AVG 2011 Edition Serveur de Fichiers

Manuel de l'utilisateur

Révision du document 2011.01 (20. 9. 2010)

Table des matières

1. Introduction

Ce manuel de l'utilisateur constitue la documentation complète du produit **AVG 2011 Edition Serveur de Fichiers**.

Nous vous remercions d'avoir choisi le programme AVG 2011 Edition Serveur de Fichiers.

AVG 2011 Edition Serveur de Fichiers·figure parmi les produits AVG primés et a été conçu pour assurer la sécurité de votre ordinateur et vous permettre de travailler en toute sérénité. Comme toute la gamme des produits AVG, la solution **AVG 2011 Edition Serveur de Fichiers**· a été entièrement repensée, afin de proposer une protection AVG reconnue et certifiée sous une présentation nouvelle, plus conviviale et plus efficace. Votre tout nouveau produit **AVG 2011 Edition Serveur de Fichiers**· bénéficie d'une interface transparente associée à une analyse encore plus approfondie et plus rapide. Davantage de fonctions de sécurité ont été automatisées pour plus de commodité et des options utilisateur « intelligentes » supplémentaires ont été incluses de manière à adapter les fonctions de sécurité à vos activités quotidiennes. La convivialité n'a fait aucun compromis à la sécurité !

AVG a été conçu et développé pour protéger vos activités en local et en réseau. Nous espérons que vous profiterez pleinement de la protection du programme AVG et qu'elle vous donnera entière satisfaction.

Une offre intégrale

- Une protection pertinente par rapport à la manière dont vous utilisez votre ordinateur et l'Internet. Achats et opérations bancaires en ligne, navigation et recherches sur Internet, discussions en ligne et communications par e-mail, téléchargements de fichiers et utilisation des réseaux sociaux : AVG a la solution de sécurité qui correspond à vos besoins.

- Une protection discrète qui a relevé le défi de la sécurité pour plus de 110 millions d'utilisateurs de par le monde et dont le niveau d'excellence est sans cesse maintenu par un réseau international de chercheurs expérimentés.

- Une protection s'appuyant sur une assistance technique spécialisée disponible 24h sur 24

2. Pré-requis à l'installation d'AVG

2.1. Systèmes d'exploitation pris en charge

AVG 2011 Edition Serveur de Fichiers sert à protéger les stations de travail/ serveurs fonctionnant avec les systèmes d'exploitation suivants :

- Windows 2003 Server et Windows 2003 Server x64 Edition
- Windows 2008 Server et Windows 2008 Server x64 Edition

(et éventuellement les service packs de versions ultérieures pour certains systèmes d'exploitation)

2.2. Configuration matérielle minimale et recommandée

Configuration matérielle minimale pour **AVG 2011 Edition Serveur de Fichiers** :

- Processeur Intel Pentium 1,5 GHz
- 512 Mo libres de RAM
- 470 Mo d'espace disque dur (pour l'installation)

Configuration matérielle recommandée pour **AVG 2011 Edition Serveur de Fichiers** :

- Processeur Intel Pentium 1,8 GHz
- 512 Mo libres de RAM
- 600 Mo d'espace disque dur (pour l'installation)

3. Options d'installation

AVG peut être installé à partir du fichier d'installation disponible sur le CD-ROM d'installation. Vous pouvez également télécharger la dernière version du fichier d'installation sur le site Web d'AVG (http://www.avg.com).

Avant de procéder à l'installation du programme AVG, nous vous recommandons vivement de consulter le site Web d'AVG (http://www.avg.com) pour vous assurer de posséder le dernier fichier d'installation en date d'AVG 2011 Edition Serveur de Fichiers.

Vous serez invité à saisir votre numéro d'achat/licence au cours du processus d'installation. Vous devez être en possession de ce numéro avant de commencer l'installation. Le numéro d'achat figure sur le coffret du CD-ROM. Si vous achetez une copie d'AVG en ligne, le numéro de licence vous sera envoyé par mail.

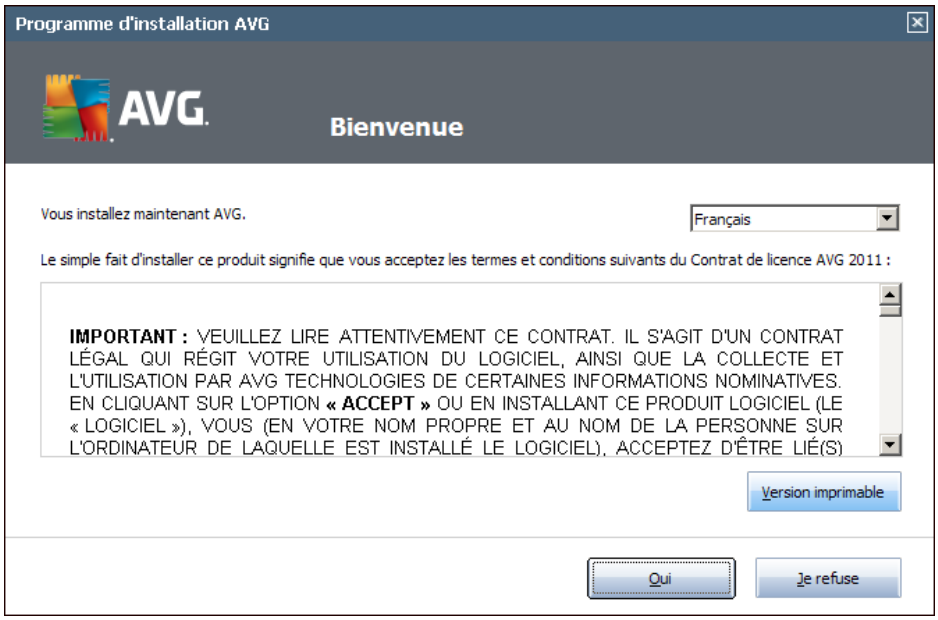
4. Processus d'installation

Pour installer **AVG 2011 Edition Serveur de Fichiers** sur l'ordinateur, vous devez posséder le fichier d'installation le plus récent. Vous pouvez utiliser le fichier d'installation figurant sur le CD et fourni avec votre édition, mais il est fort probable qu'il soit déjà périmé. En conséquence, nous vous recommandons de bien vouloir télécharger de dernier fichier d'installation, depuis Internet. Vous pouvez télécharger le fichier à partir du site Web d'AVG (http://www.avg.com), section ***Centre de support / Téléchargement.***

L'installation consiste à réaliser une série de tâches décrites à l'intérieur de boîtes de dialogue. Vous trouverez dans ce document une explication de chaque boîte de dialogue :

4.1. Bienvenue

Le processus d'installation démarre dans la fenêtre ***Bienvenue***. Dans cet écran, vous indiquez la langue utilisée par le processus d'installation, et la langue par défaut de l'interface utilisateur AVG. Dans la section supérieure de la fenêtre, recherchez le menu déroulant contenant la liste des langues proposées :



Attention : *vous choisissez ici la langue qui sera utilisée pour l'installation. La langue que vous avez choisi sera installée comme langue par défaut pour l'interface AVG, de même que l'anglais qui est installé systématiquement. Si vous voulez installer d'autres langues pour l'interface utilisateur, indiquez-les dans la boîte de dialogue du programme d'installation* ***Options personnalisées****.*

Par ailleurs, cette boîte de dialogue contient l'intégralité du texte de l'accord de licence AVG. Merci de le lire attentivement. Pour indiquer que vous avez lu, compris et accepté l'accord, cliquez sur le bouton ***Oui***. Si vous n'acceptez pas les termes de la licence, cliquez sur le bouton ***Je refuse*** ; le processus d'installation prendra fin

immédiatement.

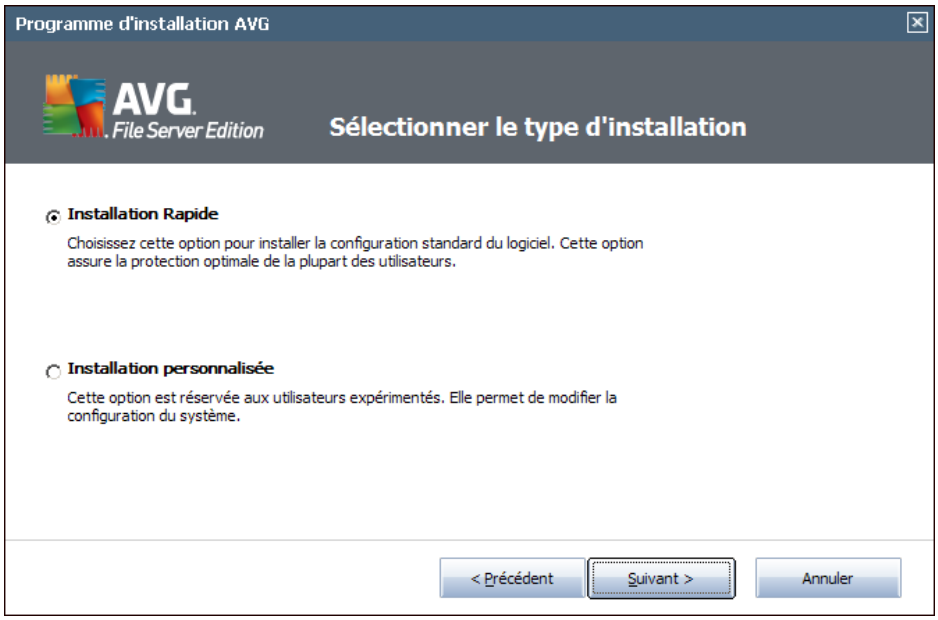
4.2. Activation de la licence AVG

Dans la boîte de dialogue visant à ***activer votre licence AVG***, indiquez votre numéro de licence dans le champ prévu à cet effet.

Le numéro d'achat se trouve dans le coffret du CD-ROM contenant le programme **AVG 2011 Edition Serveur de Fichiers** . Le numéro de licence figure dans l'e-mail de confirmation que vous avez reçu après avoir acheté le produit **par Internet.** Vous devez saisir le numéro tel qu'il apparaît. Si le numéro de licence est disponible au format électronique (*par exemple, dans un mail*), il est recommandé de l'insérer à l'aide de la méthode copier-coller.

Cliquez sur le bouton ***Suivant*** pour continuer le processus d'installation.

4.3. Sélectionner le type d'installation



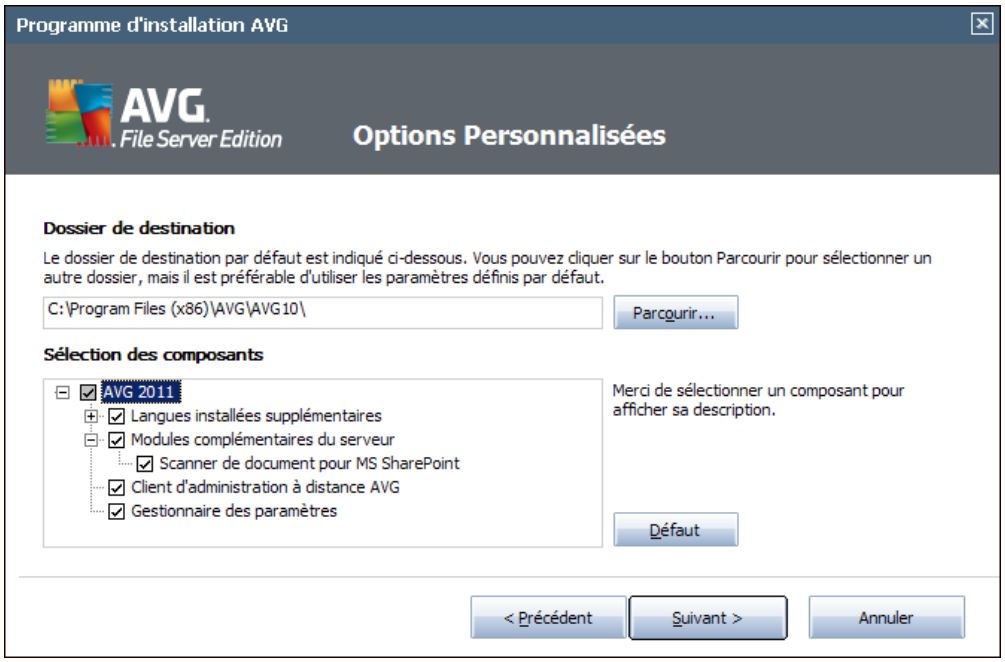
La boîte de dialogue ***Sélectionner le type d'installation*** propose deux modes d'installation : ***Installation rapide*** et ***Installation personnalisée***.

Dans la majorité des cas, il est recommandé d'opter pour l'***installation rapide***, qui installe automatiquement le programme AVG selon les paramètres prédéfinis par l'éditeur du logiciel. Cette configuration allie un maximum de sécurité et une utilisation optimale des ressources. Si besoin est, vous avez toujours la possibilité de modifier directement la configuration dans l'application AVG. Si vous avez sélectionné l'option ***Installation rapide***, cliquez sur le bouton ***Suivant*** pour passer à la boîte de dialogue ***Progression de l'installation*** suivante.

L'***installation personnalisée*** est exclusivement réservée aux utilisateurs expérimentés qui ont une raison valable d'installer AVG selon des paramètres non standard. Par exemple, cela leur permet d'adapter le programme à une configuration système spécifique. Après la sélection de cette option, cliquez sur le bouton ***Suivant*** pour ouvrir la boîte de dialogue ***Options personnalisées***.

4.4. Options personnalisées

La boîte de dialogue ***Options personnalisées*** permet de configurer deux paramètres de l'installation :



Dossier de destination

Dans la section ***Dossier de destination*** de la boîte de dialogue, vous devez indiquer l'emplacement dans lequel **AVG 2011 Edition Serveur de Fichiers** doit être installé. Par défaut, AVG est installé dans le dossier contenant les fichiers de programme sur le lecteur C:. Si un tel dossier n'existe pas, vous serez invité à confirmer, dans une nouvelle boîte de dialogue, que vous acceptez qu'AVG le crée avant l'installation. Si vous optez pour un autre emplacement, cliquez sur le bouton ***Parcourir*** pour consulter l'arborescence du lecteur, puis sélectionnez le dossier souhaité.

Sélection des composants

La section ***Sélection des composants*** présente tous les composants **AVG 2011 Edition Serveur de Fichiers** pouvant être installés. Si les paramètres par défaut ne vous satisfont pas, vous pouvez supprimer ou ajouter des composants spécifiques.

Notez que vous pouvez seulement choisir des composants inclus dans l'édition AVG dont vous avez acquis les droits.

Mettez en surbrillance un élément de la liste ***Sélection des composants*** : une brève description du composant correspondant s'affiche à droite de la section.

- ***Sélection de la langue***

Dans la liste des composants à installer, vous pouvez définir la/les langue(s) dans la/lesquelles AVG doit être installé. Cochez la case ***Langues supplémentaires installées***, puis sélectionnez les langues désirées dans le menu correspondant.

- ***Modules complémentaires serveur - Scanner de documents pour MS SharePoint***

Ce composant permet d'analyser les documents stockés dans MS SharePoint et de se prémunir contre les menaces possibles. Il est au cœur de la fonctionnalité du programme **AVG 2011 Edition Serveur de Fichiers**, c'est pourquoi nous vous recommandons de l'installer.

- ***Client AVG Remote Admin***

Si vous envisagez de connecter votre ordinateur au composant Administration à distance AVG, cochez également cet élément afin de l'installer.

- ***Gestionnaire des paramètres***

Le Gestionnaire de paramètres AVG est une application légère qui permet de configurer rapidement et simplement les installations locales d'AVG (même celles qui ne sont pas exécutées par l'administration à distance). Elle utilise les fichiers de configuration (au format .pck) qui sont faciles à créer au moyen du Gestionnaire de paramètres AVG sur chaque ordinateur doté de l'application AVG. Vous pouvez ensuite copier ces fichiers sur chaque dispositif amovible et les utiliser sur chaque ordinateur. Naturellement, le principe est le même pour le Gestionnaire de paramètres AVG. Pour plus d'informations sur cette application, cliquez **ici**.

Cliquez sur le bouton ***Suivant*** pour passer à l'écran suivant.

4.5. Progression de l'installation

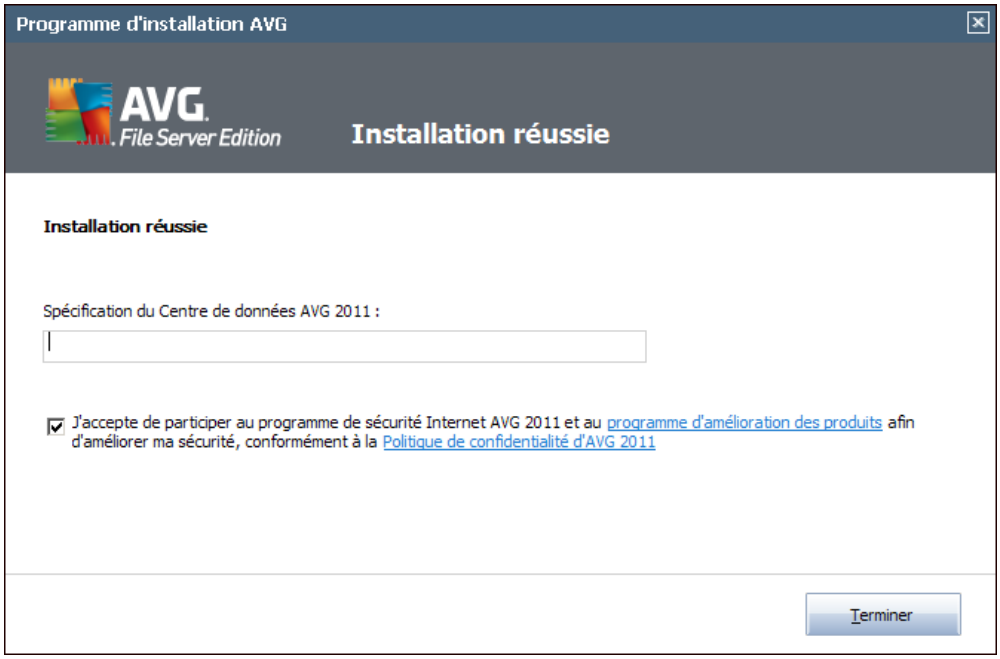
La boîte de dialogue ***Progression de l'installation*** affiche l'avancement de l'installation et ne requiert aucune intervention de votre part :

Lorsque le processus d'installation est terminé, la base de données virale et le programme sont automatiquement mis à jour. Par la suite, vous êtes redirigé vers la boîte de dialogue suivante.

4.6. Installation réussie

La boîte de dialogue ***Installation réussie*** confirme que le programme **AVG 2011 Edition Serveur de Fichiers** est bien installé et configuré.

Si vous avez choisi d'installer le client AVG Remote Admin Client (voir Options personnalisées), la boîte de dialogue qui s'affiche se présente comme suit :



Vous devez spécifier les paramètres du Centre de données AVG; indiquez la chaîne de connexion au Centre de données AVG sous la forme serveur:port. Si vous ne disposez pas de cette information pour l'instant, laissez ce champ vide ; vous pourrez définir la configuration ultérieurement dans la boîte de dialogue Paramètres avancés / Administration à distance. Pour plus d'informations sur l'administration à distance AVG, consultez le manuel de l'utilisateur des éditions professionnelles d'AVG disponible sur le site Web AVG (http://www.avg.com).

J'accepte de participer au programme de sécurité Internet AVG 2011 et au programme d'amélioration des produits... - cochez cette case si vous désirez apporter votre aide dans le cadre du programme d'amélioration des produits (*pour en savoir plus, voir le chapitre Paramètres avancés d'AVG / Programme d'amélioration des produits*) qui collecte des informations anonymes sur les menaces détectées de manière à accroître le niveau général de la sécurité sur Internet.

5. Opérations à effectuer après l'installation

5.1. Enregistrement du produit

Après l'installation d'**AVG 2011 Edition Serveur de Fichiers**, enregistrez votre produit en ligne sur le site Web d'AVG (http://www.avg.com), page ***Enregistrement*** (*suivez les instructions indiquées sur cette page*). Après l'enregistrement, vous bénéficierez de tous les avantages associés à votre compte utilisateur AVG et aurez accès à la lettre d'informations d'AVG ainsi qu'aux autres services réservés exclusivement aux utilisateurs enregistrés.

5.2. Accès à l'interface utilisateur

L'***interface utilisateur d'AVG*** est accessible de plusieurs façons :

- double-cliquez sur l'***icône de la barre d'état système AVG***
- double-cliquez sur l'icône AVG située sur le Bureau
- à partir du menu ***Démarrer/ Programmes/AVG 2011/Interface utilisateur AVG***

5.3. Analyse complète

Le risque de contamination de l'ordinateur par un virus avant l'installation d'**AVG 2011 Edition Serveur de Fichiers** ne doit pas être écarté. C'est pour cette raison qu'il est recommandé d'exécuter une ***analyse complète*** afin de s'assurer qu'aucune infection ne s'est déclarée dans votre ordinateur.

Pour obtenir des instructions sur l'exécution d'une ***analyse complète***, reportez-vous au chapitre ***Analyse AVG***.

5.4. Configuration AVG par défaut

La configuration par défaut (*c'est-à-dire la manière dont l'application est paramétrée à l'issue de l'installation*) d'**AVG 2011 Edition Serveur de Fichiers** est définie par l'éditeur du logiciel de sorte que les composants et les fonctions délivrent leurs performances optimales.

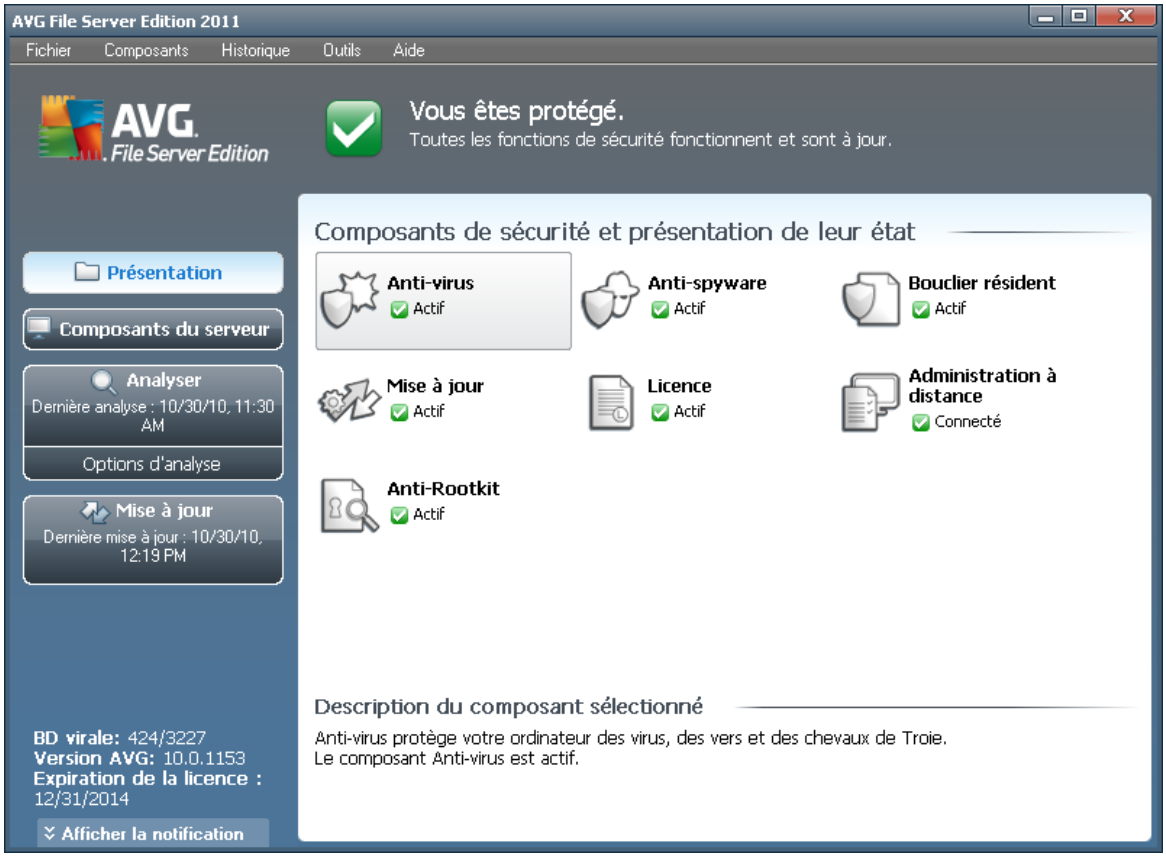
Aussi est-il recommandé de ne pas modifier la configuration AVG sans motif valable. Tout changement de ces paramètres doit être réalisé par un utilisateur expérimenté.

Il est possible d'apporter certaines corrections mineures aux paramètres des ***composants AVG***, directement dans l'interface utilisateur du composant concerné. Si vous voulez modifier la configuration AVG pour mieux l'adapter à vos besoins, accédez aux ***paramètres avancés d'AVG*** : cliquez sur le menu ***Outils/Paramètres avancés*** et modifiez la configuration AVG dans la boîte de dialogue ***Paramètres avancés***

d'AVG qui s'affiche.

6. Interface utilisateur AVG

AVG 2011 Edition Serveur de Fichiers affiche la fenêtre principale :



La fenêtre principale comprend plusieurs parties :

- ***Menu système*** *(barre de menus en haut de la fenêtre)* : ce système de navigation standard donne accès à l'ensemble des composants, des services et des fonctions AVG - détails >>
- ***Informations sur l'état de la sécurité*** *(partie supérieure de la fenêtre)* : donne des informations sur l'état actuel du programme AVG - détails >>
- ***Liens d'accès rapide*** *(partie gauche de la fenêtre)* : ces liens permettent d'accéder rapidement aux tâches AVG les plus importantes et les plus courantes - détails >>
- ***Présentation des composants*** *(partie centrale de la fenêtre)* : présentation générale de tous les composants AVG installés - détails >>
- ***Statistiques*** *(partie gauche inférieure de la fenêtre)* : toutes les données statistiques sur le fonctionnement du programme - détails >>
- ***Icône d'état AVG*** *(coin inférieur droit de l'écran, sur la barre d'état*

système) : elle indique l'état actuel du programme AVG - détails >>

6.1. Menu système

Le ***menu système*** est le système de navigation standard propre à toutes les applications Windows. Il se présente sous la forme d'une barre horizontale en haut de la fenêtre prinicipale du programme **AVG 2011 Edition Serveur de Fichiers**. Servez-vous du menu système pour accéder aux composants, fonctions et services AVG de votre choix.

Le menu système inclut cinq sections principales :

6.1.1. Fichier

- ***Quitter*** - ferme l'interface utilisateur d'**AVG 2011 Edition Serveur de Fichiers** . L'application AVG continue néanmoins de s'exécuter en arrière-plan de sorte que l'ordinateur reste protégé !

6.1.2. Composants

L'option ***Composants*** du menu système contient des liens qui renvoient vers tous les composants AVG installés et ouvrent la boîte de dialogue par défaut associée dans l'interface utilisateur :

- ***Présentation du système*** - ouvre l'interface utilisateur par défaut et affiche une présentation générale de tous les composants installés et leur état
- ***Composants serveur*** - présente les composants de sécurité disponibles et indique leur état - détails >>
- ***Le composant Anti-Virus*** garantit que l'ordinateur est protégé contre les virus essayant de pénétrer dans le système - détails >>
- ***Anti-Spyware*** garantit que l'ordinateur est protégé contre les spywares et les adwares - détails >>
- ***Le composant Bouclier résident*** s'exécute en arrière-plan et analyse les fichiers lorsqu'ils sont copiés, ouverts ou enregistrés - détails >>
- ***Le composant Mise à jour*** recherche la présence d'une mise à jour AVG - détails >>
- ***Licence*** affiche le type, le numéro et la date d'expiration de la licence - détails >>
- ***L'outil Administration à distance*** n'apparaît que dans si vous avez précisez, au cours de l'installation, que vous voulez installer ce composant.
- ***Le composant Anti-Rootkit*** détecte les programmes et les technologies cherchant à dissimuler des codes malveillants - détails >>

6.1.3. Historique

- ***Résultats des analyses*** - affiche l'interface d'analyse AVG et ouvre notamment la boîte de dialogue ***Résultats d'analyse***

- ***Détection du Bouclier résident*** - ouvre la boîte de dialogue contenant une vue générale des menaces détectées par le ***Bouclier résident***

- ***Quarantaine*** - ouvre l'interface de la zone de confinement (***Quarantaine***) dans laquelle AVG place les infections détectées qui n'ont pu, pour une raison quelconque, être réparées automatiquement A l'intérieur de cette quarantaine, les fichiers infectés sont isolés. L'intégrité de la sécurité de l'ordinateur est donc garantie et les fichiers infectés sont stockés en vue d'une éventuelle réparation future.

- ***Journal de l'historique des événements*** - ouvre l'interface de l'historique des événements présentant toutes les actions d'**AVG 2011 Edition Serveur de Fichiers** qui ont été consignées.

6.1.4. Outils

- ***Analyse complète*** - ouvre l'interface d'analyse AVG et procède à l'analyse de l'intégralité des fichiers de l'ordinateur

- ***Analyser le dossier sélectionné*** - ouvre l'interface d'analyse AVG et permet de spécifier, au sein de l'arborescence de l'ordinateur, les fichiers et les dossiers à analyser

- ***Analyser le fichier*** - permet de lancer sur demande l'analyse d'un fichier sélectionné dans l'arborescence du disque

- ***Mise à jour*** - lance automatiquement le processus de mise à jour du composant **AVG 2011 Edition Serveur de Fichiers**

- ***Mise à jour depuis le répertoire*** - procède à la mise à jour grâce aux fichiers de mise à jour situés dans le dossier spécifié de votre disque local. Notez que cette option n'est recommandée qu'en cas d'urgence, c'est-à-dire si vous ne disposez d'aucune connexion Internet (*si, par exemple, l'ordinateur est infecté et déconnecté d'Internet ou s'il est relié à un réseau sans accès à Internet, etc.*). Dans la nouvelle fenêtre qui apparaît, sélectionnez le dossier dans lequel vous avez placé le fichier de mise à jour et lancez la procédure de mise à jour.

- ***Paramètres avancés*** - ouvre la boîte de dialogue ***Paramètres avancés AVG*** dans laquelle vous modifiez au besoin la **AVG 2011 Edition Serveur de Fichiers** configuration. En général, il est recommandé de conserver les paramètres par défaut de l'application tels qu'ils ont été définis par l'éditeur du logiciel.

6.1.5. Aide

- ***Sommaire*** - ouvre les fichiers d'aide du programme AVG
- ***Obtenir de l'aide en ligne*** - affiche le site Web d'AVG (http://www.avg.com) à la page du centre de support clients
- ***Site Internet AVG*** - ouvre le site Web d'AVG (http://www.avg.com)
- ***A propos des virus et des menaces*** - ouvre l'***Encyclopédie des virus en ligne,*** dans laquelle vous obtenez des informations détaillées sur le virus identifié
- ***Télécharger AVG Rescue CD*** - ouvre un navigateur Web pointant vers la page de téléchargement de l'outil AVG Rescue CD.
- ***Réactiver*** - ouvre la boîte de dialogue ***Activer AVG*** avec les données que vous avez saisies dans la boîte de dialogue ***Personnaliser AVG*** au cours du processus d'installation. Dans cette boîte de dialogue, vous saisissez votre numéro de licence en lieu et place de la référence d'achat (*le numéro indiqué lors de l'installation d'AVG*) ou de votre ancien numéro (*si vous installez une mise à niveau du produit AVG, par exemple*).
- ***Enregistrer maintenant*** - renvoie à la page d'enregistrement du site Web d'AVG (http://www.avg.com). Merci de compléter le formulaire d'enregistrement ; seuls les clients ayant dûment enregistré leur produit AVG peuvent bénéficier de l'assistance technique gratuite.

Remarque *: si vous utilisez une version d'évaluation* **AVG 2011 Edition Serveur de Fichiers***, les deux dernières options sont remplacées par* ***Acheter maintenant*** *et* ***Activer****, ce qui vous permet de vous procurer de suite la version complète du programme. Si le programme* **AVG 2011 Edition Serveur de Fichiers** *est installé à l'aide d'un numéro d'achat, vous avez alors le choix entre les options* ***Enregistrer*** *et* ***Activer****. Pour plus d'informations, consultez la section Licence de cette documentation.*

- ***A propos de AVG*** - ouvre la boîte de dialogue ***Informations*** comportant cinq onglets, où sont précisés le nom du programme, la version du programme, la version de la base de données virale, des informations système, le contrat de licence et des informations de contact d'***AVG Technologies CZ***.

6.2. Informations sur l'état de la sécurité

La section contenant les ***informations sur l'état de la sécurité*** figure dans la partie supérieure de la fenêtre principale AVG. Vous y trouverez des informations sur l'état actuel de la sécurité du programme **AVG 2011 Edition Serveur de Fichiers**. Les icônes illustrées ont la signification suivante :

 - L'icône verte indique qu'AVG est pleinement opérationnel. Votre système est totalement protégé et à jour ; tous les composants installés fonctionnent

convenablement.

 - L'icône orange signale qu'un ou plusieurs composants ne sont pas correctement configurés, il est conseillé d'examiner leurs propriétés ou paramètres. Aucun problème critique à signaler ; vous avez sans doute choisi de désactiver certains composants. Vous êtes protégé par AVG. Certains paramètres d'un composant réclament toutefois votre attention. Son nom est indiqué dans la section d'***informations sur l'état de la sécurité***.

Cette icône s'affiche également si, pour une raison quelconque, vous décidez d' ignorer l'erreur d'un composant (*l'option Ignorer l'état du composant est disponible dans le menu contextuel apparaissant suite à un clic droit sur l'icône du composant en question, dans la vue des composants de la fenêtre principale AVG*). Vous pouvez être amené à utiliser cette option dans certaines situations, mais il est vivement conseillé de désactiver l'option ***Ignorer l'état du composant*** dès que possible.

 - L'icône de couleur rouge signale que le programme AVG est dans un état critique ! Un ou plusieurs composants ne fonctionnent pas convenablement et AVG n'est plus en mesure d'assurer la protection de l'ordinateur. Veuillez immédiatement vous porter sur le problème signalé. Si vous ne pouvez pas le résoudre, contactez l'équipe du support technique AVG.

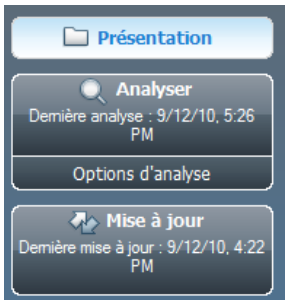
Si AVG n'utilise pas les performances optimales, un nouveau bouton, Corriger (ou Tout corriger si le problème implique plusieurs composants) apparaît près des informations relatives au statut de la sécurité. Cliquez sur le bouton pour lancer le processus automatique de vérification et de configuration du programme. C'est le moyen le simple d'optimiser les performances d'AVG et d'atteindre le plus haut niveau de sécurité.

Il est vivement conseillé de ne pas ignorer les informations sur l'état de la sécurité et, en cas de problème indiqué, de rechercher immédiatement une solution. A défaut, vous risquez de mettre en péril la sécurité de votre système.

Remarque : *vous pouvez à tout moment obtenir des informations l'état d'AVG en consultant l'icône de la barre d'état système.*

6.3. Liens d'accès rapide

Les liens d'accès rapide *(panneau gauche de l'interface utilisateur AVG)* permettent d'accéder immédiatement aux fonctions AVG les plus importantes et les plus utilisées :



- ***Présentation***- ce lien permet de passer de l'interface AVG affichée à l'interface par défaut, qui affiche tous les composants installés - voir le chapitre ***Présentation des composants >>***
- ***Analyser*** - par défaut, le bouton vous renseigne sur la dernière analyse effectuée (*type d'analyse, date de la dernière analyse*). Vous pouvez soit exécuter la commande ***Analyser*** pour relancer la même analyse ou cliquer sur le lien ***Analyse de l'ordinateur*** afin d'ouvrir l'interface d'analyse AVG. Celle-ci vous permettra d'exécuter ou de programmer des analyses ou encore d'en modifier les paramètres. Voir chapitre ***Analyse AVG >>***
- ***Mise à jour*** - le lien précise la date de la mise à jour la plus récente. Cliquez sur le lien pour lancer l'interface de mise à jour et exécuter immédiatement le processus de mise à jour AVG. Voir le chapitre ***Mises à jour d'AVG >>***
- ***Composants serveur*** - ce lien vous dirige vers l'écran ***Composants serveur***.

Ces liens sont accessibles en permanence depuis l'interface utilisateur. Lorsque vous cliquez sur un lien d'accès rapide, l'interface utilisateur graphique ouvre une nouvelle boîte de dialogue, mais les liens d'accès rapides restent disponibles. Par ailleurs, le processus est représenté de manière visuelle (voir l'illustration).

6.4. Présentation des composants

La section ***Présentation des composants*** figure dans le panneau central de l' interface utilisateur AVG. La section comprend deux parties :

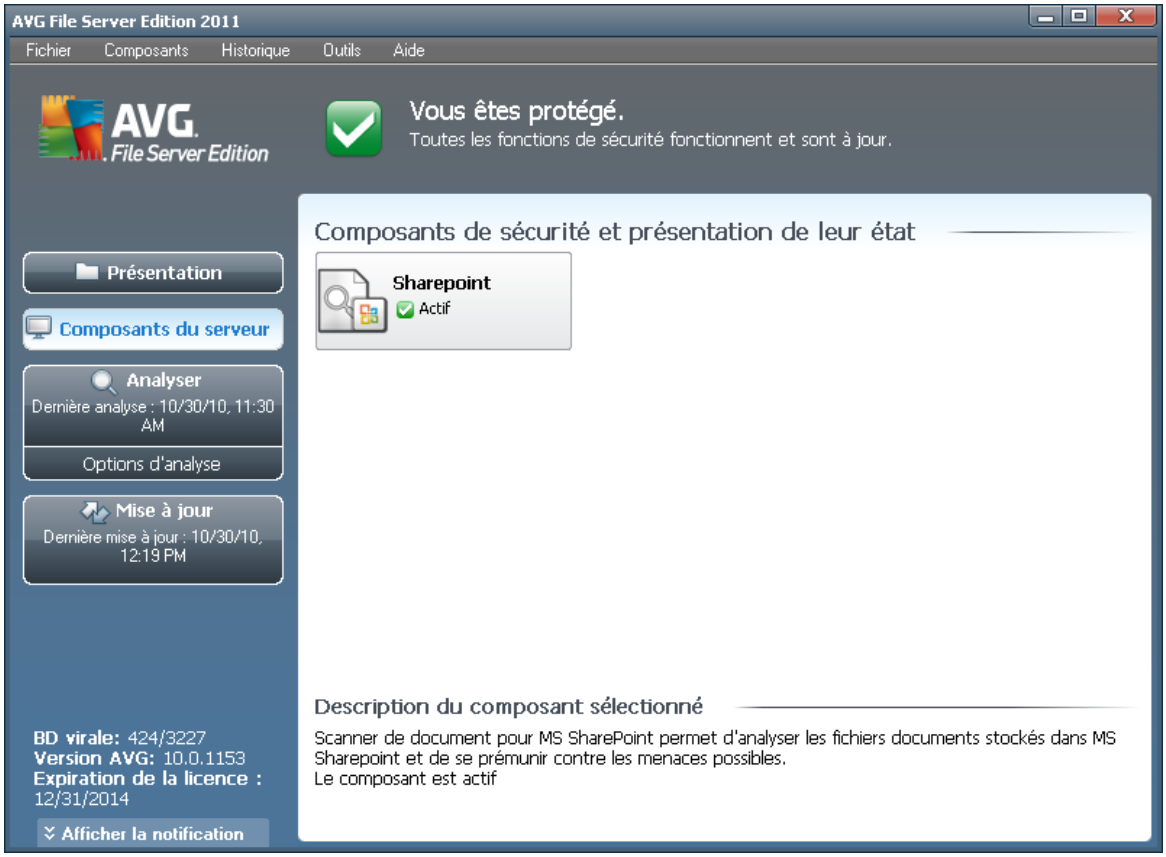
- Présentation de tous les composants installés représentés par une icône accompagnée d'un message signalant si le composant est actif ou non
- Description du composant sélectionné

Dans **AVG 2011 Edition Serveur de Fichiers**, le panneau de ***présentation des composants*** contient des renseignements sur les composants suivants :

- ***Le composant Anti-Virus*** garantit que l'ordinateur est protégé contre les virus essayant de pénétrer dans le système - détails >>

- ***Anti-Spyware*** garantit que l'ordinateur est protégé contre les spywares et les adwares - détails >>

6.5. Composants du serveur



La section ***Composants du serveur*** figure dans le panneau central de l'interface utilisateur AVG. La section comprend deux parties :

- Présentation de tous les composants installés représentés par une icône accompagnée d'un message signalant si le composant est actif ou non

- Description du composant sélectionné

Dans **AVG 2011 Edition Serveur de Fichiers**, le panneau ***Composants du serveur*** contient des renseignements sur les composants suivants :

- ***SharePoint*** permet d'analyse les fichiers de documents stockés dans MS SharePoint et de se prémunir contre toute forme de menace existante - détails >>

Cliquer sur l'icône d'un composant permet de le mettre en surbrillance dans la vue générale des composants. Par ailleurs, la fonctionnalité de base du composant est décrite en bas de l'interface utilisateur. Double-cliquez sur l'icône d'un composant a pour effet d'ouvrir l'interface du composant présentant une liste de données statistiques.

Cliquez avec le bouton droit de la souris sur l'icône d'un composant : après l'ouverture de l'interface graphique du composant en question, vous serez en mesure de sélectionner l'état ***Ignorer l'état du composant***. Sélectionnez cette option pour indiquer que vous avez noté l'état incorrect du composant, mais que vous souhaitez conserver la configuration AVG en l'état et ne plus être avisé de l'erreur par l'altération de l'icône de la barre d'état système.

6.6. Statistiques

La section ***Statistiques*** figure en bas à gauche de l'***interface utilisateur AVG***. Elle présente une liste d'informations sur le fonctionnement du programme :

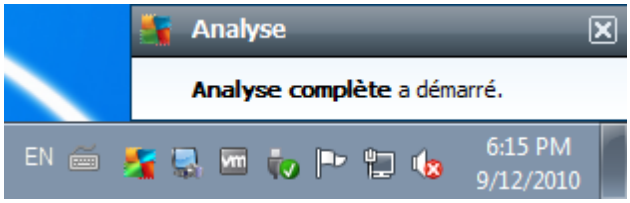
- ***Base de données virale***- précise la version de la base de données virale actuellement installée
- ***Version AVG*** - indique la version du programme actuellement installée *(le numéro se présente sous la forme 10.0.xxxx. 10.0 désigne la version du produit et xxxx le numéro du build)*
- ***Expiration de la licence*** - précise la date à laquelle votre licence AVG cessera d'être valide

6.7. Icône de la barre d'état système

L'***icône de la barre d'état système*** (*dans la barre des tâches Windows*) signale l'état actuel du programme **AVG 2011 Edition Serveur de Fichiers**. Elle est toujours visible dans la barre d'état, que la fenêtre principale AVG soit ouverte ou fermée :

Lorsqu'elle est en couleur, l'icône de la ***barre d'état système*** indique que tous les composants AVG sont actifs et entièrement opérationnels. Par ailleurs, l'icône AVG dans la barre d'état est en couleur si AVG signale une erreur mais que vous en avez été averti et avez choisi d'***ignorer l'état du composant***. Une icône marquée d'un point d'exclamation signale un problème (*composant inactif, erreur, etc.*). Double-cliquez sur l'***icône de la barre d'état système*** pour ouvrir la fenêtre et modifier un composant.

L'icône de la barre d'état système donne également des informations sur les activités actuelles du programme AVG et l'éventuel changement du statut du programme (*par exemple, le lancement automatique d'une analyse programmée ou d'une mise à jour, la modification du statut d'un composant, une erreur etc.*) par le biais de la fenêtre contextuelle qui s'affiche depuis l'icône de la barre d'état système AVG :



L'***icône de la barre d'état système*** peut aussi servir de lien d'accès rapide à la fenêtre principale AVG. Pour l'utiliser, il suffit de double-cliquer dessus. En cliquant avec le bouton droit de la souris sur l'***icône de la barre d'état système***, un menu contextuel contenant les options suivantes apparaît :

- ***Ouvrir l'Interface utilisateur AVG*** - cette commande permet d'afficher l' interface utilisateur AVG
- ***Analyses*** - cette commande permet d'ouvrir le menu contextuel desanalyses prédéfinies (*Analyse complète*, *Analyse zones sélectionnées*, *Analyse Anti-Rootkit*) et sélectionnez l'analyse requise, elle sera lancée immédiatement
- ***Analyses en cours d'exécution*** - cette option n'est visible que si une analyse est en cours sur l'ordinateur. Vous êtes libre de définir la priorité de ce type d'analyse, de l'interrompre ou de la suspendre. Les options suivantes sont disponibles : *Définir la priorité pour toutes les analyses, Suspendre toutes les analyses* ou *Arrêter toutes les analyses*.
- ***Mise à jour*** - cette option permet de lancer une mise à jour immédiate
- ***Aide*** - ouvre le fichier d'aide à la page d'accueil

7. Composants AVG

7.1. Anti-Virus

7.1.1. Principes de l'Anti-Virus

Le moteur d'analyse du logiciel anti-virus examine les fichiers et l'activité liée aux fichiers (ouverture, fermeture, etc.) afin de déceler la présence de virus connus. Tout virus détecté sera bloqué, puis effacé ou placé en quarantaine. La plupart des anti-virus font également appel à la méthode heuristique en utilisant les caractéristiques des virus, appelées également signatures des virus, pour analyser les fichiers. En d'autres termes, l'analyse anti-virus est en mesure de filtrer un virus inconnu si ce nouveau virus porte certaines caractéristiques de virus existants.

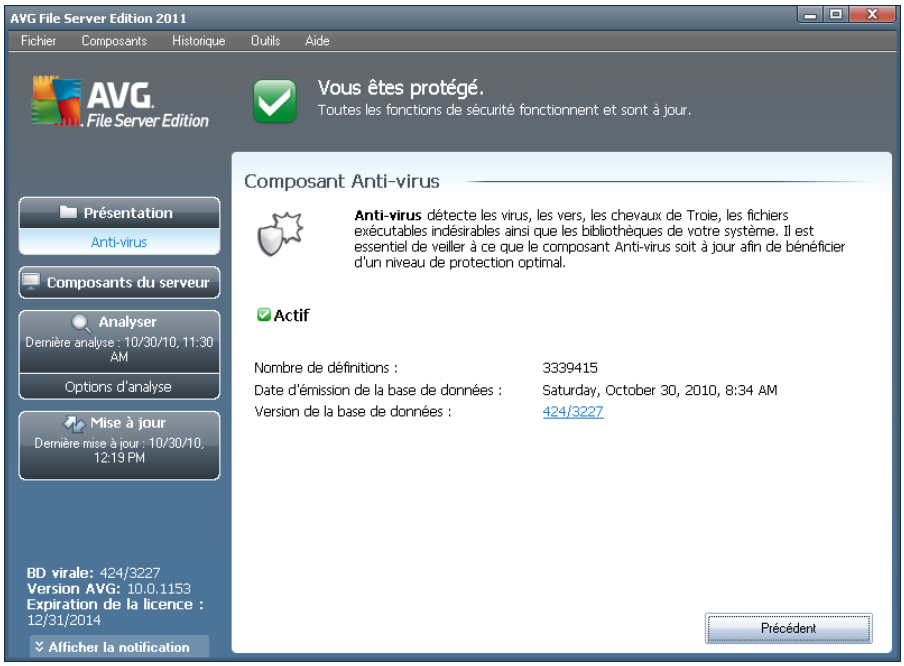
Rappelons que la fonction essentielle d'une protection anti-virus consiste à empêcher l'exécution de tout virus inconnu sur l'ordinateur.

Aucune technologie n'est infaillible, c'est pourquoi la fonction ***Anti-Virus*** combine plusieurs technologies pour repérer ou identifier un virus et garantir la protection de votre ordinateur :

- Analyse - recherche d'une chaîne de caractère typique d'un virus donné
- Analyse heuristique - émulation dynamique des instructions de l''objet analysé dans un environnement de machine virtuelle
- Détection générique - détection des instructions caractéristiques d'un virus ou d'un groupe de virus donné

AVG peut aussi analyser et détecter des exécutables ou bibliothèques DLL qui peuvent se révéler malveillants pour le système. De telles menaces portent le nom de programmes potentiellement dangereux (types variés de spywares, d'adwares, etc.). Enfin, AVG analyse la base de registre de votre système afin de rechercher toute entrée suspecte, les fichiers Internet temporaires ou les cookies. Il vous permet de traiter les éléments à risque de la même manière que les infections.

7.1.2. Interface de l'Anti-Virus



L'interface du composant ***Anti-Virus*** donne des informations de base sur la fonctionnalité du composant, sur son état actuel (Le composant *Anti-Virus est actif.*), ainsi que des statistiques sur la fonction ***anti-virus*** :

- ***Nombre de définitions*** - indique le nombre de virus définis dans la dernière version à ce jour de la base de données virale
- ***Date d'émission de la base de données*** - précise la date et l'heure à laquelle la base de données a été mise à jour
- ***Version de la base de données*** - indique le numéro de la version de la base de données virale actuellement installée; ce chiffre est incrémenté à chaque mise à jour de la base de données

L'interface du composant n'affiche qu'un seul bouton de commande (***Précédent***) - ce bouton permet de revenir à l'interface utilisateur AVG *par défaut (présentation des composants*).

7.2. Anti-Spyware

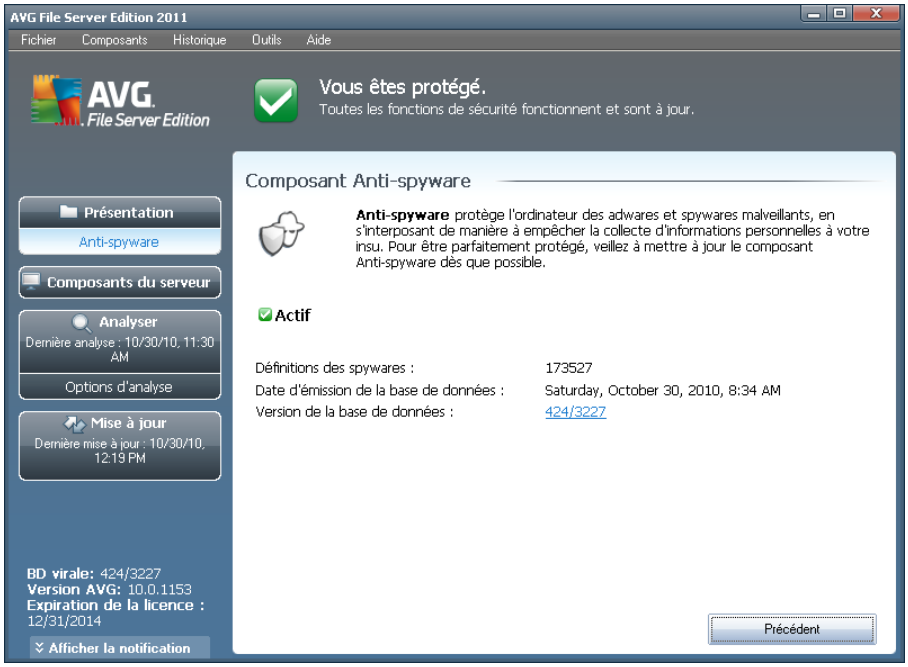
7.2.1. Principes de l'Anti-Spyware

Le terme spyware désigne généralement un code malicieux et plus précisément un logiciel qui collecte des informations depuis l'ordinateur d'un utilisateur, à l'insu de celui-ci. Certains spywares installés volontairement peuvent contenir des informations à caractère publicitaire, des pop-ups ou d'autres types de logiciels déplaisants.

Actuellement, les sites Web au contenu potentiellement dangereux sont les sources d'infection les plus courantes. D'autres vecteurs comme la diffusion par mail ou la transmission de vers et de virus prédominent également. La protection la plus importante consiste à définir un système d'analyse en arrière-plan, activé en permanence (tel que le composant ***Anti-Spyware***) agissant comme un bouclier résident afin d'analyser les applications exécutées en arrière-plan.

L'introduction de codes malicieux dans votre ordinateur, avant installation du programme AVG, ou en cas d'oubli de l'application des dernières mises à jour de la base de données et du programme **AVG 2011 Edition Serveur de Fichiers** ***est un risque potentiel. Pour cette raison, AVG vous offre la possibilité d'analyser intégralement votre ordinateur à l'aide d'une fonction prévue à cet effet. Il se charge également de détecter les codes malicieux inactifs ou en sommeil (ceux qui ont été téléchargés, mais non activés).

7.2.2. Interface de l'Anti-Spyware



L'interface du composant ***Anti-Spyware*** donne un bref aperçu de la fonctionnalité du composant et fournit des informations sur son état actuel et certaines statistiques ***Anti-Spyware*** :

- ***Définitions des spywares*** - indique le nombre de spywares définis dans la dernière version de la base de données
- ***Date d'émission de la base de données*** - précise la date et l'heure à laquelle la base de données a été mise à jour
- ***Version de la base de données*** - spécifie le numéro de la version de la base de données la plus récente ; ce nombre est incrémenté à chaque mise à jour de la base de données

L'interface du composant n'affiche qu'un seul bouton de commande (***Précédent***) - ce bouton permet de revenir à l'Interface utilisateur AVG *par défaut (présentation des composants*).

7.3. Bouclier résident

7.3.1. Principes du Bouclier résident

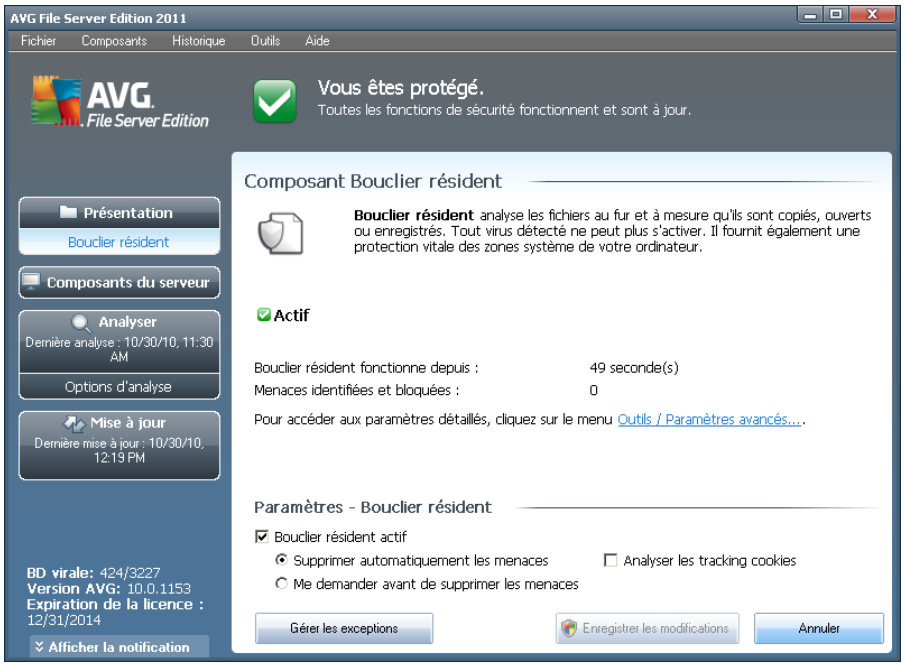
Le composant ***Bouclier résident*** assure une protection en temps réel de votre ordinateur. Il analyse chaque fichier ouvert, enregistré ou copié et surveille les zones système de l'ordinateur. Si le composant***Bouclier résident***détecte un virus dans un fichier, il interrompt l'opération en cours et ne donne pas la possibilité au virus de s'activer. Généralement, vous ne remarquez pas ce processus, car il fonctionne "en arrière-plan". Vous êtes seulement averti en cas de détection de menaces, tandis que le ***Bouclier résident*** bloque l'activation de la menace et l'éradique. Le ***Bouclier résident*** est chargé dans la mémoire de votre ordinateur au démarrage du système.

Actions possibles du Bouclier résident :

- Recherche de types spécifiques de menaces possibles
- *Analyse des supports amovibles (clés USB, etc.*)
- Analyse des fichiers ayant une extension déterminée ou sans précision d'extension
- Autorisation d'exceptions pour l'analyse – des fichiers ou des dossiers spécifiques qui ne doivent jamais être analysés

Attention : le Bouclier résident est chargé dans la mémoire de votre ordinateur au cours du démarrage; il est vital qu'il reste toujours activé !

7.3.2. Interface du Bouclier résident



Outre une présentation du fonctionnement du composant ***Bouclier résident*** et des informations sur son état, l'interface du ***Bouclier résident*** fournit quelques données statistiques :

- ***Le Bouclier résident est actif depuis***- indique le temps écoulé depuis le dernier lancement du composant
- ***Menaces identifiées et bloquées*** - indique le nombre d'infections détectées dont l'exécution ou l'ouverture a été bloquée (*il est possible de réinitialiser cette valeur, si besoin est, à des fins statistiques par exemple - Réinitialiser la valeur*)

Paramètres - Bouclier résident

Dans la partie inférieure de la boîte de dialogue figure la section ***Paramètres du Bouclier résident***, dans lequel vous pouvez modifier certains paramètres de base de la fonctionnalité du composant (*comme pour tous les autres composants, la configuration détaillée est accessible via l'élément Outils/Paramètres avancés du menu système*).

L'option ***Le Bouclier résident est actif*** permet d'activer ou désactiver la protection résidente. Par défaut, cette fonction est activée. Si la protection résidente est activée, vous pouvez définir plus précisément la manière dont les infections détectées sont traitées (c'est-à-dire supprimées) :

- automatiquement (***Supprimer automatiquement les menaces***)

- ou seulement après accord de l'utilisateur (***Me demander avant de supprimer les menaces***)

Cette option n'a pas d'impact sur le niveau de la sécurité, mais reflète uniquement les préférences de l'utilisateur.

Dans les deux cas, vous conservez la possibilité de ***supprimer automatiquement les cookies***. Dans certaines circonstances, vous pouvez activer cette option pour appliquer le niveau de sécurité le plus élevé. Notez que cette option est désactivée par défaut. (*cookies : portions de texte envoyées par un serveur à un navigateur Web et renvoyées en l'état par le navigateur chaque fois que ce dernier accède au serveur. Les cookies HTTP servent à authentifier, à suivre et à gérer certaines informations sur les utilisateurs telles que leurs préférences en matière de site ou le contenu de leur panier d'achat électronique*).

Remarque : *l'éditeur du logiciel a configuré tous les composants AVG de manière à obtenir des performances optimales. Aussi est-il recommandé de ne pas modifier la configuration AVG sans motif valable. Tout changement de ces paramètres doit être réalisé par un utilisateur expérimenté. Si vous devez modifier la configuration d'AVG, sélectionnez le menu* ***Outils / Paramètres avancés*** *et modifiez la configuration d'AVG dans la boîte de dialogue Paramètres avancés d'AVG qui apparaît.*

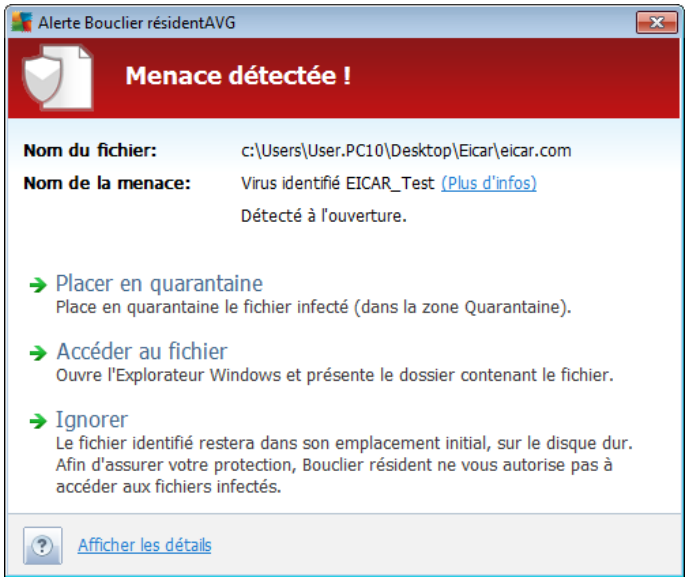
Boutons de commande

Les boutons de commande disponibles dans l'interface du ***Bouclier résident*** sont :

- ***Gérer les exceptions*** - ouvre la boîte de dialogue ***Bouclier résident - Eléments exclus*** où vous pouvez définir les dossiers à ne pas inclure dans l'analyse du ***Bouclier résident***
- ***Enregistrer les modifications*** - cliquez sur ce bouton pour enregistrer et appliquer les modifications apportées dans cette boîte de dialogue
- ***Annuler*** - cliquez sur ce bouton pour revenir à l'***interface utilisateur AVG*** par défaut (*avec la présentation générale des composants*)

7.3.3. Détection du Bouclier résident

Le composant Bouclier résident analyse les fichiers lorsqu'ils sont copiés, ouverts ou enregistrés. Lorsqu'un virus ou tout autre type de menace est détecté, vous êtes averti immédiatement via la boîte de dialogue suivante :



Dans cette fenêtre d'avertissement, vous trouverez des informations sur le fichier qui a été détecté et défini comme étant infecté (*Nom du fichier*), le nom de l'infection reconnue (*Nom de la menace*) ainsi qu'un lien renvoyant à l'***Encyclopédie des virus*** contenant de plus amples détails sur l'infection, le cas échéant (*Plus d'infos*).

Par la suite, vous devez décider la mesure à appliquer ; vous avez le choix entre les options suivantes :

Notez que, dans certaines conditions (type de fichier infecté et emplacement du fichier), certaines de ces options ne sont pas actives !

- ***Supprimer la menace en tant qu'utilisateur avancé*** - cochez cette case si, en tant que simple utilisateur, vous pensez ne pas disposer des droits suffisants pour supprimer la menace. Les utilisateurs avec pouvoirs ont des droits d'accès étendus. Si la menace est située dans un dossier système déterminé, vous pouvez avoir besoin de cocher cette case pour la supprimer.

- ***Réparer*** - ce bouton ne s'affiche que si une solution permettant de traiter l'infection décelée existe. Dans ce cas, elle élimine l'infection et rétablit l'état initial du fichier. Si le fichier lui-même est un virus, cette fonction le supprime (*en plaçant le fichier dans la zone* ***Quarantaine***)

- ***Placer en quarantaine*** : le virus sera placé dans la ***Quarantaine d'AVG***

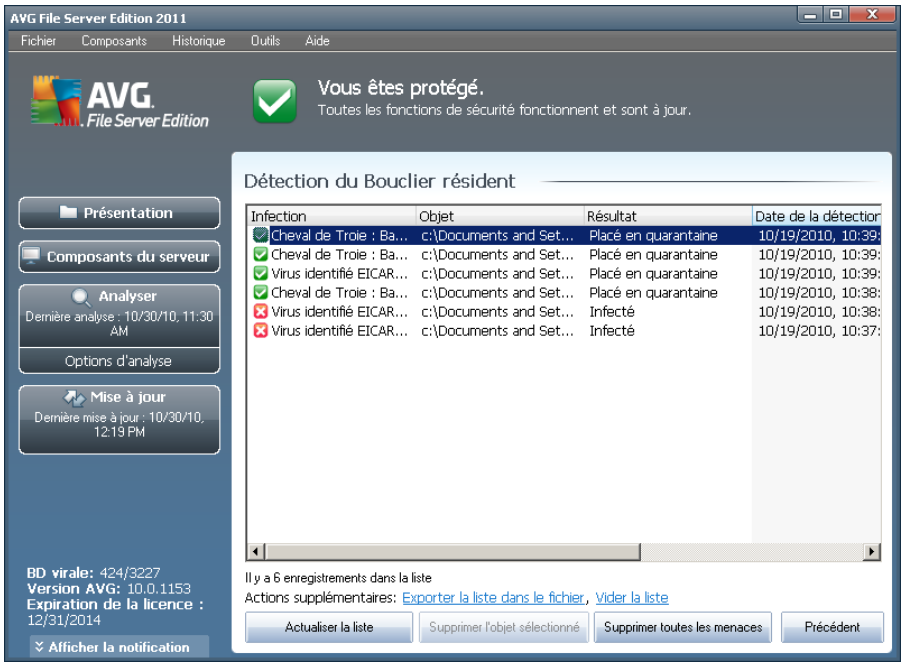
- ***Accéder au fichier*** - cette option vous redirige vers l'emplacement d'origine de l'objet suspect (*ouvre une nouvelle fenêtre de Windows Explorer*)

- ***Ignorer*** : nous vous recommandons fortement de ne PAS utiliser cette option sauf si vous avez une très bonne raison de le faire !

Dans la section inférieure de la boîte de dialogue, vous trouverez le lien ***Afficher les détails***. Cliquez dessus pour ouvrir la fenêtre contenant des informations détaillées sur

le processus en cours lorsque l'infection a été détectée et l'identification du processus.

Vous trouverez des informations sur la présentation des menaces détectées par le ***Bouclier résident*** dans la boîte de dialogue ***Détection par le Bouclier résident*** accessible par la barre de menus ***Historique / Détection du Bouclier résident*** :



La ***détection du Bouclier résident*** répertorie les objets détectés par le ***Bouclier résident*** comme étant dangereux, puis réparés ou déplacés en ***quarantaine***. Les informations suivantes accompagnent chaque objet détecté :

- ***Infection*** - description (et éventuellement le nom) de l'objet détecté
- ***Objet*** - emplacement de l'objet
- ***Résultat*** - action effectuée sur l'objet détecté
- ***Date de la détection*** - date et heure auxquelles l'objet a été détecté
- ***Type d'objet*** - type de l'objet détecté
- ***Processus*** - action réalisée pour solliciter l'objet potentiellement dangereux en vue de sa détection

Dans la partie inférieure de la boîte de dialogue, sous la liste, vous trouverez des informations sur le nombre total d'objets détectés répertoriés ci-dessus. Par ailleurs, vous êtes libre d'exporter la liste complète des objets détectés dans un fichier (***Exporter la liste dans le fichier***) et de supprimer toutes les entrées des objets détectés (***Vider la liste***). Le bouton ***Actualiser la liste*** permet de rafraîchir la liste des menaces détectées par le ***Bouclier résident***. Le bouton ***Précédent*** permet de revenir

dans l'***interface utilisateur AVG*** par défaut (*présentation des composants*).

7.4. Mise à jour

7.4.1. Principes du composant Mise à jour

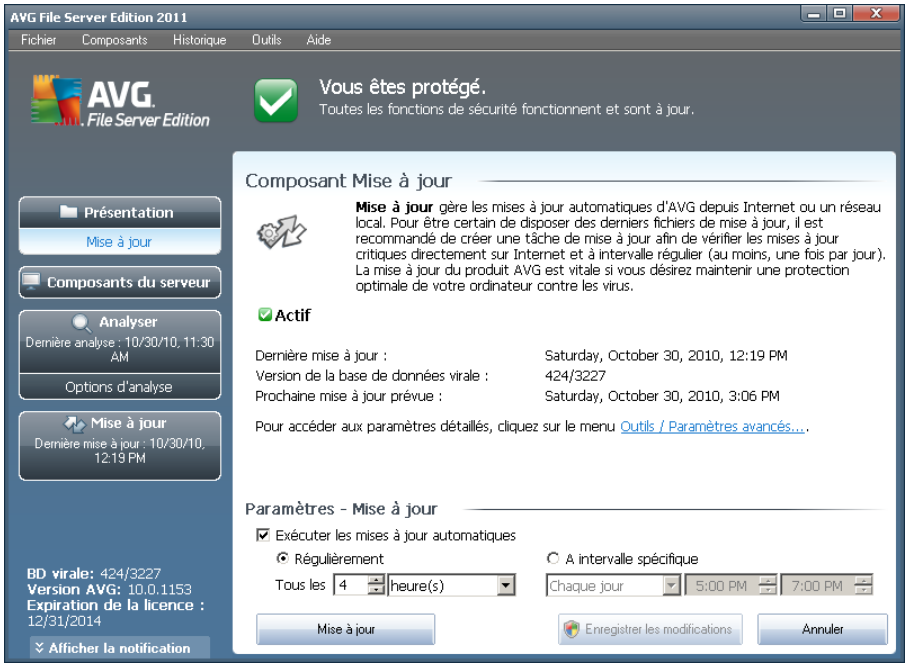
Aucun logiciel de sécurité ne peut garantir une protection fiable contre la diversité des menaces à moins d'une mise à jour régulière. Les auteurs de virus sont toujours à l'affût de nouvelles failles des logiciels ou des systèmes d'exploitation. Chaque jour apparaissent de nouveaux virus, malwares et attaques de pirates. C'est pour cette raison que les éditeurs de logiciels ne cessent de diffuser des mises à jour et des correctifs de sécurité visant à combler les vulnérabilités identifiées.

C'est pourquoi il est essentiel de mettre régulièrement à jour votre produit AVG !

L'objet du composant ***Mise à jour*** est de vous aider à gérer la régularité des mises à jour. Dans ce composant, vous pouvez planifier le téléchargement automatique des fichiers de mise à jour par Internet ou depuis le réseau local. Les mises à jours de définitions de virus fondamentales doivent être exécutées quotidiennement si possible. Les mises à jour du programme, moins urgentes, peuvent se faire sur une base hebdomadaire.

Remarque : *veuillez lire attentivement le chapitre Mises à jour d'AVG pour plus d'informations sur les différents types et niveaux de mises à jour.*

7.4.2. Interface du composant Mise à jour



L'interface ***Mise à jour*** affiche des informations sur la fonctionnalité du composant, sur son état actuel et certaines statistiques :

- ***Dernière mise à jour*** - précise la date et l'heure à laquelle la base de données a été mise à jour
- ***Version de la base de données*** - indique le numéro de la version de la base de données virale actuellement installée; ce nombre est incrémenté à chaque mise à jour de la base de données
- ***Prochaine mise à jour prévue*** - indique l'heure exacte à laquelle la prochaine mise à jour de la base de données est programmée

Paramètres - Mise à jour

Dans la partie inférieure de la boîte de dialogue, section ***Paramètres - Mise à jour***, vous pouvez modifier les règles appliquées au lancement des mises à jour. Vous pouvez choisir de télécharger automatiquement les fichiers de mise à jour (***Exécuter les mises à jour automatiques***) ou simplement à la demande. Par défaut, l'option ***Exécuter les mises à jour automatiques*** est activée (option recommandée). Le téléchargement régulier des fichiers de mise à jour les plus récents est un facteur vital pour les performances de tout logiciel de sécurité.

Il est possible de préciser le moment auquel exécuter la mise à jour :

- ***Régulièrement*** - définissez la périodicité
- ***A intervalle spécifique*** - précisez l'heure exacte à laquelle la mise à jour doit avoir lieu

Par défaut, la mise à jour a lieu toutes les 4 heures. Il est généralement recommandé de conserver les paramètres par défaut et de ne les modifier qu'en cas d'absolue nécessité.

Remarque : *l'éditeur du logiciel a configuré tous les composants AVG de manière à obtenir des performances optimales. Aussi est-il recommandé de ne pas modifier la configuration AVG sans motif valable. Tout changement de ces paramètres doit être réalisé par un utilisateur expérimenté. Si vous devez modifier la configuration d'AVG, sélectionnez le menu* ***Outils / Paramètres avancés*** *et modifiez la configuration d'AVG dans la boîte de dialogue Paramètres avancés d'AVG qui apparaît.*

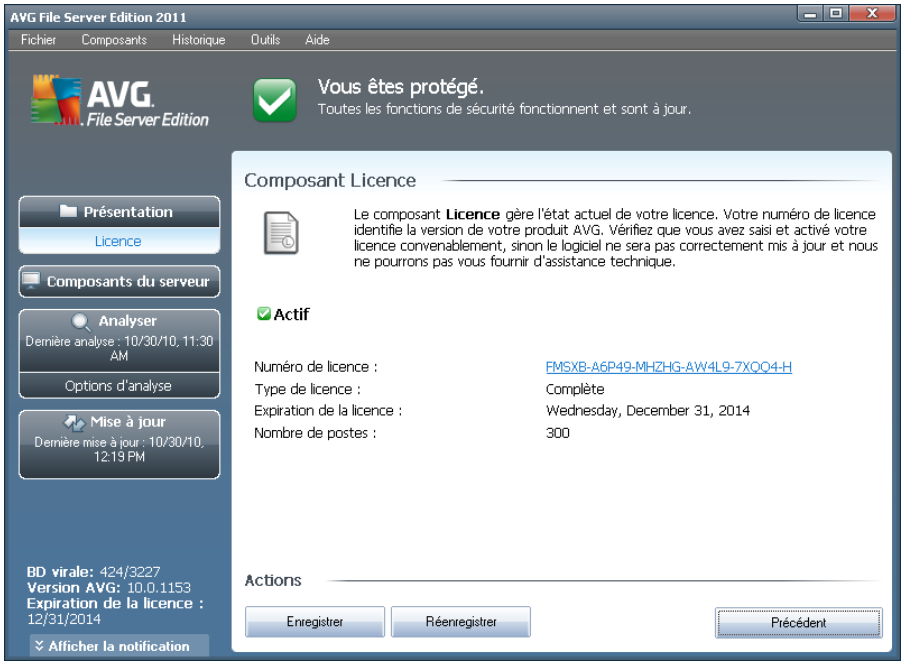
Boutons de commande

Les boutons de commande disponibles dans l'interface de ***Mise à jour*** sont :

- ***Mise à jour*** - exécute une mise à jour immédiate
- ***Enregistrer les modifications*** - cliquez sur ce bouton pour enregistrer et appliquer les modifications apportées dans cette boîte de dialogue

- ***Annuler*** - cliquez sur ce bouton pour revenir à l'***interface utilisateur AVG*** par défaut (*avec la présentation générale des composants*)

7.5. Licence



L'interface du composant ***Licence*** décrit brièvement le fonctionnement du composant, indique son état actuel et fournit les informations suivantes :

- ***Numéro de licence*** - désigne la forme abrégée de votre numéro de licence (*pour des raisons de sécurité, les quatre derniers caractères sont absents*). Lorsque vous saisissez un numéro de licence, vous devez le saisir exactement tel qu'il est affiché. Par conséquent, nous vous conseillons vivement de toujours procéder par "copier-coller" pour toute utilisation du numéro de licence.
- ***Type de licence*** - indique le type de produit installé.
- ***Expiration de la licence*** - cette date détermine la durée de validité de la licence. Pour continuer d'utiliser **AVG 2011 Edition Serveur de Fichiers** après cette date, il est nécessaire de renouveler votre licence. Le renouvellement peut être réalisé en ligne sur le site Web d'AVG.
- ***Nombre de postes*** - nombre de postes de travail sur lequel vous êtes autorisé à installer le produit **AVG 2011 Edition Serveur de Fichiers**.

Boutons de commande

- ***Enregistrer*** - renvoie à la page d'enregistrement du site Web d'AVG (http://

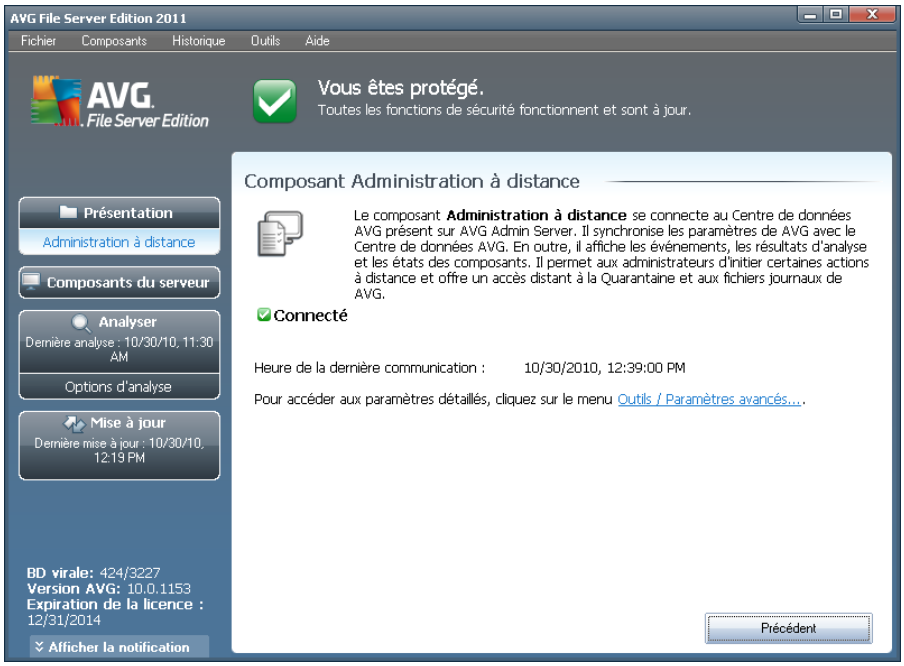
www.avg.com). Merci de compléter le formulaire d'enregistrement ; seuls les clients ayant dûment enregistré leur produit AVG peuvent bénéficier de l'assistance technique gratuite.

- ***Réactiver*** - affiche la boîte de dialogue ***Activer AVG*** avec les données saisies dans la boîte de dialogue ***Personnaliser AVG*** au cours du processus d'installation. Dans cette boîte de dialogue, vous indiquez votre numéro de licence en lieu et place de la référence d'achat (*le numéro indiqué lors de l'installation d'AVG*) ou de votre ancien numéro (*si vous installez une mise à niveau du produit AVG, par exemple*).

Remarque : si vous utilisez une version d'évaluation *AVG 2011 Edition Serveur de Fichiers*, **les boutons qui s'affichent sont** *Acheter maintenant* ***et*** *Activer et vous permettent de vous procurer de suite la version complète du programme. Si le programme* **AVG 2011 Edition Serveur de Fichiers** *est installé à l'aide d'un numéro d'achat, vous avez alors le choix entre les* ***Enregistrer*** *et* ***Activer****.*

- ***Précédent*** - cliquez sur ce bouton pour rétablir l'***interface utilisateur AVG*** paramétrée par défaut (*présentation des composants*).

7.6. Administration à distance



Le composant ***Administration à distance*** s'affiche seulement dans l'interface utilisateur **AVG 2011 Edition Serveur de Fichiers** lorsque vous avez installé l'Edition Réseau du produit (*voir le composant* ***Licence***). Dans la boîte de dialogue ***Administration à distance***, vous pouvez savoir si le composant est actif et connecté au serveur. Tous les paramètres du composant ***Administration à distance*** doivent être définis dans ***Paramètres avancés / Administration à distance***.

Pour obtenir une description détaillée des options et de la fonctionnalité du composant dans le système AVG, reportez-vous à la documentation spécifique consacrée à ce sujet. Cette documentation est téléchargeable à partir du site Web d'AVG (www.avg.com), section ***Centre de Support / Téléchargement / Documentation*** .

Boutons de commande

- ***Précédent*** - cliquez sur ce bouton pour rétablir l'interface utilisateur AVG paramétrée par défaut (*présentation des composants*).

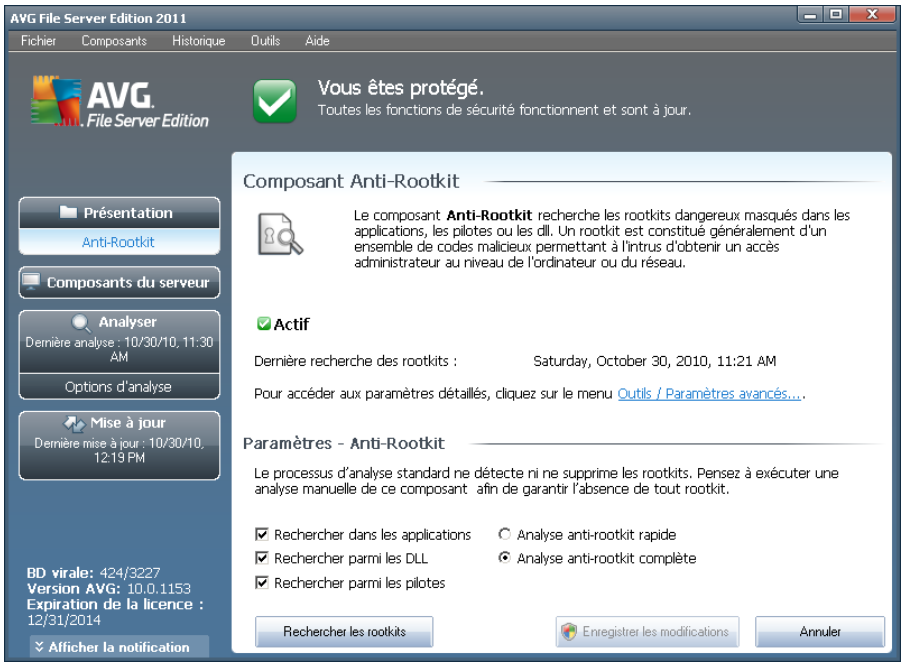
7.7. Anti-Rootkit

Un rootkit est un programme conçu pour prendre le contrôle du système, sans l'autorisation de son propriétaire et de son administrateur légitime. Un accès matériel est rarement nécessaire car un rootkit est prévu pour s'introduire dans le système d'exploitation exécuté sur le matériel. En règle générale, les rootkits dissimulent leur présence dans le système en dupant ou en contournant les mécanismes de sécurité standard du système d'exploitation. Souvent, ils prennent la forme de chevaux de Troie et font croire aux utilisateurs que leur exécution est sans danger pour leurs ordinateurs. Pour parvenir à ce résultat, différentes techniques sont employées : dissimulation de processus aux programmes de contrôle ou masquage de fichiers ou de données système, au système d'exploitation.

7.7.1. Principes de l'Anti-Rootkit

Le composant AVG Anti-Rootkit est un outil spécialisé dans la détection et la suppression des rootkits dangereux. Ces derniers sont des programmes et technologies de camouflage destinés à masquer la présence de logiciels malveillants sur l'ordinateur. ***AVG Anti-Rootkit*** peut détecter des rootkits selon un ensemble de règles prédéfinies. Notez que tous les rootkits sont détectés (*pas seulement ceux qui sont infectés*). Si ***AVG Anti-Rootkit*** détecte un rootkit, cela ne veut pas forcément dire que ce dernier est infecté. Certains rootkits peuvent être utilisés comme pilotes ou faire partie d'applications correctes.

7.7.2. Interface de l'Anti-Rootkit



L'interface utilisateur ***Anti-Rootkit*** décrit brièvement le rôle du composant , indique l'état actuel du composant et fournit des informations sur la dernière analyse effectuée par le module ***Anti-Rootkit*** (***Dernière recherche des rootkits***). La boîte de dialogue ***Anti-Rootkit*** inclut également un lien ***Outils/Paramètres avancés***. Ce lien permet d'être redirigé vers l'environnement de la configuration avancée du composant ***Anti-Rootkit***.

Remarque : *l'éditeur du logiciel a configuré tous les composants AVG de manière à obtenir des performances optimales. Aussi est-il recommandé de ne pas modifier la configuration AVG sans motif valable. Tout changement de ces paramètres doit être réalisé par un utilisateur expérimenté.*

Paramètres - Anti-Rootkit

Dans la partie inférieure de la boîte de dialogue figure la section ***Paramètres - Anti-Rootkit*** dans laquelle vous pouvez configurer les fonctions élémentaires de la détection de rootkits. Cochez tout d'abord les cases permettant d'indiquer les objets à analyser :

- ***Rechercher dans les applications***
- ***Rechercher parmi les DLL***
- ***Rechercher parmi les pilotes***

Vous pouvez ensuite choisir le mode d'analyse des rootkits :

- ***Analyse anti-rootkit rapide*** - analyse tous les processus en cours d'exécution, les pilotes chargés et le dossier système (*c:\Windows*)
- ***Analyse anti-rootkit complète*** - analyse tous les processus en cours d'exécution, les pilotes chargés et le dossier système (*c:\Windows généralement*), ainsi que tous les disques locaux (*y compris le disque flash, mais pas les lecteurs de disquettes ou de CD-ROM*)

Boutons de commande

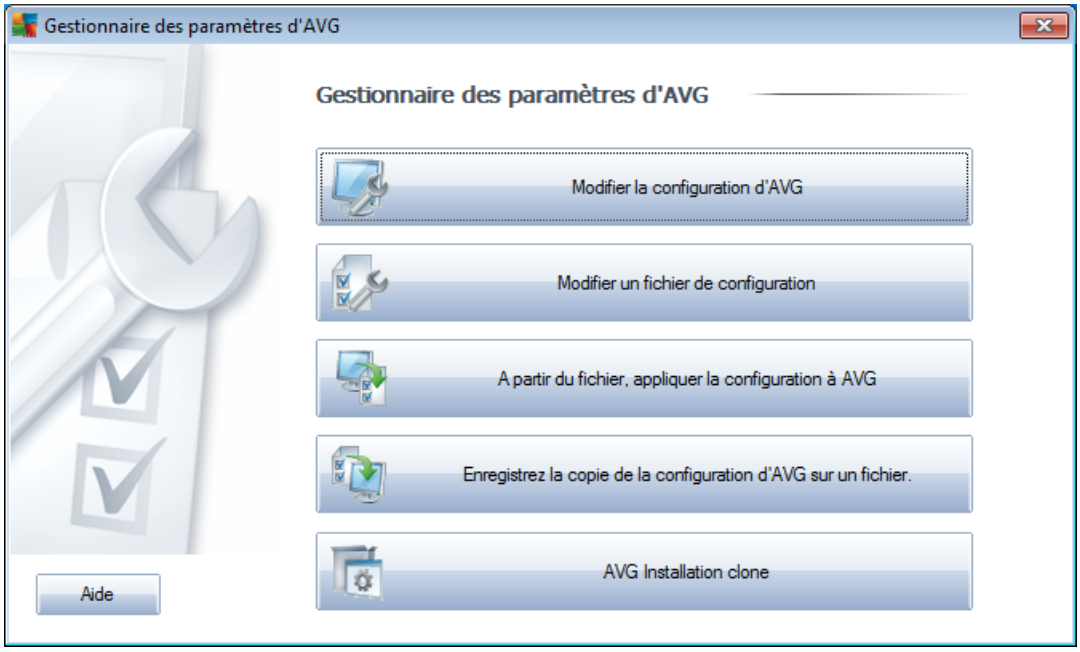
- ***Rechercher les rootkits*** - comme l'analyse anti-rootkit ne fait pas partie de l' ***analyse complète de l'ordinateur***, vous devez l'exécuter directement depuis l'interface ***Anti-Rootkit*** à l'aide de ce bouton
- ***Enregistrer les modifications*** - cliquez sur ce bouton pour enregistrer toutes les modifications réalisées dans cette interface et pour revenir à l'***interface utilisateur AVG*** par défaut (*vue d'ensemble des composants*)
- ***Annuler*** - cliquez sur ce bouton pour revenir à l'***interface utilisateur AVG*** par défaut (*vue d'ensemble des composants*) sans enregistrer les modifications que vous avez effectuées

8. Gestionnaire des paramètres AVG

Principalement indiqué pour les réseaux de petite taille, le ***Gestionnaire des paramètres AVG*** est un outil qui permet de copier, de modifier et de distribuer la configuration d'AVG. Vous pouvez enregistrer cette configuration sur un périphérique amovible (clé USB, etc.) et l'appliquer manuellement aux stations de votre choix.

Cet outil est inclus dans l'installation du programme AVG. Il est accessible via le menu Démarrer de Windows :

Tous les programmes/AVG 2011/Gestionnaire des paramètres AVG



- ***Supprimer la configuration d'AVG de cet ordinateur***

  Utilisez ce bouton pour ouvrir une boîte de dialogue qui propose des paramètres avancés de l'installation locale d'AVG. Toutes les modifications apportées à ce niveau affecteront également l'installation locale d'AVG.

- ***Charger et modifier le fichier de configuration d'AVG***

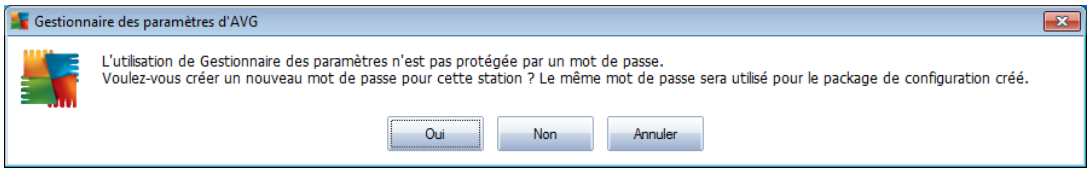
  Si vous disposez déjà d'un fichier de configuration d'AVG (.pck), utilisez ce bouton pour l'ouvrir et y apporter des modifications. Une fois les modifications confirmées à l'aide du bouton ***OK*** ou ***Appliquer***, le fichier est remplacé par les nouveaux paramètres !

- ***Appliquer la configuration depuis le fichier vers AVG sur cet ordinateur***

  Utilisez ce bouton pour ouvrir un fichier de configuration d'AVG (.pck) et appliquez-le à l'installation locale d'AVG.

- ***Conserver la configuration locale d'AVG dans un fichier***

  Utilisez ce bouton pour enregistrer le fichier de configuration (.pck) de l'installation locale d'AVG. Si vous n'avez pas défini de mot de passe pour les Actions autorisées, la boîte de dialogue suivante peut s'afficher :



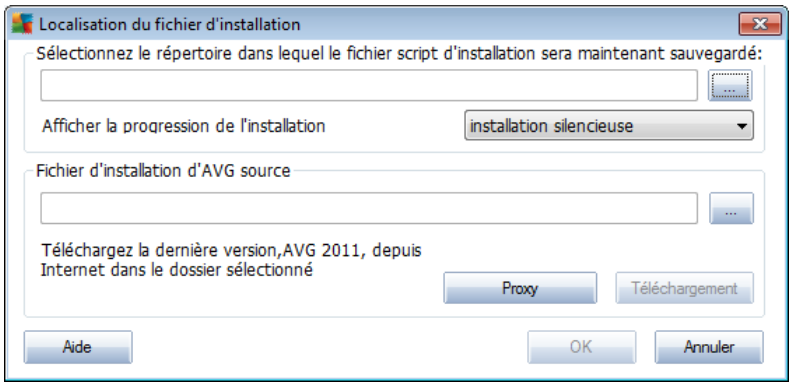
  Choisissez ***Oui*** pour créer immédiatement le mot de passe d'accès à la Liste des éléments autorisés, puis saisissez les informations requises avant de confirmer votre choix. Choisissez ***Non*** pour ignorer la création d'un mot de passe, puis enregistrez la configuration locale d'AVG dans un fichier.

- ***Cloner l'installation d'AVG***

  Cette option permet de faire une copie de l'installation locale d'AVG en créant un package d'installation qui contient des options personnalisées. Cette réplique inclut la plupart des paramètres AVG à l'exception des suivants :

  - Paramètres de langue
  - Paramètres audio
  - Configuration du pare-feu
  - Liste autorisée et exceptions PUP du composant Identity protection.

  Pour ce faire, sélectionnez d'abord le dossier où le script d'installation sera enregistré.



  Ensuite, choisissez l'une des options suivantes à partir du menu déroulant :

  - ***Installation masquée*** - aucune information n'est affichée lors de la procédure d'installation.

- ***Afficher uniquement la progression de l'installation*** - l'installation ne nécessite pas d'intervention de la part de l'utilisateur, mais la progression est parfaitement visible.

- ***Afficher l'assistant d'installation*** - l'installation est visible et l'utilisateur devra confirmer manuellement toutes les étapes.

Utilisez le bouton ***Télécharger*** pour télécharger le dernier fichier d'installation d'AVG, disponible directement sur le site Web d'AVG, dans le dossier sélectionné ou placez manuellement le fichier d'installation d'AVG dans ce dossier.

Vous pouvez utiliser le bouton ***Proxy*** pour définir les paramètres d'un serveur proxy, si le réseau l'exige pour établir une connexion.

Lorsque vous cliquez sur ***OK***, le processus de duplication démarre et prend un peu de temps. Une boîte de dialogue vous invitant à créer un mot de passe pour la liste des éléments autorisés s'affiche (voir ci-dessus). ***AvgSetup.bat*** devrait ensuite être disponible dans le dossier ainsi que d'autres fichiers. Si vous exécutez le fichier ***AvgSetup.bat***, il installe le programme AVG en fonction des paramètres précédemment choisis.

9. Composants du serveur AVG

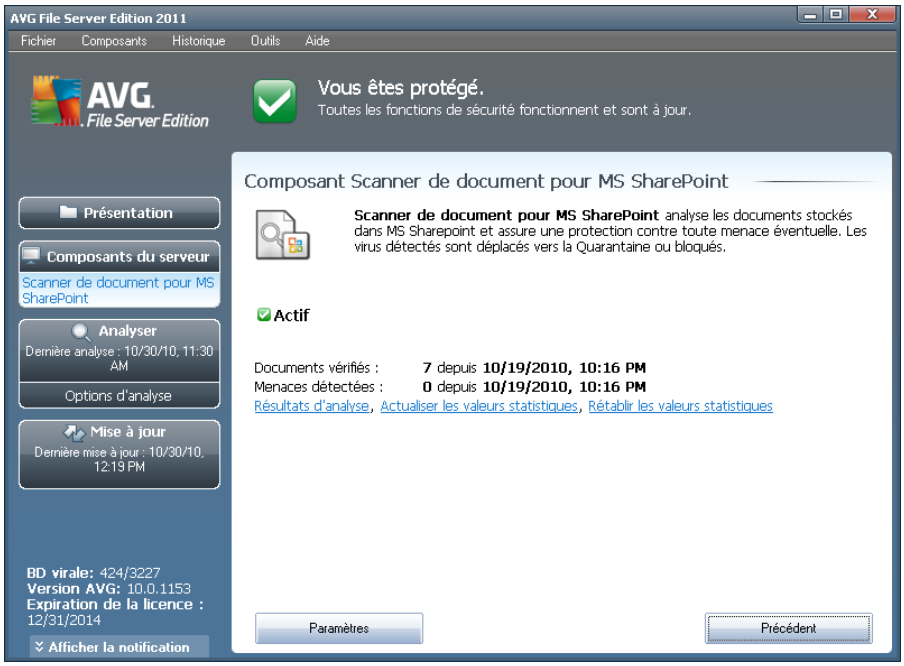
9.1. Scanner de documents pour MS SharePoint

9.1.1. Principes du Scanner de documents

Le composant serveur ***Scanner de documents pour MS SharePoint*** sert à analyser les documents enregistrés dans MS SharePoint. En cas de détection, les virus sont mis en quarantaine ou supprimés définitivement.

Microsoft SharePoint est un ensemble de produits et de logiciels qui comprend, parmi son nombre croissant de composants, des fonctions de collaboration basées sur Internet Explorer, des modules de gestion de processus, des modules de recherche et une plateforme de gestion de documents. SharePoint peut être utilisé pour héberger les sites Web qui exploitent des ressources partagées : espaces de travail, sources d'information et documents.

9.1.2. Interface de Scanner de documents



Outre une présentation des données statistiques les plus importantes et de l'état actuel du composant (*Le composant est actif*), l'interface ***Scanner de documents pour MS SharePoint*** fournit également certaines statistiques générales du composant :

- ***Documents vérifiés :***- nombre de documents analysés depuis une date donnée
- ***Menaces détectées*** - nombre d'infections décelées depuis une date donnée

Vous pouvez mettre à jour ces statistiques à tout moment en cliquant sur le lien ***Actualiser les statistiques***. De nouvelles données apparaissent de façon quasi immédiate. Pour remettre toutes les statistiques à zéro, cliquez sur le lien ***Réinitialiser les statistiques***. Pour finir, cliquez sur le lien ***Résultats d'analyses*** pour ouvrir une nouvelle boîte de dialogue contenant la liste des résultats d'analyse. Triez les données contenues dans cette liste à l'aide des boutons de radio et/ou des onglets.

Boutons de commande

Les boutons de commande disponibles dans l'interface du ***Scanner de documents pour MS Sharepoint*** sont les suivants :

- ***Paramètres*** - ouvre une nouvelle boîte de dialogue dans laquelle vous ajustez les différents paramètres de performances d'analyse antivirale du ***Scanner de documents pour MS SharePoint*** (pour plus d'informations à ce sujet, consultez les chapitres ***Paramètres avancés - Scanner de documents pour MS SharePoint*** et/ou ***Actions détectées***).

- ***Précédent*** - cliquez sur ce bouton pour revenir à l'***interface des composants du serveur***.

10. AVG pour SharePoint Portal Server

Ce chapitre est consacré à la maintenance d'AVG sur ***MS SharePoint Portal Server*** qui peut être considéré comme un type particulier de serveur de fichiers.

10.1. Maintenance du programme

AVG pour SharePoint Portal Server utilise l'interface d'analyse antivirale Microsoft SP VSAPI 1.4 pour la protection de votre serveur contre toute forme d'infection. Les objets sur le serveur sont analysés pour détecter la présence d'un code malveillant lorsqu'ils sont téléchargés depuis ou sur le serveur par vos utilisateurs. La configuration de la protection antivirale peut être installée grâce à l'interface ***Administration centrale*** de SharePoint Portal Server. Au sein de l'***administration centrale***, vous pouvez également consulter et gérer le fichier journal **AVG pour SharePoint Portal Server**.

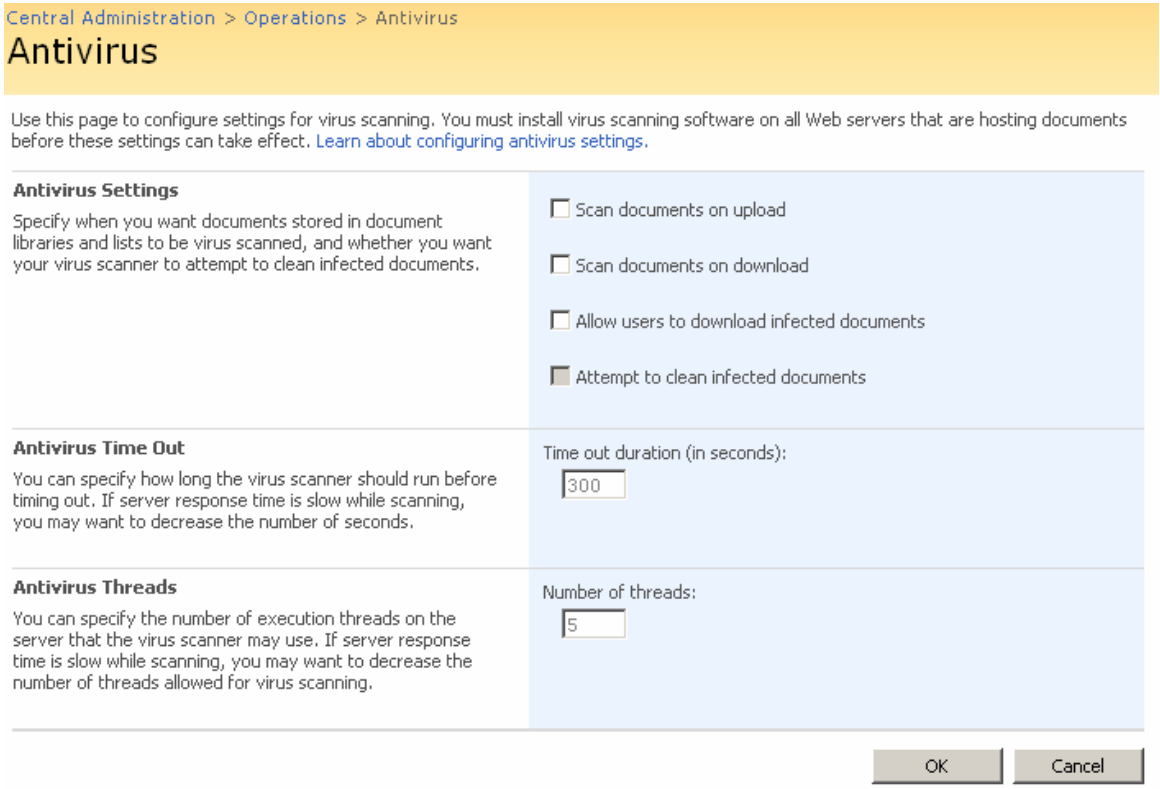
Vous pouvez lancer l'***administration centrale de SharePoint Portal Server*** lorsque vous ouvrez une session depuis l'ordinateur sur lequel votre serveur est exécuté. L'interface d'administration est une interface Web (*comme l'interface utilisateur du serveur SharePoint Portal Server*). Vous pouvez l'ouvrir grâce à l'option ***SharePoint Central Administration*** située dans le dossier ***Programs/Microsoft Office Server*** (selon votre version ***SharePoint Portal Server***) du menu ***Démarrer de Windows*** ou en accédant aux ***Outils d'administration*** et en choisissant ***Sharepoint Central Administration***.

Vous pouvez également accéder à la page Web ***Administration centrale de SharePoint Portal Server*** à distance en utilisant les droits d'accès et l'URL nécessaires.

10.2. Configuration d'AVG pour SPPS - Sharepoint 2007

Dans l'interface de l'***Administration centrale de Sharepoint 3.0***, vous pouvez facilement configurer les paramètres de performance et les tâches du scanner **AVG pour SharePoint Portal Server**. Choisissez l'option ***Opérations*** dans la section ***Administration centrale***. Une nouvelle boîte de dialogue s'affiche. Sélectionnez ***Anti-virus*** dans la section ***Configuration de la sécurité***.

La fenêtre suivante va s'afficher :

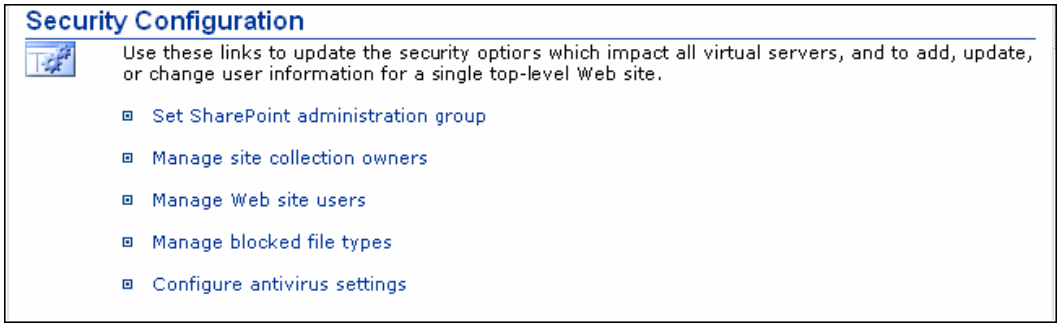


Vous pouvez, à partir d'ici, configurer différentes tâches d'analyse pour **AVG pour SharePoint Portal Server** ainsi que les caractéristiques de performance :

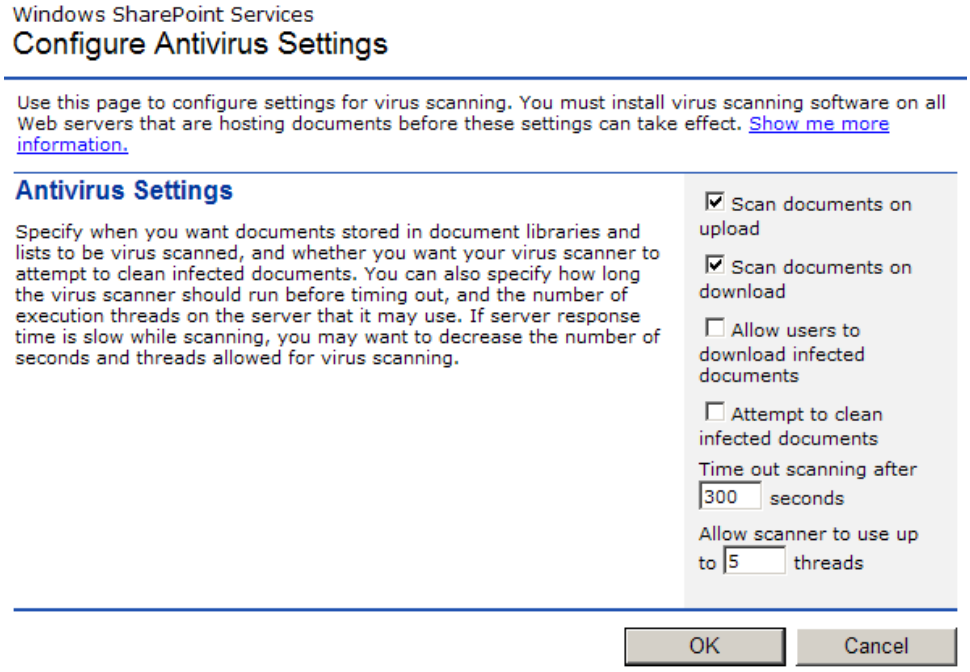
- ***Analyser les documents lors du chargement***– activer/désactiver l'analyse des documents qui sont en train d'être chargés
- ***Analyser les documents lors du téléchargement*** – activer/désactiver l'analyse des documents qui sont en train d'être téléchargés
- ***Autoriser les utilisateurs à télécharger des documents infectés*** – autoriser/empêcher le téléchargement de documents infectés par les utilisateurs
- ***Essayer de nettoyer les documents infectés*** - activer/désactiver la réparation automatique des documents infectés (dans la mesure du possible)
- ***Durée du délai d'expiration*** (*en secondes*) - la valeur maximale en secondes de la durée de la procédure d'analyse des virus après chaque lancement (diminuez cette valeur lorsque le serveur devient relativement lent lors de l'analyse de documents)
- ***Nombre de threads*** - vous pouvez spécifier le nombre de threads d'analyse de virus qui peuvent s'exécuter simultanément ; l'augmentation de ce nombre peut entraîner une accélération de l'analyse du fait du niveau de parallélisme qui est plus élevé, mais elle peut en outre accroître le temps de réaction du serveur

10.3. Configuration d'AVG pour SPPS - Sharepoint 2003

Dans l'interface de l'***Administration centrale de Sharepoint Portal Server***, vous pouvez facilement configurer les paramètres de performance et les tâches du scanner **AVG pour SharePoint Portal Server**. Choisissez l'option ***Configuration des tâches de l'anti-virus*** dans la section ***Configuration de la sécurité***



La fenêtre suivante va s'afficher :



Vous pouvez, à partir d'ici, configurer différentes tâches d'analyse pour **AVG pour SharePoint Portal Server** ainsi que les caractéristiques de performance :

- ***Analyser les documents lors du chargement***– activer/désactiver l'analyse des documents qui sont en train d'être chargés
- ***Analyser les documents lors du téléchargement*** – activer/désactiver l'analyse des documents qui sont en train d'être téléchargés

- ***Autoriser les utilisateurs à télécharger des documents infectés*** – autoriser/empêcher le téléchargement de documents infectés par les utilisateurs

- ***Essayer de nettoyer les documents infectés*** - activer/désactiver la réparation automatique des documents infectés (dans la mesure du possible)

- ***Durée maximale de l'analyse*** – valeur maximale, exprimée en secondes, de la procédure d'analyse des virus après chaque lancement (*diminuez la valeur si le serveur devient relativement lent lors de l'analyse des documents*)

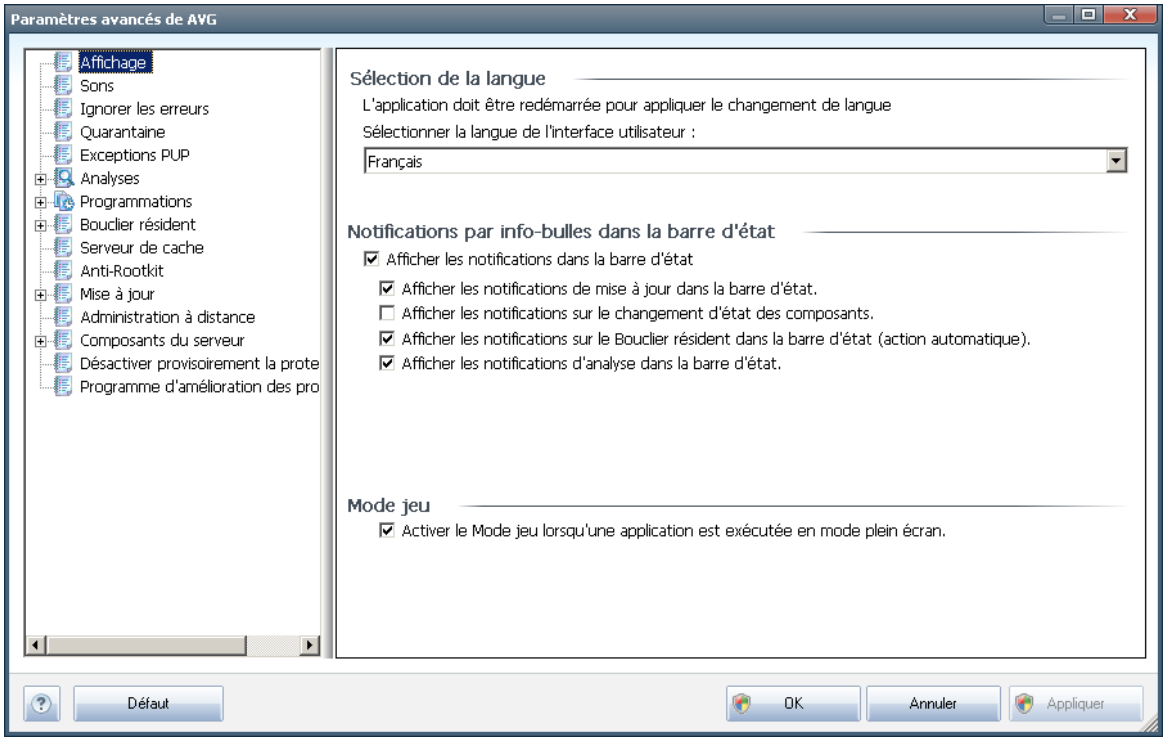
- ***Utiliser au maximum X sous-processus lors de l'analyse de documents*** – Le nombre X désigne le nombre de threads d'analyse des virus qui peuvent s'exécuter simultanément ; l'augmentation de ce nombre peut entraîner une accélération de l'analyse, du fait du niveau de parallélisme qui est plus élevé, mais elle peut aussi accroître le délai de réaction du serveur

11. Paramètres avancés d'AVG

La boîte de dialogue de configuration avancée d'**AVG 2011 Edition Serveur de Fichiers** a pour effet d'ouvrir une nouvelle fenêtre intitulée ***Paramètres avancés d'AVG***. Cette fenêtre se compose de deux parties : la partie gauche présente une arborescence qui permet d'accéder aux options de configuration du programme. Sélectionnez le composant dont vous voulez modifier la configuration (*ou celle d'une partie spécifique*) pour ouvrir la boîte de dialogue correspondante dans la partie droite de la fenêtre.

11.1. Affichage

Le premier élément de l'arborescence de navigation, ***Affichage***, porte sur les paramètres généraux de l'interface utilisateur AVG et sur des options élémentaires du comportement de l'application :



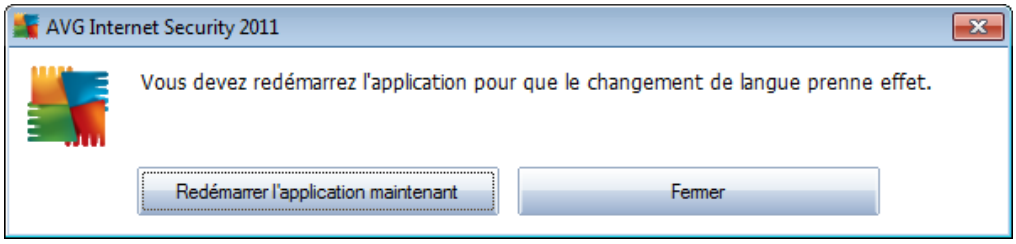
Sélection de la langue

La section ***Sélection de la langue*** permet de choisir dans le menu déroulant la langue qui sera utilisée dans l'ensemble de l'interface utilisateur AVG. Le menu déroulant ne propose que les langues que vous avez sélectionnées au cours du processus d'installation (*voir chapitre Options personnalisées*) en plus de l'anglais (*langue installée par défaut*). Pour que le changement de langue prenne effet, vous devez redémarrer l'interface utilisateur comme suit :

- Sélectionnez une langue, puis confirmez votre choix en cliquant sur le bouton

Appliquer (angle inférieur droit)

- Cliquez sur le bouton***OK*** pour confirmer
- Une nouvelle boîte de dialogue s'affiche indiquant que l'application doit être redémarrée pour que le changement de langue de l'interface utilisateur AVG soit effectif.



Notifications par info-bulles dans la barre d'état

Dans cette section, vous pouvez désactiver l'affichage des info-bulles concernant l'état de l'application. Par défaut, les notifications s'affichent et il est recommandé de conserver cette configuration. Les info-bulles signalent généralement des changements d'état de composants AVG à prendre en considération.

Si toutefois, pour une raison particulière, vous souhaitez ne pas afficher ces notifications ou en afficher seulement quelques-unes (les notifications liées à un composant déterminé d'AVG, par exemple), vous pouvez indiquer vos préférences en cochant/désélectionnant les options suivantes :

- ***Afficher les notifications dans la barre d'état système*** - par défaut, activée *(cochée)* ; les notifications s'affichent. Désélectionnez cette option pour désactiver l'affichage de toutes les notifications par info-bulles. Lorsqu'elle est active, vous pouvez sélectionner les notifications qui doivent s'afficher :
  - ***Afficher les notifications de mise à jour*** dans la barre d'état - indiquez s'il faut afficher les informations sur le lancement de la mise à jour AVG, la progression et la fin du processus ;
  - ***Afficher les notifications sur le changement d'état des composants*** - indiquez s'il faut afficher des informations sur l'activité/ arrêt d'activité des composants ou les problèmes éventuels. Lorsque cette option signale une anomalie d'un composant, elle remplit la même fonction d'information que l'icône dans la barre d'état système (changement de couleur) indiquant un problème lié à un composant AVG.
  - ***Afficher les notifications sur le Bouclier résident dans la barre d'état (action automatique)*** - indiquez s'il faut afficher ou supprimer les informations sur les processus d'enregistrement, de copie et d'ouverture de fichier (*cette configuration est applicable seulement si l'option*

Réparer automatiquement du Bouclier résident est activée).

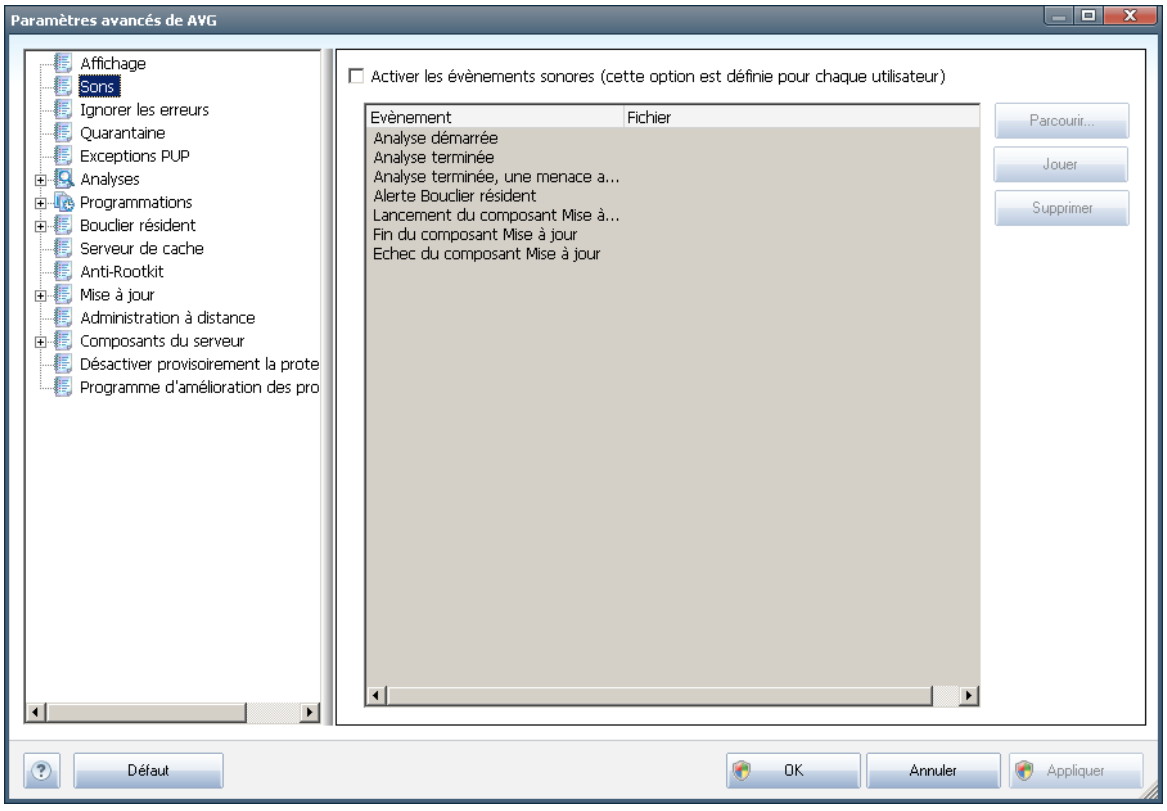
- ***Afficher les notifications d'analyse*** dans la barre d'état - indiquez s'il faut afficher les informations sur le lancement automatique de l'analyse programmée, sa progression et ses résultats.

Mode jeu

Cette fonction est conçue pour des applications plein écran pour lesquelles les éventuelles notifications d'information AVG (*qui s'affichent après le démarrage d'une analyse programmée*) seraient perturbantes (*elles risquent de réduire l'application ou de corrompre les images*). Pour éviter ce type de problème, il est recommandé de cocher la case ***Activer le mode jeu lorsqu'une application est exécutée en mode plein écran*** (*paramètre par défaut*).

11.2. Sons

Dans la boîte de dialogue ***Sons*** vous pouvez spécifier si vous désirez être informé des actions spécifiques d'AVG, par des sons. Si c'est le cas, cochez l'option***Activer les évènements sonores*** (*désactivée par défaut*) pour activer la liste des actions AVG.



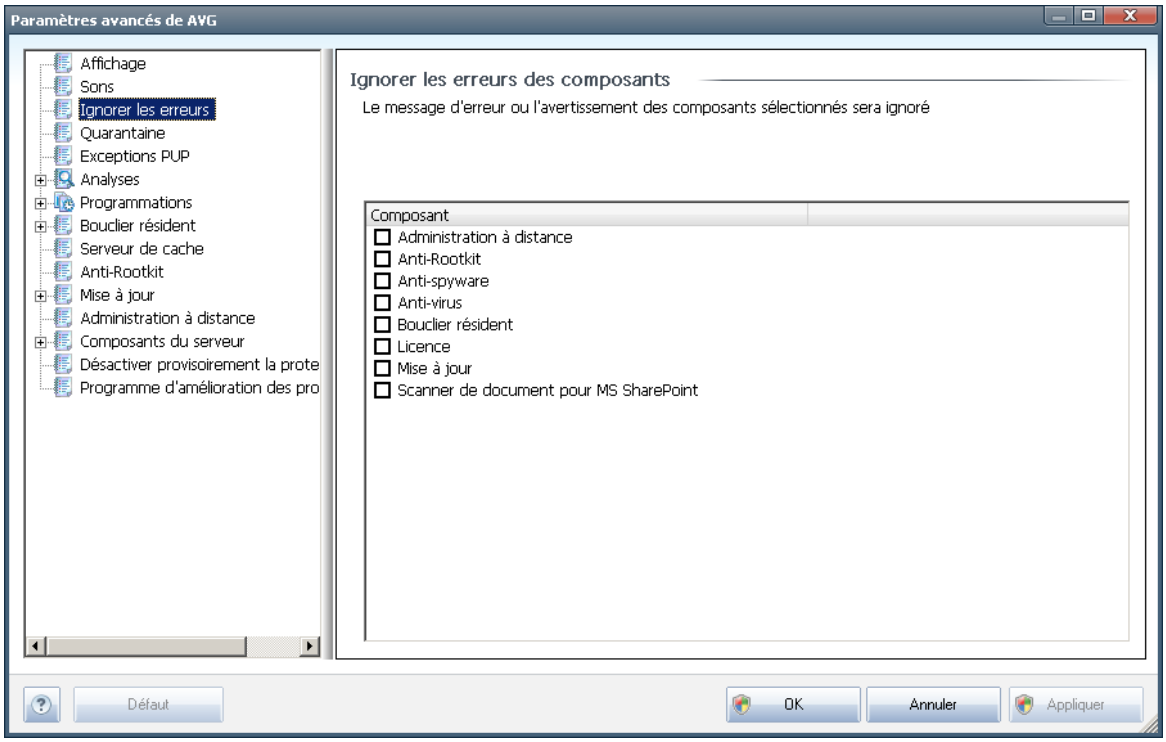
Ainsi, sélectionnez l'évènement correspondant à partir de la liste et recherchez (***Parcourir***) un son approprié que vous souhaitez affecter à cet évènement. Pour écouter le son sélectionné, mettez en surbrillance l'évènement dans la liste et cliquez

sur le bouton ***Jouer***. Utilisez le bouton ***Supprimer*** pour supprimer le son affecté à cet évènement spécifique.

Remarque : *Seuls les sons *.wav sont pris en charge!*

11.3. Ignorer les erreurs

Dans la boîte de dialogue ***Ignorer les erreurs des composants***, vous pouvez cocher les composants dont vous ne souhaitez pas connaître l'état :



Par défaut, aucun composant n'est sélectionné dans cette liste. Dans ce cas, si l'état d'un des composants est incorrect, vous en serez immédiatement informé par le biais des éléments suivants :

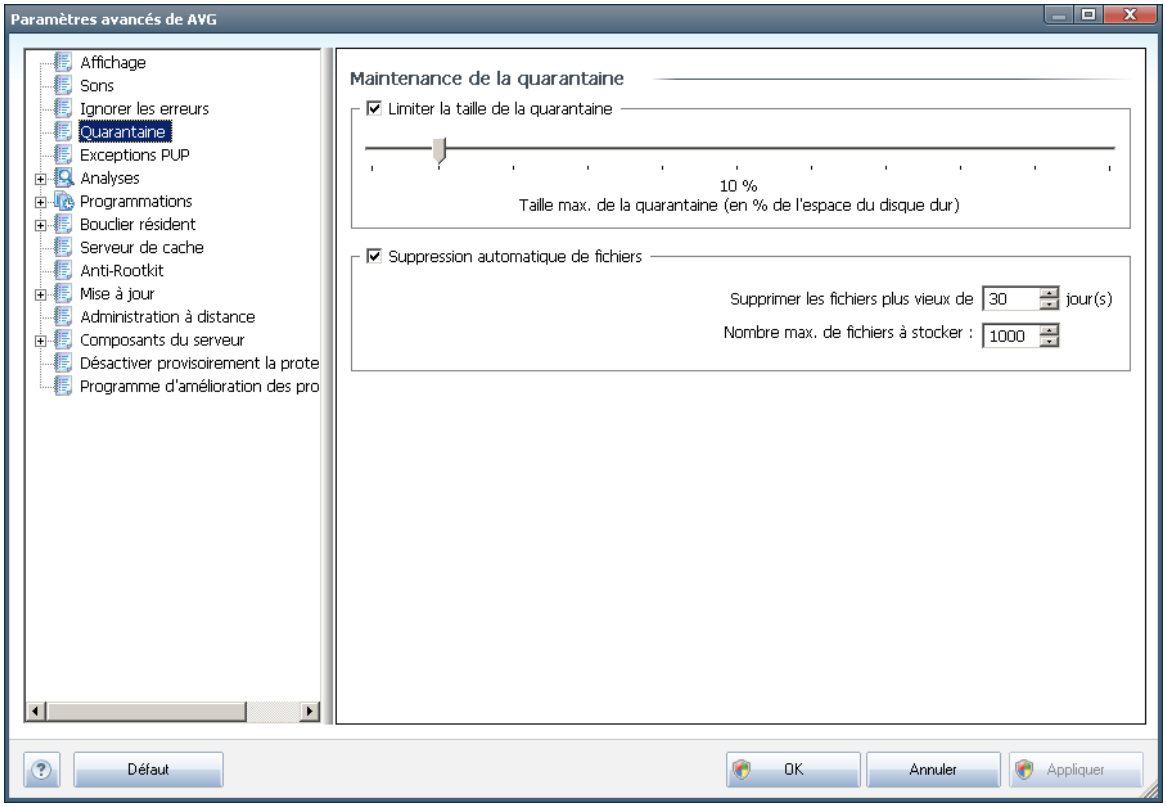
- ***icône de la barre d'état système*** - si tous les composants d'AVG fonctionnent correctement, l'icône apparaît en quatre couleurs ; cependant, si une erreur se produit l'icône apparaît avec un point d'exclamation de couleur jaune,
- Description du problème existant dans la section relative à l'***état de sécurité*** de la fenêtre principale d'AVG.

Il peut arriver que pour une raison particulière, vous soyez amené·à désactiver provisoirement un composant (*cela n'est pas recommandé ; vous devez toujours veiller à maintenir les composants activés et appliquer la configuration par défaut*). Dans ce cas, l'icône dans la barre d'état système signale automatiquement une erreur au niveau du composant. Toutefois, il est impropre de parler d'erreur alors que vous

avez délibérément provoqué la situation à l'origine du problème et que vous êtes conscient du risque potentiel. Parallèlement, dès qu'elle apparaît en couleurs pastels, l'icône ne peut plus signaler toute autre erreur susceptible d'apparaître par la suite.

Aussi, dans la boîte de dialogue ci-dessus, sélectionnez les composants qui risquent de présenter une erreur (*composants désactivés*) dont vous voulez ignorer l'état. Une option similaire, ***Ignorer l'état du composant***, est également disponible pour certains composants depuis la vue générale des composants figurant dans la fenêtre principale d'AVG.

11.4. Quarantaine

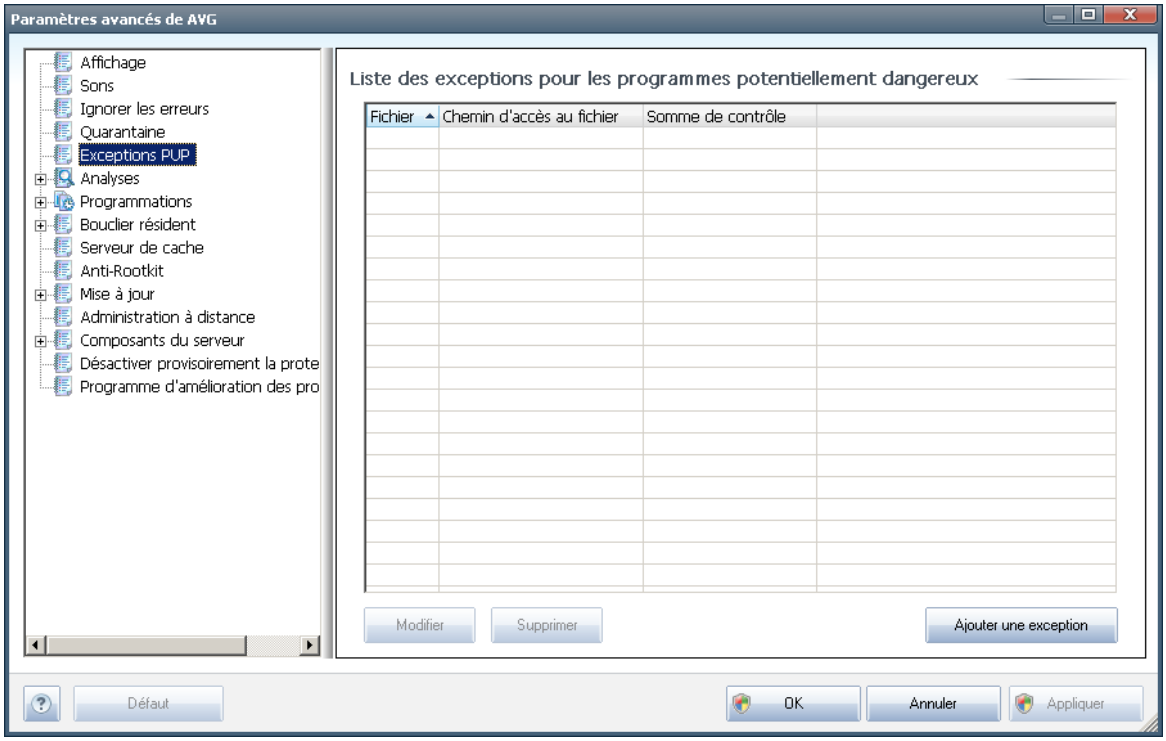


La boîte de dialogue ***Maintenance de la quarantaine*** permet de définir plusieurs paramètres liés à l'administration des objets stockés dans le module ***Quarantaine*** :

- ***Limiter la taille de la quarantaine*** - utilisez le curseur pour ajuster la taille de la ***quarantaine***. La taille est indiquée par rapport à la taille de votre disque local.
- ***Suppression automatique de fichiers*** - dans cette section, définissez la durée maximale de conservation des objets en ***quarantaine*** (***Supprimer les fichiers plus vieux de ... jours***) ainsi que le nombre maximal de fichiers à conserver en ***quarantaine*** (***Nombre max. de fichiers à stocker***)

11.5. Exceptions PUP

AVG 2011 Edition Serveur de Fichiers est en mesure d'analyser et de détecter des exécutables ou bibliothèques DLL qui peuvent s'avérer malveillants envers le système. Dans certains cas, il est possible que l'utilisateur souhaite conserver certains programmes considérés comme potentiellement dangereux sur l'ordinateur (*ceux installés volontairement, par exemple*). Certains programmes, et notamment ceux fournis gratuitement, font partie de la famille des adwares. Or, ce type de programme peut être signalé par AVG comme un ***programme potentiellement dangereux***. Si vous souhaitez malgré tout le conserver sur votre ordinateur, il suffit de le définir comme une exception de programme potentiellement dangereux :

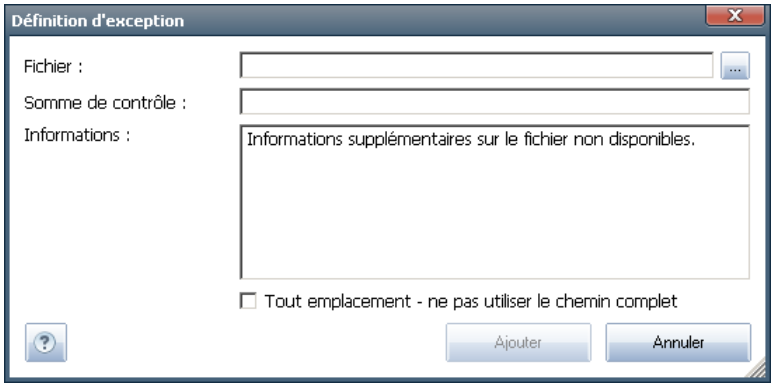


La boîte de dialogue ***Liste des exceptions pour les programmes potentiellement dangereux*** dresse la liste des exceptions déjà définies et actuellement valides par rapport aux programmes indésirables. Vous pouvez modifier la liste, supprimer des éléments existants ou ajouter une nouvelle exception. Vous trouverez les informations suivantes dans la liste de chaque exception :

- ***Fichier*** - indique le nom de l'application correspondante
- ***Chemin d'accès au fichier*** - indique le chemin d'accès à l'emplacement de l'application
- ***Somme de contrôle*** - affiche la signature unique du fichier choisi. Il s'agit d'une chaîne de caractères générée automatiquement, qui permet à AVG de distinguer sans risque d'erreur ce fichier parmi tous les autres. La somme de contrôle est générée et affichée une fois le fichier ajouté.

Boutons de commande

- ***Modifier*** - ouvre une boîte de dialogue d'édition (*identique à la boîte de dialogue permettant de définir une nouvelle exception, voir ci-dessus*) d'une exception déjà définie dans laquelle vous modifiez les paramètres de l'exception
- ***Supprimer*** - supprime l'élément sélectionné de la liste des exceptions
- ***Ajouter une exception*** - ouvre une boîte de dialogue dans laquelle vous définissez les paramètres de l'exception à créer :



  - ***Fichier*** - spécifiez le chemin d'accès complet du fichier à identifier comme étant une exception
  - ***Somme de contrôle*** - affiche la "signature" unique du fichier choisi. Il s'agit d'une chaîne de caractères générée automatiquement, qui permet à AVG de distinguer sans risque d'erreur ce fichier parmi tous les autres. La somme de contrôle est générée et affichée une fois le fichier ajouté.
  - ***Informations*** - affiche des informations supplémentaires sur le fichier (*licence, version, etc.*)
  - ***Tout emplacement - ne pas utiliser le chemin complet*** - si vous souhaitez définir ce fichier comme une exception uniquement pour un emplacement spécifique, veillez à ne pas cocher cette case. Si la case est cochée, le fichier mentionné est défini en tant qu'exception indifféremment de son emplacement (*vous devez malgré tout indiquer le chemin d'accès complet du fichier ; le fichier servira alors d'exemple unique au cas où deux fichiers portant le même nom existent dans le système*).

11.6. Analyses

Les paramètres d'analyse avancés sont répartis en quatre catégories selon le type d'analyse spécifique tel qu'il a été défini par l'éditeur du logiciel :

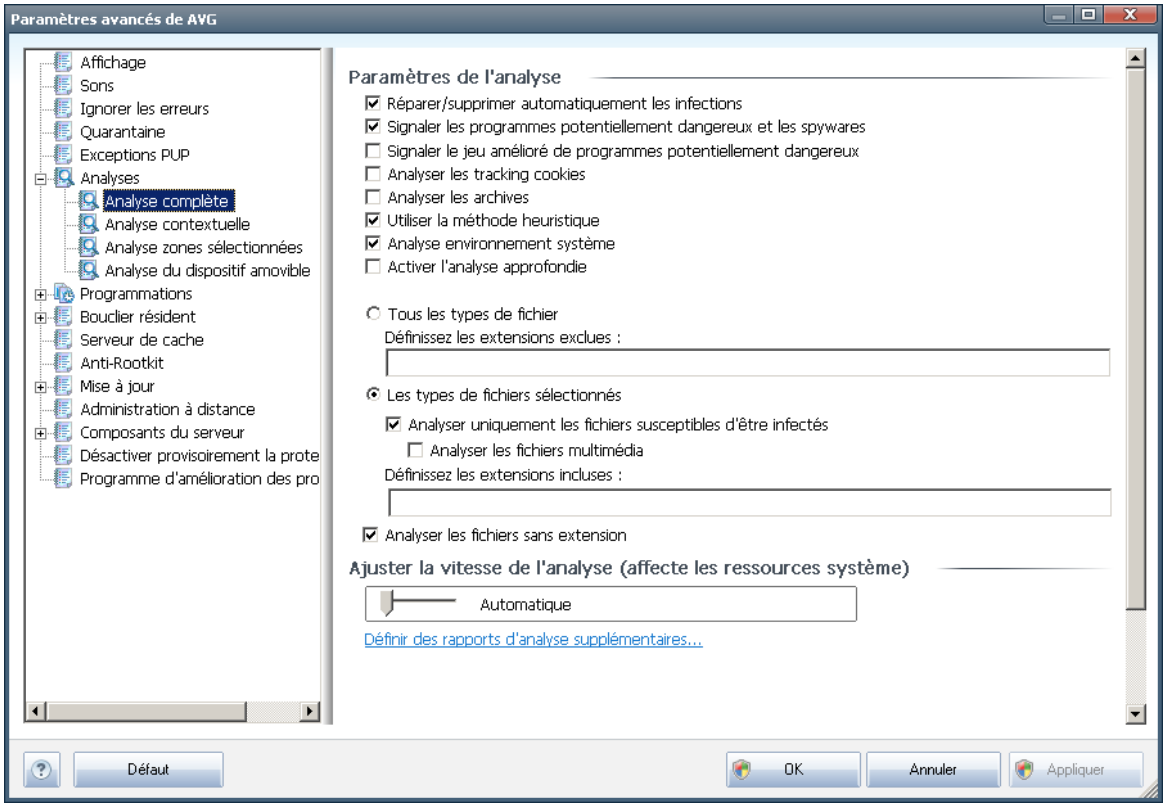
- ***Analyse complète*** - analyse standard prédéfinie appliquée à l'ensemble des

fichiers contenus dans l'ordinateur

- ***Analyse contextuelle*** : analyse spécifique d'un objet directement sélectionné dans l'environnement de l'Explorateur Windows
- ***Analyse zones sélectionnées*** - analyse standard prédéfinie appliquée aux zones spécifiées de l'ordinateur
- ***Analyse du dispositif amovible*** : analyse spécifique des périphériques amovibles connectés à votre ordinateur

11.6.1. Analyse complète

L'option ***Analyse complète*** permet de modifier les paramètres d'une analyse prédéfinie par l'éditeur du logiciel, ***Analyse de la totalité de l'ordinateur*** :



Paramètres de l'analyse

La section ***Paramètres de l'analyse*** présente la liste de paramètres d'analyse susceptibles d'être activés ou désactivés :

- ***Réparer/supprimer automatiquement les infections*** (*option activée par défaut*) : lorsqu'un virus est détecté au cours de l'analyse, il est réparé automatiquement dans la mesure du possible. S'il est impossible de réparer

automatiquement le fichier infecté, il sera placé en ***quarantaine***.

- ***Signaler les programmes potentiellement dangereux et les spywares*** (*activé par défaut*) : cochez cette case pour activer le moteur ***Anti-spyware*** et rechercher les spywares et les virus. Les spywares désignent une catégorie de codes suspects : même s'ils représentent généralement un risque pour la sécurité, certains de ces programmes peuvent être installés intentionnellement par l'utilisateur. Nous vous recommandons de laisser cette fonction activée car elle augmente de manière significative la sécurité de votre système.

- ***Signaler le jeu amélioré de programmes potentiellement dangereux*** *(option désactivée par défaut*) : permet de détecter le jeu étendu des spywares*** qui ne posent aucun problème et sont sans danger dès lors qu'ils sont achetés directement auprès de leur éditeur, mais qui peuvent ensuite être utilisées à des fins malveillantes. Il s'agit d'une mesure de sécurité supplémentaire. Cependant, elle peut bloquer des programmes légitimes de l'ordinateur ; c'est pourquoi elle est désactivée par défaut.

- ***Analyser les tracking cookies*** (*option désactivée par défaut*) : ce paramètre du composant Anti-Spyware définit les cookies qui pourront être détectés au cours de l'analyse (*les cookies HTTP servent à authentifier, à suivre et à gérer certaines informations sur les utilisateurs comme leurs préférences en matière de navigation ou le contenu de leur panier d'achat électronique*).

- ***Analyser les archives*** (*option désactivée par défaut*) : ce paramètre indique que l'analyse examine tous les fichiers même ceux stockés dans des archives (archives ZIP, RAR, par exemple).

- ***Utiliser la méthode heuristique*** (*option activée par défaut*) : l'analyse heuristique (*émulation dynamique des instructions de l'objet analysé dans un environnement informatique virtuel*) est l'une des méthodes employées pour détecter des virus pendant l'analyse.

- ***Analyse environnement système*** (*option activée par défaut*) : l'analyse vérifie les fichiers système de l'ordinateur.

- ***Activer l'analyse approfondie*** (*option désactivée par défaut*) - dans certains cas (*suspicion d'une infection de l'ordinateur*), vous pouvez cocher cette option pour exécuter des algorithmes d'analyse très pointus même s'il est peu probable que certaines zones de l'ordinateur soient infectées. Gardez à l'esprit que cette méthode prend énormément de temps.

Ensuite, vous pouvez choisir d'analyser

- ***Tous les types de fichier*** avec la possibilité de définir les éléments à exclure de l'analyse en répertoriant les extensions de fichiers séparées par des virgules (*après enregistrement de la liste, les virgules sont remplacées par des points-virgules*) à ne pas analyser ; ou les

- ***Les types de fichiers sélectionnés*** - vous pouvez choisir d'analyser uniquement les fichiers susceptibles d'être infectés (*les fichiers qui ne peuvent faire l'objet d'une infection ne sont pas analysés ; il s'agit par exemple de fichiers en texte brut ou de certains types de fichier non exécutables*), y compris les fichiers multimédia (*vidéo, audio - si vous ne sélectionnez pas cette option, la durée de l'analyse sera considérablement réduite, car ce sont souvent de gros fichiers qui sont rarement infectés par un virus*). En fonction des extensions, vous pouvez également spécifier les fichiers qui doivent toujours faire l'objet d'une analyse.

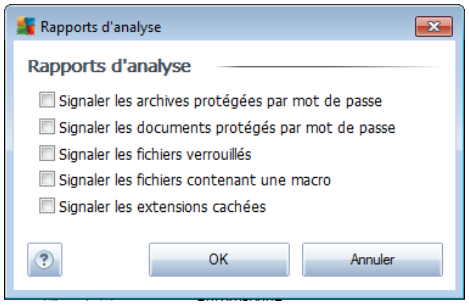
- Vous pouvez également choisir l'option ***Analyser les fichiers sans extension*** - cette option est activée par défaut et il est recommandé de la conserver et de ne la modifier qu'en cas d'absolue nécessité. Les fichiers sans extension sont relativement suspects et doivent toujours faire l'objet d'une analyse.

Ajuster la vitesse de l'analyse

Dans la section ***Ajuster la vitesse de l'analyse***, il est possible de régler la vitesse d'analyse en fonction des ressources système. Par défaut, cette option est réglée sur le niveau automatique d'utilisation des ressources. Cette configuration permet d'accélérer l'analyse : elle réduit la durée de l'analyse, mais sollicite fortement les ressources système et ralentit considérablement les autres activités de l'ordinateur (*cette option convient lorsque l'ordinateur est allumé, mais que personne n'y travaille*). Inversement, vous pouvez réduire l'utilisation des ressources système en augmentant la durée de l'analyse.

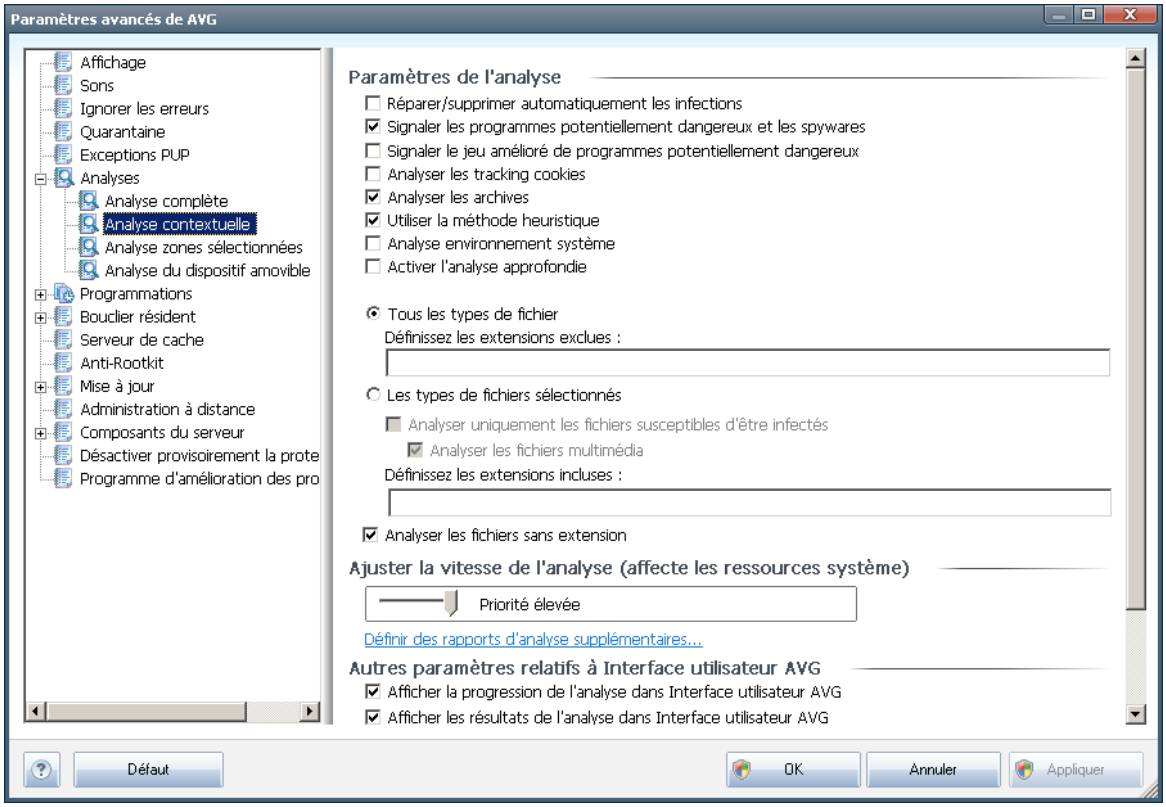
Définir des rapports d'analyse supplémentaires...

Cliquez sur le lien ***Définir des rapports d'analyse supplémentaires*** pour ouvrir la boîte de dialogue ***Rapports d'analyse*** dans laquelle vous pouvez sélectionner les types de résultats que vous souhaitez obtenir :



11.6.2. Analyse contextuelle

Similaire à l'option précédente ***Analyse complète***, l'option ***Analyse contextuelle*** propose plusieurs options permettant d'adapter les analyses prédéfinies par le fournisseur du logiciel. La configuration actuelle s'applique à l'analyse d'objets spécifiques exécutée directement dans l'Explorateur Windows (*extension des menus*), voir le chapitre ***Analyse dans l'Explorateur Windows*** :



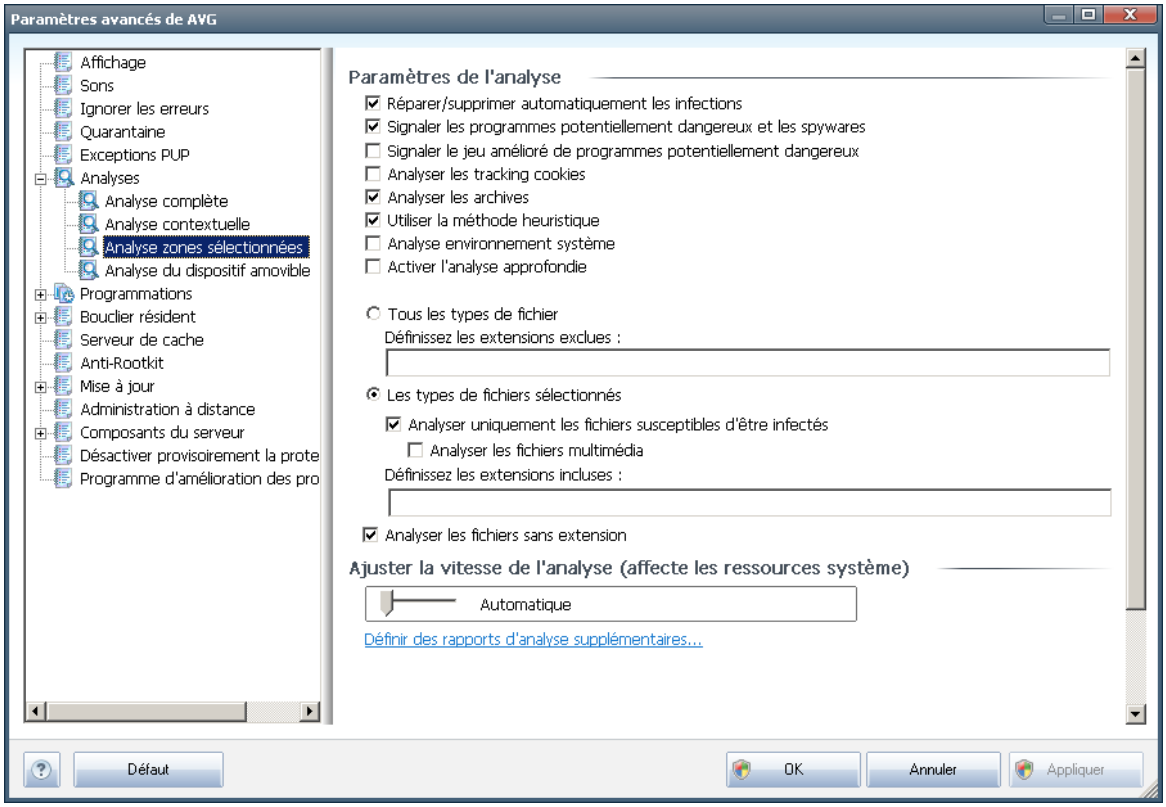
La liste des paramètres correspond à celle proposée pour l'***analyse complète***. Cependant, les paramètres par défaut diffèrent (*par exemple, l'analyse complète par défaut ne vérifie pas les archives, mais analyse l'environnement système à l'inverse de l'analyse contextuelle*).

Remarque : *pour obtenir la description des paramètres qui vous intéressent, consultez le chapitre* ***Paramètres avancés d'AVG / Analyses / Analyse complète****.*

Comme la boîte de dialogue ***Analyse complète*** , celle de l'***analyse contextuelle*** inclut la section ***Autres paramètres relatifs à l'interface utilisateur AVG***, dans laquelle vous indiquez si vous voulez que la progression de l'analyse et ses résultats soient accessibles à partir de l'interface utilisateur AVG. Vous pouvez aussi définir que les résultats d'analyse n'apparaissent qu'en cas d'infection détectée.

11.6.3. Analyse zones sélectionnées

L'interface d'édition de l'***analyse zones sélectionnées*** est identique à celle de l'***analyse complète***. Les options de configuration sont les mêmes, à ceci près que les paramètres par défaut sont plus stricts pour l'***analyse complète***.

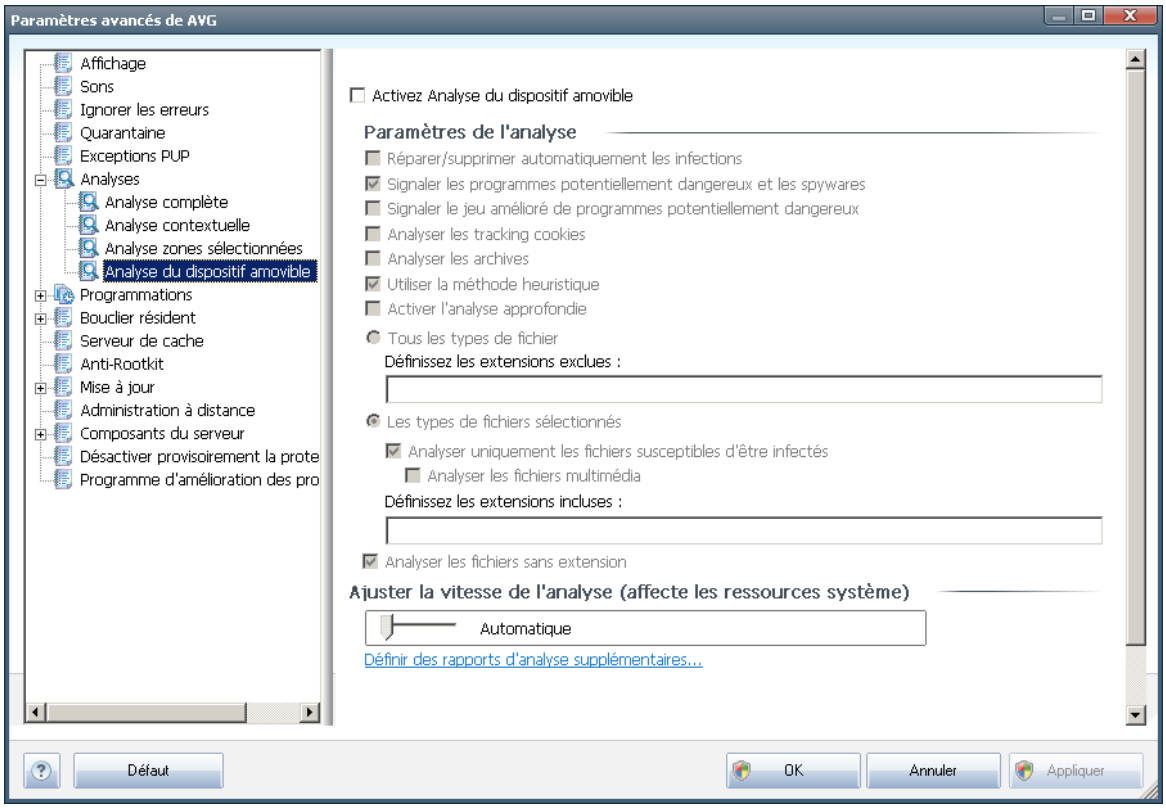


Tous les paramètres définis dans cette boîte de dialogue de configuration s'appliquent uniquement aux zones sélectionnées pour analyse dans le cadre de l'option ***Analyse zones sélectionnées***.

Remarque : *pour obtenir la description des paramètres qui vous intéressent, consultez le chapitre* ***Paramètres avancés d'AVG / Analyses / Analyse complète***.

11.6.4. Analyse du dispositif amovible

L'interface de configuration de l'***analyse du dispositif amovible*** ressemble beaucoup à celle intitulée ***Analyse complète*** :



L'***Analyse des périphériques amovibles*** est lancée automatiquement chaque fois que vous connectez un périphérique amovible à l'ordinateur. Par défaut, cette fonctionnalité est désactivée. Cependant, il est primordial d'analyser les périphériques amovibles, car ils constituent l'une des sources d'infection majeurs. Pour que cette analyse soit activée et s'effectue automatiquement en cas de besoin, cochez la case ***Activer l'analyse des périphériques amovibles***.

Remarque : *pour obtenir la description des paramètres qui vous intéressent, consultez le chapitre* ***Paramètres avancés d'AVG / Analyses / Analyser complète***.

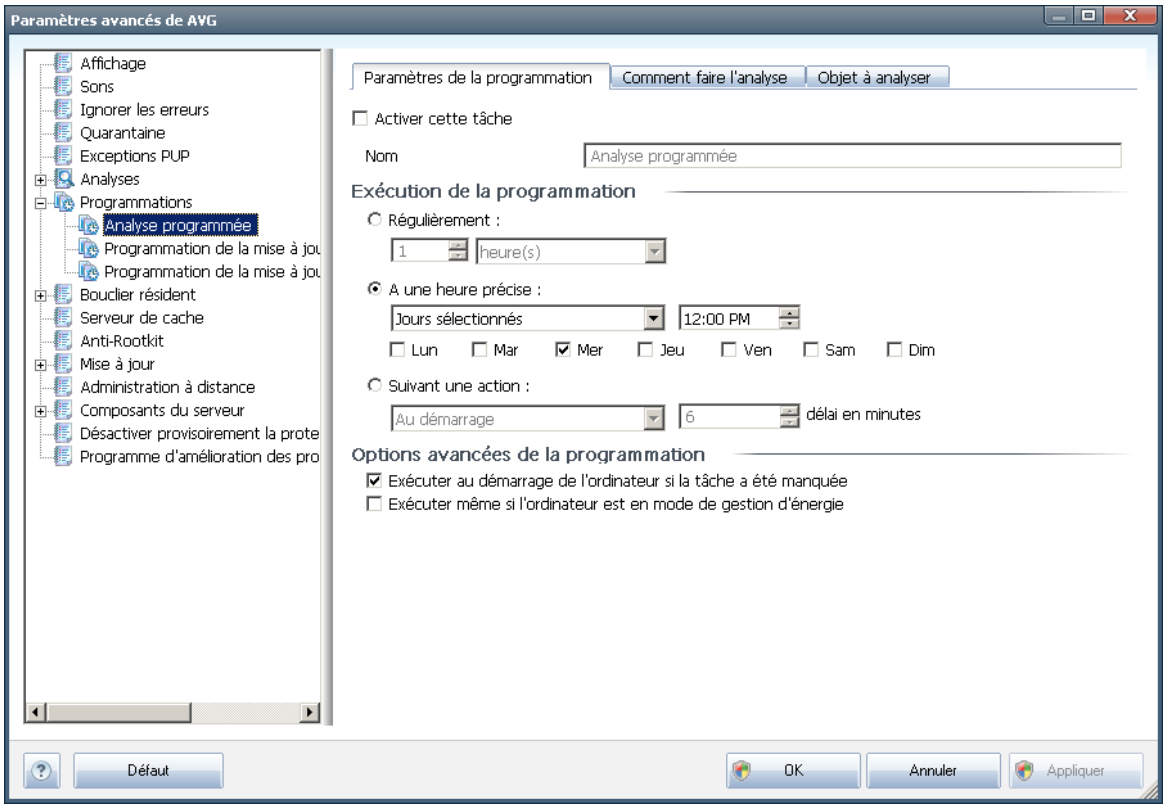
11.7. Programmations

Dans l'entrée ***Programmations***, vous êtes libre de modifier les paramètres par défaut des éléments suivants :

- Analyse programmée
- Programmation de la mise à jour de la base de données virale
- Programmation de la mise à jour du programme

11.7.1. Analyse programmée

Les paramètres de l'analyse programmée peuvent être modifiés (*ou une nouvelle analyse peut être programmée*) depuis les trois onglets :



Dans l'onglet ***Paramètres de la programmation***, vous pouvez cocher/désélectionner la case ***Activer cette tâche*** pour désactiver temporairement l'analyse programmée et le réactiver au moment opportun.

Dans la zone de texte ***Nom*** (*option désactivée pour toutes les programmations par défaut*), le nom est attribué à cette programmation par le fournisseur du programme. Pour les programmations nouvellement ajoutées (*vous pouvez ajouter une nouvelle programmation en cliquant avec le bouton droit de la souris sur l'élément* ***Programmation de l'analyse*** *situé à gauche de l'arborescence de navigation*), vous pouvez spécifier votre propre nom. Dans ce cas, la zone de texte est ouverte et vous pouvez y apporter des modifications. Veillez à utiliser toujours des noms courts, descriptifs et appropriés pour distinguer facilement les différentes analyses par la suite.

Exemple : *il n'est pas judicieux d'appeler l'analyse "Nouvelle analyse" ou "Mon analyse", car ces noms ne font pas référence au champ réel de l'analyse. A l'inverse, "Analyse des zones système" est un nom descriptif précis. Il est également nécessaire de spécifier dans le nom de l'analyse si l'analyse concerne l'ensemble de l'ordinateur ou une sélection de fichiers ou de dossiers. Notez que les analyses*

personnalisées sont toujours basées sur l'Analyse zones sélectionnés.

Dans cette boîte de dialogue, vous définissez plus précisément les paramètres de l'analyse :

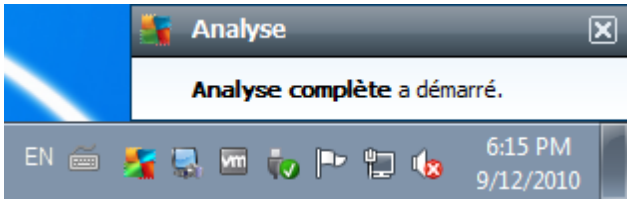
Exécution de la programmation

Ici, spécifiez l'intervalle entre chaque exécution de la nouvelle analyse. Il est possible de répéter le lancement de l'analyse après un laps de temps donné (***Régulièrement***), d'en définir la date et l'heure précises (***A une heure précise***) ou encore de définir l'évènement auquel sera associé lancement de l'analyse (***Suivant une action***).

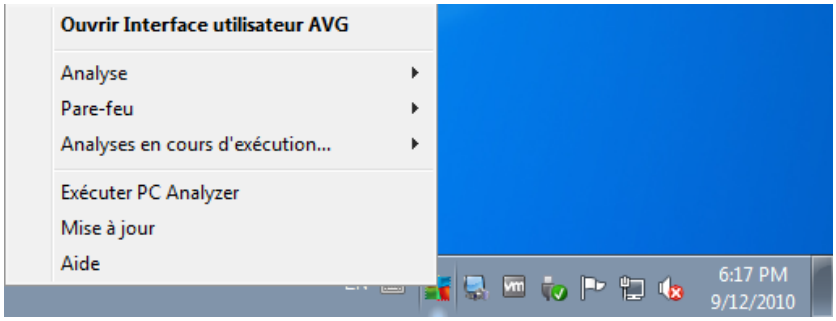
Options avancées de la programmation

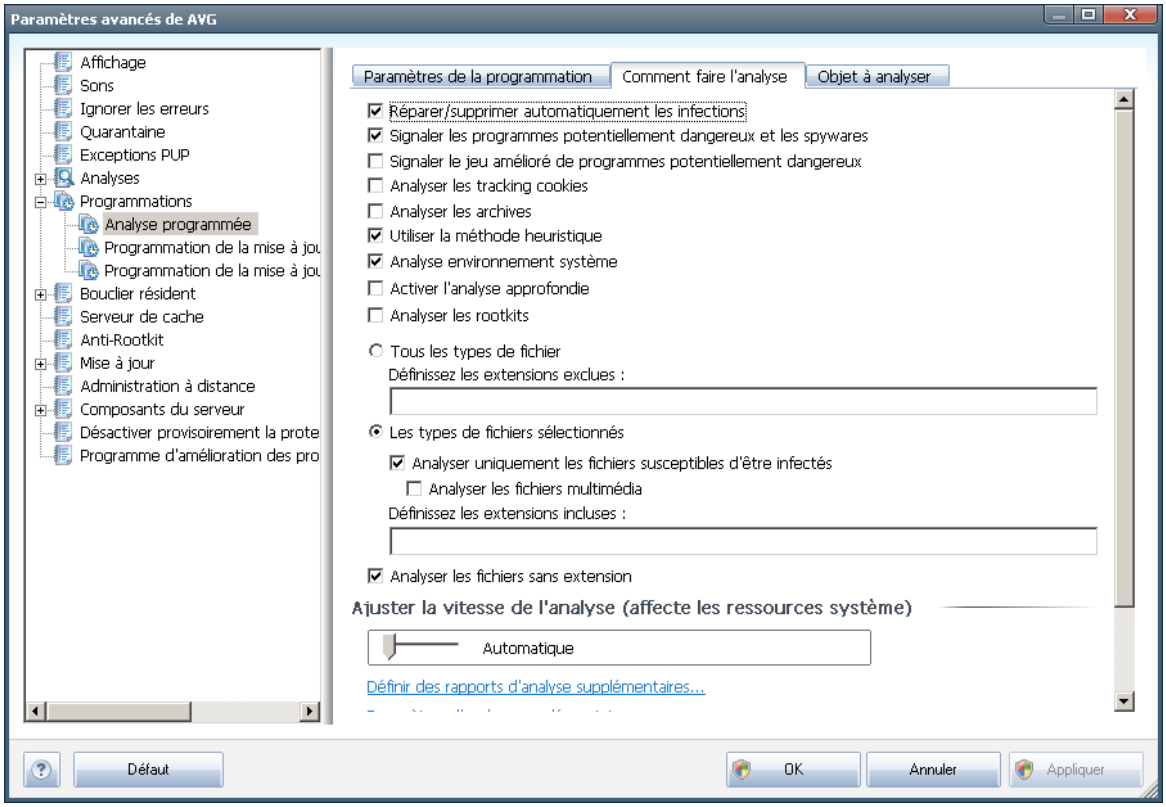
Cette section permet de définir dans quelles conditions l'analyse doit ou ne doit pas être exécutée si l'ordinateur est en mode d'économie d'énergie ou hors tension.

Lorsque l'analyse programmée est exécutée à l'heure spécifiée, une fenêtre vous en informe par le biais d'une note contextuelle de l'icône dans la barre d'état système AVG :



Une nouvelle icône de la barre d'état système AVG s'affiche alors·(*en couleurs clignotantes*) et signale qu'une analyse programmée est en cours. Cliquez avec le bouton droit de la souris sur l'icône AVG de l'analyse en cours : un menu contextuel s'affiche dans lequel vous choisissez d'interrompre momentanément ou définitivement l'analyse et pouvez également modifier la priorité de l'analyse en cours d'exécution :





Dans l'onglet ***Comment faire l'analyse***, vous trouverez la liste des paramètres d'analyse qui peuvent être activés ou désactivés. Par défaut, la plupart des paramètres sont activés et appliqués lors de l'analyse. Il est vivement conseillé de ne pas modifier la configuration prédéfinie sans motif valable :

- ***Réparer/supprimer automatiquement les infections*** *(option activée par défaut) :* lorsqu'un virus est détecté au cours de l'analyse, il est réparé automatiquement dans la mesure du possible. S'il est impossible de réparer automatiquement le fichier infecté, il sera placé en ***quarantaine***.

- ***Signaler les programmes potentiellement dangereux et les spywares*** *(option activée par défaut) :* cochez cette case pour activer le moteur ***Anti-spyware*** et rechercher les spywares et les virus. Les spywares désignent une catégorie de codes suspects : même s'ils représentent généralement un risque pour la sécurité, certains de ces programmes peuvent être installés intentionnellement par l'utilisateur. Nous vous recommandons de laisser cette fonction activée car elle augmente de manière significative la sécurité de votre système.

- ***Signaler le jeu amélioré de programmes potentiellement dangereux*** *(option désactivée par défaut)* : permet de détecter le jeu étendu des spywares*** qui ne posent aucun problème et sont sans danger dès lors qu'ils sont achetés directement auprès de leur éditeur, mais qui peuvent ensuite être utilisées à des fins malveillantes. Il s'agit d'une mesure de sécurité

supplémentaire. Cependant, elle peut bloquer des programmes légitimes de l'ordinateur ; c'est pourquoi elle est désactivée par défaut.

- ***Analyser les tracking cookies*** (*option désactivée par défaut*) : ce paramètre du composant ***Anti-Spyware*** définit que les cookies devront être détectés au cours de l'analyse (*les cookies HTTP servent à authentifier, à suivre et à gérer certaines informations sur les utilisateurs comme leurs préférences en matière de navigation ou le contenu de leur panier d'achat électronique*).

- ***Analyser les archives*** (*option désactivée par défaut*) : ce paramètre indique que l'analyse examine tous les fichiers même ceux stockés dans des formats d'archives (archives ZIP, RAR, par exemple).

- ***Utiliser la méthode heuristique*** (*option activée par défaut*) : l'analyse heuristique (*émulation dynamique des instructions de l'objet analysé dans un environnement informatique virtuel*) est l'une des méthodes employées pour détecter des virus pendant l'analyse.

- ***Analyse environnement système*** (*option activée par défaut*) : l'analyse vérifie les fichiers système de l'ordinateur.

- ***Activer l'analyse approfondie*** (*option désactivée par défaut*) - dans certains cas (*suspicion d'une infection de l'ordinateur*), vous pouvez cocher cette option pour exécuter des algorithmes d'analyse très pointus même s'il est peu probable que certaines zones de l'ordinateur soient infectées. Gardez à l'esprit que cette méthode prend énormément de temps.

- ***Analyser les rootkits*** (*option désactivée par défaut*) : cochez cette option si vous souhaitez inclure la détection de rootkits dans l'analyse complète de l'ordinateur. La détection seule de rootkits est aussi proposée dans le composant ***Anti-Rootkit***.

Ensuite, vous pouvez choisir d'analyser

- ***Tous les types de fichier*** avec la possibilité de définir les éléments à exclure de l'analyse en répertoriant les extensions de fichiers séparées par des virgules (*après enregistrement de la liste, les virgules sont remplacées par des points-virgules*) à ne pas analyser ; ou les

- ***Types de fichiers sélectionnés*** - vous pouvez choisir d'analyser uniquement les fichiers susceptibles d'être infectés (*les fichiers qui ne peuvent faire l'objet d'une infection ne sont pas analysés ; il s'agit par exemple de fichiers en texte brut ou de certains types de fichier non exécutables*), y compris les fichiers multimédia (*vidéo, audio - si vous ne sélectionnez pas cette option, la durée de l'analyse sera considérablement réduite, car ce sont souvent de gros fichiers qui sont rarement infectés par un virus*). En fonction des extensions, vous pouvez également spécifier les fichiers qui doivent toujours faire l'objet d'une analyse.

- Vous pouvez également choisir l'option ***Analyser les fichiers sans extension*** - cette option est activée par défaut et il est recommandé de la conserver et

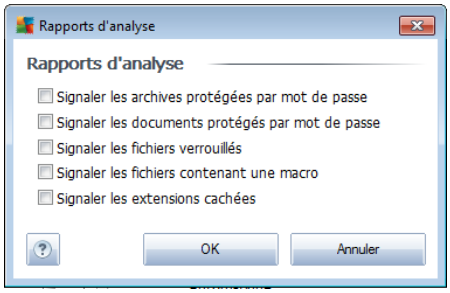
de ne la modifier qu'en cas d'absolue nécessité. Les fichiers sans extension sont relativement suspects et doivent toujours faire l'objet d'une analyse.

Ajuster la vitesse de l'analyse

Dans la section ***Ajuster la vitesse de l'analyse***, il est possible de régler la vitesse d'analyse en fonction des ressources système. Par défaut, cette option est réglée sur le niveau automatique d'utilisation des ressources. Cette configuration permet d'accélérer l'analyse : elle réduit la durée de l'analyse, mais sollicite fortement les ressources système et ralentit considérablement les autres activités de l'ordinateur (*cette option convient lorsque l'ordinateur est allumé, mais que personne n'y travaille*). Inversement, vous pouvez réduire l'utilisation des ressources système en augmentant la durée de l'analyse.

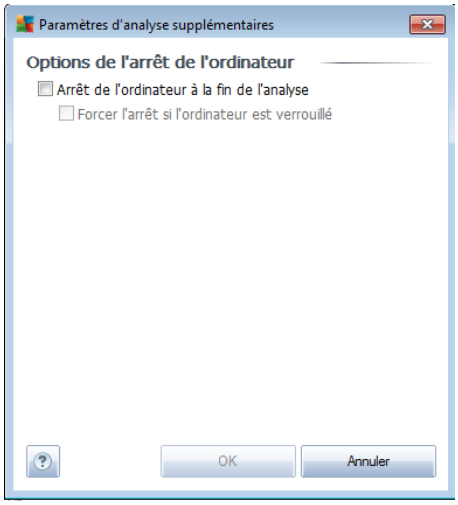
Définir des rapports d'analyse supplémentaires

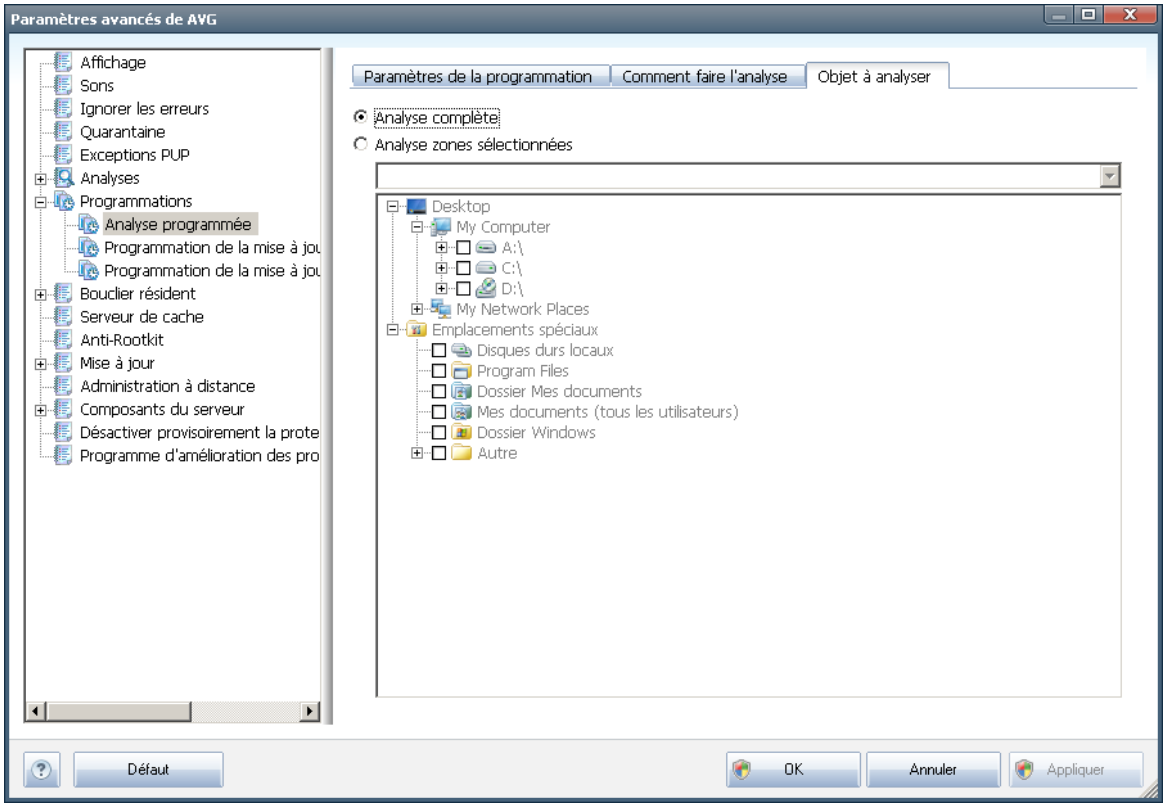
Cliquez sur le lien ***Définir des rapports d'analyse supplémentaires*** pour ouvrir la boîte de dialogue ***Rapports d'analyse*** dans laquelle vous pouvez sélectionner les types de résultats que vous souhaitez obtenir :



Paramètres d'analyse supplémentaires

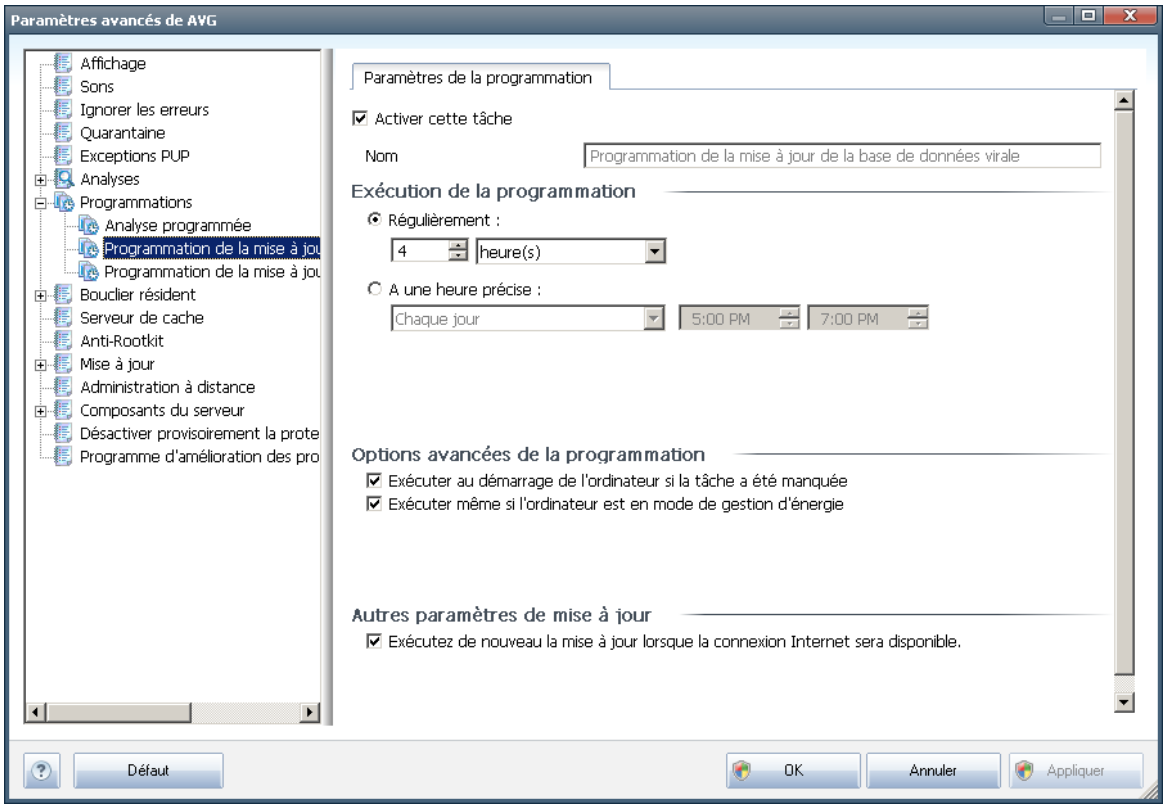
Cliquez sur ***Paramètres d'analyse supplémentaires*** pour ouvrir la boîte de dialogue ***Options de l'arrêt de l'ordinateur*** dans laquelle vous indiquez si l'ordinateur doit être arrêté automatiquement à la fin du processus d'analyse. Si l'option ***Arrêt de l'ordinateur à la fin de l'analyse*** est activée, l'option ***Forcer l'arrêt si l'ordinateur est verrouillé*** devient disponible et permet d'arrêter l'ordinateur même s'il est verrouillé.





Sous l'onglet ***Objet à analyser***, indiquez si vous voulez programmer l'analyse complète ou l'analyse des zones sélectionnées. Si vous optez pour la deuxième solution, la structure de l'arborescence affichée dans la partie inférieure de la boîte de dialogue devient active et permet de définir les dossiers qui vous intéressent.

11.7.2. Programmation de la mise à jour de la base de données virale



Dans l'onglet ***Paramètres de la programmation***, vous pouvez cocher/désélectionner la case ***Activer cette tâche*** pour désactiver temporairement la mise à jour programmée de la base virale et la réactiver au moment opportun. La programmation de la mise à jour de la base de données virale est assurée par le composant ***Mise à jour***. Dans la boîte de dialogue correspondante, vous spécifiez en détail la programmation de la mise à jour : Dans la zone de texte ***Nom*** (*désactivée pour toutes les programmations par défaut*), le nom est attribué à cette programmation par le fournisseur du programme.

Exécution de la programmation

Dans cette section, spécifiez la fréquence à laquelle la nouvelle mise à jour programmée de la base de données virale sera lancée. Il est possible de répéter le lancement de la mise à jour après un laps de temps donné (***Régulièrement***) ou d'en définir la date et l'heure précises (***A une heure précise***).

Options avancées de la programmation

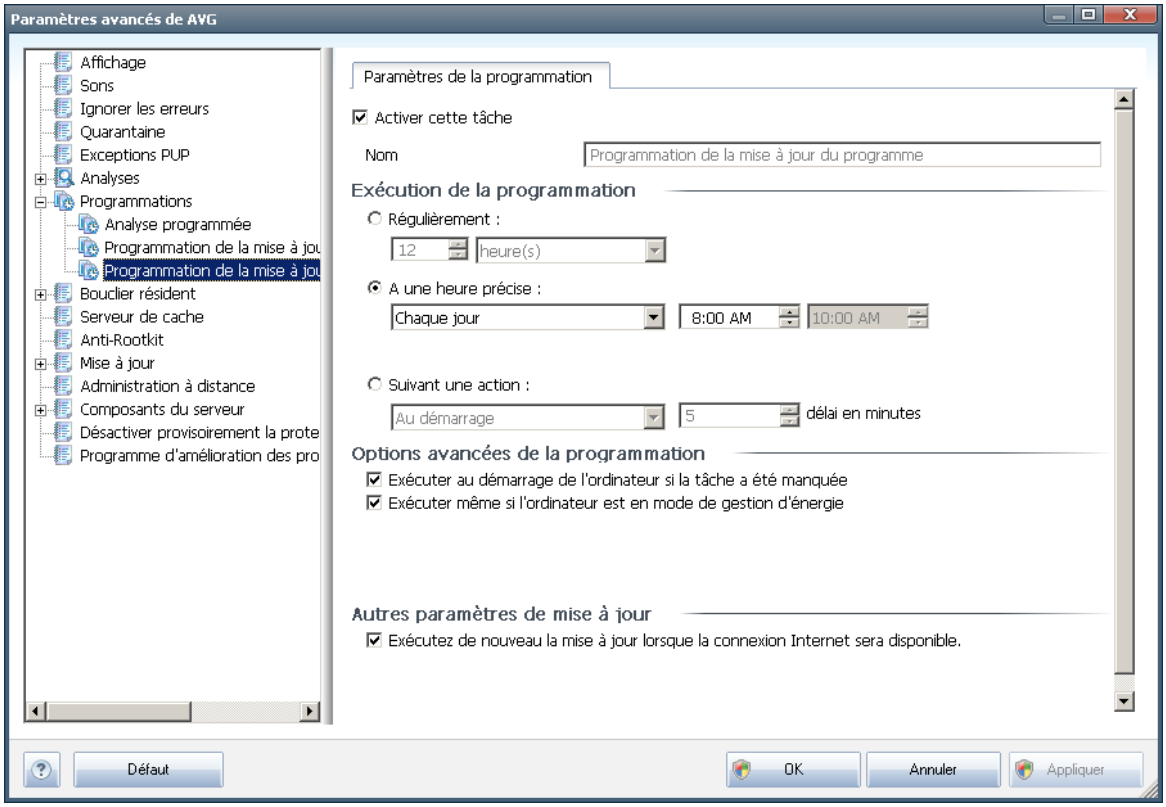
Cette section permet de définir dans quelles conditions la mise à jour de la base de données virale doit ou ne doit pas être exécutée si l'ordinateur est en mode d'économie d'énergie ou hors tension.

Autres paramètres de mise à jour

Enfin, cochez l'option ***Exécuter de nouveau la mise à jour lorsque la connexion Internet sera disponible*** pour vous assurer qu'en cas d'interruption de la connexion Internet et d'échec de la mise à jour, le processus est relancé dès le rétablissement de la connexion Internet.

Lorsque la mise à jour programmée est lancée à l'heure spécifiée, une fenêtre vous en informe par le biais d'une icône dans la barre d'état système AVG (*à condition que vous ayez conservé la configuration par défaut de la boîte de dialogue* ***Paramètres avancés/Affichage***).

11.7.3. Programmation de la mise à jour du programme



Dans l'onglet ***Paramètres de la programmation***, vous pouvez cocher/désélectionner la case ***Activer cette tâche*** pour désactiver temporairement la mise à jour de l'application programmée et la réactiver au moment opportun. Dans la zone de texte ***Nom*** (*désactivée pour toutes les programmations par défaut*), le nom est attribué à cette même programmation par l'éditeur du programme.

Exécution de la programmation

Ici, spécifiez l'intervalle entre chaque exécution de la mise à jour de l'application

programmée. Il est possible de répéter l'exécution de la mise à jour après un laps de temps donné (***Régulièrement***), d'en définir la date et l'heure précises (***A une heure précise***) ou encore de définir l'évènement auquel sera associé le lancement de la mise à jour (***Suivant une action***).

Options avancées de la programmation

Cette section permet de définir dans quelles conditions la mise à jour de l'application doit ou ne doit pas être exécutée si l'ordinateur est en mode d'économie d'énergie ou hors tension.

Autres paramètres de mise à jour

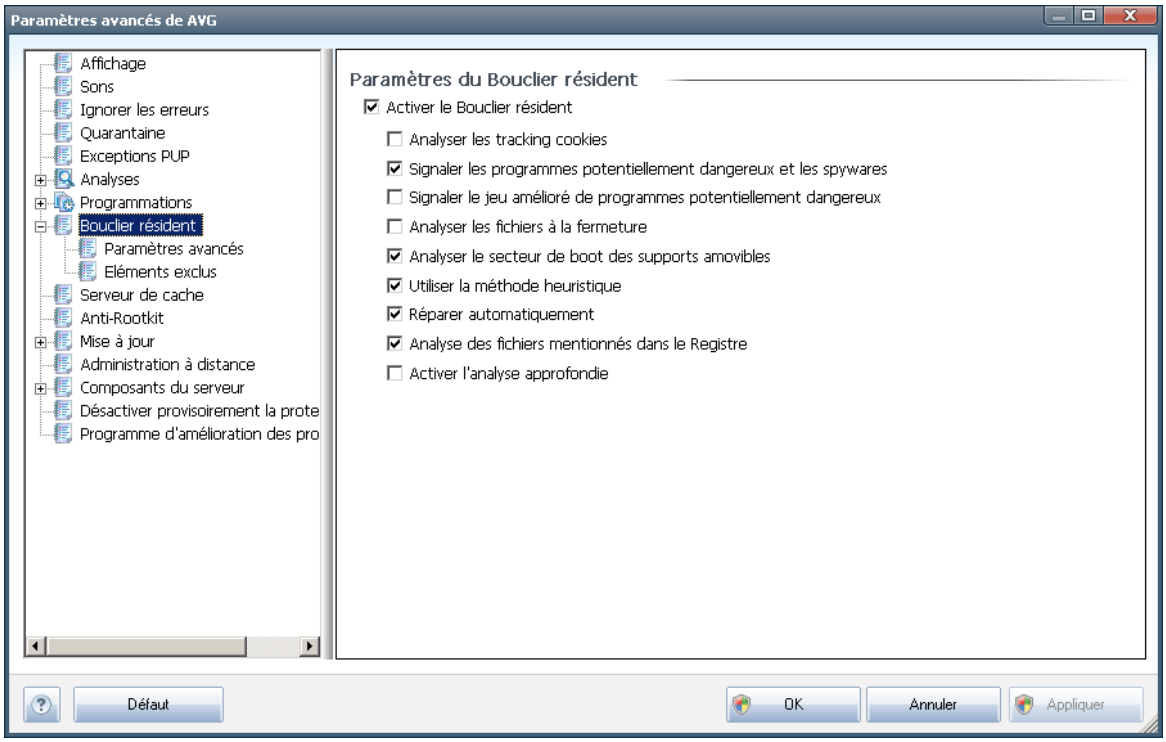
Cochez l'option ***Exécuter de nouveau la mise à jour lorsque la connexion Internet sera disponible*** pour vous assurer qu'en cas d'interruption de la connexion Internet et d'échec de la mise à jour, le processus est relancé dès le rétablissement de la connexion Internet.

Lorsque la mise à jour programmée est lancée à l'heure spécifiée, une fenêtre vous en informe par le biais d'une icône dans la barre d'état système AVG (*à condition que vous ayez conservé la configuration par défaut de la boîte de dialogue* ***Paramètres avancés/Affichage***).

Remarque : *si une mise à jour planifiée du programme coïncide avec une analyse programmée, le processus de mise à jour a priorité sur l'analyse qui est interrompue.*

11.8. Bouclier résident

Le composant ***Bouclier résident*** protège directement les fichiers et les dossiers contre les virus, les spywares et autres codes malicieux.



La boîte de dialogue ***Paramètres du Bouclier résident*** permet d'activer ou de désactiver la protection offerte par le ***Bouclier résident*** en sélectionnant ou en désélectionnant la case ***Activer le Bouclier résident*** (*option activée par défaut*). Vous pouvez aussi préciser les fonctions du ***Bouclier résident*** à appliquer :

- ***Analyser les tracking cookies*** - ce paramètre indique que l'analyse doit détecter les cookies. (*Les cookies HTTP servent à authentifier, à suivre et à gérer certaines informations sur les utilisateurs comme leurs préférences en matière de navigation ou le contenu de leur panier d'achat électronique*).

- ***Signaler les programmes potentiellement dangereux et les spywares*** – (*activé par défaut*) : cochez cette case pour activer le moteur ***Anti-spyware*** et rechercher les spywares et les virus. Les spywares désignent une catégorie de codes suspects : même s'ils représentent généralement un risque pour la sécurité, certains de ces programmes peuvent être installés intentionnellement par l'utilisateur. Nous vous recommandons de laisser cette fonction activée car elle augmente de manière significative la sécurité de votre système.

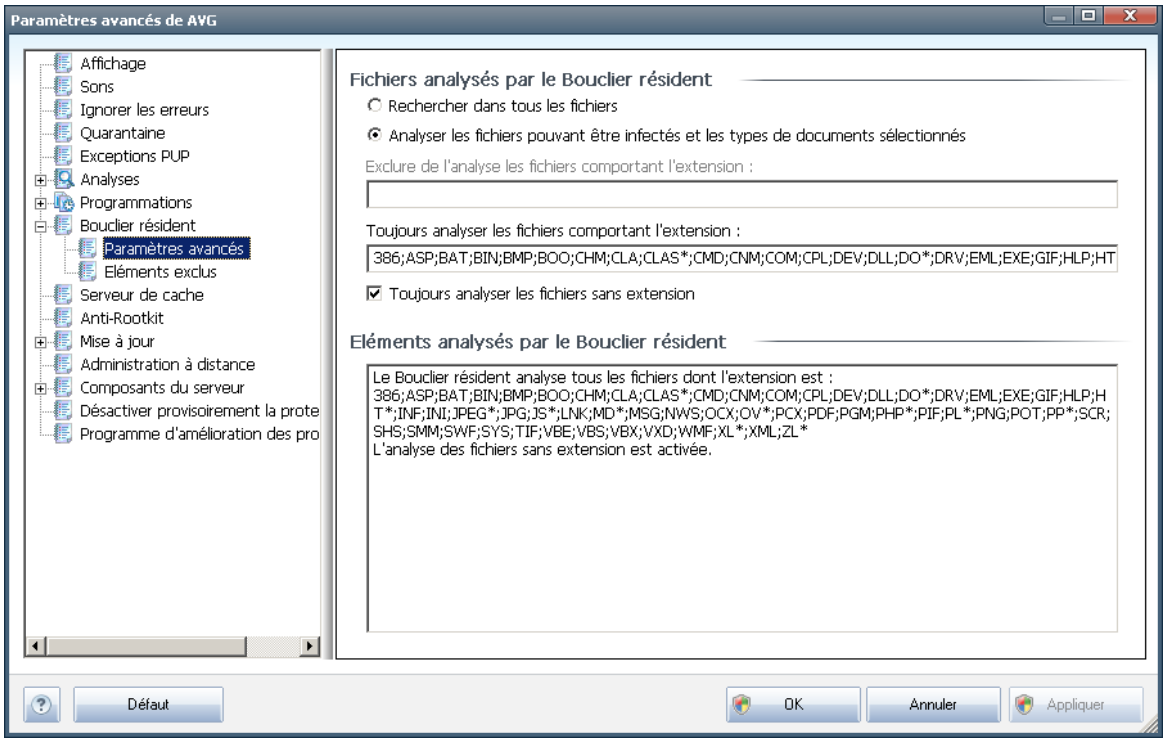
- ***Signaler le jeu amélioré de programmes potentiellement dangereux*** (*option désactivée par défaut*) : permet de détecter le jeu étendu des spywares qui ne posent aucun problème et sont sans danger dès lors qu'ils

sont achetés directement auprès de leur éditeur, mais qui peuvent ensuite être utilisées à des fins malveillantes. Il s'agit d'une mesure de sécurité supplémentaire. Cependant, elle peut bloquer des programmes légitimes de l'ordinateur ; c'est pourquoi elle est désactivée par défaut.

- ***Analyser les fichiers à la fermeture*** (*option désactivée par défaut*) - ce type d'analyse garantit qu'AVG vérifie les objets actifs (par exemple, les applications, les documents…) à leur ouverture et à leur fermeture. Cette fonction contribue à protéger l'ordinateur contre certains types de virus sophistiqués.
- ***Analyser le secteur de boot des supports amovibles*** - (*option activée par défaut*)
- ***Utiliser la méthode heuristique***- (*option activée par défaut*) - l'analyse heuristique est un moyen de détection (*émulation dynamique des instructions de l'objet analysé dans un environnement informatique virtuel*)
- ***Réparer automatiquement*** (*option désactivée par défaut*) - toute infection détectée sera réparée automatiquement dans la mesure où un traitement existe ; les infections incurables seront supprimées.
- ***Analyse des fichiers mentionnés dans le Registre***(*option activée par défaut*) - ce paramètre indique qu'AVG analyse les fichiers exécutables ajoutés au registre de démarrage pour éviter l'exécution d'une infection connue au démarrage suivant de l'ordinateur.
- ***Activer l'analyse approfondie*** (*option désactivée par défaut*) - dans certains cas (*urgence*), vous pouvez cocher cette case afin d'activer les algorithmes les plus rigoureux qui examineront au peigne fin tous les objets représentant de près ou de loin une menace. Gardez à l'esprit que cette méthode prend énormément de temps.

11.8.1. Paramètres avancés

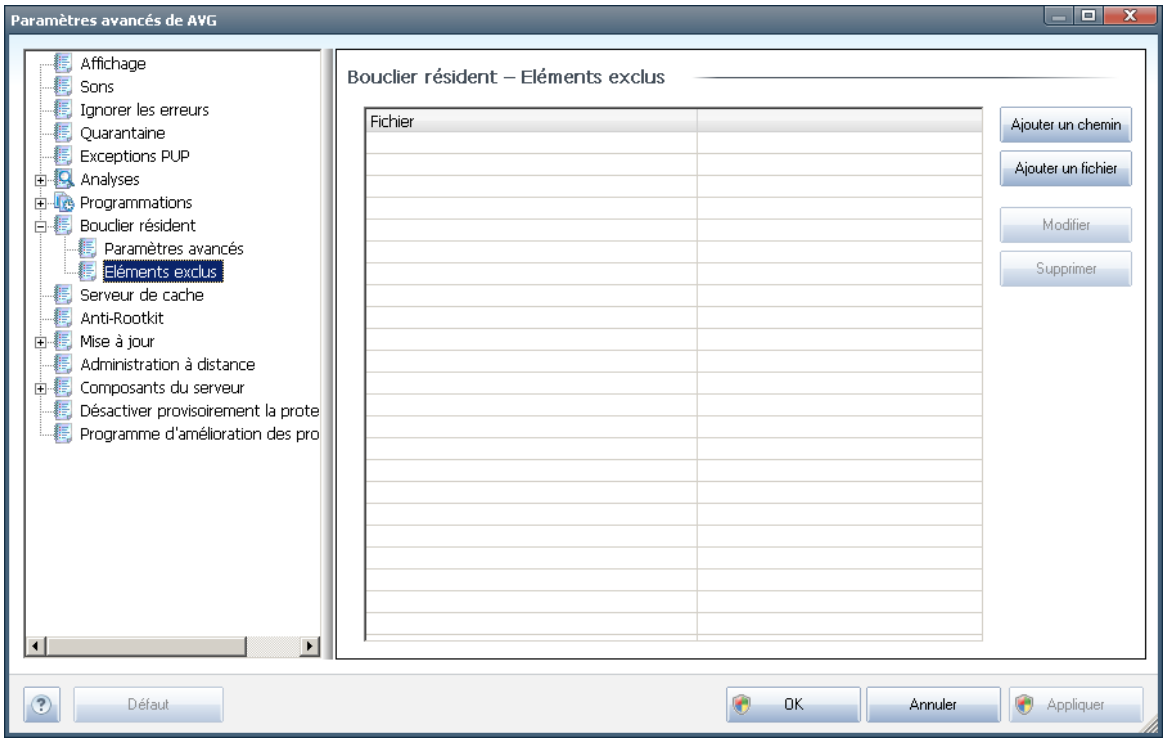
Dans la boîte de dialogue ***Fichiers analysés par le Bouclier résident***, il est possible de spécifier les fichiers à analyser (*en fonction de leurs extensions*) :



Choisissez si vous voulez analyser tous les fichiers ou seulement ceux qui sont susceptibles d'être infectés. En l'occurrence, vous pouvez dresser la liste des extensions correspondant aux fichiers à exclure de l'analyse et la liste des extensions correspondant aux fichiers à analyser systématiquement.

La section en dessous appelée ***Eléments analysés par le Bouclier résident*** récapitule les paramètres actuels et donne des informations détaillées sur les éléments examinés par le Bouclier résident.

11.8.2. Eléments exclus



La boîte de dialogue ***Bouclier résident - Eléments exclus*** offre la possibilité de définir les dossiers à exclure de l'analyse effectuée par le ***Bouclier résident***.

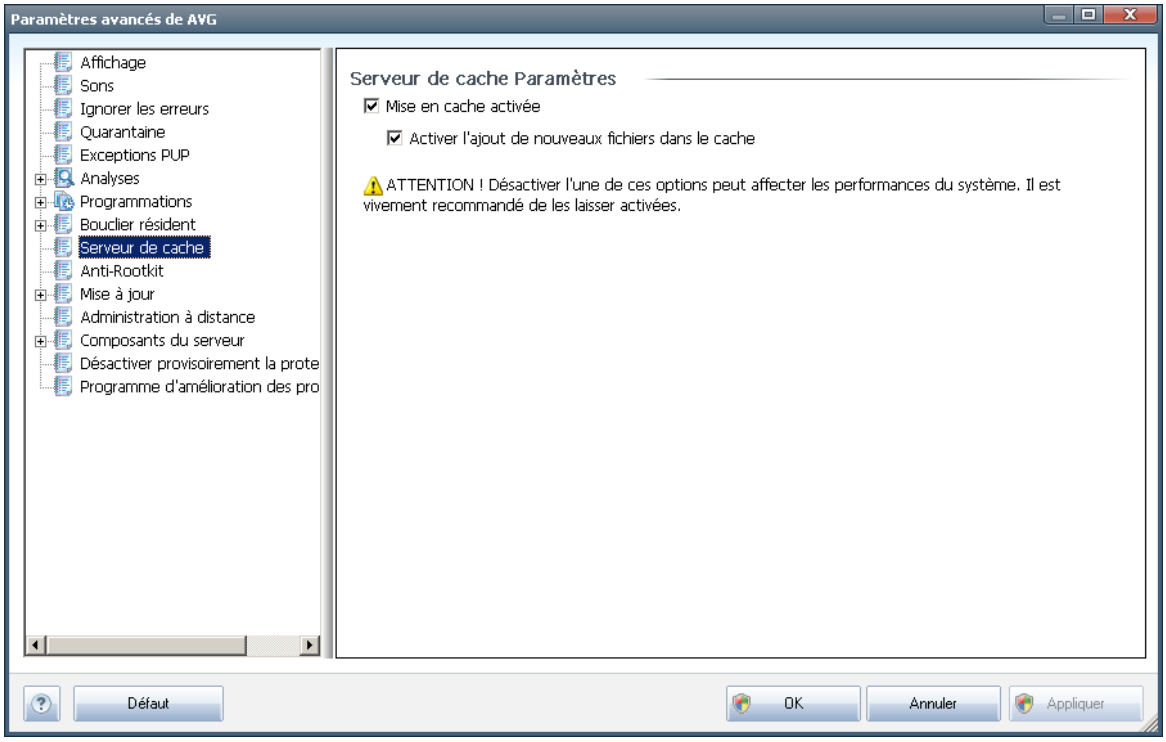
Il est vivement recommandé de n'exclure aucun fichier, sauf en cas d'absolue nécessité !

Cette boîte de dialogue présente les boutons de fonction suivantes :

- ***Ajouter un chemin*** – ce bouton permet de spécifier un répertoire ou des répertoires que vous souhaitez exclure de l'analyse en les sélectionnant un à un dans l'arborescence de navigation du disque local
- ***Ajouter un fichier*** – ce bouton permet de spécifier les fichiers que vous souhaitez exclure de l'analyse en les sélectionnant un à un dans l'arborescence de navigation du disque local
- ***Modifier***- ce bouton permet de modifier le chemin d'accès à un fichier ou dossier sélectionné
- ***Supprimer***– ce bouton permet de supprimer le chemin d'accès à un objet sélectionné dans la liste

11.9. Serveur de cache

Le ***serveur de cache*** est un processus conçu pour accélérer toutes les analyses (*analyses à la demande, analyses de l'ordinateur programmée ou analyses du Bouclier résident*). Il rassemble et conserve les informations des fichiers dignes de confiance (*fichiers système dotés d'une signature numérique, etc.).*). Ces fichiers, jugés sans danger, sont par la suite ignorés pendant l'analyse.



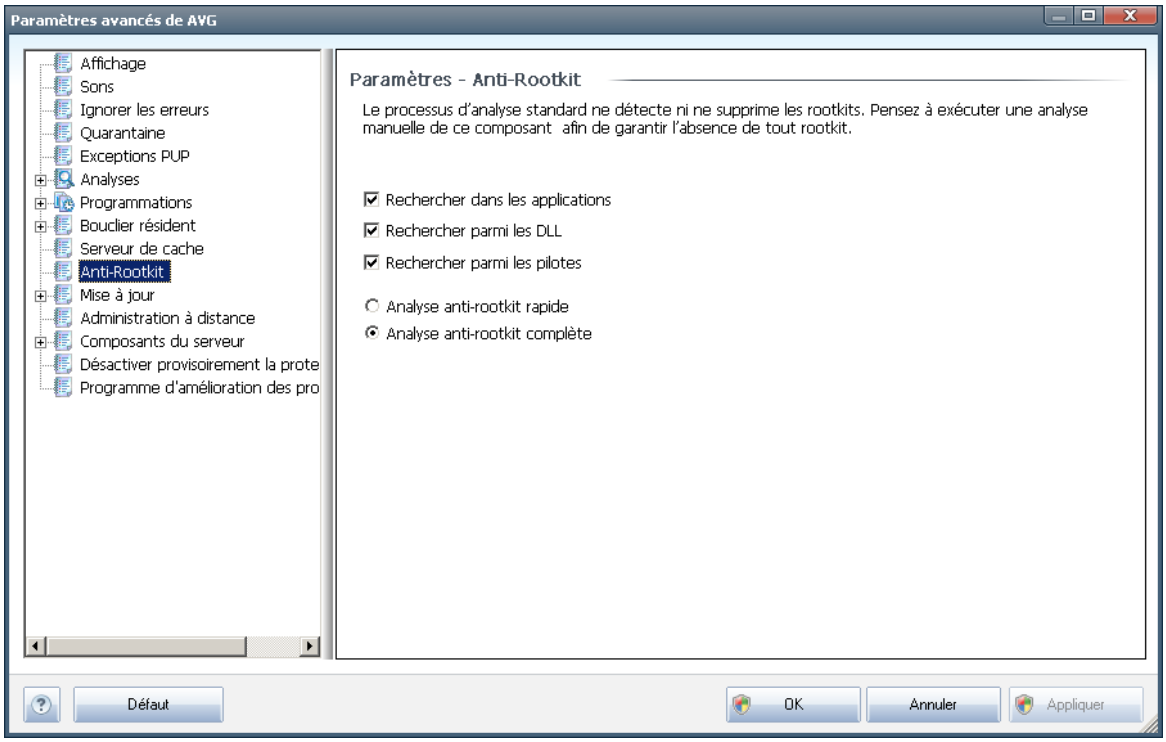
La boîte de dialogue des paramètres propose deux options :

- ***Mise en cache activée*** (*option activée par défaut*) – désélectionnez la case pour désactiver le ***serveur de cache*** et videz la mémoire de mise en cache. Notez que l'analyse risque de durer plus longtemps et que les performances de l'ordinateur risquent d'être diminuées étant donné que chaque fichier en cours d'utilisation fera d'abord l'objet d'une analyse anti-virale et anti-spyware préalable.

- ***Activer l'ajout de nouveaux fichiers dans le cache*** (*option activée par défaut*) – désélectionnez la case pour mettre fin à l'ajout de fichiers dans la mémoire cache. Tout fichier déjà mis en cache sera conservé et utilisé jusqu'à ce que la mise en cache soit complètement désactivée ou jusqu'à la prochaine mise à jour de la base de données virale.

11.10. Anti-rootkit

Dans cette boîte de dialogue, vous pouvez modifier la configuration du composant ***Anti-Rootkit*** :



Modifier le composant ***Anti-Rootkit***comme indiqué dans cette boîte de dialogue est également possible depuis l'***interface du composant Anti-Rootkit***.

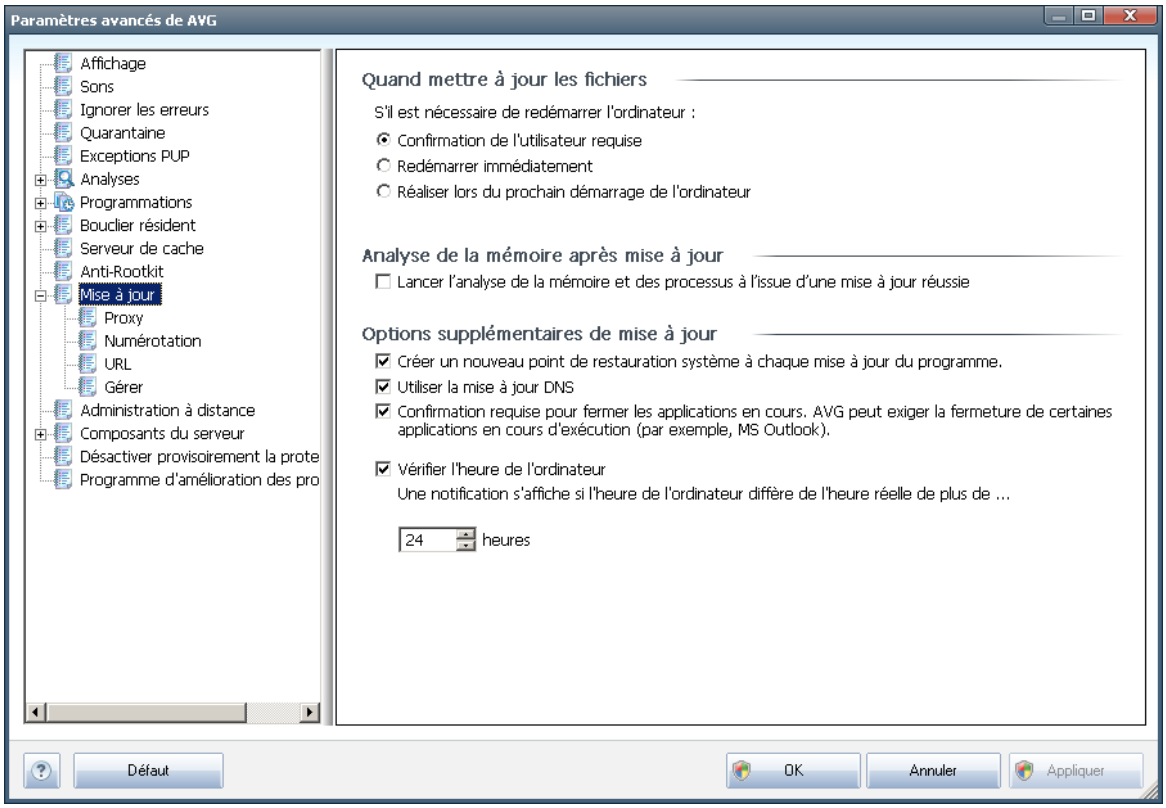
Cochez tout les cases permettant d'indiquer les objets à analyser :

- ***Rechercher dans les applications***
- ***Rechercher parmi les DLL***
- ***Rechercher parmi les pilotes***

Vous pouvez ensuite choisir le mode d'analyse des rootkits :

- ***Analyse anti-rootkit rapide*** - analyse tous les processus en cours d'exécution, les pilotes chargés et le dossier système (*c:\Windows*)
- ***Analyse anti-rootkit complète*** - analyse tous les processus en cours d'exécution, les pilotes chargés et le dossier système (*c:\Windows généralement*), ainsi que tous les disques locaux (*y compris le disque flash, mais pas les lecteurs de disquettes ou de CD-ROM*)

11.11. Mise à jour



L'élément de navigation ***Mise à jour*** ouvre une nouvelle boîte de dialogue dans laquelle vous spécifiez les paramètres généraux de la mise à jour du programme AVG :

Quand mettre à jour les fichiers

Dans cette section, vous avez le choix entre deux options : la mise à jour peut être programmée pour être lancée au redémarrage de l'ordinateur ou être exécutée immédiatement. Par défaut, l'option de mise à jour immédiate est sélectionnée, car de cette façon AVG offre le niveau de sécurité optimal. Programmer une mise à jour au redémarrage suivant est seulement recommandé si l'ordinateur est régulièrement redémarré (au moins une fois par jour).

Si vous décidez d'appliquer la configuration par défaut et lancer l'opération immédiatement, vous pouvez préciser les conditions dans lesquelles un redémarrage obligatoire doit être réalisé :

- ***Confirmation de l'utilisateur requise*** - un message vous invite à approuver le redémarrage nécessaire pour finaliser le processus de mise à jour
- ***Redémarrer immédiatement*** - l'ordinateur est redémarré automatiquement à l'issue de la mise à jour, votre accord n'est pas recherché

- ***Réaliser lors du prochain démarrage de l'ordinateur***- la finalisation du processus de mise à jour est différée jusqu'au redémarrage de l'ordinateur - rappelez-vous que cette option est à proscrire si l'ordinateur n'est pas fréquemment redémarré (moins d'une fois par jour).

Analyse de la mémoire après mise à jour

Cochez cette case pour indiquer que vous voulez exécuter une nouvelle analyse de la mémoire après chaque mise à jour achevée avec succès. La dernière mise à jour téléchargée peut contenir de nouvelles définitions de virus et celles-ci peuvent être analysées automatiquement.

Options supplémentaires de mise à jour

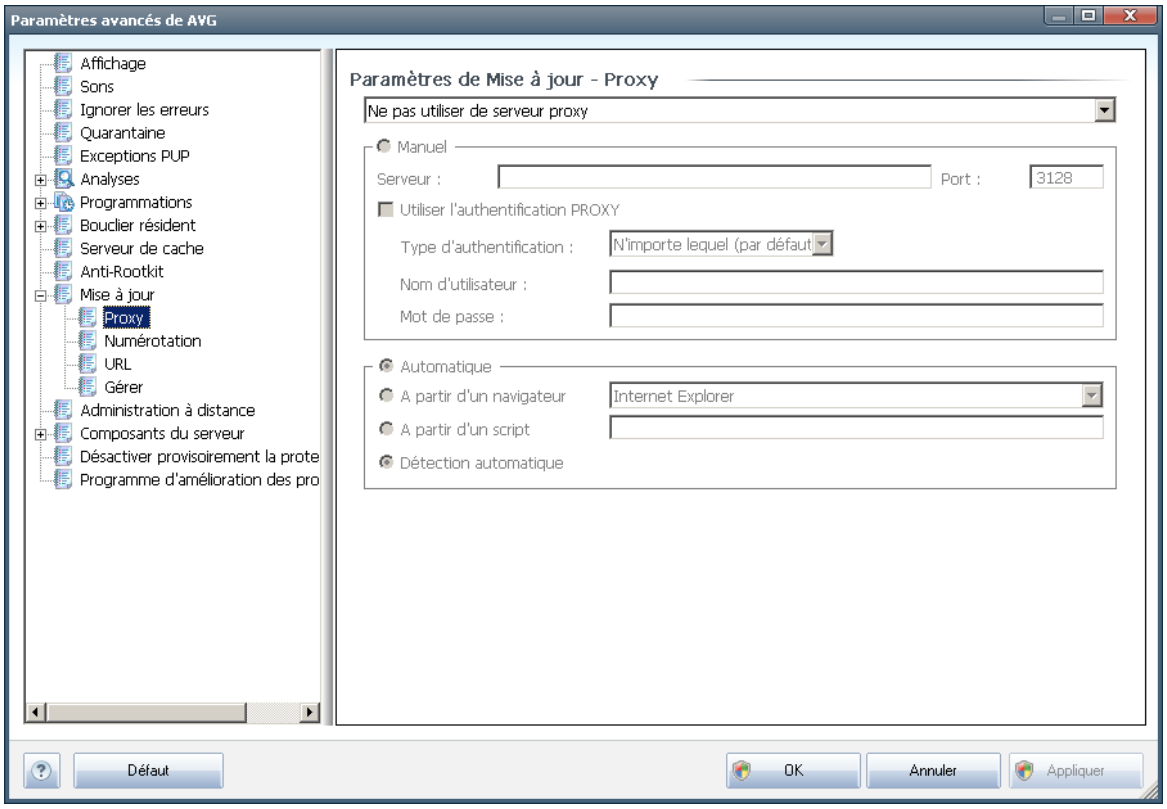
- ***Créer un nouveau point de restauration après chaque nouvelle mise à jour du programme*** : un point de restauration est créé avant le lancement d'une mise à jour du programme AVG. En cas d'échec de la mise à jour et de blocage de votre système d'exploitation, vous avez alors la possibilité de restaurer le système d'exploitation tel qu'il était configuré à partir de ce point. Cette option est accessible via Démarrer / Tous les programmes / Accessoires / Outils système / Restauration du système. Option réservée aux utilisateurs expérimentés. Laissez cette case cochée si vous voulez utiliser cette fonctionnalité.

- ***Utiliser la mise à jour DNS*** : cochez cette case si vous voulez confirmer que vous voulez utiliser la méthode de détection des fichiers de mise à jour qui élimine la quantité de données transférée entre le serveur de mise à jour et le client AVG ;

- ***Confirmation requise pour fermer les applications en cours*** (*option activée par défaut*) : cette option permet de vous assurer qu'aucune application actuellement en cours d'exécution ne sera fermée sans votre autorisation, si cette opération est requise pour la finalisation du processus de mise à jour ;

- ***Vérifier l'heure de l'ordinateur*** : cochez cette case si vous voulez être informé lorsque l'heure du système et l'heure correcte diffèrent de plus du nombre d'heures spécifié.

11.11.1. Proxy



Un serveur proxy est un serveur ou un service autonome s'exécutant sur un PC dans le but de garantir une connexion sécurisée à Internet. En fonction des règles de réseau spécifiées, vous pouvez accéder à Internet directement, via le serveur proxy ou en combinant les deux possibilités. Dans la première zone (liste déroulante) de la boîte de dialogue ***Paramètres de mise à jour - Proxy***, vous êtes amené à choisir parmi les options suivantes :

- ***Utiliser un serveur proxy***
- ***Ne pas utiliser de serveur proxy*** - paramètre par défaut
- ***Utiliser un serveur proxy. En cas d'échec, se connecter en direct***

Si vous sélectionnez une option faisant appel au serveur proxy, vous devez spécifier des données supplémentaires. Les paramètres du serveur peuvent être configurés manuellement ou automatiquement.

Configuration manuelle

Si vous choisissez la configuration manuelle (cochez la case *Manuel pour activer la section correspondante dans la boîte de dialogue*), spécifiez les éléments suivants :

- ***Serveur*** – indiquez l'adresse IP ou le nom du serveur

- ***Port*** – spécifiez le numéro du port donnant accès à Internet (*par défaut, le port 3128) – en cas de doute, prenez contact avec l'administrateur du réseau*)

Il est aussi possible de définir des règles spécifiques à chaque utilisateur pour le serveur proxy. Si votre serveur proxy est configuré de cette manière, cochez l'option ***Utiliser l'authentification PROXY*** pour vous assurer que votre nom d'utilisateur et votre mot de passe sont valides pour établir une connexion à Internet via le serveur proxy.

Configuration automatique

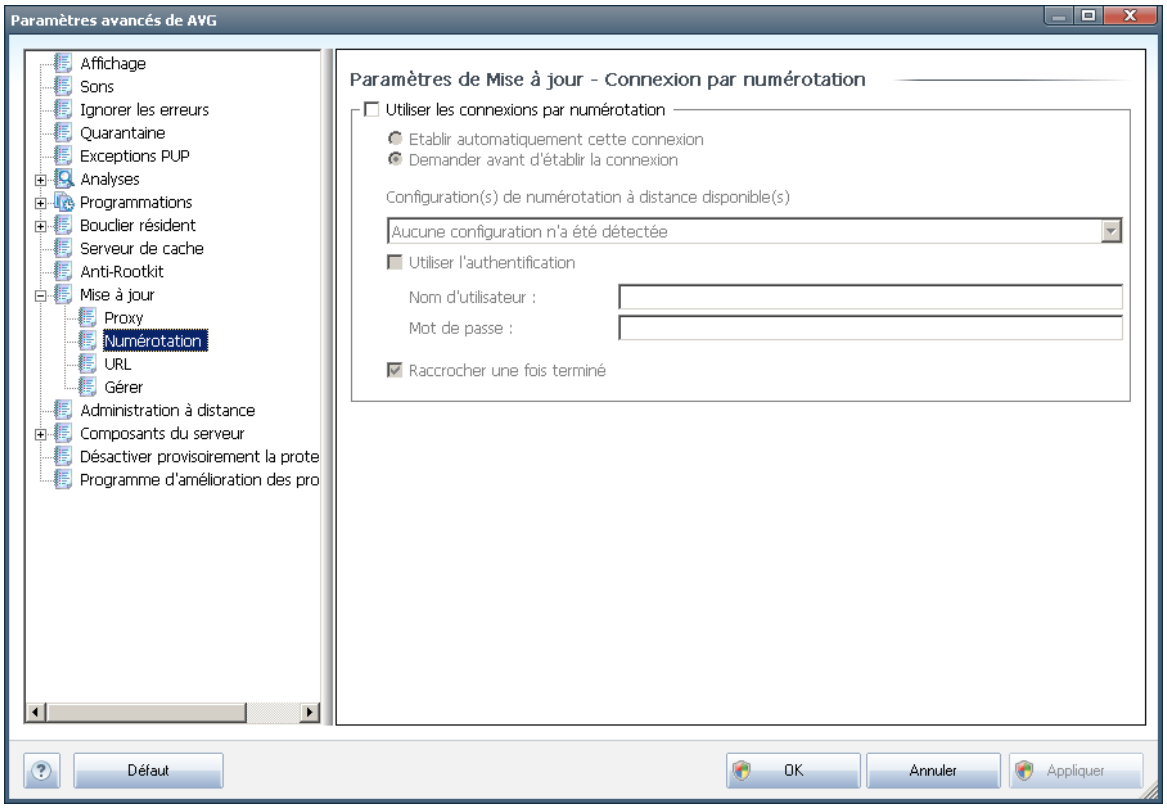
Si vous optez pour la configuration automatique (*cochez la case* ***Automatique****pour activer la section correspondante dans la boîte de dialogue*), puis spécifiez le type de configuration proxy désiré :

- ***A partir du navigateur*** - la configuration sera lue depuis votre navigateur Internet par défaut

- ***A partir d'un script*** - la configuration sera lue à partir d'un script téléchargé avec la fonction renvoyant l'adresse du proxy

- ***Détection automatique*** - la configuration sera détectée automatiquement à partir du serveur proxy

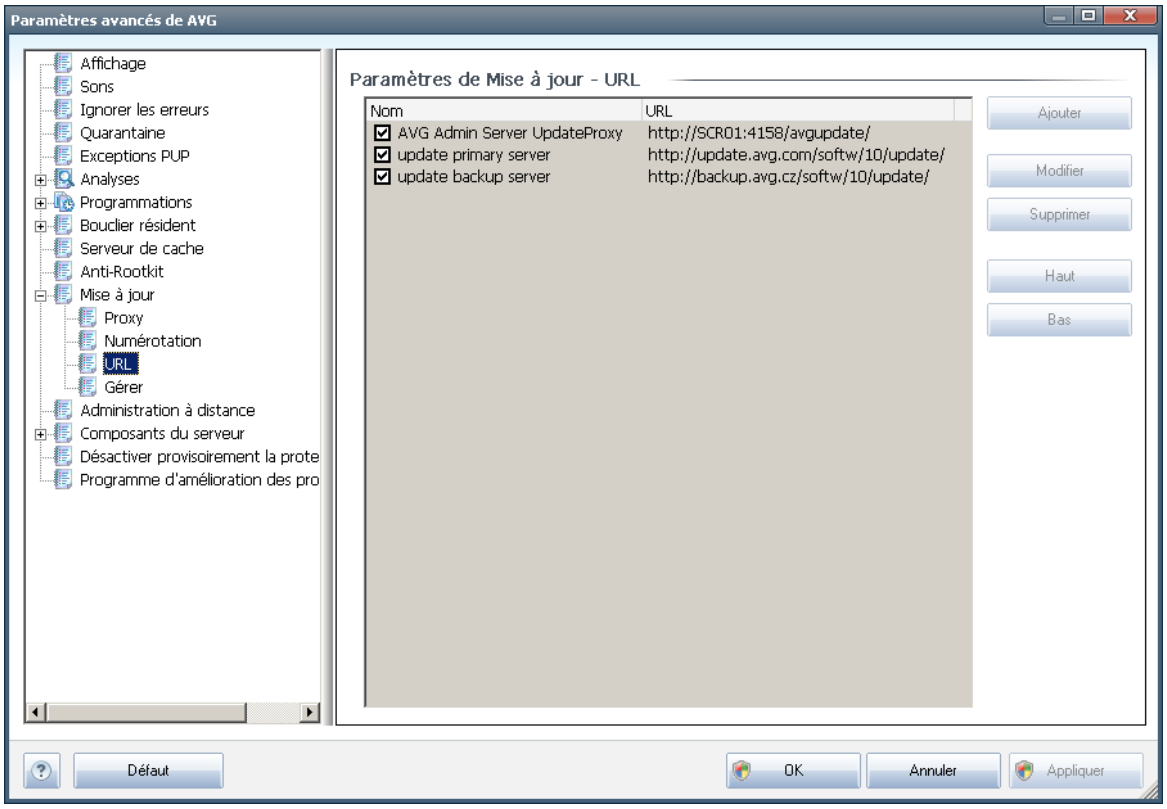
11.11.2. Numérotation



Tous les paramètres facultatifs de la boîte de dialogue ***Paramètres de mise à jour - Connexion par numérotation*** se rapportent à la connexion par numérotation à Internet. Les champs de cette boîte de dialogue sont activés à condition de cocher l'option ***Utiliser les connexions par numérotation.***

Précisez si vous souhaitez vous connecter automatiquement à Internet (***Etablir cette connexion automatiquement***) ou confirmer manuellement la connexion (***Demander avant d'établir la connexion***). En cas de connexion automatique, vous devez indiquer si la connexion doit prendre fin après la mise à jour (***Raccrocher une fois terminé***).

11.11.3. URL

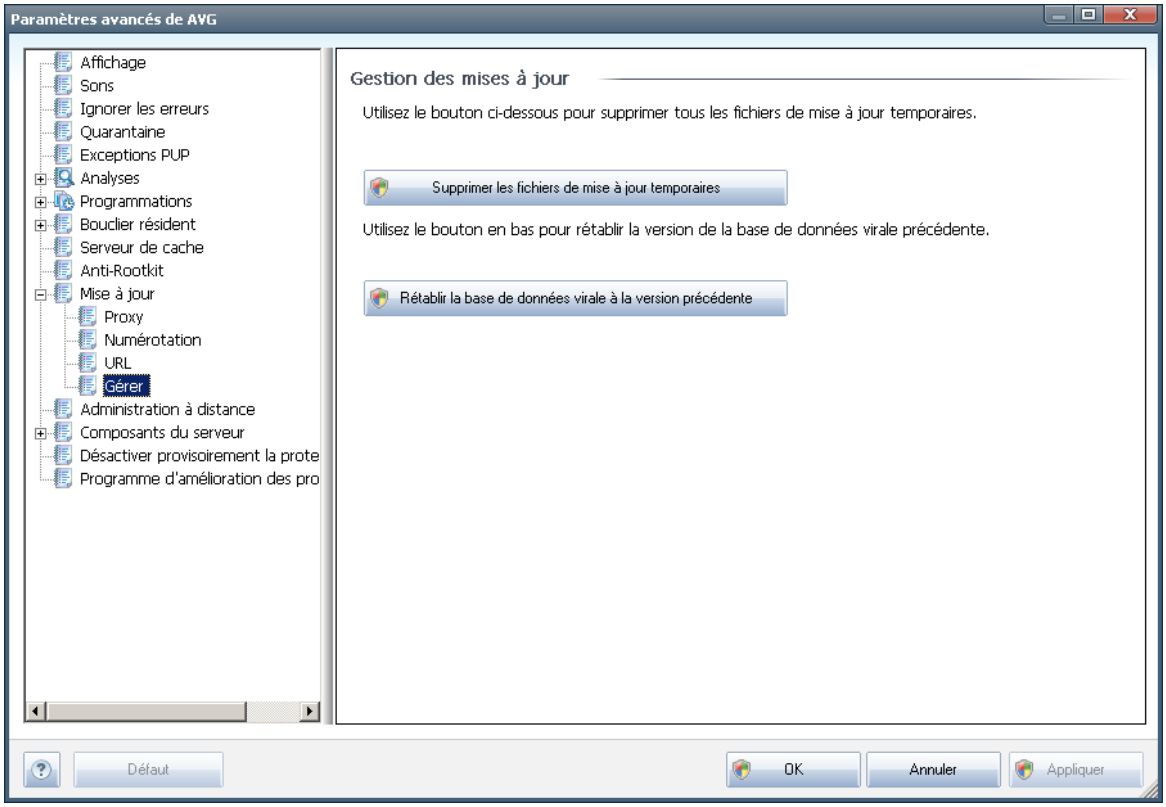


La boîte de dialogue ***URL*** contient une liste d'adresses Internet à partir desquelles il est possible de télécharger les fichiers de mise à jour. Vous pouvez redéfinir le contenu de cette liste à l'aide des boutons de fonction suivants :

- ***Ajouter*** – ouvre une boîte de dialogue permettant de spécifier une nouvelle adresse URL
- ***Modifier*** - ouvre une boîte de dialogue permettant de modifier les paramètres de l'URL sélectionnée
- ***Supprimer*** - retire l'URL sélectionnée de la liste
- ***Haut*** – déplace l'URL sélectionnée d'un rang vers le haut dans la liste
- ***Bas*** – déplace l'URL sélectionnée d'un rang vers le bas dans la liste

11.11.4. Gestion

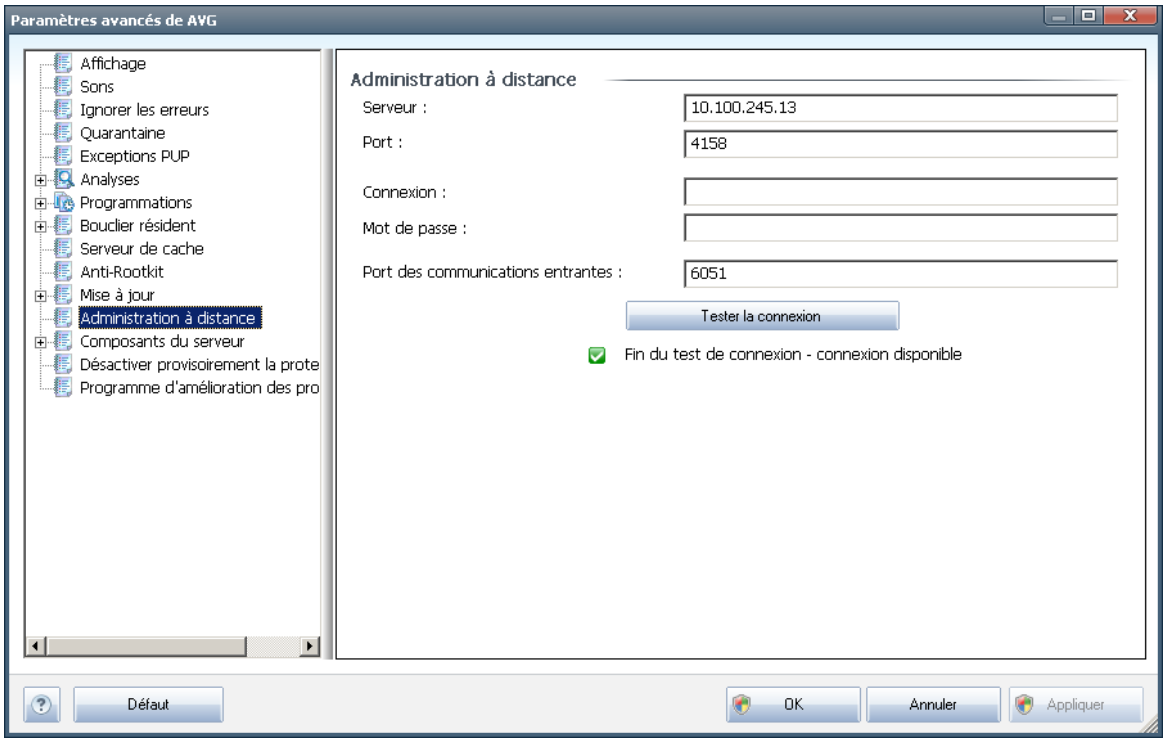
La boîte de dialogue ***Gérer*** propose deux options accessibles via deux boutons :



- ***Supprimer les fichiers de mise à jour temporaires*** - cliquez sur ce bouton pour supprimer tous les fichiers redondants de votre disque dur (*par défaut, ces fichiers sont conservés pendant 30 jours*)

- ***Revenir à la version précédente de la base virale*** – cliquez sur ce bouton pour supprimer la dernière version de la base virale de votre disque dur et revenir à la version précédente enregistrée (*la nouvelle version de la base de données sera incluse dans la mise à jour suivante*)

11.12. Administration à distance



Les paramètres de l'***administration à distance*** concernent la connexion du poste du client AVG au système d'administration à distance. Si vous envisagez de connecter la station au serveur d'administration à distance, veuillez spécifier les paramètres suivants :

- ***Serveur*** - nom du serveur (ou adresse IP) sur lequel AVG Admin Server est installé
- ***Port*** - indiquez le numéro du port sur lequel le client AVG communique avec AVG Admin Server (*le numéro de port 4158 est utilisé par défaut - si vous voulez l'utiliser, il est inutile de le spécifier de manière explicite*)
- ***Connexion*** - si les communications entre le client AVG et AVG Admin Server sont sécurisées, indiquez votre nom d'utilisateur...
- ***Mot de passe*** - ... et votre mot de passe
- ***Port des communications entrantes*** - numéro de port par lequel le client AVG accepte les messages entrants en provenance du serveur AVG Admin Server

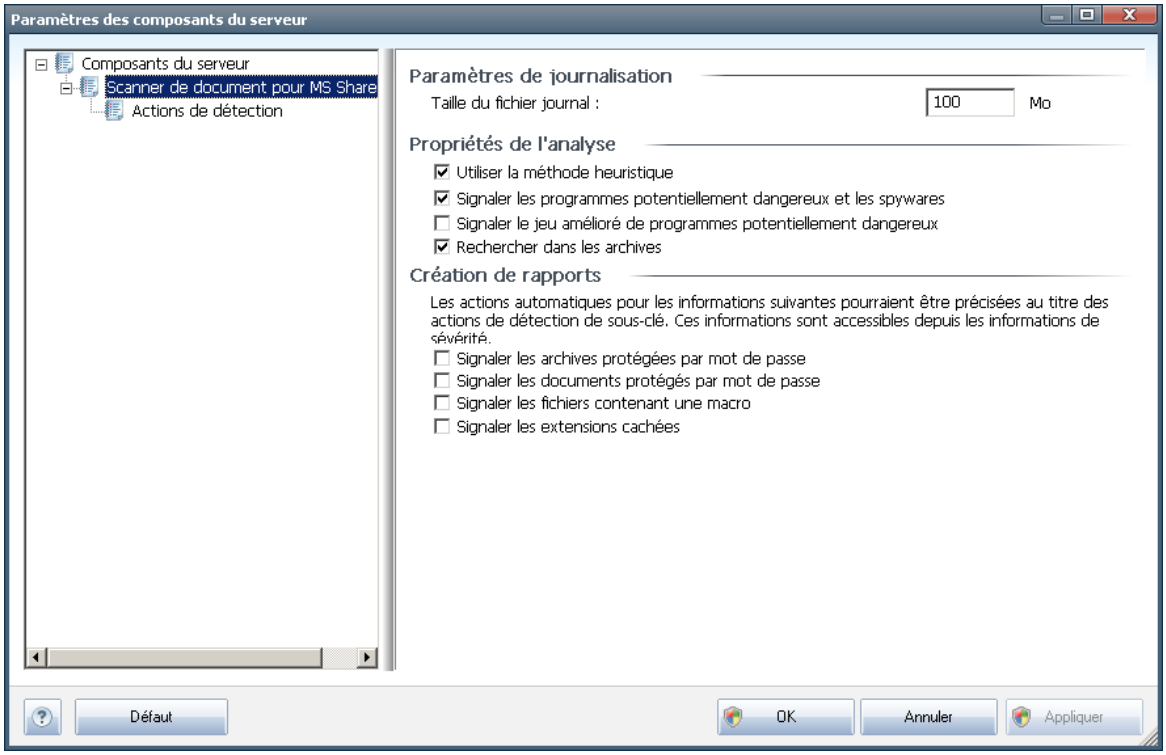
Le bouton ***Tester la connexion*** permet de vérifier que toutes les données spécifiées ci-dessus sont valables et peuvent être utilisées pour se connecter au Centre de données.

Remarque : *pour obtenir des informations détaillées sur l'administration à distance, consultez la documentation relative à une édition professionnelle d'AVG.*

11.13. Composants du serveur

11.13.1. Scanner de documents pour MS SharePoint

Cette boîte de dialogue contient plusieurs options prédéfinies relatives aux performances d'analyse antivirale du composant ***Scanner de documents pour MS SharePoint***. Cette boîte de dialogue comprend plusieurs sections :



Paramètres de journalisation

Champ Taille du fichier journal – le fichier journal contient les enregistrements des différents évènements liés au ***Scanner de documents pour MS SharePoint***, tels que les notes de chargement des bibliothèques du programme, les détections de virus, les avertissements, etc. Définissez la taille maximale de ce fichier dans ce champ.

Propriétés de l'analyse

- ***Utiliser la méthode heuristique*** – cochez cette option pour appliquer la méthode heuristique à l'analyse des documents. Lorsque cette option est activée, vous pouvez filtrer les documents non seulement selon leur extension,

mais aussi selon leur contenu.

- ***Signaler les programmes potentiellement dangereux et les spywares*** – cochez cette option afin d'utiliser le moteur Anti-spyware pour détecter et signaler les programmes suspects et potentiellement dangereux lors de l'analyse de documents.

- ***Signaler le jeu amélioré de programmes potentiellement dangereux*** - cette option permet de détecter le jeu étendu des spywares : ces programmes ne posent aucun problème et sont parfaitement sans danger dès lors qu'ils sont achetés directement auprès de leur éditeur, mais peuvent ensuite être utilisés à des fins malveillantes. Il peut aussi s'agir de programmes absolument inoffensifs, mais qui sont inopportuns (barres d'outils, etc.). Il s'agit d'une mesure de sécurité et de convivialité supplémentaire. Cependant, elle peut bloquer des programmes légitimes de l'ordinateur ; c'est pourquoi elle est désactivée par défaut. Remarque : cette fonction de détection complète l'option précédente. Aussi, si vous souhaitez bénéficiez d'une protection contre des types de spywares standard, veillez à toujours cocher la case précédente.

- ***Rechercher dans les archives*** – cochez cette case pour analyser le contenu des archives.

Création de rapports

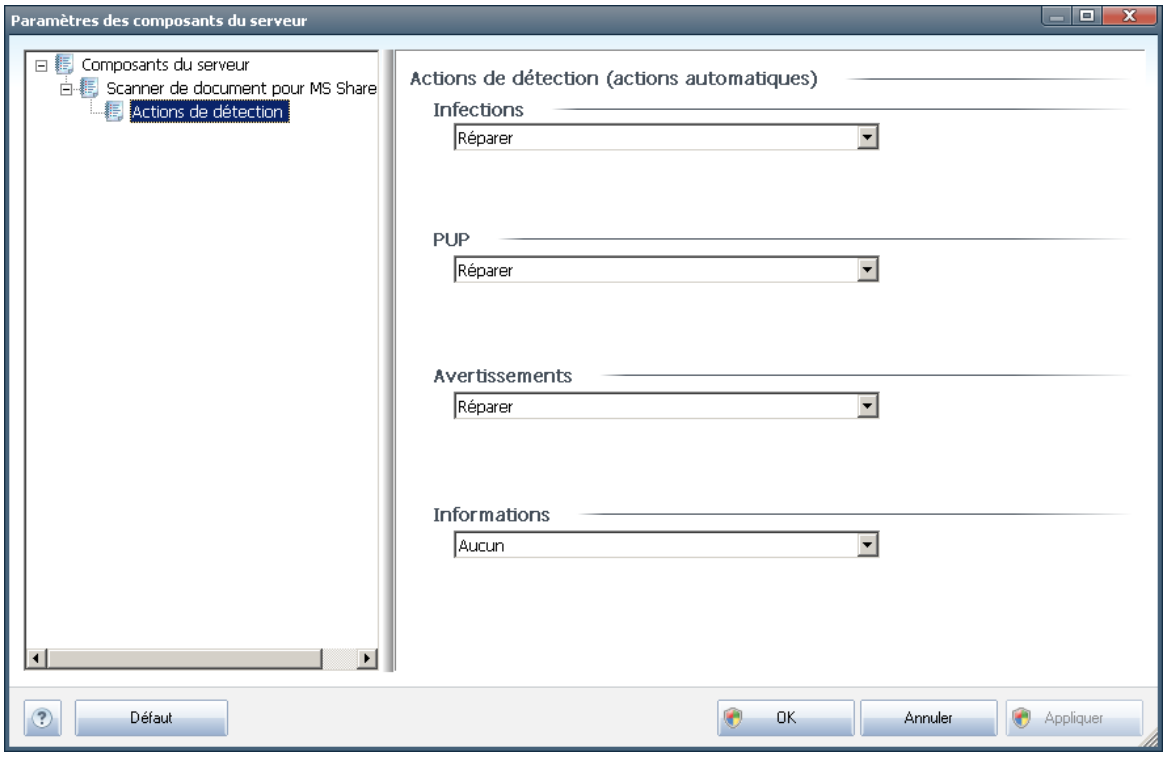
- ***Signaler les archives protégées par mot de passe*** – archives (ZIP, RAR, etc.) qui sont protégées par mot de passe et qui, à ce titre, ne peuvent pas faire l'objet d'une recherche de virus. Cochez cette case pour les signaler comme étant potentiellement dangereuses.

- ***Signaler les documents protégés par mot de passe*** – les documents protégés par mot de passe ne peuvent pas faire l'objet d'une recherche de virus. Cochez cette case pour les signaler comme étant potentiellement dangereux.

- ***Signaler les fichiers contenant une macro*** – une macro est une séquence prédéfinie d'étapes destinées à faciliter certaines tâches pour l'utilisateur (les macros MS Word en sont un exemple bien connu). A ce titre, une macro peut contenir des instructions potentiellement dangereuses. Vous pouvez cocher cette case pour garantir que les fichiers contenant des macros seront signalés comme suspects.

- ***Signaler les extensions cachées*** – masquer les extensions qui peuvent présenter un fichier exécutable suspect "objet.txt.exe" sous la forme d'un fichier texte "objet.txt" inoffensif. Cochez cette case pour signaler ces fichiers comme étant potentiellement dangereux.

11.13.2. Actions de détection



Cette boîte de dialogue permet de configurer le comportement du composant ***Scanner de documents pour MS SharePoint*** en cas de détection d'une menace. Les menaces se répartissent en plusieurs catégories :

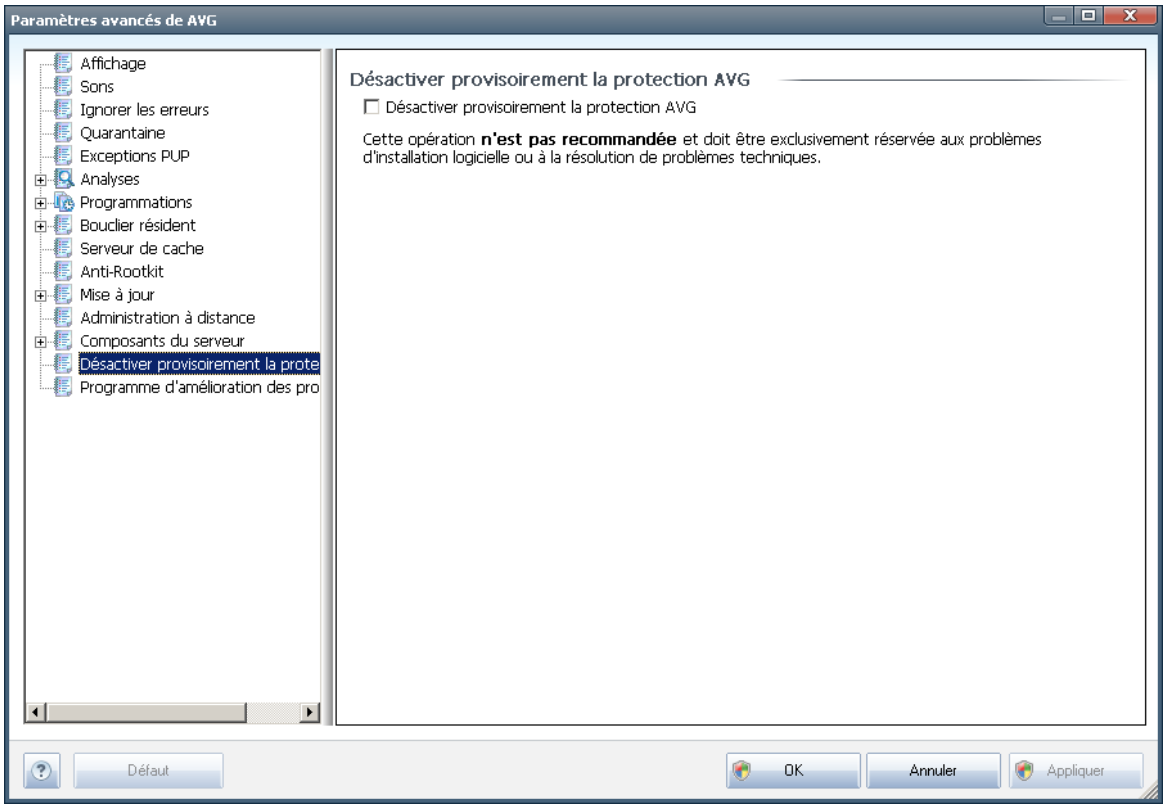
- ***Infections*** – codes malicieux capables de se répliquer et de se propager tout seuls, elles passent souvent inaperçues jusqu'à ce que le mal soit fait.
- ***PUP (Potentially Unwanted Programs, programmes potentiellement dangereux)*** – en général, ces programmes vont des menaces vraiment graves aux simples risques potentiels pour la confidentialité.
- ***Avertissements*** – impossible d'analyser des objets détectés.
- ***Informations*** – inclut toutes les menaces potentielles détectées et pouvant être classifiées dans une des catégories ci-dessus.

Utilisez les menus déroulants pour sélectionner une action automatique pour chaque élément :

- ***Aucune*** – un document contenant ce type de menace ne fera l'objet d'aucune action.
- ***Réparer*** - essaie de réparer le fichier ou document infecté.

- ***Placer en quarantaine***[***] – tous les documents infectés sont mis en quarantaine.
- ***Supprimer*** – les documents sont supprimés en cas de détection d'un virus.

11.14. Désactiver provisoirement la protection AVG



Dans la boîte de dialogue ***Désactiver provisoirement la protection AVG***, vous avez la possibilité de désactiver entièrement la protection offerte par le programme **AVG 2011 Edition Serveur de Fichiers**.

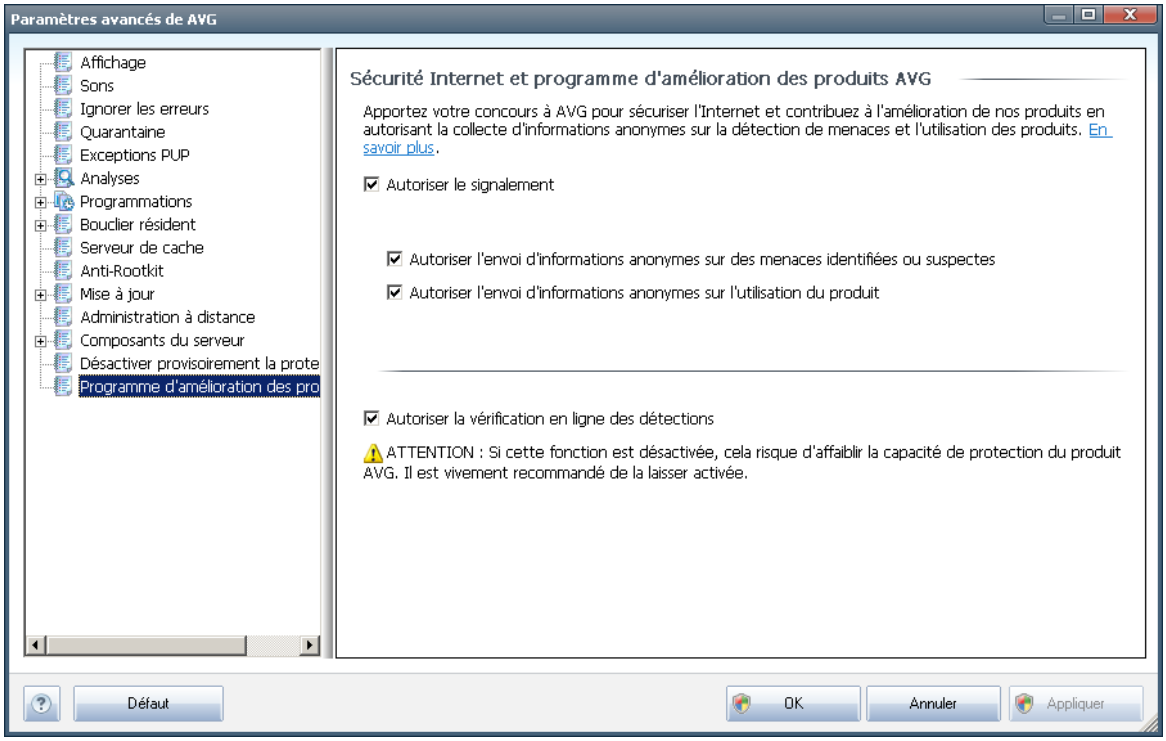
Rappelez-vous que vous ne devez utiliser cette option qu'en cas d'absolue nécessité !

Dans la plupart des cas, il ***est déconseillé*** de désactiver AVG avant d'installer un nouveau logiciel ou pilote, même si l'assistant d'installation ou le logiciel vous suggère d'arrêter d'abord tous les programmes et applications s'exécutant sur le système afin d'empêcher les interruptions inopinées lors du processus d'installation. En cas de problème au cours de l'installation, essayez de désactiver en premier lieu le composant ***Bouclier résident***. Si vous avez momentanément désactivé la protection AVG, veillez à la réactiver dès que vous avez terminé. Si vous êtes connecté à Internet ou à un réseau alors que l'antivirus est désactivé, l'ordinateur est particulièrement vulnérable.

11.15. Programme d'amélioration des produits

La boîte de dialogue ***Sécurité Internet et programme d'amélioration des produits AVG*** vous invite à contribuer à l'amélioration des produits AVG et à une plus grande sécurité sur Internet. Cochez l'option ***Autoriser le signalement*** pour transmettre les menaces détectées à AVG. Ainsi, nous pourrons recueillir les dernières informations sur les nouvelles menaces signalées par les internautes du monde entier et, en retour, fournir à tous une meilleure protection en ligne.

La création de rapports est assurée automatiquement. Il n'en résulte aucune gêne pour les utilisateurs. Notez par ailleurs qu'aucune donnée personnelle n'est incluse dans ces rapports. L'envoi de rapports sur les menaces détectées est facultatif, mais nous vous serions gré d'activer également cette option. Elle nous permet d'améliorer votre protection et celle des autres utilisateurs de produits AVG.



De nos jours, les simples virus représentent une infime partie des menaces. Les auteurs de codes malveillants et de sites Web piégés sont à la pointe de l'innovation et de nouveaux types de menaces ne cessent de voir le jour principalement sur Internet. Voici les plus courants :

- ***Un virus*** est un code malveillant qui se copie et se propage en passant souvent inaperçu jusqu'à ce qu'il ait accomplit son action. Certains virus constituent une menace non négligeable : ils suppriment ou modifient intentionnellement des fichiers sur leur passage. D'autres ont une action relativement moins nocive comme jouer un air de musique. Toutefois, tous les virus sont dangereux en raison de leur capacité de multiplication et de propagation, qui leur permet d'occuper intégralement l'espace mémoire d'un

ordinateur en quelques instants et de provoquer une défaillance générale du système.

- ***Le ver***, une sous-catégorie de virus, se distingue des virus types en ceci qu'il n'a pas besoin d'un objet porteur et peut s'envoyer lui-même vers d'autres ordinateurs, généralement dans un mail. Il en résulte souvent une surcharge des serveurs de messagerie et des systèmes réseau.

- ***Un spyware*** se définit généralement comme une catégorie de malwares (*logiciels malveillants comportant des virus*) qui comprend des programmes (généralement des chevaux de Troie), conçus pour subtiliser des informations personnelles, des mots de passe, des numéros de carte de crédit ; ou pour infiltrer des ordinateurs et permettre aux intrus d'en prendre le contrôle à distance sans l'autorisation et à l'insu de leur propriétaire.

- Λεσ ***programmes potentiellement dangereux*** forment un catégorie de codes espions qui ne sont pas nécessairement dangereux. Un adware est un exemple spécifique de programme potentiellement dangereux. Ce logiciel est spécifiquement conçu pour diffuser des publicités, généralement dans des fenêtres contextuelles intempestives, mais non malveillantes.

- Παρ αιλλευρσ, λεσ ***tracking cookies*** peuvent être considérés comme en faisant partie car ces petits fichiers, stockés dans le navigateur Web et envoyés automatiquement au site Web "parent" lors de votre visite suivante, peuvent contenir des données comme votre historique de navigation et d'autres informations comparables.

- ***Un exploit*** est un programme malveillant qui exploite une faille du système d'exploitation, du navigateur Internet ou d'un autre programme essentiel.

- ***Une opération de phishing*** consiste à tenter d'acquérir des informations confidentielles en se faisant passer pour une société connue et fiable. En règle générale, les victimes potentielles sont harcelées par des messages leur demandant de mettre à jour leurs coordonnées bancaires. Pour ce faire, elles sont invitées à suivre un lien qui les mène jusqu'à un site bancaire fictif.

- ***Le canular (hoax) est un mail envoyé en masse contenant des informations dangereuses, alarmistes ou simplement dénuées d'intérêt.*** La plupart de ces menaces utilisent des mails de type canular pour se propager.

- Λεσ ***sites Web malveillants*** opèrent en installant des programmes malveillants sur votre ordinateur. Les sites piratés font de même, à ceci près que ce sont des sites Web légitimes qui ont été contaminés par des visiteurs.

Pour vous protéger de tous ces différents types de menaces, AVG vous propose les composants spécialisés suivants :

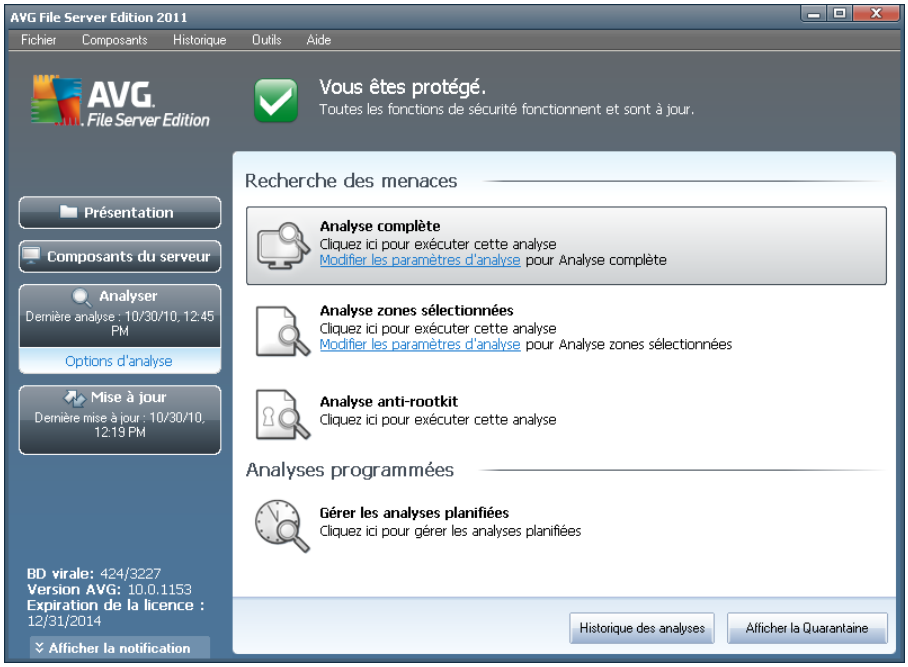
- ***Anti-Virus*** pour protéger votre ordinateur des virus,

- ***Anti-Spyware*** pour protéger votre ordinateur des spywares.

12. Analyse AVG

L'analyse est au cœur de la fonctionnalité du programme **AVG 2011 Edition Serveur de Fichiers**. Vous avez la possibilité d'exécuter des analyses à la demande ou de programmer une analyse quotidienne à l'heure qui vous convient le mieux.

12.1. Interface d'analyse



L'interface d'analyse AVG est accessible via ***Analyse de l'ordinateur*** (lien d'accès rapide). Cliquez sur ce lien pour accéder à la boîte de dialogue ***Recherche des menaces***. Dans cette boîte de dialogue, vous trouverez les éléments suivants :

- présentation des analyses prédéfinies - trois types d'analyse (définis par l'éditeur du logiciel) sont prêts à l'emploi sur demande ou par programmation :
  - ***Analyse complète***
  - ***Analyse zones sélectionnées***
  - ***Analyse anti-rootkit***
- programmation de l'analyse - dans cette section, vous définissez de nouvelles analyses et planifiez d'autres programmations selon vos besoins.

Boutons de commande

Les boutons de commande disponibles au sein de l'interface d'analyse sont les suivants :

- ***Historique des analyses*** - affiche la boîte de dialogue ***Résultats des analyses*** relatant l'historique complet des analyses

- ***Afficher la Quarantaine***- ouvre une nouvelle boîte de dialogue intitulée ***Quarantaine*** - espace dans lequel les infections sont confinées

12.2. Analyses prédéfinies

Parmi les principales fonctions d'**AVG 2011 Edition Serveur de Fichiers**, citons l'analyse à la demande. Ce type d'analyse est prévu pour analyser différentes zones de l'ordinateur en cas de doute concernant la présence éventuelle de virus. Il est vivement recommandé d'effectuer fréquemment de telles analyses même si vous pensez qu'aucun virus ne s'est introduit dans votre système.

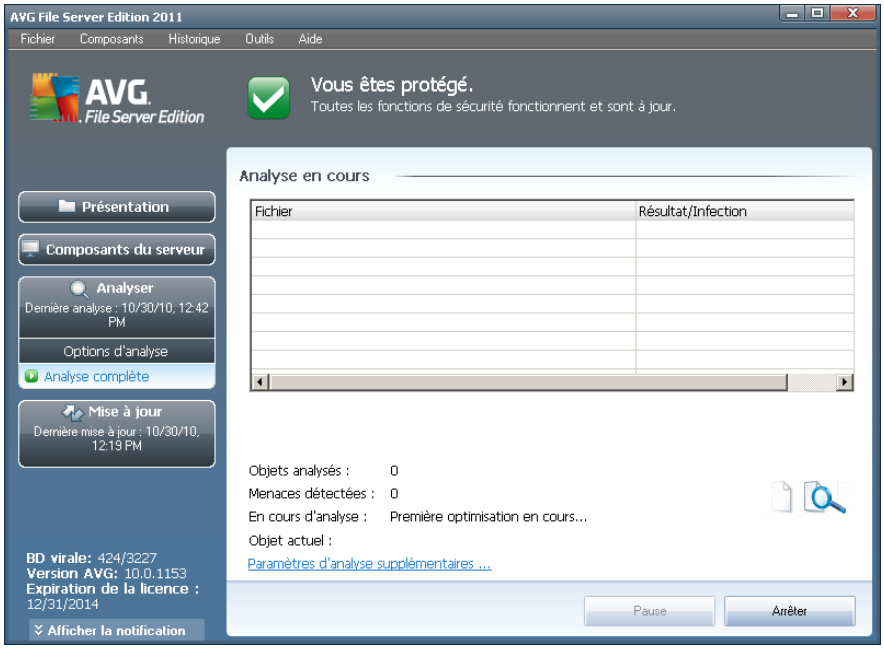
Dans **AVG 2011 Edition Serveur de Fichiers**, vous trouverez les types d'analyses prédéfinies par l'éditeur du logiciel :

12.2.1. Analyse complète

L'***analyse complète*** vérifie l'absence d'infection ainsi que la présence éventuelle de programmes potentiellement dangereux dans tous les fichiers de l'ordinateur. Cette analyse examine les disques durs de l'ordinateur, détecte et répare tout virus ou retire l'infection en la confinant dans la zone de ***quarantaine***. L'analyse de l'ordinateur doit être exécutée sur un poste de travail au moins une fois par semaine.

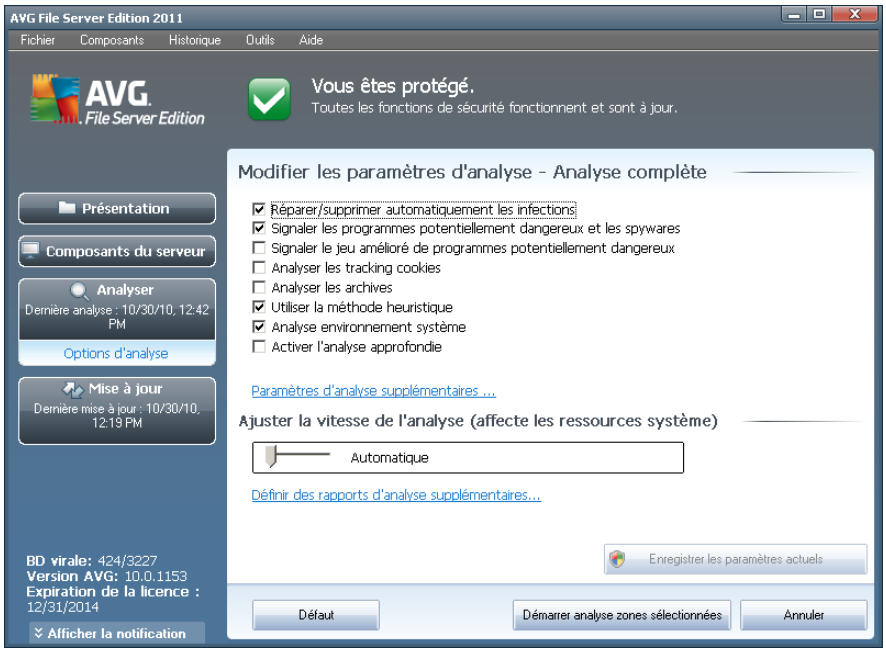
Lancement de l'analyse

L'***analyse complète***peut être lancée directement de l'interface d'analyse en cliquant sur l'icône d'analyse. Pour ce type d'analyse, il n'est pas nécessaire de configurer d'autres paramètres spécifiques. L'analyse démarre immédiatement dans la boîte de dialogue ***Analyse en cours*** (*voir la capture d'écran*). L'analyse peut être interrompue provisoirement (***Interrompre***) ou annulée (***Arrêter***) si nécessaire.



Modification de la configuration de l'analyse

Vous avez la possibilité d'ajuster les paramètres prédéfinis par défaut de l'option ***Analyse complète***. Cliquez sur le lien ***Modifier les paramètres d'analyse*** pour ouvrir la boîte de dialogue ***Modifier les paramètres d'analyse de l'analyse complète*** *(accessible par l'interface d'analyse en activant le lien Modifier les paramètres d'analyse du module Analyse complète)*. ***Il est recommandé de conserver les paramètres par défaut et de ne les modifier qu'en cas d'absolue nécessité.***



- ***Paramètres d'analyse*** - dans la liste des paramètres d'analyse, vous pouvez activer/désactiver des paramètres spécifiques en fonction de vos besoins :

  - ***Réparer/supprimer automatiquement les infections*** (*option activée par défaut*) : lorsqu'un virus est détecté au cours de l'analyse, il est réparé automatiquement dans la mesure du possible. S'il est impossible de réparer automatiquement le fichier infecté, il sera placé en ***quarantaine***.

  - ***Signaler les programmes potentiellement dangereux et les spywares*** (*option activée par défaut*) : cochez cette case pour activer le moteur ***Anti-spyware*** et rechercher les spywares et les virus. Les spywares désignent une catégorie de codes suspects : même s'ils représentent généralement un risque pour la sécurité, certains de ces programmes peuvent être installés intentionnellement par l'utilisateur. Nous vous recommandons de laisser cette fonction activée car elle augmente de manière significative la sécurité de votre système.

  - ***Signaler le jeu amélioré de programmes potentiellement dangereux*** - *(option désactivée par défaut*) : permet de détecter le jeu étendu des spywares qui ne posent aucun problème et sont sans danger dès lors qu'ils sont achetés directement auprès de leur éditeur, mais qui peuvent ensuite être utilisées à des fins malveillantes. Il s'agit d'une mesure de sécurité supplémentaire. Cependant, elle peut bloquer des programmes légitimes de l'ordinateur ; c'est pourquoi elle est désactivée par défaut.

  - ***Analyser les tracking cookies*** (*option désactivée par défaut*) : ce paramètre du composant ***Anti-Spyware*** définit les cookies qui pourront être détectés au cours de l'analyse (*les cookies HTTP servent à authentifier, à suivre et à gérer certaines informations sur les utilisateurs comme leurs préférences en matière de navigation ou le contenu de leur panier d'achat électronique*).

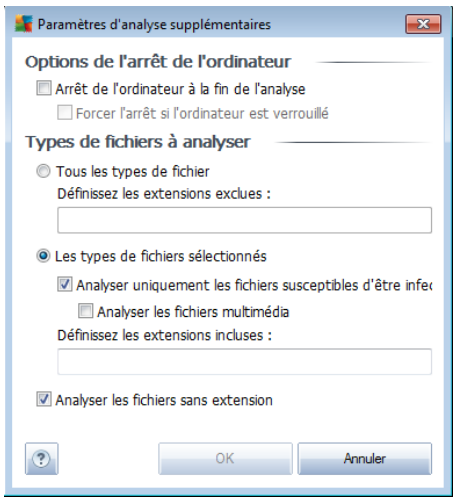
  - ***Analyser les archives*** (*option désactivée par défaut*) : ce paramètre indique que l'analyse examine tous les fichiers même ceux stockés dans des archives (archives ZIP, RAR, par exemple).

  - ***Utiliser la méthode heuristique*** (*option activée par défaut*) : l'analyse heuristique (*émulation dynamique des instructions de l'objet analysé dans un environnement informatique virtuel*) est l'une des méthodes employées pour détecter des virus pendant l'analyse.

  - ***Analyse environnement système*** (*option activée par défaut*) : l'analyse vérifie les fichiers système de l'ordinateur.

  - ***Activer l'analyse approfondie*** (*option désactivée par défaut*) - dans certains cas (*suspicion d'une infection de l'ordinateur*), vous pouvez cocher cette option pour exécuter des algorithmes d'analyse très pointus même s'il est peu probable que certaines zones de l'ordinateur soient infectées. Gardez à l'esprit que cette méthode prend énormément de temps.

- ***Paramètres d'analyse supplémentaires*** - ce lien ouvre une nouvelle boîte de dialogue ***Paramètres d'analyse supplémentaires*** permettant de spécifier les paramètres suivants :



  - ***Options de l'arrêt de l'ordinateur*** - indiquez si l'ordinateur doit être arrêté automatiquement à la fin du processus d'analyse. Si l'option ***Arrêt de l'ordinateur à la fin de l'analyse*** est activée, l'option ***Forcer l'arrêt si l'ordinateur est verrouillé*** devient disponible et permet d'arrêter l'ordinateur même s'il est verrouillé.

  - ***Définir les types de fichiers à analyser*** - vous devez également choisir d'analyser :

    - ***Tous les types de fichier*** avec la possibilité de définir les éléments à exclure de l'analyse en répertoriant les extensions de fichiers (séparées par des virgules) à ne pas analyser ; ou les;

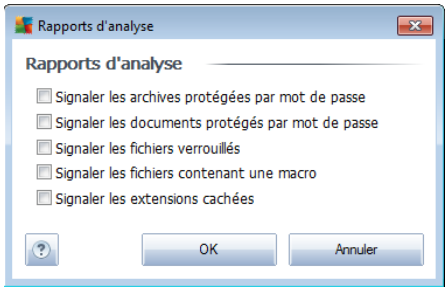
    - ***Les types de fichiers sélectionnés*** - vous pouvez choisir d'analyser uniquement les fichiers susceptibles d'être infectés (*les fichiers qui ne peuvent faire l'objet d'une infection ne sont pas analysés ; il s'agit par exemple de fichiers en texte brut ou de certains types de fichier non exécutables*), y compris les fichiers multimédia (*vidéo, audio - si vous ne sélectionnez pas cette option, la durée de l'analyse sera considérablement réduite, car ce sont souvent de gros fichiers qui sont rarement infectés par un virus*). En fonction des extensions, vous pouvez également spécifier les fichiers qui doivent toujours faire l'objet d'une analyse.

    - Vous pouvez également choisir l'option ***Analyser les fichiers sans extension*** - cette option est activée par défaut et il est recommandé de la conserver et de ne la modifier qu'en cas d'absolue nécessité. Les fichiers sans extension sont relativement suspects et doivent toujours faire l'objet d'une analyse.

- ***Ajuster la vitesse de l'analyse*** - le curseur vous permet de modifier la

priorité du processus d'analyse. Par défaut, elle est fixée sur *Automatique*, niveau qui optimise le processus d'analyse et l'utilisation des ressources système. Vous pouvez aussi choisir le processus d'analyse lent, qui réduit la charge sur les ressources système (*cette option est pratique quand vous devez travailler sur l'ordinateur sans avoir à vous soucier de la durée de l'analyse)*) ; ou rapide, qui utilise plus de ressources système (*convient notamment lorsque vous quittez temporairement votre poste de travail*).

- ***Définir des rapports d'analyse supplémentaires*** - ce lien ouvre une nouvelle boîte de dialogue ***Rapports d'analyse***, dans laquelle vous pouvez sélectionner les types de résultats que vous souhaitez obtenir :



Avertissement : *ces paramètres d'analyse sont identiques à ceux d'une nouvelle analyse, comme indiqué dans le chapitre* ***Analyse AVG / Programmation de l'analyse / Comment faire l'analyse****. Si vous décidez de modifier la configuration par défaut de l'****Analyse complète****, vous avez la possibilité d'enregistrer ces nouveaux paramètres en tant que configuration par défaut et de les appliquer à toute analyse complète de l'ordinateur.*

12.2.2. Analyse zones sélectionnées

Analyse zones sélectionnées - analyse seulement les zones de l'ordinateur que vous avez sélectionnées en vue d'une analyse (*dossiers, disque durs, disquettes, CD, etc.)*). Le déroulement de l'analyse en cas de détection virale, ainsi que la solution appliquée, est le même que pour une analyse complète de l'ordinateur ***: tout virus détecté est réparé ou déplacé en quarantaine***. L'Analyse zones sélectionnées permet de configurer vos propres analyses et de les programmer en fonction de vos besoins.

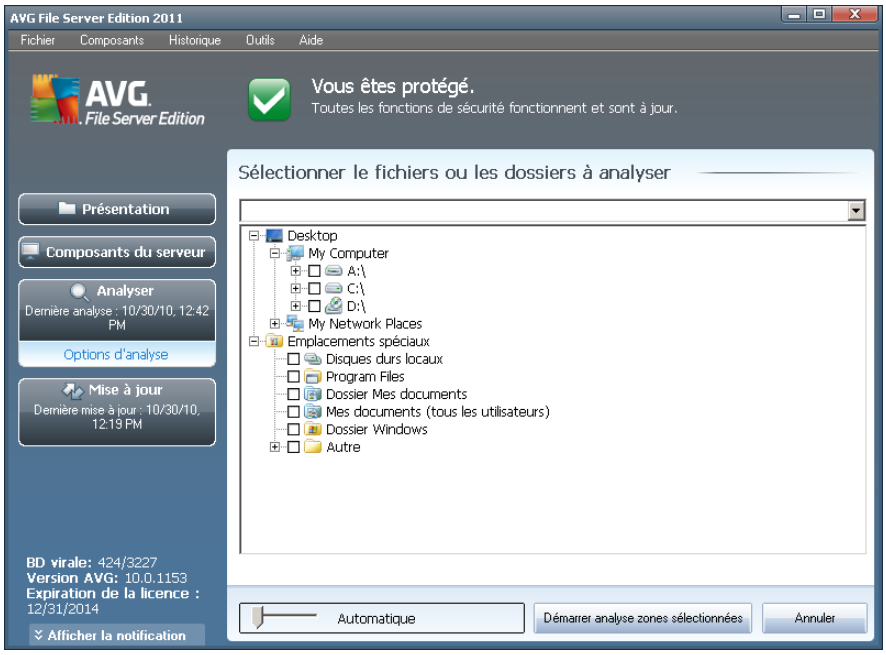
Lancement de l'analyse

L'***'Analyse zones sélectionnées***peut être lancée directement depuis l'interface d'analyse en cliquant sur l'icône correspondante. La boîte de dialogue ***Sélectionner les fichiers ou les dossiers à examiner*** s'ouvre. Dans l'arborescence de votre ordinateur, sélectionnez les dossiers que vous souhaitez analyser. Le chemin d'accès à chaque dossier sélectionné est généré automatiquement et apparaît dans la zone de texte située dans la partie supérieure de la boîte de dialogue.

Il est aussi possible d'analyser un dossier spécifique et d'exclure tous ses sous-dossiers du processus. Pour ce faire, il suffit d'insérer le signe moins "**-**" avant le

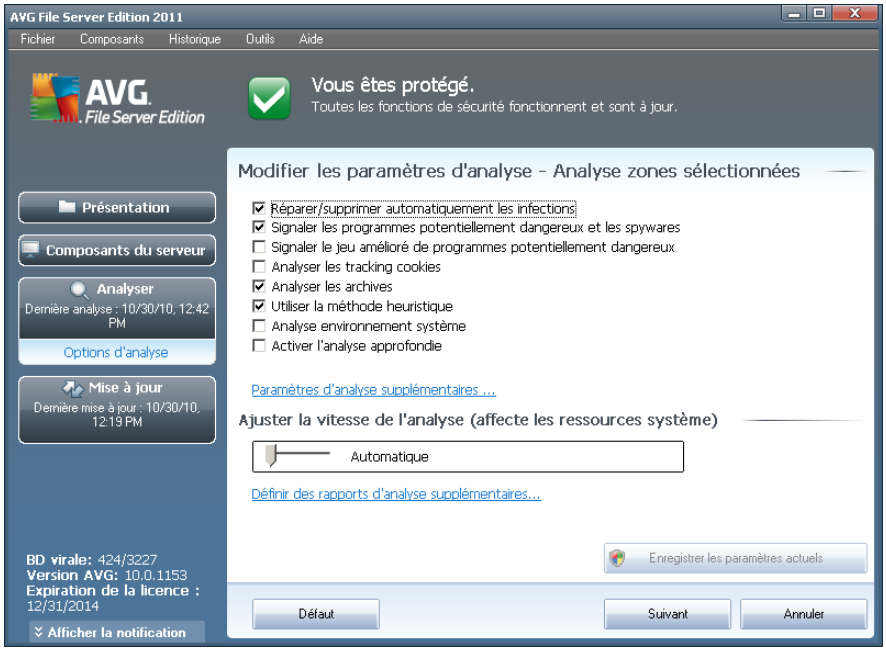
chemin d'accès généré automatiquement (*voir la capture d'écran*). Pour exclure un dossier complet de l'analyse, utilisez le paramètre « ! ».

Pour lancer l'analyse, cliquez sur le bouton ***Démarrer l'analyse*** ; le processus est fondamentalement identique à celui de l'analyse complète de l'ordinateur.



Modification de la configuration de l'analyse

Vous pouvez modifier les paramètres prédéfinis par défaut de l'option ***Analyser des fichiers ou des dossiers spécifiques***. Activez le lien ***Modifier les paramètres d'analyse*** pour accéder à la boîte de dialogue ***Modifier les paramètres d'analyse - Analyse de fichiers ou dossiers spécifiques***. ***Il est recommandé de conserver les paramètres par défaut et de ne les modifier qu'en cas d'absolue nécessité.***



- ***Paramètres d'analyse*** - dans la liste des paramètres d'analyse, vous pouvez activer/désactiver des paramètres spécifiques en fonction de vos besoins :

  - ***Réparer/supprimer automatiquement les infections*** (*option activée par défaut*) : lorsqu'un virus est détecté au cours de l'analyse, il est réparé automatiquement dans la mesure du possible. S'il est impossible de réparer automatiquement le fichier infecté, il sera placé en ***quarantaine***.

  - ***Signaler les programmes potentiellement dangereux et les spywares*** (*option activée par défaut*) : cochez cette case pour activer le moteur ***Anti-spyware*** et rechercher les spywares et les virus. Les spywares désignent une catégorie de codes suspects : même s'ils représentent généralement un risque pour la sécurité, certains de ces programmes peuvent être installés intentionnellement par l'utilisateur. Nous vous recommandons de laisser cette fonction activée car elle augmente de manière significative la sécurité de votre système.

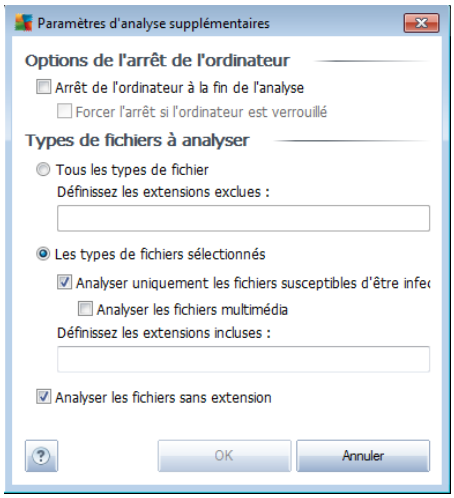
  - ***Signaler le jeu amélioré de programmes potentiellement dangereux*** - *(option désactivée par défaut*) : permet de détecter le jeu étendu des spywares qui ne posent aucun problème et sont sans danger dès lors qu'ils sont achetés directement auprès de leur éditeur, mais qui peuvent ensuite être utilisées à des fins malveillantes. Il s'agit d'une mesure de sécurité supplémentaire. Cependant, elle peut bloquer des programmes légitimes de l'ordinateur ; c'est pourquoi elle est désactivée par défaut.

  - ***Analyser les tracking cookies*** (*option désactivée par défaut*) : ce paramètre du composant ***Anti-Spyware*** définit les cookies qui pourront être détectés au cours de l'analyse (*les cookies HTTP servent à authentifier, à suivre et à gérer certaines informations sur les utilisateurs comme leurs préférences en matière de navigation ou le*

contenu de leur panier d'achat électronique).

- ***Analyser les archives*** (*option désactivée par défaut*) : ce paramètre indique que l'analyse examine tous les fichiers même ceux stockés dans des d'archives (archives ZIP, RAR, par exemple).
- ***Utiliser la méthode heuristique*** (*option désactivée par défaut*) : l'analyse heuristique (*émulation dynamique des instructions de l'objet analysé dans un environnement informatique virtuel*) est l'une des méthodes employées pour détecter des virus pendant l'analyse.
- ***Analyse environnement système*** (*option désactivée par défaut*) : l'analyse vérifie les fichiers système de l'ordinateur.
- ***Activer l'analyse approfondie*** (*option désactivée par défaut*) - dans certains cas (*suspicion d'une infection de l'ordinateur*), vous pouvez cocher cette option pour exécuter des algorithmes d'analyse très pointus même, s'il est peu probable que certaines zones de l'ordinateur soient infectées. Gardez à l'esprit que cette méthode prend énormément de temps.

- ***Paramètres d'analyse supplémentaires*** - ce lien ouvre une nouvelle boîte de dialogue ***Paramètres d'analyse supplémentaires*** permettant de spécifier les paramètres suivants :



- ***Options de l'arrêt de l'ordinateur*** - indiquez si l'ordinateur doit être arrêté automatiquement à la fin du processus d'analyse. Si l'option ***Arrêt de l'ordinateur à la fin de l'analyse*** est activée, l'option ***Forcer l'arrêt si l'ordinateur est verrouillé*** devient disponible et permet d'arrêter l'ordinateur même s'il est verrouillé.
- ***Définir les types de fichiers à analyser*** - vous devez également choisir d'analyser :
  - ***Tous les types de fichier*** avec la possibilité de définir les éléments à

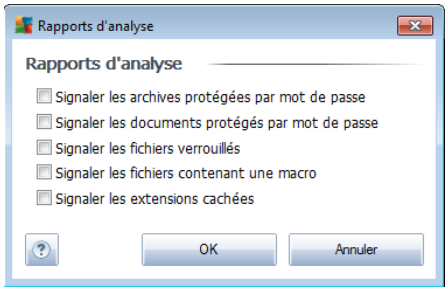
exclure de l'analyse en répertoriant les extensions de fichiers (séparées par des virgules) à ne pas analyser ; ou les

- ***Types de fichier sélectionnés*** - vous pouvez choisir d'analyser uniquement les fichiers susceptibles d'être infectés (*les fichiers qui ne peuvent faire l'objet d'une infection ne sont pas analysés ; il s'agit par exemple de fichiers en texte brut ou de certains types de fichier non exécutables*), y compris les fichiers multimédia (*vidéo, audio - si vous ne sélectionnez pas cette option, la durée de l'analyse sera considérablement réduite, car ce sont souvent de gros fichiers qui sont rarement infectés par un virus*). En fonction des extensions, vous pouvez également spécifier les fichiers qui doivent toujours faire l'objet d'une analyse.

- Vous pouvez également choisir l'option ***Analyser les fichiers sans extension*** - cette option est activée par défaut et il est recommandé de la conserver et de ne la modifier qu'en cas d'absolue nécessité. Les fichiers sans extension sont relativement suspects et doivent toujours faire l'objet d'une analyse.

- ***Priorité du processus d'analyse*** - le curseur vous permet de modifier la priorité du processus d'analyse. Par défaut, elle est fixée sur *Automatique*, niveau qui optimise le processus d'analyse et l'utilisation des ressources système. Vous pouvez aussi choisir le processus d'analyse lent, qui réduit la charge sur les ressources système (*cette option est pratique quand vous devez travailler sur l'ordinateur sans avoir à vous soucier de la durée de l'analyse)*) ; ou rapide, qui utilise plus de ressources système (*convient notamment lorsque vous quittez temporairement votre poste de travail*).

- ***Définir des rapports d'analyse supplémentaires*** - ce lien ouvre la boîte de dialogue ***Rapports d'analyse*** où vous pouvez sélectionner les types de résultats que vous souhaitez obtenir :



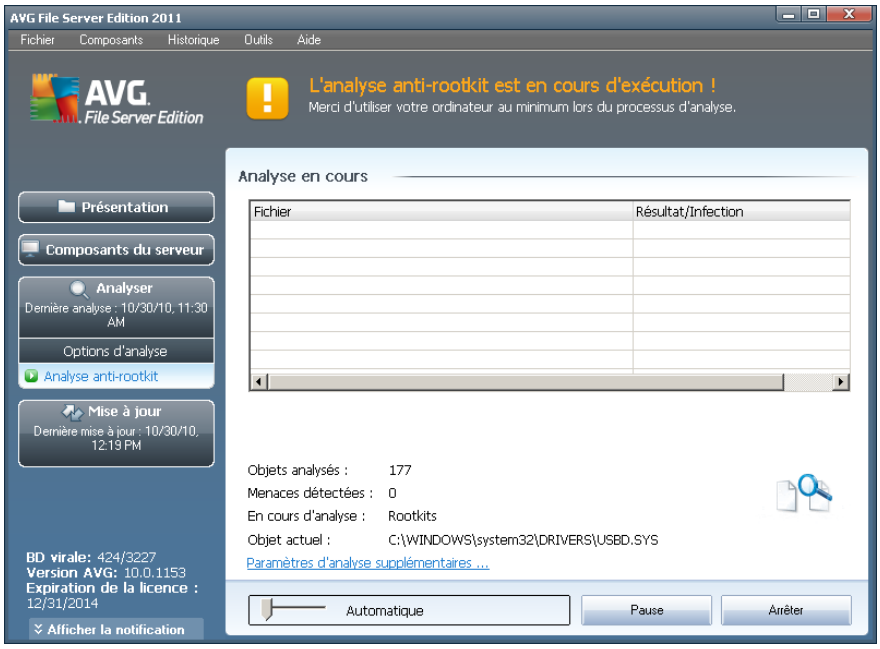
Avertissement : *ces paramètres d'analyse sont identiques à ceux d'une nouvelle analyse, comme indiqué dans le chapitre* ***Analyse AVG / Programmation de l'analyse / Comment faire l'analyse****. Si vous décidez de modifier la configuration* ***Analyse zones sélectionnées*** *par défaut, vous pouvez enregistrer les paramètres modifiés en tant que configuration par défaut et les appliquer aux analyses ultérieures de fichiers ou de dossiers spécifiques. De plus, cette configuration sera utilisée comme modèle des nouvelles analyses programmées (toutes les analyses personnalisées basées sur la configuration actuelle de l'analyse des fichiers ou dossiers spécifiques).*

12.2.3. Analyse Anti-Rootkit

L'analyse anti-rootkit permet de vérifier si votre ordinateur contient des rootkits (*programmes et technologies destinés à cacher l'activité de programmes malveillants sur l'ordinateur*). Si un rootkit est détecté, cela ne veut pas forcément dire que votre ordinateur est infecté. Dans certains cas, des pilotes spécifiques ou des sections d'applications régulières peuvent être considérés, à tort, comme des rootkits.

Lancement de l'analyse

L'analyse anti-rootkit peut être exécutée directement depuis l'interface d'analyse en cliquant sur l'icône d'analyse. Pour ce type d'analyse, il n'est pas nécessaire de configurer d'autres paramètres spécifiques. L'analyse démarre immédiatement dans la boîte de dialogue ***Analyse en cours*** (*voir la capture d'écran*). L'analyse peut être interrompue provisoirement (***Interrompre***) ou annulée (***Arrêter***) si nécessaire.



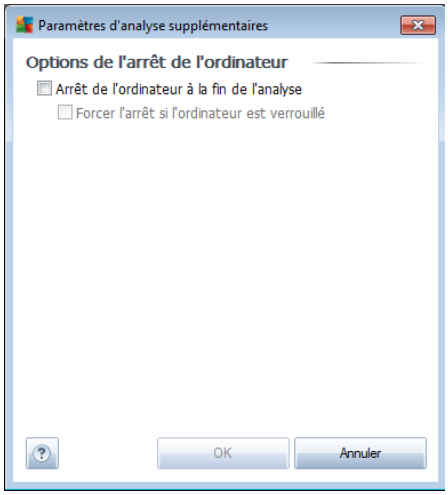
Modification de la configuration de l'analyse

L'analyse anti-rootkit est toujours exécutée avec les paramètres par défaut et les paramètres d'analyse ne peuvent être modifiés que dans la boîte de dialogue ***Paramètres avancés d'AVG / Anti-Rootkit***. Dans l'interface d'analyse, la configuration suivante est disponible, mais uniquement lorsqu'une analyse est en cours :

- ***Analyse automatique*** - le curseur vous permet de modifier la priorité du processus d'analyse. Par défaut, le niveau de priorité attribué est moyen (*Analyse automatique*), qui applique le meilleur compromis entre le processus d'analyse et l'utilisation des ressources système. Vous pouvez aussi choisir le

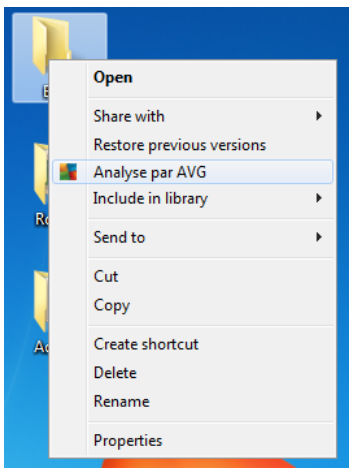
processus d'analyse lent, qui réduit la charge sur les ressources système (*cette option est pratique quand vous devez travailler sur l'ordinateur sans avoir à vous soucier de la durée de l'analyse)*) ; ou rapide, qui utilise plus de ressources système (*convient notamment lorsque vous quittez temporairement votre poste de travail*).

- ***Paramètres d'analyse supplémentaires*** - ce lien ouvre une nouvelle boîte de dialogue ***Paramètres d'analyse supplémentaires*** où vous pouvez définir les conditions de l'arrêt de l'ordinateur relatives à l'***analyse anti-rootkit*** (***Arrêt de l'ordinateur à la fin de l'analyse*** *ou éventuellement* ***Forcer l'arrêt si l'ordinateur est verrouillé***) :



12.3. Analyse contextuelle

Outre les analyses prédéfinies exécutées sur l'ensemble ou des zones sélectionnées de l'ordinateur, **AVG 2011 Edition Serveur de Fichiers** offre la possibilité d'examiner rapidement l'objet de votre choix dans l'environnement de l'Explorateur Windows. Si vous désirez ouvrir un fichier inconnu dont le contenu est incertain, vous pouvez le vérifier à la demande. Procédez comme suit :



- Dans l'Explorateur Windows, mettez le fichier (ou le dossier) en surbrillance
- Cliquez avec le bouton droit de la souris sur l'objet pour afficher le menu contextuel
- Choisissez la commande ***Analyse par AVG*** pour faire analyser le fichier par AVG

12.4. Analyse depuis la ligne de commande

Dans **AVG 2011 Edition Serveur de Fichiers**, il est possible de lancer l'analyse depuis la ligne de commande. Vous apprécierez cette possibilité sur les serveurs, par exemple, ou lors de la création d'un script de commandes qui doit s'exécuter automatiquement après l'initialisation de l'ordinateur. La plupart des paramètres proposés dans l'interface utilisateur graphique sont disponibles à partir de la ligne de commande.

Pour lancer l'analyse AVG en ligne de commande, exécutez la commande suivante depuis le dossier où AVG est installé :

- ***avgscanx*** pour un système d'exploitation 32 bits
- ***avgscana*** pour un système d'exploitation 64 bits

Syntaxe de la commande

La syntaxe de la commande est la suivante :

- ***avgscanx /paramètre***... par exemple, ***avgscanx /comp*** pour l'analyse complète de l'ordinateur
- ***avgscanx /paramètre /paramètre*** si plusieurs paramètres sont précisés, les entrer à la suite, séparés par un espace et une barre oblique
- si un paramètre requiert la saisie de valeurs spécifiques (par exemple, le paramètre ***/scan*** requiert de savoir quelles zones de votre ordinateur ont été sélectionnées afin d'être analysées et vous devez indiquer un chemin exact vers la section sélectionnée), il faut séparer les valeurs éventuelles par un point-virgule, par exemple : ***avgscanx /scan=C:\;D:***

Paramètres d'analyse

Pour afficher la liste complète des paramètres disponibles, tapez la commande concernée ainsi que le paramètre /? ou /HELP (ex : ***avgscanx /?***). Le seul paramètre obligatoire est /SCAN pour lequel il est nécessaire de spécifier les zones de l'ordinateur à analyser. Pour une description détaillée des options, voir la liste des paramètres de ligne de commande.

Pour exécuter l'analyse, appuyez sur ***Entrée***. Pendant l'analyse, vous pouvez arrêter le processus en appuyant sur ***Ctrl+C*** ou ***Ctrl+Pause***.

Analyse CMD lancée depuis l'interface d'analyse

Lorsque vous démarrez l'ordinateur en mode sans échec, il est également possible de faire appel à la ligne de commande à partir de l'interface utilisateur graphique. L'analyse à proprement parler sera lancée à partir de la ligne de commande, la boîte de dialogue ***Editeur de ligne de commande*** permet seulement de préciser la plupart des paramètres d'analyse dans l'interface graphique plus conviviale.

Etant donné que cette boîte de dialogue n'est accessible qu'en mode sans échec, consultez le fichier d'aide accessible à partir de cette boîte de dialogue si vous avez besoin de renseignements supplémentaires.

12.4.1. Paramètres d'analyse CMD

Vous trouverez ci-après la liste de tous les paramètres disponibles pour lancer une analyse depuis la ligne de commande :

- ***/SCAN*** Analyse de fichiers ou de dossiers spécifiques / SCAN=chemin;chemin (ex. : /SCAN=C:\;D:\)
- ***/COMP*** Analyse complète de l'ordinateur
- ***/HEUR*** Utiliser l'analyse heuristique
- ***/EXCLUDE*** Fichiers ou chemin exclus de l'analyse
- ***/@*** Fichier de commande /nom du fichier/
- ***/EXT*** Analyser ces extensions /par exemple EXT=EXE,DLL/
- ***/NOEXT*** Ne pas analyser ces extensions /par exemple NOEXT=JPG/
- ***/ARC*** Analyser les archives
- ***/CLEAN*** Nettoyer automatiquement
- ***/TRASH*** Mettre les fichiers en Quarantaine
- ***/QT*** Analyse rapide
- ***/MACROW*** Signaler les macros
- ***/PWDW*** Signaler les fichiers protégés par un mot de passe
- ***/IGNLOCKED*** Ignorer les fichiers verrouillés
- ***/REPORT*** Reporter dans le fichier /nom du fichier/
- ***/REPAPPEND*** Inclure dans le fichier de rapport

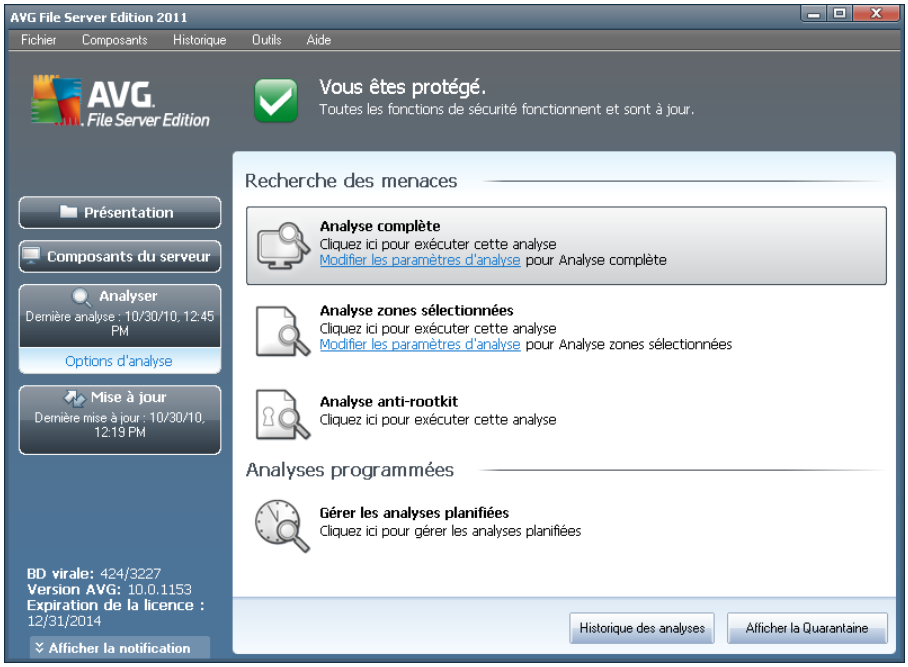
- ***/REPOK*** Avertir l'utilisateur des fichiers non infectés
- ***/NOBREAK*** Ne pas autoriser CTRL-PAUSE pour arrêter
- ***/BOOT*** Activer la vérification MBR/BOOT
- ***/PROC*** Analyser les processus actifs
- ***/PUP*** Signaler les "programmes potentiellement dangereux"
- ***/REG*** Analyser la base de registre
- ***/COO*** Analyser les cookies
- ***/?*** Affichage de l'aide sur un sujet
- ***/HELP*** Affichage de la rubrique d'aide en rapport avec l'élément actuellement sélectionné ou affiché
- ***/PRIORITY*** Définir la priorité de l'analyse /Faible, Auto, Elevée (voir Paramètres avancés / Analyses)
- ***/SHUTDOWN*** Arrêt de l'ordinateur à la fin de l'analyse
- ***/FORCESHUTDOWN*** Forcer l'arrêt de l'ordinateur à la fin de l'analyse
- ***/ADS*** Analyser les flux de données NTFS uniquement
- ***/ARCBOMBSW*** Signaler les fichiers archives compressées à plusieurs reprises

12.5. Programmation de l'analyse

Avec **AVG 2011 Edition Serveur de Fichiers**, vous pouvez effectuer une analyse à la demande (par exemple, lorsque vous soupçonnez qu'un virus s'est infiltré dans l'ordinateur) ou selon un programme prévu. Il est vivement recommandé d'exécuter des analyses planifiées. Vous serez ainsi assuré que votre ordinateur sera protégé de tout risque d'infection et vous n'aurez plus à vous soucier de la gestion des analyses.

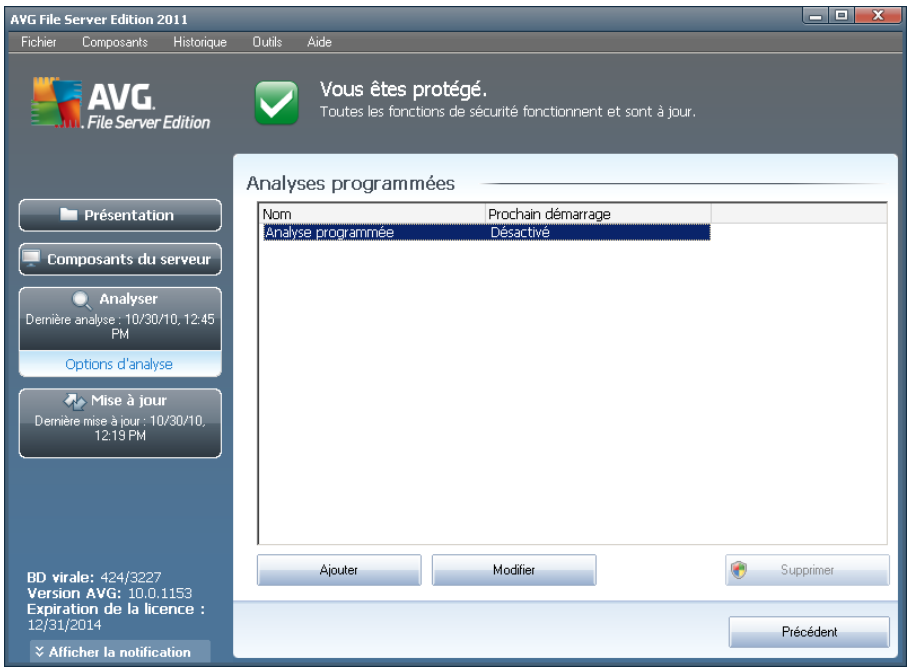
Il est possible d'effectuer une ***analyse complète*** régulièrement, c'est-à-dire une fois par semaine au moins. Si possible, faites aussi une analyse complète l'ordinateur une fois par jour, comme configuré par défaut dans la programmation de l'analyse. Si l'ordinateur est toujours sous tension, vous pouvez programmer l'analyse en dehors de vos heures de travail. Si l'ordinateur est parfois hors tension, programmez une analyse au démarrage de l'ordinateur lorsqu'elle n'a pas pu être effectuée.

Pour créer de nouvelles programmations d'analyse, consultez l'interface d'analyse AVG, dans la section du bas, ***Analyses programmées*** :



Analyses programmées

Cliquez sur l'icône située dans la section ***Analyses programmées*** pour ouvrir une nouvelle boîte de dialogue ***Analyses programmées*** présentant une liste de toutes les analyses programmées actuellement :



Vous pouvez modifier / ajouter des analyses à l'aide des boutons de commande

suivants :

- ***Ajouter*** - le bouton ouvre la boîte de dialogue ***Paramètres de l'analyse programmée***, onglet ***Paramètres de la programmation***. Dans cette boîte de dialogue, définissez les paramètres de la nouvelle analyse.

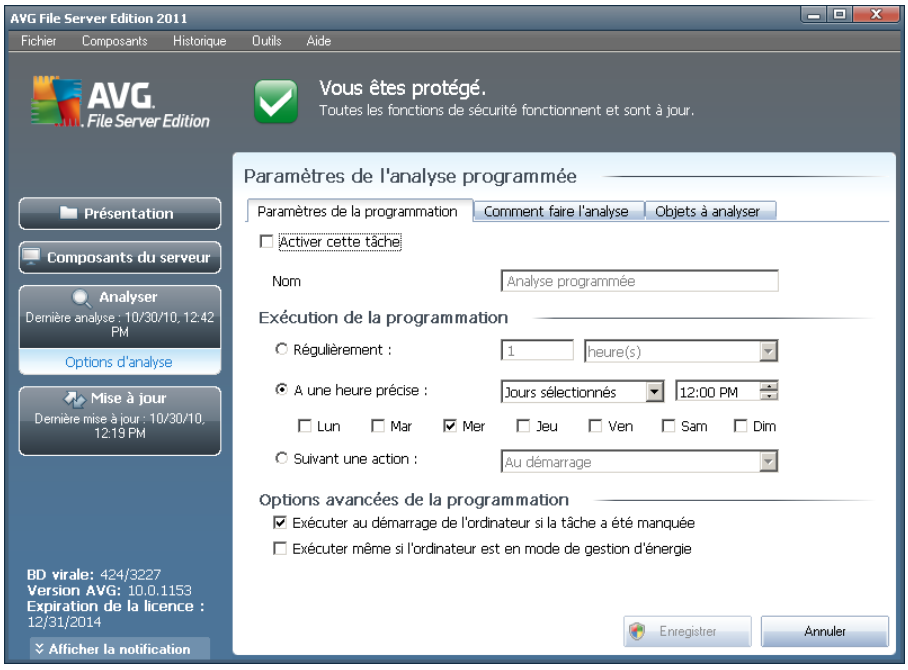
- ***Modifier*** - ce bouton n'est actif que si vous avez déjà sélectionné une analyse existante dans la liste des analyses programmées. Dans ce cas, le bouton est accessible ; il suffit de cliquer dessus pour accéder à la boîte de dialogue ***Paramètres de l'analyse programmée***, onglet ***Paramètres de la programmation***. Les paramètres de l'analyse sélectionnée sont pré-renseignés et peuvent être modifiés.

- ***Supprimer*** - ce bouton est actif si vous avez déjà sélectionné une analyse existante dans la liste des analyses programmées. Cette analyse peut ensuite être supprimée de la liste en cliquant sur ce bouton. Notez néanmoins que vous ne pouvez supprimer que vos propres analyses. Les analyses de type ***Programmation de l'analyse complète de l'ordinateur*** prédéfinies par défaut ne peuvent jamais être supprimées.

- ***Précédent*** - permet de revenir à l'interface d'analyse d'AVG

12.5.1. Paramètres de la programmation

Pour programmer une nouvelle analyse et définir son exécution régulière, ouvrez la boîte de dialogue ***Paramètres de l'analyse programmée*** (*cliquez sur le bouton* ***Ajouter une analyse programmée*** *situé dans la boîte de dialogue* ***Analyses programmées***). Cette boîte de dialogue comporte trois onglets : ***Paramètres de la programmation*** - *voir l'illustration ci-dessous* (*il s'agit de l'onglet qui s'affiche par défaut à l'ouverture de la boîte de dialogue*), ***et*** et ***Objets à analyser***.



Dans l'onglet ***Paramètres de la programmation***, vous pouvez cocher/désélectionner la case ***Activer cette tâche*** pour désactiver temporairement l'analyse programmée et le réactiver au moment opportun.

Donnez ensuite un nom à l'analyse que vous voulez créer et programmer. Saisissez le nom dans la zone de texte en regard de l'option ***Nom***. Veillez à utiliser des noms courts, descriptifs et appropriés pour distinguer facilement les différentes analyses par la suite.

Exemple : *il n'est pas judicieux d'appeler l'analyse "Nouvelle analyse" ou "Mon analyse", car ces noms ne font pas référence au champ réel de l'analyse. A l'inverse, "Analyse des zones système" est un nom descriptif précis. Il est également nécessaire de spécifier dans le nom de l'analyse si l'analyse concerne l'ensemble de l'ordinateur ou une sélection de fichiers ou de dossiers. Notez que les analyses personnalisées sont toujours basées sur l'Analyse zones sélectionnés.*

Dans cette boîte de dialogue, vous définissez plus précisément les paramètres de l'analyse :

- ***Exécution de la programmation*** - spécifiez l'intervalle entre chaque exécution de la nouvelle analyse. Il est possible de répéter le lancement de l'analyse après un laps de temps donné (***Régulièrement***), d'en définir la date et l'heure précises (***A une heure précise***) ou encore d'indiquer l'évènement auquel sera associé le lancement de l'analyse (***Suivant une action***).

- ***Options avancées de la programmation*** - cette section permet de définir dans quelles conditions l'analyse doit ou ne doit pas être exécutée si l'ordinateur est en mode d'économie d'énergie ou hors tension.

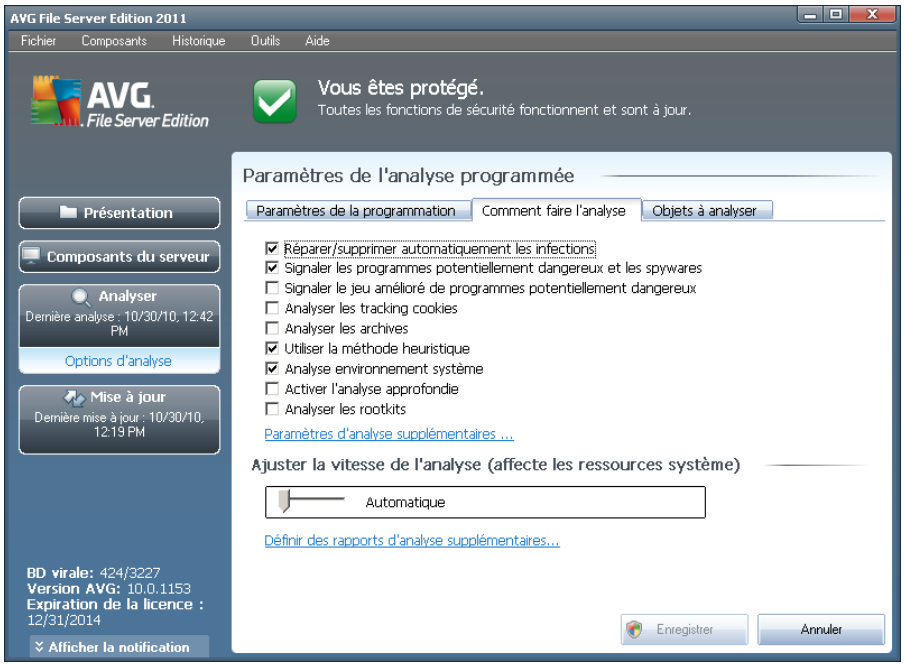
Boutons de commande de la boîte de dialogue Paramètres de l'analyse programmée

Deux boutons de commande figurent sur les trois onglets de la boîte de dialogue ***Paramètres de l'analyse programmée*** (***Paramètres de la programmation***, ***Comment faire l'analyse*** et ***Objets à analyser***). Ils ont la même fonctionnalité :

- ***Enregistrer*** - enregistre toutes les modifications entrées sous l'onglet en cours ou un autre onglet de cette boîte de dialogue et affiche la boîte de dialogue par défaut de l'interface d'analyse AVG. Par conséquent, si vous voulez configurer les paramètres d'analyse répartis sous tous les onglets, cliquez sur ce bouton uniquement après avoir défini tous vos choix.

- ***Annuler*** - annule toutes les modifications entrées sous l'onglet actif ou un autre onglet de cette boîte de dialogue et affiche la boîte de dialogue par défaut de l'interface d'analyse AVG.

12.5.2. Comment faire l'analyse



Dans l'onglet ***Comment faire l'analyse***, vous trouverez la liste des paramètres d'analyse qui peuvent être activés ou désactivés. Par défaut, la plupart des paramètres sont activés et appliqués lors de l'analyse. Aussi est-il recommandé de ne pas modifier la configuration prédéfinie d'AVG sans motif valable.

- ***Réparer/supprimer automatiquement les infections*** (*option activée par défaut*) : lorsqu'un virus est détecté au cours de l'analyse, il est réparé automatiquement dans la mesure du possible. Si la désinfection automatique du fichier n'est pas possible (ou si cette option est désactivée), un message de détection de virus s'affiche. Il vous appartient alors de déterminer le traitement à appliquer à l'infection. L'action recommandée consiste à confiner le fichier infecté en ***quarantaine***.

- ***Signaler les programmes potentiellement dangereux et les spywares*** (*activé par défaut*) : cochez cette case pour activer le moteur ***Anti-spyware*** et rechercher les spywares et les virus. Les spywares désignent une catégorie de codes suspects : même s'ils représentent généralement un risque pour la sécurité, certains de ces programmes peuvent être installés intentionnellement par l'utilisateur. Nous vous recommandons de laisser cette fonction activée car elle augmente de manière significative la sécurité de votre système.

- ***Signaler le jeu amélioré de programmes potentiellement dangereux*** (*option désactivée par défaut*) : permet de détecter le jeu étendu des spywares*** qui ne posent aucun problème et sont sans danger dès lors qu'ils sont achetés directement auprès de leur éditeur, mais qui peuvent ensuite être utilisées à des fins malveillantes. Il s'agit d'une mesure de sécurité supplémentaire. Cependant, elle peut bloquer des programmes légitimes de

l'ordinateur ; c'est pourquoi elle est désactivée par défaut.

- ***Analyser les tracking cookies*** (*option désactivée par défaut*) : ce paramètre du composant ***Anti-Spyware*** indique que les cookies devront être détectés au cours de l'analyse (*les cookies HTTP servent à authentifier, à suivre et à gérer certaines informations sur les utilisateurs comme leurs préférences en matière de navigation ou le contenu de leur panier d'achat électronique*).

- ***Analyser les archives*** (*option désactivée par défaut*) :ce paramètre indique que l'analyse doit examiner tous les fichiers, même ceux comprimés dans certains types d'archives (archives ZIP ou RAR, par exemple).

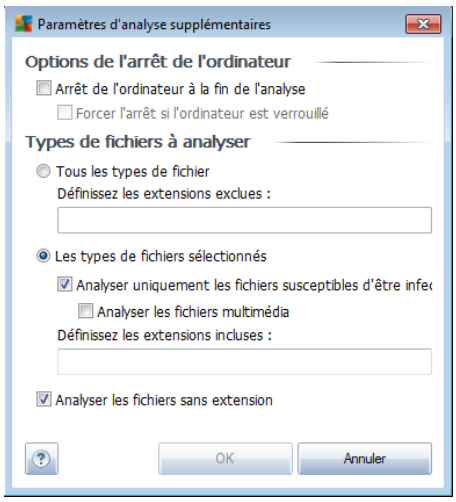
- ***Utiliser la méthode heuristique*** (*option activée par défaut*) : l'analyse heuristique (*émulation dynamique des instructions de l'objet analysé dans un environnement informatique virtuel*) est l'une des méthodes employées pour détecter des virus pendant l'analyse.

- ***Analyse environnement système*** (*option activée par défaut*) : l'analyse vérifie les fichiers système de l'ordinateur.

- ***Activer l'analyse approfondie*** (*option désactivée par défaut*) - dans certains cas (*suspicion d'une infection de l'ordinateur*), vous pouvez cocher cette option pour exécuter des algorithmes d'analyse très pointus même s'il est peu probable que certaines zones de l'ordinateur soient infectées. Gardez à l'esprit que cette méthode prend énormément de temps.

Ensuite, vous pouvez modifier les paramètres de l'analyse en procédant comme suit :

- ***Paramètres d'analyse supplémentaires*** - ce lien ouvre une nouvelle boîte de dialogue ***Paramètres d'analyse supplémentaires*** permettant de spécifier les paramètres suivants :

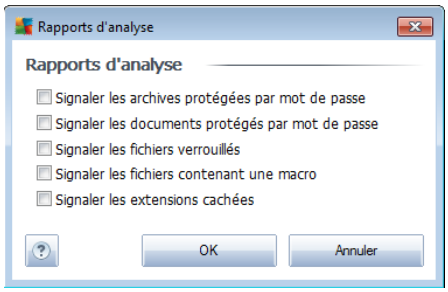


  - ***Options de l'arrêt de l'ordinateur*** - indiquez si l'ordinateur doit être arrêté automatiquement à la fin du processus d'analyse. Si l'option ***Arrêt de l'ordinateur à la fin de l'analyse*** est activée, l'option ***Forcer l'arrêt***

si l'ordinateur est verrouillé devient disponible et permet d'arrêter l'ordinateur même s'il est verrouillé.

- ***Définir les types de fichiers à analyser*** - vous devez également choisir d'analyser :
  - ***Tous les types de fichier*** avec la possibilité de définir les éléments à exclure de l'analyse en répertoriant les extensions de fichiers (séparées par des virgules) à ne pas analyser ; ou les;
  - ***Les types de fichiers sélectionnés*** - vous pouvez choisir d'analyser uniquement les fichiers susceptibles d'être infectés (*les fichiers qui ne peuvent faire l'objet d'une infection ne sont pas analysés ; il s'agit par exemple de fichiers en texte brut ou de certains types de fichier non exécutables*), y compris les fichiers multimédia (*vidéo, audio - si vous ne sélectionnez pas cette option, la durée de l'analyse sera considérablement réduite, car ce sont souvent de gros fichiers qui sont rarement infectés par un virus*). En fonction des extensions, vous pouvez également spécifier les fichiers qui doivent toujours faire l'objet d'une analyse.
  - Vous pouvez également choisir l'option ***Analyser les fichiers sans extension*** - cette option est activée par défaut et il est recommandé de la conserver et de ne la modifier qu'en cas d'absolue nécessité. Les fichiers sans extension sont relativement suspects et doivent toujours faire l'objet d'une analyse.

- ***Ajuster la vitesse de l'analyse*** - le curseur vous permet de modifier la priorité du processus d'analyse. Le niveau intermédiaire est le meilleur compromis entre vitesse d'analyse et utilisation des ressources système. Vous pouvez aussi choisir le processus d'analyse lent, qui réduit la charge sur les ressources système (*cette option est pratique quand vous devez travailler sur l'ordinateur sans avoir à vous soucier de la durée de l'analyse)*) ; ou rapide, qui utilise plus de ressources système (*convient notamment lorsque vous quittez temporairement votre poste de travail*).
- ***Définir des rapports d'analyse supplémentaires*** - ce lien ouvre une nouvelle boîte de dialogue ***Rapports d'analyse***, dans laquelle vous pouvez sélectionner les types de résultats que vous souhaitez obtenir :



Remarque :*par défaut, l'analyse est configurée pour bénéficier de performances*

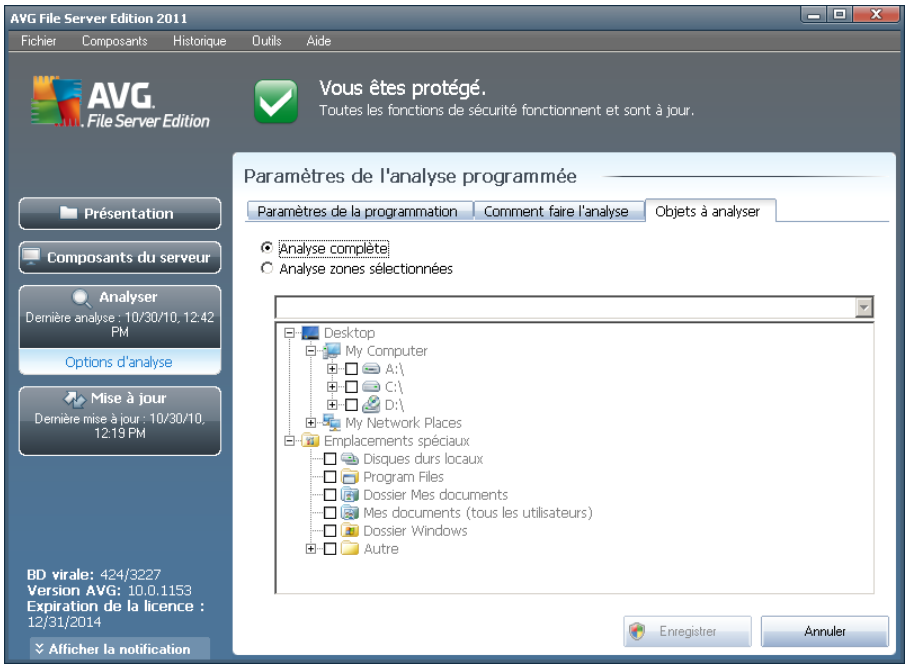
optimales. Sauf raison valable, il est fortement conseillé de conserver la configuration telle qu'elle est prédéfinie. Seuls les utilisateurs expérimentés peuvent modifier la configuration. Pour accéder à d'autres options de configuration de l'analyse, consultez la boîte de dialogue ***Paramètres avancés*** *accessible par la commande du menu système* ***Outils/ Paramètres avancés****.*

Boutons de commande

Deux boutons de commande figurent sur les trois onglets de la boîte de dialogue ***Paramètres de l'analyse programmée*** (***Paramètres de la programmation***, ***Paramètres de l'analyse et*** Objets à analyser***). Ils ont la même fonction :

- ***Enregistrer*** - enregistre toutes les modifications entrées sous l'onglet en cours ou un autre onglet de cette boîte de dialogue et affiche la boîte de dialogue par défaut de l'interface d'analyse AVG. Par conséquent, si vous voulez configurer les paramètres d'analyse répartis sous tous les onglets, cliquez sur ce bouton uniquement après avoir défini tous vos choix.
- ***Annuler*** - annule toutes les modifications entrées sous l'onglet actif ou un autre onglet de cette boîte de dialogue et affiche la boîte de dialogue par défaut de l'interface d'analyse AVG.

12.5.3. Objets à analyser



Sous l'onglet ***Objet à analyser***, indiquez si vous voulez programmer l'analyse complète ou l'analyse des zones sélectionnées.

Si vous préférez l'analyse des zones sélectionnées, cela a pour effet d'activer, dans la partie inférieure de la boîte de dialogue, l'arborescence. Vous pouvez alors sélectionner

les dossiers à analyser (*développez les catégories en cliquant sur le signe plus pour voir le dossier souhaité*). Vous pouvez sélectionner plusieurs dossiers en sélectionnant leur case respective. Les dossiers sélectionnés apparaîtront dans la zone de texte en haut de la boîte de dialogue et le menu déroulant conservera l'historique des analyses sélectionnées pour une utilisation ultérieure. *Autre solution, vous pouvez aussi saisir manuellement le chemin complet du dossier souhaité (si vous spécifiez plusieurs chemins, séparez-les par un point-virgule sans espace*).

Dans l'arborescence, vous noterez également la présence d'une entrée ***Emplacements spéciaux***. Voici la liste des emplacements qui seront analysés lorsque la case associée est cochée :

- ***Disques durs locaux*** - tous les disques durs de l'ordinateur
- ***Program Files***
    - C:\Program Files\
    - *dans la version 64 bits* C:\Program Files (x86)
- ***Dossier Mes documents***
    - *Win XP :* C:\Documents and Settings\Utilisateur\Mes Documents\
    - *Windows Vista/7* : C:\Utilisateurs\utilisateur\Documents\
- ***Documents partagés***
    - *Win XP* : C:\Documents and Settings\All Users\Documents\
    - *Windows Vista/7* : C:\Utilisateurs\Public\Documents\
- ***Dossier Windows*** - C:\Windows\
    - ***Autre***
        - *Lecteur système* - le disque dur sur lequel le système d'exploitation est installé (en général, il s'agit de C:)
        - *Dossier système* - C:\Windows\System32\
        - *Dossier Fichiers temporaires* - C:\Documents and Settings\User\Local\ (*Windows XP*) ou C:\Utilisateurs\utilisateur\AppData\Local\Temp\ (*Windows Vista/7*)
        - *Fichiers Internet temporaires* - C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (*Windows XP*) ou C:\Utilisateurs\utilisateur\AppData\Local\Microsoft\Windows\Temporary Internet Files (*Windows Vista/7*)

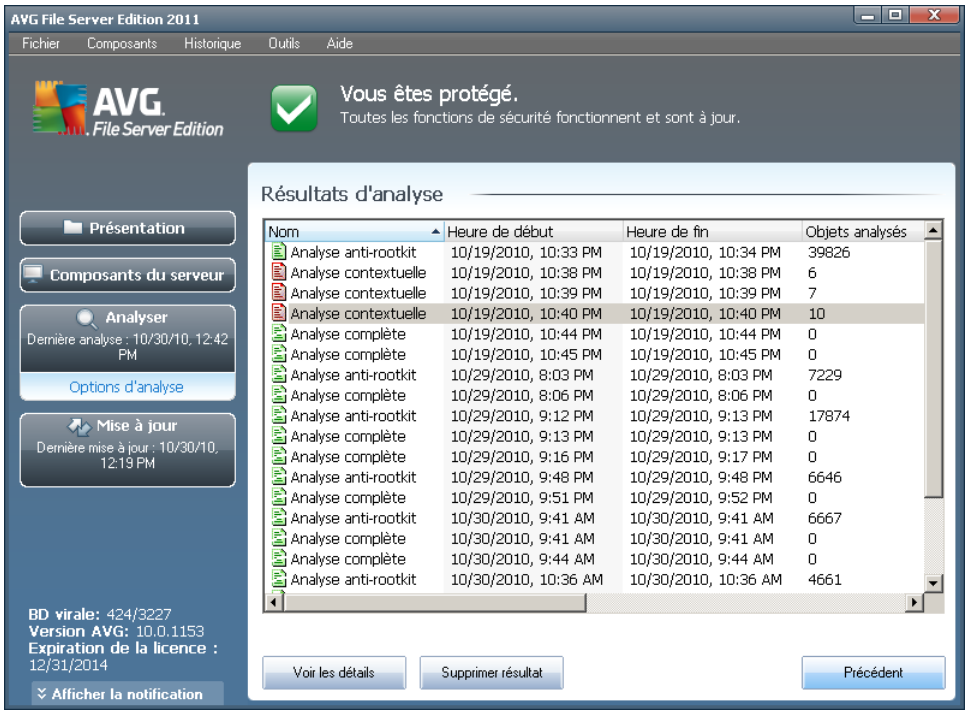
Boutons de commande de la boîte de dialogue Paramètres de l'analyse programmée

Deux boutons de commande figurent sur les trois onglets de la boîte de dialogue ***Paramètres de l'analyse programmée*** (***Paramètres de la programmation***, ***Comment faire l'analyse*** et ***Objets à analyser***). Ils possèdent la même fonctionnalité :

- ***Enregistrer*** - enregistre toutes les modifications entrées sous l'onglet en cours ou un autre onglet de cette boîte de dialogue et affiche la boîte de dialogue par défaut de l'interface d'analyse AVG. Par conséquent, si vous voulez configurer les paramètres d'analyse répartis sous tous les onglets, cliquez sur ce bouton uniquement après avoir défini tous vos choix.

- ***Annuler*** - annule toutes les modifications entrées sous l'onglet actif ou un autre onglet de cette boîte de dialogue et affiche la boîte de dialogue par défaut de l'interface d'analyse AVG.

12.6. Résultats d'analyse



La boîte de dialogue ***Résultats d'analyse*** est accessible depuis l'interface d'analyse AVG via le bouton ***Historique / Résultats des analyses***. Elle contient la liste de toutes les analyses précédemment exécutées ainsi que les informations suivantes sur les résultats :

- ***Nom*** - désignation de l'analyse ; il s'agit soit du nom d'une analyse prédéfinie, soit d'un nom que vous avez attribué à une analyse personnalisée . Chaque

nom inclut une icône indiquant le résultat de l'analyse :

 - une icône de couleur verte signale l'absence d'infection

 - une icône de couleur bleue indique l'absence d'infection, mais la suppression automatique d'un objet infecté

 - une icône de couleur rouge vous alerte sur la présence d'une infection qui a été détectée lors de l'analyse et qui n'a pas pu être traitée.

Les icônes sont entières ou brisées - l'icône entière représente une analyse exécutée et correctement terminée ; l'icône brisée désigne une analyse annulée ou interrompue.

Remarque : *pour plus d'informations sur une analyse, consultez la boîte de dialogue* ***Résultats des analyses****, par le biais du bouton* ***Voir les détails*** *(partie inférieure de la boîte de dialogue).*

- ***Heure de début*** - date et heure d'exécution de l'analyse
- ***Heure de fin*** - date et heure de fin de l'analyse
- ***Objets analysés*** - nombre d'objets qui ont été vérifiés
- ***Infections*** - nombre d'infections détectées / supprimées
- ***Spywares*** - nombre de spywares détectés / supprimés
- ***Avertissements*** - nombre d'objets suspects
- ***Rootkits*** - nombre de rootkits
- ***Informations sur le journal d'analyse*** - informations sur le déroulement de l'analyse et sur les résultats (finalisation ou interruption du processus)

Boutons de commande

Les boutons de contrôle de la boîte de dialogue ***Résultats d'analyse*** sont les suivants :

- ***Voir les détails*** - cliquez sur ce bouton pour ouvrir la boîte de dialogue ***Résultats des analyses*** et examiner les détails de l'analyse sélectionnée
- ***Supprimer résultat*** - cliquez sur ce bouton pour supprimer l'élément sélectionné de la présentation des résultats d'analyse
- ***Précédent*** - permet de revenir à la boîte de dialogue par défaut de l'interface d'analyse AVG

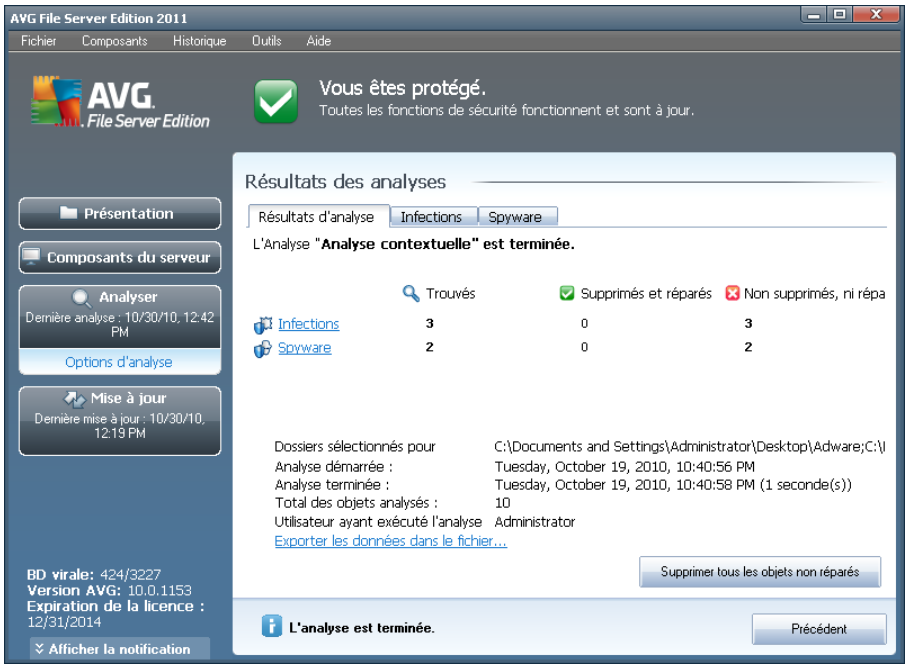
12.7. Détails des résultats d'analyse

Si, dans la boîte de dialogue ***Résultats d'analyse***, une analyse donnée est sélectionnée, cliquer sur le bouton ***Voir les détails*** a pour effet d'afficher la boîte de dialogue ***Résultats des analyses*** fournissant des détails sur la progression et le résultat de cette analyse.

La boîte de dialogue est subdivisée en plusieurs onglets :

- ***Résultats d'analyse*** - l'onglet est toujours affiché et délivre des informations statistiques sur le déroulement de l'analyse
- ***Infections*** - l'onglet s'affiche seulement en cas d'infection virale, détectée lors de l'analyse
- ***Spyware*** - l'onglet s'affiche seulement si un spyware a été trouvé lors de l'analyse
- ***Avertissements*** - l'onglet s'affiche si l'analyse détecte des cookies, par exemple
- ***Rootkits*** - l'onglet s'affiche seulement si un rootkit a été trouvé lors de l'analyse
- ***Informations*** **-** l'onglet s'affiche seulement si certaines menaces potentielles ont été détectées et ne peuvent pas être rangées dans une des catégories mentionnées. Un message d'avertissement lié à l'objet trouvé s'affiche également. Vous trouverez également des informations sur des objets que l'analyse n'a pas réussi à traiter (comme des archives protégées par mot de passe).

12.7.1. Onglet Résultats d'analyse



Sur la page de l'onglet ***Résultats des analyses***, vous trouverez des statistiques détaillées portant sur :

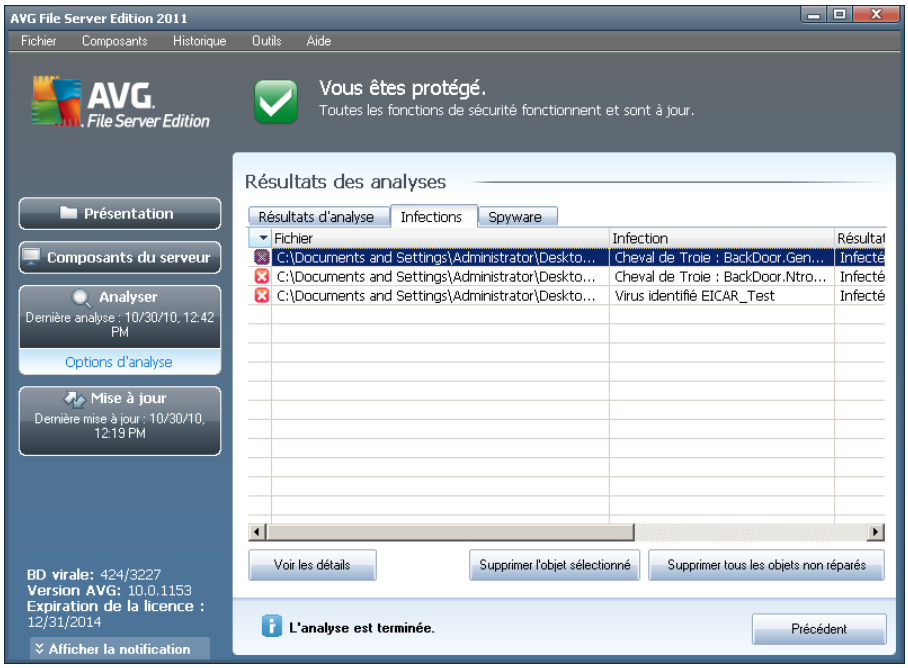
- les infections / spywares détectés
- les infections / spywares supprimés
- le nombre d'infections / de spywares qui n'ont pu être supprimés ou réparés

De plus, l'onglet signale la date et l'heure exactes du début de l'analyse, le nombre total d'objets analysés, la durée de l'analyse et le nombre d'erreurs qui se sont produites au cours de l'analyse.

Boutons de commande

Cette boîte de dialogue comporte un seul bouton de commande. Le bouton ***Fermer résultats***, qui vous renvoie à la boîte de dialogue ***Résultats d'analyse***.

12.7.2. Onglet Infections



L'onglet ***Infections*** apparaît dans la boîte de dialogue ***Résultats des analyses*** seulement si une infection virale est identifiée au cours de l'analyse. L'onglet comporte trois parties contenant les informations suivantes :

- ***Fichier*** - chemin complet vers l'emplacement d'origine de l'objet infecté
- ***Infections*** - nom du virus détecté (*pour plus de détails sur un virus particulier, consultez l'Encyclopédie des virus en ligne*)
- ***Résultat*** - indique l'état actuel de l'objet infecté détecté :
    - ***Infecté*** - l'objet infecté détecté a été laissé à son emplacement d'origine (*si, par exemple, vous avez désactivé l'option de réparation automatique pour une analyse spécifique*)
    - ***Réparé*** - l'objet infecté détecté a été réparé et conservé à son emplacement d'origine
    - ***Placé en quarantaine*** - l'objet infecté a été déplacé en ***Quarantaine***
    - ***Supprimé*** - l'objet infecté a été supprimé
    - ***Ajouté aux exceptions PUP*** - l'objet détecté est considéré comme une exception et est inclus dans la liste des exceptions PUP (*liste configurée dans la boîte de dialogue* ***Exceptions PUP*** *des paramètres avancés*)
    - ***Fichier verrouillé -*** non vérifié - l'objet considéré est verrouillé, AVG ne peut donc pas l'analyser

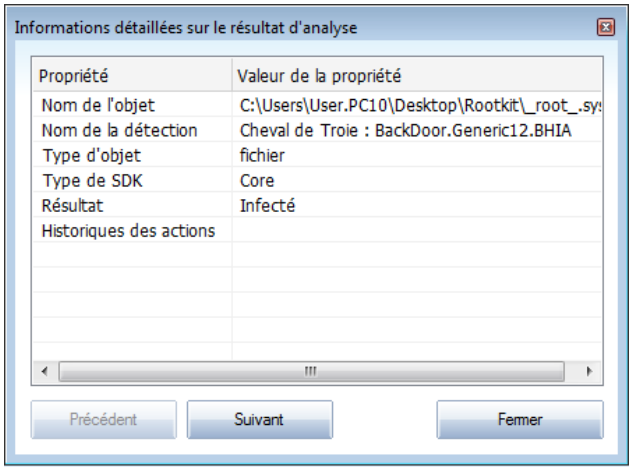
- ***Objet potentiellement dangereux*** - l'objet est considéré comme potentiellement dangereux, mais n'est pas infecté (*il contient par exemple des macros*) ; cette information est fournie à titre d'avertissement uniquement

- ***Un redémarrage de l'ordinateur est nécessaire pour terminer l'opération*** - l'objet infecté ne peut pas être supprimé ; pour ce faire, il faut redémarrer l'ordinateur

Boutons de commande

Cette boîte de dialogue compte trois boutons de commande :

- ***Voir les détails*** - le bouton ouvre la boîte de dialogue des ***informations détaillées sur l'objet*** :



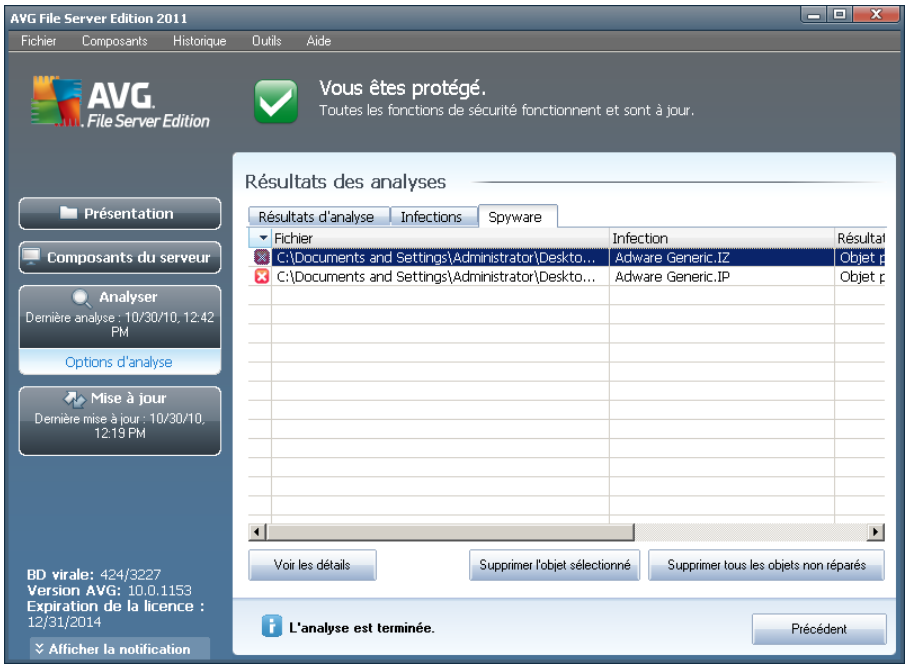
  Dans cette boîte de dialogue, vous trouverez des informations détaillées sur l'objet infectieux détecté (*ex : nom et emplacement de l'objet infecté, type d'objet, type SDK, résultat de la détection et historique des actions liées à l'objet détecté*). Les boutons ***Précédent*** et ***Suivant*** vous donnent accès aux informations sur des résultats spécifiques. Le bouton ***Fermer*** permet de quitter la boîte de dialogue.

- ***Supprimer l'objet sélectionné*** - servez-vous de ce bouton pour mettre les objets trouvés en ***quarantaine***

- ***Supprimer tous les objets non réparés*** - ce bouton supprime tous les objets trouvés qui ne peuvent être désinfectés, ni placés en ***quarantaine***

- ***Fermer résultats*** - met fin aux informations détaillées et renvoie la boîte de dialogue ***Résultats d'analyse***

12.7.3. Onglet Spywares



L'onglet ***Spyware*** apparaît dans la boîte de dialogue ***Résultats des analyses*** seulement si un spyware (ou code espion) a été détecté au cours de l'analyse. L'onglet comporte trois parties contenant les informations suivantes :

- ***Fichier*** - chemin complet vers l'emplacement d'origine de l'objet infecté
- ***Infections*** - nom du spyware détecté (*pour plus de détails sur un virus particulier, consultez l'**Encyclopédie des virus** en ligne*)
- ***Résultat*** - indique l'état actuel de l'objet infecté détecté :
    - ***Infecté*** - l'objet infecté détecté a été laissé à son emplacement d'origine (si, par exemple, vous avez désactivé l'option de réparation automatique pour une analyse spécifique)
    - ***Réparé*** - l'objet infecté détecté a été réparé et conservé à son emplacement d'origine
    - ***Placé en quarantaine*** - l'objet infecté a été déplacé en ***Quarantaine***
    - ***Supprimé*** - l'objet infecté a été supprimé
    - ***Ajouté aux exceptions PUP*** - l'objet détecté est considéré comme une exception et est inclus dans la liste des exceptions PUP (*liste configurée dans la boîte de dialogue **Exceptions PUP** des paramètres avancés*)
    - ***Fichier verrouillé - non vérifié*** - l'objet considéré est verrouillé, AVG ne peut donc pas l'analyser

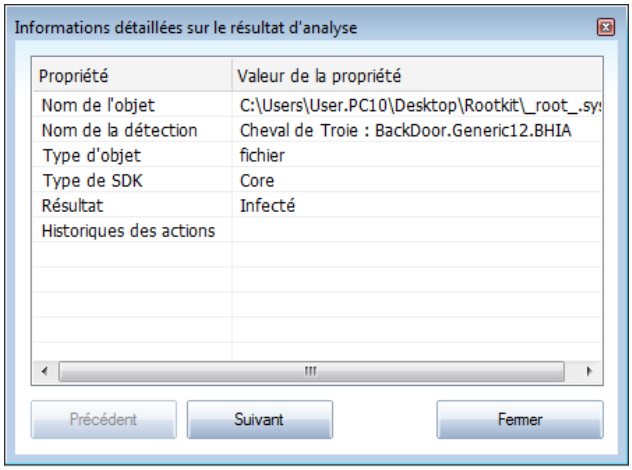
- ***Objet potentiellement dangereux*** - l'objet est considéré comme potentiellement dangereux, mais n'est pas infecté (il contient par exemple des macros) ; cette information est fournie à titre d'avertissement uniquement

- ***Un redémarrage de l'ordinateur est nécessaire pour terminer l'opération*** - l'objet infecté ne peut pas être supprimé ; pour ce faire, il faut redémarrer l'ordinateur

Boutons de commande

Cette boîte de dialogue compte trois boutons de commande :

- ***Voir les détails*** - le bouton ouvre la boîte de dialogue des ***informations détaillées sur l'objet*** :



  Dans cette boîte de dialogue, vous trouverez des informations détaillées sur l'objet infectieux détecté (*ex : nom et emplacement de l'objet infecté, type d'objet, type SDK, résultat de la détection et historique des actions liées à l'objet détecté*). Les boutons ***Précédent*** et ***Suivant*** vous donnent accès aux informations sur des résultats spécifiques. Le bouton ***Fermer*** permet de quitter la boîte de dialogue.

- ***Supprimer l'objet sélectionné*** - servez-vous de ce bouton pour mettre les objets trouvés en ***quarantaine***

- ***Supprimer tous les objets non réparés*** - ce bouton supprime tous les objets trouvés qui ne peuvent être désinfectés, ni placés en ***quarantaine***

- ***Fermer résultats*** - met fin aux informations détaillées et renvoie la boîte de dialogue ***Résultats d'analyse***

12.7.4. Onglet Avertissements

L'onglet ***Avertissements*** affiche des informations sur les objets "suspects" (*généralement des fichiers*) trouvés au cours de l'analyse. Lorsqu'ils sont détectés par le ***Bouclier résident***, l'accès à ces fichiers est bloqué. Voici des exemples types de ce genre d'objets : fichiers masqués, cookies, clés de registre suspectes, documents protégés par un mot de passe, archives, etc. De tels fichiers ne présentent pas de menace directe pour l'ordinateur ou sa sécurité. Les informations relatives à ces fichiers sont généralement utiles lorsque la présence d'adwares ou de spywares est décelée dans votre ordinateur. Se l'analyse AVG ne détecte que des avertissements, aucune action n'est nécessaire.

Cette rubrique décrit brièvement les exemples les plus courants de tels objets :

- ***Fichiers masqués*** - Les fichiers masqués sont, par défaut, non visibles et certains virus ou autres menaces peuvent empêcher leur détection en stockant leurs fichiers avec cet attribut. Si AVG signale un fichier masqué que vous soupçonnez d'être dangereux, vous pouvez le confiner en ***Quarantaine***.

- ***Cookies*** - Les cookies sont des fichiers texte bruts utilisés par les sites Web pour stocker des informations propres à l'utilisateur. Elles permettent ultérieurement de charger un contenu personnalisé d'un site Web, de saisir automatiquement le nom d'utilisateur, etc.

- ***Clés de registre suspectes*** - Certains programmes malveillants stockent leurs informations dans la base de registre de Windows. De cette manière, elles sont chargées au démarrage ou peuvent s'immiscer dans le système d'exploitation.

12.7.5. Onglet Rootkits

L'onglet ***Rootkits*** affiche des informations sur les rootkits détectés au cours de l'analyse si vous avez lancé le composant ***Analyse Anti-Rootkit***.

Un ***rootkit*** est un programme conçu pour prendre le contrôle du système, sans l'autorisation de son propriétaire et de son administrateur légitime. Un accès matériel est rarement nécessaire car un rootkit est prévu pour s'introduire dans le système d'exploitation exécuté sur le matériel. En règle générale, les rootkits dissimulent leur présence dans le système en dupant ou en contournant les mécanismes de sécurité standard du système d'exploitation. Souvent, ils prennent la forme de chevaux de Troie et font croire aux utilisateurs que leur exécution est sans danger pour leurs ordinateurs. Pour parvenir à ce résultat, différentes techniques sont employées : dissimulation de processus aux programmes de contrôle ou masquage de fichiers ou de données système, au système d'exploitation.

La structure de cet onglet est quasiment la même que celle de l'***onglet Infections*** ou de l'***onglet Spyware***.

12.7.6. Onglet Informations

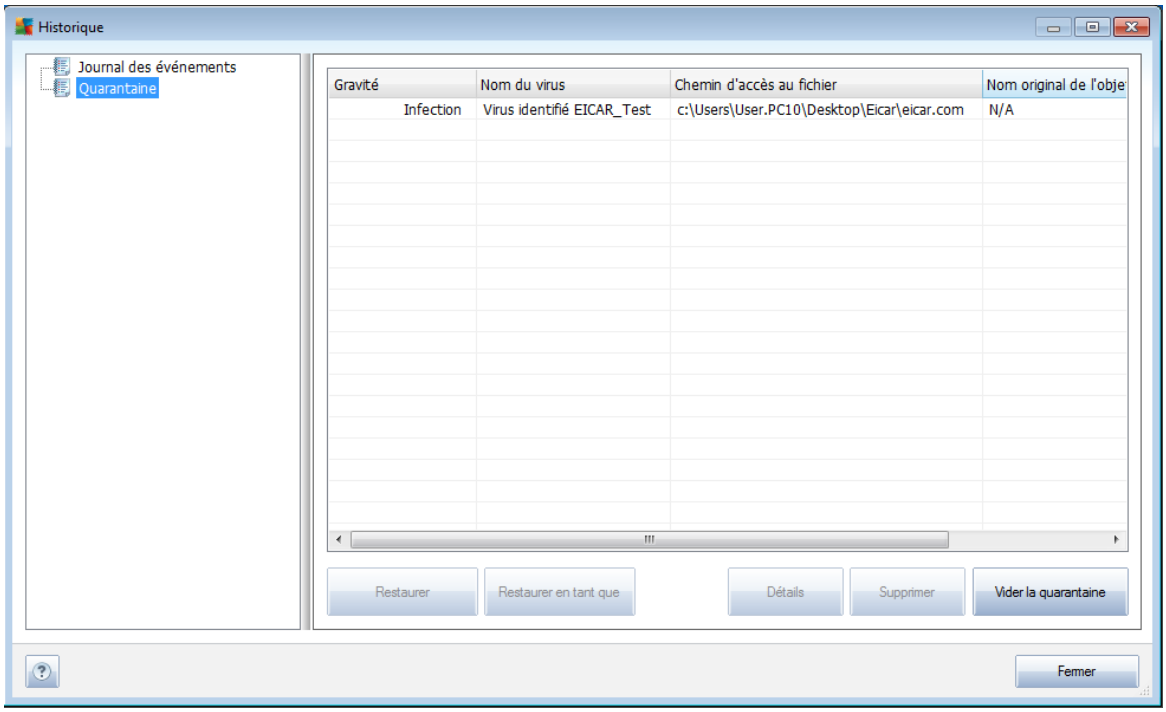
L'onglet ***Informations*** contient des renseignements sur des "objets trouvés" qui ne peuvent pas être classés dans les catégories infections, spywares, etc. Il est impossible de les désigner comme positivement dangereux, mais ils réclament malgré

tout votre attention. L'analyse AVG permet de détecter des fichiers qui ne sont peut-être pas infectés, mais malicieux. Ces fichiers sont signalés par le biais d'un ***avertissement*** ou d'une ***information***.

Les raisons suivantes peuvent expliquer la gravité des ***informations*** :

- ***Mode de compression*** - Le fichier a été compressé avec l'un des systèmes de compression les moins connus, peut-être dans le but d'en empêcher l'analyse par AVG. Cependant, il n'est pas dit qu'un tel résultat indique que ce fichier contienne un virus.
- ***Mode de compression récursif*** - Semblable au précédent, mais moins fréquent parmi les logiciels les plus connus. Ces fichiers sont malicieux et leur suppression ou envoi à AVG pour analyse doit être envisagé.
- ***Archive ou document protégé par mot de passe*** - Les fichiers protégés par mot de passe ne peuvent pas être analysés par AVG (*ou par d'autres programmes anti-malwares*).
- ***Document contenant des macros*** - Le document signalé contient des macros potentiellement dangereuses.
- ***Extension cachée*** - Les fichiers munis d'une extension cachée peuvent apparaître comme des images alors qu'en réalité ce sont des fichiers exécutables (*exemple : image.jpg.exe).* Par défaut, la deuxième extension n'est pas visible sur Windows et AVG signale ce genre de fichiers afin d'empêcher leur ouverture accidentelle.
- ***Chemin d'accès au fichier incorrect*** - Si un fichier système important est exécuté à partir d'un chemin d'accès autre que celui par défaut (*exemple : winlogon.exe exécuté à partir d'un dossier autre que Windows*), AVG signale cette contradiction. Dans certains cas, les virus utilisent des noms de processus système standards afin de se dissimuler au système.
- ***Fichier verrouillé*** - Le fichier signalé est verrouillé et, de ce fait, AVG ne peut pas l'analyser. En général, il s'agit d'un fichier qui est constamment utilisé par le système (*par exemple, un fichier d'échange*).

12.8. Quarantaine



La ***quarantaine*** offre un environnement parfaitement sûr pour la manipulation des objets infectés ou susceptibles de l'être, détectés au cours des analyses AVG. Lorsqu'un objet infecté est repéré par l'analyse et qu'AVG n'est pas en mesure de le réparer automatiquement, un message vous invite à indiquer la mesure à prendre. Il est recommandé de placer l'objet en***Quarantaine*** afin de le traiter ultérieurement. Le principal objet de la ***quarantaine*** consiste à conserver en lieu sûr et durant un laps de temps défini, tout fichier supprimé lors de l'analyse au cas où vous auriez besoin de ces fichiers ultérieurement. Si l'absence du fichier entraîne des problèmes, envoyez-nous le fichier pour analyse ou restaurez-le à son emplacement d'origine.

L'interface ***Quarantaine*** s'affiche dans une fenêtre différente et présente des informations générales sur les objets infectés et mis en quarantaine :

- ***Gravité*** - spécifie le type d'infection (*selon le degré d'infection ; tous les objets répertoriés sont potentiellement ou effectivement infectés*)
- ***Nom du virus*** - spécifie le nom de l'infection décelée conformément à l'***Encyclopédie des virus*** (disponible en ligne)
- ***Chemin d'accès au fichier*** - chemin d'accès menant à l'origine du fichier infectieux
- ***Nom original de l'objet*** - tous les objets détectés figurant dans la liste portent un nom standard attribué par AVG au cours du processus d'analyse. Si le nom initial de l'objet est connu (*telle qu'une pièce jointe qui ne correspond pas au contenu véritable de la pièce jointe*), il sera indiqué dans cette colonne.

- ***Date de l'enregistrement*** - date et heure à laquelle le fichier a été trouvé et placé en***quarantaine***

Boutons de commande

Les boutons de commande suivants sont accessibles depuis l'interface ***Quarantaine*** :

- ***Restaurer*** - rétablit le fichier infecté à sa place d'origine, sur le disque
- ***Restaurer en tant que*** - si vous décidez de transférer l'objet infecté détecté depuis la zone de ***Quarantaine*** vers un dossier de votre choix, servez-vous de ce bouton. L'objet suspect détecté sera enregistré sous son nom d'origine. Si le nom d'origine n'est pas connu, le nom standard sera utilisé.
- ***Supprimer*** - supprime définitivement le fichier infecté de la ***Quarantaine***
- ***Vider la quarantaine*** - Vider intégralement le contenu de la***Quarantaine***. Lorsque vous supprimez des fichiers de la ***quarantaine, ils sont définitivement effacés du disque dur (***ils ne sont pas mis dans la Corbeille*).*

13. Mises à jour d'AVG

Il est essentiel de mettre régulièrement à jour votre programme anti-virus de manière à assurer une détection rapide des virus récemment découverts.

Les mises à jour AVG ne sont pas diffusées selon un programme précis, mais sont plutôt la réaction à la détection d'un grand nombre de menaces ou de menaces sérieuses. C'est pourquoi, il est recommandé de vérifier au moins une fois par jour l'existence d'une éventuelle mise à jour. De cette manière, vous êtes sûr que le programme **AVG 2011 Edition Serveur de Fichiers** reste à jour tout au long de la journée.

13.1. Niveaux de mise à jour

AVG présente deux niveaux de mise à jour :

- Υνε***mise à jour des définitions*** prioritaire inclut les modifications nécessaires à une protection efficace contre les virus. En règle générale, cette action ne s'applique pas au code. Seule la base de données de définition est concernée. Il est conseillé d'effectuer cette mise à jour dès qu'elle est disponible.

- ***La mise à jour du programme*** contient diverses modifications, corrections et améliorations.

Lorsque vous programmez une mise à jour, il est possible de sélectionner le niveau de priorité voulu lors du téléchargement et de l'application de la mise à jour.

Remarque : *si une mise à jour planifiée du programme coïncide avec une analyse programmée, le processus de mise à jour a priorité sur l'analyse qui est interrompue.*

13.2. Types de mises à jour

Il existe deux types de mises à jour :

- ***Mise à jour à la demande*** - une mise à jour immédiate d'AVG que vous exécutez dès que vous en voyez l'utilité.

- ***Mise à jour programmée*** - AVG permet également de définir à l'avance un plan de mise à jour. La mise à jour planifiée est alors exécutée de façon périodique en fonction de la configuration choisie. Chaque fois que de nouveaux fichiers de mise à jour sont présents à l'emplacement indiqué, ils sont téléchargés directement depuis Internet ou à partir d'un répertoire du réseau. Lorsque aucune mise à jour n'est disponible, le processus n'a pas lieu.

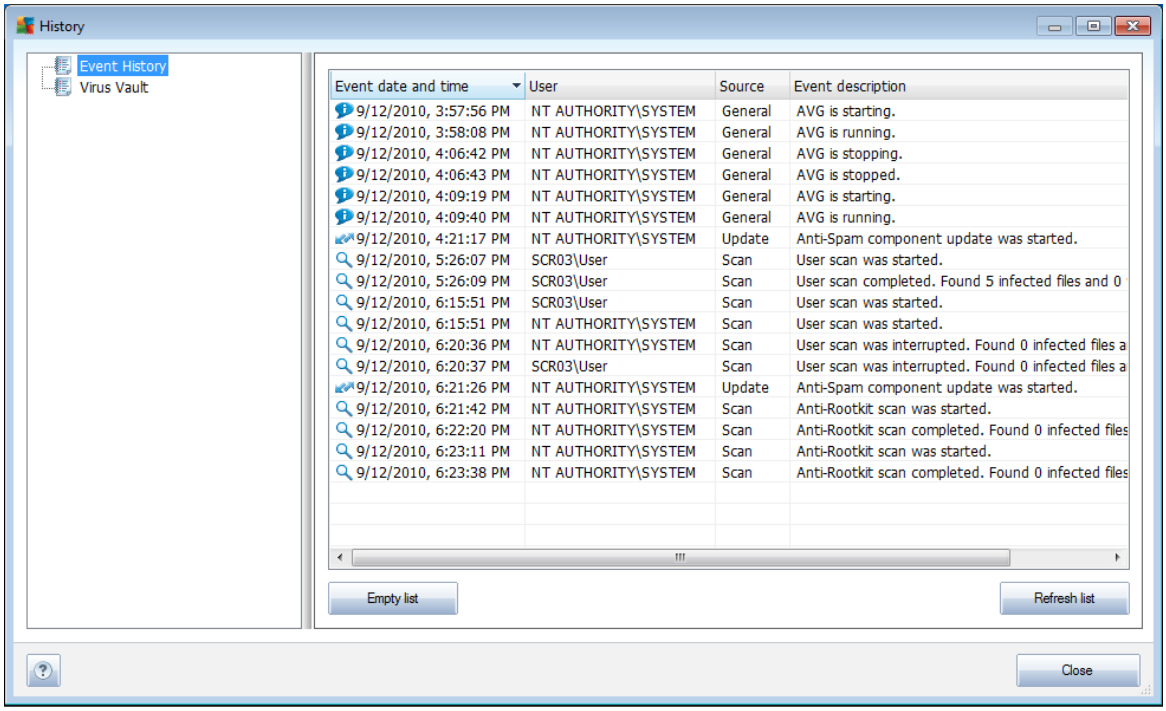
13.3. Processus de mise à jour

Le processus de mise à jour peut être lancé aussi souvent que nécessaire en cliquant sur ***Mise à jour*** (lien d'accès rapide). Ce lien est constamment disponible, quelle que soit la boîte de dialogue ouverte dans l'interface utilisateur AVG. Il est toutefois particulièrement recommandé d'effectuer des mises à jour fréquentes comme établi par défaut dans le composant Mise à jour.

Lorsque vous lancez la mise à jour, AVG vérifie en premier lieu si de nouveaux fichiers de mise à jour sont disponibles. Le cas échéant, AVG télécharge et exécute ces mises à jour. Au cours du processus de mise à jour, l'interface ***de mise à jour*** s'affiche. Elle permet d'observer le déroulement de la procédure sous forme graphique et présente des données statistiques pertinentes (*taille du fichier de mise à jour, données reçues, vitesse du téléchargement, temps écoulé...*).

***Remarque** : avant l'exécution de la mise à jour du programme AVG, un point de restauration est créé. En cas d'échec de la mise à jour et de blocage de votre système d'exploitation, vous avez alors la possibilité de restaurer le système d'exploitation tel qu'il était configuré à partir de ce point. Cette option est accessible via Démarrer / Tous les programmes / Accessoires / Outils système / Restauration du système. Seuls les utilisateurs expérimentés devraient effectuer des changements à ce niveau !*

14. Journal des évènements



La boîte de dialogue ***Journal de l'historique des évènements*** est accessible par la barre de menus, menu ***Historique, puis Journal de l'historique des évènements*** . Dans cette boîte de dialogue, vous trouverez un résumé des évènements les plus importants survenus pendant l'exécution du programme **.** La commande ***Journal de l'historique des évènements*** enregistre les types d'évènements suivants :

- Informations au sujet des mises à jour de l'application AVG
- Heure de début, de fin ou d'interruption de l'analyse (*y compris pour les analyses effectuées automatiquement*)
- *Evènements liés à la détection des virus (par le Bouclier résident ou résultant de l'analyse*) avec indication de l'emplacement des occurrences
- Autres évènements importants

Pour chaque évènement, les informations suivantes s'affichent :

- ***Date et heure de l'évènement*** donne la date et l'heure exactes de l'évènement
- ***Utilisateur*** indique qui a démarré l'évènement
- ***Source*** indique le composant source ou une autre partie du système AVG qui a déclenché l'évènement

- ***Description de l'évènement*** donne un bref résumé de ce qui s'est réellement passé

Boutons de commande

- ***Vider la liste*** - supprime toutes les entrées de la liste d'évènements
- ***Actualiser la liste*** - met à jour toutes les entrées de la liste d'évènements

15. FAQ et assistance technique

En cas de problème technique ou commercial avec votre produit AVG, consultez la section ***FAQ*** du site Web d'AVG (http://www.avg.com).

Si vous n'y trouvez pas l'aide dont vous avez besoin, vous pouvez aussi contacter notre service d'assistance technique par e-mail. Merci d'utiliser le formulaire réservé à cet effet, accessible depuis le menu du système, en passant par l'***Aide / Obtenir de l'aide en ligne***.