Dr.WEB

pour Microsoft Exchange Server

# Manuel Administrateur

**Dr.Web pour Microsoft Exchange Server**
**Version 11.5**
**Manuel Administrateur**
**11/18/2019**

Doctor Web, Siège social en Russie

125040

Moscou, Russie

2-12A, 3e rue Yamskogo polya

Site web : https://www.drweb.com/

Téléphone : +7 (495) 789-45-87

Vous pouvez trouver les informations sur les bureaux régionaux sur le site officiel de la société.

# Doctor Web

Doctor Web — éditeur russe de solutions de sécurité informatique.

Doctor Web propose des solutions antivirus et antispam efficaces pour les institutions publiques, les entreprises, ainsi que pour les particuliers.

Les solutions antivirus Dr.Web sont connues depuis 1992 pour leur excellence en matière de détection des programmes malveillants et leur conformité aux standards internationaux de sécurité.

Les certificats et les prix attribués, ainsi que l'utilisation de nos produits dans le monde entier sont les meilleurs témoins de la confiance qui leur est accordée.

**Nous remercions tous nos clients pour leur soutien !**

# Contenu

# 1. Légende et abréviations

Les styles de texte utilisées dans ce manuel :

| Styles | Utilisés |
|---|---|
|  | Avertissement sur des situations potentielles d'erreurs et sur les éléments importants auxquels il faut faire attention. |
| *Réseau antivirus* | Un nouveau terme ou l'accent mis sur un terme dans les descriptions. |
| *<IP-address>* | Champs destinés à remplacer les noms fonctionnels par leurs valeurs. |
| **Enregistrer** | Noms des boutons de l'écran, des fenêtres, des éléments de menu et d'autres éléments de l'interface du logiciel. |
| CTRL | Touches du clavier. |
| `C:\Windows\` | Noms de fichiers/dossiers ou fragments de programme. |
| Annexe A | Liens vers les autres chapitres du manuel ou liens vers des ressources externes. |

# 2. Introduction

Merci d'avoir choisi Dr.Web pour Microsoft Exchange Server (ci-après – Dr.Web). Ce produit antivirus utilise les technologies les plus récentes et fournit une protection fiable des ordinateurs et des informations au sein du réseau de l'entreprise contre les menaces propagées via le courrier électronique.

Ce manuel est destiné à aider les administrateurs des réseaux d'entreprise à installer et à configurer Dr.Web. Le manuel décrit toutes les particularités concernant l'utilisation de ce logiciel contient les coordonnées du service de support technique.

## 2.1. Usage de Dr.Web

Dr.Web est une application antivirus destinée à protéger la messagerie de l'entreprise contre les virus et les spams. L'application s'intègre dans le système et contrôle tous les messages et les pièces jointes reçus par le serveur. Tous les messages sont analysés avant qu'ils ne soient transmis au client de messagerie.

Dr.Web peut réaliser les fonctions suivantes :

- analyse de tous les messages entrants et sortants en temps réel ;
- filtrage et blocage des spams, création de listes d'adresses noire et blanche ;
- isolement des objets infectés et suspects en quarantaine ;
- filtrage des courriers selon divers critères ;
- groupement des utilisateurs permettant de faciliter l'administration ;
- envoi des notifications sur les événements viraux au journal du système d'exploitation et support de la base de données interne des événements - cmstracedb ;
- récolte des statistiques ;
- support des paramètres communs de l'application dans un système distribué de firewalls, y compris ceux qui sont groupés en clusters ;
- mise à jour automatique des bases virales et des composants.

Pour faciliter le travail avec l'application, le démarrage automatique (au lancement du système) et le mécanisme simple de mise à jour par l'ajout d'une tâche de mise à jour dans le Planificateur de tâches Windows sont disponibles.

Dr.Web utilise des bases virales constamment mises à jour et assurant ainsi une protection de haut niveau et une réactivité élevée à l'apparition des nouvelles menaces. L'analyseur heuristique embarqué renforce la protection contre les virus inconnus.

Dr.Web supporte entièrement Microsoft Exchange Server, installé en mode Groupe de disponibilité de base de données (DAG), à partir de la version Microsoft Exchange Server 2010.

L'application fonctionne sur la plateforme Dr.Web CMS (Central Management Service) supportant la gestion centralisée des paramètres de l'application et de ses composants avec la possibilité d'administration à distance via le navigateur, par le protocole sécurisé HTTPS. La plateforme Dr.Web CMS intègre le serveur Dr.Web CMS Web Console avec l'authentification du client, ce qui permet aux administrateurs autorisés d'accéder à la gestion de l'application.

Au sein d'une plateforme, l'interaction entre les composants et leur configuration est fondée sur les protocoles de service fonctionnant par-dessus TCP. Ces protocoles de service permettent au service gérant Dr.Web CMS d'exécuter sa tâche principale : fournir aux composants de l'application un canal de communication avec la base de données gérante **cmsdb** et la base d'événements de l'application cmstracedb se trouvant dans le dossier d'installation et réalisées par la base relationnelle embarquée SQLite.

L'interaction des composants de l'application avec la plateforme Dr.Web CMS s'effectue de la manière suivante :

1. Lors du démarrage (si le composant de l'application est un service) ou lors du chargement (si le composant est une bibliothèque), le composant de l'application se connecte au service Dr.Web CMS via le protocole de service par-dessus TCP.
2. Dr.Web CMS enregistre la connexion de l'application et crée dans la base **cmsdb** une structure de données répondant au composant connecté de l'application.
3. Dr.Web CMS contrôle le fonctionnement du composant de l'application en surveillant le statut de la session TCP et l'échange de messages de service avec le composant de l'application.
4. En cas de changement du statut du composant de l'application, Dr.Web CMS modifie les variables dans la base **cmsdb** reflétant le statut de l'application.

Les services Dr.Web CMS installés sur différents serveurs peuvent être réunis par l'administrateur en une arborescence pour le support de la réplication des paramètres de la base **cmsdb** avec l'attribut **Shared** de tous les composants-abonnés Dr.Web CMS. La réplication s'effectue du serveur principal au serveur subordonné (voir la rubrique Création des clusters). Ainsi, la gestion des paramètres de l'arborescence des serveurs est possible depuis l'hôte racine.

## 2.2. Objets contrôlés

Dr.Web vérifie tous les messages entrants en temps réel. Les éléments suivants sont analysés :

- corps du message ;
- pièces jointes (y compris les fichiers archivés et compressés) ;
- objets OLE incorporés.

Dr.Web analyse tous les objets avant qu'ils ne soient transmis au client de messagerie.

## 2.3. Support technique

En cas de problèmes liés à l'installation ou au fonctionnement des produits de la société, avant de contacter le support technique, essayez de trouver la solution par un des moyens suivants :

- consultez les dernières versions des descriptions et des manuels à l'adresse https://download.drweb.com/doc/ ;
- lisez la rubrique de questions fréquentes à l'adresse https://support.drweb.com/show_faq/ ;
- visitez des forums de Doctor Web à l'adresse https://forum.drweb.com/.

Si après avoir tout essayé, vous n'avez pas résolu le problème, utilisez un des moyens suivants pour contacter le support technique de Doctor Web :

- remplissez le formulaire de question dans la section correspondante de la rubrique https://support.drweb.com/ ;
- appelez au numéro : 0 825 300 230.

Vous pouvez trouver les informations sur les bureaux régionaux de Doctor Web sur le site officiel à l'adresse https://company.drweb.com/contacts/offices/.

# 3. Licence

Les droits d'utilisation du logiciel Dr.Web sont déterminés par le fichier spécial dit *fichier clé de licence*.

## 3.1. Fichier clé de licence

Le fichier clé possède l'extension .key et contient les informations suivantes :

- durée de validité de la licence ;
- liste des composants couverts par la licence (par exemple, le composant Antispam est disponible uniquement au sein de la version «Antivirus + Antispam») ;
- autres restrictions (par exemple, le nombre maximum d'utilisateurs protégés par l'application).

Le fichier clé est *valable* si les conditions suivantes sont satisfaites :

- la durée de licence n'a pas expiré ;
- les modules utilisés par le programme sont couverts par le fichier clé ;
- l'intégrité du fichier clé n'a pas été endommagée.

Si l'une de ces conditions est violée, le fichier clé devient invalide, Dr.Web ne détecte plus les programmes malveillants. Le fait que l'intégrité du fichier clé ait été endommagée sera enregistré dans le journal des événements système ainsi que dans le journal texte des événements relatifs au programme.

Le fichier clé a été conçu dans un format protégé contre l'édition. L'édition du fichier clé le rend non valide. N'ouvrez pas le fichier clé avec des éditeurs de texte afin de ne pas l'endommager accidentellement.

## 3.2. Obtenir un fichier clé

Vous pouvez obtenir un fichier clé par l'un des moyens suivants :

- sous forme d'une archive ZIP par e-mail ;
- au sein du package d'installation du produit si le fichier clé y a été inclus lors de la composition du package ;
- sur un support amovible, sous forme d'un fichier ayant l'extension .key.

Si Dr.Web Agent est installé sur votre ordinateur, vous pouvez choisir une des options pour obtenir le fichier clé du serveur de protection centralisée lors de l'installation de l'Antivirus Dr.Web.

Vous devez disposer d'un fichier clé avant de procéder à l'installation de Dr.Web puisque pour l'installation, vous serez invité à saisir le chemin vers votre fichier clé.

**Obtenir un fichier clé par e-mail**

1. Allez sur le site web dont l'adresse est indiquée dans la fiche fournie avec le produit.
2. Saisissez vos informations personnelles dans le formulaire.
3. Saisissez le numéro de série (il est indiqué sur la fiche d'enregistrement).
4. Le fichier clé sera envoyé à l'adresse e-mail que vous avez indiquée sous forme d'une archive ZIP contenant un fichier avec l'extension .key.
5. Extrayez le fichier clé vers l'ordinateur sur lequel vous souhaitez installer Dr.Web.

Pour tester le logiciel, vous pouvez obtenir un *fichier clé de démonstration*. Ce fichier clé assure le fonctionnement de l'ensemble des principaux composants antivirus mais pour un temps limité et il ne prévoit pas de fournir un service de support technique à l'utilisateur.

Pour obtenir le fichier clé démo (par e-mail), merci de vous enregistrer sur la page suivante https://download.drweb.fr/demoreq/home/.

Pour acheter un fichier clé de licence, contactez un partenaire de Doctor Web dans votre région ou visitez la boutique en ligne sur le site de la société à l'adresse http://estore.drweb.fr/home/.

Pour en savoir plus sur les licences et les fichiers clés, visitez le site web officiel de la société Doctor Web à l'adresse http://www.drweb.fr/.

## 3.3. Mise à jour de la licence

Lorsque votre licence arrive à expiration ou si la sécurité de votre système est renforcée, vous pouvez avoir besoin d'acheter une nouvelle licence ou une nouvelle licence élargie pour Dr.Web. Dans ce cas, vous devez remplacer le fichier clé existant et enregistré dans le système. L'application supporte la mise à jour de la licence « à la volée », vous n'avez pas à réinstaller ou arrêter l'application.

**Renouvellement du fichier clé**

1. Pour renouveler la licence, ajoutez un nouveau fichier clé dans le dossier d'installation du logiciel.
2. Redémarrez le service Dr.Web for MSP Scanning Service.
3. Le programme Dr.Web s'adapte automatiquement à l'utilisation du nouveau fichier clé.

Pour en savoir plus sur la durée et les types de licence, visitez le site officiel de la société Doctor Web à l'adresse http://www.drweb.fr/.

# 4. Principes de fonctionnement de Dr.Web

Toutes les solutions antivirus Dr.Web comprennent des composants principaux assurant la protection de tous les systèmes d'exploitation et de toutes les plateformes : le noyau antivirus **drweb32.dll** et les fichiers des bases virales (ayant l'extension **.vdb**) qui contiennent les enregistrements viraux qui sont mis à jour régulièrement et qui réunissent des informations sur les virus et d'autres codes malveillants.

La solution antivirus et antispam Dr.Web intègre les technologies Dr.Web dans le processus de traitement et de stockage du courrier sur les serveurs Exchange.

Le produit est doté d'une interface graphique conviviale permettant de gérer les paramètres de scan et de consulter les résultats de l'analyse des messages sur le serveur.

## 4.1. Étapes de l'analyse antivirus et antispam

Dès qu'une notification sur l'arrivée d'un message est reçue par le serveur, ce message subit les étapes d'analyse suivantes :

1. **Application des règles de filtrage** (à paramétrer dans la section Filtrage).
   - Règles d'autodistribution (limitation des listes d'envoi). Vous pouvez spécifier des règles déterminant un nombre maximum d'adresses de destinataires du message (du message contenant des pièces jointes) et applicables aux adresses des expéditeurs. Pour de tels expéditeurs, c'est seulement l'envoi des messages dont le nombre d'adresses de destinataires est inférieur à la valeur maximale spécifiée qui est autorisé.
   - Règles de filtrage des fichiers dans les pièces jointes. Vous pouvez établir des règles de suppression des pièces jointes : par extension, par masque de nom de fichier, par taille maximale de fichier.

   Si l'une de ces règles est satisfaite, le message (ou la pièce jointe) est supprimé et une notification correspondante est envoyée à l'administrateur ou à d'autres personnes intéressées (à condition que les paramètres correspondants soient configurés dans la section Notifications). En cas de suppression d'un fichier se trouvant dans la pièce jointe, un fichier texte informant sur la suppression de la pièce jointe sera joint au message. Le template de message informant sur la suppression d'une pièce jointe et le nom du message sont configurés dans la section Filtrage.
2. **Analyse antispam** (cette étape est présente uniquement en cas de licence « Antivirus + Antispam » et pour les messages reçus par le serveur via le protocole SMTP seulement. Vous pouvez la configurer dans la section Antispam).

   En premier lieu, les adresses des destinataires et des expéditeurs sont analysées pour vérifier si elles sont présentes dans les listes noire et blanche spécifiées dans la section Antispam. Puis le filtre antispam Vade Secure vérifie le texte du message et donne sa conclusion d'après laquelle est déterminée la probabilité que le message soit un spam. Si le message est classé comme spam, une notification est envoyée à l'administrateur et aux personnes

indiquées dans les paramètres de la section Notifications, l'action définie par l'administrateur dans la section Antispam sera appliquée au message.

3. **Analyse antivirus** (à paramétrer dans la section Scan).

   Les messages ayant passé avec succès les étapes précédentes de l'analyse (ou sautés selon les paramètres de l'application **Dr.Web**) sont ensuite transférés pour analyser la présence éventuelle d'un code malveillant. Si l'objet (la pièce jointe ou le corps du message) contient un code malveillant, l'antivirus essaie de désinfecter cet objet. Si l'utilisation de l'analyseur heuristique est activée dans les paramètres, il est possible de détecter les objets contenant un code malveillant modifié ou inconnu, dans ce cas, les messages sont référencés dans la catégorie **Suspects**.

   Selon les résultats de l'analyse, les objets reçoivent des statuts déterminés (par exemple, **Incurables**, **Suspects**, **Endommagés**, **Désinfectés**), les actions sur ces objets sont déterminées en fonction du statut attribué. Un fichier texte est ajouté aux messages contenant des objets infectés. Ce fichier informe sur l'infection détectée et sur les actions appliquées aux objets en question.

   Les objets désinfectés ou sains sont transférés au serveur accompagnés d'une note correspondante. Les objets incurables, endommagés et suspects seront traités conformément aux paramètres spécifiés dans la section Scan.

   L'administrateur peut recevoir des notifications sur tous les types d'événements viraux si cette option est paramétrée dans la section Notifications.

## 4.2. Quarantaine

Il est possible de spécifier l'action **Déplacer en Quarantaine** pour les fichiers incurables, endommagés et suspects. Les objets de ce type sont mis dans la base auxiliaire qui réalise les fonctions de quarantaine pouvant bloquer l'exécution du code de tels objets par les applications tournant sous OS. Pour consulter les informations sur les objets mis en quarantaine, allez dans la section Gestion de la quarantaine.

## 4.3. Surveillance des événements viraux

Pour que l'administrateur et d'autres personnes puissent avoir des informations structurées sur les événements surveillés par Dr.Web, l'administrateur doit configurer le système de notifications qui comprend les fonctions suivantes :

- Journal des événements. Il est possible d'écrire dans le journal des informations sur l'arrivée sur le serveur des messages contenant des objets désinfectés, incurables, filtrés ou classés comme endommagés ou spams (à choisir). Pour afficher ces événements, utilisez l'utilitaire standard Windows **Observateur d'événements** -> **Application** (**Event Viewer** -> **Application**) ;
- Statistique. Cette fonction permet de consulter des informations sur le nombre d'objets vérifiés depuis l'installation de Dr.Web ou depuis le nettoyage des statistiques ;

- Événements. Il est possible de consulter la liste des messages traités par Dr.Web dans lesquels des virus et des spams ont été détectés. Vous pouvez également consulter les messages filtrés.

# 5. Installation et suppression

Dr.Web est fourni sous forme d'un dossier placé dans une archive ZIP et contenant les fichiers d'installation **drweb-[version]-av-exchange-windows-x64.exe** et **drweb-[version]-av-exchange-windows-x86.exe**, où **[version]** indique la version de Dr.Web.

Extrayez le fichier d'installation sur le disque local de l'ordinateur sur lequel Microsoft Exchange Server est installé.

Pour installer et supprimer Dr.Web, l'utilisateur doit disposer des droits d'administrateur local sur l'ordinateur sur lequel est installé Microsoft Exchange Server, il doit aussi faire partie du groupe Domain Users.

Si vous utilisez le composant Windows Terminal Services, pour installer Dr.Web, il est recommandé d'utiliser l'utilitaire standard Windows **Installation et suppression de programmes**.

## 5.1. Pré-requis système

Ici vous trouverez les pré-requis nécessaires à l'installation et au fonctionnement correct de Dr.Web.

| Caractéristique | Pré-requis |
|---|---|
| RAM | 512 Mo et plus |
| Espace libre sur le disque | 1 Go et plus |
| OS | **OS 32 bits**<br>Pour Microsoft Exchange Server 2003:<br>• Microsoft® Windows Server® 2003x86 avec:<br>  ▪ MSXML 4.0 Service Pack 3 (Microsoft XML Core Services) installé;<br>  ▪ SP1 ou supérieur. |
| | **OS 64 bits**<br>Pour Microsoft Exchange Server 2007/2010:<br>• Microsoft® Windows Server® 2008 x64;<br>• Microsoft® Windows Server® 2008 R2.<br>Pour Microsoft Exchange Server 2013:<br>• Microsoft® Windows Server® 2008 R2;<br>• Microsoft® Windows Server® 2012; |

| Caractéristique | Pré-requis |
|---|---|
| | • Microsoft® Windows Server® 2012 R2;<br>▪ Sous Exchange Server 2013, SP 1 (ou la version plus récente) est requis.<br>Pour Microsoft Exchange Server 2016:<br>• Microsoft® Windows Server® 2012 R2;<br>• Microsoft® Windows Server® 2012 R2;<br>• Microsoft® Windows Server® 2016:<br>▪ Sous Exchange Server 2016, Cumulative Update 3 (ou la version plus récente) est requise. |
| Version de Microsoft Exchange Server | • Microsoft® Exchange Server 2003;<br>• Microsoft® Exchange Server 2007 x64 avec SP1 installé;<br>• Microsoft® Exchange Server 2010;<br>• Microsoft® Exchange Server 2013;<br>• Microsoft® Exchange Server 2013 avec SP1 installé (l'installation de Cumulative Update 5 ou le lancement du script Exchange2013-KB2938053-Fixit);<br>• Microsoft® Exchange Server 2016. |

## 5.2. Compatibilité

Avant d'installer Dr.Web, veuillez faire attention aux informations suivantes sur la compatibilité du logiciel :

1. Dr.Web pour Microsoft Exchange Server de la version 11.5 n'est compatible qu'avec les produits Dr.Web de la version 11.5, compris Enterprise Security Suite 11.0.
2. Dr.Web pour Microsoft Exchange Server n'est pas compatible avec d'autres logiciel antivirus. L'installation de plusieurs produits antivirus sur le même ordinateur peut entraîner des erreurs système ou une perte de données importantes. Si un autre antivirus est déjà installé sur votre ordinateur, il est nécessaire de le désinstaller en utilisant le fichier d'installation ou les outils standard du système d'exploitation.
3. Dr.Web pour Microsoft Exchange Server de la version 11.5 n'est pas compatible avec Dr.Web pour Microsoft ISA Server/Forefront TMG.

Pour le fonctionnement correct du serveur Microsoft Exchange, si le composant SpIDer Guard est activé, il est recommandé d'exclure du scan de SpIDer Guard les dossiers et les processus de Microsoft Exchange Server (vous pouvez trouver la liste des exclusions recommandées dans la documentation Microsoft).

## 5.3. Installation de Dr.Web

**Avant d'installer**

- d'installer toutes les mises à jour critiques publiées par Microsoft et relatives à l'OS utilisé sur l'ordinateur (les mises à jour sont disponibles sur le site de mise à jour à l'adresse suivante http://windowsupdate.microsoft.com) ;
- de vérifier le système de fichiers avec les outils standard et de corriger les erreurs détectées ;
- de fermer toutes les applications en cours.

Si vous utilisez Microsoft Exchange Server 2013 avec le package de mise à jour SP1 installé, mais que vous n'avez pas installé Cumulative Update 5, avant d'installer le logiciel, il est recommandé de lancer le script **Exchange2013-KB2938053-Fixit** pour éviter des erreurs d'enregistrement des agents de transport lors de l'installation. Le script est disponible sur le site de Microsoft à l'adresse http://support.microsoft.com/kb/2938053.

**Pour installer Dr.Web**

1. Lancez le fichier d'installation **drweb-[version]-av-exchange-windows-x64.exe** si vous utilisez Microsoft Exchange Server 2007/2010/2013/2016 ou **drweb-[version]-av-exchange-windows-x86.exe** pour les versions précédentes du serveur Exchange. La fenêtre de l'**Assistant d'installation** apparaît.
2. Pour continuer l'installation, vous devez lire et accepter les termes du Contrat de licence en cochant la case **J'accepte les termes du contrat de licence**.

   Cliquez sur **Suivant**.
3. Arrêtez le service Microsoft Exchange Transport (en cas d'utilisation de Microsoft Exchange Server 2007/2010/2013/2016).

   Pour ce faire, cliquez sur le lien **Ouvrir la liste de services**, puis cliquez droit sur le nom du service dans la liste et sélectionnez **Arrêter**. Après l'arrêt du service, cliquez sur **Suivant**.

L'arrêt manuel du service Microsoft Exchange Transport est lié à la nécessité d'éviter la violation d'intégrité de l'installation sur le serveur fonctionnant sous charge.

Dans certains cas, l'arrêt du service Microsoft Exchange Transport peut prendre un certain temps !

4. Sélectionnez une option de licensing. Vous pouvez enregistrer la licence après l'installation en indiquant le chemin vers le fichier clé valide ou utiliser le fichier clé de serveur de protection centralisée, si Dr.Web Agent est installé sur l'ordinateur. Cliquez sur **Suivant**.

Pour le fonctionnement correct de l'application, il est nécessaire d'indiquer le chemin vers le fichier clé de licence drweb32.key.

Pour l'enregistrement de la licence après l'installation ou lors de sa mise à jour, il suffit de placer le fichier clé de licence dans le dossier d'installation du logiciel et de redémarrer le service Dr.Web for MSP Scanning Service.

5. Avant le début d'installation, cliquez sur **Paramètres d'installation** pour configurer les paramètres suivants de l'installation :
   - **Installer les agents de transport** – permet d'installer les agents de transport (ce paramètre est sélectionné par défaut) Pour Microsoft Exchange Server 2007/2010/2013/2016, l'activation de cette option entraîne l'enregistrement de la bibliothèque DRWTransportAgent.dll et l'autorisation des agents de transports (antivirus et antispam) fournis par la bibliothèque dans le service Microsoft Exchange Transport. Pour Microsoft Exchange Server des versions antérieures, la sélection de cette option entraîne l'enregistrement de la bibliothèque DrWebSink.dll et la connexion de l'agent antispam dans Microsoft Internet Information Services (IIS).
   - **Installer le module VSAPI** permet d'installer le module DrWebVSAPI.dll pour l'analyse par l'interface du scan antivirus VSAPI (cette interface n'est pas supportée par Microsoft Exchange Server 2013) fournie par le service Microsoft Exchange Information Store. Si ce paramètre est sélectionné, vous pouvez configurer le mode de scan : activer le scan des messages sortants, le scan proactif et le scan en tâche de fond.

   De plus, vous pouvez activer la surveillance du processus d'installation et d'enregistrement des agents de transport, en cochant les cases **Contrôler le processus de connexion des agents de transport**. Lors de l'installation, les agents de transport pour Microsoft Exchange Server 2007/2010/2013/2016 seront enregistrés dans le système du transport SMTP par Exchange `PowerShell`. Dans ce cas, la console `PowerShell` ne se ferme pas automatiquement et pour terminer l'installation il faudra saisir manuellement la commande `exit` pour la fermer.

   Cliquez sur **OK**.

   Pour éviter des erreurs d'enregistrement des agents de transport lors de l'installation, il est recommandé de s'assurer que le script RemoteExchange.ps1 est installé sur le serveur Microsoft Exchange Server (par défaut, il se trouve dans le dossier C:\Program Files\Microsoft\Exchange Server\V14\bin\ pour Microsoft Exchange Server 2010 et dans le dosssier C:\Program Files\Microsoft\Exchange Server\V15\bin\ pour Microsoft Exchange Server 2013).

6. En cas d'installation réitérée, vous serez invité à utiliser les paramètres sauvegardés avant la suppression (si cette option a été sélectionnée). Vous pouvez utiliser la configuration sauvegardée ou la supprimer et configurer l'application de nouveau après l'installation. Cliquez sur **Suivant**.

   L'installation de Dr.Web sur votre ordinateur va commencer. Par défaut, les fichiers du logiciel sont placés dans les dossiers %Program Files%\DrWeb for Exchange et %Program Files%\Common Files\Doctor Web. Les journaux d'enregistrement d'événements et les composants auxiliaires sont placés dans le dossier %Program Data%\Doctor Web.

7. Si vous avez coché la case **Contrôler le processus de connexion des agents de transport** lors de la configuration des paramètres d'installation, vous devrez terminer la surveillance après l'installation et la connexion des agents de transport. Les messages **«Dr.Web AntiVirus Agent enabled»** et **«Dr.Web AntiSpam Agent enabled»** dans la console PowerShell indiquent la connexion réussie des agents de l'application au service Microsoft Exchange Transport. Dans la console PowerShell entrez la commande `exit`.
8. Après l'installation, cliquez sur **Terminer**.

En cas d'installation depuis le fichier **drweb-[version]-av-exchange-windows-x86.exe**, vous serez invité à redémarrer le serveur. En cas d'installation depuis le fichier **drweb-[version]-av-exchange-windows-x64.exe**, le redémarrage n'est pas requis : le service Microsoft Exchange Transport sera lancé automatiquement et après son lancement, le serveur sera remis en état. Pourtant, si les services de support des protocoles POP3 et IMAP4 sont lancés sur le serveur, le redémarrage de Microsoft Exchange Transport peut interrompre leur connexion au système de transport du serveur. Dans ce cas, attendez le lancement définitif du service Microsoft Exchange Transport et des services de l'application installée, ensuite redémarrez les services Microsoft Exchange POP3 ou Microsoft Exchange IMAP4 manuellement (ou redémarrez le serveur).

**Pour réinstaller Dr.Web**

1. Supprimez Dr.Web.

Le fichier de la configuration de l'application cmsdb n'est pas supprimé automatiquement lors de la suppression de l'application. Ainsi, tous les paramètres utilisateur sont sauvegardés et ils peuvent être utilisés en cas de réinstallation. Pourtant en cas d'installation d'une nouvelle version de l'application, il peut s'avérer que l'ensemble des paramètres de la configuration de base s'est élargi ou qu'il a été modifié. Dans ce cas, il est impossible d'utiliser le fichier sauvegardé car cela peut provoquer des défaillances de l'application.

Si vous voulez utiliser les paramètres sauvegardés de l'application, contactez le support technique de Doctor Web pour préciser la compatibilité des paramètres de la plateforme Dr.Web CMS des versions différentes de l'application. Si une nouvelle version contient de nouvelles paramètres, il suffit d'ajouter les variables manquantes dans la base de données existante et indiquer correctement leur type et les valeurs par défaut.

2. Supprimez manuellement les fichiers cmsdb и cmstracedb du dossier **%ProgramFiles%\DrWeb for Exchange**.
3. Procédez à l'installation de Dr.Web conformément aux instructions ci-dessus.

## 5.4. Suppression de Dr.Web

**Pour supprimer Dr.Web**

1. Lancez le fichier d'installation **drweb-[version]-av-exchange-windows-x64.exe** ou **drweb-[version]-av-exchange-windows-x86.exe** en fonction de la version de Microsoft Exchange Server. La fenêtre de l'assistant d'installation va s'ouvrir.

   

   Vous pouvez également utiliser l'utilitaire standard Windows **Installation et Suppression de programmes** accessible via le Panneau de configuration.

2. Arrêtez le service Microsoft Exchange Transport (dans l'utilisation de Microsoft Exchange Server 2007/2010/2013/2016). Pour ce faire, cliquez sur le lien **Ouvrir la liste de services**, puis cliquez droit sur le nom du service dans la liste et sélectionnez **Arrêter**. Après l'arrêt du service, cliquez sur **Suivant**.
3. Si vous voulez sauvegarder la configuration actuelle du logiciel pour l'utiliser plus tard, par exemple, après la réinstallation du logiciel, cochez la case **Sauvegarder les paramètres**. Cliquez sur **Supprimer**.
4. Lors de l'installation de l'application, les agents de transport pour Microsoft Exchange Server 2007/2010/2013/2016 seront également supprimés dans le système du transport SMTP. Les agents de transport sont supprimés par Exchange PowerShell. Confirmez la suppression des agents de transport en entrant `Yes` (ou `Y`) dans la console Exchange PowerShell. Après la suppression, entrez la commande `exit` pour fermer la console.
5. Pour terminer la suppression de l'application, le redémarrage de l'ordinateur est requis. Cliquez sur **Redémarrer maintenant** ou **Plus tard**.

# 6. Scan antivirus et analyse antispam pour Microsoft Exchange Server

Dr.Web pour les versions Exchange Server 2003/2007/2010 supporte l'interface VSAPI (interface de programmation d'applications d'analyse antivirus développée par Microsoft pour les serveurs Exchange).

A part cela, le logiciel supporte les rôles de serveur pour les versions Exchange Server 2007/2010/2013 SP1/2016 et peut être installé sur les serveurs avec des rôles différents.

Le logiciel supporte également les agents de transport (agents antivirus et agents antispam) pour les versions Exchange Server 2007/2010/2013/2016.

| Version de Microsoft Exchange Server | Modules disponibles du scan antivirus et du filtrage de messagerie | Modules disponibles de l'analyse antispam et du filtrage de messagerie |
|---|---|---|
| 2003 | DrWebVSAPI.dll (Backend) | DrWebSink.dll (IIS) |
| 2007 | DRWTransportAgent.dll (Hub, Edge)<br>DrWebVSAPI.dll (Mailbox) | DRWTransportAgent.dll (Hub, Edge) |
| 2010 | DRWTransportAgent.dll (Hub, Edge)<br>DrWebVSAPI.dll (Mailbox) | DRWTransportAgent.dll (Hub, Edge) |
| 2013 | DRWTransportAgent.dll (Frontend, Backend) | DRWTransportAgent.dll (Frontend, Backend) |
| 2013 SP1 | DRWTransportAgent.dll (Edge, MailBox) | DRWTransportAgent.dll (Edge, MailBox, CAS) |
| 2016 | DRWTransportAgent.dll (Edge, MailBox) | DRWTransportAgent.dll (Edge, MailBox) |

Si, après l'installation de Dr.Web, il est nécessaire d'installer sur le serveur de boîtes aux lettres (Mailbox) les agents d'antispam fournis avec Microsoft Exchange Server, vous devez baisser la priorité des agents Dr.Web. Ainsi, la messagerie est analysée d'abord par les agents Microsoft Exchange Server et puis par les agents Dr.Web.

## 6.1. Support VSAPI

Les solutions antivirus pour les serveurs Exchange utilisant VSAPI vérifient tous les e-mails arrivant sur le serveur avant leur envoi au client. L'analyse est réalisée en trois modes :

- proactif (proactive) ;

- sur demande (on-demand) ;
- tâche de fond (background).

Si l'adresse de l'expéditeur du message est présent dans la liste des valeurs de la variable TrustedEmails, le message est exclu du scan antivirus et il est considéré comme sain.

## Scan proactif

Tous les e-mails arrivant sur le serveur Exchange sont mis dans la file d'attente de l'analyse par l'application antivirus. Les messages dans la file reçoivent la même priorité inférieure. Si la priorité ne change pas, l'analyse est effectuée selon le principe «first in, first out» (FIFO), par ordre d'arrivée des messages.

## Scan sur demande

Si la priorité d'un message a été élevée, c'est qu'il y a une requête du client de messagerie pour ce message, il sera donc analysé de manière anticipée, compte tenu du fait que la file d'attente pour l'analyse est traitée par plusieurs flux. Une priorité inférieure des nouveaux e-mails arrivés permet de garantir que leur analyse n'aura pas d'impact sur le scan des messages ayant une priorité supérieure.

Le scan proactif ou sur demande assurent la vérification de tous les e-mails transitant via le serveur. Dans ce cas-là, le système de priorité permet de répartir la charge sur le serveur de manière optimale et de minimiser le délai d'attente d'un message par le client.

## Scan en tâche de fond

Dans le mode de scan en tâche de fond, les messages en stock sont analysés, y compris les messages se trouvant dans la banque de dossiers publics. Ceci permet de détecter les virus qui ont pénétré dans le stockage avant l'installation de Dr.Web ainsi que les virus auparavant inconnus se trouvant dans des e-mails vérifiés avant la dernière mise à jour des bases virales. Ce mode de scan est activé par l'administrateur Exchange avec un jeu de clés de registre et il est géré à l'aide de la tâche **Doctor Web For Exchange Start Background Scanning Task** dans le planificateur de tâches Windows. Par défaut, la tâche est lancée tous les jours à 01.15.

Pour en savoir plus sur les paramètres du scan antivirus utilisant VSAPI, consultez l'Annexe Paramètres du scan antivirus Microsoft Exchange Server.

En cas d'utilisation partagée de VSAPI et des agents de transport sur un serveur, il est nécessaire de désactiver l'analyse des messages sortants par VSAPI lors de leur arrivée dans le système de transport depuis le stockage de messagerie. Vous pouvez désactiver cette analyse en spécifiant la valeur 0 pour le paramètre TransportExclusion dans la rubrique du registre `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\VirusScan`.

## 6.2. Rôles de serveur

Exchange Server 2007/2010/2013 SP1/2016 peut être installé en plusieurs configurations déterminant le mode de fonctionnement du serveur et des fonctions supportées. Pour cela, on spécifie les rôles du serveur lors du déploiement du serveur Exchange.

Exchange Server 2007/2010 et 2013 SP1 permet de créer cinq rôles de serveur : le serveur de boîtes aux lettres (Mailbox), le serveur d'accès au client (Client Access), le serveur-concentrateur de transport (Hub), le serveur du système de messagerie unifié (Unified Messaging) et le serveur de transport (Edge Transport). Exchange Server 2016 permet de créer deux rôles de serveur : serveur de boîtes aux lettres et serveur de transport Edge.

Les rôles de serveur indiqués ci-dessous supportent l'analyse antivirus et antispam :

- **Serveur de boîtes aux lettres** (Mailbox) fournit les services principaux, notamment le stockage de données et le support des dossiers client, il permet également d'effectuer une analyse antivirus des messages via l'interface VSAPI ;
- **Serveur-concentrateur de transport** (Hub) répartit les messages au sein de l'entreprise et permet d'appliquer aux messages les politiques de sécurité, d'effectuer l'analyse antivirus et le filtrage antispam ;
- **Serveur de transport** (Edge) – ce rôle est attribué à un serveur autonome se trouvant dans la zone démilitarisée et qui n'utilise pas les ressources intérieures de l'entreprise (excepté la synchronisation unilatérale avec Active Directory pour enregistrer la topologie des serveurs de concentrateurs transport) ce qui permet à ce serveur d'être utilisé comme une passerelle SMTP et d'effectuer l'analyse antivirus et antispam.

Dr.Web peut être installé sur le serveur pour lequel on a spécifié l'un de ces rôles ou leur combinaison.

Dans Microsoft Exchange Server 2013, le concept de rôles de serveur n'est plus utilisé. On est revenu à l'architecture Frontend–Backend, c'est pourquoi l'analyse antispam et antivirus sera toujours effectuée par les agents au niveau du transport SMTP.

## 6.3. Agents de transport

Le concept d'organisation de Microsoft Exchange 2007/2010/2013/2016 utilise une structure modifiée des événements SMTP. Aux étapes différentes de l'acheminement SMTP, le flux de messages est traité par des agents de transport dotés des fonctions diverses.

Lorsque un message arrive sur le serveur, il est redirigé via le réseau de transport SMTP, dans ce cas, pour chaque événement SMTP, plusieurs agents de transport peuvent être enregistrés. Ces agents reçoivent l'accès au message et peuvent réaliser certaines actions sur ce message conformément à leurs priorités. Chaque agent effectue son analyse et transmet ensuite le message à l'agent suivant. Ainsi, les agents de transport permettent de réagir sur les événements liés à la réception du message et à son acheminement ultérieur dans le réseau.

Il existe deux types d'agents de transport :

- **SMTP Receive Agent** permet de réagir aux événements survenant lors de la réception d'un message via SMTP ;
- **Routing Agent** permet de réagir aux événements survenant pendant le routage du message.

Exchange Server 2007/2010/2013/2016 permet d'attribuer une priorité aux agents de transport et de gérer ainsi l'ordre de traitement des messages par les agents. L'ordre de succession des agents est déterminé ainsi non seulement pas la séquence des événements auxquels ils sont associés mais aussi par la priorité attribuée au sein d'un événement SMTP.

Les agents de transport permettent d'intégrer Dr.Web lors du traitement du courrier électronique, notamment pour effectuer l'analyse antivirus et antispam des messages.

En cas d'utilisation des agents de transport, Dr.Web effectue l'analyse antivirus et antispam uniquement dans des messages reçus par le serveur via le protocole SMTP (si vous avez la licence Antivirus+Antispam).

### 6.3.1. Agents de transport d'antispam

Les agents de transport de l'antispam réagissent à l'événement SMTP **OnEndOfData** correspondant à la fin de la réception du contenu du message par le serveur.

Le message est tout de suite exclu de l'analyse antispam et il est considéré comme sain, si :

- le domaine de l'expéditeur est présent dans la liste des valeurs de la variable TrustedDomains ;
- l'adresse de l'expéditeur est présente dans la liste des valeurs de la variable SpamTrustedEmails.

Contrairement à la liste blanche d'Antispam qui forme la politique d'application des exclusions compte tenu des adresses d'expéditeurs et de destinataires (notamment si l'expéditeur et le destinataires se trouvent sur le même domaine et que l'adresse de l'expéditeur est mentionnée dans la liste blanche, le message peut être considéré comme spam), les variables TrustedDomains et SpamTrustedEmails excluent sans réserve le message de l'analyse antispam. Il faut ajouter des domaines et des adresses à la liste des valeurs de variables uniquement en cas de nécessité absolue. Sinon il faut utiliser la liste blanche de la console Dr.Web Administrator Web Console.

Si le domaine ou l'adresse de l'expéditeur n'est pas fiable, le message est mis en file d'attente pour l'analyse. A la fin de l'analyse, si le message est considéré comme spam, il peut être supprimé, bloqué, redirigé vers une autre boîte aux lettres, marqué comme Junk email ou bien un préfixe peut être ajouté au sujet du message. Tous ces messages sont enregistrés dans la rubrique d'événements de la Console web d'administration et dans le journal d'événements du serveur.

Si le message est supprimé en tant que spam ou bloqué comme un message non conforme aux règles de filtrage, l'agent de transport interrompt la connexion au client ou créée la réponse

RejectMessage au contenu suivant Dr.Web AntiSpam Agent: Message was rejected as spam**.** Avec la Console web d'administration, vous pouvez sélectionner l'action à appliquer. Dans tous les cas, le message n'atteint pas le destinataire.

Si le message est redirigé vers une autre boîte aux lettres ou marqué comme Junk email, le préfixe supplémentaire X-header est ajouté à son en-tête.

L'en-tête **X-DrWeb-RedirectTo** contenant l'adresse du nouveau destinataire est ajouté au message redirigé. Cet en-tête est destiné à l'agent de transport antivirus qui après avoir analysé le message et après l'avoir jugé sain, supprime toute la liste des destinataires initiaux en les remplaçant par l'adresse indiquée dans l'en-tête. Le message ne sera pas délivré aux destinataires initiaux. Le message sera délivré aux destinataires initiaux s'il est marqué comme Junk e-mail. Dans ce cas, l'en-tête **X-MS-Exchange-Organization-SCL** sera ajouté au message. La valeur de l'en-tête contient le taux de méfiance au message. Cet en-tête est compris par les clients Microsoft et le serveur Microsoft Exchange Server. Si la valeur du taux de méfiance est supérieure à 4 mais inférieure à 7, les clients de messagerie d'utilisateurs peuvent déplacer ce message vers le dossier **Junk** (s'ils sont configurés correctement). Il faut noter que si la valeur du taux est supérieure à 7, le message peut être rejeté par le système de transport du serveur Microsoft Exchange Server.

L'ajout du préfixe à l'en-tête du message considéré comme spam n'influence pas sa livraison. Les destinataires peuvent configurer pour leur client de messagerie les règles de traitement des messages portant ce préfixe.

### 6.3.2. Agents de transport antivirus

Les agents antivirus réagissent à l'événement SMTP **OnSubmittedMessage** correspondant à la mise en file d'attente pour le traitement par le système de transport du serveur. Aucune exclusion de traitement par cet agent n'est prévue pour les messages.

Si l'adresse de l'expéditeur du message est présente dans la liste des valeurs de la variable TrustedEmails, le message est exclu du scan antivirus et il est considéré comme sain.

Le cycle d'analyse de l'agent antivirus représente l'analyse antivirus cohérente du corps de message et de toutes les pièces jointes. Un message infecté peut être supprimé, bloqué ou déplacé en quarantaine (pour les objets suspects il existe également la possibilité de les laisser passer sans appliquer aucune action). Tous les événements sont enregistrés dans la rubrique des événements de la console Dr.Web Administrator Web Console et dans le journal des événements du serveur.

Si la suppression est spécifiée pour les objets infectés, après la détection du premier objet infecté, le scan de pièces jointes est interrompu et un événement de suppression du message est envoyé au système de transport du serveur. Les événements de suppression sont enregistrés dans la section des événements de la console Dr.Web Administrator Web Console et dans le journal d'événements du serveur, mais ni les expéditeurs, ni les destinataires ne sont pas informés de la suppression du message. C'est le moyen le plus rapide de réaction aux infections, pourtant le moyen le plus sûr du point de vue de la perte de données possible est le

déplacement des objets infectés en Quarantaine. De plus, si le serveur supporte le protocole EWS (Exchange Web Services), il existe une possibilité de configurer avec la console Dr.Web Administrator Web Console et la console Dr.Web CMS Web Console l'envoi des notifications à une adresse électronique pour tous les cas de suppression des messages infectés.

Si la pièce jointe est bloquée en tant que non conforme aux règles de filtrage et que le déplacement en Quarantaine est spécifié pour les objets infectés, tous les objets infectés ou les pièces jointes bloquées sont remplacés dans le message initial par les fichiers texte décrivant la raison de suppression de la pièce jointe. Ensuite, la présence de l'en-tête **X-DrWeb-RedirectTo** est vérifiée dans le message désinfecté. Si cet en-tête n'est pas trouvé, le message sera délivré aux destinataires. Si le message doit être redirigé, tous les destinataires reçoivent une notification **SmtpResponce** au contenu suivant **«Dr.Web AntiVirus Agent: Message was redirected as spam.»**. Dans ce cas, le message sans pièces jointes infectées est envoyé à l'adresse indiquée dans la valeur de l'en-tête **X-DrWeb-RedirectTo**.

## 6.4. Services de Dr.Web

Sept services principaux assurent le fonctionnement de Dr.Web :

- **Dr.Web CMS** supporte le système à répartition de gestion des composants des applications, en réalisant les fonctions essentielles de contrôle de fonctionnement des modules et leur diagnostic fonctionnel. Le service supporte la base de données des paramètres des composants de l'application, la base des événements et surveille les statistiques des paramètres des composants.
- **Dr.Web CMS Web Console** contient le serveur web intégré qui fournit la possibilité de lancer les consoles d'administration de l'application dans le navigateur.
- **Dr.Web for MSP Component Host** instance tous les composants auxiliaires de l'application requis lors du fonctionnement.
- **Dr.Web for MSP Scanning Service** prépare les objets interceptés par les filtres de l'application au scan antivirus et traite les résultats obtenus.
- **Dr.Web for MSP Requests Queue** maintient la file d'attente asynchrone des requêtes d'exécution de tâches de l'application admettant l'exécution reportée.
- **Dr.Web Scanning Engine** contient le noyau du système antivirus Dr.Web.
- **Dr.Web SSM** contrôle le fonctionnement des applications tournant sous la plateforme CMS étant responsable du redémarrage des services principaux.

Les services Dr.Web Scanning Engine, Dr.Web CMS et Dr.Web SSM sont lancés juste après l'installation de l'application. Les autres services sont lancés selon les besoins.

En cas de redémarrage manuel des services, il est important de respecter le bon ordre d'arrêt des services Dr.Web CMS et Dr.Web SSM à cause des relations établies entre eux : d'abord il faut arrêter le service Dr.Web SSM, puis le service Dr.Web CMS. Une fois les deux services arrêtés, il suffit de lancer le service Dr.Web SSM, après quelque temps, l'application sera automatiquement opérationnelle.

# 7. Console Web d'Administration

Le fonctionnement de Dr.Web peut être configuré avec la console Dr.Web Administrator Web Console (voir Figure 1).

### Pour lancer la console Dr.Web Administrator Web Console

Pour le fonctionnement correct de la console Dr.Web Administrator Web Console, il est nécessaire d'utiliser les navigateurs suivants :

- Internet Explorer 11 ou supérieur ;
- Chrome ;
- Microsoft Edge 20 ou supérieur.

---

Pour le fonctionnement correct de Dr.Web Administrator Web Console dans le navigateur Internet Explorer, il est nécessaire d'autoriser l'utilisation de la technologie AJAX en désactivant la sécurité renforcée pour les administrateurs :

- Sous Windows Server 2003 : dans la section **Panneau de configuration** -> **Ajout/suppression de programmes** -> **Ajouter ou supprimer les composants Windows** décochez la case **Configuration de sécurité renforcée d'Internet Explorer** et cliquez sur **Suivant**. Puis cliquez sur **Terminer**.
- Sous Windows Server 2008 : ouvrez **le Gestionnaire de serveur** et cliquez sur **Paramétrer la configuration de sécurité renforcée d'Internet Explorer**, puis sur une option correspondante dans la section **Administrateurs**.
- Sous Windows Server 2012 : ouvrez **le Gestionnaire de serveurs**, passez sur l'onglet **Serveur local** et sélectionnez **Configuration de sécurité renforcée d'Internet Explorer**, puis cliquez sur une option correspondante dans la section **Administrateurs**.

Pour lancer la console Dr.Web Administrator Web Console, ouvrez la page suivante dans le navigateur :

`https://`<*Exchange Server address*>`:2080/exchange`,

où <*Exchange Server address*> – adresse IP du serveur Exchange.

Pour accéder à la page de Dr.Web Administrator Web Console, il est nécessaire d'entrer les données du compte administrateur. Vous pouvez ajouter, modifier et supprimer les comptes administrateurs à l'aide de la console Dr.Web CMS Web Console.

Lors du premier démarrage de Dr.Web Administrator Web Console entrez les données du compte par défaut : le nom d'utilisateur **root** et le mot de passe **drweb**.

---

Si vous ne réussissez pas à ouvrir Dr.Web Administrator Web Console sur un ordinateur distant, assurez-vous que les règles permettant l'accès sont créées pour le Pare-feu Windows.

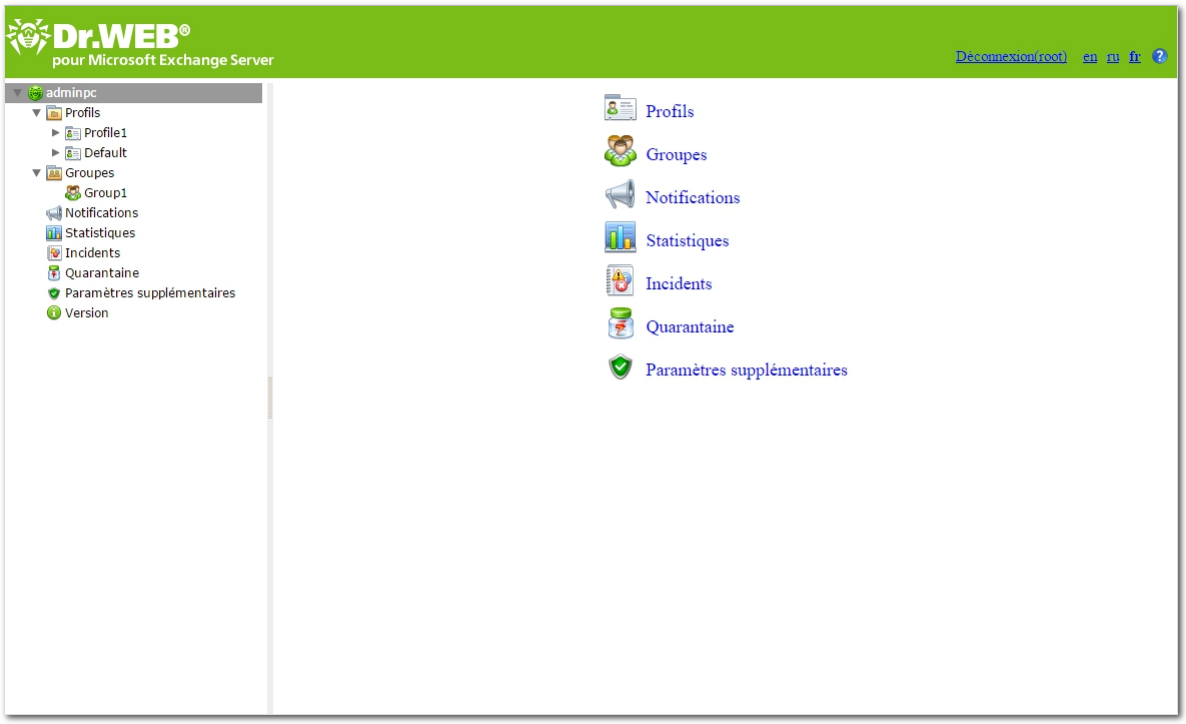


**Figure 1. Dr.Web Administrator Web Console**

### Interface

Dr.Web Administrator Web Console comprend deux parties :

1. Arborescence de la console qui fournit la navigation sur les sections des paramètres du logiciel.
2. Zone d'information, où les paramètres de la section sélectionnée sont affichés et où vous pouvez les configurer.

En haut de la zone d'information, vous trouverez l'option permettant de changer de langue de la console Dr.Web Administrator Web Console. Vous pouvez choisir entre le russe, l'anglais et le français. De plus, à droite de l'option de changement de la langue, il y a une option permettant d'afficher la rubrique d'aide sur cette console.

### Administration

Les niveaux suivants d'accès à la console Dr.Web Administrator Web Console :

- avec la possibilité de configurer les paramètres ;
- sans possibilité de configurer les paramètres.

On peut déterminer le niveau d'accès lors de l'ajout d'un nouveau compte administrateur.

## 7.1. Groupes et profils

Pour faciliter l'organisation de la protection antivirus pour l'environnement Exchange, Dr.Web permet de créer des groupes de clients et de leur attribuer des profils. Un profil est un ensemble de paramètres configurables relatifs au traitement des messages et déterminant le mode de protection de l'environnement Exchange. La configuration du profil se trouve dans la section **Profils** de l'arborescence de la console Dr.Web Administrator Web Console. Cette section comprend les sous-rubriques suivantes :

- Scan – cette sous-rubrique vous permet de configurer le composant principal de détection de virus.
- Antispam – ici vous pouvez configurer l'Antispam (les paramètres de cette rubrique ne sont accessibles qu'avec la version « Antivirus + Antispam », à condition que vous disposiez d'un fichier clé approprié (voir Fichier clé de licence).
- Filtrage – cette sous-rubrique vous permet de créer des règles de filtrage pour les messages électroniques.

Tout profil peut être attribué à un groupe de clients. Ces groupes sont créés dans la section **Groupes** de l'arborescence de console.

### 7.1.1. Création et configuration des profils

Lors de l'installation, Dr.Web crée automatiquement le profil standard **Default** que vous ne pouvez pas supprimer ou renommer. Ce profil sera appliqué à tous les messages à moins que vous ne créiez un autre profil et ne l'attribuiez à un certain groupe de clients. Lors de la création d'un nouveau profil, ses paramètres prennent les valeurs actuelles du profil standard.

Pour gérer les profils existants et créer de nouveaux profils, passez dans la zone d'information de la section **Profils**, en choisissant l'élément **Profils** dans l'arborescence de la console Dr.Web Administrator Web Console (voir Figure 2).


**Figure 2. Rubrique Profils**

La liste comprend des informations sur les paramètres de chaque profil, la priorité du profil est déterminée en fonction de sa position dans le tableau.

**Pour créer un nouveau profil**

1. Cliquez sur le bouton **Créer un profil** se trouvant au-dessus de la liste des profils existants.

Sinon, afin de créer un nouveau profil, vous pouvez également cliquer droit sur l'élément **Profils** dans l'arborescence de la console et sélectionner **Créer un profil** dans le menu contextuel qui apparaît.

2. Indiquez le nom du profil dans la fenêtre affichée. Le nouveau profil sera affiché dans l'arborescence au-dessous de l'option **Profils**. Si un profil ayant le même nom existe déjà, alors il ne sera pas créé.

**Pour modifier le nom du profil**

Sélectionnez un profil nécessaire dans la liste se trouvant dans la zone d'information de la section **Profils**, puis cliquez sur **Renommer le profil** ;

**Pour supprimer un profil**

Sélectionnez le profil dans la liste se trouvant dans la zone d'information de la section **Profils**, puis cliquez sur le bouton **Supprimer le profil**.

Sinon, afin de supprimer ou renommer le profil, cliquez droit sur le nom de ce profil dans l'arborescence de la console et dans le menu contextuel qui apparaît, sélectionnez votre choix.

Par défaut, les paramètres du profil créé seront similaires à ceux du profil **Default**.

**Pour modifier les paramètres du profil**

Sélectionnez un nom du profil dans l'arborescence de la console Dr.Web Administrator Web Console et passez dans la section nécessaire : Scan, Antispam ou Filtrage.

## 7.1.1.1. Priorité de profil

Chaque profil a une certaine priorité spécifiée par l'administrateur. Si le client fait partie de plusieurs groupes ayant des profils différents, le profil avec la priorité supérieure sera utilisé lors du traitement des messages reçus ou envoyés par ce client.

Pour changer de priorité de profil, dans la zone d'information de la rubrique **Profils**, déplacez les profils en question vers le haut ou vers le bas de la liste. Utilisez les boutons ↑ et ↓ se trouvant à droite de la liste pour déplacer les profils. Plus haut est situé le profil, plus haute est sa priorité.

Le profil standard a toujours la priorité inférieure, il ne peut pas être déplacé au-dessus de la ligne la plus basse dans la liste des profils.

## 7.1.1.2. Scan

Vous pouvez configurer le processus d'analyse dans la rubrique **Scan**. Le changement des paramètres réunis dans cette rubrique détermine les types d'objets à vérifier et par conséquent, le niveau de protection antivirale. D'autre part, l'augmentation du nombre de types d'objets à analyser peut diminuer les performances du serveur.

### Pour configurer les paramètres du scan

1. Sélectionnez l'élément **Scan** pour le profil que vous configurez dans l'arborescence de la console Dr.Web Administrator Web Console. La zone d'information sera ouverte pour la configuration du scan (voir Figure 3).

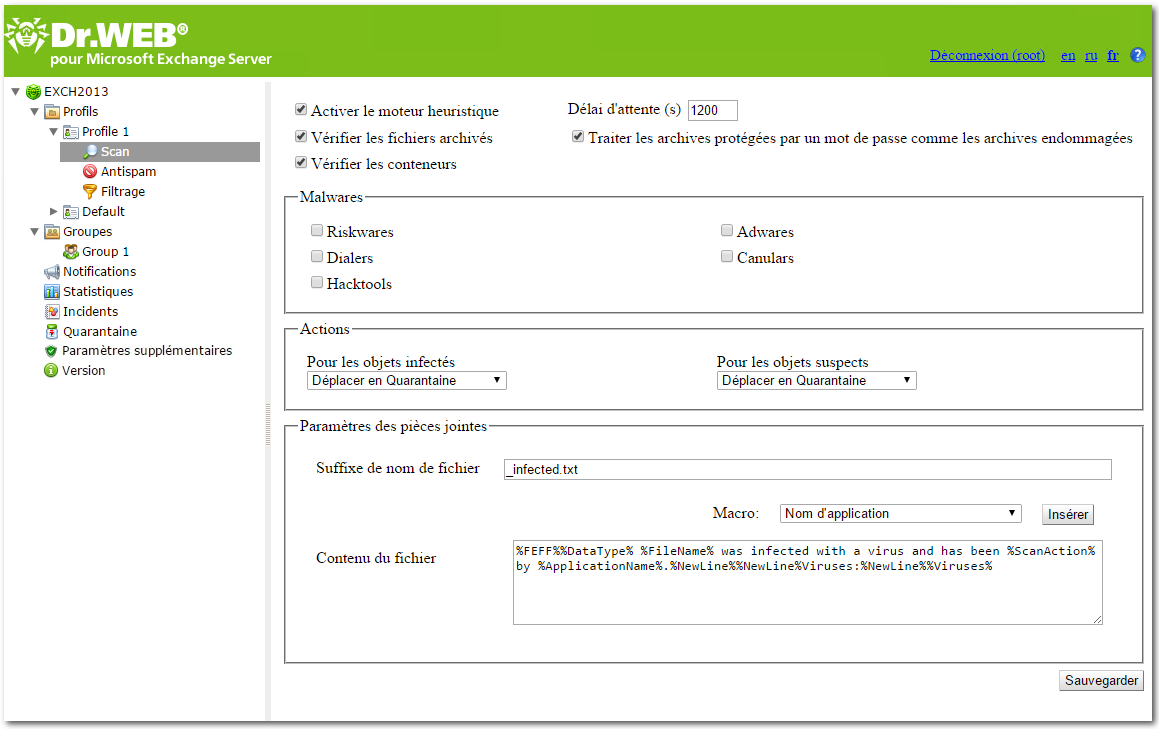


**Figure 3. Rubrique de configuration du scan**

2. Par défaut, l'analyse heuristique et l'analyse des archives et des conteneurs joints sont activées. Ceci assure une protection très fiable mais entraîne une certaine diminution des performances du serveur. Pour désactiver ces modes, décochez les cases **Activer l'analyse heuristique**, **Vérifier les fichiers dans des archives** et **Vérifier les conteneurs** en haut de la zone d'information de la rubrique **Scan**.

Il n'est pas recommandé de désactiver l'analyseur heuristique et l'analyse des archives jointes puisque cela peut considérablement affaiblir le niveau de protection antivirus.

Contre ces cases, il y a un champ de saisie permettant de spécifier un délai d'attente pour l'analyse d'un fichier. A l'expiration du délai, le fichier est considéré comme corrompu. Par défaut, la valeur de 1200000 ms est spécifiée. Vous pouvez la modifier, si nécessaire.

La case **Traiter les archives protégées par mot de passe comme endommagées** détermine si le programme ignore ce type d'archive ou les actions spécifiées pour les objets endommagés qui seront appliquées. Avec la console CMS, vous pouvez spécifier les types d'objets qui seront considérés comme endommagés.

3. Dans l'ensemble des paramètres **Programmes malveillants**, vous pouvez spécifier les types d'objets malveillants à rechercher dans les messages. Pour cela, cochez les cases correspondantes. L'action spécifiée pour les objets infectés sera appliquée aux programmes sélectionnés.
4. Dans l'ensemble des paramètres **Actions**, spécifiez les actions à appliquer aux objets infectés et suspects en utilisant les listes déroulantes correspondantes. Vous pouvez sélectionner l'une des actions suivantes :
   - **Déplacer en Quarantaine**. Le message passera sans traitement mais le fichier joint sera mis en quarantaine (voir Gestion de la quarantaine).
   - **Supprimer**. L'objet sera supprimé.
   - **Laisser passer**. On laisse passer le message et on envoie une notification à l'utilisateur (l'action est applicable uniquement aux objets suspects).
   - **Archiver**. Le fichier emboité infecté sera renommé en **inf*.tmp**, où * est un jeu aléatoire de symboles. Ensuite, le fichier sera empaqueté en archive zip. Dans ce cas, une copie du fichier sera déplacée en quarantaine. Dans la rubrique Paramètres avancés, vous pouvez indiquer le mot de passe pour cette archive et la taille maximum du fichier archivé.

Par défaut, pour tous types d'objets, l'action **Déplacer en quarantaine** est sélectionnée.

5. Dans l'ensemble de paramètres **Paramètres des fichiers joints**, vous pouvez modifier le suffixe du nom de fichier qui est joint au message après la réalisation de l'action sélectionnée. Dans le champ **Contenu du fichier**, vous pouvez modifier le contenu du fichier texte joint. Lors de l'édition du texte, vous pouvez utiliser des macros. Sélectionnez une macro nécessaire dans la liste **Macro**, puis cliquez sur **Insérer**.
6. Après avoir apporté toutes les modifications aux paramètres d'analyse, cliquez sur **Sauvegarder**.

### 7.1.1.3. Antispam

Avant le démarrage de l'antispam, les adresses des expéditeurs et destinataires sont analysées afin de savoir si elles appartiennent aux listes noire et blanche de la section **Antispam**.Puis le composant Antispam vérifie le message.

L'Antispam analyse les contenus des messages et détermine s'il s'agit de spam ou pas selon la valeur de potentialité de spam obtenue grâce à plusieurs critères. Selon les résultats de l'analyse, l'Antispam assigne un nombre entier au message (*score*). Un nombre important signifie que le message est probablement un spam. Vous pouvez modifier la valeur du seuil utilisée pour la détection de spam dans la section Dr.Web CMS Web Console.

Merci d'envoyer les faux positifs de l'Antispam à vrnonspam@drweb.com et les spam non identifiés à vrspam@drweb.com.

Vous pouvez configurer le fonctionnement de l'Antispam dans la rubrique paramètres de l'**Antispam** qui est accessible uniquement au sein de la version « Antivirus + Antispam ». Si votre fichier clé autorise l'utilisation du composant Antispam, le filtrage du spam est activé par défaut (la case **Activer l'Antispam** en haut de la zone d'information de la rubrique **Antispam** doit être cochée).

Si les paramètres se trouvant dans la rubrique **Antispam** sont inaccessibles, il est fort probable que votre licence ne couvre pas le composant Antispam (voir Fichier clé de licence).

Pour vérifier si le composant Antispam est supporté par votre licence, ouvrez votre fichier clé (le fichier drweb32.key se trouvant dans le dossier %ProgramFiles%\DrWeb for Exchange\) dans un éditeur texte et trouvez le paramètre SpamFilter.Si SpamFilter=Yes, cela signifie que votre licence autorise l'utilisation du composant Antispam, si SpamFilter=No, le composant Antispam n'est pas supporté.

L'édition du fichier clé le rend invalide ! N'enregistrez pas le fichier clé lors de la fermeture de l'éditeur texte.

### Pour configurer l'Antispam

1. Sélectionnez l'élément **Antispam** pour le profil à configurer dans l'arborescence de la console Dr.Web Administrator Web Console. La zone d'information de la rubrique **Antispam** (voir Figure 4) sera ouverte.

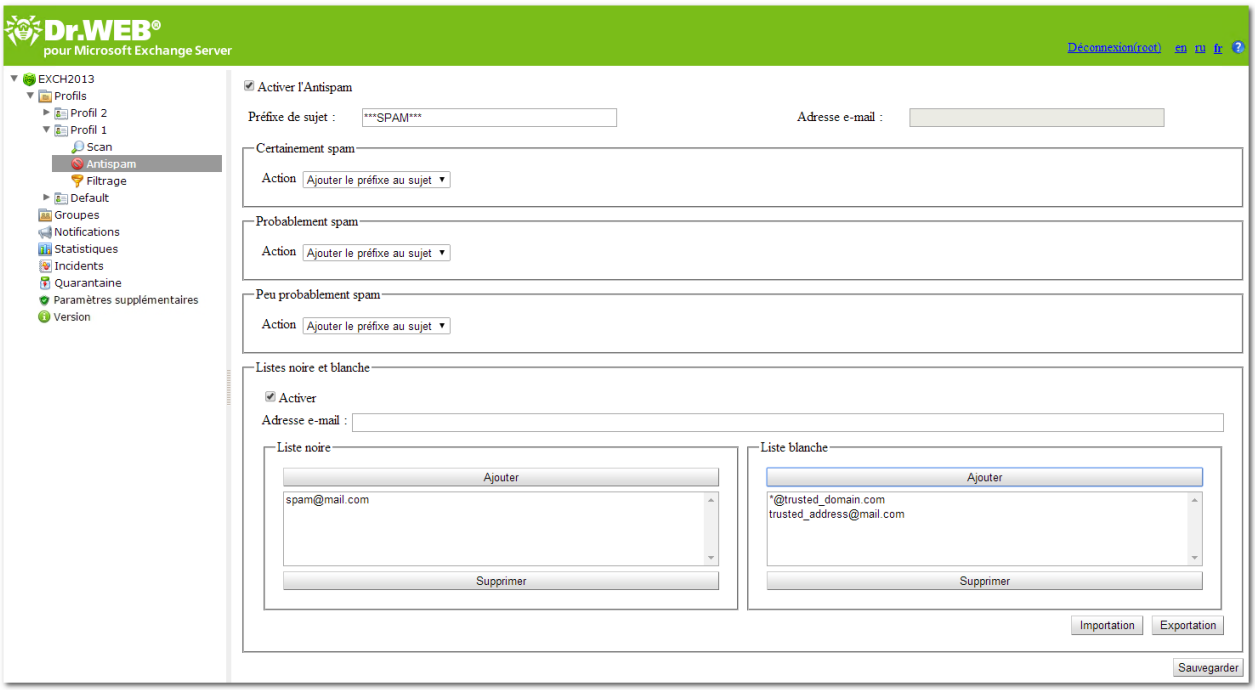


**Figure 4. Rubrique de paramètres de l'Antispam**

2. Pour désactiver l'Antispam, décochez la case **Activer l'Antispam**. Dans ce cas, tous les paramètres du composant Antispam deviennent inaccessibles. Pour activer le filtrage du spam, cochez la case **Activer l'Antispam**.
3. Dans le champ **Préfixe**, vous pouvez modifier le préfixe à ajouter au sujet du message classé comme spam. Par défaut, le préfixe installé est ***** SPAM *****.
4. Dans le champ **Adresse e-mail**, spécifiez l'adresse e-mail pour rediriger les messages.
5. Dans les champs ci-dessous, vous pouvez spécifier des actions du logiciel effectuées sur les messages en fonction de la probabilité avec laquelle ces messages sont considérés comme spams (**Certainement du spam**, **Probablement du spam**, **Peu probablement du spam**). Pour cela, sélectionnez les actions souhaitées dans les listes déroulantes correspondant à chaque catégorie :
   - **Ajouter le préfixe au sujet**. Le préfixe spécifié dans le champ **Préfixe sera ajouté au sujet**.
   - **Laiser passer**. Le message passera sans traitement et sera délivré au destinataire ;
   - **La valeur de l'en-tête contient le taux de méfiance par rapport au message**. Si la valeur est supérieure à 4 mais inférieure à 7, les clients de messagerie pour lesquels les paramètres nécessaires sont spécifiés pourront déplacer ce message dans le dossier de courrier indésirable. **L'en-tête de service** X-MS-Exchange-Organization-SCL est ajouté au message.

- **Rediriger**. Le message sera transféré à l'adresse indiquée dans le champ **Adresse e-mail** ;
- **Bloquer**. La transmission du message sera bloquée.

6. Dans la rubrique **Listes noire et blanche**, vous pouvez configurer les listes des adresses de confiance et des adresses suspectes :
   - cochez la case **Ajouter** pour activer les listes. Vous pouvez ajouter des adresses e-mail de confiance dans la liste blanche. Les messages provenant de ces adresses ne seront pas vérifiés. Si vous ajoutez l'adresse à la liste noire, le statut **Certainement du spam** sera attribué à tous les e-mails provenant de l'adresse en question.
   - pour ajouter une adresse e-mail, saisissez-la dans le champ **E-mail**, puis cliquez sur **Ajouter dans la liste blanche** ou **Ajouter dans la liste noire** pour l'ajouter dans la liste correspondante.
   - pour supprimer une adresse e-mail de la liste, sélectionnez-la dans la liste et cliquez sur **Supprimer de la liste blanche** ou **Supprimer de la liste noire** ;
   - vous pouvez utiliser les boutons **Exportation** et **Importation** pour sauvegarder les listes dans un fichier spécialisé ayant l'extension **.lst** et pour les télécharger depuis un fichier. Lors de l'édition et création manuelle des listes noire et blanche, les adresses e-mail doivent être accompagnées du préfixe **« + »** (pour ajouter l'adresse dans la liste blanche) ou **« - »** (pour ajouter l'adresse dans la liste noire), par exemple : **+trusted_address@mail.com** et **-distrusted_address@mail.com**, le fichier texte doit être enregistré avec l'extension **.lst** au format Unicode.

Vous pouvez utiliser le symbole de remplacement « * » à la place d'une partie de l'adresse (par exemple, ***@domain.org** désigne toutes les adresses dans le domaine domain.org).

Dans certains cas, l'ajout du domaine à la liste blanche par le moyen susmentionné peut échouer. Pour exclure ce domaine de la vérification à la recherche de spam, il faut l'ajouter dans la liste des valeurs de la variable TrustedDomains.

7. Cliquez sur **Enregistrer** pour accepter toutes les modifications des paramètres de l'Antispam.

## 7.1.1.4. Filtrage

Dr.Web permet d'utiliser un système spécial de filtrage pour diminuer la charge sur le serveur de messagerie. Par exemple, en cas d'attaque spam, les messages de trop sont exclus du système de transport du serveur avant le scan antispam et antivirus. Pour le fonctionnement efficace des filtres, il est nécessaire de spécifier un ensemble optimal de règles de filtrage qui ne contient pas de règles contradictoires ou inutiles.

Avant le filtrage, le groupe auquel appartient l'expéditeur du message est déterminé. Si l'expéditeur du message appartient à un des groupes créés, les règles de filtrage spécifiées dans le profil du groupe correspondant lui seront appliquées. Si l'expéditeur du message n'appartient à aucun groupe, les paramètres du profil Default lui seront appliqués. Ainsi, s'il est

nécessaire que la règle de filtrage soit appliquée à tous les messages des expéditeurs non inclus dans des groupes, créez la règle dans les paramètres de filtrage du profil standard Default.

Si le profil de l'utilisateur ne contient pas de restrictions et que le message passe, le profil à appliquer est déterminé. Le profil s'applique pour le traitement ultérieur en fonction des adresses de destinataires. Chaque adresse de la liste des destinataires sera liée à son groupe (que ce soit le groupe AD ou la liste d'adresses) et le profil correspondant de paramètres sera déterminé pour chaque groupe. Le profil avec la priorité la plus élevée sera sélectionné pour appliquer le filtrage. Ainsi, si vous voulez que des restrictions particulières s'appliquent au groupe d'utilisateurs créé, ne créez pas les règles de filtrage dans le profil Default, mais créez pour ce groupe un profil à part.!:

S'il est nécessaire de créer des groupes de destinataires particuliers auxquels aucune restriction ne soit appliquée, ne créez aucune règle de filtrage dans le profil standard Default, car un message filtré conformément aux règles de filtrage du profil d'expéditeur sera exclue du traitement ultérieur par les profils de destinataires.

En premier lieu, chaque message est traité par l'agent de transport d'antispam. A cette étape, les règles de filtrage sont appliquées au message comme à un objet entier. Le filtrage est effectué par nombre d'expéditeurs, destinataires, par sujet, nombre de pièces jointes, etc. Après le filtrage, les messages non filtrés subissent l'analyse antispam (voir le Schéma 1).

Le deuxième agent de transport que le message rencontre sur son chemin est l'agent antivirus. A cette étape, les règles de filtrage sont appliquées au message comme à l'ensemble des fichiers, le corps du message est considéré comme un fichier. Le filtrage est effectué par taille de fichiers, leurs noms, leurs extensions, etc. Après le filtrage, les messages non filtrés subissent l'analyse antivirus (voir le Schéma 1).

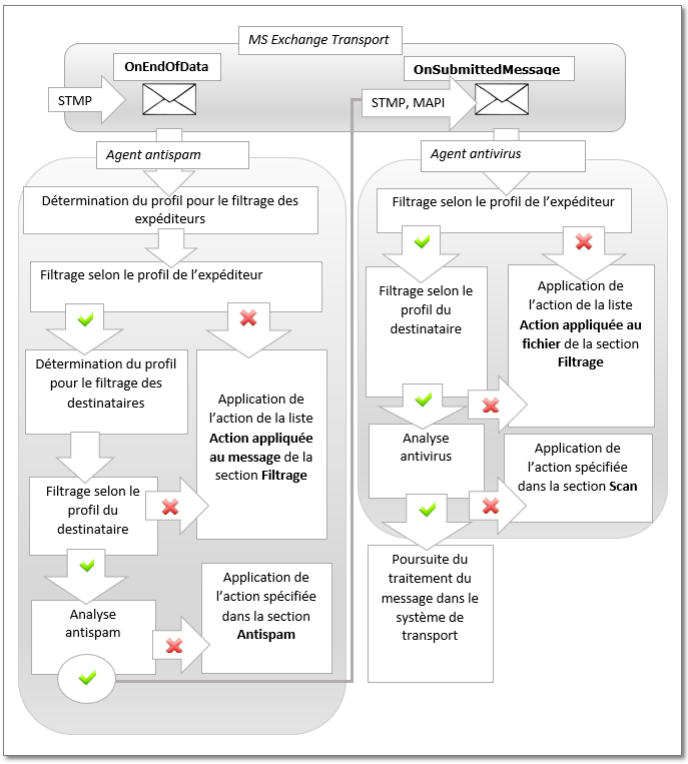


**Schéma 1. Filtrage des messages dans le système de transport**

Le filtrage des messages peut être paramétré dans la rubrique du profil **Filtrage** (voir Figure 5). Le fonctionnement des filtres est déterminé par un ensemble de règles ajoutées par l'administrateur. Les règles définissent les conditions de filtrage selon les caractéristiques principales des messages et des pièces jointes.

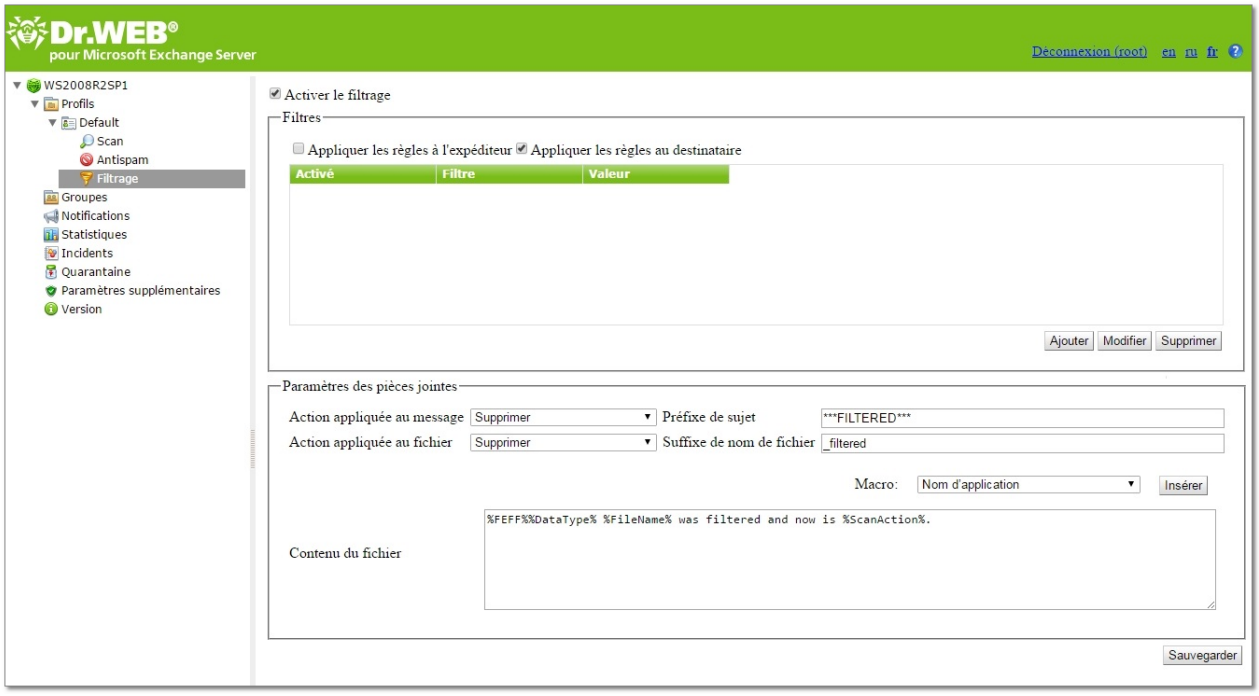


**Figure 5. Rubrique de la configuration du filtrage**

Si vous travaillez dans la section **Filtrage** pour la première fois, la liste des règles est vide. Vous pouvez créer et configurer les règles de filtrage.

### Pour configurer le filtrage des messages

1. Activez le filtrage. Pour cela, cochez la case **Activer le filtrage** en haut de la zone d'information de la rubrique **Filtrage**. Les paramètres seront ainsi accessibles.

   Les règles de filtrage peuvent s'appliquer à la fois à l'expéditeur et au destinataire. Elles peuvent également s'appliquer uniquement à l'expéditeur ou uniquement au destinataire. Par exemple, vous pouvez créer une règle dans laquelle le sujet de message contient le mot « Attention ». Si vous spécifiez cette règle uniquement pour l'expéditeur, vous ne pourrez pas envoyer les messages dont le sujet contient le mot « Attention ». Si vous spécifiez cette règle uniquement pour le destinataire, vous ne pourrez pas recevoir les messages dont le sujet contient le mot « Attention ». Si vous spécifiez cette règle pour l'expéditeur et le destinataire, vous ne pourrez ni envoyer, ni recevoir les messages dont le sujet contient le mot « Attention ».
2. Activez les filtres dans la liste en cochant les cases correspondantes. S'il n'y en a pas encore, vous pouvez les créer.
3. Dans la rubrique **Paramètres des pièces jointes** configurez les actions pour les messages avec pièces jointes.

   Vous pouvez sélectionner une des actions suivantes pour les messages :

   - **Supprimer** – pour supprimer le message ;
   - **Ajouter le préfixe au sujet** – pour laisser passer le message et ajouter à son sujet un préfixe spécifié dans le champ Préfixe de sujet.

Vous pouvez sélectionner une des actions suivantes pour les fichiers joints :

- **Déplacer en quarantaine** – pour déplacer les pièces jointes en quarantaine ;
- **Supprimer** – pour supprimer les pièces jointes.

Si cela est nécessaire, changez le préfixe à ajouter au sujet du message filtré dans le champ **Préfixe de sujet**. Par défaut le préfixe *****FILTERED***** est ajouté.

Si cela est nécessaire, changez le suffixe à ajouter au nom du fichier texte joint au message filtré dans le champ **Suffixe de nom de fichier**. Le suffixe par défaut est **_filtered.txt**.

Modifiez le texte du fichier joint dans le champ **Contenu du fichier**. Lors de l'édition du texte, vous pouvez utiliser des macros de la liste déroulante **Macro**.

### Pour configurer les règles de filtrage

1. Cliquez sur **Ajouter** sous la liste des règles. Dans la fenêtre **Règle de filtrage** (voir Figure 6) vous pouvez spécifier le nom de la règle et configurer ses conditions.

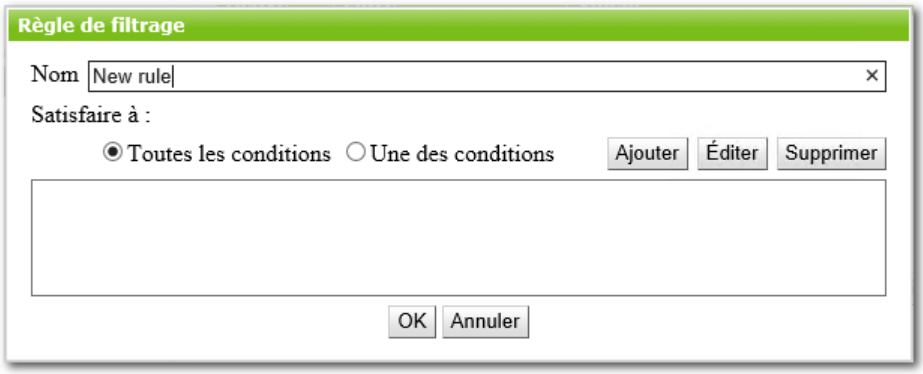


**Figure 6. Configuration des règles de filtrage**

2. Vous pouvez ajouter une ou plusieurs conditions de filtrage et spécifier si les messages doivent les respecter toutes ou n'importe laquelle d'entre elles. Pour ajouter une condition, cliquez sur **Ajouter**. Sélectionnez le type de condition, entrez sa valeur et spécifiez le type de respect à la condition de cette valeur. Le tableau ci-dessous contient les types de conditions, de respect et les valeurs possibles :

| Type de condition | Type de respect | Valeur |
|---|---|---|
| **Type de données** | Est égal<br>N'est pas égal | Fichier<br>Message |
| **Source des données** | Est égal<br>N'est pas égal<br>Contient<br>Ne contient pas<br>Correspond | Entré manuellement |

| Type de condition | Type de respect | Valeur |
|---|---|---|
| | Ne correspond pas | |
| **Destinataire des données** | Est égal<br>N'est pas égal<br>Contient<br>Ne contient pas<br>Correspond<br>Ne correspond pas | Entré manuellement |
| **Protocole** | Est égal<br>N'est pas égal | SMTP<br>MAPI |
| **Nombre de destinataires** | Est égal<br>N'est pas égal<br>Plus que<br>Pas plus que<br>Moins que<br>Pas moins que | Entré manuellement |
| **Nom de fichier** | Est égal<br>N'est pas égal<br>Contient<br>Ne contient pas<br>Correspond<br>Ne correspond pas | Entré manuellement |
| **Taille de fichier** | Est égal<br>N'est pas égal<br>Plus que<br>Pas plus que<br>Moins que | Entré manuellement (en octets) |

| Type de condition | Type de respect | Valeur |
|---|---|---|
| | Pas moins que | |
| **Sujet de message** | Est égal<br>N'est pas égal<br>Contient<br>Ne contient pas<br>Correspond<br>Ne correspond pas | Entré manuellement |
| **Pièce jointe** | Est égal<br>N'est pas égal | Faux<br>Vrai |

Si pour une des conditions **Source des données**, **Destinataire des données**, **Nom de fichier** ou **Sujet de message** le type de respect sélectionné est **Contient**, **Ne contient pas**, **Correspond** ou **Ne correspond pas,** vous pouvez utiliser les symboles de substitution « * » et « ? » pour remplacer toute séquence de symboles ou tout symbole particulier dans les valeurs à saisir.

3. Pour modifier ou supprimer une condition, sélectionnez-la dans la liste et cliquez sur **Supprimer** ou **Editer** respectivement.

### Exemple d'une règle de filtrage

Pour filtrer les fichiers de taille supérieure à 20000 octets, on peut utiliser une règle (voir Figure 7), qui consiste à accomplir simultanément les conditions suivantes :

| Type de condition | Type de respect | Valeur |
|---|---|---|
| **Type de données** | Est égal | Fichier |
| **Taille de fichier** | Plus que | 20000 |

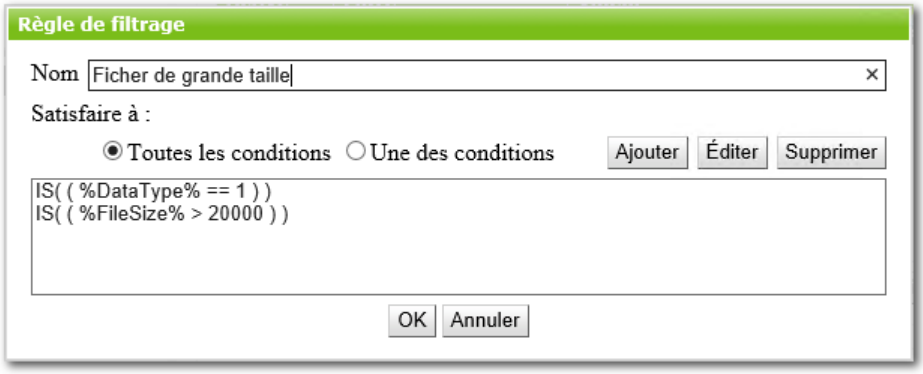


**Figure 7. Exemple d'une règle de filtrage**

**Pour modifier ou supprimer une règle de filtrage existante**

Sélectionnez la règle dans la liste et cliquez sur **Modifier** ou **Supprimer** se trouvant au-dessous de la liste des filtres.

Après avoir apporté toutes les modifications aux paramètres du filtrage, cliquez sur **Sauvegarder**.

Dans certains cas, le filtrage peut influencer la capacité du système de messagerie, c'est pourquoi il est recommandé :

- d'ajouter la variable TrustedEmails aux exclusions. Les comptes des boîtes de service sont stockés dans Active Directory, et leurs noms commencent par « HealthMailbox ».
- de ne pas créer de filtres qui servent à supprimer les fichiers de petite taille (moins de 1000 octets), pour que les notifications ne correspondent pas à ses conditions. Sinon, on peut rencontrer "le bouclage", quand la notification est refiltrée, à plusieurs reprises.

## 7.1.2. Gestion des groupes clients

Par défaut, Dr.Web applique les paramètres du profil standard à tous les clients. Si vous souhaitez appliquer les paramètres d'un autre profil (voir Création et configuration des profils) à certains clients, vous devez réunir les clients en question dans un groupe puis attribuer à ce groupe le profil créé. Ainsi, vous pouvez grouper tous les clients de sorte que chaque groupe possède ses paramètres de protection particuliers.

Lorsque vous ajoutez des groupes et attribuez les profils à des groupes existants, il faut veiller à ce que le profil standard soit toujours appliqué aux utilisateurs des groupes de type Security dans Active Directory. Pour réunir les utilisateurs du domaine en groupes pour attribuer d'autres profils de paramètres, il faut d'abord créer pour eux des groupes additionnels de type Distribution dans les paramètres d'Active Directory.

### 7.1.2.1. Création d'un nouveau groupe

Pour créer un nouveau groupe ou gérer un groupe existant, ouvrez la zone d'information de la section **Groupes**. Pour ce faire, sélectionnez l'élément **Groupes** dans l'arborescence de la console Dr.Web Administrator Web Console (voir Figure 8).


**Figure 8. Rubrique Groupes**

#### Pour créer un nouveau groupe

1. Dans la zone d'information de la rubrique **Groupes**, cliquez sur **Créer un groupe** sous la liste des groupes existants.

   Sinon, cliquez droit sur **Groupes** dans l'arborescence de la console et dans le menu contextuel qui apparaît, cliquez sur **Créer un groupe**.

2. Indiquez le nom du groupe dans la fenêtre affichée. Le nouveau groupe sera affiché dans l'arborescence de la console au-dessous de l'élément **Groupes**. Si un groupe ayant le même nom existe déjà, alors le nouveau groupe ne sera pas créé.

#### Pour modifier le nom de groupe

Sélectionnez le groupe nécessaire dans la liste de la zone d'information de la section **Groupes**, puis cliquez sur **Renommer le groupe**.

#### Pour supprimer un groupe

Sélectionnez le groupe dans la liste de la zone d'information de la section **Groupes** et cliquez sur **Supprimer le groupe**.

Sinon, pour supprimer ou renommer un groupe, cliquez droit sur le nom du groupe en question dans l'arborescence de la console Dr.Web Administrator Web Console et sélectionnez l'élément nécessaire dans le menu contextuel.

#### Pour accéder aux paramètres du groupe

Pour accéder à la zone d'information contenant les paramètres du groupe, sélectionnez le nom du groupe dans l'arborescence de la console Dr.Web Administrator Web Console.

Vous pouvez modifier le type de groupe sélectionné et lui attribuer un autre profil (voir Configuration des groupes).

Lorsque vous terminez la création et la configuration des groupes, cliquez sur **Sauvegarder**.

## 7.1.2.2. Configuration des groupes

Pour configurer les paramètres d'un groupe, cliquez sur son nom dans l'arborescence de la console Dr.Web Administrator Web Console (voir Figure 9). Vous pouvez spécifier la façon de la formation du groupe sélectionné : par l'entrée de la liste des adresses ou par la sélection de la liste des groupes AD. Dans la liste déroulante **Type**, vous pouvez sélectionner le type du groupe

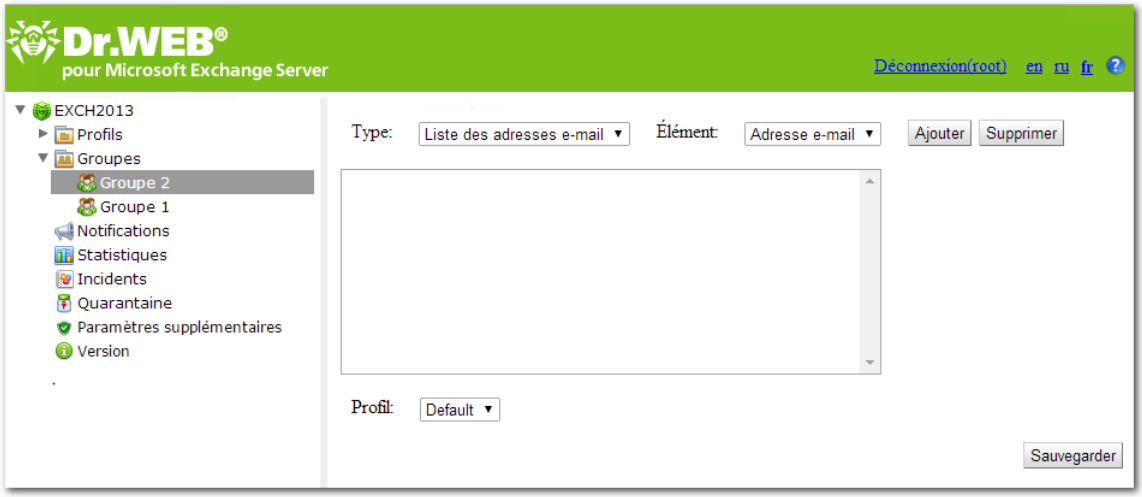


**Figure 9. Paramètres du groupe**

### Pour spécifier la liste des adresses

1. Dans la liste déroulante **Type**, cliquez sur **Liste des adresses e-mail**.
2. Pour ajouter une adresse dans la liste, cliquez sur **Ajouter**. Dans la fenêtre qui s'ouvre, entrez l'adresse et cliquez sur **OK**.
3. Pour supprimer une adresse de la liste, sélectionnez-la et cliquez sur **Supprimer**, puis confirmez la suppression de l'adresse sélectionnée.

> Vous pouvez utiliser les symboles de substitution « * » et « ? » à la place de toute séquence de symboles ou de tout symbole du texte à saisir.

### Pour créer une liste de groupes AD

1. Dans la liste déroulante **Type**, cliquez sur **Liste des groupes AD**.
2. Pour ajouter un groupe dans la liste, cliquez sur **Ajouter**. Dans la fenêtre qui s'ouvre, sélectionnez un groupe et cliquez sur **OK**.

Quand vous ajoutez un groupe AD, assurez-vous que c'est le groupe Distribution et pas le groupe Security. Sinon, vous ne pourrez lui attribuer aucun profil, sauf le profil standard.

3. Pour supprimer un groupe de la liste, sélectionnez-le et cliquez sur **Supprimer**, puis confirmez la suppression du groupe sélectionné.

La liste des groupes AD peut être formée seulement si le serveur est inclus dans le domaine. Sinon, il est nécessaire d'inclure le serveur dans le domaine ou de spécifier le nom et le mot de passe de l'utilisateur ayant accès à l'AD en tant que valeurs des paramètres **/DrWebADAccessor_1.0/Application Settings/ADAccUserName** et **/DrWebADAccessor_1.0/Application Settings/ADAccPassword** dans la Console d'Administration CMS. Par défaut, les valeurs de ces paramètres sont vides.

Dans la liste déroulante **Profil**, sélectionnez le profil que vous voulez attribuer au groupe que vous configurez.

Lorsque vous finissez la configuration du groupe sélectionné, cliquez sur **Sauvegarder**.

## 7.2. Notifications

Les notifications sont enregistrées dans le journal du système d'exploitation et sont utilisées pour informer l'administrateur et les utilisateurs du réseau des événements liés au fonctionnement de Dr.Web (par exemple, la détection des objets infectés, du spam, le filtrage des messages, etc.).

**Pour configurer les notifications**

1. Cliquez sur **Notifications** dans l'arborescence de la console Dr.Web Administrator Web Console. La zone d'information sera ouverte pour la configuration des notifications (voir Figure 10).

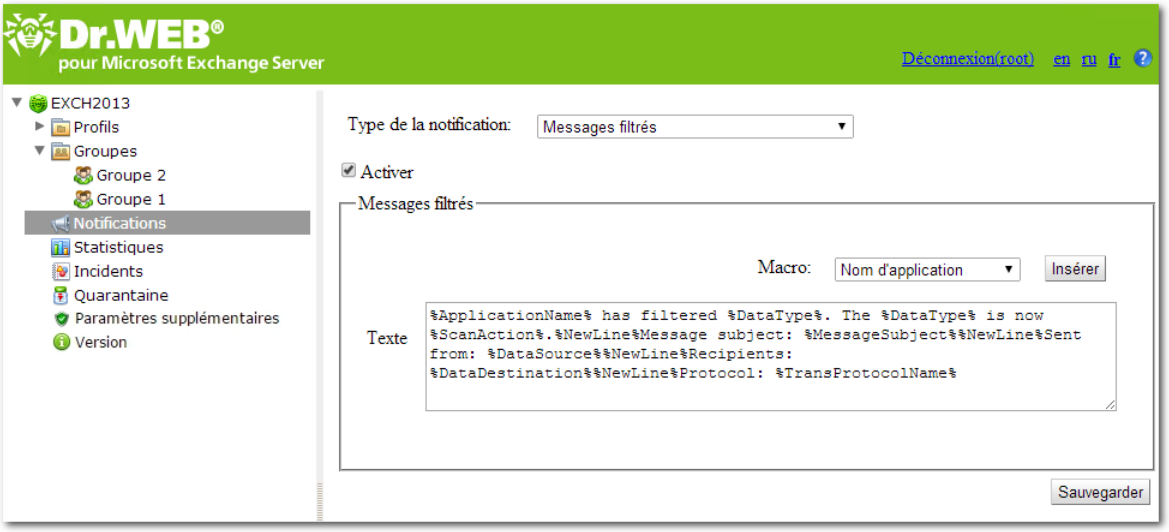


**Figure 10. Rubrique de configuration des notifications**

2. Dans la liste **Type de notification**, sélectionnez le type d'événements nécessitant d'envoyer des notifications :
   - **Messages filtrés** – pour envoyer des notifications sur les messages filtrés ;
   - **Fichiers filtrés** – pour envoyer des notifications sur les pièces jointes filtrées ;
   - **Spam** – pour envoyer des notifications sur les spams ;
   - **Infectés** – pour envoyer des notifications sur les menaces détectées ;
   - **Mise à jour** – pour envoyer des notifications avec des informations sur la dernière mise à jour ;
   - **Les bases virales ne sont plus d'actualité** – pour envoyer une alerte lorsqu'une mise à jour des bases de données virales est requise.
3. Pour activer l'envoi des notifications de votre choix, cochez la case **Activer**.
4. Dans le champ **Texte** de la section des paramètres, vous pouvez configurer le modèle des notifications choisies. Lors de l'édition du texte, vous pouvez utiliser des macros.
5. Après avoir terminé la configuration des notifications, cliquez sur **Sauvegarder**.

## 7.3. Consulter les statistiques

La rubrique **Statistiques** permet d'afficher les informations sur les statistiques de Dr.Web (données totales et moyennes) pour une période spécifiée (voir Figure 11).

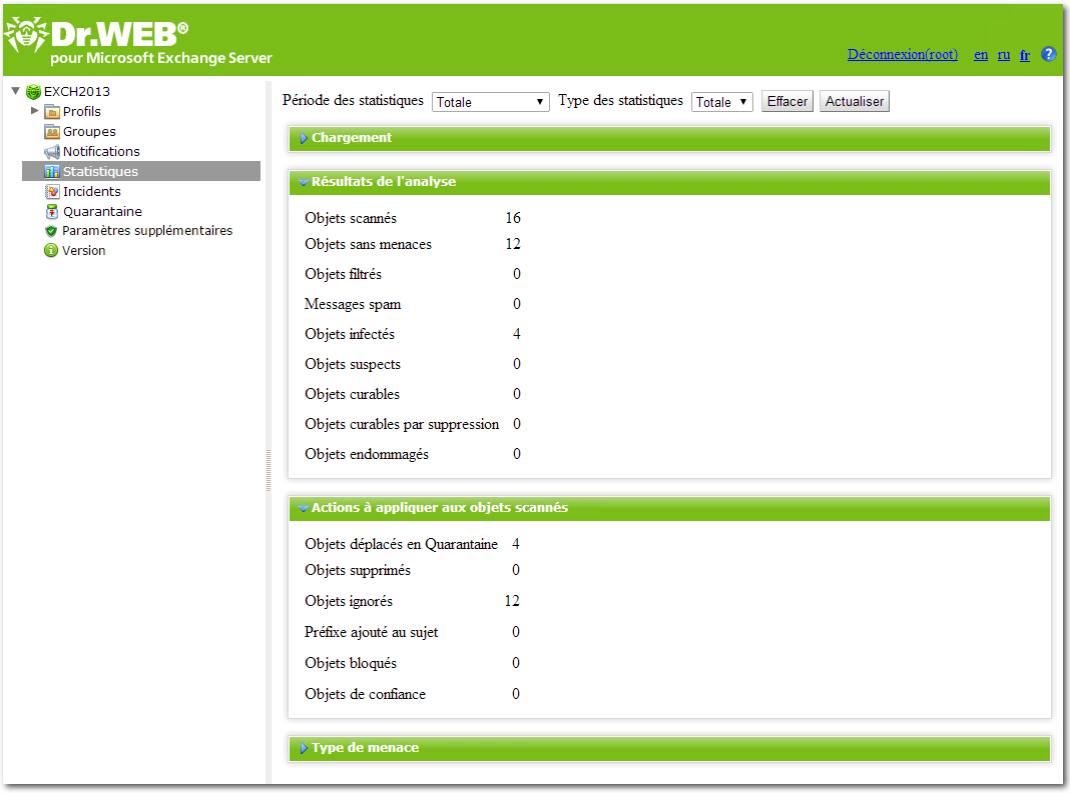


**Figure 11. Rubrique des statistiques**

### Pour configurer l'affichage des statistiques

1. En haut de la rubrique **Statistiques**, dans la liste **Période des statistiques** sélectionnez la période pour laquelle vous souhaitez des statistiques. Les variantes disponibles sont :
   - Totale – pour afficher les statistiques totales depuis le lancement Dr.Web.
   - Dernier jour – pour afficher les statistiques des dernières 24 heures de fonctionnement de Dr.Web.
   - Dernière heure – pour afficher les statistiques de la dernière heure de fonctionnement de Dr.Web.
   - Dernière minute – pour afficher les statistiques de la dernière minute de fonctionnement de Dr.Web.
2. Dans la liste **Type des statistiques**, sélectionnez le type d'informations statistiques. En fonction de la période sélectionnée, vous pouvez configurer l'affichage des données totales, données moyennes pour la période spécifiée, données minimales et maximales pour la période spécifiée.

Pour actualiser ou supprimer les statistiques, cliquez sur **Actualiser** ou **Effacer**.

### Types d'informations

En fonction des paramètres d'affichage, la zone d'information **Statistiques** peut contenir les sections suivantes :

- **Chargement**. Cette sous-rubrique permet d'afficher les informations sur la taille totale des objets analysés, ainsi sur que la taille moyenne, minimale et maximale des objets analysés pendant la période spécifiée.
- **Résultats de l'analyse**. Cette section contient les informations sur la quantité totale des objets analysés, ainsi que sur le nombre d'objets traités de différents types (y compris les objets filtrés, suspects, les spams, etc.).
- **Actions à appliquer aux objets scannés**. Cette sous-rubrique contient les statistiques des actions appliquées par Dr.Web aux menaces détectées.
- **Type de menace**. Cette sous-section contient les informations sur les types de menaces détectées par Dr.Web pendant la période sélectionnée.

## 7.4. Consulter la liste des événements

La section **Incidents** permet d'afficher la liste des événements liés au fonctionnement de Dr.Web (voir Figure 12).

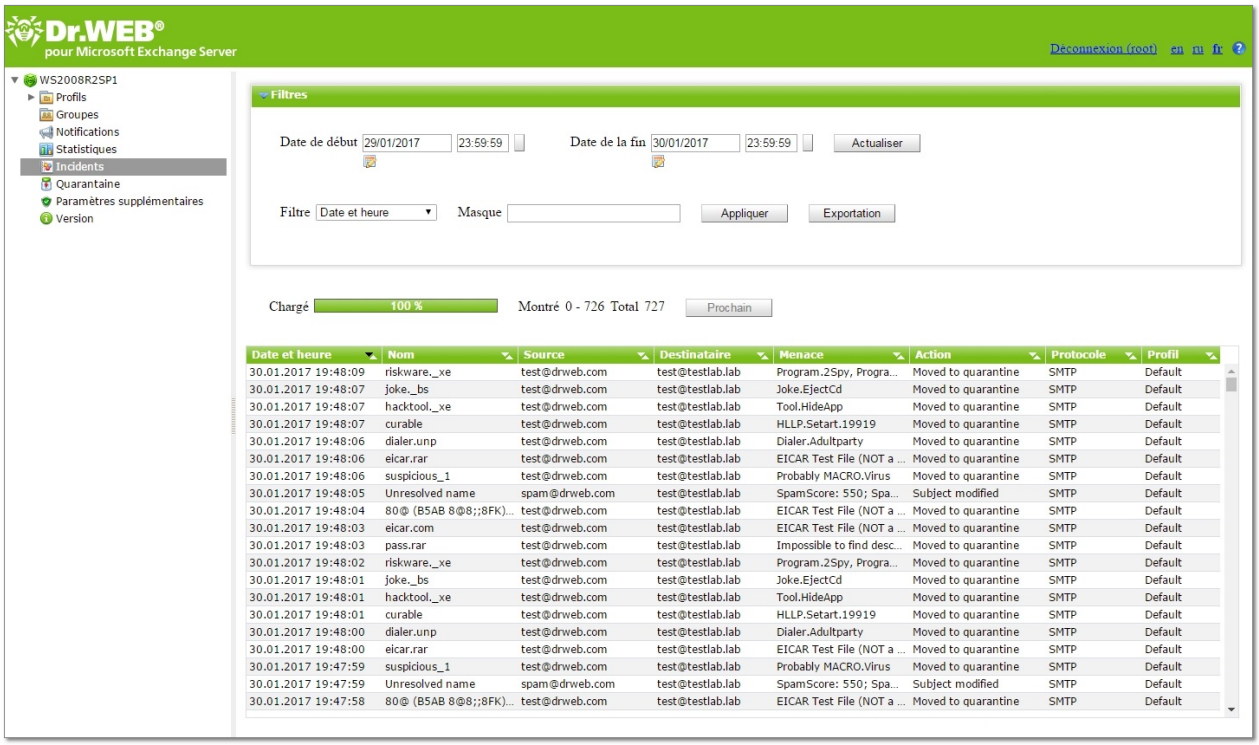


**Figure 12. La section des événements**

### Information sur les événements

Pour chaque événement, les informations suivantes sont affichées dans la liste :

- la date et l'heure de l'événement ;
- l'objet lié à cet événement ;
- les adresses e-mail de l'expéditeur et des destinataires du message contenant un objet infecté ;
- le type de menace ;
- l'action appliquée à la menace ;
- le protocole par lequel le message a été transféré ;
- le nom du profil appliqué.

Vous pouvez configurer l'affichage des informations dans la liste des événements :

1. Cliquez droit sur le titre de la liste et choisissez **Sélectionner les colonnes** dans le menu contextuel.
2. Sélectionnez les types d'informations à afficher.

Une page contient un nombre déterminé de lignes de la liste. Si le nombre de lignes pour la période sélectionnée dépasse cette limitation, vous pouvez feuilleter la liste et consulter les autres événements en cliquant sur le bouton **Suivant**.

**Pour gérer la liste des événements**

1. Vous pouvez afficher les événements pour une période donnée. Spécifiez les dates de début et de fin de la période, puis cliquez sur **Actualiser**.
2. Pour faciliter la recherche des événements, vous pouvez utiliser les filtres. Sélectionnez le filtre dans la liste **Filtre** puis entrez les valeurs des paramètres du filtrage dans le champ **Masque**. Cliquez sur **Appliquer**.

   

   Vous pouvez utiliser les symboles de remplacement « * » et « ? » pour remplacer toute séquence de symboles ou tout symbole particulier dans les valeurs à saisir.

3. Pour sauvegarder la liste des événements dans un fichier texte, cliquez sur **Exportation**. Dans la fenêtre qui s'affiche, sélectionnez le format du fichier et cliquez sur **OK**. La liste des événements peut être sauvegardée au format HTML ou TSV (Tab Separated Values).
4. Pour trier les entrées de la liste selon un critère, cliquez sur le titre de colonne correspondant.
5. Pour actualiser la liste des événements, cliquez sur **Actualiser**. La liste des événements est actualisée chaque fois que la console Dr.Web Administrator Web Console est lancée et la section **Événements** est ouverte. Cela peut prendre du temps. Pour annuler l'actualisation, par exemple, si les paramètres incorrectes du filtrage ont été entrés, cliquez sur **Annuler**.

## 7.5. Gestion de la quarantaine

La Quarantaine de Dr.Web sert à isoler les objets suspects détectés lors de l'analyse du trafic réseau.

La rubrique **Quarantaine** de la console Dr.Web Administrator Web Console contient les informations sur l'état actuel de la quarantaine. Vous pouvez également utiliser le Gestionnaire de Quarantaine pour visualiser et modifier la liste des objets mis en quarantaine.

## 7.5.1. Gérer la quarantaine avec la console web

Pour afficher la liste des objets mis en quarantaine, cliquez sur **Quarantaine** dans l'arborescence de la console Dr.Web Administrator Web Console. La zone d'information va s'ouvrir (voir Figure 13).

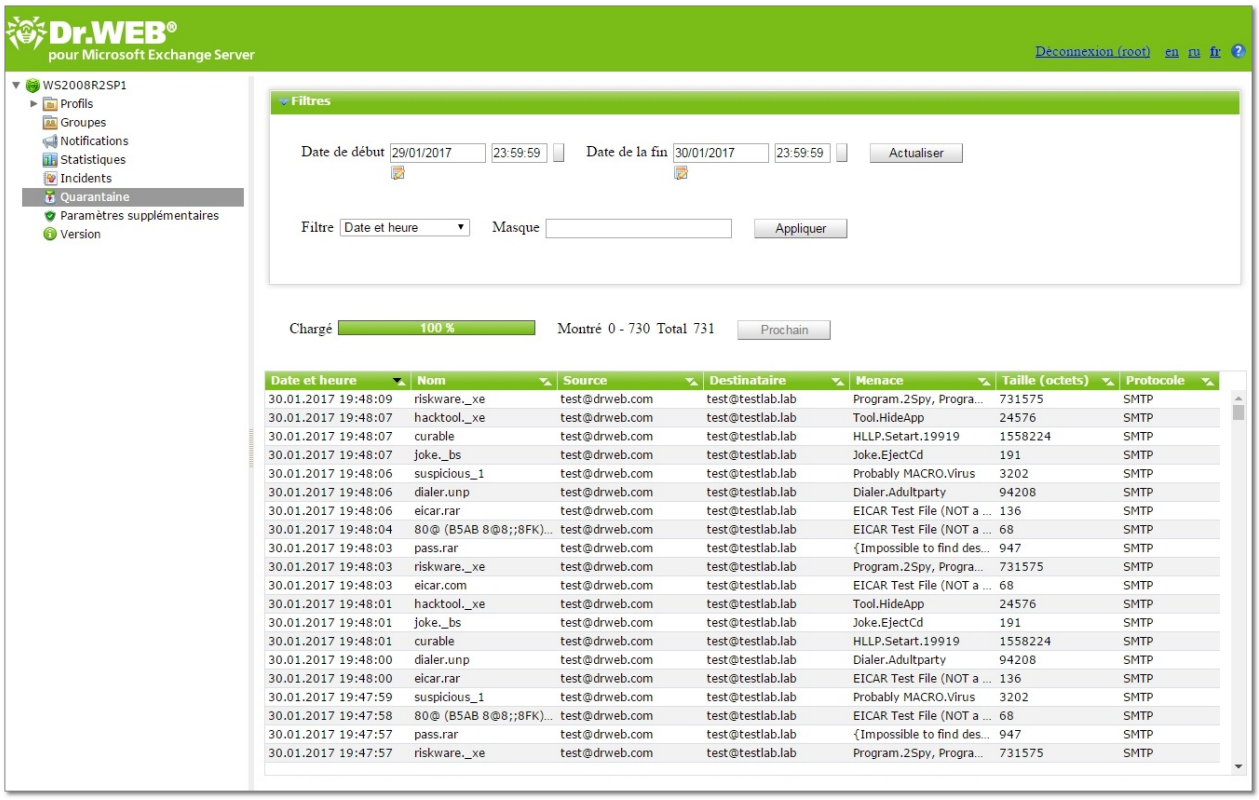


**Figure 13. Liste des objets en quarantaine**

### Information sur les objets en quarantaine

Pour chaque objet, les informations suivantes sont affichées dans la liste :

- la date et l'heure du déplacement en quarantaine ;
- le nom du fichier infecté ;
- les adresses e-mail de l'expéditeur et des destinataires du message contenant un objet infecté ;
- le nom de la menace ;
- la taille du fichier (en octets) ;
- le protocole par lequel le message a été transmis.

Vous pouvez configurer l'affichage des informations dans la liste de la quarantaine :

- Cliquez droit sur le titre de la liste et choisissez **Sélectionner les colonnes** dans le menu contextuel.
- Sélectionnez le types d'informations à afficher.

Les options suivantes sont disponibles pour la liste des objets en quarantaine :

- Une page contient un nombre déterminé de lignes de la liste d'objets. Si le nombre de lignes pour la période sélectionnée dépasse cette limitation, vous pouvez feuilleter la liste et consulter les autres objets mis en quarantaine en cliquant sur le bouton **Suivant**.
- Vous pouvez afficher les objets déplacés en quarantaine pour une période donnée. Spécifiez les dates de début et de fin de la période, puis cliquez sur **Actualiser**.
- Pour faciliter la recherche des informations sur les objets en quarantaine, vous pouvez utiliser les filtres. Sélectionnez le type de filtre dans la liste **Filtre** puis entrez les valeurs des paramètres du filtrage dans le champ **Masque**. Cliquez sur **Appliquer**.

Vous pouvez utiliser les symboles de remplacement « * » et « ? » pour remplacer toute séquence de symboles ou tout symbole particulier du texte à saisir.

- Pour trier la liste selon un critère, cliquez sur le titre correspondant d'une colonne.
- Pour actualiser la liste d'événements, cliquez sur **Actualiser**. La liste des objets en quarantaine est actualisée chaque fois que la console Dr.Web Administrator Web Console est lancée et la section **Quarantaine** est ouverte. L'actualisation peut prendre un certain temps. Pour annuler l'actualisation, par exemple, si les paramètres incorrectes du filtrage ont été entrés, cliquez sur **Annuler**.

**Actions appliquées aux objets en quarantaine**

1. Pour supprimer un objet de la liste, cliquez droit sur l'objet puis sélectionnez **Supprimer** dans le menu contextuel (pour sélectionner plusieurs objets, tenez pressée la touche SHIFT ou CTRL).
2. Pour restaurer un objet, cliquez droit sur l'objet dans la liste puis sélectionnez **Restaurer** dans le menu contextuel. Spécifiez le chemin vers lequel vous voulez restaurer le fichier.

## 7.5.2. Gestionnaire de quarantaine

**Gestionnaire de la quarantaine** est un utilitaire auxiliaire inclus dans Dr.Web. Il sert à configurer les paramètres de la quarantaine et à gérer les fichiers isolés.

Pour ouvrir le **Gestionnaire de quarantaine** (voir Figure 14), utilisez le lien **Dr.Web Quarantine** sur le Bureau.

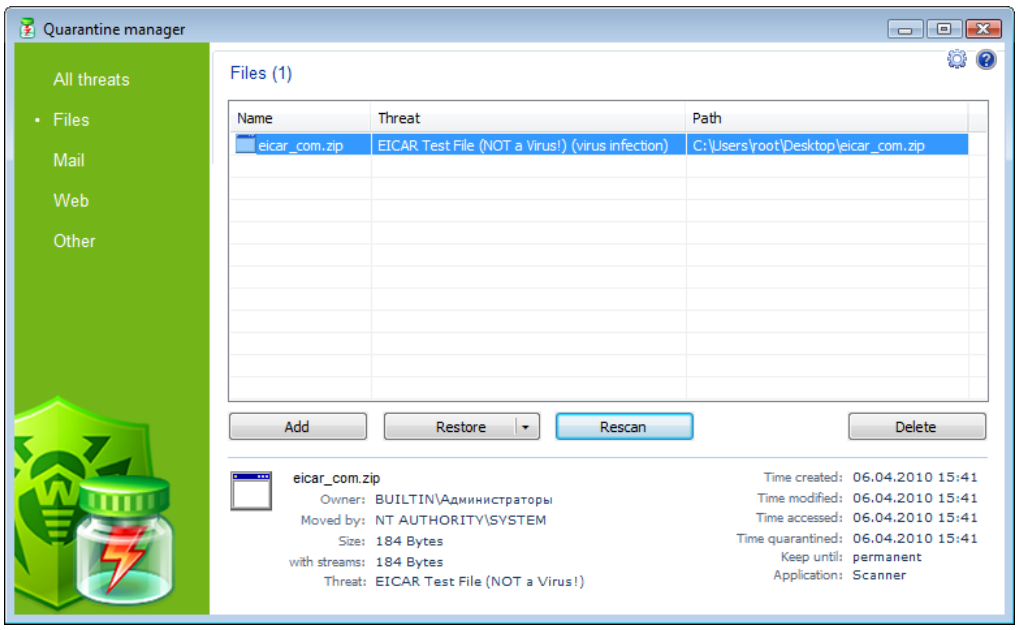


**Figure 14. Fenêtre principale de l'utilitaire de la quarantaine**

La partie centrale de la fenêtre affiche un récapitulatif contenant les informations sur le statut de la Quarantaine et notamment les champs suivants :

- **Nom** – la liste des objets se trouvant en quarantaine.
- **Menace** – type de malware déterminé par Dr.Web lorsque l'objet est placé en quarantaine.
- **Chemin** – chemin complet du fichier avant qu'il ne soit placé en quarantaine.

Dans la partie inférieure de la fenêtre, des informations détaillées sur les objets sélectionnés sont affichées. Vous pouvez activer l'affichage des informations détaillées sur l'objet, les mêmes que celles de la partie inférieure de la fenêtre.

### Pour paramétrer l'affichage des informations dans les colonnes

1. Pour configurer les paramètres d'affichage des informations dans le tableau de la **quarantaine**, cliquez droit sur l'en-tête du tableau et sélectionnez l'élément **Configurer les colonnes**.
2. Sélectionnez les types d'informations à inclure dans le tableau d'objets. Pour exclure les colonnes du tableau d'objets, décochez les cases contre les éléments correspondants. Pour ajouter/exclure tous les types d'informations, **cliquez sur Cocher tout/Décocher les cases.**
3. Pour modifier l'ordre des colonnes dans le tableau, sélectionnez une colonne à déplacer et cliquez ensuite sur un des boutons décrits ci-dessous :
   - **En haut** – pour déplacer la colonne vers le haut du tableau (plus haut dans la liste des paramètres et vers la gauche dans le tableau des objets).
   - **En bas** – pour déplacer la colonne vers la fin du tableau (plus bas dans la liste des paramètres et vers la droite dans le tableau des objets).

4. Pour sauvegarder les modifications apportées aux paramètres des colonnes, cliquez sur le bouton **OK**, pour fermer la fenêtre sans appliquer les modifications, cliquez sur **Annuler**.

Le menu latéral sert à filtrer des objets en quarantaine qui seront affichés. Cliquez sur l'élément correspondant pour afficher dans la partie centrale de la fenêtre tous les objets de la quarantaine ou seulement les groupes d'objets suivants : fichiers, e-mails, pages web ou tous autres objets hors catégories.

## 7.5.2.1. Gérer la quarantaine

**Actions appliquées aux objets en quarantaine**

La fenêtre de la quarantaine permet d'accéder aux boutons suivants :

- **Ajouter** ajouter un fichier dans la quarantaine. Avec le navigateur de fichiers qui s'ouvre, sélectionnez le fichier nécessaire.
- **Restaurer** – déplacer un fichier de la quarantaine et restaurer l'emplacement d'origine du fichier. Le chemin de restauration du fichier est affiché dans la colonne **Chemin** dans la Figure 14. Si le chemin n'est pas spécifié, l'utilisateur peut sélectionner un dossier pour y restaurer le fichier ;

  

  Utilisez cette option uniquement si vous êtes sûr que l'objet n'est pas dangereux.

  Dans le menu déroulant, vous pouvez choisir l'option **Restaurer vers** – déplacer un fichier sous le nom spécifié vers le dossier spécifié par l'administrateur.
- **Rescanner** – rescanner un fichier se trouvant dans la quarantaine. Si lors du rescan, le fichier s'avère sain, la quarantaine proposera de récupérer ce fichier.
- **Supprimer** – supprimer un fichier de la quarantaine et du système.

Pour appliquer une action à un groupe d'objets, sélectionnez les objets dans la fenêtre de la quarantaine, en tenant pressée la touche SHIFT ou CTRL, puis cliquez droit sur une ligne du tableau, puis, dans le menu déroulant, sélectionnez l'action à effectuer.

De plus, dans le menu contextuel du tableau, une option **Envoyer un fichier (des fichiers) au Laboratoire antivirus de Doctor Web** est disponible.

## 7.5.2.2. Configurer les paramètres de la quarantaine

**Pour configurer les paramètres de la quarantaine**

1. Cliquez sur le bouton **Paramètres** dans la fenêtre de la quarantaine.
2. La fenêtre **Propriétés de la quarantaine** vous permet de modifier les paramètres suivants :
   - la rubrique **Spécifier la taille de la quarantaine** permet de gérer l'espace occupé par le dossier de la quarantaine. La taille est calculée en pour-cent par rapport à l'espace total

du disque (en cas de plusieurs disques logiques, la taille sera calculée séparément pour chaque disque sur lequel se trouvent des dossiers de la quarantaine). La valeur 100% correspond à une taille maximum illimitée du dossier de la quarantaine.

- dans la rubrique **Affichage**, cochez la case **Afficher les copies de sauvegarde** afin d'afficher dans le tableau des objets les copies de sauvegarde des fichiers qui ont déjà été supprimés ou désinfectés. Les copies de sauvegarde sont créées automatiquement lors de la suppression ou la désinfection des fichiers. Les copies de sauvegarde sont stockées temporairement.

3. Après la fin de configuration, cliquez sur **OK** pour sauvegarder les modifications apportées ou sur **Annuler** pour annuler les modifications.

## 7.6. Paramètres avancés

La rubrique **Paramètres** avancés permet de spécifier la liste des exclusions, ainsi que de configurer l'archivage des fichiers infectés (voir Figure 15).

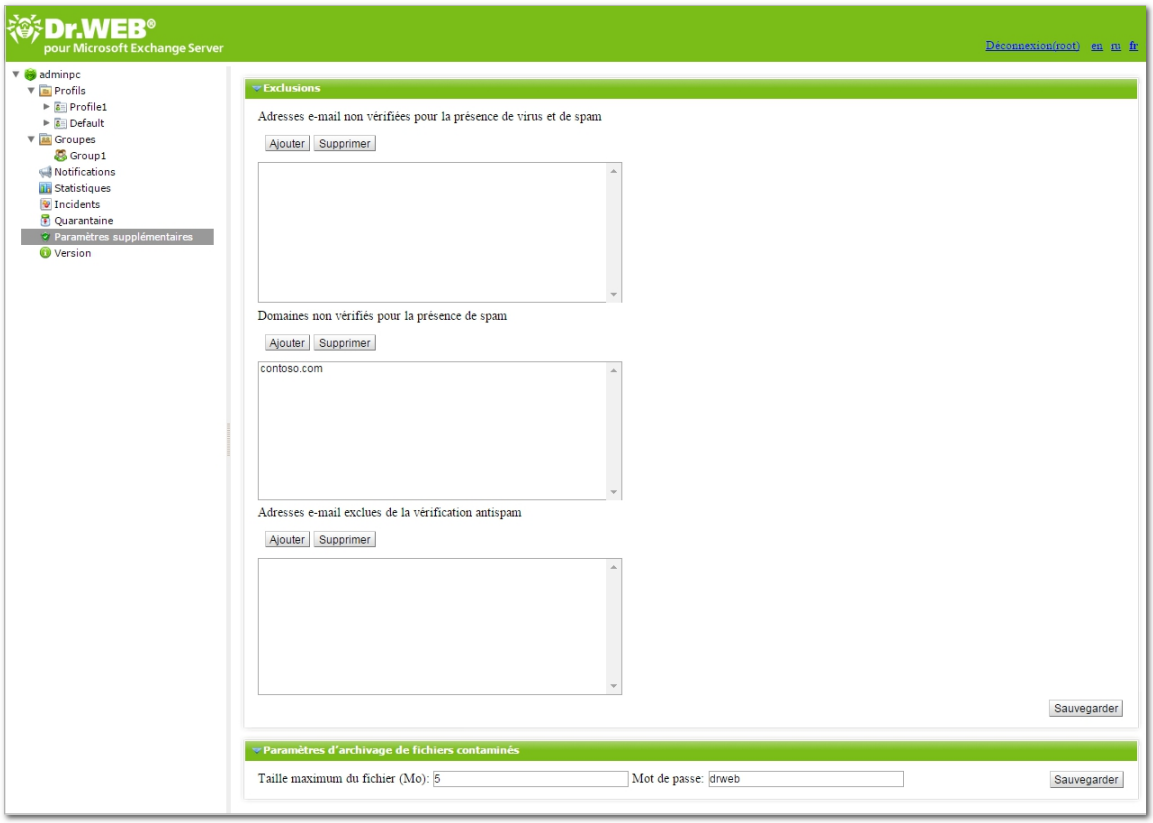


**Figure 15. Paramètres avancés**

### Exclusions

Les messages des expéditeurs fiables peuvent être exclus du scan antispam et antivirus. Pour ce faire, ajoutez leurs adresses ou domaines dans les champs correspondants de la rubrique **Exclusions**. De plus, vous pouvez configurer la liste des exclusions à l'aide de la console Dr.Web CMS Web Console.

### Configuration de l'archivage des fichiers infectés

Ces paramètres concernent les archives zip dans lesquelles sont empaquetés les fichiers infectés et suspects si, pour traiter de tels fichiers, vous avez sélectionné l'action **Archiver** dans la rubrique Scanner. Vous pouvez spécifier dans les champs correspondants la taille maximum du fichier qui peut être archivé et le mot de passe de l'archive.

# 8. Mise à jour des bases virales

Dr.Web utilise des bases virales pour détecter les objets malveillants. Ces bases contiennent des informations sur tous les logiciels malveillants connus. Vu que les logiciels malveillants modernes se caractérisent par leur évolution et leurs modifications rapides, les bases virales nécessitent des mises à jour régulières. Pour maintenir les bases virales à jour, le logiciel utilise le système de diffusion des mises à jour via Internet. Durant toute la période de validité de la licence, le module de mise à jour télécharge et installe les informations sur les nouveaux virus et les logiciels malveillants et les mises à jour.

Les informations sur la version du logiciel, la licence, les bases virales et aussi sur la date, l'heure et le résultat de la dernière mise à jour du logiciel sont affichées dans la zone d'information **Version** de la console Dr.Web Administrator Web Console. Vous pouvez lancer la mise à jour des bases des données virales en cliquant sur **Lancer** dans la section **Tâche de mise à jour**.

Vous pouvez modifier les paramètres de mise à jour dans le fichier drwupsrv.bat.

Lors de l'installation de Dr.Web, une tâche de mise à jour des bases de données virales est créée. Les mises à jours sont téléchargées depuis les serveurs de mise à jour Doctor Web avec une périodicité optimale. Vous pouvez modifier la périodicité à l'aide du Planificateur de tâches Windows :

1. Ouvrez le Planificateur de tâches.
2. Dans le menu contextuel de la tâche **Doctor Web for Exchange Update Task** cliquez sur **Propriétés**.
3. Dans la fenêtre **Doctor Web for Exchange Update Task**, ouvrez l'onglet **Déclencheurs** (ou **Planification**, si vous utilisez le système d'exploitation Windows Server 2003) et modifiez la périodicité des mises à jour. Par défaut, les mises à jour sont téléchargées une fois par heure.
4. Cliquez sur **OK**.

# 9. Dr.Web CMS Web Console

La console Dr.Web CMS Web Console (voir Figure 16) est configurée par le service spécial Dr.Web CMS Web Console qui est géré par un autre service Dr.Web CMS.

Dr.Web CMS Web Console se connecte au service gérant via un protocole d'administration.

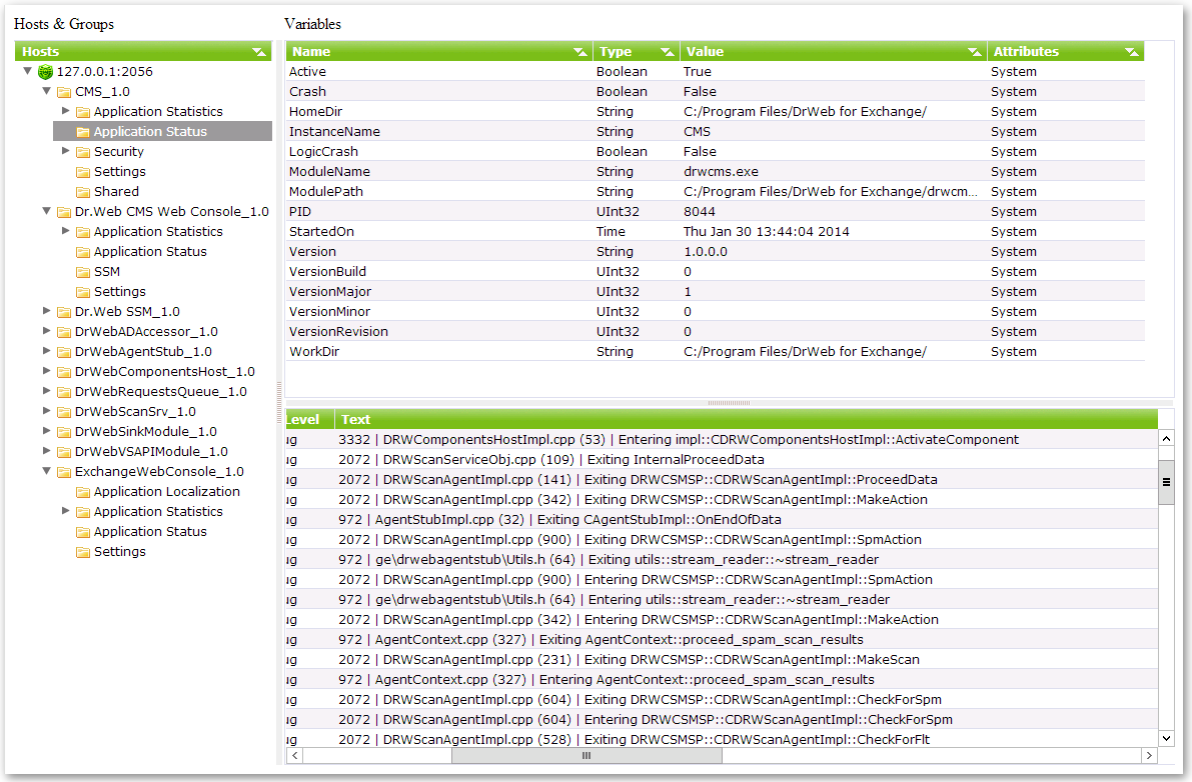


**Figure 16. Dr.Web CMS Web Console**

### Pour lancer Dr.Web CMS Web Console

Pour lancer la console Dr.Web CMS Web Console, ouvrez la page suivante dans le navigateur :

`https://<Exchange Server address>:2080/admin`,

où *<Exchange Server address>* – adresse IP du server Exchange.

Pour accéder à la page de Dr.Web CMS Web Console, il est nécessaire d'entrer les données du compte administrateur. Vous pouvez ajouter, modifier et supprimer les comptes administrateurs à l'aide de la console Dr.Web CMS Web Console.

Lors du premier démarrage de la console Dr.Web CMS Web Console utilisez les données du compte administrateur par défaut : l'identifiant **root** et le mot de passe **drweb**.

### Interface

Console Dr.Web CMS Web Console est composée de trois parties :

1. L'arborescence des hôtes et des groupes.

   L'arborescence contient les hôtes des connexions existantes. Cliquez sur le groupe dans la fenêtre des variables pour afficher la liste des variables. Cliquez droit sur le groupe pour ouvrir le menu contextuel permettant d'effectuer les actions suivantes :

   - créer un groupe ;
   - renommer le groupe ;
   - supprimer le groupe ;
   - créer une variable.

   Si vous cliquez droit sur l'adresse de l'hôte, le menu contextuel comportant les fonctions suivantes s'affiche :

   - **Add host**. Ajouter la connexion à un nouvel hôte dans l'arborescence ;
   - **Remove host**. Supprimer la connexion à l'hôte de l'arborescence ;
   - **Create group**. Créer un nouveau groupe ;
   - **Create variable**. Créer une nouvelle variable ;
   - **View traces**. Afficher les messages de traçage en temps réel ;
   - **Debug traces**. Activer le traçage de débogage ;
   - **Load traces**. Charger les messages de traçage filtrés pour les périodes antérieures ;
   - **Edit trace filter**. Modifier les paramètres du filtrage des messages de traçage.

2. Liste de variables.

   Dans la fenêtre des variables, la liste des variables du groupe sélectionné est affichée, ainsi que leurs types, leurs attributs et leurs valeurs. Cliquez sur un champ pour modifier la valeur correspondante (si cela n'est pas bloqué par les attributs). Cliquez droit sur une variable pour ouvrir le menu contextuel permettant d'effectuer les actions suivantes :

   - créer une variable (une fenêtre spéciale s'ouvre) ;
   - supprimer une variable (si cela est autorisé par les attributs) ;
   - réinitialiser la variable statistique (si cette variable a l'attribut Statistics).

3. Fenêtre de traçage des messages

   Dans cette fenêtre, s'affichent les messages de traçage contenant les informations sur les événements enregistrés par la console Dr.Web CMS Web Console.

   Pour afficher les événements de traçage en temps réel, cochez la case **View traces** dans le menu qui s'affiche quand vous cliquez droit sur l'adresse de l'hôte.

   Pour chaque message, les informations suivantes sont affichées :

   - l'heure de l'événement ;
   - le nom de l'hôte ;

- le nom de l'application ;
- le niveau des détails de l'enregistrement des événements ;
- le texte du message.

Pour filtrer les messages affichés dans la fenêtre de traçage, sélectionnez l'élément **Edit trace filter** du menu contextuel qui s'affiche quand vous cliquez droit sur l'adresse de l'hôte. Dans la fenêtre qui apparaît, spécifiez les paramètres de filtrage :

- **Log level**. Niveau de détail du journal des événements ;
- **Instances**. Sources des événements ;
- **Contents**. Texte inclus dans le message (dans le champ Text) ;
- **NonContents**. Texte non inclus dans le message (dans le champ Text).

Pour supprimer les messages, exécutez la commande **Clear** du menu contextuel qui s'affiche quand vous cliquez droit sur le message.

## 9.1. Changer le mot de passe du compte administrateur

Lors du premier démarrage de la Dr.Web Administrator Web Console ou de la Dr.Web CMS Web Console, utilisez le compte par défaut **root** avec le mot de passe **drweb**. Puis il est fortement recommandé de modifier le mot de passe pour ce compte.

**Pour changer le mot de passe du compte administrateur**

1. Dans l'arborescence des hôtes cliquez sur le groupe **CMS_1.0** -> **Security** -> **Users** -> **root**.
2. Dans la liste des variables du groupe **root** double-cliquez sur la valeur **Value** de la variable **Password**. La fenêtre **Change password variable value** va s'ouvrir.
3. Entrez un nouveau mot de passe dans le champ **Password**, puis dans le champ **Confirm password** pour confirmer les modifications apportées.

## 9.2. Ajouter de nouveaux administrateurs

Vous pouvez ajouter le nombre nécessaire de comptes administrateurs en addition au compte par défaut **root**.

**Pour ajouter un compte administrateur**

1. Dans l'arborescence des hôtes, cliquez sur le groupe **CMS_1.0** -> **Security** -> **Users**.
2. Cliquez droit sur le groupe **Users** pour ouvrir le menu contextuel. Cliquez sur**Create group**.
3. Dans la fenêtre **Enter new group name**, entrez le nom de l'administrateur dans le champ **Group name**. Puis cliquez sur **OK**.
4. Pour spécifier le mot de passe de l'administrateur, cliquez sur le groupe correspondant dans l'arborescence des hôtes et des groupes. Dans le menu contextuel, cliquez sur **Create variable**.

5. Dans la fenêtre **Add new variable**, entrez le nom de la variable **Password** et sélectionnez **Password** en tant que type de variable. Dans le champ **Value**, entrez le mot de passe de l'administrateur. Cliquez sur **Append**.
6. Pour configurer le niveau d'accès à un groupe particulier dans l'arborescence des hôtes et des groupes. Sélectionnez l'élément **Create variable** du menu contextuel.
7. La fenêtre **Add new variable** va s'afficher. Entrez le nom de la variable **UserLevel** et sélectionnez **UInt32** en tant que son type. Indiquez comme valeur de la variable :

   **0** – accès complet à tous les paramètres de la console Dr.Web Administrator Web Console ;

   **1** – accès à la console Dr.Web Administrator Web Console sans possibilité de modifier les paramètres.

Si la valeur de la variable **UserLevel** n'est pas spécifiée, l'administrateur aura l'accès à tous les paramètres de Dr.Web Administrator Web Console.

## 9.3. Créer les clusters

La console Dr.Web CMS Web Console permet d'organiser une arborescence illimitée des hôtes groupés en cluster. Dans le cluster, la modification d'une variable avec l'attribut **Shared** entraîne la même modification des variables sur tous les sous-hôtes.

### Organisation d'un cluster

Sur le sous-hôte (que vous ajoutez dans le cluster), effectuez les actions suivantes :

1. Créez un groupe **/CMS_1.0/Security/Users/host**. Ce groupe représentera un compte utilisé par l'hôte principal pour transmettre les variables avec l'attribut **Shared** sur le serveur local.
2. Dans le groupe **host**, une variable **Password** de type **Password** sera automatiquement crée. Elle contiendra le mot de passe pour se connecter à un compte. Le mot de passe par défaut est **drweb**. Il est recommandé de changer le mot de passe pour des raisons de sécurité.

Sur l'hôte principal, effectuez les actions suivantes :

1. Créez un groupe avec n'importe quel nom situé vers le chemin **/CMS_1.0/Shared/**. Ce groupe représentera le sous-hôte.
2. Dans le groupe de cet hôte, une variable **Address** de type **String** est automatiquement créée. Elle contient une ligne vide. Spécifiez l'adresse IP de la connexion MS du sous-hôte en tant que valeur de cette variable : <*Adresse IP*>:<*Port*>, par exemple, `192.168.1.1:2056`.
3. Dans le groupe de l'hôte, une autre variable **Password** de type **Password** est automatiquement créée. Elle contient le mot de passe pour se connecter au compte **host** sur le sous-hôte. Le mot de passe par défaut est **drweb**. Il est recommandé de changer ce mot de passe pour des raisons de sécurité. Si le mot de passe est le même pour tous les hôtes, vous pouvez créer la variable **Password** dans le groupe **Shared** pour l'utiliser pour toutes les connexions.

4. Les variables utilisées pour se connecter au sous-hôte ne peuvent pas avoir l'attribut **Shared**, de ce fait, les paramètres de la connexion ne sont pas transférés sur les sous-hôtes. Lors d'une tentative de modification des attributs des variables contenant les paramètres de la connexion, l'accès est refusé.

Dans le dossier **Shared**, une variable **Enabled** de type **Boolean** est automatiquement créée. Cette variable active/désactive les fonctions du cluster. Si la valeur de cette variable est **True**, toutes les connexion sont activées, si la valeur est **False**, toutes les connexions sont interrompues. La valeur par défaut est **True**.

Quand un groupe d'hôtes est créé dans le dossier **Shared**, une variable **Enabled** de type **Boolean** y est automatiquement créée avec la valeur **False** par défaut. Cette variable active/désactive la connexion séparée.

Lors de la modification de l'adresse (de la valeur de la variable **Address**), la connexion active bascule vers une nouvelle adresse. Si le mot de passe est modifié, la connexion ne se refait pas. Pour activer la connexion avec un nouveau mot de passe, il est nécessaire de désactiver puis réactiver la connexion par la variable **Enabled**.

Si la connexion est créée correctement, CMS se connecte automatiquement au sous-hôte et y transfère toutes les variables avec l'attribut **Shared**. Si la variable avec ce nom existe déjà sur le sous-hôte et que son attribut n'est pas **Shared**, elle est ignorée avec code de retour **MB_RC_SKIPPED**.

Vous pouvez créer la liste des sous-hôtes à tous les niveaux de l'arborescence.

Si le pare-feu Windows est activé, pour le fonctionnement correct du cluster, il est nécessaire d'autoriser l'échange de données via le protocole TCP entre l'hôte principal et les sous-hôtes. Pour ce faire, il faut créer les règles suivantes du pare-feu Windows :

- règle entrante pour la connexion du service de gestion **drwcms.exe** de l'hôte principal au sous-hôte via le protocole TCP et via n'importe quel port ;
- règle sortante pour la connexion du service de gestion **drwcms.exe** de l'hôte principal au sous-hôte via le protocole TCP et via le port 2056 ;
- règle entrante pour la connexion du sous-hôte au service de gestion **drwcms.exe** de l'hôte principal via le protocole TCP et le port 2056 ;
- règle sortante pour la connexion du sous-hôte au service de gestion **drwcms.exe** de l'hôte principal via le protocole TCP et n'importe quel port.

**Pour gérer les paramètres de l'analyse et du filtrage des groupes AD**

Les variables avec l'attribut **Shared** des profils et des groupes représentants les listes des adresses e-mail, et ces profils et groupes eux-mêmes sont librement transférés entre les bases de données **cmsdb** depuis le serveur gérant au sous-serveur, parce qu'ils ne dépendent pas d'Active Directory. Si le serveur gérant et le sous-serveur sont connectés à un serveur du catalogue global (Global Catalog) d'Active Directory, lorsqu'un groupe AD est créé dans Dr.Web Administrator Web Console sur le serveur gérant, ses paramètres sont transférés au sous-serveur. Mais si les serveurs ajoutés en cluster n'ont pas de catalogue global commun, les groupes AD avec gestion centralisée des paramètres sont créés autrement :

1. Sur le serveur subordonné, dans la console d'Active Directory, créez un nouveau groupe de distribution.
2. Avec la console Dr.Web Administrator Web Console ajoutez ce groupe dans la liste des groupes de l'application.
3. Dans la Console d'Administration CMS, trouvez ce groupe par le chemin **DrWebScanSrv_1.0** -> **Application Settings** ->**Groups** -> <*nom de groupe*>. Changez l'attribut **Shared** en **Default** pour la variable **ItemList** qui définit l'identificateur GUID du groupe AD créé.
4. Dans la console de gestion d'Active Directory du serveur gérant, créez un nouveau groupe de distribution avec le même nom que celui du serveur subordonné.
5. Utilisez la console Dr.Web Administrator Web Console pour ajouter le groupe créé dans la liste des groupes du serveur gérant en spécifiant le même nom pour ce groupe.
6. Les groupes seront associés par leur nom (même s'ils ont des identificateurs GUID et des listes d'utilisateurs différents). L'attribution des profils et la configuration des paramètres de l'analyse et du filtrage sera possible par Dr.Web Administrator Web Console sur le serveur gérant et ces paramètres seront transférés sur les deux serveurs.

## 9.4. Notifications sur la suppression des messages avec Exchange Web Services

Si les messages peuvent être supprimés lors de l'analyse antivirale ou lors du filtrage par l'agent antivirus , le destinataire ne reçoit aucune information sur ces messages, c'est seulement enregistré dans le journal des événement du serveur. Vous pouvez configurer l'envoi de notifications via le protocole EWS (Exchange Web Services) à l'adresse spécifiée dans le paramètre **OWSNotificationEmail**. Ces notifications contiennent les informations sur les expéditeurs, les listes des destinataires et les sujets des messages supprimés, mais elles ne contiennent pas d'informations sur le texte et les pièces jointes.

EWS (Exchange Web Services) se trouve sur les serveurs avec le rôle Client Access (CAS). Ce service fonctionne comme intermédiaire entre les requêtes des utilisateurs et la structure interne du serveur Exchange.

Les notifications sur la suppression des messages par Exchange Web Services sont configurées dans la section des paramètres **DrWebAgentStub_1.0** -> **Application Settings** de la Console d'Administration CMS par les variables suivantes :

- **OWSUrl**définit le serveur où se trouve le service EWS. Par défaut, la valeur localhost est spécifiée, mais en général, cela peut être l'adresse IP de tout autre serveur avec EWS ;
- **OWSAdministrator**, **OWSPassword**, **OWSDomain** définissent les paramètres de l'accès (le nom d'utilisateur ayant les privilèges d'accès à EWS, son mot de passe et le nom du domaine) à la boîte de réception spécifiée par le paramètre OWSOutgoingEmail ;
- **OWSNotificationEmail**.
- **OWSOutgoingEmail**.

Les paramètres sont envoyés à l'agent antivirus une fois lors du démarrage du service de transport, et les notifications par EWS ne sont pas envoyées, si au moins un des paramètres représente une ligne vide.

A chaque fois qu'un message est supprimé, l'agent antivirus de transport essaie de se connecter au serveur spécifié par le paramètre **OWSUrl**. En cas d'échec de la connexion, l'alerte **444** avec la description de l'erreur est enregistrée dans le journal des événements du système d'exploitation (Event Log).

## 9.5. Actions de l'agent antispam en cas de suppression ou de blocage d'un message

Si le message est supprimé en tant que spam ou bloqué comme non conforme aux règles de filtrage, l'agent de transport d'antispam peut fermer la connexion au client ou générer la réponse **RejectMessage**.

Pour déterminer l'action à appliquer en cas de suppression ou de blocage d'un message, procédez comme suit :

1. Dans l'arborescence des hôtes et des groupes, sélectionnez le groupe **AgentStub** ->**Application Settings**.
2. Dans le champ **Value**, spécifiez pour la variable **Disconnect** une des valeurs suivantes :
   - **false**. L'expéditeur recevra en réponse **RejectMessage** au contenu suivant : **Dr.Web AntiSpam Agent: Message was rejected as spam**. Cette action est effectuée par défaut.
   - **true**. La connexion SMTP au client sera fermée.

## 9.6. Modifier le mode de licencing

Il est nécessaire de modifier le mode de licencing si le mode protection centralisée a été activé ou désactivé.

**Pour modifier le mode de licencing**

1. Dans l'arborescence des hôtes et des groupes, sélectionnez le groupe **DrWebScanSrv_1.0** -> **Application Settings**.
2. Dans le champ **Value**, indiquez la valeur pour la variable **LicenseMode** :

   **0** - pour que Dr.Web fonctionne, il est nécessaire d'obtenir le fichier clé (par défaut) ;

   **1** - pour que Dr.Web fonctionne, il est nécessaire d'utiliser le fichier clé depuis le serveur de protection centralisée.
3. Après avoir modifié le mode, redémarrez le service Dr.Web for MSP Scanning Service.

## 9.7. Sélectionner les types d'objets endommagés

Dans certains cas, les pièces jointes peuvent être considérées comme *endommagées*. Ces objets ne peuvent pas être analysés pour vérifier la présence de virus. La même action est appliquée aux objets infectés. Pour préciser quels types d'objets seront considérés comme malveillants, faites comme suit :

1. Dans l'arborescence des groupes et hôtes, choisissez **DrWebScanSrv_1.0** -> **Application Settings** -> **Profiles** -> **%Profile name%** -> **Scanner**.
2. Choisissez les variables correspondant aux types d'objets :
   - **ScannerTreatPswrdArchivesAsBad**. Archives avec un mot de passe.
   - **ScannerTreatIncompleteArchivesAsBad**. Archives incomplètes.
   - **ScannerTreatPackedArchivesAsBad**. Archives mal empaquetées.
   - **ScannerTreatRestrictedArchivesAsBad**. Archives à accès restreint.
   - **ScannerTreatDeepArchivesAsBad**. Archives avec un haut niveau d'emboîtement.
   - **ScannerTreatBigArchivesAsBad**. Archives trop volumineuses.
3. Dans le champ **Value**, indiquez la valeur de la variable sélectionnée :

   **true**. Les objets de ce type seront traités comme des objets endommagés. L'action choisie pour les objets infectés dans la section Scanner sera appliquée à ces objets.

   **false**. Les objets de ce type seront traités comme des objets sains et seront sautés.

## 9.8. Considérer un message comme spam

Le composant Antispam assigne un nombre entier (*score*) à chaque message. Le score permet de déterminer si le message est un spam.

Pour modifier les valeurs du seuil utilisées pour assigner un message à un groupe ou un autre (**Certainement du spam**, **Probablement du spam**, **Peu probablement du spam**), faites comme suit :

1. Dans l'arborescence des hôtes et groupes, choisissez **DrWebScanSrv_1.0** -> **Application Settings** -> **Profiles** -> **%Profile name%** -> **Antispam**.

2. Spécifiez les valeurs pour les variables suivantes :

Pour que l'Antispam fonctionne correctement, ne modifiez pas les valeurs par défaut des variables **AntispamDefaultScoreMin** et **AntispamExactlyScoreMax**.

- **AntispamDefaultScoreMin**. La valeur score la plus petite qui assigne le message au groupe **Peu probablement du spam**. Valeur par défaut : 1.
- **AntispamDefaultScoreMax**. La valeur score la plus importante qui assigne le message au groupe **Peu probablement du spam**. Valeur par défaut : 199.
- **AntispamProbablyScoreMin**. La valeur score la plus petite qui assigne le message au groupe **Probablement du spam**. Valeur par défaut : 200.
- **AntispamProbablyScoreMax**. La valeur score la plus importante qui assigne le message au groupe **Probablement du spam**. Valeur par défaut : 4999.
- **AntispamExactlyScoreMin**. La valeur score la plus petite qui assigne le message au groupe **Certainement du spam**. Valeur par défaut : 5000.
- **AntispamExactlyScoreMax**. La valeur score la plus importante qui assigne le message au groupe **Certainement du spam**. Valeur par défaut : 2147483647.

## 9.9. Exclusion des messages de l'analyse

Vous pouvez exclure les messages d'expéditeurs fiables de l'analyse en indiquant leurs adresses et domaines dans les variables correspondantes.

1. Dans l'arborescence des hôtes et des groupes, sélectionnez le groupe **DrWebAgentStub_1.0** -> **Application Settings**.
2. Spécifiez les valeurs pour les variables suivantes :

Les valeurs de variables sont spécifiées par « ; » sans espace. Par exemple : **example1@mail.com;example2@mail.com**.

---

La liste des exclusions peut être configurée dans la rubrique Paramètres avancés de la console Dr.Web Administrator Web Console.

- **TrustedDomains**. La liste des domaines à exclure de l'analyse pour la présence de spam. Le nom du domaine doit contenir seulement une partie de l'adresse précédée par le caractère @. Par exemple : **domain.org;mail.com;drweb.com**.
- **SpamTrustedEmails**. La liste des adresses e-mail à exclure de l'analyse.
- **TrustedEmails**. La liste des adresses e-mail à exclure de l'analyse à la recherche de spam et de virus. Il est nécessaire d'écrire ces adresses dans la variable **TrustedEmails** du groupe **DrWebVSAPIModule_1.0** -> **Application Settings**.

## 9.10. Filtrage des fichiers en archive par leurs extensions

Si vous voulez surveiller les archives contenant des fichiers avec des extensions déterminées et appliquer à ces archives les actions spécifiées pour les objets suspects, vous pouvez utiliser la variable **SuspiciousTypesInsideContainer** :

1. Dans l'arborescence des hôtes et des groupes, sélectionnez le groupe **DrWebScanSrv_1.0->Application Settings**.
2. Spécifiez les extensions au format suivant : exe;vbs;scr en tant que valeur de la variable SuspiciousTypesInsideContainer.

D'abord, l'archive sera scannée à la recherche d'objets infectés. Une fois trouvés, l'action spécifiée pour les objets infectés est appliquée à l'archive, sinon l'archive sera scannée à la recherche de fichiers avec les extensions indiquées. Si au moins un fichier avec une telle extension est trouvé, l'action spécifiée pour les objets suspects sera appliquée à l'archive.

# 10. Journalisation des événements

Dr.Web recueille les erreurs et les événements dans les journaux suivants :

- journal des événements du système d'exploitation (Event Log) ;
- journal texte des événements de l'assistant d'installation ;
- journal des événements CMS.

Les informations sur les mises à jour sont écrites dans le journal texte `dwupdater.log` se trouvant dans le dossier `%alluserprofile%\AppData\Doctor Web\Logs\` (voir le paragraphe Vérification du module de mise à jour).

## 10.1. Journal du système d'exploitation

Les informations listées ci-dessous sont écrites dans le journal des événements système (Event Log) :

- messages sur le démarrage et l'arrêt du logiciel ;
- paramètres du fichier clé de licence : validité ou non validité de la licence, la durée de la licence ;
- paramètres des modules du logiciel : scanner, moteur, bases virales (ces informations sont écrites au démarrage et lors des mises à jour des modules correspondants) ;
- message sur la non validité de la licence : absence de fichier clé, absence d'une autorisation pour l'utilisation des modules du logiciel, blocage de la licence, dommage à l'intégrité du fichier clé (ces informations sont écrites au démarrage du programme et pendant son fonctionnement) ;
- notifications sur l'expiration de la durée de la licence (ces informations sont écrites 30, 15, 7, 3, 2 et 1 jour(s) avant la date d'expiration) ;
- informations sur les menaces détectées et sur le spam (voir le paragraphe Notifications).

Les événements Dr.Web sont enregistrés dans les journaux **Application** et Doctor Web.

#### Consultation du journal système

1. Pour consulter le journal des événements du système d'exploitation, allez dans le Panneau de configuration.
2. Sélectionnez **Outils d'administration** puis **Observateur d'événements**.
3. Dans la partie gauche de la fenêtre **Observateur d'événements**, sélectionnez **Application** (ou **Doctor Web**). La liste des événements enregistrés dans le journal par des applications utilisateur sera affichée. Les sources des messages de Dr.Web sont les applications **Dr.Web Scanning Engine**, **Dr.Web CMS**, **Dr.Web CMS Web Console**, **Dr.Web for MSP Scanning Service**, **Dr.Web for MSP Component Host** et **Dr.Web for MSP Requests Queue**.

**Redirection des événements deDr.Web**

Pour rediriger les événements de Dr.Web vers un journal particulier des événements du système d'exploitation, procédez comme suit :

1. Dans la console Dr.Web CMS Web Console sélectionnez le groupe **DrWebScanSrv_1.0** -> **Application Settings**.
2. Comme valeur de la variable **EventLog** indiquez le nom du journal dans lequel les événements de Dr.Web seront enregistrés, par exemple **Doctor Web**.

   

   Si la variable **EventLog** n'est pas présente ou que sa valeur n'est pas spécifiée, les événements de Dr.Web sont enregistrés dans le journal **Application**.

3. Redémarrez le service Dr.Web for MSP Scanning Service.
4. Supprimez la source des événements **Dr.Web for Exchange Server** depuis la rubrique du registre `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\application`.
5. Redémarrez le système d'exploitation.

## 10.2. Journal texte de l'assistant d'installation

Pour localiser les fichiers des événements liés à l'installation de **setup-starter.log** et **exchange-setup.log**, utilisez la variable de l'environnement **%ProgramData%** (en l'exécutant dans la ligne de commande **Démarrer** -> **Exécuter**) dans le dossier **%ProgramData%\Doctor Web\Logs**.

## 10.3. Journal d'événements CMS

La liste des événements est sauvegardée par le service gérant Dr.Web CMS dans la base de données cmstracedb qui se trouve dans le dossier d'installation du logiciel %Program Files% \DrWeb for Exchange. Le service gérant enregistre différents types d'événements et permet de spécifier le niveau de détails pour chaque application.

Vous pouvez supprimer la base de données cmstracedb, si nécessaire.

La liste des événements s'affiche dans la fenêtre de messages de traçage de la console Dr.Web CMS Web Console.

### 10.3.1. Types d'événements enregistrés

Le service gérant enregistre les événements des applications avec différents niveaux de détails :

| Valeur | Types des messages avec différents niveaux de détails |
|---|---|
| **Audit** | Les messages de ce type sont enregistrés par le service gérant et décrivent les événements liés aux actions de l'administrateur, par exemple, la modification des variables. |
| **Incident** | Les événements de sécurité enregistrés par les applications extérieures, par exemple, la détection des virus. |
| **Fatal** | Les événements liés aux échecs de l'application. |
| **Error** | Les erreurs après lesquelles le fonctionnement ordinaire de l'application est possible. |
| **Warning** | Les alertes sur les événements pour l'administrateur. |
| **Information** | Les messages d'information. |
| **Debug** | Les messages de débogage. |

La liste des événements est sauvegardée par le service gérant dans une base de données spéciale.

Le service gérant permet d'afficher la liste des événements enregistrés en temps réel, de filtrer les événements via différents paramètres, de sauvegarder les événements filtrés pour des périodes passées.

### 10.3.2. Niveau de détails

Pour configurer le niveau de détails optimal d'enregistrement des événements de l'application, spécifiez une des valeurs suivantes pour la variable **LogLevel** (**UInt32**) dans le groupe **Settings** :

| Valeur | Niveau de détails |
|---|---|
| **0** | Seuls les événements Error, Fatal, Incident et Audit sont enregistrés. |
| **1** | Les messages Warning sont ajoutés à tous les niveaux précédents. |
| **2** | Les messages Information sont ajoutés à tous les niveaux précédents. |
| **3** | Les messages Debug sont ajoutés à tous les niveaux précédents. |

Par défaut, pour toutes les applications abonnées au service Dr.Web CMS, le niveau de détails 2 est spécifié. Pour spécifier le niveau de détails 3 pour toutes les applications, sélectionnez

l'option **Debug Traces** quand vous cliquez droit sur l'élément racine de l'arborescence de la console Dr.Web CMS Web Console. Pourtant l'activation de cette option peut augmenter la charge du système, c'est pourquoi il n'est pas généralement recommandé de spécifier le niveau de détail 3 pour tous les modules. Si vous avez réussi à révéler un problème d'une application, vous pouvez modifier le niveau de détails uniquement pour cette application.

Si vous spécifiez le niveau de détails 3 dans la console Dr.Web CMS Web Console ouverte dans le navigateur Internet Explorer, et que vous activez l'affichage des événements en temps réel par l'option **View Traces**, il est nécessaire de contrôler le volume de mémoire allouée au processus iexplorer.exe qui correspond à la fenêtre de la console. Dans quelque temps ce processus peut prendre toute la mémoire disponible, ce qui diminue la performance du système.

### 10.3.3. Suppression de la base de données cmstracedb

Si nécessaire, vous pouvez supprimer la base de données cmstracedb qui se trouve dans le dossier d'installation de l'application %Program Files%\DrWeb for Exchange :

1. Avant la suppression de la base de données, il est recommandé de décharger le serveur en effectuant une des actions suivantes :
   - arrêtez le service de transport où les agents de transport sont installés et le service Microsoft Exchange Information Store, si le module VSAPI est installé ;
   - si le serveur ne peut pas être arrêté, désactivez les agents de transport et redémarrez le service de transport. Si le module VSAPI est installé, spécifiez la valeur **0** pour le paramètre **Enabled** dans la clé de registre `[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\VirusScan]`, puis redémarrez le service Microsoft Exchange Information Store.
2. Lancez la console de commande (cmd) avec les privilèges administrateurs.
3. Arrêtez les services de l'application dans l'ordre suivant :

   ```
   net stop "Dr.Web SSM"
   net stop "Dr.Web for MSP Scanning Service"
   net stop "Dr.Web for MSP Components Host"
   net stop "Dr.Web for MSP Requests Queue"
   net stop "Dr.Web CMS Web Console"
   net stop "Dr.Web CMS"
   ```
4. Supprimez le fichier **cmstracedb** qui se trouve dans le dossier d'installation de l'application %Program Files%\DrWeb for Exchange.
5. Lancez les services de l'application dans l'ordre suivant :

   `net start "Dr.Web CMS"` (avant de continuer, il faut attendre jusqu'à ce que ce service démarre)

   ```
   net start "Dr.Web SSM"
   ```

6. Après le démarrage du service Dr.Web SSM, vérifiez s'il a lancé les autres services de l'application.

# 11. Diagnostic

Pour vérifier le fonctionnement de l'application, effectuez les tests suivants :

- vérification de l'installation de l'application antivirus ;
- vérification du module de mise à jour ;
- vérification de la capacité de détection des virus et des spams.

## 11.1. Vérification de l'installation

Si vous utilisez Microsoft Exchange 2003 Dr.Web doit être installé dans les dossiers suivants :

- C:\Documents and Settings\All Users\Application Data\Doctor Web ;
- C:\Program Files\Common Files\Doctor Web ;
- C:\Program Files\DrWeb for Exchange.

Si vous utilisez Microsoft Exchange 2008 ou supérieur, Dr.Web doit être installé dans les dossiers suivants :

- C:\ProgramData\Doctor Web ;
- C:\Program Files\DrWeb for Exchange ;
- C:\Program Files\Common Files\Doctor Web.

Veuillez vous assurer que ces dossiers sont bien créés et qu'ils contiennent les fichiers de programme.

Puis ouvrez l'utilitaire standard **Observateur d'événements** (**Event Viewer**) et assurez-vous qu'il n'y a pas d'erreurs liées à Dr.Web.

Veuillez vous assurer que les services locaux suivants sont lancés :

- Dr.Web Scanning Engine (DrWebEngine) ;
- Dr.Web CMS ;
- Dr.Web SSM ;
- Dr.Web CMS Web Console ;
- Dr.Web for MSP Scanning Service ;
- Dr.Web for MSP Component Host ;
- Dr.Web for MSP Requests Queue.

Si Dr.Web est installé correctement, vous pouvez exécuter la commande `get-transportagent` dans la console Exchange PowerShell pour vérifier si les agents suivants sont affichés :

- Dr.Web AntiSpam Agent ;
- Dr.Web AntiVirus Agent.

## 11.2. Vérification du module de mise à jour

Le module de mise à jour **drwupsrv.exe** démarre automatiquement après l'installation de Dr.Web. Il télécharge les dernières versions du noyau antivirus **drweb32.dll** et du noyau antispam **vrcpp.dll**, il met à jour les bases virales.

**Pour vous assurer que la mise à jour a réussi**

1. En fonction de la version de l'OS, exécutez la commande **Tasks** pour ouvrir le répertoire C:\WINDOWS\Tasks ou ouvrez le **Planificateur de tâches** Windows.
2. Vérifiez la présence de la tâche Dr.Web dans le dossier qui sera ouvert (en cas de tâche correctement accomplie, le code de retour dans la colonne **Résultat de la dernière exécution** doit être **0x0**).
3. Puis ouvrez le fichier de journal des événements du module de mise à jour %AllUsersProfile %\Application Data\Doctor Web\Logs\dwupdater.logetassurez-vous qu'il n'y a pas d'erreurs repérées.

## 11.3. Vérification de la détection de virus

Pour vérifier la configuration et la capacité de Dr.Web à détecter des virus, il est recommandé d'utiliser le script de test EICAR (European Institute for Computer Antivirus Research). Le fichier texte contenant uniquement le script de test EICAR n'est pas un virus et n'est pas capable d'autoréplication, il ne représente donc aucun danger, mais ce fichier est classé comme virus par les logiciels antivirus. Vous pouvez télécharger le fichier de test dans la rubrique **Download Anti-Malware Testfile** sur le site web EICAR à l'adresse http://www.eicar.org/ ou vous pouvez créer ce fichier vous-même.

**Pour créer votre propre fichier test EICAR**

- Ouvrez NotePad et copiez-y la ligne suivante :

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

- Sauvegardez ce fichier avec l'extension **.com** (vous pouvez utiliser n'importe quel nom de fichier, par exemple, **eicar.com**), joignez-le au message électronique et envoyez à une adresse de test. Le message reçu à l'adresse spécifiée doit contenir un fichier texte ayant le suffixe **_infected.txt** et le contenu suivant :

  ```
  Le fichier eicar.com infecté par un virus a été supprimé par Dr.Web
  pour Exchange. Le nom du virus : EICAR Test File (NOT a Virus!).
  ```

De plus, Dr.Web envoie une notification avec le même texte à l'adresse de l'administrateur spécifiée lors de l'installation.

N'utilisez en aucun cas de vrais virus pour tester des logiciels antivirus !

## 11.4. Vérification de la détection de spam

Le composant Antispam est disponible uniquement au sein de la version «Antivirus+Antispam», cela signifie que vous devez disposer d'un fichier clé correspondant (voir Fichier clé de licence).

Pour vérifier la capacité du composant **Antispam** de détecter des spams, il est recommandé d'utiliser un des messages avec la ligne de test: GTUBE (Generic Test for Unsolicited Bulk Email) ou avec la ligne pour vérification intégrée.

**Pour créer le GTUBE message de test**

1. Dans le sujet du message, indiquez : **Test spam mail**.
2. Copiez la ligne ci-dessous dans le corps d'un nouveau message e-mail :

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```

Le message de test ne doit contenir aucune pièce jointe, signature ou toute autre information en dehors de le sujet du message et la ligne de test.

3. Envoyez ce message via le protocole SMTP à toute adresse de test.
4. Ouvrez l'utilitaire standard Windows **Observateur d'événements** -> **Doctor Web** (**Event Viewer** -> **Doctor Web**) et trouvez le message informant que Dr.Web a détecté un spam.

**Pour créer le message de test intégré**

1. Dans le sujet du message, indiquez : **Vade Secure**.
2. Copiez la ligne ci-dessous dans le corps d'un nouveau message e-mail:

```
tiUS4kVZrTfBBZXZPuLrnstNpdo8vJ-Spam-high-PQQMbQu22jePzuV8TLwVdPo81QpGXNJxRI
```

Le message de test ne doit contenir aucune pièce jointe, signature ou toute autre information en dehors de le sujet du message et la ligne de test.

3. Envoyez ce message via le protocole SMTP à toute adresse de test.
4. Ouvrez l'utilitaire standard Windows **Observateur d'événements** -> **Doctor Web** (**Event Viewer** -> **Doctor Web**) et trouvez le message informant que Dr.Web a détecté un spam.

# 12. Annexes

## 12.1. Paramètres de scan antivirus de Microsoft Exchange Server

Vous pouvez configurer les paramètres du scan antivirus basé sur VSAPI avec un jeu de clés de registre qui peuvent être classés selon les types suivants :

- paramètres généraux ;
- paramètres de la base de données ;
- scan du transport SMTP.

Les paramètres du scan antivirus indiqués ci-dessous sont disponibles pour Microsoft Exchange Server 2003, 2007 et 2010.

### Paramètres généraux

Les paramètres généraux sont utilisés par défaut pour tous les stockages de messagerie sur le serveur.

#### Scan lors de l'accès

Clé du registre :

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\VirusScan]
"Enabled"=dword:00000001
```

Ce paramètre assure l'activation de l'analyse antivirus pour tous les stockages de messagerie. Le scan est effectué chaque fois que le client consulte un message.

#### Scan en tâche de fond

Clé du registre :

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\VirusScan]
"BackgroundScanning"=dword:00000001
```

Ce paramètre est responsable de l'activation du scan en tâche de fond. Le scan en tâche de fond prévoit la création d'un flux séparé (thread) dans lequel sont analysés tous les stockages de messagerie, y compris les stockages de dossiers partagés sur le serveur. L'activation du scan en tâche de fond peut considérablement diminuer les performances du serveur de messagerie. Pour ne pas augmenter la charge du serveur, le scan en tâche de fond se lance par défaut tous les jours à 01h15. Si nécessaire, vous pouvez modifier la planification et sélectionner une

période de temps pendant laquelle le scan en tâche de fond n'aura pas d'impact sur les performances du serveur.

### Scan proactif

Clé du registre :

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\VirusScan]

"ProactiveScanning"=dword:00000001
```

Ce paramètre active l'analyse proactive. Dans ce cas, tous les messages sont vérifiés dès qu'ils arrivent dans le stockage de messagerie. Dans ce cas-là, les messages dont la valeur TimeStamp n'est pas modifiée et qui ont subi une analyse proactive ne seront plus scannés à l'arrivée des requêtes utilisateur.

### Désactivation de l'analyse des messages sortants

Clé du registre :

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\VirusScan

"TransportExclusion"=reg_dword:00000000
```

Ce paramètre permet d'activer/désactiver (en cas de sélection de la valeur 1 ou 0 respectivement) l'analyse des messages sortants au moment de leur arrivée dans le système de transport du stockage de messagerie. Par défaut cette analyse est désactivée.

### Limitation du nombre de flux pour l'interface du scan antivirus

Le nombre de flux pour l'interface du scan antivirus VSAPI 2.6 est déterminé par défaut par les paramètres Exchange Server, mais on peut le paramétrer manuellement par la création de la variable **ScanningThreads** dans la section du registre indiquée ci-dessous.

Clé du registre :

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeIS\VirusScan

"ScanningThreads"=reg_dword
```

Ce paramètre détermine le nombre maximum de flux créés pour le scan. La modification de ce paramètre influence le scan lors de l'accès et le scan proactif mais elle n'influence pas le scan en tâche de fond pour lequel est utilisé un seul flux pour une base de données.

Par défaut la valeur de cette variable est égale à 2*<*nombre de processeurs*> +1.

## Paramètres de la base de données

A l'aide des paramètres de ce type on peut spécifier les paramètres de scan pour chaque base de messagerie se trouvant sur le serveur de messagerie. Les paramètres sont enregistrés dans le registre par le chemin suivant :

`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\<Server-Name>\<ID Base>],`

où `<Server-Name>` est le nom du serveur, `<ID Base>` est l'identificateur de la base de messagerie, par exemple, `Private-ae39732e-fb7f-426d-98a0-298f3f014c77`.

Paramètres :

- "VirusScanEnabled"=`dword:00000001` : activation du scan antivirus pour la base de données indiquée ;
- "VirusScanBackgroundScanning"=`dword:00000001` : activation du scan en tâche de fond pour la base de données indiquée ;
- `"VirusScanProactiveScanning"=dword:00000001` : activation du scan proactif pour la base de données indiquée.

## Scan du transport SMTP

Les paramètres du scan du transport sont accessibles uniquement pour le serveur Exchange 2003.

Clé du registre :

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Exchange\TransportAVAPI\]
"Enabled"=dword:00000001
```

Par défaut le scan de transport est désactivé. Vous pouvez l'activer à la dernière étape de l'installation du programme. Par conséquent, la première analyse antivirus du message sera effectuée suite à l'événement SMTP **OnSubmission** mettant le message dans la file d'attente de traitement, au niveau du transport. La prochaine analyse sera effectuée au niveau du stockage d'information Exchange lors d'une requête de l'utilisateur pour le message.

## 12.2. Enregistrement manuel des agents de transport

Dans certains cas, par exemple en cas d'erreur d'enregistrement des agents de transport lors de l'installation de Dr.Web, il est nécessaire de les enregistrer manuellement. Pour ce faire, exécutez les commandes suivantes dans la console Exchange Management Shell :

```
Install-TransportAgent -Name "Dr.Web AntiSpam Agent" -
TransportAgentFactory "DRWTransportAgent.AntiSpamAgentFactory" -
AssemblyPath "C:\Program Files\DrWeb for
Exchange\DRWTransportAgent.dll"
```

```
Install-TransportAgent -Name "Dr.Web AntiVirus Agent" -
TransportAgentFactory "DRWTransportAgent.AntiVirusAgentFactory" -
AssemblyPath "C:\Program Files\DrWeb for
Exchange\DRWTransportAgent.dll"
```

```
Enable-TransportAgent "Dr.Web AntiSpam Agent"
```

```
Enable-TransportAgent "Dr.Web AntiVirus Agent"
```

Lorsque vous copiez les commandes du manuel, supprimez obligatoirement les fins de lignes.

Pour annuler l'enregistrement des agents de transport, exécutez les commandes suivantes dans la console Exchange Management Shell :

```
Uninstall-TransportAgent "Dr.Web AntiSpam Agent"
```

```
Uninstall-TransportAgent "Dr.Web AntiVirus Agent"
```

## 12.3. Déconnexion manuelle de Dr.Web du serveur de messagerie

En cas de défaillances de l'installation ou du fonctionnement de Dr.Web, vous pouvez le déconnecter du serveur de messagerie. Pour ce faire, effectuez les actions suivantes :

- Si les agents de transport sont installés :

  

  Les agents de transport sont disponibles pour Microsoft Exchange Server 2007, 2010, 2013 et 2016.

  - Dans la console Exchange Management Shell exécutez la commande `Get-Transportagent` (si les agents ont été installés en supplément dans les services de transport, dans le paramètre `-TransportService`, il est nécessaire de préciser le service). Pour plus d'informations sur cette commande, suivez le lien http://technet.microsoft.com/ru-ru/library/bb123536(v=exchg.150).aspx.
  - Dans la console Exchange Management Shell, s'affiche la liste des agents enregistrés dans le service de transport indiqué. Trouvez parmi eux ceux qui concernent Dr.Web (c'est-à-dire, ceux qui contiennent le préfixe **Dr.Web** dans leurs noms) et pour chaque agent, copiez le nom dans la commande `Disable-TransportAgent` <*nom de l'agent*> (si nécessaire, spécifiez le paramètre `-TransportService`). Pour plus d'informations sur cette commande, suivez le lien : http://technet.microsoft.com/ru-RU/library/aa997880(v=exchg.150).aspx.
  - Redémarrez le service de transport Microsoft Exchange Transport (et Microsoft Exchange Frontend Transport, si cela est nécessaire). Les agents de transport seront déconnectés des services de transport.
  - Exécutez la commande `Get-Transportagent` encore une fois et assurez-vous que les agents indiqués ont reçus le statut **Disable**.

  Ainsi l'application sera déconnectée de la chaîne de transport.

- Si le module VSAPI est installé :

  

  Le module VSAPI est disponible pour Microsoft Exchange Server 2003, 2007 et 2010.

  - Vérifiez la valeur du paramètre `Enabled` indiquée dans la rubrique du registre `[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\VirusScan]` : si `"Enabled »=dword:00000001`, il est nécessaire de la réinitialiser :`"Enabled"=dword:00000000`. S'il n'y a pas de telle rubrique du registre ou que la valeur zéro est déjà spécifiée pour le paramètre, le module VSAPI est déjà désactivé.
  - Redémarrez le service Microsoft Exchange Information Store. Le module de scan antivirus sera déconnecté du service indiqué.

  Maintenant l'application est déconnectée de l'assistant des stockages de messagerie.

- Si le module DrWebSink est installé :

Le module DrWebSink est disponible pour Microsoft Exchange Sever 2003.

- Lancez la console de commande (cmd) avec les privilèges administrateurs et exécutez la commande suivante :

```
regsvr32 /u "C:\Program Files\DrWeb for Exchange\DrWebSink.dll"
```

- Redémarrez Microsoft Internet Information Services (IIS).

Déconnectée du serveur de messagerie, l'application n'influence pas son fonctionnement.

## 12.4. Suppression manuelle de Dr.Web

En cas de défaillances du serveur de messagerie, vous pouvez supprimer Dr.Web manuellement. Pour ce faire, exécutez les actions suivantes :

1. Déconnectez Dr.Web du serveur de messagerie.
2. Supprimez l'enregistrement des agents de transport, en exécutant les commandes suivantes dans la console Exchange Management Shell :

```
Uninstall-TransportAgent "Dr.Web AntiSpam Agent"
Uninstall-TransportAgent "Dr.Web AntiVirus Agent"
```

3. Lancez la console de commande (cmd) avec les privilèges administrateurs.
4. Arrêtez les services de l'application dans l'ordre suivant :

```
net stop "Dr.Web SSM"
net stop "Dr.Web for MSP Scanning Service"
net stop "Dr.Web for MSP Components Host"
net stop "Dr.Web for MSP Requests Queue"
net stop "Dr.Web CMS Web Console"
net stop "Dr.Web CMS"
```

5. Supprimez les services de l'application :

```
sc delete "Dr.Web SSM"
sc delete "Dr.Web for MSP Scanning Service"
sc delete "Dr.Web for MSP Components Host"
sc delete "Dr.Web for MSP Requests Queue"
sc delete "Dr.Web CMS Web Console"
sc delete "Dr.Web CMS"
```

Pour supprimer le service Dr.Web Scanning Engine, l'utilitaire **drw_remover.exe** est requis. Pour l'obtenir, vous pouvez vous adresser au service de support technique de Doctor Web.

6. Indiquez les dossiers suivants :

```
rd /S /Q "C:\Program Files\DrWeb for Exchange"
rd /S /Q "C:\Documents and Settings\All Users\Application
Data\Doctor Web"
rd /S /Q "C:\Program Files\Common Files\Doctor Web"
```

## 12.5. Plateforme CMS

CMS (Central Management System) représente un système à répartition multi-plateforme permettant de gérer les applications (par application, on entend ci-après n'importe quel module-abonné du serveur principal). Le centre du système est le service gérant Dr.Web CMS. Ce service exécute les fonctions essentielles du système visant à contrôler le fonctionnement des applications, ainsi que la gestion des applications, des paramètres des applications et l'enregistrement des événements.

L'interaction entre les applications s'effectue via le protocole TCP. L'interaction des applications avec le service gérant peut s'effectuer de deux façons :

- l'application contrôlée interagit avec le service gérant via le protocole MB (Management Base) ;
- les applications gérantes (administrateur) interagissent avec le serveur gérant via le protocole MS (Management System).

Le service Dr.Web CMS utilise une base de données arborescente pour le stockage de données sur les applications.

### 12.5.1. Base de données

La base de données du service gérant Dr.Web CMS représente une arborescence contenant des groupes et des variables. Les variables peuvent être de types (de données) différents et avoir des attributs différents.

Types de données des variables supportées par le service gérant Dr.Web CMS :

| Type de données | Description |
|---|---|
| Int32 | entier 32 bits signé |
| UInt32 | entier 32 bits non signé |
| Int64 | entier 64 bits signé |
| UInt64 | entier 64 bits non signé |
| Float | Nombre réel 32 bits |
| Double | Nombre réel 64 bits |
| String | Ligne d'une longueur illimitée |
| Boolean | Valeur logique (true ou false) |
| Time | Date et heure |

| Type de données | Description |
|---|---|
| Binary | Données binaire d'une longueur illimitée |
| Password | Type de données pour la sauvegarde de mots de passe |

Les attributs des variables peuvent être les suivants :

| Attribut | Description |
|---|---|
| Default | Valeur ordinaire |
| Shared | Variable à répartition |
| Statistics | Variable statistique |
| System | Variable système |
| Hidden | Variable système cachée |
| Readonly | Variable à ne pas modifier |

## 12.5.2. Contrôle des applications

Pour le contrôle de l'application avec CMS, le nom et la version de l'application sont enregistrés dans la base du serveur gérant. Le service Dr.Web CMS attribue un nom unique à l'application. Ce nom contient le nom de l'application et sa version. Ensuite, le service crée dans la base de données un groupe portant le nom de l'application enregistrée. Par défaut, les sous-groupes **Application Status** et **Settings** sont créés dans ce groupe. Lors du fonctionnement de l'application, le service gérant collecte des statistiques des protocoles d'interaction. Les statistiques sont enregistrées dans le groupe **Application Statistics/Connections**, les statistiques d'interaction par protocoles sont enregistrées dans les sous-groupes **MB** et **MS**. En utilisant les données statistiques, on peut évaluer la charge sur ces serveurs et ces applications.

### Groupe Application Status

Ce groupe contient des informations sur l'application enregistrée sous forme de valeurs de variables de différents types :

| Variable (le type de variable est indiqué entre parenthèses) | Description |
|---|---|
| **Active** (Boolean) | Détermine si l'application est lancée. La valeur **true** signifie que l'application est lancée. |

| Variable (le type de variable est indiqué entre parenthèses) | Description |
|---|---|
| **Crash** (Boolean) | Détermine si l'application a été arrêtée correctement. La valeur **true** signifie que l'application a été arrêtée d'une manière incorrecte. |
| **HomeDir** (String) | Répertoire de l'application dans le système de fichiers |
| **InstanceName** (String) | Nom que l'application a déclaré lors de l'enregistrement |
| **LogicCrash** (Boolean) | Statut de la logique de l'application. La valeur **true** signifie que l'application fonctionne d'une manière incorrecte. |
| **ModuleName** (String) | Nom du fichier exécutable de l'application. Au cas où c'est la bibliothèque *.dll est une application-abonné, la variable indique le nom du processus qui l'a instanciée. |
| **ModulePath** (String) | Chemin vers le fichier exécutable de l'application dans le système de fichiers |
| **PID** (UInt32) | Numéro du processus dans le système d'exploitation |
| **StartedOn** (Time) | Heure du dernier lancement de l'application |
| **StoppedOn** (Time) | Heure du dernier arrêt de l'application |
| **Version** (String) | Version de l'application |
| **VersionBuild** (UInt32) | Numéro d'assemblage de l'application |
| **VersionMajor** (UInt32) | Numéro principal de la version de l'application |
| **VersionMinor** (UInt32) | Deuxième numéro de la version de l'application |
| **VersionRevision** (UInt32) | Numéro de révision de l'application |
| **WorkDir** (String) | Répertoire de travail de l'application dans le système de fichiers |

### Groupe Settings

Ce groupe contient les paramètres de base de l'application enregistrée.

### 12.5.3. Statistiques

Le système permet de recueillir des statistiques d'intervalle des applications. Du côté des applications, il existe une possibilité de créer des variables statistiques qui peuvent enregistrer des événements ayant lieu dans des applications et de créer l'ensemble des statistiques dans les intervalles de temps spécifiés, en fonction des paramètres de la variable statistique.

Dans la base de données du service gérant Dr.Web CMS, ces variables ont l'attribut **Statistics**. Les variables avec un tel attribut sont temporaires, elles ne sont pas sauvegardées dans la base de données permanente et elles n'existent que pendant le fonctionnement du service gérant. Après le redémarrage du service, ces variables se perdent.

### 12.5.4. Administration

La gestion du système s'effectue via le protocole d'administration. Le protocole permet de modifier au hasard les valeurs des variables, de réinitialiser les statistiques des variables statistiques, de suivre le traçage en temps réel avec l'application des filtres et de décharger les messages collectés pour les périodes précédentes avec le filtrage.

#### Modification des valeurs des variables

La modification des valeurs des variables s'effectue simultanément. Toutes les applications enregistrées reçoivent les notifications sur la modification des valeurs des variables et elles peuvent autoriser ou interdire la modification. En cas de modification de la variable, les applications reçoivent sa valeur actuelle.

#### Collection des statistiques

Le protocole d'administration permet de réinitialiser les statistiques collectées sur la configuration. Il en résulte que la collection des statistiques sur ce paramètre commence à zéro.

#### Restrictions du travail avec les variables

Lors du travail avec des variables, il existe les restrictions suivantes :

- les variables avec l'attribut **Hidden** existent dans la base, mais elles ne sont pas accessibles à la consultation ni modifiables. Elles sont créées par le service gérant pour un usage de service ;
- les variables avec l'attribut **System** sont créées par le service gérant pour l'affichage des informations de service destinées à l'administrateur. Ces variables ne peuvent pas être modifiées ou supprimées ;
- les variables avec l'attribut **Statistics** sont créées par l'application. Ces variables ne peuvent pas être modifiées ;

- les variables avec l'attribut **Readonly** sont créées par l'application pour informer l'administrateur. Ces variables ne peuvent pas être modifiées ;
- les variables avec l'attribut **Default** sont des variables ordinaires. On peut y appliquer toutes les actions ;
- les variables avec l'attribut **Shared** sont des variables à répartition. Les valeurs de ces variables sont modifiées simultanément dans tout le système à répartition.
- les variables qui ne peuvent pas être modifiées ne peuvent pas non plus être supprimées. Pourtant les groupes contenant ces variables peuvent être supprimés avec ces variables, si l'application liée à ce groupe n'est pas lancée.

**Sécurité**

Pour accéder au système, il est nécessaire d'entrer le nom d'utilisateur et le mot de passe. Par défaut, l'utilisateur **root** avec le mot de passe **drweb** existe dans le système. Il est recommandé de changer de mot de passe après l'installation du système. De plus, vous pouvez ajouter de nouveaux utilisateurs.

Les utilisateurs et leurs mots de passe sont stockés dans le groupe du service gérant, dans le sous-groupe **Security** -> **Users**, c'est-à-dire par le chemin /CMS_1.0/Security/Users. Le nom de l'utilisateur est le nom du groupe. Le mot de passe est sauvegardé dans la variable Password.

## 12.5.5. Connexion aux serveurs

La console d'administration CMS permet de se connecter aux autres serveurs sur lesquels fonctionne CMS. Pour vous connecter :

1. Cliquez droit sur l'icône de l'hôte dans l'arborescence de la console et sélectionnez l'élément **Add host**.
2. Dans la fenêtre qui s'affiche, saisissez l'adresse de l'hôte auquel vous connectez et cliquez sur **OK**.
3. Entrez le nom d'utilisateur et le mot de passe pour la connexion à l'hôte sélectionné. Une fois saisies les données correctes, une connexion s'établit et un nouvel hôte s'affiche dans l'arborescence.

Vous pouvez utiliser le moyen décrit ci-dessus pour vous connecter à un nombre illimité de postes et pour les gérer. Les paramètres de chaque connexion sont enregistrés dans un groupe à part dans la Console d'administration CMS par le chemin **/Dr.Web CMS Web Console_1.0/Application Settings/Hosts**. Chaque hôte ajouté est représenté sous forme d'un groupe ayant le nom de l'adresse de connexion à l'hôte ajouté. Trois variables sont créées au sein d'un tel groupe :

- **Address** contient l'adresse de connexion à l'hôte ;
- **Login** contient le nom d'utilisateur ;
- **Password** contient le mot de passe pour la connexion à l'hôte.

En cas de modification des données d'authentification sur l'hôte ajouté, l'accès à cet hôte peut être interdit. Dans ce cas, il est nécessaire de corriger les paramètres de connexion de la Console d'administration CMS à cet hôte.

Au lancement ultérieur, la Console d'administration CMS se connecte automatiquement aux hôtes ajoutés. Pour supprimer un hôte ajouté, il faut supprimer le groupe contenant les paramètres de connexion à cet hôte du groupe de paramètres de la Console d'administration CMS par le chemin **/Dr.Web CMS Web Console_1.0/Application Settings/Hosts**.

## 12.6. Service Dr.Web SSM

Le service Dr.Web SSM (Dr.Web Start/Stop Manager) contrôle le fonctionnement des applications tournant sous la plateforme CMS, en exécutant les fonctions suivantes :

- maintien de la productivité du service Dr.Web SSM en mode automatique ;
- lancement automatique des applications enregistrées (ayant le groupe de variables **SSM** dans la **Console d'administration CMS**) par le service en cas de défaillances de leur fonctionnement ;
- lancement forcé des applications même en cas d'arrêt inopiné ;
- lancement des applications avec Windows Service Manager ;
- lancement des services sous forme d'applications réalisées avec l'utilisation de CService из CommonComponents ;
- lancement des services à l'aide des scripts assignés ;
- arrêt et lancement des applications en mode manuel sur commande de l'utilisateur.

Les paramètres de contrôle de l'application par le service **Dr.Web SSM** sont déterminés par le groupe des variables **SSM** dans la **Console d'administration CMS**. Le groupe **SSM** peut contenir les variables suivantes :

| **Variable (le type de variable est indiqué entre parenthèses)** | **Description** |
|---|---|
| **Enabled** (Boolean) | Indique si l'activation/désactivation du contrôle SSM est lancée. |
| **Run** (Boolean) | Permet de lancer/arrêter l'application |
| **KeepAlive** (Int32) | Détermine le type de maintien de l'activité de l'application :<br>• 0 - l'application est désactivée ;<br>• 1 - l'application est activée ;<br>• 2 - forcée, ça veut dire que l'application sera activée même en cas de son arrêt correct. |
| **StartType** (Int32) | Détermine le type de lancement de l'application :<br>• 0 - en tant que service Windows ;<br>• 1 - en tant qu'application CService ;<br>• 2 - lancement à l'aide d'un script. |
| **StartScript** (String) | Contient un script pour le lancement de l'application |
| **StopScript** (String) | Contient un script pour l'arrêt de l'application |
| **Restart** (Boolean) | Effectue le redémarrage de l'application |
| **Timeout** (UInt32) | Désigne le délai d'attente d'une réaction de l'application (en secondes). La valeur 10 s est spécifiée par défaut. |

| Variable (le type de variable est indiqué entre parenthèses) | Description |
|---|---|
| **ServiceName** (String) | Désigne le nom du service dans Windows Service Manager. La valeur de la variable « /Application Status/InstanceName » est utilisée par défaut. |

La rubrique des paramètres du service Dr.Web SSM peut contenir les variables suivantes :

- **KeepAlivePeriod** (UInt32) - délai de vérification du service (en secondes). La valeur 60 secondes est utilisée par défaut.
- **RestartCMSPause** (UInt32) - délai d'attente avant le redémarrage de CMS (en secondes). La valeur 5 secondes est utilisée par défaut.

## 12.7. Configuration des paramètres de mise à jour

Pour la configuration de la mise à jour des bases virales et des composants de Dr.Web, le fichier **drwupsrv.bat** est disponible. Ce fichier se trouve dans le dossier contenant Dr.Web installé. Les commandes spécifiées dans le fichier sont appliquées au moment du démarrage de la tâche Doctor Web for Exchange Update Task dans le planificateur de tâches Windows.

Pour définir les paramètres de mise à jour, indiquez les paramètres nécessaires pour les commandes **- c update** et **- c postupdate**.

### Paramètres de la commande - c update

La commande **- c update** effectue la mise à jour automatique des bases virales et des composants Dr.Web.

| Paramètre | Description |
|---|---|
| --type arg | Type de mise à jour :<br>• update-revision - mise à jour des composants au sein de la révision actuelle. |
| --disable-postupdate | La mise à jour postérieure ne sera pas effectuée. Le module de mise à jour termine son fonctionnement après l'exécution de la mise à jour. |
| --verbosity arg | Niveau de détails du journal :<br>• error - standard ;<br>• info - accru ;<br>• debug - débogage. |
| --interactive | Si le paramètre est indiqué, un plus grand nombre de ressources sera utilisé pour l'exécution de certaines commandes. |

| Paramètre | Description |
|---|---|
| --param args | Paramètres supplémentaires transmis pour le script.<br>Format : <nom>=<valeur>.<br>La valeur "plugin=exchange". *est spécifiée par défaut.* |
| -n [ --component ] arg | Liste des composants à mettre à jour :<br>• updater - fichier drwupsrv.exe ;<br>• antispam -fichier vrcpp.dll ;<br>• scan-engine - fichiers dwengine.exe, ccsdk.dll, dwsewsc.exe, dwinctl.dll, dwarkdaemon.exe, arkdb.bin, dwqrui.exe, dwarkapi.dll;<br>• av-engine - bases virales (fichiers avec l'extension *.vdb) ;<br>• exchange-plugin-setup - fichier exchange-setup.exe.<br>⚠ Plusieurs éléments peuvent être mis à jour en même temps, par exemple :<br>`-n av-engine updater` |
| -g [ --proxy ] agr | Serveur proxy pour la mise à jour au format <adresse>: <port>. |
| -u [ --user ] agr | Nom de l'utilisateur du serveur proxy. |
| -k [ --password ] arg | Mot de passe de l'utilisateur du serveur proxy. |

Exemple de la commande - c update pour la mise à jour des bases virales via le serveur proxy :

```
-c update --type=update-revision --disable-postupdate --
verbosity=debug --interactive --param="plugin=exchange" -n av-engine
--proxy=192.168.134.128:808 --user=qwerty --password=qwerty
```

### Paramètres de la commande - c postupdate

La commande**- c postupdate** effectue la mise à jour postérieure des bases virales et des composants Dr.Web.

| Paramètre | Description |
|---|---|
| --verbosity arg | Niveau de détails du journal :<br>• error - standard ;<br>• info - accru ;<br>• debug - débogage. |

| Paramètre | Description |
|---|---|
| --interactive | Si le paramètre est indiqué, un plus grand nombre de ressources sera utilisé pour l'exécution de certaines commandes. |
| --param arg | Paramètres supplémentaires transmis pour le script.<br><br>Format : <nom>=<valeur>.<br><br>La valeur "plugin=exchange". *est spécifiée par défaut.* |

Exemple de la commande **- c postupdate** :

```
-c postupdate --verbosity=debug --interactive --
param="plugin=exchange"
```

## Miroir de mises à jour

Si vous n'avez pas la possibilité de mettre à jour Dr.Web par Internet ou que vous voulez limiter le volume de trafic externe, vous pouvez créer un miroir pour exécuter la mise à jour des produits de Doctor Web par le réseau local.

Pour créer un miroir de mises à jour, effectuez les actions suivantes sur un serveur ayant accès à Internet :

1. Lancez le fichier **drwupsrv.exe** avec les paramètres suivants :

```
-c download --zones=<file_path> --key-dir=<folder_path> --
repodir=<folder_path> --version=90 --verbosity=debug --log-dir=C:\Repo
```

Indiquez les valeurs nécessaires des paramètres :

**zones=<file_path>** — chemin vers le fichier de la zone de mise à jour drwzones.xml ;

**key-dir=<folder_path>** — chemin vers le dossier contenant le fichier clé de licence ;

**repo-dir=<folder_path>** — chemin vers le dossier contenant les mises à jour. Notez que l'accès partagé doit être configuré pour le dossier.

Par exemple :

```
drwupsrv.exe -c download --zones=C:\Mirror\drwzones.xml --key-dir=C:
\Mirror\ --repodir=C:\Mirror\Repo\ --version=90 --verbosity=debug --
log-dir=C:\Mirror\Repo\
```

2. Sur le serveur avec Dr.Web installé, ouvrez le fichier **drwupsrv.bat** dans la ligne `set upparams`, ajoutez le paramètre suivant et lancez le fichier :

```
--zone="file://<repo_folder_path>"
```

Par exemple :

```
set upparams=-c update --type=update-revision --disable-postupdate --
verbosity=debug --interactive --param="plugin=exchange" --
zone="file://<repo_folder_path>"
```

## 12.8. Fonctionnement dans le mode de protection centralisée

Dr.Web peut fonctionner dans le réseau géré par le Centre de Gestion Dr.Web. L'organisation de la protection centralisée permet d'automatiser et de faciliter la configuration et la gestion du système de sécurité informatique des ordinateurs réunis dans une structure logique (par exemple, des ordinateurs d'entreprise se trouvant dans un réseau local ainsi que hors du réseau). Les ordinateurs protégés sont réunis dans un réseau antivirus commun dont la sécurité est contrôlée par les administrateurs depuis le serveur central (Centre de Gestion Dr.Web). Si vous connectez aux systèmes de protection centralisée, vous obtenez un très haut niveau de protection avec un minimum d'effort de la part des utilisateurs finaux.

Si Dr.Web fait partie du réseau antivirus du logiciel Enterprise Security Suite 11.0, le plug-in peut être configuré depuis le Centre de gestion de la sécurité Dr.Web. La procédure de configuration du plug-in depuis le Centre de gestion de la sécurité est décrite dans le manuel administrateur d'Enterprise Security Suite. Les statistiques du fonctionnement du plug-in en mode de protection centralisée sont transférées sur le Serveur Dr.Web.

### Interaction des composants du réseau antivirus

Les solutions de Doctor Web destinées à la protection antivirus centralisée ont une architecture client-serveur (voir Figure 17).

Les ordinateurs de l'entreprise sont protégés contre les menaces et contre le spam par les composants antivirus locaux (clients ; ici –Dr.Web) assurant la protection antivirus et permettant de faciliter la connexion au serveur de protection centralisée.

La mise à jour et la configuration des composants locaux se font via le *serveur central*. Tout ensemble de commandes, données et statistiques relatif au réseau antivirus passe également par le serveur de protection centralisée. L'option de compression du trafic est incluse compte tenu du fait que le trafic circulant entre les ordinateurs protégés et le serveur antivirus peut être assez important. L'utilisation du cryptage lors de la transmission de données permet d'éviter d'éventuelles fuites d'informations confidentielles ou la substitution des logiciels téléchargés sur les ordinateurs protégés.

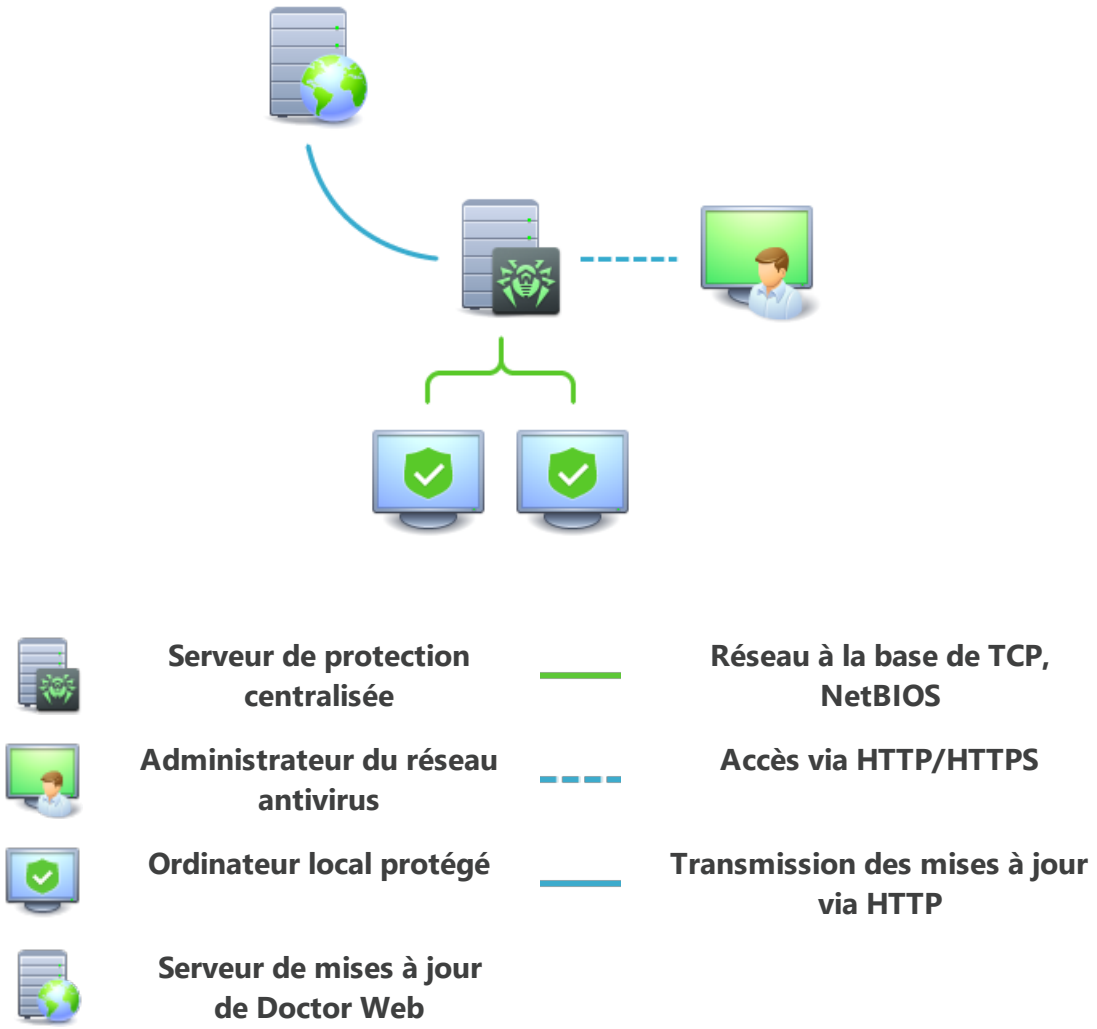


**Figure 17. Structure logique du réseau antivirus**

Toutes les mises à jour nécessaires sont téléchargées sur le serveur de protection centralisée depuis les serveurs de mises à jour Dr.Web.

Les modifications de la configuration des composants antivirus locaux et la transmission des commandes sont effectuées par le serveur antivirus selon les commandes des *administrateurs du réseau antivirus*. Les administrateurs gèrent la configuration du serveur central et l'évolution du réseau antivirus (notamment, ils valident la connexion des postes locaux au réseau), si nécessaire, ils peuvent également spécifier les paramètres des composants antivirus locaux.

## Fonctionnement de Dr.Web en mode de protection centralisée

Le fonctionnementDr.Web en mode de protection centralisée nécessite que Dr.Web Agent soit installé et fonctionne correctement dans le système d'exploitation.

Dr.Web de la version 11.5 est incompatible avec Dr.Web Agent de la version 6.

Si Dr.Web Agent a été installé après l'installation de Dr.Web :

1. Dans le planificateur de tâches Windows, désactivez **Doctor Web for Exchange Update Task**.
2. Dans la Console d'administration CMS, modifiez le mode de licensing : sélectionnez une option d'utilisation de la licence depuis le serveur de protection centralisée (voir Modification du mode de licensing).

Ensuite, lancez la mise à jour depuis la Console sur le serveur de protection centralisée et assurez-vous que la mise à jour a réussi.

### Licence

En mode de protection centralisée, on utilise le fichier clé de licence de Dr.Web enregistré pour ce poste au sein du réseau antivirus. Si à l'étape d'installation, vous avez choisi l'option d'utilisation de la licence depuis le serveur de protection centralisée, alors au moment du lancement de Microsoft Exchange Server avec Dr.Web installé, une tentative d'utiliser la clé de licence sera effectuée pour ce poste au sein du réseau antivirus. Si la clé est invalide, le scan antivirus ne sera pas exécuté. Si au moment de l'installation, vous avez choisi une autre option d'obtention de la licence, il est nécessaire de modifier le mode de licensing avec la console CMS (1).

### Mise à jour

Mise à jour des bases virales et du noyau antivirus depuis le dépôt du Centre de Gestion Dr.Web. Ceci permet de désactiver le module standard de mise à jour Dr.Web Updater lancé selon la planification. Dans ce cas-là, la mise à jour des composants sera effectuée selon la planification du Centre de Gestion Dr.Web et depuis son dépôt ;

### Actions après la suppression de Dr.Web Agent

Si Dr.Web Agent a été supprimé, pour le fonctionnement correct de Dr.Web :

1. Dans le planificateur de tâches Windows, ajoutez la tâche de mise à jour de Dr.Web. Pour ce faire :
   - Ouvrez le planificateur de tâches Windows.
   - Créez la tâche avec le nom **Doctor Web for Exchange Update Task**.
   - Dans l'onglet **Généraux** de l'assistant de création d'une tâche, activez **Exécuter pour tous les utilisateurs** et cochez la case **Exécuter avec les droits supérieurs**. Dans la liste **Configurer pour**, sélectionnez Windows Server™ 2003, Windows® XP ou Windows® 2000.
   - Dans l'onglet **Déclencheurs** spécifiez l'intervalle de temps pour l'exécution de la tâche.

- Dans l'onglet **Actions**, créez l'action **Démarrage du programme** et sélectionnez le programme **<chemin vers le dossier d'installation *Dr.Web*>\drwupsrv.bat**.
- Dans l'onglet **Conditions**, décochez toutes les cases cochées par défaut.

2. Modifiez le mode de licensing. Il est nécessaire de sélectionner l'option de licensing par obtention du fichier clé (0).

# Référence

# Référence

# Référence

## R



## S



## V