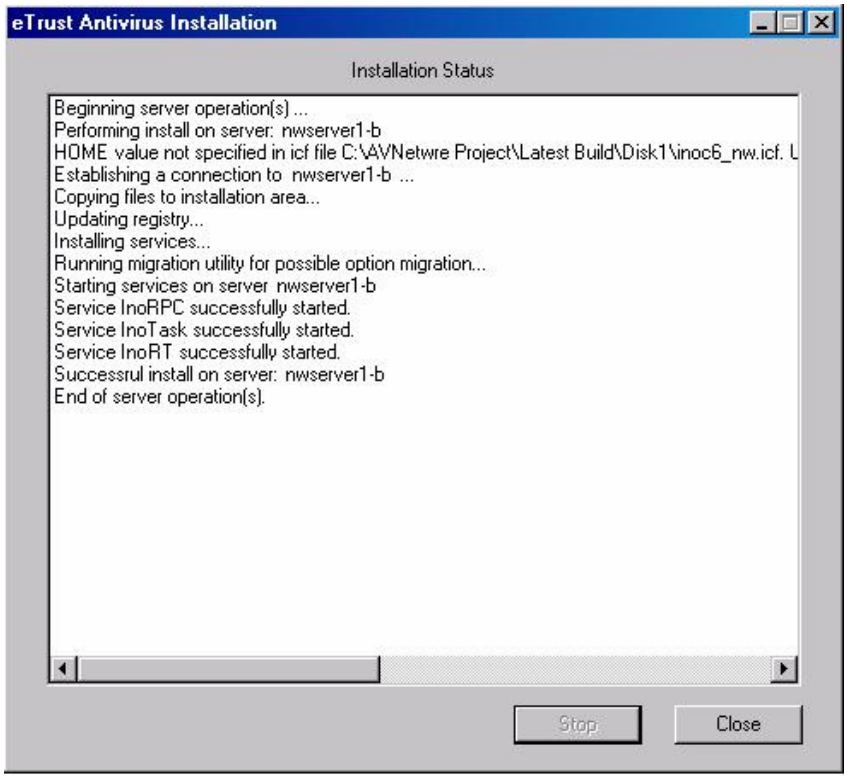
Champ/Contrôle	Description
Champs du serveur : Nom, Arborescence, Contexte	Saisissez le nom du serveur NetWare cible dans le champ Nom. Saisissez les informations d'arborescence et de contexte du conteneur du serveur NetWare dans les champs respectifs.
Champs d'accès : Nom d'utilisateur, Mot de passe, Confirmer le mot de passe	Saisissez le nom d'utilisateur et le mot de passe de votre serveur NetWare dans les champs respectifs. Vous devez confirmer votre mot de passe. **Remarque :** Vous devez disposer des droits d'administrateur NetWare sur le serveur cible.
Boutons Installer, Désinstaller	Sélectionnez Installer pour installer eTrust Antivirus pour NetWare sur le serveur spécifié. Sélectionnez Désinstaller pour supprimer le produit du serveur NetWare spécifié.
Champ Personnaliser la configuration de l'installation	Saisissez le nom d'un fichier de configuration de l'installation ou cliquez sur Parcourir pour sélectionner votre fichier. Cliquez sur le bouton Utiliser les paramètres d'usine pour installer le fichier .icf par défaut.
Champ Personnaliser la distribution des signatures	Dans le fichier .icf, vous pouvez indiquer si vous souhaitez une mise à jour des signatures à la fin de l'installation en saisissant le nom d'un fichier de distribution des signatures ou en cliquant sur Parcourir pour le rechercher. Cliquez sur Utiliser les paramètres d'usine pour indiquer le fichier InoDist.ini par défaut. Pour plus d'informations concernant le fichier InoDist.ini, consultez l'annexe « Fichier InoDist.ini » .

10. Lorsque vous avez terminé la saisie de vos informations, cliquez sur OK. Le(s) serveur(s) NetWare s'affiche(nt) dans la liste, comme dans l'exemple suivant :



Remarque : Vous pouvez enregistrer la liste des serveurs dans un fichier en cliquant sur Enregistrer vers. L'enregistrement de la liste vous d'ajouter des serveurs NetWare ou de modifier l'installation sans avoir à ressaisir les informations.

11. Après avoir saisi vos serveurs cibles, cliquez sur Terminer. Cela provoque le démarrage de l'installation et l'action sur les serveurs sélectionnés. Le statut d'une installation ayant échoué s'affiche de la façon suivante :



12. Cliquez sur Fermer pour terminer votre installation.

Changement des informations d'installation du serveur

Dans la boîte de dialogue Installation de eTrust Antivirus, vous pouvez sélectionner un serveur NetWare dans la liste pour le modifier ou le supprimer de l'installation.

Modification des informations d'installation du serveur

Sélectionnez un serveur en cliquant sur son nom pour en modifier les caractéristiques avec le bouton Modifier ou le supprimer de la liste avec le bouton Supprimer. Vous pouvez également copier les paramètres d'installation d'un serveur afin de créer des entrées similaires pour un autre, sans avoir à tout ressaisir depuis le début.

Sélectionnez un serveur en cliquant sur son nom. Cliquez sur Modifier pour ouvrir la boîte de dialogue Modifier le serveur affichant les informations d'installation de ce serveur. Vous pouvez saisir de nouvelles informations dans les champs appropriés, puis cliquer sur OK pour enregistrer vos modifications. Les informations mises à jour de votre serveur s'affichent dans la boîte de dialogue d'installation.

Sélectionnez un serveur en cliquant sur son nom. Cliquez sur Copier pour ouvrir la boîte de dialogue Ajouter un serveur avec un profil similaire. Dans cette boîte de dialogue, vous pouvez changer les informations du serveur en en saisissant de nouvelles dans les champs appropriés. Cliquez sur OK pour ajouter ce nouveau serveur à la liste.

Suppression du logiciel eTrust Antivirus d'un serveur

Sélectionnez un serveur en cliquant sur son nom. Cliquez sur Modifier pour ouvrir la boîte de dialogue Modifier le serveur affichant les informations d'installation de ce serveur. Vous pouvez supprimer le logiciel eTrust AV pour NetWare de ce serveur en cliquant sur Désinstaller.

Cliquez sur OK pour mettre à jour la liste des informations du serveur.

Action sur des serveurs spécifiques

Chaque serveur NetWare cible de la liste peut être coché ou non. Vous pouvez changer cet état en cliquant sur la case correspondant à chaque serveur. Cliquez sur Terminer pour démarrer l'installation et agir sur les serveurs sélectionnés. Le fait de cliquer sur Terminer n'a aucun effet sur les serveurs qui ne sont pas cochés, même si ceux-ci restent dans la liste.

Remarque : Lorsque l'installation est terminée, lancez eTrust Antivirus pour NetWare en saisissant ETRUSTAV à l'invite de commande NetWare. Consultez l'annexe « Utilisation du programme de console ETRUSTAV NetWare ».

Annexe

D

Utilisation du programme de console ETRUSTAV

Après avoir installé eTrust Antivirus (AV) pour NetWare sur un serveur NetWare, utilisez le programme de console ETRUSTAV pour bénéficier de ses fonctionnalités. Le programme ETRUSTAV appelle un menu à partir duquel vous pouvez contrôler un grand nombre des opérations eTrust AV sur le serveur. A partir de la ligne de commande NetWare, saisissez ETRUSTAV pour démarrer le programme.

Remarque : Lorsque vous exécutez NetWare 4.x, saisissez LOAD ETRUSTAV.

Remarque : Pour démarrer tous les services eTrust AV simultanément au démarrage d'ETRUSTAV, saisissez ETRUSTAV AUTOSTART ou LOAD ETRUSTAV AUTOSTART.

Utilisation du menu ETRUSTAV

Utilisez les touches flèches vers Haut et Bas du clavier pour naviguer parmi les options du menu ETRUSTAV. La touche Entrée active l'option de menu sélectionnée. Vous pouvez quitter le programme ETRUSTAV et les écrans contextuels d'option en utilisant la touche Echap.

Remarque : Les options par défaut du programme ETRUSTAV sont définies par le fichier inoc6_nw.icf au cours de l'installation. Pour plus d'informations concernant les paramètres du fichier inoc6_nw.icf, reportez-vous au chapitre « Utilisation du fichier de commande de l'installation ».

Les options du menu ETRUSTAV sont décrites dans le tableau suivant :

Option du menu	Description/Options disponibles
Démarrer tous les services	Charge et démarre tous les services de eTrust AV.
Arrêter tous les services	Arrête et décharge tous les services de eTrust AV.
Démarrer le service sélectionné	Démarre un service eTrust AV sélectionné. Si aucun service ne fonctionne, un élément

Option du menu	Description/Options disponibles
	de menu contextuel apparaît, dans lequel vous pouvez sélectionner le service à démarrer.
Arrêter le service sélectionné	Arrête et décharge un service eTrust AV sélectionné. Si des services fonctionnent, un élément de menu contextuel apparaît, dans lequel vous pouvez sélectionner le service à arrêter.
Configurer l'analyseur local	Ouvre un menu contextuel à partir duquel vous pouvez modifier les paramètres de l'analyseur local. Dans le menu contextuel Paramètres de l'analyseur local, vous pouvez consulter et modifier les options d'analyse ou de sélection.
Options d'analyse	
Niveau de sécurité	Indiquez le niveau de sécurité de l'analyse : **Sécurisée** – Utilisez ce mode comme méthode standard pour une analyse complète des fichiers. **Approfondie –** Utilisez ce mode si vous pensez qu'une infection n'a pas été détectée par le mode Sécurisée.
Moteur d'analyse	Indiquez le moteur antivirus à utiliser dans l'analyse : **Inoculate IT** – Le moteur Inoculate. **Vet –** Le moteur Vet
Analyseur heuristique	Utilisez cette option pour indiquer le moteur heuristique et rechercher des virus inconnus : **Non –** Ne pas utiliser l'analyseur heuristique. **Oui –** Utiliser l'analyseur heuristique

Option du menu	Description/Options disponibles
Action sur fichiers	Action sur fichier infecté. Utilisez cette option pour indiquer une option d'action à appliquer au fichier infecté : **Désinfecter** – Tente de désinfecter automatiquement le fichier infecté. Même si le fichier est désinfecté, nous vous recommandons de le supprimer et de restaurer le fichier d'origine. **Supprimer** – Supprime le fichier infecté. **Déplacer** – Déplace le fichier infecté de son répertoire actuel vers le dossier de déplacement. **Renommer** – Renomme automatiquement le fichier infecté en lui donnant l'extension AVB. Attribue des extensions incrémentielles sous la forme *numéro.AVB* (par exemple, *Fichier.0.AVB*, *Fichier.1.AVB*, etc.) aux fichiers infectés portant le même nom. Un fichier renommé avec un type d'extension AVB n'est pas analysé de nouveau par la suite. **Rapport seulement** – Génère un rapport sur un fichier infecté.

Option du menu	Description/Options disponibles
Options de désinfection	**Echec de la désinfection –** Utilisez pour indiquer l'option d'échec de la désinfection lorsque Action sur les fichiers est défini sur Désinfecter : **Copier le fichier avant de désinfecter –** Effectue une copie du fichier d'origine et la place dans le dossier de déplacement avant de tenter la désinfection. **Déplacer le fichier** – Déplace le fichier si la désinfection échoue. Déplace un fichier infecté de son répertoire actuel vers le dossier de déplacement si la désinfection échoue. **Aucune action** – Ne fait rien si la désinfection échoue. **Renommer le fichier** – Renomme le fichier si la désinfection échoue : Renomme le fichier avec une extension AVB si la désinfection échoue. **Traitement des virus de macro** – Action de désinfection de macro. Permet d'indiquer une option de suppression d'un fichier infecté lorsque Action sur les fichiers est défini sur Désinfecter : **Supprimer les macros infectées –** Supprime uniquement les macros contenant un code infecté du fichier infecté. **Supprimer toutes les macros –** Supprime toutes les macros du fichier infecté.

Option du menu	Description/Options disponibles
Options de sélection	
N'analyse pas les fichiers migrés.	Cette option vous permet d'indiquer s'il faut analyser les fichiers qui ont été migrés vers un stockage externe. **Oui** – **N**'analyse **pas** les fichiers migrés. **Non –** Analyse les fichiers migrés
Analyse les fichiers portant les extensions	Permet d'indiquer l'analyse des fichiers portant les extensions : **Toutes les extensions –** Analyse tous les fichiers. **Toutes les extensions sauf celles spécifiées –** Analyse tous les fichiers sauf ceux dont les extensions sont spécifiées dans la liste des extensions disponibles. La liste des extensions disponibles est spécifiée par l'option *Modifier la liste des extensions*. **Uniquement les extensions spécifiées –** Analyse uniquement les fichiers dont les extensions sont spécifiées dans la liste des extensions disponibles. La liste des extensions disponibles est spécifiée par l'option *Modifier la liste des extensions*.
Modifier la liste des extensions	Permet d'indiquer l'ensemble existant d'extensions de noms de fichier. **Remarque :** Vous ne pouvez consulter ou modifier la liste que lorsque vous avez choisi les sélections Toutes les extensions sauf celles spécifiées ou Uniquement les extensions spécifiées dans l'option *Analyse les fichiers portant les extensions*. Vous pouvez modifier les extensions dans la liste des extensions disponibles en sélectionnant une extension et en utilisant les touches F5, Suppr ou Inser. **Touche Suppr :** Permet de supprimer une extension sélectionnée de la liste : **Oui –** Supprime les extensions sélectionnées de la liste. **Non –** Conserve les extensions de la liste. **Touche F5 :** La touche F5 permet de marquer les extensions à supprimer de la liste à l'aide de la touche Suppr. **Touche Inser :** Permet d'ajouter une extension à la liste. Saisissez une extension de nom de fichier dans le champ Entrer extension.

Option du menu	Description/Options disponibles
Analyse des fichiers compressés	Permet de spécifier l'analyse des fichiers d'archive : **Oui –** Analyse les fichiers compressés. **Remarque :** Les options du type d'analyse de fichier d'archive et des types de fichiers compressés sont spécifiées à l'aide des options *Fichier compressé* et *Types d'archives à prendre en charge*. **Non – N**'analyse **pas** les fichiers compressés.
Options de fichier compressé	Permet de spécifier les options d'analyse des fichiers d'archive : **Remarque :** Vous ne pouvez consulter ou modifier les options des fichiers compressés que lorsque l'option Analyser les fichiers compressés est définie sur Oui. Indique s'il faut filtrer les fichiers à l'intérieur des archives par extension. Indique s'il faut arrêter d'analyser un fichier d'archive lorsqu'une infection est détectée. Détermine la compression d'un fichier par son extension ou son contenu. Le paramètre par défaut est par extension de nom de fichier.
Types d'archives à prendre en charge	Permet de spécifier les types de fichiers d'archive : **Remarque :** Vous ne pouvez consulter ou modifier les types des fichiers d'archive que lorsque l'option Analyser les fichiers compressés est définie sur Oui. Dans la liste Options de fichier compressé, indiquez le type de fichiers d'archive à analyser. Vous pouvez sélectionner Oui pour inclure le type de fichier ou Non pour exclure le type de fichier d'archive.
Exécuter l'analyseur local	Ouvre un menu contextuel à partir duquel vous pouvez indiquer un chemin complet à analyser.

Option du menu	Description/Options disponibles
Vérifier le statut des jobs planifiés	Affiche le statut de tout job d'analyse planifié actuellement en cours. Les informations affichées sont actualisées chaque seconde lors de la progression du job.
Vérifier le statut de l'analyse en temps réel	Affiche le statut de l'analyse en temps réel à partir du démarrage du moniteur temps réel. Les informations affichées sont actualisées chaque seconde.
Afficher les versions des signatures	Affiche le moteur d'analyse actuel et les versions des signatures pour les moteurs eTrust AV installés sur le serveur.
Avancé	
Vérifier le statut des services	Affiche le statut de tous les services de eTrust AV.
Définir les ports de découverte	Permet d'afficher et de spécifier les numéros de ports actuels utilisés par la procédure de découverte pour écouter les messages de diffusion. Dans le champ contextuel : Sélectionnez la touche Entrée pour afficher les numéros de ports actuels utilisés par la procédure de découverte pour écouter les messages de diffusion. Saisissez POLL et spécifiez une valeur de port pour définir le numéro du port sur lequel le client eTrust AV écoute les interrogations du serveur Admin. Saisissez SUBNET et spécifiez une valeur de port pour définir le numéro du port que les clients eTrust AV utilisent pour communiquer avec un sous-réseau. Saisissez BOTH et spécifiez une valeur de port pour utiliser la même valeur de numéro du port sur lequel les clients eTrust AV écoutent les interrogations du serveur Admin et le numéro du port que les clients eTrust AV utilisent pour communiquer avec un sous-réseau.
Restaurer les fichiers infectés dans le dossier de déplacement	Restaure un fichier infecté de son répertoire actuel vers son emplacement d'origine. Lorsque la commande a été saisie, suivez les instructions à l'écran.

Option du menu	Description/Options disponibles
Définir le(s) serveur(s) Admin approuvé(s)	Permet d'afficher et d'indiquer l'ensemble actuel de serveurs Admin eTrust AV approuvés. Dans le champ contextuel de l'adresse IP : Sélectionnez la touche Entrée pour afficher et indiquer l'ensemble actuel de serveurs Admin eTrust approuvés. Définissez les serveurs Admin eTrust AV sur l'adresse IP spécifiée approuvée pour le serveur NetWare sur lequel la commande est exécutée. Saisissez les adresses IP dans le format <adresse-ip-1> <adresse-ip-n> séparées par un espace. Par exemple, la saisie des adresses IP 192.168.130.2 192.168.130.10 définit les serveurs Admin correspondant à ces adresses IP comme des serveurs Admin eTrust AV approuvés.
Définir la variable d'environnement eTrust AV	Permet de spécifier une variable d'environnement pour eTrust AV. Par exemple, la saisie de AV_VAR1=1 définit la valeur d'une variable d'environnement hypothétique AV_VAR1 sur 1. **Remarque :** Les variables d'environnement eTrust AV ne sont utilisées qu'à l'intérieur de eTrust AV. Elles n'ont aucun effet sur les autres programmes exécutés sur votre serveur.

Annexe

E

Utilisation du fichier de commande de l'installation

Vous pouvez automatiser l'ensemble du processus d'installation de votre logiciel eTrust Antivirus en utilisant le fichier de commande d'installation. Selon la plate-forme, vous pouvez utiliser l'un des fichiers suivants :

- **INOC6.ICF –** permet d'automatiser le processus d'installation de eTrust Antivirus 7.1 pour Windows.
- **INOC6_NW.ICF –** permet d'automatiser le processus d'installation de eTrust Antivirus 7.1 pour NetWare.

Ce chapitre présente les options que vous pouvez définir dans chaque fichier et en fournit une description.

Fichier INOC6.ICF

Après avoir configuré les paramètres, placez le fichier INOC6.ICF révisé dans le répertoire des images et exécutez le programme d'installation.

Lorsque le programme d'installation démarre, le fichier INOC6.ICF est chargé et les valeurs que vous avez indiquées comme valeurs par défaut sont utilisées. Si l'installation est exécutée de manière interactive, les réponses à toutes les questions que le processus d'installation ne vous pose pas sont prédéfinies dans les paramètres du fichier INOC6.ICF.

Si vous choisissez d'exécuter le programme d'installation de manière silencieuse à partir d'un lecteur partagé ou d'un programme de commande, tous les paramètres de configuration seront tirés du fichier INOC6.ICF. Pour effectuer une installation sans requérir d'actions de l'utilisateur, utilisez le programme d'installation (emplacement : \bin\eAV_s.Win) comme suit :

SETUP /s

Si vous souhaitez installer cette image sur différents ordinateurs au sein de votre entreprise, vous pouvez utiliser la fonction d'installation à distance. Assurez-vous que les paramètres du fichier INOC6.ICF sont appropriés pour ces ordinateurs et laissez l'installation à distance s'occuper du reste.

Pour plus d'informations concernant l'utilitaire d'installation à distance, reportez-vous au chapitre 9 de ce manuel de l'administrateur.

Les tableaux suivants rassemblent les paramètres par défaut de chaque option du fichier INOC6.ICF, ainsi qu'une description rapide de l'option et des informations supplémentaires sur les variables des options.

Path

Les options de chemin vous permettent de définir les emplacements par défaut pour l'installation des différents composants de l'antivirus.

```
[Path]
HOME=
MOVE=Move
ENG=
DB=DB
OUTGOING=OUTGOING
```

Option	Description
HOME	Répertoire d'installation Entrez un lecteur et un chemin complet ou laissez cette option vide pour installer le programme dans le répertoire local des fichiers du programme. Par ex. : C:\AntiVirus
MOVE	Répertoire de déplacement Ce chemin se rapporte au chemin d'installation Par ex. : MOVE
ENG	Répertoire du moteur Entrez un lecteur et un chemin complet ou laissez cette option vide pour installer le programme dans le répertoire local des fichiers du programme. N'AJOUTEZ PAS ce répertoire comme sous-répertoire au répertoire d'installation. Par ex. : C:\AV\Engine
DB	Répertoire de la base de données Ce chemin se rapporte au chemin d'installation Par ex. : DB

Option	Description
OUTGOING	Répertoire de sortie des signatures Ce chemin se rapporte au chemin d'installation Par ex. : OUTGOING

RPCMtAdn

Les options RPCMtAdn vous permettent de spécifier les emplacements des fichiers de base de données maître RPC.

```
[RPCMtAdn]
DataBasePath=RPCMtDB
JobPath=RPCMtJob
```

Option	Description
DataBasePath	Chemin utilisé par le maître RPC pour stocker des fichiers de base de données. Remarque : Ce chemin se rapporte au répertoire d'installation.
JobPath	Chemin utilisé par le maître RPC pour stocker des fichiers de job. Remarque : Ce chemin se rapporte au répertoire d'installation.

Analyseur local

Les options de l'analyseur local vous permettent de définir la configuration des règles de l'analyseur local. Ces options sont les paramètres par défaut de l'analyseur local pour l'installation.

```
[Local Scanner]
bScanCompressed=1
bScanMemory=0
bScanBootSector=1
bScanFiles=1
dwScanMode=1
dwAction=0
dwSpecialCureAction=3
dwMacroCureAction=0
dwSpecialMode=0
dwFileFilterType=0
bIsArcByExtension=1
dwArcTypesCount=10
pdwArcTypeList=1,2,3,4,6,7,8,9,10,11
```

```
pszSpecifiedList=|386|ADE|ADP|ADT|ASX|BAS|BAT|BIN|CBT|CHM|CLA|CMD|COM|CPL|CRT|CSC
|DLL|DOC|DOT|DRV|EXE|HLP|HTA|HTM|HTT|INF|INS|ISP|JS|JSE|LNK|MDB|MDE|MSC|MSI|MSO|M
SP|MST|OCX|PCD|PIF|POT|PPT|PRF|REG|RTF|SCF|SCR|SCT|SHB|SHS|SYS|URL|VB|VBE|VBS|VSD
|VSS|VST|VXD|WIZ|WSC|WSF|WSH|XLA|XLS|XLT|XLW|
pszExcludedList=|BTR|DBF|SBF|DB|MDX|NDX|MDW|LDB|
bScanAllFilesInArc=1
bStopAtFirstInfectionInArc=1
bScanMigratedFiles=0
dwEngineChoice=1
dwShowDriveFlags=31
bShowAllFiles=0
bLogCleanFiles=0
bLogInfectedFiles=1
bLogSkippedFiles=0
dwDaysToDeleteLogs=365
dwBootAction=0
bShowSummaryAfterScan=0
```

Option	Description
bScanCompressed	Analyser les fichiers compressés ? 0 – Non 1 – Oui
bScanMemory	Rechercher des virus dans la mémoire ? 0 – Non 1 – Oui
bScanBootSector	Rechercher des virus dans le secteur d'amorçage ? 0 – Non 1 – Oui
bScanFiles	Analyser les fichiers ? (Configurez cette option sur 0 et secteur d'amorçage sur 1 pour analyser uniquement le secteur d'amorçage) 0 – Non 1 – Oui
dwScanMode	Type d'analyse : 1 – Analyse sécurisée 2 – Analyse approfondie
dwAction	Action à entreprendre lors de la détection d'un virus 0 – Rapport seulement 1 – Désinfecter 2 – Renommer 3 – Supprimer 4 – Déplacer

Option	Description
dwSpecialCureAction	Masque binaire spécifiant l'action à entreprendre lors de la détection d'un virus inconnu : 1 – Copier et désinfecter (copier le fichier vers le répertoire de déplacement avant de le désinfecter) 2 – Renommer le fichier si la désinfection échoue 4 – Déplacer le fichier si la désinfection échoue 8 – Supprimer le fichier s'il contient un cheval de Troie ou un ver.
dwMacroCureAction	Action de désinfection pour les virus de macros : 0 – Ne rien faire 1 – Supprimer toutes les macros 2 – Supprimer les macros infectées
dwSpecialMode	Masque binaire pour activer les techniques avancées de recherche des virus ? 1 – Heuristique 2 – Désinfection du système 4 – Analyser le flux de données NTFS
dwFileFilterType	Permet de spécifier le type de fichier à analyser suivant son extension. 0 – Analyser tous les fichiers 1 – Analyser les fichiers portant les extensions par défaut (spécifiées dans pszExtList) 2 – Analyser tous les fichiers sauf ceux portant les extensions par défaut (spécifiées dans pszExcludeExtList)
bIsArcByExtension	Déterminer si des archives existent pour les extensions de fichiers ? 0 – Non (déterminé par les contenus du fichier) 1 – Oui
dwArcTypesCount	Nombre de fichiers contenus dans pdwArcTypeList

Option	Description
pdwArcTypeList	Liste délimitée par des virgules des extensions archivées à analyser : 1 – ARJ 2 – GZIP 3 – Archives JAVA 4 – Archives LHA 5 – Microsoft CAB 6 – Compressé Microsoft 7 – MIME 8 – Fichiers UNIX à UNIX codés (UUEncode) 9 – ZIP 10 – RAR 11 – Compressé Unix (Z) 12 – Fichier Rich Text Format (RTF) 13 – Fichiers messages électroniques TNEF encapsulés
pszSpecifiedList	Liste des extensions par défaut. (Séparez chaque élément par « | »)
pszExcludedList	Liste des extensions exclues. (Séparez chaque élément par « | »)
bScanAllFilesInArc	Analyser tous les fichiers situés dans les archives ? 0 – Non 1 – Oui
bStopAtFirstInfectionInArc	Arrêter d'analyser des archives de fichiers dès que le premier virus a été détecté ? 0 – Non 1 – Oui
bScanMigratedFiles	Analyser les fichiers migrés vers des archives externes ? 0 – Non 1 – Oui (les fichiers doivent être migrés à nouveau vers le disque local)

Option	Description
dwEngineChoice	Sélectionnez un des deux moteurs : 1 – Moteur InoculateIT 2 – Moteur Vet
dwShowDriveFlags	Masque permettant de déterminer les lecteurs affichés : 1 – Disque dur 2 – Unités CD 4 – Unité de disquettes 8 – Unités de réseau 16 – Unités amovibles
bShowAllFiles	Options d'affichage du fichier : 0 – Afficher uniquement les fichiers dont les extensions sont contenues dans pszSpecifiedList 1 – Afficher tous les fichiers
bLogCleanFiles	Ecrire dans le fichier journal si une analyse nettoie un fichier ? 0 – Non 1 – Oui
bLogInfectedFiles	Ecrire dans le fichier journal si une analyse détecte un fichier infecté ? 0 – Non 1 – Oui
bLogSkippedFiles	Ecrire dans le fichier journal si des fichiers sont ignorés par une analyse ? 0 – Non 1 – Oui
dwDaystoDeleteLogs	Nombre de jours pendant lesquels un fichier journal est gardé avant sa suppression.
dwBootAction	Lorsqu'un secteur d'amorçage infecté est détecté : 0 – Rapport seulement 1 – Désinfecter le secteur d'amorçage

Option	Description
bShowSummaryAfterScan	Afficher la boîte de dialogue Résumé après chaque analyse ? 0 – Non 1 – Oui

Distribution

Les options de distribution vous permettent de configurer les options pour la récupération et la distribution des signatures locales.

```
[Distribution]
dwStateMask=0
tExecTime=
byRepeatMonth=0
byRepeatDay=0
byRepeatHour=0
byRepeatMinute=0
dwRepeatTimesOnFail=3
dwRepeatMinutesOnFail=5
dwHoldTimeQueryInterval=60
bDownloadNow=0
dwPopupMessage=0
bHideIcon=0
```

Option	Description
dwStateMask	Etat de distribution 0 – Désactivé 1 – Entrant (récupération des mises à jour), 2 – Sortant (permet à d'autres de récupérer des mises à jour à partir de leurs ordinateurs locaux) 3 – Les deux
tExecTime	Heure à laquelle est vérifié si des nouveaux fichiers de signatures se trouvent sur les serveurs distants. Format : JJ/MM/AAAA,HH:MM:SS,Heure d'été (Heure d'été = 1 si l'horaire est en heure d'été, 0 dans le cas contraire.) par ex.04/12/1999,23:23:23,0
byRepeatMonth	Nombre de mois entre les vérifications (0 à 12)

Option	Description
byRepeatDay	Nombre de jours entre les vérifications (0 à 31)
byRepeatHour	Nombre d'heures entre les vérifications (0 à 24)
byRepeatMinute	Nombre de minutes entre les vérifications (0 à 60)
dwRepeatTimesOnFail	Nombre de tentatives que le planificateur de jobs doit effectuer si le téléchargement des signatures échoue. Cette valeur est utilisée avec dwRepeatMinutesOnFail pour déterminer le nombre de tentatives pouvant être effectuées pour un téléchargement. Les tentatives sont effectuées jusqu'à ce que : un téléchargement réussisse. le nombre de tentatives dépasse dwRepeatTimesOnFail un téléchargement planifié s'effectue. Remarque : Définissez sur 0 pour désactiver les tentatives.
dwRepeatMinutesOnFail	Nombre de minutes entre les tentatives dans l'éventualité d'un échec. Cette valeur est utilisée avec dwRepeatTimesOnFail pour déterminer le nombre de tentatives.
dwHoldTimeQueryInterval	Nombre de fois (par minutes) où le programme vérifie dans le répertoire entrant la présence de nouvelles signatures disponibles pour les copier dans le répertoire sortant à des fins de distribution.
bDownloadNow	Télécharger une nouvelle signature directement après l'installation ? (Requiert qu'un fichier inodist.ini contienne un site ftp et un serveur proxy valides) 0 – Non 1 – Oui

Option	Description
dwPopupMessage	Afficher un message contextuel à chaque mise à jour des signatures ? 0 – Non 1 – Oui
bHideIcon	Masquer l'icône de téléchargement dans la barre des tâches ? 0 – Non 1 – Oui

Temps réel

Les options Temps réel vous permettent de configurer les règles locales de temps réel. Ces options sont les paramètres par défaut de temps réel utilisés pour l'installation locale.

```
[Realtime]
dwDirection=3
bFloppyDrive=1
bNetworkDrive=1
bCDRom=0
bFastBackup=1
bEnforcement=0
dwEnforceTime=90
pszExcludeProcessNames=
pszExcludeDirs=
dwScanMode=1
dwAction=0
dwBootAction=0
dwMacroCureAction=0
dwSpecialMode=0
dwSpecialCureAction=3
dwFileFilterType=0
pszExtList=|386|ADE|ADP|ADT|ASX|BAS|BAT|BIN|CBT|CHM|CLA|CMD|COM|CPL|CRT|CSC|DLL|D
OC|DOT|DRV|EXE|HLP|HTA|HTM|HTT|INF|INS|ISP|JS|JSE|LNK|MDB|MDE|MSC|MSI|MSO|MSP|MST
|OCX|PCD|PIF|POT|PPT|PRF|REG|RTF|SCF|SCR|SCT|SHB|SHS|SYS|URL|VB|VBE|VBS|VSD|VSS|V
ST|VXD|WIZ|WSC|WSF|WSH|XLA|XLS|XLT|XLW|
pszExcludeExtList=|BTR|DBF|SBF|DB|MDX|NDX|MDW|LDB|
bScanArc=1
bIsArcByExtension=1
dwArcTypesCount=10
pdwArcTypeList=1,2,3,4,6,7,8,9,10,11
bScanAllFilesInArc=1
bStopAtFirstInfectionInArc=1
bScanOnShutDown=0
dwEngineChoice=1
dwPopUpMsgLimit=3
pszBlockExtList=
pszBlockOverrideList=
bEnableAnimation=1
kTime=5
kScanTime=1
```

Option	Description
dwDirection	Direction à contrôler 0 – Temps réel désactivé 1 – Sortant 3 – Entrant et sortant
bFloppyDrive	Analyser le secteur d'amorçage des disquettes : 0 – Non 1 – Oui
bNetworkDrive	Temps réel unités réseau mappé : 0 – Non 1 – Oui
bCDRom	Protéger les CD-ROM : 0 – Non – Ne pas analyser les fichiers sur les lecteurs de CD-ROM 1 – Oui – Analyser les fichiers sur les lecteurs de CD-ROM
bFastBackup	Fonctionner avec ARCserve NT pour permettre la sauvegarde rapide : 0 – Non 1 – Oui
bEnforcement	Permet d'exécuter le mode Quarantaine qui bloque l'accès de l'utilisateur à ce serveur lorsqu'il essaye de copier ou de déplacer un fichier infecté vers un serveur ou de l'y exécuter. 0 – Non – Autorise les utilisateurs à accéder au serveur. 1 – Oui – Bloquer l'accès utilisateur au serveur. Remarque : La durée du verrouillage peut être modifiée par dwEnforceTime.
dwEnforceTime	Durée pendant laquelle la quarantaine doit continuer à bloquer l'accès utilisateur si la surveillance est activée et qu'une tentative d'accès a eu lieu. Cette valeur est définie en minutes et s'étend de 1 à 1440 (24 heures).
pszExcludeProcessNames	Images du processus à exclure. (Séparez chaque élément par « | »)

Option	Description
pszExcludeDirs	Répertoires à exclure. (Séparez chaque élément par « | »)
dwScanMode	Type d'analyse : 1 – Analyse sécurisée 2 – Analyse approfondie
dwAction	Action à entreprendre lors de la détection d'un virus 0 – Rapport seulement 1 – Désinfecter 2 – Renommer 3 – Supprimer 4 – Déplacer
dwBootAction	Lorsqu'un secteur d'amorçage infecté est détecté : 0 – Rapport seulement 1 – Désinfecter le secteur d'amorçage
dwMacroCureAction	Action de désinfection pour les virus de macros : 0 – Ne rien faire 1 – Supprimer toutes les macros 2 – Supprimer les macros infectées
dwSpecialMode	Masque binaire pour activer les techniques avancées de recherche des virus ? 1 – Heuristique 2 – Désinfection du système 4 – Analyser le flux de données NTFS
dwSpecialCureAction	Masque binaire spécifiant l'action à entreprendre lors de la détection d'un virus non classifié 1 – Copier et désinfecter (copier le fichier vers le répertoire de déplacement avant de le désinfecter) 2 – Renommer le fichier si la désinfection échoue 4 – Déplacer le fichier si la désinfection échoue 8 – Supprimer le fichier s'il contient un cheval de Troie

Option	Description
dwFileFilterType	Permet de spécifier le type de fichier à analyser suivant son extension. 0 – Analyser tous les fichiers 1 – Analyser les fichiers portant les extensions par défaut (spécifiées dans pszExtList) 2 – Analyser tous les fichiers sauf ceux portant les extensions par défaut (spécifiées dans pszExcludeExtList)
pszExtList	Liste des extensions par défaut. (Séparez chaque élément par « | »)
pszExcludeExtList	Liste des extensions exclues. (Séparez chaque élément par « | »)
bScanArc	Analyser les fichiers compressés ? 0 – Non 1 – Oui
bIsArcByExtension	Déterminer si des archives existent pour les extensions de fichiers ? 0 – Non (déterminé par les contenus du fichier) 1 – Oui
dwArcTypesCount	Nombre de fichiers contenus dans pdwArcTypeList

Option	Description
pdwArcTypeList	Liste délimitée par des virgules des extensions archivées à analyser : 1 – ARJ 2 – GZIP 3 – Archives JAVA 4 – Archives LHA 5 – Microsoft CAB 6 – Compressé Microsoft 7 – MIME 8 – Fichiers UNIX à UNIX codés (UUEncode) 9 – ZIP 10 – RAR 11 – Compressé Unix (Z) 12 – Fichier Rich Text Format (RTF) 13 – Fichiers messages électroniques TNEF encapsulés
bScanAllFilesInArc	'dwFilterType' s'applique aux fichiers décompressés dans le fichier archivé en cours d'analyse. 0 – Non 1 – Oui
bStopAtFirstInfectionInArc	Arrêter d'analyser des archives de fichiers dès que le premier virus a été détecté ? 0 – Non 1 – Oui
bScanOnShutDown	Rechercher des virus sur le secteur d'amorçage de disquette lors de l'arrêt : 0 – Non 1 – Oui
dwEngineChoice	Sélectionnez un des deux moteurs : 1 – Moteur InoculateIT 2 – Moteur Vet
dwPopUpMsgLimit	Nombre maximum de messages contextuels temps réel qui s'affichent lorsque plusieurs virus sont détectés consécutivement.

Option	Description
pszBlockExtList	Liste de fichiers dont l'exécution doit être bloquée suivant leur extension (séparez chaque élément par un « | »)
pszBlockOverrideList	Liste de fichiers pour lesquels le blocage doit être ignoré. (Séparez chaque élément par un « | »)
bEnableAnimation	Activer l'icône temps réel animée ? 0 – Non 1 – Oui
kTime	Délai utilisé par le pilote pour l'analyse d'un fichier entrant. (Attention si vous modifiez ces valeurs)
kScanTime	Délai utilisé par le pilote pour l'analyse d'un fichier entrant. (Attention si vous modifiez ces valeurs)

AdminServer

Les options AdminServer vous permettent de configurer les options du serveur Admin., notamment les dates et heures de lancement et d'arrêt, les options du journal et les emplacements des répertoires.

```
[AdminServer]
Retries=1
JobPurgeDays=0
LogViolations=1
NoLegacy=0
EnforcePolicy=1
DatabasePathName=Tree
PolicyPathName=Policy
JobPathName=Jobs
```

Option	Description
Retries	Nombre de tentatives à effectuer par le serveur Admin. pour réessayer une interrogation échouée.
JobPurgeDays	Nombre de jours pendant lesquels les jobs d'analyse planifiés sont conservés avant d'être purgés de la base de données du serveur Admin. Si 0 est défini, alors les résultats du job d'analyse planifié ne sont jamais purgés automatiquement.

Option	Description
LogViolations	Consigner lorsqu'un ordinateur violant une règle est détecté ? 0 – Non 1 – Oui
NoLegacy	Si 1 est défini, le serveur Admin. ne tient pas compte des diffusions provenant des ordinateurs exécutant la version 4.x de ce produit. Cela permet de réduire le nombre de threads utilisés par le serveur Admin. de deux et entraîne une utilisation réduite du processeur. Toutefois, les ordinateurs 4.x n'apparaissent pas dans la base de données du serveur Admin. et ne peuvent pas être administrés à partir de l'interface utilisateur graphique 7.0. Si 0 est défini, le serveur Admin. tient compte des diffusions 4.x et ajoute les ordinateurs 4.x à la base de données du serveur Admin.
EnforcePolicy	Contrôler les règles définies pour un ordinateur client ? 0 – Non. Si un ordinateur est trouvé qui viole les règles, rien n'est entrepris. 1 – Oui. Le serveur Admin. essaye de modifier les paramètres pour respecter les règles.
DatabasePathName	Répertoire dans lequel la base de données du serveur Admin. sera placée.
PolicyPathName	Répertoire dans lequel les fichiers de règles du serveur Admin. seront placés.
JobPathName	Répertoire dans lequel les résultats des jobs d'analyse planifiés seront placés.

Analyseur planifié

Les options de l'analyseur planifié vous permettent de définir la configuration des règles de l'analyseur planifié. Ces options sont les paramètres par défaut de l'analyseur utilisés pour l'installation locale.

```
[Scheduled Scanner]
byRepeatMonth=0
byRepeatDay=0
byRepeatHour=0
byRepeatMinute=0
wSpeedLevel=1
bTravelDir=1
dwInfectedBootAction=0
dwScanMode=1
dwAction=0
dwSpecialCureAction=3
dwMacroCureAction=0
dwSpecialMode=0
dwFileFilterType=0
pszExtList=|386|ADE|ADP|ADT|ASX|BAS|BAT|BIN|CBT|CHM|CLA|CMD|COM|CPL|CRT|CSC|DLL|D
OC|DOT|DRV|EXE|HLP|HTA|HTM|HTT|INF|INS|ISP|JS|JSE|LNK|MDB|MDE|MSC|MSI|MSO|MSP|MST
|OCX|PCD|PIF|POT|PPT|PRF|REG|RTF|SCF|SCR|SCT|SHB|SHS|SYS|URL|VB|VBE|VBS|VSD|VSS|V
ST|VXD|WIZ|WSC|WSF|WSH|XLA|XLS|XLT|XLW|
pszExcludeExtList=|BTR|DBF|SBF|DB|MDX|NDX|MDW|LDB|
bScanArc=1
bIsArcByExtension=1
dwArcTypesCount=10
pdwArcTypeList=1,2,3,4,6,7,8,9,10,11
bScanAllFilesInArc=1
bStopAtFirstInfectionInArc=1
bScanMigratedFiles=0
bSkipScannedAsRegularFile=0
bInfectedBootAction=0
dwEngineChoice=1
pszIncludeDirs=*
pszExcludeDirs=
```

Option	Description
byRepeatMonth	Nombre de mois entre les vérifications (0 à 12).
byRepeatDay	Nombre de jours entre les vérifications (0 à 31).
byRepeatHour	Nombre d'heures entre les vérifications (0 à 24).
byRepeatMinute	Nombre de minutes entre les vérifications (0 à 60).
wSpeedLevel	Taux du processeur pouvant être utilisé par l'analyse.

Option	Description
bTravelDir	Parcourir les sous-répertoires lors de l'analyse : 0 – Non 1 – Oui
dwInfectedBootAction	Lorsqu'un secteur d'amorçage infecté est détecté : 0 – Rapport seulement 1 – Désinfecter le secteur d'amorçage
dwScanMode	Type d'analyse 1 – Analyse sécurisée 2 – Analyse approfondie
dwAction	Action à entreprendre lors de la détection d'un virus 0 – Rapport seulement 1 – Désinfecter 2 – Renommer 3 – Supprimer 4 – Déplacer
dwSpecialCureAction	Masque binaire spécifiant l'action à entreprendre lors de la détection d'un virus non classifié 1 – Copier et désinfecter (copier le fichier vers le répertoire de déplacement avant de le désinfecter) 2 – Renommer le fichier si la désinfection échoue 4 – Déplacer le fichier si la désinfection échoue 8 – Supprimer le fichier s'il contient un cheval de Troie ou un ver.
dwMacroCureAction	Action de désinfection pour les virus de macros : 0 – Ne rien faire 1 – Supprimer toutes les macros 2 – Supprimer les macros infectées

Option	Description
dwSpecialMode	Masque binaire pour activer les techniques de recherche des virus avancées 1 – Heuristique 2 – Désinfection du système 4 – Analyser le flux de données NTFS
dwFileFilterType	Permet de spécifier le type de fichier à analyser suivant son extension. 0 – Analyser tous les fichiers 1 – Analyser les fichiers portant les extensions par défaut (spécifiées dans pszExtList) 2 – Analyser tous les fichiers sauf ceux portant les extensions par défaut (spécifiées dans pszExcludeExtList)
pszExtList	Liste des extensions par défaut. (Séparez chaque élément par « | »)
pszExcludeExtList	Liste des extensions exclues. (Séparez chaque élément par « | »)
bScanArc	Analyser les fichiers compressés ? 0 – Non 1 – Oui
bIsArcByExtension	Déterminer si des archives existent pour les extensions de fichiers ? 0 – Non (déterminé par les contenus du fichier) 1 – Oui
dwArcTypesCount	Nombre de fichiers contenus dans pdwArcTypeList.

Option	Description
pdwArcTypeList	Liste délimitée par des virgules des extensions archivées à analyser : 1 – ARJ 2 – GZIP 3 – Archives JAVA 4 – Archives LHA 5 – Microsoft CAB 6 – Compressé Microsoft 7 – MIME 8 – Fichiers UNIX à UNIX codés (UUEncode) 9 – ZIP 10 – RAR 11 – Compressé Unix (Z) 12 – Fichier Rich Text Format (RTF) 13 – Fichiers messages électroniques TNEF encapsulés
bScanAllFilesInArc	'dwFilterType' s'applique aux fichiers décompressés dans le fichier archivé en cours d'analyse.
bStopAtFirstInfectionInArc	Arrêter d'analyser des archives de fichiers dès que le premier virus a été détecté ? 0 – Non 1 – Oui
bScanMigratedFiles	Analyser les fichiers migrés vers des archives externes ? 0 – Non 1 – Oui (les fichiers doivent être restaurés sur l'ordinateur local)
bSkipScannedAsRegularFile	Analyser des archives de la même manière qu'un fichier ordinaire : 0 – Non 1 – Oui
bInfectedBootAction	Désinfecter un secteur d'amorçage infecté : 0 – Non 1 – Oui

Option	Description
dwEngineChoice	Sélectionnez un des deux moteurs : 1 – Moteur InoculateIT 2 – Moteur Vet
pszIncludeDirs	Répertoire par défaut à analyser '*' signifie que l'analyse est effectuée sur tous les disques durs de l'ordinateur
pszExcludeDirs	Liste des répertoires à exclure pendant l'analyse. (Séparez chaque élément par « | »)

VirusAnalyze

L'option VirusAnalyze vous permet d'indiquer où les virus inconnus doivent être envoyés pour être analysés. En général, ils doivent être envoyés à l'administrateur local qui recherche des virus dans le contenu des fichiers et les transmet ensuite à Computer Associates pour une analyse plus complète.

```
[VirusAnalyze]
szSendEMailAddr=virus@ca.com
szSubject=Nouveau virus détecté !!!
szReplyEMailAddr=
szCompanyName=Nom de votre entreprise
szCompanyAddr=Adresse de l'entreprise
szPhone=(555)555-5555
szSiteID=ID de site inconnu
szContactName=John Q. Public
szSmtpServer=
```

Option	Description
szSendEMailAddr	Adresse à laquelle l'exemplaire du virus doit être envoyé. Remarque : Si votre réseau est protégé par un pare-feu, l'adresse doit être un serveur smtp situé au sein de ce pare-feu.
szSubject	Objet du message électronique contenant l'exemplaire du virus.
szReplyEMailAddr	Adresse électronique de réponse pour le message contenant l'exemplaire du virus.
szCompanyName	Nom de la société dans laquelle l'exemplaire du virus a été détecté.

Option	Description
szCompanyAddr	Adresse de la société dans laquelle l'exemplaire du virus a été détecté.
szPhone	Numéro de téléphone de la société ou de l'utilisateur.
szSiteID	ID du site de votre société.
szContactName	Nom de l'interlocuteur ou de l'administrateur de la société.
szSmtpServer	Nom du serveur SMTP utilisé pour envoyer des messages électroniques.

Alert

L'option Alert permet de définir des options servant à la configuration d'un système de notification des alertes. Des options de configuration supplémentaires peuvent être spécifiées dans le fichier instalrt.ini situé dans l'image de l'installation.

```
[Alert]
Local=0
EventLog=0
Custom=0
Error=0
Information=0
Warning=0
NotOlderThan=30
QueueSize=10
Timeout=5
Forward=0
Host=
```

Option	Description
Local	Envoyer les informations de notification au composant du gestionnaire Alert sur l'ordinateur local ? 0 – Non 1 – Oui
EventLog	Envoyer les notifications au journal d'événements système de l'ordinateur local ? 0 – Non 1 – Oui

Option	Description
Custom	Envoyer des messages spécifiques ? 0 – Non 1 – Oui
Erreur	Indiquer que tous les messages d'erreur doivent entraîner une alerte ? 0 – Non 1 – Oui
Informations	Indiquer que tous les messages d'information doivent entraîner une alerte ? 0 – Non 1 – Oui
Avertissement	Indiquer que tous les avertissements doivent entraîner une alerte ? 0 – Non 1 – Oui
NotOlderThan	Tout enregistrement dans le journal d'événements généraux plus ancien que le nombre de jours défini n'est pas inclus dans un rapport.
QueueSize	Nombre d'enregistrements de messages collecté dans le journal des événements généraux, avant la création du rapport sur les informations comme spécifié dans les options Rapport destiné à.
Timeout	Nombre de minutes avant que les informations situées dans le journal des événements généraux ne fassent l'objet d'un rapport comme spécifié dans les options Rapport destiné à.
Forward	Transmettre la notification à un nom d'ordinateur spécifié sur lequel le logiciel antivirus de Computer Associates est installé ? 0 – Non 1 – Oui
Host	Définit le nom de l'ordinateur auquel transmettre les informations de notification.

NameClient

Les options NameClient mettent à votre disposition une liste d'adresses IP de serveurs qui sont autorisés à interroger l'ordinateur d'installation.

```
[NameClient]
ServerList=127.0.0.1
BroadcastPort=42508
PollBroadcastPort=42508
```

Option	Description
ServerList	Contient la liste des adresses IP des serveurs qui sont autorisés à interroger l'ordinateur. Si l'interrogation provient d'un serveur autorisé, l'ordinateur est automatiquement ajouté à l'arborescence. Sinon, l'ordinateur est ajouté à la base de données mais pas à l'arborescence. Aucune règle ne pourra alors être appliquée à l'ordinateur. (séparé par des virgules)
BroadcastPort	Port local recevant des interrogations du serveur Admin.
PollBroadcastPort	Port local recevant des informations à partir d'autres ordinateurs du sous réseau.

Startup

L'option Démarrage vous permet d'exécuter START.JOB pendant l'installation. Les options du job de démarrage sont contenues dans le fichier START.JOB situé dans le répertoire d'installation. C'est un fichier binaire pouvant être créé sur un ordinateur exécutant déjà le programme 7.0. Planifiez le job de démarrage sur cet ordinateur puis copiez START.JOB du répertoire de base vers le répertoire d'installation.

```
[Startup]
bStartJob=0
```

Option	Description
bStartJob	Exécuter le job de démarrage ? 0 – Non 1 – Oui – Exécuter le job au démarrage.

Divers

Cette catégorie est réservée aux options diverses.

```
[Miscellaneous]
StartServiceAfterSetup=1
```

Option	Description
StartServiceAfterSetup	Souhaitez-vous démarrer tous les services (hormis le service temps réel) juste après l'installation ? 0 – Non 1 – Oui

EngineID

L'option EngineID vous permet de spécifier les moteurs d'antivirus à installer.

```
[EngineID]
dwEngIDs=3
```

Option	Description
dwEngIDs	Quels moteurs souhaitez-vous installer ? 1 – Moteur InoculateIT 2 – Moteur Vet 3 – Les deux

PurgeLog

Les options PurgeLog vous permettent d'indiquer la fréquence de purge des anciens journaux et fichiers de l'ordinateur.

```
[PurgeLog]
dwPurgeLogDays=7
dwPurgeMoveDirDays=0
```

Option	Description
dwPurgeLogDays	Nombre de jours pendant lesquels vous souhaitez conserver un journal avant de le purger du client.

Option	Description
dwPurgeMoveDirDays	Nombre de jours pendant lesquels vous souhaitez conserver les fichiers infectés dans le répertoire de déplacement avant de les purger du client. 0 – Ne pas purger automatiquement les fichiers.

InstallComponet

Les options InstallComponent permettent d'indiquer les paramètres de l'installation silencieuse. Utilisez ces paramètres lorsque vous exécutez l'installation avec l'option /s.

```
[InstallComponent]
RealTime=1
JobScheduler=1
LocalScanner=1
AdminService=1
RemoteManagement=1
NetwareSupport=0
Alert=0
KeepOldSettingIfAny=0
Reboot=0
RebootDelay=240
CancelReboot=0
SilentInstallWithProgressBar=1
ShowSaveSettingDialog=1
WebAccess=0
```

Option	Description
Temps réel	Installer le protecteur temps réel ? 0 – Non 1 – Oui
JobScheduler	Réservé à une utilisation ultérieure. Le planificateur de jobs est toujours installé (par défaut = 1)
LocalScanner	Réservé à une utilisation ultérieure. L'analyseur local est toujours installé (par défaut = 1)
AdminService	Installer le serveur Admin. ? 0 – Non 1 – Oui

Option	Description
RemoteManagement	Installer le gestionnaire distant (client administratif) ? 0 – Non 1 – Oui
NetwareSupport	Installer le support Netware ? 0 – Non 1 – Oui
Alert	Installer CA-Alert ? 0 – Non 1 – Oui
KeepOldSettingIfAny	Conserver l'ancien paramètre si une version précédente est installée sur l'ordinateur ? 0 – Non 1 – Oui
Reboot	Redémarrer l'ordinateur après une installation silencieuse ? 0 – Non 2 – Oui
RebootDelay	Nombre de secondes d'attente avant le redémarrage consécutif à l'installation. Remarque : Utilisé uniquement pour l'installation à distance
CancelReboot	Permettre à l'utilisateur d'annuler le redémarrage après une installation silencieuse ? 0 – Non 1 – Oui
SilentInstallWithProgressBar	Affichage d'une barre de progression lors de l'installation silencieuse ? 0 – Ne pas afficher la barre de progression 1 – Afficher la barre de progression
ShowSaveSettingDialog	Afficher la boîte de dialogue d'enregistrement des paramètres ? 0 – Non 1 – Oui

Option	Description
WebAccess	Installer l'accès Web sur le serveur d'administration ? 0 – Non 1 – Oui

SystemSetting

Les options SystemSetting permettent d'indiquer les paramètres du système pour verrouiller les paramètres de configuration et d'exécuter realmon.exe.

```
[SystemSetting]
ConfigLock=0
RemoteSessionRun=1
RemoteSessionStartup=1
```

Options	Description
ConfigLock	Masque binaire permettant de verrouiller les paramètres de configuration pour les utilisateurs : 1 – Verrouiller le temps réel 2 – Verrouiller la distribution de signature(s) 4 – Verrouiller les informations de l'analyse 65535 – Ne pas modifier les paramètres
RemoteSessionRun	Autoriser realmon.exe à s'exécuter dans la barre des tâches pendant la session d'un serveur terminal ? 0 – Non 1 – Oui
RemoteSessionStartup	Autoriser realmon.exe à s'exécuter dans la barre des tâches pendant la session d'un terminal serveur ? 0 – Non 1 – Oui

Job Adjustment

Les options JobAdjustement permettent d'indiquer les paramètres temporels par défaut pour un job d'analyse planifié pour un domaine.

```
[JobAdjustment]
RequestJobMaxWaitHour=8
RequestJobTimeOutMinutes=3
RequestJobEnabled=1
```

Option	Description
RequestJobMaxWaitHour	Nombre maximum d'heures autorisé par l'utilisateur pour retarder un job de règles. (par défaut = 8 heures)
RequestJobTimeOutMinutes	Temporisation pour la boîte de dialogue du job de délai en cas de non réponse de l'utilisateur. (par défaut = 3 minutes)
RequestJobEnabled	Permettre à l'utilisateur de retarder le job de règles transmis à l'ordinateur local ? 0 – Non 1 – Oui

PreAction

Les options PreAction permettent d'indiquer les applications à exécuter avant de copier les fichiers. Ne pas modifier le paramètre App1.

```
[PreAction]
App1=silent.bat
AppDir1=..\License
```

Options	Description
App1	Application à exécuter avant la copie (NE PAS MODIFIER !)
AppDir1	Ce chemin se rapporte au répertoire de compilation. Vous pouvez également définir le chemin entier dans lequel se trouve app1.

PostAction

Les options PostAction permettent d'indiquer les applications à exécuter après l'installation. Ne pas modifier le paramètre App1=.

```
[PostAction]
App1=50comupd /q:a
App2=.\Lang\en\eAV61_en
```

Option	Description
App1	Application à exécuter après l'installation. Vous pouvez ajouter d'autres applications à exécuter dans PostAction, mais NE MODIFIEZ PAS le paramètre pour App1=.
App2	Pack de langue à exécuter après l'installation (NE PAS MODIFIER !)

Fichier INOC6_NW.ICF

Vous pouvez pré-configurer le processus d'installation de votre logiciel eTrust AV en utilisant le fichier de commande INOC6_NW.ICF. Lorsque le programme d'installation démarre, le fichier INOC6_NW.ICF se charge en utilisant les valeurs que vous indiquez.

Les tableaux suivants rassemblent les paramètres par défaut de chaque option du fichier INOC6_NW.ICF, ainsi qu'une description rapide de l'option et des informations supplémentaires sur les variables des options.

Remarque : Bien que vous puissiez utiliser le fichier INOC6_NW.icf pour les installations sous Windows et NetWare, les informations de ce chapitre résument les paramètres pour NetWare.

Path

Les options Path vous permettent de définir les emplacements par défaut pour l'installation des différents composants de eTrust AV.

```
[Path]
HOME=
MOVE=MOVE
ENG=
DB=DB
OUTGOING=OUTGOING
```

Remarque : Les paramètres MOVE, DB et OUTGOING n'ont aucun effet sous Novell. Les valeurs, fixes, sont décrites dans le tableau ci-dessous :

Option	Description
HOME	Répertoire d'installation – Saisissez un volume et un chemin complets, ou laissez cette option vide pour accepter la valeur par défaut. La valeur par défaut est SYS:eTrustAV. Par exemple, SYS:\AV.
MOVE	Répertoire de déplacement – Ce paramètre n'a aucun effet sous NetWare. Le répertoire est fixé à "HOME"\ino\Move. Par exemple, si votre répertoire d'installation est SYS:\AV, votre répertoire de déplacement sera SYS:\AV\ino\Move.
ENG	Répertoire du moteur – Saisissez un volume et un chemin complets, ou laissez cette option vide pour accepter la valeur par défaut. Le répertoire par défaut est "HOME"\AVEngine. Par exemple, si votre répertoire d'installation est SYS:\AV, le répertoire du moteur sera SYS:\AV\AVEngine.
DB	Répertoire de la base de données – Ce paramètre n'a aucun effet sous NetWare. Le répertoire est fixé à "HOME"\ino\DB. Par exemple, si votre répertoire d'installation est SYS:\AV, votre répertoire de base de données sera SYS:\AV\ino\DB.
OUTGOING	Répertoire de sortie des signatures – Ce paramètre n'a aucun effet sous NetWare. Le répertoire est fixé à "HOME"\ino\Outgoing. Par exemple, si votre répertoire d'installation est SYS:\AV, votre répertoire de sortie sera SYS:\AV\ino\Outgoing.

RPCMtAdn

Les options RPCMtAdn vous permettent de spécifier les emplacements des fichiers de base de données du proxy de distribution des règles RPC.

Remarque : NetWare ignore les paramètres de fichier DataBasePath et JobPath. Ces emplacements, fixes, sont décrits dans le tableau ci-dessous :

```
[RPCMtAdn]
DataBasePath=RPCMtDB
JobPath=RPCMtJob
```

Option	Description
DataBasePath	Chemin utilisé par le proxy pour stocker des fichiers de base de données. Ce paramètre n'a aucun effet sous NetWare. Le chemin est fixé à "HOME"\ino\config\RPCMtAdn. Par exemple, si votre répertoire d'installation est SYS:\AV, votre répertoire DataBasePath sera SYS:\AV\ino\config\RPCMtAdn.
JobPath	Chemin utilisé par le proxy pour stocker des fichiers de job. Ce paramètre n'a aucun effet sous NetWare. Le chemin est fixé à "HOME"\ino\config\RPCMtJob. Par exemple, si votre répertoire d'installation est SYS:\AV, votre répertoire JobPath sera SYS:\AV\ino\config\RPCMtJob.

Analyseur local

Les options de l'analyseur local vous permettent de définir les valeurs par défaut de l'analyseur local à partir de l'application de console ETRUSTAV. Pour plus d'informations concernant ETRUSTAV, consultez le chapitre « Utilisation du programme de console ETRUSTAV ».

```
[Local Scanner]
bScanCompressed=1
bScanMemory=0
bScanBootSector=1
bScanFiles=1
dwScanMode=1
dwAction=0
dwSpecialCureAction=3
dwMacroCureAction=0
```

```
dwSpecialMode=0
dwFileFilterType=0
bIsArcByExtension=1
dwArcTypesCount=10
pdwArcTypeList=1,2,3,4,6,7,8,9,10,11,12,13
pszSpecifiedList=|386|ADE|ADP|ADT|ASX|BAS|BAT|BIN|CBT|CHM|CLA|CMD|COM|CPL|CRT|CSC
|DLL|DOC|DOT|DRV|EXE|HLP|HTA|HTM|HTT|INF|INS|ISP|JS|JSE|LNK|MDB|MDE|MSC|MSI|MSO|M
SP|MST|OCX|PCD|PIF|POT|PPT|PRF|REG|RTF|SCF|SCR|SCT|SHB|SHS|SYS|URL|VB|VBE|VBS|VSD
|VSS|VST|VXD|WIZ|WSC|WSF|WSH|XLA|XLS|XLT|XLW|
pszExcludedList=|BTR|DBF|SBF|DB|MDX|NDX|MDW|LDB|
bScanAllFilesInArc=1
bStopAtFirstInfectionInArc=1
bScanMigratedFiles=0
dwEngineChoice=1
dwShowDriveFlags=31
bShowAllFiles=0
bLogCleanFiles=0
bLogInfectedFiles=1
bLogSkippedFiles=0
dwDaysToDeleteLogs=365
dwBootAction=0
bShowSummaryAfterScan=0
```

Option	Description
bScanCompressed	Analyser les fichiers compressés ? 0 – Non 1 – Oui
bScanMemory	Rechercher des virus dans la mémoire ? 0 – Non 1 – Oui
bScanBootSector	Rechercher des virus dans le secteur d'amorçage ? 0 – Non 1 – Oui
bScanFiles	Analyser les fichiers ? (Configurez cette option sur 0 et secteur d'amorçage sur 1 pour analyser uniquement le secteur d'amorçage) 0 – Non 1 – Oui
dwScanMode	Type d'analyse : 1 – Analyse sécurisée 2 – Analyse approfondie

Option	Description
dwAction	Action à entreprendre lors de la détection d'un virus 0 – Rapport seulement 1 – Désinfecter 2 – Renommer 3 – Supprimer 4 – Déplacer
dwSpecialCureAction	Masque binaire spécifiant l'action à entreprendre lors de la détection d'un virus inconnu : 1 – Copier et désinfecter (copier le fichier vers le répertoire de déplacement avant de le désinfecter) 2 – Renommer le fichier si la désinfection échoue 4 – Déplacer le fichier si la désinfection échoue 8 – Supprimer le fichier s'il contient un cheval de Troie ou un ver.
dwMacroCureAction	Action de désinfection pour les virus de macros : 0 – Ne rien faire 1 – Supprimer toutes les macros 2 – Supprimer les macros infectées
dwSpecialMode	Masque binaire pour activer les techniques avancées de recherche des virus ? 1 – Heuristique 2 – Désinfection du système 4 – Analyser le flux de données NTFS
dwFileFilterType	Permet de spécifier le type de fichier à analyser suivant son extension. 0 – Analyser tous les fichiers 1 – Analyser les fichiers portant les extensions par défaut (spécifiées dans pszExtList) 2 – Analyser tous les fichiers sauf ceux portant les extensions par défaut (spécifiées dans pszExcludeExtList)

Option	Description
bIsArcByExtension	Déterminer si des archives existent pour les extensions de fichiers ? 0 – Non (déterminé par les contenus du fichier) 1 – Oui
dwArcTypesCount	Nombre de fichiers contenus dans pdwArcTypeList
pdwArcTypeList	Liste délimitée par des virgules des extensions archivées à analyser : 1 – ARJ 2 – GZIP 3 – Archives JAVA 4 – Archives LHA 5 – Microsoft CAB 6 – Compressé Microsoft 7 – MIME 8 – Fichiers UNIX à UNIX codés (UUEncode) 9 – ZIP 10 – RAR 11 – Compressé Unix (Z) 12 – Fichier Rich Text Format (RTF) 13 – Fichiers messages électroniques TNEF encapsulés
pszSpecifiedList	Liste des extensions par défaut. (Séparez chaque élément par « | »)
pszExcludedList	Liste des extensions exclues. (Séparez chaque élément par « | »)
bScanAllFilesInArc	Analyser tous les fichiers situés dans les archives ? 0 – Non 1 – Oui
bStopAtFirstInfectionInArc	Arrêter d'analyser des archives de fichiers dès que le premier virus a été détecté ? 0 – Non 1 – Oui

Option	Description
bScanMigratedFiles	Analyser les fichiers migrés vers des archives externes ? 0 – Non 1 – Oui (les fichiers doivent être migrés à nouveau vers le disque local)
dwEngineChoice	Sélectionnez un des deux moteurs : 1 – Moteur InoculateIT 2 – Moteur Vet
dwShowDriveFlags	Masque permettant de déterminer les lecteurs affichés : 1 – Disque dur 2 – Unités CD 4 – Unité de disquettes 8 – Unités de réseau 16 – Unités amovibles
bShowAllFiles	Options d'affichage du fichier : 0 – Afficher uniquement les fichiers dont les extensions sont contenues dans pszSpecifiedList 1 – Afficher tous les fichiers
bLogCleanFiles	Ecrire dans le fichier journal si une analyse nettoie un fichier ? 0 – Non 1 – Oui
bLogInfectedFiles	Ecrire dans le fichier journal si une analyse détecte un fichier infecté ? 0 – Non 1 – Oui
bLogSkippedFiles	Ecrire dans le fichier journal si des fichiers sont ignorés par une analyse ? 0 – Non 1 – Oui
dwDaystoDeleteLogs	Nombre de jours pendant lesquels un fichier journal est gardé avant sa suppression.

Option	Description
dwBootAction	Lorsqu'un secteur d'amorçage infecté est détecté : 0 – Rapport seulement 1 – Désinfecter le secteur d'amorçage
bShowSummaryAfterScan	Afficher la boîte de dialogue Résumé après chaque analyse ? 0 – Non 1 – Oui

Distribution

Les options de distribution vous permettent de configurer les options pour la récupération et la distribution des signatures locales. Pour configurer la redistribution des mises à jour de signatures par un serveur NetWare, consultez l'annexe « Configuration de serveurs NetWare pour distribuer des mises à jour de signatures ».

```
[Distribution]
dwStateMask=0
tExecTime=
byRepeatMonth=0
byRepeatDay=0
byRepeatHour=0
byRepeatMinute=0
dwRepeatTimesOnFail=3
dwRepeatMinutesOnFail=5
dwHoldTimeQueryInterval=60
bDownloadNow=0
dwPopupMessage=0
bHideIcon=0
```

Option	Description
dwStateMask	Etat de distribution 0 – Désactivé 1 – Entrant (récupération des mises à jour) 2 – Sortant (permet à d'autres de récupérer des mises à jour à partir de leurs ordinateurs locaux) 3 – Entrant et sortant

Option	Description
tExecTime	Heure à laquelle est vérifié si des nouveaux fichiers de signatures se trouvent sur les serveurs distants : Format : JJ/MM/AAAA,HH:MM:SS,Heure d'été (Heure d'été = 1 si l'horaire est en heure d'été, 0 dans le cas contraire.) Par exemple, 04/12/1999,23:23:23,0
byRepeatMonth	Nombre de mois entre les vérifications (0 à 12)
byRepeatDay	Nombre de jours entre les vérifications (0 à 31)
byRepeatHour	Nombre d'heures entre les vérifications (0 à 24)
byRepeatMinute	Nombre de minutes entre les vérifications (0 à 60)
dwRepeatTimesOnFail	Nombre de tentatives que le planificateur de jobs doit effectuer si le téléchargement des signatures échoue. Utilisez cette valeur avec dwRepeatMinutesOnFail pour déterminer le nombre de tentatives pouvant être effectuées pour un téléchargement. Les tentatives sont effectuées jusqu'à ce que : ■ un téléchargement réussisse. ■ le nombre de tentatives dépasse dwRepeatTimesOnFail ■ un téléchargement planifié s'effectue **Remarque :** Définissez sur 0 pour désactiver les tentatives.
dwRepeatMinutesOnFail	Nombre de minutes entre les tentatives dans l'éventualité d'un échec. Cette valeur est utilisée avec dwRepeatTimesOnFail pour déterminer le nombre de tentatives.
dwHoldTimeQueryInterval	Nombre de fois (par minutes) où le programme vérifie dans le répertoire entrant la présence de nouvelles signatures disponibles pour les copier dans le répertoire sortant à des fins de distribution.

Option	Description
bDownloadNow	Télécharger une nouvelle signature directement après l'installation ? (Requiert qu'un fichier inodist.ini contienne un site ftp et un serveur proxy valides) 0 – Non 1 – Oui
dwPopupMessage	Ne s'applique pas à NetWare
bHideIcon	Ne s'applique pas à NetWare
dwTimeOut	Nombre de secondes sans réponse du serveur avant de considérer que le téléchargement a échoué

Realtime

Les options Realtime vous permettent de configurer les règles locales de temps réel. Ces options sont les paramètres par défaut de temps réel utilisés pour l'installation locale.

```
[Realtime]
dwDirection=3
bFloppyDrive=1
bNetworkDrive=1
bCDRom=0
bFastBackup=1
bEnforcement=0
dwEnforceTime=90
pszExcludeProcessNames=
pszExcludeDirs=
dwScanMode=1
dwAction=0
dwBootAction=0
dwMacroCureAction=0
dwSpecialMode=0
dwSpecialCureAction=3
dwFileFilterType=0
pszExtList=|386|ADE|ADP|ADT|ASX|BAS|BAT|BIN|CBT|CHM|CLA|CMD|COM|CPL|CRT|CSC|DLL|D
OC|DOT|DRV|EXE|HLP|HTA|HTM|HTT|INF|INS|ISP|JS|JSE|LNK|MDB|MDE|MSC|MSI|MSO|MSP|MST
|OCX|PCD|PIF|POT|PPT|PRF|REG|RTF|SCF|SCR|SCT|SHB|SHS|SYS|URL|VB|VBE|VBS|VSD|VSS|V
ST|VXD|WIZ|WSC|WSF|WSH|XLA|XLS|XLT|XLW|
pszExcludeExtList=|BTR|DBF|SBF|DB|MDX|NDX|MDW|LDB|
bScanArc=1
bIsArcByExtension=1
dwArcTypesCount=10
pdwArcTypeList=1,2,3,4,6,7,8,9,10,11
bScanAllFilesInArc=1
bStopAtFirstInfectionInArc=1
bScanMigratedFiles=0
bScanOnShutDown=0
dwEngineChoice=1
dwPopUpMsgLimit=3
pszBlockExtList=
pszBlockOverrideList=
bEnableAnimation=1
kTime=5
kScanTime=1
```

Option	Description
dwDirection	Direction à contrôler : 0 – Temps réel désactivé 1 – Sortant 3 – Entrant et sortant
bFloppyDrive	Ne s'applique pas à NetWare
bNetworkDrive	Ne s'applique pas à NetWare
bCDRom	Ne s'applique pas à NetWare
bFastBackup	Ne s'applique pas à NetWare
bEnforcement	Ne s'applique pas à NetWare
dwEnforceTime	Ne s'applique pas à NetWare
pszExcludeProcessNames	Noms des threads à exclure. (Séparez chaque élément par « | »)
pszExcludeDirs	Répertoires à exclure. (Séparez chaque élément par « | »)
dwScanMode	Type d'analyse : 1 – Analyse sécurisée 2 – Analyse approfondie
dwAction	Action à entreprendre lors de la détection d'un virus : 0 – Rapport seulement 1 – Désinfecter 2 – Renommer 3 – Supprimer 4 – Déplacer
dwBootAction	Ne s'applique pas à NetWare
dwMacroCureAction	Action de désinfection pour les virus de macros : 0 – Ne rien faire 1 – Supprimer toutes les macros 2 – Supprimer les macros infectées
dwSpecialMode	Masque binaire pour activer les techniques avancées de recherche des virus ? 1 – Heuristique

Option	Description
dwSpecialCureAction	Masque binaire spécifiant l'action à entreprendre lors de la détection d'un virus non classifié : 1 – Copier et désinfecter (copier le fichier vers le répertoire de déplacement avant de le désinfecter) 2 – Renommer le fichier si la désinfection échoue 4 – Déplacer le fichier si la désinfection échoue 8 – Supprimer le fichier s'il contient un cheval de Troie
dwFileFilterType	Permet de spécifier le type de fichier à analyser suivant son extension : 0 – Analyser tous les fichiers 1 – Analyser les fichiers portant les extensions par défaut (spécifiées dans pszExtList) 2 – Analyser tous les fichiers sauf ceux portant les extensions par défaut (spécifiées dans pszExcludeExtList)
pszExtList	Liste des extensions par défaut. (Séparez chaque élément par « | »)
pszExcludeExtList	Liste des extensions exclues. (Séparez chaque élément par « | »)
bScanArc	Analyser les fichiers compressés ? 0 – Non 1 – Oui
bIsArcByExtension	Déterminer si un fichier est une archive par son extension ? 0 – Non (déterminé par les contenus du fichier) 1 – Oui
dwArcTypesCount	Nombre de fichiers contenus dans pdwArcTypeList

Option	Description
pdwArcTypeList	Liste délimitée par des virgules des extensions archivées à analyser : 1 – ARJ 2 – GZIP 3 – Archives JAVA 4 – Archives LHA 5 – Microsoft CAB 6 – Compressé Microsoft 7 – MIME 8 – Fichiers UNIX à UNIX codés (UUEncode) 9 – ZIP 10 – RAR 11 – Compressé Unix (Z) 12 – Fichier Rich Text Format (RTF) 13 – Fichiers messages électroniques TNEF encapsulés
bScanAllFilesInArc	'dwFilterType' s'applique aux fichiers décompressés dans le fichier archivé. 0 – Non 1 – Oui
bStopAtFirstInfectionInArc	Arrêter d'analyser des archives de fichiers dès que le premier virus a été détecté ? 0 – Non 1 – Oui
bScanMigratedFiles	Analyser les fichiers migrés vers des archives externes ? 0 – Non 1 – Oui (les fichiers doivent être restaurés sur l'ordinateur local)
bScanOnShutDown	Ne s'applique pas à NetWare
dwEngineChoice	Sélectionnez un des deux moteurs : 1 – Moteur InoculateIT 2 – Moteur Vet
dwPopUpMsgLimit	Ne s'applique pas à NetWare

Option	Description
pszBlockExtList	Bloque l'exécution de la liste des fichiers en fonction de leur extension. (Séparez chaque élément par « | »)
pszBlockOverrideList	Liste de fichiers pour lesquels le blocage doit être ignoré. (Séparez chaque élément par « | »)
bEnableAnimation	Ne s'applique pas à NetWare
kTime	Ne s'applique pas à NetWare
kScanTime	Ne s'applique pas à NetWare

Scheduled Scanner

Les options de l'analyseur planifié vous permettent de définir la configuration des règles de l'analyseur planifié. Ces options sont les paramètres par défaut de l'analyseur utilisés pour l'installation locale :

```
[Scheduled Scanner]
byRepeatMonth=0
byRepeatDay=0
byRepeatHour=0
byRepeatMinute=0
wSpeedLevel=1
bTravelDir=1
dwInfectedBootAction=0
dwScanMode=1
dwAction=0
dwSpecialCureAction=3
dwMacroCureAction=0
dwSpecialMode=0
dwFileFilterType=0
pszExtList=|386|ADE|ADP|ADT|ASX|BAS|BAT|BIN|CBT|CHM|CLA|CMD|COM|CPL|CRT|CSC|DLL|D
OC|DOT|DRV|EXE|HLP|HTA|HTM|HTT|INF|INS|ISP|JS|JSE|LNK|MDB|MDE|MSC|MSI|MSO|MSP|MST
|OCX|PCD|PIF|POT|PPT|PRF|REG|RTF|SCF|SCR|SCT|SHB|SHS|SYS|URL|VB|VBE|VBS|VSD|VSS|V
ST|VXD|WIZ|WSC|WSF|WSH|XLA|XLS|XLT|XLW|
pszExcludeExtList=|BTR|DBF|SBF|DB|MDX|NDX|MDW|LDB|
bScanArc=1
bIsArcByExtension=1
dwArcTypesCount=10
pdwArcTypeList=1,2,3,4,6,7,8,9,10,11
bScanAllFilesInArc=1
bStopAtFirstInfectionInArc=1
bScanMigratedFiles=0
bSkipScannedAsRegularFile=0
bInfectedBootAction=0
dwEngineChoice=1
pszIncludeDirs=*
pszExcludeDirs=
```

Option	Description
byRepeatMonth	Nombre de mois entre les analyses (0 à 12)
byRepeatDay	Nombre de jours entre les analyses (0 à 31)
byRepeatHour	Nombre d'heures entre les analyses (0 à 24)
byRepeatMinute	Nombre de minutes entre les analyses (0 à 60)
wSpeedLevel	Ne s'applique pas à NetWare
bTravelDir	Parcourir les sous-répertoires lors de l'analyse : 0 – Non 1 – Oui
dwInfectedBootAction	Ne s'applique pas à NetWare
dwScanMode	Type d'analyse : 1 – Analyse sécurisée 2 – Analyse approfondie
dwAction	Action à entreprendre lors de la détection d'un virus : 0 – Rapport seulement 1 – Désinfecter 2 – Renommer 3 – Supprimer 4 – Déplacer
dwSpecialCureAction	Masque binaire spécifiant l'action à entreprendre lors de la détection d'un virus non classifié : 1 – Copier et désinfecter (copier le fichier vers le répertoire de déplacement avant de le désinfecter) 2 – Renommer le fichier si la désinfection échoue 4 – Déplacer le fichier si la désinfection échoue 8 – Supprimer le fichier s'il contient un cheval de Troie ou un ver.

Option	Description
dwMacroCureAction	Action de désinfection pour les virus de macros : 0 – Ne rien faire 1 – Supprimer toutes les macros 2 – Supprimer les macros infectées
dwSpecialMode	Masque binaire pour activer les techniques de recherche des virus avancées : 1 – Heuristique
dwFileFilterType	Permet de spécifier le type de fichier à analyser suivant son extension : 0 – Analyser tous les fichiers 1 – Analyser les fichiers portant les extensions par défaut (spécifiées dans pszExtList) 2 – Analyser tous les fichiers sauf ceux portant les extensions par défaut (spécifiées dans pszExcludeExtList)
pszExtList	Liste des extensions par défaut. (Séparez chaque élément par « | »)
pszExcludeExtList	Liste des extensions exclues. (Séparez chaque élément par « | »)
bScanArc	Analyser les fichiers compressés ? 0 – Non 1 – Oui
bIsArcByExtension	Déterminer si un fichier est une archive par son extension ? 0 – Non (déterminé par les contenus du fichier) 1 – Oui
dwArcTypesCount	Nombre de fichiers contenus dans pdwArcTypeList

Option	Description
pdwArcTypeList	Liste délimitée par des virgules des extensions archivées à analyser : 1 – ARJ 2 – GZIP 3 – Archives JAVA 4 – Archives LHA 5 – Microsoft CAB 6 – Compressé Microsoft 7 – MIME 8 – Fichiers UNIX à UNIX codés (UUEncode) 9 – ZIP 10 – RAR 11 – Compressé Unix (Z) 12 – Fichier Rich Text Format (RTF) 13 – Fichiers messages électroniques TNEF encapsulés
bScanAllFilesInArc	'dwFilterType' s'applique aux fichiers décompressés dans le fichier archivé. 0 – Non 1 – Oui
bStopAtFirstInfectionInArc	Arrêter d'analyser des archives de fichiers dès que le premier virus a été détecté ? 0 – Non 1 – Oui
bScanMigratedFiles	Analyser les fichiers migrés vers des archives externes ? 0 – Non 1 – Oui (les fichiers doivent être restaurés sur l'ordinateur local)
bSkipScannedAsRegularFile	Analyser des archives de la même manière qu'un fichier ordinaire : 0 – Non 1 – Oui
bInfectedBootAction	Ne s'applique pas à NetWare

Option	Description
dwEngineChoice	Sélectionnez un des deux moteurs : 1 – Moteur InoculateIT 2 – Moteur Vet
pszIncludeDirs	Répertoire par défaut à analyser
pszExcludeDirs	Liste des répertoires à exclure pendant l'analyse. (Séparez chaque élément par « | »)

VirusAnalyze

En l'absence d'analyseur local dans la version NetWare de eTrust AV, et dans la mesure où les options de cette section s'appliquent toutes aux opérations que l'analyseur local ne peut effectuer que sur d'autres plates-formes, cette section du fichier ne s'applique pas à NetWare.

Alert

L'option Alert permet de définir des options servant à la configuration d'un système de notification des alertes. Vous pouvez spécifier des options de configuration supplémentaires dans le fichier instalrt.ini situé dans l'image de l'installation.

```
[Alert]
Local=0
EventLog=0
Custom=0
Error=0
Information=0
Warning=0
NotOlderThan=30
QueueSize=10
Timeout=5
Forward=0
Host=
```

Option	Description
Local	Ne s'applique pas à NetWare
EventLog	Envoyer les notifications à la console de l'ordinateur local ? 0 – Non 1 – Oui

Option	Description
Custom	Envoyer des messages spécifiques ? 0 – Non 1 – Oui
Erreur	Indiquer que tous les messages d'erreur doivent entraîner une alerte ? 0 – Non 1 – Oui
Informations	Indiquer que tous les messages d'information doivent entraîner une alerte ? 0 – Non 1 – Oui
Avertissement	Indiquer que tous les avertissements doivent entraîner une alerte ? 0 – Non 1 – Oui
NotOlderThan	Tout enregistrement dans le journal d'événements généraux plus ancien que le nombre de jours défini n'est pas inclus dans un rapport.
QueueSize	Nombre d'enregistrements de messages collecté dans le journal des événements généraux, avant la création du rapport sur les informations comme spécifié dans les options Rapport destiné à.
Timeout	Nombre de minutes avant que les informations situées dans le journal des événements généraux ne fassent l'objet d'un rapport comme spécifié dans les options Rapport destiné à.
Forward	Transmettre la notification à un nom d'ordinateur spécifié sur lequel le logiciel antivirus de CA est installé ? 0 – Non 1 – Oui
Host	Définit le nom de l'ordinateur auquel transmettre les informations de notification.

NameClient

Les options NameClient mettent à votre disposition une liste d'adresses IP de serveurs qui sont autorisés à interroger l'ordinateur d'installation.

```
[NameClient]
ServerList=127.0.0.1
BroadcastPort=42508
PollBroadcastPort=42508
```

Option	Description
ServerList	Contient la liste délimitée par des virgules des adresses IP des serveurs Admin autorisés à interroger l'ordinateur. Si l'interrogation provient d'un serveur Admin autorisé, l'ordinateur est automatiquement ajouté à l'arborescence du serveur Admin. Sinon, l'ordinateur est n'ajouté qu'à la base de données, de sorte que vous ne pouvez appliquer la règle à l'ordinateur sans une authentification correcte.
PollBroadcastPort	Port local recevant des interrogations du serveur Admin.
BroadcastPort	Port local recevant des informations d'interrogation à partir d'autres ordinateurs du sous-réseau.

Divers

Cette catégorie concerne les options diverses.

```
[Miscellaneous]
StartServiceAfterSetup=1
StartServicesOnReboot=0
```

Option	Description
StartServiceAfterSetup	Souhaitez-vous démarrer tous les services après l'installation ? 0 – Non 1 – Oui
StartServicesOnReboot	Souhaitez-vous démarrer tous les services lors du démarrage du système ? 0 – Non 1 – Oui

EngineID

L'option EngineID vous permet de spécifier les moteurs d'antivirus à installer.

```
[EngineID]
dwEngIDs=3
```

Option	Description
dwEngIDs	Quels moteurs souhaitez-vous installer ? 1 – Moteur InoculateIT 2 – Moteur Vet 3 – Les deux

PurgeLog

Les options PurgeLog vous permettent d'indiquer la fréquence de purge des anciens journaux et fichiers de l'ordinateur.

```
[PurgeLog]
dwPurgeLogDays=7
dwPurgeMoveDirDays=0
```

Option	Description
dwPurgeLogDays	Nombre de jours pendant lesquels vous souhaitez conserver un journal avant de le purger
dwPurgeMoveDirDays	Nombre de jours pendant lesquels vous souhaitez conserver les fichiers infectés dans le répertoire de déplacement avant de les purger : 0 – Ne pas purger automatiquement les fichiers.

InstallComponent

NetWare utilise l'option de valeur KeepOldSettingIfAny pendant l'installation. La valeur par défaut est 1, qui conserve les anciens paramètres de configuration s'il existe déjà une installation de eTrust AV. La valeur 1 fait également migrer (le cas échéant) les paramètres d'une installation antérieure d'InoculateIT 4.x vers la nouvelle installation. La valeur 0 se traduit par une installation nouvelle de eTrust AV, aucun paramètre n'étant récupéré d'une installation antérieure.

NovellSpecific

Cette catégorie concerne les options spécifiques de Novell.

```
[NovellSpecific]
Keep4XInstall=yes
InstallArcAv=yes
```

Option	Description
Keep4XInstall	L'option Keep4XInstall permet de conserver une installation d'InoculateIT 4.x. Si cette option est définie sur oui, le programme d'installation ne supprime pas les fichiers d'installation d'InoculateIT 4.x. Si cette option est définie sur non, le programme d'installation supprime tous les fichiers d'installation d'InoculateIT 4.x, à l'exception du composant Alert.
InstallArcAv	L'option InstallArcAv permet d'installer le service ArcAV. Les valeurs correctes pour cette option sont oui et non. Si elle est définie sur oui (par défaut), le service est installé. Si elle est définie sur non, le service n'est pas installé et sera supprimé au cours d'une réinstallation. Indépendamment de cette option, le programme ArcAV (ArcAv.nlm) sera copié sur le serveur afin d'être installé (ou supprimé) ultérieurement. Le service ArcAv prend en charge la sauvegarde BrightStor ARCserve pour NetWare. ARCserve communique avec le service ArcAV lors de l'exécution des sauvegardes. Il n'est pas obligatoire d'installer ARCserve sur le même ordinateur qu'ArcAV. Si des sauvegardes distantes sont exécutées sur le serveur sur lequel fonctionne ArcAV, ArcAV est utilisé pour la prise en charge d'ARCserve.

Annexe

F

Fichier InoDist.ini

Options de mise à jour des signatures dans le fichier InoDist.ini

Le fichier InoDist.ini contient des paramètres spécifiant comment et quand les mises à jour du moteur et des signatures sont collectées à partir d'une source de distribution.

En règle générale, vous devez utiliser l'interface utilisateur du logiciel antivirus de Computer Associates pour définir les options de mise à jour des signatures. Vous pouvez accéder à ces options à partir du menu Analyseur dans l'affichage Analyseur local ou depuis l'affichage de l'administrateur. Toutefois, vous pouvez éditer les paramètres dans le fichier InoDist.ini pour rechercher la cause des problèmes rencontrés ou pour contrôler rapidement les paramètres courants pour la mise à jour des signatures dans votre environnement.

Le fichier InoDist.ini est installé dans le répertoire ScanEngine et peut être visualisé ou édité à l'aide d'un éditeur de texte.

(SOURCES)

La section [SOURCES] fournit les noms des autres sections du fichier InoDist.ini qui indiquent la connexion pour le téléchargement de la signature. Il existe trois types de connexion disponibles à partir de l'interface utilisateur : FTP, UNC/serveur de redistribution et chemin local. Veuillez vous reporter à la section Source des signatures ci-dessous pour obtenir plus d'informations sur les options relatives à chaque type de connexion.

Avertissement : Les valeurs numériques de la liste des sources doivent être consécutives. Ne modifiez pas l'ordre numérique et ne créez aucun espace vide entre les séquences numériques.

```
[SOURCES]
1=SourceA
2=SourceB
3=SourceC
```

Option	Description
1=SourceA	Première source. Par exemple, 1=UNC_0
2=SourceB	Deuxième source. Par exemple, 2=UNC_1
3=SourceC	Troisième source. Par exemple, 3=FTP_0

Source des signatures

Pour les sources de signatures décrites dans la section [SOURCES] du fichier InoDist.ini, il existe une section spécifique décrivant toutes les informations nécessaires pour le téléchargement du site distant.

FTP

Lorsque FTP est indiqué comme méthode de téléchargement, les options suivantes sont disponibles :

```
[SourceA]
Method=FTP
HostName=ftpav.ca.com
UserName=anonymous
UserPassword=Somebody@somecompany.com
FastConnection=0
ProxyName=
UpdatePath=/pub/inoculan/scaneng/
```

Option	Description
Method=FTP	Utilisation de FTP comme méthode de téléchargement.
HostName=ftpav.ca.com	Adresse du nom d'hôte.
UserName=anonymous	Nom d'utilisateur pour la connexion FTP.
UserPassword=Somebody@somecompany.com	Mot de passe utilisateur pour la connexion FTP.
FastConnection=0	Inutilisé actuellement, mais doit être défini sur zéro.

Option	Description
ProxyName=	Connexion à Internet par le serveur proxy indiqué.
UpdatePath=/pub/inoculan/scaneng/	Chemin de la mise à jour.

UNC/Redistribution Server

Lorsque UNC est indiqué comme méthode de téléchargement, les options suivantes sont disponibles :

```
[SourceB]
Method=UNC
Path=\\usprusd1\inoupd$
UserName=anonymous
UserPassword=Somebody@somecompany.com
RedistGui=1
```

Option	Description
Method=UNC	Utilisation de UNC comme méthode de téléchargement.
Path=\\redist\inoupd$	Chemin UNC.
UserName=anonymous	Nom d'utilisateur UNC.
UserPassword=Somebody@somecompany.com	Mot de passe utilisateur.
RedistGui=1	1= Affiche les informations relatives à la connexion dans l'interface utilisateur. 0= N'affiche pas les informations relatives à la connexion dans l'interface utilisateur. Les serveurs UNC affichent le nom complet du chemin. Les serveurs de redistribution affichent uniquement le nom du serveur.

Local

Lorsque Local est indiqué comme méthode de téléchargement, les options suivantes sont disponibles :

```
[SourceC]
Method=LOCAL
Path=c:\test
```

Option	Description
Méthode	Utilisation du serveur local comme méthode de téléchargement.
Path	Chemin local.

(GET)

Vous pouvez utiliser la section [GET] pour identifier la plate-forme du système d'exploitation et les mises à jour de moteurs à télécharger. Si vous choisissez UpdateLocalSignatures=1 dans la section [POLICY], la section [GET] est vide. Vous devez choisir UpdateLocalSignatures=0 dans la section [POLICY] pour activer la section [GET].

```
[GET]
;1=SIG_1_3
;2=SIG_2_3
;3=SIG_1_4
```

Option	Système d'exploitation et mises à jour de moteurs
1=SIG 1 3	Windows 9x/Me et InoculateIT
2=SIG 2 3	Windows 9x/Me et VET
3=SIG 1 4	Windows NT/2000 (x86) et InoculateIT

(POLICY)

Les options [POLICY] permettent d'identifier les mesures à prendre pendant et après le téléchargement des signatures.

```
[POLICY]
UpdateLocalSignatures=1
SignatureHoldTime=0
MakeIncDownloading=1
IsDistributionServer=0
```

Option	Description
UpdateLocalSignatures=1	1 – Télécharger les fichiers de signatures nécessaires à la mise à jour de l'ordinateur local et les utiliser pour la mise à jour de ce dernier, qu'ils soient ou non issus de la section [OBTENIR]. 0 – Télécharger uniquement les fichiers énumérés dans la section [OBTENIR]. Ces fichiers ne seront pas utilisés pour la mise à jour de l'ordinateur local.
SignatureHoldTime=0	Spécifier le nombre d'heures de mise en attente des nouvelles signatures avant de les rendre disponibles pour le téléchargement sur d'autres ordinateurs du réseau.
MakeIncDownloading=1	Vous pouvez indiquer que seuls les fichiers qui ont changé doivent être téléchargés. Il en résulte un fichier de mise à jour des signatures plus petit, appelé téléchargement incrémentiel. Un téléchargement incrémentiel assure une protection antivirus totale, mais peut être plus rapide qu'un téléchargement complet. 1 – Le programme de téléchargement détermine si une mise à jour complète est nécessaire ou si une mise à jour incrémentielle peut être utilisée. 0 – Effectuer un téléchargement complet.

Option	Description
IsDistributionServer=0	1 – Conserver les mises à jour de signatures complètes et incrémentielles en les téléchargeant toutes les deux et en les synchronisant. Défini sur 1, ce paramètre ignore la sélection de MakeIncDownloading. Computer Associates vous recommande de conserver les signatures issues des mises à jour complètes et incrémentielles sur tous les serveurs de redistribution.

(OSID)

Les options [OSID] mappent les noms des plates-formes avec les identificateurs utilisés pour reporter des éléments sur le site Web. Les valeurs spécifiées dans cette section figurent dans la section des éléments de définition des signatures, dans le fichier Siglist.txt présent sur le serveur et sur l'interface utilisateur via un fichier Platform.ini.

Les éléments de cette section sont automatiquement définis, en fonction de la liste de plates-formes actuellement prises en charge. Les éléments de la section [OSID] ne doivent pas être modifiés.

```
[OSID]
Linux (Intel)=8
Sun Solaris=9
;Windows 3x/Netware=2
Windows 9x/ME=3
Windows NT/2000 (x86)=4
```

(ENGINEID)

Les options [ENGINEID] mappent les noms de moteurs énumérés dans la signature définie sur la valeur ID.

```
[ENGINEID]
INOCULATEIT=1
```

VET=2

Annexe

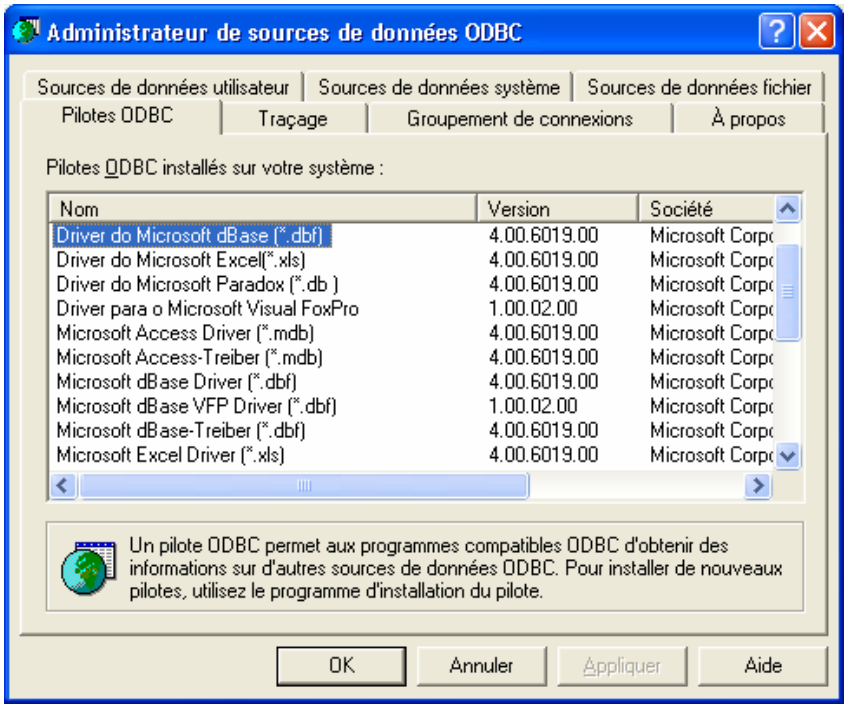
G

Installation de la connexion à la source de données ODBC

Pour pouvoir utiliser une source de données ODBC avec la base de données de rapports eTrust Antivirus, vous devez connecter votre base de données ODBC à celle de eTrust Antivirus par le biais de l'interface InfoReports.

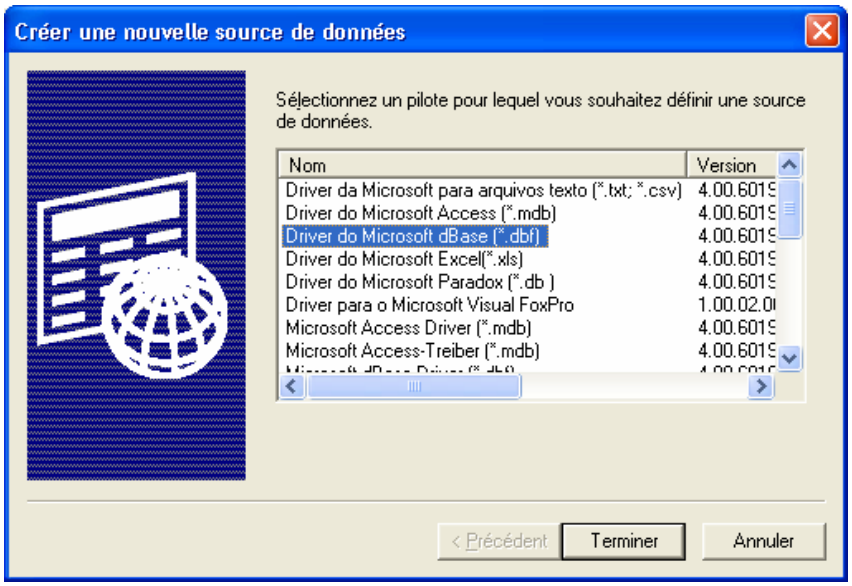
Procédure d'installation

1. Sélectionnez Démarrer, Paramètres, Panneau de configuration.
2. Sélectionnez Outils d'administration.
3. Sélectionnez Sources de données (ODBC).

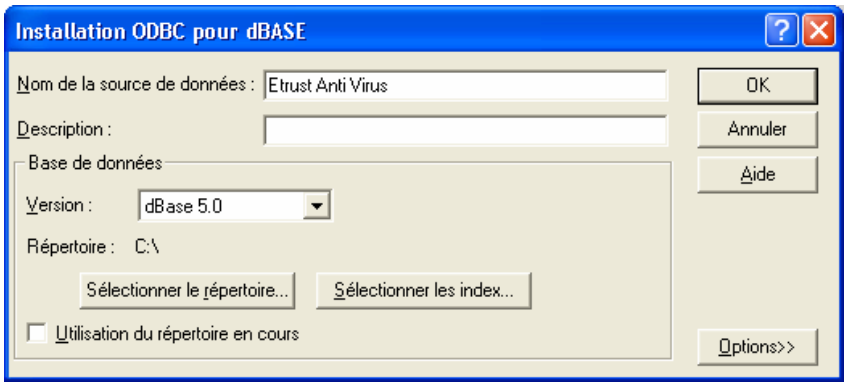


4. Sélectionnez l'onglet Source de données utilisateur et cliquez sur Ajouter. La sélection de cet onglet rend cette source de données accessible uniquement par l'utilisateur courant. Sélectionnez Sources de données système si vous souhaitez que tous les utilisateurs y aient accès.

5. Dans la fenêtre Créer une nouvelle source de données, sélectionnez Driver do Microsoft dBase (*.dbf).

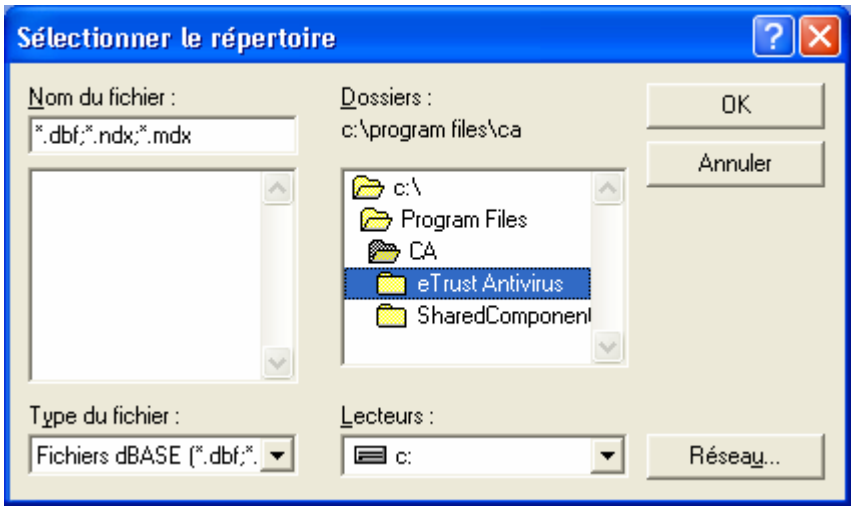


6. Cliquez sur Terminer.
7. Entrez un nom dans le champ Nom de la source de données. Utilisez une désignation descriptive, telle que Base de données Antivirus.
8. Supprimez la coche de la case Utilisation du répertoire en cours.

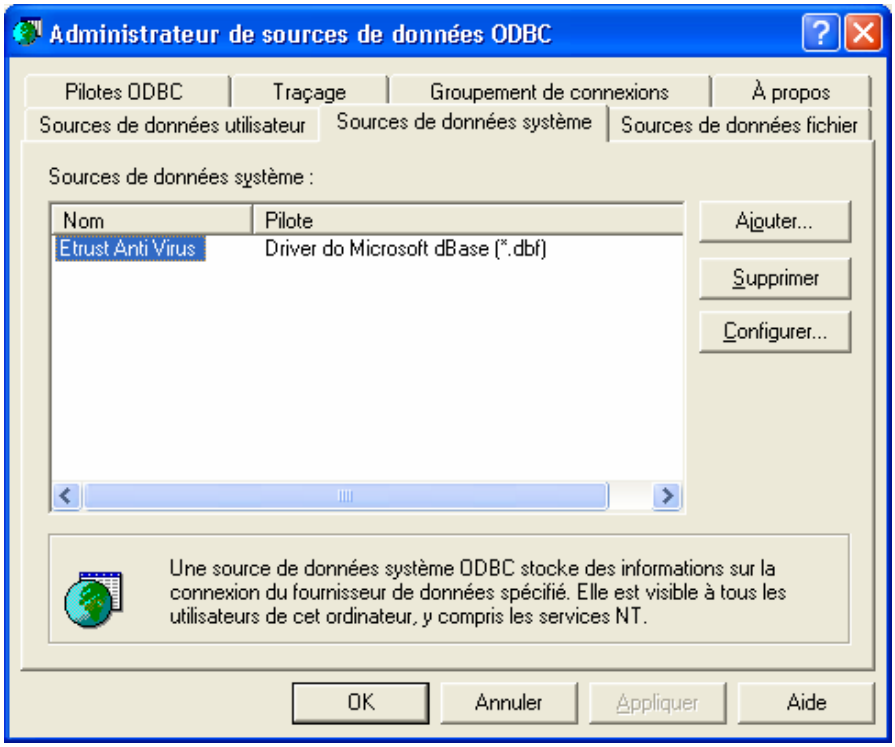


9. Cliquez sur Sélectionner le répertoire…

10. Naviguez à travers l'arborescence jusqu'au répertoire C:\Program Files\CA\eTrust Antivirus\DB\.



11. Cliquez sur OK.
12. Cliquez sur OK dans la fenêtre Installation ODBC pour dBase.



13. Cliquez sur OK pour fermer la fenêtre Administrateur de sources de données ODBC.

Le connecteur ODBC est maintenant installé.

Vous pouvez également accéder à l'administrateur de sources de données en exécutant Démarrer, Programmes, Outils d'administration, Sources de données (ODBC).

Installation d'InfoReports de CA

InfoReports de CA est situé sur le CD dans le répertoire \bin\support\report. Vous devrez installer InfoSuite et le serveur Admin. Cliquez sur OK pour continuer.

Veuillez sélectionner les composants que vous souhaitez installer. Vous devez au moins installer InfoReports. Vous pouvez installer l'administrateur InfoReports, les exemples de rapports et la documentation en ligne si vous le souhaitez.

La création de rapports est facilitée si vous copiez les exemples de rapports dans le répertoire de travail d'InfoReports afin de pas avoir à les rechercher. Lorsque vous ouvrez un exemple de rapport pour créer un rapport, veillez à sélectionner votre nouveau DSN comme source de données.

Sélectionnez Fichier/Aperçu avant impression pour visualiser le rapport.

Annexe

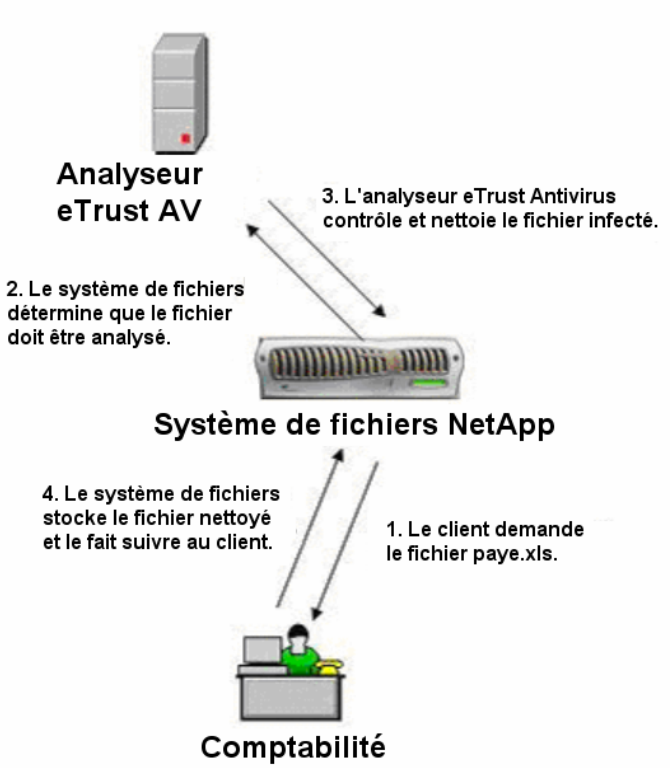
H

Installation et utilisation de l'analyseur eTrust Antivirus pour un système de fichiers NetApp

Cette annexe explique comment installer et utiliser l'analyseur Network Appliance de eTrust Antivirus avec un système de fichiers Network Appliance™ (NetApp®).

Introduction

L'analyseur Network Appliance de eTrust Antivirus s'intègre à un système de fichiers NetApp et protège vos données des virus en temps réel. L'analyseur peut automatiquement nettoyer, supprimer et mettre en quarantaine des fichiers infectés. Le diagramme ci-dessous illustre le fonctionnement de l'analyseur avec le système de fichiers NetApp.



Processus d'analyse

Ce processus fonctionne de la façon suivante : Le système de fichiers détecte la tentative d'un client d'accéder à un fichier qui n'a pas été analysé pour détecter les éventuels virus qu'il peut contenir. Pour cela, le système de fichiers contrôle son cache, où il stocke le nom des fichiers analysés. Si le nom du fichier ne se trouve pas dans le cache (et si l'extension du fichier a été configurée pour l'analyse), il notifie l'analyseur et lui fournit le chemin d'accès au fichier. L'analyseur ouvre alors une connexion vers le fichier, y recherche les virus connus et renvoie les résultats au système de fichiers. (Si possible, l'analyseur nettoie un fichier infecté.) Enfin, le système de fichiers autorise le client à accéder au fichier si ce dernier ne contient pas de virus.

L'analyseur accepte ONTAP™ 6.2 et ultérieur, ce qui permet la prise en charge de plusieurs systèmes de fichiers avec un analyseur antivirus. Ainsi, vous pouvez ajouter plusieurs analyseurs à un système de fichiers et améliorer l'évolutivité et les performances. L'augmentation du nombre d'analyseurs enregistrés dans un système de fichiers réduit la charge de chaque analyseur. En effet, les recherches de fichiers sont réparties de façon homogène parmi les analyseurs pour équilibrer la charge.

Contrôle du processus

Lorsque vous activez le processus d'analyse de virus Data ONTAP sur le système de fichiers, l'application d'analyse indique au système de fichiers de transmettre des demandes d'analyse de fichiers et surveille les demandes. Chaque fois que les types de fichiers que vous spécifiez sont ouverts ou modifiés dans le système de fichiers, Data ONTAP envoie à l'analyseur une demande d'analyse du fichier.

Le processus Data ONTAP peut analyser plusieurs systèmes de fichiers à partir d'un seul client PC si votre application d'analyse de virus est configurée pour le faire. Vous pouvez configurer l'application avec des options sur le moniteur temps réel de eTrust Antivirus.

L'application d'analyse de virus détermine automatiquement les paramètres du moniteur temps réel au démarrage (ou lors de leur modification). Lorsqu'elle surveille le système de fichiers, elle utilise ces paramètres pour rechercher les infections lors de chaque exécution, accès ou ouverture d'un fichier. Les administrateurs autorisés peuvent définir des règles pour les options depuis l'affichage de l'administrateur du moniteur temps réel.

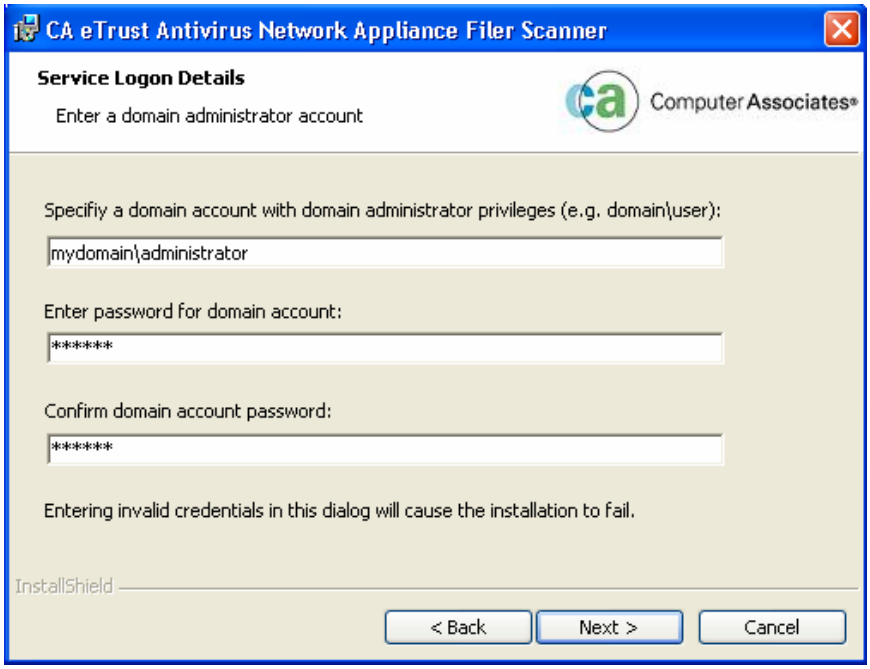
Informations d'installation

Pour installer l'analyseur Network Appliance de eTrust Antivirus, vous devez effectuer les tâches suivantes préalablement à l'installation :

- Vérifiez que le système de fichiers exécute Data ONTAP™ 6.2 ou supérieur et recherche les virus.
- Vérifiez que l'ordinateur de l'analyseur et le système de fichiers appartiennent au même domaine.

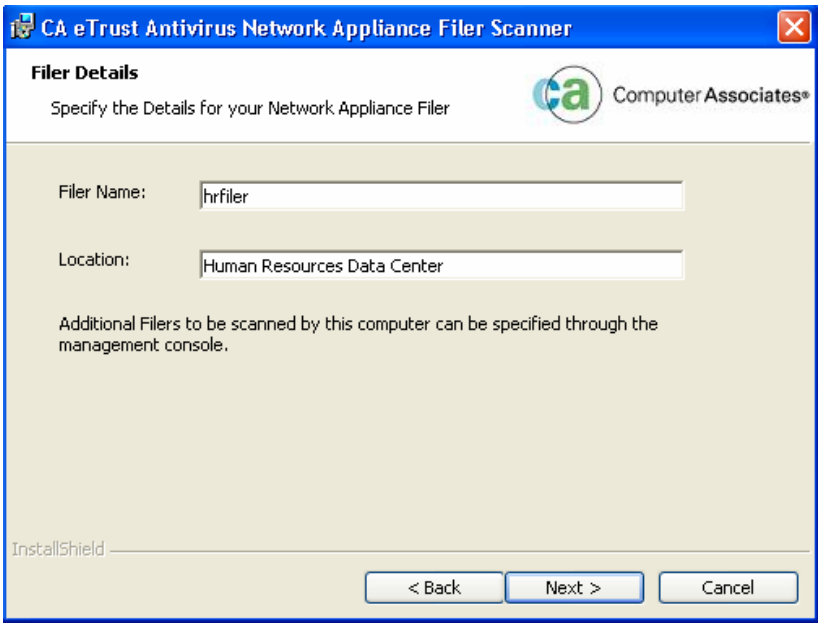
Ensuite, insérez le CD du produit dans le lecteur de CD-ROM et suivez les instructions. (Si l'explorateur du produit ne démarre pas automatiquement, sélectionnez Démarrer, Exécuter dans la barre des tâches de Windows. Naviguez ensuite jusqu'au fichier Setup.exe et exécutez-le.)

Au cours de l'installation, l'assistant demande un compte d'administrateur de domaine. Indiquez un compte avec des droits d'opérateur de sauvegarde sur le système de fichiers et des droits d'administrateur sur l'ordinateur local.



Remarque : L'assistant d'installation tente de démarrer le service de l'analyseur lors de l'installation. Si le compte ne dispose pas des droits d'administrateur de domaine, l'installation échoue.

De plus, l'assistant demande les informations du système de fichiers pour enregistrer ce dernier auprès de l'analyseur. Ne spécifiez qu'un système de fichiers au cours de cette installation. Vous pourrez en ajouter par la suite avec la console.



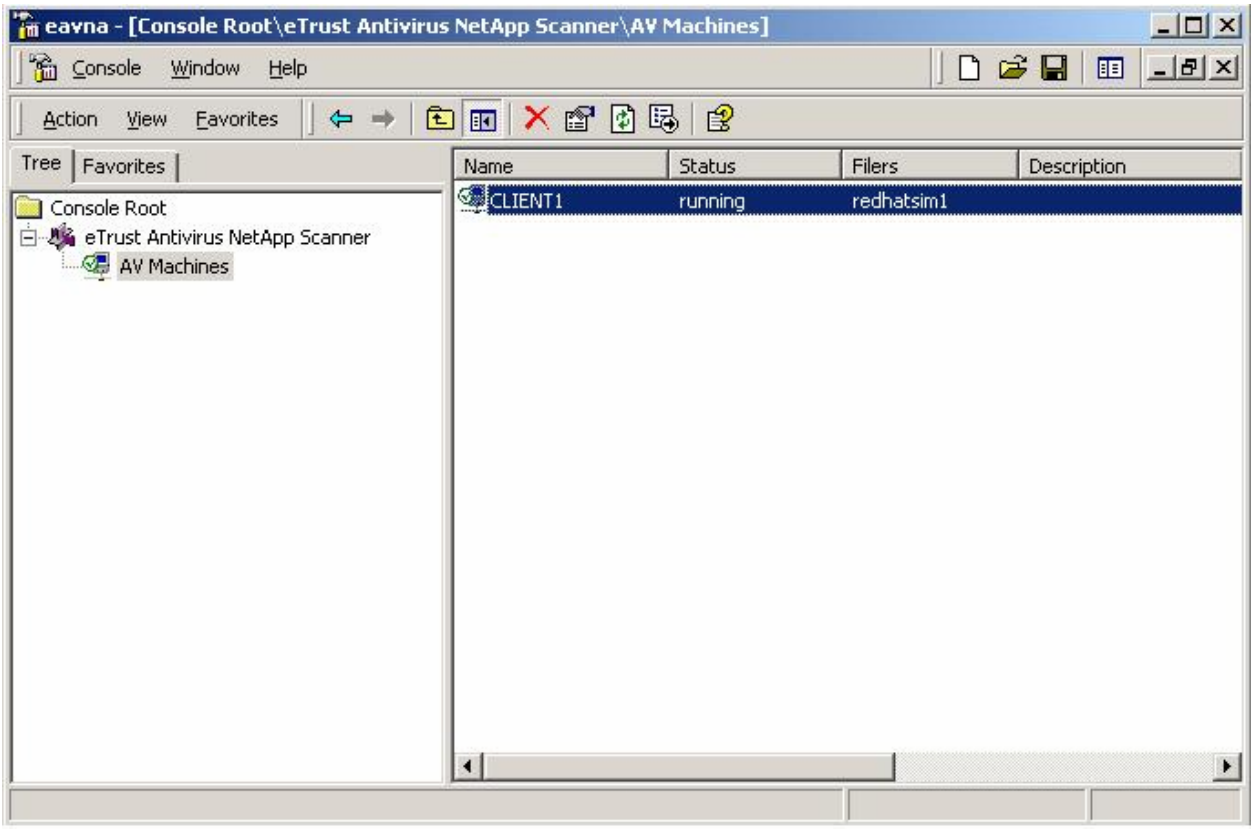
Gestion de l'analyseur

Cette section décrit comment contrôler l'analyseur et ses paramètres antivirus. Un module Microsoft Management Console (MMC) contrôle l'analyseur. Ce module MMC vous permet de configurer les systèmes de fichiers enregistrés auprès des analyseurs et de gérer ces derniers à distance.

Ajout d'un autre système de fichiers à un analyseur

L'assistant d'installation vous a permis de configurer un système de fichiers avec un analyseur. Pour ajouter un autre système de fichiers à un analyseur (enregistrer un système de fichiers auprès d'un analyseur), utilisez la procédure suivante.

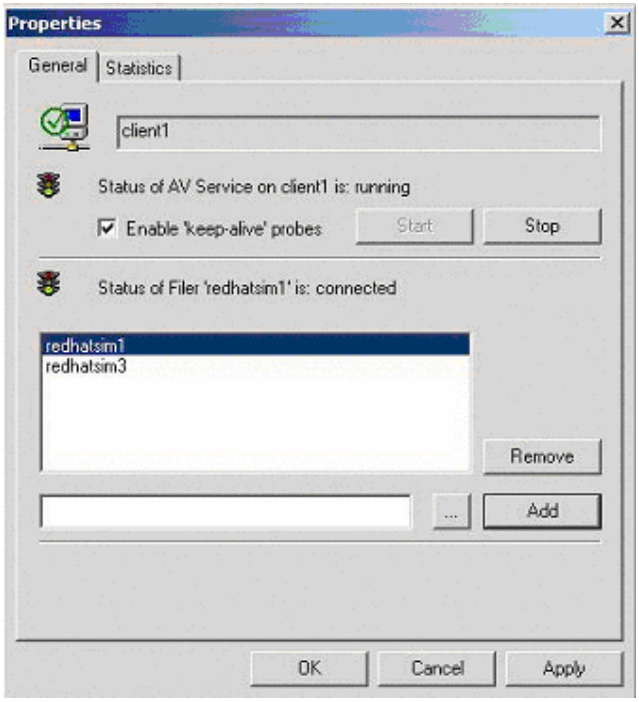
1. Dans le dossier du programme du produit, démarrez la gestion de l'analyseur (module MMC). La fenêtre de la console s'ouvre.
2. Dans le volet de gauche, développez Racine console, Analyseur eTrust Antivirus NetApp. Le nœud Ordinateurs AV apparaît.



3. Sélectionnez Ordinateurs AV. La liste des ordinateurs d'analyseur gérés apparaît dans le volet de droite.

   Si votre ordinateur ne se trouve pas dans la liste, effectuez les actions suivantes pour l'ajouter au MMC : (a) cliquez avec le bouton droit de la souris sur le nœud Ordinateurs AV et (b) sélectionnez Ordinateur AV de l'administrateur. Vous pouvez également ajouter un analyseur distant de cette manière, à condition que l'ordinateur local dispose des droits nécessaires.

4. Double-cliquez sur l'ordinateur. La boîte de dialogue Propriétés s'affiche.

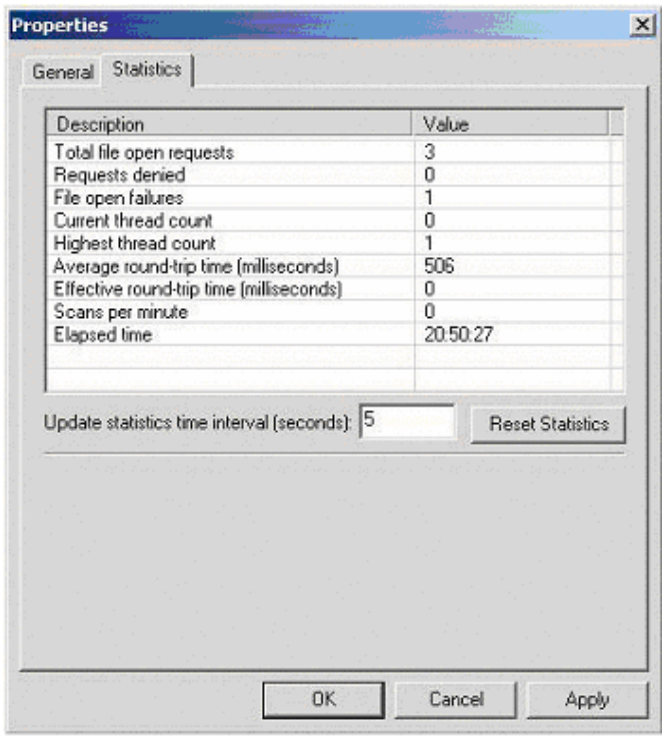


5. Utilisez le bouton Ajouter pour ajouter d'autres systèmes de fichiers à analyser.

Affichage des statistiques de l'analyseur

Pour afficher les statistiques de l'analyseur, utilisez la procédure suivante.

1. Suivez les étapes 1 à 4 de la procédure suivante.
2. Dans la base de données Propriétés, sélectionnez l'onglet Statistiques.



Modification des paramètres antivirus avec le moniteur temps réel

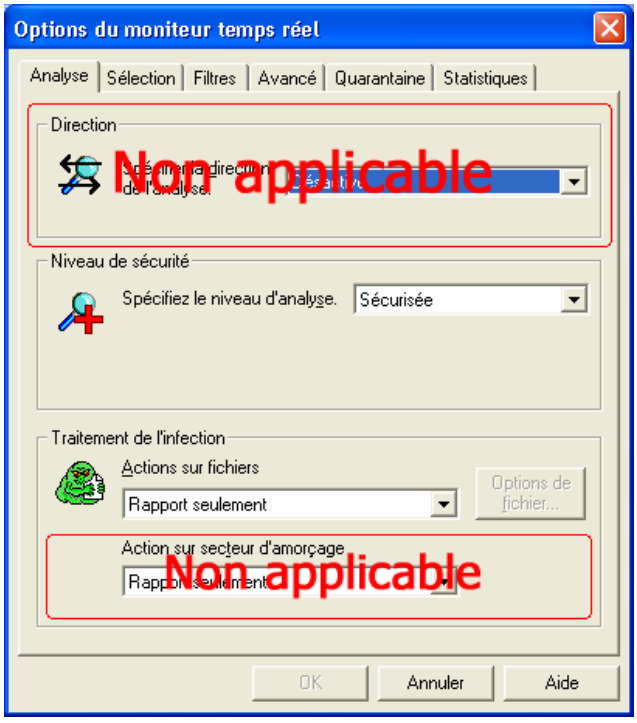
Les onglets suivants et leurs options vous permettent d'indiquer les paramètres du moniteur temps réel. La modification des paramètres du moniteur temps réel pour eTrust Antivirus sur l'ordinateur local change également ceux de l'analyseur.

Toutes les options du moniteur temps réel ne sont pas disponibles pour l'analyseur. Les sections suivantes expliquent certaines des options et illustrent dans les boîtes de dialogue quelles options ne sont pas disponibles pour l'analyseur (mention Not Applicable).

Onglet Analyse

Les paramètres suivants de l'onglet Analyse ne s'appliquent pas à l'analyseur, comme le montre la boîte de dialogue ci-dessous :

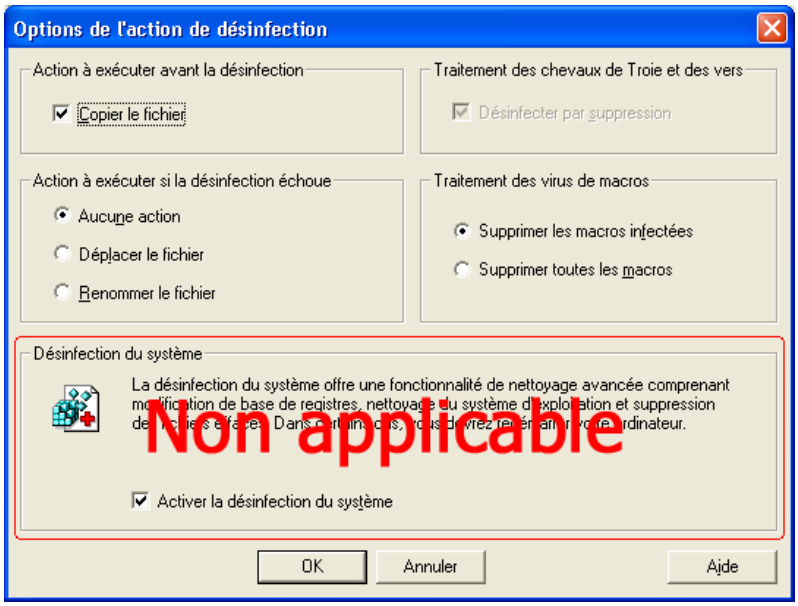
- Direction
- Actions sur secteur d'amorçage



Action Désinfecter le fichier

Le paramètre Désinfection du système ne s'applique pas à l'analyseur. (Cliquez sur le bouton Options de fichier de l'onglet Analyse pour accéder à la boîte de dialogue des options de l'action de désinfection.)

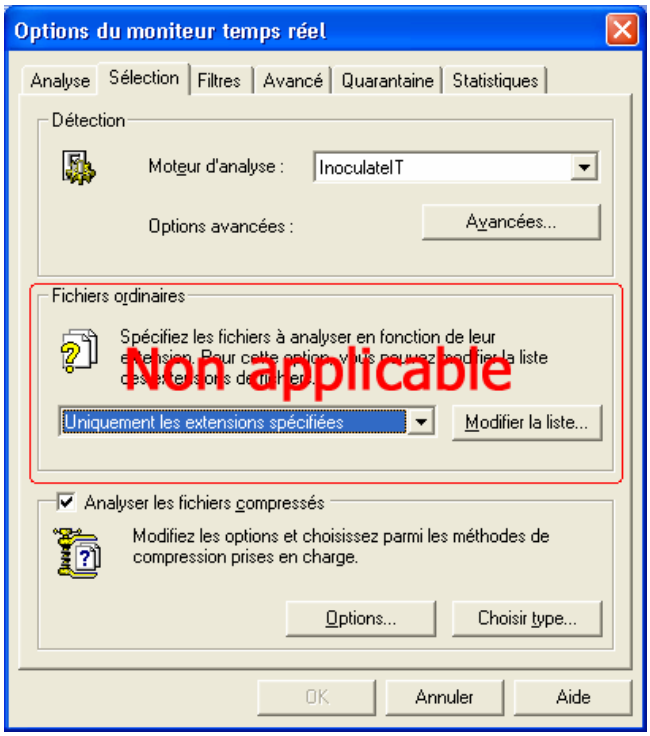
Remarque : Si vous sélectionnez Déplacer le fichier ou Copier le fichier dans la boîte de dialogue suivante, vous ne pouvez plus utiliser l'interface graphique utilisateur de eTrust Antivirus pour gérer les fichiers infectés. (Pour gérer ces fichiers, consultez la section « Gestion des répertoires de déplacement et de copie personnalisés » dans ce chapitre.)



Onglet Sélection

L'analyseur analyse **tous** les fichiers soumis par le système de fichiers. Vous pouvez contrôler l'analyse des fichiers compressés, ainsi que les fichiers à analyser à partir de cet onglet. (Sélectionnez Analyser les fichiers compressés et cliquez sur Options ou Choisir le type.) Ceci s'effectue de la même manière que lorsque vous utilisez eTrust Antivirus.

Le paramètre Fichiers ordinaires de la boîte de dialogue suivante ne s'applique pas à l'analyseur.



Onglet Filtres

Le paramètre Filtres ne s'applique pas à l'analyseur, comme le montre la boîte de dialogue ci-dessous.

Onglet Avancé

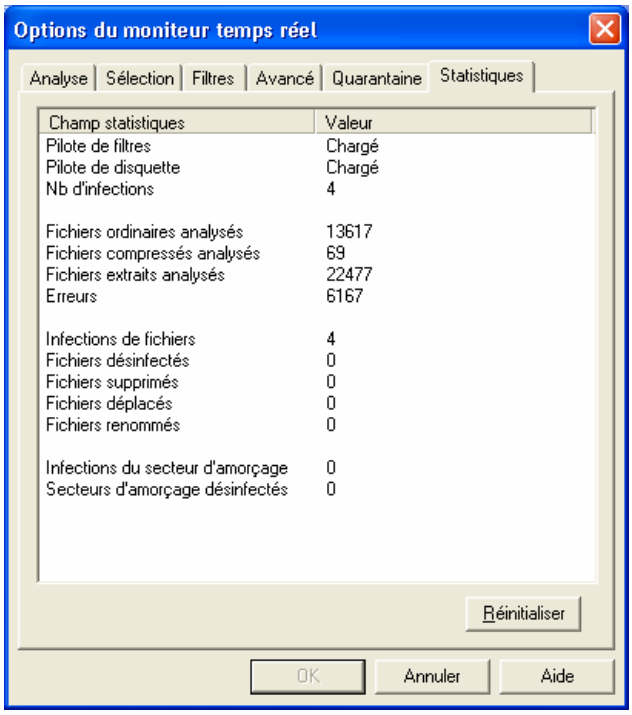
Le paramètre Avancé ne s'applique pas à l'analyseur, comme le montre la boîte de dialogue ci-dessous.

Onglet Quarantaine

Le paramètre Quarantaine ne s'applique pas à l'analyseur, comme le montre la boîte de dialogue ci-dessous.

Onglet Statistiques

Les paramètres de statistiques sont partagés entre l'analyseur et les paramètres temps réel locaux de eTrust Antivirus exécuté sur l'ordinateur.



Gestion des répertoires de déplacement et de copie personnalisés

Le processus d'installation crée les valeurs de registre suivantes et définit ces valeurs sur l'emplacement du répertoire de déplacement de eTrust Antivirus.

HKLM = HKEY_LOCAL_MACHINE.

HKLM\SOFTWARE\ComputerAssociates\eTrust Antivirus NetApp Scanner

- CopyDir
- MoveDir

Déplacement des fichiers infectés vers le système de fichiers

Dans la boîte de dialogue Options de l'action de désinfection, si vous indiquez Déplacer le fichier ou Copier le fichier, l'analyseur, par défaut, déplace les fichiers infectés du système de fichiers vers le répertoire de déplacement de eTrust Antivirus sur l'ordinateur de l'analyseur local (généralement : Program Files\CA\eTrust Antivirus\Move). Vous pouvez modifier ce paramètre.

Pour déplacer les fichiers infectés vers le système de fichiers plutôt que vers l'analyseur, utilisez **Regedit** pour changer manuellement les valeurs de configuration du registre sur l'ordinateur de l'analyseur. Les nouvelles valeurs remplacent les répertoires de déplacement et de copie du moniteur temps réel.

Les répertoires ne doivent pas avoir de barre oblique inverse à la fin et peuvent pointer vers des disques locaux ou mappés, ou être spécifiés comme des chemins UNC (Universal Naming Convention : Convention universelle de désignation de noms). Par exemple :

```
HKLM\SOFTWARE\ComputerAssociates\eTrust Antivirus NetApp
Scanner\MoveDir=\\f760\vol1\move
```

Gestion des fichiers dans un répertoire de déplacement personnalisé

Lorsque vous avez indiqué un répertoire de déplacement personnalisé, vous ne pouvez pas utiliser l'interface graphique utilisateur de eTrust Antivirus pour en gérer les fichiers. Utilisez à la place l'utilitaire de ligne de commande **RestMove**. Il se trouve dans le répertoire d'installation de l'ordinateur de l'analyseur et possède les caractéristiques suivantes :

- Affiche les noms des fichiers d'origine et leurs infections
- Prend en charge les caractères génériques DOS standard : * et ?.

Pour **afficher** des informations concernant tous les fichiers du répertoire de déplacement, saisissez la commande suivante, en pointant vers les fichiers déplacés, et spécifiez le paramètre –i :

```
RestMove \\f760\vol1\move\*.* -i
```

Exemple de résultat :

```
\\f760\vol1\move\31ed8c4e-b930-45f0-8c1e-35e1d3570cd6
Nom du fichier d'origine : \\F760\VSCAN_ADMIN$\vol\vol1\sabra01\eicar2.com
Nom de l'infection : Fichier de test EICAR
Détecté par le moteur 23.61.00, signature 23.61.50 le 16/06/2003, 13:06:11
```

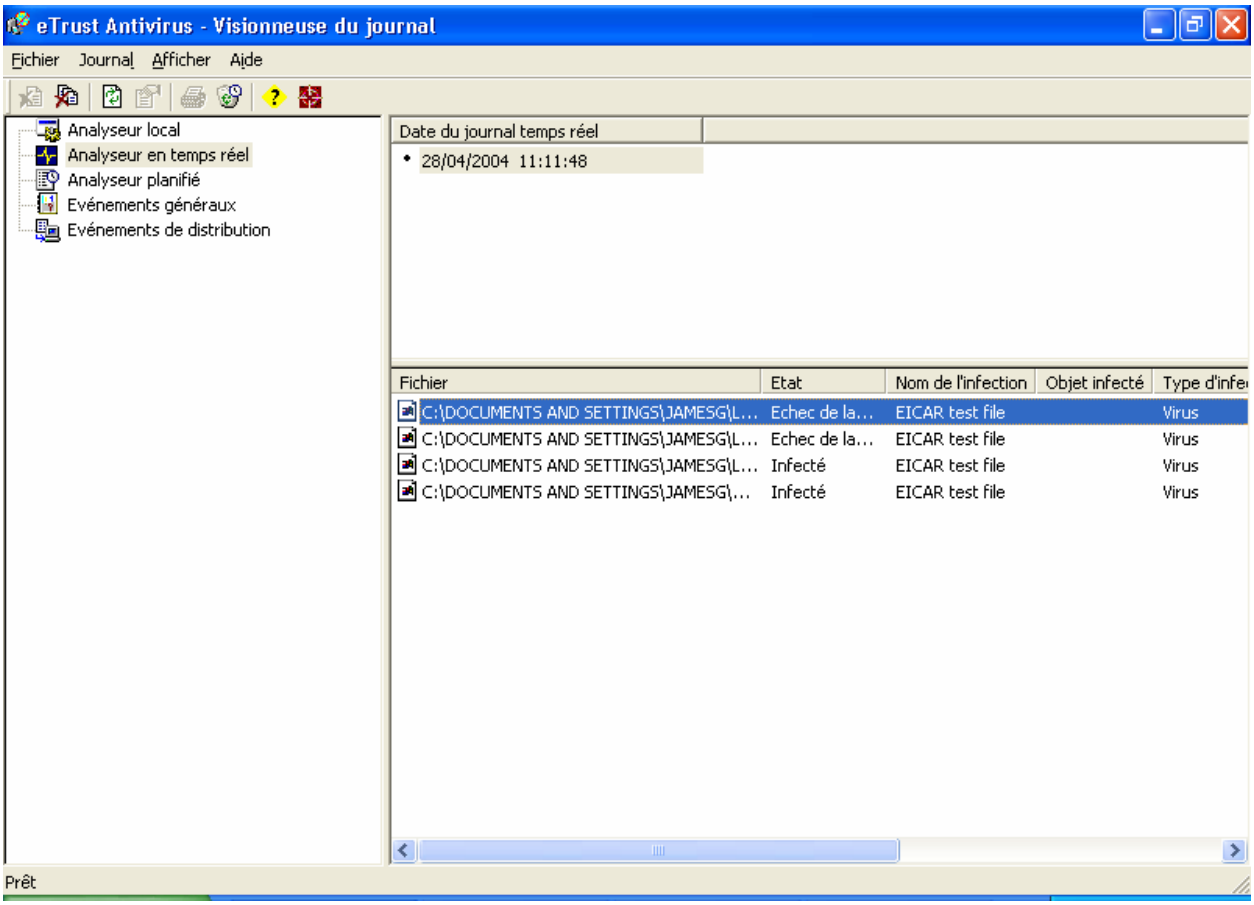
Pour restaurer les fichiers à leur emplacement d'origine, saisissez la commande RestMove sans utiliser le paramètre -i.

Vous pouvez fournir des chemins d'accès uniques pour MoveDir et CopyDir car les valeurs sont stockées dans des clés de registre uniques. Par conséquent, un analyseur servant plusieurs systèmes de fichiers peut stocker des fichiers déplacés et copiés dans différents emplacements.

Affichage du journal de détection de virus

L'analyseur ajoute une entrée à la base de données du journal temps réel chaque fois qu'il reçoit une demande de fichier contenant un virus. L'analyseur envoie également un message à la console système du système de fichiers qui notifie l'administrateur du système de fichiers de l'infection par un virus.

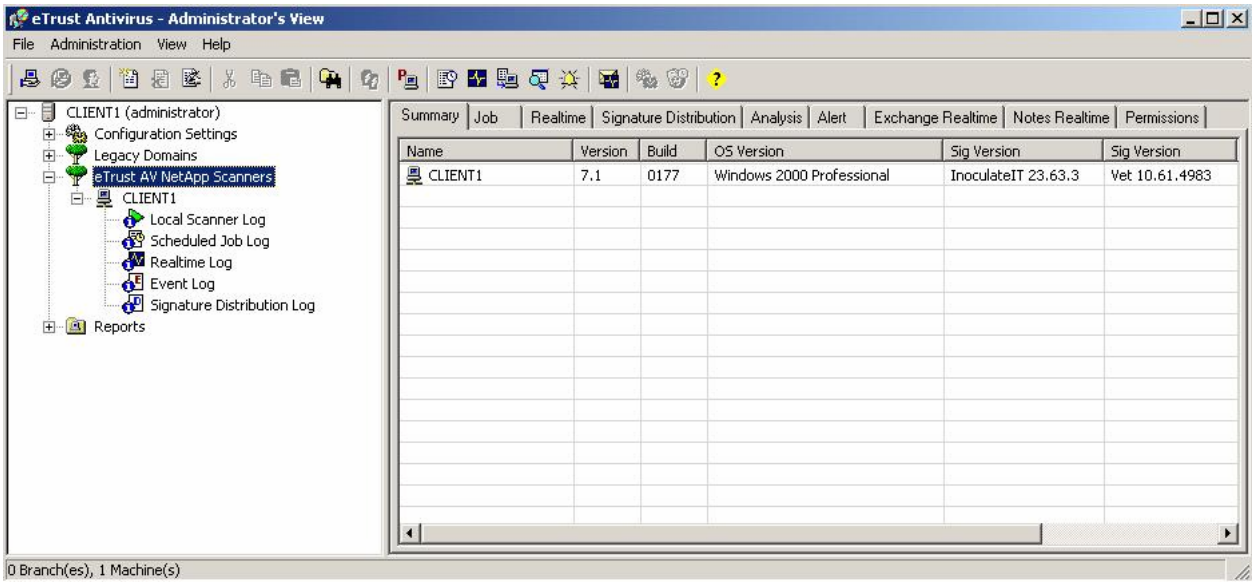
Pour afficher le journal temps réel, ouvrez la visionneuse du journal et sélectionnez Analyseur temps réel.



Gestion de l'analyseur à distance

Pour gérer les paramètres de l'analyseur antivirus à distance avec l'affichage de l'administrateur (comme d'autres options de eTrust Antivirus), suivez la procédure ci-après.

1. Faites découvrir au serveur admin tous les analyseurs.
2. Placez les analyseurs dans un groupe.



Remarque : Soyez vigilant lorsque vous choisissez des paramètres car le logiciel les applique au moteur de eTrust Antivirus et à l'analyseur exécuté sur l'ordinateur ; certains des paramètres temps réel ne correspondent pas aux deux.

3. Définissez les paramètres antivirus temps réel pour le groupe.
4. Appliquez les règles à l'analyseur du système de fichiers sélectionné.

Gestion du système de fichiers

Cette section décrit les procédures permettant de gérer le système de fichiers et son environnement. La protection antivirus CIFS (Common Internet file system) est une fonction du système d'exploitation du système de fichiers, Data ONTAP, qui donne aux clients CIFS l'analyse des virus lors de l'accès des fichiers sur un système de fichiers. L'analyse des virus lors de l'accès est l'analyse d'un fichier avant qu'un client CIFS ne soit autorisé à l'ouvrir. Consultez le Guide des recommandations de l'analyse antivirus de NetApp pour plus d'informations concernant le système de fichiers.

Activation et désactivation de l'analyse de virus

Pour activer et désactiver l'analyse des virus, saisissez la commande suivante :

```
vscan on [-f][on|off]
```

`-f` force l'activation de l'analyse des virus même si aucun client d'analyse de virus n'est disponible pour analyser les fichiers.

Remarque : L'activation de l'analyse des virus lorsque aucun client n'est disponible pour analyser les fichiers interdit aux clients CIFS d'accéder aux fichiers du système de fichiers.

Spécification d'extensions de fichiers à analyser en utilisant vscan

Une liste par défaut des extensions de fichiers est disponible lorsque vous activez **vscan**. Cette liste peut contenir jusqu'à 255 extensions.

Remarque : La liste des extensions sur le système de fichiers est traitée avant celle de l'ordinateur de l'analyseur que vous établissez par la configuration en temps réel. Par exemple, si l'extension *.vbs n'est pas configurée sur le système de fichiers pour l'analyse, les fichiers VBS ne sont pas transmis à l'analyseur. Par conséquent, même si les fichiers VBS sont configurés pour l'analyse sur l'analyseur, ils ne l'atteignent pas pour y être traités. En outre, si une extension se trouve dans la liste sur le système de fichiers mais n'est pas spécifiée dans l'option de configuration en temps réel, le système de fichiers transmet les fichiers correspondants à l'analyseur, mais ce dernier ignore ces demandes d'analyse.

Pour contrôler quels fichiers analyser, saisissez les commandes suivantes pour modifier la liste par défaut des extensions de fichiers.

Pour **afficher** la liste par défaut des extensions de fichiers que le système de fichiers doit analyser, saisissez la commande suivante :

```
vscan extensions
```

Pour **enrichir** la liste par défaut des extensions de fichiers que le système de fichiers doit analyser, saisissez la commande suivante :

```
vscan extensions add ext[,ext...]
```

où *ext* est l'extension à ajouter.

Exemple :

```
vscan extensions add txt
```

Pour **remplacer** la liste par défaut des extensions de fichiers par une nouvelle liste, saisissez la commande suivante :

```
vscan extensions set ext[,ext...]
```

où *ext* est l'extension à définir.

Pour **supprimer** des types de fichiers de la liste par défaut des extensions de fichiers, saisissez la commande suivante :

```
vscan extensions remove ext[,ext...]
```

où *ext* est l'extension à supprimer.

Pour **rétablir** la liste par défaut des extensions de fichiers, saisissez la commande suivante :

```
vscan extensions reset
```

Spécification des partages à analyser en utilisant cifs

Vous pouvez activer ou désactiver l'analyse des partages que vous spécifiez, soit pour n'importe quel accès, soit pour l'accès en lecture seule.

Désactivation de l'analyse des fichiers d'un partage

L'état par défaut d'un partage est l'activation de l'analyse de virus. Vous pouvez désactiver l'analyse de virus pour les fichiers d'un partage. Vous pouvez le faire pour les raisons suivantes : (1) lorsque les utilisateurs se limitent aux utilisateurs de confiance, (2) les fichiers sont restreints au mode lecture seule, ou (3) la vitesse d'accès est plus importante que la sécurité.

Pour désactiver l'analyse de virus pour les fichiers d'un partage, saisissez la commande suivante :

```
cifs shares -change share_name -novscan
```

Où *share_name* est le nom du partage pour lequel vous voulez désactiver l'analyse de virus.

Résultat : L'application n'effectue pas d'analyse de virus lorsque les clients ouvrent des fichiers sur ce partage. Le paramètre persiste après le redémarrage.

Désactivation de l'analyse pour l'accès en lecture seule dans un partage

Vous pouvez désactiver l'analyse de virus dans un partage pour les utilisateurs qui ouvrent des fichiers en accès en lecture seule, afin d'améliorer la vitesse d'accès à ces fichiers. L'état par défaut d'un partage est l'activation de l'analyse de virus.

Pour désactiver l'analyse de virus pour l'accès en lecture seule aux fichiers d'un partage spécifié, saisissez la commande suivante :

```
cifs shares -change share_name -novscanread
```

Où *share_name* est le nom du partage pour lequel vous voulez désactiver l'analyse de virus.

Résultat : L'application n'effectue pas d'analyse de virus lorsque les clients ouvrent des fichiers sur ce partage pour l'accès en lecture. Le paramètre persiste après le redémarrage.

Activation de l'analyse pour l'accès en lecture seule dans un partage

Pour activer l'analyse de virus pour l'accès en lecture seule aux fichiers d'un partage spécifié, saisissez la commande suivante :

```
cifs shares -change share_name -vscanread
```

Où *share_name* est le nom du partage pour lequel vous voulez activer l'analyse de virus.

Résultat : L'application effectue l'analyse de virus lorsque les clients ouvrent des fichiers sur ce partage pour l'accès en lecture. Le paramètre persiste après le redémarrage.

Ajout d'un partage lorsque l'analyse est désactivée

Vous pouvez créer un partage lorsque l'analyse de virus est désactivée. L'état par défaut d'un partage est l'activation de l'analyse de virus.

Pour ajouter un partage dont l'analyse de virus est désactivée, saisissez la commande suivante :

```
cifs shares -add share_name /path -novscan
```

Où *share_name* est le nom du partage que vous voulez créer avec l'analyse de virus désactivée, et

où *path* indique où vous voulez créer le partage.

Résultat : Data ONTAP crée un partage lorsque l'analyse de virus est désactivée.

Dépannage

Les problèmes se produisent souvent du fait de conflits de paramètres de configuration entre le système de fichiers NetApp et le moniteur temps réel. Le tableau suivant présente la description de certains problèmes ainsi que leurs causes et solutions possibles.

Problème	Cause possible	Solution possible
Echec de l'installation	Le compte de domaine du service d'analyse à utiliser comme compte de connexion n'est pas valide	Exécutez l'installation et spécifiez un compte de connexion de domaine valide pour le service
Système de fichiers : Le système de fichiers n'analyse pas les fichiers ; MMC affiche une valeur constante du nombre de fichiers analysés	L'analyse du partage correspondant n'est pas activée Le système de fichiers exclut des types de fichiers de la liste des fichiers à analyser Le système de fichiers possède le type de fichier dans la liste des fichiers à analyser, mais l'analyseur exclut ce type de fichier de sa propre liste des fichiers à analyser	vscan on cifs shares -change *share_name* -vscanread vscan extensions add *ext*[,*ext*...] Synchronisez les listes de sélection de fichier du système de fichiers et de l'analyseur
Le client CIFS/SMB peut accéder aux fichiers infectés à partir du système de fichiers	L'analyse du partage correspondant n'est pas activée sur le système de fichiers Le système de fichiers a été configuré pour ignorer le résultat de l'analyse	vscan on cifs shares -change *share_name* -vscanread vscan options mandatory_scan [on|off]
AV Scanner Admin : Démarrage du service impossible	Les autorisations (droits d'accès) n'ont pas été définies correctement	Vérifiez que le système de fichiers et l'analyseur se trouvent dans le même domaine NT Vérifiez que les droits de l'utilisateur qui démarre le service sont corrects (il doit appartenir au groupe de services de sauvegarde)

Problème	Cause possible	Solution possible
AV Scanner Admin : Le service démarré ne peut se synchroniser avec le système de fichiers	Le système de fichiers n'a pas été déconnecté correctement d'une connexion à une session existante	Arrêtez la session active sur le système de fichiers : vscan scanners stop *scanner_IP*

Annexe

I

Installation automatique de eTrust Antivirus

Vous pouvez installer eTrust Antivirus sans qu'aucune interaction ni réponse ne soit nécessaire de votre part. Il s'agit d'une installation automatique. Cette annexe indique comment effectuer une installation automatique de eTrust Antivirus.

Examen du fichier d'installation automatique

Pour effectuer une installation automatique de eTrust Antivirus, exécutez la commande correspondant à votre système d'exploitation depuis le fichier UnattendedInstall.html situé dans le répertoire eAV v7.1\Doc\html du CD du produit. Ce fichier contient des commandes permettant d'effectuer une installation automatique de eTrust Antivirus 7.1 avec les produits ou systèmes d'exploitation suivants :

- Windows
- UNIX/Linux
- NetWare
- OS X
- Analyseur eTrust Antivirus pour système de fichiers NetApp

Index

A

B

C

D

E

F

G

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

Z