



Dr.WEB

Enterprise Security Suite

Manuel Administrateur

Жасағаныңды қорға

دافع عن إبداعاتك

Защити созданное

Defend what you create

Protégez votre univers

Verteidige, was du erschaffen hast

Захисти створене

保护您创建的一切

Защити созданное

Proteggi ciò che crei

Жасағаныңды қорға

Защити созданное

Proteggi ciò che crei

Verteidige, was du erschaffen hast

Захисти створене

Defend what you create

脅威からの保護を提供します

Protégez votre univers

Proteggi ciò che crei

Захисти створене

دافع عن إبداعاتك

脅威からの保護を提供します

Defend what you create

Жасағаныңды қорға

دافع عن إبداعاتك

دافع عن إبداعاتك

Protégez votre univers

保护您创建的一切

Защити созданное

脅威からの保護を提供します

Захисти створене

Verteidige, was du erschaffen hast

© **Doctor Web, 2017. Tous droits réservés**

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

Marques déposées

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

Limitation de responsabilité

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

Dr.Web Enterprise Security Suite
Version 10.01.0
Manuel Administrateur
12/09/2017

Doctor Web, Siège social en Russie
125040
Moscou, Russie
2-12A, 3e rue Yamskogo polya
Site web : <http://www.drweb.com/>
Téléphone : +7 (495) 789-45-87

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

Doctor Web

Doctor Web – éditeur russe de solutions de sécurité informatique.

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

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

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

Nous remercions tous nos clients pour leur soutien des produits Dr.Web !



Contenu

Chapitre 1. Dr.Web Enterprise Security Suite	8
1.1. Introduction	8
1.1.1. Destination du document	8
1.1.2. Légende et abréviations	9
1.2. A propos du produit	11
1.3. Pré-requis système	20
1.4. Kit de distribution	26
Chapitre 2. Licence	28
2.1. Politique de Licencing	29
2.2. Mise à jour automatique de licences	30
Chapitre 3. Mise en route	34
3.1. Création d'un réseau antivirus	34
3.2. Configuration des connexions réseau	37
3.2.1. Connexions directes	38
3.2.2. Service de détection du Serveur Dr.Web	39
3.2.3. Utiliser le protocole SRV	39
Chapitre 4. Composants du réseau antivirus et leur interface	41
4.1. Serveur Dr.Web	41
4.1.1. Gestion du Serveur Dr.Web sous OS Windows®	42
4.1.2. Gestion du Serveur Dr.Web sous les OS de la famille UNIX®	45
4.2. Protection de postes de travail	49
4.3. Centre de gestion de la sécurité Dr.Web	50
4.3.1. Administration	53
4.3.2. Réseau antivirus	56
4.3.3. Liaisons	63
4.3.4. Barre de recherche	63
4.3.5. Événements	64
4.3.6. Paramètres	65
4.3.7. Aide	70
4.4. Composants du Centre de gestion de la sécurité Dr.Web	71
4.4.1. Scanner réseau	71
4.4.2. Gestionnaire de licences	73
4.5. Schéma d'interaction des composants du réseau antivirus	81



Chapitre 5. Administrateurs du réseau antivirus	85
5.1. Authentification des administrateurs	85
5.1.1. Authentification des administrateurs depuis la BD du Serveur	86
5.1.2. Authentification via Active Directory	86
5.1.3. Authentification via LDAP	88
5.1.4. Authentification via RADIUS	89
5.1.5. Authentification via PAM	90
5.2. Administrateurs et groupes administrateur	92
5.2.1. Hiérarchie des administrateurs	92
5.2.2. Droits d'administrateurs	93
5.3. Gestion des comptes et des groupes administrateur	97
5.3.1. Création et suppression des comptes et des groupes administrateur	97
5.3.2. Éditer les comptes et les groupes administrateur	99
Chapitre 6. Groupes. Gestion globale des postes de travail	102
6.1. Groupes système et groupes utilisateur	102
6.2. Gestion des groupes	105
6.2.1. Création et suppression des groupes	105
6.2.2. Configuration des groupes	106
6.3. Placement de postes de travail dans des groupes utilisateur	108
6.3.1. Placement manuel de postes dans des groupes	108
6.3.2. Configuration de l'appartenance automatique au groupe	109
6.4. Utilisation des groupes pour configurer les postes de travail	112
6.4.1. Héritage des éléments de la configuration du poste de travail	113
6.4.2. Copie des configurations vers d'autres groupes/postes	114
6.5. Comparaison des postes et des groupes	115
Chapitre 7. Gestion des postes de travail	116
7.1. Gestion des comptes des postes de travail	116
7.1.1. Politique d'approbation des postes	116
7.1.2. Suppression et restauration d'un poste	118
7.1.3. Fusionner des postes	119
7.2. Paramètres généraux du poste de travail	119
7.2.1. Propriétés du poste	119
7.2.2. Composants installés du package antivirus	123
7.2.3. Matériel et logiciels des postes tournant sous Windows®	124
7.3. Configuration du poste de travail	126
7.3.1. Droits des utilisateurs du poste	126



7.3.2. Planification des tâches sur un poste	129
7.3.3. Composants à installer du package antivirus	134
7.4. Configuration des composants antivirus	134
7.4.1. Composants	135
7.5. Scan antivirus des postes de travail	138
7.5.1. Consultation et interruption des composants en cours	138
7.5.2. Interruption des composants en cours selon leur type	139
7.5.3. Lancement du scan sur le poste de travail	140
7.5.4. Configuration du Scanner	141
7.6. Consultation des statistiques sur un poste	148
7.6.1. Statistiques	148
7.6.2. Graphiques	153
7.6.3. Quarantaine	155
7.7. Envoi des fichiers d'installation	157
7.8. Envoi de messages aux postes	159
Chapitre 8. Configuration du Serveur Dr.Web	162
8.1. Journalisation	162
8.1.1. Journal d'audit	162
8.1.2. Journal de fonctionnement du Serveur Dr.Web	164
8.1.3. Journal des mises à jour du dépôt	165
8.2. Configuration du Serveur Dr.Web	167
8.2.1. Général	168
8.2.2. Réseau	172
8.2.3. Statistiques	176
8.2.4. Sécurité	179
8.2.5. Cache	180
8.2.6. Base de données	180
8.2.7. Modules	182
8.2.8. Localisation	183
8.2.9. Licences	183
8.3. Accès distant au Serveur Dr.Web	184
8.4. Configuration de la planification du Serveur Dr.Web	185
8.5. Configuration du Serveur web	194
8.5.1. Général	195
8.5.2. Avancé	196
8.5.3. Transport	197



8.5.4. Sécurité	197
8.6. Procédures utilisateur	198
8.7. Configuration des notifications	202
8.7.1. Configuration des notifications	202
8.7.2. Notifications de la console Web	206
8.7.3. Notifications non envoyées	208
8.8. Gestion du dépôt du Serveur Dr.Web	209
8.8.1. Statut du dépôt	210
8.8.2. Mises à jour reportées	210
8.8.3. Configuration générale du dépôt	211
8.8.4. Configuration détaillée du dépôt	214
8.8.5. Contenu du dépôt	218
8.9. Options supplémentaires	220
8.9.1. Gestion de la base de données	220
8.9.2. Statistiques du Serveur Dr.Web	223
8.10. Particularités du réseau avec plusieurs Serveurs Dr.Web	224
8.10.1. Structure du réseau avec plusieurs Serveurs Dr.Web	225
8.10.2. Configuration des liaisons entre Serveurs Dr.Web	227
8.10.3. Utilisation du réseau antivirus avec plusieurs Serveurs Dr.Web	232
8.10.4. Cluster des Serveurs Dr.Web	234
Chapitre 9. Mise à jour des composants de Dr.Web Enterprise Security Suite	238
9.1. Mise à jour du Serveur Dr.Web et restauration depuis une copie de sauvegarde	238
9.2. Mise à jour manuelle des composants de Dr.Web Enterprise Security Suite	240
9.3. Mise à jour selon la planification	240
9.4. Mise à jour du dépôt du Serveur Dr.Web non connecté à Internet	241
9.4.1. Copier le dépôt d'un autre Serveur Dr.Web	241
9.4.2. Chargeur du dépôt Dr.Web	242
9.5. Restrictions de mises à jour des postes	247
9.6. Mise à jour des Agents mobiles Dr.Web	248
Chapitre 10. Configuration des composants supplémentaires	250
10.1. Serveur proxy	250
10.2. NAP Validator	254
Référence	257



Chapitre 1. Dr.Web Enterprise Security Suite

1.1. Introduction

1.1.1. Destination du document

La documentation de l'administrateur du réseau antivirus Dr.Web Enterprise Security Suite 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.

La documentation de l'administrateur du réseau antivirus Dr.Web Enterprise Security Suite contient les parties suivantes :

1. **Manuel d'Installation** (fichier **drweb-esuite-10-install-manual-fr.pdf**)
2. **Manuel Administrateur** (fichier **drweb-esuite-10-admin-manual-fr.pdf**)

Le Manuel Administrateur s'adresse à *l'administrateur du réseau antivirus*, la personne responsable, dans l'entreprise, de la protection antivirus des ordinateurs (postes de travail, serveurs) de ce réseau.

L'administrateur du réseau antivirus doit posséder les privilèges administrateur sur le système, savoir mettre en place la politique de protection antivirus et connaître en détails les packages antivirus Dr.Web pour tous les systèmes d'exploitation utilisés dans le réseau.

3. **Annexes** (fichier **drweb-esuite-10-appendices-fr.pdf**)



La documentation contient des renvois entre les documents mentionnés ci-dessus. Si vous téléchargez ces documents sur un ordinateur local, les renvois fonctionnent uniquement si les documents sont enregistrés dans le même dossier et portent leurs noms initiales.

La documentation Administrateur ne contient pas la description des packages antivirus Dr.Web pour les ordinateurs protégés. Pour ces informations, merci de consulter les **Manuels Utilisateurs** des solutions Dr.Web pour les OS correspondants.

Avant de prendre connaissance de ces documents, merci de vous assurer que vous lisez la dernière version des Manuels. Les manuels sont constamment mis à jour, et leur dernière version est disponible sur le site officiel de Doctor Web <https://download.drweb.fr/doc/>.





1.1.2. Légende et abréviations

Conventions

Les symboles utilisés dans ce manuel sont présentés dans le tableau 1-1.

Tableau 1-1. Conventions

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

Abréviations

Les abréviations suivantes sont utilisées dans le Manuel :

- ACL – listes de contrôle d'accès (Access Control List),
- CDN – réseau de distribution de contenu (Content Delivery Network),
- CPU – unité centrale (Central Processing Unit),
- DFS – système de fichiers distribués (Distributed File System),
- DNS – système de noms de domaine (Domain Name System),
- GUI – interface graphique utilisateur (Graphical User Interface), une version GUI du logiciel est une version utilisant des outils GUI,
- NAP – Protection d'accès réseau (Network Access Protection),
- MTU – taille maximale de l'unité de transmission (Maximum Transmission Unit),
- TTL – durée de Vie (Time To Live),
- UDS – socket du domaine UNIX (UNIX Domain socket),



- BD, SGBD – base de données, système de gestion de base de données,
- SGM Dr.Web – Système Global de Mises à jour Dr.Web,
- LAN – réseau local,
- OS – système d'exploitation.

1.2. A propos du produit

Dr.Web Enterprise Security Suite est conçu pour la mise en oeuvre et la gestion d'une protection antivirus fiable non seulement du réseau interne de l'entreprise, y compris des appareils mobiles mais aussi des ordinateurs de maison des employés.

Un ensemble d'ordinateurs et d'appareils mobiles sur lesquels les composants interagissants de Dr.Web Enterprise Security Suite sont installés représente un *réseau antivirus*.

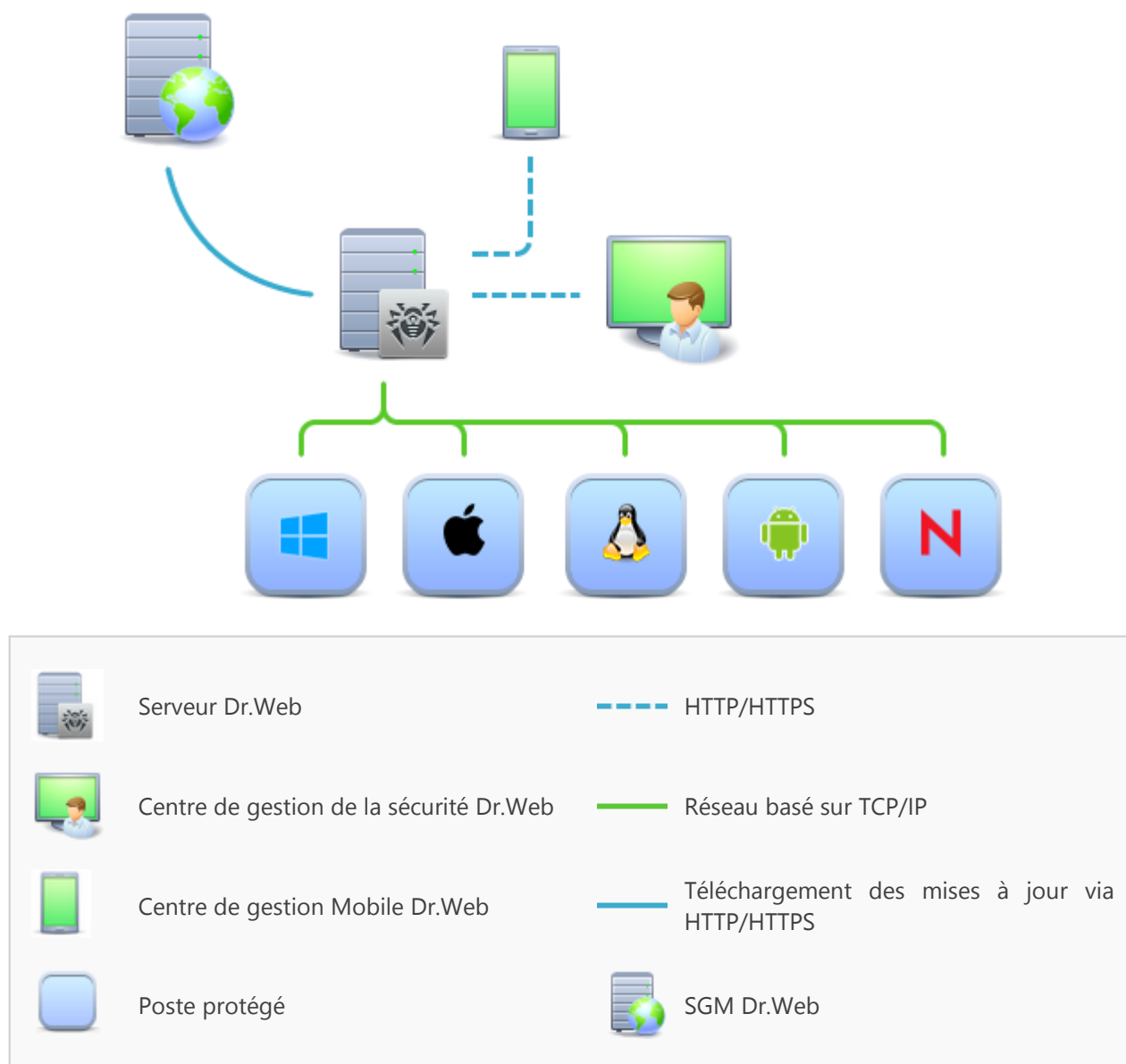


Figure 1-1. Structure logique du réseau antivirus

Le réseau antivirus Dr.Web Enterprise Security Suite repose sur une structure *client-serveur*. Ses composants sont installés sur les postes et les appareils mobiles des utilisateurs et des administrateurs ainsi que sur les postes dotés des fonctionnalités de Serveurs LAN. Ces composants échangent des informations via les protocoles réseau TCP/IP. Vous pouvez installer (et plus tard gérer) le logiciel antivirus sur les postes protégés via LAN ou via Internet.



Serveur de protection centralisée

Le Serveur de protection centralisée peut être installé sur n'importe quel ordinateur et pas uniquement sur la poste utilisé comme serveur LAN. Pour en savoir plus sur les pré-requis principaux, consultez le paragraphe [Pré-requis système](#).

Le logiciel du serveur est indépendant de la plateforme et permet d'utiliser en tant que Serveur un ordinateur tournant sous les systèmes d'exploitation suivants :

- Windows®,
- OS de la famille UNIX® (Linux®, FreeBSD®, Solaris™).

Le Serveur de protection centralisée conserve les distributions des packages antivirus appropriés aux différents OS installés sur les postes protégés, les mises à jour des bases virales ainsi que celles des packages antivirus, les clés utilisateurs et les configurations des packages pour les postes protégés. Le Serveur reçoit des mises à jour de composants de protection antivirus et des bases virales via Internet depuis les serveurs du Système Global de Mise à jour et distribue les mises à jour sur les postes protégés.

Il est possible de créer la structure hiérarchique contenant plusieurs Serveurs qui maintiennent les postes protégés du réseau antivirus.

Le Serveur supporte la fonction de sauvegarde (backup) des données critiques (les bases de données, fichiers de configuration etc.).

Le Serveur effectue la journalisation des événements du réseau antivirus.

Base de données commune

La base de données commune se connecte au Serveur de protection centralisée et contient les statistiques des événements du réseau antivirus, les paramètres du Serveur, les paramètres des postes protégés et des composants antivirus installés sur les postes protégés.

Les types suivants de bases de données peuvent être utilisés :

Base de données embarquée. Deux options de la base de données embarquée directement dans le Serveur de protection centralisée sont fournies :

- SQLite2 (InitDB),
- SQLite3.

Base de données externe. Les pilotes intégrés pour la connexion des bases de données suivantes sont fournis :

- Oracle,
- PostgreSQL,
- Pilote ODBC pour connecter d'autres bases de données, comme Microsoft SQL Server/Microsoft SQL Server Express.

Vous pouvez utiliser n'importe quelle base de données correspondant à vos attentes. Votre choix doit se baser sur les besoins que le dépôt de données doit satisfaire, par exemple : la possibilité de maintenir le réseau antivirus d'une taille correspondante, les particularités de



maintenance du logiciel de base de données, les possibilités d'administration fournies par la base de données et d'autres exigences et normes adoptées dans votre entreprise.

Centre de gestion de la protection centralisée

Le Centre de gestion de la protection centralisée s'installe automatiquement avec le Serveur et fournit l'interface web permettant la gestion à distance du Serveur et du réseau antivirus par le biais de la modification des configurations du Serveur et des postes protégés conservées sur le Serveur et sur les postes.

Le Centre de gestion peut être ouvert sur n'importe quel ordinateur ayant l'accès au Serveur. Le Centre de gestion peut être utilisé sur n'importe quel système d'exploitation avec la fonctionnalité complète sous les navigateurs web suivants :

- Windows® Internet Explorer®,
- Mozilla® Firefox®,
- Google Chrome®.

Vous pouvez consulter la liste des options d'utilisation possibles dans le p. [Pré-requis système](#).

Le Centre de gestion de la protection centralisée fournit les fonctionnalités suivantes :

- Facilité d'installation de l'Antivirus sur les postes protégés, y compris la possibilité d'installation à distance sous OS Windows avec une recherche préliminaire des ordinateurs ; création de distributions aux identifiants uniques avec les paramètres de connexion au Serveur pour faciliter le processus d'installation de l'Antivirus par l'administrateur et donner la possibilité aux utilisateurs d'installer l'Antivirus eux-même.
- Facilité de gestion des postes dans le réseau antivirus, assurée par un mécanisme de groupement (pour plus d'informations, voir la section [Chapitre 6. Groupes. Gestion globale des postes de travail](#)).
- Possibilité de gestion centralisée de packages antivirus de postes, y compris : suppression de composants particuliers ou de l'Antivirus dans son ensemble sur les postes tournant sous OS Windows ; configuration de paramètres de composants de packages antivirus ; spécification de droits d'utilisateurs de configurer et gérer les packages antivirus sur les postes protégés (pour plus d'informations, voir la section [Chapitre 7. Gestion des postes de travail](#)).
- Gestion centralisée du scan antivirus de postes de travail, y compris lancement à distance du scan antivirus selon la planification ou la requête directe de l'administrateur depuis le Centre de gestion, configuration centralisée de paramètres du scan antivirus qui sont transmis sur les postes pour lancer le scan local avec les paramètres spécifiés (pour plus d'informations voir [Scan antivirus du poste de travail](#)).
- Obtention des informations statistiques sur le statut de postes protégés, statistiques vitales, statut du logiciel installé, statut des composants lancés et liste de hardware et software du poste protégé (pour plus d'informations, voir [Consultation des statistiques d'un poste de travail](#)).
- Système flexible d'administration du Serveur et du réseau antivirus grâce à la possibilité de délimiter les droits des administrateurs différents et la possibilité de connexion des administrateurs via les systèmes d'authentification externes comme par exemple Active



Directory, LDAP, RADIUS, PAM (pour plus d'informations, voir la section [Chapitre 5. Administrateurs du réseau antivirus](#)).

- Gestion de licences de protection antivirus sur les postes de travail avec le système ramifié d'assignation de licences aux postes, groupes de postes et de transmission de licences entre plusieurs Serveurs en cas de configuration réseau multi-serveurs (pour plus d'informations, voir [Gestionnaire de licences](#)).
- Un large ensemble de paramètres pour configurer le Serveur et ses composants, y compris : configuration de planification de maintenance du Serveur ; ajout de procédures utilisateur ; configuration flexible du système de mise à jour de tous les composants du réseau antivirus depuis le SGM et diffusion de mises à jour sur les postes ; configuration de systèmes de notification de l'administrateur sur les événements du réseau antivirus avec les méthodes différentes d'envoi de notifications ; paramétrage des liaisons entre Serveurs pour configurer un réseau multi-serveurs (pour plus d'informations, voir la section [Chapitre 8. Configuration du Serveur Dr.Web](#)).



Pour l'information détaillée sur les fonctionnalités d'installation de la protection antivirus sur les postes, veuillez consulter **Manuel d'installation**.

Le Serveur web est automatiquement installé avec le Serveur et représente une partie du Centre de gestion de la sécurité Dr.Web. La tâche principale du Serveur web est d'interagir avec les pages web du Centre de gestion et les connexions réseau des clients.

Centre de gestion Mobile de la protection centralisée

Le Centre de gestion Mobile est fourni en tant que composant à part destiné à installer et lancer le logiciel sur les appareils mobiles tournant sous iOS et OS Android. Les exigences générales pour l'application sont mentionnées dans le p. [Pré-requis système](#).

La connexion du Centre de gestion Mobile au Serveur est effectuée à la base des identifiants de l'administrateur du réseau antivirus, y compris via le protocole crypté. Le Centre de gestion Mobile supporte les fonctions de base du Centre de gestion :

1. Gestion du dépôt du Serveur Dr.Web :
 - consulter le statut des produits dans le dépôt ;
 - lancer la mise à jour du dépôt depuis le Système Global de Mises à jour Dr.Web.
2. La gestion des postes sur lesquels la mise à jour du logiciel antivirus a échoué :
 - affichage des postes échoués ;
 - mise à jour des composants sur les postes échoués.
3. Affichage des statistiques sur le statut du réseau antivirus :
 - nombre des postes enregistrés sur le Serveur Dr.Web et leur statut actuel (en ligne/hors ligne) ;
 - statistiques des infections sur les postes protégés.
4. Gestion des nouveaux postes qui attendent la connexion au Serveur Dr.Web :
 - approbation de l'accès ;



- rejet des postes.
5. Gestion des composants antivirus installés sur les postes du réseau antivirus :
 - lancement du scan rapide ou complet pour les postes sélectionnés ou pour tous les postes des groupes sélectionnés ;
 - configuration de la réaction du Scanner Dr.Web sur la détection d'objets malveillants ;
 - consultation et gestion des fichiers de la Quarantaine sur un poste sélectionné ou sur tous les postes du groupe sélectionné.
 6. Gestion des postes et des groupes :
 - consultation des paramètres ;
 - consultation et gestion du contenu des composants du package antivirus ;
 - suppression ;
 - envoi de messages sur les postes ;
 - redémarrage des postes tournant sous Windows ;
 - ajout aux favoris pour l'accès rapide.
 7. Recherche des postes et des groupes sur le réseau antivirus par paramètres différents : nom, adresse, ID.
 8. Consultation et gestion des messages sur les événements majeurs dans le réseau antivirus via les notifications interactives Push :
 - affichage de toutes les notifications sur le Serveur Dr.Web ;
 - spécification de la réaction sur les événements de notifications ;
 - recherche des notifications par paramètres spécifiés du filtre ;
 - suppression des notifications ;
 - exclusion de la suppression automatique des notifications.

Vous pouvez télécharger le Centre de gestion Mobile depuis le Centre de gestion ou directement sur [App Store](#) ou [Google Play](#).

Protection des postes du réseau

Sur les postes et les appareils mobiles du réseau s'effectue l'installation du module gérant (l'Agent) et du package antivirus pour le système d'exploitation correspondant.

Le logiciel du serveur est indépendant de la plateforme et permet de protéger des ordinateurs et des appareils mobiles tournant sous les système d'exploitation suivants :

- Windows®,
- OS de la famille UNIX®,
- OS X®,
- OS Android,
- OS Novell® NetWare®.



Les ordinateurs personnels et les serveurs LAN peuvent être considérés comme postes protégés. Notamment, la protection antivirus du système de courrier Microsoft® Outlook® est supportée.

Le module gérant effectue des mises à jour régulières des composants antivirus et des bases virales depuis le Serveur et envoie sur le Serveur des informations sur les événements du poste protégé.

En cas d'indisponibilité du Serveur de protection centralisée la mise à jour de bases virales de postes protégés est effectuée directement depuis le Système Global de Mise à jour via Internet.

En fonction du système d'exploitation du poste les fonctions suivantes sont fournies :

Postes tournant sous l'OS Windows®

Protection antivirus

Scan de l'ordinateur selon la requête de l'utilisateur et selon la planification. Il est également possible de lancer sur les postes le scan antivirus à distance depuis le Centre de gestion, y compris le scan anti-rootkits.

Moniteur de fichiers

Analyse permanente à la volée du système de fichiers. Analyse de tous les processus lancés ainsi que des fichiers créés sur les disques durs et des fichiers ouverts sur les supports amovibles.

Moniteur de courrier

Analyse de tous les e-mails entrants et sortants en cas de l'utilisation de clients de messagerie.

Possibilité d'utiliser un filtre antispam (à condition que cette option soit autorisée par la licence).

Moniteur web

Analyse de toutes les requêtes vers les sites web via le protocole HTTP. Neutralisation des menaces contenues dans le trafic HTTP (par exemple dans les fichiers reçus/envoyés). Blocage de l'accès aux ressources suspectes ou incorrectes.

Office Control

Gestion de l'accès aux ressources réseau ou aux ressources locales, notamment, il contrôle l'accès aux sites web. Le composant permet non seulement de contrôler l'intégrité des fichiers importants qu'il protège contre toute modification occasionnelle ou infection virale, mais il bloque aussi l'accès des employés aux informations non sollicitées.

Pare-feu

Protection de l'ordinateur contre tout accès non autorisé de l'extérieur ainsi que contre des fuites de données importantes via le réseau. Contrôle de la connexion et de la transmission



de données via Internet et blocage des connexions suspectes au niveau des paquets et des applications.

Quarantaine

Isolation des objets malveillants ou suspects dans un répertoire spécial.

Autoprotection

Protection des fichiers et des dossiers de Dr.Web Enterprise Security Suite contre une suppression non autorisée ou involontaire ainsi que contre une modification par l'utilisateur ou par un malware. Lorsque l'autoprotection est active, seuls les processus Dr.Web ont accès aux fichiers et des dossiers de Dr.Web Enterprise Security Suite.

Protection préventive

Prévention de menaces potentielles à la sécurité. Contrôle d'accès aux objets critique du système d'exploitation, contrôle de téléchargement de pilotes, contrôle de démarrage automatique de programmes et de fonctionnement de services système. Surveillance de processus lancés et leur blocage en cas de détection d'une activité malveillante.

Postes tournant sous OS de la famille UNIX®

Protection antivirus

Le scan de l'ordinateur selon la requête de l'utilisateur et selon la planification. Il est également possible de lancer sur les postes le scan antivirus à distance depuis le Centre de gestion.

Moniteur de fichiers

Analyse permanente à la volée du système de fichiers. Analyse de tous les processus lancés ainsi que des fichiers créés sur les disques durs et des fichiers ouverts sur les supports amovibles.

Moniteur web

Analyse de toutes les requêtes vers les sites web via le protocole HTTP. Neutralisation des menaces contenues dans le trafic HTTP (par exemple dans les fichiers reçus/envoyés). Blocage de l'accès aux ressources suspectes ou incorrectes.

Quarantaine

Isolation des objets malveillants ou suspects dans un répertoire spécial.

Postes tournant OS X®

Protection antivirus

Le scan de l'ordinateur selon la requête de l'utilisateur et selon la planification. Il est également possible de lancer sur les postes le scan antivirus à distance depuis le Centre de gestion.



Moniteur de fichiers

Analyse permanente à la volée du système de fichiers. Analyse de tous les processus lancés ainsi que des fichiers créés sur les disques durs et des fichiers ouverts sur les supports amovibles.

Moniteur web

Analyse de toutes les requêtes vers les sites web via le protocole HTTP. Neutralisation des menaces contenues dans le trafic HTTP (par exemple dans les fichiers reçus/envoyés). Blocage de l'accès aux ressources suspectes ou incorrectes.

Quarantaine

Isolation des objets malveillants ou suspects dans un répertoire spécial.

Appareils mobiles tournant sous OS Android

Protection antivirus

Le scan de l'appareil mobile selon la requête de l'utilisateur et selon la planification. Il est également possible de lancer sur les postes le scan antivirus à distance depuis le Centre de gestion.

Moniteur de fichiers

Analyse permanente à la volée du système de fichiers. Scan de tous les fichiers lors de la tentative de sauvegarder ces fichiers dans la mémoire de l'appareil mobile.

Filtrage des appels et des messages

Le filtrage des appels et des messages SMS permet de bloquer des messages et des appels indésirables, par exemple, des messages publicitaires ou des appels et des messages des numéros inconnus.

Antivol

Détection de l'appareil mobile ou le blocage rapide de fonctionnalités en cas de perte ou de vol.

Restriction de l'accès aux ressources web

Le filtre URL permet de protéger l'utilisateur de l'appareil mobile contre les ressources web indésirables.

Pare-feu

Protection de l'appareil mobile contre tout accès non autorisé de l'extérieur ainsi que contre des fuites de données importantes via le réseau. Contrôle de la connexion et de la transmission de données via Internet et blocage des connexions suspectes au niveau des paquets et des applications.



Aide dans la résolution de problèmes de sécurité

Diagnostic et analyse de sécurité de l'appareil mobile et résolution de problèmes et de vulnérabilités détectés.

Contrôle de lancement des applications

Interdiction de lancer sur l'appareil mobile des applications qui ne sont pas incluses dans la liste des applications autorisées par l'administrateur.

OS Novell® NetWare®

Protection antivirus

Scan de l'ordinateur selon la requête de l'utilisateur et selon la planification.

Moniteur de fichiers

Analyse permanente à la volée du système de fichiers. Analyse de tous les processus lancés ainsi que des fichiers créés sur les disques durs et des fichiers ouverts sur les supports amovibles.

Assurance de la connexion entre les composants du réseau antivirus

Pour assurer la connexion stable et sécurisée entre les composants du réseau antivirus, les fonctionnalités suivantes sont fournies :

Serveur proxy Dr.Web

Le Serveur-proxy peut être optionnellement installé dans le réseau antivirus. L'objectif principal du Serveur proxy consiste à assurer la connexion entre le Serveur et les postes protégés dans le cas où la connexion directe devient impossible, par exemple lorsque le Serveur et les postes protégés se trouvent dans des réseaux différents entre lesquels il n'y a pas de routage de paquets. L'utilisation de la fonction de mise en cache peut diminuer le trafic réseau et la durée de téléchargement des mises à jour par les postes protégés.

Compression du trafic

Lors de la transmission de données entre les composants du réseau antivirus, les algorithmes spéciaux de compression sont utilisés, ce qui assure le trafic réseau minimum.

Chiffrement du trafic

Lors de la transmission de données entre les composants du réseau antivirus, le chiffrement est utilisé ce qui assure la protection supplémentaire.



Options supplémentaires

NAP Validator

NAP Validator est fourni en tant que composant supplémentaire qui permet d'utiliser la technologie Microsoft Network Access Protection (NAP) pour vérifier le fonctionnement du logiciel sur les postes protégés. Le niveau de sécurité est assuré grâce à la capacité de répondre aux exigences opérationnelles relatives aux systèmes dans le réseau.

Chargeur du Dépôt

Chargeur du Dépôt Dr.Web est fourni en tant qu'utilitaire supplémentaire qui permet de télécharger les produits Dr.Web Enterprise Security Suite depuis le Système global de mise à jour. Il peut être utilisé pour télécharger les mises à jour de produits Dr.Web Enterprise Security Suite pour placer les mises à jour sur le Serveur qui n'est pas connecté à Internet.

1.3. Pré-requis système

L'installation et le fonctionnement de Dr.Web Enterprise Security Suite requièrent :

- l'ordinateur sur lequel le Serveur Dr.Web est installé doit avoir un accès à Internet pour télécharger de façon automatique les mises à jour depuis les serveurs de SGM (Système global de mise à jour) Dr.Web ;



Il existe aussi une possibilité de distribuer des mises à jour sur les Serveurs qui ne sont pas connectés à Internet d'une autre manière. Notamment, en cas d'une configuration multi-serveurs du réseau antivirus, vous pouvez obtenir les mises à jour depuis SGM sur un des Serveurs et puis les diffuser sur les autres Serveurs ou vous pouvez utiliser l'utilitaire supplémentaire Chargeur du Dépôt Dr.Web pour télécharger les mises à jour depuis SGM via Internet et puis les diffuser sur les Serveurs.

- les ordinateurs se trouvant dans le réseau antivirus doivent avoir un accès au Serveur Dr.Web ou au Serveur proxy ;
- pour assurer l'interaction entre tous les composants antivirus, les ports suivants doivent être ouverts :

Numéros de ports	Protocoles	Direction des connexions	Utilisation
2193	TCP	<ul style="list-style-type: none">• entrantes, sortantes pour le Serveur et le Serveur proxy• sortantes pour l'Agent	Pour la connexion des composants antivirus au Serveur et les liaisons entre Serveurs. Le Serveur proxy est également utilisé pour établir la connexion aux clients.
	UDP	entrantes, sortantes	Pour le fonctionnement du Scanner réseau.



Numéros de ports	Protocoles	Direction des connexions	Utilisation
139, 445	TCP	<ul style="list-style-type: none">• entrantes pour le Serveur• entrantes, sortantes pour l'Agent• sortantes pour l'ordinateur sur lequel le Centre de gestion est ouvert	Pour le fonctionnement de l'Installateur réseau.
	UDP	entrantes, sortantes	
9080	HTTP	<ul style="list-style-type: none">• entrantes pour le Serveur• sortantes pour l'ordinateur sur lequel le Centre de gestion est ouvert	Pour le fonctionnement du Centre de gestion de la sécurité Dr.Web.
9081	HTTPS		Pour l'utilitaire de diagnostic à distance du Serveur.
10101	TCP		
80	HTTP	sortantes	Pour obtenir des mises à jour depuis SGM.
443	HTTPS		




Notez que le port 2371 a été utilisé dans les Serveurs de la version 4 pour assurer la connexion des composants antivirus au Serveur. Dans la version 10, ce port n'est plus supporté.

Le fonctionnement du Serveur Dr.Web requiert :

Composant	Pré-requis
CPU et système d'exploitation	<p>Les OS suivants avec le CPU correspondant sont supportés :</p> <ul style="list-style-type: none">• CPU supportant les instructions SSE2 et ayant la fréquence d'horloge de 1,3 Ghz et plus :<ul style="list-style-type: none">▫ OS Windows ;▫ OS Linux ;▫ OS FreeBSD ;▫ OS Solaris x86.• CPU V9 UltraSPARC IIIi ou supérieur :<ul style="list-style-type: none">▫ OS Solaris Sparc. <p>La liste complète des OS supportés est fournie dans les Annexes, dans l'Annexe A.</p>
Mémoire vive	<ul style="list-style-type: none">• Pré-requis minimum : 1 Go.• Pré-requis recommandés : 2 Go et plus.



Composant	Pré-requis
Espace disque	<p>pas moins de 12 Go : jusqu'à 8 Go pour une base de données intégrée (répertoire d'installation) et jusqu'à 4 Go dans le répertoire système temporaire (pour le fonctionnement des fichiers).</p> <p>En fonction des paramètres du Serveur l'espace supplémentaire peut être requis pour la sauvegarde des fichiers temporaires, par exemple pour la sauvegarde des packages personnels d'installation des Agents (environ 8,5 Mo chacun) dans le sous-répertoire <code>var\installers-cache</code> du répertoire d'installation du Serveur Dr.Web.</p> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 10px;"> Pour installer le Serveur, il est nécessaire que le disque système pour Windows ou <code>/var/tmp</code> pour les OS de la famille UNIX (ou un autre dossier pour les fichiers temporaire s'il est spécifié) ait au moins 1,2 Go pour la distribution générale et au moins 2,5 Go pour la distribution supplémentaire pour lancer l'installateur et décompresser les fichiers temporaires (quel que soit le disque d'installation du Serveur).</div>
Autre	<p>Pour l'installation du Serveur Dr.Web sous les OS de la famille UNIX, les bibliothèques suivantes sont requises : <code>lsb</code> en version 3 ou supérieure, <code>glibc</code> en version 2.7 ou supérieure.</p> <p>Pour utiliser une BD PostgreSQL, la bibliothèque <code>libpq</code> est requise.</p> <p>Pour utiliser une BD Oracle, la bibliothèque <code>libaio</code> est requise.</p> <p>En plus, sous FreeBSD, la bibliothèque <code>compat-8x</code> est requise.</p>

Le fonctionnement du Serveur proxy Dr.Web requiert :

Composant	Pré-requis
CPU	Intel® Pentium® III 667 MHz ou plus.
Mémoire vive	pas moins de 1 Go.
Espace disque	pas moins de 1 Go.
Système d'exploitation	<ul style="list-style-type: none">• Windows ;• Linux ;• FreeBSD ;• Solaris. <p>La liste complète des OS supportés est fournie dans les Annexes, dans l'Annexe A.</p>
Autre	Pour l'installation du Serveur proxy sous les OS de la famille UNIX, les bibliothèques suivantes sont requises : <code>lsb</code> en version 3 ou supérieure.



Composant	Pré-requis
	En plus, sous FreeBSD , la bibliothèque <code>compat-8x</code> est requise.

Le Centre de gestion de la sécurité Dr.Web requiert :

a) Navigateur :

Navigateur	Support
Windows Internet Explore 8 et supérieur	Navigateurs supportés
Mozilla Firefox 25 et supérieur	
Google Chrome 30 et supérieur	
Opera® 10 et supérieur	Vous pouvez les utiliser mais le fonctionnement sous ces navigateurs web n'est pas garanti.
Safari® 4 et supérieur	

En cas d'utilisation du navigateur web Windows Internet Explorer, il faut prendre en compte les particularités suivantes :

- Le fonctionnement complet du Centre de gestion sous le navigateur web Windows Internet Explorer avec le mode activé **Enhanced Security Configuration for Windows Internet Explorer** n'est pas garanti.
- Si vous installez le Serveur sur un ordinateur comportant le symbole « _ » (souligné) dans son nom, la configuration du Serveur via le Centre de gestion n'est pas possible. Dans ce cas, utilisez un autre navigateur web.
- Pour le fonctionnement correct du Centre de gestion, l'adresse IP et/ou le nom DNS de l'ordinateur sur lequel est installé le Serveur Dr.Web doivent être ajoutés à la liste des sites de confiance du navigateur web dans lequel vous ouvrez le Centre de gestion.
- Pour une ouverture correcte du Centre de gestion via le menu **Démarrer** sous Windows 8 et Windows Server 2012 avec une interface en mosaïque, configurez le navigateur web de manière suivante : **Options Internet** → **Programmes** → **Ouvrir Internet Explorer** cochez la case **Toujours dans Internet Explorer sur le Bureau**.

b) L'installation de extension pour le Centre de gestion de la sécurité Dr.Web est requise pour le fonctionnement complet du Centre de gestion. L'extension est fournie avec la distribution du Serveur. Elle s'installe sur requête du navigateur lorsque vous utilisez des éléments du Centre de gestion qui requièrent l'extension (par exemple, pour le Scanner réseau lors de l'installation à distance de composants antivirus).

L'installation de l'extension est possible uniquement dans les navigateurs suivants :



Navigateur	Version minimale supportée	Version maximale supportée
Windows Internet Explorer	8	11
Mozilla Firefox	25	50.0.1
Google Chrome	30	44.0.2403



Pour le fonctionnement de l'extension pour le Centre de gestion de la sécurité Dr.Web sur la page du Scanner réseau, sous Windows et GNU/Linux, les droits administrateur (root) sont requis.

Lorsque vous utilisez les navigateurs web Mozilla Firefox et Google Chrome, l'extension pour le Centre de gestion de la sécurité Dr.Web est disponible uniquement pour les versions tournant sous l'OS Windows ou sous les OS de la famille Linux.

c) La résolution d'écran recommandée pour utiliser le Centre de gestion est 1280x1024 pt.

Le Centre de gestion Mobile Dr.Web requiert :

Les pré-requis varient en fonction du système d'exploitation sur lequel l'application est installée :

Système d'exploitation	Pré-requis	
	Version du système d'exploitation	Appareil
iOS	iOS® 7 et supérieur	Apple® iPhone® Apple® iPad®
Android	Android 4.0 et supérieur	–

Pré-requis pour NAP :

Pour le serveur :

- OS Windows Server 2008.

Pour les agents :

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



Le fonctionnement de l'Agent Dr.Web et du package antivirus complet requiert :

Les pré-requis varient en fonction du système d'exploitation sur lequel l'application est installée (voir la liste complète des OS supportés dans les **Annexes**, l'[Annexe A. Liste complète des OS supportés](#)) :

- OS Windows :

Composant	Pré-requis
CPU	CPU ayant la fréquence d'horloge de 1 Ghz et plus.
Mémoire vive libre	Au moins 512 Mo.
Espace disque libre	Pas moins de 1 Mo pour les fichiers exécutables + espace disque supplémentaire pour les journaux et les fichiers temporaires.
Autre	<ol style="list-style-type: none">1. Pour le fonctionnement correct, l'Aide de l'Agent Dr.Web pour Windows requiert Windows® Internet Explorer® 6.0 ou supérieur.2. Pour le plug-in Dr.Web pour Outlook l'installation du client Microsoft Outlook inclus dans Microsoft Office est requise :<ul style="list-style-type: none">• Outlook 2000 ;• Outlook 2002 ;• Outlook 2003 ;• Outlook 2007 ;• Outlook 2010 SP2 ;• Outlook 2013 ;• Outlook 2016.

- OS de la famille Linux :

Composant	Pré-requis
CPU	Processeurs supportés avec architecture et système de commandes Intel/AMD : 32 bits (IA-32, x86) ; 64 bits (x86-64, x64, amd64).
Mémoire vive libre	Au moins 512 Mo.
Espace disque libre	Au moins de 400 Mo d'espace disque libre sur le volume qui contient les répertoires de l'Antivirus.

- OS X, OS Android, OS Novell NetWare : les pré-requis pour la configuration correspondent aux pré-requis pour le système d'exploitation.



Aucun autre logiciel antivirus (y compris d'autres versions de Dr.Web) ne doit être installé sur les postes dans le réseau antivirus géré par Dr.Web.



Les fonctionnalités des Agents sur les sont décrites dans le Manuel Utilisateur pour les OS correspondants.

1.4. Kit de distribution

La distribution Dr.Web Enterprise Security Suite est fournie en fonction de OS du Serveur Dr.Web sélectionné :

1. Pour les OS de la famille UNIX – sous forme de fichiers au format `run` :

Nom de package	Composant
<code>drweb-esuite-server-10.01.0-<assemblage>-<version_de_l'OS>.run</code>	Distribution principale du Serveur Dr.Web
<code>drweb-esuite-extra-10.01.0-<assemblage>-<version_de_l'OS>.run</code>	Distribution supplémentaire du Serveur Dr.Web
<code>drweb-esuite-proxy-10.01.0-<assemblage>-<version_de_l'OS>.run</code>	Serveur proxy

2. Pour OS Windows — sous forme de fichiers exécutables :

Nom de package	Composant
<code>drweb-esuite-server-10.01.0-<assemblage>-<version_de_l'OS>.exe</code>	Distribution principale du Serveur Dr.Web
<code>drweb-esuite-extra-10.01.0-<assemblage>-<version_de_l'OS>.exe</code>	Distribution supplémentaire du Serveur Dr.Web
<code>drweb-esuite-proxy-10.01.0-<assemblage>-<version_de_l'OS>.msi</code>	Serveur proxy
<code>drweb-esuite-agent-activedirectory-10.01.0-<assemblage>.msi</code>	Agent Dr.Web pour Active Directory
<code>drweb-esuite-modify-ad-schema-10.01.0-<assemblage>-<version_de_l'OS>.exe</code>	Utilitaire de la modification du schéma Active Directory
<code>drweb-esuite-aduac-10.01.0-<assemblage>-<version_de_l'OS>.msi</code>	Utilitaire de la modification des attributs des objets Active Directory
<code>drweb-esuite-napshv-10.01.0-<assemblage>-<version_de_l'OS>.msi</code>	NAP Validator
<code>drweb-esuite-agent-full-11.00.0-<version_de_l'assemblage>-windows.exe</code>	Installateur complet de l'Agent Dr.Web. Inclus dans la distribution



Nom de package	Composant
	supplémentaire du Serveur Dr.Web.

Le kit de distribution du Serveur Dr.Web contient deux packages :

1. *Distribution principale* – distribution de base pour installer le Serveur Dr.Web. Son contenu est identique à celui des précédentes versions de Dr.Web Enterprise Security Suite.

Depuis la distribution principale s'effectue l'installation du Serveur Dr.Web, contenant les packages de la protection antivirus uniquement pour les postes tournant sous l'OS Windows.

2. *Distribution supplémentaire (extra)* – inclut les distributions de tous les produits entreprises fournis pour être installés sur les postes protégés sous tous les OS supportés.

La distribution est installée comme un package supplémentaire sur un ordinateur sur lequel est installé la distribution principale du Serveur Dr.Web.



La distribution supplémentaire doit être installée depuis le package du même type que la distribution principale.

La distribution principale du Serveur Dr.Web contient les composants suivants :

- Logiciel du Serveur Dr.Web pour l'OS correspondant,
- Logiciel des Agents Dr.Web et des packages antivirus pour les postes sous OS Windows,
- Logiciel du Centre de gestion de la sécurité Dr.Web,
- bases virales,
- Extension pour le Centre de gestion de la sécurité Dr.Web,
- Extension Dr.Web Server FrontDoor,
- documentation, modèles, exemples.

Outre la distribution, les numéros de série seront également fournis. Après les avoir enregistrés, vous recevrez les fichiers contenant les clés.



Chapitre 2. Licence

Le fonctionnement de la solution antivirus Dr.Web Enterprise Security Suite nécessite une licence.

Le contenu et le prix de la licence pour l'utilisation de Dr.Web Enterprise Security Suite dépendent du nombre de postes protégés y compris les serveurs inclus dans le réseau Dr.Web Enterprise Security Suite et qui tournent comme postes protégés.



Signalez cette information au vendeur de licence au moment de l'achat de Enterprise Security Suite Dr.Web. Le nombre de Serveurs Dr.Web utilisés n'influence pas le prix de la licence.

Fichier clé de licence

Les droits de l'utilisateur relatifs à l'utilisation de Dr.Web Enterprise Security Suite sont déterminés par les fichiers clés de licence.



Le format de 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.

Les fichiers clés de licence sont fournis sous forme d'une archive zip contenant un ou plusieurs fichiers clés pour les postes à protéger.

L'utilisateur peut obtenir les fichiers clés de licence par l'un des moyens suivants :

- Le fichier clé de licence est inclus dans le package de l'antivirus Dr.Web Enterprise Security Suite au moment de l'achat, s'il a été inclus dans la distribution. Mais d'habitude seuls les numéros de série sont fournis.
- Le fichier clé de licence est envoyé aux utilisateurs par e-mail après l'enregistrement du numéro de série sur le site web de Doctor Web (<http://products.drweb.com/register>, sauf indication contraire spécifiée dans la carte d'enregistrement du produit). Veuillez visiter le site indiqué pour remplir un formulaire où vous devez spécifier quelques informations personnelles et saisir dans le champ approprié le numéro de série (vous le trouverez sur la carte produit). Une archive contenant vos fichiers clés vous sera envoyée à l'adresse que vous avez spécifiée. Vous pourrez également télécharger les fichiers clés directement sur le site mentionné ci-dessus.
- Le fichier clé de licence peut être fourni sur un support à part.

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 de licence, vous pouvez repasser la procédure d'enregistrement sur le site et obtenir le fichier clé de licence de nouveau. 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 e-mail peut être modifiée. Si c'est le cas, le fichier clé sera envoyé à la nouvelle adresse e-mail.



Pour tester l'Antivirus, vous pouvez utiliser des 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 qui se trouve sur la page suivante <https://download.drweb.com/demoreq/biz/>. 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 de licence lors de l'installation du programme est décrite dans le **Manuel d'installation**, p. [Installer le Serveur Dr.Web](#).

L'utilisation des fichiers clés de licence pour un réseau antivirus déjà déployé est décrite en détails dans le p. [Gestionnaire de licences](#).

2.1. Politique de Licencing

1. Le Serveur Dr.Web n'est pas soumis à licence.



L'IDUU du Serveur, qui a été stocké dans une clé de licence du Serveur dans les versions précédentes de Dr.Web Enterprise Security Suite, maintenant est sauvegardé dans le fichier de configuration du Serveur (à partir de la version 10).

- Lors de l'installation d'un nouveau Serveur, un nouveau UUID est généré.
- Durant la mise à niveau du Serveur depuis des versions antérieures, l'IDUU est récupéré automatiquement de la clé du Serveur de la précédente version (fichier `enterprise.key` dans le répertoire `etc` de l'installation précédente du Serveur) et écrite dans le fichier de configuration du Serveur installé.

Lors de la mise à jour du cluster des Serveurs, le Serveur responsable de la mise à jour de la BD obtient une clé de licence. Pour les autres Serveurs, il est nécessaire d'ajouter les clés de licence manuellement.

2. Les clés de licence sont valables uniquement pour les postes protégés. Vous pouvez assigner une licence à des postes particuliers ou à des groupes de postes : dans ce cas, une clé de licence est valide pour tous les postes qui l'héritent de ce groupe. Pour assigner un fichier clé en même temps pour tous les postes du réseau antivirus pour lesquels aucun paramètre personnalisé de la clé de licence n'est spécifié, assignez la clé de licence au groupe **Everyone**.
3. Le fichier clé de licence peut être spécifié durant l'installation du Serveur Dr.Web (voir le **Manuel d'installation**, p. [Installer le Serveur Dr.Web](#)).
Pourtant, le Serveur peut être installé sans clé de licence. La licence peut être ajoutée plus tard localement ou via la communication inter-serveurs.
4. Via la communication inter serveurs, un nombre optionnel de licences récupérées des clés d'un Serveur peuvent être distribuées à un Serveur voisin pour une durée déterminée.
5. Il est possible d'utiliser plusieurs licences différentes, par exemple les licences aux durées de validité différentes ou les licences avec les ensembles différents des composants antivirus pour les postes à protéger. Chaque clé de licence peut être assignée en même temps à plu-



sieurs objets soumis à licence (groupes et postes). Plusieurs clés de licence peuvent être assignées simultanément à un objet soumis à licence.

6. Si vous assignez plusieurs clés à un seul objet, prenez en considération les particularités suivantes :
 - a) Si les listes des composants antivirus autorisés dans plusieurs clés d'un seul poste diffèrent, la liste des composants autorisés pour ce poste est définie d'après le croisement des jeux de composants assignés aux clés. Par ex, si une clé avec l'Antispam et une clé sans l'Antispam sont assignées à un groupe de postes, l'Antispam ne peut pas être installé sur les postes.
 - b) Les paramètres de licencing d'un objet sont définis d'après toutes les clés assignées à cet objet. Si les dates d'expiration des clés diffèrent, une fois que la date d'expiration la plus proche est passée, vous devez remplacer ou supprimer manuellement la clé qui a expiré. Si l'expiration d'une clé empêche l'installation de composants antivirus, il est nécessaire de modifier les paramètres de licencing de l'objet à l'onglet **Composants à installer**.
 - c) Le nombre de licence de l'objet est calculé en fonction de la somme de licences de toutes les clés assignées pour cet objet. Il faut également prendre en compte la possibilité de transmission de licences au Serveur voisin via la communication inter-serveurs (voir p. 4). Dans ce cas, les licences transmises au Serveur voisin sont déduites du nombre total de licences.



Les clés de licence sont gérées via le [Gestionnaire de licences](#).

Quand vous spécifiez la clé de licence dans le Gestionnaire de licences, toutes les informations sur cette licence sont enregistrées dans la base de données.

2.2. Mise à jour automatique de licences

La licence pour Dr.Web Enterprise Security Suite ne peut pas être mise à jour automatiquement.

La mise à jour automatique de licences comprend les aspects suivants :

- À l'expiration de la clé de licence, elle peut être remplacée automatiquement par une clé de licence achetée d'avance.
- La mise à jour automatique s'effectue pour une clé de licence particulière pour laquelle a été acheté le renouvellement.
- La clé de licence pour la mise à jour automatique se trouve sur les serveurs de Doctor Web jusqu'à l'expiration de la clé de licence qui doit être renouvelé.
- Vous pouvez vérifier la disponibilité de la mise à jour automatique (la présence de la clé de licence sur les serveurs de Doctor Web) et effectuer la mise à jour lors de l'exécution de la tâche **Expiration de la clé de licence** de la planification du Serveur Dr.Web.



Si la tâche **Expiration de la clé de licence** est désactivée dans la planification du Serveur, la mise à jour automatique de la licence est impossible.

Pour lancer la tâche, il faut accomplir les conditions suivantes :



- La licence actuelle va expirer (le nombre de jours avant l'expiration est spécifié dans les paramètres de la tâche).
- La licence actuelle appartient à ce Serveur : initialement, elle a été ajoutée manuellement ou obtenue lors de la mise à jour automatique. Les licences obtenues des Serveurs voisins par les liaisons entre serveurs ne sont pas mises à jour automatiquement via la tâche de la planification du Serveur.

Mise à jour automatique des licences selon la planification

Après l'exécution de la tâche **Expiration de la clé de licence**, vous pouvez obtenir les résultats suivants :

1. *La mise à jour automatique de la licence n'est pas disponible.*

Une notification **Expiration de la clé de licence** est envoyée à l'administrateur.

2. *La mise à jour automatique de la licence est disponible. Les composants soumis à licence de la clé actuelle sont différents de ceux de la nouvelle clé (la nouvelle clé n'a pas quelques composants qui sont présents dans la clé actuelle) ou bien, la nouvelle clé a moins de licences que la clé de licence actuelle.*

La nouvelle clé est téléchargée depuis les serveurs de Doctor Web, elle est ajoutée dans le Gestionnaire de licences et la base de données du Serveur et elle est diffusée sur les objets de licence. Dans ce cas, il est nécessaire de diffuser la clé de licence manuellement.

Une notification **La clé de licence ne peut pas être mise à jour automatiquement** est envoyée à l'administrateur. La raison pour laquelle la clé ne peut pas être diffusée automatiquement sera mentionnée dans la notification.

3. *La mise à jour automatique est disponible pour la licence. Les composants soumis à licence de la clé actuelle correspondent aux ceux de la nouvelle clé (ou la nouvelle clé a plus de composants que la clé actuelle y compris tous les composants de la clé actuelle), ou bien, le nombre de licences de la nouvelle clé est supérieur ou égal au nombre de licences de la clé actuelle.*

La nouvelle clé est téléchargée depuis les serveurs de Doctor Web, elle est ajoutée dans le Gestionnaire de licences et la base de données du Serveur et elle est diffusée sur tous les objets de licence sur lesquels a été diffusée la licence précédente, y compris les Serveurs voisins.

L'ancienne licence sera supprimée quand elle ne sera utilisée par aucun Serveur subordonné. Dans ce cas, si au moment de la mise à jour automatique le Serveur subordonné a été déconnecté, l'ancienne licence sera stockée jusqu'à la connexion du Serveur subordonné.

L'ancienne licence est stockée jusqu'à ce que l'on supprime manuellement dans les cas suivants :

- S'il est impossible de diffuser sur le Serveur subordonné la licence obtenue lors de la mise à jour automatique (le Serveur est déconnecté pour toujours).
- Si le Serveur subordonné utilise la version de protocole qui ne supporte pas les mises à jour automatiques. Dans ce cas, les licences seront transmises sur le Serveurs subordonné mais elles ne seront pas diffusées.



Une notification **La clé de licence est mise à jour automatiquement** est envoyée à l'administrateur. La notification de mise à jour sera envoyée depuis tous les Serveurs sur lesquels la nouvelle licence a été diffusée.



Toutes les notifications envoyées à l'administrateur sont configurées dans la section **Administration** → **Configuration des notifications**.

Après l'envoi de chaque notification, la [procédure utilisateur](#) **Mise à jour automatique de la clé de licence** est exécutée.

Mise à jour manuelle des licences

Si vous avez acheté une clé de licence pour la mise à jour automatique de votre clé de licence actuelle, alors l'ajout manuel de la nouvelle clé dans le Gestionnaire de tâches n'est pas requis. En fonction de la situation (l'option 2 de la procédure ci-dessus), seule la diffusion manuelle sur les objets de licence peut être requise.

Pourtant, si, avant d'exécuter la tâche **Expiration de la clé de licence**, vous avez ajouté dans le Gestionnaire de licences une nouvelle clé nécessitant la mise à jour automatique conformément à l'option 3 (voir la procédure ci-dessus), alors seule la diffusion automatique de la nouvelle clé de licence sera effectuée lors de l'exécution de la tâche. Dans ce cas, les options suivantes sont possibles :

- a) La nouvelle clé a été diffusée manuellement sur tous les objets sur lesquels a été diffusée la clé précédente (mise à jour). Dans ce cas, aucune modification ne sera apportée lors de l'exécution de la tâche.
- b) La nouvelle clé a été diffusée manuellement, mais pas sur tous les objets sur lesquels a été diffusée la clé précédente (mise à jour). Dans ce cas, lors de l'exécution de la tâche, la nouvelle clé sera diffusée sur tous les objets restants de la clé précédente qui n'ont pas été encore mis à jour.

Si la nouvelle clé de licence a été diffusée manuellement sur les objets qui ne sont pas présents dans la liste de la clé précédente, alors, après l'exécution de la tâche, la nouvelle clé sera toujours diffusée sur ces objets. Dans ce cas, les options suivantes sont possibles :

- La quantité de licences est suffisante pour tous les objets de licence : pour ceux qui appartiennent à la clé précédente et pour ceux qui sont assignés manuellement à la nouvelle clé. Cette situation est possible si la nouvelle clé a plus de licences. Dans ce cas, aucune modification ne sera apportée lors de l'exécution de la tâche.
- La quantité de licences n'est pas suffisante pour la diffusion sur tous les objets de licence de la clé précédente car les licences ont été assignées manuellement aux autres objets. Les objets qui n'ont pas eu de licence ne seront pas mis à jour, pourtant la clé précédente sera supprimée et ces objets resteront sans licence. En cas d'apparition de licences libres, les objets qui n'ont pas eu de licences recevront une nouvelle clé de licence. Dans ce cas, l'action dépend du type d'objets de licence :
 - Si ce sont les postes de ce Serveur qui n'ont pas eu de licences de la nouvelle clé, alors la disponibilité de nouvelles licences sera vérifiée à chaque tentative de connexion au



Serveur. Si une licence disponible est détectée au moment de la connexion du poste, elle sera accordée au poste.

- Si ce sont les Serveurs voisins qui n'ont pas eu de licences de la nouvelle clé, alors la disponibilité de nouvelles licences sera vérifiée automatiquement environ une fois par minute. En cas de disponibilité de licences libres, elles seront remises aux Serveurs voisins.

Fichier clé de licence

Notez les particularités suivantes des fichiers clé de licence lors de la mise à jour automatique :

- En cas de la mise à jour automatique, la nouvelle licence est téléchargée depuis les serveurs de Doctor Web, les informations sur cette licence sont stockées dans la base de données du Serveur et affichées dans le Gestionnaire de licences. Dans ce cas, le fichier clé de licence n'est pas créé.
- Pour obtenir un fichier clé de licence, utilisez l'option **Administration** → **Gestionnaire de licences** → **Exporter la clé**. Vous pouvez également obtenir le fichier clé de licence lors de l'exécution de la procédure utilisateur **Mise à jour automatique de la clé de licence**.
- En cas de suppression de la licence, les informations sur cette licence sont supprimées du Gestionnaire de licences et de la base de données du Serveur, pourtant le fichier clé de licence reste dans le répertoire du Serveur.



Chapitre 3. Mise en route

3.1. Création d'un réseau antivirus

Brève instruction de déploiement d'un réseau antivirus :

1. Rédigez un plan de la structure du réseau antivirus. Le plan doit comprendre tous les postes et les appareils mobiles à protéger.

Sélectionnez l'ordinateur qui va accomplir les fonctions du Serveur Dr.Web. Le réseau antivirus peut comprendre plusieurs Serveurs Dr.Web. Les particularités d'une telle configuration sont décrites dans le p. [Particularités du réseau avec plusieurs Serveurs Dr.Web](#).



Le Serveur Dr.Web peut être installé sur n'importe quel ordinateur et pas uniquement sur la poste utilisé comme serveur LAN. Pour en savoir plus sur les pré-requis principaux, consultez le paragraphe [Pré-requis système](#).

La même version de l'Agent Dr.Web est installée sur tous les postes protégés, y compris les serveurs LAN. La différence consiste en la liste des composants antivirus installés spécifiée par les paramètres sur le Serveur.

Pour installer le Serveur Dr.Web et l'Agent Dr.Web 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 Dr.Web ni aux postes de travail.

2. Déterminez les produits à installer sur les noeuds du réseau en fonction du plan rédigé. Pour en savoir plus sur les produits fournis, consultez la rubrique [Kit de distribution](#).

Vous pouvez acheter tous les produits nécessaires en boîte Dr.Web Enterprise Security Suite ou les télécharger sur les site de Doctor Web <https://download.drweb.fr>.



Les Agents Dr.Web pour le poste sous OS Android, OS Linux peuvent également être installés depuis les packages pour les produits autonomes et connectés plus tard au Serveur centralisé Dr.Web. Vous pouvez consulter la description des paramètres correspondants des Agents dans le **Manuel d'installation**, le p. [Installation de l'Agent Dr.Web avec le package d'installation personnel](#).

3. Installez la distribution principale du Serveur Dr.Web sur un ou plusieurs ordinateurs. L'installation est décrite dans le **Manuel d'installation**, le p. [Installation du Serveur Dr.Web](#).

Le Centre de gestion de la sécurité Dr.Web est installé avec le Serveur.

Par défaut, le Serveur Dr.Web démarre de manière automatique après l'installation et après chaque redémarrage du système.

4. Si le réseau antivirus inclut les postes protégés sous OS Android, OS Linux, OS X, installez la distribution supplémentaire du Serveur Dr.Web sur tous les ordinateurs sur lesquels la distribution principale du Serveur est installée.



5. Si nécessaire, installez et configurez le Serveur proxy. Vous pouvez consulter la description dans le **Manuel d'installation**, le p. [Installation du Serveur proxy](#).
6. Pour configurer le Serveur et le logiciel antivirus sur les postes, il faut se connecter au Serveur depuis le Centre de gestion de la sécurité Dr.Web.



Le Centre de gestion peut être ouvert sur n'importe quel ordinateur et pas uniquement sur celui sur lequel est installé le Serveur. Une connexion réseau doit être établie avec l'ordinateur sur lequel le Serveur est installé.

Le Centre de gestion est accessible à l'adresse suivante :

`http://<adresse_Serveur>:9080`

ou

`https://<adresse_Serveur>:9081`

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

Dans la boîte de dialogue d'authentification, entrez le login et le mot de passe administrateur.

Le login de l'administrateur est **admin** par défaut.

Mot de passe :

- sous Windows – le mot de passe a été spécifié lors de l'installation du Serveur.
- sous les OS de la famille UNIX – **root**.



Pour le Serveur sous les OS de la famille UNIX, changez de mot de passe d'administrateur à la première connexion au Serveur.

Si la connexion au Serveur est établie, la fenêtre principale du Centre de gestion va s'ouvrir (pour en savoir plus, consultez le p. [Centre de gestion de la sécurité Dr.Web](#)).

7. Effectuez la configuration initiale du Serveur (vous pouvez consulter la description détaillée des paramètres du Serveur dans le [Chapitre 8 : Configuration du Serveur Dr.Web](#)) :
 - a. Dans la rubrique [Gestionnaire de licences](#), ajoutez une ou plusieurs clés de licence et diffusez-les sur les groupes correspondants, notamment sur le groupe **Everyone**. Cette étape est obligatoire si la clé de licence n'a pas été spécifiée lors de l'installation du Serveur.
 - b. Dans la rubrique [Configuration générale du dépôt](#), spécifiez les composants du réseau antivirus à mettre à jour depuis le SGM Dr.Web. Dans la rubrique [Statut du dépôt](#) effectuez la mise à jour des produits du dépôt du Serveur. La mise à jour peut prendre un long temps. Attendez la fin de la mise à jour avant de continuer la configuration.
 - c. Vous trouverez les informations sur la version du Serveur sur la page **Administration** → **Serveur Dr.Web**. Si la nouvelle version est disponible, mettez à jour le Serveur. La procédure est décrite dans le p. [Mise à jour du Serveur Dr.Web et restauration depuis une copie de sauvegarde](#).
 - d. Si nécessaire, configurez les [Connexions réseau](#) pour modifier les paramètres réseau spécifiés par défaut et utilisés pour l'interaction de tous les composants du réseau antivirus.



- e. Si nécessaire, configurez la liste d'administrateurs du Serveur. L'authentification externe des administrateurs est également possible. Pour en savoir plus, consultez le [Chapitre 5 : Administrateurs du réseau antivirus](#).
 - f. Avant d'utiliser l'antivirus, il est recommandé de modifier la configuration du répertoire de sauvegarde des données critiques du Serveur (voir le le p. [Configuration de la planification du Serveur Dr.Web](#)). 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.
8. Spécifiez les paramètres et la configuration du logiciel antivirus pour les postes de travail (vous pouvez consulter la description détaillée de la configuration de groupes et de postes dans le [Chapitre 6](#) et la [Chapitre 7](#)) :
- a. Si nécessaire, créez les groupes utilisateur de postes.
 - b. Spécifiez les paramètres du groupe **Everyone** et des groupes utilisateur créés. Notamment configurez la rubrique des composants à installer.
9. Installez le logiciel de l'Agent Dr.Web sur les postes de travail.

Dans la rubrique [Fichiers d'installation](#), consultez la liste des fichiers fournis pour l'installation de l'Agent. Sélectionnez le type d'installation en fonction du système d'exploitation du poste, la possibilité de l'installation à distance, la configuration du Serveur lors de l'installation de l'Agent, etc. Par exemple :

- Si les utilisateurs installent l'antivirus eux-mêmes, utilisez les packages d'installation personnels qui sont créés via le Centre de gestion séparément pour chaque poste. Vous pouvez envoyer aux utilisateurs des e-mails avec ce type de package directement du Centre de gestion. Après l'installation, les postes se connectent automatiquement au Serveur.
 - Utilisez l'installateur réseau pour l'installation à distance sur un ou plusieurs postes (uniquement pour les postes tournant sous Windows). L'installation s'effectue via le Centre de gestion à l'aide d'une extension pour le navigateur.
 - Il est également possible d'installer l'antivirus à distance par réseau à l'aide du service Active Directory sur un ou plusieurs postes en même temps. Pour ce faire, il faut utiliser l'installateur de l'Agent Dr.Web pour les réseaux Active Directory fourni avec la distribution Dr.Web Enterprise Security Suite, mais séparément de l'installateur du Serveur.
 - Si, lors de l'installation, il faut diminuer la charge sur le canal de communication entre le Serveur et les postes, vous pouvez utiliser l'installateur complet qui effectue l'installation de l'Agent et des composants de protection en même temps.
 - Installation sur les postes sous OS Android, OS Linux et OS X peut s'effectuer de manière locale conformément aux règles générales. Le produit autonome installé peut se connecter au Serveur conformément à la configuration correspondante.
10. 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 (les paramètres sont décrits dans le p. [Politique de connexion des postes](#)) :
- a. En cas d'installation depuis les packages d'installation et la configuration de l'approbation automatique sur le Serveur, les postes de travail sont enregistrés automatiquement à la première connexion au Serveur et l'approbation supplémentaire n'est pas requise.



- b. En cas d'installation depuis les installateurs et la configuration de l'approbation manuelle, l'administrateur doit approuver manuellement de nouveaux postes pour les enregistrer sur le Serveur. Dans ce cas, les nouveaux postes ne se connectent pas automatiquement, mais ils sont déplacés par le Serveur dans le groupe de novices.
11. Après la connexion au Serveur et l'obtention des paramètres, l'ensemble des composants du package antivirus est installé sur le poste. Cet ensemble est spécifié dans les paramètres du groupe primaire du poste.



Pour terminer l'installation des composants sur le poste, le redémarrage de l'ordinateur est requis.

12. La configuration des postes et du logiciel antivirus est également possible après l'installation (vous pouvez consulter la description détaillée dans le [Chapitre 7](#)).

3.2. Configuration des connexions réseau

Généralités

Les clients suivants se connectent au Serveur Dr.Web :

- Agent Dr.Web,
- Installateurs des Agents Dr.Web,
- autres Serveurs Dr.Web.

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), 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 le Serveur Dr.Web vers un autre ordinateur ou changer d'adresse IP de l'ordinateur sur lequel est installé le Serveur.

3. Via le [Protocole SRV](#).

Cette approche permet de rechercher un Serveur par le nom d'un ordinateur ou le service de Serveur via les enregistrements SRV sur le serveur DNS.

Si le réseau antivirus Dr.Web Enterprise Security Suite 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 **Groupe Multicast** (**Administration** → **Configuration du Serveur Dr.Web** → onglet **Réseau** → onglet **Transport**).



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.

Lors de l'installation du Serveur, l'installateur ajoute automatiquement les ports et les interfaces du Serveurs dans les exceptions du pare-feu Windows.

En cas d'utilisation d'un autre pare-feu que celui de Windows, l'administrateur du réseau antivirus doit configurer manuellement les paramètres concernés.

3.2.1. Connexions directes

Configuration du Serveur Dr.Web

Dans la configuration du Serveur, il doit être spécifié quelle adresse (voir les **Annexes**, p. [Annexe E. Spécification des adresses réseau](#)) est à écouter pour réceptionner les connexions TCP entrantes.

Vous pouvez configurer ce paramètre dans la configuration du Serveur : **Administration** → **Configuration du Serveur Dr.Web** → onglet **Réseau** → onglet **Transport** → champ **Adresse**.

Les paramètres suivants sont définis par défaut pour l'écoute par le Serveur :

- **Adresse** : valeur vide – utiliser *toutes les interfaces réseau* pour cet ordinateur sur lequel le Serveur est installé.
- **Port** : 2193 – utiliser le port 2193 enregistré pour Dr.Web Enterprise Security Suite dans IANA.



Notez que le port 2371 a été utilisé dans la version 4 du Serveur. Dans la version 10, ce port n'est plus supporté.

Pour assurer le fonctionnement correct du réseau antivirus Dr.Web Enterprise Security Suite, il suffit que le Serveur « soit à l'écoute » d'au moins un port TCP qui doit être connu de tous les clients.

Configuration de l'Agent Dr.Web

Lors de l'installation de l'Agent, l'adresse du Serveur (l'adresse IP ou le nom DNS de l'ordinateur sur laquelle le Serveur Dr.Web est lancé) peut être indiquée directement dans les paramètres d'installation :

```
drwinst <Adresse_Serveur>
```

Pour l'installation de l'Agent, il est recommandé d'utiliser le nom du Serveur enregistré dans le service DNS. Ceci facilite le processus de configuration du réseau antivirus relatif à la procédure de réinstallation du Serveur Dr.Web sur un autre ordinateur.



Par défaut, la commande `drwinst`, lancée sans paramètres, va scanner le réseau pour rechercher les Serveurs Dr.Web et tenter d'installer l'Agent depuis le premier Serveur trouvé dans le réseau (mode *Multicasting* utilisant le [Service de détection de Serveur](#)).

Ainsi, l'adresse du Serveur Dr.Web est connue par l'Agent lors de l'installation.

Ultérieurement, l'adresse du Serveur peut être modifiée manuellement dans les paramètres de l'Agent.

3.2.2. Service de détection du Serveur Dr.Web

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 sera effectuée. Pour cela, le client envoie une requête broadcast et attend une réponse contenant l'adresse du Serveur. Dès que la réponse est réceptionnée, le client établit une connexion au Serveur.

Pour réaliser la procédure, le Serveur doit "écouter" le réseau pour réceptionner les requêtes envoyées.

Plusieurs variantes de configuration de ce schéma sont possibles. Le plus important est que la méthode de recherche du Serveur configurée pour les clients corresponde à la configuration de réponse du Serveur.

Dr.Web Enterprise Security Suite utilise par défaut le mode *Multicast over UDP* :

1. Le Serveur s'enregistre dans le groupe multicast avec une adresse spécifiée dans les paramètres du Serveur.
2. Les Agents lorsqu'ils recherchent le Serveur, envoient des requêtes multicast à l'adresse de groupe spécifiée à l'étape 1.

Le Serveur écoute par défaut (idem pour les connexions directes) : `udp/231.0.0.1:2193`.



Notez que le port 2371 a été utilisé dans les Serveurs de la version 4. Dans la version 10, ce port n'est plus supporté.

Ce paramètre est spécifié dans les paramètres du Centre de gestion **Administration** → **Configuration du Serveur Dr.Web** → onglet **Réseau** → onglet **Transport** → champ **Groupe Multicast**.

3.2.3. Utiliser le protocole SRV

Les clients sous Windows supportent le protocole réseau client SRV (une description du format est donnée dans les **Annexes**, p. [Annexe E. Spécification des adresses réseau](#)).

L'accès au Serveur via les enregistrements SRV est implémenté de la façon suivante :

1. Durant l'installation du Serveur, l'enregistrement dans le domaine Active Directory est paramétré, les registres d'installation correspondant à l'enregistrement SRV sur le serveur DNS.



L'enregistrement SRV est inscrit sur le serveur DNS selon le RFC2782 (voir <http://tools.ietf.org/html/rfc2782>).

2. Dans une requête pour la connexion au Serveur, le client spécifie que l'accès a lieu via le protocole `srv`.

Par exemple, le lancement de l'installateur de l'Agent :

- avec mention explicite du nom du service `myservice` :

```
drwinst /server "srv/myservice"
```
- sans mention du nom du service. Dans ce cas, le nom par défaut `drwcs` sera recherchée dans les entrées SRV

```
drwinst /server "srv/"
```

3. De manière transparente pour l'utilisateur, le client utilise le protocole SRV pour accéder au Serveur.



Si le Serveur n'est pas indiqué directement, la commande `drwcs` est utilisée par défaut comme nom du service.



Chapitre 4. Composants du réseau antivirus et leur interface

4.1. Serveur Dr.Web

Le réseau antivirus doit comprendre au moins un Serveur Dr.Web.



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

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

Fonctions clés

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



La base de données intégrée peut être utilisée lorsque le nombre de postes connectés au Serveur ne dépasse pas 200-300. Si l'ordinateur sur lequel est installé le Serveur Dr.Web 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 respecter les pré-requis minimum suivants :

- processeur 3GHz,
- mémoire vive – au moins 4 Go pour le Serveur Dr.Web, au moins 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.

Le Serveur Dr.Web 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](#).

Serveur Web

Le Serveur Web est une partie du Centre de gestion Dr.Web et fournit les fonctions générales suivantes :

- authentification et autorisation des administrateurs dans le Centre de gestion ;
- automatisation du fonctionnement des pages du Centre de gestion ;
- support des pages du Centre de gestion générées dynamiquement ;
- support des connexions clients HTTPS.

4.1.1. Gestion du Serveur Dr.Web sous OS Windows®

Interface et Gestion du Serveur Dr.Web

Le Serveur Dr.Web n'a pas d'interface intégrée. La gestion du Serveur Dr.Web est effectuée à l'aide du Centre de gestion qui sert de l'interface externe du Serveur.



Les éléments qui permettent de faciliter et de paramétrer la gestion du Serveur sont placés lors de l'installation du Serveur dans le répertoire **Serveur Dr.Web** du menu principal de Windows **Programmes** :

- Le répertoire **Gestion du Serveur** contient les commandes de démarrage, de redémarrage et d'arrêt du Serveur, ainsi que les commandes déterminant le mode de journalisation et d'autres commandes du Serveur décrites dans les **Annexes**, p. [H4. Serveur Dr.Web](#).
- 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.

Le répertoire d'installation du Serveur Dr.Web présente la structure suivante :

- `bin` – fichiers exécutables du Serveur Dr.Web.
- `etc` – fichiers des paramètres principaux des composants du réseau antivirus.
- `Installer` – installateur destiné à lancer le processus d'installation de l'Antivirus sur le poste à protéger ainsi que la clé de chiffrement publique (`drwcsd.pub`).
- `update-db` – scripts nécessaires à la mise à jour de la structure des bases de données du Serveur.
- `var` – le répertoire comprend les sous-répertoires suivants :
 - `es-dl-cache` – packages d'installation des utilisateurs pendant deux semaines après la création ;
 - `backup` – copies de sauvegarde de la BD et d'autres données critiques ;
 - `extensions` – 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, c'est l'utilisateur **LocalSystem**) ;
 - `templates` – masques de rapports.
- `webmin` – éléments du Centre de gestion de la sécurité Dr.Web : documentation, icônes, modules.



Le contenu du répertoire des mises à jour `\var\repository` est téléchargé depuis le serveur de mises à jour via le protocole HTTP/HTTPS, de manière automatique selon la planification spécifiée pour le Serveur. L'administrateur du réseau antivirus peut également placer des mises à jour dans ces répertoires manuellement.



Fichiers de configuration principaux

Fichier	Description	Répertoire par défaut
agent.key (le nom peut varier)	clé de licence de l'Agent	etc
certificate.pem	certificat SSL	
download.conf	paramètres réseau pour la génération de packages d'installation de l'Agent	
drwcsd.conf (le nom peut varier)	fichier de configuration du Serveur	
drwcsd.conf.distr	template du fichier de configuration du Serveur avec les paramètres par défaut	
drwcsd.pri	clé de chiffrement privée	
enterprise.key (le nom peut varier)	clé de licence du Serveur. La clé est sauvegardé uniquement si elle est présente après la mise à niveau depuis des versions antérieurs. Elle n'est pas présente en cas d'installation du nouveau Serveur 10	
frontdoor.conf	fichier de configuration pour l'utilitaire du diagnostic distant du Serveur	
http-alerter-certs.pem	certificats pour la vérification de l'hôte apple-notify.drweb.com pour l'envoi de notifications push	
private-key.pem	clé privée RSA	
webmin.conf	fichier de configuration du Centre de gestion	
auth-ads.xml	fichier de configuration pour l'authentification externe des administrateurs via Active Directory	
auth-ldap.xml	fichier de configuration pour l'authentification externe des administrateurs via LDAP	
auth-radius.xml	fichier de configuration pour l'authentification externe des administrateurs via RADIUS	
database.sqlite	BD intégrée	var
drwcsd.pub	clé de chiffrement publique	<ul style="list-style-type: none">• Installer• webmin\install





Démarrage et arrêt du Serveur Dr.Web

Par défaut, le Serveur Dr.Web démarre de manière automatique après l'installation et après chaque redémarrage du système.

Vous pouvez également démarrer, redémarrer ou arrêter le Serveur Dr.Web de l'une des façons suivantes :

- Cas général :
 - Avec la commande correspondante se trouvant dans le menu **Démarrer** → **Tous les programmes** → **Dr.Web 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 rubrique **Administration** : le redémarrage avec le bouton , l'arrêt avec le bouton .
- Avec les commandes de console exécutées depuis le sous-répertoire `bin` du répertoire d'installation du Serveur (voir aussi **Annexes**, p. [H4. Serveur Dr.Web](#)) :
 - `drwcsd start` — démarrage du Serveur.
 - `drwcsd restart` — redémarrage complet du service du Serveur.
 - `drwcsd stop` — arrêt normal du Serveur.



Pour que le Serveur lise les variables d'environnement, veuillez redémarrer le service avec les outils de gestion de services ou avec la commande de console.

4.1.2. Gestion du Serveur Dr.Web sous les OS de la famille UNIX®

Interface et Gestion du Serveur Dr.Web

Le Serveur Dr.Web n'a pas d'interface intégrée. La gestion du Serveur Dr.Web est effectuée à l'aide du Centre de gestion qui sert de l'interface externe du Serveur.

Le répertoire d'installation du Serveur Dr.Web présente la structure suivante :

`/opt/drwcs/` pour Linux, Solaris et `/usr/local/drwcs` pour FreeBSD :

- `bin` – fichiers exécutables du Serveur Dr.Web.
- `doc` – fichiers de contrats de licence.
- `ds-modules`
- `fonts` – polices pour l'interface du Centre de gestion.
- `Installer` – installateur réseau et clé de chiffrement publique pour installer l'Antivirus sur les postes protégés.



- `lib` – jeu de bibliothèques pour le fonctionnement du Serveur.
- `update-db` – scripts nécessaires à la mise à jour de la structure de la BD du Serveur.
- `webmin` – éléments du Centre de gestion de la sécurité Dr.Web.

`/var/opt/drwcs/` pour Linux, Solaris et `/var/drwcs` pour FreeBSD :

- `backup` – copies de sauvegarde de la BD et d'autres données critiques.
- `bases` – bases virales déballées pour la compatibilité ascendante avec les versions antérieures des Agents Dr.Web.
- `coredump` – les dumps de crash du Serveur.
- `database.sqlite` – base de données intégrée du Serveur.
- `etc` – fichiers de configuration générale des composants du réseau antivirus.
- `extensions` – scripts des procédures utilisateurs destinés à automatiser la performances de certaines tâches.
- `installers-cache` – installateurs de l'Agent en cache. Destinés à sauvegarder les packages d'installation de l'Agent lorsque les postes sont créés via le Centre de gestion.
- `log` – fichiers de journal du Serveur.
- `object` – objets du Centre de gestion en cache.
- `reports` – répertoire temporaire pour la création et la sauvegarde des rapports.
- `repository` – répertoire de dépôt pour sauvegarder les mises à jour en cours des bases virales, des fichiers de packages antivirus et des composants du réseau antivirus. Il contient des sous-dossiers pour les composants du logiciel incluant des sous-dossiers pour leurs versions en fonction de l'OS. Le dossier doit être accessible en écriture à l'utilisateur sous lequel le Serveur est lancé (généralement **drwcs**).
- `run` – PID du processus Serveur.
- `sessions` – sessions du Centre de gestion.
- `upload` – dossier pour télécharger les fichiers temporaires spécifiés via le Centre de gestion (clés, etc.).

`/etc/opt/drweb.com/` pour OS Linux (uniquement lors de l'installation depuis les packages `generic *.tar.gz.run`) et `/usr/local/etc/opt/` pour OS FreeBSD :

- `software/drweb-esuite.remove` – script pour la suppression du Serveur.
- + probablement des fichiers et des répertoires supplémentaires.

`/usr/local/etc/rc.d/` pour OS FreeBSD :

- `drwcsd.sh` – script pour démarrer et arrêter le Serveur.

`/var/tmp/drwcs` – copie de sauvegarde après la suppression du Serveur.



Fichiers de configuration principaux

Fichier	Description	Répertoire par défaut
agent.key (le nom peut varier)	clé de licence de l'Agent	
certificate.pem	certificat SSL	
common.conf	fichier de configuration (pour les OS de la famille UNIX)	
download.conf	paramètres réseau pour la génération de packages d'installation de l'Agent	
drwcsd.conf (le nom peut varier)	fichier de configuration du Serveur	
drwcsd.conf.distr	template du fichier de configuration du Serveur avec les paramètres par défaut	
drwcsd.pri	clé de chiffrement privée	
enterprise.key (le nom peut varier)	clé de licence du Serveur. La clé est sauvegardé uniquement si elle est présente après la mise à niveau depuis des versions antérieurs. Elle n'est pas présente en cas d'installation du nouveau Serveur 10	<ul style="list-style-type: none">• sous Linux et Solaris : /var/opt/drwcs/etc• sous FreeBSD : /var/drwcs/etc
frontdoor.conf	fichier de configuration pour l'utilitaire du diagnostic distant du Serveur	
http-alerter-certs.pem	certificats pour la vérification de l'hôte apple-notify.drweb.com pour l'envoi de notifications push	
private-key.pem	clé privée RSA	
webmin.conf	fichier de configuration du Centre de gestion	
auth-ldap.xml	fichier de configuration pour l'authentification externe des administrateurs via LDAP	
auth-pam.xml	fichier de configuration pour l'authentification externe des administrateurs via PAM	
auth-radius.xml	fichier de configuration pour l'authentification externe des administrateurs via RADIUS	
database.sqlite	BD intégrée	<ul style="list-style-type: none">• sous Linux et Solaris : /var/opt/drwcs





Fichier	Description	Répertoire par défaut
		<ul style="list-style-type: none">• sous FreeBSD : /var/drwcs
drwcsd.pub	clé de chiffrement publique	<ul style="list-style-type: none">• sous Linux et Solaris : /opt/drwcs/Installer /opt/drwcs/webmin /install• sous FreeBSD : /usr/local/drwcs/Installer /usr/local/drwcs/webmin/install

Démarrage et arrêt du Serveur Dr.Web

Par défaut, le Serveur Dr.Web démarre de manière automatique après l'installation et après chaque redémarrage du système.

Vous pouvez également démarrer, redémarrer ou arrêter le Serveur Dr.Web de l'une des façons suivantes :

- Arrêt et redémarrage via le Centre de gestion :
Dans la rubrique **Administration** : le redémarrage avec le bouton , l'arrêt avec le bouton  (n'est pas disponible sous OS Solaris).
- Avec la commande de console (voir aussi Annexes, p. [H4. Serveur Dr.Web](#)) :
 - Démarrage :
 - sous FreeBSD :

```
# /usr/local/etc/rc.d/drwcsd.sh start
```
 - pour OS Linux et OS Solaris :

```
# /etc/init.d/drwcsd start
```
 - Redémarrage :
 - sous FreeBSD :

```
# /usr/local/etc/rc.d/drwcsd.sh restart
```
 - pour OS Linux et OS Solaris :

```
# /etc/init.d/drwcsd restart
```
 - Arrêt :
 - sous FreeBSD :

```
# /usr/local/etc/rc.d/drwcsd.sh stop
```
 - Pour OS Linux et OS Solaris :

```
# /etc/init.d/drwcsd stop
```



Pour que le Serveur lise les variables d'environnement, veuillez redémarrer le service avec la commande de console.



4.2. Protection de postes de travail



Vous pouvez consulter la description détaillée des paramètres des composants antivirus spécifiés via le Centre de gestion dans les **Manuels administrateur** consacrés à la gestion des postes pour un système d'exploitation correspondant.

L'ordinateur protégé avec le package antivirus installé est appelé le *poste de travail* conformément à ses fonctions dans le réseau antivirus. Il faut tenir compte que par ses fonctions un tel ordinateur peut être un poste de travail, un appareil mobile ou un serveur du réseau local.

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

Les packages antivirus sont installés sur les postes protégés et sont connectés au Serveur Dr.Web. Chaque poste fait partie d'un ou de plusieurs groupes enregistrés sur ce Serveur (pour en savoir plus, consultez le paragraphe [Groupes système et groupes utilisateur](#)). Les échanges d'information entre le poste et le Serveur sont effectués via le protocole utilisé dans le réseau local (TCP/IP de version 4 ou 6).

Installation

Le package antivirus peut être installé sur le poste de travail par un des moyens suivants :

1. En mode local. L'installation en mode local est effectuée directement sur l'ordinateur ou sur l'appareil mobile de l'utilisateur. Elle peut être réalisée soit par l'administrateur, soit par l'utilisateur.
2. En mode distant. L'installation en mode distant est disponible uniquement sous OS Windows et s'effectue depuis le Centre de gestion via LAN. L'installation est effectuée par l'administrateur du réseau antivirus sans aucune intervention de l'utilisateur.



Dans le **Manuel d'installation**, vous pouvez consulter la description détaillée des procédures d'installation des packages antivirus sur les postes de travail.

Gestion

Étant connecté au Serveur Dr.Web, l'administrateur peut réaliser les fonctions suivantes supportées par le package antivirus sur le poste :

- Configuration centralisée de l'Antivirus sur les postes avec le Centre de gestion.
Dans ce cas, l'administrateur peut interdire ou laisser à l'utilisateur la possibilité de configurer personnellement les paramètres de l'Antivirus sur le poste.
- Configuration de la planification des scans antivirus et d'autres tâches exécutées sur le poste.
- Obtention des statistiques du scan et d'autres informations sur le fonctionnement des composants antivirus et sur le statut du poste.



- Démarrage et arrêt du scan antivirus, etc.



Vous pouvez lancer le Scanner à distance uniquement sur les postes tournant sous OS Windows, OS de la famille UNIX et OS X.

Mise à jour

Serveur Dr.Web télécharge les mises à jour et les diffuse sur les postes connectés. Cela 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 des postes.

Au cas où le poste est temporairement déconnecté du réseau antivirus, l'Antivirus sur le poste 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 le logiciel ne sera pas mis à jour. Si le fonctionnement en *Mode mobile* est autorisé pour le poste, en cas de la perte de connexion au Serveur, la mise à jour des bases virales s'effectuera directement depuis les serveurs du SGM.

Le principe du fonctionnement des postes en mode mobile est décrit dans le paragraphe [Mise à jour des Agents mobiles Dr.Web](#).

4.3. Centre de gestion de la sécurité Dr.Web

Le Centre de gestion de la sécurité 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 Dr.Web.



Pour le fonctionnement correct du Centre de gestion sous le navigateur Windows Internet Explorer, dans les paramètres, il est nécessaire d'ajouter l'adresse du Centre de gestion dans la zone de confiance : **Service** → **Options Internet** → **Sécurité** → **Sites fiables**.

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

Connexion au Serveur Dr.Web

Le Centre de gestion est accessible depuis n'importe quel ordinateur ayant un accès réseau au Serveur Dr.Web à l'adresse suivante :

`http://<adresse_Serveur>:9080`

ou

`https://<adresse_Serveur>:9081`



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



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.



Sous certaines versions de navigateurs web, par exemple **Firefox 3** ou supérieur, une erreur survient 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** (au-dessous de la notification d'erreur). Alors, l'accès au Centre de gestion sera autorisé.

Interface du Centre de gestion de la sécurité Dr.Web

Le fenêtre du Centre de gestion (voir [4-1](#)) comprend deux zones : *l'en-tête du menu principal* et *la zone de travail*.

Zone de travail

La *zone de travail* est utilisée pour lancer toutes les fonctions principales du Centre de gestion. Elle consiste en deux ou trois panneaux en fonction des actions lancées. Les onglets dans les panneaux sont classés de gauche à droite :

- *le menu de gestion* est toujours situé dans la partie gauche de la zone de travail,
- selon l'onglet sélectionné, un ou deux panneaux supplémentaires s'affichent. Dans ce cas, le panneau le plus à droite contient les paramètres des éléments du panneau central.

La langue d'interface doit être définie séparément pour chaque compte administrateur (voir le p. [Gérer les Comptes Administrateurs](#)).

Menu principal

Le menu principal du Centre de gestion comprend les sections suivantes :

- [Administration](#),
- [Réseau antivirus](#),



- [Liaisons](#),
- [Barre de recherche](#),
- nom du compte administrateur sous lequel vous êtes connecté au Centre de gestion. Le [menu de liaisons voisines](#) peut être également disponible,
- rubrique [Événements](#),
- rubrique [Paramètres](#),
- rubrique [Aide](#),
- bouton **Quitter** pour fermer la session en cours du Centre de gestion.



Si l'[authentification automatique](#) est activée dans le Centre de gestion, après avoir cliqué sur **Quitter**, les identifiants de l'administrateur sont supprimés.

A la prochaine ouverture de session du Centre de gestion, il sera nécessaire de répéter la procédure standard d'authentification en indiquant les identifiants. Si l'[authentification automatique](#) est activée, les login et mots de passe indiqués sont sauvegardés pour la session web en cours et l'authentification sur le Centre de gestion devient automatique (sans confirmation des identifiants) jusqu'au prochain clic sur **Quitter**.

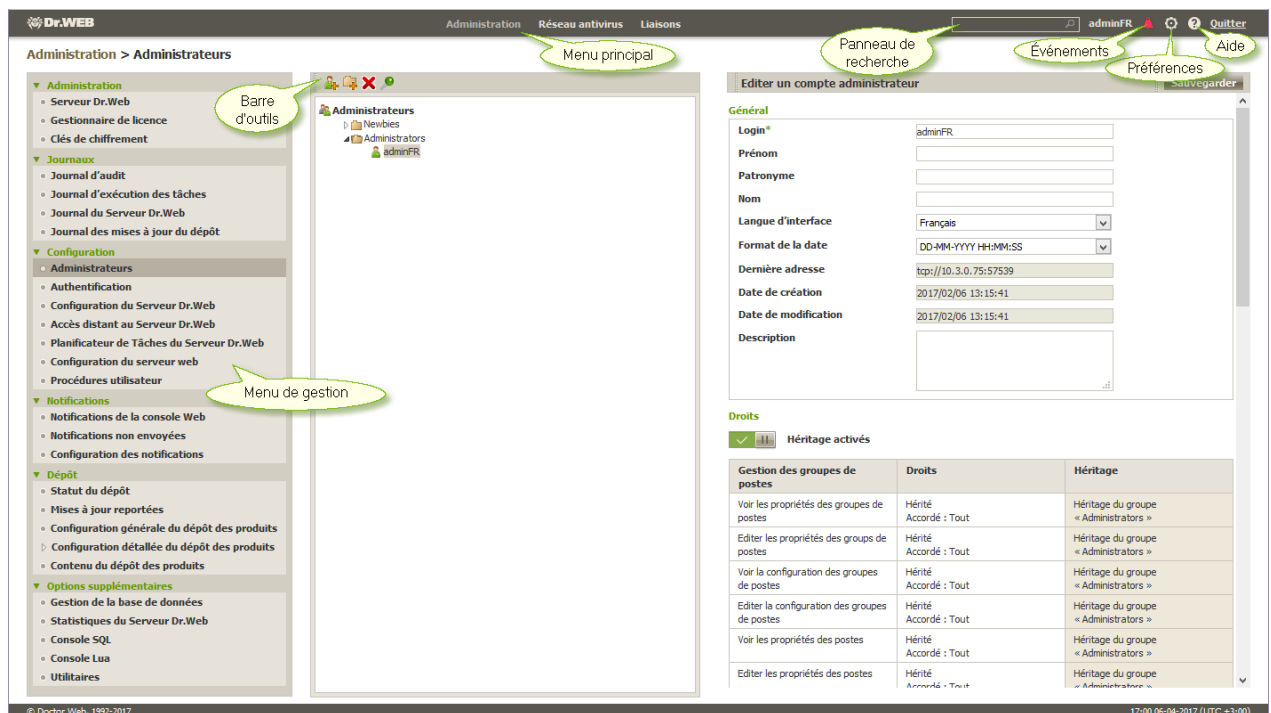


Figure 4-1. Fenêtre du Centre de gestion Dr.Web. Cliquez sur un élément du menu principal pour afficher sa description



Menu des liaisons voisines




Dans la rubrique [Particularités du réseau avec plusieurs Serveurs Dr.Web](#), vous pouvez consulter les informations sur la configuration du réseau antivirus multi-serveurs et des connexions voisines.

S'il y a des liaisons voisines avec d'autres Serveurs Dr.Web, les fonctions suivantes sont ajoutées dans le menu principal pour le login de l'administrateur :

- Le nom du Serveur Dr.Web actuel est affiché contre le nom de l'administrateur.
- Si vous cliquez sur le nom de l'administrateur, la liste déroulante contenant les Serveurs liés va s'afficher. Si le nom de la liaison n'est pas spécifié, c'est l'identificateur de la liaison qui est affiché.

Si vous cliquez sur la liaison, deux variantes sont possibles :



- Le Centre de gestion du Serveur lié va s'ouvrir, si l'adresse IP du Centre de gestion a été indiquée lors de la configuration de la liaison.
L'action est similaire au bouton  dans la barre d'outils de la rubrique **Liaisons** du menu principal.
- Si l'adresse du Centre de gestion du Serveur voisin n'est pas spécifiée pour cette liaison, la fenêtre de configuration de la rubrique **Liaisons** va s'afficher pour que vous puissiez spécifier l'adresse IP.

4.3.1. 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

- **Serveur Dr.Web** – cet élément ouvre le panneau permettant de consulter les informations principales sur le Serveur, il 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. En cas de disponibilité des mises à jour du Serveur Dr.Web téléchargées, vous pouvez accéder depuis cette rubrique à la rubrique [Mises à jour du Serveur Dr.Web](#) contenant la liste de versions du Serveur pour la mise à jour et la sauvegarde.
- [Gestionnaire de licences](#) – cet élément permet de gérer les fichiers clés de licence.
- **Clés de chiffrement** – cet élément permet d'exporter (sauvegarder de manière locale) les clés de chiffrement publiques et privées.



2. Journaux

- [Journal d'audit](#) – cet élément permet de consulter le journal des événements et des modifications effectuées via les sous-systèmes de gestion de Dr.Web Enterprise Security Suite.
- **Log d'exécution des tâches** – cet élément comprend la liste des tâches du Serveur accompagnée de notes sur leur exécution ou de commentaires.
- [Log du Serveur Dr.Web](#) – cet élément contient la liste des événements liés au fonctionnement du Serveur.
- [Log des mises à jour du dépôt des produits](#) – cet élément contient la liste de mises à jour depuis le SGM et les informations détaillées sur les révisions mises à jour de produits.

3. Configuration

- [Administrateurs](#) – cet élément ouvre le panneau permettant de gérer les comptes administrateur du réseau antivirus.
- [Authentification](#) – cet élément ouvre le panneau permettant de gérer les méthodes d'authentification des administrateurs du Centre de gestion.
- [Configuration du Serveur Dr.Web](#) – cet élément ouvre le panneau contenant les paramètres généraux du Serveur.
- [Accès distant au Serveur Dr.Web](#) – cet élément contient les paramètres de connexion de l'utilitaire du diagnostic distant du Serveur.
- [Planificateur des tâches du Serveur Dr.Web](#) – cet élément ouvre le panneau de configuration des tâches planifiées du Serveur.
- [Configuration du Serveur Web](#) – cet élément ouvre le panneau contenant les paramètres généraux du Serveur Web.
- [Procédures utilisateur.](#)

4. Installation

- [Scanner Réseau](#) – cet élément permet de spécifier une liste des réseaux et des logiciels antivirus installés dans le réseau pour déterminer le statut de la protection des postes, et installer l'antivirus.
- **Installation via réseau** – cet élément permet de faciliter la procédure d'installation de l'Agent sur les postes particuliers (voir **Manuel d'Installation**, p. [Installer l'Agent via le Centre de gestion Dr.Web](#)).

5. Notifications

- [Notification de la console web](#) – cet élément permet de consulter et gérer les notifications de l'administrateur reçues par le moyen de la **Console Web**.
- [Notifications non envoyées](#) – cet élément permet de suivre et gérer les notifications de l'administrateur dont l'envoi a échoué conformément aux paramètres de la rubrique **Configuration des notifications**.



- [Configuration des notifications](#) – cet élément permet de configurer les notifications de l'administrateur sur les événements du réseau antivirus.

6. Dépôt

- [Statut du dépôt des produits](#) – cet élément permet de contrôler le statut du dépôt : date de la dernière mise à jour des composants du dépôt et leur statut, ainsi que de mettre à jour le dépôt depuis le SGM.
- [Mises à jour reportées](#) – cet élément contient la liste des produits temporairement exclus des mises à jour dans la rubrique **Configuration détaillée du dépôt**.
- [Configuration générale du dépôt des produits](#) – cet élément ouvre la fenêtre de configuration des paramètres de connexion au SGM et des mises à jour du dépôt pour tous les produits.
- [Configuration détaillée du dépôt des produits](#) – cet élément permet de définir la configuration des révisions pour chaque dépôt de produit séparément.
- [Contenu du dépôt des produits](#) – cet élément permet de consulter et de gérer le contenu actuel du dépôt au niveau de répertoires et de fichiers du dépôt.

7. Options supplémentaires

- [Gestion de la base de données](#) – cet élément permet de maintenir la base de données avec laquelle fonctionne le Serveur Dr.Web.
- [Statistiques du Serveur Dr.Web](#) – cet élément contient les statistiques de fonctionnement de ce Serveur.
- **Console SQL** – cet élément permet d'effectuer les requêtes SQL à la base de données utilisée par le Serveur Dr.Web.
- **Console Lua** – cet élément permet d'exécuter des scripts LUA composés sur la console ainsi que des scripts chargés d'un fichier.



L'administrateur ayant l'accès à la console Lua obtient l'accès à tout le système de fichiers à l'intérieur du répertoire du Serveur et aux certaines commandes sur l'ordinateur avec le Serveur installé.

Pour interdire l'accès à la console Lua, désactivez le droit **Options supplémentaires** pour l'administrateur correspondant (voir le p. [Administrateurs et groupes administrateur](#)).

- **Utilitaires** – cet élément ouvre la rubrique de téléchargement d'utilitaires supplémentaires nécessaires pour le fonctionnement de Dr.Web Enterprise Security Suite :
 - [Chargeur du Dépôt Dr.Web](#) sert à télécharger les produits de Dr.Web Enterprise Security Suite depuis le Système global de mise à jour. La version graphique du Chargeur du Dépôt Dr.Web est disponible uniquement sous Windows.
 - Utilitaire du diagnostic distant du Serveur Dr.Web permet de se connecter au Serveur Dr.Web à distance pour la gestion de base et la consultation des statistiques de fonctionnement. Voir aussi le p. [Accès distant au Serveur Dr.Web](#).



- Centre de gestion Mobile Dr.Web sert à gérer le réseau antivirus basé sur Dr.Web Enterprise Security Suite. Destiné à installer et lancer le logiciel sur les appareils mobiles tournant sous iOS et OS Android.

4.3.2. Réseau antivirus

Sélectionnez l'onglet **Réseau antivirus** dans le menu principal du Centre de gestion.

Menu de gestion

Pour consulter et modifier les informations affichées dans la fenêtre, utilisez le menu de gestion se trouvant dans la partie gauche de la fenêtre.

Le menu de gestion comprend les éléments suivants :

1. Général

- [Graphiques](#)
- [Composants lancés](#)
- [Composants installés](#)
- [Quarantaine](#)
- [Comparaison de matériel et de logiciels](#) (lors de la sélection d'un groupe ou de plusieurs postes)
- **Sessions d'utilisateurs**
- **Postes inactifs**
- [Matériel et logiciels](#) (lors de la sélection d'un poste)
- [Propriétés](#)
- [Règles d'appartenance au groupe](#) (lors de la sélection d'un groupe utilisateur)

2. Statistiques

3. Configuration

- [Droits](#)
- [Planificateur des tâches](#)
- [Composants à installer](#)
- [Restriction des mises à jour](#)
- Liste des composants antivirus pour l'OS des postes sélectionnés ou par liste d'OS lors de la sélection d'un groupe.



Vous pouvez consulter la description détaillée des paramètres des composants antivirus spécifiés via le Centre de gestion dans les **Manuels administrateur** consacrés à la gestion des postes pour un système d'exploitation correspondant.



Liste hiérarchique (arborescence) du réseau antivirus

Dans la partie intermédiaire de la fenêtre, se trouve une liste hiérarchique du réseau antivirus. La liste (le catalogue) représente l'arborescence des éléments du réseau antivirus. Les noeuds dans cette structure sont les [groupes](#) et les [postes](#) à l'intérieur de ces groupes.

Vous pouvez effectuer les actions suivantes sur les éléments de la liste :

- cliquer sur le nom d'un groupe ou d'un poste pour ouvrir le menu de gestion (dans la partie gauche de la fenêtre) de l'élément correspondant et obtenir de brèves données sur le volet de propriétés (dans la partie droite de la fenêtre) ;
- cliquer sur l'icône d'un groupe pour ouvrir ou masquer le contenu du groupe ;
- cliquer sur l'icône d'un poste pour ouvrir la fiche des propriétés de ce poste.












Pour sélectionner plusieurs éléments de la liste hiérarchique, maintenez appuyées les touches CTRL ou SHIFT durant la sélection.

L'apparence de l'icône dépend du type et du statut de l'élément (voir le [tableau 4-1](#)).

Tableau 4-1. Icônes des éléments de la liste hiérarchique

Icône	Description
Groupes. Icônes générales	
	Groupes toujours apparents dans la liste hiérarchique.
	Les groupes ne sont pas affichés dans la liste hiérarchique si : <ul style="list-style-type: none">• pour les groupes, l'option Paramétrer la visibilité des groupes → Masquer si vide est activée et que les groupes ne contiennent pas de postes,• pour les groupes, l'option Configurer la visibilité du groupe → Masquer est activée et que, dans la rubrique Paramètres de l'arborescence, la case Montrer les groupes masqués n'est pas cochée.
Postes de travail. Icônes générales	
	Postes de travail disponibles avec l'antivirus installé.
	Le poste est indisponible.
	Le logiciel antivirus est désinstallé sur le poste.
	Statut du poste lors de l'installation de l'Agent à distance. Le poste a ce statut depuis l'installation réussie de l'Agent sur le poste jusqu'à la première connexion au Serveur.
Icônes supplémentaires	




Icône	Description
	<p>L'icône des paramètres personnalisés s'affiche au-dessus des icônes générales des groupes et postes pour lesquels des paramètres personnalisés ont été définis (ou si le groupe inclut des postes dont les paramètres sont personnalisés).</p> <p>Pour afficher l'icône, sélectionnez l'option  Paramètres d'affichage de l'arborescence dans la barre d'outils et cochez la case Afficher l'icône des paramètres personnalisés.</p> <p>Par exemple, si un poste avec l'antivirus installé possède des paramètres personnalisés, son icône est la suivante : .</p>
	<p>L'icône d'erreur de mise à jour est affichée près des icônes générales des postes sur lesquels des erreurs sont survenues durant la mise à jour de l'antivirus.</p> <p>Pour afficher l'icône, sélectionnez l'option  Paramètres d'affichage de l'arborescence dans la barre d'outils et cochez la case Afficher l'icône de l'erreur de mise à jour.</p> <p>Par exemple, si une erreur est survenue durant la mise à jour de l'antivirus sur un poste en ligne, son icône est la suivante : .</p>
	<p>L'icône des règles d'appartenance s'affiche près des icônes générales des groupes pour lesquels des règles de placement automatique de postes sont définies.</p> <p>Pour afficher le caractère, sélectionnez l'option  Paramétrage de l'arborescence dans la barre d'outils et cochez la case Montrer les icônes des règles d'appartenance.</p> <p>Par exemple, si un groupe toujours affiché dans la liste hiérarchique possède des règles d'appartenance, son icône est la suivante : .</p>

La gestion des éléments du catalogue du réseau antivirus se fait via la barre d'outils de la liste hiérarchique.


Barre d'outils


La barre d'outils de la liste hiérarchique comprend les éléments suivants :

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

 **Éditer.** Ouvre les paramètres du poste ou du groupe dans la partie droite du Centre de gestion.


 **Supprimer les objets sélectionnés.** Supprime des éléments de la liste hiérarchique. Sélectionnez l'élément dans la liste et cliquez sur **Supprimer les objets sélectionnés**.


 **Supprimer les règles d'appartenance.** Supprime les règles de placement automatique des postes dans les groupes.


 **Spécifier le groupe comme primaire.** Définit le groupe comme primaire pour tous les postes qui lui sont rattachés.




 **Spécifier un groupe primaire pour les postes.** Assigne un groupe primaire aux postes sélectionnés. Si un groupe est sélectionné dans la liste hiérarchique au lieu de postes, le groupe primaire sera spécifié pour tous les postes appartenant à ce groupe.


 **Fusionner les postes.** Fusionne les postes sous un seul compte dans la liste hiérarchique. Il est utile dans le cas où le même poste a été enregistré sous différents comptes.


 **Supprimer les paramètres personnalisés.** Supprime les paramètres personnalisés des objets sélectionnés. Dans ce cas, les paramètres seront hérités depuis le groupe primaire. Si un groupe est sélectionné dans la liste hiérarchique, les paramètres de tous les postes appartenant à ce groupe seront également supprimés.


 **Envoyer des messages aux postes.** Cet élément permet d'envoyer un message aux utilisateurs.


 **Réinitialiser le mot de passe.** Supprime le mot de passe défini par l'utilisateur pour accéder aux paramètres de composants antivirus sur les postes sélectionnés. L'option est disponible uniquement pour les postes tournant sous l'OS Windows.

 **Redémarrer un poste.** Effectue le redémarrage d'un poste à distance.


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


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

 **Restauration des postes supprimés.** Cet élément permet de restaurer les postes supprimés antérieurement. Cet élément est actif seulement en cas de sélection des postes faisant partie du sous-groupe **Deleted** dans le groupe **Status**.


 **Envoi des fichiers d'installation.** Envoie les fichiers d'installation sur les adresses email spécifiées dans la rubrique paramètres des postes sélectionnés dans la liste.


+ 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.** Cet élément permet de créer un nouveau poste (voir **Manuel d'Installation**, p. [Création d'un nouveau Compte Utilisateur](#)).


 **Créer un groupe.** Cet élément permet de créer un nouveau groupe de postes.

 **Exporter les données :**

 **Enregistrer au format CSV** – enregistrer au format CSV les informations générales sur les postes sélectionnées du réseau antivirus.

 **Enregistrer au format HTML** – enregistrer au format HTML les informations générales sur les postes sélectionnées du réseau antivirus.

 **Enregistrer au format XML** – enregistrer au format XML les informations générales sur les postes sélectionnées du réseau antivirus.

 **Enregistrer au format PDF** – enregistrer au format PDF les informations générales sur les postes sélectionnées du réseau antivirus.



Si vous sélectionnez les options de la section **Exporter les données** mentionnées ci-dessus, seules les informations sur les postes et les groupes sélectionnées inclus dans les groupes sélectionnés seront exportées.



Exporter la configuration – enregistrer la configuration de l'objet sélectionné du réseau antivirus dans un fichier. Pour cette option, vous serez invité à sélectionner les sections de configuration à enregistrer.



Importer la configuration – télécharger du fichier la configuration de l'objet sélectionné du réseau antivirus. Pour cette option, vous serez invité à choisir le fichier depuis lequel la configuration sera téléchargée, ainsi que les sections de configuration à télécharger.



Diffuser la configuration – diffuser la configuration de l'objet sélectionné sur les autres objets du réseau antivirus. Pour cette option, vous serez invité à choisir les objets depuis lesquels la configuration sera diffusée, ainsi que les sections de configuration à diffuser.

Paramétrer l'affichage du groupe. Cet élément permet de modifier les paramètres d'affichage des groupes. Pour cela, sélectionnez un des éléments suivants dans la liste déroulante (l'icône du groupe va changer d'apparence, voir [le tableau 4-1](#)) :



Masquer signifie que l'affichage du groupe dans la liste hiérarchique sera toujours désactivé.



Masquer s'il est vide signifie que le groupe ne sera pas affiché dans la liste hiérarchique s'il est vide (ne contient pas de postes).



Afficher signifie que le groupe sera toujours affiché dans la liste hiérarchique.

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



Mettre à jour les composants échoués. Cet élément prescrit la synchronisation des composants dont la mise à jour a échoué.



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



Interrompre les composants lancés. Cet élément permet d'arrêter tous les composants antivirus lancés sur un poste.



Scan. Permet d'analyser les postes dans un des modes sélectionnés dans la liste déroulante :





Scanner Dr.Web. Scan rapide. Ce mode prévoit l'analyse des objets suivants à l'aide du Scanner Dr.Web Agent :


- 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.

 **Scanner Dr.Web. Scan complet.** Ce mode assure l'analyse complète de tous les disques durs ainsi que des supports amovibles (y compris les secteurs boot) à l'aide du Scanner Dr.Web Agent.


 **Scanner Dr.Web. Scan personnalisé.** Ce mode permet de choisir les dossiers et fichiers à analyser à l'aide du Scanner Dr.Web Agent.

 **Postes non approuvés.** Cet élément permet de gérer la liste des novices – des postes dont l'enregistrement n'a pas été approuvé (pour en savoir plus, voir la rubrique [Politique d'approbation des postes](#)). Cet élément est actif seulement en cas de sélection d'un poste du sous-groupe **Newbies** dans le groupe **Status**. En cas d'approbation de l'enregistrement ou en cas d'accès refusé au Serveur, les postes seront retirés automatiquement du sous-groupe préinstallé **Newbies**. Pour ce faire, sélectionnez dans la liste déroulante une des options suivantes :

 **Approuver les postes sélectionnés et définir un groupe primaire.** Permet de confirmer l'accès d'un poste au Serveur et définir un groupe primaire dans la liste proposée.

 **Annuler l'action qui doit être exécutée à la connexion.** Permet d'annuler l'action dont l'exécution a été paramétrée au préalable sur les postes non approuvés au moment de leur connexion au Serveur.

 **Rejeter les postes sélectionnés.** Permet d'interdire l'accès du poste au Serveur.

 **Paramètres d'affichage de l'arborescence.** Cet élément permet de modifier l'apparence de l'arborescence du réseau antivirus. Pour activer le paramètre, cochez les cases correspondantes dans le menu déroulant :

- pour les groupes :
 - **Appartenance à tous les groupes** – doubler l'affichage du poste dans la liste s'il appartient à plusieurs groupes en même temps (uniquement pour les groupes accompagnés de l'image du dossier blanc – voir le [tableau 4-1](#)). Si la case est cochée, toutes les appartenances seront affichées. Sinon le poste sera affiché dans la liste une seule fois.
 - **Afficher les groupes masqués** – afficher tous les groupes faisant partie du réseau antivirus. Si la case est décochée, tous les groupes vides (ceux qui ne contiennent pas de postes) seront masqués. Ceci peut être pratique pour éviter d'afficher trop d'informations, par exemple en cas de nombreux groupes vides.
- pour les postes :
 - **Afficher les identificateurs de postes** – afficher les identificateurs uniques de postes dans la liste hiérarchique.
 - **Afficher les noms de postes** – afficher les noms de postes.



Il est impossible de désactiver l'affichage des identificateurs et des noms de postes en même temps. Au moins un des paramètres **Afficher les identificateurs de postes** ou **Afficher les noms de postes** sera toujours sélectionné.

- **Afficher les adresse de postes** – afficher les adresses IP des postes dans la liste hiérarchique.







- **Afficher les serveurs de postes** – afficher les noms ou les adresses IP des Serveurs anti-virus auxquels les postes sont connectés.
- **Afficher l'icône d'erreur de mise à jour** – afficher le marqueur sur les icônes des postes pour lesquels la mise à jour a échoué.
- pour tous les éléments :
 - **Afficher les configurations personnalisées** – afficher le marqueur sur les icônes des postes et des groupes dont les paramètres sont personnalisés.
 - **Afficher les descriptions** – afficher les descriptions des groupes et des postes (les descriptions sont spécifiées dans les propriétés de l'élément).
 - **Afficher le nombre de postes** – afficher le nombre de postes pour tous les groupes du réseau antivirus.
 - **Afficher l'icône des règles d'appartenance** – afficher le marqueur sur les icônes des postes qui sont ajoutés automatiquement aux groupes d'après les règles d'appartenance, ainsi que sur les icônes des groupes dans lesquels les postes sont ajoutés automatiquement.

↑↓ **Paramètres de tri des postes.** Cet élément permet de modifier le paramètre de tri et l'ordre de tri de postes dans l'arborescence du réseau antivirus.

- Pour sélectionner un paramètre de tri, cochez une des cases suivantes (il est possible de sélectionner un seul paramètre) :
 - **Identificateur** – trier par identificateurs uniques de postes.
 - **Nom** – trier par noms de postes.
 - **Adresse** – trier par adresse réseau de poste. Les postes qui n'ont pas d'adresse réseau, seront affichés dans l'ordre aléatoire sans tri.
 - **Date de création** – trier par date de création du compte de poste sur le Serveur.
- Pour sélectionner l'ordre de tri, cochez une des cases suivantes :
 - **Tri croissant.**
 - **Tri décroissant.**



Les sections  **Paramètres d'affichage de l'arborescence** et  **Paramètres de tri des postes** sont interdépendants :

- Si vous sélectionnez un paramètre de tri dans la rubrique  **Paramètres de tri de postes**, l'affichage de ce paramètre est activé automatiquement dans la section  **Paramètres d'affichage de l'arborescence**, s'il a été désactivé.
- Si dans la section  **Paramètres d'affichage de l'arborescence**, vous désactivez l'affichage du paramètre de tri sélectionné dans la section  **Paramètres de tri de postes**, alors le tri en fonction de ce paramètre passe automatiquement en mode de tri par noms de postes. Si l'affichage de noms de postes est désactivé, alors les postes seront triés par identificateurs (le nom et l'identificateur ne peuvent pas être désactivés en même temps).



Panneau des propriétés

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

Pour afficher le panneau des propriétés :

1. Cliquez sur le nom d'un groupe ou d'un poste dans la liste hiérarchique.
2. Le panneau affichant les propriétés du poste ou du groupe sera ouvert dans la partie droite de la fenêtre du Centre de gestion. Pour en savoir plus sur les paramètres, consultez [Éditer les groupes](#) et [Propriétés du poste](#).

4.3.3. 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 p. [Particularités du réseau avec plusieurs Serveurs Dr.Web](#)).

L'arborescence affiche tous les Serveurs Dr.Web connectés au Serveur sélectionné.

La procédure de création des liaisons entre serveurs est décrite dans le paragraphe [Configuration des liaisons entre Serveurs Dr.Web](#).

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 Dr.Web](#)).

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

4.3.4. Barre 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 les postes par leurs noms,
 - **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,
 - **Nom d'utilisateur** – pour rechercher des postes par le nom de l'utilisateur sur le poste,
 - **Adresse IP** – pour rechercher les postes par leur adresse IP,
 - **Matériel** – pour rechercher le poste par le nom ou la catégorie de hardware installé sur le poste,
 - **Logiciel** – pour rechercher le poste par le nom de software, installé sur le poste.
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. Le panneau de recherche avancée et l'arborescence du réseau antivirus vont s'ouvrir.
4. Tous les éléments trouvés seront affichés dans l'arborescence du réseau antivirus 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.**


4.3.5. Événements

La rubrique marquée de l'icône  **Événements** affichée dans le menu principal sert à avertir l'administrateur des événements exigeant de l'attention.


L'état de l'icône peut varier :

 - il n'y a pas de nouvelles notifications sur les événements sur le réseau.

 - il y a de nouvelles notifications sur les événements mineures.

 - il y a de nouvelles notifications sur les événements majeures exigeant l'intervention de l'administrateur.


Les actions suivantes sont disponibles pour la liste d'événements :

1. Si vous cliquez sur l'icône, la liste déroulante des événements du réseau antivirus va s'ouvrir. Dans ce cas, l'icône change en .
2. Si vous cliquez sur la ligne de notification d'un événement, vous passez à la rubrique du Centre de gestion associée à cette fonction.



- Le ruban de chaque notification dans la liste d'événements est marqué par la couleur qui correspond au niveau d'importance de l'événement (similaire à l'icône). Quand vous passez dans la rubrique associée à la notification, la notification est considérée comme lue et le ruban devient gris.

Tableau 4-2. Liste des notifications possibles des événements sur le réseau antivirus

Événement	Importance	Rubrique du Centre de gestion	Description
Installer l'extension pour le Centre de gestion de la sécurité Dr.Web pour le navigateur	mineure	Page de téléchargement de l'extension pour le Centre de gestion de la sécurité Dr.Web	L'installation de l'extension pour le Centre de gestion de la sécurité Dr.Web est requise.
Actualités non lues	mineure	 Aide → Actualités	Les actualités non lues de Doctor Web sont disponibles.
Nouvelles notifications	mineure	Administration → Notifiactions de la console web	Les nouvelles notifications de l'administrateur reçues via la Console web sont disponibles.
Notifications critiques	majeure		
Les mises à jour du Serveur sont disponibles	majeure	Administration Serveur Dr.Web →	La mise à jour du Serveur Dr.Web est téléchargée dans le dépôt et elle est disponible pour l'installation.
La configuration du Serveur a été modifiée. Le redémarrage du Serveur est requis.	majeure	Administration → Configuration du Serveur Dr.Web	Les paramètres du fichier de configuration du Serveur ont été modifiés après le lancement du Serveur. Pour appliquer les nouveaux paramètres, veuillez redémarrer le Serveur.
La configuration du serveur web a été modifiée. Le redémarrage du Serveur est requis.	majeure	Administration → Configuration du serveur web	Les paramètres du fichier de configuration du serveur web ont été modifiés après le lancement du Serveur. Pour appliquer les nouveaux paramètres, veuillez redémarrer le Serveur.

4.3.6. Paramètres

Pour passer dans la rubrique de paramètres du Centre de gestion, cliquez sur  **Préférences** dans le menu principal.



Tous les paramètres de cet onglet sont valables uniquement 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.**
- **Abonnement.**

Mon compte


Cette rubrique permet de gérer le compte administrateur courant du réseau antivirus (voir aussi [Administrateurs et groupes](#)).

Général



Les valeurs des champs marqués du symbole *, doivent être obligatoirement spécifiées.

Si nécessaire, éditer les paramètres suivants :

- **Login** de l'administrateur – login requis pour accéder au Centre de gestion.
- 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 : JJ-MM-AAAA HH:MM:SS
 - américain : MM/JJ/AAAA HH:MM:SS
- **Description du** compte.
- Pour changer de mot de passe, cliquez sur  **Changer de mot de passe** dans la barre d'outils.

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

- Date de la création du compte et date de la dernière modification de ses paramètres,
- **Dernière adresse** – cet élément affiche les adresses réseau de la dernière connexion sous le compte actuel.

Droits


Description des droits administrateur et leur édition à l'onglet [Édition des Administrateurs](#).

Cliquez sur **Enregistrer** après la modification des paramètres.



Interface

Configuration de l'arborescence

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

- pour les groupes :
 - **Appartenance à tous les groupes** – doubler l'affichage du poste dans la liste s'il appartient à plusieurs groupes en même temps (uniquement pour les groupes accompagnés de l'image du dossier blanc – voir le [tableau 4-1](#)). Si la case est cochée, toutes les appartenances seront affichées. Sinon le poste sera affiché dans la liste une seule fois.
 - **Afficher les groupes masqués** – afficher tous les groupes faisant partie du réseau antivirus. Si la case est décochée, tous les groupes vides (ceux qui ne contiennent pas de postes) seront masqués. Ceci peut être pratique pour éviter d'afficher trop d'informations, par exemple en cas de nombreux groupes vides.
- pour les postes :
 - **Afficher les identificateurs de postes** – afficher les identificateurs uniques de postes dans la liste hiérarchique.
 - **Afficher les noms de postes** – afficher les noms de postes.



Il est impossible de désactiver l'affichage des identificateurs et des noms de postes en même temps. Au moins un des paramètres **Afficher les identificateurs de postes** et **Afficher les noms de postes** sera toujours sélectionné.

- **Afficher les adresse de postes** – afficher les adresses IP des postes dans la liste hiérarchique.
 - **Afficher les serveurs de postes** – afficher les noms ou les adresses IP des Serveurs antivirus auxquels les postes sont connectés.
 - **Afficher l'icône d'erreur de mise à jour** – afficher le marqueur sur les icônes des postes pour lesquels la mise à jour a échoué.
- pour tous les éléments :
 - **Afficher les configurations personnalisées** – afficher le marqueur sur les icônes des postes et des groupes dont les paramètres sont personnalisés.
 - **Afficher les descriptions** – afficher les descriptions des groupes et des postes (les descriptions sont spécifiées dans les propriétés de l'élément).
 - **Afficher le nombre de postes** – afficher le nombre de postes pour tous les groupes du réseau antivirus.
 - **Afficher l'icône des règles d'appartenance** – afficher le marqueur sur les icônes des postes qui sont ajoutés automatiquement aux groupes d'après les règles d'appartenance, ainsi que sur les icônes des groupes dans lesquels les postes sont ajoutés automatiquement.



Scanner réseau



Pour le fonctionnement du Scanner réseau, veuillez installer l'extension pour le Centre de gestion de la sécurité Dr.Web.

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](#) 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 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).
2. Si nécessaire, changez de **Port** et modifiez la valeur du paramètre **Délai (s)**.
3. Afin de garder les valeurs par défaut, cliquez sur le bouton **Enregistrer**. Ultérieurement, lors de l'utilisation du [Scanner réseau](#), ces paramètres seront spécifiés de manière automatique.

Délai 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 Dr.Web ayant le même nom d'utilisateur et le même mot de passe administrateur.



Lorsque la case est activée, l'extension pour le Centre de gestion de la sécurité Dr.Web va mémoriser le nom et le mot de passe que l'administrateur entrera lors de la prochaine authentification dans le Centre de gestion.



Pour le fonctionnement de l'authentification automatique, veuillez installer l'extension pour le Centre de gestion de la sécurité Dr.Web.

Ultérieurement, à l'ouverture de n'importe quel Centre de gestion de la sécurité 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 le [menu principal](#) 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**.

Dans la liste déroulante **Session expirée**, sélectionnez un délai après lequel la session utilisateur du Centre de gestion sera automatiquement terminée dans le navigateur.

Export au format PDF

Dans cet onglet, vous pouvez indiquer les paramètres de texte pour l'export de données statistiques au format PDF :

- Dans la liste déroulante **Police des rapports**, sélectionnez la police utilisée pour l'export des rapports au format PDF.
- Dans le champ **Taille de la police des rapports**, indiquez la taille de la police pour le texte des tableaux statistiques utilisés pour l'export de rapports au format PDF.

Rapports

Dans cet onglet, vous pouvez indiquer les paramètres de visualisation des données statistiques dans l'onglet **Rapports** du Centre de gestion :

- Dans le champ **Nombre de lignes par page**, indiquez le nombre maximum de lignes sur une page de rapport pour la visualisation par page des statistiques.
- Cochez la case **Afficher les graphiques** pour afficher les graphiques sur les pages de rapports statistiques. Si la case est décochée, la visualisation des graphiques est désactivée.



Abonnement

Dans cet onglet, vous pouvez configurer l'abonnement aux actualités Doctor Web.

Cochez la case **Abonnement automatique aux nouvelles rubriques** pour ajouter de nouvelles rubriques à la page actualités du Centre de gestion automatiquement.

4.3.7. Aide

Pour ouvrir la rubrique de l'aide du Centre de gestion, cliquez sur le bouton  **Aide** dans le menu principal.

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

1. Général

- **Forum** – cet élément redirige vers le forum de Doctor Web.
- **Actualités** – cet élément redirige vers la page d'actualités de Doctor Web.
- **Contacteur le support technique** – cet élément redirige vers la page du Support technique de Doctor Web.
- **Envoyer un fichier suspect** – cet élément ouvre un formulaire permettant d'envoyer un virus au Laboratoire de Doctor Web.
- **Wikipédia Doctor Web** – cet élément redirige vers la page de Wikipédia – base de connaissance consacrée aux produits de Doctor Web.
- **Signaler un faux positif dans Office Control** – cet élément ouvre un formulaire permettant d'envoyer un message sur une fausse alerte ou sur un problème de non détection dans le module de Office Control.

2. Documentation d'administrateur

- **Manuel Administrateur** – cet élément ouvre le Manuel Administrateur au format HTML.
- **Manuel d'Installation** – cet élément ouvre la documentation au format HTML sur l'installation de Dr.Web Enterprise Security Suite.
- **Instruction de déploiement du réseau antivirus** – afficher la brève instruction de déploiement du réseau antivirus au format HTML. Il est recommandé de consulter cette instruction avant de déployer le réseau antivirus, d'installer et de configurer les composants.
- **Annexes** – cet élément ouvre les annexes du manuel administrateur au format HTML.
- **Manuel sur Web API** – cet élément ouvre la documentation de l'administrateur sur Web API (voir aussi les **Annexes**, p. [Annexe L. Intégration de Web API et de Dr.Web Enterprise Security Suite](#)) au format HTML.
- **Notes de publication** – cet élément ouvre les notes de version de Dr.Web Enterprise Security Suite pour la version que vous avez installée.

3. Documentation d'utilisateur – cet élément ouvre la Documentation d'utilisateur au format HTML pour la version correspondante du système d'exploitation figurant dans la liste.



4.4. Composants du Centre de gestion de la sécurité Dr.Web

4.4.1. Scanner réseau

Le Scanner réseau est inclus au sein du Serveur Dr.Web.



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.

Pour le fonctionnement du Scanner réseau, veuillez installer l'extension pour le Centre de gestion de la sécurité Dr.Web.

Pour utiliser le Scanner réseau avec le navigateur web Windows Internet Explorer, il est nécessaire d'ajouter l'adresse du Centre de gestion qui lance le Scanner réseau dans la zone de confiance : **Service** → **Options Internet** → **Sécurité** → **Sites fiables**.

Le scanner réseau exécute les fonctions suivantes :

- Scan (aperçu) du réseau afin de trouver les postes de travail.
- Détermination de la présence de l'Agent Dr.Web sur les postes.
- L'installation de l'Agent Dr.Web sur les postes détectés selon la commande de l'administrateur. La procédure d'installation de l'Agent Dr.Web est décrite dans le **Manuel d'installation**, p. [Installer l'Agent via le Centre de gestion de la Sécurité](#).

Pour scanner le réseau ou pour obtenir un aperçu du réseau, procédez comme suit :

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 du Scanner réseau va s'ouvrir.
2. Cochez la case **Recherche par adresses IP** pour effectuer la recherche dans le réseau d'après les adresses IP spécifiées. Dans le champ **Réseaux**, indiquez la liste de réseaux au format :
 - 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).
3. Sous Windows : cochez la case **Recherche dans Active Directory** pour effectuer la recherche de postes dans le domaine Active Directory. Dans ce cas, spécifiez les paramètres suivants :
 - **Domaines** – liste des domaines dans lesquels la recherche des postes sera effectuée. Utilisez la virgule pour séparer plusieurs domaines.
 - **Contrôleur Active Directory** – contrôleur Active Directory, par exemple, [dc.example.com](#).



Pour rechercher les postes dans le domaine Active Directory à l'aide du Scanner réseau, il faut que le navigateur dans lequel le Centre de gestion est ouvert soit lancé par l'utilisateur de domaine ayant le droit de rechercher des objets dans le domaine Active Directory.

4. Sous les OS de la famille UNIX : cochez la case **Recherche dans LDAP** pour effectuer la recherche de postes dans LDAP. Dans ce cas, spécifiez les paramètres suivants :
 - **Domaines** – liste des domaines dans lesquels la recherche des postes sera effectuée. Utilisez la virgule pour séparer plusieurs domaines.
 - **Serveur LDAP** – serveur LDAP, par exemple, <ldap://ldap.example.com>.
 - **Nom d'utilisateur** – nom d'utilisateur LDAP.
 - **Mot de passe** – mot de passe de l'utilisateur LDAP.
5. Dans le champ **Port** indiquez le numéro du port par lequel il faut s'adresser aux Agents via le protocole UDP lors de la recherche.
6. Si nécessaire, dans le champ **Délai (s)**, modifiez la valeur du délai d'attente, en secondes, durant lequel on attend une réponse des postes demandés.
7. 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.

8. Cochez la case **A comparer avec la liste des postes de la BD** pour activer la synchronisation des résultats de recherche du Scanner réseau avec la liste des postes sauvegardée dans la BD du Serveur. Si cette case est cochée, 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 ces 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.

9. Cliquez sur le bouton **Scanner**. Le scan du réseau va commencer.
10. Pendant le scan du réseau, le répertoire (arborescence) s'affiche dans une fenêtre indiquant les postes et la présence sur ces postes de l'Agent Dr.Web.

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 4-3. Apparence des icônes

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



Icône	Description
	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 actifs 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 (il n'y a pas d'antivirus 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, inactif et le port est fermé.

Les éléments du répertoire correspondant aux postes ayant les icônes ou peuvent être ouverts pour consulter le jeu des composants installés.

Interaction avec les Agents Dr.Web

L'outil **Scanner réseau** est inclus dans le produit Dr.Web Enterprise Security Suite 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.

4.4.2. Gestionnaire de licences



Pour en savoir plus sur les principes et les particularités de la licence Dr.Web Enterprise Security Suite, consultez la rubrique [Chapitre 2. Licence](#).



Interface du Gestionnaire de Licences






Le Centre de gestion contient le composant Gestionnaire de Licences. Ce composant est utilisé pour gérer le licencing des objets du réseau antivirus.


Pour ouvrir le Gestionnaire de Licences, choisissez la rubrique **Administration** dans le menu principal du Centre de gestion. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Gestionnaire de Licences** dans le [menu de gestion](#).

Liste hiérarchique des clés

La fenêtre principale du Gestionnaire de Licences contient l'arborescence des clés – la liste hiérarchique dont les nœuds sont les clés de licence des postes et des groupes auxquels ces clés de licence sont attribuées.

La barre d'outils contient les éléments de contrôle suivants :

Option	Description	Disponibilité dans l'arborescence
 Ajouter une clé	Enregistrement d'une nouvelle clé de licence.	Cette option est toujours disponible. Les fonctionnalités dépendent de la sélection de l'objet dans l'arborescence des clés (voir Ajouter une nouvelle clé de licence).
 Supprimer les objets sélectionnés	Supprimer la connexion entre la clé et l'objet soumis à licence.	L'option est disponible si un objet soumis à licence (poste ou groupe) ou une clé de licence est sélectionnée dans l'arborescence.
 Distribuer la clé aux groupes et postes	Remplacer ou ajouter la clé sélectionnée à un objet soumis à licence.	L'option est disponible si une clé de licence est sélectionnée dans l'arborescence.
 Exporter la clé	Sauvegarder une copie locale du fichier clé de licence.	
 Distribuer la clé aux serveurs voisins	Distribuer les licences de la clé sélectionnée aux Serveurs voisins.	

 **Paramètres de visualisation de l'arborescence** – cet élément permet de modifier la visualisation de l'arborescence :

- La case **Afficher le nombre de licences** active/désactive l'affichage du nombre total de licences fournies par les fichiers clés.
- Pour modifier la structure de l'arborescence, utilisez les options suivantes :



- L'option **Clés** permet d'afficher toutes les clés de licence du réseau antivirus en tant que noeuds à la racine de la liste hiérarchique. Ainsi, tous les groupes et postes auxquels ces clés sont assignées se présentent comme des éléments liés aux clés de licence (éléments "enfants"). Ce mode de visualisation de l'arborescence est une vue d'ensemble et permet de gérer les objets soumis à licence et les clés de licence.
- L'option **Groupes** permet d'afficher les groupes auxquels sont personnellement assignées les clés en tant que noeuds à la racine de la liste hiérarchique. Ainsi, les postes inclus à ces groupes et les clés de licence assignées à ces groupes se présentent comme des éléments "enfants" des groupes. Ce mode de visualisation permet d'obtenir des informations sur le licensing mais ne permet pas de gérer les objets de l'arborescence.

Gestion des licences

Via le Gestionnaire de Licences, vous pouvez effectuer les actions suivantes sous les clés de licence :

1. [Obtenir de l'information sur une licence.](#)
2. [Ajouter une nouvelle clé de licence.](#)
3. [Mettre à jour la clé de licence.](#)
4. [Remplacer la clé de licence.](#)
5. [Étendre la liste des clés de licence de l'objet.](#)
6. [Suppression de la clé de licence et suppression de l'objet de la liste de licences.](#)
7. [Distribuer une licence à un serveur voisin.](#)
8. [Modifier les licences distribuées à un serveur voisin.](#)

Accéder aux données concernant une licence


Pour voir un résumé des données sur une clé de licence, sélectionnez l'enregistrement de la clé dans le volet principal du Gestionnaire de Licences, pour obtenir des détails, cliquez sur le nom de l'enregistrement de la clé. Dans le volet qui s'ouvre, les informations suivantes s'affichent :

- le propriétaire de la licence,
- le partenaire qui a vendu la licence,
- identification et numéros de série de la licence,
- date d'expiration de la licence,
- inclusion du composant Antispam,
- nombre de postes à licencier avec ce fichier clé,
- la fonction de hachage MD5 de la clé de licence,
- la liste des composants antivirus pouvant être utilisés par cette licence.



Ajouter une nouvelle clé de licence

Pour ajouter une nouvelle clé de licence :


1. Dans la fenêtre principale du Gestionnaire de licences cliquez sur **+** **Ajouter une clé** dans la barre d'outils.
2. Dans le panneau qui s'ouvre, cliquez sur  et sélectionnez le fichier clé de licence.
3. Cliquez sur **Enregistrer**.
4. La clé de licence sera ajoutée à l'arborescence des clés mais elle ne sera assignée à aucun objet. Dans ce cas, pour spécifier les objets soumis à licence, appliquez les procédures [Remplacer la clé de licence](#) ou [Étendre la liste des clés de licence de l'objet](#) décrites ci-dessus.

Mettre à jour la clé de licence

Lors de la mise à jour d'une clé de licence, la nouvelle clé est assignée aux mêmes objets.

Utilisez la procédure de mise à jour de clé pour remplacer une clé qui a expiré ou pour remplacer une clé par une autre possédant un jeu de composants différent. La structure de l'arborescence des clés reste inchangée.


Pour mettre à jour une clé de licence :

1. Dans le volet principal du Gestionnaire de Licences, dans l'arborescence des clés, sélectionnez la clé que vous souhaitez mettre à jour.
2. Dans la fenêtre des propriétés de la clé, cliquez sur  et sélectionnez le fichier clé de licence.
3. Cliquez sur **Enregistrer**. Une fenêtre donnant les paramètres d'installation des composants, décrits dans la sous-rubrique [Paramètres de modification d'une clé de licence](#), va s'ouvrir.
4. Cliquez sur **Enregistrer** pour mettre à jour la clé de licence.

Remplacer la clé de licence

Lors du changement de clé de licence, toutes les clés en cours sont supprimées pour l'objet soumis à licence et une nouvelle clé est ajoutée.

Pour remplacer la clé de licence en cours :

1. Dans le menu principal du Gestionnaire de Licences, dans l'arborescence des clés, choisissez la clé que vous souhaitez assigner à l'objet.
2. Cliquez sur  **Distribuer la clé aux groupes et postes** dans la barre d'outils. Une fenêtre donnant la liste hiérarchique des postes et des groupes du réseau antivirus s'ouvre.
3. Sélectionnez l'objet dans la liste. Pour choisir plusieurs postes ou groupes, utilisez les touches CTRL et SHIFT.



4. Cliquez sur **Remplacer la clé**. Une fenêtre donnant les paramètres d'installation des composants, décrits dans [Paramètres de modification d'une clé de licence](#), va s'ouvrir.
5. Cliquez sur **Sauvegarder** pour remplacer la clé de licence.

Étendre la liste des clés de licence de l'objet

Lors de l'ajout d'une clé de licence, l'objet sauvegarde toutes les clés en cours et une nouvelle clé est ajoutée à la liste existante.

Pour ajouter une clé de licence à la liste des clés de licence de l'objet :


1. Dans le menu principal du Gestionnaire de Licences, dans l'arborescence des clés, sélectionnez la clé que vous souhaitez ajouter à la liste des clés de l'objet.
2. Cliquez sur  **Distribuer la clé aux groupes et postes** dans la barre d'outils. Une fenêtre donnant la liste hiérarchique des postes et des groupes du réseau antivirus s'ouvre.
3. Sélectionnez l'objet dans la liste. Pour choisir plusieurs postes ou groupes, utilisez les touches CTRL et SHIFT.
4. Cliquez sur **Ajouter une clé**. Une fenêtre donnant les paramètres des composants à installer décrits dans la sous-rubrique [Paramètres de modification d'une clé de licence](#), va s'ouvrir.
5. Cliquez sur **Sauvegarder** pour ajouter la clé de licence.

Supprimer la clé de licence et supprimer l'objet de la liste de licences



Il est impossible de supprimer le derniers enregistrement de la clé de licence assignée au groupe **Everyone**.

Pour supprimer une clé de licence ou un objet de la liste de licences :


1. Dans le menu principal du Gestionnaire de Licences, dans l'arborescence des clés, sélectionnez la clé que vous souhaitez supprimer, ou l'objet (poste ou groupe) auquel cette clé est assignée, et cliquez sur  **Supprimer les objets sélectionnés** dans la barre d'outils. Ainsi :
 - Si l'objet soumis à licence a été sélectionné, celui-ci sera supprimé de la liste d'objets pour lesquels la clé est active. Un objet dont la clé de licence personnelle a été supprimée hérite d'une clé de licence.
 - Si la clé de licence a été sélectionnée, l'enregistrement de cette clé est supprimé du réseau antivirus. Tous les objets auxquels cette clé était assignée, héritent d'une clé de licence.
2. Une fenêtre donnant les paramètres d'installation des composants, décrits dans [Paramètres de modification d'une clé de licence](#), va s'ouvrir.
3. Cliquez sur **Sauvegarder** pour supprimer l'objet sélectionné et pour passer à la clé héritée.



Distribuer une licence à un serveur voisin

Lors de la distribution de licences vacantes à un Serveur voisin depuis la clé de licence d'un Serveur, les licences distribuées ne pourront pas être utilisées sur ce Serveur avant la fin de leur propagation.

Pour distribuer des licences à un serveur voisin :

1. Dans le menu principal du Gestionnaire de Licences, dans l'arborescence des clés, sélectionnez la clé d'après laquelle vous souhaitez distribuer des licences vacantes à un Serveur voisin.
2. Cliquez sur  **Distribuer la clé aux serveurs voisins** dans la barre d'outils. Une fenêtre donnant l'arborescence des Serveurs voisins s'ouvre.
3. Sélectionnez dans la liste les Serveurs auxquels vous souhaitez distribuer les licences.
4. Configurez les paramètres suivants près de chaque Serveur :
 - **Nombre de licences** – nombre des licences vacantes que vous souhaitez distribuer depuis cette clé à un Serveur voisin.
 - **Date d'expiration de la licence** – durée de validité de la transmission des licences. A la fin de cette période, toutes les licences seront rappelées du Serveur voisin et retourneront dans la liste des licences vacantes dans cette clé de licence.
5. Cliquez sur l'un des boutons :
 - **Ajouter une clé** – pour ajouter des licences à la liste des licences des Serveurs voisins. Une fenêtre s'ouvre contenant les paramètres d'installation des composants, décrits dans la sous-rubrique [Paramètres pour ajouter une clé de licence à la liste de clés](#).
 - **Remplacer la clé** – pour supprimer les licences en cours des Serveurs voisins et traiter uniquement les licences distribuées. Une fenêtre s'ouvre contenant les paramètres d'installation des composants, décrits dans la sous-rubrique [Paramètres de modification d'une clé de licence](#).
6. Cliquez sur **Sauvegarder** pour distribuer les licences aux Serveurs voisins.

Modifier les licences distribuées à un serveur voisin

Pour modifier les licences distribuées à un serveur voisin :

1. Dans le menu principal du Gestionnaire de Licences, dans l'arborescence des clés, sélectionnez le Serveur voisin auquel des licences ont été distribuées.
2. Dans le panneau des propriétés qui s'ouvre, modifiez les paramètres suivants :
 - **Nombre de licences** – nombre des licences vacantes qui ont été distribuées depuis la clé de ce Serveur à un Serveur voisin.
 - **Date d'expiration de la licence** – durée de validité de la transmission de licences. A la fin de cette période, toutes les licences seront rappelées de ce Serveur et retourneront dans la liste des licences vacantes de la clé de licence correspondante.



3. Cliquez sur **Sauvegarder** pour mettre à jour les données sur les licences distribuées.

Modifier les listes des composants installés

Paramètres de modification d'une clé de licence

Dans cette sous-rubrique, vous trouverez une description de l'installation des composants dans le cadre des procédures suivantes :

- Mettre à jour la clé de licence.
- Remplacer la clé de licence.
- Supprimer la clé de licence.
- Distribuer une licence à un Serveur voisin avec remplacement de clé.

Lorsque vous mettez en oeuvre ces procédures, suivez ces règles pour configurer l'installation des composants :

1. Dans la fenêtre de configuration de l'installation des composants, les objets suivants sont listés :
 - Postes et groupes avec leur liste de composants à installer.
 - Dans la colonne **Clé en cours**, vous pouvez trouver la liste des clés de l'objet et les paramètres d'installation des composants associés à l'objet.
 - Dans la colonne **Clé assignée**, vous pouvez trouver la clé et les paramètres d'installation des composants spécifiés dans la clé que vous souhaitez assigner aux objets sélectionnés.
 - Si nécessaire, cochez la case **Afficher seulement si différent** pour voir dans la liste uniquement les paramètres des composants qui diffèrent dans les clés assignées et en cours.
2. Pour configurer la liste des composants installés :
 - a) Dans la colonne **Clé assignée**, vous pouvez configurer la liste finale des composants à installer.
 - Les paramètres d'installation des composants dans la colonne **Clé assignée** sont définis d'après l'utilisation autorisée (+) ou non autorisée (-) du composant dans les paramètres actuels et dans ceux de la clé, comme suit :

Paramètres actuels	Paramètres de la clé assignée	Paramètres finaux
+	+	+
-	+	+
+	-	-
-	-	-



- Vous pouvez modifier les paramètres d'installation des composants (rétrograder les droits pour installer) uniquement si les paramètres définis dans la colonne **Clé assignée** permettent d'utiliser ce composant.
- b) Cochez les cases pour les objets (postes et groupes) pour lesquels l'héritage de paramètres sera désactivé et pour lesquels les paramètres d'installation des composants de la colonne **Clé assignée** sont définis comme personnalisés. Pour les autres objets (pour lesquels les cases ne sont pas cochées), les paramètres initiaux de la colonne **Clé assignée** seront hérités.

Paramètres pour ajouter une clé de licence à la liste des clés

Dans cette sous-rubrique, vous trouverez une description de l'installation des composants dans le cadre des procédures suivantes :

- Étendre la liste des clés de licence de l'objet.
- Distribuer une licence à un Serveur voisin avec ajout de clé.

Lorsque vous mettez en oeuvre ces procédures, suivez ces règles pour configurer l'installation des composants :

1. Dans la fenêtre de configuration de l'installation des composants, les objets suivants sont listés :
 - Postes et groupes avec leur liste de composants à installer.
 - Dans la colonne **Clé en cours**, vous pouvez trouver la liste des clés de l'objet et les paramètres d'installation des composants associés à l'objet.
 - Dans la colonne **Clé assignée**, vous pouvez trouver la clé et les paramètres d'installation des composants qui sont spécifiés dans la clé que vous souhaitez ajouter aux objets sélectionnés.
2. Si nécessaire, cochez la case **Afficher seulement si différent** pour voir dans la liste uniquement les paramètres des composants qui diffèrent dans les clés assignées et en cours. Notez qu'à la rubrique **Clé assignée**, seuls les paramètres finaux des composants à installer sont listés et non pas les paramètres de la clé assignée.
3. Pour configurer la liste des composants installés :
 - a) Dans la colonne **Clé assignée**, vous pouvez configurer la liste finale des composants à installer.
 - Les paramètres d'installation des composants dans la colonne **Clé assignée** sont définis d'après l'utilisation autorisée (+) ou non autorisée (-) du composant dans les paramètres actuels et dans ceux de la clé, comme suit :

Paramètres actuels	Paramètres de la clé assignée	Paramètres finaux
+	+	+
-	+	-



Paramètres actuels	Paramètres de la clé assignée	Paramètres finaux
+	–	–
–	–	–

- Vous pouvez modifier les paramètres d'installation des composants (rétrograder les droits pour installer) uniquement si les paramètres définis dans la colonne Clé assignée permettent d'utiliser ce composant.
- b) Cochez les cases pour les objets (postes et groupes) pour lesquels l'héritage de paramètres sera désactivé et pour lesquels les paramètres d'installation des composants de la colonne **Clé assignée** sont définis comme personnalisés. Pour les autres objets (pour lesquels les cases ne sont pas cochées), les paramètres initiaux de la colonne **Clé assignée** seront hérités.

4.5. Schéma d'interaction des composants du réseau antivirus

La [figure 4-2](#) 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 Dr.Web Enterprise Security Suite et des packages antivirus ne nécessitent pas que les postes soient connectés à un LAN, une connexion Internet suffira.

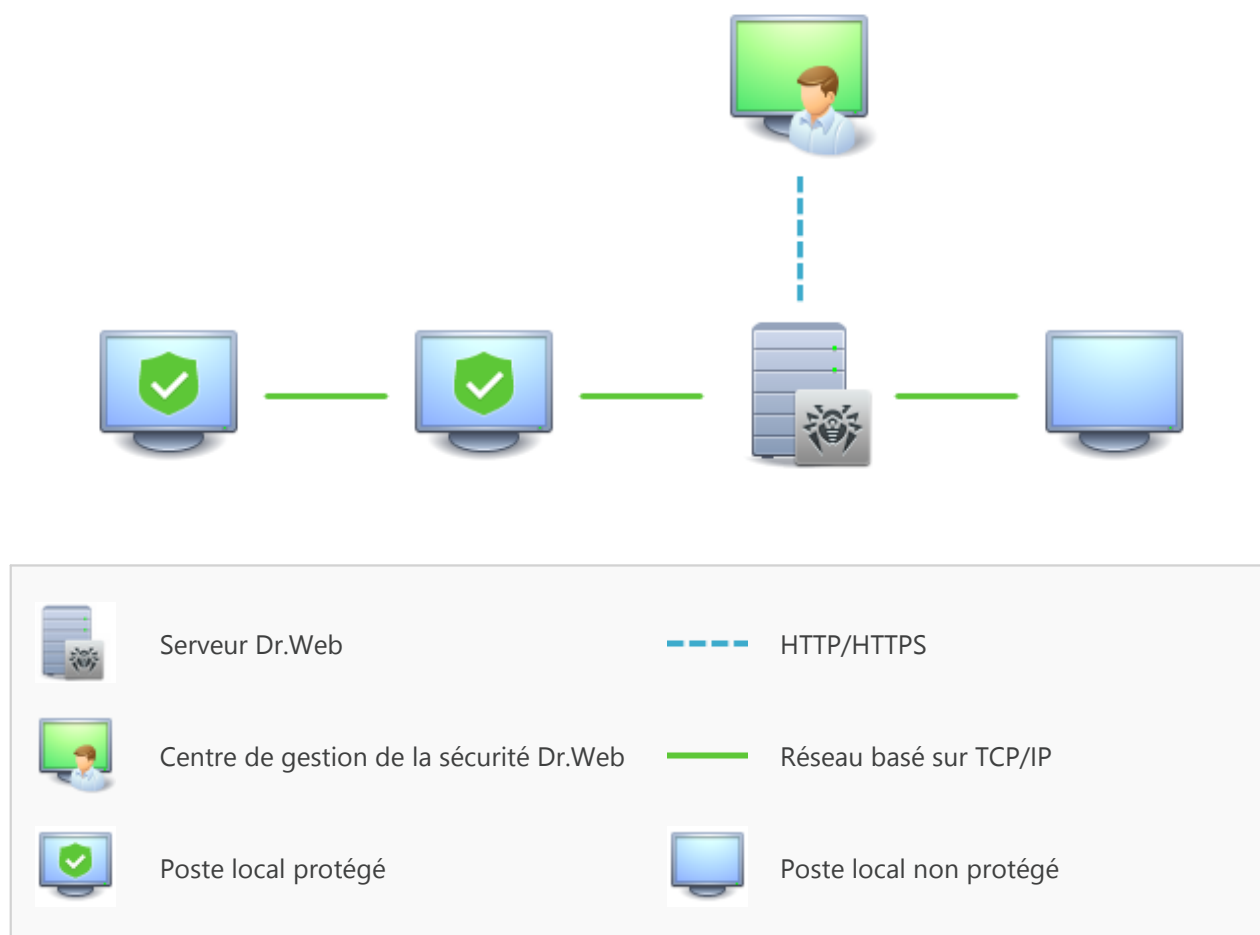


Figure 4-2. Structure du réseau antivirus

Au démarrage du Serveur Dr.Web les actions suivantes sont exécutées :

1. Téléchargement des fichiers du Serveur Dr.Web depuis le répertoire 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 les Agents Dr.Web et des commandes depuis les Centres de gestion.

Tout le flux des commandes, données, informations statistiques dans le réseau antivirus passe obligatoirement par le Serveur Dr.Web. Le Centre de gestion échange des informations uniquement avec le Serveur ; les modifications de la configuration du poste et la transmission des commandes vers l'Agent Dr.Web 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 dans la [figure 4-3](#).

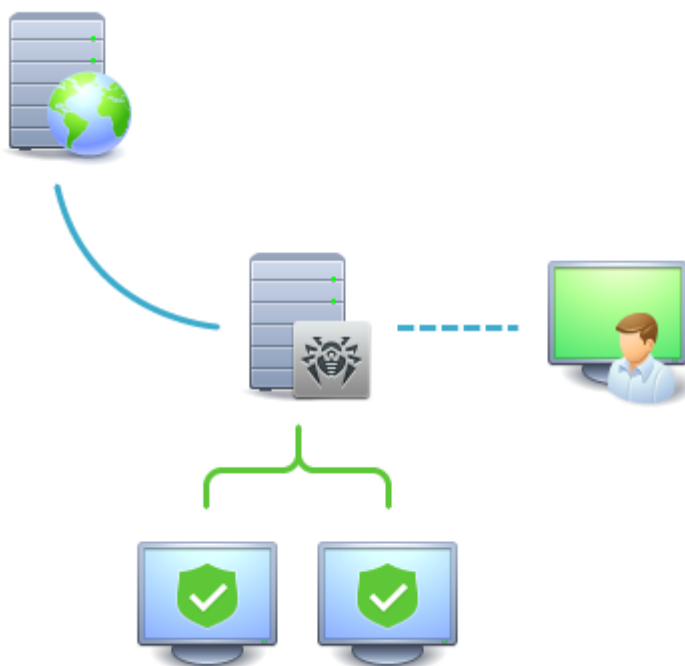


Figure 4-3. Structure logique du réseau antivirus

Entre le Serveur et les postes de travail (trait continu dans la [figure 4-3](#)), 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 Enterprise Security Suite est doté de l'option permettant de compresser le trafic. Pour en savoir plus sur ce mode facultatif, voir ci-dessous le p. [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 le Serveur Dr.Web (trait continu gras dans la [figure 4-3](#)). L'intégrité des informations transmises (fichiers de Dr.Web Enterprise Security Suite et de 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 4-3](#)) 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 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 répertoires d'installation du Serveur Dr.Web. 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 du Serveur Dr.Web requiert un accès illimité au répertoire d'installation du Serveur.

5.1. Authentification des administrateurs

Pour se connecter au Serveur Dr.Web, l'administrateur peut s'authentifier par un des moyens suivants :

1. Via la sauvegarde des données du compte administrateur dans la BD du Serveur.
2. Via Active Directory (Serveurs sous Windows).
3. Via le protocole LDAP.
4. Via le protocole RADIUS.
5. Via PAM (uniquement pour les systèmes sous UNIX).

Les modes d'authentification sont utilisés successivement d'après les règles suivantes :

1. L'ordre d'application des méthodes d'authentification est fonction de leur succession dans les paramètres spécifiés via le Centre de gestion.
2. L'authentification de l'administrateur depuis la BD du Serveur est toujours tentée en premier.
3. Par défaut, la deuxième méthode utilisée est l'authentification via LDAP, la troisième – via Active Directory, la quatrième – via RADIUS, et la cinquième via PAM pour les systèmes sous UNIX.
4. Les méthodes d'authentification via LDAP, Active Directory et RADIUS peuvent être échangées dans les paramètres du Serveur, mais la tentative d'authentification de l'administrateur depuis la BD sera toujours la première.
5. L'authentification via LDAP, Active Directory et RADIUS est désactivée par défaut.

Pour modifier l'ordre des 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. Dans la fenêtre qui s'ouvre, une liste des types d'authentification par ordre d'utilisation apparaît. Pour modifier l'ordre, glissez-déposez (drag'n'drop) les modes d'authentification dans l'ordre dans lequel il faut effectuer l'authentification.
4. Redémarrez le Serveur pour appliquer les modifications.



Le login administrateur doit être unique.

Les administrateurs ne sont pas autorisés à se connecter via des systèmes d'authentification externes si un administrateur ayant le même login existe déjà sur le Serveur.

A chaque enregistrement des modifications de la section **Authentification**, une copie de sauvegarde de la version précédente du fichier de configuration est automatiquement enregistrée avec les paramètres d'authentification d'administrateurs. 10 dernières copies sont sauvegardées.

Les copies de sauvegarde se trouvent dans le même répertoire où se trouve le fichier de configuration et elles portent les noms conformes au format suivant :

`<nom_de_fichier> ; <date_et_heure_de_création>`

où `<nom_de_fichier>` dépend du système d'authentification : `auth-ads.xml`, `auth-ldap.xml`, `auth-radius.xml`, `auth-pam.xml`.

Vous pouvez utiliser les copies de sauvegarde créées, notamment pour restaurer le fichier de configuration si l'interface du Centre de gestion n'est pas disponible.

5.1.1. Authentification des administrateurs depuis la BD du Serveur

Le mode d'authentification dans lequel les données sur les 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 [Administrateurs et groupes administrateur](#).

5.1.2. Authentification via 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**.
6. Redémarrez le Serveur pour appliquer les modifications.

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 `drweb-esuite-modify-ad-schema-xxxxxxxxxxxxxxxx-windows-nt-xYY.exe` (inclus dans la distribution du Serveur Dr.Web).

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.



Si auparavant vous avez déjà modifié le schéma Active Directory à l'aide de cet utilitaire de la version 6 du Serveur, il n'est pas nécessaire d'effectuer la modification encore une fois à l'aide de l'utilitaire de la version 10 du Serveur.

- 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-xxxxxxxxxxxxxxxx-windows-nt-xYY.msi` (inclus dans le package d'installation Dr.Web Enterprise Security Suite 10) 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** → dans la 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.



Vous pouvez consulter les algorithmes relatifs au fonctionnement et à l'analyse des attributs lors de l'authentification dans les **Annexes**, [Annexe C1](#).

5.1.3. Authentification via 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**.
6. Redémarrez le Serveur pour appliquer les modifications.

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 les **Annexes**, la rubrique [Annexe C2](#).

A la différence d'Active Directory, le mécanisme peut être configuré conformément à n'importe quel 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 forcée du schéma LDAP n'est requise. 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.

5.1.4. Authentification via RADIUS

Pour activer l'authentification via RADIUS :

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 RADIUS**.
4. Cochez la case **Utiliser l'authentification RADIUS**.
5. Cliquez sur **Sauvegarder**.
6. Redémarrez le Serveur pour appliquer les modifications.

Pour utiliser le protocole d'authentification via RADIUS, vous devez installer un serveur qui supporte ce protocole, par exemple, freeradius (pour en savoir plus, voir <http://freeradius.org/>).

Dans le Centre de gestion, vous pouvez configurer les paramètres suivants pour la communication avec le serveur RADIUS :

- **Serveur, Port, Mot de passe** – paramètres de connexion au serveur RADIUS : adresse IP/nom DNS, numéro de port, mot de passe (secret) correspondant.
- **Délai** – délai d'attente de la réponse du serveur RADIUS, en secondes.
- **Nombre de tentatives** – nombre maximum de tentatives de connexion au serveur RADIUS.

Vous pouvez également configurer des paramètres RADIUS supplémentaires via les outils suivants :

- Le fichier de configuration `auth-radius.xml` situé dans le répertoire etc du Serveur.

Outre les paramètres spécifiés via le Centre de gestion, vous pouvez indiquer, dans le fichier de configuration, la valeur de l'identificateur NAS. Cet identificateur, d'après le RFC 2865, peut être



utilisé au lieu de l'adresse IP/ nom de domaine DNS, comme un identificateur du client pour la connexion au serveur RADIUS. Il est sauvegardé dans le fichier de configuration sous cette forme :

```
<!-- NAS identifier, optional, default - hostname -->  
<nas-id value="drwcs" />
```

- Le dictionnaire `dictionary.drweb` situé dans le répertoire `etc` du Serveur.
Le dictionnaire sauvegarde l'ensemble des attributs RADIUS de la société Doctor Web (VSA – Vendor-Specific Attributes).

5.1.5. Authentification via PAM

Pour activer l'authentification via PAM :

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 PAM**.
4. Cochez la case **Utiliser l'authentification PAM**.
5. Cliquez sur **Sauvegarder**.
6. Redémarrez le Serveur pour appliquer les modifications.

L'authentification PAM sous les OS de la famille UNIX est effectuée en utilisant des plugins d'authentification.

Pour configurer les paramètres d'authentification PAM, vous pouvez utiliser l'un des moyens suivants :

- Configurez les modes d'authentification via le Centre de gestion : dans la rubrique **Administration** → **Authentification** → **Authentification PAM**.
- Le fichier de configuration `auth-pam.xml` situé dans le répertoire `etc` du Serveur. Exemple de fichier de configuration :

```
...  
<!-- Enable this authorization module -->  
<enabled value="no" />  
<!-- This authorization module number in the stack -->  
<order value="50" />  
<!-- PAM service name -->  
<service name="drwcs" />  
<!-- PAM data to be queried: PAM stack must return INT zero/non-zero -->  
<admin-flag mandatory="no" name="DrWeb_ESuite_Admin" />  
...
```



Description des paramètres d'authentification PAM configurés du côté de Dr.Web Enterprise Security Suite

Rubriques du Centre de gestion	Articles du fichier auth-pam.xml			Description
	Bloc	Para-mètre	Valeurs auto-risées	
Case Utiliser l'authentification PAM	<code><enabled></code>	<code>value</code>	yes no	Case qui détermine si la méthode d'authentification via PAM est utilisée.
Utiliser Drag and Drop	<code><order></code>	<code>value</code>	nombre entier positif, coordonné avec d'autres valeurs de méthodes	Numéro de série de l'authentification PAM si plusieurs méthodes sont utilisées.
Champ Nom du Service	<code><service></code>	<code>name</code>	-	Nom du service utilisé pour créer un contexte PAM. PAM peut lire les politiques via ce service depuis <code>/etc/pam.d/<service name></code> ou depuis <code>/etc/pam.conf</code> , si le fichier n'existe pas. Si le paramètre n'est pas configuré (il n'y a pas de tag <code><service></code> dans le fichier de configuration), le nom <code>drwcs</code> est utilisé par défaut.
La case La case de contrôle doit être cochée	<code><admin-flag></code>	<code>mandatory</code>	yes no	Ce paramètre détermine si l'indicateur de contrôle permettant d'identifier un utilisateur comme administrateur est obligatoire. Par défaut – <code>yes</code> .
Champ Nom de la case de contrôle	<code><admin-flag></code>	<code>name</code>	-	Element de la clé d'après lequel les modules PAM lisent la case. Par défaut – <code>DrWeb_ESuite_Admin</code> .

Lors de la configuration du fonctionnement des modules d'authentification PAM, utilisez les paramètres définis du côté de Dr.Web Enterprise Security Suite, et prenez en compte les valeurs utilisées par défaut si les paramètres ne sont pas spécifiés.



5.2. Administrateurs et groupes administrateur

Pour ouvrir le module de contrôle des comptes administrateurs, choisissez **Administration** dans le menu principal du Centre de gestion, puis, dans la nouvelle rubrique ouverte, choisissez la rubrique du menu de gestion **Administrateurs**.



Le sous-menu **Administrateurs** est accessible à tous les administrateurs du Centre de gestion. L'arborescence complète des administrateurs est accessible uniquement aux membres du groupe **Administrateurs** qui possèdent le droit **Voir les propriétés et la configuration des groupes Administrateurs**. Les autres administrateurs verront uniquement leurs groupes respectifs avec les sous-groupes et les comptes.

5.2.1. Hiérarchie des administrateurs

La visualisation de la hiérarchie des administrateurs est une arborescence qui représente la structure des groupes administrateurs et des comptes administrateurs. Les groupes administrateurs et leurs membres (les comptes administrateurs) peuvent être chacun des noeuds de cette arborescence. Chaque administrateur peut être membre d'un groupe seulement. Le niveau d'emboîtement des groupes dans l'arborescence n'est pas limité.

Groupes prédéfinis

Après l'installation du Serveur, deux groupes sont créés automatiquement :

- **Administrators**. Le groupe contient initialement uniquement l'administrateur **admin** avec un ensemble complet de privilèges. L'utilisateur admin est automatiquement créé durant l'installation du Serveur Dr.Web (voir ci-dessus).
- **Newbies**. Le groupe est initialement vide. Les administrateurs possédant un type d'authentification externe, comme LDAP, Active Directory ou RADIUS, seront automatiquement placés dans ce groupe.

Par défaut, les administrateurs du groupe **Novices** possèdent un accès en lecture seule.

Administrateurs prédéfinis

Après l'installation du Serveur, un compte administrateur est automatiquement créé :

Paramètre	Valeur
Nom du compte	admin
Mot de passe	Le mot de passe est spécifié lors de l'installation du Serveur (étape 9 de la procédure d'installation).
Droits	Ensemble complet de droits.



Paramètre	Valeur
Éditer le compte	Les droits administrateur ne peuvent pas être édités. Le compte administrateur ne peut pas être supprimé.

Affichage des listes hiérarchiques

- Dans la liste hiérarchique du réseau antivirus, l'administrateur ne voit que des groupes utilisateur qui sont autorisés dans le droit **Consulter les propriétés des groupes du poste**. Tous les groupes système sont affichés dans l'arborescence du réseau antivirus, mais on y voit uniquement les postes de la liste indiquée des groupes utilisateur.
- Dans la liste hiérarchique des administrateurs : l'administrateur du groupe **Novices** voit l'arborescence dont la racine est le groupe dont il fait partie. C'est-à-dire, il voit les administrateurs de son groupe et de ses sous-groupes. L'administrateur du groupe **Administrateurs** voit tous les administrateurs indépendamment de leurs groupes.

5.2.2. Droits d'administrateurs

Toute l'activité des administrateurs dans le Centre de gestion est limitée par les droits qui peuvent être définis pour un compte unique ou pour un groupe d'administrateurs.

Le système de droits administrateur inclut les options de gestion des droits suivantes :

- **Octroi de droits**

L'octroi de droits est effectué durant la création du compte administrateur ou du groupe administrateur. Lorsqu'un administrateur ou un compte administrateur est créé, il hérite des droits du groupe parent auquel il est rattaché. La modification des droits n'est pas possible durant la création.

- **Héritage de droits**

Par défaut, les droits des administrateurs et des groupes administrateurs sont hérités des groupes parents correspondants, mais la procédure peut varier.

- Si l'héritage est désactivé, l'administrateur utilise l'ensemble indépendant des paramètres personnels qui est spécifié pour son compte. Les droits du groupe parent ne sont pas pris en compte.
- L'héritage des droits d'un administrateur ou d'un groupe ne les réaffecte pas du « parent » à « l'enfant » mais établit un nouvel ensemble de privilèges basé sur tous les droits des groupes parents dans la branche de l'arborescence. Dans le p. [Fusionner les droits](#), vous pouvez consulter le tableau de calcul du droit résultant de l'objet en fonction des droits assignés et des droits de groupes parent.



• Modification des droits

Lors de la création d'administrateurs ou de groupes administrateurs, la modification des droits n'est pas autorisée. Les droits peuvent être modifiés uniquement pour les objets déjà créés, dans la section des paramètres d'un compte ou d'un groupe. Lors de la modification des paramètres personnels, seule la baisse des droits est possible. La modification des droits de l'administrateur prédéfini **admin** et des groupes prédéfinis **Administrators** et **Newbies** n'est pas autorisée.

La procédure de la modification des droits est décrite dans la section [Modification des droits](#).

Modification des droits

Pour modifier les droits d'administrateur ou de groupe administrateur :

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion, et dans la fenêtre qui s'ouvre, choisissez la rubrique **Administrateurs** dans le menu de gestion.
2. Sélectionnez le compte que vous souhaitez éditer dans la liste des administrateurs. La fenêtre de ses propriétés va s'ouvrir.
3. Dans la sous-rubrique **Droits**, vous pouvez modifier la liste des actions autorisées pour l'administrateur ou le groupe administrateur sélectionné.
4. Pour gérer l'héritage des droits du groupe parent pour l'objet sélectionné, utilisez l'interrupteur :



L'héritage est activé



L'héritage est désactivé

5. Les paramètres généraux sont spécifiés dans le tableau de droits :
 - a) Dans la première colonne s'affichent les noms des droits. L'en-tête de la colonne dépend d'une section spécifique fusionnant les droits par types.



Pour en savoir plus sur les droits des administrateurs et les rubriques du Centre de gestion qui sont à la charge des droits particuliers, consultez les **Annexes**, le paragraphe [Annexe C3](#).

- b) Dans la colonne **Droits**, vous trouverez les paramètres pour les droits correspondants de la première colonne.


Objets de gestion	Liste des paramètres de la colonne Droits	Principe de spécification du droit
Le droit est spécifié pour tous les objets		
Le droit n'implique pas la division en groupes par objets de gestion.	L'un des types de droits suivants peut être cité :	Dans la ligne du droit correspondant, cochez/décochez la case Accorder .



Objets de gestion	Liste des paramètres de la colonne Droits	Principe de spécification du droit
	<ul style="list-style-type: none">• Personnel – les paramètres personnels sont spécifiés pour cet objet.• Hérité – les paramètres sont hérités du groupe parent.	
Le droit est spécifié pour la liste d'objets (de postes, d'administrateurs ou de groupes)		
<ul style="list-style-type: none">• <i>Tout est accordé</i> – le droit est accordé pour tous les objets de gestion.• <i>Tout est interdit</i> – le droit est interdit pour tous les objets de gestion.• <i>Accordé pour certains objets</i>. Dans ce cas, vous devez spécifier la liste des objets pour lesquels ce droit est accordé. Pour les autres objets, le droit est considéré comme interdit.• <i>Interdit pour certains objets</i>. Dans ce cas, vous devez spécifier la liste des objets pour lesquels ce droit est interdit. Pour les autres objets, le droit est considéré comme accordé.	<p>En cas de fusion des paramètres, les types de droits suivants sont affichés :</p> <ul style="list-style-type: none">• Personnel – paramètres personnels spécifiés pour cet objet.• Résultant – résultat de la fusion du droit personnel de l'objet et du droit du groupe parent. <p>En cas d'héritage des paramètres, seul le type de droits Hérité s'affiche.</p>	<p>Cliquez sur la liste des objets (même si, l'option Tous est spécifiée). La fenêtre qui s'ouvre contient l'arborescence du réseau antivirus, l'arborescence des groupes administrateurs ou l'arborescence des tarifs en fonction du droit modifié. Sélectionnez dans l'arborescence les objets nécessaires. Utilisez les boutons CTRL и SHIFT pour sélectionner plusieurs objets. Si nécessaire, cochez la case Pour tous les droits de la section pour appliquer ces paramètres à tous les droits se trouvant dans la même section que le droit modifié.</p> <p>Cliquez sur le bouton :</p> <ul style="list-style-type: none">• Accorder pour accorder les droits aux objets sélectionnés.• Interdire pour interdire les droits aux objets sélectionnés.



On ne peut pas spécifier en même temps les listes des objets interdits et autorisés pour le même droit. Ces notions s'excluent mutuellement.

- c) Dans la colonne **Héritage** s'affiche le statut de ce droit par rapport au groupe parent :
- **Héritage du groupe** – l'héritage du groupe parent spécifié est activé, les droits personnels ne sont pas spécifiés.
 - **Paramètres personnels** – l'héritage du groupe parent est désactivé, les droits personnels sont spécifiés.
 - **Fusion avec le groupe** – l'héritage du groupe parent indiqué est activé, les droits personnels sont spécifiés. Le droit résultant est calculé par la fusion des droits du groupe parent avec les droits personnels. (voir le p. [Fusion des droits](#)). Dans ce cas, vous pouvez supprimer les droits personnels de l'objet. Pour ce faire, cliquez sur le bouton  dans la colonne **Héritage**. Une fois les droits personnels supprimés, l'**Héritage du groupe** sera établi.



Fusionner les droits

Le calcul du droit résultant de l'objet (l'administrateur ou le groupe d'administrateur) en cas de l'héritage activé dépend des droits de groupes parents et des droits spécifiés pour l'objet. Le tableau ci-dessous décrit le principe d'obtention du droit résultant de l'objet :

Droit du groupe parent	Droit de l'enfant en question	Droit calculé (résultat)
Tout est accordé	Accordé pour certains objets	Accordé pour les objets de l'enfant
Accordé pour certains objets	Accordé pour certains objets	Les listes des objets autorisés sont fusionnés
Accordé pour certains objets	Tout est accordé	Tout est accordé
Les droits du parent et de l'enfant sont interdisants. L'un des droits interdit tout		Tout est interdit
Interdit pour certains objets	Interdit pour certains objets	Les listes des objets interdits sont fusionnés
Tout est interdit	Tout est accordé	Tout est accordé
Interdit pour certains objets	Tout est accordé	Interdit pour les objets du parent
Interdit pour certains objets	Accordé pour certains objets	Les objets autorisés sont exclus des objets interdits. Si, après cela, la liste des objets interdits n'est pas vide, les objets restants sont interdits. Sinon, tous les objets de l'enfant sont autorisés
Accordé pour certains objets	Tout est interdit	Tout est interdit
Tout est accordé	Interdit pour certains objets	Interdit pour les objets de l'enfant
Accordé pour certains objets	Interdit pour certains objets	Les objets interdits sont exclus des objets autorisés. Si, après cela, la liste des objets autorisés n'est pas vide, tous les objets sont interdits. Sinon, tous les objets restants sont autorisés.



5.3. Gestion des comptes et des groupes administrateur

5.3.1. Création et suppression des comptes et des groupes administrateur



Le login administrateur doit être unique.

Les administrateurs ne sont pas autorisés à se connecter via des systèmes d'authentification externes si un administrateur ayant le même login existe déjà sur le Serveur.

Ajout d'un compte administrateur



Pour créer des comptes administrateurs, l'administrateur doit posséder le droit de **Créer des comptes administrateur, groupes administrateur**.

Marche à suivre pour ajouter un nouveau compte administrateur :

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion, et dans la fenêtre qui s'ouvre, choisissez la rubrique **Administrateurs** dans le menu de gestion.
2. Cliquez sur **Créer un compte** dans la barre d'outils. Une fenêtre contenant les paramètres de création d'un compte va s'ouvrir.
3. Dans la sous-rubrique **Général**, configurez les paramètres suivants :
 - Dans le champ **Login**, spécifiez le login du compte administrateur pour accéder au Centre de gestion. Il est possible d'utiliser des lettres minuscules (a-z), des majuscules (A-Z), des chiffres (0-9) et des caractères « _ » et « . ».
 - Dans la liste **Type d'authentification**, sélectionnez une des variantes suivantes :
 - **Interne** – l'authentification de l'administrateur dans le Centre de gestion est fondée sur les identifiants dans la BD du Serveur Dr.Web.
 - **Externe** – l'authentification de l'administrateur dans le Centre de gestion est effectuée via les systèmes externes LDAP, Active Directory ou RADIUS.



Pour en savoir plus, voir [Authentification des administrateurs](#).

- Dans les champs respectifs **Mot de passe** et **Confirmez le mot de passe**, spécifiez un mot de passe pour accéder au Serveur et au Centre de gestion.



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



Les champs de spécification du mot de passe sont actifs uniquement pour les administrateurs à l'authentification interne.



Les valeurs des champs spécifiés dans le Centre de gestion pour les administrateurs avec l'authentification externe n'ont pas d'importance.

- 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 (la langue du navigateur ou l'anglais est spécifié par défaut).
- 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 : JJ-MM-AAAA HH:MM:SS
 - américain : MM/JJ/AAAA HH:MM:SS
- Dans le champ **Description**, vous pouvez indiquer une description du compte.



Les valeurs des champs marqués du symbole *, doivent être obligatoirement spécifiées.

4. Dans la sous-rubrique **Groupes**, vous pouvez indiquer le groupe parent administrateur. La liste contient des groupes auxquels un administrateur peut être assigné. La case est cochée contre le groupe auquel l'administrateur créé sera rattaché. Par défaut, les administrateurs créés sont placés dans le groupe parent de l'administrateur actuel. Pour modifier le groupe assigné, cochez la case contre le groupe nécessaire.

Chaque administrateur peut être membre d'un seul groupe.

L'administrateur hérite ses droits du groupe parent (voir [Droits d'administrateurs](#)).

5. Après la configuration des paramètres, cliquez sur **Sauvegarder** pour créer un nouveau compte administrateur.

Ajouter des groupes administrateurs



Pour créer des groupes administrateurs, l'administrateur doit posséder le droit de **Créer des comptes administrateur, groupes administrateur**.

Pour ajouter un nouveau groupe administrateur :

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion, et dans la fenêtre qui s'ouvre, choisissez la rubrique **Administrateurs** dans le menu de gestion.
2. Cliquez sur l'icône **Créer un groupe** dans la barre d'outils. Une fenêtre contenant les paramètres de création d'un groupe va s'ouvrir.
3. Dans la sous-rubrique **Général**, configurez les paramètres suivants :
 - Dans le champ **Groupe**, spécifiez le nom du groupe administrateur pour accéder au Centre de gestion. Il est possible d'utiliser des lettres minuscules (a-z), des majuscules (A-Z), des chiffres (0-9) et des caractères « _ » et « . ».



- Dans le champ **Description**, vous pouvez donner une description facultative du groupe.
4. Dans la sous-rubrique **Groupes**, vous pouvez indiquer le groupe administrateur parent. La liste contient des groupes qui peuvent être définis comme groupes parents. La case est cochée contre le groupe dans lequel le groupe administrateur créé sera inclus. Par défaut, les groupes créés sont placés dans le groupe parent de l'administrateur actuel. Pour modifier le groupe assigné, cochez la case près du groupe nécessaire.

Seul un groupe parent peut être assigné.

Le groupe administrateur hérite des droits du groupe parent (voir p. [Droits d'administrateurs](#)).

5. Après la configuration de tous les paramètres, cliquez sur **Sauvegarder** pour créer un nouveau groupe administrateur.

Suppression des administrateurs et des groupes administrateur



Pour supprimer les comptes administrateurs ou les groupes administrateurs, vous devez posséder les droits de **Supprimer les comptes administrateurs** et **Modifier les propriétés et la configuration des groupes administrateur**.

Pour supprimer un compte administrateur ou un groupe, procédez comme suit :

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion, et dans la fenêtre qui s'ouvre, choisissez la rubrique **Administrateurs** dans le menu de gestion.
2. Depuis la liste des administrateurs, sélectionnez le compte ou le groupe administrateur à supprimer.
3. Sélectionnez depuis la barre d'outils le bouton **X Supprimer les objets sélectionnés**.

5.3.2. Éditer les comptes et les groupes administrateur



Pour éditer les comptes administrateurs ou les groupes administrateurs, vous devez posséder les droits **Éditer les comptes administrateurs** et **Éditer les privilèges de configuration des propriétés des comptes administrateurs**.

Pour pouvoir éditer votre compte, vous devez posséder le droit **Modifier vos propres paramètres**.


Les valeurs des champs marqués du symbole *, doivent être obligatoirement spécifiées.

Éditer un compte administrateur

Pour éditer un compte administrateur :

1. Sélectionnez le compte que vous souhaitez éditer dans la liste des administrateurs. La fenêtre de ses propriétés va s'ouvrir.



2. La sous-rubrique **Général** contient les propriétés qui ont été configurées durant la [Création](#) d'un compte. Ainsi :
 - a) Pour changer de mot de passe du compte administrateur, cliquez sur l'icône  **Changer de mot de passe** dans la barre d'outils.



Un administrateur possédant ces droits peut modifier les mots de passe de tous les administrateurs.



Le login du compte administrateur ne peut pas contenir de caractères nationaux.

- b) Les propriétés suivantes du compte administrateur sont en lecture seule :
 - Date de la création du compte et date de la dernière modification de ses paramètres,
 - **Statut** – affiche les adresses réseau de la dernière connexion sous le compte actuel.
3. Dans la sous-rubrique **Groupes**, vous pouvez modifier un groupe administrateur. La liste contient des groupes auxquels un administrateur peut être rattaché. La case est cochée près du groupe parent actuel de l'administrateur. Pour modifier le groupe assigné, cochez la case près du groupe nécessaire.

Il est obligatoire d'assigner un groupe parent à l'administrateur. Chaque administrateur peut être inclus à un seul groupe à la fois. Les droits de l'administrateur sont hérités du groupe parent assigné.

Voir aussi la sous-section [Modification de l'appartenance](#).
4. Dans la sous-rubrique **Droits**, vous pouvez modifier la liste des actions autorisées pour l'administrateur sélectionné.

La modification des droits est décrite dans la sous-rubrique [Modifier les droits](#).
5. Cliquez sur **Enregistrer** pour appliquer les modifications.

Modifier les groupes administrateur

Pour modifier un groupe administrateur :

1. Sélectionnez le groupe que vous souhaitez éditer dans la liste des administrateurs. La fenêtre de ses propriétés va s'ouvrir.
2. La sous-rubrique **Général** contient les propriétés qui ont été configurées durant la [création](#) d'un groupe.
3. Dans la sous-rubrique **Groupes** vous pouvez modifier le groupe administrateur parent. La liste contient des groupes qui peuvent être définis comme groupe parent. La case est cochée près du groupe parent actuel. Pour modifier le groupe assigné, cochez la case près du groupe nécessaire.

Il est obligatoire d'assigner un groupe parent au groupe administrateur. Le groupe hérite des droits de son groupe parent assigné.

Voir aussi la sous-section [Modification de l'appartenance](#).



4. Dans la sous-rubrique **Droits**, vous pouvez modifier la liste des actions autorisées pour le groupe administrateur sélectionné.

La modification des droits est décrite dans la sous-rubrique [Modifier les droits](#).

5. Cliquez sur **Enregistrer** pour appliquer les modifications.

Modifier l'appartenance

Il existe plusieurs moyens d'assigner un groupe parent à un administrateur ou à un groupe administrateur :

1. Modifiez les paramètres de l'administrateur ou du groupe comme décrit [ci-dessus](#).
2. Glissez/déposez (drag-and-drop) l'administrateur ou le groupe administrateur depuis la liste hiérarchique vers le groupe que vous souhaitez désigner comme parent.



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.

La fusion des postes en groupes permet d'effectuer 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](#)).
- Organisations (de 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

Initialement, Dr.Web Enterprise Security Suite comprend un jeu de groupes système pré-installés. Ces groupes sont créés au moment de l'installation de Serveur Dr.Web et ne peuvent pas être supprimés. Cependant si nécessaire, l'administrateur peut les masquer.

Chaque groupe système (sauf le groupe **Everyone**) contient un jeu de sous-groupes qui sont rassemblés par une caractéristique particulière.



Après l'installation du Serveur et jusqu'au moment de la connexion de postes au Serveur, seul le groupe **Everyone** est affiché dans le groupe. Pour afficher tous les groupes système utilisez l'option **Afficher les groupes masqués** dans la rubrique **Paramètres d'affichage de l'arborescence** dans la [barre d'outils](#).

Everyone

Groupe comprenant tous les postes connus par le Serveur Dr.Web. Le groupe **Everyone** comprend les paramètres de tous les groupes et les postes par défaut.



Configured

Le groupe comprend les postes pour lesquels les paramètres personnels ne sont pas spécifiés.

Operating system

Cette catégorie de sous-groupes affiche les système d'exploitation sous lesquels tournent les postes en ce moment. Ces groupes ne sont pas virtuels, ils peuvent contenir les paramètres de postes et servir de groupes primaires.

- Sous-groupes de la famille **Android**. Cette famille contient un jeu de groupes correspondant à une version particulière du système d'exploitation Android pour les appareils mobiles.
- Sous-groupes de la famille **OS X**. Cette famille contient l'ensemble de groupes correspondant à une version particulière du système d'exploitation 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 une version particulière du système d'exploitation Windows.

Status

Le groupe **Status** contient les groupes emboîtés affichent le statut actuel de postes : s'ils sont connectés au Serveur en ce moment ou pas, et le statut du logiciel antivirus : si le logiciel est désinstallé ou que la période d'utilisation a expiré. Ces groupes sont complètement virtuels et ne peuvent contenir aucuns paramètres, il ne peuvent pas servir de groupes primaires non plus.

- Groupe **Deinstalled**. Une fois le logiciel de l'Agent Dr.Web est désinstallé, le poste passe automatiquement en 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 **New**. Ce groupe comprendt les nouveaux postes qui ont été créés par l'administrateur via le Centre de gestion, mais on n'a pas encore installé l'Agent sur ces postes.
- Groupe **Newbies**. Ce groupe comprend tous les postes non approuvés dont l'enregistrement sur le Serveur n'a pas encore été confirmé. En cas d'approbation de l'enregistrement ou si l'accès du poste au Serveur est refusé, les postes seront retirés du groupe de manière automatique (pour en savoir plus, voir la rubrique [Politique d'approbation 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 au serveur à un certain moment (répondant aux requêtes du Serveur).
- Groupe **Update Errors**. Contient tous les postes dont la mise à jour a échoué.



Transport

Ces sous-groupes déterminent le protocole via lequel les postes sont connectés au Serveur en ce moment. Ces sous-groupes sont complètement virtuels et ne peuvent contenir aucuns paramètres, il ne peuvent pas servir de groupes primaires non plus.

- Groupe **TCP/IP**. Le groupe comprend les postes qui en ce moment sont connectés via le protocole TCP/IP de la version 4.
- Groupe **TCP/IP Version 6**. Le groupe comprend les postes qui en ce moment sont connectés via le protocole TCP/IP de la version 6.

Ungrouped

Le groupe comprend les postes qui n'appartiennent à 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.

Pour plus de commodité, le tableau [6-1](#) comprend tous les groupes et les types de groupes possibles ainsi que les paramètres typiques qui sont supportés (+) ou ne sont pas supportés (-) par ces groupes.

Les paramètres suivants sont décrits :

- **Appartenance automatique**. Le paramètre détermine la possibilité de l'intégration automatique du poste dans le groupe (support de la maintenance automatique) et la modification automatique du contenu du groupe lors du fonctionnement du Serveur.
- **Gestion de l'appartenance**. Le paramètre détermine la possibilité de l'administrateur de gérer l'appartenance dans le groupe : ajouter et supprimer les postes du groupe.
- **Groupe primaire**. Le paramètre détermine si ce groupe peut être primaire pour le poste.
- **Contenu des configurations**. Le paramètre détermine si le groupe peut contenir les paramètres des composants antivirus (pour que les postes puissent les hériter).

Tableau 6-1. Groupes et paramètres supportés

Groupe/type de groupe	Paramètre			
	Appartenance automatique	Gestion de l'appartenance	Groupe primaire	Contenu des configurations
Everyone	+	-	+	+



Groupe/type de groupe	Paramètre			
	Appartenance automatique	Gestion de l'appartenance	Groupe primaire	Contenu des configurations
Configured	+	-	-	-
Operating System	+	-	+	+
Status	+	-	-	-
Transport	+	-	-	-
Ungrouped	+	-	-	-
Groupes utilisateurs	-	+	+	+



Sous le compte *administrateur du groupe*, le groupe utilisateur qu'il gère s'affiche dans la racine de l'arborescence même s'il possède le groupe parent. Dans ce cas tous les groupes enfant sont accessibles depuis le groupe géré.

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**.
6. Cliquez sur **Enregistrer**.




Au départ, les groupes que vous avez créés sont vides. La procédure d'ajout des postes dans les groupes est décrite dans la rubrique [Placement de postes de travail dans des groupes utilisateur](#).

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. Ouvrez la rubrique de configuration du groupe d'une des façons suivantes :
 - a) Cliquez sur le nom du groupe dans la liste hiérarchique du réseau antivirus. La section contenant les propriétés du groupe va s'afficher automatiquement dans la partie droite du Centre de gestion.
 - b) Sélectionnez l'élément **Propriétés** du [menu de gestion](#). La fenêtre contenant les propriétés du groupe de postes va s'ouvrir.
3. La fenêtre de configuration du groupe 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 la partie droite du Centre de gestion (voir p.2.a)), vous pouvez accéder à la rubrique **Informations sur les postes** affichant des informations sur les postes faisant partie du groupe en question.

4. Pour enregistrer les modifications apportées, cliquez sur le bouton **Enregistrer**.

Général

La rubrique **Général** comprend les champs suivants :

- **Identificateur** – identificateur unique du groupe. Il est protégé contre l'édition.
- **Nom** – nom du groupe. Si nécessaire, vous pouvez le modifier. Pour les groupes préinstallés, le champ **Nom** ne peut pas être modifié.



- **Groupe parent** – le groupe parent dont le groupe en question fait partie et duquel il hérite sa configuration à moins que les paramètres personnalisés ne soient spécifiés. Si aucun groupe supérieur n'est spécifié, les configurations seront héritées depuis le groupe **Everyone**.
- **Description** – champ facultatif contenant une description du groupe.

Informations sur les postes

La rubrique **Informations sur les postes** comprend les champs suivants :






- **Postes** – total de postes appartenant à un groupe sélectionné.
- **Groupe primaire pour** – total de postes pour lesquels ce groupe est un groupe primaire.
- **Postes sur réseau** – total de postes dans ce groupe qui sont sur réseau à l'heure actuelle (online).

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 :

Icône	Paramètres	Rubrique contenant la description
	Droits des utilisateurs des postes, qui héritent ce paramètre d'un groupe s'il est défini comme primaire. La configuration des droits des groupes est identique à la configuration des droits des postes séparés.	Droits des utilisateurs du poste
	Planification centralisée d'une tâche pour les postes, qui héritent ce paramètre d'un groupe s'il est défini comme primaire. Configurer la planification pour un groupe est identique à la configuration de la planification centralisée pour les postes séparés.	Planification des tâches sur un poste
	Fichier clé de licence pour les postes, qui héritent ce paramètre d'un groupe s'il est défini comme primaire.	Gestionnaire de licences
	Restrictions dans la mise à jour du logiciel sur les postes, qui héritent ce paramètre d'un groupe s'il est défini comme primaire.	Restrictions de mises à jour des postes
	Liste des composants à installer sur les postes qui héritent ce paramètre d'un groupe s'il est défini comme primaire. La configuration de la liste des composants d'un groupe est identique à celle de la liste des composants pour les postes séparés.	Composants à installer du package antivirus



Icône	Paramètres	Rubrique contenant la description
	Configuration du placement automatique de postes dans ce groupe. Disponible uniquement pour les groupes utilisateur.	Configuration de l'appartenance automatique au groupe
	Paramètres des composants antivirus. La configuration des composants du package antivirus d'un groupe est identique à celle des composants du package antivirus des postes.	Configuration des composants antivirus

Le nombre des groupes emboîtés avec l'héritage interrompu et leurs propres paramètres personnels (s'il y en a) est indiqué dans la section **Configuration** pour les groupes dont les paramètres personnels sont spécifiés. Si vous cliquez sur cette option, dans la fenêtre qui s'affiche, vous trouverez la liste des groupes dont les noms et les identificateurs sont indiqués.

6.3. Placement de postes de travail dans des groupes utilisateur

Dr.Web Enterprise Security Suite fournit les moyens suivant de placement de postes dans des groupes utilisateur :

1. [Placement manuel de postes dans des groupes.](#)
2. [Utilisation des règles d'appartenance automatique au groupe.](#)

6.3.1. Placement manuel de postes dans des groupes

Il existe plusieurs façons d'ajouter manuellement des postes dans les groupes utilisateurs :

1. [Modification des paramètres du poste.](#)
2. [Glisser-déposer le poste dans la liste hiérarchique](#) (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** dans le menu principal, puis dans la fenêtre qui apparaît cliquez sur le nom du poste dans la liste hiérarchique.
2. Le panneau des propriétés du poste va s'ouvrir. Vous pouvez également ouvrir la rubrique des propriétés du poste en cliquant sur l'élément **Propriétés** du [menu de gestion](#).
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.
4. Pour ajouter un poste au groupe utilisateur, cochez la case contre ce groupe dans la liste **Appartenance**.
5. Pour supprimer un poste du groupe utilisateur, cliquez sur le nom du groupe dans la liste **Appartenance**.



Il est impossible de supprimer des postes depuis les groupes pré-installés.

6. Pour enregistrer les modifications apportées, cliquez sur le bouton **Sauvegarder**.

Dans la rubrique **Propriétés** du poste, vous pouvez également spécifier un groupe primaire pour le poste (pour en savoir plus, voir [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, glissez-déposez du poste vers le groupe choisi (drag-and-drop).
3. Pour déplacer le poste d'un groupe utilisateur vers un autre groupe, glissez-déposez le 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.

6.3.2. Configuration de l'appartenance automatique au groupe

Dr.Web Enterprise Security Suite permet de configurer les règles de l'ajout automatique d'un poste aux groupes utilisateur.

Pour spécifier les règles de l'ajout automatique d'un poste aux groupes utilisateur, procédez comme suit :

1. Sélectionnez l'élément **Réseau antivirus** du menu principal du Centre de gestion.
2. Dans la liste hiérarchique du réseau antivirus, sélectionnez le groupe utilisateur pour lequel vous voulez spécifier les règles d'appartenance.
3. Passez à la rubrique d'édition des règles d'appartenance par un des moyens suivants :
 - Dans le panneau de propriétés dans la partie droite de la fenêtre, cliquez sur **🔻 Règles d'appartenance au groupe** dans la rubrique **Configuration**.
 - Dans le [menu de gestion](#), sélectionnez l'élément **Règles d'appartenance au groupe** dans la section **Général**.
 - Dans le [menu de gestion](#), sélectionnez l'élément **Propriétés** dans la section **Général**, puis passez à l'onglet **Configuration** et cliquez sur **🔻 Règles d'appartenance au groupe**.
4. Postes en réseau – nombre de postes dans ce groupe qui sont en réseau (online) en ce moment :



- a) Si les règles d'appartenance n'étaient pas spécifiées précédemment, cliquez sur **Ajouter une règle**.
- b) Cochez la case **Spécifier le groupe comme primaire** pour que le groupe pour lequel la règle est créée soit désigné comme primaire pour tous les postes qui seront déplacés dans ce groupe d'après cette règle.
- c) Pour chaque bloc de règles spécifiez les paramètres suivants :
 - Sélectionnez une des options, déterminant le principe de regroupement de règles au sein d'un bloc : **Correspond à toutes les conditions, Correspond à n'importe quelle condition, Ne correspond à aucune condition**.
 - Dans la liste déroulante de conditions sélectionnez : un des paramètres du poste dont la conformité aux conditions sera vérifiée, le principe de conformité à cette condition, puis entrez la ligne de condition si cela est sous-entendu par le paramètre du poste.





Quand vous spécifiez le paramètre **Plateforme du poste**, il est nécessaire de sélectionner dans la liste le nom complet de la plateforme qui se trouve au dernier niveau de l'arborescence. Tous les niveaux supérieurs sont indiqués uniquement pour faciliter le groupement de la liste des plateformes et ils ne sont pas les valeurs du paramètres **Plateforme du poste**.

Par exemple, **Windows** et **Windows 7** ne sont pas les bonnes valeurs du paramètre. La sélection de la valeur **Windows 7 Professional Edition** est correcte.

Quand vous spécifiez le paramètre **LDAP DN d'Active Directory**, il faut :

1. Activer la tâche **Synchronisation avec Active Directory** dans la planification du Serveur (section **Administration** → **Planificateur de Tâches du Serveur Dr.Web**).
2. Spécifiez la valeur nécessaire de DN dans les règles d'appartenance en tant que la ligne de la condition pour le paramètre **LDAP DN d'Active Directory**, par exemple :
`OU=OrgUnit,DC=Department,DC=domain,DC=com`

- Pour ajouter encore une condition dans ce bloc, cliquez  à droite de la ligne de condition.
- d) Pour ajouter un nouveau bloc de règles cliquez  à droite du bloc. Dans ce cas spécifiez le principe d'union de ce bloc de conditions avec d'autres blocs :
 - **ET** – les conditions de blocs doivent être remplies en même temps.
 - **OU** – les conditions d'au moins un bloc doivent être remplies.





Lors de la spécification de la ligne de conditions, les expressions régulières peuvent être utilisées.

Les expressions régulières sont brièvement décrites dans les **Annexes**, dans la rubrique [Annexe J. Utilisation des expressions régulières dans Dr.Web Enterprise Security Suite](#).

Notez que si vous utilisez les paramètres du filtre **commence par** et **se termine par**, la ligne de conditions est automatiquement complétée par les symboles de gestion suivants : ^ (la ligne commence par la séquence de symboles indiqués) ou \$ (la ligne se termine par la séquence de symboles indiqués).


Pour l'utilisation performante de conditions régulières, il est recommandé de sélectionner le paramètre du filtre **contient**.

5. Pour enregistrer et appliquer les règles spécifiées cliquez sur un des boutons suivants :
 - **Appliquer maintenant** – enregistrer les règles d'appartenance spécifiées et appliquer immédiatement ces règles à tous les postes enregistrés sur ce Serveur. S'il y a beaucoup de postes qui sont connectés au Serveur, l'exécution de cette action peut prendre un certain temps. Les règles de regroupement sont appliquées à tous les postes enregistrés au moment où vous paramétrez les actions. Ultérieurement, les règles seront également appliquées à tous les postes au moment de la connexion, y compris les postes qui sont enregistrés sur le Serveur pour la première fois.
 - **Appliquer au moment de la connexion de postes** – enregistrer les règles d'appartenance spécifiées et appliquer ces règles aux postes au moment de leur connexion au Serveur. Les règles de regroupement sont appliquées à tous les postes enregistrés au moment de leur connexion suivante au Serveur. Ultérieurement, les règles seront appliquées à tous les postes au moment de la première connexion y compris les postes qui sont enregistrés sur le Serveur pour la première fois.
6. Au moment de la configuration de l'appartenance automatique pour un groupe utilisateur, l'icône  apparaît à côté de l'icône de ce groupe dans la liste hiérarchique à condition que la case **Afficher l'icône de règles d'appartenance** a été cochée dans la liste  **Paramètres d'affichage de l'arborescence** dans la barre d'outils.





Si le poste a été déplacé dans un groupe utilisateur conformément aux règles d'appartenance, la suppression du poste de ce groupe n'a aucun sens parce que le poste retournera dans ce groupe à la prochaine connexion au Serveur.

Pour supprimer les de l'ajout automatique d'un poste au groupe, procédez comme suit :

1. Sélectionnez l'élément **Réseau antivirus** du menu principal du Centre de gestion.
2. Dans la liste hiérarchique du réseau antivirus, sélectionnez le groupe utilisateur pour lequel vous voulez supprimer les règles d'appartenance.
3. Effectuez une des actions suivantes :
 - Dans la barre d'outils, cliquez sur le bouton  **Supprimer les règles d'appartenance**.



- Dans le panneau de propriétés dans la partie droite de la fenêtre, cliquez sur  **Supprimer les règles d'appartenance** dans la rubrique **Configuration**.
 - Dans le [menu de gestion](#), sélectionnez l'élément **Propriétés** dans la section **Général**, puis passez à l'onglet **Configuration** et cliquez sur  **Supprimer les règles d'appartenance au groupe**.
4. Après la suppression des règles d'appartenance du groupe, tous les postes déplacés dans ce groupe conformément aux règles d'appartenance seront supprimés du groupe. Si ce groupe a désigné par l'administrateur comme primaire pour un de ces postes, c'est le groupe **Everyone** qui sera désigné comme primaire en cas de suppression des postes depuis le groupe.

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 paramètres personnalisés pour le poste, éditez la rubrique correspondante des paramètres (voir [Propriétés du poste – Configuration](#)). 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 ges-



tion dans la rubrique relative aux paramètres concernés ou dans la rubrique correspondante depuis les propriétés du poste.

6.4.1. Héritage des éléments de la configuration du poste de travail

Principe de l'héritage des paramètres

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 désigné comme primaire. Par défaut, c'est le groupe **Everyone**.

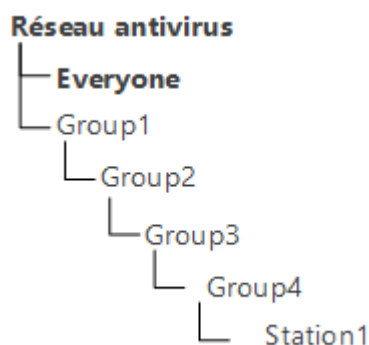


Si le groupe primaire n'est pas le groupe **Everyone** et n'a pas de configuration personnalisée, les configurations du groupe **Everyone** seront héritées.


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 :

La structure de la liste hiérarchique représente l'arborescence suivante :



Le groupe `Group4` est un groupe primaire pour le poste `Station1`. Dans ce cas lors de l'héritage de paramètres le poste `Station1` va effectuer la recherche de paramètres 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 la rubrique  **Configuration de l'arborescence** dans la barre d'outils du Centre de gestion.



Paramétrage du groupe primaire

Il existe plusieurs façons de paramétrer un nouveau groupe primaire pour un poste ou pour un groupe de postes.

Paramétrer un groupe primaire pour un 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 la liste hiérarchique.
2. Le panneau des propriétés du poste va s'ouvrir. Vous pouvez également ouvrir la rubrique des propriétés du poste en cliquant sur l'élément **Propriétés** du [menu de gestion](#). Dans la fenêtre qui s'affiche, ouvrez la sous-rubrique **Groupes**.
3. Pour spécifier un autre groupe primaire, cliquez sur l'icône du groupe dans la liste Appartenance. Le chiffre **1** s'affiche sur l'icône.
4. Cliquez sur **Enregistrer**.

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 postes pour lesquels vous souhaitez paramétrer un groupe primaire dans la liste hiérarchique (vous pouvez également sélectionner des groupes de postes, dans ce cas, l'action sera appliquée à tous les postes appartenant aux groupes concernés). Pour sélectionner plusieurs postes ou groupes, maintenez appuyées les touches CTRL et SHIFT durant la sélection.
2. Dans la barre d'outils cliquez sur **Général** → **Définir un groupe primaire pour les postes**. La fenêtre contient la liste des groupes pouvant être spécifiés comme primaires pour les postes sélectionnés.
3. Cliquez sur le nom d'un groupe pour le définir comme primaire.

Vous pouvez également définir un groupe comme primaire pour tous les postes qu'il contient. Pour cela, sélectionnez le groupe dans la liste hiérarchique et dans la barre d'outils du Centre de gestion, cliquez sur **Général** → **Définir ce 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,
-  dans la fenêtre de configuration des droits d'utilisateurs.

L'arborescence du réseau antivirus 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](#), 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 au moment actuel.
 - **Groupe primaire pour** – total de postes pour lesquels ce groupe est un groupe primaire.
 - **Configuration personnalisée** – liste des composants pour lesquels les paramètres sont personnalisés et non hérités du groupe parent.
 - Paramètres utilisés pour comparer les postes :
 - **Date de création** du poste.
 - **Groupe primaire** pour le poste.
 - **Configuration personnalisée** – liste des composants pour lesquels les paramètres sont personnalisés et non hérités du groupe primaire.
 - **Composants installés** – liste des composants antivirus installés sur le poste.



Chapitre 7. Gestion des postes 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 comptes des postes de travail

7.1.1. Politique d'approbation des postes



La procédure de création de postes via le Centre de gestion est décrite dans le **Manuel d'installation**, p. [Création d'un nouveau compte Utilisateur](#).

La gestion de la procédure d'approbation des postes sur le Serveur Dr.Web varie en fonction des paramètres suivants :

1. Si, lors de l'installation de l'Agent, la case **Autorisation manuelle sur le serveur** est cochée, le mode d'accès des postes au Serveur est déterminé selon les paramètres spécifiés sur le Serveur(utilisé par défaut), voir [ci-après](#).
2. Si, lors de l'installation de l'Agent, la case **Autorisation manuelle sur le serveur** est cochée et que les paramètres **Identificateur** et **Mot de passe** ont été spécifiés, alors, au moment de la connexion au Serveur, le poste sera approuvé automatiquement quels que soient les paramètres configurés sur le Serveur (utilisé par défaut en cas d'installation de l'Agent avec le package d'installation `drweb-esuite-install` – voir **Manuel d'installation**, p. [Fichiers d'installation](#)).



Le paramétrage du type d'autorisation de l'Agent durant son installation est décrit dans le **Manuel Utilisateur**.



Pour modifier le mode d'accès des postes au Serveur Dr.Web :

1. Ouvrez la configuration du Serveur. Pour ce faire, sélectionnez l'élément **Administration** du menu principal, puis cliquez sur l'élément **Configuration** du **Serveur Dr.Web** dans le [menu de gestion](#).
2. Dans l'onglet **Général** de la liste déroulante **Mode d'enregistrement de novices**, sélectionnez une des options suivantes :
 - **Approuver l'accès manuellement** (ce mode est spécifié par défaut à moins qu'il ne soit modifié durant l'installation du Serveur),
 - **Toujours refuser l'accès**,
 - **Approuver l'accès automatiquement**.

Approuver l'accès manuellement

Dans le mode **Approuver l'accès manuellement**, les nouveaux postes sont placés dans le sous-groupe **Newbies** du groupe **Status** jusqu'à ce que l'administrateur les soumette à autorisation.


Pour gérer l'accès des postes non approuvés :

1. Sélectionnez l'élément **Réseau antivirus** dans le menu principal du Centre de gestion. Dans l'arborescence du réseau antivirus, sélectionnez les postes dans le groupe **Status** → **Newbies**.



Le groupe **Status** → **Newbies** dans l'arborescence du réseau antivirus est accessible uniquement si les conditions suivantes sont satisfaites :

1. La valeur **Approuver l'accès manuellement** est spécifiée pour le paramètre **Mode d'enregistrement de novices** dans la rubrique **Administration** → **Configuration du Serveur Dr.Web** → **Général**.
2. Le [droit Approuver des novices](#) est autorisé aux administrateurs.

2. Pour définir un accès au Serveur, à la rubrique  **Postes non approuvés** de la barre d'outils, paramétrez l'action à appliquer aux postes sélectionnés :



Approuver les postes sélectionnés et définir le groupe primaire – approuver l'accès au poste au Serveur et spécifier le groupe primaire de la liste proposée.



Annuler l'action qui doit être exécutée à la connexion – annuler une action sur un poste non approuvé qui aurait dû être exécutée lors de la connexion du poste au Serveur.



Rejeter les postes sélectionnés – refuser l'accès des postes au Serveur.

Refus automatique de l'accès

Dans le mode **Toujours refuser l'accès**, le Serveur refuse l'accès aux requêtes reçues depuis les nouveaux postes. L'administrateur doit créer manuellement des comptes pour les nouveaux postes et leur attribuer des mots de passe d'accès.





Approbation automatique d'accès

Dans le mode **Autoriser l'accès automatiquement**, tous les postes demandant l'accès au Serveur seront approuvés automatiquement sans aucune requête à l'administrateur. Dans ce cas, le groupe spécifié dans la liste déroulante **Groupe primaire** dans la rubrique **Configuration** du **Serveur Dr.Web**, dans l'onglet **Général**, est défini comme primaire.

7.1.2. Suppression et restauration d'un poste

Suppression de postes

Pour supprimer l'entrée sur un poste de travail :


1. Sélectionnez l'élément **Réseau antivirus** du menu principal, puis dans la fenêtre qui apparaît, dans la barre d'outils, cliquez sur  **Général** →  **Supprimer les objets sélectionnés**.
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 restaurés via le Centre de gestion.


Restauration de postes

Pour restaurer 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 auquel 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** 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. La liste **Appartenance** contient la liste des groupes auxquels le poste peut être inclus. Cochez les cases contre les groupes auxquels le poste sera inclus.
4. Pour restaurer un poste avec les paramètres spécifiés, cliquez sur le bouton **Restaurer**.

7.1.3. Fusionner 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 colonne sélectionnez le poste à considérer comme principal. Tous les autres postes seront supprimés et leurs données seront associées au poste sélectionné.
4. Dans la colonne , sélectionnez le poste dont la configuration sera appliquée au poste principal sélectionné.
5. Cliquez sur **Sauvegarder**.

7.2. Paramètres généraux du poste de travail

7.2.1. Propriétés du poste

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 qui apparaît, sélectionnez un poste dans l'arborescence.
2. Ouvrez la rubrique de configuration du poste d'une des façons suivantes :
 - a) Cliquez sur le nom du poste dans la liste hiérarchique du réseau antivirus. La section contenant les propriétés du poste va s'afficher automatiquement dans la partie droite du Centre de gestion.
 - b) Sélectionnez l'élément **Propriétés** du [menu de gestion](#). La fenêtre contenant les propriétés du poste va s'ouvrir.
3. Cette fenêtre contient les groupes de paramètres suivants : **Général**, **Configuration**, **Groupes**, **Sécurité**, **Localisation**. Le contenu des groupes et leur paramétrage sont décrits ci-dessous.
4. Pour enregistrer les modifications apportées, cliquez sur le bouton **Enregistrer**.



Suppression des paramètres personnalisés du poste

Pour supprimer les paramètres personnalisés 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 dans la barre d'outils cliquez sur  **Général** →  **Supprimer les paramètres personnalisés**. La liste des paramètres du poste va s'afficher, les cases contre les paramètres personnalisés sont cochées.
2. Laissez les cases cochées contre les paramètres à supprimer. Décochez les cases contre les paramètres qui doivent rester personnels. Cliquez sur **Supprimer**. L'héritage du groupe primaire sera rétabli pour les paramètres cochés.

7.2.1.1. Général

La rubrique **Général** contient les champs suivants disponibles en lecture seule :

- **Identificateur** – un identificateur unique du poste.
- **Nom** – nom du poste.
- **Date de création** – date de création du poste sur le Serveur.
- **Dernier enregistrement** – date de la dernière connexion de ce poste au Serveur.

Vous pouvez également spécifier ou modifier les valeurs des champs suivants :

- 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 sur le poste.



Les valeurs des champs marqués du symbole *, doivent être obligatoirement spécifiées.

Cette rubrique contient également les liens suivants :

- Dans l'élément **Fichier d'installation** – un lien pour télécharger l'installateur de l'Agent pour ce poste.

Immédiatement après la création d'un nouveau poste et jusqu'au moment où un système d'exploitation pour le poste en question ne soit défini, dans la rubrique de téléchargement du package d'installation, les liens sont fournis séparément pour chaque OS pris en charge par Dr.Web Enterprise Security Suite.

- Dans l'élément **Fichier de configuration** – un lien pour télécharger le fichier contenant les paramètres de connexion au Serveur Dr.Web pour les postes sous OS Android, OS X et Linux.




7.2.1.2. Configuration

La rubrique **Configuration** vous permet de modifier la configuration du poste qui comprend :

Icône	Paramètres	Rubrique contenant la description
	Droits des utilisateurs des postes	Droits des utilisateurs du poste
	Planification centralisée pour lancer des tâches sur les postes	Planification des tâches sur un poste
	Fichiers clés de licence pour les postes	Gestionnaire de licences
	Restrictions sur la diffusion des mises à jour du logiciel antivirus	Restrictions de mises à jour des postes
	Liste des composants à installer	Composants à installer du package antivirus
	Paramètres des composants du package antivirus pour ce poste	Configuration des composants antivirus

Le Centre de gestion fournit également une option de suppression des paramètres personnalisés d'un poste. Les boutons de suppression sont situés à droite des boutons correspondants de configuration des composants. Lorsque vous supprimez des paramètres personnalisés, le poste hérite la configuration du groupe primaire.



Lorsque vous modifiez les paramètres de SplDer Gate et/ou du Office Control, merci de prendre en compte le fait que les paramètres de ces composants sont interconnectés, et que, si les paramètres personnalisés de l'un d'entre eux sont supprimés via le bouton  **Supprimer les paramètres personnalisés**, cela supprime également les paramètres de l'autre composant (l'héritage de paramètres du groupe parent est ainsi établi).

7.2.1.3. Groupes

Dans la rubrique **Groupes**, vous pouvez paramétrer la liste des groupes dans lesquels un poste est inclus. La liste **Appartenance** affiche les groupes qui incluent les postes de travail et dans lesquels vous pouvez en inclure.

Pour gérer l'appartenance d'un poste de travail il est nécessaire :

1. Pour ajouter un poste au groupe utilisateur, cochez la case contre ce groupe dans la liste **Appartenance**.
2. Pour supprimer un poste du groupe utilisateur, cliquez sur le nom du groupe dans la liste **Appartenance**.



Il est impossible de supprimer des postes depuis les groupes pré-installés.

3. Si vous souhaitez réassigner un autre groupe primaire, cliquez sur l'icône du groupe souhaité dans la liste Appartenance. Le chiffre **1** s'affiche sur l'icône.

7.2.1.4. Sécurité



La rubrique **Sécurité** permet de spécifier des limitations pour les adresses réseau depuis lesquelles l'Agent installé sur ce poste peut se connecter au Serveur.

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.

Pour autoriser l'accès depuis une adresse TCP déterminée, ajoutez l'adresse dans la liste **TCP: autorisé** ou **TCPv6: autorisé**.

Pour 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 au format suivant *<adresse IP>/ [<préfixe du réseau>]*.
2. Pour ajouter un nouveau champ d'adresse, cliquez sur le bouton  dans la rubrique correspondante.
3. Pour supprimer le champ, cliquez sur le bouton  contre l'adresse à supprimer.
4. Pour appliquer les paramètres, cliquez sur **Sauvegarder**.

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 d'hôtes dans les réseaux de ce type ont le format suivant : 125 . * . * . *

De plus, vous pouvez supprimer des adresses de la liste et éditer les adresses ajoutées dans la liste.

Les adresses non mentionnées dans aucune des listes sont autorisées ou interdites en fonction du statut de la case **Priorité de refus** : si la case est cochée, la liste **Refuser** possède une priorité plus importante que la liste **Autoriser**. Les adresses qui ne sont incluses à aucune liste ou incluses aux deux listes sont refusées. Seules les adresses appartenant à la liste **Autoriser** et non incluses à la liste **Refuser** seront autorisées.



7.2.1.5. Localisation

La rubrique **Localisation** permet d'indiquer des informations supplémentaires sur l'emplacement physique du poste de travail.

Vous pouvez également localiser géographiquement le poste sur une carte.

Pour voir l'emplacement du poste sur une carte :

1. Dans les champs **Latitude** et **Longitude**, indiquez les coordonnées géographiques du poste au format Degrés Décimaux.
2. Cliquez sur **Sauvegarder** pour conserver les données entrées.
3. Dans l'onglet **Localisation**, la visualisation OpenStreetMaps va s'ouvrir et les coordonnées indiquées seront marquées.

Si l'outil de visualisation ne peut être chargé, le texte **Afficher sur la carte** apparaît.

4. Pour consulter la carte au plus grand format, cliquez sur l'outil de visualisation ou sur le texte **Afficher sur la carte**.

7.2.2. 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](#), sélectionnez l'élément **Composants installés** dans la sous-rubrique **Général**.
3. La fenêtre qui s'affiche contient les informations sur les composants installés : nom de composant, date d'installation, adresse du Serveur depuis lequel le composant a été installé, répertoire de l'installation du composant sur le poste.



La liste des composants à installer peut varier en fonction des éléments suivants :

- Composants autorisés pour l'utilisation dans 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 ainsi qu'à tout moment après l'installation (voir [Composants à installer du package antivirus](#)).



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** dans le menu principal du Centre de gestion, puis dans la fenêtre qui apparaît, cliquez sur le nom du poste dans l'arborescence.
2. Dans le [menu de gestion](#) qui s'affiche, sélectionnez l'élément **Bases virales** depuis la sous-rubrique **Statistiques**.
3. Une fenêtre qui s'affiche contient les informations suivantes sur les bases virales installées : nom de fichier contenant la base virale, version de la base virale, date de création de la base virale, total d'entrées dans 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 du Serveur Dr.Web**. Dans l'onglet **Statistiques**, cochez les cases **Surveillance des bases virales** et **Surveillance des statuts des postes**, puis redémarrez le Serveur.

7.2.3. Matériel et logiciels des postes tournant sous Windows®

Dr.Web Enterprise Security Suite permet de collecter et consulter des informations sur le matériel et les logiciels installés sur les postes protégés tournant sous Windows.

Pour collecter des informations sur le matériel et les logiciels du poste, procédez comme suit :


1. Activer la collecte des statistiques sur le Serveur :
 - a) Sélectionnez l'élément **Administration** du menu principal du Centre de gestion.
 - b) Sélectionnez l'élément **Configuration du menu de gestion du Serveur Dr.Web**.
 - c) Dans les paramètres du Serveur, ouvrez l'onglet **Statistiques** et cochez la case **Composition de matériel et de logiciels** si cette case est décochée.
 - d) Pour appliquer les modifications apportées, cliquez sur **Sauvegarder** et redémarrez le Serveur.
2. Autoriser la collecte des statistiques sur les postes :
 - a) Sélectionnez l'élément **Réseau antivirus** du menu principal du Centre de gestion.
 - b) Dans la liste hiérarchique du réseau antivirus, sélectionnez un poste ou un groupe de postes pour lesquels vous voulez autoriser la collecte des statistiques. En cas de la sélection d'un groupe des postes, prenez en compte l'héritage des paramètres : si les paramètres



personnalisés sont spécifiés pour le groupe sélectionné, la modification des paramètres du groupe ne va pas modifier les paramètres du poste.

- c) Dans le menu de gestion, sélectionnez la section **Configuration** → **Windows**, ensuite sélectionnez l'élément **Agent Dr.Web**.
- d) Dans les paramètres de l'Agent, dans l'onglet **Général**, cochez la case **Collecter les informations sur les postes** si elle est décochée. Si nécessaire, éditez la valeur du paramètre **Période de la collecte des informations sur les postes (min)**.
- e) Pour appliquer les modifications apportées, cliquez sur **Sauvegarder**. Les paramètres seront transmis sur les postes.

Pour consulter le matériel et les logiciels du poste, procédez comme suit :

1. Sélectionnez l'élément **Réseau antivirus** du menu principal du Centre de gestion.
2. Dans la liste hiérarchique du réseau antivirus, sélectionnez le poste nécessaire.
3. Dans le menu de gestion, sélectionnez l'élément **Matériel et logiciels** dans la section **Général**.
4. La fenêtre qui s'affiche comporte l'arborescence avec la liste du matériel et des logiciels contenant les informations suivantes sur ce poste :
 - **Application** – liste des produits installés sur le poste.
 - **Hardware** – liste du matériel installé sur le poste.
 - **Operating System** – informations sur le système d'exploitation du poste.
 - **Windows Management Instrumentation** – informations sur les outils de gestion Windows.
5. Pour filtrer les paramètres affichés du matériel et du logiciel du poste, spécifiez les options correspondantes dans la section  **Paramètres d'affichage de l'arborescence** :
 - **Masquer les composants système** – masquer les composants système de la section **Application**. Si la case est cochée, la liste de toutes les applications excepté les applications système sera affichée. Si la case est décochée, les composants système seront également affichés dans la liste.
 - **Masquer les informations détaillées** – afficher l'ensemble de composant minimum qui permet d'avoir un aperçu général du poste. Cet ensemble est déterminé par les filtres prédéfinis que l'utilisateur ne peut pas modifier. Si la case est cochée, seuls les composants principaux seront affichés. Si la case est décochée, tous les composants seront affichés.
6. Pour afficher les informations détaillées sur un matériel ou un logiciel spécifique, sélectionnez l'objet nécessaire dans l'arborescence.
7. Si nécessaire, vous pouvez exporter les données du matériel et du logiciel dans un fichier. Il est possible d'exporter toutes les données affichées en ce moment dans l'arborescence conformément aux paramètres spécifiés (voir le p.5).

Pour exporter les données, cliquez sur un des boutons suivants dans la barre d'outils :



Sauvegarder les données dans un fichier CSV,



Sauvegarder les données dans un fichier HTML,



Sauvegarder les données dans un fichier XML,



Sauvegarder les données dans un fichier PDF.

Pour comparer le matériel et les logiciels sur plusieurs postes, procédez comme suit :

1. Sélectionnez l'élément **Réseau antivirus** du menu principal du Centre de gestion.
2. Dans la liste hiérarchique du réseau antivirus, sélectionnez quelques postes ou groupes de postes. Pour afficher la page de comparaison, il faut sélectionner deux postes au minimum tournant sous Windows.
3. Dans le menu de gestion, sélectionnez l'élément **Comparaison de matériel et de logiciels** dans la rubrique **Général**.
4. Dans la fenêtre qui s'affiche, les informations suivantes seront disponibles :
 - arborescence avec la liste du matériel et des logiciels ;
 - tableau de comparaison pour les postes sélectionnés.
5. Pour afficher les données à comparer, sélectionnez l'élément nécessaire dans l'arborescence de matériel et de logiciels. Toutes les valeurs disponibles de l'élément sélectionné seront affichées dans l'arborescence de comparaison.

7.3. Configuration du poste de travail

7.3.1. Droits des utilisateurs du poste

Pour configurer les droits des utilisateurs du poste de travail depuis le Centre de gestion de la sécurité Dr.Web :

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, sélectionnez l'élément **Droits**. La fenêtre de configuration des droits va s'ouvrir.
2. Vous pouvez modifier les droits aux onglets correspondant au système d'exploitation du poste de travail. Pour modifier (autoriser ou refuser) tout droit, cochez ou décochez la case pour ce droit.
3. Pour modifier les droits des postes sous Windows, OS X, Linux et Android, utilisez 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 l'Agent Dr.Web et de ses fonctions :

Case de la rubrique Droits	Action de la case	Résultat sur le poste si la case est décochée
Postes tournant sous l'OS Windows		
Lancer en mode mobile	Cochez la case pour autoriser les utilisateurs du poste à passer en mode mobile et à utiliser le Système Global de Mise à jour Dr.Web pour les mises à jour s'il n'y a pas de connexion au Serveur Dr.Web.	Le paramètre Utiliser le mode mobile s'il n'y a pas de connexion au Serveur n'est pas disponible dans la rubrique Général → Mode des paramètres de l'Agent.
Modifier le mode de fonctionnement	Cochez la case pour autoriser les utilisateurs d'un poste à modifier le mode de fonctionnement de l'Agent Dr.Web.	Les paramètres suivants ne sont pas disponibles dans la rubrique Général → Mode des paramètres de l'Agent : <ul style="list-style-type: none">• Recevoir des mises à jour du serveur,• Recevoir des tâches du serveur,• Collecter les événements.
Modifier la configuration de l'Agent Dr.Web	Cochez la case pour permettre aux utilisateurs d'un poste de modifier les paramètres de l'Agent Dr.Web.	Dans les paramètres de l'Agent, dans la rubrique Général les paramètres des sous-rubriques suivantes ne sont pas disponibles : <ul style="list-style-type: none">• Notifications : aucun paramètre n'est disponible.• Mode – aucun paramètre de connexion au Serveur n'est disponible, ainsi que la case Synchroniser l'heure système avec l'heure du serveur.• Autoprotection : les paramètres Empêcher la modification de la date et de l'heure système et Empêcher l'émulation de l'activité utilisateur ne sont pas disponibles.• Avancé : les éléments Mise à jour Dr.Web, Services Dr.Web, Créer des dumps de mémoire en cas d'erreur de scan ne sont pas disponibles dans les paramètres de la rubrique Journal.
Désactiver l'autoprotection	Cochez la case pour permettre aux utilisateurs d'un poste de désactiver l'autoprotection.	Le paramètre Activer l'autoprotection et le paramètre Activer le support de la virtualisation assistée par matériel ne






Case de la rubrique Droits	Action de la case	Résultat sur le poste si la case est décochée
		sont pas disponible dans la rubrique Général > Autoprotection dans les paramètres de l'Agent.
Désinstaller l'Agent Dr.Web	Cochez la case pour permettre aux utilisateurs d'un poste de désinstaller l'Agent Dr.Web.	Empêche la désinstallation de l'Agent sur le poste via l'installateur ou via les outils standard de Windows. Dans ce cas, l'Agent peut être désinstallé uniquement via l'option Général → Désinstaller l'Agent Dr.Web dans la barre d'outils du Centre de gestion.
Postes tournant OS X		
Lancer en mode mobile	Cochez la case pour autoriser les utilisateurs du poste à passer en mode mobile et à utiliser le Système Global de Mise à jour Dr.Web pour les mises à jour s'il n'y a pas de connexion au Serveur Dr.Web.	Dans la fenêtre principale de l'application, la rubrique Mise à jour n'est pas disponible.
Postes tournant sous OS de la famille Linux		
Lancer en mode mobile	Cochez la case pour autoriser les utilisateurs du poste à passer en mode mobile et à utiliser le Système Global de Mise à jour Dr.Web pour les mises à jour s'il n'y a pas de connexion au Serveur Dr.Web.	Pour le mode de console de l'application : la commande <code>drweb-ctl update</code> pour mettre à jour les bases virales depuis le SGM n'est pas disponible.
Postes tournant sous OS Android		
Lancer en mode mobile	Cochez la case pour autoriser les utilisateurs d'appareils mobiles à passer en mode mobile et à utiliser le Système Global de Mise à jour Dr.Web pour les mises à jour s'il n'y a pas de connexion au Serveur Dr.Web.	Dans la fenêtre principale de l'application lancée sur l'appareil mobile, la rubrique Mise à jour est bloquée.



En cas de désactivation d'un élément associé à un paramètre de l'Agent, la dernière valeur spécifiée pour ce paramètre avant la désactivation sera appliquée.

Vous pouvez consulter la description des actions associées aux éléments du menu dans la documentation **Agent Dr.Web pour Windows. Manuel Utilisateur**.



4. Vous pouvez également diffuser ces configurations vers un autre objet en cliquant sur le bouton  **Diffuser ces paramètres à un autre objet**.
5. Afin d'exporter la configuration vers un fichier, cliquez sur  **Exporter les paramètres de cette rubrique vers le fichier**.
6. Afin d'importer la configuration depuis un fichier, cliquez sur  **Importer les paramètres de cette rubrique du fichier**.
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.

7.3.2. Planification des tâches sur un poste

Dr.Web Enterprise Security Suite fournit la fonctionnalité de gestion de la *planification centralisée des tâches*. C'est une planification spécifiée par l'administrateur du réseau antivirus conformément à toutes les règles relatives à l'héritage des configurations.

Planification des tâches – 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 aux moments les plus opportuns pour les utilisateurs, sans nécessité de lancer manuellement le Scanner. De plus, l'Agent Dr.Web permet d'exécuter d'autres types d'actions décrits ci-dessous.

La planification centralisée de l'exécution régulière des tâches des postes et des groupes de postes peut être éditée depuis le Centre de gestion de la sécurité Dr.Web.



Les utilisateurs sur le poste ne sont pas autorisés à consulter et à modifier les tâches de la planification centralisée.

Résultats de l'exécution des tâches selon la planification centralisée ne sont pas inclus dans les données statistiques du côté de l'Agent mais ils sont envoyés sur le Serveur et sont sauvegardés dans les données statistiques du Serveur.

Marche à suivre pour éditer la planification centralisée :

1. Sélectionnez la rubrique **Réseau antivirus** dans le menu principal du Centre de gestion, puis, dans la liste hiérarchique de la fenêtre qui s'ouvre, sélectionnez un groupe ou un poste de travail. Dans le [menu de gestion](#) qui s'affiche, sélectionnez **Planificateur des tâches**. La liste avec les tâches pour les postes va s'ouvrir.



Pour les postes tournant sous Windows, la planification contient une tâche par défaut – **Daily scan** – scan quotidien du poste (interdit).

2. Pour gérer la planification, utilisez les éléments correspondants dans la barre d'outils :
 - a) Les éléments généraux de la barre d'outils sont utilisés pour créer de nouvelles tâches et gérer la rubrique planification dans son ensemble. Ces éléments sont toujours disponibles dans la barre d'outils.



Créer une tâche – ajouter une nouvelle tâche. Cette action est décrite en détails ci-dessous, dans la sous-rubrique [Éditeur de tâches](#).

Diffuser ces paramètres à un autre objet – copier les tâches planifiées dans d'autres objets – postes et groupes. Pour en savoir plus, voir [Diffusion de Paramètres à d'autres Groupes/Postes](#).

Exporter les paramètres de cette rubrique vers un fichier – exporter la planification vers un fichier au format spécial.

Importer les paramètres de cette rubrique depuis un fichier – importer la planification depuis un fichier au format spécial.

b) Pour gérer les tâches existantes, cochez les cases près des tâches souhaitées ou dans l'entête du tableau pour sélectionner toutes les tâche dans la liste. Les éléments de gestion des tâches sélectionnées deviennent disponibles dans la barre d'outils :

Configuration		Action
Statut	Autoriser l'exécution	Activer l'exécution des tâches sélectionnées selon leur planification, si elles étaient désactivées.
	Désactiver l'exécution	Désactiver l'exécution des tâches sélectionnées. Les tâches restent dans la liste mais ne seront pas exécutées.
Vous pouvez spécifier le même paramètre dans l'éditeur de tâches dans l'onglet Général en cochant la case Autoriser l'exécution .		
Importance	Définir comme critique	Effectuer un lancement supplémentaire de la tâche au prochain démarrage de l'Agent Dr.Web, si l'exécution planifiée de cette tâche a été omise.
	Définir comme non critique	Exécuter la tâche uniquement au moment où elle planifiée indépendamment du fait que le lancement de la tâche ait été omis ou pas.
Vous pouvez spécifier le même paramètre dans l'éditeur de tâches dans l'onglet Général en cochant la case Tâche critique .		
Dupliquer des paramètres		Permet de dupliquer des tâches sélectionnées dans la liste des planifications actuelles. Lorsque vous activez l'option Dupliquer des paramètres , les nouvelles tâches créées possèdent des paramètres identiques à ceux des tâches sélectionnées.
Planifier à plusieurs reprises		Pour les tâches qui ne sont exécutées qu'une fois : exécuter la tâche de nouveau selon les horaires configurés (la modification de la répétition d'exécution d'une tâche est décrite ci-dessous, dans la rubrique Éditeur de tâches).
Supprimer les tâches sélectionnées		Supprimer la tâche sélectionnée de la planification.




3. Pour modifier les paramètres des tâches, sélectionnez-les dans la liste. La fenêtre de l'**Éditeur de tâches**, décrit [ci-dessous](#), s'ouvre.
4. Après avoir modifié la planification, cliquez sur **Sauvegarder** pour appliquer les modifications.



Si, lors de son édition, la planification vide est créée (sans aucune tâche), le Centre de gestion vous proposera d'utiliser soit la planification héritée des groupes, soit la planification vide. Utilisez la planification vide pour refuser la planification héritée des groupes.

Éditeur de Tâches

A l'aide de l'éditeur de tâches, vous pouvez configurer les paramètres pour :

1. Créer une nouvelle tâche.
Pour ce faire, cliquez sur  **Créer une tâche** dans la barre d'outils.
2. Modifier une tâche existante.
Pour ce faire, cliquez sur le nom de la tâche dans la liste.

La fenêtre de modification de la tâche s'ouvre. Les paramètres de modification d'une tâche sont identiques à ceux de création d'une nouvelle tâche.



Les valeurs des champs marqués du symbole *, doivent être obligatoirement spécifiées.

Pour modifier les paramètres d'une tâche :

1. Dans l'onglet **Général**, vous pouvez configurer les paramètres suivants :
 - Dans le champ **Nom**, indiquez le nom de la tâche affichée dans la liste des planifications.
 - Cochez la case **Activer l'exécution** pour activer l'exécution d'une tâche. Si la case n'est pas cochée, la tâche reste dans la liste mais elle ne sera pas exécutée.



Vous pouvez spécifier le même paramètre dans la fenêtre principale du Planificateur à l'aide de l'élément **Statut** dans la barre d'outils.

- Cochez la case **Tâche critique** pour exécuter un lancement supplémentaire de la tâche au prochain démarrage du Agent Dr.Web, si l'exécution planifiée de cette tâche a été omise à l'heure prévue (l'Agent Dr.Web est arrêté au moment de l'exécution de la tâche). Si au moment de lancement, une tâche a été omise plusieurs fois, elle sera exécutée seulement une fois.



Vous pouvez spécifier le même paramètre dans la fenêtre principale du Planificateur à l'aide de l'élément **Importance** dans la barre d'outils.



Si dans ce cas, plusieurs tâches de scan doivent être exécutées, une seule tâche sera exécutée – la première de la liste.



Par exemple, si la tâche **Daily scan** est activée et que la tâche Scan critique via le Scanner Agent est omise, seule la tâche **Daily scan** sera exécutée durant le démarrage du poste et la tâche omise Scan critique ne sera pas exécutée.

Dans l'onglet **Action**, dans la liste déroulante **Action**, sélectionnez le type de tâche et configurez les paramètres nécessaires à son exécution :

Type de tâche	Paramètres et description
Écrire dans le fichier de journal	Ligne – texte du message enregistré dans le fichier de rapport.
Lancer un programme	Configurez les paramètres suivants : <ul style="list-style-type: none">• Champ Chemin – nom complet (avec le chemin) du fichier exécutable du programme qui doit être lancé.• Dans le champ Arguments – paramètres de la ligne de commande pour le programme à lancer.• Cochez la case Attendre la fin du programme pour attendre la fin du programme lancé par cette tâche. Dans ce cas, l'Agent enregistre le lancement du programme, le code de retour et l'heure de la fin du programme. Si la case Attendre la fin du programme est décochée, la tâche est considérée comme achevée dès le lancement du programme et l'Agent n'enregistre que le lancement du programme.
Scanner Dr.Web. Scan rapide	Les paramètres de configuration du scan sont décrits dans le p. Configuration du Scanner .
Scanner Dr.Web. Scan personnalisé	
Scanner Dr.Web. Scan complet	



Vous pouvez lancer le Scanner à distance uniquement sur les postes tournant sous OS Windows, OS de la famille UNIX et OS X.


2. Dans l'onglet **Heure** :

- Dans la liste déroulante **Périodicité**, sélectionnez le mode de lancement de la tâche et configurez l'heure en fonction de la périodicité indiquée :

Mode de lancement	Paramètres et description
Démarrage	La tâche sera lancée au démarrage de l'Agent. Aucun paramètre supplémentaire n'est requis pour exécuter la tâche.
Dans N minutes après la tâche initiale	Dans la liste déroulante Tâche initiale , sélectionnez la tâche par rapport à laquelle est spécifiée l'heure d'exécution de la tâche courante.



Mode de lancement	Paramètres et description
	Dans le champ Minute , indiquez ou choisissez dans la liste le nombre de minutes pour lancer l'exécution de la tâche éditée après l'exécution de la tâche initiale.
Chaque jour	Indiquez l'heure et les minutes – la tâche sera lancée chaque jour au moment spécifié.
Chaque mois	Choisissez la date (jour du mois) et indiquez l'heure et les minutes – la tâche sera lancée au jour spécifié au moment indiqué.
Chaque semaine	Choisissez le jour de la semaine et indiquez l'heure et les minutes – la tâche sera lancée au jour de la semaine spécifié au moment indiqué.
Chaque heure	Indiquez un chiffre entre 0 et 59 pour paramétrer la minute à laquelle sera lancée la tâche dans une heure.
Chaque N minutes	La valeur N doit être indiquée pour paramétrer l'intervalle entre l'exécution des tâches. Si N est égal à 60 ou plus, la tâche sera lancée chaque N minutes. Si N est inférieur à 60, la tâche sera lancée chaque minute de l'heure multiple de N .

- Cochez la case **Interdire après la première exécution** pour exécuter la tâche une seule fois conformément à la périodicité spécifiée. Si la case n'est pas cochée, la tâche sera exécutée plusieurs fois selon la périodicité indiquée.
Pour répéter le lancement d'une tâche déjà exécutée, utilisez le bouton  **Planifier à plusieurs reprises** dans la barre d'outils de la section Planification.
 - Cochez la case **Lancer la tâche selon UTC** pour lancer la tâche selon le Temps universel coordonné (fuseau horaire UTC+0). Si la case est décochée, la tâche sera lancée sur le poste selon l'heure locale.
3. Lorsque tous les paramètres sont indiqués pour une tâche, cliquez sur **Sauvegarder** pour appliquer les modifications des paramètres modifiés si vous avez modifié une tâche existante, ou pour créer une nouvelle tâche avec les paramètres spécifiés si vous avez créé une nouvelle tâche.



7.3.3. Composants à installer 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 ou le groupe. Dans le [menu de gestion](#) qui apparaît, sélectionnez l'élément **Composants à installer**.
2. Pour installer les composants nécessaires, sélectionnez l'une des variantes dans la liste déroulante :
 - **Doit être installé** – 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 être installé** est spécifiée dans la configuration du poste existant, le composant correspondant sera ajouté au package antivirus installé.
 - **Peut être installé** – détermine une possibilité d'installer le composant antivirus. C'est l'utilisateur qui décide d'installer ou de ne pas installer l'Agent.
 - **Ne peut pas être installé** – interdit la présence du composant sur le poste. Lors de la création d'un nouveau poste, le composant n'est pas inclus au package antivirus. Si la valeur **Ne peut pas être installé** est spécifiée dans la configuration du poste existant, le composant concerné sera supprimé du 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.

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.

7.4. Configuration des composants antivirus



Vous pouvez consulter la description détaillée des paramètres des composants antivirus spécifiés via le Centre de gestion dans les **Manuels administrateur** consacrés à la gestion des postes pour un système d'exploitation correspondant.



7.4.1. Composants

En fonction du système d'exploitation du poste les fonctions suivantes sont fournies :

Postes tournant sous l'OS Windows®

Scanner Dr.Web, Scanner Dr.Web Agent

Scan de l'ordinateur selon la requête de l'utilisateur et selon la planification. Il est également possible de lancer sur les postes le scan antivirus à distance depuis le Centre de gestion, y compris le scan anti-rootkits.

SpIDer Guard

Analyse permanente à la volée du système de fichiers. Analyse de tous les processus lancés ainsi que des fichiers créés sur les disques durs et des fichiers ouverts sur les supports amovibles.

SpIDer Mail

Analyse de tous les e-mails entrants et sortants en cas de l'utilisation de clients de messagerie.

Possibilité d'utiliser un filtre antispam (à condition que cette option soit autorisée par la licence).

SpIDer Gate

Analyse de toutes les requêtes vers les sites web via le protocole HTTP. Neutralisation des menaces contenues dans le trafic HTTP (par exemple dans les fichiers reçus/envoyés). Blocage de l'accès aux ressources suspectes ou incorrectes.

Office Control

Gestion de l'accès aux ressources réseau ou aux ressources locales, notamment, il contrôle l'accès aux sites web. Le composant permet non seulement de contrôler l'intégrité des fichiers importants qu'il protège contre toute modification occasionnelle ou infection virale, mais il bloque aussi l'accès des employés aux informations non sollicitées.

Pare-feu

Protection de l'ordinateur contre tout accès non autorisé de l'extérieur ainsi que contre des fuites de données importantes via le réseau. Contrôle de la connexion et de la transmission de données via Internet et blocage des connexions suspectes au niveau des paquets et des applications.

Quarantaine

Isolation des objets malveillants ou suspects dans un répertoire spécial.



Autoprotection

Protection des fichiers et des dossiers de Dr.Web Enterprise Security Suite contre une suppression non autorisée ou involontaire ainsi que contre une modification par l'utilisateur ou par un malware. Lorsque l'autoprotection est active, seuls les processus Dr.Web ont accès aux fichiers et des dossiers de Dr.Web Enterprise Security Suite.

Protection préventive (les paramètres sont fournis au sein des paramètres de l'Agent Dr.Web)

Prévention de menaces potentielles à la sécurité. Contrôle d'accès aux objets critique du système d'exploitation, contrôle de téléchargement de pilotes, contrôle de démarrage automatique de programmes et de fonctionnement de services système. Surveillance de processus lancés et leur blocage en cas de détection d'une activité malveillante.

Postes tournant sous OS de la famille UNIX®

Scanner Dr.Web, Scanner Dr.Web Agent

Le scan de l'ordinateur selon la requête de l'utilisateur et selon la planification. Il est également possible de lancer sur les postes le scan antivirus à distance depuis le Centre de gestion.

SpIDer Guard

Analyse permanente à la volée du système de fichiers. Analyse de tous les processus lancés ainsi que des fichiers créés sur les disques durs et des fichiers ouverts sur les supports amovibles.

SpIDer Gate

Analyse de toutes les requêtes vers les sites web via le protocole HTTP. Neutralisation des menaces contenues dans le trafic HTTP (par exemple dans les fichiers reçus/envoyés). Blocage de l'accès aux ressources suspectes ou incorrectes.

Quarantaine

Isolation des objets malveillants ou suspects dans un répertoire spécial.



Les autres composants dont les paramètres figurent dans le Centre de gestion pour les postes tournant sous les OS de la famille UNIX sont supplémentaires et servent pour configurer les paramètres du logiciel antivirus.

Postes tournant OS X®

Scanner Dr.Web, Scanner Dr.Web Agent

Le scan de l'ordinateur selon la requête de l'utilisateur et selon la planification. Il est également possible de lancer sur les postes le scan antivirus à distance depuis le Centre de gestion.



SpIDer Guard

Analyse permanente à la volée du système de fichiers. Analyse de tous les processus lancés ainsi que des fichiers créés sur les disques durs et des fichiers ouverts sur les supports amovibles.

SpIDer Gate (les paramètres sont disponibles uniquement sur le poste)

Analyse de toutes les requêtes vers les sites web via le protocole HTTP. Neutralisation des menaces contenues dans le trafic HTTP (par exemple dans les fichiers reçus/envoyés). Blocage de l'accès aux ressources suspectes ou incorrectes.

Quarantaine

Isolation des objets malveillants ou suspects dans un répertoire spécial.

Appareils mobiles tournant sous OS Android

Scanner Dr.Web, Scanner Dr.Web Agent

Le scan de l'appareil mobile selon la requête de l'utilisateur et selon la planification. Il est également possible de lancer sur les postes le scan antivirus à distance depuis le Centre de gestion.

SpIDer Guard

Analyse permanente à la volée du système de fichiers. Scan de tous les fichiers lors de la tentative de sauvegarder ces fichiers dans la mémoire de l'appareil mobile.

Filtrage des appels et des messages

Le filtrage des appels et des messages SMS permet de bloquer des messages et des appels indésirables, par exemple, des messages publicitaires ou des appels et des messages des numéros inconnus.

Antivol

Détection de l'appareil mobile ou le blocage rapide de fonctionnalités en cas de perte ou de vol.

Cloud Checker

Le filtre URL permet de protéger l'utilisateur de l'appareil mobile contre les ressources web indésirables.

Pare-feu (les paramètres sont disponibles uniquement sur l'appareil mobile)

Protection de l'appareil mobile contre tout accès non autorisé de l'extérieur ainsi que contre des fuites de données importantes via le réseau. Contrôle de la connexion et de la transmission de données via Internet et blocage des connexions suspectes au niveau des paquets et des applications.



Audit de Sécurité (les paramètres sont disponibles uniquement sur l'appareil mobile)

Diagnostic et analyse de sécurité de l'appareil mobile et résolution de problèmes et de vulnérabilités détectés.

Filtre d'applications

Interdiction de lancer sur l'appareil mobile des applications qui ne sont pas incluses dans la liste des applications autorisées par l'administrateur.

OS Novell® NetWare®

Scanner Dr.Web

Scan de l'ordinateur selon la requête de l'utilisateur et selon la planification.

SplDer Guard

Analyse permanente à la volée du système de fichiers. Analyse de tous les processus lancés ainsi que des fichiers créés sur les disques durs et des fichiers ouverts sur les supports amovibles.

7.5. Scan antivirus des postes de travail



L'utilisateur du poste peut effectuer lui-même le scan antivirus avec le composant Scanner Dr.Web 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, même lors de démarrage du système d'exploitation Windows en mode sans échec.

Via le Centre de gestion vous pouvez :

- 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 configurer les paramètres du scan.

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](#) qui s'ouvre, sélectionnez l'élément **Composants en cours d'exécution**.

La liste de tous les composants actifs va s'ouvrir. Cette liste contient les composants lancés manuellement via le Centre de gestion, par l'administrateur ou selon la planification, ainsi que les composants lancés par un utilisateur sur le poste.



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.



Lorsque vous utilisez cette option, les scans en cours seront interrompus, le Scanner arrêté et les moniteurs mis en pause.

Attention! Vous ne pouvez pas lancer les moniteurs SplDer Guard, SplDer Mail et SplDer Gate via le Centre de gestion.



7.5.2. Interruption des composants en cours selon leur type



Lorsque vous utilisez cette option, les scans en cours seront interrompus, le Scanner arrêté et les moniteurs mis en pause.

Attention! Vous ne pouvez pas lancer les moniteurs SplDer Guard, SplDer Mail et SplDer Gate via le Centre de gestion.


Marche à suivre pour arrêter 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 du répertoire, cliquez sur le bouton  **Gestion des composants**. Dans la liste déroulante qui s'affiche, sélectionnez l'élément  **Arrêter les composants lancés**.
 3. Dans la barre d'outils qui s'affiche, cochez les cases contre les types des composants que vous voulez arrêter immédiatement :
 - **Arrêter le Scanner Dr.Web Agent, lancé par le Planificateur de Tâches** – pour arrêter à l'aide du Scanner Dr.Web Agent le scan actif lancé conformément aux tâches de la planification centralisée.
 - **Arrêter le Scanner Dr.Web Agent lancé par l'administrateur** – pour arrêter à l'aide du Scanner Dr.Web Agent le scan actif lancé manuellement par l'administrateur via le Centre de gestion.
 - **Arrêter le Scanner Dr.Web lancé par l'utilisateur** – pour arrêter à l'aide du Scanner Dr.Web Agent le scan actif lancé par l'utilisateur sur le poste.
 - **Arrêter SplDer Guard, SplDer Mail, SplDer Gate, Office Control, le Pare-feu, l'Autoprotection et la Protection préventive**– pour suspendre le fonctionnement de ces composants.
- Pour sélectionner tous les types des composants à interrompre, cochez la case contre l'en-tête de la barre d'outils **Interrompre les composants lancés**.
4. Cliquez sur le bouton **Interrompre**.




7.5.3. Lancement du scan sur le poste de travail


Marche à suivre pour lancer le scan antivirus sur les postes de travail :

1. Sélectionnez l'élément **Réseau antivirus** du menu principal du Centre de gestion.
2. Dans la fenêtre qui apparaît, cliquez sur le nom d'un groupe ou d'un poste dans la liste hiérarchique.
3. Dans la barre d'outils cliquez sur l'élément  **Scan**. Dans la liste qui va s'afficher dans la barre d'outils sélectionnez un mode de scan :

 **Scanner Dr.Web. Scan 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 d'utilisateur temporaire.

 **Scanner Dr.Web. Scan complet.** Ce mode assure une analyse complète de tous les disques durs et des supports amovibles (y compris les secteurs de démarrage).

 **Scanner Dr.Web. Scan personnalisé.** Dans ce mode, vous pouvez choisir des fichiers et dossiers à analyser et configurer des paramètres avancés du scan.



Vous pouvez lancer le Scanner à distance uniquement si vous sélectionnez des postes actifs tournant sous un OS supportant le lancement du Scanner : Windows, OS de la famille UNIX et OS X.

4. Après la sélection du type de scan, la fenêtre des paramètres du Scanner va s'ouvrir. Modifiez les paramètres de scan si nécessaire (voir la rubrique [Configurer les Paramètres du Scanner](#)).
5. Cliquez sur **Scanner** pour lancer le processus de scan sur les postes sélectionnés.



Le scan des postes via le Scanner Dr.Web Agent lancé à distance est effectué en tâche de fond sans afficher aucune notification sur le poste de l'utilisateur.



7.5.4. Configuration du Scanner

Via le Centre de gestion, vous pouvez configurer les paramètres de contrôle antivirus suivants :

- Paramètres du Scanner Dr.Web. Ce Scanner est lancé par les utilisateurs sur les postes et ne peut pas être lancé à distance depuis le Centre de gestion. Mais l'administrateur peut modifier ses paramètres de façon centralisée et ces derniers seront transmis et sauvegardés sur les postes.
- Paramètres du Scanner Dr.Web Agent. Ce Scanner est lancé à distance depuis le Centre de gestion et effectue le contrôle des postes de la même façon que le Scanner Dr.Web. Les paramètres du Scanner Dr.Web Agent sont présentés comme des paramètres étendus du Scanner Dr.Web et configurés durant le lancement du contrôle antivirus des postes.

Configuration du Scanner Dr.Web



1. Sélectionnez l'élément **Réseau antivirus** du menu principal du Centre de gestion.
2. Dans la fenêtre qui apparaît, cliquez sur le nom d'un groupe ou d'un poste dans la liste hiérarchique.
3. Dans le [menu de gestion](#) de la rubrique **Configuration**, sélectionnez l'élément **Scanner** dans la sous-rubrique du système d'exploitation nécessaire. La fenêtre des paramètres du Scanner va s'ouvrir.
4. Configurez les paramètres nécessaires du scan. La description des paramètres du Scanner Dr.Web est disponible dans le **Manuel Utilisateur** pour le système d'exploitation correspondant.
5. Cliquez sur **Sauvegarder**. Les paramètres seront sauvegardés dans le Centre de gestion et transmis aux postes correspondants.

Configuration des paramètres du Scanner Dr.Web Agent


Les paramètres du Scanner Dr.Web Agent sont configurés durant le lancement du contrôle antivirus des postes comme décrit dans le paragraphe [Lancement du scan sur les postes](#).

La liste des paramètres du Scanner disponibles (+) ou non disponibles (-) dépend du mode de lancement du scan sur les postes. La liste est présentée dans le tableau ci-dessous.

Tableau 7-2. Liste des paramètres du Scanner en fonction du mode de lancement du scan

Mode de lancement du scan	Paramètres par rubrique			
	Général	Actions	Limitations	Exclusions
 Scanner Dr.Web. Scan personnalisé	+	+	+	+
 Scanner Dr.Web. Scan rapide	-	+	+	-



Mode de lancement du scan	Paramètres par rubrique			
	Général	Actions	Limitations	Exclusions
 Scanner Dr.Web. Scan complet	-	+	+	-

En fonction du système d'exploitation des postes sur lequel est lancé le scan à distance, seules les parties de ces paramètres du Scanner supportées par l'OS sont disponibles.



Les paramètres qui ne sont pas supportés dans le cadre du contrôle des postes sous les OS de la famille UNIX et OS X sont mis entre crochets [].

7.5.4.1. Général



Les paramètres qui ne sont pas supportés dans le cadre du contrôle des postes sous les OS de la famille UNIX et OS X sont mis entre crochets [].



Dans la rubrique **Général**, vous pouvez configurer les paramètres suivants du scan antivirus :

- Cochez la case **Utiliser l'analyse heuristique** afin que le Scanner effectue la recherche des virus inconnus avec le moteur heuristique. Ce mode n'exclut pas des faux positifs du Scanner.
- La case **Scan des secteurs boot** permet au Scanner de vérifier les secteurs boot des disques. Les secteurs boot des disques logiques ainsi que les principaux secteurs boot des disques physiques seront scannés.
- La case **[Scan des programmes lancés au démarrage]** permet de scanner les fichiers qui se lancent automatiquement au démarrage du système d'exploitation.
- Cochez la case **Suivre les liens symboliques** pour les suivre durant le scan.
- La case **[Scan des applications et modules en cours d'exécution]** permet de scanner les processus lancés en mémoire.
- Cochez la case **[Scan anti-rootkits]** pour activer le scan à la recherche des programmes malveillants qui masquent leur présence dans le système.
- Cochez la case **[Interrompre le scan lors du passage sur la batterie]** pour interrompre l'analyse lorsque l'ordinateur fonctionne sur la batterie.
- La liste déroulante **Priorité de scan** définit la priorité du processus du scan en fonction des ressources du système d'exploitation.
- Cochez la case **[Niveau de charge des ressources de l'ordinateur]** pour limiter l'utilisation des ressources de l'ordinateur durant le scan. Sélectionnez, dans la liste déroulante, la charge maximum des ressources autorisée pour le Scanner. En l'absence d'autres tâches lancées, les ressources sont utilisées au maximum.



L'option **Niveau de charge des ressources de l'ordinateur** n'a aucune influence sur la valeur de la charge des ressources lors du scan dans le système monoprocesseur à un seul noyau.



- La liste déroulante **Actions après le scan** détermine l'exécution automatique de l'a les actions automatiques après la fin de l'analyse :
 - **ne rien faire** – n'appliquer aucune action à l'ordinateur après la fin du scan.
 - **[éteindre le poste]** – éteindre l'ordinateur après la fin du scan. Avant cela, le Scanner applique les actions spécifiées aux menaces détectées.
 - **redémarrer le poste** – redémarrer le poste après la fin du scan. Avant cela, le Scanner applique les actions spécifiées aux menaces détectées.
 - **suspendre le poste.**
 - **mettre le poste en veille.**
 - Cochez la case **Désactiver le réseau durant le scan** pour désactiver les connexions réseau et Internet durant le scan.
 - Cochez la case **Scanner les disques durs** pour effectuer le scan des disques durs "fixes" (disques durs etc.).
 - Cochez la case **Scan des supports amovibles** pour analyser tous les supports amovibles, disquettes, CD/DVD, disques flash etc.
 - Dans le champ **Chemins à scanner**, indiquez la liste des chemins à scanner (voir ci-dessous comment indiquer les chemins).
 - Pour ajouter une nouvelle ligne à la liste, cliquez sur  et indiquez le chemin nécessaire dans la ligne qui s'affiche.
 - Pour supprimer un élément de la liste, cliquez sur  contre la ligne correspondante.
- Si vous avez coché la case **Chemins à scanner**, seuls les chemins indiqués seront analysés. Si la case n'est pas cochée, tous les disques seront analysés.

7.5.4.2. Actions



Les paramètres qui ne sont pas supportés dans le cadre du contrôle des postes sous les OS de la famille UNIX et OS X sont mis entre crochets [].

Dans la rubrique **Actions**, vous pouvez configurer la réaction du Scanner en cas de détection de fichiers infectés ou suspects, de programmes malveillants ou d'archives infectées.



Scanner Dr.Web Agent applique automatiquement les actions spécifiées pour les objets malveillants détectés.

Les actions suivantes peuvent être appliquées aux menaces détectées :

- **Désinfecter** – restaurer l'objet dans son état antérieur à l'infection. Si l'objet est incurable ou que les tentatives de désinfection ont échoué, le traitement pour les objets incurables est appliqué.
Cette action ne peut être appliquée qu'aux objets infectés par un virus connu, excepté les Trojans, supprimés dès leur détection, et les fichiers contaminés se trouvant dans des objets complexes (archives, fichiers email ou conteneurs de fichiers).



- **Supprimer** – supprimer les objets infectés.
- **Déplacer en Quarantaine** – déplacer les objets infectés vers le dossier de Quarantaine du poste.
- **Notifier** – envoyer une notification sur la détection d'un virus au Centre de gestion (pour plus d'information, voir la rubrique [Configurer les notifications](#)).
- **Ignorer** – laisser passer l'objet sans lui appliquer aucune action et aucune notification n'est inscrite dans les statistiques du scan.

Tableau 7-3. Les actions du Scanner appliquées aux différents événements viraux

Objet	Action				
	Désinfecter	Supprimer	Déplacer en quarantaine	Notifier	Ignorer
Infectés	+/*	+	+		
Suspects		+	+/*		+
Incurables		+	+/*		
Conteneurs		+	+/*		
Archives		+	+/*		
Fichiers e-mail			+/*		+
Secteurs boot	+/*			+	
Adwares		+	+/*		+
Dialers		+	+/*		+
Canulars		+	+/*		+
Riskwares		+	+/*		+
Hacktools		+	+/*		+

Conventions

- + l'action est autorisée pour ce type d'objets
- +/* l'action est appliquée par défaut à ce type d'objets



Pour paramétrer des actions appliquées aux menaces détectées, utilisez les options suivantes :

- La liste déroulante **Infectés** indique la réaction du Scanner à la détection d'un fichier infecté par un virus connu.
- La liste déroulante **Suspects** indique la réaction du Scanner à la détection d'un fichier présumé infecté par un virus (lors d'une réaction du moteur heuristique).



Si le scan inclut le dossier d'installation de l'OS, il est recommandé de choisir l'action **Notifier** pour les fichiers suspects.

- La liste déroulante **Incurables** indique la réaction du Scanner en cas de la détection d'un fichier infecté par un virus inconnu et si la tentative de réparation a échoué.
- La liste déroulante **Conteneurs infectés** indique la réaction du Scanner en cas de la détection d'un fichier infecté ou suspect inséré à un conteneur.
- La liste déroulante **Archives infectées** indique la réaction du Scanner en cas de la détection d'un fichier infecté ou suspect contenu dans une archive.
- La liste déroulante **Fichiers e-mail infectés** indique la réaction du Scanner en cas de la détection d'un fichier infecté ou suspect au format e-mail.



Si un code viral ou de programme malveillant est détecté au sein d'objets complexes (archives, fichiers e-mail ou conteneurs de fichiers), les actions paramétrées pour ce type de menaces s'appliquent à l'objet en entier et pas seulement à la partie infectée. En tout cas, l'utilisateur en est informé par défaut.

- La liste déroulante **Secteurs boot infectés** indique la réaction du Scanner en cas de la détection d'un virus ou d'un code suspect dans la zone des secteurs boot.
- Dans la liste déroulante suivante, configurez la réaction du Scanner en cas de la détection de logiciels non sollicités :
 - **Adwares** ;
 - **Dialers** ;
 - **Canulars** ;
 - **Riskware** ;
 - **Hacktools**.



Si vous choisissez **Ignorer**, aucune action n'est appliquée : aucune notification n'est envoyée au Centre de gestion, de la même façon que lorsque vous choisissez **Notifier** pour la détection de virus.

Cochez la case **[Redémarrer l'ordinateur automatiquement]** pour redémarrer automatiquement le poste de l'utilisateur à la fin du scan, si les objets infectés détectés et le processus de traitement requièrent le redémarrage du système d'exploitation. Si la case n'est pas cochée, le redémarrage n'aura pas lieu. Les statistiques de scan d'un poste reçues par le Centre de gestion contiennent les notifications sur la nécessité de redémarrer le poste pour terminer le processus



de traitement. Les données sur la nécessité de redémarrer le poste sont affichées dans le tableau [Statut](#). L'administrateur peut redémarrer un poste depuis le Centre de gestion si nécessaire (voir la rubrique [Réseau Antivirus](#)).

Cochez la case **Afficher la progression du scan** pour afficher une barre de progression et une barre de statut du processus de scan des postes dans le Centre de gestion.

7.5.4.3. Limitations



Les paramètres qui ne sont pas supportés dans le cadre du contrôle des postes sous les OS de la famille UNIX et OS X sont mis entre crochets [].



La rubrique **Limitations** offre les paramètres suivants :

- **Durée maximum du scan (ms)** – la durée maximum du scan d'un objet en millisecondes. A l'expiration de ce délai, le scan de l'objet sera arrêté.
- **Niveau maximum d'emboîtement d'une archive** – quantité maximum des archives emboîtés. Si le niveau d'emboîtement est supérieur à la valeur spécifiée, le scan ne sera effectué que jusqu'au niveau d'emboîtement indiqué.
- **[Taille maximum de l'archive (Ko)]** – taille maximum de l'archive à scanner en kilooctets. 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 d'un archive** – 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 d'un objet extrait (Ko)]** – taille maximum d'un objet extrait en kilooctets. Si le Scanner détermine que la taille de l'archive après l'extraction est supérieure à la valeur spécifiée, l'extraction de l'archive et son analyse ne seront pas effectuées.
- **[Seuil de contrôle de la compression (Ko)]** – taille minimum en kilooctets du fichier archivé à partir de laquelle la vérification du ratio de compression sera effectuée.

7.5.4.4. Exclusions

Dans la rubrique **Exclusions**, vous pouvez configurer la liste des fichiers et dossiers à exclure du scan antivirus.

Pour éditer les listes des chemins et fichiers exclus, procédez comme suit :

1. Entrez un chemin ou un fichier dans la ligne **Chemins et fichiers exclus**.
2. Pour ajouter une nouvelle ligne à la liste, cliquez sur  et indiquez le chemin nécessaire dans la ligne qui s'affiche.
3. Pour supprimer un élément de la liste, cliquez sur  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 du scan de tout le disque sur lequel se trouve le répertoire d'installation de Windows,
 - Un chemin qui se termine avec le symbole \ – ce répertoire sera exclu du scan,
 - 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.

Par exemple : C:\Windows – ne pas analyser les fichiers se trouvant dans le répertoire C:\Windows ni dans tous ses sous-répertoires.

2. Les masques des objets à exclure du scan. 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 et Windows XP. Vous pouvez consulter l'article contenant toutes les informations nécessaires à l'adresse suivante – <http://support.microsoft.com/kb/822158/fr>. 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}cases`

Le paramètre le plus souvent utilisé est le symbole `i`, ce paramètre désigne "ne pas prendre en compte la casse".

Exemples des chemins et des fichiers exclus qui sont spécifiés avec les expressions régulières

Expression régulière	Valeur
<code>qr{\\pagefile\.sys\$}i</code>	ne pas scanner les fichiers swap de Windows NT
<code>qr{\\notepad\.exe\$}i</code>	ne pas scanner les fichiers notepad.exe
<code>qr{^C:}i</code>	ne rien scanner sur le disque C
<code>qr{^.:\\WINNT\\}i</code>	ne rien scanner dans les répertoires WINNT sur tous les disques
<code>qr{(^C:) (^.:\\WINNT\\)}i</code>	deux derniers cas sont réunis



Expression régulière	Valeur
<code>qr{^C:\\dir1\\dir2\\file\\.ext\$}i</code>	ne pas scanner le fichier <code>c:\dir1\dir2\file.ext</code>
<code>qr{^C:\\dir1\\dir2\\(.+\\)?file\\.ext\$}i</code>	ne pas scanner le fichier <code>file.ext</code> s'il se trouve dans le répertoire <code>c:\dir1\dir2</code> ou dans ses sous-répertoires
<code>qr{^C:\\dir1\\dir2\\}i</code>	ne pas scanner le répertoire <code>c:\dir1\dir2</code> ni ses sous-répertoires
<code>qr{dir\\[^\\]+}i</code>	ne pas scanner le sous-répertoire <code>dir</code> se trouvant dans n'importe quel répertoire, mais vérifier les sous-dossiers
<code>qr{dir\\}i</code>	ne pas scanner le sous-répertoire <code>dir</code> se trouvant dans n'importe quel répertoire, ni ses sous-répertoires

Les expressions régulières sont brièvement décrites dans les **Annexes**, dans la rubrique [Annexe J. Utilisation des expressions régulières dans Dr.Web Enterprise Security Suite](#).

Dans la sous-rubrique **Vérifier le contenu des fichiers suivants**, vous pouvez désactiver le contrôle des fichiers composés. Pour ce faire, décochez les cases suivantes :

- La case **Archives** indique au Scanner de rechercher les virus dans les fichiers contenus dans les archives.
- La case **Fichiers e-mail** indique de scanner les boîtes e-mail.
- La case **Packages d'installation** indique au Scanner de vérifier les packages d'installation de logiciels.

7.6. Consultation des statistiques sur un poste

Le menu de gestion de la rubrique **Réseau antivirus** vous permet de consulter les informations suivantes :

- [Statistiques](#) – statistiques relatives au fonctionnement des outils antivirus sur le poste ainsi que les informations sur le statut des postes et des outils antivirus, pour consulter et sauvegarder les rapports contenant des données statistiques récapitulatives ou des extraits de tableaux spécifiques.
- [Graphiques](#) – les graphiques affichant des informations sur les infections détectées sur les postes.
- [Quarantaine](#) – accès distant au contenu de la Quarantaine sur le poste.

7.6.1. Statistiques



Vous pouvez également configurer la création automatique du rapport statistique contenant l'ensemble des tableaux statistiques dont vous avez besoin. Ce rapport peut être enregistré



au format nécessaire sur le Serveur ou bien il peut être envoyé par e-mail.

Pur cela, configurez la tâche **Création d'un rapport statistique** dans la [planification](#) du Serveur.

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](#) qui s'affiche, sélectionnez l'élément nécessaire dans la rubrique **Statistiques**.

La rubrique **Statistiques** comprend les éléments suivants :

- **Statistiques sommaires** – pour obtenir des statistiques sommaires (non par session).
- [Tableau récapitulatif](#) – pour consulter et sauvegarder les rapports contenant toutes les données statistiques sommaires ou les données de synthèse sélectives selon les types de tableaux spécifiés. Cet élément ne s'affiche pas dans le menu si tous les autres éléments sont masqués dans la rubrique **Statistiques**.
- **Menaces** – pour consulter les informations sur la détection des menaces de sécurité sur les postes protégés : liste des objets infectés, emplacement par postes, noms de menaces, actions réalisées par l'antivirus etc.
- **Erreurs** – pour consulter la liste des erreurs de scan sur un poste sélectionné pour une période déterminée.
- [Statistiques de scan](#) – pour obtenir des statistiques sur le fonctionnement des outils antivirus sur le poste.
- **Démarrage/Arrêt** – pour consulter la liste des composants lancés sur le poste.
- **Statistiques des menaces** – pour consulter les informations sur la détection des menaces de sécurité sur les postes. Les informations sont triées selon les types des menaces et le nombre des menaces sur les postes.
- [Statut](#) – pour consulter les informations sur un statut non-standard des postes et éventuellement nécessitant une intervention.
- **Tâches** – pour consulter la liste des tâches spécifiées pour le poste durant une période donnée.
- **Produits** – pour consulter les informations sur les produits installés sur les postes sélectionnés. Sous produits on comprend dans ce cas les produits du [dépôt](#) du Serveur.
- **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 qu'un poste soit sélectionné.
- **Modules** – pour consulter les informations détaillées sur tous les modules de l'antivirus Dr.Web : description du module : son nom fonctionnel ; fichier représentant un module particulier ; la version complète du module etc. Cet élément n'est accessible qu'à condition qu'un poste soit sélectionné.



- **Installations des Agents** – pour consulter la liste des installations de l'Agent sur le poste ou dans le groupe des postes.
- **Désinstallations des Agents** – pour consulter la liste des postes de travail sur lesquels le logiciel Dr.Web a été supprimé.



Pour afficher les éléments masqués de la rubrique **Statistiques**, sélectionnez l'élément **Administration** du menu principal, puis dans la fenêtre qui apparaît, sélectionnez l'élément du menu de gestion **Configuration du Serveur Dr.Web**. Dans l'onglet **Statistiques**, cochez les cases correspondantes (voir ci-dessous), cliquez ensuite sur **Sauvegarder** et redémarrez le Serveur.

Tableau 7-4. Correspondance entre les éléments de la rubrique Statistiques et les cases de la rubrique Statistiques dans la configuration du Serveur

Éléments de la rubrique Statistiques	Cases de la rubrique Statistiques dans la configuration du Serveur
Statistiques sommaires	Statistiques de scan
Menaces	Menaces de sécurité détectées
Erreurs	Erreurs de scan
Statistiques de scan	Statistiques de scan
Démarrage/Arrêt	Démarrage/arrêt des composants
Statistiques des menaces	Menaces de sécurité détectées
Statut	Statuts des postes
Tâches	Journal d'exécution des tâches sur les postes
Bases virales	Statuts des postes Surveillance des bases virales Journal d'exécution des tâches sur les postes
Modules	Liste des modules des postes
Installations des Agents	Installations des Agents

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.



7.6.1.1. Données sommaires

Pour consulter les statistiques sommaires :

1. Sélectionnez un poste ou un groupe dans la liste hiérarchique.
2. Sélectionnez l'onglet **Statistiques sommaires** dans la rubrique **Statistiques** du [menu de gestion](#).
3. Une fenêtre contenant les données du rapport va s'ouvrir. Pour insérer les données dans le tableau, cliquez sur **Données de synthèse** dans la barre d'outils et choisissez les types nécessaires dans la liste déroulante : **Statistiques de scan, Menaces, Tâches, Démarrage/Arrêt, Erreurs**. Les statistiques de ces rubriques sont identiques à celles de la rubrique **Tableaux**. Pour voir le rapport avec les tableaux sélectionnés, cliquez sur **Actualiser**.
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**.
5. Pour sauvegarder le rapport pour l'imprimer ou le traiter plus tard, cliquez sur l'un des boutons suivants :



Sauvegarder les données dans un fichier CSV,



Sauvegarder les données dans un fichier HTML,



Sauvegarder les données dans un fichier XML,



Sauvegarder les données dans un fichier PDF.

7.6.1.2. Statistiques de scan

Marche à suivre pour obtenir des statistiques sur le fonctionnement des outils antivirus sur le poste :





1. Sélectionnez un poste ou un groupe dans la liste hiérarchique.



Pour consulter les statistiques relatives aux plusieurs postes ou groupes, vous pouvez les sélectionner à l'aide des touches SHIFT ou CTRL.

2. Dans le [menu de gestion](#), dans la rubrique **Statistiques**, sélectionnez l'élément **Statistiques de scan**.
3. Par défaut, les statistiques relatives aux dernières vingt-quatre heures s'affichent.
4. Pour consulter les informations relatives à une période déterminée, vous pouvez indiquer dans la liste déroulante une période arbitraire 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 nécessaires ou cliquez sur les icônes du calendrier contre les champs des dates. Pour charger des données, cliquez sur **Actualiser**. Les tableaux statistiques seront chargés.



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).
6. 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. Une fenêtre (ou une rubrique de la fenêtre active) contenant le tableau avec les données détaillées va s'ouvrir.
7. 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.
8. 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.
9. Pour sauvegarder le rapport pour l'imprimer ou le traiter plus tard, cliquez sur l'un des boutons suivants :
 -  **Sauvegarder les données dans un fichier CSV,**
 -  **Sauvegarder les données dans un fichier HTML,**
 -  **Sauvegarder les données dans un fichier XML,**
 -  **Sauvegarder les données dans un fichier PDF.**
10. Pour consulter les statistiques sommaires sans marquer les sessions, cliquez sur l'élément **Statistiques sommaires** dans le menu de gestion. Une fenêtre des statistiques sommaires va s'afficher.
11. Pour consulter les statistiques sommaires triées par événements viraux sous forme graphique, dans le [menu de gestion](#), sélectionnez l'élément **Graphiques**. Une fenêtre contenant des diagrammes statistiques va s'afficher (pour en savoir plus, consultez les informations [ci-dessous](#)).

7.6.1.3. Statut

Pour consulter les données sur les statuts des postes :

1. Sélectionnez un poste ou un groupe dans la liste hiérarchique.
2. Dans le [menu de gestion](#), sélectionnez l'élément **Statut** dans la rubrique **Statistiques**.
3. Les données sur le statut de postes s'affichent conformément aux paramètres du filtre. Les paramètres suivants du filtre sont disponibles dans la barre d'outils :
 - Dans la liste déroulante **Période**, sélectionnez la période pendant laquelle l'événement s'est produit. Dans le champ de période s'affiche le nombre des jours correspondant à la valeur



sélectionnée : dans la liste s'affichent les postes dont les événements sont survenus pendant le délai spécifié.

- Dans la liste **Importance**, activez l'option de sélection du niveau d'emboîtement minimum des messages : la liste des messages sur le statut va contenir les messages avec le niveau sélectionné et supérieur.
 - Dans la liste **Source**, cochez les cases pour les sources des événements qui seront affichés dans la liste :
 - **Agent** – afficher les événements venus des Agents Dr.Web connectés à ce Serveur.
 - **Serveur** – afficher les événements venus de ce Serveur Dr.Web.
 - **Connectés** – afficher les événements pour les postes qui sont connectés à ce Serveur et qui sont en ligne (online) en ce moment.
 - **Déconnectés** – afficher les événements pour les postes qui sont connectés à ce Serveur et qui sont hors ligne (offline) en ce moment.
 - **Désinstallés** – afficher le dernier événement pour les postes sur lesquels l'antivirus Dr.Web a été supprimé.
4. Cliquez sur **Actualiser** pour appliquer tous les paramètres sélectionnés du filtre et afficher les paramètres correspondants.
 5. Les actions relatives au niveau de détails et au formatage des informations de ce tableau sont identiques aux actions pour le tableau des statistiques de scan décrites ci-dessus.



Pour consulter les rapports de fonctionnement et les statistiques de plusieurs postes, sélectionnez-les dans la liste hiérarchique réseau.

6. Pour sauvegarder le rapport pour l'imprimer ou le traiter plus tard, cliquez sur l'un des boutons suivants :



Sauvegarder les données dans un fichier CSV,



Sauvegarder les données dans un fichier HTML,



Sauvegarder les données dans un fichier XML,



Sauvegarder les données dans un fichier PDF.

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 d'un poste ou d'un groupe dans l'arborescence. Dans le [menu de gestion](#), sélectionnez l'élément **Graphiques** dans la rubrique **Général**.
2. La fenêtre affichant les graphiques suivantes va s'ouvrir :



- **Activité virale** – le graphique présente le nombre total des virus détectés pendant une période donnée pour tous les postes et les groupes sélectionnés. Ce graphique est affiché à condition que la période sélectionnée soit supérieure à 24H.
 - **Menaces les plus répandues** – le top 10 des menaces présents dans le plus grand nombre de fichiers. Le graphique présente les données numériques par objets relatifs à une menace concrète.
 - **Classes de menaces** – cet élément affiche la liste des menaces conformément à la classification des objets malveillants. Le diagramme circulaire présente le pourcentage de chaque menace détectée.
 - **Postes les plus infectés** – cet élément affiche la liste des postes sur lesquels les menaces de sécurité ont été détectées. Le graphique présente le nombre total des menaces pour chaque poste.
 - **Actions réalisées** – cet élément affiche la liste des actions appliquées aux objets malveillants détectés. Le diagramme circulaire présente le pourcentage de chaque action réalisée.
3. Pour consulter les données graphiques relatives à une période donnée, sélectionnez une période dans la liste déroulante dans la barre d'outils : le rapport pour un jour ou un mois. Vous pouvez également sélectionner n'importe quelle plage de dates, pour cela, entrez les dates nécessaires ou sélectionnez les dates dans les calendriers déroulantes. Pour afficher les données, cliquez sur le bouton **Actualiser**.
 4. Pour exclure un élément de l'affichage dans le graphique (sauf le graphique **Activité virale**) cliquez sur le nom de cet élément dans la légende sous le graphique.

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 **Statistiques** du menu de gestion. Le tableau ci-dessous contient la liste de tous les graphiques possibles et les rubriques du menu de gestion dans lesquels ces graphiques sont affichés.

Tableau 7-5. Conformité des graphiques aux rubriques du menu de gestion

Graphiques	Rubriques
Activité virale	Graphiques
Menaces les plus répandues	Graphiques Menaces Statistiques des menaces
Classes des menaces	Graphiques Statistiques des menaces
Postes les plus infectés	Graphiques



Graphiques	Rubriques
Actions réalisées	Graphiques Menaces
Nombre d'erreurs par poste	Erreurs
Nombre d'erreurs par composant	Erreurs
Menaces par composant	Démarrage/Arrêt
Erreurs par composants	Démarrage/Arrêt

- **Nombre d'erreurs par poste** – cet élément affiche la liste des postes sur lesquels survenaient des erreurs de fonctionnement des composants antivirus. Le graphique présente le nombre total d'erreurs pour chaque poste.
- **Nombre d'erreurs par composant** – cet élément affiche la liste des composants antivirus dont le fonctionnement provoquaient des erreurs. Le diagramme circulaire présente le pourcentage d'erreurs pour chaque composant.
- **Menaces par composant** – cet élément affiche la liste des composants antivirus qui ont détecté les menaces. Le graphique présente le nombre total des menaces détectées par chaque composant.
- **Erreurs par composant** – cet élément affiche une liste des composants antivirus dont le fonctionnement provoquaient des erreurs. Le graphique présente le nombre total d'erreurs pour chaque composant.

7.6.3. Quarantaine

Contenu de la quarantaine

Les fichiers peuvent être mis en Quarantaine par un des composants antivirus, par exemple, par le Scanner.

L'utilisateur peut rescanner 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](#), 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.



Les statistiques du rescane de l'objet placé en Quarantaine affichées dans la colonne **Informations** concerne uniquement le rescane lancé via le Centre de gestion.

Si l'objet placé en Quarantaine a le statut **non infecté**, cela signifie qu'après la mise en quarantaine cet objet considéré comme menace a été rescanné et il a reçu le statut sain.

Les objets de la quarantaine peuvent être restaurés seulement manuellement.






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 dans le dossier où il se trouvait avant le déplacement en Quarantaine).
 - 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 de la Quarantaine et du système.
 -  **Scanner les fichiers** – rescanner les fichiers sélectionnés dans la Quarantaine.
 -  **Exporter** – 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 plus tard pour l'analyse auprès du laboratoire antivirus de Doctor Web. Pour sauvegarder les fichiers, cochez les cases correspondantes contre les fichiers en question et cliquez ensuite sur **Exporter**.

- Exporter les données sur le statut de la Quarantaine vers un fichier sous un des formats suivants :



Sauvegarder les données dans un fichier CSV,



Sauvegarder les données dans un fichier HTML,



Sauvegarder les données dans un fichier XML,



Sauvegarder les données dans un fichier PDF.



7.7. Envoi des fichiers d'installation

Lors de la création d'un nouveau compte pour un poste, un package d'installation personnel pour l'installation de l'Agent Dr.Web est généré dans le Centre de gestion. Le package d'installation inclut l'installateur de l'Agent Dr.Web et l'ensemble de paramètres de connexion au Serveur Dr.Web ainsi que les paramètres d'authentification du poste sur le Serveur Dr.Web (vous pouvez consulter la description du package d'installation et du processus d'installation de l'Agent via ce package d'installation dans le **Manuel d'installation**, la rubrique [Installation de l'Agent Dr.Web en mode local](#)).

Après avoir créé les packages d'installation, pour plus de commodité, vous pouvez envoyer les packages d'installation concrets sur les e-mails des utilisateurs.

Lors de l'envoi des packages d'installation, le contenu de la lettre est généré de la façon suivante :



1. Le système d'exploitation est connu :
 - a) OS Windows : le package d'installation de l'Agent Dr.Web pour Windows est attaché en pièce jointe.
 - b) Linux, OS X, Android : le package d'installation de l'Agent Dr.Web pour le système d'exploitation correspondant et le fichier de configuration contenant les paramètres de connexion au Serveur Dr.Web sont attachés en pièces jointes.
2. Le système d'exploitation est inconnu – un nouveau compte du poste, l'Agent n'est pas encore installé :
 - a) Si sur le Serveur il n'y a pas de packages d'installation sous Linux, OS X, Android (notamment, la [distribution supplémentaire \(extra\)](#) n'est pas installée sur le Serveur), le package d'installation de l'Agent Dr.Web pour Windows et le fichier de configuration contenant les paramètres de connexion au Serveur Dr.Web pour les postes sous Linux, OS X, Android sont attachés à la lettre en pièces jointes.
 - b) Si sur le Serveur il y a au moins un seul package d'installation pour les postes tournant sous Windows : le package d'installation de l'Agent Dr.Web pour Windows est attaché à la lettre en pièce jointe, ainsi que le fichier de configuration avec les paramètres de connexion au Serveur Dr.Web pour les postes sous Linux, OS X, Android et le lien de téléchargement des fichiers d'installation pour les postes tournant sous Linux, OS X, Android.

Pour envoyer les packages d'installation par e-mail, procédez comme suit :

1. Sélectionnez l'élément **Réseau antivirus** du menu principal du Centre de gestion, puis dans la fenêtre qui apparaît, sélectionnez les objets suivants dans l'arborescence :
 - sélectionnez le poste pour envoyer par e-mail le package d'installation généré pour ce poste.
 - sélectionnez le groupe des postes pour envoyer par e-mail tous les packages d'installation générés pour les postes de ce groupe.

Pour sélectionner plusieurs objets en même temps utilisez les boutons CTRL et SCHIFT.



2. Dans la barre d'outils, cliquez sur  **Général** →  **Envoyer les fichiers d'installation**.
3. Dans la rubrique **Envoyer les fichiers d'installation** qui s'affiche, configurez les paramètres suivants :
 - Dans la section **Adresse e-mail du destinataire**, spécifiez l'adresse e-mail à laquelle le package d'installation sera envoyé. Si plusieurs postes ou groupes ont été sélectionnés, spécifiez les adresses e-mail pour chaque poste en particulier pour envoyer les packages d'installation.
 - Dans la section **Additionnel** cochez la case **Mettre dans une archive zip** pour mettre les fichiers d'installation dans une archive zip. L'archivage peut être utile en cas de présence des filtres e-mail du côté de l'utilisateur qui peuvent bloquer les fichiers exécutables qui se trouvent en pièces jointes.
 - Dans la section **Expéditeur**, spécifiez l'adresse e-mail qui sera indiquée comme adresse de l'expéditeur de la lettre contenant les fichiers d'installation.
 - Dans la section **Configuration du serveur SMTP** sont spécifiés les paramètres du Serveur SMTP qui sera utilisé pour envoyer les e-mails. Si les paramètres sont connus, par exemple ils ont été déjà spécifiés, cette rubrique sera masquée. Vous pouvez l'ouvrir pour modifier les paramètres spécifiés. Lors du premier envoi des packages d'installation, il faut spécifier dans cette rubrique les paramètres suivants :
 - **Adresse** – adresse du serveur SMTP qui sera utilisée pour envoyer des e-mails.
 - **Port** – port pour la connexion au serveur SMTP. C'est le port 465 qui est utilisé par défaut en cas d'ouverture d'une connexion TLS sécurisée à part, sinon, c'est le port 25.
 - **Utilisateur, Mot de passe** – si nécessaire, spécifiez le nom de l'utilisateur et le mot de passe de l'utilisateur du serveur SMTP, si le serveur SMTP exige l'authentification.
 - Cochez la case **Chiffrement STARTTLS** pour l'échange chiffré de données. Dans ce cas, le passage à la connexion sécurisée s'effectue via la commande `STARTTLS`. L'utilisation du port 25 pour la connexion est prévue par défaut.
 - Cochez la case **Chiffrement SSL** pour l'échange chiffré de données. Dans ce cas, une connexion TLS sécurisée sera ouverte à part. L'utilisation du port 465 pour la connexion est prévue par défaut.
 - Cochez la case **Utiliser l'authentification CRAM-MD5** pour utiliser l'authentification *CRAM-MD5* sur le serveur de messagerie.
 - Cochez la case **Utiliser l'authentification DIGEST-MD5** pour utiliser l'authentification *DIGEST-MD5* sur le serveur de messagerie.
 - Cochez la case **Utiliser l'authentification standard** pour utiliser l'authentification *plain text* sur le serveur de messagerie.
 - Cochez la case **Utiliser l'authentification LOGIN** pour utiliser l'authentification *LOGIN* sur le serveur de messagerie.
 - Cochez la case **Vérifier le certificat SSL du serveur** pour vérifier le certificat SSL du serveur de messagerie.
 - Cochez la case **Mode de débogage** pour consulter le journal détaillé de la session SMTP. Cliquez sur **Envoyer**.

7.8. Envoi de messages aux postes

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 du côté de l'utilisateur sous forme d'infobulles (voir [la figure 7-1](#)).

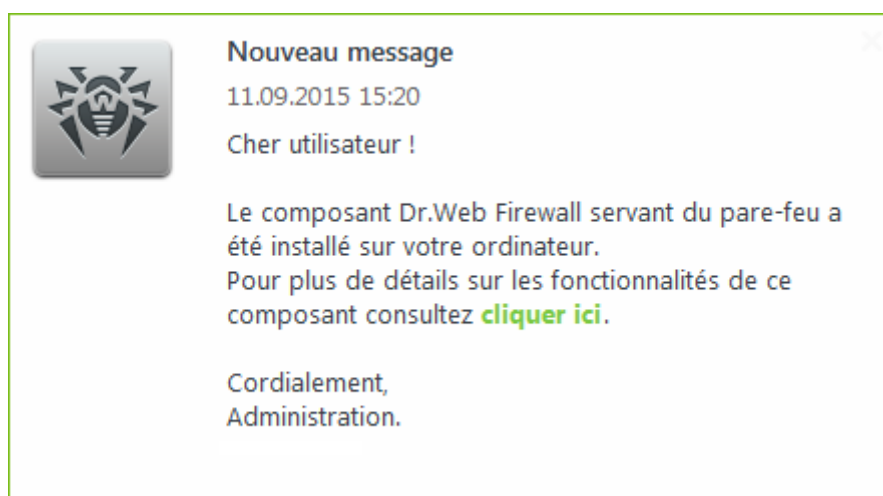



Figure 7-1. Fenêtre d'un message sur un poste tournant sous Windows

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 dans la barre d'outils cliquez sur **★ Général** → **Envoyer des messages aux postes**.
3. Dans la fenêtre qui apparaît, remplissez les champs suivants :
 - **Texte du message** est un champ obligatoire à remplir. Le champ contient le message.
 - Cochez la case **Afficher le logo dans le message** pour afficher le logo dans l'en-tête de la fenêtre de message. Spécifiez les paramètres suivants du logo :
 - Cochez cette case **Utiliser la transparence** pour utiliser la transparence dans l'affichage du logo (voir [Format du logo](#), p. 4).
 - Le champ **URL** permet de spécifier le lien vers une page web à ouvrir lors d'un clic sur le logo ou sur l'en-tête de la fenêtre.
 - Dans le champ **En-tête du message**, vous pouvez spécifier un en-tête du message, par exemple, le nom de l'entreprise. Ce texte sera affiché dans l'en-tête de la fenêtre de message (à droite du logo). Si vous laissez ce champ vide, des informations sur le message s'afficheront au lieu du logo.



- A droite du champ **Fichier du logo**, cliquez sur le bouton  pour télécharger le logo depuis une ressource locale et sélectionnez ensuite l'objet nécessaire dans le fichier dans l'explorateur (voir [Format du fichier de logo](#)).

S'il n'y a pas de logo ou la taille du logo dépasse la taille maximale (voir [Format du fichier logo](#), p. 3), l'icône de l'Agent Dr.Web sera affichée à sa place.

- Cochez la case **Afficher le lien dans le message** pour insérer le lien sur les ressources web dans le message.

Pour ajouter un lien, procédez comme suit :

1. Spécifiez le lien sur une ressource web 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 message.
 3. Dans le champ **Texte du message**, saisissez une balise `{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**).
- Cochez la case **Envoyer seulement sur les postes sur le réseau** pour envoyer le message uniquement sur les postes qui sont sur le réseau (online). Si la case est cochée, le message ne sera pas envoyé sur les postes qui sont hors réseau. Si la case est décochée, l'envoi du message sur les postes hors réseau sera reporté jusqu'au moment de leur connexion.
 - Cochez la case **Afficher le statut de l'envoi** pour afficher la notification sur le statut de l'envoi.
4. Cliquez sur **Envoyer**.

Format du fichier de logo

Le fichier contenant une image (logo) incluse dans le message doit correspondre aux critères suivants :

1. Format graphique du fichier : BMP, JPG, PNG, GIF, SVG.
2. La taille du fichier de logo ne doit pas dépasser 512 Ko.
3. Les dimensions extérieures du logo – 72x72 pixels. Les images ayant d'autres dimensions seront mises à l'échelle lors de l'envoi jusqu'aux dimensions par défaut.
4. Profondeur des couleurs (bit depth) – n'importe quelle (8 – 24 bits).
5. Dans le cas où la case **Utiliser la transparence** a été cochée 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 utilisez 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 7-2 est utilisée comme logo, le fond de couleur violette sera enlevé (devient transparent).



Figure 7-2. Logo de forme non standard



Si vous souhaitez utiliser un logo ayant un fond transparent, utilisez les fichiers au format PNG ou GIF.

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.

Exemple de l'envoi du message

Pour envoyer le message affiché sur la figure 7-1, les paramètres suivants ont été spécifiés :

Texte du message :

```
Cher utilisateur !

Le composant Dr.Web Firewall servant du pare-feu a été installé sur votre
ordinateur.

Pour plus de détails sur les fonctionnalités de ce composant consultez
{link}.

Cordialement,
Administration.
```

URL : `http://drweb.com/`

Texte : cliquer ici



Chapitre 8. Configuration du Serveur Dr.Web

Cette chapitre contient la description de fonctionnalités suivantes de configuration du réseau antivirus et du Serveur Dr.Web :

- [Journalisation](#) – consulter et gérer l'accès aux journaux du Serveur, consulter les statistiques détaillées sur le fonctionnement du Serveur ;
- [Configuration du Serveur Dr.Web](#) – configurer les paramètres du Serveur ;
- [Configuration de la planification du Serveur Dr.Web](#) – configurer la planification de tâches pour maintenir le Serveur ;
- [Configuration du Serveur web](#) – configurer les paramètres du Serveur web ;
- [Procédures utilisateur](#) – activer et configurer les procédures utilisateur ;
- [Configuration des notifications](#) – configurer le système de notification de l'administrateur sur les événements du réseau antivirus par les différents moyens de notification ;
- [Gestion du dépôt du Serveur Dr.Web](#) – configurer le dépôt pour la mise à jour de tous les composants du réseau antivirus depuis le SGM et la diffusion ultérieure des mises à jour sur les postes ;
- [Gestion de la base de données](#) – maintenir la base de données du Serveur ;
- [Particularités du réseau avec plusieurs Serveurs Dr.Web](#) – configurer le réseau antivirus multi-serveurs et les connexions voisines.

8.1. Journalisation

8.1.1. Journal d'audit

Le journal d'audit permet de consulter la liste des événements et des modifications effectuées via les sous-systèmes de gestion de Dr.Web Enterprise Security Suite.

Pour consulter le journal d'audit :

1. Sélectionnez l'élément **Administration** du menu principal du Centre de gestion.
2. Dans la fenêtre qui s'ouvre, sélectionnez l'élément **Journal d'audit** du menu de gestion.
3. Le tableau contenant les événements enregistrés va s'ouvrir. Pour configurer l'affichage du journal, spécifiez une période d'actions dans la barre d'outils. Pour cela, vous pouvez sélectionner une des périodes proposées dans la liste déroulante ou spécifier les dates aléatoires dans des calendriers qui s'affichent quand vous cliquez sur les champs de dates. Cliquez sur **Actualiser** pour afficher le journal pour les dates sélectionnés.
4. Le tableau du journal contient les données suivantes :
 - **Date** - la date et l'heure de la réalisation de l'action.



- **Login** - le nom d'enregistrement de l'administrateur du Serveur. Il est indiqué si c'est l'administrateur qui a initié l'action ou que la connexion au Serveur s'effectue avec les identifiants de l'administrateur.
- **Adresse** - l'adresse IP depuis laquelle l'action a été initiée. Elle est indiquée uniquement en cas de connexion externe au Serveur, notamment lors de la connexion via le Centre de gestion ou via Web API.
- **Sous-système** - le nom du sous-système par lequel ou via lequel l'action a été initiée. L'enregistrement d'audit s'effectue pour les sous-systèmes suivants :
 - **Centre de gestion** - l'action a été réalisée via le Centre de gestion de la sécurité Dr.Web, notamment par l'administrateur.
 - **Web API** - l'action a été réalisée via Web API, par exemple depuis une application externe connectée avec les identifiants de l'administrateur (voir aussi les **Annexes**, p. [Annexe L. Intégration de Web API et de Dr.Web Enterprise Security Suite](#)).
 - **Serveur** - l'action a été réalisée par le Serveur Dr.Web, par exemple selon sa planification.
 - **Utilitaires** - l'action a été initiée via les utilitaires externes, notamment via l'utilitaire de diagnostic distant du Serveur.
- **Résultat** - le résultat de l'exécution de l'action en bref :
 - **OK** - l'opération est effectuée avec succès.
 - **échoué** - une erreur est survenue lors de l'exécution de l'opération. L'opération n'est pas effectuée.
 - **commencé** - l'opération a été initiée. Vous allez apprendre le résultat uniquement après la fin de l'opération.
 - **pas de droits** - l'administrateur qui a lancé l'opération ne possède pas des droits nécessaires pour son exécution.
 - **reporté** - l'opération est reportée pour un délai déterminé ou jusqu'à un certain événement.
 - **impossible** - l'exécution de l'action est bloquée. Par exemple, la suppression des groupes système.



Les actions échouées (la valeur **échoué** dans la colonne **Résultat**), sont marquées en rouge.

- **Opération** - description de l'action.
5. Si nécessaire, vous pouvez exporter les données pour une période sélectionnée vers un fichier. Pour ce faire, cliquez sur un des boutons suivants dans la barre d'outils :



Sauvegarder les données dans un fichier CSV,



Sauvegarder les données dans un fichier HTML,



Sauvegarder les données dans un fichier XML,



Sauvegarder les données dans un fichier PDF.



8.1.2. Journal de fonctionnement du Serveur Dr.Web

Le Serveur Dr.Web effectue la journalisation des événements relatifs à son fonctionnement.



Le journal du Serveur est utilisé pour le débogage et pour la détection des problèmes en cas de dysfonctionnement des composants du réseau antivirus.


Par défaut, le fichier de journal a le nom `drwcsd.log` et se place dans :

- Sous **UNIX** :
 - sous Linux et Solaris : `/var/opt/drwcs/log/drwcsd.log` ;
 - sous FreeBSD : `/var/drwcs/log/drwcsd.log`.
- Sous **Windows** : dans le sous-répertoire `var` du répertoire d'installation du Serveur.

Le fichier est au format texte simple (voir les **Annexes**, la rubrique [Annexe K. Format des fichiers de journal](#)).

Pour consulter le journal du Serveur via le Centre de gestion :

1. Sélectionnez l'élément **Administration** du menu principal du Centre de gestion.
2. Dans la fenêtre qui s'ouvre, sélectionnez l'élément **Log du Serveur Dr.Web** du menu de gestion.
3. Une fenêtre affichant la liste des journaux du Serveur va s'ouvrir. Le format suivant des noms des fichiers de journal du Serveur est utilisé en fonction des paramètres du mode de rotation : `<file_name>.<N>.log` ou `<file_name>.<N>.log.gz`, où `<N>` est un numéro d'ordre : 1, 2, etc. Par exemple, si le nom du fichier de journal est `drwcsd`, la liste des fichiers de journal est la suivante :
 - `drwcsd.log` — fichier de journal actuel (dans lequel s'effectue l'écriture),
 - `drwcsd.1.log.gz` — fichier de journal précédent,
 - `drwcsd.2.log.gz` et ainsi de suite — plus le nombre est élevé, plus la version est ancienne.
4. Pour gérer les fichiers du journal, cochez la case contre un fichier ou plusieurs fichiers nécessaires. Pour sélectionner tous les fichiers de journal, cochez la case dans l'en-tête du tableau. Dans la barre d'outils, les boutons suivants seront disponibles :

 **Exporter les fichiers de journal sélectionnés** – sauvegarder la copie locale des fichiers de journal sélectionnés. La sauvegarde des copies de journal peut être utilisée, par exemple, pour consulter le contenu du fichier de journal depuis l'ordinateur distant.

 **Supprimer les fichiers de journal sélectionnés** – pour supprimer les fichiers de journal sélectionnés sans possibilité de restauration.



Configuration du journal de fonctionnement sous UNIX

Sur les Serveurs Dr.Web tournant sous les OS de la famille UNIX, il existe une possibilité d'écrire le journal de fonctionnement du Serveur via un fichier de configuration spécifique :

- sous Linux et Solaris : `/var/opt/drwcs/etc/local.conf` ;
- sous FreeBSD : `/var/drwcs/etc/local.conf`.

Contenu du fichier `local.conf` :

```
# Log level.  
DRWCS_LEV=trace3  
  
# Log rotation.  
DRWCS_ROT=10,10m
```

Les valeurs des paramètres correspondent aux valeurs des clés de la ligne de commande pour le lancement du Serveur :

- `-verbosity=<niveau_de_détail>` – niveau de détail du journal de l'Agent.
- `-rotate=<N><f>, <M><u>` – mode de rotation du journal de fonctionnement du Serveur.

Vous trouverez la description détaillée des clés dans le document **Annexes**, rubrique [H4.8](#).



Si le fichier `local.conf` a été édité lors du fonctionnement du Serveur, il faut redémarrer le Serveur pour que les modifications apportées aux paramètres d'écriture du journal entrent en vigueur. Le redémarrage doit être lancé par des moyens du système d'exploitation.

Les copies de sauvegarde du fichier `local.conf` sont créées lors de la mise à jour et la suppression du Serveur. Cela permet de gérer le niveau d'écriture du journal lors de la mise à jour de paquets du Serveur.

8.1.3. Journal des mises à jour du dépôt

Journal des mises à jour du dépôt des produits – cet élément contient la liste de mises à jour depuis le SGM et les informations détaillées sur les révisions mises à jour de produits.

Pour consulter le journal des mises à jour du dépôt :

1. Sélectionnez l'élément **Administration** du menu principal du Centre de gestion.
2. Dans la fenêtre qui s'ouvre, sélectionnez l'élément **Journal des mises à jour du dépôt des produits**.
3. Le tableau contenant les événements enregistrés va s'ouvrir. Pour configurer l'affichage du journal, spécifiez une période d'actions dans la barre d'outils. Pour cela, vous pouvez sélectionner une des périodes proposées dans la liste déroulante ou spécifier les dates aléatoires



dans des calendriers qui s'affichent quand vous cliquez sur les champs de dates. Cliquez sur **Actualiser** pour afficher le journal pour les dates sélectionnés.

4. Le tableau du journal contient les données suivantes :

- **Début** - date et heure du début du téléchargement des mises à jour depuis le SGM pour un produit concret.
- **Fin** - date et heure de la fin du téléchargement des mises à jour depuis le SGM pour un produit concret.
- **Nom du produit** - nom du produit du dépôt qui a été téléchargé ou dont le téléchargement a été sollicité.
- **Résultat de la mise à jour** - résultat de la mise à jour du dépôt. Vous pouvez consulter une brève information sur la fin réussie de la mise à jour ou sur la raison de l'erreur.



Pour les actions échouées, les cases **Code de terminaison** sont marquées en rouge.

- **Révision initiale** - numéro de la révision (les révisions sont numérotées selon la date de leur création) qui était la dernière pour ce produit avant le début de la mise à jour.
- **Révision de la mise à jour** - numéro de la révision (les révisions sont numérotées selon la date de leur création) qui était téléchargée lors de la mise à jour.
- **Fichiers mis à jour** - brève information sur les fichiers mis à jour au format suivant : *<nombre des fichiers> - <action sur les fichiers>*.
- **Initiateur** - système qui a initié le processus de la mise à jour :
 - **Lancée depuis la ligne de commande** - la mise à jour est initiée par l'administrateur avec la commande correspondante de console.
 - **Lancée par le Planificateur de tâches** - la mise à jour est lancée selon la tâche de la [planification du Serveur Dr.Web](#).
 - **Mise à jour entre serveurs** - la mise à jour a été obtenue via la liaison entre serveurs depuis le Serveur principal. Cet initiateur est présent uniquement en cas de [configuration multi-serveurs](#) du réseau antivirus avec la diffusion des mises à jour par les liaisons entre serveurs.
 - **Lancée depuis le Centre de gestion** - la mise à jour est lancée par l'administrateur via le Centre de gestion de la sécurité Dr.Web, dans la rubrique [Statut du dépôt](#).
 - **Importation du dépôt** - la mise à jour a été téléchargée par l'administrateur via la rubrique [Contenu du dépôt](#) du Centre de gestion.
- **Administrateur** - nom d'enregistrement de l'administrateur du Serveur. Il est indiqué si c'est l'administrateur qui a initié l'action.
- **Adresse réseau** - adresse IP depuis laquelle l'action a été initiée. Elle est indiquée uniquement en cas de connexion externe au Serveur, notamment lors de la connexion via le Centre de gestion ou via Web API.
- **Répertoire dans le dépôt** - nom du répertoire du dépôt du Serveur qui a été modifié selon le processus de la mise à jour.



5. Pour plus d'informations sur une mise à jour concrète, cliquez sur la ligne de cette mise à jour. Une fenêtre qui s'affiche contient le tableau des fichiers du produit qui ont été modifiés lors de la mise à jour sélectionnée. Pour chaque fichier, les informations suivantes sont disponibles : **Nom du fichier**, **Hash de fichier**, **Taille** et **Statut**.
6. Si nécessaire, vous pouvez exporter les données pour une période sélectionnée vers un fichier. Pour ce faire, cliquez sur un des boutons suivants dans la barre d'outils :

 **Sauvegarder les données dans un fichier CSV,**

 **Sauvegarder les données dans un fichier HTML,**

 **Sauvegarder les données dans un fichier XML,**

 **Sauvegarder les données dans un fichier PDF.**

8.2. Configuration du Serveur Dr.Web



A chaque enregistrement des modifications de la section **Configuration du Serveur Dr.Web**, une copie de sauvegarde de la version précédente du fichier de configuration du Serveur est automatiquement enregistrée. 10 dernières copies sont sauvegardées.

Les copies de sauvegarde se trouvent dans le même répertoire où se trouve le fichier de configuration et elles portent les noms conformes au format suivant :

```
drwcsd.conf; <date_et_heure_de_creation>
```




Vous pouvez utiliser les copies de sauvegarde créées, notamment pour restaurer le fichier de configuration si l'interface du Centre de gestion n'est pas disponible.

Pour configurer les paramètres du Serveur Dr.Web :

1. Sélectionnez l'élément **Administration** du menu principal du Centre de gestion.
2. Dans la fenêtre qui s'affiche, sélectionnez l'élément **Configuration du Serveur Dr.Web** du menu de gestion. Une fenêtre permettant de configurer le Serveur va s'ouvrir.




Les valeurs des champs marqués du symbole *, doivent être obligatoirement spécifiées.

3. Les boutons suivants de gestion des paramètres sont disponibles dans la barre d'outils :
 -  **Redémarrer le Serveur Dr.Web** – redémarrer le Serveur pour appliquer les modifications apportées dans cette rubrique. Le bouton est activé après la modification des paramètres de la rubrique et l'appui sur le bouton **Sauvegarder**.
 -  **Restaurer la configuration de la copie de sauvegarde** – liste déroulante contenant les copies de sauvegarde des paramètres de la rubrique entière que l'on peut restaurer après les modifications apportées. Le bouton est activé après la modification des paramètres de la rubrique et l'appui sur le bouton **Sauvegarder**.
 -  **Restaurer tous les paramètres à leur valeur initiale** – restaurer les valeurs données à tous les paramètres de cette rubrique avant modification (dernières valeurs sauvegardées).



 **Restaurer tous les paramètres à leur valeur par défaut** – restaurer les valeurs par défaut de tous les paramètres de la rubrique.

4. Pour appliquer les paramètres apportées dans les paramètres de la rubrique, cliquez sur **Sauvegarder**. Ensuite, le redémarrage du Serveur est requis. Pour ce faire, cliquez sur le bouton  **Redémarrer le Serveur Dr.Web** dans la barre d'outils de cette rubrique.

8.2.1. Général

Dans l'onglet **Général**, vous pouvez configurer les paramètres suivants du Serveur :

- **Nom du Serveur Dr.Web** – nom de ce Serveur. Si aucun nom n'est spécifié, le nom du poste sur lequel est installé le Serveur Dr.Web est utilisé.
- **Langue du Serveur** – langue utilisée par défaut par les composants et les systèmes du Serveur Dr.Web, si les paramètres de langue n'ont pas été reçus depuis la base de données du Serveur. Notamment, elle est utilisée pour le Centre de gestion de la sécurité Dr.Web et le système de notifications de l'administrateur si la base de données a été endommagée et il est impossible d'obtenir les paramètres de la langue.
- **Nombre de requêtes parallèles de clients** – nombre de requêtes pour le traitement des données issues des clients : Agents, installateurs des Agents, Serveurs voisins. Ce paramètre affecte les performances du Serveur. Il est recommandé de ne pas modifier la valeur spécifiée par défaut sans avoir consulté le support technique.
- **Nombre de connexions à la BD** – 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.



A partir de la version 10, la modification du paramètre **File de l'authentification** via le Centre de gestion n'est plus disponible.

Par défaut, la valeur de ce paramètre spécifiée lors de l'installation d'un nouveau Serveur est de 50. En cas de la mise à niveau de la version antérieure avec la sauvegarde du fichier de configuration, la valeur de la file de l'authentification est sauvegardée de la configuration de la version antérieure.

S'il est nécessaire de modifier la longueur de la file de l'authentification éditez la valeur du paramètre suivant dans le fichier de configuration du Serveur :

```
<!-- Maximum authorization queue length -->  
<maximum-authorization-queue size='50' />
```

- Cochez la case **Limiter le trafic des mises à jour** pour limiter l'utilisation de la bande passante lors de la transmission des mises à jour du Serveur aux Agents.

Si la case est cochée, dans le champ **Vitesse maximale du transfert (Ko/s)**, indiquez la vitesse maximale du transfert des mises à jour. Les mises à jour seront transmises par tranches de bande passante allouée au trafic réseau total relatif aux mises à jour de tous les Agents.

Si la case n'est pas cochée, les mises à jour des Agents seront transmises sans aucune limitation de la bande passante.

- Dans la liste déroulante **Mode d'enregistrement des novices**, sélectionnez le mode d'enregistrement des nouveaux postes (voir [Politique d'approbation des postes](#)).



- La liste déroulante **Groupe primaire par défaut**, détermine le groupe primaire dans lequel les postes seront placés lorsque l'accès des postes au Serveur est autorisé automatiquement.
- Cochez la case **Redéfinir les non approuvés comme novices** pour réinitialiser les paramètres d'accès au Serveur pour les postes qui n'ont pas correctement passé l'authentification. Cette option peut être utile si vous modifiez les paramètres du Serveur (comme la clé publique) ou que vous modifiez la BD. Dans ces cas, les postes ne seront pas en mesure de se connecter et auront besoin des nouveaux paramètres pour accéder au Serveur.
- Dans la liste déroulante **Chiffrement**, choisissez la politique de chiffrement du trafic entre le Serveur Dr.Web et les clients connectés : les Agents, les Serveurs voisins et les Installateurs réseau.
Pour en savoir plus sur ces paramètres, voir le p. [Utilisation du chiffrement et de la compression du trafic](#).
- Dans la liste déroulante **Chiffrement**, choisissez le mode de compression du trafic entre le Serveur Dr.Web et les clients connectés : les Agents, les Serveurs voisins et les Installateurs réseau. Pour en savoir plus sur ces paramètres, voir le p. [Utilisation du chiffrement et de la compression du trafic](#).
 - Lorsque vous choisissez **Oui** ou **Possible** pour la compression du trafic, la liste déroulante **Niveau de compression** est disponible. Dans cette liste, vous pouvez indiquer le niveau de compression des données de 1 à 9, où 1 est le niveau minimum et 9 le niveau maximum de compression.
- Dans le champ **Différence autorisée entre l'heure du Serveur et de l'Agent**, indiquez la différence autorisée entre l'heure système sur le Serveur Dr.Web et les Agents Dr.Web en minutes. Si la différence est supérieure à la valeur indiquée, ce sera noté dans le statut du poste sur le Serveur Dr.Web. 3 minutes sont autorisées par défaut. La valeur 0 indique que la vérification est désactivée.
- Cochez la case **Remplacer les adresses IP** pour remplacer les adresses IP par les noms DNS dans le fichier de journal du Serveur Dr.Web.
- Cochez la case **Remplacer les noms NetBIOS** pour afficher les noms DNS au lieu des noms NetBios dans le répertoire du réseau antivirus du Centre de gestion (lorsque les noms d'hôte ne peuvent être détectés, les adresses IP s'affichent).



Les deux cases **Remplacer les adresses IP** 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.

- Cochez la case **Synchroniser les descriptions des postes** pour synchroniser la description de l'ordinateur de l'utilisateur avec celle du poste dans le Centre de gestion (Champ Description de l'ordinateur à la page des Propriétés système). Si la description du poste n'est pas présent



dans le Centre de gestion, c'est la description de l'ordinateur du côté de l'utilisateur qui sera inscrite dans ce champ. Si les descriptions sont différentes, celles du Centre de gestion seront remplacées par les descriptions utilisateur.

- Cochez la case **Suivre les épidémies** pour activer le mode de notification de l'administrateur en cas d'épidémie virale. Si la case n'est pas cochée, les notifications sur les infections virales sont effectuées en mode standard. Si la case est cochée, vous pouvez configurer les paramètres suivants sur le tracking des épidémies :
 - **Délai (s)** – délai, en secondes, pendant lequel un certain nombre de messages sur les infections doivent être réceptionnés afin que le Serveur Dr.Web puisse envoyer une seule notification d'épidémie à l'administrateur pour tous les cas d'infection.
 - **Nombre de messages** – nombre de messages sur les infections qui doivent être réceptionnés pendant un délai spécifié, afin que le Serveur Dr.Web puisse envoyer une seule notification d'épidémie à l'administrateur pour tous les cas d'infection.
- Cochez la case **Synchroniser la géolocalisation** pour permettre la synchronisation de la géolocalisation des postes entre les Serveurs Dr.Web dans le réseau antivirus multi-serveurs. Si la case est cochée, vous pouvez configurer le paramètre suivant :
 - **Synchronisation au démarrage** – nombre de postes sans coordonnées géographiques, les informations sur lesquels sont requis lors de l'établissement d'une connexion entre les Serveurs Dr.Web.

8.2.1.1. Utilisation du chiffrement et de la compression du trafic

Le réseau antivirus Dr.Web Enterprise Security Suite permet de chiffrer le trafic entre le Serveur et les postes de travail (les Agents Dr.Web), entre les Serveurs Dr.Web (en cas de configuration réseau multi-serveurs), ainsi qu'entre le Serveur et les Installateurs 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 lors de l'interaction des composants.

Le réseau antivirus Dr.Web Enterprise Security Suite utilise des dispositifs de cryptage et de signature numérique fiables, basés sur le concept de paires de clés publique/privée.

La politique de chiffrement peut être configurée séparément sur chaque composant du réseau antivirus, la configuration d'autres composants doit être conforme à celle du Serveur.

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 analogues aux paramètres relatifs au chiffrement.



Quand vous configurez le chiffrement et la compression du côté du Serveur, prenez en compte les particularités de clients que vous projetez de connecter à ce Serveur. Pas tous les clients supportent le chiffrement et la compression du trafic (par exemple, l'Antivirus pour Android et l'Antivirus Dr.Web pour OS X ne supportent ni chiffrement, ni compression). La connexion au Serveur pour ces clients est impossible si la valeur **Oui** est spécifiée pour le chiffrement et/ou la compression du côté du Serveur.



Marche à suivre pour configurer les politiques de compression et de chiffrement pour le Serveur Dr.Web :

1. Sélectionnez l'élément **Administration** du menu principal du Centre de gestion.
2. Dans la fenêtre qui s'affiche sélectionnez l'élément du menu de gestion **Configuration de Serveur Dr.Web**.
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 paramètres 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 et de compression sur le Serveur et sur un autre composant (Agent ou Installateur réseau) il est à noter qu'il existe des paramètres incompatibles dont la sélection entraîne l'échec de connexion entre le Serveur et le composant concerné.

Le tableau [8-1](#) comprend les combinaisons des paramètres qui assurent (+) ou n'assurent pas (–) le chiffrement et la compression de la connexion entre le Serveur et le composant, ainsi que les combinaisons inappropriées (**Erreur**).

Tableau 8-1. Compatibilité des paramètres relatifs aux politiques de chiffrement et de compression

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).



Pour désactiver le mode de chiffrement, 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 et Agent-Serveur. Le non respect de cette règle peut entraîner la perte de contrôle du composant et une nécessité de le réinstaller.

L'utilisation de la compression diminue le trafic mais augmente considérablement la charge sur les ordinateurs, beaucoup plus que le chiffrement.



La valeur **Possible** spécifiée du côté de l'Agent Dr.Web signifie que le chiffrement/compression s'effectuera par défaut et ne peut pas être désactivé par la modification des paramètres du Serveur Dr.Web sans modifier les paramètres du côté de l'Agent.

8.2.2. Réseau

8.2.2.1. DNS

Dans l'onglet **DNS**, vous pouvez configurer les paramètres suivants d'utilisation du serveur DNS :

- **Délai des requêtes DNS (s)** - délai, en secondes, pour répondre aux requêtes DNS directes/inverses. Indiquez la valeur 0 pour désactiver la restriction sur le temps d'attente de la résolution de la requête DNS.
- **Nombre de requêtes DNS répétées** - nombre maximum de requêtes DNS répétées en cas d'échec durant la résolution de la requête DNS.
- Cochez la case **Indiquer la durée de stockage des réponses du serveur DNS** pour indiquer la durée de stockage des réponses du serveur DNS dans le cache (TTL).
 - **Pour les réponses positives (min)** - la durée de stockage dans le cache (TTL) des réponses positives du serveur DNS en minutes.
 - **Pour les réponses négatives (min)** - la durée de stockage dans le cache (TTL) des réponses négatives du serveur DNS en minutes.
- **Serveurs DNS** - liste des serveurs DNS, qui remplacent la liste système par défaut.
- **Domaines DNS** - liste des domaines DNS, qui remplacent la liste système par défaut.

8.2.2.2. Proxy

Dans l'onglet **Proxy**, vous pouvez configurer les paramètres du serveur proxy.

Cochez la case **Utiliser le serveur proxy** pour paramétrer les connexions avec le Serveur Dr.Web via le serveur proxy. Les paramètres suivants sont disponibles :

- **Serveur proxy** - adresse IP ou nom DNS du serveur proxy.
- Pour utiliser l'authentification pour l'accès au serveur proxy, selon les méthodes choisies, cochez la case **Utiliser l'authentification** et indiquez les paramètres suivants :



- Remplissez les champs **Utilisateur du serveur proxy** et **Mot de passe de l'utilisateur du serveur proxy**.
- Choisissez une des méthodes d'authentification suivantes :

Option	Description
Toute méthode supportée	Utilisez n'importe quelle méthode d'authentification supportée par le serveur proxy. Si le serveur proxy supporte plusieurs méthodes, la méthode la plus fiable est utilisée.
Toute méthode sécurisée supportée	Utilisez n'importe quelle méthode d'authentification sécurisée supportée par le serveur proxy. Dans ce mode, la méthode d'authentification Standard n'est pas supportée. Si le serveur proxy supporte plusieurs méthodes d'authentification, la plus sûre est utilisée.
Les méthodes suivantes :	Authentification Basic Utiliser l'authentification Basic. Il n'est pas recommandé d'utiliser cette méthode car le transfert des données d'authentification n'est pas crypté.
	Authentification Digest Utiliser l'authentification Digest. Méthode d'authentification cryptographique.
	Authentification NTLM Utiliser l'authentification NTLM. Méthode d'authentification cryptographique. Le protocole NTLM de Microsoft est utilisé pour l'authentification.
	Authentification GSS-Negotiate Utiliser l'authentification GSS-Negotiate. Méthode d'authentification cryptographique.

8.2.2.3. Transport

L'onglet **Transport** permet de configurer les protocoles de transport utilisés par le Serveur pour se connecter aux clients.

Dans la sous-rubrique **TCP/IP** sont configurés les paramètres de connexion au Serveur via les protocoles TCP/IP :

- **Adresse** et **Port** – l'adresse IP correspondante et le numéro du port de l'interface réseau à laquelle ce protocole de transport est lié. Le Serveur écoute l'interface avec les paramètres configurés pour communiquer avec les Agents installés sur les postes de travail.
- **Nom** – nom du Serveur Dr.Web. Si aucun nom n'est indiqué, le nom indiqué à l'onglet **Général** est utilisé (voir ci-dessus, si aucun nom n'est indiqué dans cet onglet, le nom de l'ordinateur est utilisé). Si un autre nom est indiqué pour le protocole que le nom spécifié dans l'onglet **Général**, le nom inscrit dans la description du protocole est utilisé. Ce nom est utilisé par le service de détection du Serveur par les Agents etc.
- Cochez la case **Détecter** pour activer le service de détection du Serveur.
- Cochez la case **Multicast** pour utiliser le mode *Multicast over UDP* pour la détection du Serveur.



- **Groupe multicast** – adresse IP du groupe multicast dans lequel le Serveur est enregistré. Il est utilisé pour la communication avec des Agents et des Installateurs réseau lors de la recherche des Serveurs Dr.Web actifs dans le réseau. Si le champ n'est pas rempli, le groupe 231.0.0.1 est utilisé par défaut.
- Uniquement sous les OS de la famille UNIX : dans le champ **Chemin** indiquez le chemin vers le socket de communication, par exemple, de la communication avec l'Agent.



Pour en savoir plus, voir la rubrique [Configuration des connexions réseau](#).

Les paramètres ci-dessus doivent être spécifiés au format d'adresse réseau décrite dans les **Annexes**, p. [Annexe E. Spécification de l'adresse réseau](#).

8.2.2.4. Cluster

Dans l'onglet **Cluster**, vous pouvez configurer les paramètres du cluster des Serveurs Dr.Web pour l'échange de données en cas de configuration du réseau antivirus multi-serveurs.

Pour utiliser le cluster, indiquez les paramètres suivants :

- **Groupe multicast** - adresse IP du groupe multicast via lequel les Serveurs vont échanger des informations.
- **Port** - numéro de port de l'interface réseau à laquelle le protocole de transport est lié pour transmettre des informations au groupe multicast.
- **Interface** - adresse IP de l'interface réseau à laquelle le protocole de transport est lié pour transmettre des informations au groupe multicast.



Vous pouvez consulter les particularités de la création du cluster des Serveurs Dr.Web dans la rubrique [Cluster des Serveurs Dr.Web](#).

8.2.2.5. Téléchargement

Dans l'onglet **Télécharger**, vous pouvez configurer les paramètres du Serveur utilisés pour générer les fichiers d'installation de l'Agent sur les postes du réseau antivirus. Ensuite, ces paramètres sont utilisés pour connecter l'installateur de l'Agent au Serveur :

- **Adresse du Serveur Dr.Web** - adresse IP ou nom DNS du Serveur Dr.Web.
Si l'adresse du Serveur n'est pas indiquée, le nom de l'ordinateur donné par le système d'exploitation est utilisé.
- **Port** - numéro du port utilisé lors de la connexion de l'installateur de l'Agent au Serveur.
Si le numéro de port n'est pas indiqué, le port 2193 est utilisé (ceci est configuré dans le Centre de gestion, dans la rubrique **Administration** → **Configuration du Serveur Dr.Web** → l'onglet **Réseau** → l'onglet **Transport**).

Les paramètres de la rubrique **Télécharger** sont sauvegardés dans le fichier de configuration `download.conf` (voir les **Annexes**, p. [G3. Fichier de Configuration download.conf](#)).



8.2.2.6. Mises à jour de groupes

Dans l'onglet **Mises à jour Multicast**, vous pouvez configurer la transmission des mises à jour aux postes de travail via le protocole multicast.

Cochez la case **Activer les mises à jour multicast** pour permettre la transmission des mises à jour aux postes via le protocole multicast, ainsi :

- Si les mises à jour de groupes sont désactivées, la mise à jour de tous les postes est effectuée uniquement en mode général – via le protocole TCP.
- Si les mises à jour de groupes sont activées, pour tous les postes connectés à un Serveur de mise à jour, la mise à jour s'effectue en deux étapes :
 1. Mise à jour via le protocole multicast.
 2. Mise à jour standard via le protocole TCP.

Pour paramétrer les mises à jour multicast, utilisez les paramètres suivants :

- **Taille du datagramme UDP (octets)** – taille des datagrammes UDP utilisés par le protocole multicast, en octets.

L'intervalle autorisé est 512 – 8192. Pour éviter la fragmentation, il est recommandé d'indiquer une valeur inférieure au MTU (Maximum Transmission Unit) du réseau utilisé.
- **Délai de transmission du fichier (ms)** – durant cet intervalle de temps, le fichier de mise à jour unique est transmis, après quoi le Serveur commence à envoyer le fichier suivant.

Tous les fichiers qui n'ont pu être transmis à l'étape de la mise à jour via le protocole multicast seront transmis lors du processus standard de mise à jour via le protocole TCP.
- **Durée des mises à jour multicast (ms)** – durée du processus de mise à jour via le protocole multicast.

Tous les fichiers qui n'ont pu être transmis à l'étape de la mise à jour via le protocole multicast seront transmis lors du processus standard de mise à jour via le protocole TCP.
- **Intervalle de transmission des packages (ms)** – intervalle de transmission des packages à un groupe multicast.

Un intervalle faible peut provoquer des pertes significatives durant le transfert des packages et une surcharge du réseau. Il est recommandé de modifier ce paramètre.
- **Intervalle entre les requêtes de retransmission (ms)** – dans cet intervalle, les Agents envoient des requêtes de retransmission des packages perdus.

Le Serveur Dr.Web accumule ces requêtes puis renvoie les blocs perdus.
- **Intervalle de "Silence" sur la ligne (ms)** – lorsqu'une transmission d'un fichier est terminée avant que la durée allouée ait expiré, si, durant l'intervalle de "silence" indiqué, aucune requête n'est envoyée par l'Agent pour la retransmission de packages perdus, le Serveur Dr.Web considère que tous les Agents ont reçu les fichiers de mise à jour et commence à envoyer le fichier suivant.
- **Intervalle d'accumulation des requêtes de retransmission (ms)** – durant cet intervalle, le Serveur accumule les requêtes des Agents pour la retransmission des packages perdus.



Les Agents redemandent les packages perdus. Le Serveur accumule ces requêtes durant un délai de temps spécifié, après quoi il envoie les blocs perdus.

Pour indiquer la liste des groupes multicast depuis lesquels les mises à jour multicast sont disponibles, configurez les paramètres suivants dans la sous-rubrique **Groupes multicast** :

- **Groupe multicast** – adresse IP du groupe multicast via lequel les postes recevront des mises à jour multicast.
- **Port** – numéro de port de l'interface réseau du Serveur Dr.Web à laquelle le protocole multicast de transport est lié pour transmettre des mises à jour.



Pour les mises à jour multicast, il faut spécifier n'importe quel port libre, autre que le port spécifié dans les paramètres pour le fonctionnement du protocole de transport du Serveur.

- **Interface** – adresse IP de l'interface réseau du Serveur Dr.Web à laquelle le protocole multicast de transport est lié pour transmettre des mises à jour.

Chaque ligne contient la configuration d'un groupe multicast. Pour ajouter un groupe multicast supplémentaire, cliquez sur .

En cas de sélection de plusieurs groupes multicast, prenez en compte les particularités suivantes :

- Pour les Serveurs Dr.Web différents qui diffuseront les mises à jour multicast, il faut spécifier les groupes multicast différents.
- Pour les Serveurs Dr.Web différents qui diffuseront les mises à jour multicast, il faut spécifier les paramètres différents **Interface** et **Port**.
- En cas d'utilisation de plusieurs groupes multicast, les ensembles des postes inclus dans ces groupes ne doivent pas se croiser. Ainsi, chaque poste du réseau antivirus peut entrer dans un seul groupe multicast.

8.2.3. Statistiques

L'onglet **Statistiques** permet de spécifier les informations statistiques à écrire dans le journal du protocole ainsi que dans la base de données du Serveur.

Pour enregistrer et ajouter des informations dans une BD correspondante, cochez les cases suivantes :

- **Statut de la quarantaine** - permet de surveiller le statut de la Quarantaine sur les postes et d'enregistrer les informations dans la base de données.
- **Composition de matériel et de logiciels** - permet de surveiller la composition de matériel et de logiciels sur les postes et d'enregistrer les informations dans la base de données.
- **Liste des modules de postes** - permet de surveiller la liste des modules de l'Antivirus et d'enregistrer les informations dans la base de données.
- **Liste des composants installés** - permet de surveiller la liste des composants de l'Antivirus (Scanner, moniteurs etc.) installés sur le poste et d'enregistrer les informations dans la base de données.



- **Sessions des utilisateurs des postes** - permet de surveiller les des sessions utilisateur sur le poste et la sauvegarde des logins des utilisateurs connectés au système avec un Agent installé, dans la base de données.
- **Démarrage/arrêt des composants** - permet de surveiller les informations sur le lancement et l'arrêt des composants de l'Antivirus (Scanner, moniteurs etc.) et d'enregistrer les informations dans la base de données.
- **Menaces de sécurité détectées** - permet de surveiller les menaces détectées sur les postes et d'enregistrer les informations dans la base de données.

Si la case **Menaces de sécurité détectées** est cochée, vous pouvez également configurer les paramètres supplémentaires des statistiques sur les menaces.

Cochez la case Envoyer des statistiques à Doctor Web pour activer l'envoi des statistiques sur les menaces détectées à Doctor Web. Les champs suivants seront disponibles :

- **Intervalle** - intervalle, en minutes, pour l'envoi des statistiques ;
- **Identificateur** - une clé MD5 (située dans le fichier de configuration du Serveur).

Le champ **Intervalle** de l'envoi des statistiques est le seul champ obligatoire.

- **Erreurs de scan** - permet de surveiller les erreurs de scan sur les postes et d'enregistrer les informations dans la base de données.
- **Statistiques de scan** - permet de surveiller les statistiques de scan et d'enregistrer les informations dans la base de données.
- **Installations des Agents** - permet de surveiller les informations sur les installations des Agents sur les postes et d'enregistrer les informations dans la base de données.
- **Journal d'exécution des tâches sur les postes** - permet de surveiller les résultats de l'exécution des tâches sur les postes et d'enregistrer les informations dans la base de données.
- **Surveillance des statuts des postes** - permet de surveiller les modifications intervenues sur les postes et d'enregistrer les informations dans la base de données.
 - **Statut des bases virales** - permet de surveiller les modifications du statut et du contenu des bases virales sur le poste et d'enregistrer les informations dans la base de données. La case est disponible seulement si la case **Statut du poste** est cochée.

Pour consulter les informations statistiques :

1. Sélectionnez l'élément **Réseau antivirus** du menu principal.
2. Sélectionnez un poste ou un groupe dans la liste hiérarchique.
3. Ouvrez la rubrique correspondante du menu de gestion (voir le tableau ci-dessous).



Pour en savoir plus sur les données statistiques, voir la rubrique [Consulter les statistiques du poste](#).

Le tableau ci-dessous présente la correspondance entre les cases de la rubrique **Statistiques** dans les paramètres du Serveur et les éléments du menu de gestion sur la page **Réseau anti-virus**.



Si les cases de l'onglet **Statistiques** sont décochées, les éléments correspondants seront masqués dans le menu de gestion.

Tableau 8-2. Correspondance entre les paramètres du Serveur et les éléments du menu de gestion

Paramètres du Serveur	Éléments du menu
Statut de la quarantaine	Général → Quarantaine Configuration → Windows → Agent Dr.Web → case Autoriser la gestion de la Quarantaine à distance
Composition de matériel et de logiciels	Général → Composition de matériel et de logiciels Général → Comparaison de matériel et de logiciels
Liste des modules du poste	Statistiques → Modules
Listes des composants installés	Général → Composants installés
Sessions des utilisateurs des postes	Général → Sessions utilisateurs
Démarrage/arrêt des composants	Statistiques → Démarrage/Arrêt
Menaces de sécurité détectées	Statistiques → Menaces Statistiques → Statistiques des menaces
Erreurs de scan	Statistiques → Erreurs
Statistiques de scan	Statistiques → Statistiques de scan Tableaux → Statistiques sommaires
Installations des Agents	Statistiques → Installations des Agents
Journal de l'exécution des tâches sur les postes	Statistiques → Tâches Statistiques → Bases virales
Statuts des postes	Statistiques → Statut Statistiques → Bases virales
Statut des bases virales	Statistiques → Bases virales



8.2.4. Sécurité

L'onglet **Sécurité** permet de spécifier des limitations pour les adresses réseau depuis lesquelles les Agents, les installateurs réseau et d'autres Serveurs Dr.Web (voisins) pourront accéder au Serveur spécifié.

Les cases ci-dessous permettent de gérer le journal d'audit du Serveur :

- **Audit des opérations de l'administrateur** 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 Dr.Web ainsi que l'écriture du journal dans la BD.
- **Audit des opérations de l'API Web** permet l'écriture des opérations effectuées via l'API XML 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 permettant de configurer des limitations pour les types correspondants de connexions :

- **Agents** – listes de restrictions des adresses IP depuis lesquelles les Agents Dr.Web peuvent se connecter à ce Serveur.
- **Installateurs** – listes de restrictions des adresses IP depuis lesquelles les installateurs des Agents Dr.Web peuvent se connecter à ce Serveur.
- **Voisins** – listes de restrictions des adresses IP depuis lesquelles les Serveurs voisins Dr.Web peuvent se connecter à ce Serveur.
- **Service de détection** – liste de restrictions des adresses IP depuis lesquelles les requêtes de recherche broadcast sont reçues par le [service de détection du Serveur](#).



Pour configurer les limitations d'accès pour tout type de connexion :

1. Ouvrez l'onglet correspondant (**Agents**, **Installations**, **Voisins** ou **Service de détection**).
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 déterminée, ajoutez l'adresse 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 nouveau 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 d'hôtes dans les réseaux de ce type ont le format suivant : 125.*.*.*

Les adresses non mentionnées dans aucune des listes sont autorisées ou interdites en fonction du statut de la case **Priorité de refus** : si la case est cochée, la liste **Refuser** possède une priorité plus importante que la liste **Autoriser**. Les adresses qui ne sont incluses à aucune liste ou incluses aux deux listes sont refusées. Seules les adresses appartenant à la liste **Autoriser** et non incluses à la liste **Refuser** seront autorisées.

8.2.5. Cache

Dans l'onglet **Cache**, vous pouvez configurer les paramètres suivants de nettoyage du cache :

- **Période de vidage du cache** - période du vidage complet du cache.
- **Fichiers de quarantaine** - périodicité de suppression des fichiers de quarantaine du côté du Serveur.
- **Fichiers du dépôt** - périodicité de suppression des fichiers dans le dépôt.
- **Packages d'installation** – périodicité de suppression des packages d'installation personnels.



Lors de l'indication des valeurs numériques, vous pouvez utiliser les listes déroulantes d'unités de mesure de périodicité.

8.2.6. Base de données

Dans l'onglet **Base de données**, vous pouvez configurer le SGBD requis pour le fonctionnement du Serveur Dr.Web.



La structure de la BD du Serveur Dr.Web peut être obtenue à l'aide du script `sql_init.sql` se trouvant dans le sous-répertoire `etc` du répertoire d'installation du Serveur Dr.Web.

1. Dans la liste déroulante **Base de données**, choisissez le type de la BD :

- **IntDB** – BD intégrée SQLite2 (un composant du Serveur Dr.Web),
- **ODBC** – pour utiliser une BD externe via la connexion ODBC,



Si un avertissement ou une erreur survient lors du travail du Serveur Dr.Web avec SGBD Microsoft SQL Server via ODBC, il faut s'assurer que vous utilisez la dernière version disponible de SGBD de cette rédaction.

Pour savoir comment vous pouvez vérifier la disponibilité des corrections, consultez la page suivante de Microsoft : <https://support.microsoft.com/en-us/kb/321185>.

- **Oracle** – BD externe pour toutes les plateformes sauf FreeBSD,



Si un SGBD externe **Oracle** est utilisé via une connexion ODBC, il est nécessaire d'installer la dernière version du pilote ODBC fourni avec ce SGBD. Il est fortement recommandé de ne pas utiliser le pilote ODBC Oracle fourni par Microsoft.

- **PostgreSQL** – BD externe,
- **SQLite3** – BD intégrée (un composant du Serveur Dr.Web). Option recommandée lors de l'utilisation d'une BD intégrée.

2. Configurez les paramètres requis pour le fonctionnement de la BD :

- Pour une BD interne, si nécessaire, indiquez le chemin complet vers le fichier de la base de données dans le champ **Nom du fichier** et spécifiez la taille du cache et le mode d'enregistrement des données.
- Les paramètres d'une BD externe sont décrits en détail dans les **Annexes**, dans l'[Annexe B. Description des paramètres du SGBD. Paramètres des pilotes du SGBD](#).

3. Cliquez sur **Enregistrer** pour appliquer les modifications.



Le kit de distribution du Serveur Dr.Web contient des clients intégrés pour les SGBD supportés, veuillez donc noter :

- Si vous prévoyez d'utiliser des clients SGBD intégrés qui sont fournis avec le Serveur Dr.Web, durant l'installation (mise à niveau) du Serveur, dans les paramètres de l'installateur, sélectionnez l'installation Personnalisée et dans la fenêtre suivante, vérifiez que l'installation du client correspondant pour le SGBD intégré est activée dans la rubrique **Support des Bases de données**.
- Si vous pensez vous connecter aux bases de données externes via ODBC, durant l'installation (mise à niveau) du Serveur, dans les paramètres de l'installateur, sélectionnez l'installation Personnalisée et dans la fenêtre suivante, désactivez l'installation du client intégré correspondant à la rubrique **Support des Bases de données**. Sinon, l'interaction avec la BD via ODBC sera impossible à cause du conflit des bibliothèques.



L'installateur du Serveur supporte la modification du produit. Pour ajouter ou supprimer des composants séparés, par exemple les pilotes de configuration de la base de données, il est nécessaire de lancer l'installateur du Serveur et de choisir **Modifier**.

L'utilisation d'un SGBD interne est spécifiée par défaut. Ce mode accroît beaucoup la charge sur le Serveur. Il est recommandé d'utiliser un SGBD externe dans les grands réseaux antivirus. La procédure de changement du type de SGBD est décrit dans les **Annexes**, la rubrique [Changement du type de SGBD Dr.Web Enterprise Security Suite](#).



La base de données intégrée peut être utilisée lorsque le nombre de postes connectés au Serveur ne dépasse pas 200-300. Si l'ordinateur sur lequel est installé le Serveur Dr.Web 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 respecter les pré-requis minimum suivants :

- processeur 3GHz,
- mémoire vive – au moins 4 Go pour le Serveur Dr.Web, au moins 8 Go pour le Serveur de BD,
- OS de la famille UNIX.



Il est possible de nettoyer la base de données utilisée par le Serveur Dr.Web, notamment supprimer des enregistrements d'événements et de données sur les postes qui n'ont pas visité le Serveur depuis un certain temps. Pour nettoyer la base de données, ouvrez la rubrique de la [planification du Serveur](#) et créez la tâche correspondante.

8.2.7. Modules

Dans l'onglet **Modules**, vous pouvez configurer le mode d'interaction du Serveur Dr.Web avec d'autres composants de Dr.Web Enterprise Security Suite :

- Cochez la case **Extension pour le Centre de gestion de la sécurité Dr.Web** pour pouvoir utiliser l'extension pour le Centre de gestion de la sécurité Dr.Web pour la gestion du Serveur et du réseau antivirus via le Centre de gestion.



Si vous décochez la case **Extension pour le Centre de gestion de la sécurité Dr.Web**, le Centre de gestion de la sécurité Dr.Web ne sera pas disponible après le redémarrage du Serveur Dr.Web. Dans ce cas, vous pourrez gérer le Serveur et le réseau antivirus uniquement via l'utilitaire de diagnostic distant, si la case **Extension Dr.Web Server FrontDoor** est cochée.

- Cochez la case du **Extension Dr.Web Server FrontDoor** pour utiliser l'Extension Dr.Web Server FrontDoor qui autorise la connexion de l'utilitaire de diagnostic distant du Serveur (voir aussi le p. [Accès distant au Serveur Dr.Web](#)).



- Cochez la case **Protocole de l'Agent Dr.Web** pour activer le protocole qui permet l'interaction du Serveur avec les Agents Dr.Web.
- Cochez la case du **Protocole Microsoft NAP Health Validator** pour activer le protocole qui permet l'interaction du Serveur avec le composant de vérification de l'état de santé du système NAP Validator de Microsoft.
- Cochez la case **Protocole de l'installateur de l'Agent Dr.Web** pour activer le protocole qui permet l'interaction du Serveur avec les installateurs des Agents Dr.Web.
- Cochez la case **Protocole du cluster des Serveurs Dr.Web** pour activer le protocole permettant l'interaction entre les Serveurs dans le système de cluster.
- Cochez la case **Protocole du Serveur Dr.Web** pour activer le protocole qui permet l'interaction d'un Serveur Dr.Web avec d'autres Serveurs Dr.Web. Le protocole est désactivé par défaut. Si vous utilisez une configuration réseau multi-serveurs (voir [Particularités du réseau avec plusieurs Serveurs Dr.Web](#)), cochez la case **Protocole du Serveur Dr.Web** pour l'activer.

8.2.8. Localisation

L'onglet **Localisation** vous permet de consulter des informations supplémentaires sur l'emplacement de l'ordinateur sur lequel le logiciel du Serveur Dr.Web est installé.

Dans cet onglet, vous pouvez également voir la localisation du Serveur sur une carte.

Pour voir la localisation du Serveur sur une carte :

1. Dans les champs **Latitude** et **Longitude**, indiquez les coordonnées géographiques du Serveur au format Degrés Décimaux.
2. Cliquez sur **Sauvegarder** pour conserver ces données dans le fichier de configuration du Serveur.

Pour consulter la carte, vous n'avez pas besoin de redémarrer le Serveur. Mais pour appliquer des changements dans les coordonnées géographiques, vous devez le redémarrer.

3. Dans l'onglet **Localisation**, la visualisation OpenStreetMaps va s'ouvrir et les coordonnées indiquées seront marquées.

Si l'outil de visualisation ne peut être chargé, le texte **Afficher sur la carte** apparaîtra.

4. Pour consulter la carte au plus grand format, cliquez sur l'outil de visualisation ou sur le texte **Afficher sur la carte**.

8.2.9. Licences

Dans l'onglet **Licences** sont spécifiés les paramètres de la diffusion des licences entre les Serveurs Dr.Web :

- **Délai de validité des licences délivrées** – délai pour lequel les licences sont délivrées depuis la clé sur ce Serveur. La configuration est utilisée si ce Serveur délivre les licences aux Serveurs voisins.



- **Période pour le renouvellement des licences obtenues** – période jusqu'à l'expiration de la licence. A commencer par cette période, ce Serveur démarre le renouvellement de la licence obtenue du Serveur voisin. La configuration est utilisée si le Serveur obtient des licences des Serveurs voisins.
- **Période de synchronisation de licences** – périodicité de synchronisation des informations sur les licences délivrées entre les Serveurs.



Pour plus d'information sur la distribution des licences entre les Serveurs, consultez la rubrique [Gestionnaire de Licences](#).

8.3. Accès distant au Serveur Dr.Web



Pour la connexion de l'utilitaire du diagnostic distant du Serveur, il est nécessaire d'activer l'extension Dr.Web Server FrontDoor. Pour ce faire cochez la case **Extension Dr.Web Server FrontDoor** dans l'onglet [Modules](#) de la rubrique **Configuration du Serveur Dr.Web**.


Pour la connexion de l'utilitaire du diagnostic distant du Serveur, il faut que l'administrateur qui se connecte via l'utilitaire possède le droit **Utilisation des fonctionnalités supplémentaires**. Sinon, l'accès au Serveur via l'utilitaire du diagnostic distant sera interdit.

Pour configurer les paramètres de connexion de l'utilitaire du diagnostic distant du Serveur :

1. Sélectionnez l'élément **Administration** du menu principal du Centre de gestion, et dans la fenêtre qui s'ouvre, sélectionnez l'élément du menu de gestion **Accès distant au Serveur Dr.Web**.
2. Spécifiez le protocole de connexion :
 - Cochez la case **Utiliser SSL** pour autoriser la connexion de l'utilitaire de diagnostic distant au Serveur Dr.Web via le protocole SSL. Si la case est décochée, la connexion sera possible uniquement via le protocole TCP.
Pour la connexion via le protocole SSL, spécifiez les paramètres suivants :
 - **Certificat SSL** – fichier du certificat SSL qui sera vérifié lors de la connexion. Dans la liste déroulante sont présentés les certificats disponibles du répertoire du Serveur.
 - **Clé privée SSL** – fichier de la clé privée SSL qui sera vérifiée lors de la connexion. Dans la liste déroulante sont présentées les clés privées disponibles du répertoire du Serveur.
3. Spécifiez les paramètres des noeuds de connexion :
 - **Adresse** – adresse de laquelle la connexion de l'utilitaire du diagnostic distant du Serveur est autorisée.
 - **Port** – port pour la connexion de l'utilitaire de diagnostics distants du Serveur. Le port 10101 est utilisé par défaut.

Pour ajouter encore une adresse autorisée, cliquez sur et spécifiez les valeurs des champs ajoutés.



Pour interdire la connexion depuis l'adresse ajoutée, supprimez cette adresse de la liste en cliquant sur  contre la ligne portant cette adresse.




4. Cliquez sur **Sauvegarder**.




L'utilisation de la version de console de l'utilitaire du diagnostic distant du Serveur est décrite en détails dans les **Annexes**, dans la rubrique [H10. Utilitaire du diagnostic distant du Serveur Dr.Web](#).





8.4. Configuration de la planification du Serveur Dr.Web

Pour configurer la planification du Serveur Dr.Web, effectuez les actions suivantes :

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion, dans la fenêtre qui s'affiche, sélectionnez l'élément du menu de gestion **Planification des tâches du Serveur Dr.Web**. La liste des tâches du Serveur va s'ouvrir.
2. Pour gérer la planification, utilisez les éléments correspondants dans la barre d'outils :
 - a) Les éléments généraux de la barre d'outils sont utilisés pour créer de nouvelles tâches et gérer la section de la planification dans son ensemble. Ces éléments sont toujours disponibles dans la barre d'outils :
 -  **Créer une tâche** – ajouter une nouvelle tâche. Cette action est décrite en détails ci-dessous, dans la sous-rubrique [Éditeur de tâches](#).
 -  **Exporter les paramètres de cette rubrique vers un fichier** – exporter la planification vers un fichier au format spécial.
 -  **Importer les paramètres de cette rubrique depuis un fichier** – importer la planification depuis un fichier au format spécial.
 - b) Pour gérer les tâches existantes, cochez les cases près des tâches souhaitées ou dans l'entête du tableau pour sélectionner toutes les tâches dans la liste. Les éléments de gestion des tâches sélectionnées deviennent disponibles dans la barre d'outils :

Configuration		Action
Statut	Autoriser l'exécution	Activer l'exécution des tâches sélectionnées selon leur planification, si elles étaient désactivées.
	Désactiver l'exécution	Désactiver l'exécution des tâches sélectionnées. Les tâches restent dans la liste mais ne seront pas exécutées.
 Vous pouvez spécifier le même paramètre dans l'éditeur de tâches dans l'onglet Général en cochant la case Autoriser l'exécution .		
Importance	Définir comme critique	Effectuer un lancement supplémentaire de la tâche, si l'exécution planifiée de cette tâche a été omise.




Configuration		Action
	Définir comme non critique	Exécute la tâche uniquement au moment où elle planifiée indépendamment du fait que le lancement de la tâche ait été omis ou pas.
 Vous pouvez spécifier le même paramètre dans l'éditeur de tâches dans l'onglet Général en cochant la case Tâche critique .		
 Dupliquer des paramètres		Permet de dupliquer des tâches sélectionnées dans la liste des planifications actuelles. Lorsque vous activez l'option Dupliquer des paramètres , les nouvelles tâches créées possèdent des paramètres identiques à ceux des tâches sélectionnées.
 Planifier à plusieurs reprises		Pour les tâches qui ne sont exécutées qu'une fois : exécuter la tâche de nouveau selon les horaires configurés (la modification de la répétition d'exécution d'une tâche est décrite ci-dessous, dans la rubrique Éditeur de tâches).
 Supprimer les tâches sélectionnée		Supprimer la tâche sélectionnée de la planification.


3. Pour modifier les paramètres des tâches, sélectionnez-les dans la liste. La fenêtre de l'**Éditeur de tâches**, décrit [ci-dessous](#), s'ouvre.
4. Après avoir modifié la planification, cliquez sur **Sauvegarder** pour appliquer les modifications.

Éditeur de Tâches

A l'aide de l'éditeur de tâches, vous pouvez configurer les paramètres pour :

1. Créer une nouvelle tâche.
Pour ce faire, cliquez sur  **Créer une tâche** dans la barre d'outils.
2. Modifier une tâche existante.
Pour cela, cliquez sur le nom de la tâche dans la liste.


La fenêtre de modification de la tâche s'ouvre. Les paramètres de modification d'une tâche sont identiques à ceux de création d'une nouvelle tâche.

 Les valeurs des champs marqués du symbole *, doivent être obligatoirement spécifiées.


Pour modifier les paramètres d'une tâche :

1. Dans l'onglet **Général**, vous pouvez configurer les paramètres suivants :
 - Dans le champ **Nom**, indiquez le nom de la tâche affichée dans la liste des planifications.
 - Cochez la case **Activer l'exécution** pour activer l'exécution d'une tâche. Si la case n'est pas cochée, la tâche reste dans la liste mais elle ne sera pas exécutée.




 Vous pouvez spécifier le même paramètre dans la fenêtre principale du Planificateur à l'aide de l'élément **Statut** dans la barre d'outils.


- Cochez la case **Tâche critique** pour effectuer un lancement supplémentaire de la tâche si l'exécution planifiée de cette tâche à l'heure prévue a été omise. Le Planificateur parcourt la liste des tâches à chaque minute et s'il détecte une tâche critique omise, il la lance. Si au moment de lancement, une tâche a été omise plusieurs fois, elle sera exécutée seulement une fois.

 Vous pouvez spécifier le même paramètre dans la fenêtre principale du Planificateur à l'aide de l'élément **Importance** dans la barre d'outils.

Dans l'onglet **Action**, dans la liste déroulante **Action**, sélectionnez le type de tâche et configurez les paramètres nécessaires à son exécution :

Type de tâche	Paramètres et description
Exécuter la procédure	<p>La tâche consiste à exécuter les procédures utilisateur (voir le p. Procédures utilisateur).</p> <p>Indiquez les paramètres suivants :</p> <ul style="list-style-type: none"> • Groupe de procédures – groupe de procédures utilisateur pour lequel la procédure sera effectuée. • Procédure – nom d'une procédure utilisateur concrète qui est incluse dans le groupe sélectionné dans la liste Groupe de procédures. • Cochez la case Exécuter pour tous les groupes de procédures pour exécuter la procédure utilisateur sélectionnée dans tous les groupes de procédures dans lesquels cette procédure est spécifiée. Dans ce cas, la procédure déterminée spécialement pour chaque groupe sera exécutée.
Exécution du script	<p>La tâche consiste à exécuter le script Lua indiqué dans le champ Script.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <p> L'exécution simultanée de plusieurs tâches de type Exécuter le script sur plusieurs Serveurs utilisant une seule base de données peut entraîner des erreurs.</p> </div> <p>Lors de l'exécution des scripts Lua, l'administrateur obtient l'accès à tout le système de fichiers à l'intérieur du répertoire du Serveur et aux certaines commandes sur l'ordinateur avec le Serveur installé.</p> <p>Pour interdire l'accès à la planification, désactivez le droit Éditer la planification du Serveur pour l'administrateur correspondant (voir le p. Administrateurs et groupes administrateur).</p>
Remplacer la clé de chiffrement	<p>La tâche consiste à remplacer périodiquement les clés de chiffrement suivantes :</p> <ul style="list-style-type: none"> • la clé privée <code>drwcsd.pri</code> sur le Serveur, • la clé publique <code>drwcsd.pub</code> sur les postes de travail.




Type de tâche	Paramètres et description
	<p>Sachant que les postes peuvent être éteints au moment du remplacement, la procédure est divisée en deux étapes. Vous devez créer deux tâches pour exécuter chacune de ces étapes, il est recommandé d'effectuer la seconde étape après la première, lorsque certains postes seront probablement connectés au Serveur.</p> <p>Lors de la création d'une tâche, choisissez l'étape de remplacement de clé appropriée dans la liste déroulante :</p> <ul style="list-style-type: none">• Ajouter une nouvelle clé – première étape de la procédure lorsque la nouvelle paire de clés de chiffrement inactive est créée. Les postes obtiennent la nouvelle clé publique à la connexion avec le Serveur.• Supprimer l'ancienne clé et passer à la nouvelle – la seconde étape qui informe les postes sur le passage aux nouvelles clés de chiffrement, suivi du remplacement des clés existantes par les nouvelles : les clés publiques sur les postes et la clé privée sur le Serveur. <p>Si pour une raison quelconque certains postes n'ont pas reçu la nouvelle clé publique, ils ne pourront pas se connecter au Serveur. Pour résoudre ce problème, les options suivantes sont disponibles :</p> <ul style="list-style-type: none">• Installer manuellement la nouvelle clé publique sur le poste (vous pouvez consulter la procédure de remplacement de la clé sur le poste dans les Annexes, la rubrique Connexion de l'Agent Dr.Web à un autre Serveur).• Autoriser les Agents à s'authentifier sur le Serveur avec une clé publique incorrecte (voir la rubrique Réseau dans les préférences de l'Agent).
Écrire dans le fichier de journal	<p>La tâche consiste à écrire dans le fichier de rapport du Serveur de la ligne spécifiée.</p> <p>Ligne – texte du message enregistré dans le fichier de rapport.</p>
Lancer un programme	<p>La tâche consiste à lancer un programme personnalisé.</p> <div style="background-color: #f0f0f0; padding: 5px;"><p> Les programmes lancés dans le cadre de cette tâche sont exécutés en tâche de fond.</p></div> <p>Indiquez les paramètres suivants :</p> <ul style="list-style-type: none">• Champ Chemin – nom complet (avec le chemin) du fichier exécutable du programme qui doit être lancé.• Dans le champ Arguments – paramètres de la ligne de commande pour le programme à lancer.• Cochez la case Attendre la fin du programme pour attendre la fin du programme lancé par cette tâche. Dans ce cas, le Serveur enregistre le lancement du programme, le code de retour et l'heure de la fin du programme. Si la case Attendre la fin du programme est décochée, la tâche est considérée comme achevée dès le lancement du programme et le Serveur n'enregistre que le lancement du programme.





Type de tâche	Paramètres et description
Rappel sur l'expiration de la licence	<p>La tâche consiste à générer des rappels sur l'expiration de la licence du produit Dr.Web.</p> <p>Vous devez indiquer la période précédant l'expiration de la licence à partir de laquelle les rappels seront générés.</p>
Mettre à jour le dépôt	<p>Les informations sur cette tâche sont disponibles dans la rubrique Mise à jour selon la planification.</p>
Arrêter le Serveur Dr.Web	<p>La tâche consiste à fermer le Serveur.</p> <p>Aucun paramètre supplémentaire n'est requis pour exécuter la tâche.</p>
Envoi du message sur le poste	<p>La tâche consiste à envoyer un message aux utilisateurs du poste ou du groupe de postes.</p> <p>Vous pouvez consulter les paramètres dans la rubrique Envoi de messages aux postes.</p>
Nettoyer la base de données	<p>La tâche consiste à recueillir et supprimer les enregistrements non utilisés dans la base de données du Serveur en utilisant la commande <code>VACUUM</code>.</p> <p>Aucun paramètre supplémentaire n'est requis pour exécuter la tâche.</p>
Supprimer les événements non envoyés	<p>La tâche consiste à supprimer les événements non envoyés de la base de données.</p> <p>Vous devez indiquer un délai de stockage des événements non envoyés après lequel ils seront supprimés.</p> <p>Cette tâche fait référence aux événements qu'un Serveur secondaire envoie à un Serveur principal. Si l'envoi d'un message échoue, il est déplacé vers la liste des messages non envoyés. Le Serveur secondaire continue ses tentatives d'envoi du message selon l'intervalle spécifié. Lorsque la tâche Supprimer les événements non envoyés est lancée, les événements seront supprimés si leur durée de stockage a été atteinte ou dépassée.</p>
Supprimer les enregistrements obsolètes	<p>La tâche consiste à supprimer les informations obsolètes sur les postes de la base de données.</p> <p>Vous devez indiquer le nombre de jours après lequel les enregistrements statistiques sur les postes (mais pas les postes eux-mêmes) sont considérés comme obsolètes et supprimés du Serveur.</p> <p>Le délai après lequel les enregistrements statistiques sont supprimés doit être indiqué pour chaque type d'enregistrement séparément.</p>
Supprimer les anciens postes	<p>La tâche consiste à supprimer les postes obsolètes de la base de données.</p>





Type de tâche	Paramètres et description
	<p>Vous devez indiquer la durée (90 jours par défaut) après laquelle tous les postes qui ne se sont pas connectés au Serveur au moins une fois seront considérés comme anciens et supprimés du Serveur.</p>
	<p> L'information obsolète est supprimée de la base de données pour libérer de l'espace disque. Le délai par défaut indiqué dans les onglets Supprimer les enregistrements obsolètes et Supprimer les anciens postes est de 90 jours. Si vous réduisez ce délai, les statistiques sur le fonctionnement des composants du réseau antivirus seront moins représentatives. De plus, le Serveur pourrait avoir besoin de beaucoup plus de ressources.</p>
Suppression des messages périmés	<p>La tâche consiste à supprimer les messages suivants de la base de données :</p> <ul style="list-style-type: none">• notifications de l'agent,• notifications pour la console web,• rapports créés d'après la planification. <p>La tâche permet également de supprimer les messages marqués comme obsolètes, c'est à dire dont la période de conservation a expiré. Vous pouvez spécifier la période de conservation :</p> <ul style="list-style-type: none">• pour les notifications : via la méthode d'envoi appropriée durant la création d'une notification (voir Configuration des notifications).• pour les rapports : dans la tâche de création de rapports. <p>Aucun paramètre supplémentaire n'est requis pour exécuter la tâche.</p>
Redémarrer le Serveur Dr.Web	<p>La tâche consiste à redémarrer le Serveur.</p> <p>Aucun paramètre supplémentaire n'est requis pour exécuter la tâche.</p>
Réveiller les postes	<p>La tâche consiste à réveiller les postes qui sont en veille, par exemple avant de lancer un scan.</p> <p>Les paramètres suivants définissent quels postes seront activés :</p> <ul style="list-style-type: none">• Réveiller tous les postes – réveiller tous les postes connectés au Serveur.• Réveiller les postes en fonction des paramètres indiqués – seuls les postes possédant les paramètres suivants seront réveillés :<ul style="list-style-type: none">▫ Adresses IP – la liste des adresses IP des postes à activer. La liste est spécifiée au format suivant : 10.3.0.127, 10.4.0.1-10.4.0.5, 10.5.0.1/30. Lors de la création d'une liste, utilisez la virgule ou le saut de ligne pour séparer les différentes adresses. Vous pouvez également utiliser les noms DNS des postes au lieu de leurs adresses IP.▫ Adresses MAC – la liste des adresses MAC des postes à activer. Les octets des adresses-MAC doivent être séparés par le symbole ':'. Utilisez la virgule ou le saut de ligne pour séparer plusieurs adresses.▫ Groupes – liste des groupes dont il faut activer les postes. Pour sélectionner plusieurs groupes, utilisez les touches CTRL ou SHIFT.



Type de tâche	Paramètres et description
	<p> Pour lancer cette tâche, tous les postes qui seront activés doivent être équipés de cartes réseau supportant Wake-on-LAN.</p> <p>Pour vérifier si votre carte réseau supporte Wake-on-LAN, consultez sa documentation ou ses propriétés (Panneau de configuration → Internet et Réseau → Connexions Réseau → Modifier les paramètres de connexion → Configurer → Avancé).</p>
Sauvegarder les données critiques du serveur	<p>La tâche consiste à sauvegarder les données critiques du Serveur suivantes :</p> <ul style="list-style-type: none">• base de données,• fichier clé de licence,• clé de chiffrement privée. <p>Indiquez les paramètres suivants :</p> <ul style="list-style-type: none">• Chemin – chemin vers le répertoire dans lequel les données seront sauvegardées (un champ vide signifie que le répertoire par défaut sera utilisé).• Nombre maximum de copies – nombre maximum de copies de sauvegarde (la valeur 0 indique qu'il n'y a pas de limitation). <p>Pour en savoir plus, voir les Annexes, p. Annexe H4.5.</p> <p> Le répertoire de copie de sauvegarde doit être vide. Sinon, le contenu du répertoire sera supprimé lors de la copie de sauvegarde.</p>
Sauvegarder le dépôt	<p>La tâche consiste à effectuer des sauvegarde régulières du dépôt.</p> <p>Indiquez les paramètres suivants :</p> <ul style="list-style-type: none">• Chemin – chemin complet vers le répertoire dans lequel la copie de sauvegarde sera stockée.• Nombre maximum de copies – nombre maximum de copies de sauvegarde du dépôt sauvegardés dans le répertoire spécifié. Si le nombre maximum de copies est atteint, la copie la plus ancienne sera effacée pour pouvoir sauvegarde la nouvelle.• Zone du dépôt indique quelles informations sur un composant antivirus seront sauvegardées :<ul style="list-style-type: none">▫ Dépôt entier – sauvegarder toutes les révisions du dépôt pour les composants sélectionnés dans la liste ci-dessous.▫ Révisions critiques seulement – seules les révisions marquées comme importantes seront sauvegardées pour les composants sélectionnés dans la liste ci-dessous.▫ Fichiers de configuration seulement – seuls les fichiers de configuration seront sauvegardés pour les composants choisis dans la liste.



Type de tâche	Paramètres et description
	<ul style="list-style-type: none">Cochez les cases près des zones que vous souhaitez sauvegarder pour les composants. <div style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> Le répertoire de copie de sauvegarde doit être vide. Sinon, le contenu du répertoire sera supprimé lors de la copie de sauvegarde.</div>
Synchronisation avec Active Directory	<p>La tâche consiste à synchroniser les structures du réseau : les conteneurs Active Directory qui contiennent des ordinateurs deviennent des groupes du réseau antivirus dans lesquels les postes de travail sont placés.</p> <p>Aucun paramètre supplémentaire n'est requis pour exécuter la tâche.</p> <div style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> Cette tâche est désactivée par défaut. Pour activer l'exécution de cette tâche, activez l'option Autoriser l'exécution dans les paramètres de tâche ou dans la basse d'outils comme décrit ci-dessus.</div>
Le serveur voisin n'a pas été connecté depuis longtemps	<p>La tâche consiste à envoyer une notifications lorsque les Serveurs voisins n'ont pas été connectés au Serveur actuel depuis longtemps.</p> <p>L'affichage des notifications peut être paramétré dans la rubrique Configuration des notifications en utilisant l'onglet Le serveur voisin n'a pas été connecté depuis longtemps.</p> <p>Indiquez les valeurs appropriées dans les champs Heures et Minutes pour définir le moment où le Serveur voisin sera considéré comme non connecté depuis longtemps.</p>
Le poste n'a pas été connecté depuis longtemps	<p>La tâche consiste à envoyer une notifications lorsque les postes n'ont pas été connectés au Serveur actuel depuis longtemps.</p> <p>L'affichage des notifications peut être paramétré à la rubrique Configuration des notifications en utilisant l'onglet Le poste n'a pas été connecté depuis longtemps.</p> <p>Dans le champ Jours, indiquez un délai après lequel le poste sera considéré comme non connecté depuis longtemps.</p>
Création d'un rapport statistique	<p>La tâche consiste à créer un rapport avec les statistiques sur le réseau antivirus.</p> <p>Pour créer un rapport, il est obligatoire d'activer la notification Rapport périodique (voir Configuration des notifications). Le rapport généré est sauvegardé sur l'ordinateur sur lequel le Serveur est installé. Le type de l'obtention du rapport dépend du type de notification :</p> <ul style="list-style-type: none">Pour envoyer des messages E-mail : un message avec le rapport en pièce jointe ainsi que le lien vers l'emplacement du rapport sont envoyés sur l'adresse e-mail indiquée dans les paramètres des notifications.Pour toute autre méthode de fourniture : envoi d'une notification avec un lien vers l'emplacement du rapport.



Type de tâche	Paramètres et description
	<p>Pour créer une tâche dans le planificateur, vous devez configurer les paramètres suivants :</p> <ul style="list-style-type: none">• Profils de notifications – nom du groupe de notifications ayant des paramètres communs pour la génération de rapports. Le titre du groupe peut être indiqué lors de la création du groupe.• Langue du rapport – langue des données dans le rapport.• Format de la date – format d’affichage des données statistiques contenant des dates. Les formats suivants sont disponibles :<ul style="list-style-type: none">▫ européen : JJ-MM-AAAA HH:MM:SS▫ américain : MM/JJ/AAAA HH:MM:SS• Format du rapport – format du document de sauvegarde des rapports statistiques.• Période du rapport – période pour laquelle les données statistiques seront intégrées au rapport.• Groupes – liste des groupes des postes du réseau antivirus dont les données seront intégrées au rapport. Pour sélectionner plusieurs groupes, utilisez les touches CTRL ou SHIFT.• Tableaux de rapports – liste des tableaux statistiques dont les données seront intégrées au rapport. Pour sélectionner plusieurs tableaux, utilisez les touches CTRL ou SHIFT.• Délai de conservation du rapport – délai de conservation du rapport sur l’ordinateur avec le Serveur installé, du moment de la génération du rapport.

2. Dans l’onglet **Heure** :


- Dans la liste déroulante **Périodicité**, sélectionnez le mode de lancement de la tâche et configurez l’heure en fonction de la périodicité indiquée :

Mode de lancement	Paramètres et description
Fermeture	<p>La tâche sera lancée à la fermeture du Serveur.</p> <p>Aucun paramètre supplémentaire n’est requis pour exécuter la tâche.</p>
Démarrage	<p>La tâche sera lancée au démarrage du Serveur.</p> <p>Aucun paramètre supplémentaire n’est requis pour exécuter la tâche.</p>
Dans N minutes après la tâche initiale	<p>Dans la liste déroulante Tâche initiale, sélectionnez la tâche par rapport à laquelle est spécifiée l’heure d’exécution de la tâche courante.</p> <p>Dans le champ Minute, indiquez ou choisissez dans la liste le nombre de minutes pour lancer l’exécution de la tâche éditée après l’exécution de la tâche initiale.</p>
Chaque jour	<p>Indiquez l’heure et les minutes – la tâche sera lancée chaque jour au moment spécifié.</p>



Mode de lancement	Paramètres et description
Chaque mois	Choisissez la date (jour du mois) et indiquez l'heure et les minutes – la tâche sera lancée au jour spécifié au moment indiqué.
Chaque semaine	Choisissez le jour de la semaine et indiquez l'heure et les minutes – la tâche sera lancée au jour de la semaine spécifié au moment indiqué.
Chaque heure	Indiquez un chiffre entre 0 et 59 pour paramétrer la minute à laquelle sera lancée la tâche dans une heure.
Chaque N minutes	La valeur N doit être indiquée pour paramétrer l'intervalle entre l'exécution des tâches. Si N est égal à 60 ou plus, la tâche sera lancée chaque N minutes. Si N est inférieur à 60, la tâche sera lancée chaque minute de l'heure multiple de N .

- Cochez la case **Interdire après la première exécution** pour exécuter la tâche une seule fois conformément à la périodicité spécifiée. Si la case n'est pas cochée, la tâche sera exécutée plusieurs fois selon la périodicité indiquée.

Pour répéter le lancement d'une tâche déjà exécutée, utilisez le bouton  **Planifier à plusieurs reprises** dans la barre d'outils de la section Planification.

3. Lorsque tous les paramètres sont indiqués pour une tâche, cliquez sur **Sauvegarder** pour appliquer les modifications des paramètres modifiés si vous avez modifié une tâche existante, ou pour créer une nouvelle tâche avec les paramètres spécifiés si vous avez créé une nouvelle tâche.

8.5. Configuration du Serveur web



A chaque enregistrement des modifications de la section **Configuration du serveur web**, une copie de sauvegarde de la version précédente du fichier de configuration du serveur web est automatiquement enregistrée. 10 dernières copies sont sauvegardées.

Les copies de sauvegarde se trouvent dans le même répertoire où se trouve le fichier de configuration et elles portent les noms conformes au format suivant :

```
webmin.conf; <date_et_heure_de_création>
```

Vous pouvez utiliser les copies de sauvegarde créées, notamment pour restaurer le fichier de configuration si l'interface du Centre de gestion n'est pas disponible.


Pour configurer les paramètres du Serveur Web :


1. Sélectionnez l'élément **Administration** du menu principal du Centre de gestion.
2. Cliquez sur **Configuration du Serveur Web** dans le menu de gestion. Une fenêtre permettant de configurer le Serveur Web va s'ouvrir.



Les valeurs des champs marqués du symbole *, doivent être obligatoirement spécifiées.


3. Les boutons suivants de gestion des paramètres sont disponibles dans la barre d'outils :

 **Redémarrer le Serveur Dr.Web** – redémarrer le Serveur pour appliquer les modifications apportées dans cette rubrique. Le bouton est activé après la modification des paramètres de la rubrique et l'appui sur le bouton **Sauvegarder**.

 **Restaurer la configuration de la copie de sauvegarde** – liste déroulante contenant les copies de sauvegarde des paramètres de la rubrique entière que l'on peut restaurer après les modifications apportées. Le bouton est activé après la modification des paramètres de la rubrique et l'appui sur le bouton **Sauvegarder**.

 **Restaurer tous les paramètres à leur valeur initiale** – restaurer les valeurs données à tous les paramètres de cette rubrique avant modification (dernières valeurs sauvegardées).

 **Restaurer tous les paramètres à leur valeur par défaut** – restaurer les valeurs par défaut de tous les paramètres de la rubrique.

4. Pour appliquer les paramètres apportées dans les paramètres de la rubrique, cliquez sur **Sauvegarder**. Ensuite, le redémarrage du Serveur est requis. Pour ce faire, cliquez sur le bouton  **Redémarrer le Serveur Dr.Web** dans la barre d'outils de cette rubrique.

8.5.1. Général

Dans l'onglet **Général**, indiquez les paramètres du Serveur Web :

- **Adresse du Serveur Dr.Web** – adresse IP ou nom DNS du Serveur Dr.Web.

Spécifié au format suivant :

<Adresse IP ou nom DNS du Serveur> [: <port>]

Si l'adresse du Serveur n'est pas spécifiée, le nom de l'ordinateur retourné par le système d'exploitation ou l'adresse réseau du Serveur : nom DNS, si disponible, sinon l'adresse IP, sont utilisés.

Si le numéro de port n'est pas indiqué, le port spécifié dans la requête est utilisé (par exemple, lors de l'accès au Serveur depuis le Centre de gestion ou via **Web API**). Notez que pour les requêtes depuis le Centre de gestion, c'est le port indiqué dans la ligne d'adresse lors de la connexion du Centre de gestion au Serveur.

La valeur est sauvegardée dans le paramètre `<server-name />` du fichier de configuration `webmin.conf`.

La valeur de ce paramètre est également utilisée pour générer le lien de téléchargement du fichier d'installation de l'Agent pour les postes du réseau antivirus.

- **Nombre de requêtes parallèles** – nombre de requêtes parallèles traitées par le Serveur Web. Ce paramètre affecte les performances du serveur. Il n'est pas recommandé de modifier ce paramètre sans nécessité.
- **Nombre de flux d'entrée/sortie** – nombre de flux traitant les données transmises via le réseau. Ce paramètre affecte les performances du Serveur. Il n'est pas recommandé de modifier ce paramètre sans nécessité.



- **Time out (s)** – timeout de la session HTTP. En cas de l'utilisation des connexions permanentes, le Serveur interrompt la connexion si pendant le délai spécifié il n'y a aucune requête de client.
- **Vitesse minimale d'envoi (O/s)** – vitesse minimum acceptable pour l'envoi de données. Si la vitesse sortante du trafic est inférieure à cette valeur, la connexion sera rejetée. Indiquez la valeur 0 pour enlever cette limite.
- **Vitesse minimale de réception (O/s)** – vitesse minimum acceptable pour la réception des données. Si le trafic entrant est inférieur à cette valeur, la connexion sera rejetée. Indiquez la valeur 0 pour ignorer cette limite.
- **Taille du tampon d'envoi (Ko)** – la taille des mémoires tampon utilisées pour envoyer des données. Ce paramètre affecte les performances du Serveur. Il n'est pas recommandé de le modifier sans nécessité.
- **Taille du tampon de réception (Ko)** – la taille des mémoires tampon utilisées pour recevoir des données. Ce paramètre affecte les performances du Serveur. Il n'est pas recommandé de le modifier sans nécessité.
- **Longueur maximum de la requête (Ko)** – Taille autorisée maximum pour une requête HTTP.
- **Utiliser la compression** – cochez la case pour utiliser la compression du trafic pour la transmission de données au Serveur Web via HTTP/HTTPS.
 - Si la case est cochée, la liste déroulante **Niveau de compression** est disponible. Dans cette liste, vous pouvez sélectionner le niveau de compression des données de 1 à 9, où 1 est le niveau minimum de compression et 9 est le niveau maximum.
- **Remplacer les adresses IP** – cochez la case pour remplacer les adresses IP par les noms d'ordinateurs dans le fichier de journal du Serveur.
- **Maintenir la session SSL active** – cochez la case pour utiliser une connexion permanente pour SSL. Les navigateurs plus anciens peuvent ne pas fonctionner correctement avec les connexion SSL régulières. Désactivez ce paramètre si vous rencontrez des problèmes avec le protocole SSL.
- **Certificat SSL** – chemin vers le fichier du certificat SSL. Dans la liste déroulante sont présentés les certificats disponibles du répertoire du Serveur.
- **Clé privée SSL** – chemin vers le fichier de la clé privée SSL. Dans la liste déroulante sont présentées les clés privées SSL disponibles du répertoire du Serveur.

8.5.2. Avancé

A l'onglet **Supplémentaire**, indiquez les paramètres du Serveur Web suivants :

- Cochez la case **Afficher les erreurs de script** pour montrer ces erreurs dans le navigateur. Ce paramètre est utilisé par le support technique et les développeurs. Il n'est pas recommandé de le modifier sans besoin.
- Cochez la case **Suivre les scripts** pour effectuer un tracing des scripts. Ce paramètre est utilisé par le support technique et les développeurs. Il n'est pas recommandé de le modifier sans besoin.



- Cochez la case **Autoriser l'arrêt des scripts** pour annuler l'exécution des scripts. Ce paramètre est utilisé par le support technique et les développeurs. Il n'est pas recommandé de le modifier sans besoin.

8.5.3. Transport

Dans l'onglet **Transport**, sont configurées les adresses réseau « écoutées » depuis lesquelles le serveur web reçoit les connexions entrantes, par exemple, pour la connexion du Centre de gestion ou pour l'exécution des requêtes via Web API :

- Dans la rubrique **Adresses écoutées via HTTP** est configurée la liste des interfaces qui seront écoutées pour recevoir des connexions via le protocole HTTP :

Dans les champs **Adresse** et **Ports**, indiquez l'adresse IP correspondante et le numéro de port de l'interface réseau depuis laquelle la réception des connexions via le protocole HTTP est autorisée.

Les paramètres suivants sont définis par défaut pour l'écoute par le serveur web :

- **Adresse** : 0.0.0.0 – utiliser « toutes les interfaces réseau » pour cet ordinateur sur lequel le Serveur web est installé.
 - **Port** : 9080 – utiliser le port standard 9080 pour le protocole HTTP.
- Dans la rubrique **Adresses écoutées via HTTPS** est configurée la liste des interfaces qui seront écoutées pour recevoir des connexions via le protocole HTTPS :

Dans les champs **Adresse** et **Ports**, indiquez l'adresse IP correspondante et le numéro de port de l'interface réseau depuis laquelle la réception des connexions via le protocole HTTPS est autorisée.

Les paramètres suivants sont définis par défaut pour l'écoute par le serveur web :

- **Adresse** : 0.0.0.0 – utiliser « toutes les interfaces réseau » pour cet ordinateur sur lequel le Serveur web est installé.
- **Le port** : 9081 – utiliser le port standard 9081 pour le protocole HTTPS.

Pour ajouter un nouveau champ d'adresse, cliquez sur le bouton dans la rubrique correspondante. Pour supprimer le champ, cliquez sur le bouton contre le champ à supprimer.

8.5.4. Sécurité

A l'onglet **Sécurité**, vous pouvez paramétrer les restrictions pour les adresses réseau depuis lesquelles le Serveur Web reçoit les requêtes HTTP et HTTPS.

Pour configurer les limitations d'accès pour tout type de connexion :

1. Pour autoriser l'accès via HTTP ou HTTPS depuis des adresses définies, ajoutez-les aux listes **HTTP: Autorisé** ou **HTTPS: Autorisé**.
2. Pour refuser l'accès via HTTP ou HTTPS depuis des adresses définies, ajoutez-les aux listes **HTTP: Refusé** ou **HTTPS: Refusé**.



3. Les adresses qui ne sont incluses dans aucune des listes sont autorisées ou refusées en fonction du statut des cases **Priorité de refus pour HTTP** et **Priorité de refus pour HTTPS** : si la case est cochée, les adresses qui ne sont incluses dans aucune des listes (ou incluses dans les deux listes) sont refusées. Sinon, ces adresses sont autorisées.

Pour éditer la liste des adresses :

1. Entrez l'adresse réseau dans le champ correspondant et cliquez ensuite sur le bouton **Sauvegarder**.
2. 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.

3. Pour ajouter un nouveau champ d'adresse, cliquez sur le bouton dans la rubrique correspondante.
4. Pour supprimer un champ, cliquez sur .

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 d'hôtes dans les réseaux de ce type ont le format suivant : 125 . * . * . *

8.6. Procédures utilisateur



Lors de l'exécution des scripts Lua, l'administrateur obtient l'accès à tout le système de fichiers à l'intérieur du répertoire du Serveur et aux certaines commandes sur l'ordinateur avec le Serveur installé.

Pour interdire l'accès aux procédures utilisateur, désactivez le droit **Éditer la configuration du Serveur et du dépôt** pour l'administrateur correspondant (voir le p. [Administrateurs et groupes administrateur](#)).

Pour faciliter et automatiser l'exécution de certaines tâches du Serveur Dr.Web, il est possible d'utiliser les procédures utilisateur effectuées en tant que scripts Lua.



Les procédures utilisateur sont placées dans le sous-répertoire suivant du répertoire d'installation du Serveur :

- sous Windows : `var\extensions`
- sous FreeBSD : `/var/drwcs/extensions`



- sous Linux et Solaris : `/var/opt/drwcs/extensions`

Après l'installation du Serveur, dans ce sous-répertoire sont placées les procédures utilisateur préinstallées.

Il est recommandé d'éditer les procédures utilisateur via le Centre de gestion.

Pour configurer l'exécution des procédures utilisateur :

1. Sélectionnez l'élément **Administration** du menu principal du Centre de gestion.
2. Dans la fenêtre qui s'ouvre, choisissez **Procédures utilisateur** dans le menu de gestion. Une autre fenêtre va s'ouvrir.

Arborescence des procédures





La liste hiérarchique des procédures affiche une arborescence, dont les noeuds sont des groupes de procédures et des procédures utilisateur appartenant à ces groupes.

Initialement, l'arborescence des procédures contient des groupes pré-installés suivants :

- **Examples of the hooks** contiennent des modèles de toutes les procédures utilisateur disponibles. Sur la base de ces modèles, vous pouvez créer vos propres procédures utilisateur.
- **IBM Tivoli integration** contiennent des modèles des procédures utilisateur utilisées lors de l'intégration avec le système IBM Tivoli.


L'apparence de l'icône dépend du type et du statut de cet élément (voir le [tableau 8-6](#)).


Tableau 8-6. Icônes des éléments de l'arborescence des procédures

Icône	Description
Groupes de procédures	
	Groupe de procédures pour lequel l'exécution des procédures est autorisée.
	Groupe de procédures pour lequel l'exécution des procédures est interdite.
Procédures	
	Procédure pour laquelle l'exécution est autorisée.
	Procédure pour laquelle l'exécution est interdite.


Gestion de l'arborescence des procédures


Pour gérer les objets de l'arborescence, utilisez les éléments suivants de la barre d'outils :


 – liste déroulante pour l'ajout d'un élément à l'arborescence des procédures :


 **Ajouter une procédure** – ajouter une nouvelle procédure utilisateur.



 **Ajouter un groupe de procédures** – ajouter un nouveau groupe utilisateur pour y placer des procédures.



 **Supprimer les objets sélectionnés** – supprimer une procédure utilisateur ou un groupe de procédures sélectionné dans l'arborescence.

 **Autoriser l'exécution de la procédure** – la même action est effectuée via l'éditeur de procédures si vous cochez la case **Autoriser l'exécution de la procédure**. Voir aussi [Activation des procédures](#).

 **Désactiver l'exécution de la procédure** – la même action est effectuée via l'éditeur de procédures si vous décochez la case **Autoriser l'exécution de la procédure**. Voir aussi [Activation des procédures](#).

Gestion des groupes de procédures

Pour créer un nouveau groupe :

1. Dans la barre d'outils, sélectionnez  →  **Ajouter un groupe de procédures**.
2. Dans la fenêtre qui s'affiche, configurez les paramètres suivants :
 - Cochez la case **Autoriser l'exécution de la procédure** pour activer les procédures qui seront incluses dans ce groupe. Voir aussi [Activation des procédures](#).
 - Dans le champ **Nom de groupe**, spécifiez un nom pour le groupe créé.
3. Cliquez sur **Enregistrer**.

Pour modifier l'ordre de l'utilisation des groupes :



1. Dans l'arborescence, glissez-déposez (drag and drop) un groupe de procédures et mettez-le dans le bon ordre par rapport aux autres groupes.
2. Si vous modifiez l'ordre des groupes, l'ordre de l'utilisation des procédures va changer automatiquement : les procédures des groupes qui sont placés plus haut dans l'arborescence seront exécutées les premières.

Pour déplacer une procédure dans un autre groupe :

1. Sélectionnez dans l'arborescence la procédure que vous voulez déplacer.
2. Dans le panneau de propriétés qui s'affiche, sélectionnez dans la liste déroulante **Groupe supérieur** le groupe dans lequel il faut placer la procédure.
3. Cliquez sur **Enregistrer**.

Gestion des procédures

Pour ajouter une nouvelle procédure :

1. Dans la barre d'outils, sélectionnez  →  **Ajouter une procédure**.
2. Dans la fenêtre qui s'affiche, configurez les paramètres suivants :



- Cochez la case **Autoriser l'exécution de la procédure** pour activer la procédure créée. Voir aussi [Activation des procédures](#).
- Dans la liste déroulante **Groupe parent**, sélectionnez le groupe dans lequel la procédure sera placée. Plus tard, vous pourrez déplacer la procédure dans un autre groupe – voir [ci-dessus](#).
- Dans la liste déroulante **Procédure**, sélectionnez le type de la procédure. Le type de la procédure désigne l'action pour laquelle cette procédure sera appelée.
- Dans le champ **Texte de procédure**, entrez le script lus qui sera exécuté lors de l'appel de cette procédure.
Dans la sous-rubrique **Information sur la procédure** vous pouvez consulter l'événement pour lequel cette procédure sera appelée, ainsi que les informations sur la disponibilité de la base de données du Serveur pour cette procédure et les listes des paramètres d'entrée et des valeurs de retour pour ce type de la procédure.

3. Cliquez sur **Enregistrer**.


Pour éditer une procédure :

1. Sélectionnez dans l'arborescence la procédure que vous voulez éditer.
2. Dans la partie droite de la fenêtre, un panneau des propriétés de cette procédure va s'afficher automatiquement. Vous pouvez modifier tous les paramètres spécifiés lors de la création de la procédure, sauf le paramètre **Procédure**. Ce paramètre désigne l'événement pour lequel cette procédure est appelée et il n'est pas modifiable après la création de la procédure.
3. Cliquez sur **Enregistrer**.

Activer une procédure

L'activation des procédures et des groupes détermine si les procédures seront exécutées quand l'événement correspondant a eu lieu ou non.

Pour activer une procédure ou un groupe de procédures :

1. Sélectionnez dans l'arborescence la procédure ou le groupe que vous voulez activer.
2. Effectuez une des actions suivantes :
 - Dans la barre d'outils, cliquez sur le bouton  **Autoriser l'exécution de la procédure**.
 - Dans la partie droite du panneau des propriétés de l'objet sélectionné, cochez la case **Autoriser l'exécution procédures**, si cette case est décochée. Cliquez sur le bouton **Sauvegarder**.

Particularités de l'activation des procédures :

Pour que la procédure soit exécutée si l'événement correspondant a eu lieu, il faut que :

- a) la procédure soit activée ;
- b) le groupe qui contient cette procédure soit activé.



Si le groupe de procédures est désactivé, les procédures qui y sont incluses ne seront pas exécutées même si elles sont activées.

Si vous activez un groupe, notez que seules les procédures activées seront exécutées.

8.7. Configuration des notifications

Dr.Web Enterprise Security Suite supporte l'envoi des notifications sur les attaques virales, sur les statuts des composants du réseau antivirus et sur d'autres événements aux administrateurs du réseau antivirus Dr.Web Enterprise Security Suite.

8.7.1. Configuration des notifications

Pour configurer les notifications de l'administrateur sur les événements du réseau antivirus :

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion. Dans la fenêtre qui s'ouvre, choisissez l'élément du menu de gestion **Configuration des notifications**.
2. Lors de la première configuration, la liste des notifications est vide. Cliquez sur **Ajouter une notification**.
3. Pour activer l'envoi des notifications, passez au mode correspondant à gauche de l'en-tête du bloc des notifications :
  – l'envoi des notifications pour ce bloc est activé.
  – les notifications pour ce bloc ne seront pas envoyées.
4. Dans cette rubrique, vous pouvez créer plusieurs blocs (profils) des notifications, par exemple, pour les différents modes d'envoi. Pour ajouter encore un bloc, cliquez sur  à droite des paramètres du bloc des notifications. Un bloc des notifications sera ajouté en bas de la page. La configuration de différents blocs de notifications et de textes de leur templates s'effectue séparément.
5. Dans le champ **En-tête**, spécifiez le nom du bloc des notifications ajouté. Ce nom sera utilisé, par exemple, pour configurer la tâche **Rapports statistiques** dans la planification du Serveur. Ensuite, pour éditer l'en-tête, cliquez avec le bouton gauche de la souris sur l'en-tête et entrez le nom nécessaire. S'il y a plus qu'un seul bloc des notifications, une liste déroulante des en-têtes des blocs des notifications existants vous sera proposé.
6. Pour configurer l'envoi des notifications, sélectionnez le type nécessaire d'envoi des notifications dans la liste déroulante **Mode d'envoi du message** :
 - [Console web](#) – envoyer des notifications pour les consulter dans la [console web](#).
 - [E-mail](#) – envoyer des notifications par e-mail.
 - [SNMP](#) – envoyer des notifications via le protocole SNMP.
 - [Notifications push](#) – envoyer des notifications push dans le Centre mobile de gestion de la sécurité Dr.Web. Cette option sera disponible dans la liste déroulante **Mode d'envoi du**



message après la connexion du Centre mobile de gestion de la sécurité à ce Serveur Dr.Web.

- [Windows Message](#) – envoyer des notifications via **Windows Messenger** (uniquement pour les Serveurs tournant sous OS Windows).


Vous pouvez consulter la description de chaque type d'envoi des notifications dans la rubrique ci-dessous.

7. Pour envoyer des notifications, le jeu préconfiguré des notifications standard du Serveur est fourni.



Vous pouvez consulter la description des notification préconfigurées et de leurs paramètres dans les **Annexes**, l'[Annexe D1. Description des notifications préconfigurées](#).

Pour configurer des notifications concrètes, procédez comme suit :

- a) Dans la liste des notifications, cochez les cases contre les notifications qui seront envoyées conformément au mode d'envoi de ce bloc des notifications.
- b) Pour modifier les paramètres des notifications, cliquez sur  contre la notification à éditer. Le template de notification va s'ouvrir. Si cela est nécessaire, éditez le texte de la notification à envoyer. Dans le texte de la notification, vous pouvez utiliser les variables du template (entre accolades). Pour ajouter des variables, les listes déroulantes dans l'en-tête de la notification sont fournies. Lors de la préparation du message, le système des notification remplace les variables du template par le texte concret qui dépend de la configuration actuelle du système des notification. Vous pouvez consulter la liste des variables disponibles dans les **Annexes**, l'[Annexe D3. Paramètres des templates du système de notifications](#).
- c) Pour la notification par e-mail, il existe une possibilité d'ajouter des champs utilisateur aléatoires dans la section avancée **En-têtes** dans l'éditeur de template de chaque notification (voir le p. **b**). Les en-têtes doivent être formés conformément aux normes RFC 822, RFC 2822 et de ne pas interférer avec les champs spécifiés dans les normes pour les messages e-mail. Notamment, la norme RFC 822 garantie l'absence de spécification des en-têtes commençant par X-, c'est pourquoi il est recommandé de spécifier les noms au format X-<nom de l'en-tête>. Par exemple, X-Template-Language: French.
- d) Pour les notifications de la sous-section **Poste**, vous pouvez également spécifier la liste des postes dont les événements seront indiqués dans les notifications. Dans la fenêtre d'édition du template, dans l'arborescence **Groupes de postes contrôlés**, sélectionnez les groupes de postes dont les événements seront contrôlés et les notifications correspondantes seront envoyées. Pour sélectionner plusieurs groupes, utilisez les touches CTRL ou SHIFT.



Pour le mode d'envoi **SNMP**, les textes des templates de notifications sont spécifiés du côté du destinataire (*station de gestion* en termes de RFC 1067). Via le Centre de gestion, dans la sous-rubrique **Poste**, vous pouvez spécifier uniquement la liste des postes dont les événements seront indiqués dans les notifications.

8. Après avoir terminé l'édition, cliquez sur **Enregistrer** pour appliquer toutes les modifications apportées.



Notifications affichées dans la Console Web

Pour les notifications affichées dans la Console Web, spécifiez les paramètres suivants :



- **Nombre de tentatives d'envoi** – nombre de tentatives réitérées en cas d'échec d'envoi de la notification. Par défaut c'est 10.
- **Timeout pour renvoyer le message** – Laps de temps en secondes, à l'expiration duquel la tentative de renvoyer le message sera reprise. Par défaut c'est 300 secondes.
- **Durée de sauvegarde du message** – durée pendant laquelle il faut sauvegarder la notification, à partir du moment de sa réception. Par défaut c'est 1 jour. A la fin de cette période, la notification est considérée comme obsolète et supprimée conformément à la tâche **Supprimer les messages obsolètes** dans les paramètres du Serveur.

Pour les notifications reçues en ce mode d'envoi, vous pouvez spécifier dans la rubrique [Notifications de la Console Web](#) un délai de sauvegarde illimité.

- **Envoyer un message de test** – envoyer un message de test conformément aux paramètres configurés du système de notifications. Le texte de la notification de test est spécifié dans les templates de notifications.

Notifications par e-mail

Pour notifier par e-mail, spécifiez les paramètres suivants :

- **Nombre de tentatives d'envoi** – nombre de tentatives réitérées en cas d'échec d'envoi de la notification. Par défaut c'est 10.
- **Timeout pour renvoyer le message** – Laps de temps en secondes, à l'expiration duquel la tentative de renvoyer le message sera reprise. Par défaut c'est 300 secondes.
- **Adresse email de l'expéditeur** – adresse e-mail de l'expéditeur des notifications.
- **Adresses e-mail du destinataire** – adresses e-mails des destinataires de la notification. Vous pouvez entrer une seule adresse du destinataire dans chaque champ de saisie. Pour ajouter encore un champ du destinataire, cliquez sur le bouton . Pour supprimer un champ, cliquez sur .
- Dans la rubrique **Configuration du serveur SMTP**, configurez les paramètres suivants :
 - **Adresse** – adresse du serveur SMTP qui sera utilisée pour envoyer des e-mails.
 - **Port** – port pour la connexion au serveur SMTP. C'est le port 465 qui est utilisé par défaut en cas d'ouverture d'une connexion TLS sécurisée à part, sinon, c'est le port 25.
 - **Utilisateur, Mot de passe** – si nécessaire, spécifiez le nom de l'utilisateur et le mot de passe de l'utilisateur du serveur SMTP, si le serveur SMTP exige l'authentification.
 - Cochez la case **Chiffrement STARTTLS** pour l'échange chiffré de données. Dans ce cas, le passage à la connexion sécurisée s'effectue via la commande `STARTTLS`. L'utilisation du port 25 pour la connexion est prévue par défaut.



- Cochez la case **Chiffrement SSL** pour l'échange chiffré de données. Dans ce cas, une connexion TLS sécurisée sera ouverte à part. L'utilisation du port 465 pour la connexion est prévue par défaut.
- Cochez la case **Utiliser l'authentification CRAM-MD5** pour utiliser l'authentification *CRAM-MD5* sur le serveur de messagerie.
- Cochez la case **Utiliser l'authentification DIGEST-MD5** pour utiliser l'authentification *DIGEST-MD5* sur le serveur de messagerie.
- Cochez la case **Utiliser l'authentification standard** pour utiliser l'authentification *plain text* sur le serveur de messagerie.
- Cochez la case **Utiliser l'authentification LOGIN** pour utiliser l'authentification *LOGIN* sur le serveur de messagerie.
- Cochez la case **Vérifier le certificat SSL** du serveur pour vérifier le certificat *SSL* du serveur de messagerie.
- Cochez la case **Mode de débogage** pour consulter le journal détaillé de la session SMTP.
- **Envoyer un message de test** – envoyer un message de test conformément aux paramètres configurés du système de notifications. Le texte de la notification de test est spécifié dans les templates de notifications.

Notifications via le protocole SNMP

Pour notifier via le protocole de SNMP spécifiez les paramètres suivants :

- **Nombre de tentatives d'envoi** – nombre de tentatives réitérées en cas d'échec d'envoi de la notification. Par défaut c'est 10.
- **Timeout pour renvoyer le message** – Laps de temps en secondes, à l'expiration duquel la tentative de renvoyer le message sera reprise. Par défaut c'est 300 secondes.
- **Destinataire** – entité de réception SNMP, par exemple, l'adresse IP ou le nom DNS de l'ordinateur. Vous pouvez entrer un seul utilisateur dans chaque champ de saisie. Pour ajouter encore un champ, cliquez sur **+**. Pour supprimer un champ, cliquez sur **-**.
- **Expéditeur** – l'entité envoyant la requête SNMP. Par exemple, l'adresse IP ou le nom DNS de l'ordinateur (doit être reconnu par le serveur DNS).

Si l'expéditeur n'est pas spécifié, « localhost » est utilisé par défaut sous Windows et "" sous les OS de la famille UNIX.

- **Communauté** – communauté SNMP ou contexte. Par défaut `public`.
- **Envoyer un message de test** – envoyer un message de test conformément aux paramètres configurés du système de notifications. Le texte de la notification de test est spécifié dans les templates de notifications.



Notifications push

Pour les notifications push envoyées au Centre mobile de gestion, configurez les paramètres suivants :

- **Nombre de tentatives d'envoi** – nombre de tentatives réitérées en cas d'échec d'envoi de la notification. Par défaut c'est 10.
- **Timeout pour renvoyer le message** – Laps de temps en secondes, à l'expiration duquel la tentative de renvoyer le message sera reprise. Par défaut c'est 300 secondes.
- **Envoyer un message de test** – envoyer un message de test conformément aux paramètres configurés du système de notifications. Le texte de la notification de test est spécifié dans les templates de notifications.

Notifications via réseau Windows



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.

Pour les messages dans le réseau OS Windows, configurez les paramètres suivants :

- **Nombre de tentatives d'envoi** – nombre de tentatives réitérées en cas d'échec d'envoi de la notification. Par défaut c'est 10.
- **Timeout pour renvoyer le message** – Laps de temps en secondes, à l'expiration duquel la tentative de renvoyer le message sera reprise. Par défaut c'est 300 secondes.
- **Destinataire** – liste des noms des ordinateurs des destinataires de messages. Vous pouvez entrer un seul nom de l'ordinateur dans chaque champ de saisie. Pour ajouter encore un champ du destinataire, cliquez sur le bouton . Pour supprimer un champ, cliquez sur .
- **Envoyer un message de test** – envoyer un message de test conformément aux paramètres configurés du système de notifications. Le texte de la notification de test est spécifié dans les templates de notifications.

8.7.2. Notifications de la console Web

Via le Centre de gestion, vous pouvez consulter et gérer les notifications de l'administrateur reçues par le moyen **Console web** (l'envoi des notifications de l'administrateur est décrit dans la rubrique [Configuration des notifications](#)).

Pour consulter et gérer les notifications :

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 **Notifiactions de la console Web**. La liste des notifications envoyées sur la console Web va s'afficher.



2. Pour consulter la notification, cliquez sur la ligne correspondante du tableau. Une fenêtre contenant le texte du message va s'ouvrir. Dans ce cas, la notification sera marquée comme lue.
3. Pour gérer la liste des notifications, utilisez les éléments suivants :
 - a) Les éléments généraux de la barre d'outils sont utilisés pour gérer la rubrique de notifications dans son ensemble. Ces éléments sont toujours disponibles dans la barre d'outils :


Configuration		Action
Importance	Maximum	Afficher seulement les notifications avec une importance Maximum
	Haute	Afficher seulement les notifications avec une importance de Haute à Maximum
	Moyenne	Afficher seulement les notifications avec une importance de Moyenne à Maximum
	Basse	Afficher seulement les notifications avec une importance de Basse à Maximum
	Minimum	Afficher seulement les notifications avec une importance de Minimum à Maximum
Source	Agent	Afficher les notifications liées aux événements sur les postes
	Serveur	Afficher les notifications liées aux événements sur le Serveur


Pour afficher les notifications reçues pendant le délai spécifié, utilisez un des moyens suivants :


- Sélectionnez un des délais préconfigurés dans la liste déroulante de la barre d'outils.
- Sélectionnez dans les calendriers déroulants les dates aléatoires du début et de la fin du délai.

Après avoir modifié les valeurs de ces paramètres, cliquez sur **Actualiser** pour afficher la liste des notifications conformément aux paramètres spécifiés.

- b) Pour gérer les notifications particulières, cochez les cases contre les notifications nécessaires ou cochez la case commune dans l'en-tête du tableau pour sélectionner toutes les notifications dans la liste. Les éléments de gestion des notifications sélectionnées deviennent disponibles dans la barre d'outils :

 **Supprimer les notifications** – supprimer toutes les notifications sans possibilité de restauration.

 **Marquer les notifications comme lues** – marquer toutes les notifications comme lues.

- c) Placez l'icône  **Sauvegarder le message sans suppression automatique** dans la liste des notifications contre les notifications qui ne doivent pas être supprimées après l'expiration du délai spécifié (le délai de sauvegarde est spécifié avant l'envoi des notifications dans la rubrique [Configuration des notifications](#) dans les paramètres du moyen d'envoi **Console Web**). Ces notifications seront gardées jusqu'à ce que vous les supprimiez manuellement





dans la rubrique **Notifications de la console web** ou n'enlevez l'icône  contre ces notifications.

8.7.3. Notifications non envoyées

Via le Centre de gestion, vous pouvez suivre et gérer les notifications de l'administrateur dont l'envoi a échoué conformément aux paramètres de la rubrique [Configuration des notifications](#).

Pour consulter et gérer les notifications non envoyées :

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion, et dans la fenêtre qui s'ouvre, choisissez la rubrique **Notifications non envoyées** dans le menu de gestion. La liste des notifications non envoyées de ce Serveur va s'ouvrir.
2. Dans la liste des notifications non envoyées sont placées les notifications dont l'envoi aux destinataires a échoué, mais le nombre de tentative d'envoi spécifié dans les paramètres de cette notification n'est pas encore dépassé.
3. Le tableau des notifications non envoyées contient des informations suivantes :
 - **Notification** – nom de la notification de la liste des notifications préinstallées.
 - **En-tête** – nom du bloc des notifications. L'envoi de notifications est effectué conformément aux paramètres de ce bloc.
 - **Nombre d'envois restants** – nombre d'envois réitérées restantes en cas d'échec d'envoi de la notification. Le nombre initial des tentatives d'envoi est spécifié lors de la configuration des notifications dans la rubrique [Configuration des notifications](#). Après l'envoi d'une notification, il n'est pas possible de modifier le nombre de tentatives de l'envoi pour cette notification.
 - **Heure du prochain envoi** – date et heure de la prochaine tentative de l'envoi de la notification. La périodicité des tentatives d'envoi est spécifiée lors de la configuration des notifications dans la rubrique [Configuration des notifications](#). Après l'envoi d'une notification, il n'est pas possible de modifier la périodicité de tentatives de l'envoi pour cette notification.
 - **Destinataire** – adresses de destinataires de la notification.
 - **Erreur** – erreur qui empêche l'envoi de la notification.
4. Pour gérer les notifications non envoyées :
 - a) Cochez les cases contre les notifications concrètes ou la case dans l'en-tête du tableau des notifications pour sélectionner toutes les notifications de la liste.
 - b) Utilisez les boutons suivants de la barre d'outils :
 -  **Envoyer encore une fois** – envoyer immédiatement les notifications sélectionnées. Dans ce cas, une tentative supplémentaire d'envoi de la notification sera entreprise. En cas d'échec d'envoi, le nombre des tentatives restantes va diminuer d'une tentative et l'heure de la prochaine va être calculée du moment de l'envoi actuel avec la périodicité spécifiée dans la rubrique [Configuration des notifications](#).
 -  **Supprimer** – supprimer toutes les notifications non envoyées sans possibilité de restauration.



5. Les notifications non envoyées sont supprimées de la liste sans les cas suivants :
 - a) La notification a été envoyée avec succès au destinataire.
 - b) La notification a été supprimée manuellement par l'administrateur avec le bouton **Supprimer** dans la barre d'outils.
 - c) Nombre de tentatives d'envoi est dépassé et la notification n'a pas été envoyée.
 - d) Dans la rubrique [Configuration des notifications](#) le bloc des notifications a été supprimé selon paramètres duquel les notifications ont été envoyées.

8.8. Gestion du dépôt du Serveur Dr.Web

Le dépôt des produits du Serveur Dr.Web est destiné à sauvegarder les échantillons standard du logiciel ainsi que leurs mises à jour depuis les Serveurs du SGM.

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 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 effectue une synchronisation des révisions du produit de manière suivante :

- a) vers le Serveur Dr.Web depuis le site de mise à jour du produit (via le protocole HTTP),
- b) entre les divers Serveurs Dr.Web dans une configuration multi-serveurs (conformément à la politique d'échange adoptée),
- c) depuis le Serveur Dr.Web vers les postes de travail.

Le dépôt 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.

À l'heure actuelle, le jeu de produits comprend les produits listés ci-dessous :

- Serveur Dr.Web,



- Agents Dr.Web (logiciel de l'Agent, logiciel antivirus du poste de travail pour les systèmes d'exploitation correspondants),
- Serveur proxy Dr.Web,
- Bases virales Dr.Web,
- Bases SplDer Gate,
- Bases de l'Antispam Dr.Web,
- Actualités de Doctor Web.


8.8.1. Statut du dépôt

Pour voir l'état du dépôt ou mettre à jour les composants du réseau antivirus :

1. Choisissez l'onglet **Administration** dans le menu principal du Centre de gestion et cliquez sur **Statut du dépôt des produits** dans le menu de gestion.
2. Dans la fenêtre qui s'ouvre, vous pouvez voir la liste des produits du dépôt, la date de la révision utilisée, la date de la dernière révision téléchargée et le statut des produits.



Dans la colonne **Statut**, vous pouvez consulter le statut des produits du dépôt du Serveur au moment de la dernière mises à jour.

3. Pour gérer les contenus du dépôt, utilisez les boutons suivants :
 - Cliquez sur **Vérifier les mises à jour** pour voir si des mises à jour sont disponibles sur les serveurs SGM et pour les télécharger.
 - Cliquez sur  **Recharger le dépôt depuis le disque**, pour charger la version actuelle du dépôt du disque.

Au démarrage, le Serveur charge les contenus du dépôt en mémoire. Si durant le fonctionnement du Serveur, l'administrateur a modifié les contenus sans tenir compte du Centre de gestion, par ex, en mettant à jour le dépôt avec un utilitaire externe ou manuellement, rechargez le dépôt pour utiliser la version téléchargée.

8.8.2. Mises à jour reportées

Dans la rubrique **Mises à jour reportées**, vous pouvez voir la liste des produits dont la mise à jour est temporairement désactivée sur la page suivante **Configuration détaillée du dépôt** → *<Produit>* → [Mises à jour reportées](#). Une révision différée est considérée comme *gelée*.

Le tableau des produits gelés contient les informations suivantes :

- **Répertoire du dépôt** – nom du répertoire dans lequel se trouve un produit gelé :
 - 10-drwgatedb – Bases SplDer Gate,
 - 10-drwspamdb – Bases AntiSpam,
 - 20-drwagent – Agent Dr.Web pour Windows,
 - 20-drwandroid – Agent Dr.Web pour Android,



- 20-drwcs – Serveur Dr.Web,
- 20-drwunix – Agent Dr.Web pour UNIX,
- 80-drwnews – actualités de Doctor Web.
- **Révision** – numéro de la révision gelée.
- **Reportée à** – Temps auquel la mise à jour du produit est reportée.

Lorsque vous cliquez sur une ligne du tableau, un autre tableau donnant des informations détaillées sur les mises à jour gelées des produits correspondants s'ouvre.

L'option de report des mises à jour est utile si vous devez temporairement annuler la distribution de la dernière mise à jour d'un produit sur tous les postes du réseau antivirus, par ex, si vous souhaitez d'abord tester cette mise à jour sur un nombre limité de postes.

Pour utiliser les fonctions de report de mises à jour, effectuez les actions décrites à la section **Configuration détaillée du dépôt** → [Mises à jour reportées](#).

Pour gérer les mises à jour reportées :

1. Cochez les cases près des produits pour lesquels vous souhaitez indiquer des actions sur les mises à jour reportées. Pour sélectionner tous les produits, cochez la case dans le titre du tableau des produits gelés.
2. Dans la barre d'outils, choisissez les actions souhaitées :
 - ✔ **Exécuter immédiatement** - désactiver l'état "gelé" du produit et ajouter la mise à jour à la liste des révisions à distribuer sur les postes d'après la [Procédure](#) générale.
 - ✘ **Annuler la mise à jour** – désactiver l'état « gelé » du produit et empêcher la mise à jour. La mise à jour via le SGM sera restaurée. La révision non gelée sera supprimée de la liste des mises à jour du produit. Au moment de la réception de la prochaine révision, la révision gelée sera supprimée du disque.
 - 🕒 **Modifier le délai de mise à jour** – indiquez un nouveau délai de report de la mise à jour du produit. La révision est gelée du moment de la réception de la prochaine révision du SGM.
3. Si vous n'avez spécifié aucune action de suppression du statut "gelé", la révision devient "dé-gelée" lorsque le délai spécifié dans la liste **Délai d'attente de mises à jour** s'écoule. Alors la révision est débloquée automatiquement et elle est incluse à la liste des révisions distribuées aux postes d'après la [Procédure](#) générale.





8.8.3. Configuration générale du dépôt

Dans la rubrique **Configuration générale du dépôt**, vous pouvez indiquer les paramètres de connexion au SGM et de mise à jour des dépôts de tous les produits.

Pour modifier la configuration du dépôt :

1. Sélectionnez l'élément **Administration** du menu principal du Centre de gestion.



2. Dans la fenêtre qui s'ouvre, choisissez l'onglet **Configuration générale du dépôt des produits** dans le menu de gestion.
3. Configurez tous les paramètres nécessaires pour la mise à jour depuis le SGM comme décrit [ci-dessous](#).
4. Si durant la modification des paramètres vous devez supprimer tous les changements effectués, utilisez les boutons suivants dans la barre d'outils :
 -  **Restaurer les valeurs initiales de tous les paramètres** – restaurer les valeurs de tous les paramètres avant modification. Pour appliquer la même action à un paramètre en particulier, utilisez le bouton  contre chaque paramètre.
 -  **Restaurer tous les paramètres dans leurs valeurs par défaut** – restaurer toutes les valeurs par défaut des paramètres spécifiées dans le fichier de configuration du Serveur. Pour appliquer la même action à un paramètre en particulier, utilisez le bouton  contre chaque paramètre.
5. Cliquez sur un des boutons suivants dans la barre d'outils :
 - **Enregistrer et resynchroniser** – sauvegarder toutes les modifications et mettre à jour le dépôt depuis le SGM conformément aux nouveaux paramètres.
 - **Enregistrer et recharger depuis le disque** – sauvegarder toutes les modifications sans mettre à jour le dépôt depuis le SGM. Ainsi, la version actuelle du dépôt est rechargée depuis le disque (voir aussi la rubrique [Statut du dépôt](#)).



Configuration du SGM Dr.Web

Dans l'onglet **SGM Dr.Web**, vous pouvez configurer les paramètres de connexion au Système Global de Mise à jour.

Pour modifier les paramètres de connexion au SGM, utilisez les options suivantes :

- **URI de base** – répertoire se trouvant sur les serveurs des mises à jour contenant les mises à jour des produits Dr.Web.
- Cochez la case **Utiliser CDN** pour autoriser l'utilisation de Content Delivery Network lors du chargement du dépôt.
- Cochez la case **Utiliser SSL** pour effectuer le chargement du dépôt via la connexion sécurisée SSL.

Dans ce cas, dans la liste déroulante **Certificats autorisés**, le type des certificats SSL qui seront appliqués automatiquement.

- Si cela est nécessaire, éditez la liste des serveur du SGM depuis lesquels la mises à jour du dépôt s'effectue dans la section Liste des serveurs du **Système global de mise à jour Dr.Web** :
 - Pour ajouter un serveur SGM à la liste des serveurs utilisés pour les mises à jour, cliquez sur  et indiquez l'adresse du serveur SGM dans le champ qui apparaît.
 - Pour supprimer un serveur SGM de la liste, cliquez sur  contre le serveur que vous souhaitez supprimer.



- Les serveurs SGM sont listés dans l'ordre dans lequel le Serveur Dr.Web les contacte lors de la mise à jour du dépôt. Pour modifier l'ordre des serveurs SGM, déplacez un serveur nécessaire en faisant glisser la ligne racine de gauche du serveur.

Au moment de l'installation du Serveur Dr.Web, seuls les serveurs de Doctor Web sont présents dans la liste. Si cela est nécessaire, vous pouvez configurer vos propres zones de mises à jour et les ajouter dans la liste des serveurs pour obtenir les mises à jour.

Configuration des mises à jour de l'Agent Dr.Web

Les mises à jour du logiciel de l'Agent et du package antivirus sont configurées séparément pour les différentes versions de l'OS sous lequel ce logiciel sera installé :

- Dans l'onglet **Agent Dr.Web pour Windows**, indiquez si vous souhaitez mettre à jour tous les composants qui seront installés sur les postes sous Windows ou mettre à jour uniquement les base de données virales.
- Dans l'onglet **Agent Dr.Web pour UNIX**, indiquez les OS UNIX pour lesquels vous voulez mettre à jour les composants installés sur les postes.



Pour désactiver complètement la réception des mises à jour depuis le SGM pour l'Agent pour UNIX, passez dans la rubrique **Configuration détaillée du dépôt des produits**, l'élément **Agent Dr.Web pour UNIX**, l'onglet **Synchronisation** et cochez la case **Désactiver la mise à jour du produit**.

Configuration des mises à jour du Serveur Dr.Web

Dans l'onglet **Serveur Dr.Web**, indiquez les OS pour lesquels vous voulez mettre à jour les fichiers du Serveur :

- Pour recevoir les mises à jour des Serveurs sous tous les OS supportés, cochez la case **Mettre à jour toutes les plateformes disponibles sur le SGM**.
- Pour recevoir les mises à jour du Serveur uniquement sous certains OS supportés, cochez les cases contre ces OS.




Pour désactiver complètement la réception des mises à jour depuis le SGM pour le Serveur, passez dans la rubrique **Configuration détaillée du dépôt des produits**, l'élément **Serveur Dr.Web**, l'onglet **Synchronisation** et cochez la case **Désactiver la mise à jour du produit**.

Actualités de Doctor Web

Dans l'onglet **Actualités de Doctor Web**, indiquez la liste des langues pour le flux d'actualités.

Vous pouvez configurer les paramètres d'abonnement aux actualités dans la section [Préférences](#) → **Abonnement**.



Vous pouvez consulter les actualités de Doctor Web dans le menu principal du Centre de gestion, dans la section  **Aide** → **Actualités**.

Langues de l'Agent Dr.Web pour Windows

Dans l'onglet **Langues de l'Agent Dr.Web pour Windows**, spécifiez la liste des langues de l'interface de l'Agent et du package antivirus pour Windows qui seront téléchargées depuis le SGM.

8.8.4. Configuration détaillée du dépôt

La rubrique **Configuration détaillée du dépôt** offre des options de configuration des mises à jour de chaque dépôt de produit séparément.



Pour modifier la configuration du dépôt :

1. Sélectionnez l'élément **Administration** du menu principal du Centre de gestion.
2. Dans la fenêtre qui s'ouvre, choisissez la sous-rubrique **Configuration détaillée du dépôt** du menu de gestion puis le produit que vous souhaitez modifier.
3. Configurez les paramètres du dépôt nécessaires, décrits [ci-dessous](#).
4. Cliquez sur **Sauvegarder et recharger depuis le disque** dans la barre d'outils pour sauvegarder les modifications. Ainsi, la version actuelle du dépôt est rechargée du disque (voir aussi [Statut du dépôt](#)).










Liste des révisions

Dans l'onglet **Liste des révisions**, vous pouvez voir toutes les révisions disponibles sur le Serveur pour un produit.

Le tableau des révisions contient les colonnes suivantes :

Nom de la colonne	Description
Distribuée	<p>Un marqueur automatique, dans cette colonne, définit l'état des mises à jour des produits. Deux types de marqueurs sont disponibles :</p> <p> – <i>Révision distribuée</i>. La révision est utilisée pour la mise à jour des Agents et du logiciel antivirus sur les postes.</p> <p>La révision à distribuer est sélectionnée comme suit :</p> <ol style="list-style-type: none">1. La révision accompagnée du marqueur  dans la colonne Actuelle est distribuée. Seule une révision peut être marquée. Pour le produit Agent Dr.Web pour Windows, une révision reçue avant la version distribuée ne peut pas être marquée.



Nom de la colonne	Description
	<p>2. Si aucune révision n'est marquée dans la colonne Actuelle, la dernière révision accompagnée du marqueur  dans la colonne Stockée est distribuée.</p> <p>3. Si aucune révision n'est marquée dans les colonnes Actuelle et Stockée, la dernière révision est distribuée.</p> <p>Le marqueur automatique désigne toujours la révision distribuée.</p> <p>  – <i>Révision gelée</i>. Cette révision n'est pas distribuée aux postes, les nouvelles révisions ne sont pas téléchargées du Serveur. Pour plus d'information sur les actions en cas de révision gelée, voir Mises à jour reportées.</p> <p>Si une révision est gelée, la révision à distribuer est sélectionnée comme suit :</p> <ol style="list-style-type: none">1. Si le marqueur  est sélectionné dans le colonne Actuelle, la révision actuelle est distribuée aux postes.2. Si le marqueur  n'est pas sélectionné dans la colonne Actuelle, c'est la révision précédente la révision actuelle qui est distribuée aux postes.
Actuelle	<p>Sélectionnez le marqueur  pour indiquer la révision utilisée pour la mise à jour des Agents et du logiciel antivirus sur les postes de travail.</p> <p>Seule une révision peut être marquée.</p> <p>De même, un marqueur indiquant la révision actuelle peut ne pas être sélectionné.</p>
Stockée	<p>Sélectionnez le marqueur  pour sauvegarder la révision lorsque le dépôt est nettoyé automatiquement.</p> <p>Le marqueur peut être sélectionné pour différentes révisions simultanément.</p> <p>De même, un marqueur peut ne pas être sélectionné.</p> <p>Le Serveur stocke un certain nombre de mises à jour de produits spécifié à l'onglet Synchronisation. Lorsque le nombre maximum de révisions stockées est atteint, la révision la plus anciennement stockée est supprimée lors de la sauvegarde d'une nouvelle révision, téléchargée du SGM.</p> <p>Lorsque le dépôt est nettoyé automatiquement, les révisions suivantes ne sont pas supprimées :</p> <ul style="list-style-type: none">• Les révisions accompagnées du marqueur  dans la colonne Stockée.• La révision accompagnée du marqueur  dans la colonne Actuelle. <p>Si la mise à jour du produit est stable, vous pouvez l'indiquer comme stockée et si une nouvelle révision, téléchargée du SGM, est instable, vous pourrez revenir à la révision précédente.</p>
Révision	La date de réception de la révision du produit.



Nom de la colonne	Description
	Si la révision est bloquée, le statut de blocage s'affiche dans cette colonne.

Synchronisation

Dans l'onglet **Synchronisation**, vous pouvez configurer les paramètres de mise à jour du dépôt du Serveur depuis le SGM :

- Dans la liste déroulante **Nombre de révisions stockées**, vous pouvez spécifier le nombre de révisions temporairement stockée sur le disque. La valeur indiquée n'inclut pas les révisions marquées au moins dans une colonne dans l'onglet **Liste des révisions**. Lorsqu'une nouvelle révision est réceptionnée et que le nombre de révisions stockées a atteint son maximum, la plus ancienne révision est supprimée. Les révisions marquées comme **Actuelle** et **Stockée** et **Distribuée** ne sont pas supprimées.
- Cochez la case **Désactiver la mise à jour du produit** pour ne plus recevoir de mises à jour des serveurs SGM pour ce produit. Les Agents seront mis à jour vers la révision actuelle sur le Serveur (ou selon la [procédure](#) utilisée pour sélectionner la révision distribuée).

Pour certains produits, les paramètres suivants sont disponibles :

- Cochez la case **Mettre à jour uniquement les fichiers suivants** pour recevoir les mises à jour du SGM uniquement pour les fichiers listés.
- Cochez la case **Ne pas mettre à jour uniquement les fichiers suivants** pour désactiver la mise à jour depuis le SGM uniquement pour les fichiers listés.

Les fichiers peuvent être sélectionnés dans un format d'expressions régulières.

Si les deux cases sont cochées, les fichiers à mettre à jour sont sélectionnés comme suit :

1. Dans la liste complète des fichiers des produits, seuls sont sélectionnés les fichiers indiqués dans la liste **Mettre à jour uniquement les fichiers suivants**.
2. Depuis la sélection à l'étape 1, les fichiers indiqués dans la liste **Ne pas mettre à jour uniquement les fichiers suivants** sont supprimés.
3. Les fichiers résultant de la sélection à l'étape 2 sont mis à jour depuis le SGM.

Notifications

A l'onglet **Notifications**, vous pouvez configurer les notifications concernant les mises à jour du dépôt :

- Cochez la case **Ne pas notifier uniquement sur ces fichiers**, pour désactiver les notifications sur les événements liés aux fichiers listés ci-dessous.
- Cochez la case **Notifier uniquement sur ces fichiers** pour activer les notifications sur les événements liés aux fichiers listés.

Les fichiers peuvent être sélectionnés dans un format d'expressions régulières.



Si aucune liste d'exceptions n'est dressée, toutes les notifications activées à la rubrique [Configuration des notifications](#) sont envoyées.

Les paramètres des notifications sur les mises à jour du dépôt sont configurés à la page Notifications, à la rubrique **Dépôt**.

Mises à jour reportées

Dans l'onglet **Mises à jour reportées**, vous pouvez reporter la distribution des mises à jour sur les postes pour un certain délai. Une révision reportée est considérée comme gelée.

L'option de report des mises à jour est utile si vous avez besoin d'annuler temporairement la distribution de la dernière révision du produit sur tous les postes du réseau antivirus, par ex, si vous souhaitez tester au préalable cette révision sur un nombre limité de postes.

Pour utiliser les fonctions de mises à jour reportées, faites comme suit :

1. Si vous souhaitez geler une mise à jour pour un produit, configurez les mises à jour reportées comme décrit [ci-dessous](#).
2. Pour désactiver la distribution de la dernière révision, indiquez une des révisions précédentes comme actuelle dans l'onglet [Liste des révisions](#).
3. Pour un groupe de postes qui recevra la dernière révision, cochez la case **Recevoir toutes les dernières mises à jour** dans la rubrique **Réseau antivirus** → [Restrictions de mises à jour des postes](#). Les autres postes recevront les révisions que vous avez indiquées comme actuelles à l'étape 2.
4. La prochaine révision téléchargée du SGM qui satisfait aux conditions requises à l'option **Reporter les mises à jour uniquement pour les fichiers suivants**, sera bloquée et reportée dans le délai indiqué dans la liste **Délai de report des mises à jour**.



Pour configurer les mises à jour reportées :

1. Cochez la case **Différer les mises à jour** pour désactiver temporairement le téléchargement des mises à jour des serveurs SGM pour le produit.
2. Dans la liste déroulante **Période de report des mises à jour**, sélectionnez la période à laquelle reporter le téléchargement des mises à jour, à partir de leur réception des serveurs SGM.
3. Si nécessaire, cochez la case **Différer les mises à jour uniquement pour les fichiers suivants** pour reporter la distribution des mises à jour contenant des fichiers correspondant aux masques spécifiés. Les masques sont indiqués au format d'expressions régulières.

Si la case n'est pas cochée, toutes les mises à jour du SGM sont bloquées.



Pour désactiver le blocage :

- Dans l'onglet **Liste des révisions**, cliquez sur  **Exécuter immédiatement** pour désactiver le blocage du produit et ajouter la révision à la liste des révisions distribuées aux postes conformément à la [procédure](#) générale.
- Dans l'onglet **Liste des révisions**, cliquez sur  **Annuler la mise à jour** pour désactiver le blocage du produit et empêcher la révision. La mise à jour depuis le SGM sera restaurée. La révision non bloquée sera supprimée de la liste des révisions du produit. Après la réception de la prochaine révision, la révision non bloquée sera supprimée du disque.
- Lorsque la période indiquée dans la liste **Heure de report des mises à jour** est dépassée, la révision sera débloquée et est incluse à la liste des révisions distribuées aux postes selon la [procédure](#) générale.

Vous pouvez gérer les révisions gelées pour tous les produits à la page [Mises à jour reportées](#).

8.8.5. Contenu du dépôt

La rubrique **Contenu du dépôt des produits** permet de consulter et gérer le contenu actuel du dépôt au niveau de répertoires et de fichiers du dépôt.

La fenêtre principal de la rubrique **Contenu du dépôt des produits** contient l'arborescence du dépôt représentant tous les répertoires et les fichiers de la version actuelle du dépôt avec la liste de toutes les révisions existantes pour chaque produit.

Voir les informations sur le dépôt

Pour consulter les informations sur les objets du dépôt sélectionnez un objet dans l'arborescence du contenu du dépôt. Le panneau de propriété contenant les informations suivantes va s'ouvrir :


- La section **Objets sélectionnés** contient des informations détaillées sur l'objet sélectionné dans l'arborescence du contenu du dépôt : **Type**, **Taille** (pour les objets particuliers), **Date de création** et **Date de modification**.
- La sous-rubrique **Contenu du dépôt des produits** contient les informations générales sur tous les objets du dépôt des produits : liste courante des objets et date de leur dernière modification.

Gestion du dépôt

Pour gérer le contenu du dépôt, utilisez les boutons suivants de la barre d'outils :

 [Exporter des fichiers de dépôt vers une archive](#),

 [Importer une archive avec des fichiers de dépôt](#),

 **Supprimer les objets sélectionnés** – supprimer les objets sélectionnés dans l'arborescence du contenu du dépôt sans possibilité de restauration.



Après la modification du contenu du dépôt, par exemple en cas de suppression ou d'importation des objets du dépôt, il est nécessaire de redémarrer le dépôt pour que le Serveur puisse utiliser les données modifiées.

Voir la rubrique [Contenu du dépôt des produits](#).

Exportation du dépôt

Pour enregistrer les fichiers du dépôt en archive zip, exécutez les actions suivantes :

1. Dans l'arborescence du contenu du dépôt, sélectionnez un produit, une révision particulière ou le dépôt entier. Le dépôt entier sera exporté, si rien n'est sélectionné dans l'arborescence ou que l'en-tête de l'arborescence **Dépôt** est sélectionné. Pour sélectionner plusieurs objets, utilisez les touches CTRL ou SHIFT.

Lors de l'exportation des objets du dépôt, prenez en compte les types principaux des objets exportés :

- a) Archives zip des produits du dépôt. Les archives pareilles contiennent un des types suivants des objets du dépôt :


- Dépôt entier.
- Produit entier.
- Révision entière du produit.

Les archives obtenues lors de l'exportation des données des objets peuvent être [importées](#) via la rubrique **Contenu du dépôt des produits**. Les noms de ces archives ont le préfixe `repository_`.

- b) Archives zip des fichiers particuliers du dépôt.

Les archives obtenues lors de l'exportation des fichiers particuliers et des répertoire se trouvant dans l'arborescence au-dessous des objets du p. **a)** ne peuvent pas être importées via la rubrique **Contenu du dépôt des produits**. Les noms de ces archives ont le préfixe `files_`.

Ces archives peuvent être utilisées en tant que copies de sauvegarde des fichiers pour le remplacement manuel. Pourtant il est recommandé de ne pas remplacer les fichier du dépôt manuellement sans faire recours à la rubrique **Contenu du dépôt des produits**.


2. Cliquez sur le bouton  **Exporter des fichiers de dépôt vers une archive** dans la barre d'outils.
3. La spécification du chemin de sauvegarde de l'archive zip avec l'objet sélectionné s'effectue conformément aux paramètres du navigateur web dans lequel le Centre de gestion est ouvert.

Importation du dépôt

Pour charger les fichiers du dépôt depuis une archive zip, exécutez les actions suivantes :

1. Cliquez sur  **Importer une archive avec des fichiers de dépôt** dans la barre d'outils.



2. Dans la fenêtre qui s'ouvre **Sélectionnez un fichier**, spécifiez l'archive zip avec les fichiers du dépôt. Pour sélectionner un fichier, utilisez le bouton .

On peut importer seulement les archives zip obtenues lors de l'exportation d'un des types suivants des objets du dépôt :

- Dépôt entier.
- Produit entier.
- Révision entière du produit.

Lors de l'exportation, le nom des archives pareilles contient le préfixe `repository_`.

3. Dans la rubrique **Importer les paramètres**, configurez les paramètres suivants :
 - **Ajouter uniquement les révisions manquantes** – dans ce mode d'importation, seules les révisions du dépôt manquantes dans la version actuelle seront ajoutées. Les autres révisions demeurent inchangées.
 - **Remplacer le dépôt entièrement** – dans ce mode d'importation, le dépôt est entièrement remplacé par le dépôt importé.
 - Cochez la case **Importer les fichiers de configuration** pour importer les fichiers de configuration lors de l'importation du dépôt.
4. Cliquez sur le bouton **Importer** pour commencer l'importation.

8.9. Options supplémentaires

8.9.1. Gestion de la base de données

La rubrique **Gestion de la base de données** permet de maintenir la base de données avec laquelle fonctionne le Serveur Dr.Web.

La section **Général** contient les paramètres suivants :

- Le champ **Dernière maintenance de la BD** – la date de la dernière exécution de commandes de maintenance de la base de données de cette rubrique.
- La liste de commandes de maintenance de la base de données contient :
 - Commandes analogues aux tâches de la [planification du Serveur Dr.Web](#). Les noms de commandes correspondent aux noms de tâches de la rubrique **Actions** dans la planification du Serveur (les tâches correspondantes de la planification sont décrites dans le tableau [Types de tâches et leurs paramètres](#)).
 - Commande **Analyse de la base de données**. Cette commande est destinée à optimiser la base de données du Serveur via l'exécution de la commande `analyze`.

Pour exécuter les commandes de maintenance de la base de données, procédez comme suit :

1. Dans la liste de commandes cochez les cases contre les commandes que vous voulez exécuter.



Si nécessaire, modifiez les délais de temps pour les commandes d'effacement de la base de données, après lesquels l'information sauvegardée est considérée comme obsolète et doit être supprimée du Serveur.

2. Cliquez sur **Appliquer maintenant**. Toutes les commandes seront exécutées tout de suite.

Pour l'exécution automatique reportée et/ou périodique de ces commandes (sauf la commande **Analyse de la base de données**), utiliser le [Planificateur des tâches du Serveur](#).

Pour gérer la base de données, utilisez les boutons situés dans la barre d'outils :


 [Importer](#),

 [Exporter](#),

 [Copie de sauvegarde](#).

Exportation de la base de données

Pour enregistrer l'information de la base de données dans un fichier, effectuez les actions suivantes :

1. Dans la barre d'outils , cliquez sur le bouton **Exporter**.
2. Dans la fenêtre des paramètres d'exportation, sélectionnez une des variantes :
 - **Exporter toute la base de données** pour enregistrer toute l'information de la base de données dans l'archive gz. Le fichier XML obtenu lors de l'exportation est analogue au fichier d'exportation de la base de données obtenu lors du lancement du fichier exécutable du Serveur depuis la ligne de commande avec la clé `xmlexportdb`. Ce fichier d'exportation peut être importé lors du lancement du fichier exécutable du Serveur depuis la ligne de commande avec la clé `xmlimportdb`.
Ces commandes sont décrites en détails dans les **Annexes**, dans la rubrique [H4.3. Commandes de gestion de la BD](#).
 - **Exporter les informations sur les postes et les groupes** pour enregistrer les informations sur les objets du réseau antivirus dans l'archive zip. En cas d'exécution de cette opération, toute l'information sur les groupes de postes et les comptes des postes du réseau antivirus maintenu par ce Serveur est sauvegardée dans un fichier au format spécial. Le fichier d'exportation comprend les informations suivantes sur les postes : propriétés, configuration des composants, droits, paramètres de limitations de mises à jour, planification, liste des composants à installer, statistiques, informations sur les postes supprimés, sur les groupes : propriétés, configuration des composants, droits, paramètres de limitations de mises à jour, planification, liste des composants à installer, statistiques, identificateur du groupe parent.
Ensuite le fichier d'exportation peut être [importé](#) via la rubrique **Gestion de la base de données**.
3. Cliquez sur le bouton **Exporter**.
4. La spécification du chemin de sauvegarde de l'archive avec la base de données s'effectue conformément aux paramètres du navigateur web dans lequel le Centre de gestion est ouvert.





Importer la base de données

La procédure de l'importation du fichier de la base de données contenant les informations sur les objets du réseau antivirus peut être utilisée pour transmettre les informations sur un nouveau Serveur, ainsi que sur un Serveur qui fonctionne déjà au sein du réseau antivirus, notamment pour fusionner les listes de postes maintenus de deux Serveurs.



Tous les postes, les informations sur lesquels sont importées, peuvent se connecter au Serveur sur lequel l'importation est effectuée. En cas d'importation, prenez en compte la nécessité d'avoir une quantité suffisante des licences disponibles pour la connexion des postes transférés. Par exemple, si nécessaire, dans la rubrique [Gestionnaire de licences](#) ajoutez une clé de licence depuis le Serveur duquel les informations sur les postes sont transférés.

Pour charger une base de données depuis un fichier, procédez comme suit :

1. Dans la barre d'outils, cliquez sur le bouton  **Importer**.
2. Dans la fenêtre d'importation, spécifiez l'archive zip avec le fichier de la base de données. Pour sélectionner un fichier, utilisez le bouton .

On peut importer seulement les archives zip obtenus lors de l'exportation de la base de données pour la variante **Exporter les informations sur les postes et les groupes**.

3. Cliquez sur le bouton **Importer** pour commencer l'importation.
4. Si lors de l'import sont détectés les postes et/ou les groupes ayant le même identificateur, inclus dans les données à importer et ainsi que dans la base de données du Serveur actuel, la rubrique **Collisions** va s'afficher pour déterminer les actions à appliquer sur les objets doublés.

Les listes des groupes et des postes sont présentés dans des tableaux différents.


Sélectionnez une variante de résolution d'une collision dans la liste déroulante **Mode de l'importation des groupes** ou **Mode de l'importation des postes** pour le tableau des objets correspondant :

- **Enregistrer les données de l'importation pour tous** – supprimer de la base de données du Serveur actuel toutes les informations sur les objets doublés et réécrire la base de données avec les informations de la base de données importée. L'action s'applique à tous les objets doublés de ce tableau en même temps.
- **Enregistrer les données actuelles pour tous** – sauvegarder dans la base de données du Serveur actuel toutes les informations sur les objets doublés. Les informations sur les objets doublés de la base de données importée seront ignorées. L'action s'applique à tous les objets doublés de ce tableau en même temps.
- **Sélectionnez manuellement** – spécifier manuellement une action pour chaque objet doublé en particulier. Dans ce mode, vous pourrez éditer la liste des objets doublés. Spécifiez les options contre les objets qui seront sauvegardés.

Cliquez sur **Sauvegarder**.



Copie de sauvegarde

Pour créer une copie de sauvegarde de données critiques du Serveur, cliquez sur  **Copie de sauvegarde** dans la barre d'outils. Les données seront sauvegardées dans une archive gz. Les fichiers obtenus lors de la copie de sauvegarde sont analogues aux fichiers obtenus lors du lancement du fichier exécutable du Serveur depuis la ligne de commande avec la clé `backup`.

Vous pouvez consulter la description détaillée de cette commande dans les **Annexes**, rubrique [H4.5. Copie de sauvegarde des données critiques du Serveur Dr.Web.](#)

8.9.2. Statistiques du Serveur Dr.Web

A l'aide du Centre de gestion vous pouvez consulter les statistiques du fonctionnement du Serveur Dr.Web au niveau de l'utilisation des ressources système de l'ordinateur sur lequel le Serveur Dr.Web est installé et de l'interaction avec les composant du réseau antivirus et les ressources externes comme SGM.

Pour consulter les statistiques du fonctionnement du Serveur Dr.Web :

1. Sélectionnez l'élément **Administration** du menu principal du Centre de gestion.
2. Dans la fenêtre qui s'affiche, sélectionnez l'élément du menu de gestion **Statistiques du Serveur Dr.Web**.
3. Dans la fenêtre qui s'affiche, sont présentées les rubriques suivantes de données statistiques :
 - **Activité des clients** – les données relatives à la quantité des clients servis qui sont connectés à ce Serveur : des Agents Dr.Web, des Serveurs Dr.Web voisins et des installateurs des Agents Dr.Web.
 - **Trafic réseau** – paramètres du trafic entrant et sortant lors de l'échange des données avec le Serveur.
 - **Utilisation des ressources système** – paramètres d'utilisation des ressources système de l'ordinateur sur lequel le Serveur est installé.
 - **Microsoft NAP** – paramètres du fonctionnement de [Dr.Web NAP Validator](#).
 - **Utilisation de la base de données** – paramètres de connexion à la base de données du Serveur.
 - **Utilisation du cache de fichiers** – paramètres de l'appel au cache de fichiers de l'ordinateur sur lequel le Serveur est installé.
 - **Utilisation du cache DNS** – paramètres de l'appel au cache qui sauvegarde les requêtes au serveurs DNS de l'ordinateur sur lequel le Serveur est installé.
 - **Notifications** – paramètres de fonctionnement du sous-système de [notifications](#) de l'administrateur.
 - **Dépôt** – paramètres de l'échange de données du dépôt du Serveur avec les serveurs du SGM.
 - **Statistiques Web** – paramètres de l'appel au Serveur Web.



- **Cluster** – paramètres d'appels via le protocole de synchronisation entre les serveurs en cas d'utilisation du cluster de Serveurs dans la configuration multi-serveurs du réseau.
4. Pour consulter les données statistiques d'une rubrique en particulier, cliquez sur le nom de la rubrique nécessaire.
 5. Dans la liste qui s'affiche sont présentés les paramètres de la rubrique avec les compteurs dynamiques de valeurs.
 6. En même temps, quand la rubrique de statistiques ouvre, la représentation graphique des modifications pour chaque paramètre est activée. Dans ce cas :
 - Pour désactiver la représentation graphique, cliquez sur le nom de la rubrique nécessaire. En cas de désactivation de la représentation graphique, la valeur numérique de paramètres sera actualisée d'une façon dynamique.
 - Pour réactiver la représentation graphique de données, cliquez encore une fois sur le nom de la rubrique nécessaire.
 - Les noms des rubriques et de leurs paramètres pour lesquels la représentation graphique est activée sont en gras.
 7. Pour modifier la périodicité d'actualisation des paramètres, utilisez les outils suivants du panneau de configuration :
 - Dans la liste déroulante **Périodicité d'actualisation** sélectionnez le délai nécessaire d'actualisation de données. En cas de modification de la valeur de la liste déroulante, le nouveau délai d'actualisation des données numériques et graphiques s'applique automatiquement.
 - Cliquez sur **Actualiser** pour actualiser toutes les valeurs de données statistiques en même temps.
 8. Si vous passez la souris sur les données graphiques, une valeur numérique du point sélectionné s'affiche sous forme de :
 - **Abs** – valeur absolue du paramètre.
 - **Delta** – accroissement de la valeur du paramètre par rapport à sa valeur précédente conformément à la périodicité de la mise à jour de données.
 9. Pour masquer les paramètres de la rubrique, cliquez sur la flèche à droite du nom de la rubrique. Quand les paramètres de la rubrique sont masqués, la représentation graphique des statistiques se vide et n'apparaît qu'en cas d'une nouvelle ouverture.

8.10. Particularités du réseau avec plusieurs Serveurs Dr.Web

Dr.Web Enterprise Security Suite permet de créer un réseau antivirus avec plusieurs Serveurs Dr.Web. 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 optimale de la charge sur le Serveur.

Pour les échanges d'information entre les Serveurs le *protocole spécial de synchronisation entre serveurs* est utilisé.



Fonctionnalités fournies par le protocole de la synchronisation entre serveurs :

- Distribution des mises à jour entre les Serveurs au sein d'un réseau antivirus.
- Rapidité de diffusion des mises à jour après leur réception des serveurs du SGM Dr.Web.
- Transfert des statistiques sur le statut des postes protégés entre les Serveurs liés.
- Transfert des licences pour les postes protégés entre les Serveurs voisins.

8.10.1. Structure du réseau avec plusieurs Serveurs Dr.Web

Le réseau antivirus permet d'installer plusieurs Serveurs Dr.Web. Ainsi, chaque Agent Dr.Web 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 Dr.Web.

Le Serveur Dr.Web peut transmettre à un autre serveur Dr.Web 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 du SGM Dr.Web ;
- informations sur les événements viraux, statistiques relatives au fonctionnement etc.
- licences pour les postes protégés (le transfert des licences entre les Serveurs est configuré dans le [Gestionnaire de licences](#)).

Dr.Web Enterprise Security Suite comprend deux types de liaisons entre les Serveurs Dr.Web :

- *liaison de type supérieur-subordonné*, dans ce cas-là, le supérieur transfère les mises à jour au subordonné et reçoit des informations sur les événements,
- *liaison 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.

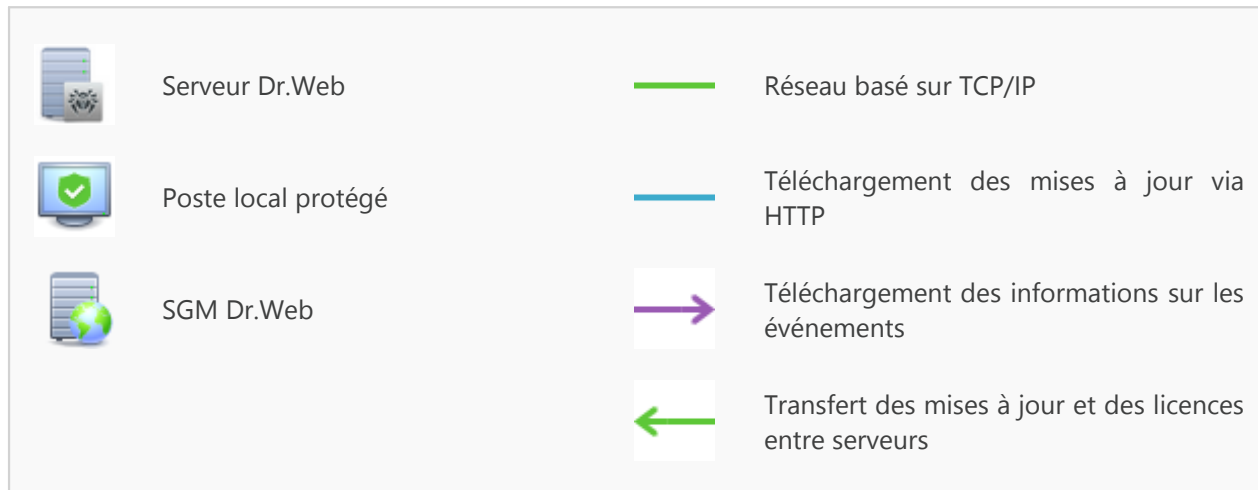
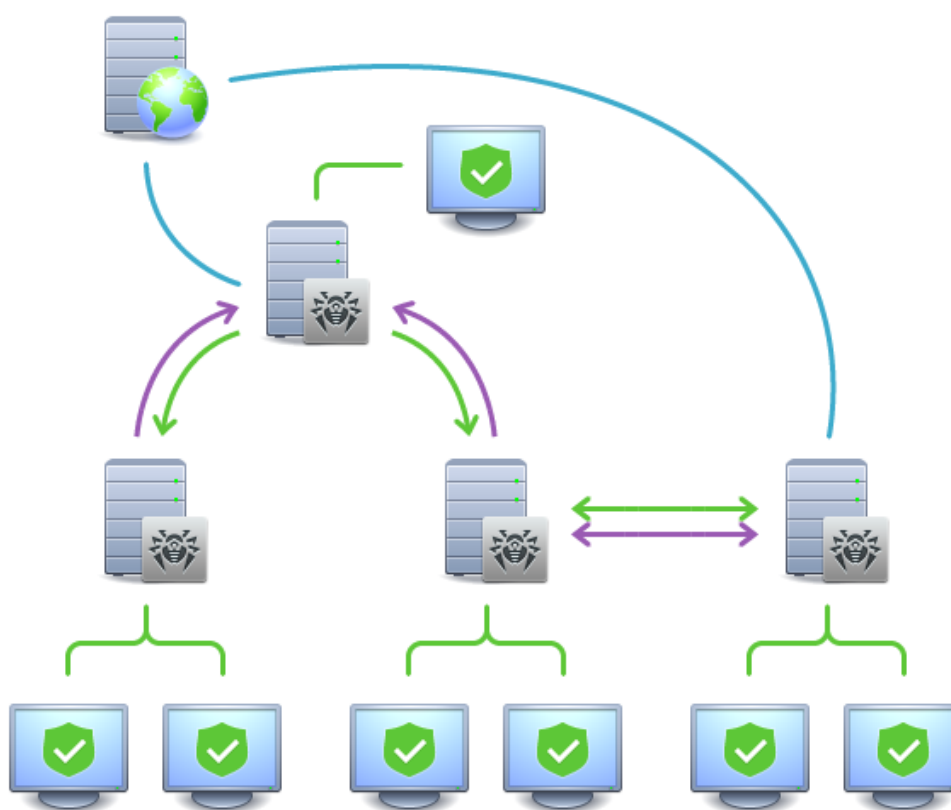


Figure 8-1. Réseau avec plusieurs Serveurs

Certains avantages du réseau avec plusieurs Serveurs Dr.Web :

1. Possibilité de recevoir les mises à jour depuis les Serveurs SGM Dr.Web via l'un des Serveurs Dr.Web afin de les transmettre plus tard directement vers d'autres Serveurs ou par intermédiaires.



Les Serveurs recevant les mises à jour du Serveur supérieur ne reçoivent pas les mises à jour depuis le SGM même si cette tâche est spécifiée dans la planification.

Pourtant, il est recommandé de laisser la tâche de mise à jour depuis les serveurs du SGM dans la planification du Serveur subordonné pour le cas où le Serveur principal serait temporairement indisponible. Cela permettra aux Agents connectés au Serveur subordonné, de recevoir la mise à jour des bases virales et des modules du logiciel (voir aussi, le p. [Configuration générale du dépôt](#)).



Dans la tâche de mise à jour depuis le SGM sur le Serveur principal qui distribue les mises à jour, il est nécessaire de spécifier la réception des mises à jour du logiciel de serveur pour tous les systèmes d'exploitation installés sur tous les Serveurs subordonnés qui reçoivent les mises à jour depuis le Serveur principal (voir le p. [Configuration générale du dépôt](#)).

2. Possibilité de répartir les postes de travail sur plusieurs Serveurs afin de diminuer la charge sur chacun d'entre eux.
3. 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 informations.

4. Possibilité de transmettre les licences disponibles de protection des postes sur le Serveur voisin. Dans ce cas, la clé de licence reste en disposition du Serveur de distribution. Les licences disponibles sont délivrées au Serveur voisin pour un délai de temps spécifié, après l'expiration duquel elles sont révoquées.

8.10.2. Configuration des liaisons entre Serveurs Dr.Web

Pour configurer un réseau avec plusieurs Serveurs, il est nécessaire de configurer des liaisons entre eux.

Il est recommandé, tout d'abord, de planifier 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 les Serveurs « voisins » (les Serveurs « voisins » sont liés au moins par un flux d'information).

Exemple de configuration d'une connexion entre serveurs supérieur et subordonné Serveur Dr.Web :



Les valeurs des champs marqués du symbole *, doivent être obligatoirement spécifiées.


1. Assurez-vous que les deux Serveurs Dr.Web sont opérationnels.







- Attribuez à chaque Serveur Dr.Web un nom mnémorique afin d'éviter d'éventuelles erreurs lors de la configuration de la connexion et de la gestion des Serveurs Dr.Web. Pour ce faire, ouvrez le menu du Centre de gestion **Administration** → **Configuration du Serveur Dr.Web**, l'onglet **Général**, le champ **Nom du Serveur Dr.Web**. Dans cet exemple, le nom du Serveur principal est `MAIN`, le nom du serveur subordonné est `AUXILIARY`.
- Activez le protocole serveur sur les deux Serveurs Dr.Web. Pour cela, dans le menu du Centre de gestion, sélectionnez l'élément **Administration** → **Configuration du Serveur Dr.Web**, puis dans l'onglet **Modules**, cochez la case **Protocole du Serveur Dr.Web** (voir le paragraphe [Modules](#)).



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.

- Redémarrez les deux Serveur Dr.Web.
- Via le Centre de gestion du Serveur subordonné (`AUXILIARY`), ajoutez le Serveur principal (`MAIN`) dans la liste des Serveurs voisins. Pour ce faire, sélectionnez l'élément **Liaisons** dans le menu principal. La fenêtre contenant l'arborescence des Serveurs voisins du réseau antivirus s'ouvrira. Pour ajouter un Serveur dans la liste, cliquez sur le bouton  **Créer une liaison** dans la barre d'outils.


La fenêtre de description des liaisons entre le Serveur existant et le Serveur ajouté va s'ouvrir. Spécifiez les paramètres suivants :

- **Type** du réseau créé – **Principal**.
- **Nom** – nom du Serveur principal (`MAIN`).
- **Mot de passe*** – mot de passe aléatoire pour accéder au Serveur principal.
- **Clés propres du Serveur Dr.Web** – liste des clés publiques de chiffrement du Serveur à configurer. Cliquez sur le bouton  et sélectionnez la clé `drwcds.pub` correspondant au Serveur actuel. Pour ajouter encore une clé, cliquez sur  et ajoutez la clé dans le nouveau champ.
- **Clés d'un Serveur Dr.Web voisin*** – liste des clés publiques de chiffrement du Serveur principal connecté. Cliquez sur le bouton  et sélectionnez la clé `drwcds.pub` correspondant au Serveur principal. Pour ajouter encore une clé, cliquez sur  et ajoutez la clé dans le nouveau champ.
- **Adresse*** – adresse réseau du Serveur principal et port de connexion. Spécifiée au format `<adresse_du_Serveur> : <port>`.

Il est possible de rechercher la liste des Serveurs disponibles dans le réseau. Pour cela :

- Cliquez sur la flèche se trouvant à droite du champ **Adresse**.
- 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 disponibles dans le réseau va commencer.
- d) Sélectionnez un Serveur dans la liste des Serveurs disponibles. Son adresse sera enregistrée dans le champ **Adresse** pour créer une liaison.
- **Adresse du Centre Gestion Sécurité Dr.Web** – vous pouvez saisir l'adresse de la page d'accueil du Centre de gestion pour le Serveur principal (voir le paragraphe [Centre de gestion de la sécurité Dr.Web](#)).
 - Dans la liste déroulante **Paramètres de connexion**, le principe de la connexion des Serveurs du réseau créé est spécifié.
 - Dans la liste déroulante **Chiffrement** et **Compression**, spécifiez les paramètres du chiffrement et de la compression du trafic entre les Serveurs connectés (voir le p. [Utilisation du chiffrement et de la compression du trafic](#)).
 - **Durée de validité des licences distribuées** – délai pour lequel les licences sont délivrées depuis la clé sur le Serveur principal. La configuration est utilisée si le Serveur principal délivre les licences au Serveur actuel.
 - **Délai d'acceptation du renouvellement de licences** – ce paramètre n'est pas utilisé lors de la création d'une liaison du Serveur principal.
 - **Période de synchronisation de licences** – périodicité de synchronisation des informations sur les licences délivrées entre les Serveurs.
 - Les cases dans les rubriques **Licences**, **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 licences vers le Serveur subordonné ;
 - le Serveur principal envoie les mises à jour vers le Serveur subordonné ;
 - le Serveur subordonné envoie des informations sur les événements vers le Serveur principal.
 - Dans la section **Restrictions de mise à jour** → **Événements**, vous pouvez spécifier la planification de transfert des événements du Serveur actuel au Serveur subordonné (l'édition du tableau **Restrictions de mises à jour** est effectuée de la même manière que l'édition du tableau de planification dans la section [Restrictions de mises à jour des postes](#)).

Cliquez sur **Enregistrer**.

Ainsi, le Serveur principal (MAIN) sera inclus dans les dossiers **Principaux** et **Déconnectés** (voir [fig. 8-2](#)).

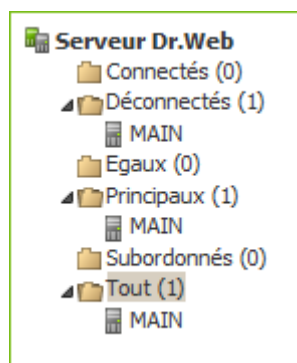


Figure 8-2.



6. Ouvrez le Centre de gestion du Serveur principal (MAIN) et ajoutez le Serveur subordonné (AUXILIARY) dans la liste des Serveurs voisins. 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 un Serveur dans la liste, cliquez sur le bouton **Créer une liaison** dans la barre d'outils.

La fenêtre de description des liaisons entre le Serveur existant et le Serveur ajouté va s'ouvrir. Spécifiez les paramètres suivants :

- **Type** du réseau créé – **Subordonné**.
- **Nom** – nom du Serveur subordonné (AUXILIARY).
- **Mot de passe*** – entrez le même mot de passe que celui indiqué dans le p. 5.
- **Clés propres du Serveur Dr.Web** – liste des clés publiques de chiffrement du Serveur à configurer. Cliquez sur le bouton et sélectionnez la clé `drwcsd.pub` correspondant au Serveur actuel. Pour ajouter encore une clé, cliquez sur et ajoutez la clé dans le nouveau champ.
- **Clés d'un Serveur voisin Dr.Web*** – liste des clés publiques de chiffrement du Serveur subordonné connecté. Cliquez sur le bouton et sélectionnez la clé `drwcsd.pub` correspondant au Serveur subordonné. Pour ajouter encore une clé, cliquez sur et ajoutez la clé dans le nouveau champ.
- **Adresse du Centre Gestion Sécurité Dr.Web** – vous pouvez saisir l'adresse de la page d'accueil du Centre de gestion pour le Serveur subordonné (voir le p. [Centre de gestion de la sécurité Dr.Web](#)).
- Dans la liste déroulante **Paramètres de connexion**, le principe de la connexion des Serveurs du réseau créé est spécifié.
- Dans la liste déroulante **Chiffrement** et **Compression**, spécifiez les paramètres du chiffrement et de la compression du trafic entre les Serveurs connectés (voir le p. [Utilisation du chiffrement et de la compression du trafic](#)).
- **Durée de validité des licences distribuées** – ce paramètre n'est pas utilisé lors de la création d'une liaison du Serveur subordonné.
- **Délai d'acceptation du renouvellement de licences** – période jusqu'à la fin de laquelle et à commencer par laquelle, le Serveur subordonné démarre le renouvellement de la licence obtenue du Serveur actuel. La configuration est utilisée si le Serveur subordonné obtient des licences du Serveur actuel.
- **Période de synchronisation de licences** – périodicité de synchronisation des informations sur les licences délivrées entre les Serveurs.
- Les cases dans les rubriques **Licences**, **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 licences du Serveur principal ;
 - le Serveur subordonné reçoit les mises à jour du Serveur principal ;
 - le Serveur subordonné envoie des informations sur les événements sur le Serveur principal.



- Dans la section **Restrictions de mise à jour** → **Mises à jour**, vous pouvez spécifier la planification de transfert des mises à jour du Serveur actuel au Serveur subordonné (l'édition du tableau **Restrictions de mises à jour** est effectuée de la même manière que l'édition du tableau de planification dans la rubrique [Restrictions de mises à jour des postes](#)).

Cliquez sur **Enregistrer**.

Ainsi, le Serveur subordonné (AUXILIARY) sera inclus dans les dossiers **Subordonnés** et **Déconnectés** (voir la [fig.8-3](#)).

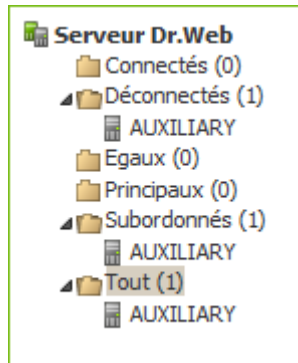


Figure 8-3.

7. 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 **Déconnectés** vers le dossier **Connectés** (voir la [fig. 8-3](#)).

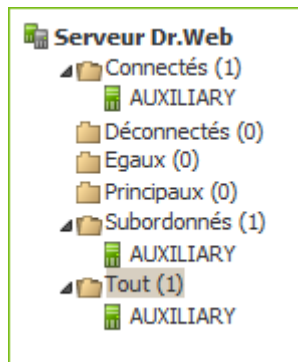


Figure 8-3.

8. Ouvrez le Centre de gestion du Serveur subordonné (AUXILIARY) et assurez-vous que le Serveur principal (MAIN) est bien connecté au serveur subordonné (AUXILIARY) (voir [fig.8-4](#)).

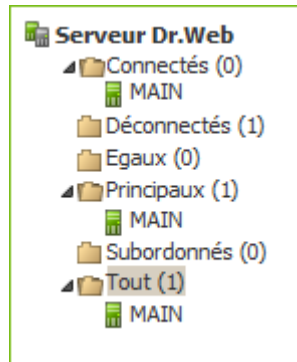


Figure 8-4.



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 Server dans les cas suivants :

- Problème de connexion via le réseau.
- Adresse invalide du Serveur principal spécifiée lors de la configuration de la connexion.
- Les clés publiques de chiffrement `drwcsd.pub` spécifiées sur un des Serveurs sont invalides.
- Mot de passe invalide sur un des Serveurs (les mots de passe ne correspondent pas sur les Serveurs à lier).

8.10.3. Utilisation du réseau antivirus avec plusieurs Serveurs Dr.Web

Une des particularités du réseau à plusieurs Serveurs consiste en l'obtention des mises à jour depuis le SGM Dr.Web via une partie des Serveurs Dr.Web (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 p. [Configuration de la planification du Serveur Dr.Web](#)). Tout Serveur recevant des mises à jour depuis les Serveurs du SGM 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 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 **Statistiques** 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
 -  **Sauvegarder les données dans un fichier CSV,**
 -  **Sauvegarder les données dans un fichier HTML,**
 -  **Sauvegarder les données dans un fichier XML,**
 -  **Sauvegarder les données dans un fichier PDF.**



8.10.4. Cluster des Serveurs Dr.Web



La mise à jour des Serveurs au sein d'un cluster doit être effectuée uniquement depuis les packages d'installation. Dans ce cas, il faut arrêter tous les Serveurs et les mettre à jour l'un après l'autre. Il ne faut pas utiliser la mise à jour via le Centre de gestion (passage vers la nouvelle révision), car en cas d'utilisation de la base de données commune, après la mise à jour du premier Serveur, les autres Serveurs ne pourront pas fonctionner et se mettre à jour.

Lors de la création du cluster des Serveurs Dr.Web dans le réseau antivirus, il faut respecter les conditions suivantes :

1. Mêmes fichiers de configuration

Tous les Serveurs doivent avoir les mêmes clés de chiffrement `drwcsd.pub` et `drwcsd.pri`.

Si les clés de chiffrement n'ont pas été créées avant, elles seront générées automatiquement lors de l'installation du premier Serveur du cluster.

Vous pouvez obtenir les clés de chiffrement nécessaires pour l'installation des autres Serveurs du cluster via le Centre de gestion : menu **Administration** → **Clés de chiffrement**. En fonction du déploiement du cluster, les deux clés peuvent être requises ou une seule clé `drwcsd.pri` :

- Si la clé de chiffrement privé `drwcsd.pri` est spécifiée lors de l'installation du Serveur, la clé de chiffrement publique `drwcsd.pub` est générée automatiquement.
- Si vous n'avez pas spécifié la clé privé nécessaire lors l'installation du Serveur, il faut remplacer les deux clés manuellement après l'installation.



Vous pouvez consulter le placement des fichiers de configuration dans la rubrique [Serveur Dr.Web](#).

2. Nom unique du Serveur

L'adresse IP et le nom DNS du Serveur doivent être les mêmes pour tous les Serveurs. Ils sont utilisés pour générer les fichiers d'installation de l'Agent sur les postes du réseau antivirus.

Ce nom est spécifié via le Centre de gestion: **Administration** → **Configuration du Serveur Dr.Web** → onglet **Réseau** → onglet [Téléchargement](#) → champ **Adresse du Serveur Dr.Web**. Les paramètres de cette section sont sauvegardés dans le fichier de configuration `download.conf` (vous trouverez la description du fichier dans le document **Annexes**, p. [G3. Fichier de configuration download.conf](#)).

3. Configuration de l'utilisation du cluster

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.

Pour appliquer automatiquement les paramètres dans le cluster des Serveurs Dr.Web, il faut utiliser le protocole spécial du cluster.



Pour configurer le protocole de cluster pour chaque Serveur dans le Centre de gestion, ouvrez le menu **Administration** → **Configuration du Serveur Dr.Web** et spécifiez les paramètres suivants :

- a) Pour activer le protocole du cluster, cochez la case **Protocole du cluster des Serveurs Dr.Web** dans l'onglet [Modules](#).
- b) Pour configurer les paramètres d'interaction des Serveurs au sein d'un cluster, spécifiez les paramètres suivants dans l'onglet [Cluster](#).
- c) Après avoir spécifié tous les paramètres nécessaires, cliquez sur le bouton **Sauvegarder** et redémarrez les Serveurs.

Exemple

- Groupe multicast : 232.0.0.1
- Port : 11111
- Interface : 0.0.0.0

Dans cet exemple, les transports pour toutes les interfaces sont configurés pour tous les Serveurs du cluster. Dans les autres cas, par exemple, quand un des réseaux est externe par rapport au cluster et les Agents se connectent via ce réseau et le deuxième réseau est interne, il vaut mieux ouvrir le protocole du cluster uniquement pour les interfaces du réseau interne. Dans ce cas, il faut spécifier les adresses du type 192.168.1.1, ..., 192.168.1.N en tant qu'interfaces.

4. Base de données commune



Pour pouvoir fonctionner avec une seule base de données, tous les Serveurs Dr.Web doivent avoir la même version.

Tous les Serveurs Dr.Web au sein d'un cluster doivent fonctionner avec la seule base de données.

Comme dans le cas de l'utilisation de la base de données sans l'organisation du cluster, chaque Serveur s'adresse à la base de données indépendamment et toutes les données des Serveurs sont sauvegardées séparément. Là où cela est valable, le Serveur prend dans la base de données seulement les entrées liées à son ID qui est unique pour chaque Serveur. L'utilisation d'une base de données unique permet aux Serveurs d'utiliser les Agents qui ont été d'abord enregistrés sur d'autres Serveurs du cluster.

Lors de la création d'un cluster des Serveurs avec la base de données unique, veuillez prendre en compte les particularités suivantes :

- La base de données peut être installée séparément de tous les Serveurs ou sur un des ordinateurs sur lequel est installé le Serveur du cluster.
- La base de données doit être créée avant l'installation du premier Serveur du cluster ou avant la connexion du premier Serveur à la base de données.
- Lors de l'ajout de nouveaux nœuds au cluster (excepté le premier Serveur) pendant l'installation des Serveurs, il n'est recommandé de spécifier la base de données unique qui est utilisée dans ce cluster. Sinon les informations qui sont déjà sauvegardées dans ce cluster peuvent être supprimées. Il est recommandé d'installer les Serveurs avec la base de données



interne et, après l'installation, les connecter à la base de données externe unique.

Vous pouvez connecter les Serveurs à la base de données externe via le Centre de gestion : menu **Administration** → **Configuration du Serveur Dr.Web** → onglet [Base de données](#) ou via le fichier de configuration des Serveurs `drwcsd.conf`.

- Il n'est pas recommandé d'ajouter à un cluster des Serveurs qui fonctionnent déjà dans le réseau antivirus avec une autre base de données interne ou externe (excepté le premier Serveur du cluster). Cela peut provoquer la perte de données : des informations sur les postes, sur les statistiques et sur les paramètres (sauf les paramètres sauvegardés dans les fichiers de configuration), car les données dans la base sont complètement supprimées lors de l'importation. Dans ce cas, seule l'importation partielle de certains paramètres est possible.

5. Une version du dépôt

Sur tous les Serveurs du cluster, les dépôts doivent contenir les mises à jours de la même version.

Vous pouvez satisfaire à cette condition d'une des façons suivantes :

- Mettre à jour tous les Serveurs du cluster depuis le SGM en même temps. Dans ce cas, tous les Serveurs auront la dernière version des mises à jour. Vous pouvez configurer la mise à jour des dépôts de tous les Serveurs depuis la zone locale des mises à jour. Dans ce cas, une version approuvée des mises à jour sera diffusée depuis la zone locale ou, en cas de création du miroir du SGM, ce sera la dernière version des mises à jour.
- Il est possible de créer la structure hybride associant le cluster des Serveurs et la structure hiérarchique à la base des liaisons voisines. Ainsi, un des Serveurs (un Serveur du cluster ou un Serveur non inclus au cluster) est désigné comme principal et il obtient les mises à jour depuis le SGM. Les autres Serveurs du cluster sont considérés comme subordonnés et ils obtiennent les mises à jour par les liaisons voisines depuis le Serveur principal.

En cas de configuration de la mise à jour des Serveurs du cluster depuis la zone locale (le miroir du SGM) ou depuis le Serveur principal, il est nécessaire de surveiller le fonctionnement de cette zone ou du Serveur principal. Si le nœud diffusant les mises à jour tombe en panne, il est nécessaire de reconfigurer un des Serveurs et le désigner Serveur principal ou créer une nouvelle zone des mises à jour pour obtenir des mises à jour depuis le SGM.

6. Particularités de la diffusion des licences sur les postes

Pour diffuser les licences sur les Serveurs du cluster vous pouvez agir d'une des façons suivantes :

- a) Créer une structure hybride associant le cluster des Serveurs et la structure hiérarchique à la base des liaisons voisines. Cette structure sera utile si pendant le fonctionnement des Agents au sein d'un système de cluster des Serveurs, il y a une répartition dynamique des postes entre les Serveurs du cluster. Dans ce cas, le nombre nécessaire des licences est diffusé par les liaisons voisines depuis le Serveur principal (cela peut être un Serveur du cluster ou un Serveur non inclus dans le cluster) sur les Serveurs subordonnés pendant le fonctionnement.



Ainsi, il suffit de placer sur le Serveur principal un fichier de licence contenant le nombre suffisant de licences correspondant au nombre total des postes servis et de diffuser le nombre nécessaire de licences sur les Serveurs subordonnés pendant le fonctionnement du cluster. C'est l'administrateur du réseau antivirus qui configure manuellement la diffusion des licences sur les Serveurs subordonnés pour un délai nécessaire.

Pour configurer la diffusion des licences sur les Serveurs voisins, utilisez le [Gestionnaire de licence](#).

Par exemple, vous pouvez configurer la structure hiérarchique des Serveurs et déterminer le Serveur principal (cela peut être un Serveur du cluster ou un Serveur non inclus dans le cluster) qui va distribuer les mises à jour du dépôt et les licences depuis le fichier de licences sur tous les nœuds du cluster.

- b) En cas de refus de la configuration de la structure hiérarchique des Serveurs, il n'est pas possible de partager les licences entre tous les Serveurs depuis un fichier de licence unique. Dans ce cas, il faut planifier la structure du réseau antivirus à l'avance en fonction de la disponibilité du cluster des Serveurs et utiliser plusieurs fichiers de licence : un fichier pour chaque Serveur du cluster. Le nombre total des licences dans tous les fichiers de licence est égal au nombre des postes sur le réseau, pourtant il faut calculer à l'avance la répartition du nombre des licences sur les Serveurs du cluster en fonction du nombre supposé des postes que vous comptez connecter à chaque Serveur.

7. Tâches dans la planification des Serveurs

Pour exclure la duplication des requêtes à la BD, il est recommandé d'exécuter les tâches suivantes de la planification du Serveur seulement sur un des Serveurs : **Purge Old Data**, **Backup sensitive data**, **Purge old stations**, **Purge expired stations**, **Purge unsent IS events** Par exemple, sur le Serveur qui est placé sur le même ordinateur que la base de données externe ou sur le plus puissant ordinateur du cluster, si les configurations des Serveurs sont différentes et la base de données est installée sur un ordinateur à part.



Chapitre 9. Mise à jour des composants de Dr.Web Enterprise Security Suite



Avant de procéder à la mise à jour de Dr.Web Enterprise Security Suite 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 au SGM Dr.Web (voir le p. [Configuration générale du dépôt](#)).

9.1. Mise à jour du Serveur Dr.Web et restauration depuis une copie de sauvegarde

Le Centre de gestion fournit les fonctionnalités suivantes de gestion du logiciel du Serveur Dr.Web :

- Mise à niveau du logiciel du Serveur vers une des versions disponibles, téléchargées depuis le SGM et stockées dans le dépôt du Serveur. Les paramètres de la mise à jour du dépôt depuis le SGM sont décrits dans la rubrique [Gestion du dépôt du Serveur Dr.Web](#).
- Recul du logiciel du Serveur vers la copie de sauvegarde. Les copies de sauvegarde du Serveur sont créés automatiquement lors du passage vers la nouvelle version dans la rubrique **Mises à jour du Serveur Dr.Web** (étape 4 dans la procédure ci-dessous).



Vous pouvez également mettre à jour le Serveur au sein de la version 10 avec la distribution du Serveur. La procédure est décrite dans le **Manuel d'installation**, dans la rubrique [Mise à jour du Serveur Dr.Web sous OS Windows®](#) ou [Mise à jour du Serveur Dr.Web sous les OS de la famille UNIX®](#).

Pas toutes les mises à jour du Serveur au sein de la version 10 contiennent le fichier de distribution. Certaines d'entre elles peuvent être installées uniquement via le Centre de gestion.

Lors de la mise à jour du Serveur sous OS de la famille UNIX via le Centre de gestion, la version du Serveur dans le gestionnaire de paquets de l'OS ne changera pas.

Pour gérer le logiciel du Serveur Dr.Web :

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion, et dans la fenêtre qui s'ouvre, choisissez l'élément **Serveur Dr.Web** dans le menu de gestion.
2. Pour passer à la liste des versions du Serveur, effectuez une des actions suivantes :



- Cliquez sur la version actuelle du Serveur dans la fenêtre principale.
 - Cliquez sur **Liste des versions**.
3. La rubrique **Mises à jour du Serveur Dr.Web** va s'afficher contenant la liste des mises à jour disponibles et des copies de sauvegarde du Serveur. Ainsi :
 - Dans la liste **Version actuelle** est indiquée la version du Serveur utilisée en ce moment. La rubrique **Liste des modifications** contient la brève liste des nouvelles fonctionnalités et la liste des erreurs corrigées dans cette version par rapport à la version précédente.
 - La liste **Toutes les versions** contient la liste des mises à jour pour ce Serveur téléchargées depuis le SGM. La rubrique **Liste des modifications** contient la brève liste des nouvelles fonctionnalités et des erreurs corrigées pour chaque composant. Pour la version qui précède l'installation initiale du Serveur depuis le package d'installation, la rubrique **Liste des modifications** est vide.
 - La liste **Copies de sauvegarde** contient la liste des copies de sauvegarde, faites pour ce Serveur. Dans la rubrique **Date** sont indiquées les informations sur la date de la copie de sauvegarde.
 4. Pour mettre à niveau le logiciel du Serveur, placez l'option contre la version nécessaire du Serveur dans la liste **Toutes les versions** et cliquez sur **Sauvegarder**.



Vous pouvez faire la mise à niveau uniquement vers la version plus récente du Serveur par rapport à la version utilisée en ce moment.

En cours de la mise à niveau du Serveur la version actuelle est sauvegardée en tant que copie de sauvegarde (placée dans la rubrique **Copies de sauvegarde**), et la version, vers laquelle la mises à niveau s'effectue est déplacée de la rubrique **Toutes les versions** vers la rubrique **Version actuelle**.

Les copies de sauvegarde sont sauvegardées dans le répertoire suivant :

```
var → update_backup_<ancienne_version>_<nouvelle_version>.
```

Lors de la mise à niveau, le fichier de journal `var → dwupdater.log` est créé, complété.

5. Pour faire reculer le logiciel du Serveur, placez l'option contre la version nécessaire du Serveur dans la liste **Copies de sauvegarde** et cliquez sur **Sauvegarder**.

Lors du recul du logiciel du Serveur, la copie de sauvegarde vers laquelle le passage s'effectue, est placée dans la rubrique **Version actuelle**.



9.2. Mise à jour manuelle des composants de Dr.Web Enterprise Security Suite


Vérification de la disponibilité des mises à jour depuis le SGM


Marche à suivre pour vérifier les mises à jour des produits Dr.Web Enterprise Security Suite sur le serveur de mises à jour :


1. Choisissez l'onglet **Administration** dans le menu principal du Centre de gestion et cliquez sur **Statut du dépôt des produits** dans le menu de gestion.
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 du SGM, cliquez sur le bouton **Vérifier les mises à jour**.
3. Si un composant vérifié est obsolète, 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 du Serveur Dr.Web](#)).

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** 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 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.

9.3. Mise à jour selon la planification

Vous pouvez planifier des tâches sur le Serveur afin d'effectuer des mises à jour régulières du logiciel (Pour en savoir plus sur la planification, voir le p. [Configuration de la planification du Serveur Dr.Web](#)).



Pour planifier l'exécution de la tâche de la mise à jour sur le Serveur Dr.Web :

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion, dans la fenêtre qui s'affiche, sélectionnez l'élément du menu de gestion **Planification des tâches du Serveur Dr.Web**. La liste actuelle des tâches du Serveur va s'ouvrir.
2. Pour ajouter une tâche dans la liste, cliquez sur le bouton  **Nouvelle tâche** dans la barre d'outils. Une fenêtre d'édition de la tâche va s'ouvrir.
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, cochez les cases près des produits à mettre à jour via cette tâche.
6. Passez à l'onglet **Heure** et dans la liste déroulante, indiquez une périodicité de lancement de la tâche, puis configurez l'heure selon la périodicité sélectionnée.
7. Pour enregistrer les modifications, cliquez sur **Enregistrer**.

9.4. Mise à jour du dépôt du Serveur Dr.Web non connecté à Internet

9.4.1. Copier le dépôt d'un autre Serveur Dr.Web

Si le Serveur Dr.Web n'est pas connecté à Internet, vous pouvez mettre à jour le dépôt manuellement en copiant le dépôt d'un autre Serveur mis à jour.



Cette manipulation n'est pas destinée à la migration du Serveur vers une nouvelle version.

Pour transférer les mises à jour du dépôt d'un autre Serveur Dr.Web :

1. Depuis la rubrique **Administration** → [Statut du dépôt](#) du Centre de gestion, mettez à jour le dépôt du Serveur connecté à Internet.
2. Depuis la rubrique [Contenu du dépôt](#) exportez le dépôt ou sa partie (les produits nécessaires) à l'aide du Centre de gestion. Dans ce cas, il est nécessaire de n'exporter que les types d'objets dont l'importation postérieure est supportée.
3. Copiez l'archive avec le dépôt exporté sur l'ordinateur avec le Serveur nécessitant les mises à jour.

Importez le dépôt téléchargé sur le Serveur via le Centre de gestion, depuis la rubrique **Administration** → [Contenu du dépôt](#).



Si vous utilisez les paramètres particuliers du dépôt, comme, par exemple, le blocage des révisions ou la mise à jour des Agents avec la révision spécifiée (pas la dernière), lors de l'importation du dépôt il est nécessaire d'activer l'option **Ajouter les révisions manquantes seulement** et désactivez l'option **Importer les fichiers de configuration**.



9.4.2. Chargeur du dépôt Dr.Web

S'il n'y a pas de possibilité de connecter un des Serveurs Dr.Web à Internet vous pouvez télécharger le dépôt depuis le SGM sans utiliser le logiciel du Serveur. Pour ce faire, l'utilitaire standard Chargeur du Dépôt Dr.Web est fourni.

Particularités de l'utilisation

- Pour télécharger le dépôt du SGM, vous avez besoin de la clé de licence de Dr.Web Enterprise Security Suite ou de son hash MD5 que vous pouvez trouver dans le Centre de gestion, dans la rubrique **Administration** → **Gestionnaire de Licences**.
- Le Chargeur du dépôt Dr.Web est disponible dans les versions suivantes :
 - [version graphique](#) de l'utilitaire (uniquement au sein de la version sous Windows),
 - [version console](#) de l'utilitaire.
- Pour télécharger le dépôt depuis le SGM, vous pouvez utiliser un serveur proxy.

Moyens d'utilisation possibles

Téléchargement avec le remplacement manuel du dépôt

1. Téléchargez le dépôt du Serveur depuis le SGM en utilisant l'utilitaire Chargeur du dépôt Dr.Web.

Lors du téléchargement, créez une archive du dépôt :

- a) Pour l'utilitaire graphique : sélectionnez le mode **Télécharger le dépôt** et cochez la case **Archiver le dépôt** dans la fenêtre principale de l'utilitaire.
- b) Pour l'utilitaire de console : utilisez la clé `--archive`.

2. Copiez l'archive avec le dépôt téléchargé sur l'ordinateur avec le Serveur Dr.Web nécessitant les mises à jour.

Importez le dépôt téléchargé sur le Serveur Dr.Web via le Centre de gestion, depuis la rubrique **Administration** → [Contenu du dépôt](#).



Si vous utilisez les paramètres particuliers du dépôt, comme, par exemple, le blocage des révisions ou la mise à jour des Agents avec la révision spécifiée (pas la dernière), lors de l'importation du dépôt il est nécessaire d'activer l'option **Ajouter les révisions manquantes seulement** et désactivez l'option **Importer les fichiers de configuration**.



Le mode de création du miroir des mises à jour est disponible uniquement dans le chargeur graphique de la dernière version que vous pouvez télécharger sur le site officiel de la société aux formats de la [version x64](#) et de la [version x32](#).



Création du miroir du dépôt sur le Serveur du réseau local

1. Téléchargez le dépôt du Serveur depuis le SGM en utilisant l'utilitaire graphique Chargeur du dépôt Dr.Web.
Lors du téléchargement, sélectionnez le mode **Synchroniser le miroir des mises à jour** dans la fenêtre principale de l'utilitaire.
2. Envoyez le dépôt téléchargé sur le serveur web de votre réseau local qui servira pour le partage des mises à jour du dépôt.
3. Dans la rubrique **Administration** → [Configuration générale du dépôt](#), configurez l'obtention des mises à jour par le Serveur Dr.Web depuis votre miroir local et non pas depuis les serveurs du SGM Dr.Web.



Assurez-vous que le miroir est placé dans le répertoire portant le nom 10.01.0. Dans ce cas, dans le champ **URI de base**, vous devez indiquer le chemin d'accès au répertoire sans indiquer le répertoire même.

9.4.2.1. Utilitaire graphique

La version graphique de l'utilitaire Chargeur du Dépôt Dr.Web peut être téléchargée via le Centre de gestion, depuis la rubrique **Administration** → **Utilitaires**. Vous pouvez lancer cette version de l'utilitaire sur n'importe quel ordinateur tournant sous Windows et ayant l'accès à Internet. Fichier exécutable – drwreloader-gui-*<version>*.exe.



Le mode de téléchargement des mises à jour et certaines rubriques des paramètres avancés sont disponibles uniquement dans la dernière version du chargeur que vous pouvez télécharger sur le site officiel de la société aux formats de la [version x64](#) et de la [version x32](#).

Pour télécharger le dépôt via la version graphique du Chargeur du dépôt Dr.Web, procédez comme suit :

1. Lancez la version graphique de l'utilitaire Chargeur du dépôt Dr.Web.
2. Dans la fenêtre principale de l'utilitaire, configurez les paramètres suivants :
 - a) **Clé de licence ou MD5 de la clé** – indiquez le fichier clé de licence Dr.Web. Pour ce faire, cliquez sur **Parcourir** et sélectionnez le fichier clé de licence valide. A la place de la clé de licence vous pouvez spécifier le hash MD5 de la clé de licence qui est visible dans le Centre de gestion, dans la rubrique **Administration** → **Gestionnaire de licence**.
 - b) **Répertoire de téléchargement** – spécifiez le répertoire dans lequel le dépôt sera téléchargé.
 - c) Dans la liste **Mode**, sélectionnez un des modes de téléchargement des mises à jour :
 - **Télécharger le dépôt** – le dépôt est téléchargé sous forme du dépôt du Serveur. Les fichiers téléchargés peuvent être importés via le Centre de gestion en tant que la mise à jour du dépôt du Serveur.



- **Synchroniser le miroir des mises à jour** – le dépôt est téléchargé sous forme de la zone des mises à jour du SGM. Les fichiers téléchargés peuvent être placés en miroir de mise à jour dans votre réseau local. Ensuite, les Serveurs peuvent être configurés pour recevoir des mises à jours directement depuis ce miroir de mise à jour contenant la dernière version du dépôt et non pas depuis les serveurs du SGM.
- d) Cochez la case **Archiver le dépôt** pour mettre automatiquement le dépôt téléchargé en archive zip. Cette option permet d'obtenir une archive du dépôt téléchargé prête à importer sur le Serveur avec le Centre de gestion de la rubrique **Administration** → [Contenu du dépôt des produits](#).
3. Si vous voulez modifier les paramètres supplémentaires de connexion au SGM et du téléchargement des mises à jour, cliquez sur **Paramètres avancés**. Dans la fenêtre qui s'affiche, les onglets suivants sont disponibles :
- a) Dans l'onglet **Produits**, vous pouvez modifier la liste des produits téléchargés. Dans la fenêtre de paramètre, vous pouvez consulter la liste de tous les produits du dépôt disponibles pour le téléchargement depuis le SGM :
- Pour actualiser la liste des produits disponibles en ce moment dans le SGM, cliquez sur **Actualiser**.
 - Cochez les cases contre les produits que vous voulez télécharger depuis le SGM ou la case dans l'en-tête du tableau pour sélectionner tous les produits de la liste.
- b) Dans l'onglet **SGM Dr.Web**, vous pouvez configurer les paramètres des serveurs de mises à jour :
- Les serveurs SGM sont listés dans l'ordre dans lequel l'utilitaire les contacte lors du téléchargement du dépôt. Pour modifier l'ordre des serveurs SGM, utilisez les boutons **En haut** et **En bas**.
 - Pour ajouter un serveur SGM dans la liste des serveurs utilisés lors du téléchargement, entrez l'adresse du Serveur SGM dans le champ au-dessus de la liste de serveurs et cliquez sur **Ajouter**.
 - Pour supprimer un serveur SGM de la liste de serveurs utilisés lors du téléchargement, sélectionnez le serveur à supprimer et cliquez sur **Supprimer**.
 - Dans le champ **URL de base**, est indiqué le répertoire se trouvant sur les serveurs SGM contenant les mises à jour des produits Dr.Web.
 - Dans la liste déroulante **Protocole**, sélectionnez le type de protocole pour obtenir les mises à jour depuis les Serveurs de mises à jour. Le téléchargement des mises à jour s'effectue conformément à la liste des serveurs du SGM pour tous les protocoles.
 - Dans la liste déroulante **Certificats autorisés**, sélectionnez le type des certificats SSL qui seront appliqués automatiquement. Ce paramètre est utilisé uniquement pour les protocoles sécurisés supportant le chiffrement.
 - **Login** et **Mot de passe** – identifiants de l'utilisateur utilisé pour l'authentification sur le Serveur des mises à jour, si le serveur exige l'authentification.
 - Cochez la case **Utiliser CDN** pour autoriser l'utilisation de Content Delivery Network lors du chargement du dépôt.



- c) Dans l'onglet **Proxy**, vous pouvez spécifier les paramètres de connexion au SGM via le serveur proxy :
- **Adresse du serveur proxy** et **Port** – adresse réseau et numéro du port du serveur proxy utilisé.
 - **Nom d'utilisateur** et **Mot de passe** – paramètres de l'authentification sur le serveur proxy, si ce serveur exige l'authentification.
- d) Dans l'onglet **Planificateur**, vous pouvez configurer la planification des mises à jour périodiques. Pour exécuter la planification, le planificateur de tâches Windows est utilisé. Dans ce cas, vous n'avez pas besoin de lancer l'utilitaire manuellement, le chargement du dépôt sera effectué automatiquement conformément à la périodicité spécifiée.
- e) Dans l'onglet **Journal**, vous pouvez configurer la journalisation des téléchargements des mises à jour.

Cliquez sur **OK** pour appliquer les modifications apportées et retourner dans la fenêtre principale du Chargeur de dépôt Dr.Web.

4. Après avoir modifié tous les paramètres, cliquez sur **Télécharger** dans la fenêtre principale du Chargeur du dépôt Dr.Web pour se connecter au SGM et commencer le téléchargement du dépôt.

9.4.2.2. Utilitaire console

La version console de l'utilitaire Chargeur du Dépôt Dr.Web est placée dans le sous-répertoire bin du répertoire d'installation du Serveur Dr.Web. Vous pouvez lancer cet utilitaire uniquement depuis ce répertoire du Serveur. Fichier exécutable – `drwreploder`.

Clés possibles

- `--help` – afficher l'aide sur les clés.
- `--show-products` – afficher la liste des produits du SGM.
- `--path <argument>` – télécharge le dépôt du SGM dans le dossier spécifié dans le paramètre `<argument>`.
- `--etc <arguments>` – chemin vers le répertoire `etc` du Serveur (utilisé pour rechercher les certificats racine et mettre à jour les clés publiques).
- `--archive` – archiver le dépôt.
- `--key <argument>` – chemin vers le fichier clé de licence (le fichier clé ou son hash MD5 doivent être indiqués).
- `--key-md5 <argument>` – Hash MD5 de la clé de licence (le fichier clé ou son hash MD5 doivent être indiqués).
- `--product <argument>` – produit mis à jour. Par défaut, le dépôt en entier est téléchargé.
- `--only-bases` – télécharger uniquement les bases virales.
- `--update-url <argument>` – répertoire se trouvant sur les serveurs du SGM contenant les mises à jour des produits Dr.Web (il est recommandé de laisser cette valeur par défaut).



- `--servers <argument>` – adresses des serveurs du SGM (il est recommandé de laisser cette valeur par défaut).
- `--prohibit-cdn` – interdire l'utilisation de CDN lors de téléchargement des mises à jour (désactivé par défaut, c'est-à-dire l'utilisation de CDN est autorisée).
- `--prohibit-ssl` – utiliser HTTP non sécurisé à la place de HTTPS (désactivé par défaut, c'est-à-dire HTTPS est utilisée).
- `--cert-mode [<argument>]` – accepter les certificats HTTPS automatiquement.
`<argument>` peut prendre une des valeurs suivantes :
 - `any` – accepter tous les certificats,
 - `valid` – accepter uniquement les certificats fiables,
 - `drweb` – accepter uniquement les certificats de Dr.Web.La valeur `drweb` est utilisée par défaut.
- `--proxy-host <argument>` – serveur proxy indiqué au format suivant : `<serveur> [: <port>]`.
- `--proxy-auth <argument>` – données d'authentification sur le serveur proxy : login et mot de passe utilisateur au format suivant : `<login> [: <mot de passe>]`.
- `--strict` – arrêter le chargement en cas d'erreur.
- `--log <argument>` – créer un fichier de journal au format des journaux du Serveur relatifs à la procédure de chargement du dépôt et le placer dans le repertoire spécifié par le paramètre `<argument>`.

Exemples d'utilisation

1. Pour créer une archive importée contenant tous les produits :

```
drwreploder.exe --path=C:\Temp\repository.zip --archive --key "C:\Program Files\DrWeb Server\etc\agent.key" --etc "C:\Program Files\DrWeb Server\etc"
```

2. Pour créer une archive importée contenant les bases virales :

```
drwreploder.exe --path=C:\Temp\repository.zip --archive --key "C:\Program Files\DrWeb Server\etc\agent.key" --only-bases --etc "C:\Program Files\DrWeb Server\etc"
```

3. Pour créer une archive importée contenant le Serveur seul :

```
drwreploder.exe --path=C:\Temp\repository.zip --archive --key "C:\Program Files\DrWeb Server\etc\agent.key" --product=20-drwcs --etc "C:\Program Files\DrWeb Server\etc"
```





Pour modifier le mode de mise à jour, cliquez sur le bloc correspondant dans le tableau :

- Pour modifier le mode de mise à jour pour une ligne (journée entière), cliquez sur la couleur correspondante dans la partie droite de la ligne du tableau.
- Pour modifier le mode de mise à jour pour une colonne (un intervalle de 15 minutes de chaque jour de la semaine), cliquez sur la couleur correspondante sous la colonne dans le tableau.

6. Après avoir apporté les modifications, cliquez sur **Sauvegarder** pour les appliquer.


Les options suivantes de gestion de la rubrique sont disponibles dans la barre d'outils :


 **Restaurer tous les paramètres à leur valeur initiale** – restaurer les valeurs données à tous les paramètres de cette rubrique avant modification (dernières valeurs sauvegardées).


 **Restaurer tous les paramètres à leur valeur par défaut** – restaurer les valeurs par défaut de tous les paramètres de la rubrique.

 **Diffuser les paramètres vers un autre objet** – copier les paramètres de cette rubrique sur un autre poste, un autre groupe ou plusieurs groupes et postes.

 **Configurer l'héritage des paramètres du groupe primaire** – supprimer les paramètres personnalisés d'un poste et configurer l'héritage des paramètres du groupe primaire.

 **Copier les paramètres du groupe primaire et les définir comme personnalisés** – copier les paramètres de cette rubrique du groupe primaire et les assigner à des postes sélectionnés. L'héritage n'est pas défini et les paramètres des postes sont considérés comme personnalisés.

 **Exporter les paramètres de cette rubrique vers un fichier** – sauvegarder tous les paramètres de cette rubrique dans un fichier au format spécifique.

 **Importer les paramètres de cette rubrique depuis un fichier** – remplacer tous les paramètres de cette rubrique par les paramètres du fichier au format spécifique.

9.6. Mise à jour des Agents mobiles Dr.Web

Si votre ordinateur, ordinateur portable ou l'appareil mobile ne sera pas connecté au Serveur Dr.Web pendant beaucoup de temps, afin de pouvoir recevoir les mises à jour depuis des Serveurs du SGM Dr.Web, il est recommandé d'installer sur le poste le mode mobile de l'Agent Dr.Web.

En mode mobile, 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'activation du mode mobile sera disponible dans les paramètres de l'Agent uniquement si l'utilisation du mode mobile est autorisée dans le Centre de gestion, dans la section **Réseau antivirus** → **Droits** → <systeme_d'exploitation> → **Général** → **Lancer en mode mobile**.



Lorsque l'Agent fonctionne en mode mobile, la connexion de l'Agent avec le Serveur Dr.Web est interrompue. Toutes les modifications pouvant être apportées sur le Serveur pour le



poste concerné entreront en vigueur dès que le mode mobile 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 mobile est activé.

La configuration des paramètres du mode mobile du côté de l'Agent est décrite dans le **Manuel Utilisateur**.



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 le Serveur Dr.Web et les Agents Dr.Web dans le cas où l'accès direct devient impossible (par exemple si le Serveur Dr.Web et les Agents Dr.Web se trouvent dans des réseaux différents entre lesquels il n'y a pas de routage de paquets).



Pour établir la connexion entre le Serveur et les clients via le Serveur proxy, il est recommandé de désactiver le chiffrement du trafic. Pour ce faire, il suffit de spécifier la valeur **non** pour le paramètre **Chiffrement** dans la rubrique [Configuration du Serveur Dr.Web → Général](#).

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 (les protocoles TCP/IP sont supportés).
3. Envoi de données entre le Serveur Dr.Web et les Agents Dr.Web 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](#).

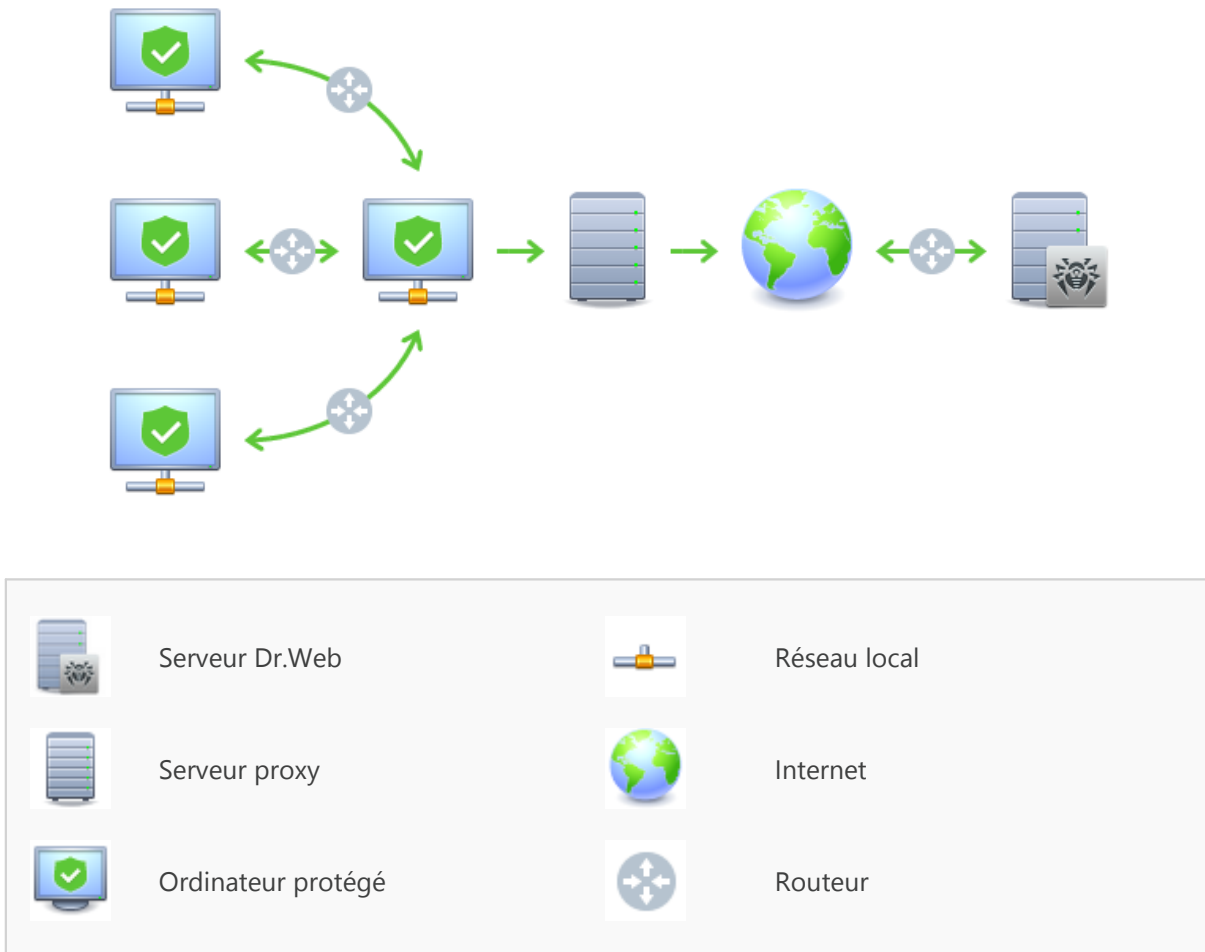


Figure 10-1. Schéma du réseau antivirus en cas d'utilisation du Serveur proxy

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 relai des connexions (le 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 Dr.Web. 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 Dr.Web.



Algorithme de redirection en cas de présence d'une liste des Serveurs Dr.Web :

1. Le Serveur proxy charge dans la mémoire vive la liste des Serveurs Dr.Web depuis le fichier de configuration `drwcsd-proxy.xml` (voir les **Annexes**, p. [Annexe G4](#)).
2. L'Agent Dr.Web se connecte au Serveur proxy.
3. Le Serveur proxy redirige l'Agent Dr.Web vers le premier Serveur Dr.Web mentionné dans la liste dans la mémoire vive.
4. Le Serveur proxy effectue une rotation de la liste chargée dans la mémoire vive en déplaçant le Serveur Dr.Web de la première place 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 Dr.Web 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.
6. Si le Serveur Dr.Web 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 l'ordinateur depuis un réseau externe par rapport aux Agents du 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 Dr.Web 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 matériels (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 paramètres spécifiés dans le fichier de configuration permettent de configurer lors de la mise en cache les actions suivantes :

- Nettoyer périodiquement les révisions périmées. Par défaut – 1 fois par heure.
- Sauvegarder les dernières révisions. Toutes les autres révisions sont considérées comme périmées et elles sont supprimées. Seules les trois dernières révisions sont conservées par défaut.
- Télécharger périodiquement les fichiers *memory mapped* non utilisés. Par défaut – toutes les 10 minutes.

Paramètres

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 **Annexes**, art. [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, double-cliquez 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 le **Manuel d'installation**, p. [Installation du serveur proxy](#)).



Pour démarrer le Serveur proxy sous Windows et les OS de la famille UNIX, vous pouvez également lancer le fichier exécutable `drwcsd-proxy` avec les paramètres nécessaires (voir [Annexe H9. 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 [site de Microsoft](#).

Utilisation de NAP dans Dr.Web Enterprise Security Suite

Dr.Web Enterprise Security Suite permet d'utiliser la technologie NAP pour vérifier la performance du logiciel antivirus sur les postes protégés. 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 l'ordinateur avec le Serveur NAP.
- Agent d'intégrité système (System Health Agent – SHA). L'agent s'installe sur le poste de travail de manière automatique avec le logiciel de l'Agent Dr.Web.
- Le serveur Dr.Web sert de serveur de correction assurant le fonctionnement de l'antivirus sur les postes.

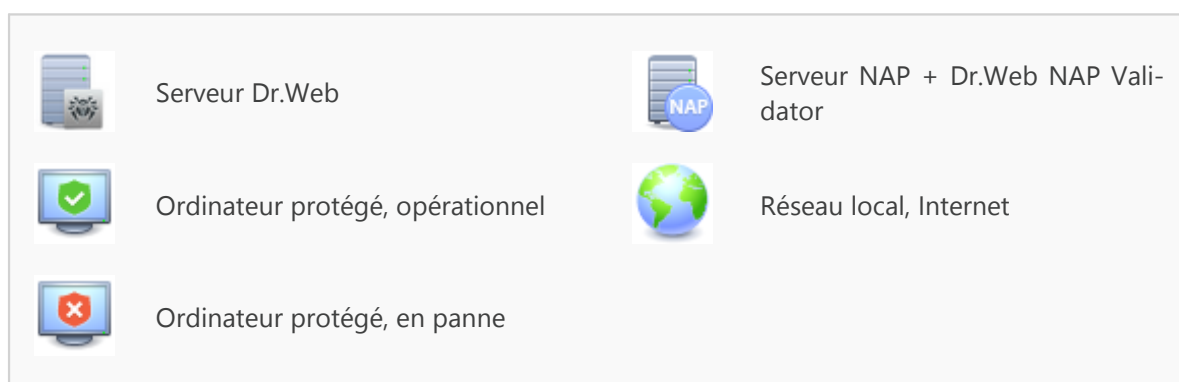


Figure 10-2. Schéma du réseau antivirus en cas d'utilisation de NAP

Marche à suivre pour effectuer la procédure de vérification :

1. Pour activer la vérification, il faut configurer les paramètres correspondants de l'Agent.
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 les éléments de la politique de sécurité sont considérés comme opérationnels et approuvés pour le fonctionnement au sein du réseau.
 - les postes non conformes au moins à un élément de la politique seront considérés comme non opérationnels. Ces postes ne peuvent que se connecter au Serveur Dr.Web, 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.

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 **Guide d'installation**, p. [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 considéré 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, sélectionnez l'élément **Client fail one or more SHV checks**. Conformément à cette option, le poste sera considéré comme non opérationnel s'il n'est pas conforme à au moins un élément de la politique adoptée.



Référence

A

administrateurs
droits 92

Agent

fonctions 49
interface 49
mise à jour 248
mode mobile 248

approbation des postes 116

authentification automatique 68

authentification, Centre de gestion 68

C

Centre de gestion

barre d'outils 58
description 50
liste hiérarchique 57
menu principal 51
panneau des propriétés 63

chargeur du dépôt 242

chiffrement

trafic 170

clés 28

démo 29

réception 28

voir aussi enregistrement 28

clés de démo 29

composants

réseau antivirus 81
synchronisation 240

composition du kit de distribution 26

compression du trafic 170

comptes 92

configuration

serveur antivirus 167

création

groupes 105

D

démarrage

Serveur Dr.Web 45, 48

dépôt

éditeur simplifié 211
paramètres généraux 210

distribution 26

distribution principale du Serveur Dr.Web

composition 26

distribution supplémentaire du Serveur Dr.Web

composition 26

droits

administrateurs 92

E

enregistrement

du produit Dr.Web 28

postes sur le Serveur 116

F

fonctions

Agent 49

Serveur Dr.Web 41

G

groupes 102

ajout des postes 108

configuration, héritage 113

paramètres 112

paramètres, copie 114

primaires 113

suppression de postes 108

groupes prédéfinis 102

groupes primaires 113

I

icônes

liste hiérarchique 57, 199

scanner réseau 72

interface

serveur antivirus 42, 45

J

journal du Serveur 41

L

langue

Centre de gestion 66, 98

liaisons, entre serveurs

configuration 227

types 225

licence 28



Référence

M

messages

- envoi à l'utilisateur 159
- format du logo 160

mise à jour

- Agent 248
- Dr.Web Enterprise Security Suite 238
- forcée 240
- limitation 247
- manuelle 240
- mode mobile 248
- réseau antivirus 232
- selon planification 240

mise à jour forcée 240

mise à jour manuelle 240

mode mobile de l'Agent 248

N

NAP Validator 254

- configuration 256

notifications

- configuration 202

novice 116

P

paramètres

- copie 114
- serveur antivirus 167

Planificateur des tâches

- Serveur 185

planification

- des mises à jour 240
- du Serveur 185

poste

- ajout vers le groupe 108
- approbation 116
- configuration, héritage 113
- gestion 116
- non approuvé 116
- novice 116
- paramètres, copie 114
- restauration 118
- scan 129, 138
- statistiques 148
- suppression 118

- suppression depuis le groupe 108

postes non approuvés 116

pré-requis système 20

privileges

- administrateurs 92

Q

quarantaine 155

R

répertoire du serveur, composition 43, 45

réseau antivirus 224

- composants 81
- configuration des liaisons 227
- événements viraux 232
- mises à jour 232
- planification 34
- structure 81, 225

restauration d'un poste 118

restriction des mises à jour 247

S

scan

- automatique 129
- manuel 138

scan antivirus 138

scanner

- antivirus 138
- réseau 71

scanner antivirus 138

serveur antivirus

- composition du répertoire 43, 45
- configuration des liaisons 227
- démarrage 45, 48
- interface 42, 45
- journal 41
- paramètres 167
- planification 185
- types de liaisons 225

Serveur Dr.Web

- composition du répertoire 43, 45
- configuration des liaisons 227
- démarrage 45, 48
- interface 42, 45
- journal 41
- paramètres 167



Référence

Serveur Dr.Web

planification 185

tâches 41

types de liaisons 225

serveur proxy

démarrage, arrêt 253

fonctions 250

SGM

voir aussi mise à jour manuelle 240

statistiques

postes 148

suppression

groupes 106

poste, depuis le groupe 108

postes 118

synchronisation, composants 240

T

trafic

chiffrement 170

composition 83

compression 170

