



Dr.WEB

pour Microsoft ISA Server et Forefront TMG

Manuel Administrateur

Жасағаныңды

دافع عن إبداعاتك

Защити созданное

Defend what you create

Protégez votre univers

Verteidige, was du erschaffen hast

Захисти створене

保护您创建的一切

Защити созданное

Proteggi ciò che crei

Жасағаныңды қорға

Защити созданное

Proteggi ciò che crei

Verteidige, was du erschaffen hast

Захисти створене

Defend what you create

脅威からの保護を提供します

Protégez votre univers

Proteggi ciò che crei

Захисти створене

دافع عن إبداعاتك

脅威からの保護を提供します

Defend what you create

Жасағаныңды қорға

دافع عن إبداعاتك

دافع عن إبداعاتك

Protégez votre univers

保护您创建的一切

Защити созданное

脅威からの保護を提供します

Захисти створене

Verteidige, was du erschaffen hast

© Doctor Web, 2018 . Tous droits réservés

Le contenu publié dans cette documentation est la propriété de la société Doctor Web et ne peut être utilisé par l'acheteur du produit qu'à des fins non commerciales. Aucune partie de cette documentation ne peut être copiée, publiée sur un lecteur réseau ou diffusée dans les médias ou ailleurs sans faire référence à la source, à moins qu'elle ne soit utilisée à des fins personnelles.

Marques déposées

Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-Desk et le logo Dr.WEB sont des marques déposées de Doctor Web en Russie et/ou dans d'autres pays. Toute autre marque ou logo ainsi que les noms de société cités ci-dessous appartiennent à leurs propriétaires.

Limitation de responsabilité

En aucun cas Doctor Web et ses revendeurs ne sont tenus responsables des erreurs/lacunes éventuelles pouvant se trouver dans cette documentation, ni des dommages directs ou indirects causés à l'acheteur du produit, y compris la perte de profit.

Dr.Web pour Microsoft ISA Server et Forefront TMG
Version 11.0
Manuel Administrateur
1/31/2018

Doctor Web, Siège social en Russie
125040
Moscou, Russie
2-12A, 3e rue Yamskogo polya
Site web : <http://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	6
2. Support technique	7
3. Introduction	8
3.1. Usage de Dr.Web	8
3.2. Objets contrôlés	9
4. Licence	10
4.1. Fichier clé de licence	10
4.2. Obtenir un fichier clé	10
4.3. Mise à jour de la licence	11
5. Composants Dr.Web	12
5.1. Filtres de Dr.Web	12
5.1.1. Filtres d'applications	12
5.1.2. Filtre web	17
5.2. Services de Dr.Web	20
5.3. Quarantaine	20
5.4. Surveillance des événements viraux	20
6. Installation et suppression	21
6.1. Pré-requis système	21
6.2. Compatibilité	22
6.3. Installation de Dr.Web	23
6.4. Suppression de Dr.Web	24
7. Console d'administration Dr.Web Administrator Web Console	25
7.1. Groupes et profils	26
7.2. Création et configuration des profils	27
7.2.1. Priorité de profil	28
7.2.2. Scan	28
7.2.3. Antispam	30
7.2.4. Office Control	32
7.2.5. Filtrage	34
7.3. Gestion des groupes clients	40
7.3.1. Création d'un nouveau groupe	40
7.3.2. Paramètres et formation des groupes	42
7.4. Notifications	43




7.5. Consulter les statistiques	45
7.6. Consulter la liste des incidents	47
7.7. Gestion de la quarantaine	48
7.7.1. Consulter la quarantaine avec Dr.Web for ISA Web Console	48
7.7.2. Gestionnaire de quarantaine	49
8. Mise à jour des bases virales	53
8.1. Informations sur la version du programme et les bases virales	53
9. Console web Dr.Web CMS Web Console	55
9.1. Changer le mot de passe du compte administrateur	57
9.2. Ajouter de nouveaux administrateurs	57
9.3. Créer les clusters	58
9.4. Sélectionner les types d'objets endommagés	60
9.5. Filtrage des fichiers en archive par leurs extensions	61
10. Journalisation des événements	62
10.1. Journal du système d'exploitation	62
10.2. Journal texte de l'assistant d'installation	63
10.3. Journal d'événements Dr.Web	63
10.3.1. Types d'événements enregistrés	64
10.3.2. Niveau de détails	64
10.3.3. Suppression de la base de données cmstracedb	65
11. Diagnostic	66
11.1. Vérification de l'installation	66
11.2. Vérification du module de mise à jour	67
11.3. Vérification de la détection de virus	67
11.4. Vérification de la détection de spam	68
12. Annexes	69
12.1. Annexe A. Suppression manuelle de Dr.Web	69
12.2. Annexe B. Plateforme CMS	70
12.2.1. Base de données	70
12.2.2. Statistiques	71
12.2.3. Connexion aux serveurs	72
12.3. Annexe C. Configuration des paramètres de mise à jour	73
Référence	76



1. Légende et abréviations

Symboles utilisés dans ce manuel :

Symbole	Utilisés
	Avertissement sur des situations potentielles d'erreurs et sur les éléments importants auxquels il faut faire attention.
<i>Réseau antivirus</i>	Un nouveau terme ou l'accent mis sur un terme dans les descriptions.
<i><IP-address></i>	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\ 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. 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.fr/doc/> ;
- lisez la rubrique de questions fréquentes à l'adresse http://support.drweb.fr/show_faq/ ;
- visitez des forums de Doctor Web à l'adresse : <http://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.fr/> ;
- 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 <http://company.drweb.fr/contacts/offices/>.



3. Introduction

Merci d'avoir acheté Dr.Web pour Microsoft ISA Server et Forefront TMG (ci-après – Dr.Web).

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 et contient les coordonnées du service de support technique.

3.1. Usage de Dr.Web

Dr.Web est une application qui sert à protéger le réseau d'entreprise contre les menaces virales et le spam. Elle s'intègre dans le système, cherche et supprime les menaces de tous les types dans le flux de données passant par Microsoft Internet Security and Acceleration Server (ci après dénommé Microsoft ISA Server) et Microsoft Forefront Threat Management Gateway (ci-après dénommé Microsoft Forefront TMG) via les protocoles HTTP, FTP, SMTP et POP3. L'application analyse le trafic entrant pour la présence de virus, dialers, adwares, riskwares, hacktools et canulars.

L'application intègre ses propres filtres de données dans les services Microsoft Firewall Service et Microsoft Forefront TMG Firewall, ce qui assure l'accès du noyau du système antivirus Dr.Web à ces services. Dr.Web fonctionne sur la plateforme qui a le serveur web intégré avec l'authentification du client et la console web de gestion.

Les services Dr.Web installés sur les serveurs différents peuvent être réunis par l'administrateur en un cluster (voir la section [Créer les clusters](#)).

Dr.Web peut réaliser les fonctions suivantes :

- scan de toutes les données passant par le pare-feu Microsoft ISA Server ou Microsoft Forefront TMG via les protocoles FTP (y compris FTP par-dessus HTTP), HTTP, SMTP et POP3 ;
- blocage de l'accès aux données infectées pour les utilisateurs des réseaux locaux protégés par le pare-feu Microsoft ISA Server ou Microsoft Forefront TMG ;
- isolement des objets infectés et suspects en quarantaine ;
- envoi des notifications sur les événements viraux au journal du système d'exploitation et support de la base de données interne des événements ;
- filtrage de spam dans les messages obtenus par le protocole SMTP ;
- ajout du texte d'accompagnement pour les e-mails contenant des menaces ;
- limitation d'accès d'utilisateurs aux ressources Internet ;
- récolte des statistiques ;
- mise à jour automatique des bases virales et des composants du programme ;
- support des paramètres communs de l'application spécifiés de manière centralisée dans le système distribué de pare-feux, y compris ceux qui sont groupés en cluster.



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.

3.2. Objets contrôlés

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

Objets de l'analyse du trafic passant par les protocoles HTTP FTP

Dr.Web effectue l'analyse du trafic HTTP et FTP passant par le pare-feu Microsoft ISA Server et Microsoft Forefront TMG en temps réel. L'objet de l'analyse est une ressource spécifiée dans la requête du client. Soit Microsoft ISA Server et Microsoft Forefront TMG se connectent au serveur mentionné dans la requête au serveur et obtiennent la ressource du serveur, soit ils retournent la ressource de leur propre cache. Les filtres et les applications interceptent les données obtenues (y compris les données dans des archives et les données empaquetées).



Dans la plupart des cas, l'analyse antivirus est possible uniquement si le fichier entier est disponible. C'est pourquoi l'accumulation et le scan des données requises peut prendre un certain temps.

Objets de l'analyse du trafic passant par les protocoles SMTP et POP3

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

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



4. Licence

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

4.1. 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.

4.2. 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.

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 *le fichier clé de démonstration*. Ce fichier clé assure le fonctionnement de tout l'ensemble de composants antivirus principaux mais pour un temps limité et il ne fournit pas de service de support technique à l'utilisateur.

Pour obtenir le fichier clé démonstration (par e-mail), merci de vous enregistrer sur la page suivante <http://download.drweb.fr/demoreq/>.

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/>.

4.3. 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, remplacez le fichier clé dans le répertoire d'installation du programme (%PROGRAMFILES%\DrWeb CMS for MSP\) par un nouveau fichier clé.
2. 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/>.



5. Composants Dr.Web

Toutes les solutions antivirus Doctor Web comprennent les composants suivants assurant la protection de tous les systèmes d'exploitation et de toutes les plateformes :

- le noyau antivirus drweb32.dll ;
- 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.

Le produit a l'interface web d'administrateur Dr.Web Administrator Web Console pour la gestion commode des paramètres de scan et le suivi des événements viraux du serveur via le navigateur. Voir la description détaillée des paramètres dans le chapitre [Console d'administration Dr.Web Administrator Web Console](#).

Dr.Web comprend également la console web auxiliaire Dr.Web CMS Web Console qui sert à détecter et corriger les erreurs. Elle fournit également la possibilité de spécifier les paramètres avancés et modifier la configuration de Dr.Web. Pour plus d'informations, voir la section [Console web Dr.Web CMS Web Console](#).

5.1. Filtres de Dr.Web

Dr.Web intercepte les données des connexions réseau pour l'analyse ultérieure à l'aide des filtres spéciaux intégrés dans le service Microsoft Firewall Service (pour Microsoft ISA Server) ou Microsoft Forefront TMG Firewall (pour Microsoft Forefront TMG).

Tous les filtres sont réalisés sous forme de bibliothèques dynamiques lancées au démarrage du pare-feu Microsoft Firewall Service ou Microsoft Forefront TMG Firewall et résident dans la mémoire jusqu'à l'arrêt de ce service. Les filtres obtiennent l'accès au flux de données dans le service de pare-feu. Si, à la suite d'une requête du client (request) ou d'une réponse (response) du serveur, un événement est créé et qu'il y a un filtre qui est enregistré pour cet événement, alors le filtre intercepte et analyse les données contenues dans le flux de données.

Trois filtres d'application (application filters) et un filtre web (web filter) sont inclus dans Dr.Web.

5.1.1. Filtres d'applications

Trois filtres d'applications sont inclus dans Dr.Web :

- [Dr.Web FTP Filter](#) ;
- [Dr.Web SMTP Filter](#) ;
- [Dr.Web POP3 Filter](#).



Les filtres d'applications se trouvent dans les répertoires suivants :

Filtre	Chemin vers la bibliothèque du filtre
Dr.Web FTP Filter	Si vous utilisez Microsoft ISA Server : %PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG\FTPFilter.dll Si vous utilisez Microsoft Forefront TMG : %PROGRAMFILES%\Microsoft Forefront Threat Management Gateway\DrWeb for ISA and TMG\FTPFilter.dll
Dr.Web SMTP Filter	Si vous utilisez Microsoft ISA Server : %PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG\SMTPFilter.dll Si vous utilisez Microsoft Forefront TMG : %PROGRAMFILES%\Microsoft Forefront Threat Management Gateway\DrWeb for ISA and TMG\SMTPFilter.dll
Dr.Web POP3 Filter	Si vous utilisez Microsoft ISA Server : %PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG\POP3Filter.dll Si vous utilisez Microsoft Forefront TMG : %PROGRAMFILES%\Microsoft Forefront Threat Management Gateway\DrWeb for ISA and TMG\POP3Filter.dll

Les filtres énumérés sont destinés à exécuter les opérations sur l'ensemble des paquets de protocoles. Ils effectuent l'analyse des données et bloquent les données en cas de détection de menaces virales. Tous les filtres sont réunis dans une branche particulière de l'arborescence de la console d'administration Microsoft ISA Server / Microsoft Forefront TMG (voir [Figure 1a](#), [Figure 1b](#)) :

- dans l'onglet Application Filters dans la section Configuration -> Add-ins pour Microsoft ISA Server ;
- dans l'onglet Application Filters dans la rubrique System pour Microsoft Forefront TMG.



Microsoft Internet Security and Acceleration Server 2006

File Action View Help

Microsoft Internet Security & Acceleration Server 2006 Configuration Storage Server: ISA-SERVER-103049 Enterprise Edition

[Click here to learn about the Customer Experience Improvement Program.](#)

Application Filters Web Filters

Name	Description	Vendor	Version
DNS Filter	Filters DNS traffic	Microsoft (R) C...	4.0
Dr.Web FTP Filter	Enables virus checking over FTP protocol	Doctor Web, Ltd.	11.0
Dr.Web POP3 Filter	Enables virus checking over POP3 protocol	Doctor Web, Ltd.	11.0
Dr.Web SMTP Filter	Enables virus checking over SMTP protocol	Doctor Web, Ltd.	11.0
FTP Access Filter	Enables FTP protocols (client and server)	Microsoft (R) C...	4.0
H.323 Filter	Enables H.323 protocol	Microsoft (R) C...	4.0
MMS Filter	Enables Microsoft Media Streaming protocol	Microsoft (R) C...	4.0
PNM Filter	Enables RealNetworks Streaming Media pr...	Microsoft (R) C...	4.0
POP Intrusion Detection Filter	Checks for POP buffer overflow attacks	Microsoft (R) C...	4.0
PPTP Filter	Enables PPTP tunneling through ISA Server	Microsoft (R) C...	4.0
RPC Filter	Enables publishing of RPC servers	Microsoft (R) C...	4.0
RTSP Filter	Enables Real Time Streaming Protocol	Microsoft (R) C...	4.0
SMTP Filter	Filters SMTP traffic	Microsoft (R) C...	4.0
SOCKS V4 Filter	Enables SOCKS 4 communication	Microsoft (R) C...	4.0
Web Proxy Filter	Enables HTTP proxy and cache	Microsoft (R) C...	4.0

Figure 1a. Filtres d'applications Dr.Web dans la console Microsoft ISA Server

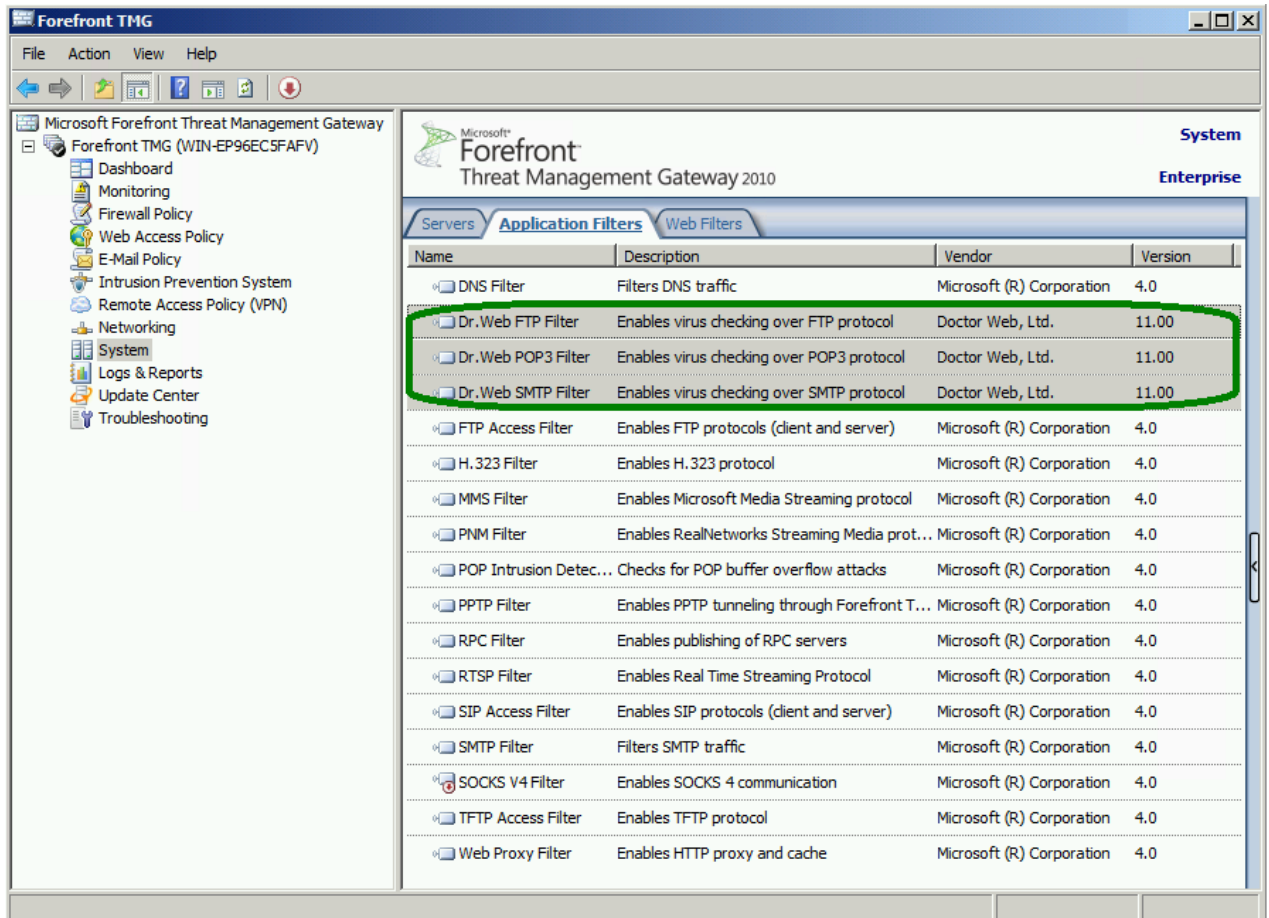


Figure 1b. Filtres d'applications Dr.Web dans la console Microsoft Forefront TMG

Juste après l'installation de l'application et l'enregistrement réussi Dr.Web FTP Filter se connecte aux événements du protocole FTP et s'affiche dans l'onglet des propriétés du protocole FTP dans la console Microsoft ISA Server ou Microsoft Forefront TMG (voir [Figure 2](#)).

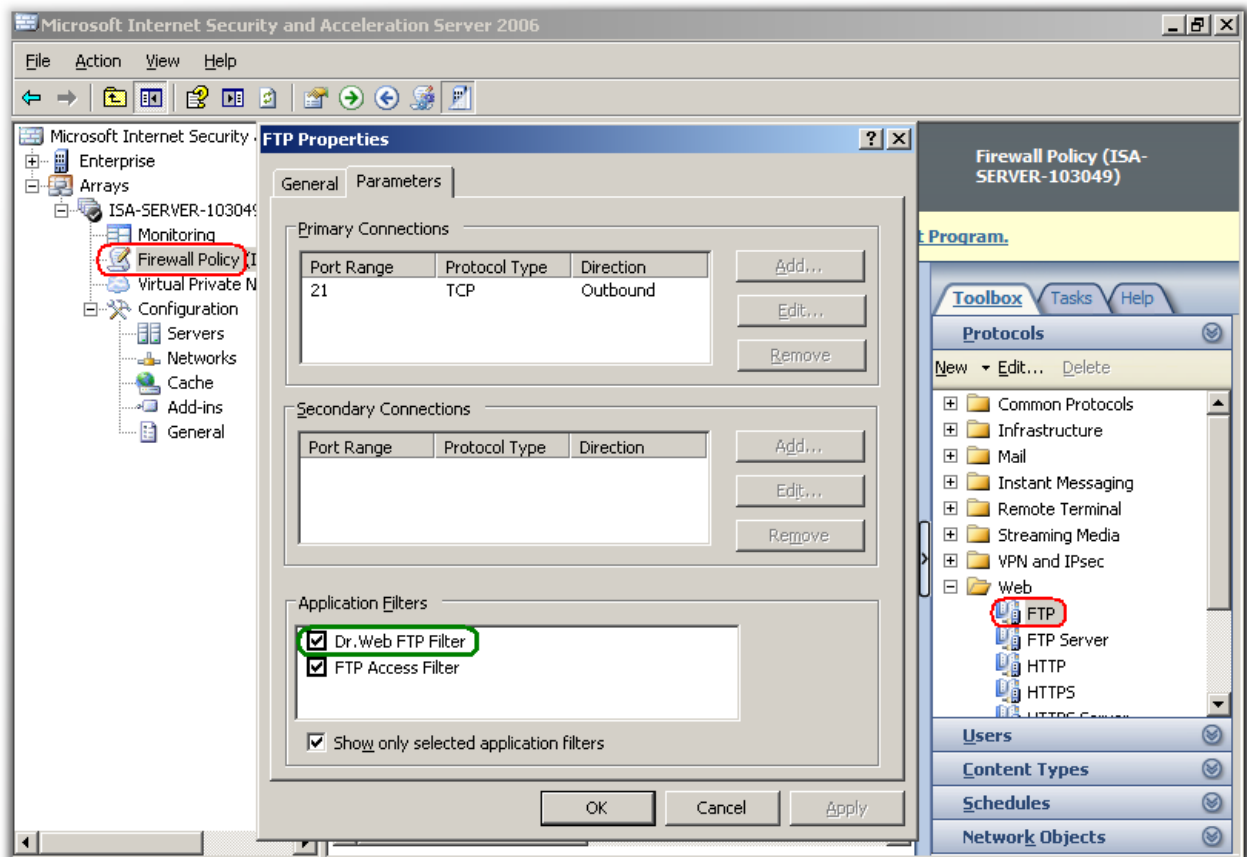


Figure 2. Filtre Dr.Web FTP Filter dans l'onglet des propriétés du protocole FTP



Microsoft ISA Server et Microsoft Forefront TMG sont fournis avec le filtre intégré d'accès à FTP – FTP Access Filter. Si le filtre d'accès à FTP est désactivé, le pare-feu Microsoft ISA Server ou Microsoft Forefront TMG ne suit pas l'interaction des application du niveau du protocole FTP. Ainsi, pour que Dr.Web FTP Filter fonctionne, il faut que FTP Access Filter soit mis en marche et activé dans l'onglet des propriétés du protocole FTP (voir [Figure 2](#)).

5.1.1.1. Dr.Web FTP Filter

Lors de l'installation, Dr.Web FTP Filter est enregistré en tant que gestionnaire d'événements en cas d'utilisation du protocole FTP. Une fois la connexion du client au serveur FTP établie, la préparation à l'analyse antivirus commence. A ce moment Microsoft ISA Server ou Microsoft Forefront TMG crée un objet de filtre qui commence à traiter les données transmises du client au serveur et à l'envers :

1. En analysant les requêtes du client Dr.Web FTP Filter détermine le moment de la réception de la requête de téléchargement de fichier par le client.
2. Après avoir reçu la requête de téléchargement de fichier, Dr.Web FTP Filter vérifie la conformité de l'adresse IP du serveur aux listes noires et blanches des adresses IP.



3. Dr.Web FTP Filter sélectionne le nom du fichier requis dans la requête de téléchargement du fichier et demande les informations sur la taille du fichier. Si la taille du fichier requis ne dépasse pas une certaine limite (par défaut 0.5 Mo), c'est le tampon dans la mémoire qui est utilisé pour l'enregistrement des données reçues. Si la limite est dépassée, c'est un fichier qui est utilisé pour l'enregistrement des données.
4. La transmission d'un fichier au client s'effectue jusqu'au niveau déterminé (par défaut 80%). Ensuite, la transmission est suspendue, Dr.Web FTP Filter accumule les données restantes et analyse le fichier. Si le fichier ne contient pas de menaces, les données restantes sont transmises au client, si le fichier est infecté, la transmission s'arrête. Le client n'obtiendra pas le fichier entier mais une signature d'un virus peut s'infiltrer dans l'ordinateur du client.



Si la connexion entre le client FTP et le serveur a été interrompue à cause d'une menace détectée lors du téléchargement du fichier, il faut se reconnecter au serveur pour continuer à travailler via le protocole FTP.

5.1.1.2. Dr.Web SMTP Filter et Dr.Web POP3 Filter

Par les protocoles POP3 et SMTP Dr.Web n'analyse que le flux de données non chiffré.

L'analyse comprend deux étapes :

1. A la première étape, le message reçu est transmis au module de l'Antispam Vade Retro qui 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 action spécifiée par l'administrateur pour cette catégorie de spam s'applique au message. L'administrateur spécifie l'action dans la section Antispam de la console d'administration [Dr.Web Administrator Web Console](#).
2. A la deuxième étape, les messages ayant passé avec succès l'analyse pour le spam (ou sautés selon les paramètres de l'application) subissent ensuite l'analyse pour la présence éventuelle d'un code malveillant. A l'issue du scan, les objets (le corps de message ou les pièces jointes) reçoivent les statuts déterminés (Infectés ou Suspects). En fonction des résultats du scan, les objets subissent les actions ultérieures (conformément aux paramètres spécifiés par l'administrateur dans la rubrique Scan de la console d'administration [Dr.Web Administrator Web Console](#)).
Si l'utilisation de l'analyseur heuristique est activée dans les paramètres, l'application peut déterminer les objets contenant le code malveillant modifié ou inconnu. Ces objets obtiennent le statut Suspects.
Un fichier texte est joint aux messages contenant des objets infectés. Ce fichier contient le rapport sur les menaces détectée et sur les actions appliquées aux objets en question..

5.1.2. Filtre web

Le filtre web Dr.Web HTTP Web Filter fait partie de Dr.Web. Il représente l'extension (run-time extension) du filtre Web Proxy Filter intégré dans Microsoft ISA Server ou Microsoft Forefront



TMG. Ainsi, le filtre web Dr.Web réagit aux événements du filtre intégré Web Proxy Filter.

Dr.Web HTTP Web Filter se trouve dans la bibliothèque HTTPWebFilter.dll des répertoires :

%PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG\ (pour Microsoft ISA Server) ;

%PROGRAMFILES%\Microsoft Forefront Threat Management Gateway\DrWeb for ISA and TMG\ (pour Microsoft Forefront TMG).

Dr.Web HTTP Web Filter est affiché dans l'arborescence de la console de gestion Microsoft ISA Server Microsoft Forefront TMG (voir [Figure 3a](#), [Figure 3b](#)) :

- dans l'onglet Web Filters dans la section Configuration -> Add-ins de la console Microsoft ISA Server ;
- dans l'onglet Web Filters dans la rubrique System de la console Microsoft Forefront TMG.

Dans ce cas, le filtre n'est pas affiché dans l'onglet des propriétés du protocole HTTP.

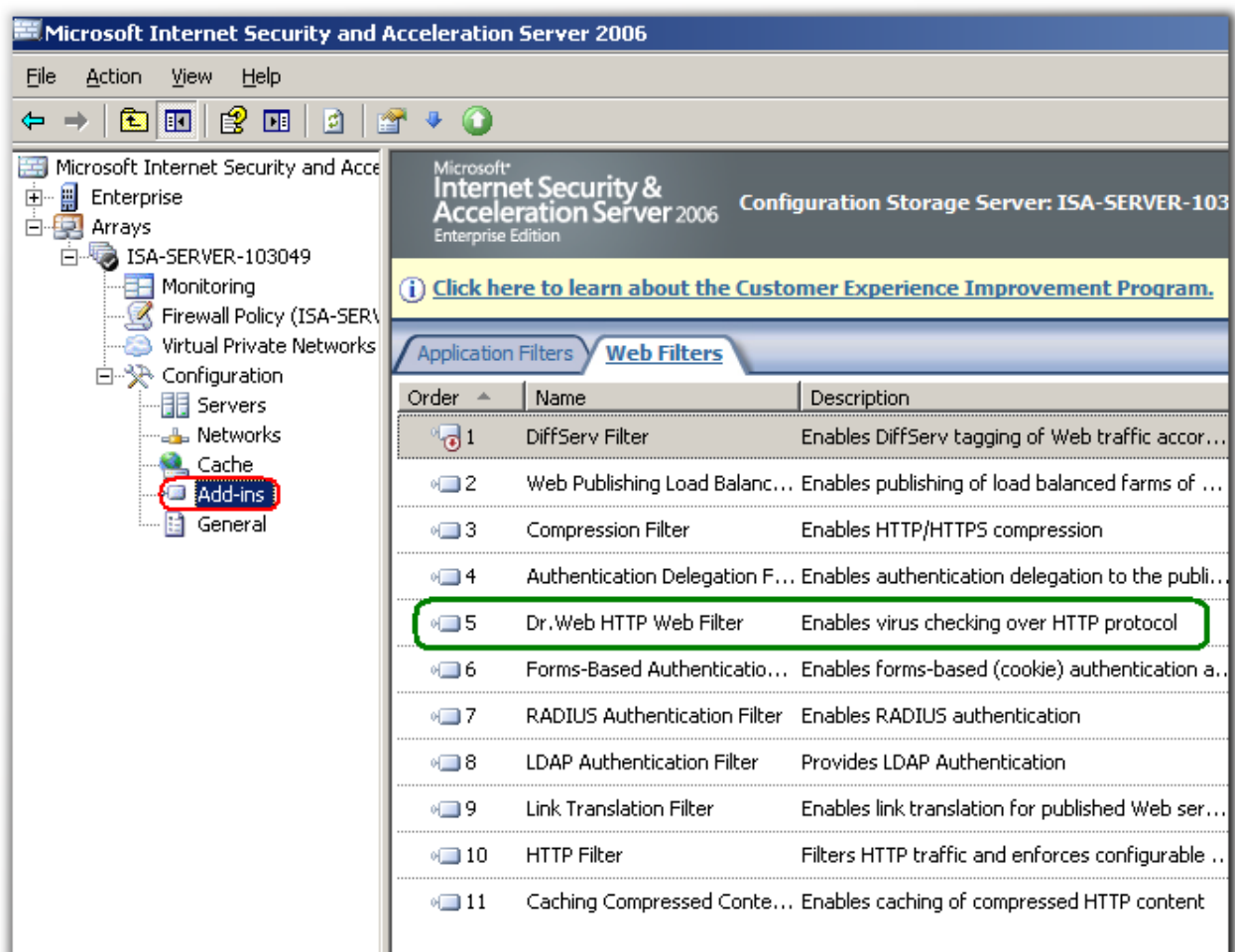


Figure 3 . Filtre Dr.Web HTTP Web Filter dans la console Microsoft ISA Server

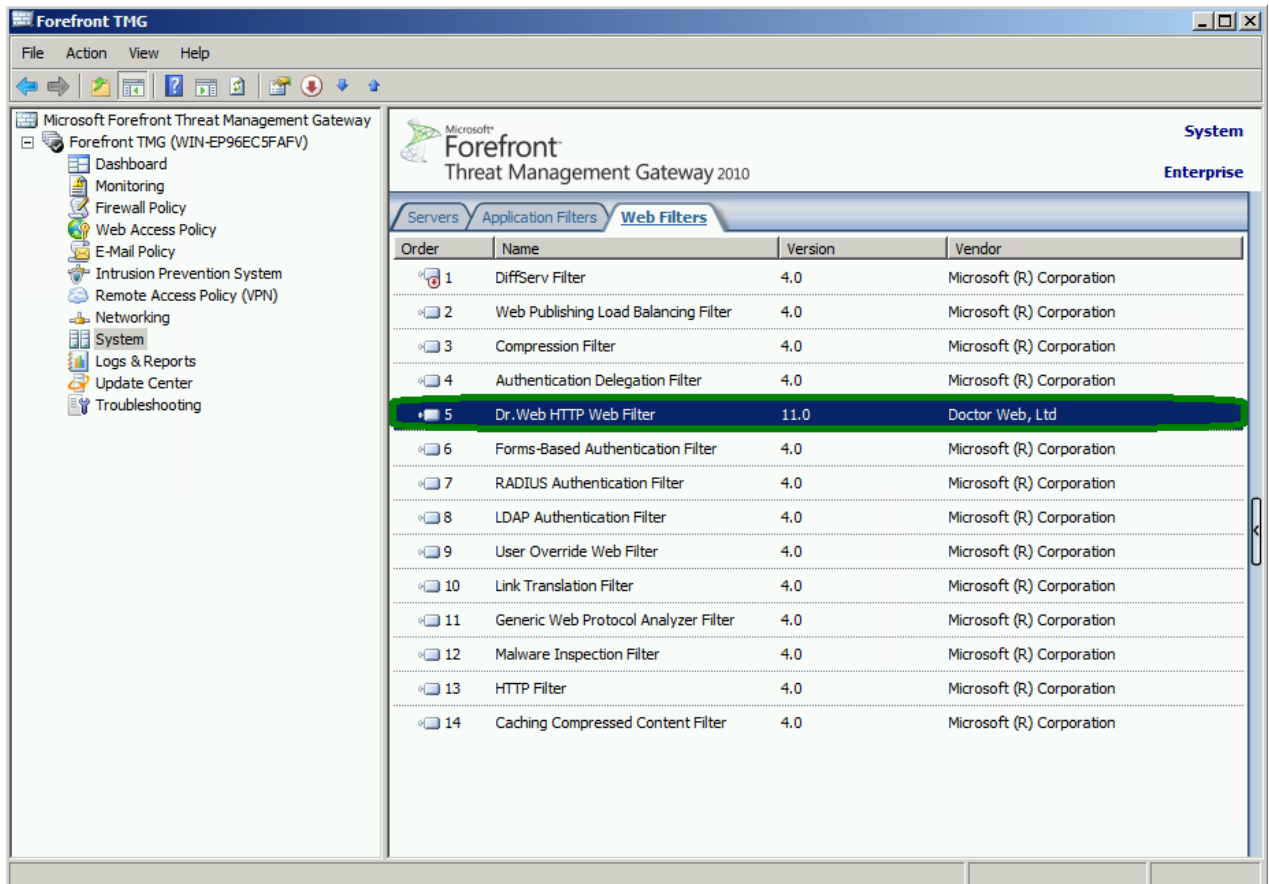


Figure 3b. Filtre Dr.Web HTTP Web Filter dans la console Microsoft Forefront TMG

5.1.2.1. Dr.Web HTTP Web Filter

La préparation à l'analyse antivirus commence au moment de l'envoi des données du serveur au client ou au moment de l'extraction des données demandées du cache Microsoft ISA Server ou Microsoft Forefront TMG.

Puisque l'objet de l'analyse antivirus est la ressource spécifiée dans la requête du client, le filtre Dr.Web HTTP Web Filter analyse les paquets du protocole en rassemblant la ressource sous forme d'un tampon ou d'un fichier temporaire (si la taille de ressource est assez grande) pour le scan antivirus postérieur.

Si l'URL n'est pas bloquée par l'[Office Control](#), la ressource peut être dans un des quatre statuts (deux statuts indéterminés et deux statuts déterminés) :

- indéterminé (non vérifié) ;
- le statut de la ressource est inconnu ;
- infecté ;
- sain (ne contient pas de menace).



Le statut de la ressource reste invariable pendant 30 minutes depuis la fin du scan. Après ce délai, la ressource bascule dans l'état non vérifié. Au bout de 60 périodes de vérification, les entrées sur la ressource seront supprimées du système.

5.2. 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 de l'application, contrôle le fonctionnement des modules différents. Le service supporte la base de données des paramètres des composants de l'application.
- Dr.Web CMS Web Console assure le fonctionnement des consoles web.
- Dr.Web for MSP Component Host et Dr.Web for MSP Scanning Service assurent l'interaction des composants du plugin.
- 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 lancement et l'arrêt des services de Dr.Web.



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 sont arrêtés, il suffit de lancer le service Dr.Web SSM après quelque temps l'application sera automatiquement mise en état opérationnel.

5.3. Quarantaine

Il est possible de spécifier l'action Déplacer en quarantaine pour les objets. Les objets de ce type sont placés dans une base auxiliaire qui réalise les fonctions de quarantaine et qui bloque l'exécution du code de ces objets par toute application système. Pour consulter les informations sur les objets mis en quarantaine, allez dans la section [Gestion de la quarantaine](#).

5.4. Surveillance des événements viraux

Pour recevoir les informations sur les événements suivis par Dr.Web, vous pouvez configurer le système de notification qui comprend les fonctionnalités suivantes :

- [Journal du système d'exploitation](#). Les événements du plugin sont écrits dans le journal des événements système (Event Log).
- [Incidents](#) représente la liste des objets traités par Dr.Web dans lesquels des virus et des spams ont été détectés. Vous pouvez également consulter les messages filtrés.
- [Statistique](#). Les statistiques contiennent des informations sur le nombre d'objets analysés pendant le délai spécifié.



6. Installation et suppression



Avant l'installation ou la suppression de Dr.Web, assurez-vous que le compte intégré de l'administrateur système est activé sur l'ordinateur avec Microsoft ISA Server ou Microsoft Forefront TMG installé !

Sinon, il peut y avoir des cas où le composant d'installation système n'a pas assez de privilèges pour créer et supprimer les composants de l'application. Si, pour cette raison, une erreur s'est produite lors de la suppression et cette erreur rend le pare-feu inopérant, consultez l'annexe [Suppression manuelle de Dr.Web](#).

Dr.Web est fourni sous forme d'un fichier d'installation (drweb-[version]-av-isa-windows-x86.exe ou drweb-[version]-av-tmg-windows-x64.exe, en fonction du pare-feu utilisé), où [version] indique la version de Dr.Web, ou sous forme d'un dossier placé dans une archive zip et contenant le fichier d'installation.

Extrayez le fichier d'installation sur le disque local du serveur.



Si vous utilisez le composant Windows Terminal Services, pour installer Dr.Web, il est recommandé d'utiliser l'utilitaire standard Windows Ajouter ou supprimer des programmes (sous Windows Server 2003) ou Programmes et fonctionnalités (sous Windows Server 2008).

L'installation de plusieurs produits antivirus sur le même ordinateur peut entraîner des erreurs système ou une perte de données importantes. Si une autre version de Dr.Web différente de la version 11 ou un antivirus d'un autre producteur est déjà installé sur votre ordinateur, il est nécessaire de le supprimer.

6.1. Pré-requis système

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



Caractéristique	Pré-requis	
	en cas d'utilisation de Microsoft ISA Server	en cas d'utilisation de Microsoft Forefront TMG
RAM	1 Go et plus	2 Go et plus
Espace libre sur le disque	700 Mo pour l'installation L'espace supplémentaire du disque est requis pour le stockage temporaire de données à l'étape de l'analyse antivirus. Il est déterminé en fonction de l'intensité des requêtes utilisateur et des tailles des fichiers téléchargés par les utilisateurs.	
OS	Un des systèmes suivants ; <ul style="list-style-type: none">• Microsoft® Windows Server® 2003 x86 avec :<ul style="list-style-type: none">J MSXML 4.0 Service Pack 3 (Microsoft XML Core Services)J Service Pack 1 (SP1) et supérieur• Microsoft® Windows Server® 2003 R2 x86 avec :<ul style="list-style-type: none">J MSXML 4.0 Service Pack 3 (Microsoft XML Core Services)	Un des systèmes suivants ; <ul style="list-style-type: none">• Microsoft® Windows Server® 2008 SP2 x64• Microsoft® Windows Server® 2008 R2 x64
Pare-feu	Microsoft® ISA Server 2004 Microsoft® ISA Server 2006	Microsoft® Forefront® TMG 2010 (Standard Edition Enterprise Edition) avec SP1 ou SP2 installé
Autres logiciels	Microsoft .NET Framework 3.5 SP1	

6.2. Compatibilité

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

1. Dr.Web pour Microsoft ISA Server et Forefront TMG de la version 11 n'est compatible qu'avec Dr.Web pour les serveurs Windows de la version 11.
2. Dr.Web pour Microsoft ISA Server et Forefront TMG de la version 11 n'est pas compatible avec l'Agent Dr.Web ES et Dr.Web AV-Desk.
3. Dr.Web pour Microsoft ISA Server et Forefront TMG 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.



6.3. Installation de Dr.Web

Avant d'installer, il est fortement recommandé :

- 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.

Pour installer Dr.Web :

1. Arrêtez le service du pare-feu Microsoft ISA Server ou Microsoft Forefront TMG.
2. Assurez-vous que le processus d'installation sera lancé sous le compte d'administrateur système.
3. Lancez le fichier d'installation du programme. La fenêtre qui s'affiche contient la proposition de sélectionner la langue d'installation. Vous pouvez sélectionner le russe ou l'anglais. Cliquez sur OK.
4. Dans la fenêtre contenant le texte du Contrat de licence, vous devez lire et accepter les termes du contrat en cochant la case J'accepte les termes du contrat de licence. Cliquez sur Suivant.
5. Si le service de pare-feu est toujours lancé, vous serez invité à l'arrêter.
6. Sélectionnez une variante de la licence.

Par défaut, l'Assistant d'enregistrement cherche le fichier de licence avec l'extension .key dans le répertoire de lancement et le répertoire

%PROGRAMFILES%\DrWeb CMS for MSP\. Si l'Assistant d'installation trouve la clé, il affiche les informations sur cette clé dans la fenêtre de sélection du mode de licencing.

Vous pouvez utiliser la clé locale en indiquant le chemin manuellement. Si vous sélectionnez l'élément Activer le produit plus tard, l'analyse du trafic n'aura pas lieu.

Cliquez sur Suivant.

7. A l'étape Le système est prêt à l'installation du programme, cliquez sur Installer. L'installation de Dr.Web sur votre ordinateur commence.
8. Les actions suivantes de l'Assistant d'installation ne nécessitent pas l'intervention de l'utilisateur. A la fin de l'installation, vous serez invité à redémarrer l'ordinateur.



Lors de l'installation du programme, il est nécessaire de redémarrer Microsoft ISA Server ou Microsoft Forefront TMG. L'arrêt est lié à la nécessité d'éviter la violation de l'intégrité de l'installation sur le serveur fonctionnant sous charge.



Le redémarrage du système d'exploitation peut être requis après la mise à jour de Dr.Web.

6.4. Suppression de Dr.Web

Pour supprimer Dr.Web :

1. Arrêtez le service du pare-feu Microsoft ISA Server ou Microsoft Forefront TMG.
2. Assurez-vous que le processus de suppression sera lancé sous le compte d'administrateur système.
3. Lancez l'utilitaire standard Windows Ajouter ou supprimer des programmes (sous Windows Server 2003) ou Programmes et fonctionnalités (sous Windows Server 2008).
4. Sélectionnez Dr.Web dans la liste des programmes installés et cliquez sur Supprimer. La fenêtre de l'Assistant d'installation va s'afficher.
5. Si le service de pare-feu n'est pas lancé, vous serez invité à l'arrêter. Arrêtez le service et cliquez sur Suivant.
6. Si nécessaire, sélectionnez l'élément Enregistrer les paramètres. Cliquez sur Supprimer.
7. A la fin de la suppression, vous serez invité à redémarrer l'ordinateur.



Lors de la suppression du programme, il est nécessaire de redémarrer Microsoft ISA Server/ Microsoft Forefront TMG. L'arrêt est lié à la nécessité d'éviter la violation de l'intégrité de l'installation sur le serveur fonctionnant sous charge. A la fin de la suppression, lancez le service Microsoft Firewall Service/Microsoft Forefront TMG Firewall.



7. Console d'administration Dr.Web Administrator Web Console

Le fonctionnement de Dr.Web peut être configuré avec la Console d'administration Dr.Web Administrator Web Console (voir [Figure 4](#)).

Lancer la console d'administration Dr.Web Administrator Web Console



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

- Internet Explorer 11 ou supérieur ;
- Chrome 46 ou supérieur ;
- Microsoft Edge 20 ou supérieur.

Pour le fonctionnement correct de la console d'administration 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 Internet Explorer Enhanced Security Configuration 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 d'administration Dr.Web Administrator Web Console, ouvrez la page suivante dans le navigateur :

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

où *<ISA Server address>* est l'adresse du serveur Microsoft ISA/Microsoft Forefront TMG.



Pour accéder à la page de Dr.Web Administrator Web Console, vous devez saisir les données du compte administrateur.

Au 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. Ensuite, il est fortement recommandé de modifier le mot de passe pour ce compte (pour plus d'informations, voir [Modifier le mot de passe de l'administrateur](#)).

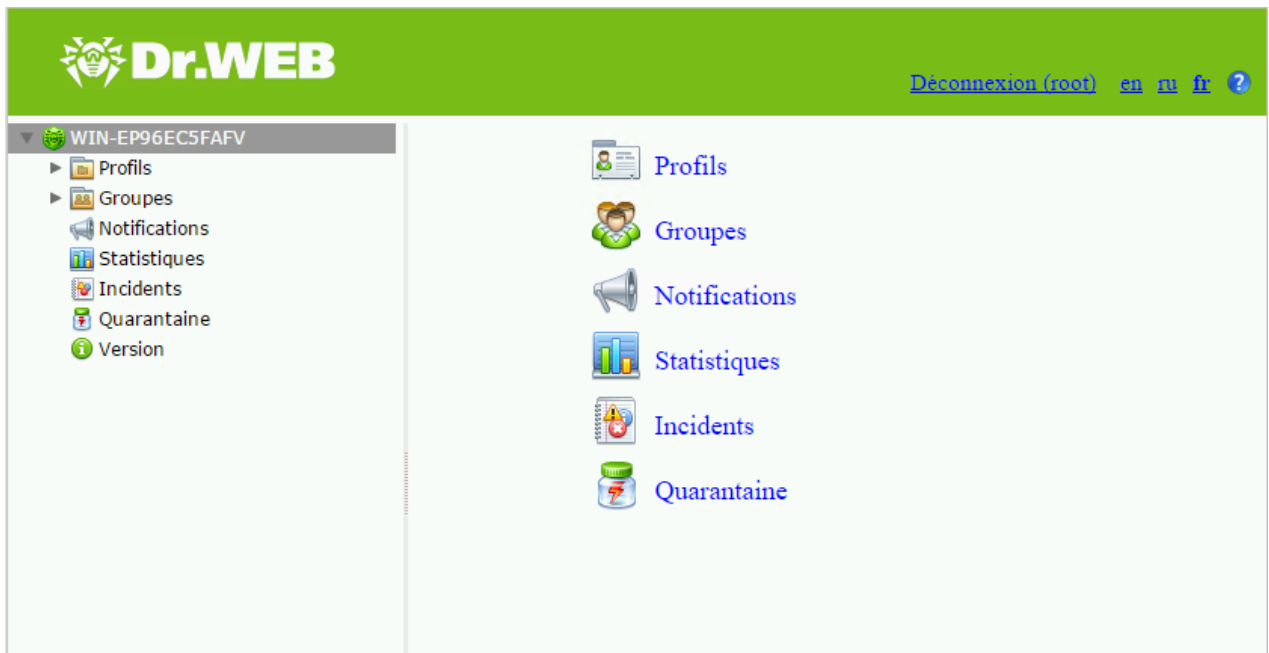


Figure 4. Console d'administration Dr.Web Administrator Web Console

Interface

Dr.Web Administrator Web Console comprend deux parties :

1. Arborescence de la console qui fournit la navigation dans 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 d'administration 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.

7.1. Groupes et profils

Pour faciliter l'organisation de la protection antivirus des utilisateurs du réseau interne protégé par le pare-feu Microsoft ISA Server et Microsoft Forefront TMG, 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 du trafic Internet et déterminant le mode de protection du réseau local. La configuration du profil se trouve dans la section Profils de l'arborescence de la console d'administration. La section Profils comprend les sous-rubriques suivantes :

- [Scan](#) vous permet de configurer le composant principal de détection de virus ;



- [Antispam](#) vous permet de configurer le composant 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](#)) ;
- [Office Control](#) permet de configurer les limitations d'accès d'utilisateurs aux ressources Internet ;
- [Filtrage](#) permet de configurer le filtrage de trafic Internet.

Pour plus d'informations sur les profils, consultez la rubrique [Création et configuration des profils](#).

Tout profil peut être attribué à un groupe de clients. Ces groupes sont créés dans la section Groupes de l'arborescence de la console (voir [Gestion des groupes clients](#)).

7.2. Création et configuration des profils

Lors de l'installation, Dr.Web crée automatiquement le profil standard Default que vous ne pouvez pas supprimer, ni renommer. Ce profil sera appliqué à tout le trafic avant que vous créiez un autre profil et l'attribuiez à un certain groupe de clients.

Pour gérer les profils existants et créer de nouveaux profils, passez dans la zone d'information de la rubrique Profils, en choisissant l'élément Profils dans l'arborescence de la Console d'administration Dr.Web Administrator Web Console (voir [Figure 5](#)).



Figure 5. Modifier les paramètres du profil

La liste comprend des informations sur les paramètres et le profil de chaque profil.

Création d'un nouveau profil

Pour créer un nouveau profil :

- cliquez sur le bouton [Créer un profil](#) se trouvant au-dessus de la liste des profils existants ;
- cliquez droit sur l'élément Profils dans l'arborescence de la console et sélectionnez [Créer un profil](#) dans le menu contextuel.

Dans la fenêtre [Créer un profil](#), spécifiez le nom du nouveau profil et cliquez sur OK.



Le nom de profil doit être composé de caractères latins.

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

Renommer le profil

Pour renommer un profil existant, sélectionnez le profil nécessaire dans la liste se trouvant dans la zone d'information de la rubrique Profils, puis cliquez sur Renommer le profil.

Modifier les paramètres du profil



Pour modifier les paramètres du profil, sélectionnez son nom dans l'arborescence de la console d'administration Dr.Web Administrator Web Console et passez à la section : [Scan](#), [Antispam](#) ou [Office Control](#).

Supprimer le profil

Pour supprimer le profil, sélectionnez-le dans la liste se trouvant dans la zone d'information de la rubrique Profils, puis cliquez sur le bouton Supprimer le profil.

7.2.1. 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 du trafic reçu ou envoyé par ce client.

Vous pouvez changer de priorité de profil dans la zone d'information de la rubrique Profils. Pour ce faire, 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. Plus haut est situé le profil, plus haute est sa priorité.



Le profil standard a toujours la priorité inférieure, il est toujours placé sur la ligne la plus basse dans la liste des profils.

7.2.2. 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 analyser et par conséquent, le niveau de protection du serveur. 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 d'administration. La zone d'information pour la configuration de l'analyse sera ouverte (voir [Figure 6](#)).

The screenshot shows the Dr.Web Administrator Web Console interface. The left sidebar contains a tree view with 'Scan' selected under the 'Default' profile. The main content area is titled 'Scan' and contains several sections:

- Activer le moteur heuristique**: (checked)
- Analyser les archives**: (checked)
- Analyser les conteneurs**: (checked)
- Délai d'attente (s)**: 1200
- Considérer les archives protégées par un mot de passe comme endommagées**: (unchecked)
- Programmes malveillants**:
 - Riskwares**: (unchecked)
 - Dialers**: (unchecked)
 - Hacktools**: (unchecked)
 - Adwares**: (unchecked)
 - Canulars**: (unchecked)
- Actions**:
 - Pour les objets infectés**: Déplacer en quarantaine
 - Pour les objets suspects**: Déplacer en quarantaine
- Paramètres des pièces jointes**:
 - Suffixe de nom de fichier**: infected
 - Macro**: Nom d'application
 - Insérer**: [button]
 - Contenu du fichier**: %FEFF%DataType% %FileName% was infected with a virus and has been %ScanAction% by %ApplicationName%. %NewLine%%NewLine%Viruses:%NewLine%%Viruses%

A 'Sauvegarder' button is located at the bottom right of the configuration area.

Figure 6. 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 plus fiable mais entraîne une certaine diminution des performances du serveur. Pour désactiver ces modes, décochez les cases Activer l'analyse heuristique, Analyser les archives et Analyser les conteneurs en haut de la zone d'information de la rubrique Scan.



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

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 1200 s 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 seront appliquées. Si les archives avec un mot de passe sont considérées comme endommagées, une action spécifiée pour les objets infectés y est appliquée (voir [Sélectionner les types d'objets endommagés](#)).

3. Dans l'ensemble des paramètres Programmes malveillants, vous pouvez spécifier les types d'objets malveillants à rechercher dans le trafic Internet. Pour cela, cochez les cases correspondantes.



4. En bas, 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 signifie que le message passera sans traitement mais le fichier joint sera envoyé en quarantaine (voir [Quarantaine](#)) ;
 - § Supprimer signifie que l'objet sera supprimé ;
 - § Ignorer signifie que le message sera envoyé à l'utilisateur (l'action est applicable uniquement aux objets suspects) ;



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

5. Dans l'ensemble des 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 Texte, vous pouvez modifier le contenu du fichier texte joint. Lors de l'édition du texte, vous pouvez utiliser des macros. Sélectionnez la macro nécessaire dans la liste Macro, puis cliquez sur Insérer.
6. Après avoir apporté toutes les modifications aux paramètres d'analyse, cliquez sur Sauvegarder.

7.2.3. Antispam

L'Antispam analyse le contenu des messages. Sur la base des valeurs obtenues, le composant détermine s'il s'agit de spam ou pas.

Vous pouvez configurer le fonctionnement de l'Antispam dans la rubrique des 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 de spam est activé par défaut (la case Activer l'Antispam en haut de la zone d'information de la section Antispam est 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](#)).

Dans la section Version de la console d'administration Dr.Web Administrator Web Console, vous pouvez vérifier si le composant Antispam est supporté par votre licence. Si le module est supporté, les informations sur le module seront affichées dans la section Informations sur le produit.

Toute édition du fichier clé le rend invalide ! N'ouvrez pas le fichier de licence dans un éditeur de texte.



Pour configurer l'Antispam :

1. Sélectionnez l'élément Antispam pour le profil à configurer dans l'arborescence de la console d'administration. La zone d'information de la rubrique Antispam (voir [Figure 7](#)) sera ouverte.

Figure 7. 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 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 :
 - Ignorer signifie que le message sera délivré au destinataire.



- Ajouter le préfixe au sujet signifie que le préfixe spécifié dans le champ Préfixe sera ajouté au sujet.
 - Mettre le cachet Move to junk signifie que le message sera délivré au destinataire mais marqué par le cachet Move to junk.
 - Rediriger signifie que le message sera délivré à un autre destinataire. Si vous sélectionnez cette option, le champ Adresse e-mail se trouvant dans l'angle supérieur droit sera activé. Dans ce champ, vous pouvez entrer l'adresse e-mail à laquelle le message doit être redirigé. Vous pouvez indiquer une seule adresse.
 - Bloquer signifie que le message sera bloqué et ne sera pas délivré au destinataire.
5. 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 pour la présence du spam. 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 .
 - pour supprimer une adresse e-mail de la liste, sélectionnez-la dans la liste nécessaire et cliquez sur Supprimer ;
 - vous pouvez utiliser les boutons Importation et Exportation pour enregistrer les listes dans un fichier spécialisé ayant l'extension .lst et pour les télécharger depuis un fichier. Vous pouvez créer et éditer les listes manuellement avec un éditeur de texte, par exemple le Bloc-notes. Le fichier texte doit être enregistré avec l'extension .lst au format Unicode. Les adresses e-mail doivent avoir le préfixe « + » (pour ajouter l'adresse ou « - » (pour ajouter l'adresse à la liste noire). 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). Par exemple:
`+trusted@example.com;+trusted_email@example.com;-suspicious@example.com;-spam@example.com;+*example.com.`
6. Cliquez sur Enregistrer pour accepter toutes les modifications des paramètres de l'Antispam.

7.2.4. Office Control

Office Control permet de restreindre l'accès des utilisateurs aux ressources Internet et aux sites web non désirables (sites consacrés à la violence, aux jeux de hasard, etc.) ou d'autoriser aux utilisateurs l'accès aux sites qui sont spécifiés par les paramètres d'Office Control.



Pour configurer Office Control :

1. Sélectionnez l'élément Office Control pour le profil que vous configurez dans l'arborescence de la console d'administration. La zone d'information pour la configuration d'Office Control sera ouverte (voir [Figure 8](#)).

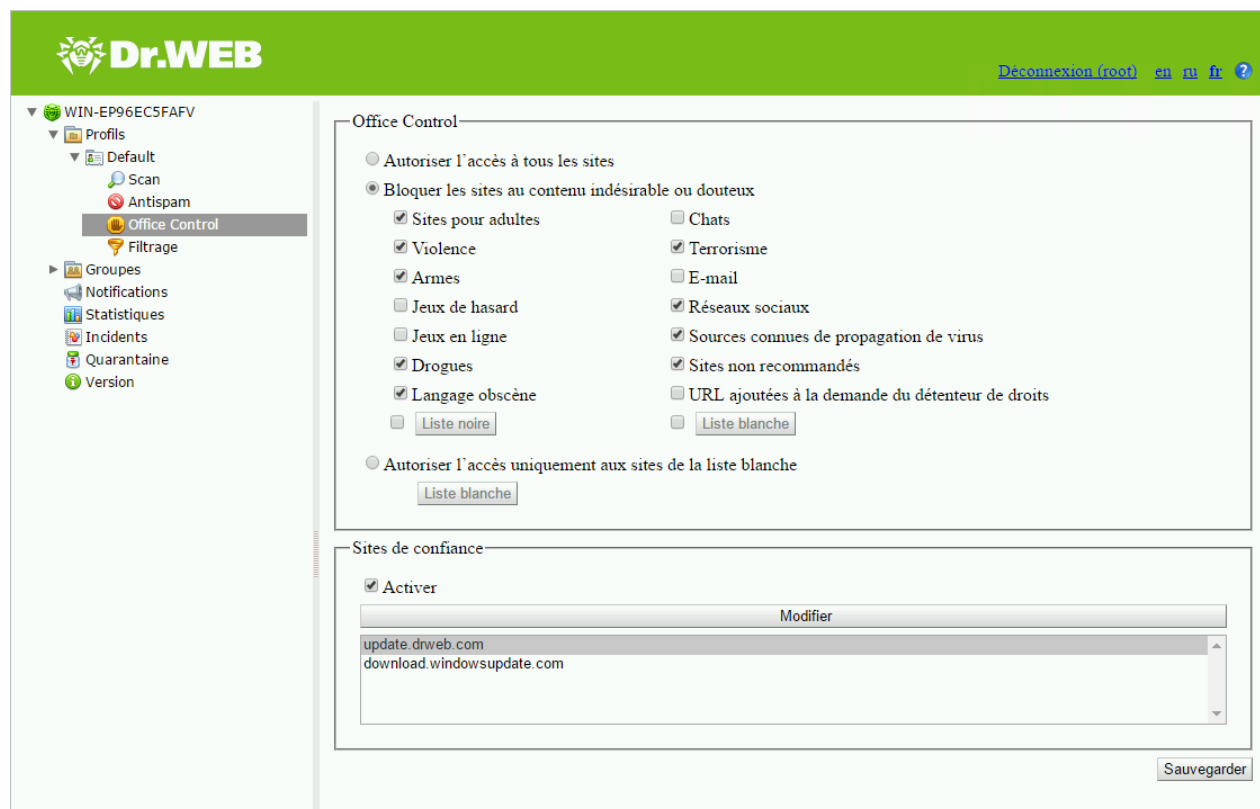


Figure 8. Rubrique de la configuration d'Office Control

2. Vous pouvez sélectionner un des modes de fonctionnement suivants :
 - Autoriser tous les sites - dans ce mode il n'y a pas de restrictions d'accès aux ressources web ;
 - Bloquer des sites au contenu indésirable ou douteux – dans ce mode, vous pouvez indiquer les catégories des ressources l'accès auxquelles vous voulez limiter. Le filtre vous permet également d'indiquer les sites l'accès auxquels vous voulez interdire ou autoriser quelles que soient les autres restrictions. Pour configurer les ressources à bloquer, cliquez sur Liste noire, indiquez la ressource et cliquez sur Ajouter.

Pour créer une liste des ressources autorisées, cliquez sur Liste blanche, indiquez la ressource et cliquez sur Ajouter.



Les listes des adresses des sites web concernant toutes les catégories thématiques sont mises à jour d'une manière régulière par le module de mise à jour automatique au moment de la mise à jour des bases virales.



- Autoriser seulement les sites de la liste blanche – dans ce mode, l'accès sera interdit à toutes les ressources web sauf les ressources mentionnées dans la liste blanche. Pour créer une liste des ressources autorisées, cliquez sur Liste blanche, indiquez la ressource et cliquez sur Ajouter.
3. Sites fiables – les sites de la liste des sites fiables ont la plus haute priorité et ils sont exclus de l'analyse ultérieure.
Cochez la case Activer dans la rubrique Sites fiables. Pour modifier la liste des ressources fiables, cliquez sur Modifier, indiquez la ressource et cliquez sur Ajouter.
 4. Cliquez sur Enregistrer pour accepter toutes les modifications des paramètres de l'Office Control.

Formation de liste blanche et noire

1. Entrez le nom de domaine (une partie du nom de domaine) dans le champ de saisie :
 - si vous voulez ajouter à la liste un site particulier, entrez son adresse complète (par exemple, www.exemple.com). L'accès à toutes les ressources de ce site sera autorisé/interdit.
 - si vous voulez autoriser/interdire l'accès aux sites dont l'adresse contient un texte particulier, entrez ce texte dans ce champ. Par exemple : exemple. L'accès aux adresses exemple.com, exemple.test.com, test.com/exemple, test.exemple222.fr, etc. sera bloqué/autorisé. Si la ligne entrée comporte le signe « . », cette ligne sera considérée comme un nom de domaine. Alors toutes les ressources dans ce domaine seront filtrées.

Si cette ligne comporte en même temps le caractère « / » (par exemple, exemple.com/test), alors, la partie avant le caractère est considéré comme un nom de domaine alors que la partie de la ligne après le caractère est considéré comme une partie de l'adresse que vous souhaitez autoriser/bloquer dans ce domaine (ainsi les adresses comme exemple.com/test11, template.exemple.com/test22, etc. seront filtrées).

2. Cliquez sur Ajouter se trouvant à gauche. L'adresse (la partie de l'adresse) sera ajoutée à la liste ci-dessus.
Au moment de l'ajout à la liste, la ligne entrée peut être transformée par le module au format universel. Par exemple : http://www.exemple.com sera transformée en www.exemple.com.
3. Pour supprimer une ressource de la liste, sélectionnez-la dans cette liste et cliquez sur Supprimer.

7.2.5. Filtrage

Le filtrage des messages peut être paramétré dans la rubrique du profil Filtrage (voir [Figure 9](#)).

Pour commencer à créer des règles, cochez la case Activer le filtrage dans la partie supérieure de la section.

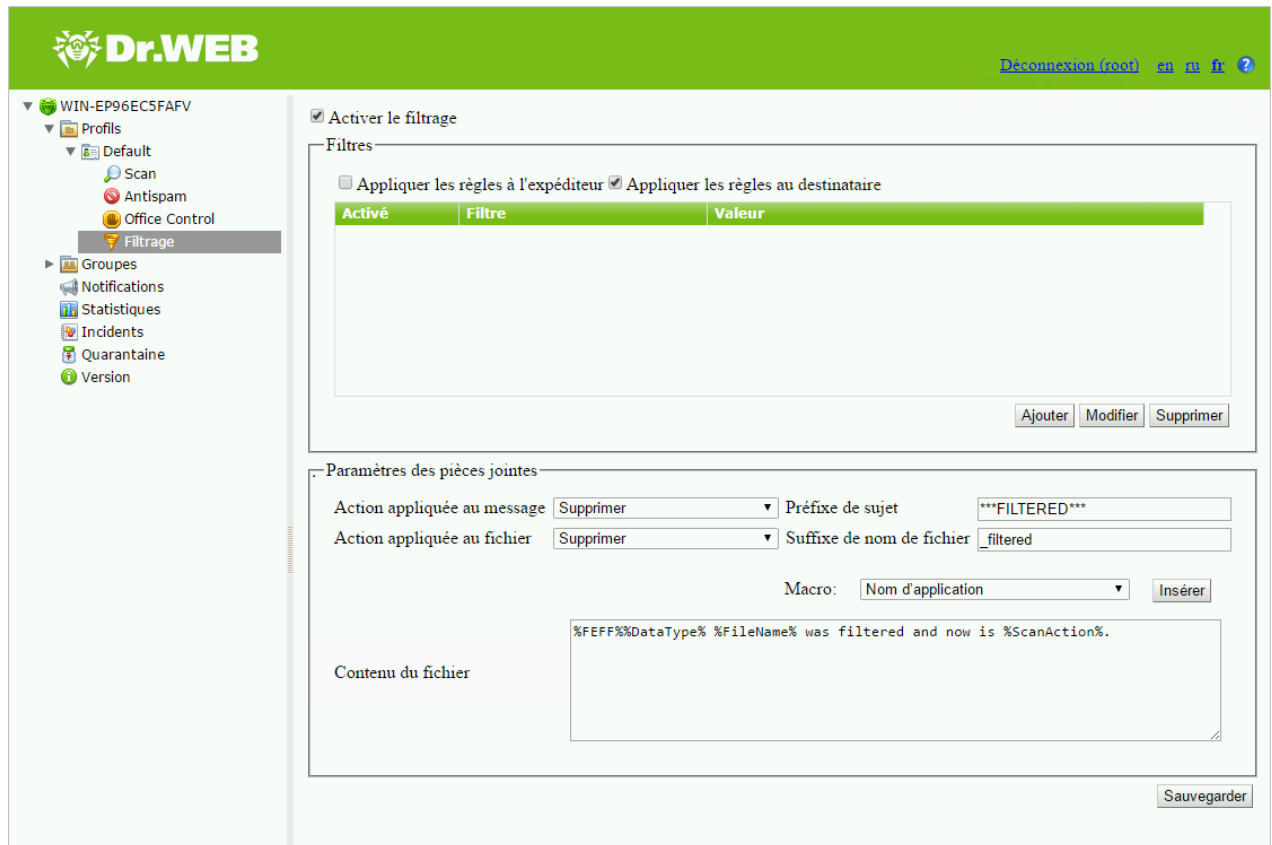


Figure 9. Rubrique de la configuration de filtrage

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.

Création d'une règle de filtrage

1. Cliquez sur Ajouter sous la liste des règles. Dans la fenêtre Règle de filtrage (voir [Figure 10](#)) vous pouvez spécifier le nom de la règle et configurer ses conditions.
2. Vous pouvez ajouter une ou plusieurs conditions et spécifier si les messages doivent les respecter toutes en même temps 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 :
3. Cliquez sur OK pour enregistrer la règle. Cliquez sur Annuler pour fermer la fenêtre sans enregistrer les modifications apportées.

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

Vous trouverez ci-dessous l'[exemple](#) de création d'une règle de filtrage.



Règle de filtrage

Nom

Exécuter :

Toutes les conditions Toute condition

Figure 10. Exemple d'une règle de filtrage

Pour configurer le filtrage des messages :

1. Activez l'utilisation d'une ou de plusieurs règles de la liste en cochant les cases correspondantes.

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. 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 :

- Supprimer – pour supprimer les pièces jointes.
- Déplacer en quarantaine – pour déplacer les pièces jointes en quarantaine ;
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 les macros de la liste déroulante Macro.

- Après avoir apporté toutes les modifications aux paramètres du filtrage, cliquez sur Enregistrer.

Tableau des conditions pour créer une règle de filtrage

Type de condition	Type de respect	Valeur
Type de données	Est égal	Fichier
	N'est pas égal	Message
Source des données	Est égal	Spécifié manuellement.
	N'est pas égal	Si vous avez sélectionné le type de conformité Contient, Ne contient pas, Correspond, Ne correspond, vous pouvez utiliser les symboles « * » et « ? » pour remplacer toute séquence de symboles ou n'importe quel symbole lorsque vous saisissez la valeur.
	Contient	
	Ne contient pas	
	Correspond	
Ne correspond pas		
Destinataire des données	Est égal	Spécifié manuellement.
	N'est pas égal	Si vous avez sélectionné le type de conformité Contient, Ne contient pas, Correspond, Ne correspond, vous pouvez utiliser les symboles « * » et « ? » pour remplacer toute séquence de symboles ou n'importe quel symbole lorsque vous saisissez la valeur.
	Contient	
	Ne contient pas	
	Correspond	
Ne correspond pas		



Protocole	Est égal N'est pas égal	HTTP FTP POP3 SMTP
Nombre de destinataires	Est égal N'est pas égal Plus que Pas plus que Moins que Pas moins que	Spécifié manuellement.
Nom de fichier	Est égal N'est pas égal Contient Ne contient pas Correspond Ne correspond pas	Spécifié manuellement. Si vous avez sélectionné le type de conformité Contient, Ne contient pas, Correspond, Ne correspond, vous pouvez utiliser les symboles « * » et « ? » pour remplacer toute séquence de symboles ou n'importe quel symbole lorsque vous saisissez la valeur.
Taille de fichier	Est égal N'est pas égal Plus que Pas plus que Moins que Pas moins que	Entré manuellement (en octets).



Sujet de message	Est égal	Spécifié manuellement.
	N'est pas égal	Si vous avez sélectionné le type de conformité Contient, Ne contient pas, Correspond, Ne correspond, vous pouvez utiliser les symboles « * » et « ? » pour remplacer toute séquence de symboles ou n'importe quel symbole lorsque vous saisissez la valeur.
	Contient	
	Ne contient pas	
	Correspond	
Ne correspond pas		
Pièce jointe	Est égal	Faux
	N'est pas égal	Vrai

Exemple d'une règle de filtrage

Pour filtrer les fichiers de taille supérieure à 20 octets, transmis via le protocole FTP, on peut utiliser une règle (voir [Figure 11](#)) qui consiste à accomplir simultanément les conditions suivantes :

Type de condition	Type de respect	Valeur
Type de données	Est égal	Fichier
Protocole	Est égal	FTP
Taille de fichier	Plus que	20000



Règle de filtrage

Nom

Exécuter :

Toutes les conditions Toute condition

```
IS( ( %DataType% == 1 ) )
IS( ( %TransProtocolName% == FTP ) )
IS( ( %FileSize% > 20000 ) )
```

Figure 11. Exemple d'une règle de filtrage

7.3. 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.

7.3.1. Création d'un nouveau groupe

Pour gérer les groupes existants et créer de nouveaux groupes, ouvrez la zone d'information de la rubrique Groupes. Pour ce faire, sélectionnez l'élément Groupes dans l'arborescence de la console d'administration Dr.Web Administrator Web Console (voir [Figure 12](#)).

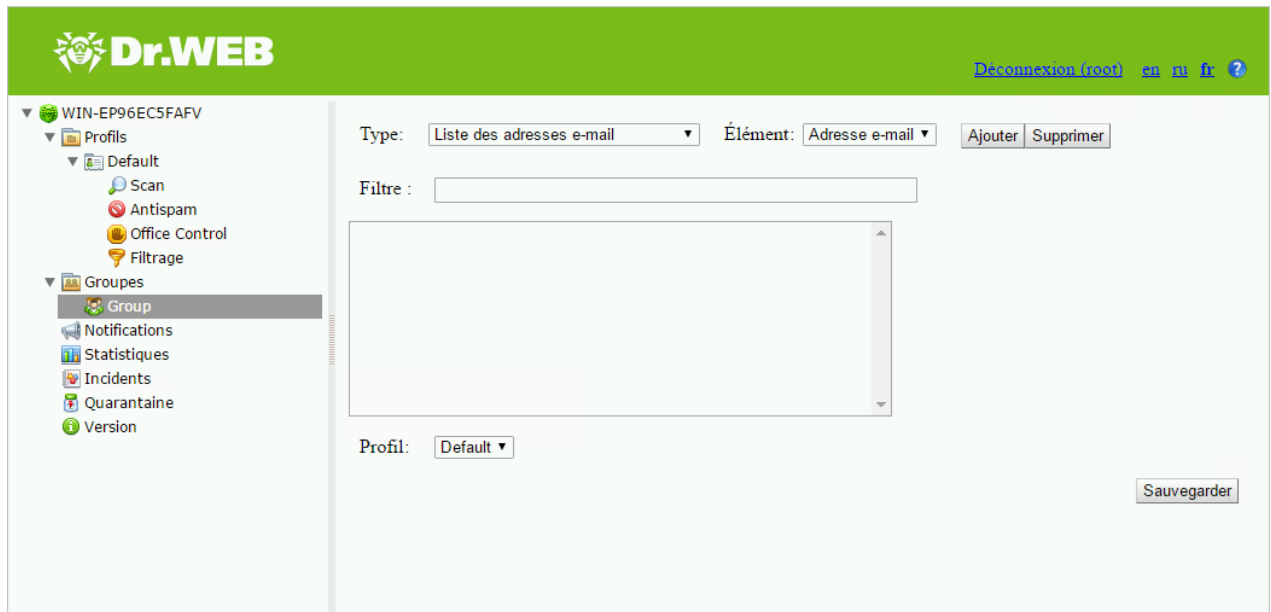


Figure 12. Rubrique Groupes

Création d'un nouveau groupe

Pour créer un nouveau groupe :

- dans la zone d'information de la rubrique Groupes, cliquez sur Créer un groupe sous la liste des groupes existants ;
- cliquez droit sur l'élément Groupes dans l'arborescence de la console et cliquez sur Créer un groupe dans le menu contextuel.

Dans la fenêtre Créer un groupe, spécifiez le nom pour le nouveau groupe et cliquez sur OK. Par défaut le profil Default est assigné au nouveau groupe.



Les noms de groupes doivent être composés de caractères latins.

Modifier le nom de groupe

Pour renommer un groupe, sélectionnez le groupe nécessaire dans la liste de la zone d'information de la rubrique Groupes, puis cliquez sur Renommer le groupe.

Supprimer le groupe

Pour supprimer un groupe, sélectionnez le groupe dans la liste de la zone d'information de la rubrique Groupes et cliquez sur Supprimer le groupe.

Parcourir les paramètres du groupe

Pour ouvrir la zone d'information contenant les paramètres du groupe, sélectionnez son nom dans l'arborescence de la console d'administration. Vous pouvez modifier le type de groupe et son profil (voir [Configuration des groupes](#)).

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

7.3.2. Paramètres et formation des groupes

Dans la zone d'information qui s'ouvre lorsque vous cliquez sur un groupe dans l'arborescence de la console web (voir [Figure 13](#)), vous pouvez modifier les paramètres du groupe sélectionné, notamment vous pouvez spécifier la façon de former le groupe : par l'entrée de la liste des adresses ou par la sélection dans la liste des groupes Active Directory.

Vous pouvez sélectionner le type de groupe dans la liste déroulante Type.

La sélection du groupe dépend du protocole via lequel vous planifiez de travailler dans le profil actuel. Par exemple, si vous travaillez via le protocole SMTP, il est recommandé de sélectionner le type Liste des adresses e-mail, si vous travaillez via le protocole FTP, il est recommandé de spécifier le type Liste des adresses IP.



Figure 13. 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 remplacement « * » et « ? » pour remplacer toute séquence de symboles ou tout symbole particulier du texte à saisir.

Pour spécifier la liste des adresses IP :

1. Dans la liste déroulante Type, cliquez sur Liste des adresses IP.
2. Dans la liste déroulante Élément, sélectionnez le type d'élément de la liste Adresse IP ou Plage des adresses IP.
3. Pour ajouter un nouveau élément dans la liste, cliquez sur le bouton Ajouter. Dans la fenêtre qui s'affiche, entrez l'adresse IP ou spécifiez la plage d'adresses en fonction du type sélectionné de l'élément de la liste. Ensuite, cliquez sur OK.
4. Pour supprimer un élément de la liste, sélectionnez-le et cliquez sur Supprimer, puis confirmez la suppression de l'élément sélectionné.

Pour créer une liste de groupes Active Directory :

1. Dans la liste déroulante Type, sélectionne la valeur Liste des groupes Active Directory.
2. Pour ajouter un groupe dans la liste, cliquez sur Ajouter. Dans la fenêtre qui s'ouvre, sélectionnez un groupe et cliquez sur OK.
3. Pour supprimer un groupe de la liste, sélectionnez-le et cliquez sur Supprimer, puis confirmez la suppression du groupe sélectionné.



La formation de la liste des groupes Active Directory est possible uniquement si le serveur est inclus dans le domaine.

Si le serveur n'est pas inclus dans le domaine, vous pouvez former la liste des groupes Active Directory à l'aide de la console Dr.Web CMS Web Console. Pour ce faire :

1. Ouvrez la console Dr.Web CMS Web Console.
2. Pour le paramètre /DrWebADAccessor_1.0/Application Settings/ADAccUserName, spécifiez le nom d'utilisateur ayant l'accès à Active Directory.
3. Pour le paramètre /DrWebADAccessor_1.0/Application Settings/ADAccPassword, spécifiez le mot de passe d'utilisateur ayant l'accès à Active Directory.

Par défaut, les valeurs de paramètres ne sont pas spécifiées.

Dans la liste déroulante Profil, sélectionnez le profil que vous voulez attribuer à ce groupe.

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

7.4. Notifications

Les notifications sont enregistrées dans le [journal du système d'exploitation](#) et elles sont utilisées

pour informer l'administrateur 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 d'administration. La zone d'information pour la configuration des notifications va s'ouvrir. (voir [Figure 14](#)).

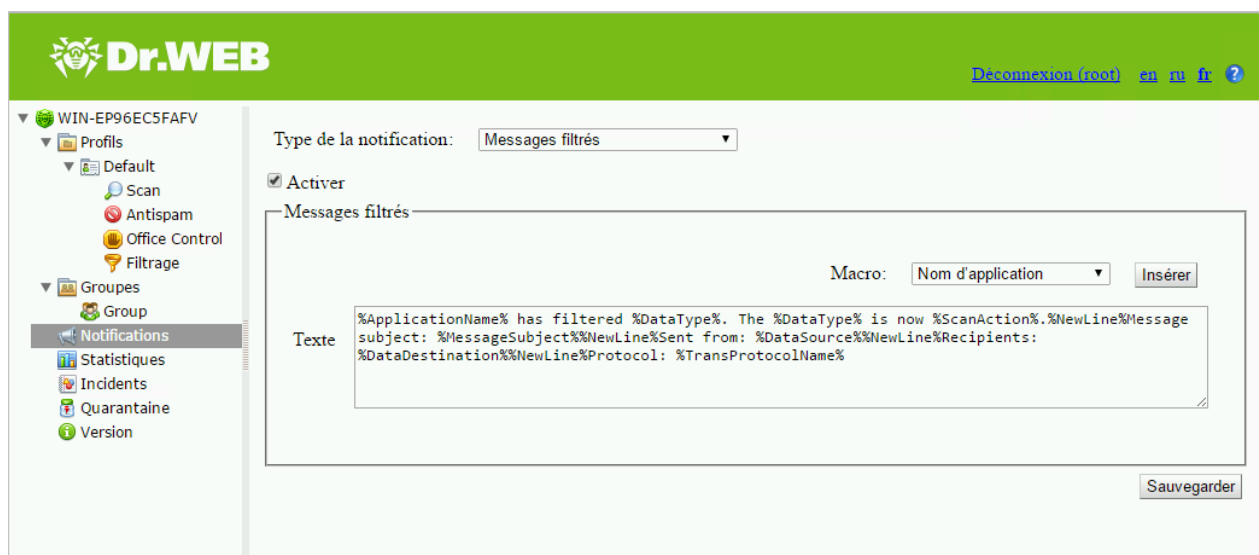


Figure 14. Rubrique de configuration des notifications

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 ;
 - Infectés – pour envoyer des notifications sur les menaces détectées ;
 - Spam – pour envoyer des notifications sur les spams ;
 - Mise à jour – pour envoyer des notifications avec des informations sur la dernière mise à jour ;
 - Bases virales dépassées – pour envoyer une notification lorsqu'une mise à jour des bases de données virales est requise ;
 - Office Control – pour envoyer des notifications sur le filtrage des ressources réseau avec Office Control.
3. Pour activer l'envoi des notifications du type sélectionné, cochez la case Activer.
4. Dans la section des paramètres ci-dessous, vous pouvez modifier le modèle de notification du type sélectionné dans le champ Texte. Lorsque vous éditez le texte, vous pouvez utiliser les macros de la liste déroulante Macro pour remplacer les mots-clés.
5. Après avoir terminé la configuration des notifications, cliquez sur Sauvegarder.



7.5. 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 15](#)).

Pour configurer l'affichage des statistiques :

1. En haut de la section Statistiques, dans la liste Période des statistiques sélectionnez la période pour laquelle vous souhaitez des statistiques. Vous pouvez sélectionner une des valeurs suivantes :
 - Totale – pour afficher les statistiques totales depuis le lancement de 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.

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-section contient les statistiques des actions appliquées par Dr.Web aux objets malveillants détectés.
- Type de menace. Cette sous-section contient les informations sur les types de menaces détectées par Dr.Web pendant la période sélectionnée.



- Catégories de sites. Dans cette sous-section, s'affichent les statistiques de fonctionnement d'Office Control et le nombre des ressources bloquées par catégories.

Période de statistiques	
Pour tout le temps	Type de statistiques
Total	Effacer
Actualiser	

Résultats de l'analyse	
Objets scannés	2857
Objets sains	2852
Objets filtrés	0
Messages spam	0
Objets infectés	1
Objets suspects	0
Objets curables	0
Objets curables par suppression	0
Objets endommagés	0

Actions appliquées aux objets analysés	
Objets déplacés en quarantaine	1
Objets supprimés	0
Objets ignorés	2852
Préfixe ajouté au sujet	0
Objets bloqués	4
Objets de confiance	0

Figure 15. Rubrique des statistiques

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



7.6. Consulter la liste des incidents

La rubrique Incidents permet de voir la liste des événements liés au déclenchement du système antivirus et de l'Antispam pendant la période spécifiée et les informations sur ces événements (voir [Figure 16](#)).

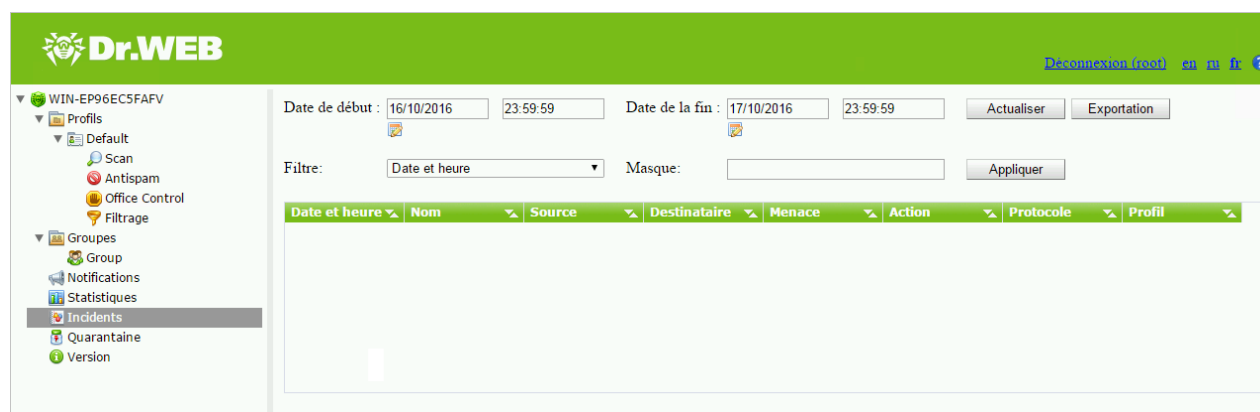


Figure 16. Incidents

Information sur les événements

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

- la date et l'heure ;
- l'objet lié à cet événement ;
- la source et le destinataire ;
- le type de menace ;
- l'action appliquée à la menace ;
- le protocole de transfert ;
- le nom du profil appliqué.

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

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.

Actions appliquées à la liste des incidents

1. Vous pouvez configurer l'affichage des incidents pour une période déterminée. Spécifiez les dates et l'heure de début et de fin de la période, puis cliquez sur Actualiser.
2. Pour faciliter la recherche et la consultation des événements des certains types, 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 « * » et « ? » pour remplacer toute séquence de symboles ou n'importe quel symbole du texte à saisir.

3. Pour sauvegarder la liste des incidents 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 incidents 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 incidents, cliquez sur Actualiser. La liste est actualisée chaque fois que la console d'administration Dr.Web Administrator Web Console est démarrée et que la section Incidents est ouverte. L'actualisation peut prendre un certain temps. Pour annuler l'actualisation, par exemple, si les paramètres du filtrage sont incorrects, cliquez sur Annuler.

7.7. 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 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 en Quarantaine.

7.7.1. Consulter la quarantaine avec Dr.Web for ISA Web Console

L'onglet Quarantaine (voir [Figure 17](#)) de la console d'administration Dr.Web Administrator Web Console est utilisée pour voir la liste des objets isolés et les informations sur ces objets.

Date et heure	Nom	Source	Destinaire	Menace	Taille (octets)	Protocole
13.10.2016 18:57:...	eicarcom2.zip	www.eicar.org	127.0.0.1	EICAR Test File (NO...	308	HTTP
13.10.2016 18:55:...	eicar.com	www.eicar.org	10.3.0.248	EICAR Test File (NO...	68	HTTP
14.10.2016 17:38:...	eicar_com.zip	www.eicar.org	127.0.0.1	EICAR Test File (NO...	184	HTTP

Figure 17. Liste des objets en quarantaine



Information sur les objets en quarantaine

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

- la date et l'heure du déplacement en quarantaine ;
- le nom du fichier infecté ;
- la source et le destinataire ;
- le nom de la menace ;
- la taille du fichier (en octets) ;
- le protocole de transfert.

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

- 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 des événements, cliquez sur Actualiser. La liste des objets en quarantaine est actualisée chaque fois que Dr.Web Administrator Web Console est démarrée et que la section Quarantaine est ouverte. L'actualisation peut prendre un certain temps. Pour annuler l'actualisation, par exemple, si les paramètres de filtrage sont incorrects, 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.

Pour configurer les paramètres de la quarantaine, utilisez l'utilitaire [Gestionnaire de quarantaine](#).

7.7.2. 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 18](#)), utilisez le lien Dr.Web Quarantine sur le Bureau.

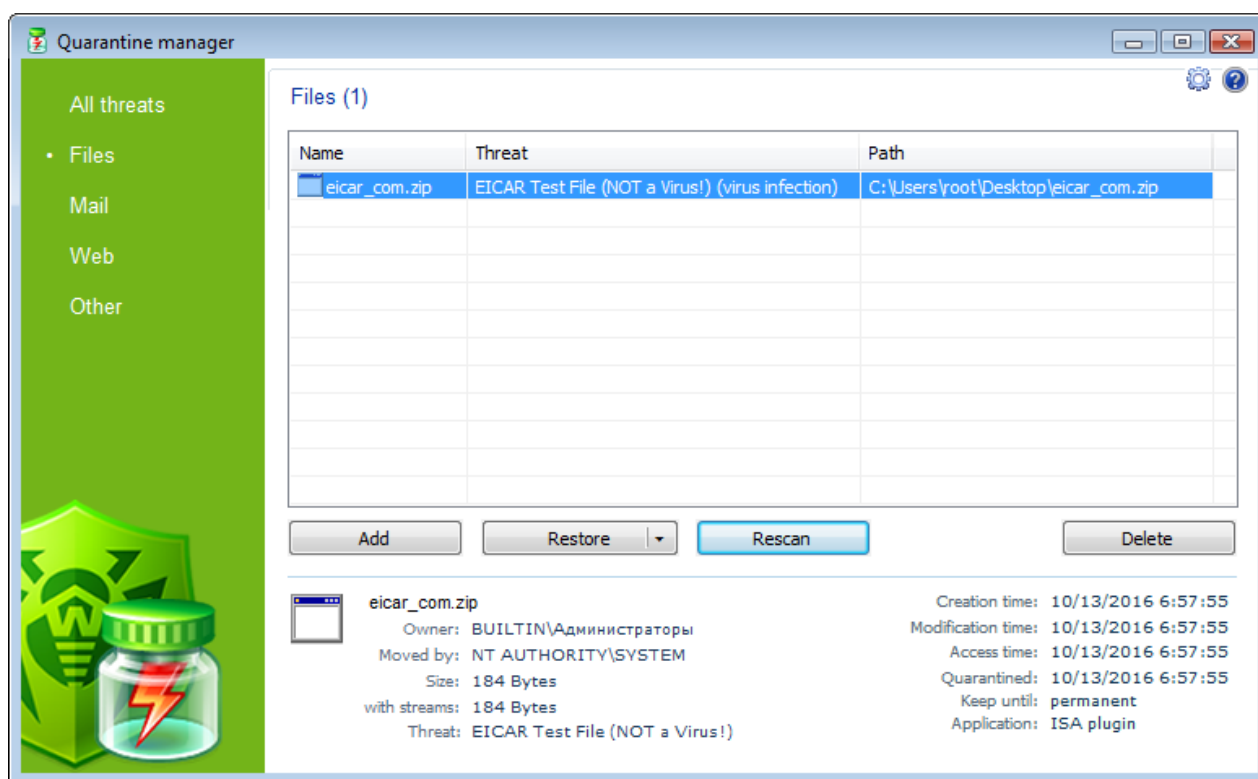


Figure 18. Fenêtre principale de l'utilitaire Dr.Web Quarantine

La fenêtre du Gestionnaire de la quarantaine est composée de plusieurs parties :

1. Le menu latéral sert à filtrer des objets de quarantaine 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 spécifiés :
 - fichiers ;
 - e-mails ;
 - pages web ;
 - tous les autres objets hors catégories .
2. 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 programme malveillant déterminé par Dr.Web lorsque l'objet est placé automatiquement en quarantaine ;
 - Chemin – chemin complet du fichier avant qu'il ne soit placé en Quarantaine.
3. Dans la partie inférieure de la fenêtre de la quarantaine, les informations détaillées sur les objets sélectionnés sont affichées



Vous pouvez activer l'affichage des colonnes contenant des informations détaillées sur l'objet.

Pour paramétrer l'affichage des informations dans les colonnes :

1. Pour configurer les paramètres d'affichage des informations dans le tableau de la Gestionnaire de quarantaine, cliquez droit sur l'en-tête du tableau et sélectionnez dans le menu contextuel 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 ou 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 suivants :
 - 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 enregistrer les modifications apportées aux paramètres, cliquez sur le bouton OK.
annulerPour fermer la fenêtre sans appliquer les modifications, cliquez sur Annuler.

7.7.2.1. Gérer la quarantaine avec le Gestionnaire de la quarantaine

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

- Ajouter – ajouter un fichier dans la quarantaine. Dans la fenêtre de sélection des fichiers, 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 19](#). 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 rescann, le fichier s'avère sain, la quarantaine proposera de récupérer ce fichier ;
- Supprimer – supprimer le 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 une action à effectuer.

7.7.2.2. Configurer les paramètres de la quarantaine

Avec le Gestionnaire de quarantaine vous pouvez spécifier les paramètres de la quarantaine. Pour ce faire:

1. Cliquez sur le bouton  Paramètres dans la fenêtre du Gestionnaire de 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  pour sauvegarder les modifications apportées ou sur Annuler pour annuler les modifications.



8. Mise à jour des bases virales

Dr.Web utilise les bases virales spéciales pour détecter les objets malveillants. Ces bases contiennent des informations sur tous les logiciels malveillants connus. Vu que chaque jour de nouveaux logiciels malveillants apparaissent, 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 complète les bases virales par les informations sur de nouveaux virus et des logiciels malveillants.

Dans la zone d'information de la console d'administration Version, vous pouvez consulter les informations sur la version de l'application, la licence, les bases virales ainsi que les informations sur la date, l'heure et le résultat de la dernière mise à jour du logiciel.

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 MSP Update Task, sélectionnez l'élément Propriétés.
3. Dans la fenêtre Doctor Web for MSP 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.

8.1. Informations sur la version du programme et les bases virales

Dans la zone d'information de la console d'administration Version ([Figure 19](#)) vous pouvez consulter les informations sur la version de l'application, la licence, les bases virales ainsi que sur l'heure et le résultat de la dernière mise à jour du logiciel.



Dr.WEB [Déconnexion \(root\)](#) [en](#) [ru](#) [fr](#) [?](#)

WS2008R2-TMG

- Profils
 - Default
 - Scan
 - Antispam
 - Office Control
 - Filtrage
 - Groupes
 - Notifications
 - Statistiques
 - Incidents
 - Quarantaine
 - Version**

Informations sur le produit

Version du produit :	11.0.0.11111
Quarantine Manager :	11.1.4.11020
Dr.Web Updater :	11.0.10.10260
Dr.Web Scanning Engine :	11.1.4.11020
Dr.Web Virus-Finding Engine :	7.0.23.8290
Module Antispam :	01.375.96

Dr.Web pour Microsoft ISA/TMG Server

Expire :	Mon May 01 11:57:27 201
Numéro de licence :	
Utilisateur :	
Nombre d'ordinateurs :	41
Filtre de spam :	Yes

Bases virales

Inscriptions :	5689933
Dernière mise à jour :	Wed Oct 12 10:01:21 2016

```
drw11000.vdb - 775743 virus records
date: Fri Apr 01 07:00:00 2016
drw11001.vdb - 881516 virus records
date: Fri Apr 01 08:00:00 2016
```

Tâche de mise à jour

Action :	Vérifier les résultats
Résultat précédent :	En cours

Figure 19. Version



9. Console web Dr.Web CMS Web Console

La console web Dr.Web CMS Web Console est une console auxiliaire incluse dans Dr.Web. A l'aide de cette console, vous pouvez spécifier les valeurs des variables pour corriger les erreurs ou modifier les paramètres de fonctionnement de l'application, par exemple, créer un cluster, ajouter un administrateur, modifier les paramètres des comptes, etc.

Utilisez Dr.Web CMS Web Console si vous savez exactement les valeurs des variables que vous indiquez manuellement. Pour la gestion générale des paramètres de l'application, utilisez la console d'administration [Dr.Web Administrator Web Console](#).

Pour lancer Dr.Web CMS Web Console

Pour lancer la console Dr.Web CMS Web Console (voir [Figure 20](#)), ouvrez la page suivante dans le navigateur :

`https://<ISA Server address>:2080/root,`

où *<ISA Server address>* est l'adresse du serveur ISA/Microsoft Forefront TMG.



Pour accéder à la page de Dr.Web CMS Web Console, vous devez saisir les données du compte administrateur.

Au premier démarrage de Dr.Web CMS Web Console, entrez les données du compte par défaut : le nom d'utilisateur root et le mot de passe drweb. Ensuite, il est fortement recommandé de modifier le mot de passe pour ce compte (pour plus d'informations, voir [Modifier le mot de passe de l'administrateur](#)).

The screenshot displays the Dr.Web CMS Web Console interface. On the left, there is a tree view under 'Hosts & Groups' showing a hierarchy for the host '127.0.0.1:2056', including folders like 'AdminWebConsole_1.0', 'Application Localization', 'Application Statistics', 'Application Status', 'Settings', and various modules such as 'CMS_1.0', 'Dr.Web CMS Web Console_1.0', 'Dr.Web SSM_1.0', 'Dr.Web AD Accessor_1.0', 'Dr.Web Agent Stub_1.0', 'Dr.Web Components Host_1.0', 'Dr.Web File Storage_1.0', 'Dr.Web Incident Registrar_1.0', 'Dr.Web Quarantine_1.0', 'Dr.Web Requests Queue_1.0', 'Dr.Web Scan Srv_1.0', 'Dr.Web Sink Module_1.0', 'Dr.Web VSAPI Module_1.0', 'FTP Filter_1.0', 'HTTP Web Filter_1.0', 'POP3 Filter_1.0', and 'SMTP Filter_1.0'. On the right, a 'Variables' table lists various system parameters.

Name	Type	Value	Attributes
Active	Boolean	True	System
Crash	Boolean	False	System
HomeDir	String	C:/Program Files/DrWeb CMS for MSP/	System
InstanceName	String	AdminWebConsole	System
LogicCrash	Boolean	False	System
ModuleName	String	drwcmswc.exe	System
ModulePath	String	C:/Program Files/DrWeb CMS for MSP/drwcmswc...	System
PID	UInt32	2156	System
StartedOn	Time	Fri Oct 14 17:29:45 2016	System
Version	String	1.0.0.0	System
VersionBuild	UInt32	0	System
VersionMajor	UInt32	1	System
VersionMinor	UInt32	0	System
VersionRevision	UInt32	0	System
WorkDir	String	C:/Program Files/DrWeb CMS for MSP/	System

Below the table, there is a section for logs with columns: Time, Host, Instance, Log Level, and Text.

Figure 20. Console web Dr.Web CMS Web Console



Interface

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 mode 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 Dr.Web Administrator Web Console ou de 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 type de la variable. Indiquez comme valeur :
 - 0 - accès complet à tous les paramètres de la console ;
 - 1 - accès à la console sans possibilité de modifier les paramètres.



Si la valeur de la variable UserLevel n'est pas spécifiée, l'administrateur aura accès à tous les paramètres de la console 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 créée. 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.

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.



Gestion des paramètres de l'analyse et du filtrage des groupes Active Directory

Les variables avec l'attribut Shared des profils et des groupes représentant les listes des adresses e-mail, et ces profils et groupes eux-mêmes sont librement transmis entre les bases de données cmsdb depuis le serveur gérant au serveur subordonné parce qu'ils ne dépendent pas d'Active Directory. Si le serveur gérant et le serveur subordonné sont connectés à un serveur du catalogue global (Global Catalog) d'Active Directory, lorsqu'un groupe Active Directory est créé dans la console d'administration 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 Dr.Web CMS Web Console, 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 d'administration 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 la console d'administration Dr.Web Administrator Web Console sur le serveur gérant et ces paramètres seront transférés sur les deux serveurs.

9.4. 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.
Ce paramètre est disponible dans la console Dr.Web Administrator Web Console. Pour plus d'infos, consultez la rubrique [Scan](#).
 - 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 [Scan](#) sera appliquée à ces objets.
- false – les objets de ce type seront traités comme des objets sains et seront ignorés.

9.5. 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. En cas de détection, 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 d'événements Dr.Web.

Les informations sur les mises à jour sont écrites dans le journal texte `dwupdater.log` se trouvant dans le répertoire suivant (voir le chapitre [Vérification du module de mise à jour](#)) :

- `%ALLUSERSPROFILE%\Application Data\Doctor Web\Logs` si vous utilisez Windows Server 2003 ;
- `%PROGRAMDATA%\Doctor Web\Logs` si vous utilisez Windows Server 2008.

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 la section [Notifications](#)). Il s'agit des types suivants des événements pour lesquels vous pouvez configurer les notifications :
 - J Messages filtrés – notifications de filtrage de messages ;
 - J Fichiers filtrés – notifications de filtrage des pièces jointes filtrées ;
 - J Infectés – notifications de menaces détectées ;
 - J Spam – notifications de spam ;
 - J Infectés – notifications de filtrage des objets infectés ;
 - J Mise à jour – notifications de la dernière mise à jour ;
 - J Bases virales dépassées – notification de nécessité d'une mise à jour des bases virales ;
 - J Office Control – notifications de filtrage des ressources réseau avec Office Control.



Consultation du journal d'enregistrement du système d'exploitation

1. Pour consulter le journal des événements du système d'exploitation, allez dans le Panneau de configuration du système d'exploitation.
2. Sélectionnez Outils d'administration puis Observateur d'événements.
3. Dans la partie gauche de la fenêtre Observateur d'événements, sélectionnez 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 de Dr.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 web 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 Doctor Web.

3. Redémarrez le service Dr.Web for MSP Scanning Service.
4. Supprimez la source d'événements Dr.Web CMS for MSP de la rubrique du registre `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Doctor Web\Dr.Web for Microsoft Server Products`.
5. Redémarrez le système d'exploitation.

10.2. Journal texte de l'assistant d'installation

Pour faciliter le processus de débogage en cas de problèmes ou d'erreurs lors de l'installation, le programme d'installation enregistre les événements. Le fichier d'enregistrement des événements isa-tmg-setup.log est créé dans le répertoire :

- %ALLUSERSPROFILE%\Application Data\Doctor Web\Logs si vous utilisez Windows Server 2003 ;
- %PROGRAMDATA%\Doctor Web\Logs si vous utilisez Windows Server 2008.

10.3. Journal d'événements Dr.Web

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 de



l'application %ProgramFiles%\DrWeb CMS for MSP.

Le service gérant enregistre différents types d'événements et permet de spécifier le niveau de détails pour chaque application- abonnée du service Dr.Web CMS.

La taille maximum de la base de données est de 500 Mo. Lorsque cette valeur est atteinte, la base de données actuelle est archivée dans le dossier d'installation de l'application, l'estampille temporelle est marquée dans le nom de fichier. Après cela, un nouveau fichier est créé pour la base de données.

Vous pouvez [supprimer la base de données](#) cmstracedb, si nécessaire.

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 qui nécessitent l'attention de l'administrateur.
Information	Les messages d'information.
Debug	Les messages de débogage.

Le service gérant permet d'afficher la liste des événements enregistrés en temps réel, de filtrer les événements par les 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.



Valeur	Niveau de détails
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 de service Dr.Web CMS le niveau de détails 2 est paramétré. Pour spécifier le niveau de détails 3 pour toutes les applications, sélectionnez l'option Debug Traces dans le menu contextuel qui s'ouvre si vous cliquez droit sur l'élément racine de l'arborescence de la console Dr.Web CMS Web Console. 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 constaté 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, puis 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. Au bout d'un certain temps, ce processus peut prendre toute la mémoire disponible, ce qui diminuera 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 %PROGRAMFILES%\DrWeb CMS for MSP:

1. Lancez la console de commande cmd avec les privilèges administrateurs.
2. 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"
```
3. Supprimez le fichier cmstracedb qui se trouve dans le dossier d'installation de l'application %PROGRAMFILES%\DrWeb for CMS for MSP.
4. 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"
```
5. 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 décrits dans ce chapitre :

- [Vérification du module de mise à jour](#) ;
- [Vérification de la détection de virus](#) ;
- [Vérification de la détection de spam](#).

11.1. Vérification de l'installation

Dr.Web doit être installé dans les dossiers suivants :

Pour Microsoft ISA Server :

- %ALLUSERSPROFILE%\Application Data\Doctor Web ;
- %PROGRAMFILES%\Common Files\Doctor Web ;
- %PROGRAMFILES%\DrWeb CMS for MSP ;
- %PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG.

Pour Microsoft Forefront TMG :

- %PROGRAMDATA%\Doctor Web ;
- %PROGRAMFILES%\DrWeb CMS for MSP ;
- %PROGRAMFILES%\Common Files\Doctor Web ;
- %PROGRAMFILES%\Microsoft Forefront Threat Management Gateway\DrWeb for ISA and TMG.

Veillez 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.

Enfin, veuillez vous assurer que les services locaux suivants sont lancés :

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



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`, des bases virales et d'autres éléments, sauf les composants de l'application.

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 `%WINDIR%\Tasks` ou ouvrez le Planificateur de tâches Windows.
2. Vérifiez la présence de la tâche Dr.Web dans le dossier qui s'ouvre (si la tâche est correctement accomplie, le code de retour dans la colonne Résultat de la dernière exécution doit être `0x0`).
3. Ensuite ouvrez le fichier de journal des événements du module de mise à jour
`%ALLUSERSPROFILE%\Application Data\Doctor Web\Logs\dwupdater.log` si vous travaillez sous Windows Server 2003 ou
`%PROGRAMDATA%\Doctor Web\Logs\dwupdater.log` si vous travaillez sous Windows Server 2008 et assurez-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.

Vérification de la détection de virus avec le fichier de test EICAR

1. Créez le fichier :
 - ouvrez NotePad ;
 - copiez-y la ligne suivante :
`X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*`
2. Sauvegardez ce fichier avec l'extension `.com`. Vous pouvez utiliser n'importe quel nom de fichier, par exemple, `eicar.com`.
3. 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 Microsoft ISA Server et Forefront TMG. Le nom du virus : EICAR Test File (NOT a Virus!).



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. Annexe A. Suppression manuelle de Dr.Web

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

1. Arrêtez le service du pare-feu Microsoft ISA Server ou Microsoft Forefront TMG.
2. Lancez la console de commande cmd avec les privilèges administrateurs.
3. Supprimez l'enregistrement des filtres des applications :

- en cas d'utilisation de Microsoft ISA Server :

```
regsvr32 /u /s "%PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG\FTPFilter.dll"
```

```
regsvr32 /u /s "%PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG\POP3Filter.dll"
```

```
regsvr32 /u /s "%PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG\SMTPFilter.dll"
```

```
regsvr32 /u /s "%PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG\HTTPWebFilter.dll"
```

- en cas d'utilisation de Microsoft Forefront TMG :

```
regsvr32 /u /s "%PROGRAMFILES%\Microsoft Forefront Threat Management Gateway\DrWeb for ISA and TMG\FTPFilter.dll"
```

```
regsvr32 /u /s "%PROGRAMFILES%\Microsoft Forefront Threat Management Gateway\DrWeb for ISA and TMG\POP3Filter.dll"
```

```
regsvr32 /u /s "%PROGRAMFILES%\Microsoft Forefront Threat Management Gateway\DrWeb for ISA and TMG\SMTPFilter.dll"
```

```
regsvr32 /u /s "%PROGRAMFILES%\Microsoft Forefront Threat Management Gateway\DrWeb for ISA and TMG\HTTPWebFilter.dll"
```

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"
```

6. Supprimez les répertoires suivants :

- en cas d'utilisation de Microsoft ISA Server :

```
rd /S /Q "%ALLUSERSPROFILE%\Application Data\Doctor Web"  
rd /S /Q "%PROGRAMFILES%\DrWeb CMS for MSP"  
rd /S /Q "%PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG"
```

- en cas d'utilisation de Microsoft Forefront TMG :

```
rd /S /Q "%PROGRAMDATA%\Doctor Web"  
rd /S /Q "%PROGRAMFILES%\DrWeb CMS for MSP"  
rd /S /Q "%PROGRAMFILES%\Microsoft Forefront Threat Management Gateway  
\DrWeb for ISA and TMG"
```

12.2. Annexe B. 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 des 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.

12.2.1. 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
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

La base de données représente une un fichier cmsdb situé dans le dossier d'installation de l'application (%PROGRAMFILES%\DrWeb CMS for MSP).

12.2.2. 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.

12.2.3. Connexion aux serveurs

La console Dr.Web CMS Web Console permet de se connecter aux autres serveurs sur lesquels fonctionne CMS. Pour vous connecter, faites le suivant :

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 Dr.Web CMS Web Console 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 connexion. 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.

Le serveur de la console Dr.Web CMS Web Console sauvegarde les paramètres de connexion à chaque hôte ajouté dans son groupe dans CMS par le chemin /Dr.Web CMS Web Console_1.0/Application Settings/Hosts.

Chaque hôte ajouté représente un groupe ayant un nom sous forme d'adresse de connexion à chaque hôte ajouté. Trois variables sont créées au sein d'un groupe Address, Login et Password. La variable Address contient l'adresse de connexion à l'hôte. La variable Login contient le nom d'utilisateur pour la connexion. La variable Password contient le mot de passe pour la connexion à l'hôte.

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



Au lancement ultérieur, la console Dr.Web CMS Web Console 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 par le chemin / Dr.Web CMS Web Console_1.0/Application Settings/Hosts.

Avec la console Dr.Web CMS Web Console, vous pouvez également [créer des clusters](#) qui permettent de spécifier les paramètres pour tous les hôtes groupés.

12.3. Annexe C. 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 MSP 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	<p>Veillez de ne pas modifier ce paramètre.</p> <p>Type de mise à jour :</p> <ul style="list-style-type: none">• update-revision - mise à jour des composants au sein de la révision actuelle.
--disable-postupdate	<p>Veillez de ne pas modifier ce paramètre.</p> <p>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.</p>
--verbosity arg	<p>Niveau de détails du journal :</p> <ul style="list-style-type: none">• error - standard ;• info - accru ;• debug - débogage.
--interactive	<p>Si le paramètre est indiqué, un plus grand nombre de ressources sera utilisé pour l'exécution de certaines commandes.</p>
--param args	<p>Veillez de ne pas modifier ce paramètre.</p> <p>Paramètres supplémentaires transmis pour le script.</p>



Paramètre	Description
	Format : <nom>=<valeur>.
-n [--component] arg	Liste des composants à mettre à jour : <ul style="list-style-type: none">• updater - fichier drwupsrv.exe ;• antisipam -fichier vrcpp.dll ;• scan-engine - fichiers dwengine.exe, dwsewsc.exe, dwinctl.dll, dwarkdaemon.exe, arkdb.bin, dwqrui.exe, dwarkapi.dll ;• av-engine - bases virales (fichiers avec l'extension *.vdb) ;• isa-and-tmg-setup - fichier isa-and-tmg-setup.exe. <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px;"> Plusieurs éléments peuvent être mis à jour en même temps, par exemple : <pre>-n av-engine updater</pre></div>
-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_name>" -n av-engine --  
proxy=192.168.134.128:808 --user=qwerty --password=qwerty
```

Paramètres de la commande - c postupdat

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

Paramètre	Description
--verbosity arg	Niveau de détails du journal : <ul style="list-style-type: none">• error - standard ;• info - accru ;• debug - débogage.
--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.



Paramètre	Description
	Format : <nom>=<valeur>.

Exemple de la commande - c postupdate :

```
-c postupdate --verbosity=debug --interactive --param="<plugin_name>"
```

Création d'un 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> --repor-dir=<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\ --repor-dir=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=<plugin_name>" --  
zone="file://<repo_folder_path>"
```



Référence

A

- abréviations 6
- administration
 - console CMS 55
 - console web 25
 - groupes 26, 40
 - profils 26, 27
- ajouter un administrateur 57
- analyse
 - filtres 16, 17, 19
- analyseur heuristique 28
- antispam
 - configuration 30
 - licence 30
- assistant d'installation
 - installation du logiciel 23
 - journalisation des événements 63

B

- base de données CMS 70
- bases virales 53

C

- configuration
 - antispam 30
 - d'office Control 32
 - de filtrage 34
 - de la quarantaine 48
 - de scan 28
 - notifications 43
- console CMS
 - ajouter un administrateur 57
 - mot de passe de l'administrateur 57
- console web CMS 55
 - créer les clusters 58
- console web d'administration 25, 28, 30, 32, 34, 43, 45, 47, 48
- consulter les statistiques 45
- créer les clusters 58

D

- diagnostic 66, 67, 68
- Dr.Web 8
 - administration 25
 - composants 12
 - console CMS 55, 57, 57, 58

- destination 8
- diagnostic 66
- Dr.Web Administrator Web Console 25
- Dr.Web CMS Web Console 55
- Dr.Web FTP Filter 16
- Dr.Web HTTP Web Filter 19
- Dr.Web POP3 Filter 17
- Dr.Web SMTP Filter 17
- filtres 12, 12, 16, 17, 17, 19
- fonctions 8
- groupes 40
- installation 21, 23
- journalisation des événements 62
- licence 10
- mise à jour 53
- objets contrôlés 9
- pré-requis système 21
- profils 27
- services 20
- statistiques du fonctionnement 45
- suppression 21, 24
- suppression manuelle 69
- Dr.Web Administrator Web Console 25, 28, 30, 32, 34, 43, 45, 47, 48
 - groupes 26
 - profils 26
- Dr.Web CMS Web Console
 - ajouter un administrateur 57
 - mot de passe de l'administrateur 57
- Dr.Web FTP Filter 16
- Dr.Web HTTP Web Filter 19
- Dr.Web POP3 Filter 17
- Dr.Web SMTP Filter 17

E

- événements 47
 - statistiques 45
 - surveillance 20
- événements viraux 47
 - journal des événements 20
 - notifications 20
 - statistiques 20, 45
 - surveillance 20
- event log 62

F

- fichier clé



Référence

fichier clé

- actualité 10
- mise à jour 11
- obtention 10, 10

fichier d'installation 23

filtrage

- règles 34

filtre antivirus 12

filtres

- analyse 16, 17, 19
- des applications 12
- filtre web 17

G

gestionnaire de quarantaine 49, 51, 52

groupes 26, 40

- création 40
- formation 42
- types 42

I

installation de Dr.Web 21, 21

- assistant d'installation 23
- fichier d'installation 23
- vérification 66

J

journal de débogage 63

journal de l'assistant d'installation 63

journal des événements 20, 43

- du système d'exploitation 62
- journal d'événements Dr.Web 63
- journal de l'assistant d'installation 63

journalisation des événements 62, 63

- journal de l'assistant d'installation 63
- journal du système d'exploitation 62

L

le fichier de test EICAR 67

légende 6

licence

- actualité 10
- antispam 30
- fichier clé 10, 10
- mise à jour 11
- obtention 10

liste blanche d'adresses 32

liste noire d'adresses 32

M

message de test GTUBE 68

miroir de mises à jour 75

mise à jour

- bases virales 53
- diagnostic 67
- licence 11
- module de mise à jour 67
- paramètres de ligne de commande 73

module de mise à jour 53, 73

- vérification 67

mot de passe de l'administrateur 57

N

notifications

- configuration 43
- journal des événements 43
- types 43

notifications e-mail 20

notifications par e-mail 20

O

objets contrôlés 9

obtenir un fichier clé 10

office Control

- configuration 32
- listes des adresses 32

P

plateforme CMS 70

- base de données 70
- statistiques des applications 71

pré-requis 21

pré-requis système 21

profils 26, 27

- configuration 27
- création 27
- priorité 28

Q

quarantaine 20, 48

- actions 48, 51
- configuration 48



Référence

- quarantaine 20, 48
 - configuration des propriétés 52
 - gestion 51
 - gestionnaire de quarantaine 49, 51, 52

R

- règles de filtrage 34

S

- scan
 - actions 28
 - configuration 28
- services 20
 - Dr.Web CSM 55
- statistiques 20
 - des applications 71
 - événements 45
 - parcourir 45
- suppression de Dr.Web 21, 24

V

- vérification
 - de l'installation 66
 - de la capacité de travail 66
 - de la détection de spam 68
 - de la détection de virus 67
 - module de mise à jour 67

