



Dr.WEB®

Enterprise Security Suite

Defend what you create

Manuel Administrateur

© Doctor Web, 2004-2013. Tous droits reserves

Ce document est la propriété de Doctor Web. Aucune partie de ce document ne peut être reproduite, publiée ou transmise sous quelque forme que ce soit, par quelque moyen que ce soit et dans quelque but que ce soit sinon pour une utilisation personnelle de l'acheteur sans attribution propre.

MARQUES DEPOSEES

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.

DECHARGE

En aucun cas Doctor Web et ses revendeurs et distributeurs ne peuvent être tenus pour responsables pour les erreurs ou omissions, pertes de profit ou tout autre dommage causés ou prétendus être causés par le présent document, son utilisation ou l'incapacité d'utiliser l'information contenue dans ce document.

Dr.Web Enterprise Security Suite

Version 6.0.4

Manuel Administrateur

08.07.2013

Doctor Web Head Office
2-12A, 3rd str. Yamskogo polya
Moscow, Russia
125124

Web site: www.drweb.com

Phone: +7 (495) 789-45-87

Consultez le site web officiel pour en savoir plus sur les bureaux régionaux ou internationaux.

Doctor Web

Doctor Web développe et distribue les solutions de sécurité de l'information Dr.Web® qui fournissent une protection efficace contre les logiciels malveillants et le spam.

Les clients de Doctor Web sont des utilisateurs particuliers dans le monde entier, ainsi que des institutions gouvernementales, des petites entreprises et des entreprises nationales.

Les solutions antivirus Dr.Web sont connues depuis 1992 pour leur excellence en matière de détection des malwares et leur conformité aux standards de sécurité de l'information internationaux. Les certificats d'Etat et les prix attribués aux solutions Dr.Web 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
et leur fidélité aux produits Dr.Web !**



Contenu

Chapitre 1. Introduction	14
1.1. Introduction	14
1.2. Légende et abréviations	16
1.3. Composants, destination, fonctions principales de l'Antivirus Dr.Web Enterprise Security Suite	17
1.4. Avantages	21
1.5. Pré-requis système	23
1.6. Composition du package d'installation	29
1.7. Fichiers clés	30
Chapitre 2. Installation et suppression des composants de Dr.Web Enterprise Security Suite	33
2.1. Création d'un réseau antivirus	33
2.2. Installation Dr.Web Enterprise Server	34
2.2.1. Installation de Dr.Web Enterprise Server sous Windows®	36
2.2.2. Installation de Dr.Web Enterprise Server sous UNIX®	48
2.2.3. Installation du module ajoutable Dr.Web Browser-Plugin	53
2.3. Installation de Dr.Web Enterprise Agent sous OS Windows®	57
2.3.1. Fichiers d'installation	58
2.3.2. Installation de Dr.Web Enterprise Agent à l'aide du Package d'installation	60
2.3.3. Installation de Dr.Web Enterprise Agent avec l'installateur réseau	66



2.4. Installation distante de Dr.Web Enterprise Agent sous Windows®	72
2.4.1. Installation de Dr.Web Enterprise Agent via le Centre de Gestion Dr.Web	75
2.4.2. Installation de Dr.Web Enterprise Agent avec le service Active Directory	82
2.5. Installation de NAP Validator	89
2.6. Installation du Serveur proxy	90
2.7. Suppression des composants sélectionnés de Dr.Web Enterprise Security Suite	94
2.7.1. Suppression des composants sous Windows®	94
2.7.2. Suppression de Dr.Web Enterprise Agent avec le service Active Directory	97
2.7.3. Suppression de Dr.Web Enterprise Server sous UNIX®	97
2.7.4. Suppression du Serveur proxy	99
Chapitre 3. Composants du réseau antivirus et leur interface	101
3.1. Dr.Web Enterprise Server	101
3.2. Dr.Web Enterprise Agent	105
3.3. Centre de Gestion Dr.Web	110
3.3.1. Administration	115
3.3.2. Réseau antivirus	117
3.3.3. Préférences	124
3.3.4. Liaisons	129
3.3.5. Aide	130
3.4. Composants du Centre de Gestion Dr.Web	131
3.4.1. Scanner réseau	131
3.4.2. Gestionnaire de licence	135



3.5. Schéma d'interaction des composants du réseau antivirus	147
Chapitre 4. Mise en route. Généralités	153
4.1. Création d'un simple réseau antivirus	153
4.2. Configuration des connexions réseau	156
Chapitre 5. Administrateurs du réseau antivirus	161
5.1. Authentification des administrateurs	161
5.2. Types d'administrateur	167
5.3. Gestion des comptes administrateur	169
5.3.1. Création et suppression des comptes administrateur	170
5.3.2. Edition des comptes administrateur	172
Chapitre 6. Groupes. Gestion globale des postes de travail	174
6.1. Groupes système et groupes utilisateur	174
6.2. Gestion des groupes	178
6.2.1. Création et suppression des groupes	178
6.2.2. Configuration des groupes	180
6.3. Ajout des postes de travail dans un groupe. Suppression des postes d'un groupe	182
6.4. Utilisation des groupes pour configurer les postes de travail	185
6.4.1. Héritage des éléments de configuration du poste de travail. Groupes primaires	186
6.4.2. Copie des configurations vers d'autres groupes/postes	189
6.5. Comparaison des postes et des groupes	189
Chapitre 7. Gestion du poste de travail	191



7.1. Gestion des entrées relatives aux postes de travail	192
7.1.1. Politique de connexion des postes	192
7.1.2. Suppression et récupération du poste	194
7.2. Configuration du poste de travail	196
7.2.1. Configuration des droits d'utilisateurs	202
7.2.2. Consultation des composants installés du package antivirus	204
7.2.3. Composition du package antivirus	206
7.3. Configuration de Dr.Web Enterprise Agent sous Windows®	208
7.4. Configuration de la planification des tâches sur le poste de travail	213
7.5. Scan antivirus du poste de travail	218
7.5.1. Consultation et interruption des composants en cours	219
7.5.2. Interruption des composants en cours selon leur type	220
7.5.3. Lancement de scan sur le poste	221
7.5.4. Configuration du Scanner pour OS Windows	222
7.6. Consultation des résultats et des statistiques récapitulatives sur un poste	234
7.6.1. Tableaux	234
7.6.2. Graphiques	239
7.6.3. Tableau récapitulatif	242
7.6.4. Quarantaine	243
7.7. Configurations de certains composants antivirus	246
7.7.1. Configuration d'Office Control pour l'accès aux ressources locales et aux celles du réseau sous OS Windows®	246



7.7.2. Configuration du composant MailD pour la protection des adresses e-mail sous OS UNIX® et Mac OS X	248
7.8. Envoi des messages à l'utilisateur	249
Chapitre 8. Configuration de Dr.Web Enterprise Server	254
8.1. Configuration de Dr.Web Enterprise Server	254
8.1.1. Chiffrement et compression du trafic	264
8.1.2. Configuration de la BD	267
8.1.3. Configuration des notifications	269
8.2. Ecriture dans le log du serveur	272
8.3. Configuration de la planification de Dr.Web Enterprise Server	273
8.4. Gestion du dépôt des produits Dr.Web Enterprise Server	277
8.4.1. Introduction	277
8.4.2. Statut du dépôt des produits	279
8.4.3. Editeur de configuration du dépôt des produits	279
8.5. Particularités du réseau avec plusieurs Serveurs Dr.Web Enterprise Server	282
8.5.1. Structure du réseau avec plusieurs serveurs Dr.Web Enterprise Server	283
8.5.2. Configuration des liaisons entre serveurs Dr.Web Enterprise Server	286
8.5.3. Utilisation du réseau antivirus avec plusieurs serveurs Dr.Web Enterprise Server	294
8.5.4. Fonctionnement de plusieurs Serveurs Dr.Web Enterprise Server avec une seule BD	296
Chapitre 9. Mise à jour de Dr.Web Enterprise Security Suite et de ses composants	297



9.1. Mise à jour de Dr.Web Enterprise Security Suite	297
9.1.1. Mise à jour de Dr.Web Enterprise Server pour OS Windows®	297
9.1.2. Mise à jour de Dr.Web Enterprise Server pour OS UNIX®	305
9.1.3. Mise à jour du module ajoutable Dr.Web Browser-Plugin	313
9.1.4. Mise à jour de l'Dr.Web Enterprise Agent	314
9.1.5. Mise à jour du Serveur proxy	314
9.2. Mise à jour manuelle des composants de Dr.Web Enterprise Security Suite	316
9.3. Mise à jour selon la planification	318
9.4. Mise à jour du dépôt des produits de Dr.Web Enterprise Server non connecté à Internet	320
9.5. Restrictions de mises à jour des postes	322
9.6. Mise à jour des Agents mobiles Dr.Web Enterprise Agent	323
9.7. Mise à jour des clés de Serveur et des clés de postes	325
Chapitre 10. Configuration des composants supplémentaires	328
10.1. Serveur proxy	328
10.2. NAP Validator	333
Annexes	338
Annexe A. Liste complète des OS supportés	338
Annexe B. Configurations requises en cas d'utilisation de SGBD. Paramètres des pilotes SGBD	345
Annexe B1. Configuration du driver ODBC	348
Annexe B2. Configuration du driver BD pour Oracle	351



Annexe B3. Configuration du driver de la BD pour SQL CE	354
Annexe B4. Utilisation du SGBD PostgreSQL	357
Annexe C. Paramètres du système de notifications	361
Annexe D. Paramètres des templates du système de notifications	362
Annexe E. Spécification de l'adresse réseau	370
E1. Format général de l'adresse	370
E2. Adresses de Dr.Web Enterprise Server	373
E3. Adresses de Dr.Web Enterprise Agent/ Installer	374
Annexe F. Gestion du dépôt des produits	376
F1. Syntaxe du fichier de configuration .config	377
F2. Règles du fichier .config	379
F3. Fichiers .id	385
F4. Exemples de gestion du dépôt des produits avec une modification du fichier de statut	386
Annexe G. Fichiers de configuration	388
G1. Fichier de configuration de Dr.Web Enterprise Server	388
G2. Fichier de configuration du Centre de Gestion Dr.Web	397
G3. Fichier de configuration download.conf	402
G4. Fichier de configuration du Serveur proxy	403
Annexe H. Paramètres de la ligne de commande relatifs aux programmes inclus dans Dr.Web Enterprise Security Suite	408
H1. Introduction	408
H2. Module d'interface Dr.Web Enterprise Agent	409
H3. Dr.Web Enterprise Agent	410
H4. Installateur réseau	414



H5. Dr.Web Enterprise Server	417
H6. Utilitaire d'administration de la BD interne	432
H7. Utilitaire de génération des paires de clés et de la signature numérique	433
H8. Gestion du Serveur Dr.Web Enterprise Server sous UNIX® avec la commande kill	434
H9. Scanner Dr.Web pour OS Windows®	435
H10. Serveur proxy	435
Annexe I. Variables d'environnement exportées par le Serveur Dr.Web Enterprise Server	438
Annexe J. Utilisation du script de l'installation initiale pour Dr.Web Enterprise Agent	439
Annexe K. Utilisation des expressions régulières dans Dr.Web Enterprise Security Suite	444
K1. Options des expressions régulières	444
K2. Particularités des expressions régulières PCRE	446
K3. Utilisation des métacaractères	448
Annexe L. Format des fichiers de log	471
Annexe M. Description des procédures utilisateur	474
Annexe N. Intégration de Dr.Web Enterprise Security Suite avec XML Web API	479
Annexe O. Procédures d'authentification des administrateurs	480
Annexe P. Licences	485
P1. Boost	486
P2. Curl	487
P3. Libradius	488
P4. MD5 implementation	489
P5. Net-snmp	490



P6. OpenLDAP	499
P7. OpenSSL	501
P8. Oracle Instant Client	505
P9. PCRE	513
P10. Sha2 implementation	516
P11. Wtl	518
P12. Zlib	525
P13. MIT License	526
P14. GNU General Public License	526
P15. GNU Lesser General Public License	544
P16. Mozilla Public License	548

Questions fréquentes **559**

Déplacement du Serveur Dr.Web Enterprise Server vers un autre ordinateur (sous Windows®) **559**

Connexion de Dr.Web Enterprise Agent à un autre serveur Dr.Web Enterprise Server **562**

Changement du type de SGBD Dr.Web Enterprise Security Suite **564**

Restauration de la BD Dr.Web Enterprise Security Suite **569**

Restauration de Dr.Web Enterprise Server depuis une copie de sauvegarde **576**

Mise à jour des Agents sur les serveurs LAN **580**

Récupération de mot de passe administrateur Dr.Web Enterprise Security Suite **581**

Utilisation de DFS lors de l'installation de l'Agent via Active Directory **583**

Diagnostic des problèmes d'installation distante **584**



Référence

588



Chapitre 1. Introduction

1.1. Introduction

Le présent Manuel décrit les principes généraux ainsi que les détails concernant la mise en oeuvre de la protection antivirus des ordinateurs d'entreprise avec **Dr.Web® Enterprise Security Suite** (nommé ci-après **Dr.Web ESS**). Ce Manuel ne décrit pas les packages antivirus **Dr.Web** pour les postes protégés. Pour ces informations, merci de consulter le **Manuel Utilisateur Dr.Web pour Windows**.

Le présent Manuel est conçu pour *l'administrateur du réseau antivirus*, un employé de l'entreprise responsable de la gestion de la protection antivirus des postes de travail et des serveurs se trouvant dans le réseau.

L'administrateur du réseau antivirus doit avoir les droits d'administrateur système ou être en contact avec l'administrateur du réseau local. Il doit également avoir une bonne maîtrise de la stratégie de la protection antivirus et connaître les packages antivirus **Dr.Web** correspondants à tous les systèmes d'exploitation utilisés dans le réseau.

Certains chapitres de ce Guide seront utiles pour le chef d'entreprise responsable de l'acquisition et de l'installation du système de protection antivirus.

Les annexes contiennent des informations techniques concernant les paramètres nécessaires à la configuration des composants antivirus, ils décrivent également la syntaxe et le contenu des commandes relatives à la gestion du logiciel.



Avant de prendre connaissance de ce Manuel, merci de vous assurer que vous lisez la dernière version du **Manuel Administrateur**. Ce manuel est constamment mis à jour, sa dernière version est disponible sur le site officiel de **Doctor Web** <http://download.drweb.com/esuite/>.





1.2. Légende et abréviations

Légende

Les symboles utilisés dans ce manuel sont présentés dans [le tableau 1-1](#).

Tableau 1-1. Légende

Symbole	Commentaire
 Notice	Une notice/indication importante.
 Attention	Un avertissement sur des erreurs éventuelles et sur les points auxquels faire attention.
Dr.Web ESS	Nom du produit/composant Dr.Web .
<i>Réseau antivirus</i>	Un terme ou un lien vers un terme.
<i><IP-address></i>	Les champs destinés à remplacer les noms fonctionnels par leurs valeurs.
Annuler	Les noms des boutons, fenêtres, éléments du menu et autres éléments de l'interface.
CTRL	Les touches du clavier.
C:\Windows\	Les noms de fichiers/dossiers ou fragments de programme.
Annexe A	Les liens croisés vers des chapitres de la documentation ou les hyperliens vers les ressources externes.

Abréviations

Dans le texte du Manuel les abréviations suivantes sont utilisées :

- ◆ ACL – listes de contrôle d'accès (Access Control List),



- ◆ DFS – système de fichiers distribué (Distributed File System),
- ◆ **Dr.Web ESS – Dr.Web Enterprise Security Suite**,
- ◆ GUI – Graphical User Interface (interface graphique utilisateur), la version du programme dotée des outils de GUI,
- ◆ NAP – Network Access Protection,
- ◆ UDS – UNIX Domain Socket (socket du domaine UNIX),
- ◆ BD, SGBD – base de données, système de gestion de base de données,
- ◆ **SGMAJ Dr.Web** — Système global de mises à jour **Dr.Web**,
- ◆ LAN – réseau local (Local Area Network),
- ◆ OS – système d'exploitation (operating system),
- ◆ EBNF – notation Backus-Naur étendue (Extended Backus-Naur form).

1.3. Composants, destination, fonctions principales de l'Antivirus Dr.Web Enterprise Security Suite

Le logiciel **Dr.Web ESS** est conçu pour la mise en oeuvre et la gestion centralisée d'une protection antivirus des ordinateurs à l'échelle de l'entreprise. Pour cela, il n'est pas indispensable de connecter les ordinateurs au réseau local, il suffit d'avoir un accès à Internet.

Dr.Web Enterprise Security Suite possède les fonctionnalités suivantes :

- ◆ installation centralisée (sans accès physique aux machines) des packages antivirus sur les postes à protéger,
- ◆ configuration centralisée des packages antivirus,
- ◆ mise à jour centralisée des bases virales et du logiciel sur les postes protégés,
- ◆ surveillance des événements viraux, du statut des packages antivirus et de l'état du système d'exploitation sur tous les postes protégés.



Dr.Web ESS permet de donner à l'utilisateur du poste protégé les droits nécessaires pour configurer et gérer le package antivirus sur le poste, il est également possible de contrôler ces droits de façon flexible voire de les restreindre ou de complètement les enlever.

Le réseau antivirus **Dr.Web ESS** repose sur une structure *client-serveur*. Les composants sont installés sur les postes des utilisateurs, administrateurs et sur le(s) poste(s) doté(s) des fonctionnalités de **Serveur Enterprise**. Ces composants échangent des informations via les protocoles réseau TCP/IP, IPX/SPX, NetBIOS. Un ensemble de postes sur lesquels les composants interagissants de **Dr.Web ESS** sont installés représente un *réseau antivirus*.

Le réseau antivirus comprend les composants suivants :

Composants principaux :

- ◆ *Dr.Web Enterprise Server (Serveur Enterprise)*. Ce composant est installé sur un poste dans le réseau antivirus. Il conserve les packages d'installation des packages antivirus appropriés aux systèmes d'exploitation installés sur les postes protégés, les mises à jour des bases virales ainsi que celles des packages antivirus et des **Enterprise Agent**. Il conserve également les clés utilisateurs et les configurations des packages pour les postes protégés. Selon les requêtes des **Enterprise Agent**, le Serveur envoie ces informations vers les postes. Le **Serveur Enterprise** effectue l'écriture dans le journal unique des événements survenants dans le réseau antivirus.
- ◆ *Centre de Gestion Dr.Web*. Ce composant s'installe automatiquement avec le **Serveur Enterprise**. Il assure la gestion à distance du réseau antivirus via le paramétrage du **Serveur Enterprise**, et à l'aide des configurations des postes protégés conservées sur le **Serveur Enterprise** ainsi que sur les postes.



- ◆ *Dr.Web Enterprise Agent (Agent Enterprise)*. Ce composant doit être installé sur le poste à protéger. Ensuite, il effectue l'installation du package antivirus sur le poste. Ultérieurement, **Enterprise Agent** assure les mises à jour régulières du logiciel antivirus, transmet les commandes et les paramètres provenant du **Serveur Enterprise** et renvoie au **Serveur Enterprise** les informations sur les événements viraux ainsi que d'autres informations sur le poste protégé.

Composants complémentaires :

- ◆ *Serveur-proxy*. Ce composant peut être optionnellement installé dans le réseau antivirus. L'objectif principal du **Serveur proxy** consiste à assurer la connexion entre le **Serveur Enterprise** et les **Enterprise Agents** dans le cas où la connexion directe devient impossible par exemple lorsque le **Serveur Enterprise** et les **Enterprise Agents** se trouvent dans des réseaux différents entre lesquels il n'y a pas de routage de packages. L'utilisation de la fonction de mise en cache peut réduire la bande passante réseau et la durée de téléchargement des mises à jour par les **Enterprise Agents**.
- ◆ *NAP Validator*. Ce composant permet d'utiliser la technologie *Microsoft Network Access Protection (NAP)* pour vérifier le fonctionnement du logiciel sur les postes protégés en conformité avec les politiques adoptées.



Le **Serveur Enterprise** peut être installé sur n'importe quel poste et non uniquement sur un poste utilisé en tant que serveur LAN. Pour les pré-requis respectifs de ce poste, consultez le paragraphe [Pré-requis système](#).

Le **Centre de Gestion** et le **Serveur** peuvent se trouver sur des postes différents. Il suffit d'avoir une connexion réseau entre eux.

Le réseau antivirus peut compter plusieurs **Serveurs Enterprise**. Pour en savoir plus sur une telle configuration, consultez le paragraphe [Particularités du réseau ayant plusieurs serveurs antivirus](#).



Le package antivirus Dr.Web installé sur les postes à protéger comprend les composants suivants :

Composants principaux :

- ◆ *Dr.Web Scanner pour Windows* est intégré dans le produit **Dr.Web pour Windows**. La configuration du scanner peut être paramétrée (via les paramètres de groupe ou avec les paramètres personnalisés du poste). Le scanner analyse le PC à la demande de l'utilisateur ou selon une planification locale de l'utilisateur. De plus, le scanner comprend un module assurant la protection contre les rootkit.
- ◆ *Dr.Web Enterprise Scanner pour Windows* est une fonction de **Enterprise Agent**. C'est aussi un scanner antivirus utilisant les mêmes bases virales et le même moteur. Mais cette fonctionnalité est implantée dans **Enterprise Agent**. **Dr.Web Enterprise Scanner pour Windows** est destiné à réaliser le scan antivirus sur demande : soit il démarre selon une planification, soit suite à la commande **Scanner** depuis le **Centre de Gestion Dr.Web**. Le scanner n'a pas d'interface spécialisée ni de paramètres à spécifier, tout est configuré via le **Centre de Gestion** au démarrage du **Scanner** (lors de la configuration du lancement selon la planification ou lors du lancement manuel).
- ◆ *Moniteur système SelfPROtect* assure la protection des fichiers et des dossiers de **Dr.Web ESS** contre une suppression non autorisée ou involontaire ainsi que contre une modification par l'utilisateur ou par un malware. Lorsque le moniteur est actif, seuls les programmes **Dr.Web** ont accès aux ressources listées ci-dessus.

Composants supplémentaires :

- ◆ *SpIDer Guard (moniteur de fichiers)* reste résident en mémoire et analyse à la volée tous les fichiers consultés se trouvant sur les supports amovibles ainsi que les fichiers ouverts en écriture sur les disques durs. De plus, le moniteur surveille les activités des processus lancés pouvant ressembler à une activité virale et en cas de détection d'une telle activité, il bloque les processus correspondants et notifie l'utilisateur.
- ◆ *SpIDer Mail (moniteur de courrier)* est aussi un composant



constamment présent en mémoire. Le composant intercepte toutes les requêtes de votre client de messagerie envoyées vers les serveurs de messagerie via les protocoles POP3/SMTP/IMAP4/NNTP et analyse les emails entrants/sortants avant leurs envoi/réception par le client de messagerie.

- ◆ *SpIDer Gate (Le gardien HTTP)* reste résident en mémoire de l'ordinateur et intercepte toutes les requêtes vers les sites web via le protocole HTTP. Le moniteur neutralise les menaces contenues dans le trafic HTTP (par exemple dans les fichiers reçus/envoyés), il bloque l'accès aux ressources suspectes ou incorrectes.
- ◆ *Dr.Web Office Control* est constamment présent en mémoire de l'ordinateur. Ce composant paramétré de façon appropriée gère l'accès aux ressources réseau ou aux ressources locales spécifiées. Notamment, il permet de contrôler l'accès aux sites web, en autorisant ou pas l'accès aux sites web spécifiés. Le composant permet non seulement de contrôler l'intégrité des fichiers importants, qu'il protège contre toute modification occasionnelle ou liée à une activité virale, mais il bloque aussi l'accès du personnel aux informations non sollicitées.
- ◆ *Le pare-feu Dr.Web FireWall* est destiné à protéger l'ordinateur contre tout accès non autorisé de l'extérieur ainsi que contre des fuites de données importantes via Internet. Le composant permet de contrôler la connexion et la transmission de données via Internet et de bloquer des connexions suspectes au niveau des paquets et des applications.

1.4. Avantages

- ◆ Le logiciel du serveur est indépendant de la plateforme et permet d'utiliser en tant que **Serveur Entreprise** un ordinateur tournant sous Microsoft® Windows® ainsi que sous les OS de la famille UNIX® ;
- ◆ Le logiciel de l'**Agent** est indépendant de la plate-forme et permet d'assurer une protection antivirus des ordinateurs tournant sous Microsoft Windows, Android, Microsoft® Windows Mobile® et Novell® NetWare®, les OS de la famille UNIX, et Mac OS X ;



- ◆ Protection antivirus de la messagerie Microsoft® Outlook®, ainsi que des messageries basées sur le serveur IBM Lotus Domino ou sur Microsoft Exchange Server ;
- ◆ Optimisation de l'utilisation de la bande passante dans les réseaux locaux via les protocoles TCP/IP, IPX et NetBIOS avec une possibilité d'appliquer des algorithmes spéciaux de compression ;
- ◆ Possibilité d'encryptage des données lors des échanges entre les composants du système ;
- ◆ Facilité de gestion des postes dans le réseau antivirus, assurée par un mécanisme de groupement ;
- ◆ Possibilité de gérer la protection antivirus (via le **Centre de Gestion Dr.Web**) depuis tout poste sous n'importe quel OS ;
- ◆ Possibilité d'installation et de suppression distantes des composants du package par l'administrateur système via le **Centre de Gestion** ;
- ◆ Installation centralisée des **Enterprise Agent** (avec une possibilité de configurer le logiciel des **Agents Enterprise** sur le **Serveur Enterprise** avant l'installation sur les postes client) ;
- ◆ Possibilité d'utiliser un filtre antispam sur le poste antivirus (à condition que cette option soit autorisée par la licence) ;
- ◆ Rapidité et efficacité de la répartition des mises à jour des bases virales et des modules par le **Serveur** vers les postes protégés ;
- ◆ Fonction de sauvegarde (backup) des données critiques du **Serveur** (les bases de données, fichiers de configuration etc.).



A la différence d'autres produits antivirus, l'**Antivirus Dr.Web ESS** peut être installé même sur des machines infectées.



1.5. Pré-requis système

Pour l'installation et le fonctionnement, Dr.Web ESS requiert :

- ◆ l'ordinateur sur lequel le **Serveur Enterprise** est installé doit avoir un accès à Internet pour télécharger de façon automatique les mises à jour depuis les serveurs de **SGMAJ** (Système global de mise à jour) **Dr.Web** ;
- ◆ les ordinateurs se trouvant dans le réseau antivirus doivent avoir un accès à Internet afin de se connecter au **Serveur Enterprise** ou au **serveur proxy** sinon il est nécessaire qu'ils se trouvent dans le même réseau local ;
- ◆ pour assurer l'interaction des composants antivirus, tous les ports et socket respectifs doivent être ouverts sur les machines utilisées :

Numéro	Protocole	Utilisation
ports 2193, 2371	TCP, UDP	Pour la connexion des composants antivirus au Serveur
socket 2371	IPX/SPX	Pour la connexion des composants antivirus au Serveur
ports 2193, 2372	UDP	Pour le fonctionnement du <u>Scanner réseau</u>
ports 139, 445	TCP, UDP	Pour le fonctionnement de l' Installateur réseau
port 9080	http	Pour le fonctionnement du <u>Centre de Gestion Dr.Web</u>
port 9081	https	Pour le fonctionnement du <u>Centre de Gestion Dr.Web</u>



Le port 2371 est nécessaire pour la connexion (via les protocoles TCP et UDP) avec les composants en version **4.XX**. Il est notamment utilisé pour assurer la compatibilité lors des mises à jour des composants du réseau antivirus.

Le fonctionnement de Dr.Web Enterprise Server requiert :

- ◆ un processeur Intel® Pentium® III 667 MHz ou supérieur,
- ◆ RAM 512 Mo (1 Go en cas d'utilisation de la BD interne),
- ◆ Espace disque jusqu'à 12 Go : 8 Go maximum pour la base de donnée interne (répertoire d'installation) et jusqu'à 4 Go maximum dans le répertoire système temporaire (pour les fichiers de travail),



Lors de l'installation du **Serveur**, il est requis (quel que soit l'emplacement d'installation du **Serveur**) au moins 2,5 Go de mémoire libre pour le package d'installation complet ou 650 Mo pour le package allégé – afin de démarrer l'installateur et d'extraire les fichiers temporaires.

- ◆ Windows 2000 ou supérieur, Linux®, FreeBSD® ou Solaris™ (voir [Annexe A. Liste complète des systèmes d'exploitation supportés](#)),
- ◆ pour l'installation du **Serveur Enterprise** sous UNIX, les bibliothèques suivantes sont requises : libiconv en version 1.8.2 ou supérieure, pcre, ncurses, openssl, libcrypto et libssl (les bibliothèques partagées, normalement, elles font partie de openssl), libxml2, libpq (uniquement pour l'utilisation avec la base **PostgreSQL** ; en cas d'installation avec les packages génériques, la bibliothèque est déjà incluse dans les packages), libcurl en version 7.20.0 ou supérieure, libldap.

Le serveur proxy requiert :

- ◆ un processeur Intel Pentium III 667 MHz ou supérieur,
- ◆ au minimum 512 Mo de RAM,
- ◆ espace du disque dur : 1 Go au minimum,
- ◆ OS Windows 2000 ou supérieur, Linux, FreeBSD ou Solaris



(comme pour **Enterprise Server**, voir [Annexe A. Liste complète des systèmes d'exploitation supportés](#)),

- ◆ pour l'installation du **Serveur Enterprise** sous UNIX, les bibliothèques suivantes sont requises : `libcconv` en version 1.8.2 ou supérieure, `pcrc`, `libxml2`.



La bibliothèque `libcconv` est disponible en téléchargement depuis le serveur <ftp://ftp.freebsd.org>.

Pré-requis pour NAP :

Pour le serveur :

- ◆ Windows Server 2008.

Pour les agents :

- ◆ Windows XP SP3, Windows Vista, Windows Server 2008.

Le Centre de Gestion Dr.Webrequiert :

- ◆ Un navigateur web Windows® Internet Explorer® 7 ou supérieur ou bien un navigateur web Mozilla® Firefox® 3.0 ou supérieur.



Il est également possible d'utiliser les navigateurs web Opera® 10 ou supérieur, Safari® 4 ou supérieur, Chrome® 7 ou supérieur. Cependant, dans ces cas-là, le fonctionnement correct n'est pas garanti.

En cas d'installation du **Serveur** sur l'ordinateur dont le nom contient le symbole "_" (trait de soulignement), il sera impossible de travailler avec le **Serveur** via le **Centre de Gestion** dans le navigateur Windows Internet Explorer.

Dans ce cas là, veuillez utiliser un autre navigateur web.

Pour le bon fonctionnement du **Centre de Gestion Dr.Web** sous navigateur Web Windows Internet Explorer, l'adresse IP et/ou le nom DNS de l'ordinateur sur lequel est installé le **Serveur Enterprise** doivent être ajoutés aux sites de confiance du navigateur dans lequel est ouvert le **Centre de Gestion Dr.Web**.



Pour ouvrir correctement le **Centre de Gestion** depuis le menu **Démarrer**, si vous utilisez le navigateur Web Windows Internet Explorer sous Windows 8 et l'OS Windows Server 2012 avec une interface en mosaïque, il est nécessaire de définir les paramètres de navigateur Web suivants : **Options Internet** → **Programmes** → **Ouvrez Internet Explorer**, activer la case **Toujours dans Internet Explorer en version classique**.

- ◆ Un module ajoutable **Dr.Web Browser-Plugin** assurant le fonctionnement du **Centre de Gestion**. Le module est fourni avec le package d'installation du **Serveur** et s'installe selon une requête du navigateur lorsque les éléments du **Centre de Gestion** le demandent (ou lors de l'installation distante des composants antivirus en cas de **Scanner réseau**).



Pour assurer le fonctionnement du module ajoutable **Dr.Web Browser-Plugin** sur la page du **Scanner réseau** sous Windows ainsi que sous les OS de la famille GNU/Linux, les droits d'administrateur (root) sont requis.

Lors de l'utilisation du navigateur web Safari, le module ajoutable **Dr.Web Browser-Plugin** n'est disponible que sous les versions opérant sous Windows.

En cas d'utilisation des navigateurs web Mozilla Firefox, Opera et Chrome, le module ajoutable **Dr.Web Browser-Plugin** est disponible uniquement pour leurs versions tournant sous OS Windows ou sous OS de la famille Linux.

- ◆ La résolution de l'écran recommandée pour l'utilisation du **Centre de Gestion** est de 1280x1024 pt.

Le fonctionnement de Dr.Web Enterprise Agent et du package antivirus requiert :

1. Pré-requis minimum :
 - ◆ un processeur Intel Pentium IV, 1.6 GHz ;
 - ◆ RAM 512 Mo.
2. Pré-requis recommandés :



- ◆ un processeur Intel Pentium IV, 2.4 GHz ou supérieur ;
 - ◆ RAM au moins 1 Go.
3. Espace libre sur le disque dur : au moins 250 Mo pour les exécutables + de l'espace pour les fichiers de log et les fichiers temporaires ;
4. Systèmes d'exploitation (voir [Annexe A. Liste complète des OS supportés](#)) :
- a) Windows 98, Windows Me, Windows NT4 (SP6) ou supérieur. Selon le système d'exploitation, les composants suivants peuvent être installés :

Composant	OS
SpIDer Gate, SelfPROtect, Office Control, Dr.Web Plug-in pour Outlook	Windows 2000 avec SP4 et supérieur.
SpIDer Guard NT4, Dr.Web Scanner NT4	<ul style="list-style-type: none">• Windows 98,• Windows ME,• Windows NT4 (SP6a),• Windows 2000 avec SP4, sans Update Rollup1,• Windows XP sans SP ainsi qu'avec SP1,• Windows 2003 sans SP.
FireWall, SpIDer Guard G3, Dr.Web Scanner	<ul style="list-style-type: none">• Windows 2000 avec SP4 et Update Rollup1,• Windows XP avec SP2 et supérieur,• Windows 2003 avec SP1 et supérieur,• Windows Vista et supérieur.
SpIDer Mail NT4	<ul style="list-style-type: none">• Windows 98,• Windows NT4 avec SP6a.



Composant	OS
SpIDer Mail	tous les OS supportés supérieurs aux OS listés ci-dessus pour la version SpIDer Mail NT4 .

- b) Microsoft Windows Mobile ;
 - c) Novell NetWare ;
 - d) OS de la famille UNIX : Linux, FreeBSD, Solaris ;
 - e) Android ;
 - f) Mac OS X.
5. Le module ajoutable **Dr.Web pour Outlook** requiert l'installation d'un client Microsoft Outlook du package MS Office :
- ◆ Outlook 2000 (Outlook 9),
 - ◆ Outlook 2002 (Outlook 10 ou Outlook XP),
 - ◆ Office Outlook 2003 (Outlook 11),
 - ◆ Office Outlook 2007,
 - ◆ Office Outlook 2010.
6. Le fonctionnement de la rubrique d'aide contextuelle **Dr.Web Agent pour Windows** requiert Windows® Internet Explorer® 6.0 ou supérieur.



Aucun autre logiciel antivirus y compris d'autres versions de **Dr.Web** ne doivent être installés sur les postes dans le réseau antivirus géré par **Dr.Web**.



Les fonctions de l'**Agent** sous OS Windows Mobile et Novell NetWare sont décrites dans les manuels respectifs **Dr.Web Agent pour Windows Mobile** et **Dr.Web Agent pour Novell NetWare**.



1.6. Composition du package d'installation

Le package d'installation de Dr.Web Enterprise Security Suite peut être fourni en deux variantes en fonction de l'OS du Serveur Enterprise sélectionné :

1. Pour installer sous OS UNIX – sous forme de fichiers archivés au format `bzip2` ou en packages d'installation pour les OS respectifs destinés à l'installation des composants suivants :
 - ◆ **Dr.Web Enterprise Server,**
 - ◆ **Serveur proxy.**
2. Pour installer sous OS Windows — sous forme de fichiers exécutables de l'assistant d'installation destinés à l'installation des composants suivants :
 - ◆ **Dr.Web Enterprise Server,**
 - ◆ **Serveur proxy,**
 - ◆ **Dr.Web Enterprise Agent** pour Active Directory,
 - ◆ **NAP Validator.**

Les deux types de package d'installation d'EnterpriseServer peuvent être fournis :

1. *Package d'installation complet* – contient des packages d'installation de tous les produits fournis pour installer sur les postes protégés et correspondant à tous les OS supportés.
2. *Package d'installation allégé* – un package d'installation dont la composition est pareille aux packages en versions précédentes de **Dr.Web Enterprise Security Suite**.

Ce package peut être utilisé pour l'installation de la protection antivirus gérée par **Dr.Web Enterprise Security Suite** uniquement sur les postes tournant sous OS Windows.

Le package d'installation d'Enterprise Server contient les composants suivants :

- ◆ Logiciel du **Serveur Enterprise** pour l'OS respectif,



- ◆ Logiciel des **Dr.Web Enterprise Agent** et des packages antivirus pour les OS supportés,
- ◆ Logiciel du **Centre de Gestion Dr.Web**,
- ◆ base virales,
- ◆ documentation, modèles, exemples.

Outre le package d'installation, les numéros de série seront également fournis. Après les avoir enregistrés, vous recevrez les fichiers contenant la clé serveur et la clé pour les postes de travail.

1.7. Fichiers clés

Les droits de l'utilisateur relatifs à l'utilisation de l'antivirus sont déterminés par les fichiers clés suivants.

1. Fichier clé pour le **Serveur** - `enterprise.key`.
2. Fichier clé pour les postes de travail - `agent.key`.



Le fichier clé est protégé contre l'édition avec un mécanisme de signature numérique. Toute modification de ce fichier le rend invalide. Afin d'éviter tout endommagement involontaire du fichier clé, il ne faut pas le modifier ni l'enregistrer à la fermeture de l'éditeur de texte.

Le jeu de composants et le prix de la licence pour **Dr.Web ESS** est fonction du nombre de postes protégés dans le réseau (y compris les serveurs se trouvant dans le réseau **Dr.Web ESS** et qui tournent comme postes protégés).



Il est nécessaire de fournir cette information à votre revendeur lors de l'achat de la licence **Dr.Web ESS**. Veuillez spécifier également le nombre de **Serveurs Enterprise** nécessaires pour déployer le réseau antivirus. Le nombre de **Serveurs Enterprise** utilisés séparément (sans interaction entre eux) n'a pas d'impact sur le prix de la licence (voir aussi le p. [Planification de la structure du réseau antivirus](#)).



Merci de prendre en compte qu'en cas de création du réseau antivirus avec plusieurs **Serveurs** (voir le p. [Particularité du réseau ayant plusieurs serveurs](#)), lors du calcul du nombre de postes protégés, il est nécessaire de prendre en compte les connexions entre les **Serveurs Entreprise** puisque de telles connexions doivent être autorisées par une licence supplémentaire. Dans ce cas, pour chaque **Serveur Entreprise**, toute connexion avec un autre serveur doit être couverte par une licence, quel que soit le type de connexion (voir le paragraphe [Architecture réseau ayant plusieurs serveurs antivirus](#)), par exemple, en cas de connexion entre deux serveurs, pour chaque serveur il faut avoir une licence autorisant la connexion entre serveurs.

Les fichiers clé de licence peuvent être fournis lors de l'achat de l'antivirus **Dr.Web ESS** en option. En général, seuls les numéros de série sont fournis.

Les fichiers clé de licence sont envoyés aux utilisateurs par email après l'enregistrement du numéro de série sur le site web dédié (<http://buy.drweb.com/register/>, si une autre adresse web n'est pas spécifiée dans la fiche produit). Veuillez visiter ce site pour remplir un formulaire où vous devez spécifier quelques informations personnelles et saisir dans le champ approprié le numéro de série (vous le trouverez dans votre fiche produit). Le fichier archivé contenant vos fichiers clé vous sera envoyé à l'adresse que vous avez spécifiée. Vous pouvez également le télécharger depuis le site mentionné ci-dessus.

Les fichiers clé sont fournis sous forme d'archive zip contenant les fichiers clés pour le **Serveur** et pour les postes de travail.

L'utilisateur peut recevoir les fichiers clés par un des moyens suivants :

- ◆ par email (après la procédure d'enregistrement sur le site web décrite ci-dessus) ;
- ◆ avec le package d'installation du produit, si les fichiers clés ont été spécifiés parmi les composants lors de l'achat du produit ;
- ◆ sur un support séparé sous forme de fichier.



Il est recommandé de conserver le fichier clé de licence pendant la durée de validité de la licence, vous pouvez l'utiliser en cas de réinstallation ou restauration des composants de l'antivirus. En cas de perte du fichier clé, vous pouvez repasser la procédure d'enregistrement sur le site et recevoir le fichier clé. Dans ce cas, il est nécessaire de spécifier le même numéro de série et les mêmes informations sur l'utilisateur que vous avez soumis lors du premier enregistrement ; seule l'adresse email peut être modifiée. Si c'est le cas, le fichier clé sera envoyé à la nouvelle adresse email.

Pour tester l'antivirus, vous pouvez utiliser les fichiers clé de démonstration. Les fichiers clés de démo fournissent les fonctionnalités complètes des composants antivirus, mais leur durée de validité est limitée. Pour obtenir des fichiers clés de démo, vous devez remplir un formulaire se trouvant sur la page suivante <http://download.drweb.com/demo/>. Votre demande sera traitée à titre individuel. En cas de réponse positive, une archive contenant les fichiers clés vous sera envoyée à l'adresse spécifiée.

L'utilisation des fichiers clés lors de l'installation du programme est décrite dans le paragraphe [Installation de Dr.Web Enterprise Server](#).

L'utilisation des fichiers clés dans le cas où le logiciel est déjà installé est décrite dans le paragraphe [Mise à jour de la clé serveur et de la clé pour les postes de travail](#).



Chapitre 2. Installation et suppression des composants de Dr.Web Enterprise Security Suite

2.1. Création d'un réseau antivirus

La marche à suivre pour créer un réseau antivirus :

1. Rédigez un plan de la structure du réseau antivirus. Le plan doit comprendre tous les postes protégés parmi lesquels il faut déterminer ceux qui vont servir de **Serveur Enterprise**.
2. Installer le logiciel de **Serveur Enterprise** (avec lequel le **Centre de Gestion Dr.Web** sera installé) sur le(s) poste(s) sélectionné(s).
3. Mettre à jour le dépôt des produits depuis le **Centre de Gestion**.
4. Configurer le logiciel des postes de travail et du **Serveur (des Serveurs)**.
5. Si nécessaire, installer et configurer le **Serveur proxy**.
6. Installer le logiciel d'**Enterprise Agent** sur les postes les postes de travail.



Une fois installés sur les postes, les **Agents** se connectent automatiquement au **Serveur**. L'approbation des postes antivirus sur le **Serveur** est effectuée selon la politique que vous sélectionnez (voir [Politique de connexion des postes](#)).

7. Depuis le **Centre de Gestion**, configurer et démarrer les modules nécessaires.

Au stade de la planification de la structure du réseau antivirus, il faut choisir en premier lieu un poste qui sera utilisé en tant que **Serveur Enterprise**.



Serveur Enterprise peut être installé sur n'importe quel ordinateur et pas uniquement sur une machine utilisée comme serveur LAN. Pour en savoir plus sur les pré-requis de cet ordinateur, consultez le paragraphe [Pré-requis système](#).

Le **Centre de Gestion** et le **Serveur** peuvent se trouver sur des machines différentes. Il suffit d'avoir une connexion réseau entre eux.

Le réseau antivirus peut comprendre plusieurs **Serveur Enterprise**. Les particularités d'une telle configuration sont décrites dans le paragraphe [Particularités du réseau avec plusieurs Serveurs](#).

Pour installer **Serveur Enterprise** et **Enterprise Agent** une procédure d'accès unitaire aux ordinateurs respectifs sera requise (accès physique ou via des outils de gestion à distance permettant de lancer et de contrôler les programmes). Toutes les opérations ultérieures seront effectuées depuis le poste de l'administrateur du réseau antivirus (voire de l'extérieur du réseau local) et ne nécessitent aucun accès aux **Serveurs Enterprise** ni aux postes de travail.

2.2. Installation Dr.Web Enterprise Server

L'installation de **Serveur Enterprise** est la première étape du déploiement du réseau antivirus. Aucun autre composant du réseau antivirus ne peut être installé avant que l'installation du serveur ne soit réussie.

La procédure d'installation de **Serveur Enterprise** est fonction de la version du **Serveur** (pour Windows ou pour UNIX) à installer. D'ailleurs, le jeu de paramètres à configurer lors de l'installation ainsi que la structure du logiciel à installer sont les mêmes.



Tous les paramètres configurés lors de l'installation peuvent être modifiés ultérieurement par l'administrateur du réseau antivirus pendant le fonctionnement du **Serveur**.

Si le logiciel du **Serveur** est déjà installé, consultez les paragraphes [Mise à jour de Dr.Web ESS pour OS Windows®](#) ou [Mise à jour de Dr.Web ESS pour OS de la famille UNIX®](#).



Dans le cas où la suppression du **Serveur** a précédé l'installation du logiciel du **Serveur**, le contenu du dépôt des produits sera supprimé et une nouvelle version du dépôt sera installée. Si pour une raison quelconque le dépôt des produits de la version précédente a été conservé, il sera nécessaire de supprimer manuellement tout son contenu avant l'installation d'une nouvelle version du **Serveur**. Après l'installation du **Serveur**, il faut effectuer une mise à jour complète du dépôt des produits.

La langue du nom du dossier dans lequel le **Serveur** est installé doit correspondre à la langue spécifiée dans la rubrique Langue pour les programmes non unicode du système Windows.

Sinon le **Serveur** ne sera pas installé, excepté le cas où l'anglais est utilisé pour le nom du dossier d'installation.

Le **Centre de Gestion Dr.Web** s'installe automatiquement avec **Serveur Enterprise**, il sert à gérer le réseau antivirus et la configuration du **Serveur**.

Par défaut, **Serveur Enterprise** démarre de manière automatique après la fin de l'installation (sous UNIX, ceci est spécifié dans les paramètres de l'installateur).



2.2.1. Installation de Dr.Web Enterprise Server sous Windows®

Ci-après vous trouverez la description de la procédure d'installation de **Serveur Enterprise** sous Windows. La marche à suivre peut varier en fonction des versions du package d'installation.

Avant l'installation de Dr.Web Enterprise Server, il est recommandé de prendre en compte les informations ci-dessous :



Dans le cas où les services **Terminal Services** sont installés dans le système Windows, vous devez installer le logiciel avec l'assistant **Ajout et suppression de programmes** depuis le **Panneau de configuration** Windows.

Le fichier de package d'installation et d'autres fichiers requis lors de l'installation doivent se trouver sur les disques locaux du poste sur lequel le logiciel du **Serveur** sera installé. Les droits d'accès doivent être paramétrés de sorte que ces fichiers soient accessibles à l'utilisateur **LOCALSYSTEM**.

L'installation de **Serveur Enterprise** doit être effectuée en mode administrateur.



Après l'installation de **Serveur Enterprise**, une mise à jour de tous les composants de **Dr.Web ESS** sera requise (voir [Mise à jour manuelle des composants de Dr.Web ESS](#)).

En cas d'utilisation de la BD externe, il faut d'abord créer une BD et paramétrer ensuite le pilote respectif (voir [Annexe B. Paramètres requis pour le SGBD. Paramètres des pilotes de SGBD](#)).

La [Fig. 2-1](#). présente un organigramme de la procédure d'installation de **Serveur Enterprise** avec l'installateur. La description détaillée [ci-dessous](#) correspond aux étapes de la procédure.

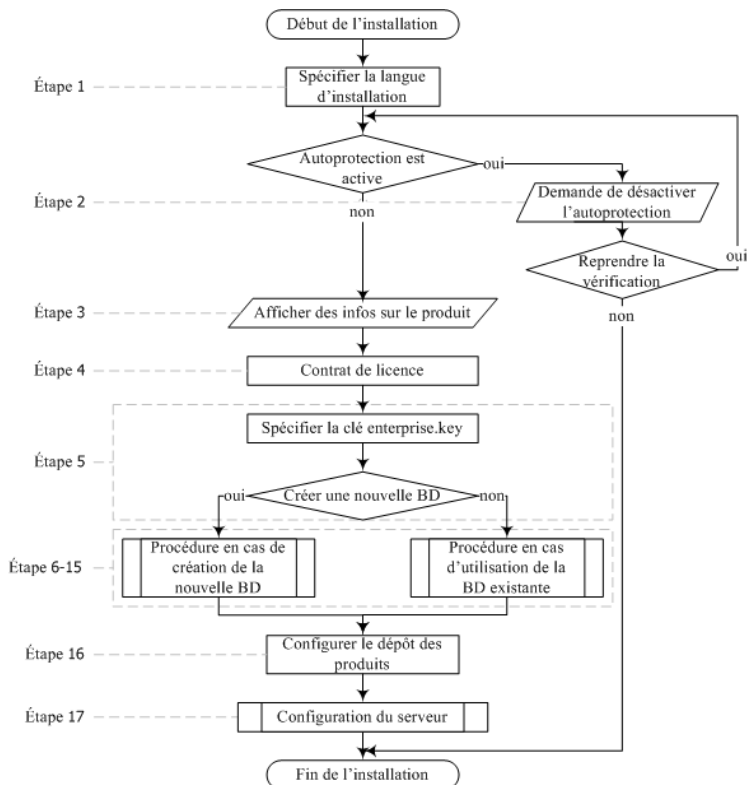


Fig. 2-1. Schéma de la procédure d'installation de Dr.Web Enterprise Server (Cliquez sur un élément de l'organigramme pour consulter la description)

L'organigramme comprend trois procédures intégrées. La procédure **Installation du Serveur** (étape 17) ne nécessite aucune intervention de l'utilisateur (voir l'explication [ci-dessous](#)) et elle est effectuée directement par l'installateur.

Les organigrammes des procédures relatives à la **création d'une nouvelle BD** et à **l'utilisation de la BD existante** sont présentés sur les [Fig. 2-2.](#) et [Fig. 2-3.](#)

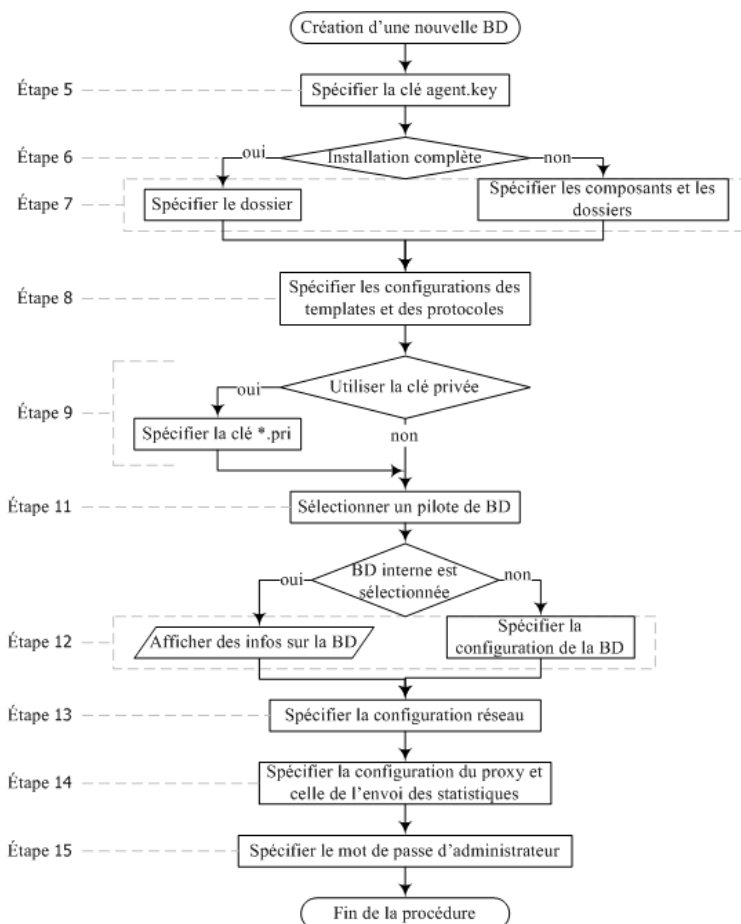


Fig. 2-2. Schéma de la procédure d'installation lors en cas de création d'une nouvelle BD (Cliquez sur un élément de l'organigramme pour consulter la description)

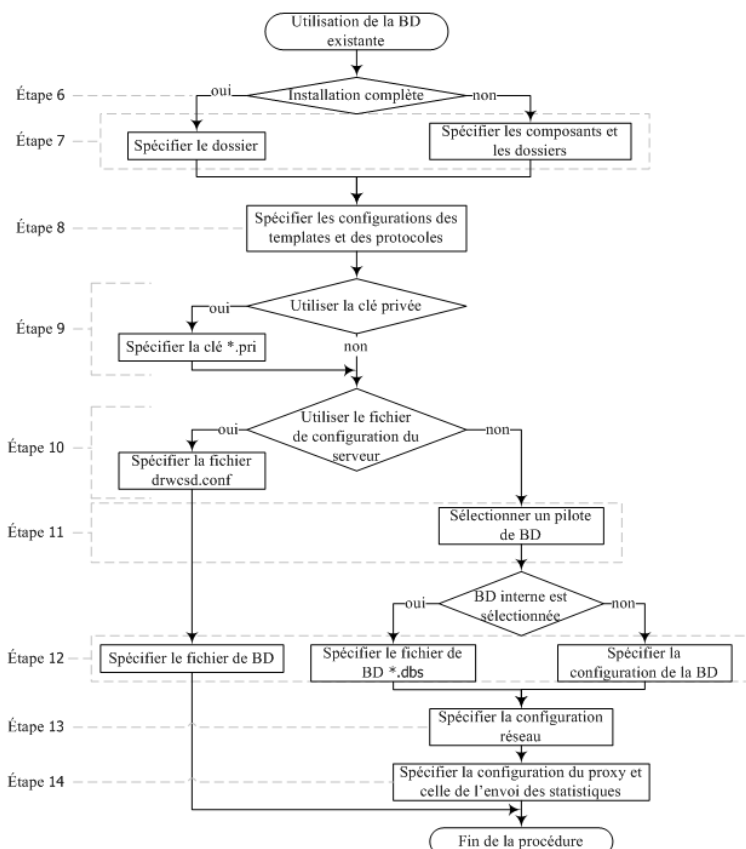


Fig. 2-3. Schéma de la procédure d'installation de Dr.Web Enterprise Server en cas d'utilisation de la BD existante(Cliquez sur un élément de l'organigramme pour consulter la description)

La marche à suivre pour installer Dr.Web Enterprise Server sur l'ordinateur sous Windows :

1. Lancez le fichier de package d'installation. Dans la fenêtre qui apparaît, sélectionnez la langue à utiliser lors de l'installation. Sélectionnez **Français** et cliquez ensuite sur le bouton **Suivant**.
2. Si **Enterprise Agent** avec la fonction d'autoprotection active



tourne sur le poste sur lequel se trouve **Serveur Enterprise**, un message informant sur l'activité de l'autoprotection **Dr.Web** sera affiché. Désactivez ce composant via les paramètres de l'**Agent** et cliquez ensuite sur **OK** pour continuer la procédure ou sur le bouton **Annuler** - pour refuser l'installation du **Serveur**.

3. La fenêtre de l'assistant **InstallShield Wizard** apparaît et affiche des informations sur le produit à installer. Cliquez ensuite sur le bouton **Suivant**.
4. La fenêtre affichant le texte du Contrat de licence va s'ouvrir. Après avoir pris connaissance des termes du Contrat de licence, cochez la case se trouvant en bas de la fenêtre **J'accepte les termes du Contrat de licence** et cliquez ensuite sur le bouton **Suivant**.
5. La fenêtre permettant de sélectionner les fichiers clés de licence apparaîtra.

Cliquez sur le bouton **Parcourir** se trouvant contre le champ **Clé de Dr.Web Enterprise Server**, puis dans la fenêtre standard de Windows, spécifiez l'emplacement du fichier clé de licence du **Serveur** - `enterprise.key`.

En cas de première installation du **Serveur**, sélectionnez l'option **Initialiser une nouvelle base de données** et dans la rubrique **Initialiser la base avec la clé de licence de Dr.Web Enterprise Agent**, spécifiez le fichier clé agent (`agent.key`).

Si vous souhaitez garder la base de données du **Serveur** relative à l'installation précédente, sélectionnez l'option **utiliser la base de données existante**. Vous pouvez spécifier le fichier de la base de données ultérieurement (voir étape **10**).

Pour tester le produit, utilisez les fichiers clés de démonstration. Cliquez sur le bouton **Clés démo** pour visiter le site web de **Doctor Web** et obtenir les fichiers clés démo (voir [Fichiers clés de démonstration](#)).

Cliquez sur le bouton **Suivant**.

6. La fenêtre de sélection des types d'installation apparaîtra. Si la



case **Installation standard** est cochée, tous les composants de **Serveur Enterprise** seront installés. L'option **Installation personnalisée** vous permet de spécifier les composants à installer. Après avoir choisi un type d'installation, cliquez sur **Suivant**.



Si vous souhaitez utiliser ODBC pour Oracle en tant que base de données externe, sélectionnez l'option **Installation personnalisée** et dans la fenêtre qui apparaît, annulez l'installation du client implanté pour SGBD Oracle (dans la rubrique **Support de la Base de données - Driver de la BD Oracle**).

Sinon le fonctionnement de la BD Oracle sera perturbé par un conflit des bibliothèques.

7. Si lors de l'étape précédente, l'**Installation standard** a été sélectionnée, la fenêtre de sélection du dossier d'installation s'affichera. Si nécessaire, vous pouvez modifier le dossier spécifié par défaut. Pour cela, cliquez sur le bouton **Modifier** et sélectionnez ensuite un dossier d'installation. Cliquez sur le bouton **Suivant** pour continuer.

Si lors de l'étape précédente, l'option **Installation personnalisée** a été choisie, la fenêtre vous proposant de sélectionner des composants à installer et les dossiers appropriés à chacun d'entre eux s'ouvrira. Le menu contextuel des composants vous permet de modifier le mode d'installation : installer le composant sur un poste local ou via le réseau (dans certains cas l'option est indisponible) ou annuler l'installation du composant. Pour changer le dossier d'installation du composant sélectionné, cliquez sur le bouton **Modifier** et spécifiez un dossier d'installation, puis cliquez sur **Suivant**.

8. La fenêtre suivante vous offre la possibilité de choisir une langue pour les templates de messages. Là, vous pouvez également paramétrer le mode d'utilisation et le nom pour la ressource système partagée destinée au dossier d'installation de l'**Agent** (par défaut, un nom caché de ressource partagée est spécifié) ainsi que configurer les paramètres d'écriture dans le fichier de log.

Si après l'installation vous souhaitez démarrer le **Serveur** de



manière automatique, cochez la case **Enregistrer et lancer le service lors du setup**.

Pour ajouter le **Serveur** dans les exclusions du pare-feu de l'OS (sauf Windows 2000), cochez la case **Ajouter les ports et interfaces serveur aux exclusions de pare-feu**.

9. En cas de première installation du **Serveur**, cliquez sur le bouton **Suivant** dans la fenêtre. Les clés de chiffrement seront générées automatiquement durant l'installation.

Si vous installez le **Serveur** pour un réseau déjà existant, cochez la case **Installation des clés d'encryptage existantes**. Dès que vous spécifiez le fichier de clé privée, un fichier de clé publique sera créé (le contenu de la clé publique sera le même que dans la clé publique antérieure). Ceci permet aux **Agents** de reconnaître le **Serveur** installé. Sinon vous devez copier la nouvelle clé publique de chiffrement vers tous les postes sur lesquels les **Enterprise Agent** ont été installés.

10. Si lors de l'étape **4** vous avez choisi la base de données existante, une boîte de dialogue s'affichera pour vous permettre de pointer sur le fichier de configuration du **Serveur** préformé.

La série de boîtes de dialogue suivantes spécifie les paramètres principaux sauvegardés dans le fichier de configuration du **Serveur** (voir [Annexe G1. Fichier de configuration de Dr.Web Enterprise Server](#)).

11. La fenêtre de configuration de la base de données permet de configurer les paramètres de la base utilisée. Ces paramètres sont fonction du choix du type de base de données effectué à l'étape **4** et ils dépendent aussi du fichier de configuration du **Serveur** spécifié à l'étape **9**.

En cas de création d'une nouvelle BD ou dans le cas où le fichier de configuration du **Serveur** (pour la base existante) n'a pas été spécifié, il vous faut pointer sur le driver à utiliser. L'option **Driver de la BD IntDB** active l'utilisation des outils intégrés de **Serveur Enterprise**. D'autres options correspondent à l'utilisation des bases externes respectives. La configuration du SGBD est décrite dans les Annexes (voir [Annexe B](#)).



Configurations requises en cas d'utilisation de SGBD. Paramètres des drivers de SGBD).

Cliquez ensuite sur le bouton **Suivant**.

12. Si l'option **Driver de la BD IntDB** a été sélectionnée au stade précédent, la fenêtre suivante affichera des informations sur une nouvelle base de données créée.

Si en cas d'utilisation de la BD existante, vous avez pointé sur le fichier de configuration du **Serveur** ou avez sélectionné l'élément **Driver de la BD IntDB** lors de l'étape précédente, vous devez spécifier le fichier de BD dans la fenêtre suivante. Pour cela, cliquez sur le bouton **Parcourir**. Cochez la case **Lancer le scan de la base interne durant l'installation** pour vérifier l'intégrité de la BD lors de l'installation du **Serveur**.

Si une des variantes correspondantes aux BD externes a été sélectionnée, la fenêtre qui apparaît vous proposera de spécifier les paramètres d'accès à la BD.

13. Si lors de l'étape **4** vous avez choisi l'initialisation d'une nouvelle BD ou à l'étape **9** vous n'avez pas spécifié le fichier de configuration du **Serveur** de l'installation précédente (pour la BD existante), la fenêtre de configuration réseau s'affichera. Cette fenêtre vous permet de configurer le protocole réseau pour le **Serveur** (un seul protocole réseau peut être spécifié, des protocoles supplémentaires peuvent être paramétrés plus tard).

Dans les champs **Interface** et **Port**, spécifiez les valeurs correspondantes pour l'accès au **Serveur**. Par défaut, l'interface suivante est définie 0.0.0.0, ce qui signifie que l'accès au **Serveur** est possible via toutes les interfaces.



Le port 2193 est utilisé par défaut, cependant le port 2371 est également supporté pour assurer la compatibilité avec les antivirus des versions antérieures.

Pour restreindre l'accès local au **Serveur**, cochez la case **Accès limité au Serveur Dr.Web Enterprise**. Ainsi l'accès sera



interdit à l'installateur, aux **Agents** et aux autres **Serveurs** (en cas de réseau antivirus existant créé avec **Dr.Web Enterprise Security Suite**). Vous pouvez modifier ces paramètres ultérieurement depuis le menu **Administration** du **Centre de Gestion**, l'élément **Configuration de Dr.Web Enterprise Server**, onglet **Modules**.

Cochez la case **Service de détection de serveur** si vous souhaitez que le **Serveur** réponde aux requêtes de recherche multicast ou broadcast de la part des autres **Serveurs**.

Pour spécifier la configuration réseau par défaut, cliquez sur le bouton **Standard**. Pour limiter le fonctionnement du **Serveur** par l'interface réseau locale – 127.0.0.1 – cliquez sur le bouton **Restreindre**. Cette configuration permet de contrôler le Serveur uniquement via le **Centre de Gestion** lancé sur le même poste, de plus, seul l'**Agent** lancé sur le même poste peut se connecter au Serveur. Dès que le réglage des paramètres du **Serveur** est achevé, vous pouvez modifier les paramètres réseau.

Cliquez ensuite sur le bouton **Suivant**.

14. Si vous avez choisi l'initialisation d'une nouvelle BD à l'étape 4 ou si le fichier de configuration du **Serveur** de l'installation précédente n'a pas été spécifié lors de l'étape 9 (pour la BD existante), une requête d'envoi des statistiques sur les événements viraux à **Doctor Web** s'affiche. Pour cela, cochez la case **Autoriser l'envoi des statistiques** et remplissez les champs respectifs. Dans le champ **Serveur** de statistiques, saisissez – `stat.drweb.com`, dans le champ **URL**, `\update`. Vous pouvez remplir également les champs **Nom d'utilisateur** et **Mot de passe** si les statistiques envoyées nécessitent une authentification (vous pouvez obtenir le nom d'utilisateur et le mot de passe auprès du **Service Support technique Doctor Web**). Dans le champ **Envoyer chaque**, entrez un espacement d'envoi en minutes. Seuls les deux champs sont obligatoires à remplir : l'adresse du serveur de statistiques et l'espacement d'envoi.

En cas d'utilisation d'un serveur proxy, vous pouvez le



configurer dans la même fenêtre. Pour cela, cochez la case **Utiliser proxy** et entrez l'adresse du serveur proxy (obligatoire) ainsi que le nom d'utilisateur et le mot de passe pour accéder au serveur.

L'option **Utiliser proxy** est disponible à condition que le dossier d'installation du **Serveur** ne contienne pas de fichiers de configuration de l'installation précédente.

15. Si lors de l'étape **4** vous avez choisi l'initialisation d'une nouvelle BD, la fenêtre suivante vous invitera à spécifier le mot de passe de l'administrateur du réseau antivirus.



Le mot de passe de l'administrateur ne doit pas contenir des caractères nationaux.

Cliquez ensuite sur le bouton **Suivant**.

16. Il est recommandé de mettre à jour le dépôt des produits (repository) lors de l'installation. Pour activer cette option, cochez la case **Mettre à jour le dépôt des produits**. Cliquez ensuite sur le bouton **Suivant**.
17. Dans la fenêtre qui apparaît, cliquez sur le bouton **Installer**. A partir de ce moment-là, l'installation se déroule automatiquement sans intervention de l'utilisateur.
18. Après la fin de l'installation, cliquez sur le bouton **Terminer**.



Après l'installation du **Serveur**, pour la formation correcte des liens lors de la création de packages d'installation de l'**Agent**, veuillez modifier le paramètre **ServerName** dans le fichier de configuration `webmin.conf` se trouvant dans le sous-répertoire `etc` du répertoire d'installation du **Serveur Enterprise**. Décommentez ce paramètre et, à la place de www.example.com, mettez l'adresse IP ou le nom DNS de l'ordinateur sur lequel est installé le **Serveur Enterprise**, spécifiez également le numéro de port au format suivant :

```
ServerName<Adresse_du_Serveur>: <numéro_du_port>
```



Enregistrez les modifications et redémarrez le **Serveur Enterprise**.

En cas d'utilisation du système de cluster des **Serveurs Enterprise**, ainsi que dans le cas où un port non standard est utilisé sur le **Serveur Enterprise**, éditez les paramètres correspondants dans le fichier de configuration `download.conf` se trouvant dans le sous-répertoire `etc` du répertoire d'installation du **Serveur Enterprise** (Voir aussi l'annexe [G3. Fichier de configuration `download.conf`](#)).

En général, le serveur installé **Serveur Enterprise** est géré depuis le **Centre de Gestion Dr.Web**. Le programme d'installation met également dans le menu principal du système d'exploitation Windows les éléments permettant de configurer et de gérer le **Serveur**.

Le dossier **Dr.Web Enterprise Server** contenant les éléments suivants sera placé dans le menu **Démarrer** → **Tous les programmes** :

- ◆ Le dossier **Contrôle du Serveur** comprend les commandes de démarrage, redémarrage et d'arrêt du **Serveur**, ainsi que les commandes déterminant le mode de journalisation et d'autres commandes du **Serveur** décrites dans l'Annexe [H5. Dr.Web Enterprise Server](#).
- ◆ L'élément **Interface Web** permet d'ouvrir le **Centre de Gestion** et de se connecter au **Serveur** installé sur ce poste (à l'adresse <http://localhost:9080>).
- ◆ L'élément **Documentation** sert à afficher le Manuel Administrateur au format HTML.

Structure du répertoire d'installation de Dr.Web Enterprise Server :

- ◆ `bin` – contient les exécutables de **Serveur Enterprise** ;
- ◆ `etc` – ce dossier comprend les fichiers des paramètres principaux des composants du réseau antivirus ainsi que les fichiers clés **Serveur** (`enterprise.key`) et **Agent** (`agent.key`) ;
- ◆ `Installer` – le dossier comprend le programme destiné à



lancer le processus d'installation de l'**Antivirus** sur le poste à protéger ainsi que la clé publique de chiffrement (`drwcsd.pub`) ;

- ◆ `update-db` – comprend les script nécessaires à la mise à jour de la structure des bases de données du **Serveur** ;
- ◆ `var` – le dossier comprend les sous-dossiers suivants :
 - `backup` – sert à conserver les copies de sauvegarde de la BD et d'autres données critiques ;
 - `extensions` – contient des scripts utilisateur destinés à l'automatisation de l'exécution de certaines tâches, tous les scripts sont désactivés par défaut ;
 - `repository` – répertoire des mises à jour dans lequel sont déposées les mises à jour actuelles des bases virales, des fichiers des packages antivirus et des fichiers des composants du réseau antivirus. Le répertoire comprend des sous-répertoires pour certains composants du logiciel et ces sous-répertoires à leur tour comprennent des sous-dossiers appropriés aux OS respectifs. Ce répertoire doit être accessible en écriture à l'utilisateur sous le nom duquel le **Serveur** démarre (d'habitude, sous UNIX, c'est l'utilisateur **drwcs**, sous Windows — **LocalSystem**) ;
 - `templates` – motifs de fichiers de log ;
- ◆ `webmin` – ce dossier contient les éléments du **Centre de Gestion Dr.Web** : la documentation, les icônes, les modules.



Le contenu du répertoire des mises à jour `\var\repository` est téléchargé depuis le serveur de mises à jour via le protocole HTTP, de manière automatique selon la planification spécifiée pour le **Serveur**. L'administrateur du réseau antivirus peut également mettre des mises à jour vers ces dossiers de manière manuelle.



2.2.2. Installation de Dr.Web Enterprise Server sous UNIX®



Toutes les actions relatives à l'installation doivent être effectuées depuis la console sous le nom de super-utilisateur **root**.

Marche à suivre pour installer Dr.Web Enterprise Server pour les OS de la famille UNIX :

1. Pour lancer l'installation de `drweb-esuite`, exécutez la commande suivante :

Pour le Serveur sous OS		Commande
FreeBSD		<code>pkg_add <fichier_de_distribution>.tbz</code>
Solaris		1. <code>bzip2 -d <fichier_de_distribution>.bz2</code> 2. <code>pkgadd -d <fichier_de_distribution></code>
Linux	Debian®	<code>dpkg -i <fichier_de_distribution>.deb</code>
	Ubuntu®	
	packages rpm	<code>rpm -i <fichier_de_distribution>.rpm</code>



Si vous avez déjà installé le logiciel de **Serveur Enterprise**, vous pouvez mettre à jour les composants installés. Pour cela, lancez la distribution avec la commande suivante :

- `rpm -U <nom_de_fichier_de_distribution>.rpm` pour les distributions **rpm**,
- `dpkg -i <nom_de_fichier_de_distribution>.deb` pour les packages **deb**.

Il existe également des packages génériques (`generic packages`) pouvant être installés sur n'importe quel système de



la famille Linux, voire sur un système non listé parmi les OS supportés.



Lors de l'installation des `generic-package` sous Linux, la bibliothèque `glibc` en même version que la version du `packagegeneric` est requise.

L'installation se fait avec l'installateur intégré dans le package. Veuillez utiliser la commande :

```
tar -xjf <nom_de_fichier_de_distribution>.tar.bz2
```

Puis exécutez le script ci-dessous en tant que super-utilisateur :

```
./drweb-esuite-install.sh
```



L'installation du **Serveur** peut être interrompue à tout moment par envoi au processus d'un des signaux suivants : `SIGHUP`, `SIGINT`, `SIGTERM`, `SIGQUIT` et `SIGWINCH` (sous OS **FreeBSD** la modification des dimensions de la fenêtre de terminal entraîne un envoi du signal `SIGWINCH`). En cas d'interruption du processus d'installation, un rollback des modifications apportées au système de fichiers sera effectué afin de revenir au statut d'avant l'installation. Vous pouvez interrompre l'installation du package `rpm` avec les touches `CTRL + C`.

La touche `ESC` pressée lors de l'installation du **Serveur** permet de reculer d'une étape. De plus, pressée lors de l'étape 2 (la première fenêtre de dialogue de l'installateur affichant le texte du Contrat de licence), la touche `ESC` interrompt le fonctionnement de l'installateur.

Le nom de l'administrateur du réseau antivirus déterminé par défaut est **admin**.

2. Les fenêtres suivantes (dont le nombre et l'ordre d'apparition dépendent de l'OS) affichent les messages sur les droits d'auteur ainsi que le texte du Contrat de licence. Pour continuer l'installation, vous devez accepter les termes du Contrat de licence.



3. Puis vous serez invité à entrer le groupe et le nom d'utilisateur sous lequel le **Serveur** va fonctionner. Le même utilisateur sera propriétaire des fichiers du **Serveur Enterprise**.

Sélectionnez **new** pour répondre à la requête pour la création d'un nouvel utilisateur sous le nom de qui le logiciel sera lancé. Dans le menu suivant, il est recommandé de garder la valeur par défaut et cliquez sur **OK**. Dans le menu de sélection d'un groupe, créez un nouveau groupe. Dans la requête suivante, gardez la valeur par défaut.

4. Puis vous serez invité à spécifier les chemins vers le fichier clé de **Serveur** (`enterprise.key`) et celui de l'**Agent** (`agent.key`). Ces fichiers clé sont fournis au sein du package d'installation ou (en cas de mise à niveau depuis une version plus ancienne) sont conservés par défaut dans le dossier `/root/esuite_backup` ou dans le dossier que vous avez spécifié.



Lors de l'installation en mode ligne de commande, le nombre de tentatives autorisées relatives à la spécification des clés est limité (en cas d'échec) :

- sous OS FreeBSD - 3 tentatives ;
- sous OS Solaris - 2 tentatives.

Si le nombre autorisé de tentatives est utilisé, l'installateur sera arrêté.

5. Ensuite :
 - ◆ En cas d'installation du logiciel sous **Solaris**, vous serez invité à créer une nouvelle base de données du **Serveur**. Si vous effectuez une mise à jour du **Serveur** en disposant d'une base de données sauvegardée, entrez `no` et cliquez ensuite sur ENTER, puis spécifiez le chemin vers le fichier de la BD sauvegardée. En cas de première installation du **Serveur Enterprise**, cliquez sur ENTER et entrez le mot de passe de l'administrateur (**admin**) qui pourra accéder au logiciel (par défaut, le mot de passe est **root**). Lorsque vous spécifiez votre mot de passe, pour des raisons de sécurité, le mot de passe entré ne s'affiche pas sur l'écran. C'est pourquoi vous devez



confirmer le mot de passe (si les mots de passe entrés ne sont pas identiques, il faudra reprendre la procédure en suivant les notices affichées). Le mot de passe doit comprendre au moins 4 symboles.

Ensuite il vous sera proposé de créer des nouvelles clés de chiffrement. Si vous disposez des clés sauvegardées `drwcsd.pri` et `drwcsd.pub`, refuser la création des nouvelles clés (taper `no`, cliquez sur ENTER) et spécifiez le chemin complet vers les fichiers existants. S'il n'y a pas de clés, cliquez sur ENTER pour créer des nouvelles clés de chiffrement.

- ◆ En cas d'installation depuis les packages **deb**, vous serez invité à entrer le mot de passe administrateur (utilisateur **admin**). Vous pouvez garder le mot de passe par défaut - **root**. Lorsque vous spécifiez votre mot de passe, pour des raisons de sécurité, le mot de passe entré ne s'affiche pas sur l'écran. C'est pourquoi vous devez confirmer le mot de passe (si les mots de passe entrés ne sont pas identiques, il faudra reprendre la procédure en suivant les notices affichées). Le mot de passe doit comprendre au moins 4 symboles.
- ◆ Dans d'autres cas, vous serez invité à entrer le mot de passe administrateur (utilisateur **admin**). Lorsque vous spécifiez votre mot de passe, pour des raisons de sécurité, le mot de passe entré ne s'affiche pas sur l'écran. C'est pourquoi vous devez confirmer le mot de passe (si les mots de passe entrés ne sont pas identiques, il faudra reprendre la procédure en suivant les notices affichées). Le mot de passe doit comprendre au moins 8 symboles.



Le mot de passe de l'administrateur ne doit pas contenir de caractères nationaux.

6. S'il y a un interpréteur perl, en fonction de l'OS utilisé, vous serez invité à spécifier certains paramètres de configuration du **Serveur**. Lors du paramétrage de certains types de paramètres, la valeur `no` est définie par défaut (suite à un clic sur la touche ENTER), étant donné que les paramètres concernés reprennent les valeurs par défaut. Si vous saisissez `yes`, il sera proposé de spécifier des valeurs pour les



paramètres correspondants (les valeurs définies pas défaut seront affichées entre crochets, pour les spécifier, il suffit de cliquer sur la touche ENTER).

La procédure de paramétrage du **Serveur** peut être lancée manuellement (l'interpréteur perl sera requis). Pour cela, il suffit de lancer le script `configure.pl` se trouvant dans :

- ◆ le répertoire `/usr/local/drwcs/bin/` sous **FreeBSD**,
- ◆ le répertoire `/opt/drwcs/bin/` sous **Linux** et **Solaris**.

Vous pouvez consulter les paramètres relatifs à l'utilisation du script dans l'Annexe [H5.10. Configuration de Dr.Web Enterprise Server sous UNIX](#).

7. L'installation du logiciel se poursuivra. Lors de la procédure, l'installateur peut vous demander de confirmer vos actions en tant qu'administrateur.



Après l'installation du **Serveur**, pour la formation correcte des liens lors de la création de packages d'installation de l'**Agent**, veuillez modifier le paramètre **ServerName** dans le fichier de configuration `webmin.conf` se trouvant dans le sous-répertoire :

- ◆ `/var/drwcs/etc` pour OS **FreeBSD** et OS **Solaris**
- ◆ `/var/opt/drwcs/etc` pour OS **Linux**

Décommentez ce paramètre et, à la place de [www.example.com](#), mettez l'adresse IP ou le nom DNS de l'ordinateur sur lequel est installé le **Serveur Enterprise**, spécifiez également le numéro de port au format suivant :

```
ServerName <nom_DNS>:<numéro_du_port>
```

Enregistrez les modifications et redémarrez le **Serveur Enterprise**.



En cas d'utilisation du système de cluster des **Serveurs Enterprise**, ainsi que dans le cas où un port non standard est utilisé sur le **Serveur Enterprise**, éditez les paramètres correspondants dans le fichier de configuration `download.conf` se trouvant dans le sous-répertoire :

- ◆ `/var/drwcs/etc` pour OS **FreeBSD** et OS **Solaris**
- ◆ `/var/opt/drwcs/etc` pour OS **Linux**

(Voir aussi l'annexe [G3. Fichier de configuration download.conf](#)).



Lors de l'installation du logiciel sous **FreeBSD** le script rc suivant sera créé :

```
/usr/local/etc/rc.d/drwcsd.sh.
```

Utilisez les commandes :

- ◆ `/usr/local/etc/rc.d/drwcsd.sh stop` - pour arrêter le **Serveur** manuellement ;
- ◆ `/usr/local/etc/rc.d/drwcsd.sh start` - pour démarrer le **Serveur** manuellement.

Lors de l'installation du logiciel sous OS **Linux** et OS **Solaris**, le script `init` sera créé pour réaliser le démarrage et l'arrêt du **Serveur** : `/etc/init.d/drwcsd` utilisant `/opt/drwcs/bin/drwcs.sh`. Ce dernier n'est pas destiné au démarrage manuel.

2.2.3. Installation du module ajoutable Dr.Web Browser-Plugin



L'installation du module ajoutable **Dr.Web Browser-Plugin** pour les navigateurs web Mozilla Firefox, Opera et Chrome est possible uniquement pour leurs versions tournant sous OS Windows ou sous OS de la famille Linux.



Le module ajoutable **Dr.Web Browser-Plugin** assure le fonctionnement complet du **Centre de Gestion** (voir aussi [Pré-requis système pour le Centre de Gestion Dr.Web](#)).

Le module est fourni avec le package d'installation du **Serveur** et peut être installé de la façon suivante :

1. Automatiquement, en réponse à une requête du navigateur web pendant l'utilisation des éléments du **Centre de Gestion** nécessitant le chargement du module (**Scanner réseau**, installation distante des composants antivirus).
2. Manuellement, avec l'installateur du module **Dr.Web Browser-Plugin**.

Installation manuelle de Dr.Web Browser-Plugin

Marche à suivre pour télécharger l'installateur du module Dr.Web Browser-Plugin afin de réaliser l'installation manuelle :

1. Ouvrez le **Centre de Gestion**. Si **Dr.Web Browser-Plugin** pour le navigateur utilisé n'est pas encore installé, une invitation à installer le module ajoutable sera affichée au-dessous du menu principal.
2. Cliquez sur le lien **Installer Dr.Web Browser-Plugin**.



Fig. 2-4. Rubrique de téléchargement du module Dr.Web Browser-Plugin

3. Dans la rubrique de téléchargement du module ajoutable, la version courante du navigateur web utilisé sera affichée ainsi que le type de plateforme (x86 ou x64).

Pour les OS de la famille UNIX, il sera également proposé de sélectionner depuis la liste une version de la distribution correspondant au système d'exploitation utilisé.

4. Pour télécharger et sauvegarder le module, cliquez sur le bouton **Télécharger**. Puis vous pouvez procéder à l'installation [manuelle](#).
5. Afin de basculer entre les différents types de plateforme, cliquez sur le lien se trouvant au-dessous du bouton de téléchargement, puis téléchargez le plugin comme décrit à l'étape 4.

La marche à suivre pour installer le module Dr.Web Browser-Plugin sous Windows :

1. Lancez le fichier du package d'installation. La fenêtre de l'assistant **InstallShield Wizard** va s'ouvrir. Cliquez sur **Suivant**.
2. La fenêtre affichant le texte du Contrat de licence s'ouvrira. Après avoir pris connaissance des termes du Contrat, cochez la case **J'accepte les termes du Contrat de licence** et cliquez



ensuite sur le bouton **Suivant**.

3. La fenêtre de sélection du dossier d'installation s'ouvrira. Pour modifier le dossier d'installation spécifié par défaut, cliquez sur **Modifier** et sélectionnez un dossier. Puis cliquez sur **Suivant**.
4. Dans la fenêtre suivante, cliquez sur le bouton **Installer** afin de lancer la procédure d'installation. Les actions suivantes de l'assistant d'installation ne nécessitent aucune intervention de l'utilisateur.
5. Après la fin de l'installation, cliquez sur le bouton **Terminer**.

Marche à suivre pour installer le module Dr.Web Browser-Plugin sous UNIX :

Exécutez la commande suivante :

- ◆ pour les packages **deb** :

```
dpkg -i drweb-esuite-plugins-linux-  
<version_de_la_distribution>.deb
```

- ◆ pour les packages **rpm** :

```
rpm -i drweb-esuite-plugins-linux-  
<version_de_la_distribution>.rpm
```

- ◆ pour d'autres systèmes (packages **tar.bz2** et **tar.gz**):

1. Déballez l'archive contenant le module ajoutable.
2. Créez un dossier pour les modules ajoutables si un tel dossier n'a pas encore été créé.

Par exemple pour le navigateur Mozilla Firefox : `mkdir /usr/lib/mozilla/plugins`

3. Copiez la bibliothèque déballée à l'étape 1 vers le dossier pour les modules ajoutables.

Par exemple pour le navigateur Mozilla Firefox : `cp libnp*.so /usr/lib/mozilla/plugins`



Après avoir installé le plugin **Dr.Web Browser-Plugin**, sous OS de la famille UNIX, redémarrez le navigateur Web, s'il a été déjà lancé.



2.3. Installation de Dr.Web Enterprise Agent sous OS Windows®



Les droits d'administrateur sur le poste sont requis pour l'installation d'**Enterprise Agent**.

Si l'**Agent** est déjà installé sur le poste, il faudra le désinstaller avant de procéder à la nouvelle [installation](#).

L'installation d'Enterprise Agent et du package antivirus peut être réalisée en deux modes :

1. Mode distant : depuis le **Serveur Enterprise** via LAN. Dans ce cas, l'installation est effectuée par l'administrateur du réseau antivirus sans aucune intervention de l'utilisateur. Pour en savoir plus, consultez le paragraphe [Installation distante de Dr.Web Enterprise Agent sous Windows®](#).
2. Mode local : directement sur la machine de l'utilisateur. L'installation peut être réalisée par l'administrateur ainsi que par l'utilisateur. Dans ce cas, il est possible d'utiliser (voir aussi [Fichiers d'installation](#)) :
 - ◆ [Package d'installation](#) esinst.exe.
 - ◆ [Installation réseau](#) de l'**Agent** drwinst

Lors de l'installation des Enterprise Agent sur les serveurs de LAN et sur les ordinateurs du cluster, il faut prendre en compte les informations suivantes :

- ◆ En cas d'installation sur les ordinateurs servant des serveurs terminaux (sous OS Windows les services **Terminal Services** sont installés), afin d'assurer le fonctionnement des **Agents** lors des sessions terminales des utilisateurs, l'installation des **Agents** doit être réalisée de manière locale avec l'assistant d'installation et de suppression des programmes depuis le **Panneau de configuration** Windows.
- ◆ Il est déconseillé d'installer sur les serveurs ayant les fonctions réseau importantes (contrôleurs de domaine, serveurs de licences etc.) les composants **SpIDer Gate**, **SpIDer Mail** et



Dr.Web Firewall afin d'éviter d'éventuels conflits entre les services réseau et les composants intégrés de l'antivirus **Dr.Web**.

- ◆ L'installation de l'**Agent** sur le cluster doit être réalisée séparément pour chaque nœud du cluster.
- ◆ Les principes de fonctionnement de l'**Agent** et des composants du package antivirus sur un nœud du cluster sont pareils aux principes relatifs à un serveur LAN, il n'est pas recommandé d'installer sur les nœuds du cluster les composants **Dr.Web Firewall**, **SpIDer Mail**, **SpIDer Gate**.
- ◆ Si l'accès à la ressource quorum du cluster est strictement limité, il est recommandé de l'exclure de l'analyse par **SpIDer Guard** et de se contenter de l'analyse régulière de cette ressource par le **Scanner**, lancé selon la planification ou manuellement.

2.3.1. Fichiers d'installation

Package d'installation (esinst)

Lors de la création d'un nouveau compte utilisateur, un package d'installation `esinst` assurant l'installation de l'**Agent** sera généré.

Le lien de téléchargement du package d'installation de l'**Agent** sur le poste en question est disponible :

1. Immédiatement après la création d'un nouveau poste (étape **11** dans la rubrique [Création d'un nouveau compte](#)).
2. A n'importe quel moment après la création du poste :
 - ◆ dans la rubrique [propriétés](#) du poste,
 - ◆ dans la rubrique **Objets sélectionnés** lors de la sélection du poste depuis l'arborescence.

Installateur réseau (drwinst)

L'installateur réseau de l'**Agent** `drwinst` ainsi que la clé publique de chiffrement `drwcsd.pub` se trouvent dans le



dossier `Installer` (par défaut, c'est une ressource partagée cachée) du répertoire d'installation de **Serveur Enterprise**. L'accessibilité de cette ressource via le réseau peut être paramétrée à l'[étape 8](#) pendant l'installation de **Serveur Enterprise**. Vous pouvez modifier cette ressource ultérieurement.

L'installateur de l'**Agent** et la clé publique de chiffrement sont également disponibles depuis la page d'installation du **Centre de Gestion Dr.Web**.

Page d'installation

La page d'installation du **Centre de Gestion Dr.Web** vous permet de télécharger :

1. L'installateur réseau de l'**Agent** `drwinst`.
Les installateurs pour les différents OS se trouvent dans les dossiers aux noms correspondants.
2. La clé publique de chiffrement `drwcsd.pub`.

La page d'installation est accessible sur n'importe quel ordinateur ayant un accès réseau à **Serveur Enterprise**, à l'adresse suivante :

```
http://<Adresse_du_Serveur>:<numéro_du_port>/install/
```

avec `<Adresse_du_Serveur>` - l'adresse IP ou le nom de domaine de l'ordinateur sur lequel est installé **Serveur Enterprise**. Comme `<numéro_du_port>`, spécifiez le port 9080 (ou 9081 si https).



2.3.2. Installation de Dr.Web Enterprise Agent à l'aide du Package d'installation

Pour installer l'Agent et le package antivirus, procédez comme suit :

1. Depuis le **Centre de Gestion** :
 - ◆ [Créez un compte](#) de nouvel utilisateur sur le **Serveur**.
 - ◆ Recevez un lien de téléchargement de l'installateur de l'**Agent**.
2. Envoyez à l'utilisateur le lien vers l'installateur de l'**Agent**.
3. [Installez l'Agent](#) sur un poste. En général, l'installation du logiciel d'**Enterprise Agent** se fait par l'utilisateur lui-même.
4. Par défaut, le nouveau poste antivirus sera automatiquement approuvé sur le **Serveur** (voir aussi [Politique de connexion des postes](#)).

2.3.2.1. Création d'un nouveau compte

Afin de créer un compte ou plusieurs comptes utilisateur, utilisez le [Centre de Gestion Dr.Web](#).



Assurez-vous que le paramètre **ServerName** dans le fichier de configuration `webmin.conf` a la valeur

```
<Adresse_du_Serveur>: 9080,
```

avec `<Adresse_du_Serveur>` - l'adresse IP ou le nom DNS de l'ordinateur sur lequel est installé **Serveur Enterprise**.



A la création d'un compte utilisateur, il est nécessaire que le **Centre de Gestion** se connecte au **Serveur** à l'adresse IP relative au domaine dans lequel sera créé le compte. Sinon il sera impossible de se connecter au **Serveur** lors de l'installation du package, puisque l'adresse du **Serveur** à laquelle le **Centre de Gestion** doit être connectée sera écrite dans le package d'installation lors de la création du package **Enterprise Agent**.



En cas de connexion du **Centre de Gestion** au **Serveur** depuis un ordinateur local, faites attention à ce que l'adresse **Serveur** ne soit pas spécifiée comme loopback (127.0.0.1).

Marche à suivre pour créer un nouvel utilisateur depuis le Centre de Gestion Dr.Web :

1. Sélectionnez l'élément **Réseau antivirus** du menu principal du **Centre de Gestion**.
2. Depuis la barre d'outils, cliquez sur le bouton **+ Ajouter un poste ou un groupe**. Dans le sous-menu qui s'ouvre, sélectionnez l'élément **+ Créer un poste**. Le panneau de création du compte utilisateur sera affiché dans la partie droite de la fenêtre du **Centre de Gestion**.
3. Spécifiez le nombre de comptes utilisateur à créer dans le champ **Nombre**.
4. L'identificateur unique du poste sera spécifié de manière automatique dans le champ **Identificateur**. Si nécessaire, vous pouvez le modifier.
5. Dans le champ **Nom**, spécifiez le nom du poste à afficher dans l'arborescence du réseau antivirus. Par la suite, après la connexion du poste au **Serveur**, ce nom peut être automatiquement remplacé par le nom spécifié de manière locale.
6. Dans les champs **Mot de passe** et **Confirmez le mot de passe**, entrez le mot de passe nécessaire pour que le poste puisse accéder au **Serveur**.



En cas de création de plusieurs comptes, les valeurs pour les champs respectifs **Identificateur**, **Nom** et **Mot de passe (Confirmez le mot de passe)** seront spécifiées de manière automatique et impossibles à modifier lors de la création du poste.

7. Dans le champ **Description**, entrez des informations supplémentaires sur l'utilisateur. Ce paramètre est facultatif.
8. Dans la rubrique **Groupe**, sélectionnez les groupes auxquels va appartenir le poste antivirus que vous créez. Par défaut, le poste



fait partie du groupe **Everyone**. S'il existe des groupes d'utilisateurs, vous pouvez y inclure le poste que vous créez. Pour cela, cliquez sur le nom du groupe dans la rubrique **Groupes connus**. Afin de retirer un poste des groupes utilisateur dont il fait partie, cliquez sur le nom du groupe dans la rubrique **Appartenance à**.

Pour spécifier le groupe primaire pour le poste en cours de création, cliquez sur l'icône du groupe sélectionné dans la rubrique **Appartenance à**. Le symbole **1** sera affiché dans l'icône du groupe.

Il est impossible de retirer le poste depuis le groupe **Everyone** ou depuis le groupe primaire.

9. Si nécessaire, spécifiez des informations dans la rubrique **Sécurité**. Pour en savoir plus sur la configuration de cet élément, consultez le paragraphe [Configuration du poste de travail](#).
10. Si nécessaire, spécifiez les paramètres dans la rubrique **Emplacement**.
11. Cliquez sur le bouton **Sauvegarder** se trouvant en haut, au coin droit de la fenêtre. La fenêtre informant sur la création d'un nouveau poste apparaît et affiche l'identificateur du poste et le lien de téléchargement du package d'installation de l'**Agent**.



Le lien de téléchargement de l'installateur de l'**Agent** est également disponible :

- ◆ depuis l'élément [propriétés](#) du poste après sa création,
- ◆ dans la rubrique **Objets sélectionnés** lors de la sélection du poste créé dans l'arborescence.

Voir aussi [Fichiers d'installation](#).

12. La marche à suivre pour installer le logiciel de l'**Agent** est décrite ci-dessous.



Les droits d'administrateur sur le poste sont requis pour l'installation d'**Enterprise Agent**.

Si un antivirus est déjà installé sur le poste, avant de procéder à l'installation, l'installateur va essayer de le supprimer. En cas d'échec, l'utilisateur doit désinstaller le logiciel antivirus opérant sur le poste lui-même.

2.3.2.2. Installation de Dr.Web Enterprise Agent et du package antivirus

Pour installer Dr.Web Enterprise Agent et le package antivirus sur le poste, procédez comme suit :

1. Téléchargez le fichier d'installation de l'**Agent**. Pour cela, cliquez sur le lien que vous avez reçu lors de la création du poste dans le **Centre de Gestion**.
2. Exécutez sur le poste le fichier téléchargé `esinst.exe`. La fenêtre de l'assistant d'installation de l'antivirus **Dr.Web** apparaît.
3. Avant de procéder à l'installation, l'assistant vous proposera de confirmer qu'aucun logiciel antivirus n'est installé sur votre machine. Veuillez vous assurer que vous n'utilisez aucun autre antivirus (y compris d'autres versions de l'antivirus **Dr.Web**), puis cochez la case **Aucun antivirus n'est présent sur mon PC**. Puis cliquez sur **Suivant**.
4. La prochaine fenêtre vous propose de choisir un mode d'installation :
 - ◆ **Rapide (recommandé)** - l'installation la plus facile. Tous les paramètres sont spécifiés automatiquement. Puis passez à l'étape **8**.
 - ◆ **Sélective** - l'installation permettant de sélectionner des composants antivirus à installer sur votre ordinateur.
 - ◆ **Mode administrateur** - l'installation la plus complète, permettant de spécifier/modifier tout paramètre d'installation et tout paramètre du logiciel antivirus installé.



5. En cas de mode **Sélective** ou **Mode administrateur**, il vous sera ensuite demandé de choisir les composants antivirus **Dr.Web** à installer. Cochez les cases contre les composants à installer.

La rubrique **Chemin d'installation** vous permet de spécifier le répertoire dans lequel vous souhaitez installer l'antivirus. Par défaut c'est le dossier Dr.Web Enterprise Suite se trouvant dans le répertoire Program files sur le disque système. Pour spécifier/modifier le chemin donné par défaut, cliquez sur **Parcourir** et entrez ensuite le chemin nécessaire.

Puis cliquez sur **Suivant**.

Pour effectuer l'installation **Sélective**, passez à l'étape **8**.

6. En cas d'installation en **Mode administrateur**, spécifiez dans la fenêtre suivante les paramètres de l'**Installeur réseau** :
 - ◆ Dans le champ **Dr.Web Enterprise Server**, entrez l'adresse réseau du **Serveur Enterprise** depuis lequel **l'Agent** et le package antivirus seront installés. Si vous avez déjà spécifié l'adresse du **Serveur** lors du démarrage de l'installeur, l'adresse sera automatiquement entrée dans ce champ.



Lors de l'installation d'**Enterprise Agent** avec l'installeur créée dans le **Centre de Gestion**, le champ **Dr.Web Enterprise Server** sera rempli automatiquement.

Si vous ignorez l'adresse du **Serveur**, cliquez sur le bouton **Rechercher**. Une fenêtre permettant de rechercher les **Serveurs Enterprise** actifs dans le réseau sera ouverte. Configurez les paramètres nécessaires (au format `<nom_du_serveur>@<adresseIP>/<suffix_reseau>:<port>`) et cliquez sur le bouton **Rechercher**. Dans la liste des Serveurs, sélectionnez le serveur depuis lequel vous voulez installer l'antivirus, cliquez ensuite sur le bouton **OK**.



- ◆ Dans le champ **Clé publique Dr.Web Enterprise Server** vous pouvez spécifier le chemin complet vers la clé publique (`drwosd.pub`) se trouvant sur votre poste (si l'installateur est lancé depuis le **Serveur** via le réseau, la clé est copiée vers les fichiers temporaires du système. Après l'installation, la clé sera déplacée vers le répertoire d'installation).
- ◆ Dans la rubrique **Utiliser la compression durant le téléchargement**, sélectionnez une variante de compression : **Oui** - utiliser la compression, **Non** - ne pas utiliser la compression, **Possible** - utiliser la compression en fonction de la configuration sur le **Serveur**.
- ◆ La case cochée **Ajouter Dr.Web Agent à la liste des exclusions du pare-feu Windows** assure l'ajout des ports et des interfaces utilisés par l'**Agent** dans la liste des exclusions du pare-feu. Il est recommandé de cocher la case afin d'éviter d'éventuelles erreurs, par exemple, lors de la mise à jour automatique des composants antivirus et des bases virales.
- ◆ Si nécessaire, vous pouvez cocher la case **Enregistrer l'Agent dans la liste des programmes installés**.

Cette option vous permet, entre autres, de supprimer l'**Agent** et le package antivirus avec les outils standard de l'OS Windows (voir le paragraphe [Suppression des composants sous Windows®](#)).

7. En cas d'installation en **Mode administrateur** : configurez l'**Agent** dans la fenêtre suivante :
 - ◆ Dans la rubrique **Authentification**, veuillez spécifier les paramètres d'authentification de l'**Agent** sur le **Serveur**. En cas de mode **Automatique (par défaut)**, les paramètres d'authentification (identificateur et mot de passe) seront générés de manière automatique sur le **Serveur**, dans ce cas, le mode d'accès du poste sera défini sur le **Serveur** (voir [Politique de connexion des postes](#)). Lorsque le mode d'authentification **Manuelle** est choisi, il faudra spécifier les paramètres d'authentification du poste : son **Identificateur** sur le **Serveur** et un **Mot de passe** pour y accéder. Dans ce cas, le poste aura l'accès sur le **Serveur** sans approbation manuelle par l'administrateur.



Lors de l'installation d'**Enterprise Agent** avec l'installateur créée dans le **Centre de Gestion**, les champs respectifs **Identificateur** et **Mot de passe** relatifs au mode **Manuelle** seront remplis automatiquement.

- ◆ Les rubriques **Compression** et **Chiffrage** permettent de configurer la bande passante entre le **Serveur** et l'**Agent** (pour plus d'information, consultez le paragraphe [Chiffrement et compression du trafic](#)).

Puis cliquez sur **Suivant**.

8. L'installation de l'**Agent** et des composants antivirus commence (aucune intervention de l'utilisateur n'est requise).
9. Après la fin du processus d'installation, l'assistant va vous demander de redémarrer l'ordinateur. Cliquez sur **Terminer** pour quitter l'assistant.
10. Redémarrez la machine.



Immédiatement après l'installation, les **Agents** se connectent au **Serveur** de manière automatique. Dès que la connexion entre l'**Agent** et le **Serveur** est établie, le nom du poste respectif s'affiche dans la fenêtre du **Centre de Gestion**.

Enterprise Agent peut être installé sur un poste de manière distante via le **Centre de Gestion**.

2.3.3. Installation de Dr.Web Enterprise Agent avec l'installateur réseau



En cas de première installation d'**Enterprise Agent**, il faut d'abord mettre à jour le dépôt des produits du **Serveur** (voir [Mise à jour manuelle des composants de Dr.Web Enterprise Security Suite](#), paragraphe Vérification des mises à jour).



Si l'installateur réseau a été lancé au cours de l'installation standard (sans clé `-uninstall`) sur un poste sur lequel l'installation avait déjà été effectuée, cela n'entraîne aucune action. L'installateur achève son fonctionnement et affiche une fenêtre avec la liste des clés supportées.

L'installation avec l'installateur réseau peut être effectuée dans les deux modes principaux :

1. [En tâche de fond.](#)
2. [En mode graphique.](#)

Vous pouvez également installer **Enterprise Agent** sur le poste de manière distante via le **Centre de Gestion**, ou avec le service **Active Directory** (voir [Installation distante de Dr.Web Enterprise Agent](#)).

2.3.3.1. Installation de Dr.Web Enterprise Agent avec l'installateur en tâche de fond

Marche à suivre pour installer Dr.Web Enterprise Agent sur le poste avec l'installateur en tâche de fond :

1. Sur le poste sur lequel vous souhaitez installer l'antivirus, ouvrez le répertoire réseau d'installation de **l'Agent** (en cas d'installation du **Serveur**, ouvrez-le sous le répertoire `Installer` dans le répertoire d'installation du **Serveur**. Vous pourrez le déplacer ultérieurement), puis lancez le programme `drwinst`.

Par défaut, la commande `drwinst` lancée sans aucune clé utilise le mode **Multicast** pour scanner le réseau afin de trouver des Serveurs **ESS** actifs et tente d'installer **l'Agent** depuis le premier **Serveur** trouvé dans le réseau.



En cas d'utilisation du mode **Multicast** pour rechercher les **Serveurs** actifs, l'installation de l'**Agent** sera effectuée depuis le premier **Serveur** trouvé. Dans ce cas, si la clé existante `pub` ne correspond pas à la clé du **Serveur**, l'installation se termine avec une erreur. Si c'est le cas, veuillez spécifier l'adresse du **Serveur** au démarrage de l'installateur de manière explicite (voir ci-dessous).

La commande `drwinst` peut également être lancée avec les clés complémentaires suivantes :

- ◆ Dans le cas où le mode **Multicast** n'est pas utilisé, lors de l'installation de l'**Agent**, il est recommandé d'utiliser le nom du **Serveur** (pré-enregistré dans le service DNS) :

```
drwinst <DNS_nom_du_Serveur>
```

Ceci facilite le processus de configuration du réseau antivirus relatif à la procédure de réinstallation de **Serveur Enterprise** sur un autre ordinateur.

- ◆ Vous pouvez aussi spécifier l'adresse du **Serveur** de façon explicite :

```
drwinst 192.168.1.3
```

- ◆ La clé `-regagent` permet d'enregistrer l'**Agent** dans la liste d'ajout/suppression de programmes lors de l'installation.
- ◆ Pour lancer l'installateur en mode graphique, utilisez le paramètre `-interactive`.



Vous pouvez consulter la liste complète des paramètres de l'**Installateur réseau** dans l'Annexe [H4. Installateur réseau](#).

2. Lorsque l'installation est finie, le logiciel de l'**Agent** antivirus est installé sur le poste (ce n'est pas encore le package antivirus).
3. Dès que le poste est approuvé sur le **Serveur** (dans le cas où l'approbation est requise par la configuration du **Serveur**), le package antivirus sera automatiquement installé.



4. Veuillez redémarrer votre ordinateur sur demande de l'**Agent**.

2.3.3.2. Installation de Dr.Web Enterprise Agent avec l'installateur en mode graphique

Marche à suivre pour installer Dr.Web Enterprise Agent sur le poste avec l'installateur en mode graphique :

1. Sur le poste sur lequel vous souhaitez installer l'antivirus, ouvrez le répertoire réseau d'installation de l'**Agent** (en cas d'installation du **Serveur**, ouvrez-le sous le répertoire Installer dans le répertoire d'installation du **Serveur**. Vous pourrez le déplacer ultérieurement) puis lancez le programme drwinst avec la clé -interactive.

La fenêtre de l'assistant d'installation de l'antivirus **Dr.Web** va s'ouvrir.

2. Avant l'installation, l'assistant vous demandera de confirmer qu'aucun logiciel antivirus n'est installé sur le poste. Veuillez vous assurer qu'aucun logiciel antivirus n'est utilisé sur votre poste (y compris d'autres versions de l'antivirus **Dr.Web**), puis cochez la case **Aucun antivirus n'est présent sur mon PC**. Puis cliquez sur **Suivant**.
3. La prochaine fenêtre vous propose de choisir un mode d'installation :
 - ◆ **Rapide (recommandé)** - l'installation la plus facile. Tous les paramètres sont spécifiés automatiquement. Puis passez à l'étape **7**.
 - ◆ **Sélective** - l'installation permettant de sélectionner les composants antivirus à installer sur votre ordinateur.
 - ◆ **Mode administrateur** - l'installation la plus complète, permettant de spécifier/modifier tout paramètre d'installation et tout paramètre du logiciel antivirus installé.
4. En cas de mode **Sélective** ou **Mode administrateur**, il sera ensuite demandé de choisir les composants antivirus **Dr.Web** à installer. Cochez les cases correspondantes aux composants à installer.



La rubrique **Chemin d'installation** vous permet de spécifier le répertoire dans lequel vous souhaitez installer l'antivirus. Par défaut c'est le dossier `Dr.Web Enterprise Suite` se trouvant dans le répertoire `Program files` sur le disque système. Pour spécifier/modifier le chemin donné par défaut, cliquez sur **Parcourir** et entrez ensuite le chemin nécessaire.

Puis cliquez sur **Suivant**.

Pour effectuer l'installation **Sélective**, passez à l'étape **7**.

5. En cas d'installation en **Mode administrateur**, spécifiez dans la fenêtre suivante les paramètres de l'**Installeur réseau** :
 - ◆ Dans le champ **Dr.Web Enterprise Server**, entrez l'adresse réseau du serveur **ESS** depuis lequel l'**Agent** et le package antivirus seront installés. Si vous avez déjà spécifié l'adresse du **Serveur** lors du démarrage de l'installateur, l'adresse sera automatiquement entrée dans ce champ. Si vous ne connaissez pas l'adresse du **Serveur**, cliquez sur le bouton **Rechercher**. Une fenêtre permettant de rechercher les serveurs **ESS** actifs dans le réseau sera ouverte. Configurez les paramètres nécessaires (au format `<nom_du_serveur>@<adresseIP>/<suffix_reseau>:<port>`) et cliquez sur le bouton **Rechercher**. Dans la liste des Serveurs, sélectionnez le serveur depuis lequel vous voulez installer l'antivirus, cliquez ensuite sur le bouton **OK**.
 - ◆ Dans le champ **Clé publique Dr.Web Enterprise Server** vous pouvez spécifier le chemin complet vers la clé publique (`drwcsd.pub`) se trouvant sur votre poste (si l'installateur est lancé depuis le **Serveur** via le réseau, la clé est copiée vers les fichiers temporaires du système. Après l'installation, la clé sera déplacée vers le répertoire d'installation).
 - ◆ Dans la rubrique **Utiliser la compression durant le téléchargement**, sélectionnez une variante de compression : **Oui** - utiliser la compression, **Non** - ne pas utiliser la compression, **Possible** - utiliser la compression en fonction de la configuration sur le **Serveur**.



- ◆ La case cochée **Ajouter Dr.Web Agent à la liste des exclusions du pare-feu Windows** assure l'ajout des ports et des interfaces utilisés par l'**Agent** dans la liste des exclusions du pare-feu (excepté le système Windows 2000). Il est recommandé de cocher la case afin d'éviter d'éventuelles erreurs, par exemple, lors de la mise à jour automatique des composants antivirus et des bases virales.
- ◆ Si nécessaire, vous pouvez cocher la case **Enregistrer l'Agent dans la liste des programmes installés**.

Cette option vous permet, entre autres, de supprimer l'**Agent** et le package antivirus avec les outils standard de l'OS Windows (voir le paragraphe [Suppression des composants sous Windows®](#)).

6. En cas d'installation en **Mode administrateur** : configurez l'**Agent** dans la fenêtre suivante :
 - ◆ Dans la rubrique **Authentification**, veuillez spécifier les paramètres d'authentification de l'**Agent** sur le **Serveur**. En cas de mode **Automatique (par défaut)**, le mode d'accès au poste sera déterminé sur le **Serveur**. Lorsque le mode d'authentification **Manuelle** est choisi, il faudra spécifier les paramètres d'authentification du poste : son **Identificateur** sur le **Serveur** et un **Mot de passe** pour y accéder. Dans ce cas, le poste aura l'accès sur le **Serveur** sans approbation manuelle par l'administrateur.
 - ◆ Les rubriques **Compression** et **Chiffrement** permettent de configurer la bande passante entre le **Serveur** et l'**Agent** (pour plus d'information, consultez le paragraphe [Chiffrement et compression du trafic](#)).

Puis cliquez sur **Suivant**.

7. L'installation d'**Enterprise Agent** commence. Après la fin du processus d'installation de l'**Agent**, cliquez sur **Terminer** pour quitter l'assistant d'installation.
8. Après l'approbation du poste sur le **Serveur** (dans le cas où ceci est prévu par la configuration du **Serveur** et à condition que le mode d'authentification **Manuelle** ne soit sélectionné à l'étape **6** de l'installation en **Mode administrateur**), le package antivirus sera installé automatiquement.



9. Veuillez redémarrer votre ordinateur sur demande de l'**Agent**.

2.4. Installation distante de Dr.Web Enterprise Agent sous Windows®

Dr.Web Enterprise Security Suite permet de détecter les ordinateurs sur lesquels la protection antivirus **Dr.Web Enterprise Security Suite** n'a pas encore été installée et dans certains cas, il permet également d'installer la protection.



L'installation à distance d'**Enterprise Agent** n'est possible que sur les postes tournant sous Windows 2000 ou supérieur (voir [Annexe A. Liste complète des OS supportés](#)) exceptées les éditions Starter et Home.

L'installation à distance d'**Enterprise Agent** est possible uniquement via le **Centre de Gestion** lancé sous un OS de la famille Windows XP ou supérieur (voir [Annexe A. Liste complète des OS supportés](#)), excepté les éditions Starter et Home.

Les droits d'administrateur sur les postes sont requis pour pouvoir installer **Enterprise Agent** sur les postes.

Aucun paramétrage supplémentaire sur le poste distant n'est requis lors de l'installation à distance, à condition que le poste fasse partie du même domaine et utilise un compte administrateur de ce domaine. Dans le cas où le poste distant n'appartient pas au domaine ou en cas d'utilisation du compte local pour l'installation, sous certaines versions de l'OS, un paramétrage supplémentaire de la machine distante sera nécessaire.



Paramétrage supplémentaire en cas d'installation à distance vers un poste se trouvant hors du domaine ou en cas d'utilisation du compte local



Les paramètres en question peuvent affaiblir le niveau de protection du poste distant. Il est fortement recommandé de prendre connaissance de l'utilisation de ces paramètres avant d'apporter des modifications dans le système ou de refuser l'installation à distance et d'installer l'**Agent** manuellement.

En cas d'installation à distance de l'**Agent** sur un poste se trouvant hors du domaine et/ou en cas d'utilisation du compte local, réalisez les actions suivantes sur la machine sur laquelle sera installé l'**Agent** :

OS	Paramétrage
◆ Windows 2000	Aucun paramétrage supplémentaire n'est requis.
◆ Windows Server 2000	
◆ Windows XP	<ol style="list-style-type: none">1. Configurez le mode d'accès aux fichiers partagés : Panneau de configuration → Options des dossiers → onglet Affichage → décochez la case Utiliser le partage de fichiers simple (recommandé).2. Configurez le mode d'authentification réseau suivant dans les politiques locales : Panneau de configuration → Outils d'administration → Stratégie de sécurité locale → Paramètres de sécurité → Stratégies locales → Options de sécurité → Accès réseau : modèle de partage et de sécurité pour les comptes locaux → Classique – les utilisateurs locaux s'authentifient eux-mêmes.



OS	Paramétrage
◆ Windows Server 2003	Aucun paramétrage supplémentaire n'est requis.
◆ Windows Vista ◆ Windows 7 ◆ Windows Server 2008	<ol style="list-style-type: none">1. Activez l'option File sharing : Control Panel → Network and Internet → Network and Sharing Center → Sharing and discovery → File Sharing → Enable.2. Activez le compte administrateur local intégré et spécifiez pour ce compte un mot de passe. Utilisez ce compte lors de l'installation : Control Panel → System and Maintenance → Administrative Tools → Computer management → Local Users and Groups → Users. Cliquez sur Administrator → décochez la case Account is disabled → OK. Cliquez droit sur → Change password → spécifiez un mot de passe.

Dans le cas où le compte se trouvant sur le poste local n'a pas de mot de passe, spécifiez dans les politiques locales une stratégie d'accès sans mot de passe : **Control Panel** → **Administrative Tools** → **Local Security Policy** → **Security Settings** → **Local Policies** → **Security Options** → **Accounts: Limit local account use of blank passwords to console logon only** → **Disabled**.



Le fichier de l'installateur de l'**Agent** `drwinst.exe` ainsi que la clé publique de chiffrement `drwcsd.pub` doivent être déposés dans une ressource partagée.



2.4.1. Installation de Dr.Web Enterprise Agent via le Centre de Gestion Dr.Web

Il existe des méthodes suivantes d'installation distante des Agents sur les postes de travail au sein du réseau :

1. Installation avec le scanner réseau.

Permet d'effectuer une recherche préliminaire des ordinateurs non protégés dans le réseau et d'installer sur tels ordinateurs les **Agents Enterprise**.

2. Installation avec l'outil Installation via réseau.

A choisir dans le cas où vous connaissez l'adresse du poste ou du groupe des postes sur lesquels seront installés les **Agents**.

3. Installation sur les postes avec les ID spécifiés.

Permet d'installer sur les postes et vers les groupes des postes des **Agents** pour les comptes sélectionnés (y compris tous les nouveaux comptes existants) avec les ID spécifiés et les mots de passe pour accéder au **Serveur**.



Pour le bon fonctionnement du **Scanner réseau** et de l'outil **Installation via réseau** sous le navigateur Windows Internet Explorer, l'adresse IP ou/et le nom DNS de l'ordinateur sur lequel est installé le **Serveur Enterprise** doivent être ajoutés aux sites de confiance du navigateur dans lequel est ouvert le **Centre Gestion Sécurité** pour l'installation à distance.

Utilisation du Scanner Réseau

L'arborescence du réseau antivirus affichée dans le **Centre de Gestion** contient les ordinateurs déjà inclus dans le réseau antivirus. **Dr.Web Enterprise Security Suite** permet également de détecter les ordinateurs non protégés par l'antivirus **Dr.Web ESS** et d'installer à distance des composants antivirus.



Afin d'effectuer une installation rapide des logiciels **Agent** vers les postes de travail, il est recommandé d'utiliser le **Scanner réseau** (voir [Scanner réseau](#)) qui recherche les postes par leurs adresses IP.


Pour installer l'Agent avec le Scanner réseau, procédez comme suit :

1. Ouvrez la fenêtre du [Scanner réseau](#). Dans le menu principal du **Centre de Gestion**, sélectionnez l'élément **Administration** et depuis la fenêtre qui apparaît sélectionnez l'élément du menu de gestion **Scanner réseau**. Une fenêtre vide portant le même nom s'ouvrira.
2. Dans le champ de saisie **Réseau**, spécifiez les réseaux au format suivant :
 - ◆ espacé par un trait d'union (par exemple, 10.4.0.1-10.4.0.10),
 - ◆ espacé par une virgule-espace (par exemple, 10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90),
 - ◆ avec un préfixe réseau (par exemple, 10.4.0.0/24).







Pour une description détaillée des paramètres supplémentaires, consultez la rubrique [Scanner réseau](#).



3. Cliquez sur le bouton **Lancer le scanner**. L'arborescence dans laquelle il est indiqué pour chaque poste si l'antivirus est installé ou pas sera téléchargée dans la fenêtre.
4. Déployez les éléments de l'arborescence correspondant aux groupes de travail (domaines). Tous les éléments de l'arborescence correspondant aux groupes de travail et aux postes sont marqués par des icônes dont vous pouvez consulter la description ci-dessous.


Tableau 2-1. Apparences des icônes

Icône	Description
Groupes de travail	
	Groupes de travail contenant entre autres les ordinateurs sur lesquels l'antivirus Dr.Web ESS peut être installé.



Icône	Description
	Groupes restants qui contiennent les ordinateurs sur lesquels l'antivirus est déjà installé ou les ordinateurs inaccessibles via le réseau.
Postes de travail	
	Le poste détecté est enregistré dans la base et actif (postes actifs avec l'antivirus installé).
	Le poste détecté est enregistré dans la base dans le tableau des postes supprimés.
	Le poste détecté n'est pas enregistré dans la base (l'antivirus n'est pas installé sur le poste).
	Le poste détecté n'est pas enregistré dans la base (le poste est connecté à un autre Serveur).
	Le poste détecté est enregistré dans la base mais inactif, le port est fermé.

Les éléments de l'arborescence correspondant aux postes auxquels les icônes  ou  sont associées peuvent être déployés afin de consulter le jeu de composants installés.

Lorsque vous cliquez sur l'icône  associée à un composant du poste connecté au **Serveur**, la fenêtre de configuration du composant s'ouvre.

5. Dans la fenêtre du **Scanner réseau**, sélectionnez un ordinateur non protégé (ou plusieurs ordinateurs non protégés en utilisant les boutons CTRL ou SHIFT).
6. Depuis la barre d'outils sélectionnez l'élément **Installer Dr.Web Enterprise Agent**.
7. La fenêtre d'installation de l'**Agent** va s'ouvrir.
8. Dans la rubrique **Dr.Web Network Installer**, vous pouvez configurer les paramètres d'installation de l'**Agent**.
9. Dans le champ **Ordinateurs**, spécifiez l'adresse IP de l'ordinateur (des ordinateurs) sur lequel l'antivirus sera installé.
 - ◆ En cas d'installation vers les postes trouvés avec le **Scanner Réseau**, dans le champ **Ordinateurs**, l'adresse du poste ou



des plusieurs postes vers lesquels sera effectuée l'installation sera indiquée.

- ◆ Dans le cas contraire, spécifiez l'adresse du poste ou de plusieurs postes. En cas d'installation de l'**Agent** sur plusieurs postes à la fois, vous pouvez spécifier plusieurs adresses IP au format suivant :
 - espacé par un trait d'union (par exemple, 10.4.0.1-10.4.0.10),
 - espacé par une virgule-espace (par exemple, 10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90),
 - avec un préfixe réseau (par exemple, 10.4.0.0/24).



De plus, à la place des adresses IP, vous pouvez mettre les adresses de domaine des postes respectifs.

Si l'installation utilise un nom d'hôte contenant le caractère '-', tel nom doit être mis entre guillemets, par exemple, "123-456".

10. Par défaut, le logiciel de l'**Agent** sera installé vers le répertoire C:\Program Files\DrWeb Enterprise Suite. Si nécessaire, vous pouvez spécifier un autre chemin dans le champ **Répertoire d'installation**.
11. Par défaut, dans le champ **Serveur**, l'adresse IP ou le nom DNS de **Serveur Enterprise** auquel le **Centre de Gestion** est connecté seront affichés. Si nécessaire, spécifiez dans ce champ l'adresse du **Serveur** depuis lequel le logiciel antivirus sera installé.
12. Le champ **Clé publique** contient le chemin vers le fichier de la clé publique, le champ **Fichier exécutable** - le nom complet de l'installateur réseau. Si nécessaire, éditez les valeurs spécifiées ou donnez d'autres valeurs aux paramètres.



Les chemins vers la clé publique et vers le fichier exécutable doivent être spécifiés au format adresse réseau.

13. Si nécessaire, dans le champ **Paramètres complémentaires**, saisissez les clés de la ligne de commande



de l'installateur réseau (pour en savoir plus, consultez l'Annexe [H4. Installateur réseau](#)).

14. Dans la liste déroulante **Niveau de détails du log**, spécifiez un niveau de détail du journal d'installation.
15. Dans le champ **Timeout d'installation (sec)**, spécifiez un délai d'attente maximum avant la fin d'installation de l'**Agent** en secondes. Les valeurs admissibles sont les suivantes : 1-600. Par défaut, le délai de 180 secondes est spécifié. En cas de faible bande passante de la connexion entre le **Serveur** et l'**Agent**, il est recommandé d'augmenter la valeur spécifiée par défaut.
16. Si nécessaire, cochez la case **Enregistrer l'installation dans la BD des applications installées**.
17. Dans la rubrique **Installer**, sélectionnez les composants du package antivirus à installer sur le poste. Spécifiez aussi les paramètres de compression du trafic lors de l'installation.
18. Dans la rubrique **Authentification**, spécifiez les paramètres d'authentification nécessaires pour accéder au poste distant.

Il est possible de spécifier plusieurs comptes administrateur. Pour cela, procédez comme suit :

- a) cliquez sur pour ajouter le compte spécifié dans la rubrique **Authentification** dans la liste des comptes utilisés lors de l'installation.
- b) pour ajouter encore un compte, remplissez les champs relatifs à l'authentification et cliquez ensuite sur . De façon analogique pour chaque nouvelle entrée.
- c) la liste des comptes utilisés vous permet d'exclure ou d'activer l'utilisation des comptes précédemment désactivés. Pour cela, décochez/cochez les cases contres les comptes en question.

Lors de l'installation de l'**Agent**, en premier lieu, le premier compte de la liste est utilisé. Si l'installation sous ce compte a échoué, le compte suivant sera utilisé etc.

19. Après avoir spécifié les paramètres nécessaires dans la rubrique **Dr.Web Network Installer**, cliquez sur le bouton **Suivant**.



20. L'onglet **Dr.Web Enterprise Agent pour Windows** vous permet de spécifier les paramètres suivants :

- ◆ Dans la rubrique **Authentification**, vous pouvez spécifier les paramètres d'authentification de l'**Agent** sur le **Serveur**. Si la case **Spécifier les paramètres** n'est pas cochée et les champs respectifs ne sont pas remplis, les paramètres d'authentification seront déterminés de manière automatique.
- ◆ Les rubriques **Chiffrement** et **Compression** vous permettent d'autoriser le chiffrement et la compression du trafic entre l'**Agent** et le **Serveur**.

Ultérieurement, vous pouvez modifier ces paramètres dans les [configuration d'Enterprise Agent](#) et [propriétés du poste](#).

21. Après avoir spécifié tous les paramètres nécessaires, cliquez sur le bouton **Installer**.



Un service intégré est utilisé pour lancer l'installation de l'antivirus.

22. **Enterprise Agent** sera installé sur les postes spécifiés. Après l'approbation du poste sur le **Serveur** (si l'approbation est requise selon la configuration de **Serveur Enterprise**, voir aussi [Création d'un simple réseau antivirus](#)), le package antivirus sera installé de manière automatique.

23. Redémarrez l'ordinateur selon la requête de l'**Agent**.

Utilisation de l'outil Installation via réseau

Lorsque le réseau antivirus est créé et qu'il faut installer l'**Agent** sur les postes spécifiés, il est recommandé d'utiliser l' **Installation via réseau**.

Pour effectuer une installation via réseau, procédez comme suit :

1. Dans le menu principal, sélectionnez l'élément **Administration** puis dans la fenêtre qui apparaît, sélectionnez l'élément du menu de gestion **Installation via réseau**.



2. Les étapes suivantes sont équivalentes aux étapes **8-23** [ci-dessus](#).

Installation pour les comptes avec les ID spécifiés

Pour l'installation distante des Agents pour les comptes avec les ID sélectionnés procédez comme suit :

- a) En cas de création d'un nouveau compte de poste :
 1. Créez un nouveau compte ou plusieurs comptes pour les postes de travail (voir [Création d'un nouveau compte](#)).
 2. Immédiatement après la création du compte, dans la partie droite de la fenêtre principale, le panneau suivant apparaît : **Installer Dr.Web Agent**. Cliquez sur **OK**.
 3. La fenêtre **Scanner réseau** sera ouverte.
 4. Les étapes d'installation suivantes sont similaires aux étapes **2-23** de la procédure décrite [ci-dessus](#).
 5. Après la fin de l'installation, vérifiez que les [cônes](#) se trouvant contre les postes en question dans l'arborescence ont été changées.
- b) En cas d'utilisation d'un compte de poste existant :
 1. Dans l'arborescence du réseau antivirus, sélectionnez un nouveau poste ou un groupe des postes pour lesquels les **Agents** n'ont pas encore été installés, vous pouvez également sélectionner le groupe **New** (pour l'installation vers tous les nouveaux comptes).
 2. Dans la barre d'outils, cliquez sur le bouton **Installer Dr.Web Enterprise Agent**.
 3. La fenêtre **Scanner réseau** sera ouverte.
 4. Les étapes d'installation suivantes sont similaires aux étapes **2-23** de la procédure décrite [ci-dessus](#).
 5. Après la fin de l'installation, vérifiez que les [icônes](#) se trouvant contre les postes en question dans l'arborescence ont été changées.



L'installation de l'**Agent** sur les postes avec les ID sélectionnées est également disponible pour l'administrateur des groupes.



En cas d'erreurs lors de l'installation via réseau, consultez le paragraphe [Diagnostic des problèmes d'installation distante](#).

2.4.2. Installation de Dr.Web Enterprise Agent avec le service Active Directory

Si le service **Active Directory** est utilisé dans le réseau protégé, vous pouvez installer **Enterprise Agent** sur les postes de manière distante. Pour cela, procédez comme suit :

- ◆ Téléchargez depuis le site <http://download.drweb.com/esuite/> l'installateur d'**Enterprise Agent** pour les réseaux avec **Active Directory**.
- ◆ Depuis le serveur du réseau local supportant le service **Active Directory**, exécutez l'installation d'**Enterprise Agent** en mode administrateur. L'installation peut être réalisée en mode ligne de commande (**A**), ainsi qu'en mode graphique de l'installateur (**B**).



Lors de la mise à jour du **Serveur**, il n'est pas requis de mettre à jour l'installateur d'**Enterprise Agent** pour les réseaux avec Active Directory. Après la mise à jour du logiciel de **Serveur**, les **Agents** et l'antivirus sur les postes seront mis à jour de manière automatique après l'installation.



(A) Configuration de l'installation de Dr.Web Enterprise Agent en mode ligne de commande

Exécutez la commande suivante accompagnée de tous les paramètres nécessaires et du paramètre obligatoire de désactivation du mode graphique /qn :

```
msiexec /a <nom_du_package>.msi /qn [<paramètres>]
```

La clé /a lance le déploiement du package administrateur.

Nom du package

Le nom du package d'installation d'**Enterprise Agent** pour les réseaux avec **Active Directory** est dans la plupart des cas présenté au format suivant :

```
drweb-es-agent-<version>-<date_de_publication>-windows-nt-<plateforme>.msi.
```

Paramètres

/qn - paramètre de désactivation du mode graphique. En cas d'utilisation de cette clé, les paramètres ci-dessous sont obligatoires à spécifier :

- ◆ ESSERVERADDRESS=<nom_DNS> - désigne l'adresse de **Serveur Enterprise** auquel l'**Agent** va se connecter. Pour en savoir plus sur les formats possibles, consultez l'[Annexe E3](#).
- ◆ ESSERVERPATH=<chemin_nom_du_fichier> - désigne le chemin complet vers la clé publique de chiffrement de **Serveur Enterprise** et le nom du fichier (par défaut c'est drwcsd.pub dans le sous-dossier `Installer` du dossier d'installation de **Serveur Enterprise**).



- ◆ TARGETDIR - désigne le répertoire réseau destiné pour un prototype de l'**Agent** (package d'installation modifié de l'**Agent**), ce répertoire peut être sélectionné depuis l'éditeur des politiques de groupes pour l'installation spécifiée. Le répertoire doit avoir les droits en lecture et en écriture. Le chemin vers le répertoire doit être spécifié au format adresse réseau même si le répertoire se trouve sur la machine locale ; ce répertoire doit être accessible depuis les postes ciblés.



Avant l'installation en mode administrateur, le répertoire cible pour le prototype de l'**Agent** (voir le paramètre TARGETDIR) ne doit pas contenir l'installateur de **Enterprise Agent** pour les réseaux avec **Active Directory** (<nom_du_package>.msi).



Après le déploiement du package administrateur, le répertoire :

```
<répertoire_cible>\Program Files\DrWeb  
Enterprise Suite
```

ne doit contenir que le fichier README.txt.

Exemples :

```
msiexec /a ES_Agent.msi /qn  
ESSERVERADDRESS=servername.net ESSERVERPATH=  
\win_serv\drwcs_inst\drwcsd.pub TARGETDIR=\\comp  
\share
```

```
msiexec /a ES_Agent.msi /qn  
ESSERVERADDRESS=192.168.14.1  
ESSERVERPATH="C:\Program Files\DrWeb Enterprise  
Server\Installer\drwcsd.pub" TARGETDIR=\\comp  
\share
```



Les mêmes paramètres peuvent être spécifiés en cas de mode graphique de l'installateur.

Puis il est nécessaire de spécifier l'installation du package (voir la description de la procédure [ci-dessous](#)) sur le serveur du réseau local sur lequel est installé le logiciel de gestion du service Active Directory.

(B) Configuration de l'installation de Dr.Web Enterprise Agent en mode graphique



Avant l'installation en mode administrateur, veuillez vous assurer que le répertoire cible pour le prototype de l'**Agent** ne contient pas l'installateur **Enterprise Agent** pour les réseaux avec **Active Directory** (`<nom_du_package>.msi`).



Après le déploiement du package administrateur, le répertoire :

```
<répertoire_cible>\Program Files\DrWeb  
Enterprise Suite
```

ne doit contenir que le fichier `README.txt`.

1. Afin de lancer l'installateur en mode graphique, exécutez la commande suivante :

```
msiexec /a <chemin_vers_installateur>\<nom_du_package>.msi
```

2. La fenêtre de l'assistant **InstallShield Wizard** apparaît et vous informe sur le produit en cours d'installation. Cliquez sur le bouton **Suivant**.



L'installateur de l'**Agent** utilise la langue spécifiée dans les options linguistiques de l'ordinateur.

3. Dans la nouvelle fenêtre, spécifiez le nom DNS ou l'adresse IP de **Serveur Enterprise** (voir [Annexe E3](#)). Spécifiez également l'emplacement de la clé publique de **Serveur Enterprise**



(drwcsd.pub). Cliquez ensuite sur le bouton **Suivant**.

4. Dans la fenêtre suivante, spécifiez le répertoire réseau vers lequel le prototype de l'**Agent** sera enregistré. Le chemin vers le prototype doit être spécifié au format adresse réseau même si le répertoire se trouve sur la machine locale ; ce répertoire doit être accessible depuis les postes ciblés. Cliquez ensuite sur **Installer**.
5. Après la fin de l'installation, la fenêtre de configuration permettant de spécifier l'installation des packages sur les postes dans le réseau sera affichée de manière automatique.

Configuration de l'installation du package sur les postes sélectionnés

1. Depuis le **Panneau de configuration** (ou depuis le menu **Démarrer** sous Windows Server 2003/2008, menu **Démarrer** → **Tous les programmes** sous Windows Server 2000) sélectionnez **Administrative Tools** → **Active Directory Users and Computers** (en mode graphique de l'installation de l'**Agent** cette fenêtre s'affiche de manière automatique).
2. Dans le domaine contenant les ordinateurs sur lesquels l'**Enterprise Agent** seront installés, créez une nouvelle **Unité** (sous Windows Server 2000 - **Unité d'organisation**) nommée par exemple **ESS**. Pour cela, depuis le menu contextuel sélectionnez **New** → **Organizational unit**. Dans la fenêtre qui apparaît, entrez le nom de cette nouvelle unité et cliquez sur **OK**. Ajoutez à cette unité les ordinateurs sur lesquels vous souhaitez installer l'**Agent**.
3. Ouvrez la fenêtre d'édition des politiques de groupe. Pour cela, procédez comme suit :
 - a) sous Windows Server 2000/2003 : dans le menu contextuel de l'unité créée **ESS**, sélectionnez l'élément **Propriétés**. Dans la fenêtre qui apparaît, passez à l'onglet **Politique de groupe**.
 - b) sous Windows Server 2008 : cliquez sur **Start** → **Administrative tools** → **Group Policy management**.
4. Spécifiez une politique de groupe pour l'unité créée. Pour cela,



procédez comme suit :

- a) Sous Windows Server 2000/2003 : double cliquez sur le bouton **Ajouter** et créez un élément de la liste avec le nom de la politique **ESS**. Double cliquez sur cet élément.
 - b) Sous Windows Server 2008 : dans le menu contextuel de l'unité créée **ESS**, sélectionnez l'élément **Create a GPO in this domain, and Link it here**. Dans la fenêtre qui apparaît, spécifiez le nom du nouvel objet de la politique de groupe et cliquez ensuite sur **OK**. Dans le menu contextuel de la nouvelle politique, sélectionnez l'élément **Edit**.
5. La fenêtre **Group Policy Object Editor** sera ouverte, spécifiez les paramètres relatifs à la politique de groupe créée à l'étape 4. Pour cela, procédez comme suit :
- a) Sous Windows Server 2000/2003 : depuis l'arborescence sélectionnez l'élément **Computer Configuration** → **Software Settings** → **Software Installations**.
 - b) Sous Windows Server 2008 : depuis l'arborescence sélectionnez l'élément **Computer Configuration** → **Politiques** → **Software Settings** → **Software Installations**.
6. Dans le menu contextuel de l'élément **Software Installations**, sélectionnez l'élément **New** → **Package**.
7. Spécifiez le package d'installation de l'**Agent**. Pour cela, spécifiez l'adresse de la ressource réseau partagée (prototype de l'**Agent** créé lors de l'installation en mode administrateur). Le chemin vers le répertoire contenant le package doit être spécifié au format adresse réseau même si le répertoire se trouve sur la machine locale.
8. La fenêtre **Deploy Software** apparaît. Sélectionnez l'option **Assigned**. Cliquez sur **OK**.
9. L'élément **Dr.Web Enterprise Agent** sera présent dans la fenêtre de gestion des politiques de groupe. Depuis le menu contextuel de cet élément sélectionnez **Properties**.
10. Dans la fenêtre de propriétés du package qui apparaît, passez à l'onglet **Deployment**. Cliquez sur le bouton **Advanced**.



11. La fenêtre **Advanced Deployment Options** sera ouverte.
 - ◆ Cochez la case **Ignore language when deploying this package**.
 - ◆ Si vous planifiez l'installation de l'**Agent Enterprise** avec un package msi configurable sur les OS 64 bits, activez la case **Make this 32-bit x86 application available to Win64 machines**.
12. Double cliquez sur **OK**.
13. **Enterprise Agent** sera installé sur les postes sélectionnés au prochain enregistrement dans le domaine.

Réalisation des politiques en fonction des installations antérieures de l'Agent

Lors de la spécification des politiques Active Directory relatives à l'installation de l'**Agent**, il est nécessaire de prendre en compte le cas où l'**Agent** pouvait déjà être installé sur le poste. Les trois variantes ci-dessous sont possibles :

1. **Enterprise Agent** n'est pas présent sur le poste.

Après l'application des politiques, l'**Agent** sera installé selon la règle générale.
2. **Enterprise Agent est déjà installé sur le poste mais sans utiliser le service Active Directory**.

Après l'application de la politique Active Directory, l'**Agent** installé reste sur le poste.



Dans ce cas-là, l'**Agent** est installé sur le poste, mais le service Active Directory considère l'**Agent** comme non installé. C'est pourquoi, à chaque démarrage du poste, il y aura des tentatives inutiles d'installer l'**Agent** via le service Active Directory.

Afin d'installer l'**Agent** via Active Directory, il est nécessaire de supprimer l'**Agent** de manière manuelle (ou avec le **Centre de Gestion**) et de redéterminer les politiques Active Directory pour



le poste en question.

3. Enterprise Agent est déjà installé sur le poste via le service Active Directory.

Après l'application de la politique :

- a) Si le poste dispose des droits de supprimer l'**Agent**, ce dernier sera supprimé depuis le poste. Afin d'installer l'**Agent** via Active Directory, il est nécessaire de redéterminer les politiques Active Directory pour ce poste.



Dans ce cas, il faut spécifier de nouveau les politiques relatives à l'installation de l'**Agent** puisque après la première spécification des politiques, l'**Agent** sera supprimé depuis le poste mais le service Active Directory va continuer à considérer l'**Agent** comme installé.

- b) Si le poste ne dispose pas des droits pour supprimer l'**Agent**, la spécification des politiques n'aura pas d'impact sur le statut de l'antivirus sur le poste. Pour continuer, il faut configurer les droits permettant de supprimer l'**Agent** (voir [Configuration des droits d'utilisateur](#)) puis redéterminer les politiques Active Directory pour ce poste. Les actions suivantes sont équivalentes à celles décrites à l'étape **a**).



La redétermination des politiques Active Directory peut être effectuée de n'importe quelle manière.

2.5. Installation de NAP Validator

Dr.Web NAP Validator sert à vérifier le fonctionnement de l'antivirus tournant sur les postes protégés.

Ce composant peut être installé sur le poste ayant le serveur NAP configuré.



Marche à suivre pour installer NAP Validator :

1. Exécutez le fichier de package d'installation. La fenêtre permettant de sélectionner une langue d'installation apparaît. Sélectionnez **Français** et cliquez sur **Suivant**.
2. La fenêtre de l'assistant **InstallShield Wizard** informant sur le produit en cours d'installation va s'ouvrir. Cliquez sur **Suivant**.
3. La fenêtre affichant le texte du Contrat de licence va s'ouvrir. Après avoir pris connaissance des termes du Contrat, cochez la case **J'accepte les termes du Contrat de licence** et cliquez sur le bouton **Suivant**.
4. Dans la fenêtre qui apparaît, dans les champs **Adresse** et **Port** entrez l'adresse IP et le port de **Serveur Enterprise**. Cliquez sur **Suivant**.
5. Cliquez sur le bouton **Installer**. Les actions suivantes du programme d'installation ne nécessitent aucune intervention de l'utilisateur.
6. Après la fin de l'installation, cliquez sur le bouton **Terminer**.

Après l'installation de **Dr.Web NAP Validator**, il est nécessaire d'ajouter **Serveur Enterprise** dans le groupe de serveurs NAP de confiance. Pour cela, procédez comme suit :

1. Ouvrez le composant de configuration du serveur NAP (commande `nps.msc`).
2. Dans la rubrique **Groupe de Serveurs de remédiation** cliquez sur le bouton **Ajouter**.
3. Dans la boîte de dialogue qui s'ouvre, spécifiez le nom pour le serveur de remédiation et l'adresse IP de **Serveur Enterprise**.
4. Pour sauvegarder les modifications apportées, cliquez sur **OK**.

2.6. Installation du Serveur proxy

Le réseau antivirus peut comprendre un ou plusieurs **Serveurs proxy**.



Pour sélectionner l'ordinateur sur lequel sera installé le **Serveur proxy**, il faut prendre en compte que le critère principal est l'accessibilité du **Serveur proxy** depuis tous les réseaux/fragments de réseau entre lesquels il doit rediriger des informations.



Les droits d'administrateur sur le poste sont requis pour installer le **Serveur proxy**.

La procédure d'installation du **Serveur proxy** est décrite ci-dessous. La marche à suivre peut varier en fonction de la version du package d'installation.

Marche à suivre pour installer le serveur proxy sur un ordinateur tournant sous Windows :

1. Exécutez le fichier de package d'installation. La fenêtre de l'assistant **InstallShield Wizard** informant sur le produit en cours d'installation apparaît. Cliquez sur le bouton **Next**.
2. La fenêtre affichant le texte du Contrat de Licence apparaît. Après avoir pris connaissance des termes de ce Contrat, cochez la case contre la rubrique **J'accepte les termes du Contrat de Licence** et cliquez ensuite sur le bouton **Suivant**.
3. La fenêtre de sélection du dossier d'installation apparaît. Si vous souhaitez modifier le dossier donné par défaut, cliquez sur le bouton **Change** et sélectionnez un dossier. Puis cliquez sur le bouton **Suivant**.
4. La fenêtre de configuration du **Serveur proxy** vous permet d'accéder aux paramètres suivants :
 - ◆ Dans le champ **Listen to**, spécifiez l'adresse IP "écoutée" par le **Serveur proxy**. Par défaut c'est - any (0.0.0.0) – ce qui signifie "écouter" toutes les interfaces.
 - ◆ Dans le champ **Port**, spécifiez le numéro du port qui va "écouter" le **Serveur proxy**. Par défaut c'est le port **2193** ou **23** pour le protocole NetBIOS.
 - ◆ Dans la liste déroulante **Protocol**, sélectionnez le type de protocole pour réceptionner les connexions entrantes par le **Serveur proxy**.



- ◆ Cochez la case **Enable discovery** afin d'activer le mode d'imitation du **Serveur**. Ce mode permet au **Scanner réseau** de détecter le **Serveur proxy** en tant que **Serveur Enterprise**.
- ◆ Dans le champ **Multicast group**, entrez l'adresse IP du groupe multi-adresses dont le **Serveur proxy** fera partie. L'interface spécifiée sera "écoutée" par le **Serveur proxy** afin d'assurer l'interaction avec les **Installeurs réseau** lors des recherches des **Serveur Enterprise** actifs dans le réseau. Si vous laissez le champ vide, le **Serveur proxy** ne sera inclus dans aucun groupe multi-adresses.
- ◆ La rubrique **Redirect to** vous permet de spécifier l'adresse ou une liste d'adresses de **Serveur Enterprise** dont l'une sera désignée pour accepter les connexions redirigées établies par le **Serveur proxy**.

Après la fin de la configuration du **Serveur proxy**, cliquez sur **Next**.

5. La fenêtre informant sur la disponibilité de l'installation du **Serveur proxy** va s'ouvrir. Cliquez alors sur le bouton **Install**.
6. Après la fin de l'installation, cliquez sur le bouton **Finish**.

Après la fin de l'installation, vous pouvez modifier les paramètres du **Serveur proxy**. Pour cela, vous pouvez utiliser le fichier de configuration `drwcsd-proxy.xml` se trouvant dans le dossier d'installation du **Serveur proxy**. Pour plus d'informations sur les paramètres du fichier de configuration, consultez l'[Annexe G4](#).

Pour installer le Serveur proxy sur un poste tournant sous UNIX, procédez comme suit :

Exécutez la commande suivante :

- ◆ sous OS **FreeBSD** :
`pkg_add <nom_du_fichier_de_distribution>.tbz`
- ◆ sous OS **Solaris** :
`bzip2 -d <nom_du_fichier_de_distribution>.bz2`
et puis :
`pkgadd -d <nom_du_fichier_de_distribution>`



◆ sous OS **Linux** :

- sous OS **Debian** et OS **Ubuntu** :

```
dpkg -i <nom_du_fichier_de_distribution>.deb
```

- **pour les distributions rpm** :

```
rpm -i <nom_du_fichier_de_distribution>.rpm
```

Il existe également des packages générique (generic packages) pouvant être installés sur n'importe quel système de la famille Linux, voire sur un système non listé parmi les OS supportés. L'installation se fait avec l'installateur intégré dans le package. Veuillez utiliser la commande :

```
tar -xjf <nom_du_fichier_de_distribution>.tar.bz2
```

Puis il est nécessaire de déplacer tout le contenu de l'archive extraite vers le répertoire racine.



Lors de l'installation du logiciel sous OS **FreeBSD** le script rc suivant sera créé :

```
/usr/local/etc/rc.d/0.dwcp-proxy.sh.
```

Utilisez les commandes :

- ◆ `/usr/local/etc/rc.d/0.dwcp-proxy.sh stop` - pour arrêter le **Serveur proxy** manuellement ;
- ◆ `/usr/local/etc/rc.d/0.dwcp-proxy.sh start` - pour arrêter le **Serveur proxy** de manière automatique.

Lors de l'installation du logiciel sous **Linux** ou **Solaris**, le script `init` pour le lancement et l'arrêt du **Serveur proxy** sera créé `/etc/init.d/dwcp-proxy`.



2.7. Suppression des composants sélectionnés de Dr.Web Enterprise Security Suite

2.7.1. Suppression des composants sous Windows®

Suppression de Dr.Web Enterprise Server

Afin de désinstaller le logiciel de **Serveur Enterprise** ou le module ajoutable **Dr.Web Browser-Plugin**, lancez le package d'installation dans la version correspondant à la version installée. L'installateur va détecter le produit installé de manière automatique et proposera de le supprimer. Pour désinstaller le logiciel, cliquez sur le bouton **Supprimer**.

La suppression du logiciel de **Serveur Enterprise** et du module ajoutable **Dr.Web Browser-Plugin** peut également être effectuée avec les outils standard de l'OS Windows via l'élément suivant : **Panneau de configuration** → **Ajout/Suppression de programmes**.

Suppression de Dr.Web Enterprise Agent et du package antivirus via le réseau





L'installation à distance ainsi que la suppression du logiciel de l'**Agent** ne peuvent être réalisées que dans le réseau local et nécessitent les droits d'administrateur dans ce réseau.



En cas de suppression de l'**Agent** et du package antivirus via le **Centre de Contrôle**, la **Quarantaine** ne sera pas supprimée depuis le poste.

Marche à suivre pour supprimer l'antivirus du poste de manière distante (uniquement pour les OS Windows) :

1. Sélectionnez l'élément **Réseau antivirus** depuis le menu principal du **Centre de Gestion**.
2. Dans la fenêtre qui apparaît, depuis l'arborescence, sélectionnez un groupe ou des postes.
3. Depuis la barre d'outils de l'arborescence du réseau antivirus cliquez sur les boutons  **Général** →  **Désinstaller Dr.Web Agent**.
4. Le logiciel de l'**Agent** et le package antivirus seront supprimés sur les postes sélectionnés.



Si le processus de suppression est lancé alors qu'il n'y a pas de connexion entre le **Serveur Enterprise** et le poste antivirus, la suppression du logiciel de l'**Agent** sur le poste sélectionné sera effectuée lorsque la connexion aura été rétablie.

Suppression de Dr.Web Enterprise Agent et du package antivirus de manière locale



La suppression locale de l'**Agent** et du package antivirus est possible à condition que cette option soit autorisée sur le **Serveur** dans la rubrique **Droits**.

Il existe deux variantes de suppression de l'antivirus (**Agent** et package antivirus) depuis le poste :

1. Avec les outils standard de Windows.
2. Avec l'installateur de l'**Agent**.



En cas de suppression de l'**Agent** et du package antivirus avec les outils standards de Windows ou avec l'installateur de l' **Agent**, il sera demandé à l'utilisateur de supprimer la **Quarantaine**.

Suppression avec les outils standard de Windows



Cette technique n'est applicable que dans le cas où, durant l'installation de l'**Agent** en mode graphique, la case **Enregistrer l'Agent dans la liste des programmes installés** a été cochée.

Dans le cas où l'**Agent** a été installé avec l'installateur en tâche de fond, la suppression de l'antivirus avec les outils standards ne sera possible qu'à condition que la clé - `regagent ait` été appliquée lors de l'installation.

Pour supprimer l'**Agent** et le package antivirus avec des outils standards de Windows, utilisez l'élément suivant **Panneau de configuration** → **Ajout/Suppression de programmes** (pour en savoir plus, consultez le Manuel Utilisateur pour l'**Agent**).

Suppression avec l'installateur

Pour désinstaller le logiciel de l'**Agent** et le package antivirus depuis le poste de manière locale, il est nécessaire d'exécuter depuis le dossier d'installation d'**Enterprise Agent** (par défaut - C:\Program Files\DrWeb Enterprise Suite) la commande `drwinst` accompagnée du paramètre `-uninstall` (ou du paramètre `-uninstall -interactive`, si vous souhaitez surveiller la progression du processus de suppression).

Exemple :

```
drwinst -uninstall -interactive
```




2.7.2. Suppression de Dr.Web Enterprise Agent avec le service Active Directory

1. Dans le panneau de configuration sous Windows, sélectionnez l'élément **Outils d'administration** puis l'élément **Active Directory - Users and computers**.
2. Dans le domaine, sélectionnez l'unité d'organisation **ESS** que vous avez créée. Depuis le menu contextuel, sélectionnez l'élément **Properties**. La fenêtre **ESS Properties** s'ouvre.
3. Passez à l'onglet **Group Policy**. Sélectionnez l'élément **ESS Politicies** dans la liste. Double cliquez sur cet élément. La fenêtre **Group Policy Object Editor** va s'ouvrir.
4. Dans l'arborescence, sélectionnez **Computer configuration** → **Software settings** → **Software installations** → **Package**. Puis dans le menu contextuel du package contenant le package d'installation de l'**Agent**, sélectionnez **All tasks** → **Uninstall** → **OK**.
5. Dans l'onglet **Group Policy**, cliquez sur **OK**.
6. **Enterprise Agent** sera supprimé sur les postes lors du prochain enregistrement dans le domaine.

2.7.3. Suppression de Dr.Web Enterprise Server sous UNIX®



Toutes les actions relatives à la suppression doivent être effectuées sous le nom de super-utilisateur **root**.

Afin de supprimer Dr.Web Enterprise Server :

1. Exécutez la commande suivante :

Pour le Serveur sous OS	Commande
FreeBSD	<code>pkg_delete drweb-esuite</code>



Pour le Serveur sous OS		Commande
Solaris		1. Arrêtez le Serveur : <code>/etc/init.d/drwcsd stop</code> 2. Exécutez la commande : <code>pkgrm DWEBesuit</code>
Linux	Debian	<code>dpkg -r drweb-esuite</code>
	Ubuntu	
	package rpm	<code>rpm -e drweb-esuite</code>
	package generic	<code>/opt/drwcs/bin/drweb-esuite-uninstall.sh</code>



La suppression du **Serveur** peut être interrompue à tout moment par envoi au processus d'un des signaux suivants : `SIGHUP`, `SIGINT`, `SIGTERM`, `SIGQUIT` et `SIGWINCH` (sous **FreeBSD** la modification des dimensions de la fenêtre de terminal entraîne un envoi du signal `SIGWINCH`). Il est fortement déconseillé d'interrompre le processus de suppression sans nécessité, sinon il vaut mieux l'arrêter le plus tôt possible.

2. Puis (en cas de suppression du **Serveur** installé sous **Solaris**) il est nécessaire de confirmer la suppression du logiciel ainsi que d'accepter l'exécution des scripts de suppression en mode administrateur.



Lors de la suppression du **Serveur** (sous **FreeBSD** ou **Linux**) les processus serveur seront arrêtés automatiquement, la base de données, les fichiers clés et les fichiers de configuration seront sauvegardés - sous **Linux** - vers le dossier spécifié par `${HOME}/drwcs/` (en général, c'est `/root/drwcs/`). Sous **FreeBSD**, il sera proposé de sélectionner un chemin, par défaut c'est `/var/tmp/drwcs`.

Sous **Solaris**, après la suppression du **Serveur**, la base de données, les fichiers clés et les fichiers de configuration seront copiés vers le dossier `/var/tmp/DrWebES`.



Marche à suivre pour supprimer le module Dr.Web Browser-Plugin :

Exécutez la commande suivante :

- ◆ pour les packages **deb** :
`dpkg -P drweb-esuite-plugins`
- ◆ pour les packages **rpm** :
`rpm -e drweb-esuite-plugins`
- ◆ pour d'autres systèmes (packages **tar.bz2** et **tar.gz**):
`rm -f <dossier_des_modules>/libnp*.so`
Par exemple pour le navigateur Mozilla Firefox :
`rm -f /usr/lib/mozilla/plugins/libnp*.so`

2.7.4. Suppression du Serveur proxy

Suppression du Serveur proxy sous Windows



Lorsque vous supprimez le **Serveur proxy**, le fichier de configuration `drwcsd-proxy.xml` sera supprimé. Si besoin est, sauvegardez le fichier de configuration manuellement avant de supprimer le **Serveur proxy**.

La suppression du **Serveur proxy** est effectuée avec les outils standard de l'OS Windows via le **Panneau de configuration** → **Ajout et suppression des programmes** (**Programmes et fonctionnalités** sous OS Windows 2008).



Suppression du Serveur proxy sous l'OS de la famille UNIX

Pour supprimer le serveur proxy, procédez comme suit :

Pour le Serveur proxy sous OS		Commande
FreeBSD		<code>pkg_delete drweb-esuite-proxy</code>
Solaris		<code>pkgrm DWEBespxy</code>
Linux	package deb	<code>dpkg -P drweb-esuite-proxy</code>
	package rpm	<code>rpm -e drweb-esuite-proxy</code>
	package generic	Supprimez manuellement les fichiers se trouvant dans le répertoire d'installation du Serveur proxy .



Chapitre 3. Composants du réseau antivirus et leur interface

3.1. Dr.Web Enterprise Server

Le réseau antivirus doit comprendre au moins un **Serveur Enterprise**.



Pour augmenter la fiabilité et les performances du réseau antivirus ainsi que pour répartir la charge, **Dr.Web ESS** permet de créer un réseau antivirus à plusieurs **Serveurs**. Dans ce cas, le logiciel de serveur s'installe simultanément sur plusieurs postes.

Dr.Web Enterprise Server est un service qui reste en permanence en mémoire vive. Le logiciel de **Serveur Enterprise** est conçu pour divers OS (consultez la liste complète des systèmes supportés dans l'[Annexe A](#)).

Fonctions clés

Dr.Web Enterprise Server exécute les fonctions suivantes :

- ◆ initialisation de l'installation des packages antivirus sur un poste sélectionné ou sur un groupe de postes,
- ◆ envoi de requêtes pour le numéro de version du package antivirus ainsi que pour les dates de création et les numéros de version des bases virales sur chaque poste protégé,
- ◆ mise à jour du répertoire d'installation centralisée et du répertoire de mises à jour,
- ◆ mise à jour des bases virales et des fichiers exécutables des packages antivirus ainsi que des exécutables des composants du réseau antivirus sur les postes protégés.



Récolte des informations sur le statut du réseau antivirus

Serveur Enterprise recueille et journalise les informations sur le fonctionnement des packages antivirus, il reçoit ces informations depuis les logiciels installés sur les postes protégés (**Enterprise Agent** décrits ci-après). La journalisation est effectuée dans un journal commun se présentant sous forme de base de données. Dans un réseau de taille moyenne (200-300 pc au maximum) la base de données interne peut être utilisée pour écrire le journal commun (le log) des événements. Pour les grands réseaux il est possible d'utiliser des bases de données externes.



La BD interne peut être utilisée à condition que le nombre total de postes connectés au **Serveur** ne dépasse pas 200-300 postes. Si les caractéristiques de l'ordinateur sur lequel tourne **Serveur Enterprise** et la charge relative à d'autres tâches exécutées sur cet ordinateur le permettent, il est possible de connecter jusqu'à 1000 postes.

Sinon, une BD externe doit être utilisée.

En cas d'utilisation de la BD externe et si plus de 10000 postes sont connectés au **Serveur**, il est recommandé de respecter les pré-requis minimum suivants :

- ◆ processeur 3GHz,
- ◆ mémoire vive - à partir de 4 Go pour **Serveur Enterprise**, et à partir de 8 Go pour le serveur de BD,
- ◆ OS de la famille UNIX.

Les informations à récolter et à écrire dans le journal commun d'événements :

- ◆ informations sur la version des packages antivirus sur les postes protégés,
- ◆ heure et date d'installation et de mise à jour du logiciel sur les postes antivirus (y compris la version du logiciel),
- ◆ heure et date de mise à jour des bases virales et leurs versions,



- ◆ information sur la version du système d'exploitation installé sur les postes protégés, sur le type de processeur, l'emplacement des répertoires système etc.,
- ◆ configuration et mode de fonctionnement des packages antivirus (méthodes heuristiques, liste des types de fichiers à analyser, actions en cas de détection des virus etc.),
- ◆ informations sur les événements viraux et notamment les noms des virus détectés, la date de la détection, les actions réalisées, les résultats de la neutralisation, etc.

Serveur Enterprise notifie l'administrateur du réseau antivirus sur les événements survenus lors du fonctionnement du logiciel. L'administrateur peut être notifié par email ou via les outils standards de Windows. Pour en savoir plus sur la configuration des événements et d'autres paramètres des notifications, consultez le paragraphe [Configuration des notifications](#).

Interface

Serveur Enterprise n'a pas d'interface intégrée. Les commandes standard relatives à la gestion du **Serveur** se trouvent dans le répertoire [Gestion du Serveur](#).

En général, la gestion de **Serveur Enterprise** se fait avec le **Centre de Gestion** qui sert d'interface externe au **Serveur**.

Démarrage et arrêt du Dr.Web Enterprise Server

Par défaut, **Serveur Enterprise** démarre de manière automatique après chaque installation et après chaque redémarrage du système.

Vous pouvez également démarrer, redémarrer ou arrêter **Serveur Enterprise** de l'une des façons suivantes :

Pour OS de la famille UNIX

- ◆ Avec la commande de console (voir aussi l'Annexe [H5. Dr.Web Enterprise Server](#)) :



- Démarrage :
 - Pour OS FreeBSD:
/usr/local/etc/rc.d/drwcsd.sh start
 - Pour OS Linux et OS Solaris:
/etc/init.d/drwcsd start
- Redémarrage :
 - Pour OS FreeBSD:
/usr/local/etc/rc.d/drwcsd.sh restart
 - Pour OS Linux et OS Solaris:
/etc/init.d/drwcsd restart
- Arrêt :
 - Pour OS FreeBSD :
/usr/local/etc/rc.d/drwcsd.sh stop
 - Pour OS Linux et OS Solaris:
/etc/init.d/drwcsd stop
- ◆ Arrêt et redémarrage via le **Centre de Gestion** :
 - Dans la partie **Administration** : le redémarrage avec le bouton, l'arrêt avec le bouton (n'est pas présent en version pour l'OS Solaris).

Pour OS Windows

- ◆ Cas général :
 - Avec la commande correspondante se trouvant dans le menu **Démarrer** → **Tous les programmes** → **Dr.Web Enterprise Server**.
 - Avec les outils de gestion des services depuis la rubrique **Outils d'administration** dans le **Panneau de configuration** Windows.
- ◆ Arrêt et redémarrage via le **Centre de Gestion** :
 - Dans la partie **Administration** : le redémarrage avec le bouton, l'arrêt avec le bouton.
- ◆ Avec les commandes de console exécutées depuis le sous-dossier `bin` du dossier d'installation du **Serveur** (voir aussi l'Annexe [H5. Dr.Web Enterprise Server](#)) :
 - `drwcsd start` — démarrage du **Serveur**.



- `drwcsd restart` — redémarrage complet du service du **Serveur**.
- `drwcsd stop` — terminaison normale du **Serveur**.

3.2. Dr.Web Enterprise Agent

Principe de fonctionnement

La protection antivirus des postes de travail est assurée par les packages antivirus **Dr.Web** conçus pour les systèmes d'exploitation appropriés.

Au sein de l'**Antivirus Dr.Web ESS** ces packages sont gérés par le composant (**Enterprise Agent**) qui est installé sur le poste protégé et reste en permanence dans la mémoire. En étant connecté au **Serveur Enterprise**, l'administrateur peut configurer de façon centralisée les **antivirus** sur les postes de travail via le **Centre de Gestion** ainsi que créer une planification des analyses, il peut également consulter les statistiques et d'autres informations relatives aux composants antivirus, lancer et arrêter le scan antivirus etc.

Serveur Enterprise télécharge des mises à jour et en diffuse vers les **Agents** connectés. Ainsi, **Enterprise Agent** permet d'installer de manière automatique, de maintenir et de gérer la meilleure stratégie de protection antivirus quel que soit le niveau de compétence des utilisateurs.

Cependant, au cas où le poste est temporairement déconnecté du réseau antivirus, **Enterprise Agent** utilise une copie locale de la configuration et la protection antivirus sur le poste reste donc opérationnelle (durant une période inférieure ou égale à la durée de la licence de l'utilisateur), mais les bases virales et le logiciel ne seront pas mis à jour.

La procédure de mise à jour des **Agents** mobiles est décrite dans le paragraphe [Mise à jour des Agents mobiles Dr.Web Enterprise Agent](#).



Fonctions clés

Dr.Web Enterprise Agent exécute les fonctions suivantes :

- ◆ installation, mise à jour et configuration du package antivirus **Dr.Web**, démarrage du scan ainsi que réalisation des tâches définies par **Serveur Enterprise** ;
- ◆ activation des composants du package antivirus Dr.Web via l'**interface** spécialisée ;
- ◆ transmission des résultats des tâches accomplies à **Serveur Enterprise** ;
- ◆ transmission des messages à **Serveur Enterprise** dans le cas où des événements préconfigurés liés au fonctionnement du package antivirus surviennent.

Chaque **Enterprise Agent** est connecté à **Serveur Enterprise** et fait partie d'un ou plusieurs groupes enregistrés sur ce **Serveur** (pour en savoir plus, consultez le paragraphe [Groupes système et groupes utilisateur](#)). Les échanges d'information entre l'**Agent** et le **Serveur** sont effectués via le protocole utilisé dans le réseau local (TCP/IP, IPX ou NetBIOS).



Ci-après, le poste protégé avec l'**Agent** installé sera nommé, selon ses fonctions dans le réseau antivirus, le *poste de travail*. Il est à noter que selon les fonctions accomplies, telle machine peut être aussi bien un poste de travail qu'un serveur du réseau local.

Interface de gestion sous OS Windows

Lancé sous l'OS Windows, **Enterprise Agent** affiche l'icône  dans la zone de notification de la barre des tâches.

Les variantes possibles de l'apparence de l'icône de l'**Agent** et le statut des composants correspondant sont présentées dans le [tableau 3-1](#).



Tableau 3-1. L'apparence de l'icône et le statut correspondant des composants

Apparence	Description	Action
	Araignée noire sur un fond vert.	L' Agent est opérationnel et se connecte au Serveur .
	Les flèches rouge sur un fond vert.	Pas de connexion au Serveur .
	Point d'exclamation dans un triangle jaune sur un fond vert.	L' Agent requiert un redémarrage de l'ordinateur ou les composants SelfPROtection ou Spider Guard sont inactifs.
	La couleur de fond passe du vert au rouge.	Une erreur est survenue lors de la mise à jour des composants.
	La couleur de fond reste en permanence rouge.	L' Agent est arrêté ou inactif.
	La couleur de fond reste jaune.	L' Agent fonctionne en mode itinérant (pour en savoir plus, consultez Mise à jour des Agents mobiles Dr.Web Enterprise Agent).

Certaines fonctions de gestion du poste sont accessibles depuis le menu contextuel de l'icône de l'**Agent** présenté sur la [figure 3-1](#).

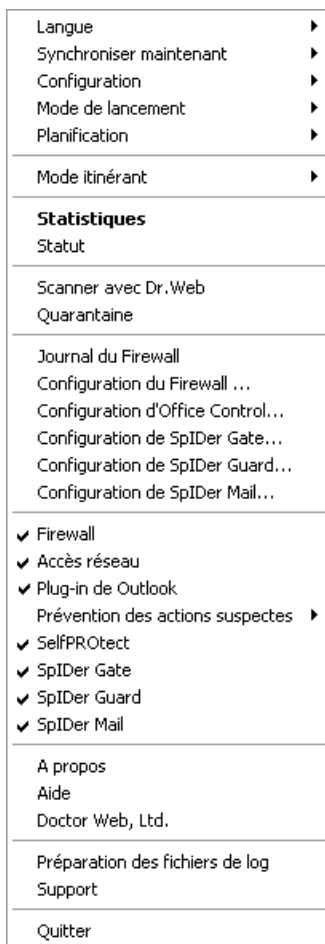


Figure 3-1. Menu contextuel d'Enterprise Agent

Le jeu de paramètres disponibles depuis le menu contextuel de l'**Agent** est fonction de la configuration du poste déterminée sur **Serveur Enterprise** ainsi que des droits de l'utilisateur sur le poste.



Pour en savoir plus sur le jeu de paramètres d'**Enterprise Agent** ainsi que sur les fonctions relatives à la gestion du poste, consultez le Manuel d'**Enterprise Agent**.

Pour en savoir plus sur la configuration d'**Enterprise Agent**, consultez le paragraphe [Configuration de Dr.Web Enterprise Agent](#).

Démarrage et arrêt de Dr.Web Enterprise Agent sous OS Windows



La commande **Quitter** retire l'icône de la zone de notifications mais n'arrête pas le fonctionnement de l'**Agent**.

Pour arrêter le programme, exécutez la commande ci-dessous :

```
net stop drwagntd
```

Il n'est pas recommandé d'arrêter l'**Agent** puisque dans ce cas-là, l'antivirus n'est pas mis à jour et le **Serveur** ne reçoit pas d'information sur le statut du poste. D'ailleurs, la protection permanente du poste reste active.

L'**Agent** redémarre automatiquement au redémarrage de l'ordinateur. Pour redémarrer l'**Agent** sans redémarrer la machine, exécutez la commande suivante depuis la ligne de commande :

```
net start drwagntd
```



3.3. Centre de Gestion Dr.Web

Le **Centre de Gestion Dr.Web** sert à gérer le réseau antivirus dans son ensemble (y compris les modifications de sa composition et structure), les composants du réseau ainsi que la configuration du **Serveur Enterprise**.



Pour utiliser le **Centre de Gestion** avec le navigateur web Microsoft Internet Explorer, il est nécessaire d'ajouter l'adresse du **Centre de Gestion** dans la zone de confiance : **Outils** → **Options Internet** → **Sécurité** → **Sites de confiance**.

L'utilisation correcte du **Centre de Gestion** sous le navigateur web Chrome requiert que les cookies soient activés dans les options du navigateur.

Connexion à Dr.Web Enterprise Server

Le **Centre de Gestion** est accessible depuis n'importe quel ordinateur ayant un accès réseau à **Serveur Enterprise** à l'adresse suivante :

`http://<adresse_Serveur>:9080`

ou

`https://<adresse_Serveur>:9081`

comme valeur `<adresse_Serveur>` spécifiez l'adresse IP ou le nom de domaine de l'ordinateur sur lequel est installé **Serveur Enterprise**.



Les numéros des ports relatifs à la connexion http et à la connexion sécurisée https ne sont pas les mêmes : 9080 et 9081 respectivement.

Dans la boîte de dialogue d'authentification, entrez le nom et le mot de passe administrateur (le nom de l'administrateur spécifié par défaut est **admin**, le mot de passe est celui que vous avez spécifié lors de l'installation du **Serveur**).



En cas de téléchargement via https (connexion sécurisée utilisant SSL), le navigateur demande de confirmer le certificat utilisé par le **Serveur**. Dans ce cas, la demande peut générer une alerte de la part du navigateur, notamment à propos de l'invalidité du certificat. Ces alertes sont transmises à l'utilisateur car le certificat est inconnu pour le navigateur. Afin de pouvoir télécharger le **Centre de Gestion**, il faut accepter le certificat proposé. Sinon le téléchargement est impossible.



Avec certaines versions de navigateur web, par exemple **Firefox 3** ou supérieur, une erreur se produit lors du téléchargement via https et le **Centre de Gestion** ne sera pas téléchargé. Dans ce cas-là, il est nécessaire de sélectionner l'élément **Ajouter le site dans la liste des exclusions** depuis la page informant sur l'erreur (au-dessous du message d'erreur). Là, l'accès au **Centre de Gestion** sera autorisé.

Interface du Centre de Gestion Dr.Web

Le fenêtre du **Centre de Gestion** (voir figure 3-2) comprend deux zones : *l'en-tête* et la *zone de travail*.

L'en-tête comprend :

- ◆ le logo du produit **Dr.Web Enterprise Security Suite** : en cliquant dessus, la fenêtre d'accueil du **Centre de Gestion** s'affiche (la fenêtre est la même que celle de l'élément **Réseau antivirus** du menu principal),
- ◆ [menu principal](#),
- ◆ le nom du compte administrateur spécifié lors de l'authentification pour accéder au **Centre de Gestion**,
- ◆ le bouton **Logout** pour terminer la session du **Centre de Gestion**.



Si [l'authentification automatique](#) est activée dans le **Centre de Gestion**, lorsque vous pressez le bouton **Logout**, les informations sur le nom et sur le mot de passe de l'administrateur seront effacées.



Pour accéder de nouveau au **Centre de Gestion**, vous devez passer une procédure d'authentification et entrez votre nom et le mot de passe. En cas de [l'authentification automatique](#) activée, le nom et le mot de passe spécifiés seront sauvegardés dans le navigateur web et votre authentification dans le **Centre de Gestion** devient alors automatique (sans saisir le nom et le mot de passe) jusqu'au moment où vous pressez de nouveau le bouton **Logout**.

La *zone de travail* présente les fonctions principales du **Centre de Gestion**. Elle comprend deux ou trois panneaux en fonction des actions réalisées. Le système des menus présenté dans les panneaux s'ouvre de gauche à droite :

- ◆ *le menu de gestion* est toujours à gauche,
- ◆ en fonction de l'élément sélectionné depuis le menu de gestion, l'un ou les deux autres panneaux de menu s'affichent. Si les deux panneaux s'affichent, la partie droite comprend les propriétés ou les champs relatifs aux paramètres des éléments se trouvant dans le panneau central.

La langue de l'interface est spécifiée séparément pour chaque compte administrateur (voir [Gestion des comptes administrateur](#)).

Menu principal

Le menu principal du **Centre de Gestion** comprend les éléments suivants :

- ◆ [Administration](#),
- ◆ [Réseau antivirus](#),
- ◆ [Préférences](#),
- ◆ [Liaisons](#),
- ◆ [Aide](#),
- ◆ ainsi que [Panneau de recherche](#).

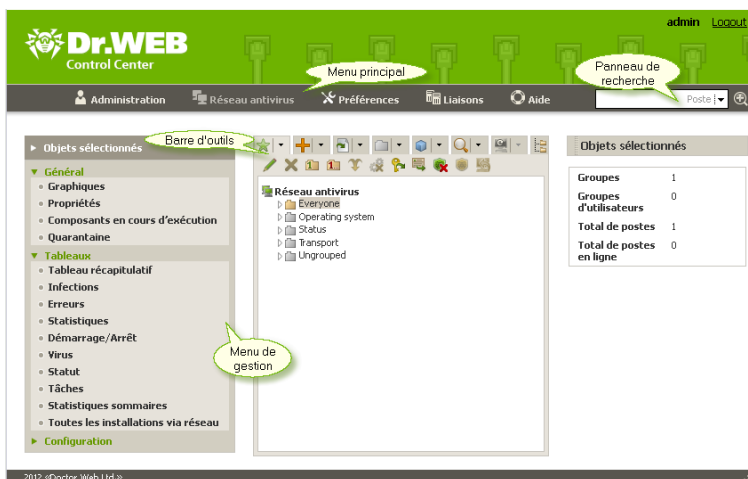


Figure 3-2. Fenêtre du Centre de Gestion. Cliquez sur un élément du menu principal pour afficher sa description

Panneau de recherche

Le *panneau de recherche* se trouvant dans la partie droite du menu principal du **Centre de Gestion** sert à faciliter les recherches. Le panneau permet de rechercher des groupes ainsi que des postes conformément aux paramètres spécifiés.

Pour rechercher un poste ou un groupe de postes, procédez comme suit :


1. Dans la liste déroulante du panneau de recherche sélectionnez un critère de recherche :
 - ◆ **Poste** - pour rechercher le poste par son nom,
 - ◆ **Groupe** - pour rechercher les groupes par leurs noms,
 - ◆ **ID** - pour rechercher les groupes et les postes par leurs identificateurs uniques,
 - ◆ **Description** - pour rechercher les groupes et les postes par leurs descriptions,



- ◆ **Adresse IP** - pour rechercher les postes par leur adresse IP.
2. Saisissez les informations d'après lesquelles la recherche sera effectuée. Vous pouvez entrer :
 - ◆ une ligne afin d'obtenir une coïncidence totale avec le paramètre de recherche,
 - ◆ un masque correspondant à la ligne recherchée : les symboles * et ? sont autorisés.
 3. Pressez la touche ENTER pour commencer la recherche.
 4. Tous les éléments trouvés seront affichés dans l'arborescence conformément aux paramètres de recherche :
 - ◆ en cas de recherche d'un poste, toutes les appartenances à des groupes seront affichées,
 - ◆ dans le cas où aucun élément n'est trouvé, l'arborescence s'affichera vide et accompagnée du message suivant :
Aucun résultat de recherche.

Vous pouvez également utiliser l'option **Recherche avancée**.

Pour réaliser une recherche avancée, procédez comme suit :

1. Cliquez sur le bouton  se trouvant sur le panneau de recherche.
2. Depuis le panneau **Recherche des groupes et des postes** spécifiez les paramètres suivants :
 - ◆ **Nom de poste** - saisissez le nom d'après lequel la recherche par nom de poste sera effectuée.
 - ◆ **Nom de groupe** - saisissez le nom d'après lequel la recherche par nom de groupe sera effectuée.
 - ◆ **ID** - saisissez la ligne d'après laquelle la recherche par ID des groupes et des postes sera effectuée.
 - ◆ **Adresse IP du poste** - saisissez l'adresse d'après laquelle la recherche par l'adresse IP du poste sera effectuée.
 - ◆ **Description** - Saisissez une ligne de description d'après laquelle la recherche sera effectuée.



Vous pouvez paramétrer les valeurs pour un, plusieurs ou pour tous les champs de recherche avancée.

Si vous spécifiez plusieurs champs, les éléments pouvant satisfaire au moins à une condition spécifiée sera recherché (réunion des valeurs de recherche - fonction *OU*).


3. Après avoir spécifié les paramètres nécessaires, cliquez sur le bouton **Rechercher**.
4. Les éléments retrouvés seront affichés dans l'arborescence, sinon le message suivant s'affichera : **Aucun résultat de recherche**.

3.3.1. Administration

Dans le menu principal du **Centre de Gestion**, sélectionnez l'élément **Administration**. Pour consulter ou éditer les informations affichées dans la fenêtre qui apparaît, utilisez le menu de gestion se trouvant dans la partie gauche de la fenêtre.

Le menu de gestion comprend les éléments suivants :

1. Administration

- ◆ **Dr.Web Enterprise Server** — ouvre le panneau permettant de consulter les informations principales sur le **Server**, ce panneau vous permet également de redémarrer le serveur avec le bouton  ou de l'arrêter avec le bouton  (l'option n'est pas présente dans la version pour Solaris) se trouvant en haut dans la partie droite du panneau ;
- ◆ **Postes non approuvés** — ouvre le panneau affichant la liste des postes non approuvés (voir [Politique de connexion des postes](#)) ;
- ◆ **Gestionnaire de licence** — permet de gérer les fichiers clés de licence relatifs au **Serveur** et aux **Agents** (voir [Gestionnaire de licence](#)) ;
- ◆ **Clés de chiffrement** — permet d'exporter (sauvegarder de manière locale) les clés publiques et privées de chiffrement.



2. Tableaux

- ◆ **Journal d'audit** — permet de consulter le journal des événements et des modifications effectuées via le **Centre de Gestion** ;
- ◆ **Log d'exécution des tâches** — cet élément comprend une liste des tâches définies sur le **Serveur** et accompagnées des notes sur leur exécution ou des commentaires ;
- ◆ **Statistiques du serveur** — cet élément contient des statistiques sur le **Serveur** sélectionné.

3. Configuration

- ◆ **Administrateurs** — ouvre le panneau permettant de gérer les comptes administrateur du réseau antivirus (voir [Gestion des comptes administrateur](#)) ;
- ◆ **Authentification** — ouvre le panneau permettant de gérer l'authentification des administrateurs dans le **Centre de Gestion** (voir [Authentification des administrateurs](#)) ;
- ◆ **Statut du dépôt des produits** — cet élément sert à vérifier le statut du dépôt des produits : la date de la dernière mise à jour des composants du dépôt et leur statut (voir [Statut du dépôt des produits](#)) ;
- ◆ **Configuration du dépôt des produits** — cet élément ouvre l'éditeur du dépôt des produits (voir [Editeur de configuration du dépôt des produits](#)) ;
- ◆ **Configuration de Dr.Web Enterprise Server** — cet élément ouvre le panneau des principaux paramètres du **Serveur** (voir [Configuration de Dr.Web Enterprise Server](#)) ;
- ◆ **Planification de Dr.Web Enterprise Server** — cet élément ouvre le panneau de configuration de la planification des tâches du **Serveur** (voir [Configuration de planification de Dr.Web Enterprise Server](#)) ;
- ◆ **Editeur de templates** — cet élément ouvre la fenêtre de l'éditeur des templates de notifications (voir [Configuration des notifications](#)).



4. Installations

- ◆ **Scanner réseau** — cet élément permet de spécifier une liste des réseaux et de scanner les réseaux afin de détecter la présence du logiciel antivirus, le statut de la protection ainsi que d'effectuer l'installation de l'antivirus (voir [Scanner réseau](#)) ;
- ◆ **Installation via réseau** — cet élément permet de faciliter la procédure d'installation de l'**Agent** sur les postes (voir [Installation de Dr.Web Enterprise Agent via le Centre de Gestion](#)).

3.3.2. Réseau antivirus

Dans le menu principal du **Centre de Gestion**, sélectionnez l'élément **Réseau antivirus**. Pour consulter ou éditer les informations affichées dans la fenêtre qui apparaît, utilisez le menu de gestion se trouvant dans la partie gauche de la fenêtre.

Arborescence

L'arborescence du réseau antivirus se trouve dans la partie centrale de la fenêtre. Cette liste présente la structure hiérarchique des éléments du réseau antivirus. Les noeuds de l'arborescence sont des [groupes](#) et les [postes](#) appartenant à ces groupes.

Les actions suivantes peuvent être appliquées aux éléments de l'arborescence :

- ◆ cliquez sur le nom du groupe ou du poste afin d'afficher le menu de gestion (dans la partie gauche de la fenêtre) relatif à l'élément sélectionné ;
- ◆ cliquer sur l'icône du groupe afin de consulter la composition du groupe.








Pour sélectionner plusieurs postes ou groupes dans l'arborescence, utilisez la souris tout en maintenant pressée la touche CTRL ou SHIFT.






L'apparence de l'icône est fonction du type ou du statut de l'élément sélectionné (voir le [tableau 3-2](#)).

Tableau 3-2. Apparence des icônes de l'arborescence

icône	Apparence	Description
Groupes		
	dossier jaune	Groupes qui sont toujours présents dans l'arborescence.
	dossier blanc	Groupes dont l'affichage peut être désactivé s'ils sont vides.
Postes de travail		
	icône verte	Poste disponible avec l'antivirus installé.
	icône grise	Poste inaccessible.
	icône barrée	L'antivirus est désinstallé sur le poste.



Si des configurations personnalisées sont spécifiées pour un poste ou pour un groupe (ou bien qu'un groupe contient des postes ayant des configurations personnalisées), dans l'arborescence, les icônes correspondantes du groupe ou du poste seront accompagnées de l'image . Par exemple, si des configurations personnalisées sont spécifiées pour un poste accessible avec l'antivirus installé, l'apparence de son icône est la suivante : .

Pour afficher les icônes avec les configurations personnalisées, sélectionnez l'élément  **Configuration de l'arborescence** depuis la barre d'outils et cochez ensuite la case **Afficher les configurations personnalisées**.

Les éléments de l'arborescence du réseau antivirus peuvent être gérés depuis la barre d'outils de l'arborescence.



Barre d'outils

La barre d'outils de l'arborescence comprend les éléments suivants :

★ **Général.** Cet élément permet de gérer les paramètres communs de l'arborescence. Sélectionnez un élément dans la liste déroulante :

✗ **Supprimer les objets sélectionnés.** Cet élément permet de supprimer les objets depuis l'arborescence. Pour cela, sélectionnez un ou plusieurs éléments dans la liste et cliquez sur le bouton **Supprimer les objets sélectionnés**.

✍ **Editer.** Cet élément ouvre le panneau affichant les propriétés du poste ou du groupe, ce panneau se trouve dans la partie droite de la fenêtre du **Centre de Gestion**.

1 **Spécifier le groupe comme primaire.** Cet élément permet de spécifier le groupe sélectionné depuis l'arborescence comme primaire pour tous les postes qui lui sont rattachés.

1 **Spécifier le groupe primaire.** Cet élément permet de spécifier le groupe primaire pour les postes sélectionnés dans l'arborescence. Si un groupe entier est sélectionné, le groupe primaire sera spécifié pour tous les postes appartenant à ce groupe.

👉 **Fusionner les postes.** Cet élément permet de fusionner les postes sous un compte dans l'arborescence. Il est utile dans le cas où le même poste a été enregistré sous différents comptes (voir [Fusion des postes](#)).


✗ **Supprimer les configurations personnalisées de l'objet.** Cet élément permet de supprimer les configurations personnalisées de l'objet sélectionné dans l'arborescence. Dans ce cas, les configurations seront héritées depuis le groupe primaire. Si un groupe entier est sélectionné dans l'arborescence, les configurations seront supprimées pour tous les postes appartenant à ce groupe.

🔑 **Importation de la clé.** Cet élément permet de spécifier le fichier clé pour le poste ou le groupe.


📧 **Envoyer des messages aux postes.** Cet élément permet





d'envoyer un message aux utilisateurs (voir [Envoi de messages à l'utilisateur](#)).

 **Désinstaller Dr.Web Agent.** Cet élément supprime l'**Agent** et le logiciel antivirus sur le poste et le groupe de postes sélectionnés.


 **Installer Dr.Web Enterprise Agent.** Cet élément ouvre le [Scanner réseau](#) pour installer l'**Agent** sur les postes sélectionnés. Cet élément est actif seulement en cas de sélection des nouveaux postes non approuvés ou des postes depuis lesquels l'**Agent** a été désinstallé.


 **Restaurer les postes supprimés.** Cet élément permet de restaurer les postes supprimés (voir aussi [Suppression et restauration des postes](#)). Cet élément est actif seulement en cas de sélection des postes faisant partie du sous-groupe **Deleted** dans le groupe **Status**.


 **Ajouter un poste ou un groupe.** Ce bouton permet de créer un nouvel élément du réseau antivirus. Pour cela, sélectionnez un élément dans la liste déroulante :

 **Créer un poste.** Permet de créer un nouveau poste (voir [Création d'un nouveau compte](#)).

 **Créer un groupe.** Permet de créer un nouveau groupe (voir [Création et suppression des groupes](#)).

 **Exporter les données.** Cet élément permet d'exporter les données sommaires sur les postes du réseau antivirus vers un fichier au format CSV, HTML ou XML. Le format souhaité peut être sélectionné depuis la liste déroulante.


 **Paramétrer l'affichage du groupe.** Cet élément permet de modifier les paramètres d'affichage des groupes. Pour cela, sélectionnez un groupe dans l'arborescence et depuis la liste déroulante spécifiez une des variantes suivantes (l'icône du groupe va changer d'apparence, voir le [tableau 3-2](#)) :


 **Cacher le groupe** - signifie que l'affichage du groupe dans l'arborescence sera toujours désactivé.


 **Cacher s'il est vide** - signifie que l'affichage du groupe dans





l'arborescence sera désactivé si tel groupe est vide (ne contient pas de postes).


 **Afficher** - signifie que le groupe sera toujours affiché dans l'arborescence.


 **Gestion des composants.** Cet élément permet de gérer les composants antivirus tournant sur les postes. Pour cela, sélectionnez un élément dans la liste déroulante :

 **Mettre à jour tous les composants.** Cet élément commande de mettre à jour tous les composants installés de l'antivirus, par exemple, si l'**Agent** n'a pas été connecté au **Serveur** durant une longue période etc. (voir [Mise à jour manuelle des composants de Dr.Web Enterprise Security Suite](#)) ;

 **Mettre à jour les composants échoués.** Cet élément force la mise à jour des composants dont la mise à jour a échoué ;

 **Interrompre des composants lancés.** Cet élément enjoint d'arrêter les processus de scan lancés sur le poste. Pour en savoir plus sur la procédure d'interruption des processus de scan selon leur type, consultez le paragraphe [Interruption des composants en cours selon leur type](#).

 **Scan.** Cet élément permet de réaliser une procédure de scan dans un mode sélectionné depuis la liste déroulante (voir aussi [Lancement de scan sur le poste](#)) :

 **Dr.Web Scanner pour Windows. Analyse rapide.** Ce mode prévoit l'analyse des objets suivants :

- ◆ mémoire vive,
- ◆ secteurs de démarrage de tous les disques,
- ◆ objets d'autodémarrage,
- ◆ répertoire racine du disque boot,
- ◆ répertoire racine du disque d'installation Windows,
- ◆ répertoire système Windows,
- ◆ dossier Mes Documents,
- ◆ répertoire système temporaire,
- ◆ répertoire d'utilisateur temporaire.



Dr.Web Scanner pour Windows. Analyse complète. Ce mode assure l'analyse complète de tous les disques durs ainsi que des supports amovibles (y compris les secteurs boot).



Dr.Web Scanner pour Windows. Analyse sélective. Ce mode permet de choisir les dossiers et fichiers à analyser.



Dr.Web Enterprise Scanner pour Windows. Ce mode active l'analyse sélective avec **Dr.Web Enterprise Scanner**.



Dr.Web Enterprise Scanner pour Mac OS X. Pour scanner les postes de travail tournant sous OS de la famille Mac OS X selon les paramètres de scan spécifiés.



Dr.Web Enterprise Scanner pour Unix. Pour scanner les postes tournant sous OS de la famille UNIX selon les paramètres de scan spécifiés.



Configuration de l'arborescence. Cet élément permet de modifier l'apparence de la liste :

◆ pour les groupes :

- **Appartenance à tous les groupes.** L'élément double l'apparition du poste dans la liste s'il fait partie de plusieurs groupes (uniquement pour les groupes accompagnés de l'image du dossier blanc - voir le [tableau 3-2](#)). Si la case est cochée, toutes les appartenances seront affichées. Sinon le poste figure dans la liste une seule fois.
- **Afficher les groupes cachés.** L'élément active l'affichage de tous les groupes faisant partie du réseau antivirus. Si la case est décochée, les groupes vides seront cachés. Ceci peut être pratique pour éviter d'afficher trop d'informations par exemple en cas de nombreux groupes vides.

◆ pour les postes :

- **Afficher l'ID du poste.** L'élément active l'affichage des postes dans l'arborescence par identificateur unique ;
- **Afficher le nom du poste.** L'élément active l'affichage des noms de postes s'ils ont été spécifiés ;





- **Afficher l'adresse du poste.** L'élément active l'affichage des postes dans l'arborescence par adresse IP ;
 - **Afficher le serveur du poste.** L'élément active l'affichage des noms ou des adresses des **Serveurs** antivirus auxquels les postes sont connectés.
- ◆ pour tous les éléments :
- **Afficher les configurations personnalisées.** L'élément active/désactive l'affichage du marqueur sur les icônes des postes et des groupes en cas de configurations personnalisées.
 - **Afficher les descriptions.** L'élément active/désactive l'affichage des descriptions des groupes et des postes (les descriptions sont configurées dans les propriétés des objets).
 - **Afficher le nombre de postes.** L'élément active/désactive l'affichage du nombre total de postes se trouvant dans tous les groupes du réseau antivirus.

Panneau des propriétés

Le panneau des propriétés sert à afficher les propriétés et les paramètres des postes et des groupes.

Pour afficher le panneau des propriétés :

1. Dans l'arborescence, sélectionnez le poste ou le groupe et cliquez ensuite sur le bouton  **Général** →  **Editer** se trouvant dans la barre d'outils.
2. Le panneau affichant les propriétés du poste sera ouvert dans la partie droite de la fenêtre du **Centre de Gestion**. Ce panneau comprend les groupes de paramètres suivants : **Général, Configuration, Groupes, Emplacement**. Pour en savoir plus sur les paramètres, consultez le paragraphe [Configuration du poste de travail](#).



3.3.3. Préférences

Dans le menu principal du **Centre de Gestion**, sélectionnez l'élément **Préférences**.



Toutes les préférences se trouvant dans cet onglet ne seront prises en compte que pour le compte administrateur courant.

Le menu de gestion se trouvant dans la partie gauche de la fenêtre comprend les éléments suivants :

- ◆ **Mon compte.**
- ◆ **Interface.**

Mon compte

Cette rubrique permet de gérer le compte administrateur courant du réseau antivirus (voir aussi [Gestion des comptes administrateur](#)).




Les champs marqués par le symbole * sont obligatoires à remplir.

Si nécessaire, éditer les paramètres suivants :

- ◆ **Login** de l'administrateur - login requis pour accéder au **Centre de Gestion**.
- ◆ Cochez la case **En lecture seule** si vous souhaitez limiter les droits d'accès.
- ◆ Entrez le nom, prénom et patronyme de l'administrateur.
- ◆ **Langue** d'interface utilisée par cet administrateur.
- ◆ **Format de la date** utilisé par l'administrateur lors de l'édition des paramètres contenant des dates. Les formats suivants peuvent être sélectionnés :
 - européen : DD-MM-YYYY HH:MM:SS



- américain : MM/DD/YYYY HH:MM:SS
- ◆ **Description** du compte.
- ◆ Afin de spécifier une liste des groupes accessibles à l'administrateur courant, cochez la case **Peut gérer un nombre limité de groupes**.
- ◆ Pour changer de mot de passe, cliquez sur le bouton  **Nouveau mot de passe** depuis la barre d'outils.

Les paramètres ci-dessous ne sont disponibles qu'en lecture seule :

- ◆ Date de création et de la dernière modification du compte et des paramètres correspondants,
- ◆ **Statut** - affiche l'adresse réseau de la dernière connexion sous le compte courant.


Après avoir apporté les modifications nécessaires, cliquez sur le bouton **Sauvegarder**.

Pour les comptes ayant des droits en lecture seule, seuls les champs ci-dessous sont disponibles pour modification :

- ◆ **Langue d'interface**,
- ◆ **Description**.

Interface

Configuration de l'arborescence

Les paramètres se trouvant dans cette rubrique permettent de modifier l'apparence de l'arborescence et sont équivalents aux paramètres de la barre d'outils se trouvant dans l'élément  dans l'onglet **Réseau antivirus** du menu principal :

- ◆ pour les groupes :



- **Appartenance à tous les groupes.** L'élément double l'apparition du poste dans la liste si le poste fait partie de plusieurs groupes (uniquement pour les groupes accompagnés de l'image du dossier blanc - voir le [tableau 3-2](#)). Si la case est cochée, toutes les appartenances seront affichées. Sinon le poste figure dans la liste une seule fois.
 - **Afficher les groupes cachés.** L'élément active l'affichage de tous les groupes faisant partie du réseau antivirus. Si la case est décochée, les groupes vides seront cachés. Ceci peut être pratique pour éviter d'afficher trop d'informations, par exemple en cas de nombreux groupes vides.
- ◆ pour les postes :
- **Afficher l'ID du poste.** L'élément active l'affichage des postes dans l'arborescence par identificateur unique ;
 - **Afficher le nom du poste.** L'élément active l'affichage des noms de postes s'ils ont été spécifiés ;
 - **Afficher l'adresse du poste.** L'élément active l'affichage des postes dans l'arborescence par adresse IP ;
 - **Afficher le serveur du poste.** L'élément active l'affichage des noms ou des adresses des **Serveur Enterprise** auxquels les postes sont connectés.
- ◆ pour tous les éléments :
- **Afficher les configurations personnalisées.** L'élément active/désactive l'affichage du marqueur sur les icônes des postes et des groupes en cas de configurations personnalisées.
 - **Afficher les descriptions.** L'élément active/désactive l'affichage des descriptions des groupes et des postes (les descriptions sont configurées dans les propriétés des éléments respectifs).

Scanner réseau



Le Scanner réseau requiert que le module ajoutable **Dr.Web Browser-Plugin** soit installé.



Cette rubrique permet de configurer les paramètres du [Scanner réseau](#) spécifiés par défaut.

Pour lancer le **Scanner réseau**, sélectionnez dans le menu principal du **Centre de Gestion** l'élément **Administration**, puis dans le menu de gestion (panneau de gauche) sélectionnez l'élément **Scanner réseau**.

Spécifiez les paramètres suivants du **Scanner réseau** :

1. Dans le champ **Réseaux** entrez une liste des réseaux au format suivant :
 - ◆ espacé par un trait d'union (par exemple, 10.4.0.1-10.4.0.10),
 - ◆ espacé par une virgule-espace (par exemple, 10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90),
 - ◆ en utilisant le préfixe réseau (par exemple, 10.4.0.0/24).
2. Si nécessaire, modifiez les valeurs dans les champs **Port** et **Time out**.
3. Afin de sauvegarder les valeurs par défaut, cliquez sur le bouton **Sauvegarder**. Ultérieurement, lors de l'utilisation du [Scanner réseau](#) ces paramètres seront spécifiés de manière automatique.

Laps de temps

Cette rubrique vous permet de configurer les paramètres du délai d'affichage des données statistiques (voir [Consultation des résultats et des statistiques sommaires du poste](#)) :

- ◆ Dans la liste déroulante **Délai d'affichage des statistiques**, vous pouvez spécifier un délai à appliquer par défaut à toutes les rubriques relatives aux statistiques.

Lors de la première ouverture de la page, les statistiques seront affichées conformément au délai spécifié. Si nécessaire, vous pouvez le modifier directement depuis les rubriques de statistiques.



- ◆ Afin de conserver le dernier délai spécifié dans les rubriques de statistiques, cochez la case **Sauvegarder le dernier délai d'affichage des statistiques**.

Si la case est cochée, lors de la première ouverture de la page, les statistiques relatives à la dernière période sélectionnée dans le navigateur web seront affichées.

En cas de case décochée, lors de la première ouverture de la page, les statistiques relatives à la période spécifiée dans la rubrique **Délai d'affichage des statistiques** seront affichées.

Authentification

Cochez la case **Authentification automatique** afin d'autoriser dans le navigateur web courant l'authentification automatique de tous les **Centres de Gestion** ayant le même nom d'utilisateur et le même mot de passe administrateur.

Lorsque la case est activée, l'extension de **Dr.Web Browser-Plugin** va mémoriser le nom et le mot de passe que l'administrateur entrera lors de la prochaine authentification dans le **Centre de Gestion**.



Le module ajoutable **Dr.Web Browser-Plugin** doit être installé pour utiliser l'authentification automatique.

Ultérieurement, à l'ouverture de n'importe quel **Centre de Gestion Dr.Web** dans ce navigateur web, l'authentification se fait de manière automatique à condition que l'utilisateur avec le nom et le mot de passe correspondants existe sur le **Serveur**. Si le nom et le mot de passe ne correspondent pas (par exemple, l'utilisateur n'est pas présent ou l'utilisateur ayant ce nom a un autre mot de passe), la fenêtre standard d'authentification du **Centre de Gestion** sera ouverte.



Lorsque vous cliquez sur **Logout** dans **l'en-tête** de l'interface du **Centre de Gestion**, les informations sur le nom et le mot de passe de l'administrateur sont effacées.



Pour accéder de nouveau au **Centre de Gestion**, il est nécessaire de passer une procédure standard d'authentification et soumettre le nom et le mot de passe. Si l'authentification automatique est activée, le nom et le mot de passe soumis sont mémorisés dans le navigateur web de sorte que l'authentification dans le **Centre de Gestion** sera automatique (sans entrer le nom et le mot de passe) jusqu'au moment où vous pressez de nouveau le bouton **Logout**.

3.3.4. Liaisons

Dans le menu principal du **Centre de Gestion**, sélectionnez l'élément **Liaisons**. Le menu de gestion se trouvant dans la partie gauche de la fenêtre sert à sélectionner les informations à afficher.

Administration

La rubrique **Administration** du menu de gestion comprend l'élément **Liaisons** servant à gérer les liaisons entre les **Serveurs** dans un réseau antivirus en contenant plusieurs (voir [Particularités du réseau avec plusieurs Serveurs](#)).

L'arborescence affiche tous les serveurs **Serveur Enterprise** connectés au **Serveur** sélectionné.

La procédure de création des liaisons entre serveurs est décrite dans le paragraphe [Configuration des liaisons entre les Serveurs du réseau antivirus](#).

Tableaux

La rubrique **Tableaux** du menu de gestion offre accès aux informations sur le fonctionnement du réseau antivirus reçues depuis d'autres **Serveurs** (voir [Particularités du réseau avec plusieurs Serveurs](#)).



Afin de consulter le rapport récapitulatif affichant les données relatives aux autres **Serveurs**, cliquez sur l'élément correspondant de la rubrique **Tableaux**.

3.3.5. Aide

Dans le menu principal du **Centre de Gestion**, sélectionnez l'élément **Aide**.

Le menu de gestion se trouvant dans la partie gauche de la fenêtre comprend les éléments suivants :

1. Général

- ◆ **Documentation** - cet élément ouvre la documentation en ligne au format HTML.
- ◆ **Forum** - cet élément redirige vers le forum de **Doctor Web**.
- ◆ **Poster une question** - cet élément permet de passer à la page de **Support technique Doctor Web**.
- ◆ **Soumettre un virus** - cet élément ouvre le formulaire permettant d'envoyer un virus au laboratoire **Doctor Web**.
- ◆ **Signaler une erreur relative au fonctionnement du module de Contrôle Parental** - cet élément ouvre le formulaire permettant d'envoyer un message sur une fausse alerte ou sur un problème de non détection des liens indésirables dans le module de **Contrôle Parental**.

2. Documentation

- ◆ **Manuel Administrateur** - cet élément affiche le Manuel Administrateur au format HTML.
- ◆ **Manuel Utilisateur** - cet élément affiche le Manuel Utilisateur au format HTML.
- ◆ **XML Web API** - cet élément affiche le Manuel Administrateur sur XML Web API (voir aussi [Annexe N. Intégration de Dr.Web Enterprise Security Suite avec XML Web API](#)) au format HTML.



- ◆ **Remarques sur l'édition** - cet élément affiche les remarques relatives à l'édition **Dr.Web Enterprise Security Suite** dans la version que vous avez installée.

3.4. Composants du Centre de Gestion Dr.Web

3.4.1. Scanner réseau

Le **Scanner réseau** est inclus au sein de **Serveur Enterprise**.



Il est déconseillé de lancer le **Scanner réseau** sous Windows 2000 ou antérieur puisque dans ce cas-là, l'aperçu réseau peut être incomplet.

Le **Scanner réseau** est pleinement compatible avec les OS de la famille UNIX ou Windows XP et supérieurs.

Le **Scanner réseau** requiert que le module ajoutable [Dr.Web Browser-Plugin](#) soit installé.

Le scanner réseau exécute les fonctions suivantes :

- ◆ Scan (aperçu) du réseau afin de trouver les postes de travail.
- ◆ Détection d'**Enterprise Agent** sur les postes.
- ◆ Installation d'**Enterprise Agent** sur les postes détectés selon la commande de l'administrateur. La procédure d'installation de **Enterprise Agent** est décrite dans le paragraphe [Installation de Dr.Web Enterprise Agent avec le Centre de Gestion](#).

La marche à suivre pour obtenir un aperçu du réseau :

1. Ouvrez la fenêtre du **Scanner réseau**. Pour cela, sélectionnez l'élément **Administration** du menu principal du **Centre de Gestion**, dans la fenêtre qui apparaît, sélectionnez l'élément du menu de gestion **Scanner réseau**. La fenêtre de **Scanner réseau** va s'ouvrir.
2. Si nécessaire, cochez la case **Scan rapide** pour exécuter



l'analyse en **mode accéléré**.

3. Dans le champ de saisie **Réseaux**, entrez la liste des réseaux au format suivant :
 - ◆ espacé par un trait d'union (par exemple 10.4.0.1-10.4.0.10),
 - ◆ espacé par une virgule et un espace (par exemple 10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90),
 - ◆ avec le préfixe de réseau (par exemple 10.4.0.0/24).
4. Spécifiez le port via lequel il faut se connecter à l'**Agent**.
5. Si nécessaire, modifiez la valeur du délai d'attente, en secondes, durant lequel on attend une réponse des postes demandés.
6. Cochez la case **Afficher le nom du poste** pour afficher non seulement les adresses IP des ordinateurs détectés mais aussi leurs noms de domaine.

Si le poste n'est pas enregistré sur le serveur DNS, uniquement son adresse IP sera affichée.

7. Cochez la case **A comparer avec la liste des postes de la BD** pour activer la synchronisation des résultats des recherches du **Scanner réseau** avec la liste des postes sauvegardée dans la BD du **Serveur**. Si cette case est activée, la liste des postes détectés dans le réseau va également contenir les postes listés dans la BD du **Serveur** mais qui n'ont pas été trouvés par le **Scanner réseau** durant la recherche courante, par exemple, dans le cas où un pare-feu est installé sur tels postes et qu'il bloque la transmission des paquets nécessaires pour établir une connexion TCP.

Lors de la synchronisation des résultats de la recherche du **Scanner réseau** avec les données de la BD du **Serveur**, les données de la BD du **Serveur** sont prioritaires, en cas de non correspondance du statut de poste reçu lors de la recherche à celui enregistré dans la BD, le statut enregistré dans la BD sera attribué.








8. Cliquez sur le bouton **Lancer le scanner**. Le scan du réseau sera activé.
9. Pendant le scan du réseau, l'arborescence du réseau s'affiche






dans une fenêtre indiquant les postes et la présence sur ces postes d'**Enterprise Agent**.

Ouvrez les éléments de l'arborescence correspondant aux groupes de travail (domaines). Tous les éléments de l'arborescence correspondant aux divers groupes de travail et aux postes sont marqués par les icônes dont vous trouverez la description ci-dessous.

Tableau 3-3. Apparence des icônes

Icône	Description
Groupes de travail	
	Groupes de travail contenant entre autres les ordinateurs sur lesquels l'antivirus Dr.Web ESS peut être installé.
	Groupes restants contenant les ordinateurs sur lesquels l'antivirus est déjà installé ou les ordinateurs inaccessibles via le réseau.
Postes de travail	
	Le poste détecté est enregistré dans la base et actif (postes avec l'antivirus installé).
	Le poste détecté est enregistré dans la base dans le tableau des postes détectés.
	Le poste détecté n'est pas enregistré dans la base (pas d'antivirus installé sur le poste).
	Le poste détecté n'est pas enregistré dans la base (connecté à un autre Serveur).
	Le poste détecté est enregistré dans la base, inactif et le port respectif est fermé.

Les éléments de l'arborescence correspondant aux postes ayant les icônes  ou  peuvent être ouverts pour consulter le jeu des composants installés.

En cliquant sur l'icône  du composant du poste connecté au **Serveur** donné, la fenêtre de configuration du composant s'ouvrira.



Interaction avec Dr.Web Enterprise Agent

L'outil **Scanner réseau** est inclus dans le produit **Dr.Web ESS** à partir de la version **4.44**.



Le **Scanner réseau** peut détecter l'**Agent** installé sur le poste en cas de version **4.44** ou supérieures, mais il n'est pas compatible avec les Agents en versions antérieures.

Installé sur le poste protégé, l'**Agent** en version **4.44** ou supérieure traite les requêtes du **Scanner réseau** reçues sur le port spécifié. Par défaut, le port `udp/2193` sera utilisé, mais afin d'assurer la compatibilité avec le logiciel des versions antérieures, le port `udp/2372` est également supporté. Dans le **Scanner réseau**, les requêtes seront envoyées vers les mêmes ports. En fonction des réponses aux requêtes envoyées via le port indiqué, le **Scanner réseau** détermine la présence de l'**Agent** sur le poste.



Si la réception des packages sur `udp/2193` est interdit sur le poste (par exemple par le pare-feu), l'**Agent** ne peut pas être détecté et par conséquent, le **Scanner réseau** conclut que l'**Agent** n'est pas installé sur le poste.

Scan rapide

Etant activée, l'option **Scan rapide** effectue les actions suivantes :

1. Envoi des requêtes ping vers les machines se trouvant dans le réseau.
2. Uniquement pour les machines qui ont répondu aux requêtes ping, les requêtes relatives à la détection de l'**Agent** sont envoyées en parallèle.
3. La procédure de détection de l'**Agent** s'effectue selon les règles générales.



Les requêtes ping peuvent être bloquées conformément aux politiques réseau adoptées (par exemple suite à la configuration du pare-feu).

Par exemple :

Si sous Windows Vista ou supérieur le paramètre **Réseau public** est spécifié, l'OS bloque toutes les requêtes ping.

Durant le processus de scan standard, les requêtes ping ne sont pas envoyées, mais les postes sont interrogés l'un après l'autre sur la présence de l'**Agent**. Cette technique peut être utilisée comme un complément au scan rapide dans le cas où le réseau compte des postes sur lesquels les requêtes ping sont bloquées.

La scan rapide s'effectue en parallèle, le scan standard - de manière successive.

Les performances du **Scanner réseau** peuvent varier. La durée maximum du scan peut être estimée de manière suivante :

- ◆ en cas de scan standard : $\langle N \rangle * \langle timeout \rangle$,
- ◆ en cas de scan rapide : $\langle N \rangle / 40 + 2 * \langle timeout \rangle$,

avec : $\langle N \rangle$ - nombre de postes, $\langle timeout \rangle$ - la valeur depuis le champ **Time out**.

3.4.2. Gestionnaire de licence

Le **gestionnaire de licence** est un composant de **Serveur Enterprise**. Ce composant facilite la gestion des fichiers clés de licence du **Serveur** et des **Agents**.

Pour accéder à la fenêtre du **Gestionnaire de licence**, dans le menu principal du **Centre de Gestion** sélectionnez l'élément **Administration**, puis dans la fenêtre qui apparaît, sélectionnez l'élément **Gestionnaire de licence** depuis le menu de gestion (panneau de gauche).



La fenêtre principale du **Gestionnaire de licence** comprend une arborescence contenant les éléments suivants :


- ◆ **Clés serveur.** Cet élément affiche les comptes contenant les fichiers clés de licence relatifs au **Serveur**. Un seul compte peut être actif (utilisé par le **Serveur** à un moment donné).
- ◆ **Clés agent.** Cet élément affiche les comptes contenant les fichiers clés de licence relatifs à l'**Agent**. Chaque fichier clé peut être spécifié pour plusieurs groupes ou postes affichés dans la fenêtre du **Gestionnaire de licence** comme des éléments imbriqués du compte correspondant à la clé.

Afin de gérer les fichiers clés de licence, utilisez les éléments suivants de la barre d'outils :

+ Importation de la clé - permet d'ajouter une nouvelle entrée relative au fichier clé. Pour cela, sélectionnez l'élément correspondant du menu déroulant :


 **Importation de la clé serveur** - pour ajouter un nouveau fichier clé du **Serveur**.

 **Importation de la clé agent** - pour ajouter un nouveau fichier clé des **Agents**.

 **Supprimer la clé** - permet de supprimer les comptes relatifs aux fichiers clé.



Il est impossible de supprimer le compte de la clé **Agent** spécifiée pour le groupe **Everyone** ainsi que le compte courant actif de la clé **Serveur**.

 **Editer** - permet de consulter les informations relatives à la licence et à son activation (uniquement pour le **Serveur**), cet élément permet également de remplacer le fichier clé si c'est nécessaire (uniquement pour l'**Agent**). Cet élément n'est activé que dans le cas où un compte du fichier clé du **Serveur** ou de l'**Agent** est sélectionné dans la fenêtre principale.

 **Diffuser les configurations vers un autre objet** - permet de



spécifier la clé sélectionnée pour un groupe défini ou pour un poste sélectionnés dans la liste déroulante. Cet élément n'est activé que dans le cas où un compte du fichier clé de l'**Agent** est sélectionné dans la fenêtre principale.



Exporter la clé - permet de garder une copie locale du fichier pour la clé sélectionnée depuis la liste.

Exemple de remplacement des clés

Si vous souhaitez remplacer complètement tous les fichiers clés des composants du réseau antivirus (par exemple en cas de licences expirées), relatifs au **Serveur** ainsi qu'à l'**Agent**, suivez les instructions ci-dessous à exécuter via le **Gestionnaire de licence** :

1. [Ajouter une nouvelle clé Serveur.](#)
2. [Activer la nouvelle clé Serveur.](#)
3. [Supprimer l'ancienne clé Serveur.](#)
4. [Remplacer le fichier clé de licence Agent](#) pour le groupe **Everyone** et si nécessaire, pour les autres groupes et postes pour lesquels les fichiers clés de licence ont été spécifiés de manière personnalisée.


3.4.2.1. Clés Dr.Web Enterprise Server

Le Gestionnaire de licence vous permet de réaliser les actions suivantes sur les clés de licence Dr.Web Enterprise Server :

1. [Consulter des informations sur la licence.](#)
2. [Ajouter de nouveaux fichiers clés Serveur.](#)
3. [Changer le statut de la licence Serveur.](#)
4. [Supprimer des fichiers clés Serveur.](#)





Consultation des informations sur la licence

Afin de consulter les données relatives à la licence, sélectionnez depuis la fenêtre principale du **Gestionnaire de licence** le compte dont les données vous intéressent et cliquez ensuite sur le bouton  **Editer** dans la barre d'outils. Le panneau s'ouvre et affiche les informations suivantes :

- ◆ titulaire de la licence,
- ◆ revendeur qui vous a vendu la licence,
- ◆ identificateur de la licence,
- ◆ date d'expiration de la licence,
- ◆ disponibilité de l'**Antispam** dans la licence.

Ajout d'un fichier clé Serveur

Pour ajouter un nouveau fichier clé de licence Serveur, procédez comme suit :

1. Cliquez sur le bouton  **Importation de la clé** depuis la barre d'outils, puis dans la liste déroulante, sélectionnez l'élément  **Importer la clé serveur**.
2. Dans le panneau qui apparaît, cliquez sur le bouton **Parcourir** et sélectionnez le fichier clé de licence **Serveur**.
3. Cliquez sur le bouton **Sauvegarder**.



Il est possible de sauvegarder plusieurs comptes de fichiers clés. Cependant, seule une des licences **Serveur** peut être activée.




Si, lors du changement de fichier clé **Serveur** (activation d'un nouveau fichier clé), les paramètres ID1 du **Serveur** enregistrés dans l'ancien et dans le nouveau fichiers clés ne sont pas les mêmes, alors la planification du **Serveur**, les configurations des liaisons entre serveurs et les statistiques des tâches du **Serveur** seront perdues.

Pour conserver la planification du **Serveur**, il est nécessaire de l'exporter avant le remplacement de la clé de licence et de l'importer après le remplacement.

Changement de statut de la licence Serveur

En cas de plusieurs comptes de fichiers clés, seule une licence **Serveur** est active (utilisée par le **Serveur** à un moment donné).

Pour changer de licence active Serveur, procédez comme suit :

1. Sélectionnez le compte correspondant à la licence à installer pour le **Serveur** et cliquez sur le bouton  **Editer** se trouvant dans la barre d'outils.
2. Dans le panneau qui apparaît, cliquez sur le bouton **Activer**.
3. Après l'activation de la nouvelle clé serveur, redémarrez le **Serveur** pour continuer.

Suppression du fichier clé de licence Serveur



Il est impossible de supprimer le compte actif du fichier clé **Serveur**.

Pour supprimer le fichier clé Serveur, procédez comme suit :

1. Dans la fenêtre principale du **Gestionnaire de licence**, sélectionnez la clé à supprimer et depuis la barre d'outils cliquez ensuite sur le bouton  **Supprimer la clé**.




2. Dans la fenêtre de dialogue, confirmez la suppression de la clé.

3.4.2.2. Clés Dr.Web Enterprise Agent

Le Gestionnaire de licence vous permet de réaliser les actions suivantes sur les clés de licence Dr.Web Enterprise Agent:

1. [Consulter des informations sur la licence.](#)
2. [Ajouter de nouveaux fichiers clés de licence Agent.](#)
3. [Remplacer les fichiers clé de licence Agent par les nouvelles clés.](#)
4. [Remplacer les fichiers clés de licence Agent par les clés correspondantes déjà activées dans le réseau.](#)
5. [Supprimer des fichiers clés de licence Agent.](#)

Consultation des données relatives à la licence

Afin de consulter les données relatives à la licence, sélectionnez depuis la fenêtre principale du **Gestionnaire de licence** le compte dont les données vous intéressent et cliquez ensuite sur le bouton  **Editer** dans la barre d'outils. Le panneau s'ouvre et affiche les informations suivantes:

- ◆ titulaire de la licence,
- ◆ revendeur qui a vendu la licence,
- ◆ identificateur de la licence,
- ◆ date d'expiration de la licence,
- ◆ disponibilité du module **Antispam** dans la licence,
- ◆ jeu de composants antivirus couverts par la licence.





Ajout d'un fichier clé de licence Agent




Il est possible de spécifier plusieurs comptes ayant des fichiers clés **Agent**.

Pour ajouter un nouveau fichier clé de licence Agent, procédez comme suit :

1. Cliquez sur le bouton  **Importation de la clé** depuis la barre d'outils puis sélectionnez dans la liste déroulante l'élément  **Importation de la clé Agent**.
2. Depuis le panneau qui apparaît, cliquez sur le bouton **Parcourir** et sélectionnez le fichier clé de licence **Agent**.
3. Cliquez sur le bouton **Sauvegarder**.

Remplacement du fichier clé de licence Agent par un nouveau fichier clé

Marche à suivre pour remplacer le fichier clé de licence Agent existant par un nouveau fichier clé :

1. Dans la fenêtre principale du **Gestionnaire de licence**, sélectionnez l'objet (poste ou groupe) auquel la clé existante est associée et cliquez ensuite sur le bouton  **Editer** depuis la barre d'outils.
2. Dans le panneau qui apparaît, cliquez sur le bouton **Parcourir** et sélectionnez le fichier clé de licence **Agent**.
3. Cliquez sur le bouton **Sauvegarder**.
4. Dans le cas où le jeu de composants couverts par la licence correspondant au nouveau fichier clé ne correspond pas au jeu de composants associés à l'ancien fichier clé, une requête pour la configuration des paramètres des composants du nouveau fichier clé s'affichera.


La liste des objets comprend les postes et groupes dont les listes des composants (relatives à l'ancienne et à la nouvelle clé)



ne correspondent pas, ainsi que la liste des différences (composants ajoutés ou manquants par rapport à l'ancienne clé). Cochez la case contre les objets pour lesquels de nouvelles configurations des composants à installer seront spécifiées. Pour les objets restants (pour lesquels aucune case n'est cochée), les configurations gardent leur statut antérieur au remplacement de la clé.

Remplacement du fichier clé de licence Agent par un fichier clé existant

Marche à suivre pour remplacer le fichier clé de licence Agent courant par un fichier clé de licence déjà opérationnel dans le réseau antivirus :

1. Depuis la fenêtre principale du **Gestionnaire de licence** sélectionnez la clé que vous souhaitez spécifier pour l'objet (poste ou groupe) et cliquez ensuite sur le bouton  **Diffuser les configurations vers un autre objet** dans la barre d'outils.
2. Dans la fenêtre qui apparaît, sélectionnez depuis la liste un poste ou un groupe (le groupe doit contenir des postes). Pour sélectionner un ou plusieurs objets, il suffit de cliquer sur ces objets ; pour désélectionner, procédez de la même façon.
3. Cliquez sur le bouton **Sauvegarder**.



Si un fichier clé est déjà spécifié pour le poste ou le groupe dans les configurations personnalisées, avant de spécifier un nouveau fichier clé depuis la liste affichée dans la fenêtre principale du **Gestionnaire de licence**, il suffit de déplacer ce groupe ou poste avec la souris (glisser-déposer) vers le compte relatif à la clé (un petit délai d'affichage lié à la mise à jour de la liste peut avoir lieu).

4. Dans le cas où la liste des composants à installer couverts par la licence ne correspond pas à la liste relative à l'ancien fichier clé, une requête pour la configuration des paramètres des composants du nouveau fichier clé s'affichera.




La liste des objets comprend les postes et groupes dont les listes de composants (relatifs à l'ancienne et à la nouvelle clé) ne correspondent pas, ainsi que la liste des différences (composants ajoutés ou manquants par rapport à l'ancienne clé). Cochez la case contre les objets pour lesquels de nouvelles configurations des composants à installer seront spécifiées. Pour les objets restants (pour lesquels aucune case n'est cochée), les configurations gardent leur statut antérieur au remplacement de la clé.

Suppression du fichier clé de licence Agent



Il est impossible de supprimer le compte de la clé **Agent** spécifiée pour le groupe **Everyone**.

Pour supprimer un fichier clé de licence Agent existant, procédez comme suit :

1. Dans la fenêtre principale du **Gestionnaire de licence**, sélectionnez la clé que vous souhaitez supprimer ou l'objet (poste ou groupe) auquel la clé en question est associée, cliquez ensuite sur le bouton  **Supprimer la clé** depuis la barre d'outils.
2. Dans la fenêtre de dialogue, confirmez la suppression de la clé.
3. Si les composants de l'objet dont la clé doit être supprimée possèdent des configurations personnalisées, une requête pour la suppression de ces configurations s'affichera.

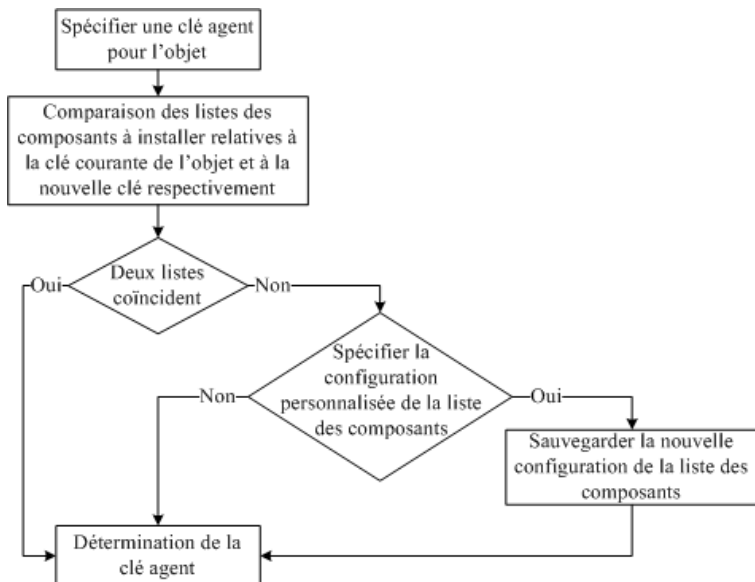
La liste des objets proposée contient des postes et des groupes ayant des configurations personnalisées. Cochez les cases contre les objets qui vont hériter des configurations du groupe parent. Pour les objets restants, les configurations des composants installés conservent leur statut antérieur à la suppression de la clé.



Modification de la liste des composants à installer

Remplacement ou ajout d'un nouveau fichier clé de licence

Si les listes des composants à installer relatives à l'ancien et au nouveau fichiers clés de licence ne correspondent pas, les configurations des composants à installer peuvent être remplacées par de nouvelles configurations, soit conservées (voir [Remplacement de fichier clé de licence Agent](#)).



Procédure à exécuter en cas de remplacement ou ajout d'un nouveau fichier clé de licence Agent



Lors de la configuration des nouveaux paramètres :

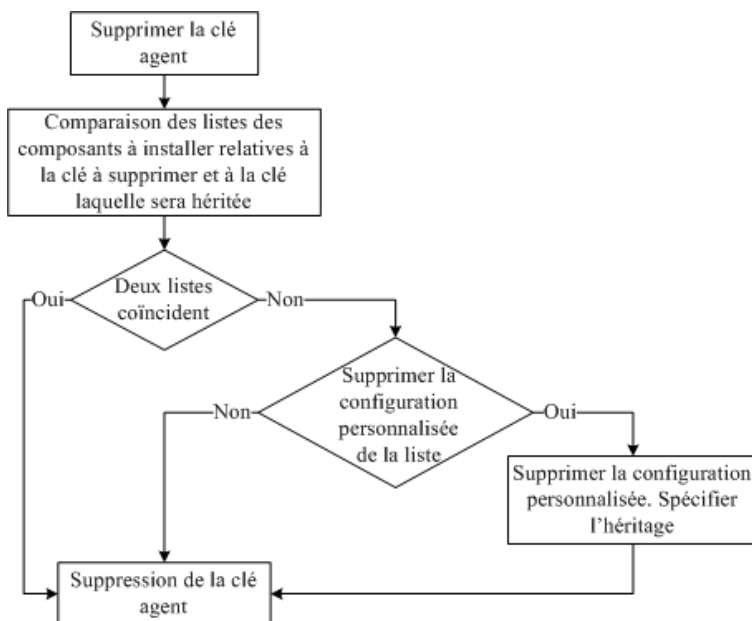
1. Si la nouvelle clé comprend des composants absents dans l'ancienne clé, la valeur **peut** sera spécifiée pour ces composants dans la liste **Composants à installer** (voir [Configuration du poste de travail](#)). Ultérieurement, l'utilisateur peut installer les composants sur les postes conformément à la nouvelle clé.
2. Si les composants présents dans l'ancienne clé ne sont plus présents dans la nouvelle, la valeur **ne peut pas** sera spécifiée dans la liste **Composants à installer** et les composants concernés seront supprimés depuis les postes auxquels la nouvelle clé a été attribuée.
3. Les autres composants mentionnés dans l'ancienne et la nouvelle clés conservent leurs configurations listées à la page **Composants à installer** telles qu'elles étaient avant le remplacement de la clé.

Lors de la sauvegarde des configurations :

Les configurations définies à la page **Composants à installer** gardent les valeurs spécifiées avant le remplacement de la clé.

Suppression du fichier clé de licence

La configuration des listes de composants à installer peut être héritée du groupe parent, sinon elles sont conservées (voir [Suppression du fichier clé de licence Agent](#)).



Procédure à exécuter en cas de suppression du fichier clé de licence Agent

Si les configurations sont héritées :

A la page **Composants à installer**, les configurations personnalisées seront supprimées et l'héritage des paramètres depuis le groupe parent sera spécifié.

Si les configurations sont conservées :

A la page **Composants à installer**, les configurations seront conservées telles qu'elles étaient avant la suppression de la clé.



3.5. Schéma d'interaction des composants du réseau antivirus

La [figure 3-3](#) présente le schéma d'un fragment du réseau antivirus.

Ce schéma représente un réseau antivirus comprenant un seul **Serveur**. Pour les grandes entreprises, il est préférable de déployer un réseau antivirus à plusieurs **Serveurs** afin de pouvoir répartir la charge entre eux.

Dans cet exemple, le réseau antivirus est déployé dans le cadre d'un LAN. Néanmoins, l'installation et l'utilisation de **ESS** et des packages antivirus ne nécessitent pas que les postes soient connectés à un LAN, une connexion Internet suffira.

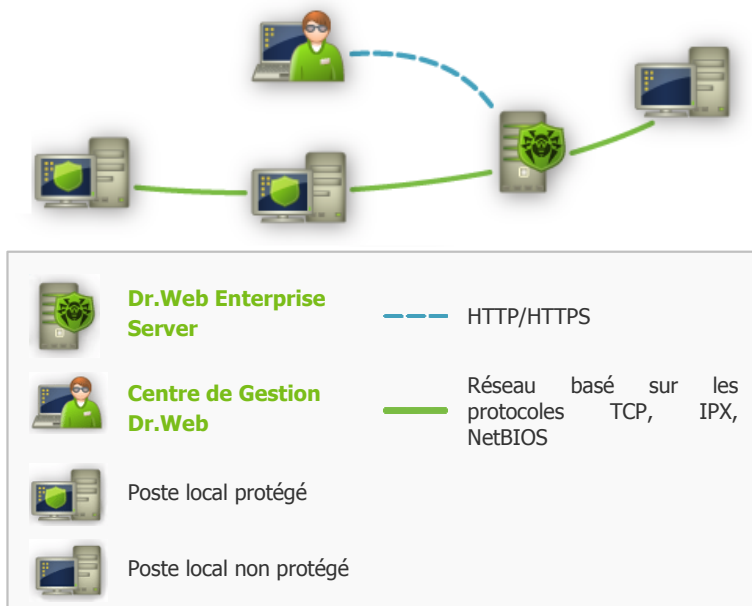


Figure 3-3. Structure du réseau antivirus

Au démarrage de Dr.Web Enterprise Server les actions suivantes sont exécutées :

1. Téléchargement des fichiers de **Serveur Enterprise** depuis le dossier `bin`.
2. Téléchargement du **Planificateur des tâches du Serveur**.
3. Téléchargement du répertoire d'installation centralisée et du répertoire de mise à jour, initialisation du système de notification.
4. Vérification de l'intégrité de la BD du **Serveur**.
5. Exécution des tâches du **Planificateur des tâches du Serveur**.
6. Attente des informations depuis **Enterprise Agents** et des commandes depuis les **Centres de Gestion**.



Tout le flux des commandes, données, informations statistiques dans le réseau antivirus passe nécessairement par **Serveur Enterprise**. Le **Centre de Gestion** échange des informations uniquement avec le **Serveur** ; les modifications de la configuration des postes et la transmission des commandes vers **Enterprise Agent** sont effectuées par le **Serveur** selon les commandes reçues depuis le **Centre de Gestion**.

La structure logique de ce fragment du réseau antivirus est présentée sur la [figure 3-4](#).

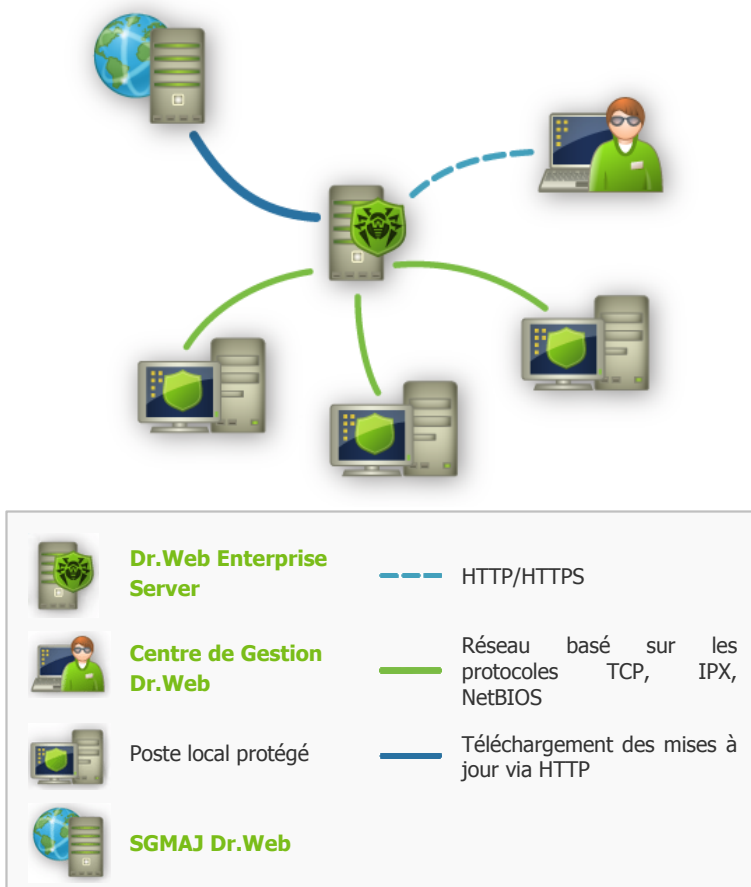


Figure 3-4. Structure logique du réseau antivirus

Entre le **Serveur** et les postes de travail (trait continu dans la [figure 3-4](#)), via un des protocoles supportés (TCP/IP, IPX ou NetBIOS) les informations suivantes sont transmises :

- ◆ requêtes de l'**Agent** pour la réception de la planification centralisée et la planification centralisée du poste,



- ◆ configuration de l'**Agent** et du package antivirus,
- ◆ requêtes pour les tâches urgentes à exécuter (scan, mise à jour des bases virales etc.),
- ◆ fichiers des packages antivirus — lorsque l'**Agent** reçoit des commandes relatives à leur installation,
- ◆ mises à jour du logiciel et des bases virales — lors de l'exécution de la tâche de mise à jour,
- ◆ messages de l'**Agent** relatifs à la configuration du poste,
- ◆ statistiques sur le fonctionnement de l'**Agent** et des packages antivirus à inclure dans le journal centralisé,
- ◆ messages sur les événements viraux et d'autres événements à mémoriser.

Le volume du trafic entre les postes de travail et le **Serveur** varie en fonction des configurations des postes et peut être important. C'est pourquoi le réseau antivirus **Dr.Web ESS** est doté de l'option permettant de compresser le trafic. Pour en savoir plus sur ce mode facultatif, consultez le paragraphe [Chiffrement et compression du trafic](#)

Le trafic entre le **Serveur** et le poste peut être chiffré. Ceci permet d'éviter la perte des informations transmises via ce canal ainsi que d'éventuels remplacements des logiciels installés sur les postes. Cette option est activée par défaut. Pour en savoir plus sur ce mode, consultez le paragraphe [Chiffrement et compression du trafic](#).

Les fichiers nécessaires à la réplication de répertoires d'installation centralisés et de mises à jour ainsi que des informations de service sur la progression de ce processus sont transmis, via le protocole HTTP, depuis le serveur web de mises à jour vers **Serveur Enterprise** (trait continu gras dans la [figure 3-4](#)). L'intégrité des informations transmises (fichiers de **Dr.Web ESS** et packages antivirus) est assurée par le mécanisme utilisant la somme de contrôle : un fichier endommagé lors de la transmission ou un fichier qui a été remplacé ne seront pas réceptionnés par le **Serveur**.

Entre le **Serveur** et le **Centre de Gestion** (trait pointillé dans la [figure 3-4](#)) sont transmises les informations sur la configuration du **Serveur** (y compris les informations sur la topologie du réseau) et sur les configurations des postes de travail. Ces informations sont affichées dans le **Centre de Gestion** et si les configurations sont



modifiées par l'utilisateur (l'administrateur du réseau antivirus), les informations sur les modifications apportées seront transmises au **Serveur**.

La connexion entre le **Centre de Gestion** et le **Serveur** sélectionné est établie après la procédure d'authentification de l'administrateur du réseau antivirus. Le nom et le mot de passe administrateur relatifs au **Serveur** concerné seront requis.



Chapitre 4. Mise en route. Généralités

4.1. Création d'un simple réseau antivirus



Avant l'utilisation de l'antivirus, il est recommandé de modifier la configuration du répertoire de sauvegarde des données critiques du **Serveur** (voir le p. [Configuration de la planification de Dr.Web Enterprise Server](#)). Il est préférable de placer ce répertoire sur un autre disque local afin de minimiser la probabilité de perte simultanée des fichiers du logiciel **Serveur** et de ceux de la copie de sauvegarde.

Connexion via le Centre de Gestion Dr.Web

Par défaut, **Serveur Enterprise** démarre de manière automatique après l'installation ainsi qu'après chaque redémarrage système. (voir aussi [Dr.Web Enterprise Server](#)).

Pour configurer le **Serveur** et le logiciel antivirus, il faut se connecter au **Serveur** depuis le **Centre de Gestion Dr.Web**.

Vous pouvez accéder au **Centre de Gestion** depuis n'importe quel ordinateur connecté via le réseau au **Serveur Enterprise**, à l'adresse suivante :

`http://<adresse_Serveur>:9080`

ou

`https://<adresse_Serveur>:9081`

comme valeur `<adresse_Serveur>` spécifiez l'adresse IP ou le nom de domaine de l'ordinateur sur lequel est installé **Serveur Enterprise**.



Dans la boîte de dialogue d'authentification, entrez le nom et le mot de passe d'administrateur (le nom d'administrateur spécifié par défaut est **admin**, le mot de passe par défaut est celui que vous avez spécifié lors de l'installation du **Serveur**, voir le paragraphe [Installation de Dr.Web Enterprise Server](#)).

Si la connexion au **Serveur** est établie, la fenêtre principale du **Centre de Gestion** va s'ouvrir. Cette fenêtre affiche des informations sur le réseau antivirus (pour en savoir plus, consultez le paragraphe [Centre de Gestion Dr.Web](#)).

Gestion du réseau antivirus

Avec le **Centre de Gestion** vous pouvez gérer le **Serveur** et le réseau antivirus :

- ◆ créer des postes antivirus (voir [Installation de Dr.Web Enterprise Agent avec le Centre de Gestion Dr.Web](#)),
- ◆ [approuver des postes](#),
- ◆ éditer, configurer et supprimer des postes antivirus (voir [Gestion du poste de travail](#)),
- ◆ configurer et éditer les connexions aux **Serveurs Enterprise** voisins (voir [Particularités du réseau avec plusieurs Serveurs](#)),
- ◆ consulter les journaux d'événements et d'autres données des **Serveurs**.

Les outils de contrôle principaux sont rassemblés dans le menu principal, dans le menu de gestion et dans la barre d'outils (voir [Centre de Gestion Dr.Web](#)).

Connexion des Dr.Web Enterprise Agent

Après l'installation de l'**Agent** sur un poste depuis le [package d'installation](#), l'**Agent** tente de se connecter au **Serveur Enterprise**.



En cas de configuration de **Serveur Enterprise Server** spécifiée par défaut, l'administrateur doit approuver les nouveaux postes de manière manuelle afin de les enregistrer sur le **Serveur** (pour en savoir plus sur la politique de connexion de nouveaux postes, voir le paragraphe [Politique de connexion des postes](#)). Dans ce cas, les nouveaux postes ne seront pas automatiquement enregistrés mais placés par le **Serveur** sur la liste des postes non approuvés.

Marche à suivre pour autoriser la connexion d'un nouveau poste à Dr.Web Enterprise Server :

1. Sélectionnez l'élément **Administration** depuis le menu principal du **Centre de Gestion**.
2. Dans la fenêtre qui apparaît, sélectionnez l'élément du menu de gestion **Postes non approuvés**.
3. Une fenêtre s'ouvre et affiche la liste des postes sur lesquels **Agent** est installé mais dont l'accès n'est pas encore approuvé.
4. Sélectionnez un poste dans la liste (cochez la case contre le nom du poste) puis, depuis la barre d'outils, sélectionnez l'élément **Autoriser l'accès et spécifier un groupe primaire** afin d'approuver l'accès pour ce poste. Il vous sera proposé de sélectionner un groupe primaire pour le poste.



Pour plus d'information sur les groupes primaires, consultez le paragraphe [Héritage des éléments de la configuration du poste. Groupes primaires](#).

5. Le poste sera connecté au **Serveur** et l'apparence de l'icône du poste dans le réseau antivirus changera.

Le poste de travail sera placé dans les groupes pré-configurés de postes **Everyone**, **Online**, ainsi que dans les groupes correspondant au protocole de la connexion et au système d'exploitation correspondant.

Installation du logiciel antivirus

A partir de ce moment-là, l'installation des composants du package antivirus sur le poste se déroule sans intervention de l'administrateur.



Les composants du package antivirus spécifiés dans la configuration du groupe primaire du poste seront installés sur le poste. (pour en savoir plus, consultez le paragraphe [Composition du package antivirus](#)).

Pour terminer l'installation de certains composants du poste antivirus, le redémarrage du poste peut être requis. Dans ce cas-là, un point d'exclamation dans un triangle jaune apparaît sur le fond de l'icône d'**Enterprise Agent** dans la **Barre des tâches** (voir aussi [Dr.Web Enterprise Agent](#)).

4.2. Configuration des connexions réseau

Informations générales

Les clients listés ci-après se connectent au **Serveur Enterprise** :

- ◆ **Enterprise Agent**,
- ◆ **Installateurs réseau** des **Enterprise Agent**,
- ◆ autres **Serveurs Enterprise**.

La connexion est toujours initiée par le client.

Les schémas suivants de connexion au **Serveur** sont disponibles :

1. Via les [connexions directes](#) (direct connections).

Cette approche présente certains avantages mais il n'est pas toujours recommandé de l'utiliser.

2. En utilisant le [Service de détection de Serveur](#).

Par défaut (si une autre configuration n'est pas spécifiée de manière explicite), les clients utilisent ce **Service**.

Cette approche est recommandée dans le cas où une reconfiguration de tout le système est nécessaire et notamment



s'il faut déplacer **Serveur Enterprise** vers un autre ordinateur ou changer d'adresse IP sur la machine sur laquelle est installé le **Serveur**.

Si le réseau antivirus **ESS** est configuré pour utiliser les connexions directes, le **Service de détection de Serveur** peut être désactivé. Pour cela, dans la partie transport, laissez vide le champ **Adresse du cluster** (**Administration** → **Configuration de Dr.Web Enterprise Server** → onglet **Transport**).

Connexions directes

Configuration de Dr.Web Enterprise Server

Dans la configuration du **Serveur**, il doit être spécifié quelle adresse (voir [Annexe E. Spécification de l'adresse réseau](#)) est à écouter pour réceptionner les connexions TCP entrantes.

Ce paramètre est à spécifier dans la configuration du **Serveur Administration** → **Configuration de Dr.Web Enterprise Server** → onglet **Transport** → champ **Adresse**.

Les paramètres suivants sont définis par défaut pour l'écoute par le **Serveur** :

- ◆ tcp/0.0.0.0:2371 - est supporté afin d'assurer la compatibilité inverse, notamment pour remédier aux problèmes relatifs à la mise à niveau depuis les versions **4.XX** utilisant le port 2371.
- ◆ tcp/0.0.0.0:2193 - en cas d'utilisation du port 2193 enregistré pour **Dr.Web Enterprise Security Suite** dans IANA.

La valeur 0.0.0.0 désigne "toutes les interfaces réseaux" pour le poste sélectionné, sur lequel le **Serveur** est installé.



Pour assurer le fonctionnement de tout le système **ESS**, il suffit que le **Serveur** "soit à l'écoute" d'au moins un port TCP qui doit être connu par tous les clients.

Configuration de Dr.Web Enterprise Agent

Lors de l'installation de l'**Agent**, l'adresse du **Serveur** (l'adresse IP ou le nom réseau de la machine sur laquelle tourne **Serveur Enterprise**) peut être spécifiée de manière explicite dans les paramètres d'installation :

```
drwinst <Adresse_Serveur>
```

Pour l'installation de l'**Agent**, il est recommandé d'utiliser le nom du **Serveur** pré-enregistré dans le service DNS. Ceci facilite le processus de configuration du réseau antivirus relatif à la réinstallation de **Serveur Enterprise** sur un autre ordinateur.

Par défaut, si la commande `drwinst` est lancée sans aucun paramètre, le réseau sera scanné pour rechercher des **Serveur Enterprise** et des tentatives d'installer l'**Agent** depuis le premier **Serveur** trouvé dans le réseau seront lancées (mode *Multicasting* utilisant le [Service de détection de Serveur](#)).

Ainsi, l'adresse de **Serveur Enterprise** est connue par l'**Agent** lors de l'installation.

L'adresse du **Serveur** peut être modifiée ultérieurement de manière manuelle dans la configuration de l'**Agent**. La consultation et l'édition de la configuration de la connexion au **Serveur Enterprise** peuvent être effectuées depuis le menu contextuel de l'icône de l'**Agent Configuration** → **Connexion**.

Service de détection de Dr.Web Enterprise Server

En cas de connexion selon ce schéma, le client ne connaît pas d'avance l'adresse du **Serveur**. Avant d'établir chaque connexion, une recherche du **Serveur** dans le réseau est effectuée. Pour cela, le client



envoie vers le réseau une requête broadcast et attend une réponse du **Serveur** contenant son adresse. Dès que la réponse est réceptionnée, le client établit une connexion au **Serveur**.

Pour réaliser la procédure, le **Serveur** doit écouter le réseau en attendant des requêtes envoyées.

Plusieurs variantes de la configuration de ce schéma sont possibles. Il est important que la méthode de recherche du **Serveur** configurée pour les clients corresponde à la configuration sur le **Serveur**.

Dr.Web Enterprise Security Suite utilise par défaut le mode *Multicast over UDP* :

1. Le **Serveur** s'enregistre dans le groupe multicast avec l'adresse 231.0.0.1.
2. Les **Agents** lorsqu'ils recherchent le **Serveur** envoient vers le réseau les requêtes multicast à l'adresse de groupe 231.0.0.1.

Par défaut, pour l'écoute sur le **Serveur**, les protocoles suivants sont installés (de manière analogue aux connexions directes) :

- ◆ udp/231.0.0.1:2371
- ◆ udp/231.0.0.1:2193

Ce paramètre est spécifié dans la configuration du **Serveur Administration** → **Configuration de Dr.Web Enterprise Server** → onglet **Transport** → champ **Adresse du cluster**.

Configuration du pare-feu

Afin d'assurer l'interaction entre les composants du réseau antivirus, il est nécessaire que tous les ports et interfaces utilisés soient ouverts sur tous les postes se trouvant dans le réseau antivirus.

Pendant l'installation du **Serveur**, l'installateur permet d'ajouter de manière automatique des exclusions à la configuration du pare-feu système Windows (excepté sous Windows 2000). Pour cela, il suffit de



cocher la case **Ajouter les ports et interfaces serveur aux exclusions du pare-feu.**

En cas d'utilisation d'un autre pare-feu que celui de Windows, l'administrateur du réseau antivirus doit configurer manuellement les paramètres concernés.



Chapitre 5. Administrateurs du réseau antivirus

L'administrateur du réseau antivirus doit avoir une expérience en administration des réseaux locaux et il doit être compétent en matière de protection antivirus. L'administrateur doit avoir accès aux dossiers d'installation de **Serveur Enterprise**. En fonction des politiques de sécurité adoptées dans la société et selon sa structure, l'administrateur du réseau antivirus doit bénéficier des droits d'administrateur du réseau local, sinon il doit travailler en contact étroit avec l'administrateur du réseau local.



Les droits d'administrateur sur les postes faisant partie du réseau ne sont pas indispensables à l'administrateur du réseau antivirus pour sa gestion courante. Cependant, l'installation à distance ainsi que la désinstallation du logiciel de l'**Agent** n'est possible que dans le réseau local et nécessite les droits d'administrateur dans ce réseau, le débogage de **Serveur Enterprise** requiert un accès illimité au dossier d'installation du **Serveur**.

5.1. Authentification des administrateurs

La procédure d'authentification de l'administrateur pour se connecter à Enterprise Server peut être réalisée en modes suivants :

1. Avec la sauvegarde des données sur les administrateurs dans la BD du **Serveur**.
2. A l'aide de service Active Directory (en cas de versions du **Serveur** pour OS Windows).
3. A l'aide du protocole LDAP.
4. A l'aide du protocole RADIUS.



Les modes d'authentification sont utilisés successivement et d'après les principes suivants :

1. L'ordre d'application des méthodes d'authentification est fonction de leur succession dans les paramètres spécifiés via le **Centre de Gestion**.
2. En premier lieu, une tentative d'authentification de l'administrateur depuis la BD du **Serveur** est réalisée.
3. Par défaut, la deuxième méthode utilisée est l'authentification via LDAP, la troisième - via Active Directory, et la quatrième - via RADIUS.
4. Dans la configuration du **Serveur**, vous pouvez changer de place les modes LDAP, Active Directory et RADIUS, cependant la tentative d'authentification de l'administrateur depuis la BD sera toujours la première.
5. Par défaut, les modes LDAP, Active Directory et RADIUS sont désactivés.

Pour modifier l'ordre de méthodes d'authentification :

1. Sélectionnez l'élément **Administration** dans le menu principal du **Centre de Gestion**.
2. Dans le menu de gestion, sélectionnez la rubrique **Authentification**.
3. La fenêtre qui apparaît affiche une liste des types d'authentification dans l'ordre d'utilisation. Pour modifier l'ordre, cliquez sur la flèche se trouvant à gauche du type d'authentification. Les éléments avec les noms des méthodes d'authentification changent de place.

Authentification des administrateurs depuis la BD du Serveur

Le mode d'authentification dans lequel les données sur l'administrateurs sont conservées dans la BD du **Serveur** est utilisé par défaut.



Pour gérer la liste des administrateurs :

1. Sélectionnez l'élément **Administration** dans le menu principal du **Centre de Gestion**.
2. Dans le menu de gestion, sélectionnez la rubrique **Administrateurs**. La listes contenant tous les administrateurs enregistrés dans la BD sera affichée.

Pour en savoir plus, consultez [Gestion des comptes administrateur](#).

Authentification en cas d'Active Directory

Pour activer l'authentification via Active Directory :

1. Sélectionnez l'élément **Administration** dans le menu principal du **Centre de Gestion**.
2. Dans le menu de gestion, sélectionnez la rubrique **Authentification**.
3. Dans la fenêtre qui apparaît, passez dans la rubrique **Microsoft Active Directory**.
4. Cochez la case **Utiliser l'authentification Microsoft Active Directory**.
5. Cliquez sur **Sauvegarder**.

Lors de l'authentification des administrateurs via Active Directory, dans le **Centre de Gestion**, vous pouvez configurer uniquement l'autorisation d'utiliser ce mode d'authentification.

L'édition des propriétés des administrateurs d'Active Directory se fait de manière manuelle sur le serveur d'Active Directory.

Pour éditer les administrateurs d'Active Directory :



Les opérations listées ci-après doivent être exécutées sur un PC sur lequel est installé le composant logiciel enfichable Schéma Active Directory.



1. Pour pouvoir éditer les paramètres des administrateurs, il est nécessaire de réaliser les opérations suivantes :
 - a) Afin de modifier le schéma d'Active Directory, lancez l'utilitaire `drwschema-modify.exe` (inclus dans le package d'installation du **Serveur Enterprise**).
La modification du schéma d'Active Directory peut prendre un certain temps. En fonction de la configuration de votre domaine, la synchronisation et l'application du schéma modifié peuvent prendre 5 minutes au minimum.
 - b) Pour enregistrer le composant logiciel enfichable Schéma Active Directory, exécutez la commande `regsvr32 schmmgmt.dll` en mode administrateur, puis lancez `mmc` et ajoutez le composant logiciel enfichable **Schéma Active Directory**.
 - c) En utilisant le composant logiciel enfichable Schéma Active Directory, ajoutez à la classe **User** et (si nécessaire) à la classe **Group** la classe auxiliaire **DrWebEnterpriseUser**.



Si l'application du schéma modifié n'est pas encore achevée, la classe **DrWebEnterpriseUser** est introuvable. Dans ce cas, patientez un certain temps et réessayez comme décrit dans le p. c).

- d) Dans le mode administrateur, lancez le fichier `drweb-esuite-aduac-600-xxxxxxxxx-windows-nt-xYY.msi` (inclus dans le package d'installation **Dr.Web Enterprise Security Suite 6.0.4**) et attendez la fin d'installation.
2. Interface graphique permettant d'éditer les attributs est disponible depuis le panneau de configuration **Active Directory Users and Computers** → rubrique **Users** → dans la fenêtre d'édition des propriétés de l'utilisateur sélectionné **Administrator Properties** → sur l'onglet **Dr.Web Authentication**.
3. Les paramètres ci-dessous sont disponibles en édition (chaque attribut peut prendre les valeurs **yes**, **no** ou **not set**):



- ◆ **User is administrator** signifie que l'utilisateur est administrateur ayant les droits complets.
- ◆ **User is read-only administrator** signifie que l'utilisateur est administrateur ayant les droits en lecture seule.

Si la valeur **yes** est attribuée uniquement au paramètre **User is administrator**, cela signifie que l'utilisateur est administrateur ayant les droits complets.

Si la valeur **yes** est spécifiée pour les paramètres **User is administrator** et **User is read-only administrator** en même temps, cela signifie que l'utilisateur est administrateur ayant les droits en lecture seule.

- ◆ **Inherit permissions from groups** est le paramètre autorisant l'héritage des valeurs pour les autres paramètres depuis les groupes de l'utilisateur. Si un paramètre (ou un groupe de paramètres) prend la valeur **not set** et que le paramètre **Inherit permissions from groups** prend la valeur **yes**, les valeurs des paramètres non configurés seront héritées depuis les groupes dont l'utilisateur fait partie.



Vous pouvez consulter les algorithmes relatifs au fonctionnement et à l'analyse des attributs dans l'[Annexe O](#).

Authentification en cas d'utilisation LDAP

Pour activer l'authentification via LDAP :

1. Sélectionnez l'élément **Administration** dans le menu principal du **Centre de Gestion**.
2. Dans le menu de gestion, sélectionnez la rubrique **Authentification**.
3. Dans la fenêtre qui apparaît, passez dans la rubrique **Authentification LDAP**.
4. Cochez la case **Utiliser l'authentification LDAP**.
5. Cliquez sur **Sauvegarder**.



Il est possible de configurer l'authentification via le protocole LDAP sur n'importe quel serveur LDAP. En utilisant ce mécanisme, vous pouvez configurer le **Serveur** tournant sous l'OS de la famille UNIX pour l'authentification dans Active Directory sur le contrôleur de domaine.



Les paramètres relatifs à l'authentification LDAP sont sauvegardés dans le fichier de configuration `auth-ldap.xml`.

Pour en savoir plus sur les attributs xml principaux, consultez l'[Annexe O](#).

A la différence d'Active Directory, le mécanisme peut être configuré conformément à tout schéma LDAP. Par défaut, une tentative d'utiliser les attributs de **Dr.Web Enterprise Security Suite** sera entreprise, puisque ces attributs sont spécifiés pour Active Directory.

Le processus d'authentification LDAP :

1. L'adresse du serveur LDAP est spécifiée via le **Centre de Gestion** ou dans le fichier de configuration xml.
2. Pour un nom d'utilisateur spécifié, les actions suivantes sont réalisées :
 - ◆ Transformation du nom vers le nom distingué DN (Distinguished Name) à l'aide des masques de type DOS (en utilisant le symbole *) si les règles sont spécifiées.
 - ◆ Transformation du nom vers le nom distingué DN avec les expressions régulières si les règles sont spécifiées.
 - ◆ Utilisation du script utilisateur pour la transformation des noms vers les DN si ce script est spécifié dans les paramètres.
 - ◆ Si aucune règle de transformation ne correspond, le nom spécifié est utilisé tel qu'il est.



Le format dans lequel est spécifié le nom d'utilisateur n'est pas déterminé ni fixé, l'entreprise peut utiliser un format adopté, dans ce cas, aucune modification du schéma LDAP n'est indispensable. La transformation d'après ce schéma se fait conformément aux règles de transformation de noms vers LDAP DN.

3. Après la transformation, tout comme en cas d'Active Directory, avec le DN reçu et le mot de passe entré, une tentative d'enregistrer l'utilisateur sur le serveur LDAP sélectionné sera réalisée.
4. Puis, tout comme en cas d'Active Directory, les attributs de l'objet LDAP pour le DN reçu sont lus. Les attributs et leurs valeurs admissibles peuvent être modifiés dans le fichier de configuration.
5. S'il reste des valeurs des attributs de l'administrateur non déterminées et que l'héritage est spécifié (dans le fichier de configuration), la recherche des attributs nécessaires dans les groupes dont l'utilisateur fait partie se fait de la même manière qu'en cas d'utilisation d'Active Directory.

5.2. Types d'administrateur



Cette rubrique contient des informations sur les administrateurs dont les données relatives aux comptes administrateur sont conservées dans la BD de **Serveur Enterprise**.

Les comptes administrateur du réseau antivirus sont divisés en 4 groupes :

- ◆ administrateur avec les droits complets,
- ◆ administrateurs avec les droits "en lecture seule",
- ◆ administrateurs des groupes avec les droits complets,
- ◆ administrateurs des groupes avec les droits "en lecture seule".



Administrateurs possédant les privilèges administrateur complets

Les administrateurs possédant les privilèges administrateur complets disposent des droits exclusifs de gestion de **Serveur Enterprise** et du réseau entier. Ils sont autorisés à consulter et éditer la structure du réseau antivirus ainsi qu'à créer de nouveaux comptes administrateur. L'administrateur ayant ces droits dispose de tous les privilèges pour gérer l'antivirus sur les postes de travail. De plus, il peut restreindre, voire bloquer l'intervention de l'utilisateur du poste dans la gestion de l'antivirus (voir le paragraphe [Configuration des privilèges utilisateur](#)).

L'administrateur disposant des privilèges complets peut consulter et éditer la liste des comptes administrateur.

Administrateurs disposant des droits "en lecture seule"

Les administrateurs disposant des droits "en lecture seule" sont autorisés à consulter la configuration du réseau dans son ensemble et de ses éléments, mais il ne peuvent pas y apporter de modifications.

Administrateurs des groupes possédant des droits complets

Les administrateurs des groupes ont accès à tous les groupes système et aux groupes utilisateurs qu'ils sont autorisés à gérer (y compris les groupes emboîtés). De tels comptes peuvent être créés pour les groupes utilisateurs seulement (voir le paragraphe [Groupes système et groupes utilisateur](#)). Dans l'arborescence, seuls les groupes auxquels l'administrateur est autorisé à accéder seront affichés.

Les administrateurs des groupes ne peuvent pas consulter la liste des comptes administrateur.



Administrateurs des groupes possédant des droits "en lecture seule"

Les administrateurs des groupes peuvent disposer des privilèges complets pour éditer les groupes autorisés ainsi que des privilèges "en lecture seule".

Administrateurs par défaut

Après l'installation du **Serveur**, automatiquement le compte **admin** sera créé. C'est un compte administrateur avec les droits complets. Le mot de passe correspondant à ce compte est spécifié lors de l'installation du **Serveur** ([étape 15 de la procédure d'installation](#)).

5.3. Gestion des comptes administrateur



Cette rubrique contient des informations sur la gestion des administrateurs dont les données relatives aux comptes administrateur sont conservées dans la BD de **Serveur Enterprise**.

Les administrateurs disposant des droits complets sont autorisés à :

- ◆ [Créer](#) de nouveaux comptes et [supprimer](#) des comptes administrateurs existants.
- ◆ [Editer](#) les configurations de tous les administrateurs du réseau antivirus.

Les administrateurs des groupes et les administrateurs possédant des droits "en lecture seule" sont autorisés à :


- ◆ [Editer](#) certains paramètres relatifs à leur propre compte.



5.3.1. Création et suppression des comptes administrateur

Ajout d'un compte administrateur

Marche à suivre pour ajouter un nouveau compte administrateur :

1. Sélectionnez l'élément **Administration** depuis le menu principal du **Centre de Gestion**, dans la fenêtre qui apparaît, choisissez l'élément du menu de gestion **Administrateurs**.
2. Depuis la barre d'outils sélectionnez le bouton  **Créer un compte**.
3. La fenêtre de configuration du compte va s'ouvrir. Spécifiez les paramètres suivants :
 - ◆ Dans le champ **Login** spécifiez le nom d'administrateur à utiliser lors de l'authentification sur le **Centre de Gestion**.
 - ◆ Dans les champs respectifs **Mot de passe** et **Réentrez le mot de passe**, spécifiez un mot de passe pour accéder au **Serveur**.



Le mot de passe de l'administrateur ne doit pas contenir de caractères nationaux.

-
- ◆ Pour limiter les droits d'accès, cochez la case **En lecture seule**.
 - ◆ Dans les champs **Nom**, **Prénom** et **Patronyme** vous pouvez spécifier les données personnelles de l'administrateur.
 - ◆ Dans la liste déroulante **Langue d'interface**, sélectionnez la langue à utiliser par l'administrateur que vous créez.



- ◆ Dans la liste déroulante **Format de la date**, sélectionnez le format qui sera utilisé par l'administrateur lors de l'édition des paramètres contenant des dates. Les formats suivants peuvent être sélectionnés :

- européen : DD-MM-YYYY HH:MM:SS
- américain : MM/DD/YYYY HH:MM:SS

- ◆ **Description** du compte,
- ◆ Afin de spécifier des groupes disponibles, cochez la case **Peut administrer un nombre limité de groupes** pour le compte de l'administrateur des groupes.

Dans ce cas-là, la rubrique **Groupes gérés** sera activée. Dans cette rubrique, sélectionnez les groupes utilisateur qui seront gérés par l'administrateur. Pour cela, cliquez sur le nom du groupe dans la rubrique **Groupes connus**. Pour retirer de la liste des groupes gérés par l'administrateur, cliquez sur le nom du groupe dans la rubrique **Groupes gérés**.




Les champs marqués avec le symbole * sont obligatoires à remplir.

4. Après la fin de la configuration, cliquez sur le bouton **Sauvegarder** pour créer un compte administrateur.

Suppression d'un compte administrateur

Pour supprimer un compte administrateur, procédez comme suit :

1. Sélectionnez l'élément **Administration** depuis le menu principal du **Centre de Gestion**, dans la fenêtre qui apparaît, choisissez l'élément du menu de gestion **Administrateurs**.
2. Depuis la liste des administrateurs, sélectionnez le compte à supprimer.
3. Sélectionnez depuis la barre d'outils le bouton  **Supprimer le compte**.




5.3.2. Edition des comptes administrateur

Pour éditer un compte administrateur, procédez comme suit :

1. Ouvrez la rubrique de configuration du compte.

Les administrateurs disposant des droits complets peuvent procéder d'une des façons suivantes :

- ◆ Sélectionnez l'élément **Administration** depuis le menu principal du **Centre de Gestion**, dans la fenêtre qui apparaît, sélectionnez l'élément du menu de gestion **Administrateurs**. Dans la liste des administrateurs, sélectionnez le compte que vous souhaitez éditer. Dans la barre d'outils, cliquez sur le bouton  **Editer**.
- ◆ Sélectionnez l'élément **Préférences** du menu principal du **Centre de Gestion**, puis dans la fenêtre qui apparaît, sélectionnez l'élément **Mon compte**.

Les administrateurs des groupes et les administrateurs disposant des droits en lecture seule peuvent accéder à la configuration du compte uniquement via la rubrique **Préférences** du menu principal du **Centre de Gestion**.

2. Si nécessaire, vous pouvez éditer les paramètres qui ont été spécifiés lors de la [création d'un nouveau compte](#).




Les champs marqués par le symbole* sont obligatoires à remplir.

Pour les administrateurs des groupes et les administrateurs disposant des droits en lecture seule, la listes des paramètres disponibles pour l'édition est limitée.

3. Les paramètres suivants ne sont disponibles qu'en lecture seule :
 - ◆ Date de création du compte et date de la dernière modification de ses paramètres,
 - ◆ **Statut** - cet élément affiche l'adresse réseau de la dernière connexion sous le compte courant.



4. A la fin de l'édition, cliquez sur le bouton **Sauvegarder**.
5. Pour modifier le mot de passe relatif à un compte, sélectionnez depuis la barre d'outil l'icône  **Nouveau mot de passe**.



L'administrateur disposant des droits complets peut éditer les mots de passe d'autres administrateurs excepté le mot de passe de l'administrateur **drweb-monitoring**.



Le mot de passe de l'administrateur ne doit pas contenir de caractères nationaux.



Chapitre 6. Groupes. Gestion globale des postes de travail

Le mécanisme de groupes est conçu pour faciliter la gestion des postes de travail dans le réseau antivirus.

Les groupes peuvent être utilisés pour réaliser les actions suivantes :

- ◆ Exécution des opérations de groupe sur tous les postes faisant partie des groupes concernés.

Pour un groupe sélectionné ainsi que pour plusieurs groupes, vous pouvez lancer, consulter et arrêter les tâches de scan sur les postes faisant partie du groupe correspondant. Vous pouvez également consulter les statistiques (y compris les infections, virus, procédures de démarrage/arrêt, erreurs de scan et d'installation etc.) ainsi que les statistiques sommaires relatives à tous les postes du groupe ou à plusieurs groupes.

- ◆ Configuration des paramètres communs pour des postes via le groupe dont ils font partie. (voir [Utilisation des groupes pour configurer les postes de travail](#)).
- ◆ Structuration de la liste des postes de travail.

Il est possible de créer des groupes emboîtés.

6.1. Groupes système et groupes utilisateur

Groupes système

Lors de l'installation du **Serveur**, des groupes pré-installés (groupes système) seront créés.



Dr.Web Enterprise Security Suite comprend un jeu de groupes système. Ces groupes sont créés à l'installation de **Serveur Enterprise** et ne peuvent pas être supprimés. Cependant si nécessaire, l'administrateur peut les masquer.

Chaque groupe système (excepté le groupe **Everyone**) contient un jeu de sous-groupes unis selon un critère défini.

Everyone

C'est le groupe contenant les postes connus par **Serveur Enterprise**. Le groupe **Everyone** comprend la configuration définie par défaut.

Status

Le groupe **Status** comprend des groupes emboîtés affichant le statut actuel des postes : connecté ou non connecté au **Serveur**, le statut du logiciel antivirus : logiciel supprimé ou expiré. Ces groupes sont virtuels et ne peuvent contenir aucune configuration, ils ne peuvent pas être des groupes primaires.

- ◆ Groupe **Deinstalled**. Après la suppression du logiciel de **Enterprise Agent**, le poste est déplacé vers le groupe **Deinstalled**.
- ◆ Groupe **Deleted**. Ce groupe comprend les postes qui ont été précédemment supprimés depuis le **Serveur** par l'administrateur. Ces postes peuvent être restaurés (voir [Suppression et restauration des postes](#)).
- ◆ Groupe **Offline**. Le groupe comprend tous les postes non connectés au serveur à un certain moment.
- ◆ Groupe **Online**. Le groupe comprend tous les postes connectés à un certain moment (réagissant aux requêtes du **Serveur**).

Operating system

Cette catégorie de sous-groupes affiche les systèmes d'exploitation sous lesquels les postes tournent. Ces groupes ne sont pas virtuels et



peuvent comprendre des configurations de postes, ils peuvent également être des groupes primaires.

- ◆ Sous-groupes de la famille **Android**. Cette famille comprend un ensemble de groupes correspondant aux versions du système d'exploitation Android pour les appareils mobiles.
- ◆ Sous-groupes de la famille **Mac OS X**. Cette famille inclut un jeu de groupes correspondant à la version spécifiée de Mac OS X.
- ◆ Sous-groupe **Netware**. Ce groupe contient les postes tournant sous Novell NetWare.
- ◆ Sous-groupes de la famille **UNIX**. Cette famille contient un jeu de groupes correspondant aux systèmes d'exploitation de la famille UNIX, par exemple Linux, FreeBSD, Solaris etc.
- ◆ Sous-groupes de la famille **Windows**. Cette famille contient un jeu de groupes correspondant à la version spécifiée de Windows.
- ◆ Sous-groupe **Windows CE**. Ce sous-groupe contient les postes tournant sous OS Windows Mobile pour les appareils mobiles.

Transport

Ces sous-groupes déterminent le protocole via lequel les postes sont connectés au **Serveur** à un moment donné. Les sous-groupes sont complètement virtuels et ne peuvent contenir aucune configuration, il ne peuvent non plus être des groupes primaires.

- ◆ Groupe **TCP/IP**. Le groupe comprend les postes connectés via le protocole TCP/IP à un moment donné.
- ◆ Groupe **TCP/IP Version 6**. Le groupe comprend les postes connectés via le protocole TCP/IP à un moment donné.
- ◆ Groupe **IPX**. Le groupe comprend les postes connectés via le protocole IPX à un moment donné.
- ◆ Groupe **NetBIOS**. Le groupe comprend les postes connectés via le protocole NetBIOS à un moment donné.



Ungrouped

Ce groupe comprend les postes qui ne sont inclus dans aucun groupe utilisateur.

Groupes utilisateurs

Ce sont les groupes déterminés par l'administrateur du réseau antivirus. L'administrateur peut créer ses propres groupes ainsi que des groupes emboîtés et y ajouter des postes. **Dr.Web Enterprise Security Suite** n'a aucune limitation concernant les composants ou le nom des groupes.

Le tableau [ci-dessous](#) rassemble tous les groupes possibles ainsi que les types de groupe et les paramètres caractéristiques supportés (+) ou non supportés (-) par les groupes.

Les paramètres ci-dessous sont présentés :

- ◆ **Appartenance automatique.** Ce paramètre désigne la possibilité d'ajouter de manière automatique des postes dans un groupe (support de l'appartenance automatique) ainsi que la possibilité de modifier des composants du groupe lorsque le **Serveur** fonctionne.
- ◆ **Gestion de l'appartenance.** Ce paramètre désigne la possibilité pour l'administrateur de gérer l'appartenance à un groupe : ajouter ou supprimer des postes dans le groupe.
- ◆ **Groupe primaire.** Ce paramètre désigne la possibilité pour le groupe d'être le groupe primaire du poste.
- ◆ **Présence des configurations.** Ce paramètre détermine la possibilité du groupe de contenir des configurations (pour que les postes puissent en hériter).



Tableau 6-1. Groupes et paramètres supportés

Groupe/type de groupe	Paramètre			
	Appartenance automatique	Gestion de l'appartenance	Groupe primaire	Présence des configurations
Everyone	+	-	+	+
Status	+	-	-	-
Transport	+	-	-	-
Operating System	+	-	+	+
Ungrouped	+	-	-	-
Groupes utilisateur	-	+	+	+



En mode *Administrateur de groupe*, le groupe utilisateur géré par l'administrateur sera affiché dans la racine de l'arborescence même s'il y a un groupe parent. Tous les groupes enfants relatifs à ce groupe géré seront disponibles.

6.2. Gestion des groupes

6.2.1. Création et suppression des groupes

Création d'un groupe

Pour créer un nouveau groupe, procédez comme suit :

1. Sélectionnez l'élément **+** **Ajouter un poste ou un groupe** depuis la barre d'outils, puis depuis le sous-menu qui apparaît, sélectionnez l'élément **Créer un groupe**.

La fenêtre de création d'un groupe va s'ouvrir.





2. Le champ de saisie **Identificateur** sera rempli automatiquement. Si nécessaire, vous pouvez l'éditer lors de la création. L'identificateur ne doit pas contenir d'espaces. Vous ne pourrez pas le modifier ultérieurement.
3. Saisissez le nom du groupe dans le champ **Nom**.
4. Pour les groupes emboîtés, dans le champ **Groupe supérieur**, sélectionnez depuis la liste déroulante un groupe à spécifier en tant que parent. Si aucune configuration personnalisée n'est spécifiée, c'est depuis ce groupe que les configurations seront héritées. Pour le groupe racine (qui n'a pas de parent) laissez ce champ vide, le groupe sera ajouté dans la racine de l'arborescence. Dans ce cas, les configurations seront héritées depuis le groupe **Everyone**.
5. Laissez un commentaire dans le champ **Description**. Cliquez sur le bouton **Sauvegarder**.

Au départ, les groupes que vous avez créés sont vides. La procédure d'ajout des postes dans les groupes est décrite dans le paragraphe [Ajout des postes de travail dans le groupe. Suppression des postes depuis le groupe.](#)

Suppression d'un groupe

Pour supprimer un groupe existant, procédez comme suit:

1. Sélectionnez le groupe dans l'arborescence **Centre de Gestion**.
2. Depuis la barre d'outils, cliquez sur  **Général** →  **Supprimer les objets sélectionnés**.



Il est impossible de supprimer les groupes pré-installés.





6.2.2. Configuration des groupes

Pour configurer le groupe, procédez comme suit :

1. Sélectionnez l'élément **Réseau antivirus** du menu principal du **Centre de Gestion**, puis dans la fenêtre qui apparaît, sélectionnez un groupe dans l'arborescence.
2. Cliquez sur l'élément **Propriétés** dans le menu de gestion (panneau de gauche).
3. La fenêtre de configuration du groupe va s'ouvrir. Cette fenêtre comprend les onglets **Général** et **Configuration** dont vous trouverez la description et le paramétrage ci-après.



Lors de l'ouverture des propriétés du poste depuis l'élément  **Général** →  **Editer**, la barre d'outils permet également d'accéder à la rubrique **Informations sur les postes** affichant des informations sur les postes faisant partie du groupe en question.

4. Pour sauvegarder les modifications apportées, cliquez sur le bouton **Sauvegarder**.

Général

La rubrique **Général** comprend les champs suivants :

- ◆ **Identificateur** - l'identificateur unique du groupe. Il est protégé contre l'édition.
- ◆ **Nom** - le nom du groupe. Si nécessaire, vous pouvez le modifier.



Pour les groupes pré-installés, les champs **Identificateur** et **Nom** sont protégés contre l'édition.

- ◆ **Groupe supérieur** - le groupe parent dont le groupe en question fait partie et depuis lequel il hérite sa configuration à moins que des configuration personnalisées ne soient spécifiées.



Si aucun groupe supérieur n'est spécifié, les configurations seront héritées depuis le groupe **Everyone**.





- ◆ **Description** - champ facultatif pouvant comprendre une description du groupe.

Configuration




Pour en savoir plus sur l'héritage des configurations de groupe par les postes pour lesquels le groupe en question est primaire, consultez le paragraphe [Utilisation des groupes pour configurer les postes de travail](#).

La rubrique **Configuration** vous permet de modifier les paramètres suivants :

- ◆  - modification des droits des utilisateurs du poste pour lesquels ce groupe est primaire. La configuration des droits s'effectue de la même façon qu'en cas de postes séparés (voir [Configuration des droits d'utilisateurs](#)).
- ◆  - configuration de la planification des tâches à lancer sur les postes pour lesquels ce groupe est primaire. La configuration de la planification pour le groupe s'effectue de la même façon qu'en cas de planification centralisée des postes séparés (voir [Edition de la planification des lancements automatiques des tâches sur le poste](#)).
- ◆  - assignement de la clé de licence pour les postes pour lesquels ce groupe est primaire.
- ◆  - configuration des restrictions des mises à jour de l'antivirus sur les postes pour lesquels ce groupe est primaire (voir [Restriction de mise à jour](#)).
- ◆  - configuration de la liste des composants à installer sur les postes pour lesquels ce groupe est primaire. L'édition de la liste des composants pour les groupes se fait de même manière qu'en cas de composants à installer sur les postes (voir [Composition du package antivirus](#)).





- ◆ Configuration des composants du package antivirus : **Dr.Web Scanner pour Windows, SpIDer Guard G3 pour Windows, SpIDer Mail pour postes de travail Windows** etc. Pour modifier les paramètres, cliquez sur le bouton  se trouvant contre le composant correspondant. La configuration des composants du package antivirus pour un groupe s'effectue de la même façon que la configuration des composants du poste (voir aussi [Configuration du poste de travail](#)).

6.3. Ajout des postes de travail dans un groupe. Suppression des postes d'un groupe

Il existe plusieurs façons d'ajouter des postes dans les groupes utilisateurs :

1. [Modifier la configuration du poste.](#)
2. [Faire un glisser-déposer du poste dans l'arborescence](#) (drag-and-drop).

Pour éditer la liste des groupes dont le poste fait partie via la configuration du poste, procédez comme suit :

1. Sélectionnez l'élément **Réseau antivirus** du menu principal et dans la fenêtre qui apparaît, cliquez sur le nom du poste dans l'arborescence.
2. Ouvrez la rubrique de configuration du poste d'une des façons suivantes :
 - ◆ Sélectionnez l'élément **Propriétés** dans le menu de gestion (panneau de gauche).
 - ◆ Cliquez sur le bouton  **Général** →  **Editer** depuis la barre d'outils.
3. Depuis le panneau affiché **Propriétés du poste** passez à l'onglet **Groupes**.

La liste **Appartenance à** contient les groupes dont le poste fait déjà partie.



La liste **Groupes connus** contient la liste d'autres groupes utilisateurs.

4. Pour ajouter un poste au groupe utilisateur, cliquez sur le nom du groupe dans la liste **Groupes connus**. Le poste sera ajouté dans ce groupe et le groupe sera alors déplacé vers la liste **Appartenance à**.
5. Pour supprimer un poste du groupe utilisateur, cliquez sur le nom du groupe dans la liste **Appartenance à**. Le poste sera retiré du groupe et le groupe sera déplacé vers la liste **Groupes connus**.



Il est impossible de supprimer des postes depuis les groupes pré-installés.

6. Pour sauvegarder les modifications apportées, cliquez sur le bouton **Sauvegarder**.

Dans la rubrique de configuration du poste, vous pouvez également spécifier un groupe primaire pour le poste (pour en savoir plus, consultez le paragraphe [Héritage des éléments de configuration du poste de travail. Groupes primaires](#)).

Pour éditer la liste des groupes dont le poste fait partie via l'arborescence, procédez comme suit :

1. Sélectionnez l'élément **Réseau antivirus** du menu principal et ouvrez l'arborescence des groupes et des postes.
2. Pour ajouter un poste au groupe utilisateur, pressez la touche CTRL et tout en maintenant la touche, faites un glisser-déposer du poste vers le groupe choisi (drag-and-drop).
3. Pour déplacer le poste d'un groupe utilisateur vers un autre groupe, faites un glisser-déposer du poste (drag-and-drop) depuis le groupe utilisateur (duquel le poste sera supprimé) vers l'autre groupe utilisateur (où le poste sera ajouté).



En cas de déplacement du poste depuis un groupe pré-installé selon les variantes 2 ou 3, le poste sera ajouté au groupe utilisateur mais ne sera pas supprimé du groupe pré-installé.





Cette méthode - glisser-déposer (drag-and-drop) n'est pas supportée par le navigateur web Windows Internet Explorer 7.

Fusion des postes

Suite aux opérations avec la base de données ou en cas de réinstallation du logiciel sur les postes, l'arborescence peut contenir plusieurs postes ayant le même nom (dont un seul correspond à un poste antivirus).

Afin de supprimer les noms en doublons, procédez comme suit :

1. Sélectionnez tous les doublons relatifs à un poste. Pour cela, utilisez la touche CTRL.
2. Depuis la barre d'outils sélectionnez le bouton  **Général** →  **Fusionner les postes.**
3. Dans la liste proposée, sélectionnez le poste à considérer comme principal. Tous les autres postes seront supprimés et leurs données seront associées au poste principal.
4. Dans la liste proposée, sélectionnez le poste dont la configuration sera appliquée au poste principal sélectionné.
5. Cliquez sur le bouton **Sauvegarder.**



6.4. Utilisation des groupes pour configurer les postes de travail

La configuration du poste peut être :

1. [Héritées du groupe primaire.](#)
2. [Spécifiée de manière personnalisée.](#)

Configurations héritées

Lors de la création d'un nouveau groupe, sa configuration est héritée depuis le groupe parent ou depuis le groupe **Everyone** si le groupe parent n'est pas spécifié.

Lors de la création d'un nouveau poste, sa configuration est héritée depuis le groupe primaire.



Pour plus d'information, consultez le paragraphe [Héritage des éléments de configuration du poste de travail. Groupes primaires.](#)

Lors de la consultation ou de l'édition de la configuration du poste héritée du groupe primaire, les fenêtres informent que l'un ou l'autre paramètre est hérité du groupe primaire.

Vous pouvez spécifier des configurations pour des [groupes](#) et des [postes](#) différents en modifiant les paramètres.


Configurations personnalisées

Pour spécifier des configurations personnalisées pour le poste, éditez la rubrique des paramètres correspondante (voir [Configuration du poste de travail](#)). Il sera indiqué dans la rubrique que le paramètre en question est spécifié de manière personnalisée pour le poste concerné.



Lors de la définition des configurations personnalisées d'un poste, les configurations du groupe primaire et toutes ses modifications n'auront aucun impact sur les configurations du poste.

Vous pouvez rétablir la configuration héritée depuis le groupe primaire.

Pour cela, cliquez sur le bouton  **Supprimer les configurations** se trouvant dans la barre d'outils du **Centre de Gestion** dans la rubrique relative aux paramètres concernés ou dans la rubrique correspondante depuis les propriétés du poste.

6.4.1. Héritage des éléments de configuration du poste de travail. Groupes primaires

Héritage des configurations

Lors de la création d'un nouveau poste, ses paramètres de configuration sont hérités d'un des groupes dont il fait partie. Ce groupe est nommé *primaire*. En cas de modifications apportées dans la configuration du groupe primaire, elles seront héritées par les postes appartenant au groupe, excepté le cas où les postes possèdent des configurations personnalisées. A la création du poste, vous pouvez désigner quel groupe sera spécifié comme primaire. Par défaut, c'est le groupe **Everyone**.



Si le groupe primaire n'est pas le groupe **Everyone** et n'a pas de configuration personnalisée, les configurations du groupe **Everyone** seront héritées.

Il est possible de créer des groupes emboîtés.

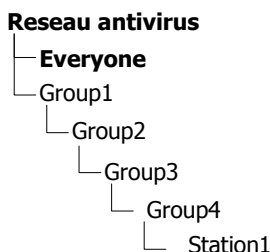
En cas de groupes emboîtés, si la configuration du poste n'est pas personnalisée, l'héritage des éléments de configuration se fait selon la structure des groupes emboîtés. La recherche se déroule vers le haut de l'arborescence à partir du groupe primaire du poste, son groupe supérieur et jusqu'à l'élément racine de l'arborescence. Dans le cas où




aucune configuration personnalisée n'est trouvée, les paramètres de configuration du groupe **Everyone** seront hérités.

Exemple :

Voici la structure de l'arborescence :



Le groupe `Group4` est primaire pour le poste `Station1`. Lors de l'héritage des configurations par le poste `Station1`, la recherche sera effectuée dans l'ordre suivant : `Station1` → `Group4` → `Group3` → `Group2` → `Group1` → `Everyone`.

Par défaut, la structure du réseau est présentée de façon à ce que l'on puisse voir tous les groupes dont le poste fait partie. Si vous souhaitez afficher seulement l'appartenance aux groupes primaires, décochez la case **Appartenance à tous les groupes** dans l'élément  **Configuration de l'arborescence** dans la barre d'outils du **Centre de Gestion**.

Paramétrage du groupe primaire



Il existe plusieurs moyens pour spécifier un groupe primaire pour un poste et pour un groupe de postes.





Afin de spécifier un groupe primaire pour le poste de travail :

1. Sélectionnez l'élément **Réseau antivirus** dans le menu principal, puis dans la fenêtre qui apparaît cliquez sur le nom du poste dans l'arborescence.
2. Dans le menu de gestion qui s'ouvre (panneau de gauche), sélectionnez l'élément **Propriétés**. Dans la fenêtre qui s'ouvre, allez à l'onglet **Groupe**.
3. Pour spécifier un autre groupe comme primaire, cliquez sur l'icône du groupe depuis la liste **Appartenance à**.
4. Cliquez sur le bouton **Sauvegarder**.

Pour spécifier un groupe primaire pour plusieurs postes de travail :

1. Sélectionnez l'élément **Réseau antivirus** dans le menu principal puis dans la fenêtre qui apparaît, cliquez sur les noms des groupes souhaités dans l'arborescence (vous pouvez également sélectionner des groupes, dans ce cas là, l'action sera appliquée à tous les postes appartenant aux groupes concernés ; pour sélectionner plusieurs postes et groupes, cliquez dessus tout en maintenant pressées les touches CTRL ou SHIFT).
2. Depuis la barre d'outils cliquez sur  **Général** →  **Spécifier le groupe primaire**. La fenêtre contenant une liste des groupes pouvant être spécifiés comme primaires pour les postes sélectionnés apparaîtra.
3. Afin de spécifier le groupe primaire, cliquez sur le nom de groupe.





Vous pouvez spécifier le groupe comme primaire pour tous les postes qu'il comprend. Pour cela, sélectionnez le groupe dans l'arborescence et depuis la barre d'outils du **Centre de Gestion** cliquez sur  **Général** →  **Spécifier le groupe comme primaire**.



6.4.2. Copie des configurations vers d'autres groupes/postes

Les configurations des outils antivirus, planifications, droits des utilisateurs ainsi que d'autres configurations de groupe ou de poste peuvent être copiées (diffusées) vers un groupe ou vers des groupes ou des postes.

Pour copier les configurations, procédez comme suit :

1. Cliquez sur le bouton **Diffuser les configurations vers un autre objet** :
 - ◆  dans la fenêtre d'édition de la configuration du composant antivirus,
 - ◆  dans la fenêtre d'édition de la planification,
 - ◆  dans la fenêtre d'édition des restrictions de mises à jour,
 - ◆  dans la fenêtre de composants à installer.L'arborescence réseau sera affichée.
2. Sélectionnez dans l'arborescence les groupes et les postes vers lesquels vous souhaitez diffuser la configuration.
3. Afin de réaliser la modification de la configuration des groupes concernés, cliquez sur le bouton **Sauvegarder**.

6.5. Comparaison des postes et des groupes

Il existe une possibilité de comparer les postes et les groupes selon les paramètres principaux.



Pour comparer plusieurs objets du réseau antivirus :

1. Sélectionnez l'élément **Réseau antivirus** dans le menu principal et sélectionnez ensuite depuis l'arborescence les objets que vous souhaitez comparer. Utilisez les touches CTRL et SHIFT. Les variantes ci-dessous sont possibles :
 - ◆ Sélection de plusieurs postes - pour comparer les postes sélectionnés ;
 - ◆ Sélection de plusieurs groupes - pour comparer les groupes sélectionnés et tous les groupes emboîtés ;
 - ◆ Sélection de plusieurs postes et groupes - pour comparer tous les postes : les postes sélectionnés dans l'arborescence ainsi que ceux appartenant à tous les groupes sélectionnés et à leurs groupes emboîtés.
2. Dans le menu de gestion (panneau de gauche) cliquez sur l'élément **Comparer**.
3. Le tableau comparatif pour les objets sélectionnés s'affichera.
 - ◆ Paramètres utilisés pour comparer les groupes :
 - **Postes** - total de postes appartenant à un groupe sélectionné.
 - **Postes sur réseau** - total de postes actifs à l'heure actuelle.
 - **Groupe primaire pour** - total de postes pour lesquels le groupe sélectionné est un groupe primaire.
 - **Configuration personnalisée** - liste des composants pour lesquels les configurations sont personnalisées et non héritées du groupe supérieur.
 - ◆ Paramètres utilisés pour comparer les postes :
 - **Date de création** du poste.
 - **Groupe primaire** pour le poste.
 - **Configurations personnalisées** - la liste des composants pour lesquels les configurations sont personnalisées et non héritées du groupe primaire.
 - **Composants installés** - la liste des composants antivirus installés sur le poste.



Chapitre 7. Gestion du poste de travail

Le réseau antivirus géré par **Dr.Web Enterprise Security Suite** permet de configurer les packages antivirus sur les postes de manière centralisée. **Dr.Web Enterprise Security Suite** permet de réaliser les paramétrages suivants :

- ◆ configuration des paramètres des outils antivirus,
- ◆ configuration de la planification des lancements de tâches de scan,
- ◆ lancement des tâches sur des postes indépendamment de la planification,
- ◆ lancement du processus de mise à jour des postes y compris le lancement d'une mise à jour après une erreur survenue, avec remise à zéro du statut d'erreur.

L'administrateur du réseau antivirus peut accorder à l'utilisateur des droits autorisant la configuration et le lancement des tâches ainsi que limiter ou enlever ces droits.

Des modifications peuvent être apportées dans la configuration du poste même lorsqu'il est temporairement inaccessible pour le **Serveur**. Ces modifications seront prises en compte sur le poste dès que la connexion au **Serveur** aura été rétablie.



7.1. Gestion des entrées relatives aux postes de travail

7.1.1. Politique de connexion des postes



La procédure de création du poste via le **Centre de Gestion** est décrite dans le paragraphe [Création d'un nouveau compte](#).

La gestion de la procédure d'approbation des postes sur **Serveur Enterprise** est fonction des paramètres suivants :

1. Si lors de l'installation de l'**Agent** sur le poste, le mode d'approbation **Automatique** a été sélectionné, alors le mode d'accès des postes au **Serveur** sera déterminé conformément aux paramètres spécifiés sur le **Serveur** (utilisé par défaut), voir [ci-après](#).
2. Si lors de l'installation de l'**Agent** sur le poste, le mode d'approbation **Manuel** a été choisi et que les paramètres **Identificateur** et **Mot de passe** ont été spécifiés, alors pendant la connexion au **Serveur**, le poste sera approuvé de manière automatique quels que soient les paramètres configurés sur le **Serveur** (utilisé par défaut en cas d'installation de l'**Agent** avec le package d'installation *esinst* - voir [Fichiers d'installation](#)).



La procédure de configuration d'un mode d'approbation de l'**Agent** pendant son installation est décrite dans la rubrique [Installation de Dr.Web Enterprise Agent avec l'installateur en mode graphique](#) (étape 6).




Marche à suivre pour modifier le mode d'accès des postes au Dr.Web Enterprise Server :

1. Ouvrez la configuration du **Serveur**. Pour cela, sélectionnez l'élément **Administration** depuis le menu principal puis dans la fenêtre qui apparaît, sélectionnez l'élément du menu de gestion **Configuration de Dr.Web Enterprise Server**.
2. Sur l'onglet **Général**, dans la liste déroulante **Novices**, sélectionnez l'une des valeurs disponibles :
 - ◆ **Confirmation d'accès manuelle** (ce mode est spécifié par défaut à moins qu'il ne soit modifié lors de l'installation du **Serveur**),
 - ◆ **Autoriser l'accès automatiquement**,
 - ◆ **Toujours refuser l'accès**.



Confirmation d'accès manuelle

Si le mode **Confirmation d'accès manuelle** est activé, les nouveaux postes seront inscrits dans la liste des postes non approuvés avant qu'ils ne soient traités par l'administrateur.

Pour accéder à la liste des postes non approuvés :

1. Sélectionnez l'élément **Administration** dans le menu principal du **Centre de Gestion**, dans la fenêtre qui apparaît, sélectionnez l'élément du menu de gestion **Postes non approuvés**.
2. Dans la fenêtre qui s'ouvre, vous trouverez le tableau affichant les postes avec les **Agents** déjà installés ainsi que ceux qui demandent un accès au **Serveur**, des informations générales sur les postes seront également affichées : heure de réception de la requête, le nom réseau du poste, l'adresse IP du poste et le système d'exploitation installé.
3. Pour configurer l'accès au **Serveur**, cochez les cases contres les postes concernés ou cochez la case dans l'en-tête du tableau afin de sélectionner tous les postes. Depuis la barre d'outils sélectionnez une action à appliquer aux postes choisis :
 - ◆  - autoriser l'accès aux postes sélectionnés et spécifier le groupe primaire depuis la liste proposée,



  - refuser l'accès aux postes sélectionnés.

Autorisation d'accès automatique



Si le mode **Autoriser l'accès automatiquement** est actif, tous les postes demandant l'accès au **Serveur** se connectent de manière automatique sans aucune requête à l'administrateur. Dans ce cas, le groupe **Everyone** sera spécifié en tant que primaire.

Accès refusé

Si le mode **Toujours refuser l'accès** est actif, le **Serveur** refuse l'accès aux requêtes reçues depuis des nouveaux postes. L'administrateur doit créer des comptes sur les postes de manière manuelle puis leur accorder des mots de passe d'accès.

7.1.2. Suppression et récupération du poste

Pour supprimer l'entrée sur un poste de travail :

1. Afin de supprimer un poste via le **Centre de Gestion** : sélectionnez l'élément du menu principal **Réseau antivirus** puis dans la fenêtre qui apparaît, cliquez sur les boutons  **Général** →  **Supprimer les objets sélectionnés** dans la barre d'outils.
2. La fenêtre de confirmation de la suppression va s'ouvrir. Cliquez alors sur **OK**.



Après la suppression des postes depuis l'arborescence, ils sont placés dans le tableau des postes supprimés depuis lequel ils peuvent être récupérés via le **Centre de Gestion**.

Pour récupérer une entrée sur le poste :

1. Sélectionnez l'élément du menu principal **Réseau antivirus**, puis dans la fenêtre qui apparaît, sélectionnez dans l'arborescence un ou plusieurs postes distants à restaurer.



Tous les postes supprimés se trouvent dans le sous-groupe **Deleted** du groupe **Status**.

2. Depuis la barre d'outils sélectionnez l'élément  **Général** →  **Restaurer les postes supprimés**.
3. La rubrique relative à la restauration des postes supprimés va s'ouvrir. Vous pouvez alors configurer les paramètres du poste à spécifier lors de sa restauration :
 - ◆ **Groupe primaire** - sélectionnez un groupe primaire vers lequel le poste sera ajouté après la restauration. Par défaut, le groupe primaire associé au poste avant sa suppression sera spécifié.



En cas de restauration de plusieurs postes à la fois, la variante suivante est spécifiée par défaut : **Ancien groupe primaire**, ce qui signifie que pour chaque poste restauré, l'ancien groupe primaire où les postes ont figuré avant la suppression sera spécifié. En cas de sélection d'un groupe pour tous les postes restaurés, ce groupe sélectionné sera spécifié pour tous les postes restaurés.



- ◆ La rubrique **Appartenance à** vous permet de modifier la liste des groupes dont le poste fait partie. Par défaut, la liste des groupes où le poste a figuré avant la suppression est spécifiée. Afin d'ajouter des postes vers les groupes utilisateur, cliquez sur les noms des groupes utilisateur disponibles dans la rubrique **Liste des groupes**. Pour enlever les groupes utilisateur dont le poste faisait partie avant la suppression, cliquez sur les noms des groupes respectifs dans la rubrique **Appartenance à**.
4. Pour restaurer un poste avec les paramètres spécifiés, cliquez sur le bouton **Restaurer**.



7.2. Configuration du poste de travail

Propriétés du poste

Marche à suivre pour consulter et éditer les propriétés du poste de travail :

1. Sélectionnez l'élément **Réseau antivirus** du menu principal du **Centre de Gestion**, puis dans la fenêtre suivante, sélectionnez le poste depuis l'arborescence et cliquez sur  **Général** →  **Editer** dans la barre d'outils.
2. Dans la partie droite de la fenêtre du **Centre de Gestion**, la fenêtre affichant les propriétés du poste va s'ouvrir. Cette fenêtre contient les groupes de paramètres suivants : **Général**, **Configuration**, **Groupes**, **Sécurité**, **Emplacement**. Le contenu des groupes et leur paramétrage sont décrits ci-dessous.
3. Pour sauvegarder les modifications apportées, cliquez sur le bouton **Sauvegarder**.

Général

La rubrique **Général** contient les champs suivants disponibles en lecture seule :

- ◆ **Identificateur** - un identificateur unique du poste.
- ◆ **Nom** - nom du poste.

Vous pouvez également spécifier les valeurs dans les champs ci-dessous :

- ◆ Dans le champ **Mot de passe** - le mot de passe pour l'authentification du poste sur le **Serveur** (il sera nécessaire de réentrer ce mot de passe dans le champ **Confirmer le mot de passe**). En cas de changement de mot de passe, pour pouvoir connecter l'**Agent**, il est nécessaire d'effectuer une procédure équivalente dans la configuration de la connexion de l'**Agent** sur



le poste.







- ◆ Dans le champ **Description** vous pouvez entrer des informations supplémentaires.



Les valeurs dans les champs marqués par le symbole * sont obligatoires à spécifier.

Configuration

La rubrique **Configuration** vous permet de modifier la configuration du poste qui comprend :

- ◆  - modification des droits de l'utilisateur du poste (voir aussi le paragraphe [Configuration des droits des utilisateurs](#)).
- ◆  - configuration de la planification des lancements des tâches sur le poste. La configuration de la planification centralisée est décrite dans le paragraphe [Configuration de la planification des tâches sur le poste de travail](#).
- ◆  - assignement de la clé de licence au poste.
- ◆  - configuration des restrictions de mise à jour du logiciel antivirus. La configuration des mises à jour est décrite dans le paragraphe [Restriction de mise à jour](#).
- ◆  - liste des composants à installer (voir [Composition du package antivirus](#)).
- ◆ Configuration des composants du package antivirus - **Dr.Web Scanner pour Windows, SpIDer Guard G3 pour Windows, SpIDer Mail pour postes de travail Windows** etc. Pour modifier les configurations, cliquez sur le bouton  contre le composant à modifier.

Depuis le **Centre de Gestion** vous pouvez accéder aux boutons permettant de supprimer les configurations personnalisées. Ces boutons se trouvent à droite des boutons correspondants de la configuration. Après la suppression de la configuration personnalisée du poste, la configuration héritée du groupe primaire sera spécifiée.



Le jeu de composants et les recommandations sur leur installation sont décrits dans le manuel **Antivirus Dr.Web® pour Windows. Manuel utilisateur** et **Dr.Web® Agent pour Windows. Manuel utilisateur**.

Cependant, la gestion des configurations via le **Centre de Gestion** est différente de la gestion des configurations effectuée directement depuis les composants antivirus :

- ◆ pour modifier les paramètres pouvant avoir les valeurs **Oui** ou **Non**, cliquez sur la valeur souhaitée. Les champs de saisie et les listes déroulantes ont une interface standard,
- ◆ pour gérer des paramètres, utilisez les boutons se trouvant à droite, contre les paramètres :



- rétablir la valeur d'avant l'édition,



- spécifier la valeur par défaut pour le paramètre,

- ◆ pour gérer un jeu de paramètres, utilisez les boutons se trouvant dans la barre d'outils (partie haute dans la plupart des fenêtres de configuration, par exemple **Planification, Droits, Dr.Web Scanner pour Windows, SpIDer Guard pour Windows** et **SpIDer Mail pour postes de travail Windows**) :



- diffuser les configurations vers d'autres objets (groupe ou plusieurs groupes et postes de travail),



- rétablir les valeurs des paramètres d'avant l'édition,



- spécifier les valeurs par défaut pour tous les paramètres,



- exporter les paramètres vers un fichier de format spécifique,



- importer les paramètres depuis un fichier de format spécifique,



- supprimer la configuration spécifique pour le poste de travail (la configuration héritée des groupes sera spécifiée, pour en savoir plus, consultez le paragraphe [Utilisation des groupes pour configurer les postes de travail](#)).



- ◆ Cliquez sur le bouton **Sauvegarder** pour accepter les modifications apportées.

Groupes

La rubrique **Groupes** vous permet de configurer une liste des groupes dont le poste sélectionné fait partie (voir [Ajout des poste dans le groupe. Suppression des postes depuis le groupe](#)).

Cette rubrique vous permet aussi de modifier le groupe primaire pour le poste. Cette procédure est décrite dans le paragraphe [Héritage des éléments de configuration du poste. Groupes primaires](#).

Sécurité

La rubrique **Sécurité** permet de spécifier des limitations pour les adresses réseau depuis lesquelles l'accès à cette page est autorisé.

Afin d'autoriser toute connexion, décochez la case **Utiliser cette liste de contrôle d'accès**. Pour paramétrer les listes d'adresses autorisées et interdites, cochez la case.

Afin d'autoriser l'accès depuis une adresse TCP déterminée, ajoutez l'adresse dans la liste **TCP: autorisé** ou **TCPv6: autorisé**.

Afin d'interdire une adresse TCP, ajoutez-la dans la liste **TCP: interdit** ou **TCPv6: interdit**.

Pour ajouter une adresse dans la liste :

1. Entrez l'adresse réseau dans le champ correspondant et cliquez ensuite sur le bouton **Sauvegarder**.
2. Pour ajouter un nouveau champ d'adresse, cliquez sur le bouton dans la rubrique correspondante. Pour supprimer le champ, cliquez sur le bouton .

L'adresse réseau doit être spécifiée au format suivant : `<adresse IP>/ [<préfixe>]`.



Exemple d'utilisation de préfixe :

1. Le préfixe 24 désigne les réseaux ayant le masque :
255.255.255.0

Un réseau associé contient 254 adresses

Les adresses d'hôtes dans de tels réseaux ont le format :
195.136.12.*

2. Le préfixe 8 désigne les réseaux ayant le masque
255.0.0.0

Un réseau associé contient jusqu'à 16387064 adresses
(256*256*256)

Les adresses d'hôtes dans de tels réseaux ont le format :
125.*.*.*

De plus, vous pouvez supprimer des adresses dans la liste et éditer les adresses ajoutées dans la liste.

Des limitations pour les adresses IPX peuvent être spécifiées de manière analogue.

Les adresses non mentionnées dans aucune des listes sont autorisées ou interdites en fonction du statut de la case **Priorité de l'interdiction** : si la case est cochée, les adresses non incluses dans aucune des listes (ou celles incluses dans les deux listes) seront interdites. Sinon les adresses sont autorisées.

Emplacement



La rubrique **Emplacement** permet de spécifier les paramètres de l'emplacement géographique du poste de travail.



Il est possible de créer des groupes d'utilisateurs en fonction des droits et configurations optimales. La configuration des paramètres principaux du postes à l'aide des groupes vous permettra de gagner le temps nécessaire pour éditer la configuration de chaque poste séparément.

Suppression des configurations de poste

Pour supprimer la configuration personnalisée du poste :

1. Sélectionnez l'élément **Réseau antivirus** du menu principal du **Centre de Gestion**, puis dans la fenêtre qui apparaît, sélectionnez le poste dans l'arborescence et depuis la barre d'outils cliquez les boutons  **Général** →  **Supprimer les configurations personnalisées de l'objet**. La liste des configurations du poste sera affichée, les cases contre les configurations personnalisées sont cochées.
2. Décochez les cases contre les configurations à supprimer et cliquez ensuite sur le bouton **Sauvegarder**. Les configurations du poste héritées du groupe primaire seront rétablies.



A l'édition de la configuration du poste relative aux composants **SpIDer Guard pour Windows** et **Dr.Web Scanner pour Windows**, merci de consulter les recommandations sur l'utilisation des logiciels antivirus sous Windows Server 2003, Windows 2000 et Windows XP. La rubrique respective se trouve à l'adresse suivante : <http://support.microsoft.com/kb/822158/ru> et vous permettra d'optimiser le fonctionnement du système.

Si votre clé de l'**Agent** (agent.key) autorise l'utilisation du filtre antispam pour le composant **SpIDer Mail**, vous pouvez configurer le filtre sur l'onglet **Antispam** (sélectionnez depuis le menu contextuel de tout groupe ou tout poste l'élément **SpIDer Mail pour postes de travail Windows**).



A partir de la version **5.0**, le jeu de composants du package antivirus **Dr.Web Enterprise Security Suite** comprend les produits **SpIDer Gate** et **Office Control**, dont l'utilisation est autorisée à condition que ces produits soient mentionnés dans votre licence (**Antivirus + Antispam**) que vous pouvez consulter dans la clé de l'**Agent**.

Pour en savoir plus sur la configuration du filtre antispam ainsi que sur les composants **SpIDer Gate** et **Office Control**, merci de consulter le manuel **Antivirus Dr.Web® pour Windows. Manuel Utilisateur**.

7.2.1. Configuration des droits d'utilisateurs

Les postes de travail héritent les droits du groupe primaire. D'ailleurs, vous pouvez modifier la configuration des droits non seulement pour un groupe entier mais aussi pour un poste sélectionné.

Pour configurer les droits des utilisateurs du poste de travail depuis le Centre de Gestion :

1. Sélectionnez l'élément **Réseau antivirus** dans le menu principal, puis cliquez sur le nom du poste dans l'arborescence. Dans le menu de gestion qui va s'ouvrir (panneau de gauche), sélectionnez l'élément **Droits**. La fenêtre de configuration des droits va s'ouvrir.
2. Vous pouvez éditer les droits dans les onglets suivants :
 - ◆ **Composants** - configuration des droits relatifs à la gestion des composants antivirus. Par défaut, l'utilisateur conserve le droit de lancer chaque composant mais il n'est pas autorisé à éditer la configuration des composants ni à stopper des composants.
 - ◆ **Général** - configuration des droits relatifs à la gestion de **Enterprise Agent** et de ses fonctions :
 - **Mode itinérant et utilisation de SGMAJ Dr.Web** - désactive l'élément **Mode itinérant** dans le menu contextuel de l'**Agent**.



- **Création d'une planification locale** - désactive l'élément **Locale** dans la rubrique **Planification** dans le menu contextuel de l'**Agent**.
- **Changement de mode de fonctionnement** - désactive l'élément **Mode de lancement** et le groupe de paramètres **Composants à installer** dans le menu contextuel de l'**Agent**.
- **Changement de paramètres de Dr.Web Enterprise Agent** - désactive les éléments **Synchroniser l'heure** et le groupe de paramètres **Niveau de détail du journal** dans la rubrique **Configuration** du menu contextuel de l'**Agent**.
- **Arrêt de l'interface Dr.Web Enterprise Agent** - désactive l'élément **Quitter** dans le menu contextuel de l'**Agent** excepté le cas où l'interface de l'**Agent** a été lancée en mode Administrateur.
- **Blocage d'accès réseau** - désactive l'élément **Accès réseau** dans le menu contextuel de l'**Agent**.
- **Désactivation du système d'autoprotection** - désactive le jeu de paramètres **Protection du système** dans le menu contextuel de l'**Agent**.
- **Suspension de l'autoprotection** - désactive l'élément **SelfPROtect** dans le menu contextuel de l'**Agent**.
- **Désinstallation de Dr.Web Agent** - interdit la suppression de l'**Agent** depuis le poste avec l'installateur ainsi qu'avec les outils standard de Windows (voir [Suppression des composants du logiciel pour Windows®](#)). Dans ce cas, vous pouvez supprimer l'**Agent** uniquement depuis l'élément  **Général** →  **Désinstaller Dr.Web Agent** dans la barre d'outils du **Centre de Gestion**.





Pour modifier (accorder ou enlever) un droit, cochez ou décochez la case correspondante.



En cas de désactivation d'un élément associé à un paramètre de l'**Agent**, la dernière valeur spécifiée pour ce paramètre avant l'extinction sera appliquée.



Pour prendre connaissance de la description des actions associées aux éléments du menu, merci de consulter la documentation **Dr.Web Agent pour Windows. Manuel Utilisateur**.

3. Pour refuser une configuration des droits et revenir vers la configuration spécifiée par défaut et héritée des groupes pré-installés, cliquez sur le bouton  **Supprimer les configurations**.
4. Vous pouvez également diffuser ces configurations vers un autre objet en cliquant sur le bouton .
5. Afin d'exporter les configuration vers un fichier, cliquez sur .
6. Afin d'importer les configurations depuis un fichier, cliquez sur .
7. Pour accepter les modifications des droits, cliquez sur le bouton **Sauvegarder**.



Si lors de l'édition des paramètres du poste, le poste n'est pas connecté au **Serveur**, les paramètres seront pris en compte dès que **l'Agent** aura rétabli la connexion au **Serveur**.

7.2.2. Consultation des composants installés du package antivirus

Composants

Pour consulter les composants installés sur le poste de travail :

1. Sélectionnez l'élément **Réseau antivirus** dans le menu principal du **Centre de Gestion**, puis dans la fenêtre qui apparaît, cliquez sur le nom du poste ou du groupe dans l'arborescence.
2. Dans le menu de gestion qui s'ouvre (panneau de gauche),



sélectionnez l'élément **Composants installés**. La fenêtre affichant la liste des composants installés va s'ouvrir.



La liste des composants à installer peut varier en fonction des éléments suivants :

- ◆ Composants autorisés par le fichier clé de licence.
- ◆ OS installé sur le poste de travail.
- ◆ Paramètres configurés par l'administrateur sur le **Serveur** du réseau antivirus. L'administrateur peut modifier le jeu de composants du package antivirus sur le poste avant l'installation de l'**Agent** (voir [Composition du package antivirus](#)) ainsi qu'à tout moment après l'installation.



Il n'est pas recommandé d'installer les composants **SpIDer Gate**, **SpIDer Mail** et **Dr.Web Firewall** sur les serveurs exécutant des fonctions réseau importantes (contrôleurs de domaine, serveurs de licences etc.) afin d'éviter d'éventuels conflits entre les services réseau et les composants antivirus **Dr.Web**.

Bases virales

La marche à suivre pour consulter les bases virales installées sur le poste :

1. Sélectionnez l'élément **Réseau antivirus** du menu principal du **Centre de Gestion**, puis dans la fenêtre qui apparaît, cliquez sur le nom du poste dans l'arborescence. Dans le menu de gestion (panneau de gauche) qui s'ouvre, sélectionnez l'élément **Bases virales** depuis la rubrique **Tables**.
2. Une fenêtre apparaît et affiche les informations suivantes sur les bases virales installées : nom de fichier contenant la base virale, version de la base virale, total d'entrées dans la base virale, date de création de la base virale.



En cas de désactivation de l'affichage de l'élément **Bases virales**, pour l'activer, sélectionnez l'élément **Administration** du menu principal et dans la fenêtre qui apparaît, sélectionnez l'élément du menu de gestion **Configuration de Dr.Web Enterprise Server**. Dans l'onglet **Données statistiques**, cochez les cases **Surveillance des bases virales** et **Surveillance des statuts des postes**, puis redémarrez le **Serveur**.

7.2.3. Composition du package antivirus

Pour configurer la liste des composants du package antivirus à installer, procédez comme suit :

1. Sélectionnez l'élément **Réseau antivirus** depuis le menu principal du **Centre de Gestion**, dans la fenêtre qui s'ouvre, depuis l'arborescence, sélectionnez le poste. Dans la fenêtre de gestion qui apparaît (panneau de gauche), sélectionnez l'élément **Composants à installer**.
2. Pour installer les composants nécessaires, sélectionnez l'une des variantes dans la liste déroulante :
 - ◆ **doit** - la présence du composant sur le poste est obligatoire. Lors de la création d'un nouveau poste, le composant fait partie du package antivirus. Si la valeur **doit** est spécifiée dans la configuration du poste existant, le composant correspondant sera ajouté au package antivirus installé ;
 - ◆ **peut** - détermine une possibilité d'installer le composant antivirus. C'est l'utilisateur qui décide d'installer ou de ne pas installer le composant ;
 - ◆ **ne peut pas** - interdit la présence du composant sur le poste. Lors de la création d'un nouveau poste, le composant ne fait pas partie du package antivirus. Si la valeur **ne peut pas** est spécifiée dans la configuration du poste existant, le composant concerné sera enlevé depuis le package antivirus.



Le tableau 7-1 indique si le composant sera installé sur le poste (+) en fonction des paramètres spécifiés par l'utilisateur et des configurations spécifiées par l'administrateur sur le **Serveur** :

Tableau 7-1.

Paramètres spécifiés par l'utilisateur	Configuré sur le Serveur		
	Doit	Peut	Ne peut pas
Installer	+	+	
Ne pas installer	+		

3. Cliquez sur le bouton **Sauvegarder** pour enregistrer les paramètres et sauvegarder le jeu de composants modifié du package antivirus installé sur le poste.



Il est impossible d'installer le composant **Antispam VadeRetro** si au moins un des produits listés ci-après n'est pas installé sur le poste :

- ◆ **SpIDer Mail,**
- ◆ **Dr.Web plug-in pour MS Outlook,**
- ◆ **Dr.Web pour IBM Lotus Domino,**
- ◆ **Dr.Web pour MS Exchange Server,**
- ◆ **Dr.Web pour Qbik WinGate plug-in.**



7.3. Configuration de Dr.Web Enterprise Agent sous Windows®

Marche à suivre pour consulter ou modifier la configuration de Dr.Web Enterprise Agent sur le poste de travail sous Windows :

1. Sélectionnez l'élément **Réseau antivirus** du menu principal du **Centre de Gestion**.
2. Dans la fenêtre qui apparaît, cliquez sur le nom du groupe ou du poste dans l'arborescence.
3. Depuis le menu de gestion (panneau de gauche) ouvert, sélectionnez l'élément **Dr.Web Enterprise Agent pour Windows**.
4. La fenêtre de configuration de l'**Agent** va s'afficher.



En cas de modifications apportées dans la configuration sans prendre en compte les paramètres du **Serveur** (notamment la modification du mode de chiffrement et de compression, ainsi que la modification de la clé de chiffrage), l'**Agent** sera déconnecté du **Serveur**.

En cas de modifications apportées dans la configuration de l'**Agent** via le **Centre de Gestion**, cliquez sur le bouton **Sauvegarder** pour accepter les modifications.

Onglet Général

L'onglet **Général** présente les paramètres généraux de l'**Agent** :

- ◆ Dans le champ **Clé publique du Serveur**, spécifiez le chemin vers la clé ouverte de chiffrement du **Serveur Enterprise** sur le poste de l'utilisateur.
- ◆ Dans le champ **Fichier clé local Dr.Web**, spécifiez le chemin vers le fichier clé de licence local du produit **Dr.Web** si vous souhaitez sauvegarder une copie du fichier clé de licence sur le poste. Sinon le fichier clé sera placé uniquement sur le **Serveur**.




- ◆ Dans le champ **Périodicité d'envoi des statistiques (en minutes.)**, spécifiez un délai relatif à l'envoi de toutes les informations statistiques récoltées sur le poste par l'**Agent** au **Serveur**.
- ◆ Dans la liste déroulante **langue**, spécifiez la langue d'interface de l'**Agent**.
- ◆ Cochez la case **Microsoft Network Access Protection** pour activer le support de la technologie *Microsoft® Network Access Protection* utilisée pour surveiller le statut des postes (pour en savoir plus, consultez le paragraphe [NAP Validator](#)).
- ◆ Cochez la case **Synchroniser l'heure** pour activer la synchronisation de l'horloge système sur la machine où tourne l'**Agent** avec celui de la machine où **Dr.Web ESS Server** est installé.
- ◆ La case cochée **Protéger le fichier système HOSTS** bloque toute modification du fichier HOSTS utilisé par le système d'exploitation pour faciliter l'accès à Internet : transformation des noms de site au format texte vers les adresses IP respectives. Une modification du fichier HOSTS peut témoigner d'une activité malveillante.
- ◆ La case cochée **Protéger les objets système critiques** bloque la modification des objets critiques du système d'exploitation (base de registre etc.).

Onglet Réseau

L'onglet **Réseau** présente les paramètres déterminant la configuration de l'interaction avec le **Serveur** :

- ◆ Dans le champ **Serveur**, spécifiez l'adresse de **Serveur Enterprise**. Vous pouvez laisser ce champ vide. Dans ce cas, l'**Agent** va utiliser comme adresse de **Serveur Enterprise** la valeur du paramètre spécifié dans la configuration de la machine locale de l'utilisateur (l'adresse du **Serveur** depuis laquelle l'installation a été effectuée).

Vous pouvez spécifier une adresse de **Serveur** ainsi que plusieurs adresses des **Serveurs** différents. Pour ajouter encore une adresse de **Serveur**, cliquez sur le bouton  et entrez



l'adresse dans le champ ajouté. Le format des adresses réseau de **Serveur** est décrit dans l'Annexe E. [Spécification de l'adresse réseau](#).

Exemple de spécification de l'adresse de **Serveur** :

tcp/10.4.0.18:2193

tcp/10.4.0.19

10.4.0.20



Si plusieurs adresses sont spécifiées côté **Agent**, les adresses des **Serveurs** sont indiquées et séparées par un espace dans le champ **Serveur** de la rubrique **Configuration** → **Connexion**, ce champ est disponible via le menu contextuel de l'icône de l'**Agent**.



Si une valeur non valide/incorrecte du paramètre **Serveur** est spécifiée, les **Agent** seront déconnectés du **Serveur** et ils ne pourront plus se connecter. Si c'est le cas, il faudra spécifier l'adresse du **Serveur** directement sur le poste.

- ◆ Dans le champ **Nombre de reprises de recherche**, spécifier une valeur déterminant le nombre de reprises de recherche de **Serveur Enterprise** si le mode [Multicasting](#) est activé.
- ◆ Dans le champ **Timeout de recherche (sec.)**, spécifiez un délai entre les tentatives de recherche de **Serveur Enterprise** en secondes, si le mode [Multicasting](#) est activé.
- ◆ Les champs **Mode de compression** et **Mode de chiffrement** permettent de spécifier les paramètres de compression et de chiffrement du trafic réseau (voir aussi [Chiffrement et compression du trafic](#)).
- ◆ Le champ **Ecouter le scan réseau** permet de spécifier le port UDP utilisé par le **Centre de Gestion** pour rechercher dans le réseau des **Enterprise Agent** actifs. Pour interdire l'écoute des ports, entrez la valeur **NONE**.

Le paramètre doit être spécifié au format d'adresse réseau décrit dans l'Annexe E. [Spécification de l'adresse réseau](#).



La valeur par défaut est **udp:2193**, ceci désigne "toutes les interfaces, port 2193".

Onglet *Mobilité*

L'onglet **Mobilité** présente les paramètres du *Mode itinérant* de l'**Agent** :

- ◆ Dans le champ **Périodicité de mise à jour (sec)**, spécifiez un délai entre les mises à jour du logiciel antivirus en secondes.
- ◆ Cochez la case **Vérifier la connexion Internet** pour activer la vérification de la connexion Internet avant le lancement de la procédure de mise à jour.
- ◆ Cochez la case **Utiliser le serveur proxy** pour utiliser le serveur proxy HTTP lors des téléchargements des mises à jour via Internet. Dans ce cas, les champs associés aux paramètres du serveur proxy utilisé seront activés.

Onglet *Rapport*

L'onglet **Rapport** permet de configurer les paramètres d'écriture dans le log de l'**Agent** :

- ◆ Le champ **Fichier de log** permet de spécifier le chemin vers le fichier de log et son nom sur la machine de l'utilisateur.
- ◆ Le paramètre **Niveau de détail du log** détermine le niveau de détail du journal (voir aussi [Ecriture dans le journal du serveur](#)).
- ◆ Cases suivantes : **Limitation du fichier de log**, **Compresser les fichiers périmés** et les champs : **Conserver au maximum <...> fichiers dont la taille est de <...>** déterminent les paramètres suivants : le nombre et la taille des fichiers de log ainsi que la nécessité de compression des fichiers périmés.
- ◆ Le paramètre **Nombre de fichiers du journal de mises à jour** détermine un nombre maximum de fichiers de log des mises à jour.



Onglet Interface

L'onglet **Interface** permet de configurer l'interface d'**Enterprise Agent**.

Dans le champ **Délai pour le mot de bienvenue**, spécifiez en délai entre le démarrage de l'interface de l'**Agent** et l'affichage du mot de bienvenue en minutes. Attribuez à ce paramètre la valeur **-1** pour annuler l'affichage du mot de bienvenue. Le mot de bienvenue est affiché sous forme d'une info bulle contenant le nom du produit **Dr.Web**, sa version et des informations sur les droits d'auteur.

L'onglet **Interface** vous permet de configurer des types de messages sur les événements à envoyer à l'utilisateur. Pour cela, cochez la case correspondante :

- ◆ **Notifications critiques** - pour ne recevoir que des notifications critiques qui comprennent les rappels périodiques sur les événements suivants :
 - sur des erreurs de mise à jour de l'antivirus ou de ses composants ;
 - sur la nécessité de redémarrer l'ordinateur après la mise à jour.

La notification sera affichée à condition que l'utilisateur dispose des droits d'administrateur.

- ◆ **Notifications virales** - pour ne recevoir que des notifications sur des virus. Ce type de notifications comprend les messages sur la détection des virus par un des composants du logiciel antivirus.
- ◆ **Notifications importantes** - pour ne recevoir que des notifications importantes. Ce type de notifications comprend les messages ci-dessous :
 - sur les erreurs lors du démarrage des composants antivirus ;
 - sur les erreurs lors des mises à jour de l'antivirus et des composants antivirus, ce type de notification s'affiche dès la fin de la procédure de mise à jour si elle a échoué ;



- sur le redémarrage requis après la mise à jour, la notification s'affiche dès que la mise à jour s'achève ;
 - sur la nécessité de patienter pendant qu'une invitation à redémarrer le poste pour terminer l'installation des composants s'affiche.
- ◆ **Notifications insignifiantes** - pour ne recevoir que des notifications insignifiantes comprenant les messages suivants :
- sur le lancement du scan à distance ;
 - sur la fin de la procédure de scan à distance ;
 - sur le lancement d'une mise à jour de l'antivirus ou des composants antivirus ;
 - sur la mise à jour réussie de l'antivirus ou des ses composants (sans nécessité de redémarrer la machine).

Si vous souhaitez que l'utilisateur puisse recevoir tous les types de messages, cochez les quatre cases. Sinon seules les notifications correspondant aux cases cochées seront affichées.



L'utilisateur peut gérer la réception des messages exceptées les **Notifications critiques**, dont la réception peut être gérée par l'administrateur seulement.

7.4. Configuration de la planification des tâches sur le poste de travail

La Planification est une liste d'actions à exécuter de manière automatique à une heure définie sur les postes de travail. La planification sert à exécuter le scan antivirus des postes durant les moments les plus opportuns pour les utilisateurs, sans nécessité de lancer manuellement le **Scanner**. De plus, **Enterprise Agent** permet d'exécuter d'autres types d'actions décrits ci-dessous.



Il existe deux types de planification :

- ◆ *Planification centralisée.* C'est une planification spécifiée par l'administrateur du réseau antivirus conformément à toutes les règles relatives à l'héritage des configurations.
- ◆ *Planification locale de poste.* C'est une planification configurée par l'utilisateur sur un poste (à condition que le poste dispose des droits nécessaires) et qui est sauvegardée de manière locale sur ce poste ; cette planification n'est pas un objet géré par le **Serveur Enterprise**.

Planification centralisée

La planification centralisée des tâches sur un poste (il en est de même pour les groupes de postes) peut être éditée depuis le **Centre de Gestion**.

Marche à suivre pour éditer la planification centralisée :

1. Pour accéder à la fenêtre d'édition de la planification, sélectionnez l'élément **Réseau antivirus** dans le menu principal du **Centre de Gestion**, puis dans la fenêtre qui apparaît, cliquez sur le nom du poste ou du groupe dans l'arborescence. Dans le menu de gestion (panneau de gauche) qui s'ouvre, sélectionnez l'élément **Planification**.
2. Vous pouvez supprimer des tâches existantes ainsi qu'ajouter de nouvelles tâches ou éditer des tâches existantes. Vous pouvez également interdire l'exécution de tâches ou autoriser l'exécution de la tâche qui a été précédemment interdite. Cette action est décrite ci-dessous.


Par défaut, la planification pour les postes tournant sous Windows ou Windows Mobile comprend 2 tâches :

- ◆ **Startup scan** - scan du poste au démarrage (autorisé),
 - ◆ **Daily scan** - scan journalier du poste (interdit).
3. A la fin de l'édition, cliquez sur le bouton **Sauvegarder** pour accepter les modifications apportées.



Si lors de l'édition, une planification vide (qui ne contient aucune tâche) est créée, le **Centre de Gestion** vous proposera soit d'utiliser la planification héritée des groupes, soit d'utiliser la planification vide. Il est nécessaire de spécifier la planification vide dans le cas où vous souhaitez refuser la planification héritée des groupes.

Marche à suivre pour ajouter une nouvelle tâche :

1. Pour créer une nouvelle tâche, cliquez sur le bouton  **Nouvelle tâche** se trouvant dans la barre d'outils du **Centre de Gestion**.



Les champs marqués par le symbole * sont obligatoires à remplir.

2. Dans l'onglet **Général**, spécifiez les paramètres suivants :
 - ◆ Entrez dans le champs **Nom** le nom de la tâche à afficher dans la planification.
 - ◆ Afin d'activer l'exécution de la tâche, cochez la case **Autoriser l'exécution**.

Si une case est décochée, la tâche figure dans la liste mais elle ne sera pas exécutée.
 - ◆ Si la case **Tâche critique** est cochée et que la tâche n'a pas été exécutée (par exemple si **Enterprise Agent** a été désactivé au moment de l'exécution de la tâche), cette tâche sera exécutée au prochain démarrage d'**Enterprise Agent**. Si durant une période la tâche n'a pas été exécutée plusieurs fois, elle sera exécutée une seule fois au prochain démarrage d'**Enterprise Agent**.



S'il est prévu que plusieurs tâches d'analyse s'exécutent avec le même scanner au démarrage du poste (**Scanner pour Windows** ou **Enterprise Scanner**), une seule tâche sera exécutée - celle qui est la première dans la file.



Par exemple, si la tâche **Startup scan** (Scan au démarrage du poste) est autorisée et qu'une tâche critique d'analyse avec **Enterprise Scanner** a été planifiée, c'est la tâche **Startup scan** qui sera exécutée au démarrage du poste, tandis que la tâche d'analyse critique ne le sera pas.

3. Dans l'onglet **Action**, sélectionnez un type de tâche depuis la liste déroulante. Une fois que votre choix est fait, la partie basse de la fenêtre varie en fonction des variantes disponibles.
 - ◆ Si le type **Démarrage** est sélectionné, entrez dans le champ **Chemin**, le nom complet (avec le chemin) du fichier exécutable à lancer, dans le champ **Arguments** - les clés de la ligne de commande relatives au programme à lancer.
 - ◆ Si le type **Dr.Web Scanner pour Windows** ou **Dr.Web Enterprise Scanner pour Windows** est sélectionné, la fenêtre de configuration de l'analyse va s'ouvrir. Vous pouvez consulter sa description dans le paragraphe [Lancement et arrêt du Scanner antivirus sur le poste](#).
 - ◆ Si le type **Journalisation** est sélectionné, entrez dans le champ **Ligne**, le texte du message à mettre dans le journal.
4. L'onglet **Heure** vous permet de configurer l'heure de lancement de la tâche.

Pour cela, sélectionnez en premier lieu, dans la liste déroulante **Périodicité**, un mode de lancement :

- ◆ Tous les jours,
- ◆ Chaque mois,
- ◆ Chaque semaine,
- ◆ Toutes les heures,
- ◆ Chaque X minutes,
- ◆ Au démarrage.

Vous pouvez consulter la description des paramètres relatifs à chaque mode dans le [tableau 7-2](#).

5. A la fin de l'entrée des paramètres, cliquez sur le bouton **Sauvegarder**.



Tableau 7-2. Mode de lancement et paramètres respectifs

Mode de lancement	Paramètres et description
Tous les jours	Il faut entrer l'heure et les minutes — la tâche sera lancée tous les jours à l'heure spécifiée.
Chaque mois	Il faut sélectionner la date (le jour du mois) et entrer l'heure et les minutes — la tâche sera lancée chaque mois au jour et à l'heure spécifiés.
Chaque semaine	Il faut sélectionner le jour de la semaine, entrer l'heure et les minutes — la tâche sera lancée chaque semaine au jour et à l'heure spécifiés.
Toutes les heures	Il faut entrer un nombre entre 0 et 59 déterminant la minute à laquelle la tâche sera lancée toutes les heures.
Chaque X minutes	Il faut entrer une valeur X . En cas de X égale à 60 ou supérieur, la tâche sera lancée toutes les X minutes. En cas de X inférieur à 60, la tâche sera lancée toutes les heures, chaque X minute.
Au démarrage	Aucun paramètre supplémentaire n'est requis. La tâche sera lancée au démarrage de l' Agent .

Pour éditer la tâche existante : sélectionnez la tâche dans la liste en cliquant dessus. Les actions suivantes s'effectuent de manière analogue à la création d'une nouvelle tâche (décrite ci-dessus).

Pour supprimer une tâche :

1. Cochez la case contre la tâche à supprimer.
2. Cliquez sur le bouton  **Supprimer les configurations** dans la barre d'outils du **Centre de Gestion**.

Planification locale

Marche à suivre pour éditer la planification locale du poste de travail :

1. Depuis le menu contextuel de l'**Agent**, dans l'élément **Planification**, sélectionnez la variante **Locale**.



2. La fenêtre d'édition de la planification locale d'**Enterprise Agent** va s'ouvrir.



Dans le menu contextuel de l'**Agent**, dans l'élément **Planification**, la variante **Locale** sera disponible à condition que lors de l'édition des droits du poste antivirus, la case **Création d'une planification locale** soit cochée.

A l'aide de la planification locale, l'utilisateur peut lancer le scan en utilisant des paramètres. Pour en savoir plus sur les moyens de spécifier des objets à scanner, sur les clés en ligne de commande déterminant les paramètres du programme ainsi que sur les paramètres de la ligne de commande relatifs au **Scanner**, consultez le manuel **Dr.Web® Antivirus pour Windows. Manuel Utilisateur**.

3. A la fin de l'édition, cliquez sur le bouton **OK**.



En cas d'installation du poste par défaut, sans aucune intervention de l'administrateur, le moniteur antivirus sera actif et les tâches de mises à jour et de scan antivirus seront lancées périodiquement.

7.5. Scan antivirus du poste de travail



L'utilisateur du poste peut effectuer lui-même le scan antivirus avec le composant **Dr.Web Scanner pour Windows**. L'icône permettant de lancer ce composant est placée sur le bureau lors de l'installation du logiciel antivirus. Le lancement et le fonctionnement du **Scanner** sont possibles même en cas d'**Agent** inactif, y compris le démarrage du système d'exploitation Windows en mode sans échec.



Pour chaque poste vous pouvez réaliser les opérations suivantes :

- ◆ Consulter la liste de tous les composants antivirus en cours d'exécution au moment spécifié.
- ◆ Interrompre des composants en cours selon leur type.
- ◆ Lancer des tâches de scan antivirus et paramétrer la procédure de scan. Les procédures de scan peuvent être lancées pour :
 - **Dr.Web Scanner pour Windows,**
 - **Dr.Web Enterprise Scanner pour Windows,**
 - **Dr.Web Enterprise Scanner pour Unix,**
 - **Dr.Web Enterprise Scanner pour Mac OS X.**

7.5.1. Consultation et interruption des composants en cours

Pour consulter la liste et interrompre le fonctionnement des composants lancés, procédez comme suit :

1. Sélectionnez l'élément **Réseau antivirus** du menu principal du **Centre de Gestion**, puis dans la fenêtre qui apparaît, cliquez sur le nom du poste ou du groupe dans l'arborescence. Dans le menu de gestion (panneau de gauche) qui s'ouvre, sélectionnez l'élément **Composants en cours d'exécution**.

La liste des composants actifs lancés de manière manuelle par vous-même ou par un utilisateur ou lancés selon la planification va s'afficher.

2. Pour arrêter un composant, cochez la case contre le composant, puis dans la barre d'outils, cliquez sur le bouton **Arrêter**. Le composant sera arrêté et enlevé de la liste.



7.5.2. Interruption des composants en cours selon leur type



En cas d'utilisation de cette option, le processus de scan et les moniteurs en cours seront stoppés excepté **SpIDer Guard**.



Attention ! Les moniteurs **SpIDer Mail** et **SpIDer Gate** ne peuvent pas être lancés depuis le **Centre de Gestion**.

Vous pouvez arrêter les composants tournant sur le poste qui ont été lancés de la manière suivante :

- ◆ ceux que vous avez lancés manuellement,
- ◆ ceux lancés par l'utilisateur,
- ◆ ceux lancés selon la planification.

Vous pouvez également arrêter tous les composants qui sont en cours d'exécution à la fois, selon un critère défini. Cela peut être utile si une commande est envoyée à plusieurs postes en même temps.


Marche à suivre pour interrompre tous les composants en cours d'exécution en fonction du type spécifié :

1. Sélectionnez l'élément **Réseau antivirus** du menu principal du **Centre de Gestion**, puis dans la fenêtre qui apparaît, sélectionnez le groupe ou les postes dans l'arborescence.
2. Dans la barre d'outils, cliquez sur le bouton  **Gestion des composants**. Dans la liste déroulante qui s'affiche, sélectionnez l'élément  **Interrompre des composants lancés**. La fenêtre de configuration des types de composants à interrompre va s'ouvrir.
3. Cochez les cases contre les types de composants à interrompre immédiatement ou contre l'en-tête de la rubrique **Interrompre les processus de scan** - pour sélectionner tous les processus dans la liste.
4. Cliquez sur le bouton **Interrompre**.



7.5.3. Lancement de scan sur le poste

Marche à suivre pour lancer une tâche de scan :

1. Sélectionnez l'élément **Réseau antivirus** du menu principal du **Centre de Gestion**.
2. Dans la fenêtre qui apparaît, cliquez sur le nom du poste ou du groupe dans l'arborescence.
3. Depuis la barre d'outils cliquez sur l'élément  **Scan**.
4. Dans la liste qui sera ouverte, depuis la barre d'outils sélectionnez un mode de scan :



Dr.Web Scanner pour Windows. Analyse rapide. Ce mode assure le scan des objets suivants :

- ◆ mémoire vive,
- ◆ secteurs de démarrage de tous les disques,
- ◆ objets d'autodémarrage,
- ◆ répertoire racine du disque boot,
- ◆ répertoire racine du disque d'installation Windows,
- ◆ répertoire système Windows,
- ◆ dossier Mes Documents,
- ◆ répertoire système temporaire,
- ◆ répertoire utilisateur temporaire.

Si cette option est sélectionnée, l'analyse antivirus avec les paramètres du **Scanner** par défaut sera lancée.



Dr.Web Scanner pour Windows. Analyse complète. Ce mode assure une analyse complète de tous les disques durs et des supports amovibles (y compris les secteurs de démarrage). Si cette option est sélectionnée, l'analyse antivirus avec les paramètres du **Scanner** par défaut sera lancée.



Dr.Web Scanner pour Windows. Analyse sélective. Ce mode assure une possibilité de sélectionner des dossiers et des fichiers à analyser. Si cette option est sélectionnée, la fenêtre de



configuration du **Scanner** va s'ouvrir. Spécifiez les paramètres de scan ainsi que les éléments à scanner (la procédure est décrite ci-dessous), cliquez ensuite sur **Scan antivirus**.



Dr.Web Enterprise Scanner pour Windows. Ce mode assure une analyse sélective avec **Dr.Web Enterprise Scanner**. Si cette option est sélectionnée, la fenêtre de configuration du **Scanner** va s'ouvrir. Spécifiez les paramètres de scan ainsi que les éléments à scanner (la procédure est décrite ci-dessous), cliquez ensuite sur **Scan antivirus**.



Dr.Web Enterprise Scanner pour Unix destiné à scanner les postes tournant sous l'OS de la famille UNIX. Spécifiez les paramètres de scan ainsi que les éléments à scanner et cliquez ensuite sur **Scan antivirus**.





Dr.Web Enterprise Scanner pour Mac OS X destiné à scanner les postes tournant sous l'OS de la famille Mac OS X. Spécifiez les paramètres de scan ainsi que les éléments à scanner et cliquez ensuite sur **Scan antivirus**.



7.5.4. Configuration du Scanner pour OS Windows

Il existe plusieurs moyens pour consulter et éditer les paramètres du Scanner :

1. Sélectionnez l'élément **Réseau antivirus** du menu principal du **Centre de Gestion**, dans la fenêtre qui apparaît, cliquez sur le nom du poste ou du groupe dans l'arborescence. Dans le menu de gestion (panneau de gauche), sélectionnez l'élément **Dr.Web Scanner pour Windows**. La fenêtre de configuration du **Scanner** va s'ouvrir. La liste des paramètres affichés est la plus complète et comprend tous les groupes de paramètres décrits ci-dessous.
2. Sélectionnez l'élément **Réseau antivirus** du menu principal du **Centre de Gestion**, dans la fenêtre qui apparaît, cliquez sur le nom du poste ou du groupe dans l'arborescence. Dans le



menu de gestion, cliquez sur l'élément  **Scan**. Dans la liste qui s'affichera sur la barre d'outils, sélectionnez l'élément  **Dr.Web Scanner pour Windows. Analyse sélective**. Le panneau se trouvant à droite vous ouvrira la fenêtre de configuration du **Scanner**. La liste des paramètres affichés est abrégée et ne permet que de configurer les paramètres basiques faisant partie des groupes de paramètres tels que **Général, Actions, Rapport et Divers**.

3. Sélectionnez l'élément **Réseau antivirus** du menu principal du **Centre de Gestion**, dans la fenêtre qui apparaît, cliquez sur le nom du poste ou du groupe dans l'arborescence. Dans le menu de gestion, cliquez sur l'élément  **Scan**. Dans la liste qui s'affichera sur la barre d'outils, sélectionnez l'élément  **Dr.Web Enterprise Scanner pour Windows**. Le panneau se trouvant à droite vous ouvrira la fenêtre de configuration du **Scanner**. Cette liste des paramètres ne permet que de spécifier des paramètres principaux pour **Enterprise Scanner** faisant partie des groupes de paramètres tels que **Général, Actions et Chemins exclus**.

Général

- ◆ La case **Analyse heuristique** est cochée par défaut ; dans ce cas le **Scanner** tente de détecter des virus inconnus avec le moteur heuristique. Ce mode n'exclut pas des fausses alertes du **Scanner**.
- ◆ La case **Scan des archives** est cochée par défaut. Dans ce cas, le **Scanner** cherche des virus dans les fichiers archivés.
- ◆ La case **Scan des fichiers email** est cochée par défaut et active le scan des Boîtes aux lettres.
- ◆ La case **Scan des applications et modules en cours d'exécution (Scan dans la mémoire** en cas d'**Enterprise Scanner**) est cochée par défaut. Ceci active le scan des processus lancés dans la mémoire vive.
- ◆ La case **Scan des programmes lancés automatiquement** est cochée par défaut. Ceci active le scan des fichiers lancés de manière automatique au démarrage du système d'exploitation.
- ◆ La case **Scan des secteurs boot** est cochée par défaut. Dans



ce cas, le **Scanner** effectue l'analyse des secteurs boot. Les secteurs boot des disques logiques seront scannés ainsi que les secteurs principaux boot sur les disques physiques.

- ◆ La case **Scan des sous-répertoires** (absente si **Enterprise Scanner**) est cochée par défaut. L'option est utilisée lors du paramétrage des chemins à scanner et commande au **Scanner** de vérifier non seulement les fichiers mais aussi les sous-dossier emboîtés correspondant au chemin spécifié.

Lors du paramétrage du Scanner via l'élément du menu de gestion (panneau de gauche) Dr.Web Scanner pour Windows, les paramètres suivants sont disponibles :

- ◆ La case **Protéger le fichier HOSTS** active la vérification du fichier système HOSTS utilisé par le système afin de faciliter l'accès à Internet : pour transformer les noms de certains sites au format texte vers les adresses IP correspondantes. Une modification du fichier HOSTS peut témoigner de l'activité de programmes malveillants.
- ◆ L'élément **Scanner** détermine le mode de scan. Dans la liste déroulante, sélectionnez une des variantes suivantes :
 - **Tous les fichiers** - pour scanner tous les fichiers quels que soient leurs noms et extensions.
 - **Par masque** - pour ne scanner que les fichiers dont les noms et extensions sont mentionnés dans la liste paramétrée à la rubrique **Liste des masques**.
 - **Types sélectionnés** - pour scanner uniquement les fichiers dont les extensions font partie de la liste paramétrée à la rubrique **Liste des extensions**.
- ◆ La case cochée **Demande de confirmation** active l'envoi aux utilisateurs des notifications sur les événements ainsi que des notifications invitant à confirmer les actions du **Scanner**.
- ◆ La case **Requête pour le scan d'une disquette suivante** est utilisée lors de l'analyse des supports amovibles (lecteurs de type CD/DVD, lecteurs flash) et active l'envoi d'une requête à l'utilisateur pour confirmer la connexion puis l'analyse d'un support amovible.



Lors du paramétrage du Scanner lancé depuis la barre d'outils, sélectionnez une des deux variantes disponibles :

1. Scanner tous les disques.

pour **Enterprise Scanner** spécifiez les disques à analyser :

- ◆ cochez la case **Disques durs internes** pour analyser les disques durs internes ;
- ◆ cochez la case **Disques amovibles** pour vérifier tous les supports amovibles tels que lecteurs de disques CD/DVD, lecteurs flash etc. ;

Ce mode vous permet également de spécifier une liste de **Chemins exclus** (dont la procédure de configuration est décrite ci-dessous).

2. Scanner les chemins spécifiés.

Spécifiez une liste de chemins à vérifier (la procédure de configuration est décrite ci-dessous) ;

Enterprise Scanner pour Windows propose les options suivantes à cocher :

- ◆ **Technologie BurstScan** : active l'utilisation de cette technologie permettant d'accélérer considérablement le processus de scan sur les systèmes modernes équipés de processeurs multicœurs.
- ◆ Etant cochée par défaut, la case **Scan en basse priorité** permet de diminuer la charge système liée au fonctionnement du **Scanner**. Dans ce cas, d'autres processus peuvent avoir une priorité d'exécution plus élevée que si la case décochée. Ceci est assuré par le changement dynamique des priorités des flux d'analyse.
- ◆ Si la case **Scan des conteneurs** est cochée, le **Scanner** vérifie les conteneurs de fichier de divers types.
- ◆ La liste **Actions effectuées après le scan** assure l'exécution automatique d'une action immédiatement après la fin du processus de scan : éteindre, redémarrer, mettre en mode sélectionné ou ne rien faire sur la machine de l'utilisateur.



- ◆ La case **Bloquer le réseau durant le scan** permet de déconnecter l'ordinateur du réseau local ainsi que d'Internet durant l'analyse.

La rubrique **Limitations** offre les paramètres suivants :

- ◆ **Durée maximum d'analyse d'un fichier** - la durée maximum en millisecondes, durant laquelle le fichier peut être traité. A l'expiration de ce délai, la vérification de l'objet sera arrêtée.
- ◆ **Niveau maximum d'emboîtement des archives** - si le niveau d'emboîtement est supérieur à la valeur spécifiée, l'analyse ne sera effectuée que jusqu'au niveau correspondant à cette valeur.
- ◆ **Taille maximum de l'archive** - si la taille de l'archive est supérieure à la valeur spécifiée, l'extraction de l'archive et son analyse ne seront pas effectuées.
- ◆ **Ratio maximum de compression** - si le **Scanner** détermine que le ratio de compression est supérieur à la valeur spécifiée, l'extraction de l'archive et son analyse ne seront pas effectuées.
- ◆ **Taille maximum des fichiers extraits (Ko)** - si le **Scanner** détermine que la taille de l'archive après l'extraction est supérieure à la valeur spécifiée (en Ko), l'extraction de l'archive et son analyse ne seront pas effectuées.
- ◆ **Seuil de contrôle de la compression** - taille minimum du fichier archivé à partir de laquelle la vérification du ratio de compression sera effectuée.

Actions

La rubrique des paramètres **Actions** permet de configurer une réaction de l'**Antivirus** en cas de détection de fichiers infectés ou suspects, de programmes malveillants ou d'archives infectées.

Les actions suivantes sont disponibles à appliquer aux objets détectés :

- ◆ **Réparer** - réparer l'objet afin de rétablir son état antérieur à la contamination. Si la désinfection est impossible, une réaction pour les objets incurables sera appliquée.



Cette action ne peut être appliquée qu'aux objets infectés par un virus connu et curable, excepté les trojans et les fichiers contaminés se trouvant dans les objets complexes (archives, fichiers email ou conteneurs de fichiers).

- ◆ **Supprimer** - supprimer les objets infectés.
- ◆ **En Quarantaine** - déplacer les objets infectés vers le dossier de **Quarantaine**.
- ◆ **Renommer** - renommer les objets infectés selon la règle définie dans le champ **Template pour renommer les fichiers**.
- ◆ **Notifier** - envoyer une alerte sur la détection d'un virus (pour en savoir plus sur la configuration des notifications, merci de consulter le paragraphe [Configuration des notifications](#)).
- ◆ **Ignorer** - laisser passer l'objet sans aucune action appliquée ni notification affichée.

Tableau 7-3. Les réaction du Scanner applicables aux objets malicieux

Action	Objet				
	Adwares	Conteneurs infectés	Infectés	Suspects	Incurables
Réparer			+/*		
Supprimer	+	+	+	+	+
En quarantaine	+	+/*	+	+	+/*
Renommer	+	+	+	+	+
Notifier	+/*	+	+	+/*	+
Ignorer	+				

Légende

- + l'action est autorisée pour ce type d'objets
- +/* l'action est spécifiée comme réaction par défaut à appliquer à certains types d'objets



Les paramètres ci-dessous permettent de configurer les actions à appliquer aux objets malveillants détectés :

- ◆ Dans le champ **Template pour renommer les fichiers**, spécifiez le masque de l'extension à attribuer aux objets renommés si l'action **Renommer** a été spécifiée pour ce type d'objets détectés. Par défaut, la variante #?? sera proposée, le premier symbole sera remplacé par le symbole #. Ce masque peut être modifié, cependant, il ne faut pas utiliser les extensions standard pour une variante de remplacement (EXE, COM, BAT, DOC, PAS, BAS etc.).
- ◆ La liste déroulante **Adwares** permet de spécifier une réaction du **Scanner** en cas de détection des adwares.



Si la réaction **Ignorer** est spécifiée pour les adwares détectés, aucune action ne sera effectuée : l'utilisateur ne sera pas notifié en cas de détection d'un objet, comme par exemple il l'est si l'option **Notifier** est activée.

- ◆ La réaction du **Scanner** en cas de détection des objets indésirables listés ci-dessous peut être configurée de manière analogue à la configuration de la réaction en cas d'adwares :
 - dialers payants ;
 - canulars ;
 - riskwares ;
 - hacktools.
- ◆ La liste déroulante **Redémarrage** permet de spécifier un mode de redémarrage de l'ordinateur après la fin du processus de scan.
- ◆ La liste déroulante **Conteneurs infectés** permet de spécifier une réaction du **Scanner** en cas de détection d'un objet infecté ou suspect faisant partie d'une archive ou d'un conteneur. La réaction sera appliquée à l'archive entière.
- ◆ La liste déroulante **Infectés** permet de spécifier une réaction du **Scanner** en cas de détection d'un fichier contaminé par un virus connu.



- ◆ La liste déroulante **Suspects** permet de spécifier une réaction du **Scanner** en cas de détection d'un fichier probablement infecté par un virus (réaction du moteur heuristique).





En cas de scan prenant en compte le répertoire d'installation du système d'exploitation, il est recommandé de choisir la réaction **Notifier** pour les objets suspects.

- ◆ La liste déroulante **Incurable** permet de configurer une réaction du **Scanner** en cas de détection d'un fichier infecté par un virus connu mais irréparable (ainsi que dans le cas où la tentative de désinfection a échoué).
- ◆ La case cochée **Permettre la suppression des archives** permet de supprimer les archives infectées détectées ainsi que les fichiers email. Si la case est cochée, les éléments **Archives infectées** et **Fichiers email infectés**, comprennent en option l'action **Supprimer**. Si la case est décochée, seules les variantes **En quarantaine** (applicable aux archives par défaut), **Renommer** et **Notifier** (applicable aux fichiers email par défaut) seront disponibles.

Les chemins et fichiers à exclure

Pour éditer les listes des chemins et fichiers exclus, procédez comme suit :

- ◆ Entrez un chemin ou un fichier dans la ligne **Chemins exclus** ou **Fichiers exclus**.
- ◆ Pour ajouter une nouvelle ligne dans la liste, cliquez sur le bouton  et entrez le chemin dans la ligne qui apparaît.
- ◆ Pour supprimer l'élément dans la liste, cliquez sur le bouton  contre la ligne correspondante.

La liste des objets exclus peut contenir les éléments suivants :

1. Le chemin vers l'objet à exclure spécifié de manière explicite, avec :



- ◆ Les symboles \ ou / – désignent l'exclusion de l'analyse de tout le disque sur lequel se trouve le répertoire d'installation de Windows,
- ◆ Un chemin qui se termine avec le symbole \ – tout le répertoire sera exclu de l'analyse,
- ◆ Un chemin qui ne se termine pas avec le symbole \ – tout sous-dossier dont le chemin commence par la ligne spécifiée sera exclu de l'analyse s'il ne se termine par pas le symbole \.

Par exemple : `C:\Windows` - ne pas vérifier les fichiers se trouvant dans le répertoire `C:\Windows` ni dans tous ses sous-répertoires.

2. Les masques des objets à exclure de l'analyse. Pour spécifier les masques, les symboles ? et * peuvent être utilisés.

Par exemple : `C:\Windows**.dll` - ne pas vérifier tous les fichiers ayant l'extension `dll` et se trouvant dans tous les sous-répertoires du répertoire `C:\Windows`.

3. L'expression régulière. Les chemins peuvent être spécifiés avec des expressions régulières. A part cela, tout fichier dont le nom complet (avec le chemin) correspond à une expression régulière sera exclu de l'analyse.



Avant de commencer le processus de scan antivirus, merci de prendre connaissance des recommandations sur l'utilisation des logiciels antivirus pour les ordinateurs tournant sous Windows Server 2003, Windows 2000 et Windows XP. Vous pouvez consulter l'article dédié à l'adresse suivante - <http://support.microsoft.com/kb/822158/ru>. Cet article vous permettra d'optimiser les performances système.

La syntaxe des expressions régulières utilisées pour spécifier les chemins exclus est la suivante :

`qr{expression}paramètres`

Le paramètre le plus fréquemment utilisé est le symbole `i`, ce paramètre désigne "ne pas prendre en compte la casse".



Exemples des chemins et fichiers exclus spécifiés avec les expressions régulières :

- ◆ `qr{\\pagefile\\.sys$}i` — ne pas vérifier les fichiers swap de Windows NT,
- ◆ `qr{\\notepad\\.exe$}i` — ne pas vérifier les fichiers notepad.exe,
- ◆ `qr{^C:}i` — ne rien vérifier sur le disque C,
- ◆ `qr{^.:\\WINNT\\}i` — ne rien vérifier dans les dossiers WINNT sur tous les disques,
- ◆ `qr{(^C:)|(^.:\\WINNT\\)}i` — deux derniers cas réunis,
- ◆ `qr{^C:\\dir1\\dir2\\file\\.ext$}i` — ne pas vérifier le fichier `c:\dir1\dir2\file.ext`,
- ◆ `qr{^C:\\dir1\\dir2\\(.+\\)?file\\.ext$}i` — ne pas vérifier le fichier `file.ext` s'il se trouve dans le dossier `c:\dir1\dir2` ou dans ses sous-dossiers,
- ◆ `qr{^C:\\dir1\\dir2\\}i` — ne pas vérifier le dossier `c:\dir1\dir2` ni ses sous-dossiers,
- ◆ `qr{dir\\[^\\]+}i` — ne pas vérifier le sous-dossier `dir` se trouvant dans n'importe quel dossier, mais vérifier les sous-dossiers,
- ◆ `qr{dir\\}i` — ne pas vérifier le sous-dossier `dir` se trouvant dans n'importe quel dossier, ni ses sous-dossiers.

Pour en savoir plus sur l'utilisation des expressions régulières, merci de consulter [Annexe K](#).



Vous trouverez les liens vers les descriptions détaillées de la syntaxe des expressions régulières dans la rubrique [Liens](#).


Liste des extensions (en cas de consultation des configurations depuis le menu de gestion)

La rubrique **Liste des extensions** n'est activée que si la variante **Types sélectionnés** est spécifiée dans la rubrique **Général**, dans





l'élément **Scan**. Dans ce cas, seuls les fichiers dont les extensions sont mentionnées dans la liste seront scannés.


Pour modifier la liste des extensions, utilisez le bouton  pour ajouter de nouveaux éléments dans la liste ou le bouton  - pour supprimer des éléments existants.

Les symboles * et ? peuvent être utilisés dans les éléments de la liste. Par défaut, la liste des extensions des fichiers exécutables ou archivés sera sauvegardée. Afin de rétablir l'état de la liste spécifié par défaut, cliquez sur le bouton .

Liste des masques (en cas de consultation des configurations depuis le menu de gestion)

La rubrique **Liste des masques** n'est activée que si la variante **Par masque** est spécifiée dans la rubrique **Général**, dans l'élément **Scan**. Dans ce cas, seuls les fichiers dont les noms et extensions sont listés seront scannés.

Pour modifier la liste des masques, utilisez le bouton  pour ajouter de nouveaux éléments dans la liste ou le bouton  - pour supprimer des éléments existants.

Les symboles * et ? peuvent être utilisés dans les éléments de la liste. Par défaut, la liste des extensions des fichiers exécutables ou archivés sera sauvegardée. Afin de rétablir l'état de la liste spécifié par défaut, cliquez sur le bouton .

Divers (excepté Enterprise Scanner)

La rubrique **Divers** vous permet d'accéder aux paramètres avancés du **Scanner** :



- ◆ Si la case **Utiliser le disque pour la création d'un fichier dump** est cochée, le disque dur sera utilisé pour créer un fichier swap afin d'éviter un manque de mémoire vive, utilisée par le **Scanner** lors de la vérification de grands volumes de données (archives volumineuses etc.).
- ◆ La case cochée **Récupérer la date d'accès** active la restauration de la date de la dernière consultation du fichier après le processus de scan (la date sera remplacée par celle d'avant l'analyse).
- ◆ La case cochée **Sauvegarder les configurations automatiquement** active la sauvegarde automatique de la configuration du **Scanner** après la fin de la session.
- ◆ Le champ **Priorité de scan** permet de spécifier une priorité des flux du processus de scan. Vous pouvez sélectionner une des priorités ci-dessous :
 - **suspendue** - il n'est pas recommandé de spécifier ce niveau de priorité afin d'éviter un ralentissement du fonctionnement du **Scanner** et par suite une augmentation importante de la durée d'analyse.
 - **inférieure.**
 - **inférieure à la standard.**
 - **standard.** Ce niveau de priorité est recommandé.
 - **supérieure à la standard.**
 - **supérieure.**
 - **critique en termes de temps.** Il n'est pas recommandé de spécifier ce niveau de priorité afin d'éviter une surcharge système due au fonctionnement du **Scanner** lors de la procédure de scan.

Rapport

La rubrique **Rapport** vous permet de configurer la journalisation du fonctionnement du **Scanner**. Pour cela, cochez la case **Ecrire le log dans un fichier** et spécifiez les paramètres de journalisation.



Sons (en cas de consultation des configurations depuis le menu de gestion)

La rubrique **Sons** vous offre une possibilité de configurer les sons associés à certains types d'événements. Pour cela, cochez la case **Activer les sons** et spécifiez les noms des fichiers sonores dans les champs correspondants aux événements correspondants.

7.6. Consultation des résultats et des statistiques récapitulatives sur un poste

Le menu de gestion de la rubrique **Réseau antivirus** vous permet de consulter les informations suivantes :

- ◆ **Tableaux** - pour consulter les statistiques relatives au fonctionnement des outils antivirus sur le poste ainsi que les informations sur le statut des postes et des logiciels antivirus.
- ◆ **Graphiques** - pour consulter les graphiques affichant des informations sur les infections détectées sur les postes.
- ◆ **Tableau récapitulatif** - pour consulter et sauvegarder les rapports contenant des données statistiques récapitulatives ou des extraits de tableaux spécifiques. Cet élément n'est pas affiché dans le menu si tous les autres éléments de la rubrique **Tableaux** sont masqués.
- ◆ **Quarantaine** - pour consulter et éditer à distance le contenu de la **Quarantaine**.

7.6.1. Tableaux

Pour consulter les tableaux :

1. Sélectionnez l'élément **Réseau antivirus** dans le menu principal du **Centre de Gestion**, puis dans la fenêtre qui apparaît, cliquez sur le nom du poste ou du groupe dans l'arborescence.



2. Dans le menu de gestion (panneau de gauche), sélectionnez un élément dont vous avez besoin depuis la rubrique **Tableaux**.

La rubrique **Tableaux** comprend les éléments suivants :

- ◆ **Tableau récapitulatif** - pour consulter et sauvegarder les rapports contenant toutes les données statistiques sommaires ou les données de synthèse sélectives selon les extraits de tableaux spécifiés. Cet élément ne s'affiche pas dans le menu si tous les autres éléments sont masqués (voir [Tableau récapitulatif](#)).
- ◆ **Infections** - pour consulter les informations sur la détection des virus (liste des objets infectés, virus, actions réalisées par l'antivirus etc.).
- ◆ **Erreurs** - pour consulter la liste des erreurs de scan sur un poste sélectionné pour une période choisie.
- ◆ **Statistiques** - pour obtenir des statistiques sur le fonctionnement des outils antivirus sur le poste (voir [Statistiques](#)).
- ◆ **Démarrage/Arrêt** - pour consulter la liste des composants lancés sur le poste.
- ◆ **Virus** - pour consulter les informations sur la détection des virus sur le poste, triées selon les types de virus.
- ◆ **Statut** - pour consulter les informations sur un statut non-standard des postes (et éventuellement nécessitant une intervention) durant une période spécifiée (voir [Statut](#)).
- ◆ **Tâches** - pour consulter la liste des tâches spécifiées pour le poste durant une période donnée.
- ◆ **Statistiques sommaires** - pour obtenir des statistiques sommaires (non par session).
- ◆ **Bases virales** - pour consulter les informations sur les bases virales installées : nom du fichier contenant la base virale, version de la base virale; total d'entrées dans la base; date de création de la base. Cet élément n'est accessible qu'à condition que le poste soit sélectionné.
- ◆ **Modules** - pour consulter les informations détaillées sur tous les modules de l'antivirus **Dr.Web** : description du module - son nom fonctionnel ; fichiers correspondant à des modules du produit ; la version complète du module etc. Cet élément n'est accessible qu'à condition que le poste soit sélectionné.



- ◆ **Toutes les installations via réseau** - pour consulter la liste des installations du logiciel sur le poste de travail.



Pour afficher les éléments masqués de la rubrique **Tableaux**, sélectionnez l'élément **Administration** du menu principal, puis dans la fenêtre qui apparaît, sélectionnez l'élément du menu de gestion **Configuration de Dr.Web Enterprise Server**. Dans l'onglet **Données statistiques**, cochez les cases respectives (voir ci-dessous), cliquez ensuite sur **Sauvegarder** et redémarrez le **Serveur**.

Tableau 7-4. Correspondance entre les éléments de la rubrique Tableaux et les cases de la rubrique Données statistiques

Eléments de la rubrique Tableaux	Cases de la rubrique Données statistiques
Infections	Infections dans la BD
Erreurs	Erreurs de scan dans la BD
Statistiques	Statistiques de scan dans la BD
Démarrage/Arrêt	Informations sur le démarrage/arrêt des composants dans la BD
Virus	Infections dans la BD
Statut	Surveillance des statuts des postes
Tâches	Log d'exécution des tâches
Statistiques sommaires	Statistiques de scan dans la BD
Bases virales	Surveillance des statuts des postes Surveillance des bases virales Log d'exécution des tâches
Modules	Liste des modules de poste dans la BD
Toutes les installations via réseau	Informations sur les installations dans la BD

Les fenêtres affichant les résultats du fonctionnement des composants divers ainsi que des statistiques sommaires ont la même interface et les actions permettant d'entrer dans les détails de chaque fenêtre sont



analogues.

Vous trouverez ci-après quelques exemples de consultation des statistiques sommaires via le **Centre de Gestion**.

Statistiques

Marche à suivre pour obtenir des statistiques sur le fonctionnement des outils antivirus sur le poste :

1. Sélectionnez le poste nécessaire dans l'arborescence.



Pour consulter les statistiques relatives aux postes ou groupes, vous pouvez les sélectionner à l'aide des touches SHIFT ou CTRL.

2. Dans le menu de gestion (panneau de gauche) depuis la rubrique **Tableaux**, sélectionnez l'élément **Statistiques**.
3. Par défaut, les statistiques relatives aux dernières vingt-quatre heures s'affichent.
4. Pour consulter les informations relatives à une période donnée, vous pouvez sélectionner depuis la liste déroulante une période par rapport à la date courante ou choisir depuis la barre d'outils une plage de dates nécessaire. Pour spécifier une plage de dates, saisissez les dates correspondantes ou cliquez sur l'image représentant un calendrier contre le champ de date. Pour télécharger des données, cliquez sur **Actualiser**. Les tableaux statistiques seront téléchargés.
5. La rubrique **Statistiques générales** permet d'accéder aux données sommaires :
 - ◆ en cas de sélection des postes - par postes sélectionnés ;
 - ◆ en cas de sélection des groupes - par groupes sélectionnés. Si plusieurs groupes sont sélectionnés, seuls les groupes contenant des postes seront affichés ;
 - ◆ en cas de sélection des groupes et des postes à la fois - séparément par tous les postes y compris les postes faisant partie des groupes sélectionnés (qui ne sont pas vides).



- Afin de consulter les statistiques détaillées sur le fonctionnement des outils antivirus, cliquez sur le nom du poste dans le tableau. Si vous sélectionnez des groupes, cliquez sur le nom du groupe dans le tableau des statistiques générales puis cliquez sur le nom du poste. La fenêtre (ou une rubrique de la fenêtre active) contenant le tableau avec les données détaillées va s'ouvrir.
- Depuis le tableau contenant des statistiques sur le fonctionnement des outils antivirus du poste ou du groupe, vous pouvez accéder à la fenêtre de configuration des composants antivirus. Pour cela, cliquez sur le nom du composant dans le tableau statistiques.
- Pour effectuer un tri des données contenues dans une colonne du tableau, cliquez sur la flèche correspondante (afin de trier par ordre croissant ou décroissant) dans l'en-tête respectif.
- Afin de sauvegarder un tableau de statistiques pour l'imprimer ou le traiter ultérieurement, cliquez sur le bouton  ou le bouton 
Sauvegarder les données vers un fichier CSV, ou sur 
Sauvegarder les données vers un fichier HTML ou bien sur le bouton  **Sauvegarder les données vers un fichier XML**.
- Pour consulter les statistiques sommaires sans marquer les sessions, cliquez sur l'élément **Statistiques sommaires** dans le menu de gestion.
- Pour consulter les statistiques sommaires triées par événements viraux sous forme de graphiques, dans le menu de gestion (panneau de gauche), sélectionnez l'élément **Graphiques** (pour en savoir plus, consultez les informations [ci-dessous](#)).

Statut

Marche à suivre pour consulter les informations sur un statut non-standard des postes relatif à une période donnée et nécessitant éventuellement une intervention :

- Sélectionnez l'élément **Statut** dans le menu de gestion depuis la rubrique **Tableaux**.



2. Des informations sur le statut des postes sont affichées dans la fenêtre de manière automatique selon les paramètres spécifiés dans la barre d'outils.
3. Pour limiter la liste des notifications sur le statut de sorte que seuls les messages d'une certaine importance soient affichés, sélectionnez le niveau d'importance dans la liste déroulante **Importance** sur la barre d'outils. Par défaut, le niveau **Très basse** est spécifié. Cela correspond à l'affichage de la liste exhaustive.
4. La liste comprend également les poste non vus sur le **Serveur** durant une période spécifiée. Entrez une valeur correspondante au nombre de jours dans le champ se trouvant à gauche de la liste **Importance**. Si le nombre de jours est supérieur à la valeur spécifiée, la situation sera classée comme critique et les informations associées seront affichées dans la fenêtre de la rubrique **Statut**.
5. La marche à suivre pour obtenir un niveau de détail particulier du tableau ou pour formater le tableau est analogue à celle décrite ci-dessus pour le tableau de statistiques.



Vous pouvez également consulter les statistiques relatifs à plusieurs postes. Pour cela, sélectionnez les postes concernés dans l'arborescence.

7.6.2. Graphiques

Graphiques des infections

Afin de consulter les graphiques communs relatifs aux infections détectées, procédez comme suit :

1. Sélectionnez l'élément **Réseau antivirus** du menu principal du **Centre de Gestion**, puis dans la fenêtre qui apparaît, cliquez sur le nom du poste ou du groupe dans l'arborescence. Dans le menu de gestion (panneau de gauche), sélectionnez l'élément **Graphiques** depuis la rubrique **Général**.
2. La fenêtre affichant les graphiques ci-dessous va s'ouvrir :



- ◆ **Top 10 des virus les plus répandus** - le top 10 des virus ayant contaminé le plus grand nombre de fichiers. Le graphique présente les données numériques relatives aux objets infectés par les virus désignés.
 - ◆ **Activité journalière des virus** - la période spécifiée est divisée en tranches de 24 h. Le graphique présente le total de virus détectés toutes les 24 heures par objets du réseau (postes et groupes). Ce graphique est affiché à condition que la période sélectionnée soit supérieure à 24H.
 - ◆ **Types d'infections** - affiche les données relatives aux objets infectés par types d'infections.
 - ◆ **Nombre de postes infectés dans le groupe** - affiche les données selon le nombre de postes contaminés par groupe.
 - ◆ **Actions réalisées** - affiche les données relatives aux actions définies par le logiciel antivirus appliquées aux objets.
3. Pour consulter les données graphiques relatives à une période donnée, sélectionnez une période dans la liste déroulante dans la barre d'outils : le jour ou le mois. Vous pouvez également sélectionner n'importe quelle plage de dates, pour cela, entrez les dates correspondantes ou cliquez sur les images des calendriers contre les champs de date. Pour afficher les données, cliquez sur le bouton **Actualiser**.

Graphiques des statistiques sommaires

Les données graphiques sont présentées dans l'élément **Graphique** de la rubrique **Général** ainsi que dans certains éléments de la rubrique **Tableaux** du menu de gestion.

En fonction de l'objet sélectionné depuis l'arborescence (un groupe ou un poste), différents jeux de graphiques seront affichés. Le tableau ci-dessous présente la listes des graphiques et les rubriques correspondantes du menu de gestion, où les graphiques relatifs à l'objet sélectionné dans l'arborescence seront affichés.



Tableau 7-5. Correspondance entre les graphiques, les éléments de l'arborescence et les rubriques du menu de gestion

Graphiques	Pour les groupes	Pour les postes	Rubriques
Top 10 des virus les plus répandus	+	+	Infections Virus Graphiques
Top 10 des postes les plus infectés	+		Infections
Types d'infections	+	+	Virus
Résultats des installations			Toutes les installations via réseau
Activité moyenne de contamination	+		Statistiques
Par nombre d'erreurs	+	+	Erreurs
Par composants	+	+	Erreurs
Résultats des tâches exécutées	+	+	Tâches
Classes des infections	+	+	Graphiques
Actions réalisées	+	+	Graphiques
Activité journalière des virus	+	+	Graphiques
Nombre de postes infectés dans le groupe	+		Graphiques

- ◆ **Top 10 des postes les plus infectés** - cet élément affiche une liste de 10 postes infectés par nombre maximum d'objets malveillants. Le graphique présente les données numériques sur le nombre total d'objets malveillants détectés sur les postes sélectionnés.
- ◆ **Types d'infections** - cet élément ouvre un diagramme circulaire affichant le nombre total d'objets malveillants détectés par type d'objet.
- ◆ **Résultats des installations** - cet élément ouvre un diagramme circulaire affichant le nombre total d'installations lancées depuis le **Serveur**, trié par résultat d'installation. En cas



d'échec de l'installation, la cause en sera affichée. Le diagramme s'affiche pour toutes les installations réalisées depuis le **Serveur**, quel que soit l'objet sélectionné depuis l'arborescence.

- ◆ **Activité moyenne de contamination** - cet élément affiche la valeur moyenne de contamination sur les postes faisant partie du groupe sélectionné. La valeur est calculée comme le nombre total d'objets malicieux détectés divisé par le nombre d'objets scannés sur chaque poste.
- ◆ **Par nombre d'erreurs** - cet élément affiche une liste des postes sur lesquels des erreurs de fonctionnement des composants antivirus ont été détectées. Le graphique présente le nombre d'erreurs par poste.
- ◆ **Par composants** - cet élément affiche une liste des composants antivirus installés sur les postes pour lesquels des erreurs sont survenues durant le fonctionnement. Le diagramme circulaire présente un nombre total d'erreurs relatives à chaque composant.
- ◆ **Résultats de l'exécution des tâches** - cet élément affiche une liste des tâches lancées sur les objets sélectionnés. Le graphique présente le nombre de démarrage de chaque tâche. Le tableau se trouvant au-dessous du graphique présente les résultats de l'exécution des tâches.




7.6.3. Tableau récapitulatif

Pour consulter le Tableau récapitulatif :

1. Sélectionnez l'élément **Réseau antivirus** du menu principal du **Centre de Gestion**, puis dans la fenêtre qui apparaît, cliquez sur le nom du poste et du groupe dans l'arborescence. Dans le menu de gestion (panneau de gauche), depuis la rubrique **Tableaux**, sélectionnez l'élément **Tableau récapitulatif**.
2. La fenêtre présentant des tableaux de données va s'ouvrir. Pour ajouter des données statistiques au rapport, cliquez sur le bouton **Tableau récapitulatif** dans la barre d'outils et sélectionnez les types dans la liste déroulante : **Statistiques, Infections, Tâches, Démarrage/termination, Erreurs**. Les statistiques incluses dans les rubriques du rapport correspondent aux statistiques de la rubrique **Tableaux**. Pour



consulter le rapport avec les tableaux sélectionnés, cliquez sur le bouton **Actualiser**.

3. Pour consulter les informations relatives à une période donnée, vous pouvez sélectionner depuis la liste déroulante une période par rapport à la date courante ou choisir depuis la barre d'outils une plage de dates nécessaire. Pour spécifier une plage de dates, saisissez les dates correspondantes ou cliquez sur l'image représentant un calendrier contre le champ de date. Pour télécharger des données, cliquez sur **Actualiser**.
4. Afin de sauvegarder le rapport pour l'imprimer ou le traiter ultérieurement, cliquez sur le bouton  **Sauvegarder les données vers un fichier CSV**, sur le bouton  **Sauvegarder les données vers un fichier HTML** ou sur le bouton  **Sauvegarder les données vers un fichier XML**.

7.6.4. Quarantaine



Afin de pouvoir gérer la **Quarantaine** depuis le **Serveur**, il est nécessaire que les postes possédant le module de **Quarantaine** puissent fonctionner sous un OS supportant l'installation de **SpIDer Guard G3**, voir [Pré-requis système](#).

Sinon la gestion à distance est impossible. La **Quarantaine** ne pourra pas non plus gérer les fichiers se trouvant dans le dossier `Infected`.!!! et les informations sur le contenu de la **Quarantaine** ne seront pas envoyées au **Serveur**.

Contenu de la quarantaine

Des fichiers peuvent être mis en **Quarantaine** de manière suivante :

- ◆ par l'un des composants antivirus, par exemple, par le **Scanner**,
- ◆ manuellement, par l'utilisateur via le Gestionnaire de **Quarantaine**.



Mis en **Quarantaine**, les fichiers sont automatiquement scannés à nouveau. Dans ce cas :

- ◆ le statut de contamination sera précisé - la présence d'une infection et son type (compte tenu qu'en cas d'ajout manuel dans la **Quarantaine**, l'information sur le statut de contamination des fichiers n'est pas disponible),
- ◆ le nom et le type d'infections sont modifiés de sorte qu'ils correspondent au classement commun.

L'utilisateur peut également re-scanner lui-même les fichiers se trouvant dans la **Quarantaine** via le **Centre de Gestion** ou via le Gestionnaire de **Quarantaine** sur le poste.

Pour consulter et modifier le contenu de la quarantaine dans le Centre de Gestion :

1. Sélectionnez l'élément **Réseau antivirus** du menu principal du **Centre de Gestion**, puis dans la fenêtre qui apparaît, cliquez sur le nom du poste ou du groupe dans l'arborescence. Dans le menu de gestion (panneau de gauche), sélectionnez l'élément **Quarantaine** dans la rubrique **Général**.
2. La fenêtre contenant les données sur le statut actuel de la **Quarantaine** va s'ouvrir.

Si un seul poste a été sélectionné, le tableau contenant les objets se trouvant dans la Quarantaine sur ce poste sera affiché.

Si plusieurs postes ou un groupe/plusieurs groupes ont été sélectionnés, le jeu de tableaux contenant les objets se trouvant en Quarantaine sur chaque poste sera affiché.

3. Pour consulter les fichiers placés dans la **Quarantaine** durant une certaine période, spécifiez un délai dans la barre d'outils et cliquez ensuite sur **Actualiser**.
4. Pour gérer les fichiers se trouvant dans la **Quarantaine**, cochez les cases correspondantes à un fichier, un groupe de fichiers ou pour tous les fichiers placés en **Quarantaine** (la case se trouve dans l'en-tête du tableau). Dans la barre d'outils, sélectionnez une des actions suivantes :

- ◆  **Récupérer les fichiers** - pour récupérer les fichiers








depuis la **Quarantaine**.



N'utilisez cette option que dans le cas où vous êtes vraiment sûr que l'objet ne présente aucun danger.

Sélectionnez une des variantes listées ci-dessous depuis le menu déroulant :

- a)  **Récupérer les fichiers** - pour restaurer l'emplacement d'origine du fichier sur l'ordinateur (restaurer le fichier vers le dossier où il était avant le déplacement).
- b)  **Récupérer les fichiers depuis la quarantaine selon le chemin** - pour déplacer le fichier vers le dossier spécifié par l'administrateur.
- ◆  **Supprimer les fichiers** - pour supprimer les fichiers sélectionnés dans la **Quarantaine** et dans le système.
- ◆  **Scanner les fichiers** - rescanner les fichiers sélectionnés dans la **Quarantaine**.
- ◆  **Exportation** - pour copier et sauvegarder les fichiers sélectionnés dans la **Quarantaine**.

Après avoir déplacé les fichiers suspects dans la **Quarantaine** locale sur l'ordinateur de l'utilisateur, vous pouvez copier ces fichiers via le **Centre de Gestion** et les sauvegarder à l'aide du navigateur web, notamment, pour les envoyer ultérieurement pour l'analyse auprès du laboratoire antiviral de **Doctor Web**. Pour sauvegarder les fichiers, cochez les cases correspondantes contre les fichiers en question et cliquez ensuite sur **Exportation**.

- ◆ Exporter les données sur le statut de la **Quarantaine** vers un fichier sous un des formats suivants :



- enregistrer les données dans un fichier au format CSV,



- enregistrer les données dans un fichier au format HTML,



- enregistrer les données dans un fichier au format XML.

7.7. Configurations de certains composants antivirus



Le jeu de paramètres des composants ainsi que les recommandations sur leur configuration sont décrits dans les manuels **Antivirus Dr.Web® pour Windows. Manuel Utilisateur** et **Dr.Web® Agent pour Windows. Manuel utilisateur**.

Vous trouverez ci-après les configurations de certains composants antivirus autres que les configurations disponibles depuis le poste.

7.7.1. Configuration d'Office Control pour l'accès aux ressources locales et aux celles du réseau sous OS Windows®

Vous pouvez limiter de manière centralisée l'accès aux ressources locales ainsi qu'aux noeuds du réseau Internet. Pour cela, utilisez le composant **Dr.Web Office Control**.

Configuration d'Office Control :

1. Pour accéder à la fenêtre d'édition des paramètres, sélectionnez l'élément **Réseau antivirus** du menu principal du **Centre de Gestion**, puis dans la fenêtre qui apparaît, cliquez sur le nom du poste ou du groupe dans l'arborescence. Dans le menu de gestion (panneau de gauche), sélectionnez l'élément **Dr.Web Office Control**.
2. Dans l'onglet **Général**, sélectionnez les paramètres relatifs au blocage et spécifiez les ressources (fichiers et dossiers locaux) auxquelles l'accès sera bloqué :



- ◆ Pour activer le blocage de l'accès aux ressources locales, cochez la case **Activer le blocage d'accès**.
- ◆ Cochez la case **Blocage d'accès aux supports amovibles** pour bloquer l'accès aux supports amovibles.
- ◆ Cochez la case **Protéger les répertoires et fichiers** pour bloquer l'accès aux dossiers et fichiers. Les chemins vers les ressources à bloquer sont spécifiés dans le champ **Répertoires et fichiers protégés**. Pour ajouter un nouveau chemin, cliquez sur le bouton , puis éditez la ligne ajoutée.



Si le fichier à bloquer est spécifié sans désigner le chemin, il sera compris comme se trouvant dans le dossier %system32% et dans la configuration d'**Office Control** du côté client, il sera affiché avec le préfixe c:\windows\system32.

3. Dans l'onglet **Accès**, cochez la case **Filtrage WWW** afin de paramétrer l'accès aux domaines Internet. Cochez la case **Bloquer l'accès à tous les sites** pour interdire l'accès à Internet. Ajouter dans les listes respectives les domaines auxquels l'accès sera autorisé ou interdit. Pour créer une entrée, cliquez sur le bouton et saisissez les informations nécessaires dans le champ qui apparaît.

Dans la rubrique **Bloquer le contenu**, cochez les cases contre les catégories de sites à bloquer. Ces cases activent le filtre intégré et bloquent l'accès aux sites web correspondant aux catégories associées.

4. A la fin du paramétrage, cliquez sur le bouton **Sauvegarder**. Les paramètres seront pris en compte dès que la nouvelle configuration du poste aura été approuvée.



Dans la configuration d'**Office Control**, il est interdit de protéger les répertoires suivants y compris leurs répertoires racine :

- ◆ %SYSTEMROOT%,
- ◆ %USERPROFILE%,



◆ %PROGRAMFILES%.

Par ailleurs, il est possible de bloquer leurs sous-dossiers.

Office Control ne permet pas de bloquer les fichiers et dossiers se trouvant dans le réseau.

Dans le cas où l'édition de la configuration d'**Office Control** (voir [Configuration des droits des utilisateurs](#)) est autorisée sur le poste, l'utilisateur a une possibilité de limiter lui-même l'accès aux ressources. Il sera également possible de spécifier les paramètres concernés depuis le **Serveur**. Les paramètres spécifiés sur le **Serveur** seront mis à jour sur le côté client de manière automatique.



En cas d'erreur de la part de l'administrateur lors du paramétrage d'**Office Control** sur le **Serveur** (par exemple une erreur dans le chemin vers une ressource à bloquer ou une tentative de bloquer un répertoire à ne pas bloquer), les paramètres seront mis à jour sur le côté client, mais le blocage ne sera pas activé. Dans ce cas, l'erreur d'administration ne sera pas signalée.

7.7.2. Configuration du composant MailD pour la protection des adresses e-mail sous OS UNIX® et Mac OS X



Si l'**Agent** tourne sous l'OS de la famille UNIX ou Mac OS X, vous pouvez spécifier une liste des adresses e-mail à protéger. Vous pouvez spécifier une des variantes suivantes : 15, 30, 50 ou un nombre supérieur afin de vérifier le nombre spécifié d'adresses par le composant **Dr.Web MailD**.



Vous pouvez consulter le nombre d'adresses protégées dans le fichier clé de l'**Agent** (`agent.key`).



Pour spécifier une liste d'adresses e-mail à protéger :

1. Sélectionnez dans l'arborescence du **Centre de Gestion** un poste et un groupe de postes, puis, depuis le menu de gestion (panneau de gauche), cliquez sur l'élément **Emails**.
2. Dans la fenêtre qui apparaît, saisissez l'adresse email nécessaire.
3. Pour ajouter une nouvelle adresse, cliquez sur le bouton . Il faut saisir chaque nouvelle adresse à la ligne.
4. Pour supprimer une adresse, cliquez sur le bouton  contre le champ correspondant.
5. Cliquez sur le bouton **Sauvegarder** pour sauvegarder les modifications apportées.

7.8. Envoi des messages à l'utilisateur

L'administrateur système peut envoyer des messages aux utilisateurs, qui peuvent contenir les informations suivantes :

- ◆ texte du message ;
- ◆ hyperliens vers des ressources Internet ;
- ◆ logo de société (ou tout visuel) ;
- ◆ l'en-tête du message comprend toujours la date précise de réception du message.

Les messages sont affichés côté utilisateur sous forme d'infobulles (voir la figure [7-1](#)).

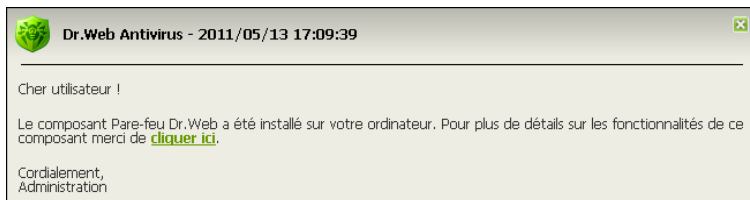




Figure 7-1. Fenêtre d'un message du côté utilisateur



Marche à suivre pour envoyer un message à l'utilisateur :

1. Sélectionnez l'élément **Réseau antivirus** du menu principal du **Centre de Gestion**.
2. Dans la fenêtre qui apparaît, sélectionnez un groupe ou un poste dans l'arborescence, puis depuis la barre d'outils cliquez sur  **Général** →  **Envoyer des messages aux postes**.

Dans la fenêtre qui apparaît, remplissez les champs suivants :

- ◆ **Texte du message** est un champ obligatoire à remplir. Le champ contient le message.
- ◆ **Afficher le logo d'entreprise dans le message** - cochez la case pour afficher dans l'en-tête du message le logo. Pour télécharger le logo depuis une ressource locale, cliquez sur le bouton **Parcourir** se trouvant à droite du champ **Fichier de logo** et sélectionnez ensuite le fichier dans l'explorateur.

Vous pouvez également spécifier un en-tête du message ainsi que le nom de l'entreprise dans le champ **Nom**. Ce texte sera affiché dans l'en-tête de la fenêtre affichant le message (à droite du logo). Si vous laissez ce champ vide, des informations sur **l'Agent** s'afficheront.

Le champ **URL** permet de spécifier le lien vers une page web à ouvrir lors d'un clic sur le logo (ainsi que lors d'un clic sur l'en-tête de la fenêtre si cet en-tête n'est pas spécifié dans le champ **Nom**).

S'il n'y a pas de logo ou la taille du logo dépasse la taille maximale (voir [Format du logo](#), p. 3), l'icône d'**Enterprise Agent** sera affichée à sa place.

La case cochée **Afficher le logo d'entreprise dans le message** active la case **Utiliser la transparence**. Cochez cette case pour utiliser la transparence dans l'affichage du logo (voir [Format du logo](#), p. 4).

- ◆ **Afficher le lien contenu dans le message** - cochez la case si vous souhaitez mettre des hyperliens dans le message à envoyer à l'utilisateur. Pour ajouter un lien :



1. Spécifiez le lien dans le champ **URL**.
2. Dans le champ **Texte**, spécifiez le nom du lien - le texte à afficher à la place du lien dans le texte.
3. Dans le champ **Texte du message**, saisissez le tag `{link}` partout où le lien sera inséré. Dans le message final, le lien sera inséré selon les paramètres spécifiés. Le nombre de balises `{link}` dans le texte est illimité, cependant, toutes les balises auront les mêmes paramètres (depuis les champs respectifs **URL** et **Texte**).

Exemple :

Pour envoyer le message affiché sur la figure [7-1](#), les paramètres suivants ont été spécifiés :

Texte du message :

```
Cher utilisateur !

Le composant Pare-feu Dr.Web a été
installé sur votre ordinateur.
Pour plus de détails sur les
fonctionnalités de ce composant merci de
{link}.

Cordialement,
L'administrateur.
```

URL : `http://drweb.com/`

Texte : cliquer ici

- ◆ **Afficher le résultat de livraison** - cochez la case si vous souhaitez recevoir un rapport sur la délivrance du message à l'utilisateur.



Format du logo

Le fichier contenant une image (logo) incluse dans le message doit correspondre aux critères suivants :

1. Format du fichier - BMP.
2. Profondeur de couleur (bit depth) - n'importe quelle (8 - 24 bits).
3. Taille maximum de la partie visible du logo est 120x90 px (largeur x hauteur). Dimensions supplémentaires 2x2 px - un supplément pour le cadre des pixels de transparence (voir p. 4), ainsi la taille complète maximum de l'image est de 122x92 px (voir la figure 7-2).

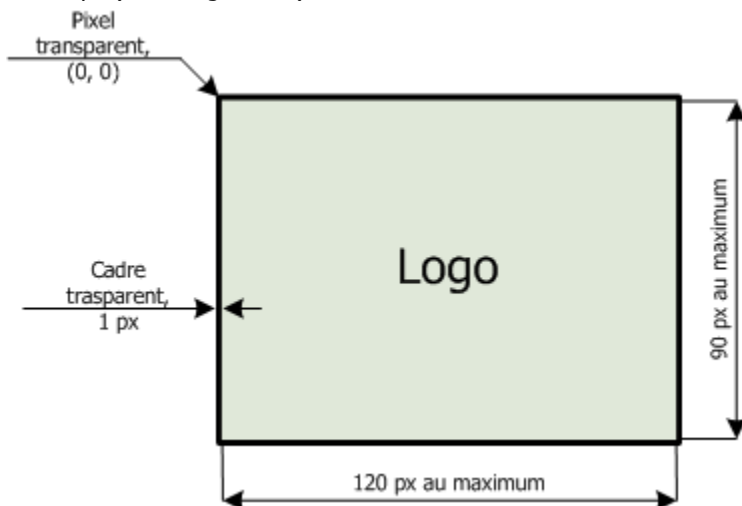


Figure 7-2. Format du fichier de logo

4. Dans le cas où l'option **Utiliser la transparence** a été activée lors de l'envoi du message, le premier pixel dans la position (0,0) est désigné *transparent*. Tous les pixels ayant la même couleur deviennent aussi transparents et le fond de la fenêtre du message sera affiché à leurs places.

Si vous activez l'option **Utiliser la transparence** pour un logo



rectangulaire, il est recommandé de créer un cadre rectangulaire afin d'éviter une spécification incorrecte des pixels de l'image comme transparents.

L'option **Utiliser la transparence** est utile en cas de forme non standard (non rectangulaire) du logo et permet d'éviter l'apparition du fond indésirable complétant la partie informant du message pour obtenir une forme rectangulaire. Par exemple, si l'image dans l'illustration sur la figure 7-3 est utilisée comme logo, le fond de couleur violette sera enlevé (devient transparent).



Figure 7-3. Logo de forme non standard



Avant l'envoi du message aux utilisateurs (surtout en cas de message à plusieurs destinataires), il est recommandé de tester l'envoi en envoyant le message vers un poste avec un **Agent** installé pour être sûr que cela fonctionne correctement.



Chapitre 8. Configuration de Dr.Web Enterprise Server

8.1. Configuration de Dr.Web Enterprise Server

Pour configurer Dr.Web Enterprise Server :

1. Sélectionnez l'élément **Administration** du menu principal du **Centre de Gestion**.
2. Dans la fenêtre du menu de gestion qui apparaît, sélectionnez l'élément **Configuration de Dr.Web Enterprise Server**.
3. La fenêtre de configuration du **Serveur** va s'ouvrir.



Les champs marqués par le symbole * sont obligatoires à remplir.

Onglet Général

Le paramètre **Nom** désigne le nom du **Serveur**. Si aucun nom n'est saisi, le nom du poste sur lequel tourne le logiciel de **Serveur Enterprise** sera spécifié.

Le paramètre **Processus légers** détermine le nombre de processus légers à traiter provenant des **Agents**. Il est recommandé de ne pas modifier la valeur spécifiée par défaut sans avoir consulté le support technique.

Le paramètre **Nombre de connexions à la BD** définit un nombre de connexions du **Serveur** à la BD. Il est recommandé de ne pas modifier la valeur spécifiée par défaut sans avoir consulté le support technique.



Le champ **File d'attente pour l'authentification** permet de spécifier un nombre maximum de postes pouvant être dans la file d'attente pour l'authentification sur le **Serveur**. Tout nombre entier peut être spécifié.

La liste déroulante **Bande passante des mises à jour** permet de paramétrer la bande passante maximum lors des téléchargements des mises à jour entre le **Serveur** et les **Agents**. Dans ce cas, les paramètres suivants sont disponibles :

- ◆ En cas de valeur **illimité**, les mises à jour pour les **Agents** seront téléchargées sans aucune limitation de la bande passante.
- ◆ En cas de valeur autre qu'**illimité** (une valeur numérique), les mises à jour sont téléchargées dans les limites de la bande passante allouée au trafic réseau total relatif aux mises à jour de tous les **Agents**.

La liste déroulante **Novices** permet de paramétrer la politique de connexion de nouveaux postes de travail (voir [Politique de connexion de nouveaux postes](#)). La case cochée **Spécifier les non approuvés comme novices** enjoint au programme de réinitialiser les paramètres de connexion au **Serveur** sur les postes non approuvés. Cette option peut être utile lors de la modification des paramètres du **Serveur** (notamment en cas de modification de la clé publique) ou en cas de changement de BD. Dans ces cas, les postes ne peuvent pas se connecter et il faudra obtenir de nouveaux paramètres permettant d'accéder au **Serveur**.

Les listes déroulantes **Chiffrement** et **Compression** permettent de choisir une politique de chiffrement et de compression du trafic entre **Serveur Enterprise**, **Agents** et le **Centre de Gestion** (pour en savoir plus sur ces paramètres, consultez le paragraphe [Utilisation du chiffrement et de la compression du trafic](#)).

Vous pouvez également modifier le statut des cases suivantes :

- ◆ **Afficher les noms de domaine** enjoint au programme d'écrire dans le fichier de log les noms de domaine à la place des adresses IP.
- ◆ **Remplacer les noms NetBIOS** active l'affichage, dans



l'arborescence du réseau antivirus, des noms de domaine à la place des noms de poste (dans le cas où il est impossible de déterminer les noms de domaine, les adresses IP seront affichées).



Les deux cases **Afficher les noms de domaine** et **Remplacer les noms NetBIOS** sont décochées par défaut. En cas de paramétrage incorrect du service DNS, l'activation de ces fonctions peut ralentir considérablement le fonctionnement du **Serveur**. En cas d'activation d'un de ces deux modes, il est recommandé d'autoriser la mise en cache des noms sur le serveur DNS.



Si la case **Remplacer les noms NetBios** est cochée et un **serveur proxy** est utilisé dans le réseau antivirus, pour tous les postes connectés au **Serveur** via le **serveur proxy**, dans le **Centre de Gestion**, le nom de l'ordinateur sur lequel est installé le **serveur proxy** sera affiché à la place du nom du poste.

- ◆ **Synchroniser les descriptions des postes** - enjoint de synchroniser la description du poste utilisateur avec celle du **Centre de Gestion**. Si la description du poste n'a pas été effectuée dans le **Centre de Gestion**, la description du poste du côté utilisateur sera insérée dans le champ correspondant. Si les descriptions sont différentes, les données inscrites dans le **Centre de Gestion** seront remplacées par la description utilisateur.

Onglet Données statistiques

L'onglet **Données statistiques** permet de spécifier les informations statistiques à écrire dans le fichier de log ainsi que dans la base de données du **Serveur**.

Pour ajouter des informations dans la BD, cochez les cases correspondantes :

- ◆ **Quarantaine** - autorise l'écriture du statut de la **Quarantaine** sur les postes.



- ◆ **Liste des modules de poste dans la BD** - autorise l'écriture des informations sur les jeux de composants des modules de l'**Antivirus** sur le poste.
- ◆ **Liste des composants installés dans la BD** - autorise l'écriture des informations sur les composants de l'**Antivirus** (**Scanner**, **Moniteurs** etc.) installés sur le poste.
- ◆ **Informations sur le démarrage/arrêt des composants dans la BD** - autorise l'écriture des informations sur le lancement et l'arrêt des composants de l'**Antivirus** (**Scanner**, **Moniteurs** etc.) installés sur le poste.
- ◆ **Infections dans la BD** - autorise l'écriture des données statistiques sur les infections détectées sur les postes.
- ◆ **Erreurs de scan dans la BD** - autorise l'écriture des informations sur toutes les erreurs survenues lors du scan sur les postes de travail.
- ◆ **Statistiques de scan dans la BD** - autorise l'écriture des résultats du scan sur les postes.
- ◆ **Informations sur les installations dans la BD** - autorise l'écriture des informations sur les installations des **Agents** sur les postes de travail.
- ◆ **Log d'exécution des tâches** - autorise l'écriture dans la BD des résultats de l'exécution des tâches sur les postes.
- ◆ **Surveillance des statuts des postes** - autorise le contrôle des modifications du statut des postes et l'écriture des informations associées dans la BD.
- ◆ **Surveillance des bases virales** - autorise le contrôle du statut (composants et modifications) des bases virales sur le poste ainsi que l'écriture des informations correspondantes dans la BD.

Pour consulter les informations statistiques, procédez comme suit :

1. Sélectionnez l'élément **Réseau antivirus** du menu principal.
2. Depuis l'arborescence sélectionnez un poste ou un groupe.
3. Ouvrez la rubrique correspondante du menu de gestion (voir le tableau ci-dessous).



Pour en savoir plus sur les données statistiques, consultez le paragraphe [Consultation des résultats et des statistiques sommaires du poste](#).

Le tableau ci-dessous présente la correspondance entre les cases relatives à la rubrique **Données statistiques** dans la configuration du **Serveur** et les éléments du menu de gestion depuis la page **Réseau antivirus**.

Si les cases sur l'onglet **Données statistiques** sont décochées, les éléments correspondants seront cachés dans le menu de gestion.

Tableau 8-1. Correspondance entre les paramètres du Serveur et les éléments du menu de gestion

Paramètres du Serveur	Eléments du menu
Quarantaine	Général → Quarantaine
Liste des modules de poste dans la BD	Tableaux → Modules
Listes des composants installés dans la BD	Général → Composants installés
Informations sur le démarrage/arrêt des composants dans la BD	Tableaux → Démarrage/Arrêt
Infections dans la BD	Tableaux → Infections Tableaux → Virus
Erreurs de scan dans la BD	Tableaux → Erreurs
Statistiques de scan dans la BD	Tableaux → Statistiques Tableaux → Statistiques sommaires
Informations sur les installations dans la BD	Tableaux → Toutes les installations via réseau
Log de l'exécution des tâches	Tableaux → Tâches Tableaux → Bases virales
Surveillance des statuts des postes	Tableaux → Statut Tableaux → Bases virales



Paramètres du Serveur	Éléments du menu
Surveillance des bases virales	Tableaux → Bases virales

Onglet Statistiques

L'onglet **Statistiques** permet de configurer l'envoi des statistiques sur les événements viraux à **Doctor Web**.

Pour activer l'envoi des statistiques, cochez la case **Statistiques**. Les champs listés ci-dessous seront activés :

- ◆ **Intervalle** - un intervalle entre les envois des statistiques, en minutes ;
- ◆ **Adresse du Serveur** - l'adresse IP ou le nom DNS et le port du Serveur de statistiques (par défaut c'est `stat.drweb.com:80`) ;
- ◆ **Répertoire** - répertoire sur le Serveur de statistiques (par défaut c'est `/update`) ;
- ◆ **Identificateur du client** - clé MD5 du **Serveur** (qui se trouve dans le fichier clé de **Serveur** `enterprise.key`) ;
- ◆ **Utilisateur** - le nom utilisateur pour l'enregistrement des statistiques. Le nom peut être obtenu auprès du **Service Support technique Doctor Web** ;
- ◆ **Mot de passe** - le mot de passe à utiliser pour enregistrer des statistiques. Le mot de passe peut être obtenu auprès du **Service Support technique Doctor Web** ;
- ◆ **Serveur proxy** - spécifiez si nécessaire l'adresse du serveur proxy à utiliser pour envoyer des statistiques ;
- ◆ **Utilisateur du proxy** - entrez ici le nom de l'utilisateur du serveur proxy (à ne pas entrer en cas d'authentification anonyme du proxy) ;
- ◆ **Mot de passe d'utilisateur du proxy** - entrez ici le mot de passe pour accéder au serveur proxy (à ne pas entrer en cas d'authentification anonyme du proxy).



Seuls les champs **Adresse du Serveur** de statistiques et **Intervalle** entre les envois des statistiques sont obligatoires à remplir.

Pour enregistrer les modifications apportées, cliquez sur le bouton **Sauvegarder**.

Onglet Sécurité

L'onglet **Sécurité** permet de spécifier des limitations pour les adresses réseau depuis lesquelles les **Agents**, les installateurs réseau et d'autres **Serveurs** ("voisins") pourront accéder au **Serveur** spécifié.

Les cases ci-dessous permettent de gérer le journal d'audit du **Serveur** :

- ◆ **Audit des opérations** autorise l'écriture dans le journal d'audit des opérations de l'administrateur avec le **Centre de Gestion** ainsi que l'écriture du journal dans la BD.
- ◆ **Audit des opérations internes du serveur** autorise l'écriture dans le journal d'audit des opérations internes du **Serveur** ainsi que l'écriture du journal dans la BD.



Pour consulter le journal d'audit, sélectionnez l'élément **Journal d'audit** dans le menu principal **Administration**.

L'onglet **Sécurité** comprend les onglets supplémentaires **Agents**, **Installations** et **Voisins** permettant de configurer des limitations pour les types correspondants de connexion.

Marche à suivre pour configurer les restrictions d'accès pour un type de connexion sélectionné :



1. Ouvrez un onglet (**Agents**, **Installations** ou **Voisins**).
2. Pour autoriser toutes les connexions, décochez la case **Utiliser cette liste de contrôle d'accès**.
3. Pour spécifier les listes d'adresses autorisées ou bloquées, cochez la case **Utiliser cette liste de contrôle d'accès**.
4. Pour autoriser l'accès depuis une adresse TCP spécifiée,



ajoutez-la dans la liste **TCP: autorisé** ou **TCPv6: autorisé**.

5. Pour interdire une adresse TCP, ajoutez-la dans la liste **TCP: interdit** ou **TCPv6: interdit**.

Pour éditer la liste des adresses :

1. Entrez l'adresse réseau dans le champ correspondant et cliquez ensuite sur le bouton **Sauvegarder**.
2. Pour ajouter un champ d'adresse, cliquez sur le bouton  dans la rubrique correspondante.
3. Pour supprimer un champ, cliquez sur .

L'adresse réseau doit être spécifiée au format suivant : *<adresse IP>/ [<préfixe>]*.



Les listes pour les adresses TCPv6 ne seront affichées que dans le cas où l'interface IPv6 est installée sur le poste.

Exemple d'utilisation du préfixe :

1. Le préfixe 24 désigne les réseaux ayant le masque 255.255.255.0

Il contient 254 adresses

Les adresses hôte dans les réseaux de ce type : 195.136.12.*

2. Le préfixe 8 désigne les réseaux ayant le masque 255.0.0.0

Il contient jusqu'à 16387064 adresses (256*256*256)

Les adresses hôte dans les réseaux de ce type : 125.*.*.*

Les restrictions pour les adresses IPX peuvent être configurées de manière analogue.



Les adresses qui ne sont répertoriées dans aucune liste peuvent être interdites ou autorisées en fonction du statut de la case **Priorité de l'interdiction** : si la case est cochée, les adresses qui ne sont répertoriées dans aucune liste ou incluses dans les deux listes seront interdites. Sinon elles seront autorisées.

Onglet Base de données

L'onglet **Base de données** permet de sélectionner un SGBD pour sauvegarder le journal centralisé du réseau antivirus et sa configuration (pour en savoir plus, voir [Configuration du mode de la BD](#)).

Onglet Notifications

Les paramètres se trouvant à l'onglet **Notifications** permettent de configurer le mode de notifications adressées aux administrateurs du réseau antivirus ainsi qu'à d'autres personnes sur les attaques virales et sur d'autres événements détectés par les composants **Dr.Web Enterprise Security Suite** (pour en savoir plus sur ce paramètre, consultez le paragraphe [Configuration des notifications](#)).

Onglet Transport

L'onglet **Transport** permet de configurer les protocoles de transport utilisés par le **Serveur**.

Pour chaque protocole, vous pouvez spécifier le nom de **Serveur Enterprise** dans le champ **Nom**. Dans le cas où aucun nom n'est spécifié, le nom désigné à l'onglet **Général** sera utilisé (comme il est décrit ci-dessus, notamment dans le cas où aucun nom n'est spécifié, le nom du poste sera utilisé). Dans le cas où un nom différent du nom saisi à l'onglet **Général** est spécifié, le nom de la description du protocole sera utilisé. Ce nom est utilisé par le service de détection du **Serveur** par les **Agents**.



Dans le champ **Adresse**, il est nécessaire de spécifier l'adresse de l'interface écoutée par le **Serveur** pour assurer l'interaction avec les **Agents** installés sur les postes de travail.

Dans le champ **Adresse du cluster**, il faut spécifier une langue d'interface écoutée par le **Serveur** interagissant avec les **Agents** et **Installateurs réseau** lors des recherches des **Serveurs Enterprise** actifs dans le réseau. Pour en savoir plus, consultez le paragraphe [Service de détection de Serveur](#).

Les paramètres ci-dessus doivent être spécifiés au format d'adresse réseau décrit dans l'Annexe E. [Spécification d'une adresse réseau](#).

Onglet Modules

L'onglet **Modules** permet de configurer le mode d'utilisation des protocoles d'interaction du **Serveur** avec d'autres composants **Dr.Web ESS**.

Par défaut, l'interaction avec les composants suivants est autorisée :

- ◆ **Enterprise Agents**,
- ◆ composant **NAP Validator**,
- ◆ **Installateurs réseau de l'Agent**.

L'interaction de **Serveur Enterprise** avec d'autres **Serveur Enterprise** est désactivée par défaut. En cas de configuration réseau multi serveurs, (voir [Particularités du réseau avec plusieurs Serveurs](#)), cochez la case pour activer ce protocole.

Onglet Emplacement

L'onglet **Emplacement** vous permet de consulter des informations supplémentaires sur l'ordinateur sur lequel le logiciel de **Serveur Enterprise** est installé.



8.1.1. Chiffrement et compression du trafic

Le réseau antivirus **Dr.Web Enterprise Security Suite** permet de chiffrer le trafic entre le **Serveur** et les postes de travail (**Enterprise Agents**), entre les **Serveur Enterprise** (en cas de configuration réseau multi-serveurs), ainsi qu'entre le **Serveur** et les **Installeurs réseau**. Ce mode est utilisé afin d'éviter une divulgation des clés utilisateur ainsi que des informations sur les équipements ou sur les utilisateurs du réseau antivirus.

Le réseau antivirus **Dr.Web Enterprise Security Suite** utilise des dispositifs de cryptage et de signature numérique très sûrs, basés sur le concept de cryptographie à clé publique.

La politique de chiffrement peut être configurée séparément depuis chaque composant du réseau antivirus, la configuration d'autres composants doit correspondre à celle du **Serveur**.

Marche à suivre pour configurer les politiques de compression et de chiffrement pour Dr.Web Enterprise Server:

1. Sélectionnez l'élément **Administration** du menu principal du **Centre de Gestion**.
2. Dans la fenêtre qui apparaît, sélectionnez l'élément du menu de gestion **Configuration de Dr.Web Enterprise Server**.
3. Dans l'onglet **Général**, sélectionnez depuis les listes déroulantes **Chiffrement** et **Compression** l'une des variantes suivantes :
 - ◆ **Oui** — le chiffrement (ou la compression) du trafic entre tous les composants est obligatoire (la valeur est spécifiée par défaut pour le chiffrement, si le paramètre n'a pas été modifié lors de l'installation du **Serveur**),
 - ◆ **Possible** — le chiffrement (ou la compression) sera appliqué au trafic relatif aux composants dont les configurations le permettent,



- ◆ **Non** — le chiffrement (ou la compression) n'est pas supporté (la valeur est spécifiée par défaut pour la compression si le paramètre n'a pas été modifié lors de l'installation du **Serveur**).

Pour assurer une concordance entre les politiques de chiffrement sur le **Serveur** et sur un autre composant (**Agent** ou **Installateur réseau**) il est à prendre en compte qu'il existe des paramètres incompatibles dont la sélection entraîne l'échec de connexion entre le **Serveur** et le composant concerné.

Le tableau 8-2 comprend les combinaisons des paramètres qui assurent (+) ou n'assurent pas (-) le chiffrement de connexion entre le **Serveur** et le composant, ainsi que les combinaisons inappropriées (**Erreur**).

Tableau 8-2. Compatibilité des paramètres relatifs à la politique de chiffrement

Paramètres du composant	Paramètres du Serveur	Oui	Possible	Non
Oui		+	+	Erreur
Possible		+	+	-
Non		Erreur	-	-



Le chiffrement du trafic entraîne une charge importante sur les ordinateurs dont les performances sont proches de la limite inférieure des pré-requis relatifs aux composants installés. Dans le cas où le chiffrement du trafic n'est pas indispensable pour la sécurité, il est possible de ne pas l'utiliser. Le chiffrement n'est pas non plus recommandé pour des réseaux importants (à partir de 2000 clients). Dans ce cas, il faut d'abord basculer les paramètres du **Serveur** et des composants vers le statut **Possible** afin d'éviter l'apparition de paires de paramètres incompatibles **Installateur réseau-Serveur** ou **Agent-Serveur**. Le non respect de cette règle peut entraîner la perte de contrôle du composant et une nécessité de le réinstaller.



Par défaut, **Enterprise Agent** est installé avec le paramètre de chiffrement **Possible**. Ceci désigne que le chiffrement est actif par défaut, mais il peut être désactivé via les paramètres du **Serveur Enterprise**.

Compte tenu du fait que le trafic entre les composants (surtout entre les **Serveurs**) peut être assez important, le réseau antivirus permet de compresser le trafic. La politique de compression et la compatibilité des paramètres des divers composants sont complètement analogues aux paramètres relatifs au chiffrement décrits ci-dessus, excepté le fait qu'en cas de **Serveur**, la valeur donnée par défaut au paramètre de compression est **Non**.



L'utilisation de la compression diminue le trafic mais augmente considérablement la charge sur les ordinateurs, beaucoup plus que le chiffrement.



8.1.2. Configuration de la BD



La structure de la BD de **Serveur Enterprise** peut être obtenue à l'aide du script `sql init.sql` se trouvant dans le sous-dossier `etc` du dossier d'installation de **Serveur Enterprise**.

Marche à suivre pour configurer la BD :

1. Sélectionnez l'élément **Administration** du menu principal du **Centre de Gestion**.
2. Dans la fenêtre qui apparaît, sélectionnez l'élément du menu de gestion **Configuration de Dr.Web Enterprise Server**.
3. Ouvrez l'onglet **Base de données** et sélectionnez dans la liste déroulante un type de base :
 - ◆ **IntDB** – BD interne (composant de **Serveur Enterprise**),
 - ◆ **MS SQL CE** – BD externe pour les **Serveurs** opérant sous Windows,



Les performances de la BD **MS SQL CE** sont basses et inférieures aux caractéristiques de la BD interne.

Il est déconseillé d'utiliser cette BD en cas de charge supérieure à 30 postes client.

Cependant, la BD **MS SQL CE** peut être utilisée pour la création des rapports via API ADO.NET. Si cette option n'est pas nécessaire, il est recommandé d'utiliser la BD interne ou une autre BD externe disponible.

- ◆ **ODBC** (pour les **Serveurs** opérant sous Windows) ou **PostgreSQL** (pour les **Serveurs** sous UNIX) – BD externe,
- ◆ **Oracle** – BD externe (pour les plateformes, excepté FreeBSD).



En cas d'utilisation du **SGBD** externe **Oracle**, il est nécessaire d'installer la dernière version du **driver ODBC** fourni avec le SGBD. L'utilisation du **driver ODBC Oracle** fourni par **Microsoft** est fortement déconseillé.

Pour la BD interne, si nécessaire, entrez dans le champ **Fichier** le chemin complet vers le fichier contenant la BD et spécifiez la taille de la mémoire-cache ainsi que le mode d'écriture de données.

Pour en savoir plus sur les paramètres relatifs aux BD externes, consultez les Annexes (voir [Annexe B. Configurations requises pour SGBD. Paramètres des driver SGBD](#)).

Par défaut, l'utilisation du SGBD interne est prévue. Ce mode entraîne une charge importante sur le **Serveur**. En cas de réseau antivirus de grande taille, l'utilisation du SGBD externe est recommandée.



L'utilisation de la BD interne est possible dans le cas où le nombre de postes connectés au **Serveur** varie entre 200 et 300. Si la configuration matérielle de l'ordinateur sur lequel est installé **Serveur Enterprise** le permet, ainsi que d'autres tâches exécutées sur le même ordinateur, il est possible de connecter jusqu'à 1000 postes.

Sinon, une BD externe doit être utilisée.

En cas d'utilisation d'une BD externe et si le nombre de postes connectés au **Serveur** est supérieur à 10000, il est recommandé de respecter les pré-requis minimum suivants :

- ◆ processeur 3Ghz,
- ◆ mémoire vive - à partir de 4 Go pour **Serveur Enterprise**, à partir de 8 Go - pour le Serveur BD,
- ◆ OS de la famille UNIX.



Il existe une option de nettoyage de la base utilisée par **Serveur Enterprise**, notamment : suppression des entrées sur les événements ainsi que des informations sur les postes non vus sur le **Serveur** durant une période spécifiée. Pour nettoyer la base de données, allez à la rubrique [Planifications du Serveur](#) et créez une tâche.


8.1.3. Configuration des notifications

Pour configurer le mode d'envoi des notifications sur les événements survenus dans le réseau antivirus :

1. Sélectionnez l'élément **Administration** du menu principal du **Centre de Gestion**.
2. Dans la fenêtre qui apparaît, sélectionnez l'élément du menu de gestion **Configuration de Dr.Web Enterprise Server**.
3. Passez à l'onglet **Notifications** et sélectionnez un mode de notification depuis la liste déroulante :
 - ◆ **Ne pas inclure** — ne pas envoyer de notifications (mode défini par défaut),
 - ◆ **Email** — envoyer par email,
 - ◆ **Messages via réseau Windows** — envoyer en utilisant **Windows Messenger** (uniquement en cas de **Serveur sous Windows**).

Notifications par email

Spécifiez les paramètres listés ci-dessous pour les notifications à envoyer par email :

- ◆ **Expéditeur** - l'adresse de l'expéditeur du message,
- ◆ **Destinataire** - l'adresse du destinataire ou les adresses des destinataires du message ; pour ajouter un nouveau champ de destinataire, cliquez sur le bouton ,
- ◆ **Serveur SMTP, Port** - l'adresse et le port du Serveur SMTP vers lequel le courriel sera envoyé,



- ◆ **Utilisateur, Mot de passe (Confirmez le mot de passe)** - si nécessaire, spécifiez le nom utilisateur et le mot de passe pour l'authentification sur le Serveur SMTP.

Si nécessaire, cochez les cases suivantes :

- ◆ **Mode débogage** – pour avoir un protocole détaillé de la session SMTP.
- ◆ **Utiliser le chiffage TLS/SSL** – pour utiliser le chiffage TLS/SSL du trafic lors de l'envoi des notifications par email.
- ◆ **Autoriser l'authentification en texte brut** – utiliser l'authentification en *texte brut (plein)* sur le serveur de messagerie.
- ◆ **Autoriser l'authentification CRAM-MD5** – pour utiliser l'authentification *CRAM-MD5* sur le serveur de messagerie.

Dans la rubrique **Messages autorisés**, cochez les cases contre les événements à signaler par email.



Messages adressés via le réseau Windows



Le système de notifications via le réseau Windows ne fonctionne que sous les OS Windows supportant le service Windows Messenger (Net Send).

Le service Windows Messenger n'est pas supporté dans Windows Vista ou versions supérieures.

Pour envoyer les messages via Windows, configurez une liste de noms de postes destinataires des messages.

Pour ajouter un nouveau champ, cliquez sur le bouton  et entrez le nom du poste. Pour supprimer un champ, cliquez sur le bouton .

Dans la rubrique **Messages autorisés**, cochez les cases pour les événements à signaler via le réseau Windows.



Templates des messages

Le texte du message est défini par le template. Les templates sont sauvegardés dans le sous-répertoire `var/templates` du répertoire d'installation du **Serveur**. Pour configurer le texte du message à envoyer en cas d'événement spécifié, éditez le template correspondant.

Lors de la préparation du message, le système de notification remplace les variables de template (entre accolades) par le texte défini en fonction des paramètres actuels. La liste des variables disponibles est décrite dans les Annexes (voir [Annexe D. Paramètres des templates du système de notifications](#)).

Il est recommandé d'utiliser **Editeur des templates** pour l'édition des templates. Pour cela :

1. Sélectionnez l'élément **Administration** du menu principal du **Centre de Gestion**, puis dans la fenêtre qui apparaît, sélectionnez l'élément du menu de gestion **Editeur des templates**.
2. Sélectionnez un template dans la liste pour l'éditer.
 - ◆ Le champ **Sujet** permet d'éditer le sujet du message à envoyer.
 - ◆ Le champ **En-têtes** permet de spécifier des en-têtes supplémentaires du message électronique si vous en avez besoin.
 - ◆ Le champ **Message** spécifie le template du texte du message.

Pour ajouter des variables, vous pouvez utiliser les listes déroulantes dans l'en-tête du message.

3. Pour sauvegarder les modifications apportées au template, cliquez sur le bouton **Sauvegarder**.



Dans le cas où vous utilisez un éditeur externe pour éditer les templates, veuillez sauvegarder les templates dans le codage **UTF-8**. Il est fortement déconseillé d'utiliser le **Notepad** ainsi que d'autres éditeurs insérant dans le texte un marqueur d'ordre des octets ou BOM afin de détecter le codage **UTF-8**, **UTF-16** ou **UTF-32**.

8.2. Ecriture dans le log du serveur

Serveur Enterprise effectue la journalisation des événements relatifs à son fonctionnement. Le nom du fichier de log est `drwcsd.log`.

Par défaut, le fichier de log se trouve dans l'emplacement suivant :

- ◆ Sous **UNIX** :
 - Linux : `/var/opt/drwcs/log/drwcsd.log`;
 - FreeBSD et Solaris: `/var/drwcs/log/drwcsd.log`.
- ◆ Sous **Windows** : dans le sous-répertoire `var` du répertoire d'installation du **Serveur**.

Le fichier est dans un format texte simple (voir [Annexe L. Format des fichiers de log](#)).







Le journal du **Serveur** est utilisé pour le débogage ainsi que pour remédier à un fonctionnement anormal des composants du réseau antivirus.



8.3. Configuration de la planification de Dr.Web Enterprise Server

Marche à suivre pour configurer la planification des tâches pour Dr.Web Enterprise Server :

1. Sélectionnez l'élément **Administration** du menu principal du **Centre de Gestion**, puis dans la fenêtre qui apparaît, sélectionnez l'élément du menu de gestion **Planification de Dr.Web Enterprise Server**. La liste des tâches actuelles du **Serveur** va s'afficher.
2. Pour supprimer une tâche de la liste, cochez la case correspondante et cliquez ensuite sur le bouton  **Supprimer les configurations** dans la barre d'outils.
3. Pour éditer les paramètres d'une tâche, sélectionnez-la dans la liste. La fenêtre de l'**Editeur des tâches** décrite [ci-dessous](#) va s'ouvrir.
4. Pour ajouter une tâche dans la liste, sélectionnez l'élément  **Nouvelle tâche** dans la barre d'outils. La fenêtre **Nouvelle tâche** va s'ouvrir de la même façon que la fenêtre **Editeur des tâches**. Spécifiez ensuite les paramètres nécessaires (voir [ci-dessous](#)) et cliquez sur le bouton **Sauvegarder**.
5. Vous pouvez également interdire l'exécution d'une tâche ou autoriser l'exécution de la tâche qui a été interdite.
6. Pour exporter la planification vers un fichier de format spécifique, cliquez sur le bouton  dans la barre d'outils.
7. Pour importer les paramètres depuis tel fichier, cliquez sur le bouton  dans la barre d'outils.



Les champs marqués par le symbole * sont obligatoires à remplir.

Edition des paramètres de la tâche :

1. Dans l'onglet **Général**, spécifiez les paramètres suivants :



- ◆ Dans le champ **Nom**, saisissez le nom sous lequel la tâche sera affichée dans la planification.
- ◆ Pour activer l'exécution de la tâche, cochez la case **Autoriser l'exécution**.

Si la case n'est pas cochée, la tâche sera présente dans la liste mais ne sera pas exécutée.

- ◆ La case cochée **Tâche critique** enjoint d'exécuter la tâche au prochain démarrage de **Serveur Enterprise** au cas où son exécution a échoué (**Serveur Enterprise** déconnecté à l'heure correspondant à l'exécution de la tâche). Si l'exécution d'une tâche a échoué plusieurs fois durant une période déterminée, elle sera exécutée une seule fois au démarrage de **Serveur Enterprise**.
2. Dans l'onglet **Action**, sélectionnez un type d'action dans la liste déroulante. L'apparence de la partie inférieure de la fenêtre sera modifiée afin que les paramètres supplémentaires soient affichés. Spécifiez ces paramètres (pour en savoir plus sur les paramètres relatifs aux divers types de tâches, consultez le [tableau 8-3](#)).
 3. Dans l'onglet **Heure**, depuis la liste déroulante **Heure**, sélectionnez une périodicité de lancement de la tâche et paramétrez l'heure selon la périodicité sélectionnée (cette procédure est similaire à la configuration de l'heure dans la planification du poste), voir ci-dessus le paragraphe [Edition de la planification des lancements automatiques des tâches sur le poste](#)).
 4. Cliquez sur le bouton **Sauvegarder**.

Tableau 8-3. Types de tâches et leurs paramètres

Type de tâche	Paramètre et son description
Exécution de la procédure	Il faut spécifier le nom de la procédure dans le champ Nom . Le nom de la procédure doit correspondre au nom du script exécutable d'utilisateur lua-script (sans extension) se trouvant dans le dossier <code>var/extensions</code> du répertoire d'installation du Serveur (voir aussi la description des script dans le dossier <code>var/extensions</code> , décrite dans l' Annexe M).



Type de tâche	Paramètre et son description
Arrêt	Pour arrêter le Serveur . Aucun paramètre supplémentaire n'est requis.
Redémarrage	Pour redémarrer le Serveur . Aucun paramètre supplémentaire n'est requis.
Démarrage	Dans le champ Chemin , il faut spécifier le chemin vers le fichier exécutable du programme exécuté à l'heure spécifiée, dans le champ Arguments — les paramètres de la ligne de commande relatifs au lancement du programme. Cochez la case Exécuter simultanément pour effectuer la synchronisation avec le Serveur — attendre la fin du programme avant l'exécution d'autres tâches de type Démarrage . Si la case Exécuter simultanément n'est pas cochée, le Serveur lance le programme et n'écrit dans le journal que son lancement. Si la case Exécuter simultanément est cochée, le Serveur écrit dans le journal son lancement, le code de retour et l'heure de la fin du programme.
Avertissement sur l'expiration de la licence	Il faut spécifier une période jusqu'à l'expiration de la licence, durant laquelle l'avertissement sur l'expiration de la licence Dr. Web (licence de Serveur , ainsi que celle d' Agent) sera affiché.
Mise à jour	Pour plus d'information, voir le paragraphe Mise à jour selon la planification .
Journalisation	Il faut spécifier le texte du message à écrire dans le journal.
Backup de données critiques du Serveur	Les tâches sont destinées à créer une copie de sauvegarde des données critiques du Serveur (base de données, fichier clé de licence du Serveur, clé privée de chiffrement). Il faut spécifier le chemin vers le répertoire dans lequel les données seront sauvegardées (le chemin vide désigne le répertoire spécifié par défaut) et un nombre maximum de copies de sauvegarde (la valeur 0 enlève la limitation). Pour en savoir plus, voir Annexe H5.5 .
Le poste n'a pas été vu sur le Serveur depuis longtemps	Il faut spécifier une période à l'expiration de laquelle le poste sera classé comme non vu sur le Serveur depuis longtemps, une notification sera envoyée.



Type de tâche	Paramètre et son description
Suppression des événements non envoyés	Il faut spécifier une période à l'expiration de laquelle les événements non envoyés seront supprimés. Il s'agit des messages envoyés par le Serveur subordonné au Serveur principal. En cas d'échec de transfert d'un événement, il sera inscrit dans la liste des non envoyés. Le Serveur subordonné avec une périodicité spécifiée va effectuer des tentatives de transmettre l'événement. Lors de l'exécution de la tâche Suppression des événements non envoyés , tous les événements dont la durée de sauvegarde dépasse ou atteint la limite spécifiée seront supprimés.
Suppression des postes périmés	Il faut spécifier la période à l'expiration de laquelle les postes seront classés comme périmés (par défaut 90 jours). Les postes non connectés au Serveur depuis la période spécifiée seront classés comme périmés et supprimés depuis le Serveur .
Suppression des entrées périmées	Il faut spécifier une période à l'expiration de laquelle les données statistiques sur les postes (mais pas les postes mêmes) seront classées comme périmées et supprimées depuis le Serveur . La périodicité de suppression des données statistiques est paramétrée séparément pour chaque type d'entrée.



Les données périmées seront supprimées depuis la base de manière automatique afin de libérer l'espace disque. La période spécifiée par défaut pour les éléments **Suppression des entrées périmées** et **Suppression des postes périmés** est fixée à 90 jours. En cas de valeur inférieure à 90 jours, les statistiques obtenues sur le fonctionnement des composants antivirus sont moins représentatives. L'augmentation de la valeur peut entraîner des besoins accrus en ressources du **Serveur**.



8.4. Gestion du dépôt des produits Dr.Web Enterprise Server

8.4.1. Introduction

Le dépôt des produits de **Serveur Enterprise** est destiné à sauvegarder les échantillons standard du logiciel ainsi que leurs mises à jour depuis les Serveurs de **SGMAJ**.

Pour cela, le dépôt des produits manipule des jeux de fichiers dits *produits*. Chaque produit se trouve dans un sous-dossier séparé du répertoire `repository` se trouvant dans le répertoire `var`, en cas d'installation par défaut, ce dernier est un sous-dossier du répertoire racine du **Serveur**. Les fonctions du dépôt des produits et sa gestion sont réalisées séparément pour chaque produit.

Dans la gestion de la mise à jour, le dépôt des produits utilise la notion de *révision* du produit. La révision correspond à un statut correct des fichiers du produit à un moment donné. Ce statut comprend les noms de fichiers et les sommes de contrôle correspondantes. Chaque révision possède un numéro unique. Le dépôt des produits effectue une synchronisation des révisions du produit de manière suivante :

- a) vers **Serveur Enterprise** depuis le site de mise à jour du produit (via le protocole HTTP),



En cas de version **Serveur 5.0** ou supérieure, quels que soient les paramètres du dépôt des produits pour le **Serveur**, les mises à jour depuis les Serveurs **SGMAJ** ne seront pas fournies.

Pour mettre à jour le **Serveur**, utilisez l'installateur de la version appropriée et effectuez la procédure conformément aux règles décrites dans les paragraphes [Mise à jour de Dr.Web ESS sous OS Windows®](#) ou [Mise à jour de Dr.Web ESS sous OS de la famille UNIX®](#).

- b) entre les divers **Serveur Enterprise** dans une configuration multi-serveurs (conformément à la politique d'échange



adoptée),

- c) depuis **Serveur Enterprise** vers les postes de travail.

Le dépôt des produits permet à l'Administrateur du réseau antivirus de configurer les paramètres suivants :

- ◆ liste des sites de mise à jour lors des opérations de type **a)** ;
- ◆ limitations relatives au jeu de composants à synchroniser de type **a)** (ainsi, l'utilisateur a une possibilité de surveiller uniquement les modifications des catégories de produits dont il a besoin) ;
- ◆ limitation des composants du produit nécessitant une synchronisation de type **c)** (l'utilisateur peut choisir les composants à installer sur les postes) ;
- ◆ passage contrôlé vers les nouvelles révisions (ceci permet de tester le produit avant leur mise en place) ;
- ◆ ajout de ses propres composants vers les produits ;
- ◆ création de nouveaux produits pour lesquels la synchronisation sera effectuée.

A l'heure actuelle, le jeu de produits comprend les produits listés ci-dessous :

- ◆ **Serveur Enterprise**,
- ◆ **Enterprise Agent** (logiciel de l'**Agent**, logiciel antivirus du poste de travail),
- ◆ **Centre de Gestion Dr.Web**,
- ◆ Bases virales.

Pour en savoir plus sur le dépôt des produits, consultez l'[Annexe F. Gestion du dépôt des produits](#).



8.4.2. Statut du dépôt des produits

Pour vérifier le statut du dépôt des produits ou pour mettre à jour les composants du réseau antivirus, sélectionnez l'élément **Administration** du menu principal du **Centre de Gestion**, puis dans la fenêtre qui apparaît, sélectionnez l'élément **Statut du dépôt des produits**.

Dans la fenêtre qui apparaît, sera affichée la liste des composants du réseau antivirus ainsi que les dates des dernières mises à jour et les statuts actuels.

Pour vérifier la disponibilité des mises à jour et télécharger les mises à jour des composants disponibles depuis les serveurs de **SGMAJ**, cliquez sur le bouton **Vérifier les mises à jour**.

8.4.3. Editeur de configuration du dépôt des produits

L'éditeur de configuration du dépôt des produits permet de configurer les paramètres généraux du dépôt pour tous les produits.



Après l'édition des paramètres du dépôt des produits, il est nécessaire de mettre à jour les composants du réseau antivirus afin de réaliser une modification du statut du dépôt conformément aux paramètres spécifiés.


Afin d'éditer la configuration du dépôt des produits, sélectionnez l'élément **Administration** du menu principal du **Centre de Gestion**, puis dans la fenêtre qui apparaît, sélectionnez l'élément du menu de gestion **Configuration du dépôt des produits**.

Configuration du SGMAJ Dr.Web

L'onglet **BCO Dr.Web** permet de configurer les paramètres du **Système Global de Mises à jour**.




Le Centre de Gestion vous permet de réaliser les opérations suivantes :

- ◆ Supprimer un Serveur dans la liste. Pour cela, sélectionnez un ou plusieurs Serveurs et depuis la barre d'outils cliquez sur le bouton **Supprimer les Serveurs dans la liste** .



Pour sélectionner plusieurs Serveurs, utilisez les touches CTRL ou SHIFT.

- ◆ Ajouter un Serveur à la liste. Pour cela, cliquez sur le bouton **Créer un Serveur**  depuis la barre d'outils et configurez les paramètres du Serveur conformément à la procédure décrite ci-dessous.
- ◆ Configurer un Serveur proxy. Pour cela, cochez la case **Utiliser un Serveur proxy** (les paramètres du proxy sont analogues aux paramètres des Serveurs de mises à jour).
- ◆ Configurer l'adresse du Serveur et les paramètres d'authentification de l'utilisateur. Pour cela, cliquez sur l'icône du Serveur.

En cas de paramétrage ou ajout d'un Serveur, la fenêtre de configuration du Serveur s'ouvrira.

Pour configurer les paramètres du Serveur de mise à jour :

1. Cliquez sur l'icône du Serveur correspondant.
2. Dans les champs respectifs, spécifiez l'adresse et le port du **Serveur**.
3. Dans les champs **Utilisateur** et **Mot de passe** vous pouvez spécifier le nom d'utilisateur et le mot de passe pour l'authentification sur le Serveur de mise à jour. Dans le cas où aucune procédure d'authentification n'est requise, laissez ces champs vides.
4. Pour sauvegarder les modifications apportées, cliquez sur le bouton **Sauvegarder**.



Vous pouvez également configurer toutes les connexions aux Serveurs de mises à jour via le Serveur proxy.

Afin d'ajouter un serveur proxy :

1. Cochez la case **Utiliser un serveur proxy**.
2. Dans la fenêtre de configuration du Serveur proxy qui apparaît, configurez les paramètres de manière analogue au paramétrage du Serveur de mise à jour.
3. Cliquez sur le bouton **Ajouter**.
4. Cliquez sur le bouton **Sauvegarder**.



Lors de la configuration du Serveur proxy, veuillez faire attention au type d'authentification utilisé.

La version actuelle de **Dr.Web Enterprise Security Suite** ne supporte que l'authentification HTTP de base, l'authentification HTTP proxy et l'authentification RADIUS.

Pour déconnecter le Serveur de mise à jour du Serveur proxy, décochez la case **Utiliser un serveur proxy**.

Configuration des mises à jour de Dr.Web Enterprise Agent

La configuration de la mise à jour du dépôt des produits pour le logiciel de l'**Agent** et le package antivirus est effectuée de manière différente en fonction de la version d'OS sous laquelle sera installé le logiciel :

- ◆ Sur l'onglet **Dr.Web Enterprise Agent pour Windows**, dans la section des boutons de sélection, indiquez si vous souhaitez mettre à jour tous les composants à installer sur les postes tournant sous l'OS Windows ou les bases virales seulement.
- ◆ Sur l'onglet **Dr.Web Enterprise Agent pour Unix**, dans la section des boutons de sélection, spécifiez les OS de la famille UNIX nécessitant une mise à jour des composants à installer sur les postes de travail.



Configuration des mises à jour de Dr.Web Enterprise Server

L'onglet **Dr.Web Enterprise Server** offre un jeu de cases permettant de spécifier les OS nécessitant une mise à jour des fichiers du **Serveur** : respectivement pour Windows, UNIX, pour les deux types d'OS ou pour aucun des OS disponibles.



Pour les versions du **Serveur 5.0** ou supérieures, quels que soient les paramètres décrits ci-dessus, les mises à jour depuis des serveurs de **SGMAJ** ne seront pas fournies.

Pour mettre à jour le **Serveur**, utilisez l'installateur de la version adéquate et effectuez la procédure de mise à jour conformément aux règles décrites dans les paragraphes [Mise à jour de Dr.Web ESS pour OS Windows®](#) ou [Mise à jour de Dr.Web ESS pour OS de la famille UNIX®](#).

8.5. Particularités du réseau avec plusieurs Serveurs Dr.Web Enterprise Server

Dr.Web Enterprise Security Suite permet de créer un réseau antivirus avec plusieurs **Serveur Enterprise**. Ainsi, chaque poste est associé à un certain **Serveur** ce qui permet de répartir la charge entre eux.

Les liaisons entre les **Serveurs** peuvent avoir une structure hiérarchique assurant une répartition optimum de la charge.



A l'étape de planification de la structure du réseau antivirus, il faut prendre en compte les particularités de licensing du réseau avec plusieurs **Serveurs**. Pour en savoir plus, consultez le paragraphe [Fichiers clés](#).



Pour les échanges d'information entre les **Serveurs** (les mises à jour des fichiers des composants et les informations sur le fonctionnement des **Serveurs** et des postes connectés) le *protocole spécialisé de synchronisation entre serveurs* est utilisé.

La particularité la plus importante du protocole est la rapidité de transmission des mises à jour.

Ce protocole offre les avantages suivants :

- ◆ transmission des mises à jour dès leur réception,
- ◆ Il n'est pas nécessaire de configurer la planification des mises à jour sur le **Serveur** (excepté les **Serveurs** recevant les mises à jour depuis les Serveurs du **SGMAJ Dr.Web** via le protocole HTTP).

8.5.1. Structure du réseau avec plusieurs serveurs Dr.Web Enterprise Server

Le réseau antivirus permet d'installer plusieurs **Serveurs Enterprise**. Ainsi, chaque **Enterprise Agent** se connecte à un des **Serveurs**. Chaque **Serveur** avec des postes antivirus connectés représente un réseau antivirus, comme il est décrit ci-dessus.

Dr.Web Enterprise Security Suite permet de lier ces réseaux antivirus afin d'établir des échanges d'information entre les **Serveurs Enterprise**.

Dr.Web Enterprise Server peut transmettre à un autre serveur Dr.Web Enterprise Server les informations suivantes :

- ◆ mises à jour du logiciel et des bases virales. Seul un des deux serveurs va recevoir des mises à jour depuis les Serveurs de **SGMAJ Dr.Web** ;



Nous recommandons d'ajouter dans la planification du serveur subordonné **Serveur Enterprise** une tâche de mise à jour depuis les Serveurs de **SGMAJ** pour le cas où le **Serveur** principal est indisponible. Ceci permet aux **Agents** de recevoir les mises à jour des bases virales et des modules (voir aussi le paragraphe [Editeur de configuration du dépôt des produits](#)).

- ◆ informations sur les événements viraux, statistiques relatives au fonctionnement etc.

Dr.Web Enterprise Security Suite comprend deux types de liens entre les Serveurs Dr.Web Enterprise Server :

- ◆ *lien de type supérieur-subordonné*, dans ce cas-là, le supérieur transfère les mises à jour au subordonné et reçoit des informations sur les événements,
- ◆ *lien entres les égaux*, dans ce cas, les directions de la transmission ainsi que les types d'information à transmettre sont paramétrés de manière personnalisée.

La [figure 8-1](#) présente un exemple de la structure réseau avec plusieurs **Serveurs**.

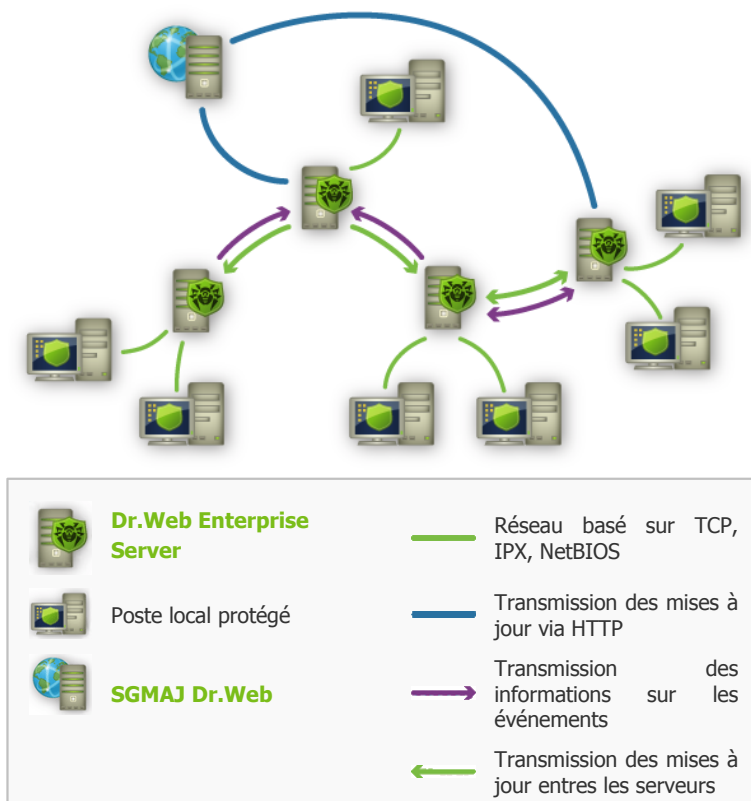


Figure 8-1. Réseau avec plusieurs Serveurs

Certains avantages du réseau avec plusieurs Serveurs Dr.Web Enterprise Server :

- ◆ possibilité de recevoir les mises à jour depuis les Serveurs **SGMAJ Dr.Web** via l'un des **Serveurs Enterprise** afin de les transmettre ultérieurement vers d'autres **Serveurs** sans intermédiaire,
- ◆ possibilité de répartir les postes de travail sur plusieurs **Serveurs** afin de minimiser la charge sur chacun d'entre eux,



- ◆ stockage des informations provenant de plusieurs **Serveurs** sur un seul serveur, ce qui permet d'afficher ces informations via le **Centre de Gestion** de manière consolidée.



Dr.Web Enterprise Security Suite surveille la communication des informations en évitant les échanges répétitifs des mêmes statistiques.

8.5.2. Configuration des liaisons entre serveurs Dr.Web Enterprise Server

Pour configurer un réseau avec plusieurs **Serveurs**, il est nécessaire de configurer des liaisons entre eux.

Il est recommandé en premier lieu de planifier et de mettre sur papier la structure du réseau antivirus ainsi que de bien déterminer tous les flux d'information et de désigner les liaisons de type "entre les égaux" et ceux de type "principal-subordonné". Puis pour chaque **Serveur** faisant partie du réseau, il est nécessaire de configurer des liaisons avec n'importe quel **Serveur** "voisin"- le serveur avec lequel il est lié au moins par un flux d'information.

Exemple de configuration d'une connexion entre serveurs supérieur et subordonné Dr.Web Enterprise Server :



Les champs marqués par le symbole * sont obligatoires à remplir.

1. Assurez-vous que les deux **Serveurs Enterprise** sont opérationnels.
2. Assurez-vous que les deux **Serveurs Enterprise** utilisent des clés `enterprise.key` différentes.
3. Depuis le **Centre de Gestion**, connectez-vous à chaque **Serveur Enterprise** et attribuez-lui un nom mnémorique afin d'éviter d'éventuelles erreurs lors des manipulations nécessaires à la connexion et à la gestion. Pour cela, allez dans




le menu du **Centre de Gestion Administration** → **Configuration de Dr.Web Enterprise Server**, à l'onglet **Général**, dans le champ **Nom**. Dans cet exemple, le nom du **Serveur** supérieur est `MAIN`, le nom du serveur supplémentaire qui lui sera subordonné est `AUXILIARY`.

4. Sur les deux **Serveurs Enterprise**, activez le protocole serveur. Pour cela, dans le menu du **Centre de Gestion**, sélectionnez l'élément **Administration** → **Configuration de Dr.Web Enterprise Server**, puis dans l'onglet **Modules**, cochez la case **Dr.Web Enterprise Server** (voir le paragraphe [Configuration de Dr.Web Enterprise Server](#)).



En cas de protocole serveur non activé, lors de la création d'une nouvelle liaison dans le **Centre de Gestion**, un message sur la nécessité d'activer le protocole s'affichera ainsi que le lien vers la rubrique correspondante du **Centre de Gestion**.

5. Redémarrez les deux **Serveurs Enterprise**.
6. Connectez le **Centre de Gestion** au **Serveur** subordonné (`AUXILIARY`) puis ajoutez le **Serveur** principal (`MAIN`) dans la liste des **Serveurs** voisins du **Serveur** subordonné. Pour cela, sélectionnez l'élément **Liaisons** dans le menu principal. La fenêtre affichant l'arborescence des **Serveurs** dans le réseau antivirus s'ouvrira. Pour ajouter le **Serveur** dans la liste, cliquez sur le bouton **Créer une liaison**  depuis la barre d'outils.

La fenêtre Nouvelle liaison relative aux liaisons entre le **Serveur** actuel et celui à ajouter s'affichera (voir [fig. 8-2](#)). Sélectionnez le type **Principal**. Dans le champ **Nom**, saisissez le nom du **Serveur** principal (`MAIN`), dans le champ **Mot de passe**, spécifiez un mot de passe pour accéder au **Serveur** principal. Cliquez sur le bouton **Parcourir** contre le champ **Clé** et spécifiez la clé `drwcsd.pub` correspondant au **Serveur** principal ; dans le champ **Adresse**, saisissez l'adresse du **Serveur** principal.



Il est possible de rechercher la liste des **Serveurs** accessibles dans le réseau. Pour cela :

- a) Cliquez sur la flèche se trouvant à droite du champ **Adresse**.
- b) Dans la fenêtre qui apparaît, spécifiez une liste des réseaux au format suivant : séparés par un trait d'union (par exemple, 10.4.0.1-10.4.0.10), par une virgule ou un espace (par exemple, 10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90), en utilisant le préfixe réseau (par exemple, 10.4.0.0/24).
- c) Cliquez sur le bouton. La recherche des **Serveurs** accessibles dans le réseau sera commencée.
- d) Sélectionnez un **Serveur** dans la liste des **Serveurs** accessibles. Son adresse sera entrée dans le champ **Adresse** pour créer une liaison.

Dans le champ **Adresse de la console d'administration**, vous pouvez saisir l'adresse de la page d'accueil du **Centre de Gestion** pour le Serveur principal (voir le paragraphe [Centre de Gestion Dr.Web](#)).

Les cases dans les rubriques **Mises à jour** et **Événements** sont configurées conformément au principe de liaison *principal-subordonné* et ne doivent pas être modifiées :

- ◆ le **Serveur** principal envoie les mises à jour vers les **Serveur** subordonnés ;
- ◆ le **Serveur** principal reçoit les informations des **Serveurs** subordonnés.

Cliquez sur le bouton **Sauvegarder**.



Nouvelle liaison Sauvegarder

Généraux

Type
 Principal
 Subordonné
 Egal

Nom

Mot de passe*

Clé* Où aller...

Adresse* ▼

Adresse de la console d'administration

Configuration de la connexion ▼

Mises à jour Recevoir Envoyer

Événements Recevoir Envoyer

Figure 8-2.

Ainsi, le **Serveur** principal (MAIN) sera inclus dans les dossiers **Principaux** et **Hors ligne** (voir [fig. 8-3](#)).

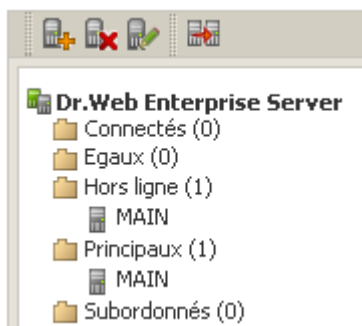



Figure 8-3.



7. Connectez le **Centre de Gestion** au **Serveur** principal (MAIN) et ajoutez le **Serveur** subordonné (AUXILIARY) dans la liste des **Serveurs** voisins du **Serveur** principal. Pour cela, sélectionnez l'élément **Liaisons** dans le menu principal. La fenêtre affichant l'arborescence des **Serveurs** voisins se trouvant dans le réseau antivirus s'ouvrira. Pour ajouter le Serveur dans la liste, cliquez sur le bouton **Créer une liaison**  depuis la barre d'outils.

Dans la fenêtre qui apparaît (voir [fig. 8-4](#)), sélectionnez le type **Subordonné**. Dans le champ **Nom** entrez le nom du **Serveur** subordonné (AUXILIARY), puis dans le champ **Mot de passe**, saisissez le mot de passe spécifié à l'étape 6. Cliquez sur le bouton **Parcourir** contre le champ **Clé** et spécifiez la clé `drwcsd.pub` relative au **Serveur** subordonné.

Dans le champ **Adresse de la console d'administration**, vous pouvez saisir l'adresse de la page d'accueil du **Centre de Gestion** pour le **Serveur** subordonné (voir le paragraphe [Centre de Gestion Dr.Web](#)).

Les cases dans les rubriques **Mises à jour** et **Événements** sont configurées conformément au principe de liaison *principal-subordonné* et ne doivent pas être modifiées :

- ◆ le **Serveur** subordonné reçoit les mises à jour du **Serveur** principal ;
- ◆ le **Serveur** subordonné envoie des informations sur les événements vers le **Serveur** principal.

Cliquez sur le bouton **Sauvegarder**.



Nouvelle liaison Sauvegarder

Généraux

Type	<input type="radio"/> Principal <input checked="" type="radio"/> Subordonné <input type="radio"/> Egal
Nom	AUXILIARY
Mot de passe*	●●●●●●●●
Clé*	D:\Distr\ES\drwcsd.pub Oùsop...
Adresse	
Adresse de la console d'administration	
Configuration de la connexion	Toujours connecté
Mises à jour	<input checked="" type="checkbox"/> Recevoir <input type="checkbox"/> Envoyer
Événements	<input type="checkbox"/> Recevoir <input checked="" type="checkbox"/> Envoyer

Figure 8-4.

Ainsi, le **Serveur** subordonné (AUXILIARY) sera inclus dans les dossiers **Principaux** et **Hors ligne** (voir [fig. 8-5](#)).

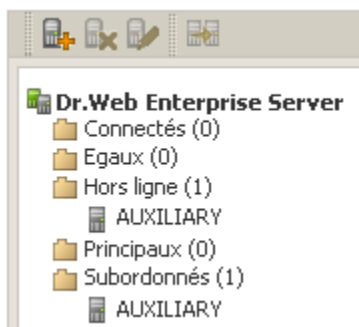


Figure 8-5.

8. Patientez pendant que la connexion entre les **Serveurs** s'établit (cela prend une minute au maximum). Pour vérifier la connexion, actualisez périodiquement l'arborescence des



Serveurs avec la touche F5. Dès que la connexion est établie, le **Serveur** subordonné (AUXILIARY) passe depuis le dossier **Hors ligne** vers le dossier **Connectés** (voir. [fig. 8-6](#)).

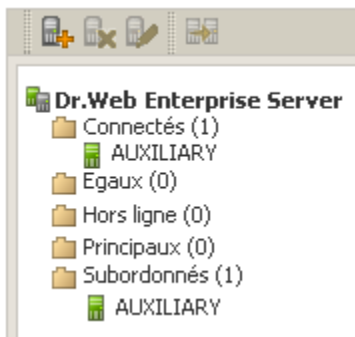


Figure 8-6.

9. Connectez le **Centre de Gestion** au **Serveur subordonné** (AUXILIARY) et assurez-vous que le **Serveur principal** (MAIN) est bien connecté au serveur subordonné (AUXILIARY) (voir [fig. 8-7](#)).

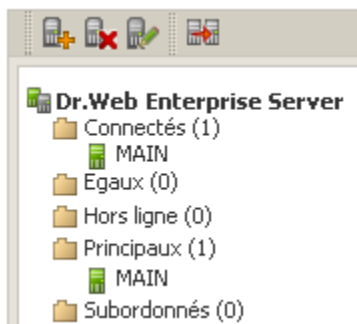


Figure 8-7.



Il est impossible de relier deux **Serveurs** ayant la même clé de licence (enterprise.key).



Il est impossible de lier plusieurs **Serveurs** ayant la même paire de paramètres : mot de passe et clé publique de chiffrement `drwcsd.pub`.




Lors de la création d'une liaison entre les **Serveurs** égaux, il est recommandé de spécifier l'adresse du **Serveur** à ajouter uniquement dans la configuration de l'un des deux serveurs.

Cela n'a pas d'impact sur l'interaction entre les **Serveurs** mais permet d'éviter les entrées de type `Link with the same key id is already activated` dans le journal du fonctionnement des **Serveurs**.

Il est impossible d'établir une connexion entre les Serveurs Dr.Web Enterprise Server dans les cas suivants :

- ◆ Problème de connexion via le réseau.
- ◆ Adresse invalide du **Serveur** principal spécifiée lors de la configuration de la connexion.
- ◆ Clé de chiffrement `drwcsd.pub` invalide sur un des **Serveurs**.
- ◆ Mot de passe invalide sur un des **Serveurs** (les mots de passe ne correspondent pas aux **Serveurs** à lier).
- ◆ La même clé de licence `enterprise.key` sur les deux **Serveurs**.
- ◆ La clé de licence `enterprise.key` du **Serveur** subordonné à connecter coïncide avec la clé de licence du **Serveur** subordonné qui est déjà connecté au même **Serveur** principal.



Lors de la création des liaisons entre les **Serveurs**, il est possible de spécifier une limitation des mises à jour pour les **Serveurs** à lier. Pour cela, à la création d'une liaison, dans l'élément **Restriction des mises à jour**, cliquez sur le bouton . La fenêtre d'édition des modes des mises à jour s'ouvrira. Pour en savoir plus, consultez le paragraphe [Restrictions des mises à jour](#).



8.5.3. Utilisation du réseau antivirus avec plusieurs serveurs Dr.Web Enterprise Server

Une des particularités du réseau à plusieurs **Serveurs** consiste en l'obtention des mises à jour depuis le **SGMAJ Dr.Web** via une partie des **Serveurs Enterprise** (en général, un ou plusieurs **Serveurs** principaux). Dans ce cas, la planification de la tâche de mise à jour ne doit être configurée que sur les **Serveurs** concernés (voir le paragraphe [Configuration de la planification de Dr.Web Enterprise Server](#)). Tout **Serveur** recevant des mises à jour depuis les Serveurs de **SGMAJ Dr.Web** ou depuis un autre **Serveur**, les transmet immédiatement à tous les **Serveurs** pour lesquels cette option est configurée (vers tous les serveurs subordonnés ainsi que vers les serveurs égaux pour lesquels l'option permettant de recevoir les mises à jour est configurée de manière explicite).






Dr.Web Enterprise Security Suite surveille de manière automatique les situations où une planification incorrecte de la topologie du réseau ainsi que des erreurs de configuration des **Serveurs** peuvent entraîner un double envoi de la même mise à jour (déjà réceptionnée depuis d'autres sources) vers le même **Serveur** à la place d'une nouvelle mise à jour.

L'administrateur peut également recevoir des informations récapitulatives sur les événements viraux importants survenant sur les fragments du réseau liés à tel ou tel **Serveur**, via des liaisons entre serveurs (par exemple, dans la configuration décrite ci-dessus "un serveur principal, les autres - subordonnés", ces informations sont stockées sur le **Serveur** principal).

Marche à suivre pour consulter les informations sur les événements viraux sur tous les Serveurs Dr.Web Enterprise Server liés au serveur sélectionné :

1. Sélectionnez l'élément **Liaisons** du menu principal du **Centre de Gestion**.



2. Dans la fenêtre qui apparaît, depuis la rubrique **Tableaux** sélectionnez l'élément **Rapport récapitulatif** pour afficher des informations sur le nombre total d'entrées relatives aux événements survenus sur les **Serveurs** voisins. Dans le tableau contenant les statistiques sur les **Serveurs** voisins, les données sont affichées par les rubriques suivantes :
 - ◆ **Infections** – infections détectées sur les postes connectés aux **Serveurs** voisins.
 - ◆ **Erreurs** – erreurs de scan.
 - ◆ **Statistiques** – statistiques sur les infections détectées.
 - ◆ **Démarrage/Arrêt** – démarrage et arrêt des tâches de scan sur les postes.
 - ◆ **Statut** – statut du logiciel antivirus sur les postes.
 - ◆ **Toutes les installations via réseau** – installations des **Agents** via le réseau.
3. Pour passer à la page contenant des informations détaillées sur les événements survenus sur les **Serveurs** voisins, depuis le tableau affiché dans la rubrique **Rapport récapitulatif**, cliquez sur le chiffre représentant un nombre d'entrées relatif à l'événement donné.
4. Pour passez aux tableaux affichant les données sur les événements survenus sur les **Serveurs** voisins, sélectionnez un élément nécessaire (voir étape 2) dans la rubrique **Tableaux** du menu de gestion.
5. Pour consulter les informations relatives à une période donnée, vous pouvez sélectionner depuis la liste déroulante une période par rapport à la date courante ou choisir depuis la barre d'outils une plage de dates nécessaire. Pour spécifier une plage de dates, saisissez les dates correspondantes ou cliquez sur l'image représentant un calendrier contre le champ de date. Pour télécharger des données, cliquez sur **Actualiser**.
6. Pour sauvegarder le tableau (pour l'imprimer ou le traiter ultérieurement), cliquez sur le bouton  **Sauvegarder les données vers un fichier CSV**, ou sur  **Sauvegarder les données vers un fichier HTML** ou sur  **Sauvegarder les données vers un fichier XML**.



8.5.4. Fonctionnement de plusieurs Serveurs Dr.Web Enterprise Server avec une seule BD

Les conditions à respecter obligatoirement lors de la création d'un réseau antivirus contenant plusieurs **Serveurs Enterprise** et une seule Base de données :

1. Tous les **Serveurs** doivent avoir les mêmes clés de chiffrement `drwcsd.pub`, `drwcsd.pri`, les certificats `certificate.pem`, `private-key.pem` et la clé Agent `agent.key`.
2. Le fichier de configuration du **Centre de Gestion** `webmin.conf` doit contenir le même nom DNS de Serveur pour tous les **Serveurs**, ce nom doit être écrit dans le paramètre `ServerName`.
3. Le nom commun du cluster doit être enregistré sur le Serveur DNS dans le réseau pour chaque Serveur séparément et la méthode de répartition de la charge doit être spécifiée.
4. Chaque **Serveur** doit avoir sa clé `enterprise.key` avec l'identificateur unique `ID1`.
5. Dans les fichiers de configuration des **Serveurs** `drwcsd.conf`, pour tous les **Serveurs**, une BD externe commune doit être spécifiée.
6. Les tâches **Purge Old Data**, **Prepare and send fiscal report periodic job**, **Backup sensitive data**, **Purge old stations**, **Purge expired stations**, **Purge old data**, **Purge unsent IS events** doivent être présentes dans la planification sur un seul **Serveur** (le plus performant si les configurations des serveurs ne sont pas les mêmes).



Chapitre 9. Mise à jour de Dr.Web Enterprise Security Suite et de ses composants



Avant de procéder à la mise à jour de **Dr.Web ESS** et de ses composants, il est fortement recommandé de vérifier les paramètres du protocole TCP/IP relatifs à l'accès à Internet. Le service DNS doit notamment être actif et correctement configuré.

Vous pouvez mettre à jour les bases virales et le logiciel de manière manuelle ainsi que selon la planification des tâches du **Serveur** et de l'**Agent**.



Avant la mise à jour du logiciel, il est recommandé de configurer le dépôt des produits y compris l'accès à **SGBD Dr.Web** (voir [Editeur de configuratino du dépôt des produits](#)).

9.1. Mise à jour de Dr.Web Enterprise Security Suite

9.1.1. Mise à jour de Dr.Web Enterprise Server pour OS Windows®

Le logiciel du **Serveur** peut être mis au niveau vers la version **6.0.4** par l'un des deux biais :

1. [Automatiquement](#). La mise à niveau du **Serveur** en version **5.0** ou **6.0.0** se fait automatiquement avec les outils de l'installateur.



Seuls les **Serveurs** ayant la même architecture peuvent être mis à jour de manière automatique.

Dans le cas contraire, il est nécessaire de supprimer l'ancien **Serveur** et d'installer le nouveau **Serveur manuellement**.

2. **Manuellement**. En cas de mise à niveau du **Serveur** depuis les versions **4.XX**, **6.0.2** ou supérieures, il est nécessaire de supprimer manuellement le **Serveur** antérieur et d'installer le nouveau **Serveur**.

Sauvegarde des fichiers de configuration

En cas de suppression manuelle du **Serveur** ou lors de la mise à jour du **Serveur** avec l'installateur, les fichiers listés ci-après seront sauvegardés automatiquement :

Fichier	Description	Répertoire par défaut
dbinternal.dbs	BD interne	var
drwcsd.conf (peut avoir un autre nom)	fichier de configuration du Serveur	etc
drwcsd.pri	clé privée de chiffrement	
drwcsd.pub	clé publique de chiffrement	<ul style="list-style-type: none">• Installer• webmin\install
enterprise.key (peut avoir un autre nom)	clé de licence du Serveur	etc
agent.key (peut avoir un autre nom)	clé de licence de l' Agent	
certificate.pem	certificat pour SSL	
private-key.pem	clé privée RSA	



Si nécessaire, sauvegardez d'autres fichiers importants dans un répertoire différent de celui d'installation du **Serveur**, notamment le fichier de configuration du **Centre de Gestion** `webmin.conf` et les fichiers contenant les template des rapports qui se trouvent dans le dossier `\var\templates`.

Sauvegarde de la base de données

Avant la mise à jour de **Dr.Web Enterprise Security Suite**, il est recommandé de réaliser une copie de sauvegarde de la base de données.

Pour sauvegarder la base de données :

1. Arrêter le **Serveur**.
2. Exportez la base de données vers le fichier :

```
"C:\Program Files\DrWeb Enterprise Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Enterprise Server" -var-root="C:\Program Files\DrWeb Enterprise Server\var" -verbosity=all exportdb <dossier_de_copie_de_sauvegarde>\esbase.es
```

Pour les **Serveurs** utilisant une base de données externe, il est recommandé d'utiliser les outils standard fournis avec la base de données.



Assurez-vous que l'exportation de la base de données **Dr.Web ESS** a réussi. Sans avoir une copie de sauvegarde de la BD, vous ne pourrez pas restaurer le **Serveur** en cas imprévu.



Notes importantes



A partir de la version **5.0**, le package antivirus **Dr.Web Enterprise Security Suite** inclut les produits **SpIDER Gate** et **Office Control**. Afin d'utiliser ces produits, il convient de posséder la licence appropriée (**Antivirus +Antispam**). Si les produits ne sont pas mentionnés dans la licence, il est recommandé d'effectuer les procédures décrites [ci-dessous](#).

Lorsqu'un **Agent** dont l'autoprotection est activée tourne sur un ordinateur avec **Serveur Enterprise**, un avertissement sur l'activité du composant d'autoprotection **Dr.Web SelfPROtect** sera affiché durant la mise à jour du logiciel et **Serveur**, désactivez ce composant à l'aide des paramètres de l'**Agent**.

Dans le cas où vous utilisez la BD ODBC pour Oracle en tant que base externe, lors de la mise à jour (ou en cas de réinstallation) du **Serveur**, sélectionnez l'élément **Installation sélective** dans les paramètres de l'installateur. Dans la fenêtre suivante, refusez l'installation du client intégré pour SGBD Oracle (dans la rubrique **Database support - Oracle database driver**).

Sinon l'utilisation de la BD Oracle via ODBC ne sera pas possible à cause du conflit des bibliothèques.

Mise à niveau automatique du serveur Dr.Web Enterprise depuis les versions 5.0 et 6.0.0

La mise à niveau du logiciel de **Serveur** depuis la version **5.0** ou **6.0.0** vers la version **6.0.4** se fait automatiquement avec des outils de l'installateur.



Pour mettre à jour Dr.Web Enterprise Server, lancez l'installateur et suivez les instructions de l'assistant d'installation :

1. Lors de la mise à jour, la fenêtre **Dr.Web Enterprise Server - notification de mise à jour** vous informera que le logiciel **Serveur** est dans une version antérieure. L'installateur va définir de manière automatique le répertoire d'installation du **Serveur**.
2. Durant les étapes suivantes, l'assistant d'installation va afficher les chemins vers les fichiers du **Serveur** en version antérieure (voir [ci-dessus](#)) qui seront utilisés lors de l'installation du **Serveur** en version **6.0.4**. Si nécessaire, vous pouvez modifier les chemins trouvés par l'installateur de manière automatique.

En cas d'utilisation de la base de données externe du **Serveur**, lors de la mise à jour, sélectionnez aussi la variante **utiliser la base de données existante**. Lors de la sélection ultérieure de fichier de configuration du **Serveur** et de clé privée de chiffrement, la mise à jour sera réalisée automatiquement.

3. Afin de procéder à la suppression du **Serveur** en version antérieure et à l'installation du **Serveur** en version **6.0.4**, cliquez sur le bouton **Installer**.



Lors de la procédure de mise à jour du logiciel **Serveur**, le contenu du dépôt des produits sera supprimé et sa nouvelle version sera installée.

Si, pour une raison quelconque, lors de la mise à niveau du **Serveur** depuis la version **5.0** ou plus ancienne, le dépôt des produits en version périmée a été sauvegardé, il est nécessaire de supprimer manuellement tout le contenu du dépôt et de réaliser sa mise à jour complète.

En cas de configuration multi-serveur du réseau antivirus, seules les bases virales seront transmises depuis le **Serveur** principale en version **6.0.4** vers les **Serveurs** subordonnées en version **5.0** ou plus ancienne.

Afin de pouvoir transmettre les mises à jour de tout le logiciel, il faut migrer le **Serveur** subordonné vers la version **6.0.4** (pour assurer la compatibilité des structures de dépôt des produits).

Après la mise à niveau du Serveur Dr.Web Enterprise vers la version 6.0.4, il est recommandé de réaliser les actions suivantes :

Après la mise à jour de **Dr.Web Enterprise Server** selon le [schéma général](#), il est nécessaire de réaliser les opérations requises pour le fonctionnement du **Centre de Gestion** :

1. Vider le cache du navigateur web utilisé pour se connecter au **Centre de Gestion**.
2. [Mettre à jour](#) le module ajoutable **Dr.Web Browser-Plugin**.

Mise à niveau manuelle de Dr.Web Enterprise Server depuis les versions 4.XX, 6.0.2 ou supérieures

La mise à niveau du logiciel de **Serveur** depuis les versions **4.XX**, **6.0.2** ou supérieures avec l'installateur du **Serveur Enterprise 6.0.4** n'est pas supportée. Pour passer vers la version **6.0.4**, vous devez supprimer manuellement le **Serveur** installé et puis installer le



nouveau **Serveur**.

Marche à suivre pour mettre à jour Dr.Web Enterprise Server :

1. Arrêtez le **Enterprise Server** (voir [Démarrage et arrêt du Dr.Web Enterprise Server](#)).
2. En cas d'utilisation d'une BD externe, sauvegardez la BD avec les outils du Serveur SQL.
3. Si vous souhaitez utiliser ultérieurement des fichiers (à part les [fichiers](#) qui seront sauvegardés automatiquement lors de la suppression du **Serveur**), créez une copie de sauvegarde de manière manuelle (par exemple, les copies des fichiers de template, des rapports etc.).
4. Supprimez le **Serveur**.
5. Installez le nouveau **Serveur** (voir [Installation de Dr.Web Enterprise Server pour OS Windows®](#)). Lors de l'installation du **Serveur**, spécifiez dans les paramètres de l'installateur les [fichiers](#) sauvegardés automatiquement.

Spécifiez l'utilisation d'une nouvelle BD si vous souhaitez utiliser une BD externe.

En cas d'utilisation de la BD interne, spécifiez le fichier sauvegardé de BD `dbinternal.dbs`.

6. Arrêtez le **Serveur**.
7. Dans le cas où vous avez enregistré des fichiers de manière manuelle avant la suppression du **Serveur**, mettez ces fichiers dans les mêmes répertoires que dans la version antérieure du **Serveur**.
8. Pour utiliser une BD externe, restaurez la BD sur le nouveau **Serveur** et spécifiez le chemin vers la BD dans le fichier de configuration `drwcsd.conf`.

Depuis la ligne de commande lancez le fichier `drwcsd.exe` avec la clé `upgradedb` pour mettre la BD à jour. Voici l'apparence de la ligne de commande :

```
"C:\Program Files\DrWeb Enterprise Server\bin
```



```
\drwcsd.exe" upgradedb "C:\Program Files  
\DrWeb Enterprise Server\update-db"
```

9. Lancez le service **Dr.Web Enterprise Server** (voir [Démarrage et arrêt du Dr.Web Enterprise Server](#)).

Lors de la mise à niveau de Dr.Web Enterprise Server depuis la version 4.XX vers la version 6.0.4, il est recommandé de suivre les instructions suivantes :

1. Avant de procéder à la mise à jour, déconnectez les protocoles de l'**Installateur réseau** et de l'**Agent**. Pour cela, sélectionnez l'élément **Administration** du menu principal du **Centre de Gestion**, puis **Configuration de Dr.Web Enterprise Server** et passez ensuite à l'onglet **Modules**. Décochez les cases **Protocole Dr.Web Enterprise Agent** et **Protocole Dr.Web Network Installer** puis cliquez sur **Sauvegarder**.
2. Réalisez une mise à niveau du **Serveur** vers la version **6.0.4** comme il est décrit [ci-dessus](#) (tout en sauvegardant le fichier de configuration du **Serveur**).
3. Après la mise à jour du **Serveur**, configurez la liste des composants à installer sur les postes de travail (voir [Composition du package antivirus](#)). Si vous ne disposez pas de la licence **Antispam**, vous devez spécifier la valeur **ne peut pas** pour les composants **SpIDer Gate** et **Office Control**.
4. Mettez à jour les composants de **Dr.Web ESS**. Pour cela, sélectionnez l'élément **Administration** du menu principal du **Centre de Gestion**, puis sélectionnez **Statut du dépôt des produits**. Pour vérifier la disponibilité des mises à jour sur le Serveur **SGMAJ**, cliquez sur le bouton **Vérifier les mises à jour**. Si nécessaire, configurez les paramètres des Serveurs proxy afin d'effectuer les mises à jour depuis **SGMAJ**.
5. Si nécessaire, éditez les ports via lesquels les **Agents** vont se connecter au **Serveur**. Pour cela, utilisez le menu **Administration** → **Configuration de Dr.Web Enterprise Server** → onglet **Transport**.
6. Activez les protocoles de l'**Installateur réseau** et de l'**Agent**, ils ont été désactivés à l'étape 1.



7. Mettez à jour le logiciel sur les postes de travail.



Après la mise à niveau du **Serveur** en version **4.XX** vers la version **6.0.4**, il est nécessaire que le paramètre **Transport** soit spécifié dans le fichier de configuration du **Serveur** `drwcsd.conf` :

```
Transport "drwcs" "tcp/0.0.0.0:2193"  
"udp/231.0.0.1:2193"
```

`drwcs` est le nom du **Serveur**.

Si le paramètre n'est pas spécifié, ajoutez-le de manière manuelle puis redémarrez le **Serveur**.

9.1.2. Mise à jour de Dr.Web Enterprise Server pour OS UNIX®

La mise à jour du logiciel **Serveur** par-dessus la version installée n'est pas toujours possible pour tous les OS de la famille UNIX. En cas de l'OS de la famille UNIX sous lequel il est impossible de réaliser une mise à jour par-dessus le package installé, il est nécessaire d'abord de supprimer le logiciel de **Serveur** en version antérieure et d'installer ensuite le logiciel en version **6.0.4**.

Sauvegarde des fichiers de configuration

Les fichiers listés ci-dessous seront sauvegardés automatiquement lors de la suppression du **Serveur** :

Fichier	Description	Répertoire par défaut
<code>dbinternal.dbs</code>	BD interne	<ul style="list-style-type: none">pour Linux: <code>/var/opt/drwcs/</code>pour Solaris et FreeBSD: <code>/var/drwcs/</code>
<code>drwcsd.conf</code> (peut avoir un autre nom)	fichier de configuration du Serveur	<ul style="list-style-type: none">pour Linux: <code>/var/opt/drwcs/etc</code>



Fichier	Description	Répertoire par défaut
webmin.conf	fichier de configuration du Centre de Gestion	
common.conf	fichier de configuration (pour certains OS de la famille UNIX)	
enterprise.key (peut avoir un autre nom)	clé de licence du Serveur	• pour Solaris et FreeBSD: /var/drwcs/ etc
agent.key (peut avoir un autre nom)	clé de licence de l'Agent	
certificate.pem	certificat pour SSL	
private-key.pem	clé privée RSA	
drwcsd.pri	clé privée de chiffrement	
drwcsd.pub	clé publique de chiffrement	pour Linux et Solaris: <ul style="list-style-type: none">• /opt/drwcs/Installer/• /opt/drwcs/webmin/install pour FreeBSD: <ul style="list-style-type: none">• /usr/local/drwcs/Installer/• /usr/local/drwcs/webmin/install

Sauvegarde de la base de données

Avant la mise à jour de **Dr.Web Enterprise Security Suite**, il est recommandé de réaliser une copie de sauvegarde de la base de données.

Pour sauvegarder la base de données :

1. Arrêter le **Serveur**.



2. Exportez la base de données vers le fichier :

- ◆ Sous OS FreeBSD :

```
# /usr/local/etc/rc.d/drwcsd.sh exportdb /var/drwcs/etc/esbase.es
```
- ◆ Sous OS Linux :

```
# /etc/init.d/drwcsd exportdb /var/opt/drwcs/etc/esbase.es
```
- ◆ Sous OS Solaris :

```
# /etc/init.d/drwcsd exportdb /var/drwcs/etc/esbase.es
```

Pour les **Serveurs** utilisant une base de données externe, il est recommandé d'utiliser les outils standard fournis avec la base de données.



Assurez-vous que l'exportation de la base de données **Dr.Web ESS** a réussi. Sans avoir une copie de sauvegarde de la BD, vous ne pourrez pas restaurer le **Serveur** en cas imprévu.

Notes importantes



Toutes les opérations relatives à la mise à jour doivent être réalisées en mode administrateur, sous le nom d'administrateur **root**.

En cas de mise à niveau du **Serveur** vers la version **6.0.4** depuis la version **5.0** ou plus ancienne, il est nécessaire de supprimer complètement le dépôt des produits et d'installer sa nouvelle version.

En cas de configuration multi-serveur du réseau antivirus, seules les bases virales seront transmises depuis le **Serveur** principale en version **6.0.4** vers les **Serveurs** subordonnées en version **5.0** ou plus ancienne.

Afin de pouvoir transmettre les mises à jour de tout le logiciel, il faut migrer le **Serveur** subordonné vers la version **6.0.4** (pour assurer la compatibilité des structures de dépôt des produits).



A partir de la version **5.0**, le package antivirus **Dr.Web Enterprise Security Suite** inclut les produits **SpIDer Gate** et **Office Control**, leur utilisation requiert la licence **Antivirus+Antispam**. Si ces produits ne sont pas mentionnés dans votre licence, il est recommandé de réaliser les opérations décrites [ci-dessous](#).

Mise à jour automatique

En cas de mise à niveau du **Serveur** depuis la version **5.0** ou supérieure vers la version **6.0.4** sous **Linux**, au lieu de supprimer la version antérieure et d'installer une nouvelle version du **Serveur**, il est possible de réaliser une mise à niveau du **Serveur** avec les commandes suivantes :

- ◆ pour **rpm** : `rpm -U <nom de package>`
 - ◆ pour **dpkg** : `dpkg -i <nom de package>`
- Lors de la mise à jour des packages deb, le répertoire `/root/drwcs` doit être vide ou absent.

Dans ce cas, tous les [fichiers](#) enregistrés de manière automatique seront mis dans les dossiers appropriés, aucune opération de remplacement manuelle ne sera requise.

Lors de la mise à jour du package au sein des distributions **rpm** pour le **Serveur** en version **5.0** ou **6.0**, si des modifications ont été apportées dans le fichier de configuration du **Centre de Gestion** `webmin.conf` avant la mise à jour du **Serveur**, le fichier `webmin.conf` relatif à la version antérieure sera sauvegardé et un nouveau fichier nommé `webmin.conf.rpmnew` sera créé.

Si vous souhaitez utiliser les fonctions déterminées par les paramètres modifiés du fichier de configuration (entre autres, que l'installateur de l'**Agent** soit accessible à l'adresse http://<server_name>:9080/install, voir [Fichiers d'installation](#)), copiez les paramètres modifiés depuis le fichier ancien vers le nouveau et changez ensuite le nom du nouveau fichier `webmin.conf.rpmnew` pour `webmin.conf` en écrasant le fichier ancien.



Mise à jour manuelle

Marche à suivre pour mettre à jour Dr.Web Enterprise Server en cas d'utilisation de la base de données interne :

1. Arrêtez le **Serveur**.
2. Si vous souhaitez utiliser ultérieurement des fichiers (à part les **fichiers** qui seront sauvegardés automatiquement lors de la suppression du **Serveur** à l'étape **4**), créez leurs copies de sauvegarde de manière manuelle (il s'agit par exemple des fichiers de template des rapports etc.).
3. Supprimez tout le contenu du dépôt des produits.
4. Supprimez le logiciel **Serveur** (voir [Suppression de Dr.Web Enterprise Server pour OS de la famille UNIX®](#)). Il vous sera proposé de sauvegarder de manière automatique les copies des **fichiers**. Pour cela, il suffira de saisir le chemin ou d'accepter le chemin proposé par défaut.
5. Installez **Serveur Enterprise** en version **6.0.4** (voir [Installation Dr.Web Enterprise Server pour OS de la famille UNIX®](#)).
6. Si nécessaire, remplacez les fichiers créés lors de l'installation par les fichiers sauvegardés automatiquement lors de la suppression du **Serveur** en version antérieure. Les fichiers à remplacer se trouvent dans les répertoires suivants :

Fichiers	Chemin pour OS respectif		
	Linux	Solaris	FreeBSD
drwcsd.pub	/opt/drwcs/Installer/ /opt/drwcs/webmin/install		/usr/local/drwcs/ Installer/ /usr/local/drwcs/ webmin/install
dbinternal.dbs	/var/opt/drwcs/	/var/drwcs/	
drwcsd.conf	/var/opt/drwcs/etc	/var/drwcs/etc	



Fichiers	Chemin pour OS respectif		
	Linux	Solaris	FreeBSD
drwcsd.pri enterprise.key agent.key certificate.pem private-key.pem			



Le fichier de configuration du **Centre de Gestion** (`webmin.conf`) en versions plus anciennes que la version **6.0.2** n'est pas compatible avec le logiciel en version **6.0.4**. En cas de réinstallation du **Serveur** depuis une version inférieure à la version **6.0.2**, ce fichier ne sera pas remplacé par une copie automatiquement sauvegardée. Dans ce cas, vous avez à saisir tous les paramètres inscrits dans ce fichier manuellement.

Si vous avez des fichiers sauvegardés de manière manuelle, placez-les dans les mêmes répertoires que ceux dans lesquels ils se trouvaient dans la version antérieure du **Serveur**.



Pour tous les fichiers sauvegardés depuis la version antérieure du **Serveur** (voir l'étape **6**), il faut spécifier, en tant que propriétaire des fichiers, l'utilisateur sélectionné lors de l'installation de la nouvelle version du **Serveur** (par défaut - **drwcs**).

7. Exécutez les commandes suivantes :
 - ◆ pour OS **Linux** et OS **Solaris** :
`/etc/init.d/drwcsd upgradedb`
 - ◆ pour OS **FreeBSD** :
`/usr/local/etc/rc.d/drwcsd.sh upgradedb`
8. Démarrez le **Serveur**.
9. Configurez la mise à jour du dépôt des produits et effectuez sa mise à jour complète.



10. Redémarrez le **Serveur**.

Marche à suivre pour mettre à jour Dr.Web Enterprise Server en cas d'utilisation d'une BD externe :

1. Arrêtez le **Serveur**.
2. Si vous souhaitez utiliser ultérieurement des fichiers (à part les **fichiers** qui seront sauvegardés automatiquement lors de la suppression du **Serveur** à l'étape **4**), créez leurs copies de sauvegarde de manière manuelle (il s'agit par exemple des fichiers de template des rapports etc.).
3. Supprimez tout le contenu du dépôt des produits.
4. Supprimez le logiciel **Serveur** (voir [Suppression de Dr.Web Enterprise Server pour OS de la famille UNIX®](#)). Il vous sera proposé de sauvegarder de manière automatique les copies des **fichiers**. Pour cela, il suffira de saisir le chemin ou d'accepter le chemin proposé par défaut.
5. Installez **Serveur Enterprise** en version **6.0.4** (voir [Installation de Dr.Web Enterprise Server pour OS de la famille UNIX®](#)).
6. Placez les fichiers sauvegardés (voir [ci-dessus](#)) de manière automatique dans les emplacements suivants :

◆ sous **Linux** :

dans le répertoire `/var/opt/drwcs/etc`, excepté la clé `pub` qui est à mettre dans `/opt/drwcs/Installer/` et dans `/opt/drwcs/webmin/install`

◆ sous **FreeBSD** :

dans le répertoire `/var/drwcs/etc`, excepté la clé `pub` qui est à mettre dans `/usr/local/drwcs/Installer/` et dans `/usr/local/drwcs/webmin/install`

◆ sous **Solaris** :

dans le répertoire `/var/drwcs/etc`, excepté la clé `pub` qui est à mettre dans `/opt/drwcs/Installer/` et dans `/opt/drwcs/webmin/install`

Si vous avez des fichiers sauvegardés de manière manuelle, placez-les dans les mêmes répertoires que ceux dans lesquels ils



se trouvaient dans la version antérieure du **Serveur**.



Pour tous les fichiers sauvegardés depuis la version antérieure du **Serveur** (voir l'étape **6**), il faut spécifier, en tant que propriétaire des fichiers, l'utilisateur sélectionné lors de l'installation de la nouvelle version du **Serveur** (par défaut - **drwcs**).

7. Exécutez les commandes ci-dessous :
 - ◆ pour OS **Linux** et OS **Solaris** :
`/etc/init.d/drwcsd upgradedb`
 - ◆ pour OS **FreeBSD** :
`/usr/local/etc/rc.d/drwcsd.sh upgradedb`
8. Démarrez le **Serveur**.
9. Configurez la mise à jour du dépôt des produits et effectuez une mise à jour complète du dépôt.
10. Redémarrez le **Serveur**.

Lors de la mise à niveau de Dr.Web Enterprise Server depuis la version 4.XX vers la version 6.0.4, il est recommandé de réaliser les opérations suivantes :

1. Avant de procéder à la mise à jour, déconnectez les protocoles de l'**Installeur** et de l'**Agent**. Pour cela, sélectionnez l'élément **Administration** du menu principal du **Centre de Gestion**, puis **Configuration de Enterprise Server**, et ouvrez l'onglet **Modules**. Décochez les cases **Protocoles Dr.Web Enterprise Agent** et **Protocole de Dr.Web Network Installer**, cliquez ensuite sur **Sauvegarder**.
2. Réalisez une mise à niveau du **Serveur** vers la version **6.0.4** conformément à la description [ci-dessus](#) (tout en gardant le fichier de configuration du **Serveur**).
3. Après la mise à niveau du **Serveur**, configurez la liste des composants à installer sur les postes de travail (voir [Composition du package antivirus](#)). Si vous ne disposez pas de la licence pour **Antispam**, spécifiez la valeur **ne peut pas** pour les composants **SpIDer Gate** et **Office Control**.
4. Mettez à jour les composants de **Dr.Web ESS**. Pour cela,



sélectionnez l'élément **Administration** du menu principal du **Centre de Gestion**, puis dans la fenêtre qui apparaît, sélectionnez **Statut du dépôt des produits**. Pour vérifier la disponibilité des mises à jour sur le Serveur **SGMAJ**, cliquez sur le bouton **Vérifier les mises à jour**. Si nécessaire, spécifiez d'abord les paramètres des Serveurs proxy pour effectuer les mises à jour depuis **SGBD**.

5. Si nécessaire, éditez les ports via lesquels les **Agents** vont se connecter au **Serveur**.
6. Activez les protocoles de l'**Installateur réseau** et de l'**Agent**, qui ont été désactivés lors de l'étape **1**.
7. Mettez à jour le logiciel sur les postes de travail.



Après la mise à niveau du **Serveur** en version **4.XX** vers la version **6.0.4**, il est nécessaire que le paramètre **Transport** soit spécifié dans le fichier de configuration du **Serveur** `drwcsd.conf` :

```
Transport "drwcs" "tcp/0.0.0.0:2193"  
"udp/231.0.0.1:2193"
```

`drwcs` - nom du **Serveur**.

Si le paramètre n'est pas spécifié, ajoutez-le de manière manuelle et redémarrez ensuite le **Serveur**.

9.1.3. Mise à jour du module ajoutable Dr.Web Browser-Plugin

Pour mettre à jour le module ajoutable **Dr.Web Browser-Plugin** (via le **Centre de Gestion**), il est nécessaire de supprimer la version antérieure du module de manière manuelle et d'installer ensuite le nouveau module **Dr.Web Browser-Plugin**.

Pour en savoir plus sur la suppression du module, consultez les paragraphes [Suppression des composants pour OS Windows®](#), [Suppression de Dr.Web Enterprise Server pour OS de la famille UNIX®](#)

Pour en savoir plus sur la procédure d'installation, consultez le paragraphe [Installation du module ajoutable Dr.Web Browser-Plugin](#).



9.1.4. Mise à jour de l'Dr.Web Enterprise Agent

Après la mise à jour du logiciel **Serveur**, les **Agents** connectés seront mis à jour de manière automatique.



Pour en savoir plus sur la mise à jour des **Agents** installés sur les postes ayant des fonctions importantes de LAN, consultez la rubrique [Mise à jour des Agents sur les serveurs LAN](#).

9.1.5. Mise à jour du Serveur proxy

Mise à jour du serveur proxy sous l'OS Windows

La mise à jour automatique du **Serveur proxy** n'est pas prise en charge.

Lors du démarrage de l'installateur sur l'ordinateur sur lequel le **Serveur proxy** est installé :

- ◆ Si l'installateur ayant le même type de système que le **Serveur proxy** installé démarre, une alerte sur l'installation impossible sera affichée.
- ◆ Si l'installateur lancé a un type de système autre que le type de plateforme du **Serveur proxy**, le **Serveur proxy** sera installé dans le répertoire autre que celui en version déjà installée.



Si vous installez deux **Serveurs proxy** sur la même machine et que vous les paramétrez de sorte qu'ils utilisent le même port, ceci met hors service les deux **Serveurs proxy**.



Pour mettre à jour le serveur proxy :

1. Si sur l'ordinateur avec le **Serveur proxy** tourne l'**Agent** dont la fonction d'auto protection est activée, désactivez le composant d'auto protection **Dr.Web SelfPROtect** à l'aide des paramètres de l'**Agent**.
2. Supprimez le **Serveur proxy** conformément à la procédure standard (voir [Suppression du Serveur proxy](#)).



Lorsque vous supprimez le **Serveur proxy**, le fichier de configuration `drwcsd-proxy.xml` sera supprimé. Si besoin est, sauvegardez le fichier de configuration manuellement avant de supprimer le **Serveur proxy**.

3. Installez une nouvelle version du **Serveur proxy** conformément à la procédure standard (voir [Installation du Serveur proxy](#)).
4. Si besoin est, remplacez le fichier de configuration par le fichier sauvegardé depuis la version antérieure.
5. Si à l'étape 1 le composant d'auto protection **Dr.Web SelfPROtect** a été désactivé, activez-le à l'aide des paramètres de l'**Agent**.

Mise à jour du serveur proxy sous l'OS de la famille UNIX

Pour mettre à jour le serveur proxy, procédez comme suit :

Pour le Serveur proxy sous OS	Commande
FreeBSD Solaris	Réalisez une suppression et une réinstallation selon la procédure standard décrite dans les paragraphes Suppression du serveur proxy et Installation du serveur proxy
Linux package deb	<code>dpkg -i drweb-esuite-proxy</code>



Pour le Serveur proxy sous OS	Commande
package rpm	<code>rpm -U drweb-esuite-proxy</code>
package generic	<p>Déballiez le package d'installation à l'aide de la commande suivante :</p> <pre>tar -xjf <nom_du_fichier_de_distribution>.tar.bz2</pre> <p>Puis remplacez manuellement les fichiers se trouvant dans le répertoire d'installation du Serveur proxy par ceux depuis l'archive déballée.</p>

9.2. Mise à jour manuelle des composants de Dr.Web Enterprise Security Suite



Avant de procéder à la mise à jour de **Dr.Web ESS** et de ses composants, il est fortement recommandé de vérifier les paramètres du protocole TCP/IP relatifs à l'accès à Internet. Le service DNS doit notamment être actif et correctement configuré.

Vérification des mises à jour

Marche à suivre pour vérifier les mises à jour des produits Dr.Web ESS sur le Serveur de mises à jour :

1. Sélectionnez l'élément **Administration** du menu principal du **Centre de Gestion**, puis, dans la fenêtre qui apparaît, sélectionnez **Statut du dépôt des produits**.
2. Des informations sur tous les composants ainsi que la date de leur dernière révision et leur statut actuel seront affichées. Pour vérifier la disponibilité des mises à jour sur le Serveur de **SGMAJ**, cliquez sur le bouton **Vérifier les mises à jour**.



3. Si un composant n'est pas à jour, il sera mis à jour de manière automatique lors de la vérification. La mise à jour se fait conformément aux paramètres du dépôt des produits (voir [Gestion du dépôt des produits Dr.Web Enterprise Server](#)).
4. Après la fin de la mise à jour, la date du jour sera indiquée dans la ligne **Dernière révision** contre les composants actualisés.

Lancement de la mise à jour du logiciel sur le poste de travail

Afin de lancer la mise à jour du logiciel sur le poste :

1. Sélectionnez l'élément **Réseau antivirus** du menu principal du **Centre de Gestion**, puis dans la fenêtre qui apparaît, cliquez sur le nom du poste ou du groupe dans l'arborescence.
2. Dans la barre d'outils, cliquez sur le bouton  **Gestion des composants**. Dans la liste déroulante, sélectionnez un des éléments suivants :
 - ◆  **Mettre à jour les composants échoués** pour mettre à jour uniquement les composants dont la mise à jour précédente a échoué ainsi que pour remettre à zéro le statut d'erreur,
 - ◆  **Mettre à jour tous les composants** pour forcer la mise à jour de tous les composants y compris les composants dont la dernière version est déjà installée.



En cas de synchronisation forcée de tous les composants, deux redémarrages du poste sont requis. Veuillez suivre les instructions de l'**Agent**.

Vous pouvez également réaliser cette procédure depuis les outils de gestion d'**Enterprise Agent**.



Afin de lancer la mise à jour du logiciel sur le poste depuis le Dr.Web Enterprise Agent :

1. Autorisez l'utilisateur du poste à modifier la configuration d'**Enterprise Agent** (voir [Configuration des droits des utilisateurs](#)).
2. Sélectionnez dans le menu contextuel de l'icône de l'**Agent** l'élément **Synchroniser maintenant**.
3. Dans le menu qui apparaît, sélectionner un des deux éléments :
 - ◆ **Seuls les composants en échec** - pour mettre à jour uniquement les composants dont la mise à jour précédente a échoué ainsi que pour remettre à zéro le statut d'erreur,
 - ◆ **Tous les composants** - pour mettre à jour non seulement les composants en échec mais également tous les autres composants.

Erreur critique de mise à jour

En cas d'erreur critique de mise à jour :


1. Lancez une procédure de mise à jour forcée et complète du poste (voir ci-dessus).
2. Si l'erreur persiste, déterminez la cause de l'erreur à l'aide des fichiers de log de l'**Agent** et du module de mises à jour sur le poste (les fichiers de log se trouvent par défaut dans le sous-dossier `logs` du répertoire d'installation de l'**Agent** : `drwagntd.log` et `drwupgrade.log` respectivement).
3. Remédiez au problème et relancez la mise à jour forcée du poste.

9.3. Mise à jour selon la planification

Vous pouvez configurer la planification des tâches sur le **Serveur** afin d'effectuer des mises à jour régulières du logiciel (pour en savoir plus sur la planification des tâches, voir [Configuration de planification Dr.Web Enterprise Server](#)).



Marche à suivre pour configurer la planification de la tâche de mise à jour sur le Serveur Dr.Web Enterprise Server :

1. Sélectionnez l'élément **Administration** du menu principal du **Centre de Gestion**, puis dans la fenêtre qui apparaît, sélectionnez **Planification de Dr.Web Enterprise Server**. La listes des tâches courantes du **Serveur** va s'afficher.
2. Pour ajouter une tâche dans la liste, cliquez sur le bouton  **Nouvelle tâche** depuis la barre d'outils. La fenêtre d'édition de la nouvelle tâche s'ouvrira.
3. Spécifiez le nom de la tâche à afficher dans le champ **Nom**.
4. Passez à l'onglet **Action** et sélectionnez la tâche **Mise à jour** dans la liste déroulante.
5. Dans la liste déroulante, sélectionnez le produit à mettre à jour lors de l'exécution de la tâche :
 - ◆ **Dr.Web Enterprise Agent**
 - ◆ **Dr.Web Enterprise Server**
 - ◆ **Dr.Web Enterprise Updater**
 - ◆ **Dr.Web pour UNIX**
 - ◆ **Dr.Web Virus Bases**
 - ◆ **Tous les produits Dr.Web Enterprise** - si vous souhaitez configurer une tâche de mise à jour de tous les composants **Dr.Web ESS**.



Dans les versions **5.0** et supérieures, les mises à jour du logiciel **Serveur** ne sont pas fournies depuis les serveurs **SGBD**.

Pour mettre le **Serveur** à jour, utilisez l'installateur de la version appropriée et réalisez la procédure de mise à jour conformément au schéma général décrit dans les paragraphes [Mise à jour de Dr.Web ESS pour OS Windows®](#) ou [Mise à jour de Dr.Web ESS pour OS de la famille UNIX®](#).

6. Passez à l'onglet **Heure** et dans la liste déroulante, spécifiez une périodicité de lancement de la tâche, puis configurez l'heure selon la périodicité sélectionnée (la procédure est analogue à la configuration de l'heure dans la planification du poste de travail, voir [Edition de la planification des lancements](#))



[automatiques des tâches sur le poste](#)).

7. Pour sauvegarder les modifications, cliquez sur le bouton **Sauvegarder**.

9.4. Mise à jour du dépôt des produits de Dr.Web Enterprise Server non connecté à Internet

Si **Serveur Enterprise** n'est pas connecté à Internet, son dépôt des produits peut être mis à jour de manière manuelle. Pour cela, il faut copier le dépôt des produits d'un autre **Serveur Enterprise** qui a été mis à jour.



Cette manipulation n'est pas destinée à la migration vers une autre version.

Dans les versions **5.0** ou supérieures, les mises à jour du logiciel de **Serveur** ne sont pas fournies depuis les serveurs de **SGMAJ**.

Pour mettre à jour le **Serveur**, utilisez l'installateur en version appropriée et réalisez la procédure conformément à la règle générale décrite dans les paragraphes [Mise à jour de Dr.Web ESS pour OS Windows®](#) ou [Mise à jour de Dr.Web ESS pour OS de la famille UNIX®](#).

Marche à suivre recommandée pour obtenir des mises à jour du logiciel antivirus :

1. Installez le logiciel de **Serveur Enterprise** sur un poste ayant accès à Internet comme décrit dans le paragraphe [Installation du serveur antivirus](#).
2. Arrêtez les deux **Serveurs Enterprise**.
3. Pour recevoir les mises à jour du logiciel antivirus, démarrez le **Serveur** connecté à Internet avec la clé `syncrepository`.

Exemple pour **Windows** :



```
"C:\Program Files\DrWeb Enterprise Server  
\bin\drwcsd.exe" -home="C:\Program Files  
\DrWeb Enterprise Server" syncrepository
```

4. Remplacez complètement le contenu du répertoire du dépôt des produits du **Serveur** (principal) par le contenu du répertoire équivalent du dépôt du **Serveur** connecté à Internet. En général, c'est :

- ◆ var\repository sous **Windows**,
- ◆ /var/drwcs/repository sous **FreeBSD** et **Solaris**,
- ◆ /var/opt/drwcs/repository sous **Linux**.



Si, sur le poste sur lequel **Serveur Enterprise** est installé, l'**Agent** tourne avec l'option d'autoprotection **Dr.Web SelfPROtect** activée, il est nécessaire de désactiver ce composant via les paramètres de l'**Agent** avant de procéder à la mise à jour du dépôt des produits.

5. Si le **Serveur** principal tourne sous UNIX, il est nécessaire d'attribuer les droits d'utilisateur, créé/sélectionné lors de l'installation du **Serveur**, au dépôt des produits qui a été copié.
6. Exécutez sur le **Serveur** principal la commande suivante :

```
drwcsd rerepository
```

Sous **Windows**, la commande peut être lancée depuis la *ligne de commande* :

```
"C:\Program Files\DrWeb Enterprise Server  
\bin\drwcsd.exe" -home="C:\Program Files  
\DrWeb Enterprise Server" rerepository
```

ainsi que depuis le menu *Démarrer* :

```
Démarrer → Tous les programmes → DrWeb  
Enterprise Server → Contrôle du Serveur →  
Recharger le dépôt des produits.
```

7. Démarrez le **Serveur** principal.



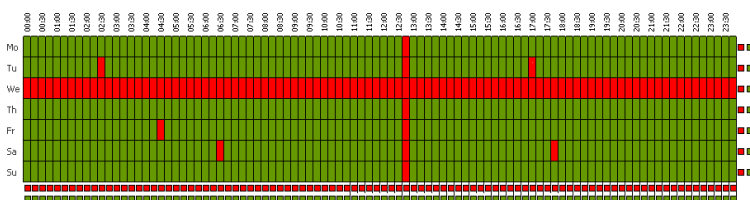
Si le composant d'autoprotection **Dr.Web SelfPROtect** a été désactivé lors de la mise à jour du dépôt des produits, il est recommandé de réactiver ce composant.

9.5. Restrictions de mises à jour des postes

Le **Centre de Gestion** vous permet de configurer le mode de mises à jour (autorisé/non autorisé) des composants de **Dr.Web Enterprise Security Suite** sur les postes protégés dans des délais spécifiés. Pour cela, suivez les instructions suivantes :

1. Sélectionnez l'élément **Réseau antivirus** du menu principal et dans la fenêtre qui apparaît, cliquez sur le nom du poste ou du groupe dans l'arborescence. Dans le menu de gestion (panneau de gauche), sélectionnez l'élément **Restrictions de mise à jour**.
2. Le tableau affichant les modes de mise à jour va s'ouvrir :
 - vert - mise à jour autorisée ;
 - rouge - mise à jour interdite.

La restriction peut être paramétrée avec un espacement de 15 minutes pour chaque jour de la semaine.



3. Pour modifier le mode de mise à jour, cliquez sur le fragment correspondant du tableau.


Pour modifier le mode pour une ligne entière (correspondant à un jour entier de la semaine), cliquez sur le marqueur de couleur se trouvant à droite de la ligne concernée du tableau.




Pour modifier le mode pour une colonne entière (un délai de 15 minutes pour tous les jours de la semaine), cliquez sur le marqueur de couleur se trouvant au-dessous de la colonne concernée du tableau.


4. Après la fin de l'édition, cliquez sur le bouton **Sauvegarder** pour accepter les modifications apportées.

Les options suivantes sont disponibles depuis la barre d'outils :

 **Diffuser les configurations vers un autre objet** - pour copier les configurations des mises à jour du poste ou du groupe vers un autre poste ou un autre groupe.

 **Supprimer les configurations** - pour revenir aux configurations par défaut (toutes les mises à jour sont autorisées).

 **Exporter les configuration vers un fichier** - pour sauvegarder les configurations des mises à jour vers un fichier dans un format spécialisé.

 **Importer les configurations depuis un fichier** - pour télécharger les configurations des mises à jour depuis un fichier dans un format spécialisé.

9.6. Mise à jour des Agents mobiles Dr.Web Enterprise Agent

Si votre ordinateur ou ordinateur portable n'est pas connecté à **Serveur Enterprise** durant un certain temps, afin de pouvoir recevoir les mises à jour depuis des Serveurs de **SGMAJ Dr.Web**, il est recommandé d'installer le mode itinérant d'**Enterprise Agent**. Pour cela, depuis le menu contextuel de l'icône de l'**Agent** dans la zone de notifications de la **Barre des tâches**, sélectionnez **Mode Itinérant** → **Autorisé**. La couleur de l'icône de l'**Agent** passera au jaune.

En mode itinérant, l'**Agent** fait trois tentatives pour se connecter au **Serveur** et en cas d'échec, il effectue une mise à jour via HTTP. Les tentatives de trouver le **Serveur** sont effectuées chaque minute.



L'élément **Mode itinérant** est disponible depuis le menu contextuel à condition que le mode itinérant d'utilisation de **SGMAJ Dr.Web** soit autorisé dans les droits du poste (pour en savoir plus, consultez le paragraphe [Configuration des droits des utilisateurs](#)).



Lorsque l'**Agent** fonctionne en mode itinérant, la connexion avec **Serveur Enterprise** est interrompue. Toutes les modifications pouvant être apportées sur le **Serveur** pour le poste concerné seront prises en compte dès que le mode itinérant de l'**Agent** aura été désactivé et que la connexion entre l'**Agent** et le **Serveur** aura été rétablie.

Seules les bases virales sont mises à jour lorsque le mode itinérant est activé.

Pour configurer les paramètres du mode itinérant, sélectionnez **Mode itinérant** → **Paramètres**. Dans la rubrique **Périodicité de mise à jour**, spécifiez un délai pour la vérification des mises à jour sur **SGMAJ**. Si nécessaire, cochez la case **Uniquement lors de la connexion Internet**.

En cas d'utilisation d'un Serveur proxy, dans la rubrique **Proxy**, cochez la case **Utilisez proxy** et spécifiez dans les champs se trouvant en bas de la fenêtre l'adresse et le port du Serveur proxy ainsi que les paramètres d'authentification.

Pour effectuer immédiatement une mise à jour en mode itinérant, sélectionnez **Mode itinérant** → **Lancer la mise à jour**.



L'élément **Lancer la mise à jour** ne sera pas disponible en cas de connexion au **Serveur**.

Pour désactiver le mode itinérant, sélectionnez l'élément **Mode itinérant** dans le menu contextuel de l'icône de l'**Agent** puis décochez la case **Autorisé**. La couleur de l'icône de l'**Agent** passera du jaune au vert et la connexion de l'**Agent** au **Serveur** sera rétablie.



9.7. Mise à jour des clés de Serveur et des clés de postes

Les fichiers contenant la clé de Serveur et la clé de poste sont installés avec **Serveur Enterprise** (voir [Installation de Dr.Web Enterprise Server](#)). Ultérieurement vous pouvez obtenir des nouvelles clés d'une durée de validité plus longue.

Il existe deux variantes de procédure permettant de remplacer les fichiers clé en fonction de la correspondance du paramètre ID **Serveur** dans le nouveau fichier clé et dans le fichier qui a été utilisé précédemment. Ouvrez le nouveau fichier et le fichier antérieur `enterprise.key` avec n'importe quel éditeur de texte et consultez la valeur du paramètre ID1 dans la rubrique [Enterprise].



Le fichier clé est dans un format protégé en écriture avec un mécanisme de signature numérique. L'édition du fichier le rend invalide. Afin d'éviter tout endommagement du fichier clé, il ne faut pas le modifier ni sauvegarder lors de la fermeture de l'éditeur de texte.

Si l'ordinateur possédant **Serveur Enterprise** tourne avec un **Agent** dont le composant d'autoprotection **Dr.Web SelfPROtect** est activé, il est nécessaire de désactiver le composant via les paramètres de l'**Agent** avant le remplacement des fichiers clés.



Les paramètres ID1 ont les mêmes valeurs



Utilisez le [Gestionnaire de licence](#) pour installer les nouveaux fichiers clés des composants du réseau antivirus.



Marche à suivre pour installer les nouveaux fichiers clés des composants du réseau antivirus de manière manuelle :


1. Placez le fichier contenant la clé de Serveur (nommé `enterprise.key`) dans le sous-dossier `etc` du répertoire d'installation du **Serveur** à la place du fichier existant ayant le même nom.
2. Redémarrez le **Serveur**.
3. Dans l'arborescence du réseau antivirus, sélectionnez le groupe **Everyone**, puis cliquez sur le bouton  **Général** →  **Importation de la clé**.
4. Dans la fenêtre qui apparaît, spécifiez le fichier clé pour le poste de travail (`agent.key`) puis cliquez sur **OK**.

Les valeurs des paramètres ID1 ne correspondent pas

Marche à suivre pour installer les nouveaux fichiers clés des composants du réseau antivirus :

1. Déconnectez les protocoles de l'**Agent** et de l'**Installeur réseau**. Pour cela, sélectionnez l'élément **Administration** du menu principal du **Centre de Gestion**, puis dans la fenêtre qui apparaît, sélectionnez **Configuration de Dr.Web Enterprise Server** et ouvrez l'onglet **Modules**. Décochez les cases **Protocole Dr.Web Enterprise Agent** et **Protocole Dr.Web Network Installer** puis cliquez sur **Sauvegarder**. Vous serez invité à redémarrer le **Serveur**. Cliquez sur le bouton **Oui**.
2. Exportez la planification de **Serveur Enterprise** vers un fichier. Pour cela, sélectionnez l'élément **Administration** du menu principal du **Centre de Gestion**, dans la fenêtre qui apparaît, sélectionnez **Planification de Dr.Web Enterprise Server** et depuis la barre d'outils cliquez ensuite sur le bouton  **Exporter les configurations vers un fichier**.
3. Pour gagner de la place dans la base de données, supprimez la planification de **Serveur Enterprise**. Pour cela, sélectionnez l'élément **Administration** du menu principal du **Centre de**



Gestion, dans la fenêtre qui apparaît, sélectionnez **Planification de Dr.Web Enterprise Server** et depuis la barre d'outils cliquez sur le bouton  **Supprimer les configurations**.

4. En cas de réseau multi-serveurs :
 - a) Pour sauvegarder des informations statistiques relatives aux **Serveurs** voisins, exportez les tableaux statistiques, compte tenu du fait qu'après la suppression des liaisons, telles informations seront perdues.
 - b) Supprimez toutes les liaisons entre serveurs. Vous pouvez les supprimer via le menu **Administration**, depuis l'item **Liaisons**.
5. Installez les nouveaux fichiers clés des composants du réseau antivirus :
 - ◆ Utilisez le [Gestionnaire de licence](#).
 - ◆ Pour remplacer les clés de manière manuelle, suivez la procédure décrite [ci-dessus](#).
6. Activez les protocoles de l'**Agent** et de l'**Installeur réseau** désactivés à l'étape **1**.
7. Reconfigurez la planification du **Serveur** ou importez d'un fichier la planification sauvegardée à l'étape **2**.
8. En cas de réseau multi serveurs, configurez toutes les liaisons entre serveurs qui ont été supprimées à l'étape **4**.
9. Redémarrez le **Serveur**.



Chapitre 10. Configuration des composants supplémentaires

10.1. Serveur proxy

Le réseau antivirus peut comprendre un ou plusieurs **Serveurs proxy**.

L'objectif principal du **Serveur proxy** est d'assurer la connexion entre **Serveur Enterprise** et **Enterprise Agent** dans le cas où l'accès direct devient impossible (par exemple si **Serveur Enterprise** et **Enterprise Agent** se trouvent dans des réseaux différents entre lesquels il n'y a pas de routage de paquets).

Fonctions clés

Le Serveur proxy remplit les fonctions suivantes :

1. Écoute du réseau et réception des connexions conformément au protocole et au port spécifiés.
2. Relais des protocoles (TCP/IP, IPv6, IPX et NetBIOS sont supportés).
3. Envoi de données entre **Serveur Enterprise** et les **Enterprise Agents** conformément à la configuration du Serveur proxy.
4. Mise en cache des mises à jour de l'**Agent** et du package antivirus transmis par le **Serveur**. La répartition des mises à jour depuis le cache du **Serveur proxy** offre les avantages suivants :
 - ◆ diminution du trafic réseau,
 - ◆ minimisation de la durée de réception des mises à jour par les **Agents**.



Il est possible de créer une hiérarchie des **Serveurs proxy**.

Le schéma général du réseau antivirus en cas d'utilisation du **Serveur proxy** est présent sur la [figure 10-1](#).

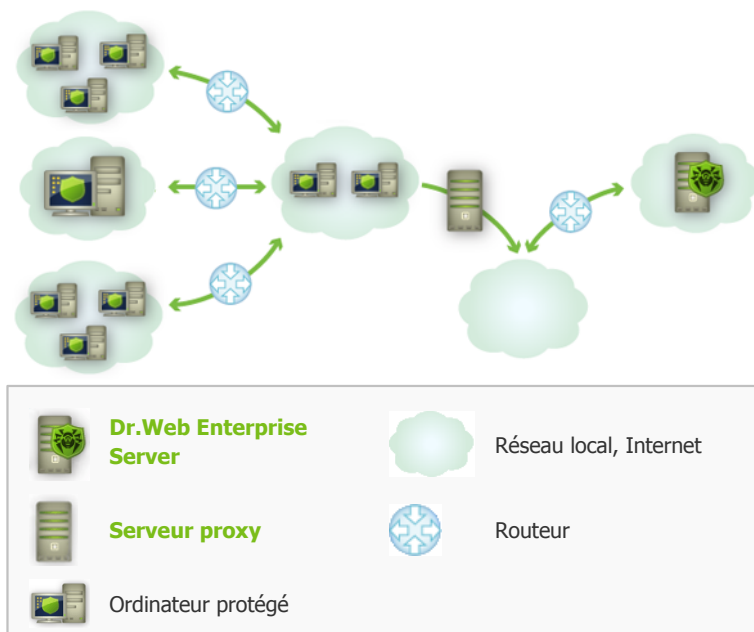


Figure 10-1. Schéma du réseau antivirus en cas d'utilisation du Serveur proxy

Principe de fonctionnement

Les instructions à suivre en cas d'utilisation du Serveur proxy :

1. Si l'adresse du **Serveur** n'est pas spécifiée dans les paramètres de l'**Agent**, l'**Agent** envoie une requête multi-adresses conformément au protocole réseau dans lequel il se trouve.



2. Si le **Serveur proxy** est configuré pour le relais des connexions (la valeur du paramètre `discovery="yes"`), un message sera envoyé vers l'**Agent** pour l'informer sur la présence du **Serveur proxy** opérationnel.
3. L'**Agent** spécifie les paramètres reçus du **Serveur proxy** en tant que paramètres du **Serveur Enterprise**. L'interaction ultérieure se fait de manière transparente pour l'**Agent**.
4. Conformément aux paramètres du fichier de configuration, le **Serveur proxy** écoute les ports spécifiés afin de contrôler les connexions entrantes via les protocoles spécifiés.
5. Pour chaque connexion entrante depuis l'**Agent**, le **Serveur proxy** établit une connexion avec le **Serveur Enterprise**.

Algorithme de redirection si une liste des Serveurs Enterprise est présente

1. Le **Serveur proxy** charge dans la mémoire vive la liste des **Serveurs Enterprise** depuis le fichier de configuration `drwcsd-proxy.xml` (voir [Annexe G4](#)).
2. L'**Agent Enterprise** se connecte au **Serveur proxy**.
3. Le **Serveur proxy** redirige l'**Agent Enterprise** vers le premier **Serveur Enterprise** mentionné dans la liste chargée dans la mémoire vive.
4. Le **Serveur proxy** effectue une rotation des éléments de la liste chargée dans la mémoire vive en déplaçant le **Serveur Enterprise** vers la fin de la liste.



Le **Serveur proxy** ne conserve pas l'ordre modifié des **Serveurs** dans son fichier de configuration. Au redémarrage du **Serveur proxy**, la liste des **Serveurs Enterprise** est chargée dans la mémoire vive dans son état initial dans lequel elle est enregistrée dans le fichier de configuration.

5. Lorsqu'un **Agent** suivant se connecte au **Serveur proxy**, la procédure se reproduit à partir de l'étape 2.



- Si le **Serveur Enterprise** se déconnecte du réseau antivirus (par exemple, en cas d'arrêt ou refus de service), l'**Agent** se connecte à nouveau au **Serveur proxy** et la procédure se reproduit à partir de l'étape 2.



Lancé sur la machine depuis un réseau externe par rapport aux **Agents** se trouvant dans le réseau, le **Scanner réseau** ne pourra pas détecter les **Agents** installés.



Si la case **Remplacer les noms NetBios** est cochée et un **serveur proxy** est utilisé dans le réseau antivirus, pour tous les postes connectés au **Serveur** via le **serveur proxy**, dans le **Centre de Gestion**, le nom de l'ordinateur sur lequel est installé le **serveur proxy** sera affiché à la place du nom du poste.

Chiffrement et compression du trafic

Le **serveur proxy** supporte la compression du trafic. Les informations transférées seront traitées selon la compression/non compression du trafic.

Le chiffrement n'est pas supporté par le **serveur proxy**. Le serveur analyse les informations transférées, si le trafic entre **Serveur Enterprise** et l'**Agent** est crypté, alors le **serveur proxy** passe en mode transparent, c'est-à-dire qu'il transmet tout le trafic passant entre le **Serveur** et l'**Agent** sans aucune analyse des informations.



Si le chiffrement du trafic entre l'**Agent** et le **Serveur** est activé, la mise en cache des mises à jour sur le **Serveur proxy** ne sera pas effectuée.

Mise en cache

Le **serveur proxy** supporte la mise en cache du trafic.

La mise en cache des produits se fait selon les révisions. Chaque révision se trouve dans un dossier séparé. Le dossier de chaque révision suivante contient des *liens matériel (hard links)* vers les



fichiers existants des révisions antérieures ainsi que vers les originaux des fichiers modifiés. Ainsi, les fichiers de chaque version sont sauvegardés sur le disque dur en un seul exemplaire, tous les dossiers relatifs aux révisions postérieures ne contiennent que des liens vers les fichiers non modifiés.

Les révisions périmées sont nettoyées toutes les heures. Seules les trois dernières révisions sont conservées. Les révisions plus récentes sont classées comme périmées et supprimées.

Outre cela, toutes les 10 minutes, les fichiers *memory mapped* non utilisés sont déchargés.

Configurations

Le **Serveur-proxy** n'a pas d'interface graphique. Les paramètres peuvent être configurés dans le fichier de configuration. Le format du fichier de configuration du **Serveur proxy** est décrit dans l'[Annexe G4](#)



Pour modifier les paramètres (éditer le fichier de configuration) du **Serveur proxy**, les droits d'administrateur sur la machine sont requis.

Pour le fonctionnement correct du **Serveur Proxy** sous OS de la famille Linux, après un redémarrage de l'ordinateur, un paramétrage système du réseau sans utiliser le Gestionnaire de réseau sera requis.

Démarrage et arrêt

Sous Windows, le démarrage et l'arrêt du **Serveur proxy** se font avec les outils standard depuis l'élément **Panneau de configuration** → **Outils d'administration** → **Services** → dans la liste des services, faites un double clic sur **drwcsd-proxy**, puis dans la fenêtre qui apparaît, sélectionnez l'action nécessaire.

Sous UNIX, le démarrage et l'arrêt du **Serveur proxy** s'effectuent avec les commandes `start` et `stop` via les scripts créés lors de



l'installation du **Serveur proxy** (voir [Installation du Serveur proxy](#)).

Pour démarrer le **serveur proxy** sous Windows et UNIX, vous pouvez également lancer le fichier exécutable `drwcsd-proxy` accompagné des paramètres nécessaires (voir Annexe [H10. Serveur proxy](#)).

10.2. NAP Validator

Généralités

Microsoft® Network Access Protection (NAP) est une plateforme de politique intégrée dans les systèmes d'exploitation Windows afin de renforcer la sécurité du réseau. Le niveau de sécurité est assuré grâce à la capacité de répondre aux exigences opérationnelles relatives aux systèmes dans le réseau.

En cas d'utilisation de la technologie NAP, il est possible de créer des politiques utilisateur permettant d'évaluer le niveau de performance de l'ordinateur. Les évaluations obtenues sont prises en comptes dans les cas suivants :

- ◆ avant d'autoriser l'accès ou l'interaction,
- ◆ pour réaliser une mise à jour automatique des ordinateurs se conformant aux exigences spécifiées afin d'assurer leur compatibilité de manière permanente,
- ◆ pour adapter les ordinateurs qui ne se conforment pas aux exigences spécifiées afin qu'ils leur correspondent.

Pour en savoir plus sur la technologie NAP, consultez le lien <http://www.microsoft.com/windowsserver2008/en/us/nap-product-home.aspx>.

Utilisation de NAP dans Dr.Web Enterprise Security Suite

Dr.Web ESS permet d'utiliser la technologie NAP pour vérifier la performance du logiciel antivirus sur les postes de travail. Cette



fonction est assurée par le composant **Dr.Web NAP Validator**.

Les moyens utilisés lors de la vérification de la performance :

- ◆ Le Serveur NAP destiné à vérifier la performance (installé et configuré de façon appropriée).
- ◆ **Dr.Web NAP Validator** est un moyen d'évaluation de la performance du logiciel antivirus sur le système protégé (System Health Validator - SHV) via les politiques utilisateur ajoutables **Dr.Web**. Il doit être installé sur la machine avec le Serveur NAP.
- ◆ L'agent SHA (System Health Agent - SHA). L'agent s'installe sur le poste de travail de manière automatique avec le logiciel d'**Enterprise Agent**.
- ◆ **Serveur Enterprise** sert de Serveur de correction assurant le fonctionnement de l'antivirus sur les postes.



Figure 10-2. Schéma du réseau antivirus en cas d'utilisation de NAP

Marche à suivre pour effectuer la procédure de vérification :

1. Pour activer la vérification, il faut configurer les paramètres correspondants de l'**Agent** (voir [Configuration de Dr.Web Enterprise Agent](#)).
2. L'agent SHA se trouvant sur le poste de travail se connecte au composant **Dr.Web NAP Validator** installé sur le Serveur NAP.
3. **Dr.Web NAP Validator** effectue une vérification des politiques de performance (voir [ci-dessous](#)). La vérification des politiques est une procédure durant laquelle **NAP Validator** réalise une évaluation des outils antivirus en prenant en



compte l'exécution des règles définies pour ces outils et donne l'état courant du système :

- ◆ les postes en conformité avec la politique de sécurité sont classés comme opérationnels et approuvés pour le fonctionnement au sein du réseau.
- ◆ les postes non conformes au moins à un élément de la politique seront classés comme non opérationnels. Ces postes ne peuvent que se connecter au **Serveur Enterprise**, mais ils sont déconnectés de l'autre partie du réseau. La performance du poste peut être rétablie à l'aide du **Serveur**, puis le poste doit repasser une procédure de vérification.

Les pré-requis pour le fonctionnement :

1. L'Agent doit être opérationnel (actif et opérationnel).
2. Le statut des bases virales qui doivent être à jour (les bases correspondent aux bases se trouvant sur le Serveur).

Configuration de NAP Validator

Après l'installation de **Dr.Web NAP Validator** (voir [Installation de NAP Validator](#)) sur la machine où tourne le Serveur NAP, il est nécessaire de réaliser les opérations suivantes :

1. Ouvrez le composant de la configuration du Serveur NAP (avec la commande `nps.msc`).
2. Dans la rubrique **Policies**, sélectionnez l'élément **Health Policies**.
3. Dans la fenêtre qui sera affichée, ouvrez les propriétés des éléments suivants :
 - ◆ **NAP DHCP Compliant**. Dans la fenêtre de configuration, cochez la case **Dr.Web System Health Validator** qui enjoint l'utilisation des politiques du composant **Dr.Web NAP Validator**. Dans la liste déroulante des types de vérification, désignez l'élément **Client passed all SHV checks**. Conformément à cette option, le poste sera classé comme opérationnel s'il correspond à tous les éléments de la politique adoptée.



- ◆ **NAP DHCP Noncompliant.** Dans la fenêtre de configuration, cochez la case **Dr.Web System Health Validator** qui enjoint l'utilisation des politiques du composant **Dr.Web NAP Validator**. Dans la liste déroulante des types de vérification, désignez l'élément **Client fail one or more SHV checks**. Conformément à cette option, le poste sera classé comme non opérationnel s'il n'est pas conforme à au moins un élément de la politique adoptée.



Annexes

Annexe A. Liste complète des OS supportés

Pour Dr.Web Enterprise Server:

OS de la famille UNIX:

- ALT Linux School Server 5.0
- ALT Linux School Server 5.0 x86_64
- ASP Linux 12
- ASP Linux 14
- Debian/GNU Linux Lenny
- Debian/GNU Linux Lenny x86_64
- Debian/GNU Linux Sid x86_64
- Debian/GNU Linux Squeeze
- Debian/GNU Linux Squeeze x86_64
- FreeBSD 7.3
- FreeBSD 7.3 amd64
- FreeBSD 7.4
- FreeBSD 7.4 amd64
- FreeBSD 8.1
- FreeBSD 8.1 amd64
- FreeBSD 8.2
- FreeBSD 8.2 amd64
- Linux glibc2.7
- Linux glibc2.7 x86_64
- Linux glibc2.8
- Linux glibc2.8 x86_64



Linux glibc2.9
Linux glibc2.9 x86_64
Linux glibc2.10
Linux glibc2.10 x86_64
Linux glibc2.11
Linux glibc2.11 x86_64
Linux glibc2.12
Linux glibc2.12 x86_64
Linux glibc2.13
Linux glibc2.13 x86_64
Mandriva Linux 2010
Mandriva Linux 2010 x86_64
Mandriva Linux Corporate Server 5.1
Mandriva Linux Corporate Server 5.1 x86_64
openSUSE 11
openSUSE 11 x86_64
RedHat Enterprise Linux 5.3
RedHat Enterprise Linux 5.3 x86_64
RedHat Enterprise Linux 6
RedHat Enterprise Linux 6 x86_64
RedHat Fedora 8
RedHat Fedora 8 x86_64
RedHat Fedora 9
RedHat Fedora 9 x86_64
RedHat Fedora 10
RedHat Fedora 10 x86_64
RedHat Fedora 11
RedHat Fedora 11 x86_64
RedHat Fedora 12
RedHat Fedora 12 x86_64
RedHat Fedora 13
RedHat Fedora 13 x86_64
RedHat Fedora 14



RedHat Fedora 14 x86_64
RedHat Fedora 15
RedHat Fedora 15 x86_64
SUSE Linux Enterprise Server 10
SUSE Linux Enterprise Server 10 x86_64
SUSE Linux Enterprise Server 11
SUSE Linux Enterprise Server 11 x86_64
Sun Solaris 10 x86
Sun Solaris 10 Sparc 32bit (processeur Sparc V9; UltraSparc au minimum)
Sun Solaris 10 Sparc 64bit (processeur Sparc V9; UltraSparc au minimum)
Ubuntu 8.04
Ubuntu 8.04 x86_64
Ubuntu 10.04
Ubuntu 10.04 x86_64
Ubuntu 10.10
Ubuntu 10.10 x86_64
Ubuntu 11.04
Ubuntu 11.04 x86_64
Ubuntu 11.10
Ubuntu 11.10 x86_64

OS Windows:

- 32 bits:

Windows 2000 Professional (SP4)
Windows 2000 Server (SP4)
Windows XP Professional (SP3)
Windows XP Home (SP3)
Windows Server 2003 (SP2)
Windows Vista (ou avec SP1 ou supérieur)
Windows Server 2008 (ou avec SP1 ou supérieur)



Windows 7

Windows 8

- 64 bits:

Windows Server 2003 (SP2)

Windows Vista (ou avec SP1 ou supérieur)

Windows Server 2008 (ou avec SP1 ou supérieur)

Windows Server 2008 R2

Windows 7

Windows Server 2012

Windows 8

Pour Dr.Web Enterprise Agent et package antivirus :

OS de la famille UNIX :

Linux glibc 2.7 ou supérieur

FreeBSD 7.3 ou supérieur

Sun Solaris 10 (uniquement pour la plateforme Intel)

OS Windows :

- 32 bits:

Windows 98

Windows Millennium Edition

Windows NT4 (SP6a)

Windows 2000 Professional (SP4 ou avec Update Rollup 1)

Windows 2000 Server (SP4 ou avec Update Rollup 1)

Windows XP Professional (ou avec SP1 ou supérieur)

Windows XP Home (ou avec SP1 ou supérieur)

Windows Server 2003 (ou avec SP1 ou supérieur)

Windows Vista (ou avec SP1 ou supérieur)



Windows Server 2008 (ou avec SP1 ou supérieur)
Windows 7
Windows 8

- 64 bits:

Windows Server 2003 (ou avec SP1 ou supérieur)
Windows Vista (ou avec SP1 ou supérieur)
Windows Server 2008 (ou avec SP1 ou supérieur)
Windows Server 2008 R2
Windows 7
Windows Server 2012
Windows 8

SelfPROtect, SpIDer Gate, Office Control, FireWall

- 32 bits:

Windows 2000 Professional (SP4 ou avec Update Rollup 1)
Windows 2000 Server (SP4 ou avec Update Rollup 1)
Windows XP Professional (ou avec SP1 ou supérieur)
Windows XP Home (ou avec SP1 ou supérieur)
Windows Server 2003 (ou avec SP1 ou supérieur)
Windows Vista (ou avec SP1 ou supérieur)
Windows Server 2008 (ou avec SP1 ou supérieur)
Windows 7
Windows 8

- 64 bits:

Windows Server 2003 (ou avec SP1 ou supérieur)
Windows Vista (ou avec SP1 ou supérieur)
Windows Server 2008 (ou avec SP1 ou supérieur)
Windows Server 2008 R2
Windows 7
Windows Server 2012
Windows 8



OS Windows Mobile

Windows Mobile 2003
Windows Mobile 2003 Second Edition
Windows Mobile 5.0
Windows Mobile 6.0
Windows Mobile 6.1
Windows Mobile 6.5

OS Novell NetWare

Novell NetWare 4.11 SP9
Novell NetWare 4.2
Novell NetWare 5.1
Novell NetWare 6.0
Novell NetWare 6.5

Mac OS X

Mac OS 10.4 (Tiger)
Mac OS 10.4 Server (Tiger Server)
Mac OS 10.5 (Leopard)
Mac OS 10.5 Server (Leopard Server)
Mac OS 10.6 (Snow Leopard)
Mac OS 10.6 Server (Snow Leopard Server)
Mac OS 10.7 (Lion)
Mac OS 10.7 Server (Lion Server)

OS Android

Android 1.6
Android 2.0
Android 2.1



Android 2.2
Android 2.3
Android 3.0
Android 3.1
Android 3.2
Android 4.0.



Annexe B. Configurations requises en cas d'utilisation de SGBD. Paramètres des pilotes SGBD



La structure de la BD de **Serveur Enterprise** peut être obtenue à l'aide du script `sql init.sql` se trouvant dans le sous-dossier etc du dossier d'installation de **Serveur Enterprise**.

En tant que base de données de **Serveur Enterprise** les bases suivantes peuvent être utilisées :

- ◆ SGBD interne (IntDB) ;
- ◆ SGBD externe.

SGBD interne

Les paramètres listés dans le tableau B-1 sont utilisés pour configurer la procédure de consultation du SGBD interne afin de stocker ou de traiter des données.

Tableau B-1. SGBD interne (IntDB)

Nom	Valeurs par défaut	Description
DBFILE	dbinternal.dbs	Chemin vers le fichier de la base de données
CACHESIZE	2000	La taille de la mémoire cache de la base de données en pages
SYNCHRONOUS	FULL	Le mode d'enregistrement synchrone des modifications apportées dans la base de données vers le disque : <ul style="list-style-type: none">• FULL — enregistrement complètement synchrone sur le disque,



Nom	Valeurs par défaut	Description
		<ul style="list-style-type: none">• NORMAL — enregistrement synchrone des données critiques,• OFF — enregistrement asynchrone

SGBD externe

Les SGBD pouvant être utilisés en tant que base de données externe de **Serveur Enterprise** sont listés ci-dessous :

- ◆ SGBD Oracle. Pour en savoir plus sur la configuration, consultez l'Annexe B2. [Configuration du driver de BD pour Oracle](#).
- ◆ SGBD Microsoft SQL Server Compact Edition (SQL CE). Pour en savoir plus sur la configuration, consultez l'Annexe B3. [Configuration du driver de BD pour SQL CE](#).
- ◆ SGBD PostgreSQL. Pour en savoir plus sur la configuration, consultez l'Annexe B4. [Utilisation de SGBD PostgreSQL](#).
- ◆ Microsoft SQL Server/Microsoft SQL Server Express. Pour accéder aux données de SGBD, un pilote ODBC peut être utilisé (Pour en savoir plus sur la configuration du driver ODBC pour OS Windows, consultez l'Annexe B1. [Configuration du driver ODBC](#)).



En cas d'utilisation de Microsoft SQL Server 2005, le driver ODBC fourni avec ce SGBD est requis.

Microsoft SQL Server 2005 (SP4) ou supérieur supporté.

Il est vivement recommandé d'installer les dernières mises à jour pour le serveur de la BD utilisé.

La BD Microsoft SQL Server Express n'est pas recommandée en cas de déploiement d'un réseau antivirus avec un grand nombre de postes (supérieur à 100).



Caractéristiques comparatives



La base de données interne peut être utilisée lorsque le nombre de postes connectés au **Serveur** est inférieur à 200-300. Si l'ordinateur sur lequel est installé **Serveur Enterprise** et la charge relative à d'autres tâches exécutées sur la même machine le permettent, il est possible de connecter jusqu'à 1000 postes.

Sinon, il est nécessaire d'utiliser une BD externe.

En cas d'utilisation d'une BD externe et si le nombre de postes connectés au **Serveur** est supérieur à 10000, il est recommandé de prendre en compte les pré-requis minimum suivants :

- ◆ processeur 3GHz,
 - ◆ mémoire vive - à partir de 4 Go pour **Serveur Enterprise**, à partir de 8 Go - pour le Serveur de BD,
 - ◆ OS de la famille UNIX.
-

Pour faire votre choix entre les bases de données interne et externe, il faut prendre en compte les paramètres relatifs à chacun des deux SGBD :

- ◆ Dans les grands réseaux (comptant plus de 200-300 postes) il est recommandé d'utiliser une BD externe qui est plus résistante en cas d'incidents de fonctionnement par rapport aux BD internes.
- ◆ En cas d'utilisation de la BD interne, aucun composant tiers n'est requis. Cette variante est recommandée pour une utilisation standard.
- ◆ La base de données interne ne nécessite pas de maîtriser l'administration du SGBD et présente un bon choix pour les petits et moyens réseaux antivirus.



- ◆ Il est recommandé d'utiliser une base externe dans le cas où vous planifiez des tâches pour lesquelles l'accès direct au SGBD sera requis. Il est possible d'utiliser les API standard : OLE DB, ADO.NET ou ODBC. Cependant, il est à noter qu'il n'existe pas de driver ODBC pour le SGBD Microsoft SQL CE. Le support des technologies ADO.NET ainsi que de la langue LINQ facilitent considérablement l'utilisation du SGBD dans les applications et permettent de profiter de toutes les fonctions de la plateformes .NET Framework y compris le système de reporting CrystalReports.

Annexe B1. Configuration du driver ODBC

Lors de la configuration de la connexion au SGBD externe pour le stockage et le traitement de données, les paramètres listés dans le tableau B-2 sont utilisés.

Tableau B-2. ODBC (uniquement en version pour Windows)

Nom	Valeur par défaut	Description
DSN	drwcs	Nom du jeu de données
USER	drwcs	Nom d'utilisateur
PASS	drwcs	Mot de passe
TRANSACTION	DEFAULT	Voir ci-dessous

Les valeurs possibles du paramètre TRANSACTION :

- ◆ SERIALIZABLE
- ◆ READ_UNCOMMITTED
- ◆ READ_COMMITTED
- ◆ REPEATABLE_READ
- ◆ DEFAULT



La valeur déterminée par défaut - `DEFAULT` signifie : "utiliser les valeurs par défaut relatives à la configuration du Serveur SQL". Pour plus d'informations sur les niveaux d'isolation des transactions, consultez la documentation de la base de données appropriée.



Afin d'éviter d'éventuels problèmes concernant le codage, il est nécessaire de désactiver les paramètres suivants du driver ODBC :

- ◆ **Use regional settings when outputting currency, numbers, dates and times** - peut entraîner des erreurs lors du formatage des valeurs numériques.
 - ◆ **Perform translation for character** - peut entraîner l'affichage incorrect des symboles dans les paramètres provenant de la base de données dans le **Centre de Gestion**. Ce paramètre établit une correspondance entre l'affichage des symboles et le paramètre de langue pour les programmes n'utilisant pas Unicode.
-

La base de données est créée préalablement sur le Serveur SQL avec les paramètres ci-dessus. **Il est nécessaire de configurer également les paramètres du driver ODBC pour l'ordinateur sur lequel est installé **Serveur Enterprise**. Pour cela :**

1. Dans le **Panneau de configuration Windows**, sélectionnez l'élément **Outils d'administration**, puis dans la fenêtre qui apparaît, faites un double clic sur l'icône **Sources de données (ODBC)**. La fenêtre **Administrateur de sources de données ODBC** va s'ouvrir. Passez à l'onglet **Sources de données système**.
2. Cliquez sur le bouton **Ajouter**. La fenêtre permettant de choisir un driver va s'ouvrir.
3. Sélectionnez dans la liste l'élément correspondant au pilote ODBC pour la BD sélectionnée et cliquez ensuite sur le bouton **Terminer**. La première fenêtre de configuration d'accès au Serveur de BD va s'ouvrir.



En cas d'utilisation d'un SGBD externe, il faut installer la dernière version du pilote ODBC fournie avec ce SGBD. Il n'est pas recommandé d'utiliser le pilote ODBC au sein de l'OS Windows, sauf en cas de BD fournies par Microsoft sans pilote ODBC.

4. Spécifiez les paramètres d'accès à la source de données correspondant aux paramètres spécifiés dans la configuration de **Serveur Enterprise**. Si le Serveur de BD se trouve sur un ordinateur autre que celui sur lequel tourne **Serveur Enterprise**, spécifiez son adresse et son nom dans le champ de saisie **Serveur**. Cliquez sur le bouton **Suivant**.
5. Saisissez les paramètres d'accès à la BD dans cette fenêtre. Cliquez sur le bouton **Configuration client**. La fenêtre de sélection et de configuration du protocole réseau va s'ouvrir.
6. Sélectionnez la bibliothèque réseau pour le protocole **TCP/IP** ou **Named pipes** (recommandé). Si le Serveur de BD tourne sur un ordinateur autre que l'ordinateur local, à la place du point dans les champs de saisie **Alias Serveur** et **Nom d'ordinateur**, spécifiez son nom ou son adresse. Cliquez sur le bouton **OK**. La fenêtre se fermera. Vous retournez vers la fenêtre de configuration du driver. Cliquez sur le bouton **Suivant**.
7. Assurez-vous que l'option **A la déconnexion seulement** est bien choisie et les cases suivantes : **Identificateurs entre guillemets au format ANSI**, **Valeurs null**, **Templates et notifications au format ANSI** sont cochées. Cliquez ensuite sur le bouton **Suivant**.



S'il est possible de changer la langue des messages système lors de la configuration du driver ODBC, il est nécessaire de spécifier l'anglais.

8. A la fin de l'édition cliquez sur **Terminer**. La fenêtre contenant le tableau des paramètres configurés va s'afficher.
9. Pour vérifier les paramètres, cliquez sur le bouton **Tester la source de données**. Après avoir reçu un message de réussite de la vérification, cliquez sur le bouton **OK**.



Annexe B2. Configuration du driver BD pour Oracle

Généralités

Oracle Database (ou Oracle DBMS) est un SGBD objet-relationnel. Oracle peut être utilisé en tant que base de données externe pour **Dr.Web ESS**.



Serveur Enterprise peut utiliser le SGBD Oracle en tant que base externe sur toutes les plateformes excepté FreeBSD (voir [Installation et versions supportées](#)).

L'utilisation du SGBD Oracle requiert :

1. installation d'une BD Oracle avec le codage `AL32UTF8`. Vous pouvez également utiliser la BD existante avec ce codage ;
2. configuration du driver de BD afin de pouvoir utiliser la base de données externe. Vous pouvez le configurer dans le [fichier de configuration](#) ou via le **Centre de Gestion** : menu **Configuration de Dr.Web Enterprise Server**, onglet **Base de données**.



Si vous planifiez d'utiliser ODBC pour Oracle comme base de données externe, sélectionnez l'élément **Installation sélective** et puis dans la fenêtre suivante, refusez l'installation du client intégré pour SGBD Oracle (dans les rubriques respectives **Database support - Oracle database driver**) dans les paramètres de l'installateur lors de l'installation (mise à jour) du **Serveur**.

Sinon, le fonctionnement avec la BD Oracle via ODBC ne sera pas possible à cause du conflit des bibliothèques.



Installation et versions supportées

Pour pouvoir utiliser la BD Oracle en tant que base externe, il est nécessaire de configurer, pour la base, le codage AL32UTF8 (CHARACTER SET AL32UTF8 / NATIONAL CHARACTER SET AL16UTF16). Ceci peut être réalisé par les moyens suivants :

1. avec l'installateur de BD Oracle (utilisez le mode avancé d'installation et de configuration de la BD),
2. avec la commande SQL `CREATE DATABASE`.

Pour en savoir plus sur la création et la configuration de la BD, consultez la documentation relative à la BD Oracle.



En cas d'utilisation d'un codage autre que le codage indiqué, les symboles régionaux ne seront pas affichés correctement.

Le client d'accès à la BD (Oracle Instant Client) fait partie du package d'installation de **Dr.Web ESS**.

Les plateformes supportées par le SGBD Oracle sont listées sur le site de l'éditeur <http://www.oracle.com/technology/software/tech/oci/instantclient/index.html>.

Dr.Web ESS supporte les versions suivantes du SGBD : Oracle9i Database Release 2: 9.2.0.1 - 9.2.0.8 ou supérieures.

Paramètres

Lors de la configuration de la connexion au SGBD, les paramètres décrits dans le tableau B-3 sont utilisés.

Tableau B-3. Paramètres de SGBD Oracle

Paramètre	Description
drworacle	Nom du driver



Paramètre	Description
User	Nom de l'utilisateur de la BD (obligatoire)
Password	Mot de passe utilisateur (obligatoire)
ConnectionString	Ligne de connexion à la BD (obligatoire)

Format de la ligne de connexion au SGBD Oracle :

// <host> : <port> / <service name>

où :

- ◆ <host> - adresse IP ou nom du Serveur Oracle ;
- ◆ <port> - port écoutant le Serveur ;
- ◆ <service name> - nom de la BD à laquelle il faut se connecter.

Exemple :

//myserver111:1521/bjava21

où :

- ◆ myserver111 - nom de Serveur Oracle.
- ◆ 1521 - port écoutant le Serveur.
- ◆ bjava21 - nom de la BD à laquelle il faut se connecter.

Exemple du fichier de configuration drwcsd.conf

Si vous utilisez SGBD Oracle, il est nécessaire de modifier le mode de détection et les paramètres du pilote de base de données d'une des manières suivantes :

- ◆ Dans le **Centre de Gestion** : l'élément **Administration** du menu principal → l'élément **Configuration Dr.Web Enterprise Server** du menu de gestion → l'onglet **Base de données** → sélectionnez dans la liste déroulante **Base de données** type **Oracle**, configurez les paramètres selon le format indiqué ci-dessus.



- ◆ dans le [fichier de configuration](#) du **Serveur**. Ci-dessous, vous trouverez un fragment du fichier de configuration avec les paramètres appropriés :

```
...  
;Database definition. Mandatory.  
;Only one definition is allowed.  
  
database  
  
;DB driver (DLL or shared object name)  
drworacle ; Oracle DB, unix & windows  
  
;load library from this path; empty - use default  
from ""  
  
using "User=DRWCS Password=root  
ConnectionString=//192.168.0.1:1521/ORADB"
```

Annexe B3. Configuration du driver de la BD pour SQL CE



Il est recommandé d'utiliser la BD interne à la place de la BD MS SQL CE si vous n'avez pas besoin de travailler avec la BD via ADO.NET. L'avantage de la BD interne est sa haute stabilité de fonctionnement et ses performances supérieures à celles de MS SQL CE.

Généralités

Microsoft SQL Server Compact Edition (SQL CE) est une BD relationnelle de Microsoft. C'est une BD pouvant s'intégrer dans les applications desktop ainsi que dans les appareils mobiles. SQL CE peut être utilisée en tant que BD externe pour **Dr.Web ESS**.



L'utilisation de SQL Server CE requiert :

1. L'installation d'un Serveur SQL CE ;
2. La configuration du driver de BD afin de pouvoir utiliser la base de données externe existante. Ceci peut être effectué dans le [fichier de configuration](#) ou via le **Centre de Gestion** : menu **Configuration de Dr.Web Enterprise Server**, onglet **base de données**.

Installation et plateformes supportées



SGBD SQL CE supporte les OS Windows 2000 ou supérieurs (en versions x86 et x64).

Dr.Web Enterprise Security Suite supporte SQL CE en version 3.5 SP1/SP2 pour les plateformes x64 et x86. La compatibilité avec les versions plus récentes de la BD SQL CE n'est pas garantie.

Pour utiliser la BD SQL Server Compact Edition, il est nécessaire de télécharger un package d'installation depuis le site de l'éditeur <http://www.microsoft.com/sqlserver/2005/en/us/compact-downloads.aspx> et d'installer le Serveur dans une version appropriée :

- ◆ Windows 2000 requiert la version SQL Server Compact 3.1 (pour en savoir plus, voir [Pré-requis système pour la version 3.1](#)).
- ◆ en cas de plateformes plus anciennes que Windows 2000, il est recommandé d'installer la version plus récente SQL Server Compact 3.5 (pour en savoir plus, voir [Pré-requis système pour la version 3.5](#)).



Il n'est pas recommandé d'installer plus d'une version SQL Server Compact pour éviter d'éventuels problèmes de compatibilité.

Les BD créées sous différentes versions de SQL Server Compact peuvent ne pas être compatibles, puisqu'à la différence de la version 3.5, la version 3.1 ne supporte pas le chiffrage. C'est pourquoi, en cas de changement de



version, le déplacement de la BD ne se fait qu'avec les commandes de **Dr.Web Enterprise Security Suite** `exportdb` et `importdb`.

Le client d'accès à la BD fait partie du package d'installation de **Dr.Web ESS**.

Paramètres

Lors de la configuration de la connexion au SGBD SQL CE, les paramètres décrits dans le tableau B-4 sont utilisés.

Tableau B-4. Paramètres de SGBD SQL CE

Paramètre	Description
<code>drwsqldb</code>	Nom du driver.
<code>DBFILE</code>	Nom de la BD (par défaut c'est <code>mssqlce.sdf</code>).
<code>PASSWORD</code>	Mot de passe utilisé pour le chiffrement de la BD.



Le paramètre `PASSWORD` est une clé de chiffrement et n'a rien à voir avec le système utilisateur/mot de passe.

Par défaut, le mot de passe est vide (le chiffrement ne s'applique pas à la BD).

Exemple du fichier de configuration `drwcsd.conf`

En cas d'utilisation du SGBD SQL CE, il faut modifier la détermination et la configuration de la BD dans le [fichier de configuration de Serveur Enterprise](#). Un fragment du fichier de configuration contenant les paramètres concernés est présenté ci-dessous :

```
...  
;Database definition. Mandatory.  
;Only one definition is allowed.
```



```
database

;DB driver (DLL or shared object name)
drwsqlce ; sql server compact, windows only

;load library from this path; empty - use default
from ""

;parameters describing database connection
;defaults (DBFILE: varroot/mssqlce.sdf)
;using "DBFILE=mssqlce.sdf PASSWORD=drwcs"
using "DBFILE=mssqlce.sdf PASSWORD=drwcs"
```

Annexe B4. Utilisation du SGBD PostgreSQL

Généralités

PostgreSQL est un SGBD objet-relationnel. C'est une alternative aux SGBD commercialisés (tels que Oracle Database, Microsoft SQL Server etc.). Dans les grands réseaux, le SGBD PostgreSQL peut être utilisé en tant que BD externe pour **Dr.Web ESS**.

Pour cela, il est nécessaire d'effectuer les opérations suivantes :

1. installer le Serveur PostgreSQL ;
2. configurer le driver ODBC ;
3. configurer **Serveur Enterprise** conformément à l'utilisation de la base externe. Ceci peut être effectué dans le [fichier de configuration](#) ou via le **Centre de Gestion** : menu **Configuration de Dr.Web Enterprise Server**, onglet **Base de données**.



Installation et versions supportées

Téléchargez la dernière version du produit gratuit PostgreSQL (serveur PostgreSQL et le pilote ODBC correspondant) et surtout n'utilisez pas une version plus ancienne que 8.2.



SGBD PostgreSQL existe pour les plateformes suivantes : Linux, Solaris/OpenSolaris, Win32, Mac OS X, FreeBSD.

Pour plus d'information sur l'installation et l'utilisation de PostgreSQL avec **Serveur Enterprise**, cliquez [ici](#).

Cet article vous propose une description détaillée de la procédure de création de la base de données externe PostgreSQL et de l'installation de **Dr.Web Enterprise Security Suite** avec la base créée préalablement. Si **Dr.Web Enterprise Security Suite** est installé, la procédure de création de la BD PostgreSQL est analogue ; pour migrer vers la BD externe, consultez le paragraphe [Changement de type de SGBD Dr.Web Enterprise Suite](#).



La version ANSI du pilote ODBC peut être utilisée uniquement à partir de la version PostgreSQL 8.2.4. Le pilote ODBC pour Unicode est opérationnel dans toutes les versions.

Installation sur les systèmes 64-x

Le driver psqLODBC pour les OS 64-x n'est pas fourni officiellement par l'éditeur. Par ailleurs, selon les informations publiées sur le site officiel du SGBD PostgreSQL, l'installation des packages préliminaires est possible depuis les liens suivants :

- ◆ <http://www.enterprisedb.com/products/pgdownload.do#windows>
- ◆ <http://code.google.com/p/visionmap/wiki/psqLODBC>
- ◆ <http://www.geocities.jp/inocchichichi/psqlodbc/index.html>



Après l'installation du driver ODBC sur un OS 64-x, pour pouvoir accéder aux drivers, utilisez le panneau d'administration se trouvant ici : `C:\WINDOWS\SYSTEM32\odbcad32.exe`.

Paramètres

Lors de la configuration de la connexion à la BD PostgreSQL, les paramètres décrits dans le tableau B-5 sont utilisés.

Tableau B-5. PostgreSQL (uniquement en version pour OS UNIX)

Nom	Valeurs par défaut	Description
host	<code><Socket local UNIX></code>	Hôte du Serveur PostgreSQL
port		Port du Serveur PostgreSQL ou extension du nom de fichier du socket
dbname	<code>drwcs</code>	Nom de la BD
user	<code>drwcs</code>	Nom utilisateur
password	<code>drwcs</code>	Mot de passe
options		Options de débogage/traçage à envoyer au Serveur
tty		Fichier ou <code>tty</code> output lors du débogage
requiressl		1 pour la demande de connexion SSL ou 0 pour ne pas demander

Pour plus d'information technique, visitez le lien <http://www.postgresql.org/docs/manuals/>.



Interaction entre Dr.Web Enterprise Server et la BD PostgreSQL via UDS

Lors de l'installation de **Serveur Enterprise** et de la BD PostgreSQL sur la même machine, leur interaction peut être configurée via UDS (socket du domaine UNIX).

Pour configurer l'interaction via UDS, procédez comme suit :

1. Dans le fichier de configuration de la BD PostgreSQL `postgresql.conf`, indiquez le dossier suivant pour UDS :

```
unix_socket_directory = '/var/run/postgresql'
```
2. Redémarrez PostgreSQL.



Annexe C. Paramètres du système de notifications

Lors de la configuration du système de notifications sur les événements relatifs au fonctionnement des composants du réseau antivirus, les paramètres listés ci-dessous correspondent aux divers types de drivers du module de notifications.

Tableau C-1. Notifications par email (driver drwemail)

Paramètre	Valeur par défaut	Description
HOST	127.0.0.1	Hôte du Serveur SMTP
PORT	25	Port du Serveur SMTP
PASS		Mot de passe SMTP
USER		Utilisateur SMTP
DEBUG	NO	Mode de débogage
FROM	drwcsd@localhost	Adresse de l'expéditeur
TO	root@localhost	Adresse du destinataire

Tableau C-2. Notifications via Windows Messenger (driver drwwnetm), uniquement au sein de la version pour Windows

Paramètre	Valeur par défaut	Description
TO	Admin	Nom réseau de la machine



Annexe D. Paramètres des templates du système de notifications

Les textes des messages à envoyer (par email ou via **Windows Messenger**) sont générés depuis les fichiers de templates par un composant du **Serveur** nommé processeur de templates.



Le système de notifications via le réseau Windows fonctionne uniquement sous OS Windows supportant le service Windows Messenger (Net Send).

Windows Vista et les systèmes supérieurs ne supportent pas le service Windows Messenger.

Le fichier de template comprend un texte et des variables entre accolades. Lors de l'édition des fichiers de templates, utilisez les variables listées ci-dessous.



Le processeur de templates ne fait pas de substitutions récursives.

Les variables sont écrites sous un des formats suivants :

- ◆ {<VAR>} – mettre la valeur de la variable <VAR>.
- ◆ {<VAR>:<N>} – les <N> premiers caractères de la variable <VAR>.
- ◆ {<VAR>:<first>:<N>} – <N> caractères de la variable <VAR> suivante après les <first> premiers caractères (à partir du <first> +1er caractère), si le reste est inférieur à ce nombre, il est complété par des espaces à droite.
- ◆ {<VAR>:<first>:-<N>} – <N> caractères de la variable <VAR>, suivante après les <first> premiers caractères (à partir du <first>+1er caractère), si le reste est inférieur à ce nombre, il est complété par des espaces à gauche.



- ◆ { <VAR>/<original1>/<replace1> [/<original2>/<replace2>] } – les caractères spécifiés seront remplacés par la valeur <VAR> afin d'attribuer les valeurs données : les symboles <original1> seront remplacés par les symboles <replace1>, si les symboles <original2> sont présents, ils seront remplacés par les symboles <replace2> etc.

Le nombre de paires de substitution est illimité.

Tableau D-1. Format des variables

Variable	Valeur	Expression	Valeur
SYS.TIME	10:35:17:456	{SYS.TIME:5}	10:35
SYS.TIME	10:35:17:456	{SYS.TIME:3:5}	35:17
SYS.TIME	10:35:17:456	{SYS.TIME:3:-12}	°°35:17:456
SYS.TIME	10:35:17:456	{SYS.TIME:3:12}	35:17:456°°
SYS.TIME	10:35:17:456	{SYS.TIME/10/99/35/77}	99:77:17:456

Légende

° - espace.

Variables système :

- ◆ SYS.TIME — heure système courante,
- ◆ SYS.DATE — date système courante,
- ◆ SYS.DATETIME — date et heure système courantes,
- ◆ SYS.VERSION — version du **Serveur**,
- ◆ SYS.BUILD — date du build de **Serveur**,
- ◆ SYS.PLATFORM — plateforme du **Serveur**,
- ◆ SYS.PLATFORM.SHORT — variante abrégée de SYS.PLATFORM,
- ◆ SYS.OS — nom du système d'exploitation du **Serveur**,
- ◆ SYS.BRANCH — version des **Agents** et du **Serveur**,
- ◆ SYS.SERVER — le nom du produit (**Dr.Web Enterprise Server**).



Les variables d'environnement ont les mêmes noms que les variables spécifiées dans l'environnement avec l'ajout du préfixe ENV. (le préfixe se termine avec le point).

Vairables communes des messages, Agent :

- ◆ GEN.LoginTime — heure de l'authentification du poste,
- ◆ GEN.StationAddress — adresse du poste,
- ◆ GEN.StationID — UUID du poste,
- ◆ GEN.StationName — nom du poste.

Variables communes des messages, sous-système de mises à jour du Serveur :

- ◆ GEN.CurrentRevision — identificateur courant de version,
- ◆ GEN.NextRevision — identificateur de la version mise à jour,
- ◆ GEN.Folder — répertoire d'emplacement du produit,
- ◆ GEN.Product — description du produit.

Variables des messages, par messages (pour Agent) :

Administrator_Authorization_Failed:

- ◆ MSG.Login — nom d'enregistrement,
- ◆ MSG.Address — adresse réseau du **Centre de Gestion** ;

Approved_Newbie:

- ◆ MSG.AdminName — nom de l'administrateur,
- ◆ MSG.AdminAddress — adresse du **Centre de Gestion** ;

AutoApproved_Newbie : aucune variable ;



Awaiting_Approval: aucune variable ;

Cannot_Add_Station:

- ◆ MSG.ID — UUID du poste ;

Connection_Terminated_Abnormally:

- ◆ MSG.Reason — cause de l'arrêt ;

Infection:

- ◆ MSG.Component — nom du composant,
- ◆ MSG.RunBy — composant lancé par l'utilisateur,
- ◆ MSG.ServerTime — heure de réception de l'événement, GMT,
- ◆ MSG.ObjectName — nom de l'objet infecté,
- ◆ MSG.ObjectOwner — propriétaire de l'objet infecté,
- ◆ MSG.InfectionType — type d'infection,
- ◆ MSG.Virus — nom de virus,
- ◆ MSG.Action — action de désinfection ;

Installation_Bad:

- ◆ MSG.Error — message d'erreur ;

Installation_OK: aucune variable ;

License_Limit - envoyé au cas où le nombre de postes enregistrés atteint la limitation déterminée par la licence, s'il reste moins de 5% de la limitation prévue par la licence non utilisée ou s'il reste moins de deux postes :

- ◆ MSG.Used — nombre de postes dans la base,
- ◆ MSG.Licensed — autorisé par la licence ;

Low_Var_Free_Space:

- ◆ MSG.Path - chemin vers le répertoire de petit volume de mémoire,
- ◆ MSG.FreeSpace - espace libre en octets,
- ◆ MSG.FreeInodes - nombre de descripteurs inode disponibles (s'applique uniquement pour certains systèmes "UNIX-like"),



- ◆ `MSG.RequiredSpace` - volume de mémoire requis,
- ◆ `MSG.RequiredInodes` - nombre d'inodes disponibles requis (s'applique uniquement pour certains système "UNIX-like") ;

Near_Max_Stations (envoyé à chaque démarrage du **Serveur** au cas où le **Serveur** est lancé avec une clé autorisant moins de postes qu'il n'existe déjà):

- ◆ `MSG.Used` — nombre de postes dans la base,
- ◆ `MSG.Licensed` — autorisé par la licence,
- ◆ `MSG.Percent` — pourcentage des licences disponibles ;

Newbie_Not_Allowed: aucune variable ;

Not_Seen_For_A_Long_Time:

- ◆ `MSG.StationName` — nom du poste,
- ◆ `MSG.StationID` — UUID du poste,
- ◆ `MSG.DaysAgo` — nombre de jours écoulés depuis la dernière connexion,
- ◆ `MSG.LastSeenFrom` — adresse depuis laquelle le poste a été vu pour la dernière fois ;

Processing_Error:

- ◆ `MSG.Component` — nom du composant,
- ◆ `MSG.RunBy` — composant lancé par l'utilisateur,
- ◆ `MSG.ServerTime` — heure de réception de l'événement, GMT,
- ◆ `MSG.ObjectName` — nom de l'objet,
- ◆ `MSG.ObjectOwner` — propriétaire de l'objet,
- ◆ `MSG.Error` — message d'erreur ;

Rejected_Newbie:

- ◆ `MSG.AdminName` — nom de l'administrateur,
- ◆ `MSG.AdminAddress` — adresse du **Centre de Gestion** ;

Station_Already_Logged_In – envoyé au où le poste est déjà



enregistré sur l'un ou sur l'autre **Serveur** :

- ◆ `MSG.ID` — UUID du poste,
- ◆ `MSG.StationName` — nom du poste,
- ◆ `MSG.Server` — ID du **Serveur** sur lequel est enregistré le poste ;

Station_Authorization_Failed:

- ◆ `MSG.ID` — UUID du poste,
- ◆ `MSG.Rejected` — valeurs `rejected` — accès au poste refusé, `newbie` — tentative de basculer le poste vers le statut "novice" ;

Statistics:

- ◆ `MSG.Component` — nom du composant,
- ◆ `MSG.ServerTime` — heure de la réception de l'événement, GMT,
- ◆ `MSG.Scanned` — nombre d'objets scannés,
- ◆ `MSG.Infected` — nombre d'objets infectés,
- ◆ `MSG.Modifications` — nombre d'objets infectés par des modifications de virus,
- ◆ `MSG.Suspicious` — nombre d'objets suspects,
- ◆ `MSG.Cured` — nombre d'objets réparés,
- ◆ `MSG.Deleted` — nombre d'objets supprimés,
- ◆ `MSG.Renamed` — nombre d'objets renommés,
- ◆ `MSG.Moved` — nombre d'objets déplacés,
- ◆ `MSG.Speed` — vitesse de traitement en Ko/s ;

Too_Many_Stations - envoyé lorsqu'un nouveau poste ne peut pas être enregistré sur le **Serveur** à cause des limitations de licence :

- ◆ `MSG.ID` — UUID du poste ;

Unknown_Administrator:

- ◆ `MSG.Login` — nom d'enregistrement,
- ◆ `MSG.Address` — adresse réseau du **Centre de Gestion** ;

**Unknown_Station:**

- ◆ MSG.ID — UUID du poste inconnu,
- ◆ MSG.Rejected — valeurs rejected — accès au poste refusé, newbie — tentative de passer le poste en mode "novice" ;

Update_Failed:

- ◆ MSG.Product — produit à mettre à jour,
- ◆ MSG.ServerTime — heure locale de réception du message par le **Serveur** ;

Update_Wants_Reboot:

- ◆ MSG.Product — produit à mettre à jour,
- ◆ MSG.ServerTime — heure locale de réception du message par le **Serveur**.

Variables des messages, par messages (pour le sous-système de mises à jour du Serveur) :

Srv_Repository_Cannot_flush: aucune variable ;

Srv_Repository_UpToDate: aucune variable ;

Srv_Repository_Frozen: aucune variable ;

Srv_Repository_Load_failure:

- ◆ MSG.Reason — message sur la cause de l'erreur ;

Srv_Repository_Update:

- ◆ MSG.AdddedCount — nombre de fichiers ajoutés,
- ◆ MSG.ReplacedCount — nombre de fichiers remplacés,
- ◆ MSG.DeletedCount — nombre de fichiers supprimés,
- ◆ MSG.Added — liste des fichiers ajoutés (chaque nom à la ligne),
- ◆ MSG.Replaced — liste des fichiers remplacés (chaque nom à la ligne),



- ◆ `MSG.Deleted` — liste des fichiers supprimés (chaque nom à la ligne) ;

Srv_Repository_UpdateFailed:

- ◆ `MSG.Error` — message d'erreur,
- ◆ `MSG.ExtendedError` — description détaillée de l'erreur.



Les variables du dernier template ne comprennent pas les fichiers marqués comme "**ignorés lors des notifications**" dans le fichier de configuration du produit, voir [F1. Syntaxe du fichier de configuration .config](#).

Variables du message du Serveur sur l'expiration de la licence :

Key_Expiration:

- ◆ `MSG.Expiration` — date d'expiration,
- ◆ `MSG.Expired` — 1, si la date d'expiration est déjà arrivée, sinon - 0,
- ◆ `MSG.ObjId` — GUID de l'objet,
- ◆ `MSG.ObjName` — nom de l'objet,
- ◆ `MSG.ObjType` — objet utilisant la clé qui va bientôt expirer (server/station/group).



Annexe E. Spécification de l'adresse réseau

La spécification présente comprend les termes suivants :

- ◆ les variables (les champs à remplacer par des valeurs spécifiées) sont à mettre entre `< >` et en italique,
- ◆ le texte permanent (qui reste après les substitutions) doit utiliser une police non proportionnelle (largeur fixe),
- ◆ les éléments facultatifs sont à mettre entre crochets,
- ◆ à gauche de la séquence des symboles `:=` se trouve une notion à déterminer, à droite - sa détermination (comme dans La forme de Backus-Naur).

E1. Format général de l'adresse

L'adresse réseau est au format suivant :

[`<protocol>/`] [`<protocol-specific-part>`]

Par défaut, `<protocol>` reçoit la valeur TCP. Il est également possible d'indiquer les valeurs IPX et NetBIOS. Les valeurs par défaut de `<protocol-specific-part>` sont déterminées par l'application.

Adresses de la famille IP

- ◆ `<interface> := <ip-address>`
`<ip-address>` peut être un nom DNS ou une adresse IP espacée par des points (exemple 127.0.0.1).
- ◆ `<socket-address> := <interface> : <port-number>`
`<port-number>` doit être un nombre décimal.



Adresses de la famille IPX

- ◆ `<interface> : := <ipx-network> . <mac-address>`
`<ipx-network>` doit contenir 8 chiffres hexadécimaux, `<mac-address>` doit comprendre 12 chiffres hexadécimaux.
- ◆ `<socket-address> : := <interface> : <socket-number>`
`<socket-number>` doit comprendre 4 chiffres hexadécimaux.

Adresses de la famille NetBIOS

- ◆ Protocole orienté datagramme :
`nbd/<NAME> [: <PORT> [: <LANA>]]`
- ◆ Protocole orienté connexion :
`nbs/<NAME> [: <PORT> [: <LANA>]]`

où `<NAME>` — nom NetBIOS de l'ordinateur, `<PORT>` — port (par défaut 23), `<LANA>` — numéro de l'adaptateur réseau (pris en compte en cas de NetBEUI).

Exemples :

1. `tcp/127.0.0.1:2193`

désigne le protocole TCP, le port 2193 sur interface 127.0.0.1.

2. `tcp/[::]:2193`

désigne le protocole TCP, le port 2193 sur interface IPv6 0:0:0:0:0:0:0:0

3. `localhost:2193`

idem.

4. `tcp/:9999`

désigne pour le Serveur : l'interface par défaut qui est fonction de



l'application (en général, toutes les interfaces disponibles), le port 9999; désigne pour le client : connexion avec l'hôte par défaut, en fonction de l'application (en général localhost), le port 9999.

5. `tcp/`

le protocole TCP, le port est déterminé par défaut.

6. `spx/00000000.000000000001:2193`

désigne le socket SPX loopback 0x2193.

Adresses de la famille UDS

- ◆ Le protocole orienté connexion :
`unx/ <file_name>`
- ◆ Le protocole orienté datagramme :
`udx/ <file_name>`

Exemples :

1. `unx/tmp/drwcd:stream`
2. `unx/tmp/drwcd:datagram`

Protocole orienté connexion

`<protocol>/ <socket-address>`

ou `<socket-address>` détermine l'adresse locale du socket pour le Serveur ou un Serveur distant pour le client.

Protocole orienté datagramme

`<protocol>/ <endpoint-socket-address> [-<interface>]`

**Exemples :**

1.udp/231.0.0.1:2193

désigne l'utilisation du groupe multicast 231.0.0.1:2193 sur l'interface par défaut qui est fonction de l'application.

2.udp/[ff18::231.0.0.1]:2193

désigne l'utilisation du groupe multicast [ff18::231.0.0.1] sur l'interface par défaut qui est fonction de l'application.

3.udp/

l'interface en fonction de l'application et le point final.

4.udp/255.255.255.255:9999-<myhost1>

l'utilisation des messages broadcast sur le port 9999 et sur l'interface <myhost1>.

E2. Adresses de Dr.Web Enterprise Server

Réception des connexions

<connection-protocol>/ [<socket-address>]

Par défaut, en fonction de <connection-protocol>:

◆ tcp/0.0.0.0:2193

désigne "toutes les interfaces (excepté les interface auxquelles les adresses IPv6 sont attribuées), le port 2193";

◆ tcp/[::]:2193

désigne "toutes les interfaces IPv6, le port 2193";

◆ spx/00000000.000000000001:2193

désigne "toutes les interfaces, le port 0x2193";

◆ nbs/drwcs:23:0



désigne l'utilisation du protocole NetBIOS stream, le port 23, l'ordinateur `drwcs`.

Service de détection de Dr.Web Enterprise Server

`<datagram-protocol> / [<endpoint-socket-address> [- <interface>]]`

Par défaut, en fonction de `<datagram-protocol>`:

◆ `udp/231.0.0.1:2193-0.0.0.0`

désigne l'utilisation du groupe multicast `231.0.0.1:2193` sur toutes les interfaces ;

◆ `udp/[ff18::231.0.0.1]:2193-[:]:0`

désigne l'utilisation du groupe multicast `[ff18::231.0.0.1:2193]` sur toutes les interfaces ;

◆ `ipx/00000000.FFFFFFFF:2193-00000000.000000000000`

désigne la réception des messages broadcast sur le socket `0x2193` sur toutes les interfaces ;

◆ `nbd/drwcs:23:0`

désigne l'utilisation du protocole NetBIOS datagram, le port 23, l'ordinateur `drwcs`.

E3. Adresses de Dr.Web Enterprise Agent/ Installer

Connexion directe à Dr.Web Enterprise Server

`[<connection-protocol>] / [<remote-socket-address>]`

Par défaut, en fonction de `<connection-protocol>`:



- ◆ `tcp/127.0.0.1:2193`
où `127.0.0.1` - loopback, `2193` - port ;
- ◆ `tcp/[::1]:2193`
où `[::1]` - loopback (IPv6), `2193` - port ;
- ◆ `spx/00000000.000000000001:2193`
où `00000000.000000000001` - loopback, `2193` - port.

Recherche du Serveur <drwcs-name> utilisant la famille spécifiée de protocoles et le point final

`[<drwcs-name>]@<datagram-protocol>/[<endpoint-socket-address>[-<interface>]]`

Par défaut, en fonction de `<datagram-protocol>`:

- ◆ `drwcs@udp/231.0.0.1:2193-0.0.0.0`
recherche du **Serveur** avec le nom `drwcs` pour la connexion TCP en utilisant le groupe multicast `231.0.0.1:2193` sur toutes les interfaces,
- ◆ `drwcs@ipx/00000000.FFFFFFFF:2193-00000000.000000000000`
recherche du **Serveur** avec le nom `drwcs` pour la connexion SPX en utilisant les messages broadcast sur le socket `0x2193` sur toutes les interfaces.



Annexe F. Gestion du dépôt des produits

La gestion du dépôt des produits est effectuée avec les fichiers suivants se trouvant dans la racine du répertoire des produits :

- ◆ Fichier de configuration `.config`. Il détermine le jeu de fichiers et les paramètres du Serveur de mises à jour. Ce fichier a le format texte et sa structure est décrite ci-après dans les Annexes respectives [F1. Syntaxe du fichier de configuration .config](#) et [F2. Instructions du fichier .config](#).
- ◆ Fichier de statut `.id`. Ce fichier affiche le statut généralisé du produit (numéro de révision et étape d'exécution de la transaction). Le format respectif est décrit dans l'Annexe ci-dessous : [F3. Fichiers .id](#).



Lors de la configuration des liaisons entre serveurs (voir [Particularités du réseau avec plusieurs Serveurs](#)), pour répartir en miroir les produits, il est à prendre en compte que les fichiers de configuration ne font pas partie du produit et ne sont pas traités par le système de répartition en miroir. Afin d'éviter des failles du système de mises à jour, veuillez respecter les instructions suivantes :

- ◆ pour les **Serveurs** égaux, sauvegardez la configuration identique,
- ◆ pour les **Serveurs** subordonnés, désactivez la synchronisation des composants via le protocole HTTP ou sauvegardez la configuration identique.



Après l'édition des fichiers de configuration et de statut, le redémarrage du **Serveur** est requis.



F1. Syntaxe du fichier de configuration `.config`

Pour décrire le format du fichier de configuration `.config`, la grammaire formelle basée sur la forme EBNF est utilisée et comprend la légende suivante :

- ◆ (...) – groupe de symboles (fragment du fichier de configuration) ;
- ◆ "... " – symbole terminal ;
- ◆ <...> – symbole non terminal ;
- ◆ | – symbole de sélection d'un des éléments proposés ;
- ◆ (...) ? – le symbole (ou groupe de symboles entre guillemets) se trouvant à gauche de l'opérateur n'est pas obligatoire (peut être utilisé 0 ou 1 fois) ;
- ◆ (...) * – le symbole (ou groupe de symboles entre guillemets) se trouvant à gauche de l'opérateur peut se répéter n'importe quel nombre de fois (il peut également être omis) ;
- ◆ (...) + – le symbole (ou groupe de symboles entre guillemets) se trouvant à gauche de l'opérateur peut être utilisé 1 fois ou plus d'une fois ;
- ◆ [...] – n'importe quel symbole appartenant à la plage spécifiée ;
- ◆ point à la fin – symbole spécifique désignant la fin de la règle.

Format du fichier de configuration du dépôt des produits `.config` :

```
<ligne> := <instruction>? (<séparateur>+ <commentaire>?)*.

<instruction> := <nom> "{"? <paramètre>* "}"?.

<nom> := "description" | "sync-with" |
        "sync-delay" | "sync-only" |
        "sync-ignore" | "state-only" |
        "state-ignore" | "notify-only" |
        "notify-ignore" | "notify-off".
```



```
<paramètre> := <texte>.
<texte> := <mot> <séparateur>*.
<mot> := (<symbole> | <signe>)+.
<symbole> := [a-zA-Z] | [0-9].
<signe> := "\"" | "/" | "\" | "*" | "^" | "." | "-" | "$".

<séparateur> := \r | \t | \n | \s.

<commentaire> := ";"<texte> | "#"<M1><symbole>+<M1> |
"'"<M2><texte>+<M2>.
<M1> := <symbole>+.
<M2> := <signe>+.
```

Le fichier de configuration est une séquence de mots séparés par des séparateurs. Le *séparateur* représente n'importe quelle séquence de symboles suivants : espace (\s), tabulation (\t), retour à la ligne (\r), saut de ligne (\n).

Le mot commençant par un point-virgule (;) désigne le commencement d'un commentaire qui s'étend jusqu'à la fin de la ligne.

Exemples :

```
ghgh 123 ;c'est un commentaire
123;ce; n'est pas; un commentaire - un
séparateur au début est requis.
```

Le mot commençant par le symbole dièse (#) désigne le début du commentaire de type flux; le reste du mot est spécifié par le marqueur de la fin du commentaire.

Exemple :

```
123 456 #COMM Depuis cet endroit le
commentaireCOMM est terminé
```

Pour inclure des symboles dans le mot, vous pouvez utiliser le préfixe ' (apostrophe) — un séparateur spécifique pour ce mot (c'est ce symbole qui sera classé comme séparateur achevant ce mot).

**Exemple :**

```
xy123 '*Un mot*Déjàunautre
```



Si le mot commence par un des symboles suivants : apostrophe, point-virgule, dièse (', ;, #), il doit se limiter par des symboles spécifiques séparateurs comme il est décrit ci-dessus.

Le fichier `.config` comprend des commentaires et des instructions. L'ordre des instructions n'a pas d'importance.



Le format des instructions des fichiers de configuration est sensible à la casse.

Le dépôt des produits est sensible à la casse quels que soient le système de fichier et l'OS sous lequel tourne le **Serveur**.

Pour plus d'information sur les instructions, consultez l'Annexe [F2. Instructions du fichier .config](#).

F2. Règles du fichier `.config`

La règle "description"

La règle `description` désigne le nom du produit à afficher dans le **Centre de Gestion**. Si la règle n'est pas configurée, le nom du répertoire du produit sera utilisé comme nom du produit.

Exemple :

```
description "'Dr.Web® Enterprise Agent"
```



Règle *sync-with*

La règle `sync-with` détermine la liste des Serveurs HTTP et des Serveurs HTTP proxy à mettre à jour. Le paramètre `name` détermine le nom du domaine ou l'adresse IP. L'élément `:port` peut être absent, auquel cas la valeur 80 est attribuée comme numéro de port pour le Serveur HTTP et 3128 pour le Serveur proxy.

Les Serveurs se trouvant dans la liste seront interrogés successivement, après une mise à jour réussie, la procédure se termine.



La version actuelle de **Dr.Web Enterprise Security Suite** ne supporte que l'authentification HTTP de base, l'authentification HTTP proxy et l'authentification RADIUS.

Les redirections HTTP permanentes (code 301) sont mises en cache avant de redémarrer le Serveur.

Exemple :

```
sync-with{
  http{ esuite.msk3.drweb.com /update }
  http{ esuite.msk4.drweb.com /update }
  http{ esuite.msk.drweb.com /update }
  http{ esuite.us.drweb.com /update }
  http{ esuite.jp.drweb.com /update }
}
```

Exemple en cas d'utilisation d'un Serveur proxy

```
sync-with{
  http-proxy{ 10.3.0.74 auth user:pass http
  { esuite.msk7.drweb.com /update } }
  http-proxy{ 10.3.0.74 auth user:pass http
  { esuite.jp.drweb.com /update } }
  http-proxy{ 10.3.0.74 auth user:pass http
```



```
{ esuite.msk5.drweb.com /update } }  
http-proxy{ 10.3.0.74 auth user:pass http  
{ esuite.msk6.drweb.com /update } }  
http-proxy{ 10.3.0.74 auth user:pass http  
{ esuite.msk.drweb.com /update } }  
http-proxy{ 10.3.0.74 auth user:pass http  
{ esuite.us1.drweb.com /update } }  
http-proxy{ 10.3.0.74 auth user:pass http  
{ esuite.msk3.drweb.com /update } }  
http-proxy{ 10.3.0.74 auth user:pass http  
{ esuite.msk4.drweb.com /update } }  
http-proxy{ 10.3.0.74 auth user:pass http  
{ esuite.us.drweb.com /update } }  
http-proxy{ 10.3.0.74 auth user:pass http  
{ esuite.frl.drweb.com /update } }  
}
```

où :

- ◆ 10.3.0.74 - adresse IP du Serveur proxy ;
- ◆ user - nom d'utilisateur du Serveur proxy (peut être absent si le serveur proxy ne requiert pas d'authentification) ;
- ◆ pass - mot de passe pour accéder au Serveur proxy (peut être absent si le serveur proxy ne requiert pas d'authentification).

Règle sync-only

La règle `sync-only` détermine de manière explicite un ensemble de noms de fichiers (spécifiés avec des expressions régulières sous la forme simplifiée comme il est décrit dans ce paragraphe, ainsi que sous forme complète `qr{}` comme dans le paragraphe [Lancement et arrêt du scanner antivirus sur le poste](#)) à synchroniser. Si la règle n'est pas présente, tout le contenu du répertoire est à synchroniser par défaut (excepté les fichiers dont les noms commencent par un point).

**Exemple :**

```
sync-only{^common/drw.*vdb$}
```

enjoint de mettre à jour seulement les bases virales.

Règle *sync-ignore*

La règle `sync-ignore`, par contre, détermine de manière explicite un ensemble de fichiers à ne pas synchroniser.



S'il y a des fichiers ajoutés dans le produit de manière locale (qui ne sont pas présents dans les originaux) et que la règle `sync-only` n'est pas utilisée, les fichiers à ajouter doivent être mentionnés dans `sync-ignore`, sinon ces fichiers seront supprimés lors de la synchronisation.

Règle *sync-delay*

La règle `sync-delay` détermine la liste des fichiers dont la modification entraîne une interdiction de passer le produit vers la nouvelle révision. Dans ce cas-là, le dépôt des produits continue à diffuser la révision antérieure et la synchronisation ne se fait plus (le statut du produit est "bloqué"). Si l'utilisateur trouve que la révision réceptionnée est bonne à diffuser, il doit éditer le fichier de statut `.id` et redémarrer ensuite le **Serveur** (voir Annexe [F3. Fichiers .id](#)).

Exemples :

- ◆ La diffusion automatique de nouvelles révisions est interdite :

```
sync-delay{ .* }  
  
; aucune automatisation, tout doit être testé  
de manière personnalisée
```

- ◆ La diffusion automatique est interdite pour les révisions dans lesquelles des fichiers exécutables ont été mis à jour :



```
sync-delay{ .*\.exe$ .*\.dll$ }
```

Règles *state-only* et *state-ignore*

Les règles *state-only* et *state-ignore* déterminent (ou limitent) la liste des fichiers à diffuser de façon analogue.

Exemple :

Pour le produit **Enterprise Agent** :

- ◆ il n'est pas requis de télécharger les langues d'interface allemande, polonaise et espagnole (les autres langues doivent être téléchargées),
- ◆ il n'est pas requis de recevoir les composants conçus pour Windows 98/Windows Me.

```
sync-ignore{
    ; à noter que si les fichiers listés sont déjà
    ; présents dans le dépôt des produits, ils sont
    toujours
    ; à diffuser.
    ; c'est pourquoi, il est nécessaire de les
    enlever ou
    ; passer vers state-ignore{ }, ou réaliser
    ; une synchronisation complète dans
    ; la configuration spécifiée
; ^common/ru-.*\.dwl$ nous en avons besoin
^common/de-.*\.dwl$
^common/pl-.*\.dwl$
^common/es-.*\.dwl$
^win/de-.*
^win/pl-.*
^win-9x\.*
}
```



Règles du groupe `notify`

Les règles du groupe `notify` permettent de configurer le système de notification pour les produits sélectionnés (la configuration complète du système de notification est décrite dans le paragraphe [Configuration des notifications](#)).

Le dépôt des produit peut générer les types de notifications suivants :

- ◆ `update` — en cas de mise à jour réussie du produit,
- ◆ `delay` — en cas de blocage de transaction,
- ◆ `flushfail` — en cas d'erreur d'écriture sur le disque,
- ◆ `loadfail` — en cas d'erreur de téléchargement.

Par défaut tous les types de notification sont autorisés.

La règle `notify-off` permet d'interdire les types sélectionnés de notification pour le produit courant.

Les règles `notify-ignore` et `notify-only` permettent de limiter ou de spécifier de manière explicite la liste des fichiers dont la modification entraîne l'envoi d'une notification de type `update`.



Si dans le même fichier au moins deux des règles `sync-only`, `sync-ignore` ou `sync-delay` sont présentes, la règle suivante sera appliquée :

- ◆ la règle `sync-only` s'applique la première. Les fichiers non listés dans la liste de cette instruction (si elle est présente) ne seront pas traités,
 - ◆ la règle `sync-ignore` s'applique aux fichiers restants,
 - ◆ la règle `sync-delay` ne s'applique qu'aux fichiers restants après l'exécution des deux opérations ci-dessus.
-

L'ordre d'application des règles `state-only` et `state-ignore` est déterminé de manière analogue.



F3. Fichiers .id

Le *Fichier de statut du produit* est un fichier texte dans lequel le **Serveur** sauvegarde les numéros des révisions du produit. Dans son état standard, le fichier contient un seul nombre - le numéro de la révision courante. La synchronisation du produit se fait à condition que le numéro de la révision sur le Serveur de **SGMAJ** soit supérieur au numéro courant, dans ce cas, la synchronisation comprend les 4 étapes suivantes :

- 1) Deux nombres sont écrits dans le fichier .id :

```
<nouvelle_révision> <révision_périmée>.
```

Ainsi, il est clair que le produit est en phase de transaction inachevée depuis

```
<révision périmée> vers <nouvelle révision>.
```

- 2) Tous les fichiers modifiés sont reçus via HTTP puis sont placés dans les sous-répertoires appropriés dont les noms ont le format suivant :

```
<nom-d'origine_du_fichier> . <nouvelle_révision>.
```

- 3) Le résultat de la transaction est écrit dans le fichier .id.

Ceci peut être un statut standard mais avec un nouveau numéro ou le statut "bloqué" (*frozen*) suit à l'exécution de la règle `sync-delay`:

```
<nouvelle_révision> <révision_périmée> frozen.
```

- 4) Si le statut est autre que "bloqué", les nouveaux fichiers remplacent les originaux.

Au redémarrage du **Serveur** après l'analyse du fichier `.id`, la transaction inachevée est annulée; sinon elle sera exécutée **4**).



F4. Exemples de gestion du dépôt des produits avec une modification du fichier de statut

Synchronisation complète du produit :

1. Arrêter le **Serveur**.
2. Supprimer tout le contenu du répertoire du produit excepté `.id` et `.config`.
3. Écrivez 0 dans le fichier `.id`.
4. Démarrez le **Serveur**.
5. Effectuez une mise à jour du produit.



La révision 0 a une signification particulière puisque dans ce cas là, la diffusion est interdite, le statut "vide" du produit ne sera pas propagé vers les **Agents**.

Interdiction de la diffusion :

1. Arrêtez le **Serveur**.
2. Écrivez 0 dans le fichier `.id`.
3. Mettez la règle `sync-with` se trouvant dans le fichier `.config` entre guillemets afin d'interdire la synchronisation.
4. Démarrez le **Serveur**.
5. Réalisez une mise à jour du produit.

Migration du statut "bloqué" vers une nouvelle révision :

1. Remplacez le contenu du `.id`

```
<nouvelle-révision> <révision_périmée> frozen
par
<nouvelle_révision>
```
2. Redémarrez le **Serveur**.
3. Réalisez une mise à jour du produit.



Rollback depuis le statut "bloqué" vers la version antérieure :

1. Remplacez le contenu du `.id`
`<nouvelle_révision> <révision_périmée> frozen`

par

`<nouvelle_révision> <révision_périmée>`,
2. Redémarrez le **Serveur**.
3. Réalisez une mise à jour du produit.



Lors des tentatives ultérieures de réaliser une synchronisation vers une `<nouvelle_révision>`, le dépôt des produits reprend le statut "bloqué" (frozen). Vous pouvez garder la `<révision_périmée>` du dépôt et refuser la mise à jour, ceci peut s'avérer juste dans le cas où vous disposez d'une révision appropriée, par exemple, réussie lors du testing.



Annexe G. Fichiers de configuration

Ce paragraphe vous propose une description du format des fichiers suivants :

- ◆ fichier de configuration de **Enterprise Server** `drwcsd.conf` ;
- ◆ fichier de configuration du **Serveur proxy** `drwcsd-proxy.xml` ;
- ◆ fichier de configuration du **Centre de Gestion** `webmin.conf` ;
- ◆ fichier de configuration `download.conf`.



Dans le cas où l'Agent tourne sur le poste sur lequel est installé un de ces composants et que l'option d'autoprotection est activée, il est nécessaire de désactiver le composant d'autoprotection **Dr.Web SelfPROtect** depuis les paramètres de l'Agent avant de procéder à la modification des fichiers de configuration.

Après l'enregistrement de toutes les modifications apportées, il est recommandé de réactiver le composant **Dr.Web SelfPROtect**.

G1. Fichier de configuration de Dr.Web Enterprise Server

Le fichier de configuration de **Serveur Enterprise** `drwcsd.conf` se trouve par défaut dans le sous-répertoire `etc` du répertoire racine du **Serveur**. Au démarrage du **Serveur**, il est possible de spécifier un emplacement non standard du fichier de configuration ainsi que son nom avec une clé de la ligne de commande (pour en savoir plus, consultez l'Annexe [H5. Dr.Web Enterprise Server](#)).



Marche à suivre pour éditer de manière manuelle le fichier de configuration de Dr.Web Enterprise Server :

1. Arrêtez le **Serveur** depuis le **Centre de Gestion** ou avec la commande se trouvant dans le menu Démarrer → Tous les programmes → Dr.Web Enterprise Server → Contrôle du Serveur → Arrêter.
2. Désactivez l'autoprotection (si l'**Agent** tourne sur la machine avec l'autoprotection activée, utilisez le menu contextuel de l'**Agent**).
3. Apportez les modifications nécessaires dans le fichier de configuration du **Serveur**.
4. Démarrez le **Serveur** avec la commande se trouvant dans le menu Démarrer → Tous les programmes → Dr.Web Enterprise Server → Contrôle du Serveur → Démarrer.

Format du fichier de configuration de Dr.Web Enterprise Server

Pour décrire le format du fichier de configuration du **Serveur**, la grammaire formelle basée sur la forme EBNF est utilisée et comprend la légende suivante :

- ◆ (...) — groupe de symboles (fragment du fichier de configuration) ;
- ◆ '...' — symbole terminal ;
- ◆ <...> — symbole non terminal ;
- ◆ | — symbole de sélection d'un des éléments proposés ;
- ◆ (...) ? — le symbole (ou groupe de symboles entre guillemets) se trouvant à gauche de l'opérateur n'est pas obligatoire (peut être utilisé 0 ou 1 fois) ;
- ◆ (...) * — le symbole (ou groupe de symboles entre guillemets) se trouvant à gauche de l'opérateur peut se répéter n'importe quel nombre de fois (il peut également être omis) ;
- ◆ (...) + — le symbole (ou groupe de symboles entre



guillemets) se trouvant à gauche de l'opérateur peut être utilisé 1 fois ou plus d'une fois ;

- ◆ [...] – n'importe quel symbole appartenant à la plage spécifiée ;
- ◆ point à la fin – symbole spécifique désignant la fin de la règle.

Format du fichier de configuration du Serveur :

```
<règle> := (<paramètre> '"'<valeur>'"' )? ( ';' <commentaire> )? .
<paramètre> := <mot> .
<valeur> := (<mot> <séparateur>*)* .
<mot> := ([a-zA-Z] | [0-9] | <symbole spécifique>)+ .
<symbole spécifique> := '&&' | '&r' | '&t' | '&n' | '&v' |
'&f' | '&b' | '&e' | '&l' | '&s' .
<séparateur> := \s | \t | \r | \n | \f .
```

Le fichier de configuration est au format texte. Les éléments structurels principaux du fichier sont les mots séparés par des séparateurs — des espaces (\s), symboles de tabulation (\t), retour à la ligne (\r), saut de ligne (\n), saut de format (\f). Toute séquence de symboles limitée par les guillemets droits "... " est compris comme un mot.

Le mot peut également comprendre (sans ruptures) des séquences spéciales de deux symboles commençant par le perluète (ampersand, &). Elles sont interprétées de la façon suivante :

- ◆ && — comme le symbole & ,
- ◆ &r — symbole de retour à la ligne,
- ◆ &t — tabulation,
- ◆ &n — symbole de saut de ligne,
- ◆ &v — tabulation verticale,
- ◆ &f — saut de format,
- ◆ &b — recul d'un pas,
- ◆ &e — symbole d'égalité (=) ,
- ◆ &l —trait vertical (|) ,



- ◆ &s — espace.

Le dernier perluète (&) dans la ligne signifie la même chose que &n.



Ainsi, le perluète standard (non utilisé pour déterminer une séquence spéciale) doit être doublé.

Les commentaires commencent par un point-virgule et continuent jusqu'à la fin de la ligne.

La configuration du **Serveur** est spécifiée dans le fichier de configuration sous forme de consignes dont chacune est un paramètre fait d'un mot suivi de sa valeur (un ou plusieurs mots).

Les règles disponibles sont décrites ci-dessous. L'ordre des règles dans le fichier n'a pas d'importance. Entre les symboles < > se trouvent les valeurs des paramètres spécifiés par l'utilisateur.

- ◆ Name <nom> j

Détermine le nom du **Serveur** auquel il va répondre lors des recherches du **Serveur** par l'**Agent** ou par le **Centre de Gestion**. La valeur par défaut est une ligne vide (""), qui signifie l'utilisation du nom du poste.

- ◆ Threads <nombre>

Le nombre de thread du **Serveur** servant les clients. La valeur spécifiée par défaut est 5. Il n'est pas recommandé de modifier la valeur du paramètre sans avoir contacté le service de support technique.

- ◆ DBPool <nombre>

Le nombre de connexions de la base au **Serveur**. Pour les **Serveurs** Windows et **Serveurs** UNIX, la valeur spécifiée par défaut est 2. Il n'est pas recommandé de modifier la valeur du paramètre sans avoir contacté le service de support technique.

- ◆ MaximumAuthorizationQueue <nombre>

Détermine le nombre maximum de postes dans la file pour



l'approbation sur le **Serveur**. Il n'est pas recommandé de modifier la valeur du paramètre sans avoir contacté le service de support technique.

◆ **Newbie** <mode>

Le mode d'accès des nouveaux postes peut avoir les valeurs suivantes : `Open`, `Close` ou `Approval` (la valeur par défaut est `Approval`). Pour en savoir plus, consultez le paragraphe [Politique de connexion des nouveaux postes](#).

◆ **UnauthorizedToNewbie** <mode>

Le mode peut prendre la valeur `Yes` — ce qui signifie que les postes non approuvés (par exemple en cas d'endommagement de la base de données) seront mis en mode novice de manière automatique, sinon le paramètre prend la valeur `No` (par défaut) correspondant au mode standard de fonctionnement.

◆ **WEBStatistics** "Interval=<nombre>
Server=<adresse_du_Serveur>
URL=<répertoire>
ID=<ID_client>
User=<utilisateur>
Password=<mot_de_passe>
Proxy=<Serveur_proxy>
ProxyUser=<utilisateur_proxy>
ProxyPassword=<mot_de_passe_proxy>"

C'est une description du serveur web sur lequel **Serveur Enterprise** va publier les statistiques sur les virus détectés.

La périodicité de publication est spécifiée en minutes, par défaut c'est 30.

L'adresse du Serveur par défaut est `stat.drweb.com:80`

URL par défaut `/update`.

ID — identificateur du client (par défaut il est calculé depuis la



clé serveur `enterprise.key`).

Les champs `User` et `Password` décrivent la procédure d'authentification sur le serveur web, les restes - Serveur proxy et l'authentification sur le serveur proxy. Par défaut les champs sont vides (aucune authentification n'est requise).

Pour accéder aux informations sauvegardées sur le Serveur de statistiques, veuillez contacter le service de support technique.

◆ Encryption `<mode>`

Mode de chiffrement du trafic. Les valeurs autorisées sont les suivantes : `Yes`, `No`, `Possible` (par défaut c'est `Yes`). Pour en savoir plus, consultez le paragraphe [Chiffrement et compression du trafic](#).

◆ Compression `<mode>`

Mode de compression du trafic. Les valeurs avancées : `Yes`, `No`, `Possible` (par défaut c'est `No`). Pour en savoir plus, consultez le paragraphe [Chiffrement et compression du trafic](#).

◆ `InstallAccess`, `AgentAccess` et `LinksAccess` ne s'affichent pas dans le fichier de configuration si la case **Utiliser cette liste d'accès** n'est pas cochée (voir [Configuration de Dr.Web Enterprise Server](#)). Si la case est cochée, les valeurs affichées des paramètres désactivés sont "none". Pour les paramètres activés, les adresses spécifiées seront affichées.

◆ Database `<DRIVER>` from `<PATH>` using `<PARAMETERS>`

Détermination de la base de données. `<DRIVER>` — nom du driver de la base, `<PATH>` — chemin depuis lequel le driver sera téléchargé, `<PARAMETERS>` — paramètres de connexion avec le Serveur de la BD. Pour en savoir plus, consultez le paragraphe [Configuration de la BD](#).



Cette règle ne peut être utilisée dans le fichier de configuration qu'une seule fois.



- ◆ Alert `<DRIVER>` from `<PATH>` using `<PARAMETERS>`

Détermination du "notificateur". `<DRIVER>` — nom du driver du notificateur, `<PATH>` — chemin depuis lequel le driver sera téléchargé, `<PARAMETERS>` — paramètres du notificateur. Pour en savoir plus, consultez le paragraphe [Configuration des notifications](#).



Cette règle ne peut être utilisée dans le fichier de configuration qu'une seule fois.

Les paramètres figurant dans le champ using de cette notice ainsi que dans la notice suivante sont séparés par des espaces. Le nom du paramètre est séparé de sa valeur par un signe égal (=) qui ne doit pas être délimité par des espaces. Si le paramètre peut prendre plusieurs valeurs, les valeurs doivent être délimitées par un trait vertical (|). Si la valeur du paramètre contient un signe égal, un trait vertical ou un espace, ils doivent être remplacés par les séquences respectives `&e`, `&l`, `&s`.

- ◆ transport `<NAME>` `<STREAM>` `<DATAGRAM>`

Détermination des protocoles de transport et leur rattachement aux interfaces réseau. `<NAME>` — nom du **Serveur** spécifié comme dans la règle `name` ci-dessus, si la ligne est vide, le nom sera repris depuis `name`. `<STREAM>` (par exemple, `tcp/`), `<DATAGRAM>` (par exemple, `udp/`) sont décrits dans l'[Annexe E. Spécification de l'adresse réseau](#).

- ◆ Disable Message `<message>`

Interdire d'envoyer les messages d'un certain type, les valeurs disponibles du paramètre : type de message, la liste complète de tous les types de messages se trouve dans le répertoire `templates`.

- ◆ Disable Protocol `<protocole>`

Interdire l'utilisation d'un des protocoles Serveur, les valeurs disponibles du paramètre : `AGENT`, `SERVER`, `INSTALL`, `CONSOLE`. Par défaut, le fichier de configuration contient une



consigne qui interdit le protocole `SERVER`. Pour en savoir plus, voir [Configuration de Dr.Web Enterprise Server](#).



L'interdiction des protocoles non utilisés permet d'épargner les ressources système.

◆ `Disable Plugin <module>`

Interdire l'utilisation des modules supplémentaires du **Serveur**, la valeur possible : `WEBMIN`. Pour en savoir plus, consultez le paragraphe [Configuration de Dr.Web Enterprise Server](#).

◆ `ShowHostNames <valeur>`

Autoriser l'affichage des nom de domaine des ordinateurs à la place de l'adresse TCP dans le protocole. Les valeurs possibles : `Yes` ou `No`.

◆ `ReplaceNetBIOSNames <valeur>`

Autoriser le remplacement des noms NetBIOS des ordinateurs par le nom DNS. Les valeurs possibles : `Yes` ou `No`.

◆ **Paramètres** `Organization`, `Department`, `Country`, `Province`, `City`, `Street`, `Floor`, `Room`, `Latitude` et `Longitude` déterminent des informations supplémentaires sur l'emplacement géographique du poste ainsi que sur son emplacement au sein de l'entreprise.

◆ `TrackAgentJobs <valeur>`

Autoriser l'écriture dans la BD du résultat de l'exécution des tâches sur les postes. Les valeurs possibles : `Yes` ou `No`.

◆ `TrackAgentStatus <valeur>`

Autoriser la journalisation des modifications du statut du poste et l'écriture des informations correspondantes dans la BD. Les valeurs possibles : `Yes` ou `No`.

◆ `TrackVirusBases <valeur>`

Autoriser la journalisation du statut (jeu d'entrées, modifications)



des bases virales sur le poste et l'écriture des informations correspondantes dans la BD. Les valeurs possibles : Yes ou No.

◆ TrackAgentModules <valeur>

Autoriser l'écriture dans la BD des informations sur tous les modules de programme de l'antivirus **Dr.Web** installés sur les postes. Les valeurs possibles : Yes ou No.

◆ TrackAgentComponents <valeur>

Autoriser l'écriture dans la BD des informations sur tous les composants antivirus installés sur les postes. Les valeurs possibles : Yes ou No.

◆ KeepRunInformation <valeur>

Autoriser l'écriture dans la BD des informations sur le démarrage et l'arrêt des composants de l'**Antivirus (Scanner, Moniteurs etc.)** sur les postes. Les valeurs possibles : Yes ou No.

◆ KeepInfections <valeur>

Autoriser l'écriture dans la BD des données statistiques sur les infections détectées sur les postes de travail. Les valeurs possibles : Yes ou No.

◆ KeepScanErrors <valeur>

Autoriser l'écriture dans la BD des informations sur toutes les erreurs survenues lors du scan sur les postes. Les valeurs possibles : Yes ou No.

◆ KeepScanStatistics <valeur>

Autoriser l'écriture dans la BD des résultats du scan sur les postes. Les valeurs possibles : Yes ou No.

◆ KeepInstallation <valeur>

Autoriser l'écriture dans la BD des informations sur les installations des **Agents** sur les postes. Les valeurs possibles : Yes ou No.

◆ Quarantine <valeur>



Autoriser l'écriture du statut de la **Quarantaine** sur les postes.
Les valeurs possibles : Yes ou No.

- ◆ `UpdatesBandwidth <valeur>`
Largeur de bande passante réseau maximum en Ko lors de la transmission des mises à jour entre le **Serveur** et les **Agents**. La valeur 0 désigne une bande passante illimitée.
- ◆ `Audit <valeur>`
Autoriser la journalisation de l'audit des opérations de l'administrateur avec le **Centre de Gestion** et l'écriture du journal dans la BD. Les valeurs possibles : Yes ou No.
- ◆ `AuditInternals <valeur>`
Autoriser la journalisation de l'audit des opérations internes du **Serveur** et l'écriture du journal dans la BD. Les valeurs possibles : Yes ou No.

G2. Fichier de configuration du Centre de Gestion Dr.Web

Le fichier de configuration du **Centre de Gestion** `webmin.conf` se trouve dans le sous-répertoire `etc` du répertoire racine du **Serveur**.

Pour décrire le format du fichier de configuration du **Centre de Gestion**, la grammaire formelle basée sur la forme EBNF est utilisée et comprend la légende suivante :

- ◆ (...) – groupe de symboles (fragment du fichier de configuration) ;
- ◆ "..." – symbole terminal ;
- ◆ <...> – symbole non terminal ;
- ◆ | – symbole de sélection d'un des éléments proposés ;
- ◆ (...) ? – le symbole (ou groupe de symboles entre guillemets) se trouvant à gauche de l'opérateur n'est pas obligatoire (peut être utilisé 0 ou 1 fois) ;
- ◆ (...) * – le symbole (ou groupe de symboles entre



guillemets) se trouvant à gauche de l'opérateur peut se répéter n'importe quel nombre de fois (il peut également être omis) ;

- ◆ $(...)^+$ – le symbole (ou groupe de symboles entre guillemets) se trouvant à gauche de l'opérateur peut être utilisé 1 fois ou plus d'une fois ;
- ◆ $[...]$ – n'importe quel symbole appartenant à la plage spécifiée ;
- ◆ point à la fin – symbole spécifique désignant la fin de la règle.

Format du fichier de configuration du Centre de Gestion :

```
<règle> := <paramètre>* ( ';' <commentaire> ) ? .

<paramètre> := <unitaire> | <bloc> .
<unitaire> := <nom> <valeur> .
<groupe> := <nom> '{' ( <valeur> ' ' )+ '}' .
<bloc> := <préfixe>? <nom> '{' <unitaire>* | <groupe>* |
<accès>? | <authentification>? '}' .

<préfixe> := 'Static' | 'Handler' | 'Scripts' | 'Mixed' .
<accès> := 'Access { '
           'Secure { '
               'Priority ' <priorité>?
               ('Allow { ' <valeur>* '}' ) ?
               ('Deny { ' <valeur>* '}' ) ?
           '}'
           'InSecure { '
               'Priority ' <priorité>?
               ('Allow { ' <valeur>* '}' ) ?
               ('Deny { ' <valeur>* '}' ) ?
           '}'
       '}' .
<priorité> := 'deny' | 'allow' .

<authentification>:= 'Authorization { ' <unitaire>+ | <groupe>+ '}' .
```



```
<nom> := <mot> .  
<valeur> := <mot> <séparateur>* .  
<mot> := ( [a-zA-Z] | [0-9] | <caractère> )+ .  
<séparateur> := \s | \t | \r | \n | \f .  
<caractère> := '/' | '*' | ':' | '.' | '-' | '?' | '^' | '['  
| ']' .
```

Le fichier de configuration est au format texte. Les éléments structurels principaux du fichier sont les mots séparés par des séparateurs — des espaces (\s), symboles de tabulation (\t), retour à la ligne (\r), saut de ligne (\n), saut de format (\f).

Les commentaires commencent pas un point-virgule et continuent jusqu'à la fin de ligne.

La configuration du **Centre de Gestion** est spécifiée dans le fichier de configuration sous forme de consignes dont chacune est un des éléments décrits ci-dessous :

- ◆ un paramètre consistant en un mot (nom du paramètre) et suivi de sa valeur (un ou plusieurs mots),
- ◆ un jeu de paramètres consistant en un mot (nom du jeu) pouvant être suivi des éléments ci-dessous entre accolades :
 - simples paramètres consistant en un seul mot (nom du paramètre) suivi de sa valeur (un ou deux mot(s)),
 - groupe de paramètres consistant en un seul mot (nom du paramètre) suivi d'un ensemble de valeurs entre accolades (par un mot ou par plusieurs mots),
 - groupe de paramètres *Access* déterminant les règles d'accès aux ressources spécifiées du Serveur (voir ci-dessous),
 - groupe de paramètres *Authorization* déterminant les paramètres d'authentification pour accéder aux ressources spécifiées (voir ci-dessous).

Un préfixe peut être spécifié avant le nom de l'ensemble de paramètres - un mot déterminant le principe de traitement des paramètres de l'ensemble.



Certaines règles sont décrites ci-dessous. L'ordre des règles dans le fichier n'a pas d'importance.

La plupart des simples paramètres (unitaires) sont spécifiés avec les valeurs par défaut et ne nécessitent aucune modification. Mais lors de l'utilisation du **Serveur**, d'autres valeurs peuvent être spécifiées pour certains paramètres :

- ◆ `ServerName <nom_DNS>:<numéro_du_port>` – détermine le nom du **Serveur** et le port. Le paramètre est utilisé pour la substitution dans les requêtes adressées au **Serveur**. Il est nécessaire de spécifier les valeurs appropriées immédiatement après l'installation du **Serveur** (voir [Installation de Dr.Web Enterprise Server](#)).
- ◆ `Listen <protocole> <interface>:<numéro_du_port>` – détermine les paramètres des interfaces écoutées. Il est utilisé pour la configuration de l'accès au **Centre de Gestion**.

Les ensembles de paramètre comprennent les groupes et les paramètres suivants :

- ◆ Le préfixe (`Static`, `Script`, `Handler` ou `Mixed`) peut être placé avant le nom de l'ensemble de paramètres et définit le principe du traitement des requêtes utilisateur respectives.
 - Le préfixe `Static` définit la méthode statique du traitement assurant la transmission à l'utilisateur d'une valeur, c'est-à-dire d'un fichier demandé sans modification (par exemple une image sauvegardée sur le **Serveur**).
 - Le préfixe `Handler` définit la méthode de traitement assurant une exécution du script spécifié dans les paramètres de l'ensemble à la réception de la requête utilisateur (la correspondance des chemins désignés dans la requête n'a pas d'importance). Dans ce cas, le corps suivant de l'ensemble des règles doit contenir la règle `Script <nom_du_script>` déterminant le script exécutable.
 - Le préfixe `Scripts` définit la méthode de traitement des requêtes assurant l'exécution de tous les fichiers relatifs à la requête utilisateur en tant que scripts.



- Le préfixe `Mixed` définit la méthode mixte de traitement assurant la cumulation de deux méthodes - `Static` et `Scripts`. Dans ce cas, le corps suivant de l'ensemble des règles doit contenir le groupe des paramètres `Scripts` { `<extensions_des_scripts>` } déterminant les script exécutables (par extension). Tous les autres fichiers non correspondant aux valeurs de ce groupe de paramètres seront transmis de manière statique ("as is", sans traitement).
- ◆ Le groupe des paramètres `Access` comprend une détermination des droits d'accès aux ressources du **Serveur** lors du traitement des requêtes utilisateur reçues.
 - Le groupe `Secure` définit les droits d'accès pour les connexions sécurisées via le protocole HTTPS.
 - Le groupe `InSecure` définit les droits d'accès pour les connexions non sécurisées via le protocole HTTP.
 - Le paramètre `Priority` `<priorité>` définit la priorité du traitement des listes relatives aux connexions autorisées et interdites. Si la valeur `deny` est spécifiée, toutes les adresses non incluses dans les deux groupes (`Allow` et `Deny`) seront interdites, en cas de valeur `allow` - autorisées.
 - La liste des paramètres du groupe `Allow` définit les adresses des éléments depuis lesquels l'accès au **Serveur** sera autorisé.
 - La liste des paramètres du groupe `Deny` définit les adresses des éléments depuis lesquels l'accès au **Serveur** sera interdit.

Les adresses mentionnées dans les listes des éléments interdits/ autorisés sont spécifiées au format suivant :

pour TCP/IP: `tcp/<adresse_IP>[/<préfixe>];`

pour SPX: `spx/<numéro_du_réseau> [.<adresse_du_poste>].`

- ◆ Le groupe des paramètres `Authorization` définit les paramètres relatifs à l'authentification de l'utilisateur lors des



consultations du **Serveur** relatives au traitement des requêtes.

G3. Fichier de configuration download.conf

Le fichier download.conf :

1. Lors de la création et l'utilisation du système de cluster des **Serveurs Enterprise**, ce fichier permet de répartir la charge entre les **Serveurs** de clusters si un grand nombre de nouveaux postes est connecté.
2. Dans le cas où un port non standard est utilisé sur le **Serveur Enterprise**, ce fichier vous permet de spécifier la formation du fichier d'installation de l'**Agent**.

Le fichier `download.conf` est utilisé lors de la création du fichier d'installation de l'**Agent** pour un nouveau poste au sein du réseau antivirus. Les paramètres de ce fichier permettent de spécifier l'adresse du **Serveur Enterprise** et le port utilisés pour connecter l'installateur de l'**Agent** au **Serveur** au format suivant :

```
download = { server = '<Server_Address>'; port = <port_number> }
```

avec :

- ◆ `<Server_Address>` - l'adresse IP ou le nom DNS du **Serveur**.

Lors de la création du package d'installation de l'**Agent**, l'adresse du **Serveur** indiquée dans le fichier `download.conf` est utilisée. Si l'adresse du **Serveur** n'est pas spécifiée dans le fichier `download.conf`, la valeur du paramètre `ServerName` depuis le fichier `webmin.conf` sera utilisée. Sinon, le nom de l'ordinateur retourné par l'OS sera pris en compte.

- ◆ `<port_number>` - le port pour connecter l'installateur de l'**Agent** au **Serveur**.

Si le port n'est pas spécifié dans les paramètres du fichier `download.conf`, par défaut, le port 2193 sera utilisé (à configurer dans le **Centre de Gestion** depuis la rubrique



Administration → Configuration de Dr.Web Enterprise Server → onglet Transport).

Par défaut, le paramètre `download` dans le fichier `download.conf` est commenté. Pour utiliser le fichier `download.conf`, il est nécessaire de décommenter ce paramètre. Pour ce faire, enlevez "--" au début de la ligne et spécifiez des valeurs appropriées à l'adresse et le port du **Serveur**.

G4.Fichier de configuration du Serveur proxy

Le fichier de configuration du **Serveur proxy** `drwcsd-proxy.xml` a le format XML et se trouve :

- ◆ sous Windows : dans le dossier d'installation du **Serveur proxy**.
- ◆ sous UNIX : dans le sous-dossier `etc` du dossier d'installation du **Serveur proxy** ou bien dans le dossier d'utilisateur courant.

Élément <cache-root />

L'élément racine `<drwcsd-proxy />` peut également contenir un élément non obligatoire `<cache-root />` dans lequel le chemin vers le répertoire de cache du **Serveur proxy** est spécifié. Si l'élément `<cache-root />` n'est pas spécifié, les données mises en cache seront sauvegardées dans le répertoire temporaire de l'utilisateur.

Élément <listen />

L'élément racine `<drwcsd-proxy />` comprend un ou plusieurs éléments obligatoires `<listen />` déterminant les principaux paramètres relatifs à la réception des connexions par le **Serveur proxy**. L'élément `<listen />` contient un seul attribut obligatoire, `spec`, dont les propriétés pointent l'interface sur laquelle les



connexions entrantes des clients seront écoutées. Les propriétés de cet attribut déterminent également si le mode `discovery` sera lancé sur cette interface. L'attribut `spec` contient les propriétés suivantes :

- ◆ `protocole` – type de protocole pour réceptionner les connexions entrantes. En tant que paramètre, l'adresse écoutée par le **Serveur proxy** est spécifiée.
- ◆ `port` – numéro de port écouté par le **Serveur proxy**.
- ◆ `mode d'imitation` – mode d'imitation du **Serveur**. Ce mode permet au **Scanner réseau** de détecter le **Serveur proxy** en tant que **Enterprise Server**.
- ◆ `groupe multicast` – groupe multi-adresses dans lequel se trouve le **Serveur proxy**.

Les valeurs des propriétés de l'attribut `spec` et leurs paramètres sont présentés dans le tableau G-1.

Tableau G-1. Propriétés de l'élément `spec`

Propriété	Obligatoire	Valeurs admissibles	Paramètres des valeurs autorisées	
			admissible	par défaut
<code>protocole</code>	oui	<code>ip</code> , <code>ipx</code> , <code>netbios</code>		<code>0.0.0.0</code> – –
<code>port</code>	non	<code>port</code>		2193
<code>mode d'imitation</code>	non	<code>discovery</code>	<code>yes</code> , <code>no</code>	<code>no</code>
<code>groupe multicast</code>	non	<code>multicast</code>		<code>231.0.0.1</code>

l'attribut `spec` contient une propriété obligatoire : `protocole`, et trois propriétés non obligatoires : `port`, `mode d'imitation` et `groupe multicast`. En fonction de la valeur de la propriété `protocole`, la liste des propriétés non obligatoires spécifiées dans l'attribut `spec` peut varier.

Le tableau G-2 présente la liste des propriétés non obligatoires pouvant



être spécifiées (+) ou non spécifiées (-) dans l'attribut `spec` en fonction de la valeur du paramètre `protocole`.

Tableau G-2. Présence des propriétés non obligatoires en fonction du paramètre protocole

Protocole	Présence des propriétés		
	port	discovery	multicast
ip	+	+	+
ipx	+	+	-
netbios	+	+	-

Élément <forward />

Les paramètres déterminant la redirection des connexions entrantes sont spécifiés par l'élément `<forward />`, qui est un élément fille pour l'élément `<listen />`. L'élément `<forward />` contient un ou plusieurs attributs obligatoires `to` dont les valeurs sont les adresses des **Enterprise Server**, la connexion sera redirigée vers un de ces serveurs. L'adresse de **Enterprise Server** est spécifiée conformément à la [spécification de l'adresse réseau](#), notamment au format `tcp/<DNS_name>:<port>`.

L'élément `<forward />` est obligatoire. L'élément `<listen />` peut comprendre plusieurs éléments `<forward />`.

Algorithme de redirection si une liste des Serveurs Enterprise est présente

1. Le **Serveur proxy** charge dans la mémoire vive la liste des **Serveurs Enterprise** depuis le fichier de configuration `drwcsd-proxy.xml`.
2. L'**Agent Enterprise** se connecte au **Serveur proxy**.
3. Le **Serveur proxy** redirige l'**Agent Enterprise** vers le premier **Serveur Enterprise** mentionné dans la liste chargée dans la mémoire vive.
4. Le **Serveur proxy** effectue une rotation des éléments de la



liste chargée dans la mémoire vive en déplaçant le **Serveur Enterprise** vers la fin de la liste.



Le **Serveur proxy** ne conserve pas l'ordre modifié des **Serveurs** dans son fichier de configuration. Au redémarrage du **Serveur proxy**, la liste des **Serveurs Enterprise** est chargée dans la mémoire vive dans son état initiale dans lequel elle est enregistrée dans le fichier de configuration.

5. Lorsqu'un **Agent** suivant se connecte au **Serveur proxy**, la procédure se reproduit à partir de l'étape 2.
6. Si le **Serveur Enterprise** se déconnecte du réseau antivirus (par exemple, en cas d'arrêt ou refus de service), l'**Agent** se connecte à nouveau au **Serveur proxy** et la procédure se reproduit à partir de l'étape 2.

Exemple de fichier de configuration drwcsd-proxy.xml

```
<?xml version="1.0"?>
<drwcsd-proxy>
  <!-- Specify path to cahe directory, if not specified
  will create directory in user temp -->
  <cache-root>C:\Work\es_head\build\a-x86\bin\var</cache-
  root>

  <!-- property: ip, ipx, netbios, unx: define protocol
  family and address of addapter -->
  <!-- property: port: define port to listen on. Default
  2193 or 23 for netbios -->
  <!-- property: name: define discovery name. Default
  drwcs -->
  <!-- property: discovery: define should proxy run
  discovery server too -->
  <!-- property: multicast: define should proxy enter to
  multicast group -->

  <!-- For example -->
  <!-- Listen on IN_ADDR_ANY port 2193, run discovery on
  231.0.0.1 -->
  <listen spec="ip(), multicast() ">
  <!-- one or more forward tags-->
```



```
<forward to="tcp/server1.isp.net:2193"/>
<forward to="tcp/server2.isp.net:2193"/>
</listen>

<!-- Listen on ipv6 IN6_ADDR_ANY, port 2194, run
discovery on ff18::231.0.0.1 -->
<listen spec="ip([], port(2194), multicast())">
  <forward to="tcp/server1.isp.net:2193"/>
  <forward to="tcp/server2.isp.net:2193"/>
</listen>

<!-- Listen on default ipx, port 2194, run simple
discovery -->
<listen spec="ipx(), discovery()">
  <forward to="tcp/server1.isp.net:2193"/>
  <forward to="tcp/server2.isp.net:2193"/>
</listen>

<!-- Listen on default netbios, port 23, lana 0, run
simple discovery -->
<listen spec="netbios(), discovery()">
  <forward to="tcp/server1.isp.net:2193"/>
  <forward to="tcp/server2.isp.net:2193"/>
</listen>
</drwcsd-proxy>
```



Annexe H. Paramètres de la ligne de commande relatifs aux programmes inclus dans Dr.Web Enterprise Security Suite

H1. Introduction

Les paramètres de la ligne de commande ont une priorité supérieure à celle des paramètres définis par défaut ou à celle des paramètres permanents (spécifiés dans le fichier de configuration du **Serveur**, dans la base de registre Windows etc.). Dans certains cas décrits ci-après, les paramètres spécifiés au démarrage modifient les paramètres permanents.

Certains paramètres de la ligne de commande commencent par un trait d'union. Ces paramètres sont appelés des clés.

Beaucoup de clés peuvent être présentes sous diverses formes équivalentes. Les clés pouvant avoir une valeur logique (oui/non, interdire/autoriser) ont des variantes négatives formant des paires, par exemple la clé `-admin-rights` a la variante paire `-no-admin-rights` ayant une valeur opposée. De telles clés peuvent être spécifiées en déterminant leur valeur de manière explicite, par exemple `-admin-rights=yes` et `-admin-rights=no`.



La valeur `yes` comporte les synonymes suivants : `on`, `true`, `OK`! La valeur `no` possède les synonymes `off`, `false`.

Si la valeur de la clé contient des espaces ou des symboles de tabulation, tout le paramètre doit être mis entre guillemets comme dans l'exemple ci-dessous :

```
"-home=c:\Program Files\DrWeb Enterprise Suite"
```




Lors de la description de la syntaxe des paramètres des programmes, leur partie facultative est mise entre crochets [. . .] .



Les noms des clés peuvent être abrégés (il est possible d'omettre les derniers caractères) à condition que le nom abrégé ne corresponde pas à la partie abrégée d'une autre clé.

H2. Module d'interface Dr.Web Enterprise Agent

Le module d'interface de l'**Agent** est lancé pour chaque utilisateur enregistré sur la machine. Sur les ordinateurs sous Windows NT, Windows 2000, Windows XP, Windows 2003, le module fonctionne conformément aux droits utilisateur. Pour son fonctionnement, l'**Agent** requiert un shell utilisateur tel que **Explorateur Windows** standard ou un autre programme complètement compatible.

Syntaxe de la commande de démarrage :

`drwagnui [<clés>]`

Clés admissibles :

- ◆ `-admin-rights` ou `-no-admin-rights` — autoriser ou interdire le mode administrateur sous les OS Windows 98/Windows Me (si l'on peut classer l'utilisateur opérant sous ces versions d'OS comme administrateur). L'administrateur peut notamment modifier les paramètres de l'**Agent**. Sous Windows NT ou antérieurs, ceci est déterminé par le système de privilèges de l'OS. Par défaut ce n'est pas autorisé.
- ◆ `-delay=<nombre>` — le délai à l'expiration duquel le mot de bienvenue sera affiché à l'utilisateur. La valeur par défaut est 2 minutes, la valeur `-1` désactive l'affichage du mot de bienvenue.
- ◆ `-help` — afficher la rubrique d'aide sur le format de la commande.



- ◆ `-trace` — réaliser une journalisation détaillée de l'emplacement de l'erreur survenue, cette clé est applicable dans d'autres applications.

H3. Dr.Web Enterprise Agent

Les paramètres de l'**Agent** sont enregistrés dans la base de registre Windows, dans la branche `HKEY_LOCAL_MACHINE\SOFTWARE\IDAVLab\Enterprise Suite\Dr.Web Enterprise Agent\Settings`, pour les paramètres spécifiés par les clés, le nom du paramètre correspond au nom de la clé.

La liste des Serveurs **SGMAJ** auxquels l'**Agent** peut se connecter est sauvegardée dans les fichiers `.config` se trouvant dans les sous-répertoires du dépôt des produits (sous Windows : `DrWeb Enterprise Server\var\repository\`).

En cas de démarrage de l'**Agent** avec des paramètres spécifiés de manière explicite, ceux-ci seront non seulement utilisés dans la session courante mais également enregistrés dans la base de registre en tant que paramètres permanents. Ainsi, une fois lancé avec tous les paramètres nécessaires, **Enterprise Agent** ne requiert aucune spécification des paramètres lors des lancements ultérieurs.



Les paramètres de l'**Agent** spécifiés directement sur le poste sont écrasés par les valeurs reçues depuis le **Serveur**.

Dans le cas, où une liste vide des **Serveurs** auxquels le poste peut se connecter est spécifiée sur le **Serveur**, la liste des **Serveurs** établie sur le poste sera prise en compte.

L'**Agent Enterprise** démarre par le système en tant que service, et est géré via le **Panneau de configuration**.

Syntaxe de la commande de démarrage :

```
drwagntd [<clés>] [<Serveurs>]
```



Clés

Clés admissibles :

- ◆ `-compression=<mode>` — mode de compression du trafic de **Serveur**. Les valeurs possibles sont les suivantes : `yes`, `no`, `possible` (la valeur par défaut est `possible`).
- ◆ `-control=<action>` — gestion du statut du service de l'**Agent**. Les actions possibles :
 - `install` — installer le service,
 - `uninstall` — supprimer le service,
 - `start` — lancer le service (uniquement sous Windows NT ou supérieur),
 - `stop` — arrêter le service (uniquement sous Windows NT ou supérieur),
 - `restart` — redémarrer le service (uniquement sous Windows NT ou supérieur).
- ◆ `-crypt=<mode>` — mode de chiffrement du trafic de **Serveur**. Les valeurs possibles sont les suivantes : `yes`, `no`, `possible` (la valeur par défaut est `yes`).
- ◆ `-drweb-key=<clé_de_licence>` — la clé de licence de l'utilisateur. Cette clé sera utilisée par le logiciel client en cas d'absence prolongée de connexion avec le **Serveur** ainsi que lorsque la clé reçue depuis le **Serveur** a expiré. Lorsque la connexion avec le **Serveur** est opérationnelle, la clé n'est pas nécessaire. Par défaut — n'importe quelle clé valide se trouvant dans le répertoire spécifié avec la clé `-home`.
- ◆ `-help` — afficher la rubrique d'aide relative au format de la commande et à ses paramètres. L'option est analogue à la clé `-help` du module d'interface, voir l'Annexe [H2. Module d'interface de l'Agent Dr.Web Enterprise Agent](#).
- ◆ `-home=<répertoire>` — le répertoire vers lequel est installé l'**Agent**. Si la clé n'est pas spécifiée, le répertoire dans lequel se trouve le fichier exécutable de l'**Agent** sera pris en compte.
- ◆ `-key=<clé_publique_du_Serveur>` — le fichier de la clé



publique du **Serveur**, par défaut - drwcsd.pub dans le répertoire paramétré par la clé -home.

- ◆ -log=<fichier_de_log> — le fichier de log de l'**Agent**, par défaut ce fichier se trouve dans le sous-répertoire logs du répertoire d'installation de l'**Agent**. Pour sauvegarder le fichier de log relatif à la suppression de l'**Agent**, le répertoire temporaire système est utilisé.
- ◆ -retry=<nombre> — nombre de tentatives de recherche du **Serveur** par envoi de requêtes multicast (en cas d'utilisation de la recherche), avant que le message d'échec ne s'affiche. La valeur par défaut est **3**.
- ◆ -rotate=<N><f>, <M><u> — mode de rotation du journal de l'**Agent** avec :
 - <N> — nombre total de fichiers de log (y compris le journal courant et ceux d'archive) ;
 - <f> — format de sauvegarde des fichiers de log, les valeurs possibles sont les suivantes : z (gzip) - compresser les fichiers (utilisé par défaut) ou p (plain) - ne pas compresser les fichiers ;
 - <M> — taille du fichier ;
 - <u> — unité de mesure, les valeurs possibles sont les suivantes : k (kilo), m (mega), g (giga).

Les valeurs par défaut sont 10,10m, ce qui enjoint de sauvegarder 10 fichiers, de 10 Mo chacun, et d'utiliser la compression. Il est également possible d'utiliser le format spécialisé none (-rotate=none) - ce qui désigne "ne pas utiliser la rotation, écrire toujours dans le même fichier à taille illimitée".

Dans le mode de rotation, les noms des fichiers de log sont générés au format suivant : file.<N>.log ou file.<N>.log.dz, avec <N> - numéro d'ordre : 1, 2, etc.

Si le nom du fichier de log (voir ci-dessus la clé -log) est, par exemple, file.log. Dans ce cas-là :

- file.log — le fichier courant (vers lequel l'écriture est effectuée),



- `file.1.log` — le fichier précédent,
- `file.2.log` etc. — l'ordre croissant des nombres correspond aux versions plus anciennes du fichier.
- ◆ `-save <adresse IP>` — vérifie la validité de l'adresse IP du **Serveur** et sauvegarde les paramètres dans la base de registre.
- ◆ `-spiderstat=<espacement>` — intervalle en minutes d'envoi vers le **Serveur** de statistiques de **SpIDer Guard**, la valeur par défaut est **30**. Les statistiques seront envoyées vers le **Serveur** avec les espacements spécifiés à condition qu'il y ait des changements.
- ◆ `-timeout=<durée>` — délai maximum d'attente pour chaque réponse en secondes lors de la recherche du **Serveur**. La réception des messages de réponse continue jusqu'au moment où la durée d'attente ne dépasse pas la valeur spécifiée. La valeur par défaut est **5**.
- ◆ `-trace` — réaliser une journalisation détaillée de l'emplacement de l'erreur survenue, la clé est applicable dans d'autres applications.
- ◆ `-verbosity=<niveau_de_détail>` — niveau de détail du journal. La valeur par défaut est `INFO`, il est possible de mettre les valeurs suivantes `ALL`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `DEBUG`, `TRACE3`, `TRACE2`, `TRACE1`, `TRACE`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `CRIT`. Les valeurs `ALL` et `DEBUG3` sont les synonymes (voir aussi [Annexe L. Format des fichiers de log](#)).



Cette clé détermine un niveau de détail de la journalisation dans le fichier spécifié par la clé qui suit après `-log` (voir ci-dessus). Une commande peut comprendre plusieurs clés de ce type.

Les clés `-verbosity` et `-log` sont sensibles à la position.

En cas d'utilisation de ces deux clés à la fois, la clé `-verbosity` doit précéder la clé `-log`: la clé `-verbosity` modifie le niveau de détail des journaux se trouvant sur les chemins spécifiés après dans la ligne de commande.



Serveurs

<Serveurs> — liste des **Serveurs**. Par défaut - drwcs@udp/231.0.0.1:2193, ce qui enjoint de rechercher le **Serveur** drwcs en utilisant les requêtes multicast pour le groupe 231.0.0.1 port 2193.

H4. Installateur réseau

Syntaxe de la commande de démarrage :

```
drwinst [<clés>] [<variables>] [<Serveurs>]
```

Clés

Clés applicables :

- ◆ -compression=<mode> — mode de compression du trafic de **Serveur**. Les valeurs possibles sont les suivantes : yes, no, possible (par défaut c'est no).
- ◆ -help — afficher la rubrique d'aide. Analogue au module d'interface de l'**Agent**.
- ◆ -home=<répertoire> — répertoire d'installation. Par défaut c'est "Program Files\DrWeb Enterprise Suite" sur le disque système.
- ◆ -id=<identificateur du poste> — spécifie l'identificateur du poste sur lequel est installé l'**Agent**.
- ◆ -interactive — lancer l'installateur en mode interactif.

La description de l'installation de l'**Agent** en mode interactif (graphique) se trouve dans le paragraphe [Installation de Dr.Web Enterprise Agent](#).

Si la clé -interactive n'est pas spécifiée, l'installation de l'**Agent** se fait avec l'installateur en tâche de fond (voir [Installation Dr.Web Enterprise Agent](#)). Dans ce cas-là, l'interface



graphique interactive de l'installateur peut être affichée en cas d'erreur d'installation ou en cas d'erreur survenue lors du démarrage de l'installation.



Cette clé n'est pas opérationnelle en cas d'installation distante des **Agents** via le **Centre de Gestion**.

La clé `-interactive` ne peut pas être appliquée en même temps que les [variables](#). Si des variables sont spécifiées, elle seront ignorées.

- ◆ `-key=<clé_publicue>` — chemin complet vers le fichier de la clé publique du **Serveur**. Par défaut la clé `drwcsd.pub` se trouve dans le sous-répertoire `Installer` du répertoire d'installation du **Serveur**.
- ◆ `-log=<fichier_de_log>` — chemin complet vers le fichier de log d'installation (spécifié lors de l'installation de l'**Agent**) ou vers le fichier de log de suppression (spécifié lors de la désinstallation de l'**Agent**).

Pour sauvegarder le fichier de log d'installation, le sous-répertoire `logs` du répertoire spécifié par la clé `-home` lors de l'installation est utilisé par défaut.

Pour sauvegarder le fichier de log de suppression, le répertoire temporaire utilisateur est utilisé par défaut.



Si la clé `-log` n'est pas spécifiée, les noms des fichiers de log seront générés de manière automatique en utilisant GUID et le nom de l'ordinateur.

- ◆ `-platforms=p1,p2,p3...` — ordre de téléchargement des plateformes (par défaut standard, voir l'[Annexe J. Utilisation du script d'installation initiale pour Dr.Web Enterprise Agent](#)).
- ◆ `-pwd=<mot_de_passe>` — entrez le mot de passe de l'**Agent** pour accéder au **Serveur**.
- ◆ `-regagent` — enregistrer l'**Agent** dans la liste **Ajout/Suppression de programmes (Add or Remove Programs)**.



- ◆ `-retry=<nombre>` — analogue à la clé de l'**Agent**.
- ◆ `-script=<nom_du_script>` — spécifie le fichier avec un script exécutable. A utiliser avec la clé `-uninstall` afin de désinstaller le logiciel antivirus.
- ◆ `-timeout=<durée>` — analogue à la clé de l'**Agent**.
- ◆ `-trace` — réaliser une journalisation détaillée de l'emplacement de l'erreur survenue, la clé est applicable dans d'autres applications.
- ◆ `-uninstall` — désinstallation du package depuis le poste avec le script de désinstallation (voir la clé `-script`). Si le script n'est pas spécifié de manière explicite, le script interne de désinstallation sera exécuté.

En cas d'absence de clé (équivalent à la clé `-no-uninstall`), l'installation sera effectuée.

- ◆ `-verbosity=<niveau_de_détail>` — niveau de détail du journal (analogue à la journalisation relative à l'**Agent**, voir [H3. Dr.Web Enterprise Agent](#)). Par défaut c'est ALL.



Cette clé détermine un niveau de détail de la journalisation dans le fichier spécifié par la clé qui suit après `-log` (voir ci-dessus). Une commande peut comprendre plusieurs clés de ce type.

Les clés `-verbosity` et `-log` sont sensibles à la position.

En cas d'utilisation de ces deux clés à la fois, la clé `-verbosity` doit précéder la clé `-log`: la clé `-verbosity` modifie le niveau de détail des journaux se trouvant sur les chemins spécifiés après dans la ligne de commande.

Variables

Les variables sont spécifiées après les clés sous forme de listes dont les éléments ont le format suivant :

`<variable>=<valeur>`



Les variables les plus importantes :

- ◆ `agent.language="C:\Program Files\DrWeb Enterprise Suite\RU-ESAU1.DWL"` — ce paramètre détermine le mode d'affichage du menu contextuel de l'**Agent** en russe. Comme valeur de la clé, indiquez le chemin complet vers le fichier de ressources langue (par défaut c'est l'anglais).
- ◆ `spider.install=no` — ne pas installer **SpIDer Guard**. En cas d'absence de la variable — installer.
- ◆ `spiderml.install=no` — idem, ne pas installer **SpIDer Mail**.
- ◆ `scanner.install=no` — idem, ne pas installer le **Scanner Dr.Web pour Windows**.
- ◆ `spidergate.install=no` — idem, ne pas installer **SpIDer Gate**.
- ◆ `agent.id=<identificateur>`.
- ◆ `agent.password=<mot_de_passe>` — identificateur et mot de passe du poste ; si les paramètres sont spécifiés, le poste se connecte avec les paramètres définis et non pas comme un "novice".

Serveurs

La liste des **Serveurs** est la même que celle décrite pour l'**Agent**.

H5. Dr.Web Enterprise Server

Il existe plusieurs variantes des commandes de démarrage du **Serveur** qui sont décrites séparément ci-dessous.

Les commande décrites dans les paragraphes [H5.1](#) – [H5.5](#) sont cross-plateforme, elles peuvent être utilisées sous Windows, ainsi que sous les OS de la famille UNIX (si le contraire n'est pas spécifié).



H5.1. Gestion du Serveur Dr.Web Enterprise Server

`drwcsd` [*<clés>*] — spécifier les paramètres du **Serveur** (les clés respectives sont décrites ci-dessous).

H5.2. Commandes standard

- ◆ `drwcsd start` — démarrer le **Serveur**.
- ◆ `drwcsd restart` — réaliser un redémarrage complet du service de **Serveur** (la commande est exécutée comme la paire : `stop` et puis `start`).
- ◆ `drwcsd stop` — arrêter le **Serveur**.
- ◆ `drwcsd reconfigure` — relire le fichier de configuration et redémarrer (la commande s'exécute plus vite, sans lancer un nouveau processus).
- ◆ `drwcsd retemplate` — relire les templates des notifications depuis le disque.
- ◆ `drwcsd verifyakey <chemin_vers_la_clé>` — vérification de la validité de la clé Agent (`agent.key`).
- ◆ `drwcsd verifyekey <chemin_vers_la_clé>` — vérification de la validité de la clé Serveur (`enterprise.key`).
- ◆ `drwcsd verifyconfig <chemin_vers_la_clé>` — vérification de la syntaxe du fichier de configuration du **Serveur** (`drwcsd.conf`).
- ◆ `drwcsd stat` — sortie des statistiques relatives au fonctionnement vers le fichier de log : heure CPU, utilisation de la mémoire etc. (sous UNIX - équivalent de la commande `send_signal WINCH` ou `kill SIGWINCH`).



H5.3. Commandes de gestion de la BD

Initialisation des bases de données

`drwcsd [<clés>] initdb <clé_Agent> [<script_BD> [<fichier_ini> [<mot_de_passe>]]]` — initialisation de la base de données.

- ◆ `<clé_Agent>` — chemin vers le fichier clé de licence d'**Enterprise Agent** `agent.key` (obligatoire à spécifier).
- ◆ `<script_BD>` — script d'initialisation de la BD. La valeur spéciale - (moins) enjoint de ne pas utiliser le script.
- ◆ `<fichier_ini>` — fichier préconfiguré au format `drweb32.ini` qui détermine la configuration initiale des composants **Dr.Web** (pour le groupe **Everyone**). La valeur spéciale - (moins) enjoint de ne pas utiliser ce fichier.
- ◆ `<mot_de_passe>` — mot de passe initial de l'administrateur du **Serveur** (le nom est **admin**). Par défaut c'est **root**.



Le signe "moins" peut être omis s'il n'y a pas de paramètres après.

Paramétrage de l'initialisation de la base de données

En cas d'utilisation de la BD interne, les paramètres d'initialisation peuvent être spécifiés depuis un fichier externe. Dans ce cas-là, la commande suivante est utilisée :

`drwcsd.exe initdbex <response-file>`

`<response-file>` - fichier dans lequel sont enregistrés les paramètres d'initialisation de la BD, chacun d'eux à la ligne et dans le même ordre que les paramètres `initdb`.



Le fichier a le format suivant :

```
<chemin_vers_le_fichier_clé>  
<chemin_vers_le_fichier_initdb.sql>  
<chemin_vers_le_fichier_drweb32.ini>  
<mot_de_passe_administrateur>
```



En cas d'utilisation du response-file sous Windows, il est possible d'utiliser n'importe quels symboles dans le mot de passe administrateur.

Les dernières lignes qui suivent le paramètre ne sont pas obligatoires. Si la ligne représente le signe "-" (un signe moins), la valeur par défaut sera appliquée (comme en cas de `initdb`).

Mise à jour de la base de données

`drwcsd [<clés>] updatedb <script>` — effectuer une manipulation avec la base de données (par exemple une mise à jour en cas de changement de version) en exécutant les opérateurs SQL depuis le fichier `<script>`.

Mise à jour de la version de la base de données

`drwcsd upgradedb <répertoire>` — démarrer le **Serveur** pour mettre à jour la structure de la base de données lors de la mise à niveau vers une nouvelle version (voir le répertoire `update-db`).

Exportation de la base de données

`drwcsd exportdb <fichier>` — exportation de la base de données vers le fichier spécifié.



Exemple pour OS Windows :

```
C:\Program Files\DrWeb Enterprise Server\bin
\drwcsd.exe -home="C:\Program Files\DrWeb
Enterprise Server" -var-root="C:\Program Files
\DrWeb Enterprise Server\var" -verbosity=all
exportdb "C:\Program Files\DrWeb Enterprise
Server\esbase.es"
```

Sous **UNIX**, l'action s'exécute sous le nom de l'utilisateur `drwcs:drwcs` vers le répertoire `$DRWCS_VAR` (excepté **FreeBSD**, qui enregistre par défaut le fichier vers le répertoire depuis lequel a été lancé le script ; si le chemin est spécifié de manière explicite, le répertoire doit être disponible en écriture pour `<utilisateur>:<groupe>` qui ont été créés lors de l'installation, par défaut c'est `drwcs:drwcs`).

Importation de la base de données

`drwcsd importdb <fichier>` — importation de la base de données depuis le fichier spécifié (le contenu périmé de la BD sera effacé).

Vérification de la base de données

`drwcsd verifydb` — démarrer le **Serveur** pour vérifier la base de données. A la fin de vérification, le **Serveur** écrit des informations sur les résultats vers le fichier de log (par défaut - `drwcsd.log`).

H5.4. Commandes de gestion du dépôt des produits

- ◆ `drwcsd syncrepository` — réaliser une synchronisation du dépôt des produits depuis le **SGMAJ**. Arrêtez le **Serveur** avant de lancer la commande !
- ◆ `drwcsd rerepository` — relire le dépôt des produits depuis le disque.



H5.5. Copie de sauvegarde des données critiques du Serveur Dr.Web Enterprise Server

La commande ci-dessous permet de créer une copie de sauvegarde des données critiques du **Serveur** (le contenu de la base de données, le fichier clé de licence du **Serveur**, la clé privée de chiffrement, le fichier de configuration du **Serveur** et du **Centre de Gestion**) :

```
drwcsd -home=<chemin> backup [<répertoire>
[<nombre>]] — les données critiques du Serveur seront
sauvegardées vers le répertoire spécifié. -home définit le répertoire de
l'installation du Serveur. <nombre> - nombre de copies
sauvegardées du même fichier.
```

Exemple pour OS Windows :

```
C:\Program Files\DrWeb Enterprise Server
\bin>drwcsd -home="C:\Program Files\DrWeb
Enterprise Server" backup C:\a
```

Les copies de sauvegarde sont enregistrées au format `.dz` compatible avec `gzip` ainsi qu'avec d'autres utilitaires d'archivage. Après l'extraction, tous les fichiers, excepté le contenu de la BD, sont prêts à être utilisés. Le contenu de la BD sauvegardé dans la copie de sauvegarde peut être importé vers une autre BD du **Serveur** avec la clé `importdb`, ainsi, les données seront récupérées (voir le paragraphe [Récupération de la BD Dr.Web Enterprise Security Suite](#)).

ESS à partir de la version **4.32** réalise une procédure régulière de copie de sauvegarde des informations importantes vers `\var\Backup` du répertoire du **Serveur**. Pour cela, la planification du **Serveur** inclut une tâche correspondante. Si cette tâche n'est pas paramétrée, il est recommandé de la créer. La tâche de copie de sauvegarde des données critiques est notamment absente lorsque la version du **Serveur** - **4.32** à été installée au départ et les versions suivantes par-dessus.



H5.6. Commandes disponibles uniquement sous Windows®

- ◆ `drwcsd [<clés>] install` — installer le service de **Serveur** dans le système.
- ◆ `drwcsd uninstall` — supprimer le service de **Serveur** depuis le système.
- ◆ `drwcsd kill` — arrêt forcé du service de **Serveur** (dans le cas où la terminaison normale a été un échec). Il n'est pas recommandé d'exécuter cette commande sans nécessité urgente.
- ◆ `drwcsd silent` — interdire la sortie des messages depuis le **Serveur**. La commande est utilisée dans les fichiers de commande afin de désactiver l'interactivité du **Serveur**.

H5.7. Commandes disponibles uniquement sous les OS de la famille UNIX®

- ◆ `drwcsd config` — équivalent de la commande `reconfigure` ou `kill SIGHUP` — redémarrage du **Serveur**.
- ◆ `drwcsd dumpimportdb` — écrire dans le fichier de log du **Serveur** des informations détaillées lors de l'importation vers la base interne ou externe.
- ◆ `drwcsd interactive` — démarre le **Serveur** en mode interactif.
- ◆ `drwcsd newkey` — génération des nouvelles clés de chiffrement (`drwcsd.pri` et `drwcsd.pub`).
- ◆ `drwcsd readtempl` — relire les templates de notifications depuis le disque.
- ◆ `drwcsd readrepo` — relire le dépôt des produits depuis le disque.
- ◆ `drwcsd selfcert` — génération d'un nouveau certificat SSL (`certificate.pem`) et clé privée RSA (`private-key.pem`).



- ◆ `drwcsd shell <nom_du_fichier>` – lancement du fichier binaire.
- ◆ `drwcsd showpath` – afficher tous les chemins du programme enregistrés dans le système.
- ◆ `drwcsd status` – afficher le statut courant du **Serveur** (en cours, arrêté).

H5.8. Description des clés

Clés cross-plateforme

- ◆ `-activation-key=<clé_de_licence>` — fichier clé de licence du **Serveur**. Par défaut, c'est le fichier `enterprise.key` se trouvant dans le sous-répertoire `etc` du répertoire racine.
- ◆ `-bin-root=<répertoire_pour_exécutables>` — chemin vers les fichiers exécutables. Par défaut, c'est le sous-répertoire `bin` du répertoire racine.
- ◆ `-conf=<fichier_de_configuration>` — nom et emplacement du fichier de configuration du **Serveur**. Par défaut, c'est le fichier `drwcsd.conf` se trouvant dans le sous-répertoire `etc` du répertoire racine.
- ◆ `-daemon` — pour les plateformes Windows ceci désigne le lancement en tant que service ; en cas de plateformes UNIX : lancement en tant que service (daemon) : passer vers le répertoire racine, se déconnecter du terminal et basculer vers le mode en tâche de fond.
- ◆ `-db-verify=on` — vérifier l'intégrité de la BD au démarrage du **Serveur**. La valeur par défaut est spécifiée. Il est fortement déconseillé de lancer la clé avec une valeur opposée spécifiée de manière explicite, excepté en cas de démarrage immédiat après la vérification de la BD avec la commande `drwcsd verifydb` (voir ci-dessus).
- ◆ `-help` — afficher la rubrique d'aide. Ceci est équivalent aux programmes décrits ci-dessus.
- ◆ `-hooks` — autoriser l'exécution par le **Serveur** des scripts d'extension utilisateur se trouvant dans le dossier suivant :



- sous Windows : `var\extensions`
- sous FreeBSD et OC Solaris : `/var/drwcs/extensions`
- sous Linux : `/var/opt/drwcs/extensions`

se trouvant dans le répertoire d'installation de **Serveur Enterprise**. Les scripts sont destinés à automatiser les opérations de l'administrateur afin de faciliter et d'accélérer l'exécution de certaines tâches. Par défaut, tous les scripts sont désactivés.

- ◆ `-home=<racine>` — répertoire d'installation du **Serveur** (répertoire racine). La structure de ce répertoire est décrite dans le paragraphe [Installation de Dr.Web Enterprise Server sous OS Windows®](#). Par défaut c'est le répertoire courant au démarrage.
- ◆ `-log=<journal>` — nom du fichier de log du **Serveur**. A la place du nom de fichier il est possible de mettre le signe "moins" (uniquement pour le **Serveur** sur plateforme UNIX), ce qui désigne la sortie du journal vers la sortie standard. Par défaut : en cas de plateformes Windows - `drwcsd.log` dans le répertoire spécifié par la clé `-var-root`, en cas de plateformes UNIX - avec la clé `-syslog=user` (voir ci-dessous).
- ◆ `-private-key=<clé_privée>` — clé privée du **Serveur**. Par défaut, c'est `drwcsd.pri` dans le sous-répertoire `etc` du répertoire racine.
- ◆ `-rotate=<N><f>, <M><u>` - mode de rotation du log de l'**Agent**, où :
 - `<N>` - nombre total de fichiers de log (y compris le journal courant et ceux d'archive) ;
 - `<f>` — format de sauvegarde des fichiers de log, les valeurs possibles sont les suivantes : `z` (gzip) - compresser les fichiers (utilisé par défaut) ou `p` (plain) - ne pas compresser les fichiers.
 - `<M>` — taille du fichier ;
 - `<u>` — unité de mesure, les valeurs possibles sont les suivantes : `k` (kilo), `m` (mega), `g` (giga).



Les valeurs par défaut sont 10,10m, ce qui enjoint de sauvegarder 10 fichiers, de 10 Mo chacun, et d'utiliser la compression. Il est également possible d'utiliser le format spécialisé none (-rotate=none) - ce qui désigne "ne pas utiliser la rotation, écrire toujours dans le même fichier à taille illimitée".

Dans le mode de rotation, les noms des fichiers de log sont générés au format suivant : file.<N>.log ou file.<N>.log.dz, avec <N> - numéro d'ordre : 1, 2, etc.

Si le nom du fichier de log (voir ci-dessus la clé -log) est, par exemple, file.log. Dans ce cas-là :

- file.log — fichier courant (vers lequel l'écriture est effectuée),
 - file.1.log — fichier précédent,
 - file.2.log etc. — l'ordre croissant des nombres correspond aux versions plus anciennes du fichier.
- ◆ -trace — réaliser une journalisation détaillée de l'emplacement de l'erreur survenue.
 - ◆ -var-root=<répertoire_pour_modifiables> — chemin vers le répertoire vers lequel le **Serveur** est autorisé à écrire et qui est destiné à sauvegarder les fichiers modifiables (par exemple les journaux ainsi que les fichiers du dépôt des produits). Par défaut c'est le sous-répertoire var du répertoire racine.
 - ◆ -verbosity=<niveau_de_détail> — niveau de détail du journal. Par défaut c'est WARNING, les valeurs possibles sont les suivantes : ALL, DEBUG3, DEBUG2, DEBUG1, DEBUG, TRACE3, TRACE2, TRACE1, TRACE, INFO, NOTICE, WARNING, ERROR, CRIT. Les valeurs ALL et DEBUG3 sont les synonymes (voir aussi [Annexe L. Format des fichiers de log](#)).



Cette clé détermine un niveau de détail de la journalisation dans le fichier spécifié par la clé qui suit après -log (voir ci-dessus). Une commande peut contenir plusieurs clés de ce type.



Les d s `-verbosity` et `-log` sont sensibles   la position.

En cas d'utilisation de ces deux d s   la fois, la cl  `-verbosity` doit pr c der la cl  `-log`: la cl  `-verbosity` modifie le niveau de d tail des journaux se trouvant sur les chemins sp cifi s apr s dans la ligne de commande.

Cl s disponibles uniquement sous Windows

- ◆ `-minimized` — (uniquement en cas de d marrage en mode interactif et non pas comme service) — r duire la fen tre.
- ◆ `-screen-size=<taille>` — (uniquement en cas de d marrage en mode interactif et non pas comme service) — taille sp cifi e en lignes du journal visible dans la fen tre du **Serveur**, par d faut c'est 1000.

Cl s disponibles uniquement sous les OS de la famille UNIX

- ◆ `-etc=<path>` — chemin vers le r pertoire `etc` (`<var>/etc`).
- ◆ `-pid=<fichier>` — fichier vers lequel le **Serveur**  crit l'identificateur de son processus.
- ◆ `-syslog=<mode>` — journalisation vers le journal syst me. Les modes disponibles sont les suivants : `auth`, `cron`, `daemon`, `kern`, `lpr`, `mail`, `news`, `syslog`, `user`, `uucp`, `local0` – `local7` et en cas de certaines plateformes : `ftp`, `authpriv` et `console`.



Les param tres `-syslog` et `-log` fonctionnent en parall le. C'est- dire, lorsque vous d marrez le **Serveur** avec la cl  `-syslog` (par exemple, `service drwcsd start -syslog=user`), le **Serveur** d marre avec la valeur sp cifi e pour la cl  `-syslog` et avec la valeur par d faut de la cl  `-log`.



- ◆ `-user=<utilisateur>`, `-group=<groupe>` — ne sont disponibles que sous UNIX, en cas de lancement sous le nom utilisateur **root** ; les clés enjoignent de modifier l'utilisateur ou le groupe du processus et de s'exécuter avec les privilèges de l'utilisateur/groupe spécifié.

H5.9. Variables disponibles sous les OS de la famille UNIX

Afin de faciliter la gestion du **Serveur** sous les OS de la famille UNIX, l'administrateur dispose des variables se trouvant dans le fichier de script `/etc/init.d/drwcsd`.

Le Tableau H-1 affiche la correspondance entre les variables et les [clés de la ligne de commande](#) pour `drwcsd`.

Tableau H-1.

Clé	Variable	Paramètres par défaut
<code>-home</code>	<code>DRWCS_HOME</code>	<ul style="list-style-type: none">• <code>/usr/local/drwcs</code> - pour OS FreeBSD,• <code>/usr/drwcs</code> - pour tous les autres OS.
<code>-var-root</code>	<code>DRWCS_VAR</code>	
<code>-etc</code>	<code>DRWCS_ETC</code>	<code>DRWCS_VAR/etc</code>
<code>-rotate</code>	<code>DRWCS_ROT</code>	<code>10,10m</code>
<code>-verbosity</code>	<code>DRWCS_LEV</code>	<code>trace3</code>
<code>-log</code>	<code>DRWCS_LOG</code>	<code>DRWCS_VAR/log/drwcsd.log</code>
<code>-conf</code>	<code>DRWCS_CFG</code>	<code>DRWCS_ETC/drwcsd.conf</code>
<code>-pid</code>	<code>DRWCS_PID</code>	
<code>-user</code>	<code>DRWCS_USER</code>	
<code>-group</code>	<code>DRWCS_GROUP</code>	
<code>-hooks</code>	<code>DRWCS_HOOKS</code>	
<code>-trace</code>	<code>DRWCS_TRACE</code>	



Les variables `DRWCS_HOOKS` et `DRWCS_TRACE` n'ont pas de paramètres. Lors de la spécification des variables, les clés respectives sont ajoutées à l'exécution du script. Si les variables ne sont pas spécifiées, les clés ne seront pas ajoutées.

Les autres variables sont présentes dans le Tableau H-2.

Tableau H-2.

Variable	Paramètres par défaut	Description
<code>DRWCS_ADDOPT</code>		
<code>DRWCS_CORE</code>	unlimited	Taille maximum du fichier core.
<code>DRWCS_FILES</code>	8192	Nombre maximum de descripteurs de fichiers pouvant être ouverts par le Serveur .
<code>DRWCS_BIN</code>	<code>\$DRWCS_HOME/bin</code>	Répertoire depuis lequel <code>drwcsd</code> sera lancé.
<code>DRWCS_LIB</code>	<code>\$DRWCS_HOME/lib</code>	Répertoire avec les bibliothèques du Serveur .

Les valeurs des paramètres seront prises en compte à condition que les variables ne soient pas déterminées dans le script `/etc/init.d/drwcsd`.



Les variables `DRWCS_HOME`, `DRWCS_VAR`, `DRWCS_ETC`, `DRWCS_USER`, `DRWCS_GROUP`, `DRWCS_HOOKS` sont déjà déterminées dans le fichier du script `/etc/init.d/drwcsd`.

S'il existe le fichier `${TGT_ES_ETC}/common.conf`, ce fichier sera inclus dans `/etc/init.d/drwcsd`, dans ce cas-là, certaines variables peuvent être modifiées ; cependant si elles ne sont pas exportées (avec la commande `export`), ceci n'a pas d'impact.



Marche à suivre pour déterminer les variables :

1. Ajouter la définition de la variable dans le fichier du script /
etc/init.d/drwcsd.
2. Exporter la variable avec la commande `export` (la commande est spécifiée dans le même emplacement).
3. Au lancement d'un autre processus du même script, ce processus lit les valeurs qui ont été déterminées.

Exemple :

Pour modifier le niveau de détail du journal de **Serveur** vers le maximum :

1. Ajouter les lignes suivantes dans /etc/init.d/drwcsd :

```
DRWCS_LEV=ALL
export DRWCS_LEV
```

2. Démarrer le **Serveur** s'il a été arrêté :

```
/etc/init.d/drwcsd start (ou service drwcsd start)
```

Sinon redémarrer le **Serveur** s'il a déjà été démarré :

```
/etc/init.d/drwcsd restart (ou service drwcsd restart)
```

3. Le niveau de détail du journal prendra la valeur `ALL`.

H5.10. Configuration de Dr.Web Enterprise Server sous UNIX

Lors de l'installation du **Serveur** sous UNIX, vous devez configurer certains paramètres. La procédure de configuration des paramètres du **Serveur** peut être lancée de manière manuelle (il est nécessaire que l'environnement perl soit installé). Pour cela, il suffit de lancer le script `configure.pl` se trouvant :



- ◆ dans le répertoire `/usr/local/drwcs/bise n/` sous **FreeBSD**,
- ◆ dans le répertoire `/opt/drwcs/bin/` sous **Linux** et **Solaris**.

Syntaxe de la commande de démarrage :

`configure.pl <clés>`

Clés admissibles :

- ◆ `--proxy server=<proxy_server>` – spécifier l'adresse du Serveur proxy.
 - `user=<proxy_user>` – spécifier le nom de l'utilisateur du Serveur proxy.
 - `password=<proxy_password>` – spécifier le mot de passe pour l'utilisateur du Serveur proxy.
- ◆ `--stat server=<stat_server>` – spécifier l'adresse du Serveur de statistiques (par défaut c'est `stat.drweb.com:80`).
 - `url=<url_on_server>` – spécifier l'URL sur le Serveur de statistiques (par défaut `/update`).
 - `interval=<send_interval>` – spécifier un délai d'envoi des statistiques.
- ◆ `--initbase` – initialiser la BD du **Serveur**.
- ◆ `--upgradebase` – mettre à jour la BD sur le **Serveur**.
- ◆ `--interactive` – lancer en mode interactif.
- ◆ `--skip proxy=1` – sauter un pas dans le mode interactif.
 - `stat=1` |
 - `initbase=1` |
 - `upgradebase=1`
- ◆ `--verbose` – afficher des informations détaillées.
- ◆ `--help` | `?` – afficher la rubrique d'aide sur les paramètres du programme.



H6. Utilitaire d'administration de la BD interne

L'utilitaire d'administration de la BD interne se trouve dans les répertoires suivants :

- ◆ sous **Linux** et **Solaris** : /opt/drwcs/bin
- ◆ sous **FreeBSD** : /usr/local/drwcs/bin
- ◆ sous **Windows** :

`<répertoire_d_installation_du_Serveur>\bin`

(par défaut, le répertoire d'installation du **Serveur** est :
C:\Program Files\DrWeb Enterprise Server).

Syntaxe de la commande de démarrage :

`drwidbsh`

Le programme fonctionne en mode dialogué et attend de la part de l'utilisateur l'entrée des commandes (les commandes commencent avec le point).

Pour la rubrique d'aide sur d'autres commandes, entrez `.help`. La rubrique d'aide s'affichera.

Pour plus d'information, consulter la documentation sur le langage SQL.



H7. Utilitaire de génération des paires de clés et de la signature numérique

Noms et emplacement des fichiers clés de chiffrement dans le répertoire d'installation du Serveur :

- ◆ `\etc\drwcsd.pri` - privée,
- ◆ `\Installer\drwcsd.pub` - publique.

Variantes de syntaxe de la commande :

- ◆ `\bin\drwsign check [-public-key=<publique>] <fichier>`

vérifier la signature du fichier en utilisant *<publique>* en tant que clé publique de la personne qui a signé le fichier.

- ◆ `\bin\drwsign extract [-private-key=<privée>] <publique>`

extrait la clé publique depuis le fichier de clé privée (version **4.33** ou supérieure).

- ◆ `\bin\drwsign genkey [<privée> [<publique>]]`

génération d'une paire de clé publique-privée et leur enregistrement vers les fichiers appropriés.



La version de l'utilitaire pour les plateformes Windows (à la différence de la version pour UNIX) ne protège pas la clé privée contre la copie.

- ◆ `\bin\drwsign help [<commande>]`

rubrique d'aide abrégée sur le programme et le format de la ligne de commande.

- ◆ `\bin\drwsign join432 [-public-key=<publique>] [-private-key=<privée>] <nouvelle_privée>`

fusionne les clés publique et privée au format correspondant à la version **4.32** vers le nouveau format de clé privée en version



4.33 ou supérieure.

```
◆ \bin\drwsign sign [-private-key=<privée>]  
  <fichier>
```

signer le fichier <fichier> en utilisant la clé privée spécifiée.

H8. Gestion du Serveur Dr.Web Enterprise Server sous UNIX® avec la commande kill

Le **Serveur** sous UNIX est géré par les signaux envoyés vers le processus du **Serveur** par l'utilitaire `kill`.



Pour la rubrique d'aide détaillée sur l'utilitaire `kill`, utilisez la commande `man kill`.

Liste des signaux de l'utilitaire et des actions qu'ils effectuent :

- ◆ SIGWINCH - sortie des statistiques vers le fichier de log (heure CPU, utilisation de la mémoire etc.),
- ◆ SIGUSR1 - relire le dépôt des produit depuis le disque,
- ◆ SIGUSR2 - relire les templates des messages depuis le disque,
- ◆ SIGHUP - redémarrage du **Serveur**,
- ◆ SIGTERM - arrêt du **Serveur**,
- ◆ SIGQUIT - arrêt du **Serveur**,
- ◆ SIGINT - arrêt du **Serveur**.

Les actions équivalentes pour le **Serveur** sous Windows sont effectuées avec les clés de la commande `drwcsd`, voir l'Annexe [H5.3](#).



H9. Scanner Dr.Web pour OS Windows®

Ce composant du logiciel installé sur le poste de travail a les paramètres de la ligne de commande décrits dans le Manuel Utilisateur **Antivirus Dr.Web® pour Windows**. La seule différence est que lors du démarrage du **Scanner** effectué par **l'Agent**, les paramètres `/go /st` sont transmis au **Scanner** de manière automatique et obligatoire.

H10. Serveur proxy

Pour configurer certains paramètres du **Serveur proxy**, lancez le fichier exécutable `drwcsd-proxy`, accompagné des clés nécessaires dont l'emplacement est le suivant :

- ◆ sous Windows : le dossier d'installation du **Serveur proxy**.
- ◆ sous UNIX : le sous-dossier `bin` du dossier d'installation du **Serveur proxy**.

Syntaxe de la commande de démarrage :

```
drwcsd-proxy <clés>
```

Clés admissibles :

- ◆ `--help` – afficher la rubrique d'aide sur les clés pour configurer le **Serveur proxy**.
- ◆ `--daemon` – uniquement sous UNIX : lancer le **Serveur proxy** en mode daemon.
- ◆ `--control <arg>` – uniquement sous Windows : configurer les paramètres du service.

Paramètres possibles :

- `run` – (par défaut) lancer le **Serveur proxy** en tâche de fond, en tant que service de Windows.
- `install` – installer le **Serveur proxy**.
- `uninstall` – supprimer le **Serveur proxy**.



- ◆ `--cfg <path>` – spécifier le chemin vers le [fichier de configuration](#) du **Serveur proxy**.
- ◆ `--pool-size <N>` – la taille du pool pour connecter les clients. La valeur par défaut est 2.
- ◆ `--trace` – activer la journalisation détaillée des requêtes vers le **Serveur proxy**. Ce paramètre est accessible uniquement dans le cas où le build de **Serveur proxy** supporte la journalisation détaillée de la pile des requêtes.
- ◆ `--use-console-log` – journaliser le fonctionnement du **Serveur proxy** dans la console.
- ◆ `--use-file-log <file>` – écrire le log du **Serveur proxy** dans un fichier avec `<file>` - chemin vers le fichier de log.
- ◆ `--rotate=<N><f>, <M><u>` – mode de rotation du fichier de log du **Serveur proxy** avec :
 - `<N>` – nombre total de fichiers de log (y compris le log courant et ceux d'archive);
 - `<f>` – format de sauvegarde des fichiers de log, valeurs possibles : `z` (gzip) – compresser les fichiers (par défaut) sinon `p` (plain) – ne pas compresser les fichiers ;
 - `<M>` – taille de fichier ;
 - `<u>` – unité de mesure, valeurs possibles : `k` (kilo), `m` (méga), `g` (giga).

Par défaut, c'est `10,10m`, ce qui commande de conserver 10 fichiers, 10 Mo chacun et d'utiliser la compression.

- ◆ `--verbosity=<niveau de détail>` – niveau de détail du log. Par défaut `TRACE3`. Les valeurs possibles sont les suivantes : `ALL`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `DEBUG`, `TRACE3`, `TRACE2`, `TRACE1`, `TRACE`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `CRIT`. Les valeurs `ALL` et `DEBUG3` sont les synonymes.



Toutes les clés relatives au paramétrage du **Serveur proxy** peuvent être spécifiées simultanément.

Il est impossible de sortir le log vers un fichier et vers la console en même temps :



- ◆ si aucune clé n'est spécifiée, le log sera écrit dans la console.
 - ◆ si les deux clés sont spécifiées, le log sera écrit vers un fichier.
-



Annexe I. Variables d'environnement exportées par le Serveur Dr.Web Enterprise Server

Pour faciliter le paramétrage des processus lancés par **Serveur Enterprise** selon la planification, les données sur l'emplacement des répertoires du **Serveur** sera requise. C'est pour cette raison que le **Serveur** exporte dans l'environnement des processus lancés les variables suivantes :

- ◆ **DRWCSD_HOME** — chemin vers le répertoire racine (répertoire d'installation). La valeur de la clé est `-home` si la clé n'a pas été spécifiée au démarrage du **Serveur**, sinon c'est le répertoire courant lors du démarrage.
- ◆ **DRWCSD_EXE** — chemin vers le répertoire pour les exécutables. La valeur de la clé est `-bin-root` si la clé n'a pas été spécifiée au démarrage du **Serveur**, sinon c'est le sous-répertoire `bin` du répertoire racine.
- ◆ **DRWCSD_VAR** — chemin vers le répertoire vers lequel le **Serveur** est autorisé à écrire et qui est destiné à sauvegarder les fichiers modifiables (par exemple, les journaux et les fichiers du dépôt des produits). La valeur de la clé est `-var-root` si la clé n'a pas été spécifiée au démarrage du **Serveur**, sinon c'est le sous-répertoire `var` du répertoire racine.



Annexe J. Utilisation du script de l'installation initiale pour Dr.Web Enterprise Agent

Le scénario du processus d'installation initiale des **Agents** sur les postes avec l'installateur réseau (`drwinst.exe`) est déterminé par le fichier `install.script`. Ces fichiers se trouvent dans le répertoire racine des produits dans le dépôt des produits. En cas de package standard, ces fichiers sont présents dans les répertoires `10-drwupgrade` et `20-drwagntd` et ils décrivent l'installation effectuée par défaut.

Si le fichier `.custom.install.script` est présent dans le répertoire, ce fichier sera utilisé à la place du scénario standard.



Les fichiers ayant d'autres noms commençant par un point ne sont pas mis à jour lors des mises à jour du produit et ils n'ont pas d'impact sur le fonctionnement du dépôt des produits.

La marche à suivre lors de l'installation initiale :

1. L'installateur réseau demande l'installation des plateformes depuis le **Serveur** : `win-setup`, `common`, `win`, `win-nt` et `win-9x` — c'est la liste des plateformes standard dans l'ordre défini par défaut. L'ordre peut être modifié avec la clé `-platforms=p1,p2,p3...` au lancement de `drwinst`. La plateforme `win-setup` ne fait pas partie du package standard et peut créer ses propres scénarios d'installation si nécessaire.
2. Le **Serveur** crée une liste de fichiers conformément à la liste des plateformes, en examinant tous les produits dans l'ordre alphabétique, il crée également des listes de fichiers déterminés par les constructions suivantes : `files{ }` pour la plateforme spécifiée dans le scénario d'installation `install.script` (voir ci-dessous). En parallèle, le script sommaire est créé en se basant sur les constructions



```
scripts{ }.
```

3. Le **Serveur** reçoit la liste commune des fichiers et le script sommaire.
4. Le **Serveur** envoie les fichiers et le script qui sera exécuté par l'installateur réseau.

Envisageons `install.script` en nous basant sur l'exemple du répertoire `20-drwagntd`.

```
; master part of installation: Agent & its stuff.
; drwscr.dll goes with upgrader, so unlisted here.

platform{ ; win - for all Windows OS
          ; `name: XXX' MUST go first!

    name: win ; (mandatory stanza)
           ; this platform name

           ; include, scripts{ }, files{ }
           ; can go in any order

    scripts { ; (optional)
              ; script being merged with all others
win.inst.rexx ; and executed after transfer all
              ; files for all platforms requested
              ; by installer
              ; Windows installer request order:
              ; - win-setup (optional! for
              ;               customization)
              ; - common
              ; - win
              ; - win-nt OR win-9x
    }

    files { ; (optional)
            ; this platform files being
```




```
        ; transfered to installer
        win/uninstall.rexx
        win/drwinst.exe
        win/drwagntd.exe
        win/drwagnui.exe
        win/drwhard.dll
    }
}

platform {      ; win-9x - for Windows 95-ME
    name: win-9x
    scripts{ win-9x.inst.rexx }
}

platform {      ; win-nt - for Windows NT-2003
    name: win-nt
    scripts{ win-nt.inst.rexx }
}

platform{      ; common - for any OS including
UNICES
    name: common
    scripts { common.inst.rexx }
}

; include file.name ; (optional)
    ; this stanza tells to include other file.
    ; including file will be searched in the
    ; same directory where current file are
    ; located if `file.name' does not include
    ; directory specifier
```

Le script est constitué de la liste des constructions `platform{ }` et permet, avec la construction `include`, d'ajouter les définitions depuis d'autres fichiers (`include` est admissible au niveau supérieur



seulement et n'est pas disponible dans `platform{ }`). Si `file.name` dans `include` ne contient pas de chemin mais seulement un nom de fichier, il sera recherché dans le même répertoire.

Il est possible d'avoir ses propres constructions `include` dans les fichiers ajoutables.

La description de la plateforme commence avec la construction `name : XXX`. Puis une paire de listes `files{ }` et `scripts{ }` suivent. L'ordre d'apparition des listes n'a pas d'importance ; les listes peuvent comprendre n'importe quel nombre d'éléments. L'ordre des éléments dans la liste est important puisque cet ordre détermine l'ordre de la transmission des fichiers vers le poste ainsi que la construction du script créé.

L'ordre d'apparition des constructions `platform{ }` n'a pas d'importance non plus.

Vous trouverez ci-dessous les variables des scripts d'installation (des valeurs peuvent être attribuées à ces variables depuis la ligne de commande de l'installateur réseau) ainsi que leurs valeurs par défaut :

- ◆ `spider.install = 'yes'`
- ◆ `spiderml.install = 'yes'`
- ◆ `scanner.install = 'yes'`
- ◆ `install.home` — répertoire d'installation
- ◆ `agent.logfile = install.home'\logs\drwagntd.log'`
- ◆ `agent.loglevel = 'trace'`
- ◆ `agent.logrotate = '10,10m'`
- ◆ `agent.servers = install.servers`
- ◆ `agent.serverkey = install.home'\drwcsd.pub'`
- ◆ `agent.compression = 'possible'`
- ◆ `agent.encryption = 'yes'`
- ◆ `agent.findretry = '3'`
- ◆ `agent.findtimeout = '5'`



- ◆ `agent.spiderstatistics = '30'`
- ◆ `agent.importantmsg = '2'`
- ◆ `agent.discovery = 'udp/:2193'`
- ◆ `agent.startmsg = '2' (ou agent.startmsg = 'NONE')`

Le paramètre `agent.importantmsg` détermine les fonctions "afficher" ou "ne pas afficher" à l'utilisateur les messages d'erreurs de mises à jour, et les messages sur la nécessité de redémarrer etc. **0** — ne pas afficher le message, **1** — afficher une infobulle.

Création d'un scénario non standard d'installation qui ne prévoit pas l'installation de Spider Guard et qui spécifie le niveau maximum de détail du journal :

1. Créez dans le répertoire `20-drwagntd` le fichier `.win-setup.inst.rexx` et écrivez dans ce fichier :

```
spider.install = 'no'
agent.loglevel = 'all'
```

2. Créez dans le répertoire `20-drwagntd` le fichier `.custom.install.script` et écrivez dans ce fichier :

```
include install.script

platform{
    name: win-setup
    scripts{ .win-setup.inst.rexx }
}
```

3. Redémarrez le **Serveur** ou commandez de redémarrer le dépôt des produits :

- ◆ sous **UNIX**: `kill -USR1 cat `drwcsd.pid``
- ◆ sous **Windows**: `drwcsd.exe rerepository`



Annexe K. Utilisation des expressions régulières dans Dr.Web Enterprise Security Suite

Certains paramètres de **Dr.Web ESS** sont spécifiés sous forme d'expressions régulières. Les expressions régulières sont traitées avec la bibliothèque de programme PCRE.

Pour en savoir plus sur la syntaxe de la bibliothèque PCRE, consultez les informations sur le Serveur <http://www.pcre.org/>.

La présente annexe ne contient qu'une description abrégée des principaux points relatifs à l'utilisation des expressions régulières.

K1. Options des expressions régulières

Les expressions régulières sont utilisées dans le fichier de configuration du **Serveur** ainsi que dans le **Centre de Gestion** lors du paramétrage des objets à exclure de l'analyse dans la configuration du **Scanner**.

Les expressions régulières ont le format suivant :

```
qr{EXP}options
```

où EXP – expression même, options – séquence des options (ligne de caractères). Voici un exemple de construction :

```
qr{pagefile\.sys}i – fichier swap de Windows NT
```

Vous trouverez ci-dessous une description des options et des expressions régulières. Pour plus d'information, visitez le lien <http://www.pcre.org/pcre.txt>.

- ◆ Option 'a' correspondant à PCRE_ANCHORED

Avec cette option, le motif est ancré, il est limité par la comparaison uniquement avec la première position recherchée dans la ligne de recherche ("chaîne sujet"). Il est possible d'y



arriver avec des constructions respectives dans le motif.

- ◆ Option 'i' correspondant à `PCRE_CASELESS`

Avec cette option, les caractères du motif sont comparés aux majuscules et aux minuscules. Cette possibilité peut être modifiée dans le motif par le paramétrage de l'option `(?i)`.

- ◆ Option 'x' correspondant à `PCRE_EXTENDED`

Avec cette option, les caractères d'espace sont ignorés, sauf lorsqu'ils sont échappés, ou à l'intérieur d'une classe de caractères. L'espace ne comprend pas le symbole `\t` (code 11). De plus, tous les caractères entre `#` non échappés et en dehors d'une classe de caractères, ainsi que le caractère de nouvelle ligne sont ignorés. Cette option peut être modifiée dans le motif par le paramétrage de l'option `(?x)`. Le paramétrage permet d'inclure les commentaires dans les masques compliqués. Il est à noter cependant que ceci n'est applicable qu'aux symboles de données. Les caractères d'espace ne peuvent pas apparaître dans les séquences spécifiques d'un masque, par exemple à l'intérieur de la séquence `(?(` qui introduit une parenthèse conditionnelle.

- ◆ Option 'm' correspondant à `PCRE_MULTILINE`

Par défaut, PCRE traite la chaîne sujet comme une seule ligne (même si cette chaîne contient des retours chariot). Le métacaractère "début de ligne" (`^`) ne sera valable qu'une seule fois, au début de la ligne, et le méta caractère "fin de ligne" (`$`) ne sera valable qu'à la fin de la chaîne, ou avant le retour chariot final (à moins que l'option `PCRE_DOLLAR_ENDONLY` ne soit activée).

Lorsque cette option est activée, " début de ligne " et " fin de ligne " correspondront alors aux caractères suivant et précédant immédiatement un caractère de nouvelle ligne, en plus du début et de la fin de la chaîne. Cette option peut être modifiée dans le masque par le paramétrage de l'option `(?m)`. Si le texte ne contient pas les caractères `"\n"` ou que le masque ne contient pas les caractères `^` ou `$`, l'option `PCRE_MULTILINE` perd son sens.



- ◆ Option 'u' correspondant à `PCRE_UNGREEDY`

Cette option inverse la tendance à la gourmandise des expressions régulières. Vous pouvez aussi inverser cette tendance au coup par coup avec un `?`. De même, si cette option est activée, le `?` rendra gourmand une séquence. Ceci peut également être paramétré avec l'option `(?U)` dans le motif.

- ◆ Option 'd' correspondant à `PCRE_DOTALL`

Avec cette option, le méta caractère point "." dans le masque est comparé avec tous les caractères, y compris le caractère de la nouvelle ligne. Si le méta caractère n'est pas présent, les caractères de la nouvelle ligne seront exclus. Cette option peut être modifiée dans le motif avec la spécification de la nouvelle option `(?s)`. La classe négative, par exemple `[^a]` est toujours comparée avec le caractère de la nouvelle ligne quels que soient les paramètres de l'option.

- ◆ Option 'e' correspondant à `PCRE_DOLLAR_ENDONLY`

Avec cette option, le métacaractère `$` ne sera valable qu'à la fin de la chaîne sujet. Sans cette option, `$` est aussi valable avant une nouvelle ligne, si cette dernière est le dernier caractère de la chaîne. L'option `PCRE_DOLLAR_ENDONLY` est ignorée si l'option `PCRE_MULTILINE` est activée.

K2. Particularités des expressions régulières PCRE

L'*expression régulière* est un masque à comparer avec le texte de gauche à droite. La plupart des caractères contenus dans le masque se représentent eux-mêmes et s'appliquent aux caractères correspondants dans le texte.

L'avantage principal des expressions régulières consiste en la possibilité d'inclure dans le masque les variantes et les répétitions. Elles sont codées avec les métacaractères qui à leur tour ne se représentent pas eux-mêmes mais sont interprétés de manière appropriée.



Il existe deux ensembles de métacaractères : ceux qui sont utilisés entre crochets et ceux qui sont utilisés à l'extérieur. Nous allons les envisager de plus près. Les métacaractères listés ci-dessous sont utilisés hors crochets :

- \ caractère de contrôle standard (*escape*) permettant plusieurs variantes d'utilisation,
- ^ indique le début de la chaîne (ou du texte en mode multi-lignes),
- \$ indique la fin de la chaîne (ou du texte en mode multi-lignes),
- correspond à n'importe quel caractère sauf le caractère de saut de ligne (par défaut),
- [début de la description d'une classe de caractères,
-] fin de description d'une classe de caractères
- | début d'une branche de l'alternative,
- (début du sous-masque,
-) fin du sous-masque,
- ? étend la valeur (,
aussi quantificateur 0 ou 1,
aussi quantificateur-minimisateur ;
- * 0 ou plus,
- + 1 ou plus,
aussi "quantificateur possessif",
- { début du quantificateur minimum/maximum.

La partie du masque se trouvant entre crochets est nommée "classe de caractères". La classe de caractère comprend les métacaractères suivants :

- \ caractère de contrôle standard (*escape*),



- ^ négation de la classe mais uniquement dans la position au début de la classe,
- détermine la plage de caractères,
- [classe de caractères POSIX (uniquement dans le cas où elle est suivie de la syntaxe POSIX),
-] ferme la classe de caractères.

K3. Utilisation des métacaractères

Antislash (\)

Le caractère antislash a de nombreuses fonctions. En premier lieu, s'il est suivi d'un caractère non alpha-numérique, il ne prendra pas la signification spéciale qui y est rattachée. Cette utilisation de l'antislash comme caractère d'échappement s'applique à l'intérieur et à l'extérieur des classes de caractères.

Par exemple, pour rechercher le caractère étoile " * ", il faut écrire dans le masque : " \`*` ". Cela s'applique dans tous les cas, que le caractère qui suit soit un métacaractère ou non. C'est un moyen sûr pour s'assurer qu'un caractère sera recherché pour sa valeur littérale, plutôt que pour sa valeur spéciale. En particulier, pour rechercher les antislash, il faut écrire : " \`\\` ".

Si un masque est utilisé avec l'option `PCRE_EXTENDED` , les espaces blancs du masque, mais qui ne sont pas dans une classe de caractères, et les caractères entre dièses " # ", ainsi que les nouvelles lignes sont ignorés. L'antislash peut être utilisé pour échapper et ainsi rechercher un espace ou un dièse.

Si vous voulez désactiver la valeur spécifique de la séquence de caractères, mettez-la entre `\Q` et `\E`. La séquence `\Q... \E` fonctionne à l'intérieur et à l'extérieur des classes de caractères.



Caractères invisibles

La deuxième utilité de l'antislash est de pouvoir coder des caractères invisibles dans les masques. Il n'y a pas de restriction sur la place de ces caractères invisibles, hormis pour le caractère nul qui doit terminer le masque. Dans le cas où le masque est créé avec un éditeur de texte, il est plus facile d'utiliser une séquence d'échappement plutôt que le caractère binaire qu'elle représente :

- ◆ `\a` caractère alarme BEL (hex 07I),
- ◆ `\cx` "control-x", x - n'importe quel caractère,
- ◆ `\e` caractère escape (hex 1B),
- ◆ `\f` saut de page (hex 0C),
- ◆ `\n` saut de ligne (hex 0A),
- ◆ `\r` retour chariot (hex 0D),
- ◆ `\t` tabulation (hex 09),
- ◆ `\ddd` caractère avec le code octal ddd ou une référence arrière,
- ◆ `\xhh` caractère avec le code hexadécimal hh.

Dans la séquence "`\cx`", si "x" est en minuscule, il est converti en majuscule. Puis, le bit 6 (hex 40) est inversé. Ainsi "`\cz`" devient 1A, mais "`\c{`" devient hex 3B, tandis que "`\c;`" devient hex 7B.

Après "`\x`", deux caractères hexadécimaux sont lus (les lettres peuvent être en majuscule ou en minuscule).

Après "`\0`", deux caractères octal sont lus. Dans chacun des cas, le métacaractère tente de lire autant de caractères que possible.

Ainsi la séquence "`\0\x07`", sera comprise comme deux caractères nuls, suivi d'un caractère alarme (BEL), code 7. Dans le cas où vous utilisez le système de numération octal, assurez-vous que vous



fournissez deux chiffres significatifs après le nul initial.

La gestion de la séquence "`\y`", avec $y < 0$ est plutôt compliquée. En dehors des caractères de classes, PCRE va lire "y" et tous les caractères qui suivent comme des chiffres décimaux. Si "y" est plus petit que 10, ou bien s'il y a déjà eu au moins autant de parenthèses ouvrantes auparavant, la séquence est prise pour une référence arrière.

A l'intérieur d'un caractère de classe, ou si "y" est plus grand que 9, et qu'il n'y a pas eu assez de parenthèses ouvrantes auparavant, PCRE lit jusqu'à 3 chiffres octals à la suite de l'antislash et génère un octet unique, à partir des 8 bits de poids faible de la séquence. Tous les chiffres qui suivent ne sont pas interprétés, et se représentent eux-mêmes. Par exemple

- ◆ `\040` une autre manière d'écrire un espace,
- ◆ `\40` identique, dans la mesure où il y a moins de 40 parenthèses ouvrantes auparavant,
- ◆ `\7` est toujours une référence arrière,
- ◆ `\11` peut être une référence arrière, ou une tabulation,
- ◆ `\011` toujours une tabulation,
- ◆ `\0113` est une tabulation suivie du caractère "3",
- ◆ `\113` peut être une référence arrière, sinon - le caractère ayant le code octal 113,
- ◆ `\377` peut être une référence arrière, sinon - un octet dont tous les bits sont à 1,
- ◆ `\81` peut être soit une référence arrière, soit le caractère NULL, suivi des caractères "8" et "1".

Les valeurs octales supérieures ou égales à 100 ne doivent pas être introduites par un 0, car seuls les trois premiers octets seront lus.

Toutes les séquences qui définissent une valeur d'un seul octet peuvent être utilisées dans les classes de caractères et à l'extérieur. De



plus, dans une classe de caractères, la séquence " \b " est interprétée comme un caractère effacer (backspace, hex 08) ; la séquence \X comme caractère "X". A l'extérieur de la classe de caractères, les séquences peuvent avoir d'autres significations.

Types de caractères génériques

On peut encore se servir de l'antislash pour préciser des types génériques de valeurs. Les types listés ci-dessous sont toujours reconnus :

- ◆ \d tout caractère décimal,
- ◆ \D tout caractère qui n'est pas un caractère décimal,
- ◆ \s tout caractère blanc (whitespace),
- ◆ \S tout caractère qui n'est pas un caractère blanc,
- ◆ \w tout caractère alphanumérique et le caractère de soulignement,
- ◆ \W tout caractère sauf les caractères alphanumériques et de soulignement.

Chaque paire précédente définit une partition de la table des caractères : les deux ensembles sont disjoints. Un caractère satisfera soit un ensemble, soit l'autre.

Ces séquences de caractères peuvent apparaître à l'intérieur ou à l'extérieur des classes de caractères. Elles remplacent à chaque fois un caractère de type correspondant. Si cette séquence est placée en fin de masque, et qu'il n'y a plus de caractère à comparer dans la chaîne sujet, la recherche échoue.

\s ne correspond pas au caractère VT (code 11). C'est ce qui fait la différence par rapport à la classe "espace" dans POSIX. Les caractères \s sont HT (9), LF (10), FF (12), CR (13) et espace (32).



Assertions simples

La quatrième utilisation de l'antislash intervient lors d'assertions simples. Une assertion impose une condition à un certain point, sans remplacer de caractère. L'utilisation de sous-masques pour réaliser des assertions plus complexes est décrite plus-bas. Les assertions avec antislash sont les suivantes :

- ◆ `\b` comparaison à la limite de mot,
- ◆ `\B` pas de limite de mot,
- ◆ `\A` début de la chaîne sujet,
- ◆ `\Z` comparaison à la fin de la chaîne sujet ou avant le caractère de saut de ligne se trouvant à la fin,
- ◆ `\z` comparaison à la fin de la chaîne sujet,
- ◆ `\G` comparaison à la première position de recherche dans la chaîne sujet.

Ces assertions ne peuvent pas apparaître dans une classe de caractères (mais `"\b"` a une autre signification à l'intérieur d'une classe de caractères) – caractère de retour (`backspace`)).

Accent circonflexe (^) et Dollar (\$)

En dehors d'une classe de caractères, avec les options par défaut, `^` est une assertion qui n'est vraie que si elle est placée au tout début de la chaîne. A l'intérieur d'une classe de caractères, `^` a un tout autre sens (voir ci-dessous).

Le métacaractère `^` n'a pas besoin d'être le premier caractère du masque, si plusieurs alternatives sont proposées, mais il doit être placé en premier dans chaque alternative. Si toutes les alternatives commencent par `^`, alors le masque est dit ancré (il y a une autre construction qui porte cette appellation).



Le métacaractère `$` est une assertion qui n'est vraie que si elle est placée tout en fin de chaîne ou juste avant un caractère de nouvelle ligne qui serait le dernier caractère de la chaîne (par défaut). `$` n'a pas besoin d'être le dernier caractère du masque, si plusieurs alternatives sont proposées, mais il doit être placé en dernier dans chaque alternative. `$` n'a pas de valeur particulière dans la classe de caractères.

La signification de `$` peut changer, de manière à l'amener à ce qu'il ne puisse se trouver qu'en toute fin de la chaîne sujet. Cela se fait en ajoutant l'option `PCRE_DOLLAR_ENDONLY` au moment de la compilation, ou de l'exécution. Cette option est inopérante sur `\Z`.

La signification de `^` et de `$` peuvent changer si l'option `PCRE_MULTILINE` est activée. Dans ce cas, outre la comparaison au début et à la fin de la chaîne sujet, ils sont mis en comparaison immédiatement avant et immédiatement après un caractère interne de nouvelle ligne. Par exemple, le masque `/^abc$/` accepte la chaîne "def\nabc" uniquement en mode multi-lignes (`\n` - caractère de saut de ligne). Par conséquent, toutes les parties du masques qui commencent par "`^`" ne sont pas ancrées, en mode multi-lignes. Ainsi, la comparaison avec `^` est possible en cas de déplacement initial non nul de l'argument de la fonction `pcre_exec()`.

Point

En dehors d'une classe de caractères, un point remplace n'importe quel caractère, même invisible et à l'exception (par défaut) du caractère de nouvelle ligne. La gestion des points est complètement indépendante de `^` et `$`. Le seul point commun est que les deux ont un comportement particulier vis-à-vis des caractères de nouvelle ligne. Le point n'a pas de comportement particulier dans la classe de caractères.

Crochets et classes de caractères

Un crochet ouvrant `[` introduit une classe de caractères, et le crochet fermant `]` la conclut. Le crochet fermant n'a pas de signification en lui-même. Si le crochet fermant est nécessaire à l'intérieur d'une classe de



caractères, il faut qu'il soit le premier caractère (après un ^ éventuel) ou échappé avec un antislash. Une classe de caractère correspond à un seul caractère dans le texte.

Une classe de caractères remplace un seul caractère dans la chaîne sujet, à moins que le premier caractère de la classe soit un accent circonflexe ^ , qui représente une négation : le caractère ne doit pas se trouver dans la classe. Si ^ est nécessaire dans la classe, il suffit qu'il ne soit pas le premier caractère, ou bien qu'il soit échappé avec un antislash.

Par exemple, le caractère [aeiou] remplace n'importe quelle voyelle minuscule, tandis que [^aeiou] remplace n'importe quel caractère qui n'est pas une voyelle minuscule.

Il est à noter que l'accent circonflexe sert seulement à spécifier des caractères qui ne sont pas dans la classe en facilitant ainsi l'indication des caractères au sein de la classe. La classe commençant par un accent circonflexe n'est pas une assertion : une telle classe nécessite un caractère depuis le texte, au cas où l'indicateur courant est placé à la fin de la ligne, la comparaison avec le masque ne se fait pas.

En cas de comparaison insensible à la casse, tous les caractères dans la classe représentent en même temps les versions minuscules et les versions majuscules.

Le signe moins (-) est utilisé pour spécifier un intervalle de caractères, dans une classe. Par exemple, [d-m] remplace toutes les lettres entre d et m inclus. Si le caractère moins est requis dans une classe, il faut l'échapper avec un antislash, ou le faire apparaître à une position où il ne pourra pas être interprété comme une indication d'intervalle, c'est-à-dire au début ou à la fin de la classe.

Il n'est pas possible d'avoir le caractère crochet fermant "] " comme fin d'intervalle. Un masque tel que [W-]46] est compris comme la classe de caractères contenant deux caractères ("W" et "-") suivie de la chaîne littérale "46]", ce qui fait qu'il va accepter " W46] " ou " -46] ". Cependant, si "] " est échappé avec un antislash, le masque [W-\] 46] est interprété comme une classe d'un seul caractère, contenant un intervalle de caractères suivi de deux caractères. La valeur octale ou hexadécimale de "] " peut aussi être utilisée pour déterminer les



limites de l'intervalle.

Les types de caractères `\d`, `\D`, `\p`, `\P`, `\s`, `\S`, `\w`, `\W` peuvent aussi intervenir dans les classes de caractères en y ajoutant les caractères correspondants.

Par exemple, "`[^\^_`wxyzabc][\dABCDEF]`" acceptera n'importe quel caractère hexadécimal. Un accent circonflexe peut aussi être utilisé pour spécifier adroitement des ensembles de caractères plus restrictifs : par exemple `[\^\W_]` accepte toutes les lettres et les chiffres, mais pas les soulignés. Tous les caractères non alpha- numériques autres que `\`, `-`, `^` (placés en début de chaîne) et `]` n'ont pas de signification particulière, mais ils ne perdront rien à être échappés.

Les seuls métacaractères qui ne sont pas reconnus dans les classes de caractères sont l'antislash, le trait d'union (uniquement dans le cas où il peut être compris comme un déterminant d'un intervalle), l'accent circonflexe (uniquement dans le cas où il est placé en début de chaîne), le crochet ouvrant (uniquement là où il peut être compris comme l'entrée du nom de la classe POSIX, - voir le paragraphe suivant) et le crochet fermant. Cependant, l'échappement avec l'antislash de tous les caractères non alphanumériques est toujours utile.

Classes de caractères POSIX

PCRE supporte la légende de POSIX pour les classes de caractères. Par exemple

```
[01[:alpha:]]%
```

correspond à "0", "1", n'importe quel caractère alphabétique ou à "%". Les noms des classes suivants sont supportés

- ◆ `alnum` des caractères alphanumériques,
- ◆ `alpha` des caractères alphabétiques,
- ◆ `ascii` des codes de caractères 0 - 127,
- ◆ `blank` un espace ou une tabulation,
- ◆ `cntrl` des caractères de contrôle,



- ◆ `digit` des chiffres hexadécimaux (identique à `\d`),
- ◆ `graph` des caractères visibles excepté l'espace,
- ◆ `lower` des minuscules,
- ◆ `print` des caractères visibles y compris l'espace,
- ◆ `punct` des caractères visibles excepté les caractères alphanumériques,
- ◆ `space` un caractère d'espace blanc (n'est pas tout à fait identique à `\s`),
- ◆ `upper` majuscules,
- ◆ `word` des caractères alphanumériques (identique à `\w`),
- ◆ `xdigit` chiffres décimaux.

Barre verticale (|)

La barre verticale `|` sert à séparer des masques alternatifs. Par exemple, dans le masque `/gilbert|sullivan/` recherche soit "gilbert", soit "sullivan". Le nombre d'alternatives n'est pas limité, et il est même possible d'utiliser la chaîne vide. Lors de la recherche, toutes les alternatives sont testées, de gauche à droite, et la première qui est acceptée est utilisée.

Si les alternatives sont dans un sous-masque (voir ci-dessous), elles ne réussiront que si le masque principal réussit aussi.

Installation des options internes

Les options `PCRE_CASELESS`, `PCRE_MULTILINE` et `PCRE_EXTENDED` peuvent être modifiés de manière locale dans le masque avec une séquence de caractères-options Perl se trouvant entre les symboles `"(?"` et `)"`.

Caractères-options :

- ◆ `i` pour `PCRE_CASELESS`
- ◆ `m` pour `PCRE_MULTILINE`



◆ x pour PCRE_EXTENDED

Par exemple `(?im)` spécifie une recherche multi-lignes insensible à la casse. Il est également possible de désactiver les options avec un échappement par un trait d'union ; vous pouvez aussi combiner l'activation et la désactivation des options, par exemple `(?im-x)` active les options `PCRE_CASELESS` et `PCRE_MULTILINE` mais désactive `PCRE_EXTENDED`. Si le trait d'union est précédé ou suivi d'un caractère, l'option est désactivée.

Sous-masques

Les sous-masques sont délimités par des parenthèses, et peuvent être imbriqués. Ajouter des sous-masques a deux utilités :

1. Délimiter des alternatives. Par exemple, le masque

```
cat(aract|erpillar|)
```

correspond à un des mots : "cat", "cataract" ou "caterpillar". Sans les parenthèses, il n'accepterait que "cataract", "erpillar" ou une ligne vide.

2. Le sous-masque est considéré comme capturant : lorsqu'une chaîne sujet est acceptée par le masque complet, les sous-masques sont transmis à l'appelant grâce à un vecteur de sous-masques. Les parenthèses ouvrantes sont comptées de gauche à droite, (commençant à 1) et leur numéros d'ordre servent à numéroter les sous-masques respectifs dans le résultat.

Par exemple, si la ligne "the red king" est mise en comparaison avec le masque

```
the ((red|white) (king|queen))
```

les sous-masques "red king", "red" et "king" seront capturés et numérotés respectivement 1, 2 et 3.

L'ubiquité des parenthèses n'est pas toujours simple d'emploi. Parfois, regrouper des sous-masques est nécessaire, sans pour autant capturer la valeur trouvée. Si une parenthèse ouvrante est suivie de " ? ", le



sous-masque ne capture pas la chaîne assortie, et ne sera pas compté lors de la numérotation des captures. Par exemple, avec la chaîne "the white queen", utilisée avec le masque

```
((?:red|white) (king|queen))
```

les chaînes capturées seront "white queen" et "queen", numérotées respectivement 1 et 2

Le nombre maximal de chaînes capturées est de 65535, et le nombre total maximum (niveau d'emboîtement) de sous-masques (capturant ou non) est de 200.

Dans le cas où le masque non capturant doit comprendre des options supplémentaires, il est possible d'utiliser l'astuce suivante : placez le caractère correspondant à une option à activer entre "?" et ":". Ainsi, les deux masques suivants

```
(?i:saturday|sunday)
```

```
(?: (?i) saturday|sunday)
```

vont correspondre à la même chaîne. Puisque les alternatives sont vérifiées de gauche à droite et les options activées sont prises en compte jusqu'à la fin du masque, l'option activée dans une alternative est également activée dans toutes les alternatives suivantes. Ainsi, les masques ci-dessus accepteront aussi bien "SUNDAY" que "Saturday".

Répétitions

Les répétitions sont spécifiées avec des quantificateurs, qui peuvent être placés à la suite des caractères suivants :

- ◆ caractère alphabétique de données,
- ◆ métacaractère . (point),
- ◆ séquence de contrôle \C,
- ◆ séquence de contrôle correspondant à un caractère, par exemple \d,
- ◆ classe de caractères,



- ◆ référence arrière (voir le paragraphe précédent),
- ◆ sous-masque délimité pas des parenthèses (à moins que ce ne soit une assertion).

Les quantificateurs généraux précisent un nombre minimum et maximum de répétitions possibles, donnés par deux nombres entre accolades, et séparés par une virgule. Ces nombres doivent être inférieurs à 65536, et le premier nombre doit être égal ou inférieur au second. Par exemple

```
z{2,4}
```

accepte "zz", "zzz", ou "zzzz". L'accolade fermante n'a pas de signification par elle-même.

Si le second nombre est omis, mais que la virgule est là, cela signifie qu'il n'y a pas de limite supérieure. Si le second nombre et la virgule sont omis, le quantificateur correspond au nombre exact de répétitions attendues. Par exemple :

```
[aeiou]{3,}
```

accepte n'importe quelle succession d'au moins 3 voyelles minuscules, tandis que

```
\d{8}
```

n'accepte que 8 chiffres exactement.

Une accolade ouvrante qui apparaît à une position où le quantificateur n'est pas accepté, ou si la syntaxe des quantificateurs n'est pas respectée, sera considérée comme littérale. Par exemple, "{,6}" n'est pas un quantificateur, mais une chaîne de 4 caractères.

Le quantificateur {0} est autorisé, mais l'expression est alors ignorée.

Par convenance (et pour la compatibilité ascendante), les trois quantificateurs les plus communs ont une abréviation d'un seul caractère :

- ◆ * équivalent à {0,}
- ◆ + équivalent à {1,}
- ◆ ? équivalent à {0,1}



Il est possible de constituer des boucles infinies en créant un sous-masque sans caractères, mais pourvu d'un quantificateur sans limite supérieure. Par exemple

```
(a?) *
```

Par défaut, les quantificateurs sont dits "gourmands", c'est-à-dire, qu'ils cherchent d'abord à trouver le nombre maximal de répétitions qui autorise le succès de la recherche. L'exemple classique posé par cette gourmandise est la recherche de commentaires d'un programme en C. Les commentaires apparaissent entre les séquences `/*...*/` et à l'intérieur de ces délimiteurs, les `*` et `/` sont autorisés. Appliquer le masque

```
/\*.*\*/
```

à la chaîne

```
/* firs comment */ not comment
```

```
/* second comment */
```

ne peut réussir, car le masque travaille sur toute la chaîne, à cause de la gourmandise du caractère `*`.

Cependant, un quantificateur suivi d'un point d'interrogation cesse d'être gourmand, et au contraire, ne recherche que le nombre minimum de répétitions. Dans ces conditions, le masque

```
/\*.*?\*/
```

trouvera bien les commentaires du code C. La signification des autres quantificateurs n'est pas modifiée, ils assurent un nombre approprié de répétitions. Attention à ne pas confondre l'utilisation du point d'interrogation ici avec son utilisation comme quantificateur lui-même. A cause de cette ambiguïté, il peut être nécessaire de le doubler :

```
\d??\d
```

Ce masque va tenter de lire un seul chiffre, mais le cas échéant, il acceptera 2 chiffres pour permettre à la recherche d'aboutir.

Si l'option `PCRE_UNGREEDY` est activée, alors les quantificateurs sont non gourmands par défaut, mais peuvent être rendus gourmands au cas par cas, en ajoutant un point d'interrogation après. En d'autres



termes, cette option inverse le comportement par défaut.

Lorsqu'un sous-masque est quantifié avec un nombre minimum de répétitions, qui soit plus grand que 1, ou avec un maximum de répétitions, le masque compilé aura besoin de plus de place de stockage, proportionnellement au minimum et au maximum.

Groupement des éléments et quantificateurs possessifs

Si aucune coïncidence n'est obtenue lors d'un nombre maximum de répétitions ainsi qu'en cas d'un nombre minimum de répétitions, ceci entraîne une reprise de comparaison de la chaîne répétitive afin de vérifier si un autre nombre de répétitions permet d'obtenir une coïncidence avec la partie restante du masque. Dans certains cas, il est nécessaire de changer la logique décrite pour réaliser une comparaison spécifique ou afin de minimiser le nombre de tentatives de comparaison (si l'auteur est sûr que continuer les recherches n'a pas de sens).

Prenons par exemple le masque `\d+f00` à appliquer à la chaîne suivante :

```
123456bar
```

Après avoir capturé les 6 chiffres et sans trouver une coïncidence avec "f00", le moteur de recherche effectue encore une tentative de trouver une coïncidence pour l'élément `\d+`, mais cette fois, avec 5 chiffres, en cas d'échec, les 4 chiffres seront mis en comparaison etc.

Le «*groupement des éléments*» (dit *atomic grouping* ou *groupement atomique*, selon le terme utilisé par Jeffrey Friedl dans son livre) indique que dans le cas où une partie de masque coïncide, elle ne doit pas être analysée de nouveau.

Si nous utilisons le groupement dans l'exemple donné ci-dessus, le moteur de recherche arrête la recherche dès qu'il détecte une coïncidence avec "f00" pour la première fois. Les simples masques s'écrivent avec les parenthèses de la manière suivante : `(?>`. Par exemple :



```
(?>\d+)foo
```

Utilisés de cette façon, les parenthèses "verrouillent" la partie du masque qu'elles délimitent lors de la première détection d'une coïncidence; en cas de détection de non coïncidence avec la partie restante du masque, les parenthèses empêchent la reprise de l'analyse de la partie verrouillée. Cependant, ceci n'empêche pas de reprendre l'analyse d'autres éléments y compris ceux qui précèdent le groupe.

Autrement dit, le sous-masque de ce type correspond à la ligne de caractères avec laquelle on pourrait mettre en comparaison un autre masque identique s'il était ancré à la position courante de la chaîne.

Les sous-masques de groupement atomique ne sont pas capturants. Les exemples équivalents à celui ci-dessus peuvent être classés comme une capture inconditionnelle d'un nombre maximum de coïncidences. Ainsi, tandis que `\d+` et `\d+?` sont utilisés pour ajuster le nombre de chiffres à correspondre afin que la partie restante du masque puisse coïncider, `(?>\d+)` peut correspondre seulement à toute séquence des chiffres.

Les groupes atomiques peuvent comprendre n'importe quels sous-masques complexes, ils peuvent aussi être imbriqués. Cependant, lorsque un sous-masque utilisé pour le groupement est un élément simple qui se répète, tout comme dans l'exemple ci-dessus, il est possible d'utiliser un déterminant plus simple dit «quantificateur possessif». Le quantificateur possessif est spécifié avec un signe additionnel plus `+` placé après le quantificateur. Dans ce cas, l'exemple donné ci-dessus peut être interprété de la manière suivante

```
\d++foo
```

Les quantificateurs possessifs sont toujours gourmands ; l'activation de l'option `PCRE_UNGREEDY` est ignorée. Les quantificateurs représentent un moyen très commode pour désigner les simples formes du groupement atomique. Cependant, il n'y a pas de différence dans les valeurs ni dans le traitement d'un quantificateur possessif ou d'un groupe atomique.

Si le masque contient une répétition illimitée à l'intérieur du sous-masque, compte tenu du fait que ce dernier peut également être répété un nombre illimité de fois, l'utilisation du groupement atomique



est le seul moyen permettant d'éviter des fausses coïncidences pouvant prendre beaucoup de temps. Le masque

```
(\D+|<\d+>)*[!?]
```

correspond à un nombre illimité de sous-lignes qui ne contiennent pas de chiffres ou contiennent des chiffres délimités par les symboles <> suivis d'un point d'exclamation ! ou d'un point d'interrogation ?. Le processus est assez rapide en cas de détection d'une coïncidence. Cependant, l'exemple suivant prendra beaucoup de temps

```
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

avant que la conclusion de non correspondance ne soit établie. Ceci est possible puisque la ligne peut être délimitée de diverses manières entre une répétition interne \D+ et une répétition externe *, mais toutes les répétitions doivent être vérifiées. (L'exemple utilise [!?], ce qui est préférable par rapport à un caractère simple à la fin, puisque PCRE prévoit une optimisation qui permet la détection rapide des non coïncidences lors de l'utilisation d'un caractère simple. Le dernier caractère simple nécessaire à la correspondance sera mémorisé, dans le cas où le caractère n'est pas présent dans la chaîne, le résultat de non coïncidence revient très vite). Lorsque le masque est modifié en utilisant le groupement atomique, comme par exemple dans le cas suivant :

```
((?>\D+)|<\d+>)*[!?]
```

la séquence de caractères non numériques ne peut être rompue et la conclusion de non coïncidence se fait rapidement.

Les références arrières

En dehors des classes de caractères, un antislash suivi d'un nombre plus grand que 0 (et plusieurs chiffres suivants) est une référence arrière (c'est-à-dire vers la gauche) dans le masque, en supposant qu'il y ait suffisamment de sous-masques capturant précédents (parenthèses ouvrantes).

Cependant, si le nombre décimal suivant l'antislash est plus petit que 10, il sera toujours considéré comme une référence arrière, et cela générera une erreur si le nombre de captures n'est pas suffisant. En



d'autres termes, il faut qu'il existe suffisamment de parenthèses ouvrantes à gauche de la référence, surtout si la référence est inférieure à 10. Reportez-vous à la section "Caractères invisibles" pour avoir de plus amples détails à propos du traitement des chiffres qui suivent l'antislash.

La référence arrière remplace ce qui a été capturé par un sous-masque dans le masque courant, plutôt que de remplacer le sous-masque lui-même.

Ainsi le masque

```
(sens|respons)e and \libility
```

trouvera "sense and sensibility" et "response and responsibility", mais pas "sense and responsibility". Si la recherche tient compte de la casse, alors la casse de la chaîne capturée sera importante. Par exemple,

```
((?i)rah)\s+\1
```

trouve "rah rah" et "RAH RAH", mais pas "RAH rah", même si le sous-masque capturant initial ne tenait pas compte de la casse

Les références arrières relatives aux sous-masques décrits utilisent la syntaxe Python (`?P=name`). L'exemple cité ci-dessus pourrait être interprété de la manière suivante :

```
(?(?i)rah)\s+(?P=p1)
```

Il peut y avoir plusieurs références arrières dans le même sous-masque. Si un sous-masque n'a pas été utilisé dans une recherche, alors les références arrières échoueront. Par exemple le masque

```
(a|(bc))\2
```

échouera toujours s'il trouve une correspondance avec "a" plus tôt qu'avec "bc". Puisque le sous-masque peut contenir plusieurs parenthèses capturantes, tous les chiffres suivant l'antislash sont compris comme une partie de la référence arrière potentielle.

Si le masque recherche un chiffre après la référence, alors il faut



impérativement utiliser des délimiteurs pour terminer la référence arrière. Si l'option `PCRE_EXTENDED` est activée, on peut utiliser un espace. Sinon, un commentaire vide fait l'affaire.

Une référence arrière qui intervient à l'intérieur de parenthèses auxquelles elle fait référence échouera dès que le sous-masque sera utilisé. Par exemple, `(a\1)` échouera toujours. Cependant, ces références peuvent être utiles dans les sous-masques répétitifs. Par exemple le masque.

```
(a|b\1)+
```

pourra convenir pour "a" et "aba", "ababbaa", etc. À chaque itération du sous-masque, la référence arrière utilise le résultat du dernier sous-masque. Pour que cela fonctionne, il faut que la première itération n'ait pas besoin d'utiliser la référence arrière. Cela arrive avec les alternatives, comme dans l'exemple ci-dessus, ou avec un quantificateur de minimum 0.

Assertions

Une assertion est un test sur les caractères suivant ou précédant celui qui est en cours d'étude et ne concerne pas les caractères depuis la chaîne sujet. Les assertions simples `\b`, `\B`, `\A`, `\G`, `\Z`, `\z`, `^` et `$` sont décrites précédemment.

Il existe cependant des types d'assertions plus complexes, codées sous la forme de sous-masques. Il en existe deux types : celles qui travaillent au-delà de la position courante, et celles qui travaillent en-deça. Une assertion se comporte comme un sous-masque, hormis le fait qu'elle ne déplace pas le pointeur de position.

Les assertions ne sont pas capturantes, et ne peuvent pas être répétées. Si une assertion contient des sous-masques capturants en son sein, ils seront compris dans le nombre de sous-masques capturants du masque entier. La capture est réalisée pour les assertions positives, mais cela n'a pas de sens pour les assertions négatives.



Assertions avant

Les assertions avant commencent par `(?=` pour les assertions positives, et par `(?!` , pour les assertions négatives. Par exemple

```
\w+(?=;)
```

s'assure qu'un mot est suivi d'un point-virgule, mais n'inclut pas le point virgule dans la capture.

D'autre part,

```
foo(?!bar)
```

correspond à tout "foo" trouvé non suivi de "bar". Il est à noter que le masque

```
(?!foo)bar
```

en est proche, mais ne trouve pas une occurrence de " bar " qui soit précédée par quelque chose d'autre que " foo foo"; il trouve toutes les occurrences de " bar ", quel que soit ce qui le précède, car l'assertion `(?!foo)` est toujours vraie quand les trois caractères suivants sont " bar". Une assertion arrière est ici nécessaire.

Pour arrêter la recherche dans un point spécifié du masque, il vaut mieux utiliser `(?!)`, puisque la ligne vide est toujours mise en comparaison et ainsi l'assertion exigeant qu'il n'y ait pas de ligne vide échouera toujours.

Assertions arrières

Les assertions arrières commencent par `(?<=` pour les assertions positives, et `(?<!` pour les assertions négatives.

Par exemple,

```
(?<!foo)bar
```



trouve les occurrences de "bar" qui ne sont pas précédées par "foo".

Le contenu d'une référence arrière est limité de telle façon que les chaînes qu'il utilise soient toujours de la même taille. Cependant, lorsqu'il y a plusieurs alternatives, elles n'ont pas besoin d'être de la même taille,

```
(?<=bullock|donkey)
```

est autorisé, tandis que

```
(?<!dogs?|cats?)
```

provoque une erreur. Les alternatives qui ont des longueurs différentes ne sont autorisées qu'au niveau supérieur des assertions arrières. Une assertion telle que

```
(?<=ab(c|de))
```

n'est pas autorisée, car l'assertion de bas niveau (la deuxième, ici) a deux alternatives de longueurs différentes. Pour la rendre acceptable, il faut écrire:

```
(?<=abc|abde)
```

L'implémentation des assertions arrières déplace temporairement le pointeur de position vers l'arrière, et cherche à vérifier l'assertion. Si le nombre de caractères est différent, la position ne sera pas correcte, et l'assertion échouera.

PCRE n'autorise pas la séquence d'échappement `\C` dans les assertions arrières puisqu'il est impossible de calculer la longueur de vérification arrière. La séquence d'échappement `\X` pouvant correspondre à des nombres divers d'octets n'est pas autorisée non plus.

La combinaison d'assertions arrières avec des groupes atomiques peut être particulièrement pratique à la fin des chaînes afin de désigner les correspondances efficaces. Envisageons l'application du masque simple suivant :

```
abcd$
```

à une longue chaîne non correspondante au masque. Puisque la recherche se fait de gauche à droite, PCRE vérifie d'abord chaque "a"



dans le sujet et commence à analyser seulement après les éléments suivants dans le masque. Si le masque est spécifié de la manière suivante,

```
^.*abcd$
```

D'abord, `.*` est comparé à toute la ligne et lorsque la recherche échoue (puisque'il n'y a aucun "a"), la comparaison avec tous les caractères sauf le dernier sera effectuée, puis la procédure sera reprise, exceptés les deux derniers caractères etc. Finalement, la recherche de "a" prend toute la ligne de droite à gauche ce qui n'est pas mieux par rapport à la recherche précédente. Mais si le masque est spécifié de la manière ci-dessous

```
^(?>.*)(?<=abcd)
```

ou avec la syntaxe de quantificateur possessif (ce qui est identique)

```
^.*+(?<=abcd)
```

la reprise de recherche pour le symbole `.*` ne se fait pas; il ne peut que correspondre à la ligne entière. L'assertion arrière suivante ne vérifie qu'une seule fois les quatre derniers caractères. Si la recherche échoue, toute la correspondance échoue immédiatement. Lors de l'analyse des longues lignes, la différence de durée peut être importante.

Utilisations de plusieurs assertions

Plusieurs assertions peuvent intervenir successivement, leur nombre n'est pas limité. Par exemple, le masque

```
(?<=\d{3})(?!999)foo
```

recherche les chaînes "foo", précédées par trois chiffres qui ne sont pas "999". Notez que chaque assertion est appliquée indépendamment, au même point de la chaîne à traiter. Tout d'abord, il est vérifié que les trois premiers caractères ont tous des chiffres, puis on s'assure que ces trois caractères ne sont pas "999". Le masque précédent n'accepte pas "foo", précédé de 6 caractères, les trois premiers étant des chiffres et les trois suivants étant différents de "999". Par exemple, ce masque n'acceptera pas la chaîne "123abc-



foo". Pour ce faire, il faut utiliser le masque suivant :

```
(?<=\d{3}...) (?<!999)foo
```

Dans ce masque, la première assertion vérifie les six premiers caractères, s'assure que les trois premiers sont des entiers, et la deuxième assertion s'assure que les trois derniers caractères ne sont pas "999".

De plus, les assertions peuvent être imbriquées. Par exemple

```
(?<=(?!foo)bar)baz
```

recherche les occurrences de "baz" qui sont précédées par "bar" qui, à son tour, n'est pas précédé par "foo", tandis que

```
(?<=\d{3}(?!999)...)foo
```

est un autre masque, qui recherche les caractères "foo", précédés par trois chiffres, suivis de trois autres caractères qui ne forment pas "999".

Sous-masques conditionnels

Il est possible de lier un sous-masque à une condition, ou de choisir entre deux sous-masques alternatifs, en fonction du résultat d'une assertion, ou suivant les résultats de recherche précédents. Les deux formes possibles de sous-masques conditionnels sont

```
(?(condition)yes-pattern)
```

```
(?(condition)yes-pattern|no-pattern)
```

Si les conditions sont satisfaites, le masque positif est utilisé, sinon, le masque négatif est utilisé, s'il existe. S'il y a plus de deux alternatives, une erreur est générée à la compilation.

Il y a trois types de conditions : si le texte entre parenthèses est une séquence de chiffres, alors la condition est satisfaite si le sous-masque correspondant à ce numéro a réussi. Le nombre doit être positif. Considérons le masque suivant, qui contient des espaces non significatifs pour le rendre plus compréhensible (on supposera l'option `PCRE_EXTENDED` activée) et qui est divisé en trois parties pour



simplifier les explications :

```
( \ ( ) ? [ ^ ( ) ] + ( ? ( 1 ) \ ) )
```

La première partie recherche une parenthèse ouvrante optionnelle et, si elle existe, elle est capturée. La deuxième partie recherche une séquence de caractères qui ne contiennent pas de parenthèses. La troisième partie est conditionnée à la première, et s'assure que s'il y a une parenthèse ouvrante, il en existe une fermante. Si une parenthèse ouvrante a été trouvée, elle a été capturée, et donc la première capture existe, et la condition est exécutée. Sinon, elle est ignorée. Ce masque recherche donc une séquence de lettres, éventuellement placées entre parenthèses.

Si la condition est la chaîne (R), elle sera satisfaite si un appel récursif au masque ou au sous-masque a été fait. Au premier appel, la condition n'est pas vérifiée.

Si la condition n'est pas une séquence de chiffres, il faut que ce soit une assertion. Ce peut être une assertion positive ou négative, arrière ou avant. Considérons le masque suivant (mêmes conditions que le précédent) et avec deux alternatives en seconde ligne :

```
( ? ( ? = [ ^ a - z ] * [ a - z ] )  
\ d { 2 } - [ a - z ] { 3 } - \ d { 2 } | \ d { 2 } - \ d { 2 } - \ d { 2 } )
```

La condition est une assertion avant positive, qui recherche une séquence optionnelle de caractères non-lettres. En d'autres termes, elle teste la présence d'au moins une lettre dans la chaîne sujet. Si une lettre est trouvée, la recherche se poursuit avec la première alternative, et sinon, avec la seconde. Ce masque recherche des chaînes de la forme : dd-aaa-dd ou dd-dd-dd, avec aaa qui sont des lettres et dd qui sont des chiffres.



Annexe L. Format des fichiers de log

Les fichiers de log du **Serveur** (voir [Ecriture dans le log du serveur](#)) et de l'**Agent** sont au format texte, chaque ligne est comprise comme un message séparé.

La ligne de message a le format suivant :

```
<année><mois><date>  
. <heure><minute><seconde> . <centièmes_de_seconde>  
<type_de_message> [ <id_du_processus> ] <nom_du_flux>  
[ <source_du_message> ] <message>
```

avec :

- ◆ `<année><mois><date>`
. `<heure><minute><seconde>` . `<centièmes_de_seconde>` est la date précise de l'écriture du message dans le fichier de log.
- ◆ `<type_de_message>` – niveau de log :
 - **ftl** (fatal error – erreur fatale) – messages sur des erreurs critiques relatives au fonctionnement ;
 - **err** (error – erreur) – messages sur des erreurs de fonctionnement ;
 - **wrn** (warning – avertissement) – avertissements sur des erreurs ;
 - **ntc** (notice – note) – messages d'information importants ;
 - **inf** (info – information) – messages d'information ;
 - **tr0..3** (trace0..3 – traçage) – traçage des actions réalisées de divers niveaux de détail (**Traçage3** – niveau de détail maximum) ;
 - **db0..3** (debug0..3 – débogage) – message de débogage de divers niveaux de détail (**Débogage3** – niveau maximum de détail).



Les messages de niveau de log **tr0..3** (traçage) et **db0..3** (débogage) sont écrits seulement pour les développeurs de **Dr. Web ESS**.



- ◆ [*<id_du_processus>*] – identificateur numérique unique du processus durant lequel le flux écrivant le message dans le fichier de log a été exécuté. Sous certains OS [*<id_du_processus>*] peut être représenté sous la forme [*<id_du_processus> <id_du_flux>*].
- ◆ *<nom_du_flux>* – désignation symbolique du flux au sein duquel l'écriture du message vers le fichier de log a été effectuée.
- ◆ [*<source_du_message>*] – désignation du système initiateur de l'écriture du message vers le fichier de log. La source n'est pas toujours présente.
- ◆ *<message>* – message texte décrivant les actions conformément au niveau du journal. Il peut comprendre une description formelle ainsi que les valeurs des variables importantes pour le cas courant.

Par exemple :

1) 20081023.171700.74 inf [001316] mth:12 [Sch]
Job "Purge unsent IS events" said OK

avec :

- ◆ 20081023 – *<année><mois><jour>*,
- ◆ 171700 – *<heure><minute><seconde>*,
- ◆ 74 – *<centièmes_de_seconde>*,
- ◆ inf – *<type_de_message>* - message d'information,
- ◆ [001316] – [*<id_du_processus>*],
- ◆ mth:12 – *<nom_du_flux>*,
- ◆ [Sch] – [*<source_du_message>*] - planificateur,
- ◆ Job "Purge unsent IS events" said OK – *<message>* sur l'exécution correcte de la tâche **Suppression des événements non envoyés**.

2) 20081028.135755.61 inf [001556] srv:0
tcp/10.3.0.55:3575/025D4F80:2: new connection
at tcp/10.3.0.75:2193

avec :

- ◆ 20081028 – *<année><mois><jour>*,



- ◆ 135755 – *<heure><minute><seconde>*,
- ◆ 61 – *<centième_de_seconde>*,
- ◆ inf – *<type_de_message>* - message d'information,
- ◆ [001556] – [*<id_du_processus>*],
- ◆ srv:0 – *<nom_du_flux>*,
- ◆ tcp/10.3.0.55:3575/025D4F80:2: new connection at tcp/10.3.0.75:2193 – *<message>* sur l'installation d'une nouvelle connexion via le socket spécifié.



Annexe M. Description des procédures utilisateur

Pour faciliter et automatiser l'exécution de certaines tâches de **Serveur Enterprise**, il est possible d'utiliser les procédures utilisateur effectuées en tant que scripts Lua. Les scripts doivent être placés dans le dossier suivant :

- ◆ sous Windows: `var\extensions`
- ◆ sous FreeBSD et OS Solaris: `/var/drwcs/extensions`
- ◆ sous Linux: `/var/opt/drwcs/extensions`

du répertoire d'installation du **Serveur**. Après l'installation du **Serveur**, les procédures pré-installées pouvant être utilisées sont placées dans ce répertoire. Afin de pouvoir les exécuter, le **Serveur** doit être démarré avec la clé `-hooks`.

Par défaut tous les scripts sont désactivés. Pour activer les scripts, il est nécessaire de supprimer le paramètre `initial disabled` ou tout le commentaire (laisser la ligne vide) dans le fichier du script.

Le répertoire `extensions` contient les scripts suivants :

- ◆ `access_check.ds` – appelé avant la vérification d'accès conformément à ACL (Access Control List - listes de contrôle d'accès) respectif ;
- ◆ `access_denied.ds` – appelé en cas d'interdiction d'accès conformément aux paramètres de ACL ou selon le résultat de l'exécution de la procédure `access_check` ;
- ◆ `admin_logged.ds` – appelé en cas d'authentification réussite de l'administrateur dans le **Centre de Gestion** ;
- ◆ `admin_noauth.ds` – appelé en cas d'erreur lors de l'authentification de l'administrateur dans le **Centre de Gestion** ;
- ◆ `agent_status.ds` – appelé lorsque l'**Agent** communique ses politiques locales ;
- ◆ `backup.ds` – appelé après la fin de la sauvegarde des fichiers



(backup) mais avant la suppression des fichiers relatifs à la copie précédente de sauvegarde ;

- ◆ `bad_connection.ds` – appelé en cas d'impossibilité de se connecter au client ;
- ◆ `connection_denied.ds` – appelé en cas d'interdiction d'une nouvelle connexion selon des limitations relatives à la licence ;
- ◆ `database_load.ds` – appelé après la fin du processus de téléchargement du pilote de la base de données ;
- ◆ `database_verify.ds` – appelé après la fin de la vérification de la base de données ;
- ◆ `deinstallation.ds` – appelé après la fin de la suppression de l'**Agent** ;
- ◆ `disconnected.ds` – appelé après la fin de la connexion au client ;
- ◆ `group_changed.ds` – appelé lors de la modification des paramètres du groupe ;
- ◆ `group_created.ds` – appelé lors de la création d'un nouveau groupe ;
- ◆ `group_deleted.ds` – appelé lors de la suppression d'un groupe ;
- ◆ `install.ds` – appelé à la réception de l'événement installation ;
- ◆ `installed_components.ds` – appelé lorsque l'**Agent** communique la liste des composants installés sur le poste ;
- ◆ `jobexecuted.ds` – appelé à la réception depuis l'**Agent** de l'événement `job executed`;
- ◆ `license_error.ds` – appelé en cas d'impossibilité de se connecter au client selon des limitations relatives à la licence ;
- ◆ `load_plugin.ds` – appelé après le chargement d'un module ajoutable (plugin) ;
- ◆ `load_protocol.ds` – appelé après le chargement du module de journal ;
- ◆ `neighbor_connected.ds` – appelé à la connexion au **Serveur** ;



- ◆ `neighbor_install.ds` – appelé à la réception de l'événement `installation` depuis un **Serveur** voisin ;
- ◆ `neighbor_noauth.ds` – appelé après une connexion refusée avec le **Serveur** suite à une erreur d'authentification ;
- ◆ `neighbor_run_begin.ds` – appelé à la réception de l'événement `component started` depuis un **Serveur** voisin ;
- ◆ `neighbor_run_end.ds` – appelé à la réception de l'événement `component completed` depuis un **Serveur** voisin ;
- ◆ `neighbor_scan_error.ds` – appelé à la réception de l'événement `scan error` depuis un **Serveur** voisin ;
- ◆ `neighbor_scan_statistics.ds` – appelé à la réception de l'événement `scan statistics` depuis un **Serveur** voisin ;
- ◆ `neighbor_station_status.ds` – appelé à la réception depuis un **Serveur** voisin des politiques/configurations locales du poste ;
- ◆ `neighbor_virus.ds` – appelé à la réception de l'événement `virus detected` depuis un **Serveur** voisin ;
- ◆ `newbie_accepted.ds` – appelé à l'attribution d'accès à un novice ainsi que lors de son authentification réussie et la création d'un poste dans la base de données ;
- ◆ `newbie_came.ds` – appelé à la connexion d'un novice ;
- ◆ `newbie_registered.ds` – appelé après l'attribution d'accès à un novice mais avant l'enregistrement des informations respectives dans la base de données ;
- ◆ `pong.ds` – appelé à la réception de `PONG` depuis le client ;
- ◆ `run_begin.ds` – appelé à la réception de l'événement `component started` depuis l'**Agent** ;
- ◆ `run_end.ds` – appelé à la réception de l'événement `component completed` depuis l'**Agent** ;
- ◆ `scan_error.ds` – appelé à la réception de l'événement `scan error` depuis l'**Agent** ;
- ◆ `scan_statistics.ds` – appelé à la réception de



l'événement `scan statistics` depuis l'**Agent** ;

- ◆ `server_jobexecuted.ds` – appelé après l'exécution d'une tâche sur le **Serveur** ;
- ◆ `server_load.ds` – appelé après le chargement du fichier binaire du **Serveur** nécessaire pour accomplir certaines fonctions de service (**Serveur** ne va pas servir les clients) ;
- ◆ `server_start.ds` – appelé au démarrage du **Serveur** et lorsqu'il est prêt à servir les clients ;
- ◆ `server_terminate.ds` – appelé après la fin du traitement des clients par le **Serveur** ;
- ◆ `server_unload.ds` – appelé après la fin de l'exécution de certaines fonctions par le **Serveur** (le **Serveur** n'a pas servi les clients) ;
- ◆ `station_connected.ds` – appelé à la connexion réussie à l'**Agent** ;
- ◆ `station_create.ds` – appelé à la fin de création d'un poste ;
- ◆ `station_date.ds` – appelé en cas de détection de l'heure/ de la date incorrecte du poste ;
- ◆ `station_deleted.ds` – appelé à la suppression d'un poste ;
- ◆ `station_noauth.ds` – appelé après une connexion refusée à l'**Agent** suite à une erreur d'authentification ;
- ◆ `station_update_failed.ds` – appelé après la réception d'un message de l'**Agent** sur une erreur de mise à jour du poste ;
- ◆ `station_update_reboot.ds` – appelé après la réception d'un message de l'**Agent** sur la nécessité de redémarrer le poste après la mise à jour ;
- ◆ `unload_plugin.ds` – appelé au déchargement d'un module ajoutable (plugin) ;
- ◆ `unload_protocol.ds` – appelé au déchargement du module de journal ;
- ◆ `virus.ds` – appelé à la réception de l'événement `virus detected` depuis l'**Agent** ;



- ◆ `virusbases.ds` – appelé à l'envoi par l'**Agent** des informations sur la base de données virales.



Annexe N. Intégration de Dr.Web Enterprise Security Suite avec XML Web API



Pour en savoir plus sur **XML Web API**, consultez le manuel **XML API pour Dr.Web® Enterprise Security Suite** (voir aussi [Aide](#)).

Application

L'intégration de **XML Web API** avec **Dr.Web Enterprise Security Suite** offre les fonctionnalités réalisant des opérations avec les comptes et permettant d'automatiser le processus d'administration des utilisateurs du service. Vous pouvez l'utiliser, par exemple, lors de la création des pages dynamiques destinées à recevoir des requêtes utilisateur et permettant de fournir à l'utilisateur du fichier d'installation.

Authentification

L'interaction avec **Serveur Enterprise** est effectuée via le protocole HTTP(S). XML API reçoit des requêtes RESET et retourne XML. Pour accéder à XML API, l'authentification Basic http est utilisée (conformément à la norme [RFC 2617](#)). Si la norme RFC 2617 n'est pas respectée, le serveur HTTP(S) ne va pas demander les données d'authentification du client ; pour réussir l'authentification (le nom de login et le mot de passe de l'administrateur de **Dr.Web ESS**).



Annexe O. Procédures d'authentification des administrateurs



Vous trouverez des informations de base relatives à l'authentification des administrateurs sur **Serveur Enterprise** dans le paragraphe [Authentification des administrateurs](#).

Authentification en cas d'utilisation d'Active Directory

Seuls la disponibilité et l'ordre dans la liste des authentificateurs doivent être configurés : balises `<enabled/>` et `<order/>` dans `auth-ads.xml`.

Principe de fonctionnement :

1. L'administrateur définit le nom d'utilisateur et le mot de passe à l'un des formats suivants :
 - ◆ `username`,
 - ◆ `domain\username`,
 - ◆ `username@domain`,
 - ◆ LDAP DN de l'utilisateur.
2. Le serveur s'authentifie sur le contrôleur de domaine par défaut avec ce nom d'utilisateur et ce mot de passe (ou sur un contrôleur de domaine pour le domaine spécifié dans le nom d'utilisateur).
3. En cas d'authentification échouée, le mécanisme d'authentification suivant sera essayé.
4. Puis LDAP DN de l'utilisateur enregistré sera déterminé.
5. L'attribut `DrWeb_Admin` est lu depuis l'objet ayant le DN déterminé. Si l'attribut prend la valeur `FALSE`, la tentative est classée comme échouée et le mécanisme d'authentification suivant sera appliqué.



6. L'attribut `DrWeb_AdminReadOnly` est lu. Si l'attribut prend la valeur `TRUE`, l'administrateur dispose des droits en lecture seule.
7. L'attribut `DrWeb_AdminGroupOnly` est lu. Si l'attribut prend la valeur `TRUE`, l'administrateur dispose des droits lui permettant de gérer uniquement les certains groupes.
8. L'attribut `DrWeb_AdminGroup` est lu. Cet attribut doit contenir une liste des groupes à gérer par l'administrateur spécifié.
9. Si lors de cette étape, certains attributs ne sont pas déterminés, ils seront recherchés dans les groupes dont l'utilisateur fait partie. Les groupes parentaux de chaque groupe seront vérifiés (stratégie de recherche - en profondeur).



En cas de n'importe quel erreur, le mécanisme d'authentification suivant sera appliqué.

L'utilitaire `drwschema-modify.exe` (inclus dans le package d'installation du **Serveur**) crée une nouvelle classe d'objets dans Active Directory et décrit les nouveaux attributs pour cette classe.

Dans l'espace **Enterprise**, les attributs ont les OID suivants :

```
#define DrWeb_enterprise_OID      "1.3.6.1.4.1"
// iso.org.dod.internet.private.enterprise
#define DrWeb_DrWeb_OID          DrWeb_enterprise_OID
".29690" // DrWeb
#define DrWeb_EnterpriseSuite_OID DrWeb_DrWeb_OID
".1" // EnterpriseSuite
#define DrWeb_Alerts_OID
DrWeb_EnterpriseSuite_OID ".1" // Alerts
#define DrWeb_Vars_OID
DrWeb_EnterpriseSuite_OID ".2" // Vars
#define DrWeb_AdminAttrs_OID
DrWeb_EnterpriseSuite_OID ".3" // AdminAttrs

// 1.3.6.1.4.1.29690.1.3.1 (AKA
iso.org.dod.internet.private.enterprise.DrWeb.EnterpriseSuite.AdminAttrs.Admin)

#define DrWeb_Admin_OID          DrWeb_AdminAttrs_OID
".1" // R/W admin
```



```
#define DrWeb_AdminReadOnly_OID    DrWeb_AdminAttrs_OID
".2"                               // R/O admin
#define DrWeb_AdminGroupOnly_OID  DrWeb_AdminAttrs_OID
".3"                               // Group admin
#define DrWeb_AdminGroup_OID      DrWeb_AdminAttrs_OID
".4"                               // Admin's group
#define DrWeb_Admin_AttrName      "DrWebAdmin"
#define DrWeb_AdminReadOnly_AttrName
"DrWebAdminReadOnly"
#define DrWeb_AdminGroupOnly_AttrName
"DrWebAdminGroupOnly"
#define DrWeb_AdminGroup_AttrName "DrWebAdminGroup"
```

L'édition des propriétés des utilisateurs d'Active Directory se fait de manière manuelle sur le serveur d'Active Directory (voir [Authentification des administrateurs](#)).

Algorithme d'analyse des attributs lors de l'authentification :

1. Les attributs de l'utilisateur sont lus.
2. Si l'attribut `DrWebAdmin` prend la valeur `TRUE` :
 - 2.1. S'il y a des attributs manquants et que l'attribut `DrWebInheritPermissions` prend la valeur `TRUE`, les attributs manquants seront lus depuis les groupes. La procédure de recherche dans les groupes est terminée dès que tous les attributs sont spécifiés. Ainsi, plus tôt les attributs sont lus, plus haute est leur priorité. L'accès de l'administrateur est autorisé.
 - 2.2. S'il y a des attributs manquants et que l'attribut `DrWebInheritPermissions` prend la valeur `FALSE` (ou non déterminé), l'accès de l'administrateur est autorisé.
 - 2.3. Si tous les attributs sont spécifiés, l'accès de l'administrateur est autorisé.
3. Si l'attribut `DrWebAdmin` prend la valeur `FALSE`, l'accès de l'administrateur est interdit.
4. Si l'attribut `DrWebAdmin` n'est pas spécifié :
 - 4.1. Si l'attribut `DrWebInheritPermissions` prend la valeur `TRUE`, les attributs sont lus depuis les groupes. Puis on procède comme à l'étape 2.



4.2. Si l'attribut `DrWebInheritPermissions` prend la valeur `FALSE` (ou non spécifié), on procède comme à l'étape 3.

Authentification en cas d'utilisation de LDAP

Les paramètres sont écrits dans le fichier de configuration `auth-ldap.xml`.

Les balises principales du fichier de configuration :

- ◆ `<enabled/>` et `<order/>` - comme dans le cas Active Directory.
- ◆ `<server/>` spécifie l'adresse du serveur LDAP.
- ◆ `<user-dn/>` détermine les règles de transformation des noms vers DN à l'aide des masque de type DOS.

La balise `<user-dn/>` permet d'utiliser les caractères de substitution :

- * remplace une séquence de n'importe quels caractères sauf `.`, `,`, `=`, `@`, `\` et des espaces ;
- # remplace une séquence de n'importe quels caractères.
- ◆ `<user-dn-expr/>` détermine les règles de transformation des noms vers DN à l'aide des expressions régulières.

Pour l'exemple, la même règle dans deux variantes :

```
<user-dn user="*@example.com" dn="CN=\1,DC=example,DC=com"/>
<user-dn-expr user="(.* )@example.com" dn="CN=\1,DC=example,DC=com"/>
```

`\1 .. \9` déterminent la place de substitution dans le template des valeurs *, # ou des expressions entre parenthèses.

Selon ce principe, si le nom d'utilisateur est spécifié au format `login@example.com`, après la transformation, le DN a le format suivant : `"CN=login,DC=example,DC=com"`.

- ◆ `<user-dn-extension-enabled/>` autorise l'exécution du script `Lua ldap-user-dn-translate.ds` (depuis le dossier `extensions`) pour transformer le nom d'utilisateur vers DN.



Ce script est exécuté après avoir essayé toutes les règles `user-dn`, `user-dn-expr` et si aucune règle correspondante n'est trouvée. Le script a un seul paramètre - le nom d'utilisateur entré. Le script retourne la ligne contenant DN, sinon il retourne la ligne vide. Dans le cas, où aucune règle ne correspond et que le script n'est pas autorisé ou il n'a rien retourné, le nom d'utilisateur entré sera utilisé tel qu'il est.

- ◆ Les attributs de l'objet LDAP pour DN reçu suit à la transformation, leurs valeurs possibles peuvent être modifiées à l'aide des balises (les valeurs par défaut sont décrites):

```
<!-- DrWebAdmin attribute equivalent (OID
1.3.6.1.4.1.29690.1.3.1) -->
<admin-attribute-name value="DrWebAdmin" true-
value="^TRUE$" false-value="^FALSE$"/>

<!-- DrWebAdminGroupOnly attribute equivalent (OID
1.3.6.1.4.1.29690.1.3.2) -->
<readonly-admin-attribute-name
value="DrWebAdminReadOnly" true-value="^TRUE$" false-
value="^FALSE$"/>

<!-- DrWebAdminGroupOnly attribute equivalent (OID
1.3.6.1.4.1.29690.1.3.3) -->
<grouponly-admin-attribute-name
value="DrWebAdminGroupOnly" true-value="^TRUE$" false-
value="^FALSE$"/>

<!-- DrWebAdminGroup attribute equivalent (OID
1.3.6.1.4.1.29690.1.3.4) -->
<groups-admin-attribute-name
value="DrWebAdminGroup"/>
```

En tant que les valeurs de paramètres `true-value/false-value` des expressions régulières sont spécifiées.

- ◆ S'il reste des valeurs des attributs de l'administrateur non déterminées et que dans le fichier de configuration, la balise `<group-reference-attribute-name value="memberOf"/>` est spécifiée, la valeur de l'attribut `memberOf` sera comprise comme une liste de DN des groupes dont l'administrateur fait partie. Dans ce cas, la recherche des attributs nécessaires sera effectuée par groupes tout comme dans le cas avec l'utilisation d'Active Directory.



Annexe P. Licences

Cette section contient une liste de bibliothèques de logiciels tiers qui sont utilisés par le logiciel **Dr.Web ESS** ainsi que des informations sur leurs licences et les adresses des projets de développement.

Bibliothèque tierce	Licence	URL du projet
boost	http://www.boost.org/users/license.html *	http://www.boost.org/
c-ares	MIT License*	http://c-ares.haxx.se/
Gecko SDK	Mozilla Public License* GNU Lesser General Public License* GNU General Public License*	https:// developer.mozilla.org/ru/ docs/Gecko_SDK
jQuery	MIT License* GNU General Public License*	http://jquery.com/
libcurl	http://curl.haxx.se/docs/ copyright.html *	http://curl.haxx.se/libcurl/
libradius	© Juniper Networks, Inc.*	http://www.freebsd.org
libxml2	MIT License*	http://www.xmlsoft.org/
lua	MIT License*	http://www.lua.org/
lua-xmlreader	MIT License*	http://asbradbury.org/ projects/lua-xmlreader/
md5 implementation	© WIDE Project*	–
Net-snmp	http://www.net-snmp.org/ about/license.html *	http://www.net-snmp.org/
OpenLDAP	http://www.openldap.org/ software/release/ license.html *	http://www.openldap.org
OpenSSL	http://www.openssl.org/ source/license.html *	http://www.openssl.org/



Bibliothèque tierce	Licence	URL du projet
Oracle Instant Client	http://www.oracle.com/technetwork/licenses/instant-client-lic-152016.html *	http://www.oracle.com
pcre	http://www.pcre.org/licence.txt *	http://www.pcre.org
Prototype JavaScript framework	MIT License*	http://prototypejs.org/assets/2009/8/31/prototype.js
Regina Rexx Interpreter	GNU Lesser General Public License*	http://regina-rexx.sourceforge.net/
sha2 implementation	© Dr. Brian Gladman, Worcester, UK*	–
SQLite	Public Domain (http://www.sqlite.org/copyright.html)	http://www.sqlite.org/
wtl	Common Public License (http://opensource.org/licenses/cpl1.0.php)*	http://sourceforge.net/projects/wtl/
XML/SWF Charts	Bulk License (http://maani.us/xml_charts/index.php?menu=Buy)	http://www.maani.us/xml_charts/index.php?menu=Introduction
zlib	http://www.zlib.net/zlib_license.html *	http://www.zlib.net/

* - consultez les textes de licences ci-dessous.

P1. Boost

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute,



execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

P2. Curl

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2013, Daniel Stenberg,
<daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.



THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

P3. Libradius

Copyright 1998 Juniper Networks, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES



```
(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR
PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON
ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN
IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

```
$FreeBSD: src/lib/libradius/radlib_private.h,v 1.6.30.3
2012/04/21 18:30:48 melifaro Exp $
```

P4. MD5 implementation

Copyright (C) 1995, 1996, 1997, and 1998 WIDE Project.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

```
THIS SOFTWARE IS PROVIDED BY THE PROJECT AND
CONTRIBUTORS 'AS IS' AND ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL
THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT,
INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
```



PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

P5. Net-snmp

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts.

---- Part 1: CMU/UCD copyright notice: (BSD like) ----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.



CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc
copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS 'AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED



WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER 'AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING,



BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara,

California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.



* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS 'AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) ----

Copyright (c) 2003-2009, Sparta, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.



* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS 'AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) ----

Copyright (c) 2004, Cisco, Inc and Information Network

Center of Beijing University of Posts and Telecommunications.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.



* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS 'AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG
copyright notice (BSD) ----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003
oss@fabasoft.com

Author: Bernhard Penz

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:



* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER 'AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

----- Part 8: Apple Inc. copyright notice (BSD) -----

Copyright (c) 2007 Apple Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the



following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of Apple Inc. ("Apple") nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY APPLE AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL APPLE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 9: ScienceLogic, LLC copyright notice (BSD)

Copyright (c) 2009, ScienceLogic, LLC

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.



* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of ScienceLogic, LLC nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS 'AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

P6. OpenLDAP

The OpenLDAP Public License

Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,



2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following

 disclaimer in the documentation and/or other materials provided with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time.

Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS 'AS IS' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP



Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City,

California, USA. All Rights Reserved. Permission to copy and

distribute verbatim copies of this document is granted.

P7. OpenSSL

LICENSE ISSUES

=====

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit.

See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

=====

Copyright (c) 1998-2011 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the



above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT 'AS IS' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR



PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

=====

This product includes cryptographic software written by Eric Young

(eay@cryptsoft.com). This product includes software written by Tim

Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young



should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

```
"This product includes cryptographic software  
written by Eric Young (eay@cryptsoft.com)"
```

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

```
"This product includes software written by Tim  
Hudson (tjh@cryptsoft.com)"
```

```
THIS SOFTWARE IS PROVIDED BY ERIC YOUNG 'AS IS' AND  
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT  
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY  
AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN  
NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR  
ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR  
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,  
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF  
USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER  
CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN  
CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING  
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
```




USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence

[including the GNU Public Licence.]

P8. Oracle Instant Client

Export Controls on the Programs

Selecting the "Accept License Agreement" button is a confirmation of your agreement that you comply, now and during the trial term, with each of the following statements:

-You are not a citizen, national, or resident of, and are not under control of, the government of Cuba, Iran, Sudan, Libya, North Korea, Syria, nor any country to which the United States has prohibited export.

-You will not download or otherwise export or re-export the Programs, directly or indirectly, to the above mentioned countries nor to citizens, nationals or residents of those countries.

-You are not listed on the United States Department of Treasury lists of Specially Designated Nationals, Specially Designated Terrorists, and Specially Designated Narcotic Traffickers, nor are you listed on the United States Department of Commerce Table of Denial Orders.

You will not download or otherwise export or re-export the Programs, directly or indirectly, to persons on the above mentioned lists.

You will not use the Programs for, and will not allow the Programs to be used for, any purposes prohibited by



United States law, including, without limitation, for the development, design, manufacture or production of nuclear, chemical or biological weapons of mass destruction.

EXPORT RESTRICTIONS

You agree that U.S. export control laws and other applicable export and import laws govern your use of the programs, including technical data; additional information can be found on Oracle®'s Global Trade Compliance web site (<http://www.oracle.com/products/export>).

You agree that neither the programs nor any direct product thereof will be exported, directly, or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation.

Oracle Employees: Under no circumstances are Oracle Employees authorized to download software for the purpose of distributing it to customers. Oracle products are available to employees for internal use or demonstration purposes only. In keeping with Oracle's trade compliance obligations under U.S. and applicable multilateral law, failure to comply with this policy could result in disciplinary action up to and including termination.

Note: You are bound by the Oracle Technology Network ("OTN") License Agreement terms. The OTN License Agreement terms also apply to all updates you receive under your Technology Track subscription.

The OTN License Agreement terms below supercede any shrinkwrap license on the OTN Technology Track software CDs and previous OTN License terms (including the Oracle Program License as modified by the OTN Program Use Certificate).



Oracle Technology Network Development and Distribution
License Agreement for Instant Client

"We," "us," and "our" refers to Oracle America, Inc. "You" and "your" refers to the individual or entity that wishes to use the Programs from Oracle under this Agreement. "Programs" refers to the Software Products referenced below that you wish to download and use and Program documentation. "License" refers to your right to use the Programs and Program documentation under the terms of this Agreement. The substantive and procedural laws of California govern this Agreement. You and Oracle agree to submit to the exclusive jurisdiction of, and venue in, the courts of San Francisco, San Mateo, or Santa Clara counties in California in any dispute arising out of or relating to this Agreement.

We are willing to license the Programs to you only upon the condition that you accept all of the terms contained in this Agreement. Read the terms carefully and select the "Accept" button at the bottom of the page to confirm your acceptance. If you are not willing to be bound by these terms, select the "Do Not Accept" button and the registration process will not continue.

Software Product

- Instant Client

License Rights

License.

We grant you a non-exclusive right and license to use the Programs solely for your business purposes and development and testing purposes, subject to the terms of this Agreement. You may allow third parties to use the Programs, subject to the terms of this Agreement, provided such third party use is for your business operations only.



Distribution License

We grant you a non-exclusive right and license to distribute the Programs, provided that you do not charge your end users for use of the Programs. Your distribution of such Programs shall at a minimum include the following terms in an executed license agreement between you and the end user that: (1) restrict the use of the Programs to the business operations of the end user; (2) prohibit (a) the end user from assigning, giving, or transferring the Programs or an interest in them to another individual or entity (and if your end user grants a security interest in the Programs, the secured party has no right to use or transfer the Programs); (b) make the Programs available in any manner to any third party for use in the third party's business operations (unless such access is expressly permitted for the specific program license or materials from the services you have acquired); and (c) title to the Programs from passing to the end user or any other party; (3) prohibit the reverse engineering (unless required by law for interoperability), disassembly or decompilation of the Programs and prohibit duplication of the Programs except for a sufficient number of copies of each Program for the end user's licensed use and one copy of each Program media; (4) disclaim, to the extent permitted by applicable law, our liability for any damages, whether direct, indirect, incidental, or consequential, arising from the use of the Programs; (5) require the end user at the termination of the Agreement, to discontinue use and destroy or return to you all copies of the Programs and documentation; (6) prohibit publication of any results of benchmark tests run on the Programs; (7) require the end user to comply fully with all relevant export laws and regulations of the United States and other applicable export and import laws to assure that neither the Programs, nor any direct product thereof, are exported, directly or indirectly, in violation of applicable laws; (8) do not require us to perform any obligations or incur any liability not previously agreed to between you and us; (9) permit you to audit your end user's use of the Programs or to assign your right to audit the end user's use of the Programs to us; (10) designate us as a third party beneficiary of the end user license agreement; (11) include terms consistent with those contained in the sections of this Agreement entitled "Disclaimer of Warranties and Exclusive Remedies," "No Technical Support," "End of Agreement," "Relationship Between the Parties," and "Open Source"; and (11) exclude the application of the Uniform Computer Information



Transactions Act.

You may allow your end users to permit third parties to use the Programs on such end user's behalf for the purposes set forth in the end user license agreement, subject to the terms of such agreement. You shall be financially responsible for all claims and damages to us caused by your failure to include the required contractual terms set forth above in each end user license agreement between you and an end user. We are a third party beneficiary of any end user license agreement between you and the end user, but do not assume any of your obligations thereunder, and you agree that you will not enter into any end user license agreement that excludes us as a third party beneficiary and will inform your end users of our rights.

If you want to use the Programs for any purpose other than as expressly permitted under this Agreement you must contact us to obtain the appropriate license. We may audit your use of the Programs. Program documentation is either shipped with the Programs, or documentation may be accessed online at <http://www.oracle.com/technetwork/indexes/documentation/index.html>.

You agree to: (a) defend and indemnify us against all claims and damages caused by your distribution of the Programs in breach of this Agreement and/or failure to include the required contractual provisions in your end user agreement as stated above; (b) keep executed end user agreements and records of end user information including name, address, date of distribution and identity of Programs distributed; (c) allow us to inspect your end user agreements and records upon request; and, (d) enforce the terms of your end user agreements so as to effect a timely cure of any end user breach, and to notify us of any breach of the terms.

Ownership and Restrictions

We retain all ownership and intellectual property rights in the Programs. You may make a sufficient number of copies of the Programs for the licensed use and one copy



of the Programs for backup purposes.

You may not:

- use the Programs for any purpose other than as provided above;
- charge your end users for use of the Programs;
- remove or modify any Program markings or any notice of our proprietary rights;
- assign this agreement or give the Programs, Program access or an interest in the Programs to any individual or entity except as provided under this agreement;
- cause or permit reverse engineering (unless required by law for interoperability), disassembly or decompilation of the Programs;
- disclose results of any Program benchmark tests without our prior consent.

Export

You agree that U.S. export control laws and other applicable export and import laws govern your use of the Programs, including technical data; additional information can be found on Oracle's Global Trade Compliance web site located at <http://www.oracle.com/products/export/index.html>. You agree that neither the Programs nor any direct product thereof will be exported, directly, or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation.

Disclaimer of Warranty and Exclusive Remedies

THE PROGRAMS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. WE FURTHER DISCLAIM ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT.



IN NO EVENT SHALL WE BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR DATA USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR ENTIRE LIABILITY FOR DAMAGES HEREUNDER SHALL IN NO EVENT EXCEED ONE THOUSAND DOLLARS (U.S. \$1,000).

No Technical Support

Our technical support organization will not provide technical support, phone support, or updates to you or end users for the Programs licensed under this agreement.

Restricted Rights

If you distribute a license to the United States government, the Programs, including documentation, shall be considered commercial computer software and you will place a legend, in addition to applicable copyright notices, on the documentation, and on the media label, substantially similar to the following:

NOTICE OF RESTRICTED RIGHTS

"Programs delivered subject to the DOD FAR Supplement are 'commercial computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement. Otherwise, programs delivered subject to the Federal Acquisition Regulations are 'restricted computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065."

End of Agreement

You may terminate this Agreement by destroying all copies of the Programs. We have the right to terminate your right to use the Programs if you fail to comply with any of the terms of this Agreement, in which case you shall destroy all copies of the Programs.



Relationship Between the Parties

The relationship between you and us is that of licensee/licensor. Neither party will represent that it has any authority to assume or create any obligation, express or implied, on behalf of the other party, nor to represent the other party as agent, employee, franchisee, or in any other capacity. Nothing in this Agreement shall be construed to limit either party's right to independently develop or distribute software that is functionally similar to the other party's products, so long as proprietary information of the other party is not included in such software.

Open Source

"Open Source" software - software available without charge for use, modification and distribution - is often licensed under terms that require the user to make the user's modifications to the Open Source software or any software that the user 'combines' with the Open Source software freely available in source code form. If you use Open Source software in conjunction with the Programs, you must ensure that your use does not: (i) create, or purport to create, obligations of us with respect to the Oracle Programs; or (ii) grant, or purport to grant, to any third party any rights to or immunities under our intellectual property or proprietary rights in the Oracle Programs. For example, you may not develop a software program using an Oracle Program and an Open Source program where such use results in a program file(s) that contains code from both the Oracle Program and the Open Source program (including without limitation libraries) if the Open Source program is licensed under a license that requires any "modifications" be made freely available. You also may not combine the Oracle Program with programs licensed under the GNU General Public License ("GPL") in any manner that could cause, or could be interpreted or asserted to cause, the Oracle Program or any modifications thereto to become subject to the terms of the GPL.

Entire Agreement

You agree that this Agreement is the complete agreement



for the Programs and licenses, and this Agreement supersedes all prior or contemporaneous Agreements or representations. If any term of this Agreement is found to be invalid or unenforceable, the remaining provisions will remain effective.

Last updated: 01/24/08

Should you have any questions concerning this License Agreement, or if you desire to contact Oracle for any reason, please write:

Oracle America, Inc.
500 Oracle Parkway,
Redwood City, CA 94065

Oracle may contact you to ask if you had a satisfactory experience installing and using this OTN software download.

P9. PCRE

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 8 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

The basic library functions are written in C and are freestanding. Also included in the distribution is a set of C++ wrapper functions, and a just-in-time compiler that can be used to optimize pattern matching. These are both optional features that can be omitted when the library is built.



THE BASIC LIBRARY FUNCTIONS

Written by: Philip Hazel

Email local part: ph10

Email domain: cam.ac.uk

University of Cambridge Computing Service,
Cambridge, England.

Copyright (c) 1997-2013 University of Cambridge
All rights reserved.

PCRE JUST-IN-TIME COMPILATION SUPPORT

Written by: Zoltan Herczeg

Email local part: hzmester

Email domain: freemail.hu

Copyright(c) 2010-2013 Zoltan Herczeg
All rights reserved.

STACK-LESS JUST-IN-TIME COMPILER

Written by: Zoltan Herczeg



```
Email local part: hzmester
Emain domain:      freemail.hu
```

```
Copyright(c) 2009-2013 Zoltan Herczeg
All rights reserved.
```

```
THE C++ WRAPPER FUNCTIONS
-----
```

```
Contributed by:   Google Inc.
```

```
Copyright (c) 2007-2012, Google Inc.
All rights reserved.
```

```
THE "BSD" LICENCE
-----
```

```
Redistribution and use in source and binary forms, with
or without modification, are permitted provided that the
following conditions are met:
```

```
* Redistributions of source code must retain the
above copyright notice, this list of conditions and the
following disclaimer.
```

```
* Redistributions in binary form must reproduce the
above copyright notice, this list of conditions and the
following disclaimer in the documentation and/or other
materials provided with the distribution.
```

```
* Neither the name of the University of Cambridge
nor the name of Google Inc. nor the names of their
```



contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

P10. Sha2 implementation

```
Copyright (c) 2001, Dr Brian Gladman  
<brg@gladman.me.uk>, Worcester, UK.
```

```
All rights reserved.
```

```
TERMS
```

```
Redistribution and use in source and binary forms,  
with or without modification, are permitted subject to  
the following conditions:
```

```
1. Redistributions of source code must retain the  
above copyright notice, this list of conditions and the  
following disclaimer.
```

```
2. Redistributions in binary form must reproduce the  
above copyright notice, this list of conditions and the
```



following disclaimer in the documentation and/or other materials provided with the distribution.

3. The copyright holder's name must not be used to endorse or promote any products derived from this software without his specific prior written permission.

This software is provided 'as is' with no express or implied warranties of correctness or fitness for purpose.

This is a byte oriented version of SHA256 that operates on arrays of bytes stored in memory. The operation uses a type 'sha256_ctx' to hold details of the current hash state and uses the following three calls:

```
void sha256_begin(sha256_ctx ctx[])
void sha256_hash(const unsigned char data[], unsigned
long len, sha256_ctx ctx[])
void sha256_end(unsigned char hval[], sha256_ctx ctx
[])
```

The first subroutine initialises a hash computation by setting up the context in the sha256_ctx context.

The second subroutine hashes 8-bit bytes from array data[] into the hash state withinh sha256_ctx context, the number of bytes to be hashed being given by the the unsigned long integer len.

The third subroutine completes the hash calculation and places the resulting digest value in the array of 8-bit bytes hval[]



This implementation of SHA256 also supports SHA384 and SHA512 but these hash functions depend on the use of 64-bit long integers and are not very efficient on 32-bit machines. This code is NOT recommended for these hash functions.

My thanks to Erik Andersen <andersen@codepoet-consulting.com> for testing this code on big-endian systems and for his assistance with corrections

P11. Wtl

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

- a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and
- b) in the case of each subsequent Contributor:
 - i) changes to the Program, and
 - ii) additions to the Program;



where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and



otherwise transfer the Contribution of such Contributor, if any, in source code and object code form.

This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and



b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.



4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.



5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to



software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent (s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.



This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

P12. Zlib

```
zlib.h -- interface of the 'zlib' general purpose
compression library
```

```
version 1.2.8, April 28th, 2013
```

```
Copyright (C) 1995-2013 Jean-loup Gailly and Mark
Adler
```

```
This software is provided 'as-is', without any express
or implied warranty. In no event will the authors be
held liable for any damages arising from the use of this
software.
```

```
Permission is granted to anyone to use this software for
any purpose, including commercial applications, and to
alter it and redistribute it freely, subject to the
following restrictions:
```

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any



source distribution.

Jean-loup Gailly

Mark Adler

jloup@gzip.org

madler@alumni.caltech.edu

P13. MIT License

Copyright (c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

P14. GNU General Public License

Version 3, 29 June 2007



Copyright © 2007 Free Software Foundation, Inc. <<http://fsf.org/>>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program,



whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying,



distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.



An interactive user interface displays “Appropriate Legal Notices” to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The “source code” for a work means the preferred form of the work for making modifications to it. “Object code” means any non-source form of a work.

A “Standard Interface” means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The “System Libraries” of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A “Major Component”, in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The “Corresponding Source” for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include



the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.



Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.



You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under



the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.



A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).



The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

“Additional permissions” are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material)



supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered “further restrictions” within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.



Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary



propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the



Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe



are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent



obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.



Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.



END OF TERMS AND CONDITIONS

P15. GNU Lesser General Public License

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <<http://fsf.org/>>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, “this License” refers to version 3 of the GNU Lesser General Public License, and the “GNU GPL” refers to version 3 of the GNU General Public License.

“The Library” refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An “Application” is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.



A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.



3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

- a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.
- b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

- a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.
- b) Accompany the Combined Work with a copy of the GNU GPL and this license document.
- c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.
- d) Do one of the following:
 - 0) Convey the Minimal Corresponding Source under



the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4dl, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.



6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

P16. Mozilla Public License

Version 2.0

1. Definitions

1.1. “Contributor”

means each individual or legal entity that creates,



contributes to the creation of, or owns Covered Software.

1.2. "Contributor Version"

means the combination of the Contributions of others (if any) used by a Contributor and that particular Contributor's Contribution.

1.3. "Contribution"

means Covered Software of a particular Contributor.

1.4. "Covered Software"

means Source Code Form to which the initial Contributor has attached the notice in Exhibit A, the Executable Form of such Source Code Form, and Modifications of such Source Code Form, in each case including portions thereof.

1.5. "Incompatible With Secondary Licenses"

means

that the initial Contributor has attached the notice described in Exhibit B to the Covered Software; or

that the Covered Software was made available under the terms of version 1.1 or earlier of the License, but not also under the terms of a Secondary License.

1.6. "Executable Form"

means any form of the work other than Source Code Form.

1.7. "Larger Work"



means a work that combines Covered Software with other material, in a separate file or files, that is not Covered Software.

1.8. "License"

means this document.

1.9. "Licensable"

means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently, any and all of the rights conveyed by this License.

1.10. "Modifications"

means any of the following:

any file in Source Code Form that results from an addition to, deletion from, or modification of the contents of Covered Software; or

any new file in Source Code Form that contains any Covered Software.

1.11. "Patent Claims" of a Contributor

means any patent claim(s), including without limitation, method, process, and apparatus claims, in any patent Licensable by such Contributor that would be infringed, but for the grant of the License, by the making, using, selling, offering for sale, having made, import, or transfer of either its Contributions or its Contributor Version.

1.12. "Secondary License"



means either the GNU General Public License, Version 2.0, the GNU Lesser General Public License, Version 2.1, the GNU Affero General Public License, Version 3.0, or any later versions of those licenses.

1.13. "Source Code Form"

means the form of the work preferred for making modifications.

1.14. "You" (or "Your")

means an individual or a legal entity exercising rights under this License. For legal entities, "You" includes any entity that controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. License Grants and Conditions

2.1. Grants

Each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license:

under intellectual property rights (other than patent or trademark) Licensable by such Contributor to use, reproduce, make available, modify, display, perform, distribute, and otherwise exploit its Contributions, either on an unmodified basis, with Modifications, or as part of a Larger Work; and

under Patent Claims of such Contributor to make, use, sell, offer for sale, have made, import, and otherwise transfer either its Contributions or its Contributor Version.



2.2. Effective Date

The licenses granted in Section 2.1 with respect to any Contribution become effective for each Contribution on the date the Contributor first distributes such Contribution.

2.3. Limitations on Grant Scope

The licenses granted in this Section 2 are the only rights granted under this License. No additional rights or licenses will be implied from the distribution or licensing of Covered Software under this License. Notwithstanding Section 2.1(b) above, no patent license is granted by a Contributor:

for any code that a Contributor has removed from Covered Software; or

for infringements caused by: (i) Your and any other third party's modifications of Covered Software, or (ii) the combination of its Contributions with other software (except as part of its Contributor Version); or

under Patent Claims infringed by Covered Software in the absence of its Contributions.

This License does not grant any rights in the trademarks, service marks, or logos of any Contributor (except as may be necessary to comply with the notice requirements in Section 3.4).

2.4. Subsequent Licenses

No Contributor makes additional grants as a result of Your choice to distribute the Covered Software under a subsequent version of this License (see Section 10.2) or under the terms of a Secondary License (if permitted



under the terms of Section 3.3).

2.5. Representation

Each Contributor represents that the Contributor believes its Contributions are its original creation(s) or it has sufficient rights to grant the rights to its Contributions conveyed by this License.

2.6. Fair Use

This License is not intended to limit any rights You have under applicable copyright doctrines of fair use, fair dealing, or other equivalents.

2.7. Conditions

Sections 3.1, 3.2, 3.3, and 3.4 are conditions of the licenses granted in Section 2.1.

3. Responsibilities

3.1. Distribution of Source Form

All distribution of Covered Software in Source Code Form, including any Modifications that You create or to which You contribute, must be under the terms of this License. You must inform recipients that the Source Code Form of the Covered Software is governed by the terms of this License, and how they can obtain a copy of this License. You may not attempt to alter or restrict the recipients' rights in the Source Code Form.

3.2. Distribution of Executable Form

If You distribute Covered Software in Executable Form then:

such Covered Software must also be made available in Source Code Form, as described in Section 3.1, and You must inform recipients of the Executable Form how they can obtain a copy of such Source Code Form by reasonable



means in a timely manner, at a charge no more than the cost of distribution to the recipient; and

You may distribute such Executable Form under the terms of this License, or sublicense it under different terms, provided that the license for the Executable Form does not attempt to limit or alter the recipients' rights in the Source Code Form under this License.

3.3. Distribution of a Larger Work

You may create and distribute a Larger Work under terms of Your choice, provided that You also comply with the requirements of this License for the Covered Software. If the Larger Work is a combination of Covered Software with a work governed by one or more Secondary Licenses, and the Covered Software is not Incompatible With Secondary Licenses, this License permits You to additionally distribute such Covered Software under the terms of such Secondary License(s), so that the recipient of the Larger Work may, at their option, further distribute the Covered Software under the terms of either this License or such Secondary License(s).

3.4. Notices

You may not remove or alter the substance of any license notices (including copyright notices, patent notices, disclaimers of warranty, or limitations of liability) contained within the Source Code Form of the Covered Software, except that You may alter any license notices to the extent required to remedy known factual inaccuracies.

3.5. Application of Additional Terms

You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Software. However, You may do so only on Your own behalf, and not on behalf of any Contributor. You must make it absolutely clear that any such warranty, support, indemnity, or liability obligation is offered by You alone, and You hereby agree



to indemnify every Contributor for any liability incurred by such Contributor as a result of warranty, support, indemnity or liability terms You offer. You may include additional disclaimers of warranty and limitations of liability specific to any jurisdiction.

4. Inability to Comply Due to Statute or Regulation

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Software due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be placed in a text file included with all distributions of the Covered Software under this License. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Termination

5.1. The rights granted under this License will terminate automatically if You fail to comply with any of its terms. However, if You become compliant, then the rights granted under this License from a particular Contributor are reinstated (a) provisionally, unless and until such Contributor explicitly and finally terminates Your grants, and (b) on an ongoing basis, if such Contributor fails to notify You of the non-compliance by some reasonable means prior to 60 days after You have come back into compliance. Moreover, Your grants from a particular Contributor are reinstated on an ongoing basis if such Contributor notifies You of the non-compliance by some reasonable means, this is the first time You have received notice of non-compliance with this License from such Contributor, and You become compliant prior to 30 days after Your receipt of the notice.

5.2. If You initiate litigation against any entity by asserting a patent infringement claim (excluding declaratory judgment actions, counter-claims, and cross-claims) alleging that a Contributor Version directly or indirectly infringes any patent, then the rights granted



to You by any and all Contributors for the Covered Software under Section 2.1 of this License shall terminate.

5.3. In the event of termination under Sections 5.1 or 5.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or Your distributors under this License prior to termination shall survive termination.

6. Disclaimer of Warranty

Covered Software is provided under this License on an "as is" basis, without warranty of any kind, either expressed, implied, or statutory, including, without limitation, warranties that the Covered Software is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the Covered Software is with You. Should any Covered Software prove defective in any respect, You (not any Contributor) assume the cost of any necessary servicing, repair, or correction. This disclaimer of warranty constitutes an essential part of this License. No use of any Covered Software is authorized under this License except under this disclaimer.

7. Limitation of Liability

Under no circumstances and under no legal theory, whether tort (including negligence), contract, or otherwise, shall any Contributor, or anyone who distributes Covered Software as permitted above, be liable to You for any direct, indirect, special, incidental, or consequential damages of any character including, without limitation, damages for lost profits, loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses, even if such party shall have been informed of the possibility of such damages. This limitation of liability shall not apply to liability for death or personal injury resulting from such party's negligence to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not apply to You.

8. Litigation



Any litigation relating to this License may be brought only in the courts of a jurisdiction where the defendant maintains its principal place of business and such litigation shall be governed by laws of that jurisdiction, without reference to its conflict-of-law provisions. Nothing in this Section shall prevent a party's ability to bring cross-claims or counter-claims.

9. Miscellaneous

This License represents the complete agreement concerning the subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not be used to construe this License against a Contributor.

10. Versions of the License

10.1. New Versions

Mozilla Foundation is the license steward. Except as provided in Section 10.3, no one other than the license steward has the right to modify or publish new versions of this License. Each version will be given a distinguishing version number.

10.2. Effect of New Versions

You may distribute the Covered Software under the terms of the version of the License under which You originally received the Covered Software, or under the terms of any subsequent version published by the license steward.

10.3. Modified Versions

If you create software not governed by this License, and you want to create a new license for such software, you may create and use a modified version of this License if you rename the license and remove any references to the name of the license steward (except to note that such



modified license differs from this License).

10.4. Distributing Source Code Form that is Incompatible With Secondary Licenses

If You choose to distribute Source Code Form that is Incompatible With Secondary Licenses under the terms of this version of the License, the notice described in Exhibit B of this License must be attached.

Exhibit A - Source Code Form License Notice

This Source Code Form is subject to the terms of the Mozilla Public License, v. 2.0. If a copy of the MPL was not distributed with this file, You can obtain one at <http://mozilla.org/MPL/2.0/>.

If it is not possible or desirable to put the notice in a particular file, then You may include the notice in a location (such as a LICENSE file in a relevant directory) where a recipient would be likely to look for such a notice.

You may add additional accurate notices of copyright ownership.

Exhibit B - "Incompatible With Secondary Licenses" Notice

This Source Code Form is "Incompatible With Secondary Licenses", as defined by the Mozilla Public License, v. 2.0.



Questions fréquentes

Déplacement du Serveur Dr.Web Enterprise Server vers un autre ordinateur (sous Windows®)

Marche à suivre pour déplacer le Serveur Dr.Web Enterprise Server (en cas d'installation d'une version équivalente de Dr.Web Enterprise Server) sous Windows :

1. Arrêtez le service **Dr.Web Enterprise Server** (voir [Démarriage et arrêt du Dr.Web Enterprise Server](#)).
2. Depuis la ligne de commande lancez le fichier `drwcsd.exe` accompagné de la clé `exportdb` afin d'exporter le contenu de la base de données vers le fichier. La ligne de commande complète relative à l'exportation sous Windows est la suivante :

```
"C:\Program Files\DrWeb Enterprise Server\bin\drwcsd.exe" exportdb <chemin_vers_le_fichier>
```

3. Sauvegardez le contenu du répertoire `C:\Program Files\DrWeb Enterprise Server\etc`, ainsi que la clé `drwcsd.pub` depuis `C:\Program Files\DrWeb Enterprise Server\Installer`.
4. Supprimez le **Serveur**.
5. Installez un nouveau **Serveur** (vide et avec une nouvelle base) sur un ordinateur choisi. Arrêtez le service **Dr.Web Enterprise Server** avec les outils de gestion des services de Windows ou depuis le **Centre de Gestion**.
6. Copiez le contenu du répertoire `etc` sauvegardé précédemment vers le répertoire `C:\Program Files\DrWeb Enterprise Server\etc` ainsi que la clé `drwcsd.pub` - vers `C:\Program Files\DrWeb Enterprise Server\Installer`.
7. Depuis la ligne de commande lancez le fichier `drwcsd.exe`



accompagné de la clé `importdb` pour l'importation du contenu de la base de données depuis le fichier. La ligne de commande complète relative à la version sous Windows est la suivante :

```
"C:\Program Files\DrWeb Enterprise Server\bin\drwcsd.exe" importdb <chemin_vers_le_fichier>
```

8. Lancez le service **Dr.Web Enterprise Server** (voir [Démarrage et arrêt du Dr.Web Enterprise Server](#)).



En cas d'utilisation de la base de données interne, il est possible de ne pas effectuer les procédures d'exportation/importation de la BD, il suffit de sauvegarder le fichier de la base interne `dbinternal.dbs` et de remplacer ensuite le nouveau fichier de la BD sur le **Serveur** installé par le fichier sauvegardé précédemment depuis le **Serveur** antérieur.

Marche à suivre pour déplacer le Serveur Dr.Web Enterprise Server (en cas d'installation d'une autre version de Dr.Web Enterprise Server) sous OS Windows :

1. Arrêtez le service de **Dr.Web Enterprise Server** (voir [Démarrage et arrêt du Dr.Web Enterprise Server](#)).
2. Sauvegardez la base de données avec les outils du Serveur SQL (en cas d'utilisation de la BD interne, sauvegardez tout simplement le fichier `dbinternal.dbs`).
3. Sauvegardez le contenu du répertoire `C:\Program Files\DrWeb Enterprise Server\etc` et la clé `drwcsd.pub` se trouvant dans `C:\Program Files\DrWeb Enterprise Server\Installer`.
4. Supprimez le **Serveur**.
5. Installez un nouveau **Serveur** (vide et avec une nouvelle base) sur un ordinateur choisi. Arrêtez le service **Dr.Web Enterprise Server** avec les outils de gestion des services de Windows ou depuis le **Centre de Gestion**.
6. Copiez le contenu du répertoire `etc` sauvegardé précédemment vers le répertoire `C:\Program Files`



\DrWeb Enterprise Server\etc, copiez la clé drwcsd.pub vers C:\Program Files\DrWeb Enterprise Server\Installer.

7. Restaurez la base de données sur le nouveau **Serveur**, dans le fichier de configuration drwcsd.conf, spécifiez le chemin vers la base de données.
8. Depuis la ligne de commande lancez le fichier drwcsd.exe accompagné de la clé upgradedb pour mettre à jour la base de données. La ligne de commande complète relative à l'importation en cas de version sous Windows est la suivante :

```
"C:\Program Files\DrWeb Enterprise Server\bin\drwcsd.exe" upgradedb "C:\Program Files\DrWeb Enterprise Server\update-db"
```

9. Lancez le service **Dr.Web Enterprise Server** (voir [Démarage et arrêt du Dr.Web Enterprise Server](#)).

En cas de changement d'adresse IP lors du déplacement du serveur :

1. Réalisez un déplacement du **Serveur** conformément à la procédure décrite ci-dessus.
2. Dans la configuration de tous les **Agents** connectés au **Serveur** déplacé, spécifiez l'adresse du nouveau **Serveur** (voir [Connexion de Dr.Web Enterprise Agent à un autre serveur Dr.Web Enterprise Server](#)).
3. Pour connecter les **Agents** pour lesquels l'adresse du nouveau **Serveur** a été spécifiée via le **Centre de Gestion** et non pas dans la configuration de l'**Agent** sur le poste, laissez les deux Serveurs tourner (sur les deux serveurs, dans la configuration de l'**Agent**, l'adresse du nouveau **Serveur** doit être spécifiée) jusqu'au moment où tous les **Agents** se connectent à l'ancien **Serveur** afin d'obtenir la nouvelle adresse IP et passent après vers le nouveau **Serveur**.



Connexion de Dr.Web Enterprise Agent à un autre serveur Dr.Web Enterprise Server



Pour connecter l'**Agent** à un autre **Serveur**, toutes les opérations doivent être réalisées en mode administrateur.

Marche à suivre pour reconnecter Dr.Web Enterprise Agent à un autre serveur Dr.Web Enterprise Server :

1. Si la clé publique de chiffrement `drwcsd.pub` du nouveau **Serveur** ne correspond pas à la clé de chiffrement du **Serveur** antérieur, il faut remplacer la clé sur l'**Agent** :
 - 1.1. Si l'option d'autoprotection est activée sur l'ordinateur sur lequel est installé l'**Agent**, il est nécessaire de désactiver le composant **SelfPROtect** via les paramètres de l'**Agent** (les droits d'administrateur du poste sont requis ainsi que les droits permettant de désactiver l'autoprotection qui sont spécifiés sur le **Serveur**).
 - 1.2. Copiez la clé publique de chiffrement `drwcsd.pub` depuis le nouveau **Serveur** vers le répertoire d'installation de l'**Agent**.
2. Modifiez l'adresse du **Serveur** dans la configuration de l'**Agent** :
 - ◆ Dans le **Centre de Gestion** (du **Serveur** antérieur): **Réseau antivirus** → **Dr.Web Enterprise Agent pour Windows** → onglet **Réseau** → champ **Serveur**.
 - ◆ Directement sur le poste : depuis le menu contextuel de l'**Agent**, sélectionnez l'élément **Configuration** → **Connexion** → champ **Serveur**.
3. Basculer le poste vers le statut novice (remettre à zéro les paramètres de connexion au **Serveur**) :



- ◆ Dans le **Centre de Gestion** (sur le nouveau **Serveur**) : **Administration** → **Configuration de Dr.Web Enterprise Server** → onglet **Général** → cochez la case **Spécifier les non approuvés comme novices**.
 - ◆ Directement sur le poste : depuis le menu contextuel de l'**Agent**, sélectionnez l'élément **Configuration** → **Connexion** → bouton **Novice**.
4. Redémarrez le service de l'**Agent** (voir le paragraphe [Dr.Web Enterprise Agent](#)).

Dans le cas où le poste ne dispose pas des droits nécessaires pour modifier la configuration de Dr.Web Enterprise Agent, utilisez la procédure suivante :

1. Si la clé publique de chiffrement `drwcsd.pub` du nouveau **Serveur** ne correspond pas à la clé de chiffrement du **Serveur** antérieur, il est nécessaire de remplacer cette clé sur l'**Agent** :
 - 1.1. Si l'option d'autoprotection est activée sur l'ordinateur sur lequel est installé l'**Agent**, il est nécessaire de désactiver le composant **SelfPROtect** via les paramètres de l'**Agent** (les droits d'administrateur du poste sont requis ainsi que les droits permettant de désactiver l'autoprotection qui sont spécifiés sur le **Serveur**).
 - 1.2. Copiez la clé publique de chiffrement `drwcsd.pub` depuis le nouveau **Serveur** vers le répertoire d'installation de l'**Agent**.
2. Configurez les paramètres de l'**Agent** avec la commande suivante :

```
drwagntd -save <new_server_ip>
```

avec `<new_server_ip>` - adresse du nouveau **Serveur** auquel l'**Agent** doit se connecter. L'adresse doit avoir le format d'[adresses réseau](#).

3. Redémarrez le service de l'**Agent** (voir le paragraphe [Dr.Web Enterprise Agent](#)).



Changement du type de SGBD Dr.Web Enterprise Security Suite

Sous Windows

1. Arrêtez le service **Dr.Web Enterprise Server** (voir [Démarriage et arrêt du Dr.Web Enterprise Server](#)).
2. Lancez le fichier `drwcsd.exe` accompagné de la clé `exportdb` pour exporter le contenu de la base de données vers le fichier. La ligne de commande complète pour l'exportation sous Windows est la suivante :

```
"C:\Program Files\DrWeb Enterprise Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Enterprise Server" -var-root="C:\Program Files\DrWeb Enterprise Server\var" -verbosity=all exportdb D:\esbase.es
```

Ceci sous-entend que **Dr.Web Enterprise Server** est installé dans le répertoire `C:\Program Files\DrWeb Enterprise Server` et que la base sera exportée vers le fichier `esbase.es` se trouvant dans la racine du disque D. Copiez cette ligne (c'est une ligne seulement) via le presse-papiers vers le fichier `cmd` et exécutez-le.

Si le chemin vers le fichier comporte des espaces et/ou des caractères nationaux (ou le nom du fichier inclut des espaces et/ou des caractères nationaux), il est nécessaire de délimiter le chemin avec les guillemets : `"D:\nom_long\esbase.es"`.

3. Lancez le service **Dr.Web Enterprise Server** (voir [Démarriage et arrêt du Dr.Web Enterprise Server](#)), connectez le **Centre de Gestion** et reconfigurez ensuite le **Serveur** de sorte qu'il utilise un autre SGBD. Refusez le redémarrage du **Serveur**.
4. Arrêtez le service **Dr.Web Enterprise Server** (voir [Démarriage et arrêt du Dr.Web Enterprise Server](#)).
5. Lancez le fichier `drwcsd.exe` accompagné de la clé `initdb`



pour initialiser la nouvelle base de données. La ligne de commande relative à l'initialisation de la base de données correspondante à la version du **Serveur** pour Windows est la suivante :

```
"C:\Program Files\DrWeb Enterprise Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Enterprise Server" -var-root="C:\Program Files\DrWeb Enterprise Server\var" -verbosity=all initdb D:\Keys\agent.key - - <mot de passe>
```

Ceci sous-entend que le **Serveur** est installé dans le répertoire "C:\Program Files\DrWeb Enterprise Server", la clé Agent `agent.key` se trouve dans le répertoire D:\Keys. Copiez cette ligne (une seule ligne) via le presse-papier vers le fichier `cmd` puis exécutez-le.

Si le chemin vers le fichier comporte des espaces et/ou des caractères nationaux (ou le nom du fichier inclut des espaces et/ou des caractères nationaux), il est nécessaire de délimiter le chemin vers la clé par des guillemets : "D:\nom_long\agent.key".

6. Lancez le fichier `drwcsd.exe` accompagné de la clé `importdb` pour importer le contenu de la base de données depuis le fichier. La ligne de commande complète relative à l'importation en cas de version sous Windows est la suivante :

```
"C:\Program Files\DrWeb Enterprise Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Enterprise Server" -var-root="C:\Program Files\DrWeb Enterprise Server\var" -verbosity=all importdb D:\esbase.es"
```

Copiez cette ligne (une seule ligne) via le presse-papier vers le fichier `cmd` puis exécutez-le.

7. Lancez le service **Dr.Web Enterprise Server** (voir [Démarrage et arrêt du Dr.Web Enterprise Server](#)).



Sous UNIX

1. Arrêtez le service de **Dr.Web Enterprise Server** avec le script :

- ◆ sous **Linux** et **Solaris** : `/etc/init.d/drwcsd stop`
- ◆ sous **FreeBSD** : `/usr/local/etc/rc.d/drwcsd.sh stop`

ou depuis le **Centre de Gestion** (sauf Solaris).

2. Démarrez le **Serveur** avec la clé `exportdb` pour exporter le contenu de la base vers le fichier. La ligne de commande depuis le répertoire d'installation du **Serveur** est la suivante :

- ◆ sous **Linux** : `"/etc/init.d/drwcsd exportdb /var/opt/drwcs/esbase.es"`
- ◆ sous **Solaris** : `"/etc/init.d/drwcsd exportdb /var/drwcs/etc/esbase.es"`
- ◆ sous **FreeBSD** : `"/usr/local/etc/rc.d/drwcsd.sh exportdb /var/drwcs/esbase.es"`

Ceci sous-entend que l'exportation de la base se fait vers le fichier `esbase.es` se trouvant dans le répertoire d'utilisateur.

3. Démarrez le service de **Dr.Web Enterprise Server** avec le script :

- ◆ sous **Linux** et **Solaris** : `/etc/init.d/drwcsd start`
- ◆ sous **FreeBSD** : `/usr/local/etc/rc.d/drwcsd.sh start`

connectez le **Centre de Gestion** et reconfigurez le **Serveur** de sorte qu'il utilise un autre SGBD : dans le menu **Administration** → l'élément **Configuration de Dr.Web Enterprise Server** → l'onglet **Base de données**.



Vous pouvez également reconfigurer le **Serveur** pour utiliser un autre SGBD en éditant directement le fichier de configuration du **Serveur** `drwcsd.conf`. Pour cela, mettez en commentaire/supprimer l'entrée sur la BD courante et écrivez une nouvelle BD (pour en savoir plus, consultez l'[Annexe G1. Fichier de configuration de Dr.Web Enterprise Server](#)).

Refusez le redémarrage du **Serveur**.

4. Arrêtez **Dr.Web Enterprise Server** (voir étape 1).
5. Lancez le fichier `drwcsd` accompagné de la clé `initdb` pour initialiser une nouvelle base de données. La ligne d'initialisation est la suivante :
 - ◆ sous **Linux** et **Solaris** : `/etc/init.d/drwcsd initdb`
 - ◆ sous **FreeBSD** : `/usr/local/etc/rc.d/drwcsd.sh initdb`
6. Lancez le fichier `drwcsd` accompagné de la clé `importdb` pour importer le contenu de la base de données depuis le fichier. La ligne de commande relative à l'importation est la suivante :
 - ◆ sous **Linux** : `"/etc/init.d/drwcsd importdb /var/opt/drwcs/esbase.es"`
 - ◆ sous **Solaris** : `"/etc/init.d/drwcsd importdb /var/drwcs/etc/esbase.es"`
 - ◆ sous **FreeBSD** : `"/usr/local/etc/rc.d/drwcsd.sh importdb /var/drwcs/esbase.es"`
7. Démarrez **Dr.Web Enterprise Server** (voir étape 3).



Si vous avez besoin de spécifier des paramètres lors du lancement du script de **Serveur** (par exemple pour spécifier le répertoire d'installation du **Serveur**, pour modifier le niveau de détail du journal etc.), vous pouvez modifier les valeurs correspondantes dans le script de lancement :



- ◆ sous **FreeBSD**: /usr/local/etc/rc.d/drwcd.sh
 - ◆ sous **Linux** et **Solaris**: /etc/init.d/drwcd
-



Restauration de la BD Dr.Web Enterprise Security Suite

Durant son fonctionnement, **Serveur Enterprise** réalise de manière régulière une procédure de sauvegarde des informations importantes (contenu de la base de données, fichier clé de licence du **Serveur**, clé privée de chiffrement, fichier de configuration du **Serveur** et fichier de configuration du **Centre de Gestion**). Les copies de sauvegarde sont conservées dans les dossiers suivants du répertoire de **Serveur** :

- ◆ pour OS **Windows**: `\var\Backup`
- ◆ pour OS **Linux**: `/var/opt/drwcs/backup`
- ◆ pour OS **FreeBSD** et **Solaris**: `/var/drwcs/backup`

Pour cela, la planification du **Serveur** contient une tâche journalière réalisant cette fonction. Si la tâche n'est pas paramétrée, il est recommandé de la créer.

Les copies de sauvegarde sont enregistrées au format `.dz` compatible avec `gzip` ainsi qu'avec d'autres outils d'archivage. Après l'extraction, tous les fichiers excepté le contenu de la BD sont prêts à être utilisés. Le contenu de la BD se trouvant dans la copie de sauvegarde peut être importé vers la BD opérationnelle du **Serveur** avec la clé `importdb` pour récupérer ainsi les données.

Restauration de la BD sous diverses versions Dr.Web Enterprise Server

La BD ne peut être restaurée que depuis la copie de sauvegarde créée avec le **Serveur** dans la même version que celle du **Serveur** sur lequel la restauration est effectuée.

Par exemple :

- ◆ La BD restaurée depuis la copie de sauvegarde créée avec le **Serveur** en version **5.0** ne peut être restaurée qu'avec le **Serveur** en version **5.0**.



- ◆ La BD restaurée depuis la copie de sauvegarde créée avec le **Serveur** en version **6.0** ne peut être restaurée qu'avec le **Serveur** en version **6.0**.
- ◆ La BD restaurée depuis la copie de sauvegarde créée avec le **Serveur** en version **5.0** ou **4.XX** ne peut être restaurée avec le **Serveur** en version **6.0**.

Si lors de la mise à niveau du Serveur vers la version 6.0 depuis des versions antérieures, la BD a été corrompue, procédez comme suit :

1. Supprimez le **Serveur** en version **6.0**. Les copies de sauvegarde des **fichiers** utilisés par le **Serveur** seront sauvegardées de manière automatique.
2. Installez le **Serveur** en même version que la version d'avant la mise à jour et avec laquelle la copie de sauvegarde a été créée.

Selon la procédure de mise à jour standard, il faut utiliser tous les fichiers sauvegardés du **Serveur** excepté le fichier de BD.

Pendant l'installation du **Serveur** créez une nouvelle BD.

3. Restaurez la BD depuis la copie de sauvegarde conformément à la règle générale (voir [ci-dessous](#)).
4. Dans la configuration du **Serveur**, désactivez les protocoles de l'**Agent**, du **Serveur** et de l'**Installeur réseau**. Pour cela, sélectionnez l'élément **Administration** du menu principal du **Centre de Gestion**, puis dans la fenêtre qui apparaît, sélectionnez **Configuration de Dr.Web Enterprise Server**, passez ensuite à l'onglet **Modules** et décochez les cases respectives.
5. Mettez le **Serveur** à jour vers la version **6.0** selon la règle générale (voir [Mise à jour de Dr.Web Enterprise Security Suite et des ses composants](#)).
6. Activez les protocoles de l'**Agent**, du **Serveur** et de l'**Installeur réseau** qui ont été désactivés lors de l'étape 4.



Sous Windows

Marche à suivre pour restaurer la BD depuis une copie de sauvegarde :

1. Arrêtez le service de **Serveur Enterprise** (s'il a été lancé, voir [Démarrage et arrêt du Dr.Web Enterprise Server](#)).
2. Importez le contenu de la BD depuis le fichier correspondant de la copie de sauvegarde. Voici un exemple de la ligne d'importation :

```
"C:\Program Files\DrWeb Enterprise Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Enterprise Server" -var-root="C:\Program Files\DrWeb Enterprise Server\var" -verbosity=all importdb "<disque>:\<chemin_vers_le_fichier_de_backup>\database.dz".
```

Cette commande doit être mise dans une seule ligne. Cet exemple sous-entend que le **Serveur** est installé dans le répertoire C:\Program Files\DrWeb Enterprise Server.

3. Lancez le service **Dr.Web Enterprise Server** (voir [Démarrage et arrêt du Dr.Web Enterprise Server](#)).

Marche à suivre pour restaurer la BD depuis sa copie de sauvegarde lors du changement de version du Serveur Dr.Web Enterprise Server ou en cas d'endommagement de la version courante de la BD :

1. Arrêtez le service de **Serveur Enterprise** (s'il a été lancé, voir [Démarrage et arrêt du Dr.Web Enterprise Server](#)).
2. Supprimez le contenu de la BD courante. Pour cela :
 - 2.1. En cas d'utilisation de la BD interne :
 - a) Supprimez le fichier de la base de données dbinternal.dbs.



- b) Réalisez une initialisation d'une nouvelle base de données. La ligne d'initialisation de la base de données relative à la version du **Serveur** opérant sous Windows est la suivante :

```
"C:\Program Files\DrWeb Enterprise Server
\bin\drwcsd.exe" -home="C:\Program Files
\DrWeb Enterprise Server" -var-
root="C:\Program Files\DrWeb Enterprise
Server\var" -verbosity=all initdb D:\Keys
\agent.key - - <mot de passe>
```

Cette commande doit être indiquée en une seule ligne (voir aussi le format de la commande `drwcsd` accompagnée de la clé `initdb` dans l'[Annexe. H5.3](#)). L'exemple sous-entend que le **Serveur** est installé dans le répertoire `C:\Program Files\DrWeb Enterprise Server`, la clé `Agent agent.key` se trouve dans le répertoire `D:\Keys`.

- c) Après l'exécution de la commande, dans le dossier `var` du répertoire d'installation de **Serveur Enterprise**, un nouveau fichier de la base de donnée `dbinternal.dbs` dont la taille est de 200 Ko apparaîtra.

2.2. En cas d'utilisation d'une BD externe : réalisez un nettoyage de la BD avec le script `clean.sql` se trouvant dans le dossier `etc` du répertoire d'installation du **Serveur**.

3. Importez le contenu de la base de données depuis le fichier respectif de la copie de sauvegarde. la ligne d'importation est la suivante :

```
"C:\Program Files\DrWeb Enterprise Server\bin
\drwcsd.exe" -home="C:\Program Files\DrWeb
Enterprise Server" -var-root="C:\Program
Files\DrWeb Enterprise Server\var" -
verbosity=all importdb
"<disque>:\<chemin_vers_le_fichier_de_backup>
\database.dz".
```

Cette commande doit également être indiquée en une seule ligne. L'exemple sous-entend que le **Serveur** est installé dans le répertoire `C:\Program Files\DrWeb Enterprise`



Server.

4. Lancez le service **Serveur Enterprise** (voir [Démarrage et arrêt du Dr.Web Enterprise Server](#)).

Sous UNIX

1. Arrêtez **Serveur Enterprise** (s'il a été lancé) :

- ◆ sous **Linux** et **Solaris**:

```
/etc/init.d/drwcsd stop
```

- ◆ sous **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd.sh stop
```

- ◆ pour les **autres** versions supportées :

```
/bin/drwcs.sh stop
```

2. Supprimez le fichier de la base de données `dbinternal.dbs` depuis le dossier ci-dessous du répertoire d'installation de **Serveur Enterprise** :

- ◆ sous **Linux** :

```
/var/opt/drwcs/
```

- ◆ sous **FreeBSD** et **Solaris** :

```
/var/drwcs/
```



Lorsque vous utilisez une BD externe, son nettoyage se fait avec le script `clean.sql` se trouvant dans le dossier :

- ◆ `/var/opt/drwcs/etc` pour OS Linux,

- ◆ `/var/drwcs/etc` pour OS Solaris et OS FreeBSD.

3. Réalisez une initialisation de la base de données du **Serveur**. Pour cela, utilisez la commande suivante :

- ◆ sous **Linux** et **Solaris** :

```
/etc/init.d/drwcsd initdb
```

- ◆ sous **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd.sh initdb
```

- ◆ pour les **autres** versions supportées :



```
su drwcs -c "bin/drwcsd -var-root=./var
-verbosity=all -log=./var/server.log
initdb etc/agent.key - - <mot de passe>"
```

4. Après l'exécution de la commande, un nouveau fichier de la base de données `binternal.dbs` dont la taille est d'environ 200 Ko apparaîtra dans le dossier `var` du répertoire d'installation de **Serveur Enterprise**.

5. Importez le contenu de la base depuis le fichier respectif de la copie de sauvegarde. La ligne d'importation est la suivante :

- ◆ sous **Linux** et **Solaris** :

```
/etc/init.d/drwcsd importdb "/
<chemin_vers_le_fichier_de_backup>/database.dz"
```

- ◆ sous **FreeBSD** :

```
/usr/local/etc/rc.d/drwcsd.sh importdb
"/<chemin_vers_le_fichier_de_backup>/
database.dz"
```

- ◆ pour les **autres** versions supportées :

```
bin/drwcsd -var-root=./var -
verbosity=all -log=logfile.log importdb
"/<chemin_vers_le_fichier_de_backup>/
database.dz"
```

6. Démarrez **Serveur Enterprise**.

- ◆ sous **Linux** et **Solaris** :

```
/etc/init.d/drwcsd start
```

- ◆ sous **FreeBSD** :

```
/usr/local/etc/rc.d/drwcsd.sh start
```

- ◆ pour les **autres** versions supportées :

```
/bin/drwcs.sh start
```



Si vous avez besoin de spécifier des paramètres lors du lancement du script de **Serveur** (par exemple pour spécifier le répertoire d'installation du **Serveur**, pour modifier le niveau de détail du journal etc.), vous pouvez modifier les valeurs correspondantes dans le script de lancement :

- ◆ sous **FreeBSD** : `/usr/local/etc/rc.d/drwcsd.sh`

- ◆ sous **Linux** et **Solaris** : `/etc/init.d/drwcsd`



Si certains **Agents** ont été installés après la création de la dernière copie de sauvegarde et ne sont pas présents dans la BD après la restauration, il est recommandé d'activer l'option **Spécifier les non autorisés comme novices**. Pour cela, dans le **Centre de Gestion**, depuis le menu **Administration**, sélectionnez l'élément **Configuration de Dr.Web Enterprise Server**. Dans l'onglet **Général**, cochez la case correspondante.

Après la restauration de la base, il est recommandé de se connecter au **Serveur** depuis le **Centre de Gestion**, puis dans le menu **Administration** sélectionnez l'élément **Planification de Dr.Web Enterprise Server** et vérifiez la présence de la tâche **Backup de données critiques du Serveur**. Si la tâche est absente, il est recommandé de la créer.



Restauration de Dr.Web Enterprise Server depuis une copie de sauvegarde

Dr.Web Enterprise Security Suite réalise de manière régulière des copies de sauvegarde des informations importantes du **Serveur** : fichier clé de licence du **Serveur**, contenu de la base de données, clé de chiffrement, configuration du **Serveur** et du **Centre de Gestion**. Les copies de sauvegarde sont conservées dans les dossiers suivants du répertoire de **Serveur** :

- ◆ sous **Windows** : `\var\Backup`
- ◆ sous **Linux** : `/var/opt/drwcs/backup`
- ◆ sous **FreeBSD** et **Solaris**: `/var/drwcs/backup`

Pour assurer cette fonction, la planification du **Serveur** contient une tâche journalière correspondante. Si la tâche n'est pas configurée, il est recommandé de la créer.

Les copies de sauvegarde sont enregistrées au format `.dz` compatible avec `gzip` ainsi qu'avec d'autres outils d'archivage. Après l'extraction, tous les fichiers sauf le contenu de la BD sont prêts à être utilisés. Le contenu de la BD se trouvant dans la copie de sauvegarde peut être importé vers une autre BD du **Serveur** avec la clé `importdb` afin de restaurer les données (voir le paragraphe [Restauration de la BD de Dr.Web Enterprise Security Suite](#)).

Il est également recommandé de sauvegarder sur un autre ordinateur les copies des fichiers suivants : fichiers clé de chiffrement `drwcsd.pri` et `drwcsd.pub`, fichiers clé de licence `enterprise.key` et `agent.key`, fichier de certificat SSL `certificate.pem`, clé privée RSA `private-key.pem` ainsi que les copies de sauvegarde du contenu de la base de données du **Serveur** `database.dz`, fichier de configuration du **Serveur** `drwcsd.conf` et fichier de configuration du **Centre de Gestion** `webmin.conf`. Vous pourrez ainsi éviter le risque de perdre des données en cas d'endommagement de l'ordinateur sur lequel est installé **Serveur Enterprise**, dans ce cas-là, ceci vous permet de récupérer les données et de rétablir le fonctionnement du **Serveur**. En



cas de perte des fichiers clés de licence, vous pouvez en redemander comme décrit au paragraphe [Fichiers clé](#).

Restauration de Dr.Web Enterprise Server sous Windows

Installez sur un poste le logiciel **Serveur Enterprise** dans la même version que celle qui a été perdue (voir [Installation de Dr.Web Enterprise Server sous OS Windows®](#)) :

- ◆ Si une copie intacte de la BD (interne ou externe) existe sur un autre ordinateur, désignez-la dans la fenêtre de dialogue correspondante de l'installateur ainsi que les fichiers sauvegardés suivants : fichiers clé de licence du **Serveur**, clé privée de chiffrement et fichier de configuration du **Serveur**.
- ◆ Si la BD du **Serveur** (interne ou externe) a été perdue, mais qu'une copie de sauvegarde de son contenu `database.dz` existe, alors vous sélectionnez la création d'une nouvelle base de données lors de l'installation et vous spécifiez ensuite les fichiers sauvegardés des clés de licence **Serveur** et **Agent**, ainsi que la clé de chiffrement et le fichier de configuration du **Serveur**. Après la fin de l'installation, veuillez importer le contenu de la BD depuis la copie de sauvegarde (voir [Restauration de la BD de Web Enterprise Security Suite](#)).

Restauration de Dr.Web Enterprise Server sous UNIX

1. Installez sur l'ordinateur le logiciel **Serveur Enterprise** dans la même version que celle qui a été perdue (voir [Installation de Dr.Web Enterprise Server sous OS de la famille UNIX®](#)).
2. Placez les fichiers sauvegardés dans les dossiers suivants :
 - ◆ sous **Linux** : vers le répertoire `/var/opt/drwcs/` etc, excepté la clé `pub` qui doit être mise dans le dossier `/opt/drwcs/Installer/`



- ◆ sous **FreeBSD** : vers le répertoire `/var/drwcs/etc`, excepté la clé `pub` qui doit être mise dans le dossier `/usr/local/drwcs/Installer/`
- ◆ sous **Solaris** : vers le répertoire `/var/drwcs/etc`, excepté la clé `pub` qui doit être mise dans le dossier `/opt/drwcs/Installer/`



Tous les fichiers remplaçants du **Serveur** doivent avoir les mêmes droits système que les droits attribués lors de l'installation précédente (perdue) du **Serveur**.

3. Générez un nouveau certificat SSL :

- ◆ sous **Linux** et **Solaris** :
`/etc/init.d/drwcsd selfcert`
- ◆ sous **FreeBSD** :
`/usr/local/etc/rc.d/drwcsd.sh selfcert`
- ◆ pour les **autres** versions supportées :
`/opt/drwcs/bin/drwcsd -var-root=/var/
drwcs -log=/var/drwcs/log/drwcsd.log
selfcert`

4. Les actions suivantes dépendent de la présence de la base de données du **Serveur** :

- a) En cas d'utilisation d'une BD externe, aucune procédure de restauration n'est requise à condition que le fichier de configuration soit intact et que le build de **Serveur** soit identique au précédent. Sinon, il est nécessaire de spécifier la BD dans le fichier de configuration du **Serveur** et/ou de mettre à jour la structure de la base de données avec la clé `upgradedb` (voir la variante **c**) ci-dessous).
- b) Si vous disposez d'une copie de sauvegarde de la BD `database.dz` (interne ou externe), démarrez le **Serveur** et supprimez ensuite la BD interne créée lors de l'installation, puis initialisez une nouvelle base de données et importez le contenu de la base antérieure depuis la copie de sauvegarde (voir [Restauration de la BD de Dr.Web Enterprise Security Suite](#)).
- c) Si vous disposez du fichier sauvegardé de la BD interne, alors mettez-le à la place du nouveau fichier :



- sous **Linux** :
`/var/opt/drwcs/dbinternal.dbs`
- sous **FreeBSD et Solaris** :
`/var/drwcs/dbinternal.dbs`



Tous les fichiers remplaçant du **Serveur** doivent avoir les mêmes droits système que les droits attribués lors de l'installation précédente (perdue) du **Serveur**.

Veillez exécuter les commandes suivantes :

- sous **Linux et Solaris** :
`/etc/init.d/drwcsd upgradedb`
- sous **FreeBSD** :
`/usr/local/etc/rc.d/drwcsd.sh upgradedb`
- pour les **autres** versions supportées :
`/opt/drwcs/bin/drwcsd -var-root=/var/
drwcs -log=/var/drwcs/log/drwcsd.log
upgradedb update-db`

Démarrez le **Serveur**.



S'il y a des **Agents** non installés après la création de la dernière copie de sauvegarde et qu'ils ne sont pas présents dans la BD après sa restauration, il est possible de les basculer vers le statut "**Novice**" de façon distante. Pour cela, il est nécessaire de connecter le **Centre de Gestion** au **Serveur**, puis d'entrer dans le menu **Administration** → **Configuration de Dr.Web Enterprise Server** → l'onglet **Général** et d'activer ensuite le mode **Spécifier les non approuvés comme novices**.



Mise à jour des Agents sur les serveurs LAN

Lors des mises à jour des **Agents** installés sur les serveurs LAN, il vaut mieux éviter la surcharge des postes ainsi que d'éventuels arrêts du logiciel réseau tournant sur ces postes.

Afin d'assurer la stabilité du fonctionnement des postes nécessaires à l'utilisation du LAN, le mode suivant de mise à jour des **Agents** et du logiciel antivirus est recommandé :

1. Modifiez les tâches standard de mise à jour de tous les composants dans la planification du **Serveur** de sorte que seules les bases virales soient mises à jour.
2. Créez une nouvelle tâche de mise à jour de tous les composants à l'heure où cela n'aura aucun impact sur le fonctionnement des serveurs LAN.

Pour en savoir plus sur la création et l'édition des tâches dans la planification du **Serveur**, consultez le paragraphe [Configuration de la planification de Dr.Web Enterprise Server](#).



Il n'est pas recommandé d'installer les composants **SpIDer Gate** et **SpIDer Mail** sur les serveurs exécutant des fonctions réseau importantes (contrôleurs de domaine, serveurs de licences etc.) afin d'éviter d'éventuels conflits entre les services réseau et les composants antivirus **Dr.Web**.



Récupération de mot de passe administrateur Dr.Web Enterprise Security Suite

En cas de perte de mot de passe pour l'accès au **Serveur Enterprise**, il est possible de l'afficher ou modifier, en utilisant l'accès direct à la base de données du **Serveur** :

- a) En cas d'utilisation de la base interne, pour afficher ou modifier le mot de passe administrateur, utilisez l'utilitaire `drwidbsh` inclus dans le package d'installation de **Serveur**.
- b) Pour une BD externe, utilisez le client sql correspondant.



Les paramètres des comptes administrateur sont conservés dans le tableau `admins`.

Exemples d'utilisation de l'utilitaire `drwidbsh`

1. Lancez l'utilitaire, en spécifiant le chemin vers le fichier de BD :

- ◆ Pour la BD interne sous OS Linux :

```
/opt/drwcs/bin/drwidbsh /var/opt/drwcs/dbinternal.dbs
```

- ◆ Pour la BD interne sous OS Windows :

```
"C:\Program Files\DrWeb Enterprise Server\nbin\drwidbsh" "C:\Program Files\DrWeb Enterprise Server\var\dbinternal.dbs"
```

2. Pour consulter toutes les données réunies dans le tableau `admins`, exécutez la commande :

```
select * from admins;
```

3. Pour afficher les noms, les mots de passe de tous les comptes administrateur, exécutez la commande :



```
select login,password from admins;
```

4. La capture d'écran ci-dessous correspond au cas où il n'y a qu'un seul compte ayant le nom `admin` et dont le mot de passe est `root` :

```
drwidsbsh> select login,password from admins;
admin|root
  0 ms
drwidsbsh> _
```

5. Pour changer de mot de passe, utilisez la commande `update`. Voici un exemple de commande qui change le mot de passe correspondant au compte `admin` pour le mot de passe `qwerty` :

```
update admins set password='qwerty' where
login='admin';
```

6. Pour quitter l'utilitaire, exécutez la commande suivante :

```
.exit
```

Pour en savoir plus sur le fonctionnement de l'utilitaire `drwidsbsh`, consultez l'annexe [H6. Utilitaire d'administration de la BD interne](#).



Utilisation de DFS lors de l'installation de l'Agent via Active Directory

Lors de l'installation d'**Enterprise Agent** via Active Directory, il est possible d'utiliser le service DFS (Distributed File System).

Ceci peut être utile notamment en cas de plusieurs contrôleurs de domaines présents dans le LAN.

En cas d'installation dans un réseau avec plusieurs contrôleurs de domaine :

1. Créer sur chaque contrôleur de domaine un répertoire de sorte que les répertoires reçoivent les mêmes noms.
2. Avec DSF fusionnez les répertoires créés vers un répertoire racine.
3. Réalisez une installation du package *.msi vers ce répertoire cible en mode administrateur.
4. Utilisez ce répertoire cible créé lors de la spécification de package dans l'éditeur des objets de la politique de groupes.

Utilisez le nom réseau au format suivant : \\<domain>\<folder>

avec : <domain> - nom du domaine, <folder> - nom du répertoire cible.



Diagnostic des problèmes d'installation distante

Principe d'installation :

1. Le navigateur (module **Dr.Web Browser-Plugin**) se connecte à la ressource ADMIN\$ se trouvant sur une machine distante (`\\<machine_distante>\ADMIN$`) et copie les fichiers d'installation (`drwinst.exe`, `drwcsd.pub`) dont les chemins sont spécifiés dans le **Centre de Gestion** vers le dossier `\\<machine_distante>\ADMIN$\Temp`.
2. Le plugin lance le fichier `drwinst.exe` sur la machine distante avec les clés correspondantes aux paramètres respectifs dans le **Centre de Gestion**.

Pour réussir l'installation, il est nécessaire que les conditions suivantes soient remplies sur la machine depuis laquelle se fait l'installation :

1. La ressource ADMIN\$ doit être accessible sur la machine distante.

L'accessibilité de la ressource peut être vérifiée de la manière suivante :

Dans la ligne d'adresse de l'application Windows Explorer, entrez :

```
\\<machine_distante>\ADMIN$
```

Alors vous devez être invités à entrer le nom d'utilisateur et le mot de passe pour accéder à cette ressource. Veuillez entrer les informations d'authentification qui ont été spécifiées à la page d'installation.

La ressource ADMIN\$ peut être inaccessible pour des raisons listées ci-dessous :

- a) le compte n'a pas de droits d'administrateur ;



- b) la machine est déconnectée ou le pare-feu bloque l'accès au port 445 ;
 - c) l'accès à la ressource ADMIN\$ peut être restreinte sous Windows Vista ou supérieur dans le cas où ils ne font pas partie du domaine.
2. Les fichiers `drwinst.exe` ou `drwcsd.pub` doivent être accessibles.

Le **Centre de Gestion** affiche les informations exhaustives (étape et code d'erreur) pouvant aider à diagnostiquer la cause de l'erreur.

Liste des erreurs les plus fréquentes

Etape	Code d'erreur	Cause
Vérification des adresses des machines distantes (1)	Hôte inconnu (11001)	Impossible de convertir le nom DNS de la machine en une adresse. Ce nom DNS n'existe pas ou le Serveur des noms n'est pas correctement configuré.
Vérification de la disponibilité des ressources réseau sur la machine distante (2)	Erreur de socket - hôte impossible à atteindre (10064)	Le port TCP 445 sur la machine distante est indisponible, les causes possibles sont les suivantes : <ul style="list-style-type: none">◆ la machine est déconnectée ;◆ le port est bloqué par le pare-feu ;◆ l'OS installé sur la machine distante n'est pas Windows.
Connexion à la ressource d'administrateur ADMIN\$ (1001)	A ce stade, la connexion à la ressource d'administrateur ADMIN\$ se trouvant sur une machine distante est en cours d'établissement.	



Étape	Code d'erreur	Cause
	Le système a détecté une tentative potentielle d'atteinte à la sécurité. Vérifiez que vous pouvez contacter le serveur qui vous a authentifié (1265).	<ul style="list-style-type: none">◆ Aucun modèle d'accès partage et de sécurité pour les comptes locaux n'est configuré.◆ Serveur d'authentification indisponible (contrôleur de domaine)
	L'authentification a échoué : le nom d'utilisateur et le mot de passe n'est pas reconnu (1326).	Utilisateur inconnu ou mot de passe invalide.
	Erreur syntaxique : le nom de fichier, nom de répertoire ou syntaxe d'étiquette de volume est incorrect (123).	Ressource ADMIN\$ n'existe pas sur la machine distante.
Vérification du statut de fin de l'installateur (1009)	A ce stade, la vérification du résultat du fonctionnement de l'installateur a été effectuée.	
	Erreur inconnue (2).	Veillez contacter le service de support technique de Doctor Web .
	Agent est déjà installé, aucune installation n'est requise (4).	L' Agent est déjà installé sur cette machine ou il a été supprimé de manière incorrecte (dans ce cas-là, utilisez l'utilitaire drwebremove).
	Non respect du protocole (6).	L'installateur (drwinst.exe) ne correspond pas à la version de Serveur . Vérifiez si l'installateur fait partie du package d'installation du Serveur .



Etape	Code d'erreur	Cause
	Erreur d'initialisation REXX (7).	Erreur système. Veuillez contacter le service support technique Doctor Web .
	Délai de connexion au Serveur (8).	Enterprise Server est inaccessible depuis la machine distante.
	Afin de terminer la désinstallation précédente, le redémarrage est requis (9).	Redémarrez la machine pour terminer la procédure de désinstallation précédente.



Référence

A

- Active Directory
 - installation de l'agent 82
 - suppression de l'agent 97
- Administrateurs
 - comptes 169
 - droits 167
- adresse réseau 370
 - Enterprise Agent/ Installer 374
 - Enterprise Server 373
- agent
 - clés de démarrage 411
 - démarrage 109
 - fonctions 105
 - installation 57
 - installation, Active Directory 82
 - installation, distante 75, 82
 - interface 105, 106
 - mise à jour 314, 323
 - mode itinérant 323
 - paramètres 208
 - suppression 94, 97
- analyse
 - manuelle 218
- analyse antivirus 218
- authentification automatique 128
- authentification, Centre de Gestion 128

B

- BD (base de données)
 - configuration 267
 - copie de sauvegarde 569
 - intégrée 345
 - Oracle 351
 - PostgreSQL 357
 - restauration 569
 - SGBD 564
 - SQL CE 354
- blocage
 - ressources locales 246
 - trafic HTTP 248

C

- Centre de Gestion
 - arborescence 117
 - barre d'outils 119
 - description 110
 - fichier de configuration 397
 - menu principal 112
 - panneau de recherche 113
 - panneau des propriétés 123
- chiffrement
 - clés, génération 433
 - trafic 264
- clés 30
 - chiffrement, génération 433
 - démo 32



Référence

- clés 30
 - mise à jour 325
 - réception 30
 - voir aussi enregistrement 30
 - clés de démarrage
 - agent 411
 - installateur réseau 414
 - module d'interface 409
 - serveur antivirus 417
 - clés démo 32
 - composants
 - antivirus, composition 196
 - composition 18
 - réseau antivirus 147
 - synchronisation 316
 - composition du package d'installation 29
 - compression du trafic 264
 - comptes 167, 169
 - poste, création 66
 - configuration 254
 - agent 208
 - poste 196
 - serveur antivirus 254
 - configuration de SGBD 345
 - configurations
 - copie 189
 - du package antivirus 196
 - postes 196
 - console web
 - création d'un compte 66
 - copie de sauvegarde
 - BD (base de données) 569
 - serveur antivirus 576
 - création
 - comptes des postes 66
 - entrées sur les postes 192
 - groupe 178
- ## D
- démarrage
 - Dr.Web Enterprise Agent 109
 - Dr.Web Enterprise Server 103
 - dépôt des produits 277
 - éditeur simplifié 279
 - mise à jour 320
 - paramètres généraux 279
 - Dr.Web Browser-Plugin
 - installation 53
 - mise à jour 313
 - suppression 94
 - suppression, sous OS UNIX 99
 - Dr.Web Enterprise Agent
 - clés de démarrage 411
 - configuration 208
 - démarrage 109
 - fonctions 105
 - installation 57



Référence

- Dr.Web Enterprise Agent
 - types de liaisons 283
 - installation, Active Directory 82
 - installation, distante 75, 82
 - interface 105, 106
 - mise à jour 314, 323
 - modé itinérant 323
 - suppression 94, 97
 - Dr.Web Enterprise Server
 - clés de démarrage 417
 - configuration 254
 - configuration de liaisons 286
 - démarrage 103
 - déplacement 559
 - fichier de configuration 388
 - installation, sous OS UNIX 48
 - installation, sous OS Windows 36
 - interface 103
 - journal 272
 - mise à jour, pour OS UNIX 305
 - mise à jour, pour OS Windows 297
 - planification 273
 - protocole 102
 - restauration 576
 - structure du répertoire 46
 - suppression, sous OS UNIX 97
 - suppression, sous OS Windows 94
 - tâches 101
 - droits
 - Administrateurs 167
- ## E
- enregistrement
 - du produit Dr.Web 30
 - expressions régulières 444, 446
- ## F
- fichier de configuration
 - Centre de Gestion 397
 - dépôt des produits 377
 - serveur antivirus 388
 - serveur proxy 403
 - fichier de statut 385, 386
 - fonctions
 - agent 105
 - Dr. Web ESS 17
 - serveur antivirus 101
- ## G
- groupes 174
 - ajout des postes 182
 - configuration 185
 - configuration, héritage 186
 - configurations, copie 189
 - primaires 186
 - suppression des postes 182
 - groupes préconfigurés 174



Référence

groupes primaires 186

I

icônes

- agent 106
- arborescence 118
- scanner résea 76
- scanner réseau 133

installateur réseau 414

installation

- agent 57, 66
- agent, Active Directory 82
- agent, distante 75, 82
- NAP Validator 89
- serveur antivirus 36, 48

interface

- Agent 105, 106
- serveur antivirus 103

L

langue

- Centre de Gestion 124, 170

liaisons, entre serveurs

- configuration 286
- types 283

licensing 30

log du serveur 272

M

messages

envoi à l'utilisateur 249

format du logo 252

métacaractères 448

mise à jour

- agent 314, 323
- clés 325
- dépôt des produits 320
- Dr.Web Browser-Plugin 297
- Dr.Web ESS 297

forcée 316

limitation 322

manuelle 316

mode itinérant 323

réseau antivirus 294

selon planification 318

Serveur proxy 314

serveur, pour OS UNIX 305

serveur, pour OS Windows 297

mise à jour forcée 316

mise à jour manuelle 316

mode itinérant de l'agent 323

N

NAP Validator 333

configuration 336

installation 89

notifications

configuration 269

configuration de templates 362



Référence

- notifications
 - paramètres 361
- novice 208
- O**
- office control 246, 248
- P**
- package antivirus
 - composant, composition 196
 - installation 57, 82, 196
 - suppression 94, 196
 - composition 20
- package d'installation 29
- paramètres
 - agent 208
- planification
 - centralisée 214
 - des mises à jour 318
 - du serveur 273
 - locale 217
- planification centralisée 214
- planification locale 217
- poste
 - ajout vers le groupe 182
 - configuration 196
 - configuration, héritage 186
 - configurations, copie 189
 - création d'un compte 66
 - création d'une entrée 192
 - gestion 191
 - propriétés 196
 - scan 213, 218
 - statistiques 234
 - suppression depuis le groupe 182
- pré-requis système 23, 338
- procédures 474
- propriétés du poste 196
- protocole du serveur 102
- Q**
- quarantaine 243
- R**
- répertoire du serveur, structure 46
- réseau antivirus 282
 - composants 18, 147
 - configuration de liaisons 286
 - événements viraux 294
 - licensing 31
 - mises à jour 294
 - planification 33
 - structure 147, 283
- restauration
 - BD (base de données) 569
 - serveur antivirus 576
- restauration du poste
 - restauration 194
 - suppression 194



Référence

- restriction d'accès
 - Internet 248
 - ressources locales 246
- restriction des mises à jour 322
- S**
- scan
 - automatique 213
- scanner
 - antivirus 218, 435
 - réseau 75, 131
- scanner antivirus 218, 435
- serveur antivirus
 - clés de démarrage 417
 - configuration 254
 - configuration de liaisons 286
 - démarrage 103
 - déplacement 559
 - fichier de configuration 388
 - installation, sous OS UNIX 48
 - installation, sous OS Windows 36
 - interface 103
 - journal 272
 - mise à jour, pour OS UNIX 305
 - mise à jour, pour OS Windows 297
 - protocole 102
 - restauration 576
 - structure du répertoire 46
 - suppression, sous OS UNIX 97
 - suppression, sous OS Windows 94
 - tâches 101
 - types de liaisons 283
- serveur antivirius
 - planification 273
- serveur proxy
 - démarrage, arrêt 332
 - fichier de configuration 403
 - fonctions 328
 - installation 90
 - mise à jour 314
 - suppression 99
- SGMAJ
 - voir aussi mise à jour manuelle 316
- statistiques
 - du poste 234
- suppression
 - agent 94
 - agent, Active Directory 97
 - composants 94
 - composants antivirus 196
 - Dr.Web Browser-Plugin 94, 99
 - du poste 194
 - package antivirus 94
 - poste, depuis le groupe 182
 - serveur antivirus 94, 97
 - Serveur proxy 99



Référence

supression
 groupe 179
synchronisation, composants 316
système de facturation (billing) 479

T

trafic
 chiffrement 264
 composition 150
 compression 264
 HTTP, blocage 248
trafic HTTP, blocage 248

V

variables d'environnement 438

