Manuel d'Installation

Dr.Web Enterprise Security Suite
Version 10.01.0
Manuel d'Installation
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

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**)

   Le Manuel d'installation sera utile à la personne responsable de l'achat et de l'installation d'un système de protection antivirus complète.

   Le Manuel d'installation explique comment construire un réseau antivirus et installer ses composants.
2. **Manuel Administrateur** (fichier **drweb-esuite-10-admin-manual-fr.pdf**)
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.
Réseau antivirus	Un nouveau terme ou l'accent mis sur un terme dans les descriptions.
<IP-address>	Champs destinés à remplacer les noms fonctionnels par leurs valeurs.
Enregistrer	Noms des boutons de l'écran, des fenêtres, des éléments de menu et d'autres éléments de l'interface du logiciel.
CTRL	Touches du clavier.
`C:\Windows\`	Noms de fichiers/dossiers ou fragments de programme.
Annexe A	Liens vers les autres chapitres du manuel ou liens vers des ressources externes.

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*.

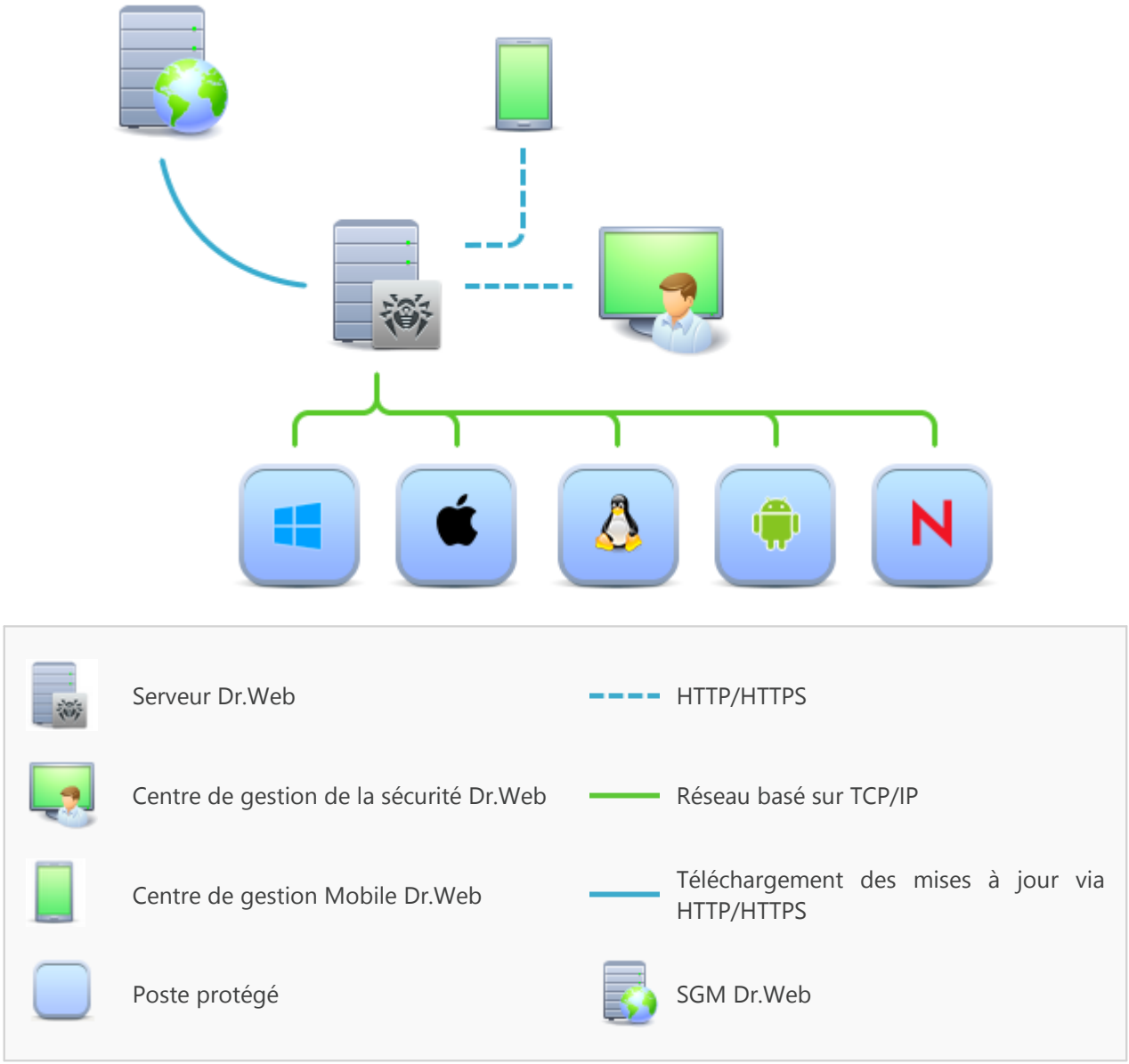

Figure 1-1. Structure logique du réseau antivirus

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 sus 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 (pour plus d'informations, voir Installation de l'Agent Dr.Web).
- Facilité de gestion des postes dans le réseau antivirus, assurée par un mécanisme de groupement.
- 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.
- 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.
- Obtention des informations statistiques sur le statut de postes protégés, statistiques virales, statut du logiciel installé, statut des composants lancés et liste de hardware et software du poste protégé .
- 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.

- 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.
- 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 événement du réseau antivirus avec les méthodes différentes d'envoi de notifications ; paramétrage des liaisons entre Serveurs pour configurer un réseau multi-serveurs.

Pour l'information détaillée sur les fonctionnalités décrites veuillez consulter **Manuel Administrateur**.

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 crées 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 crées 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 crées 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 crées 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 :

<table>
<tr><th>Numéros de ports</th><th>Protocoles</th><th>Direction des connexions</th><th>Utilisation</th></tr>
<tr><td rowspan="2">2193</td><td>TCP</td><td>• entrantes, sortantes pour le Serveur et le Serveur proxy
• sortantes pour l'Agent</td><td>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.</td></tr>
<tr><td>UDP</td><td>entrantes, sortantes</td><td>Pour le fonctionnement du Scanner réseau.</td></tr>
<tr><td rowspan="2">139, 445</td><td>TCP</td><td>• entrantes pour le Serveur
• entrantes, sortantes pour l'Agent
• sortantes pour l'ordinateur sur lequel le Centre de gestion est ouvert</td><td rowspan="2">Pour le fonctionnement de l'Installateur réseau.</td></tr>
<tr><td>UDP</td><td>entrantes, sortantes</td></tr>
<tr><td>9080</td><td>HTTP</td><td rowspan="3">• entrantes pour le Serveur
• sortantes pour l'ordinateur sur lequel le Centre de gestion est ouvert</td><td rowspan="2">Pour le fonctionnement du Centre de gestion de la sécurité Dr.Web.</td></tr>
<tr><td>9081</td><td>HTTPS</td></tr>
<tr><td>10101</td><td>TCP</td><td>Pour l'utilitaire de diagnostique à distance du Serveur.</td></tr>
</table>

Numéros de ports	Protocoles	Direction des connexions	Utilisation
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	Les OS suivants avec le CPU correspondant sont supportés : • CPU supportant les instructions SSE2 et ayant la fréquence d'horloge de 1,3 Ghz et plus : ▫ OS Windows ; ▫ OS Linux ; ▫ OS FreeBSD ; ▫ OS Solaris x86. • CPU V9 UltraSPARC IIIi ou supérieur : ▫ OS Solaris Sparc. La liste complète des OS supportés est fournie dans les **Annexes**, dans l'Annexe A.
Mémoire vive	• Pré-requis minimum : 1 Go. • Pré-requis recommandés : 2 Go et plus.
Espace disque	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). 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 `var\installers-cache` du répertoire d'installation du Serveur Dr.Web. Pour installer le Serveur, il est nécessaire que le disque système pour Windows ou `/var/tmp` 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).

Composant	Pré-requis
Autre	Pour l'installation du Serveur Dr.Web sous les OS de la famille UNIX, les bibliothèques suivantes sont requises : `lsb` en version 3 ou supérieure, `glibc` en version 2.7 ou supérieure. Pour utiliser une BD **PostgreSQL**, la bibliothèque `libpq` est requise. Pour utiliser une BD **Oracle**, la bibliothèque `libaio` est requise. En plus, sous **FreeBSD**, la bibliothèque `compat-8x` est requise.

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	• Windows ; • Linux ; • FreeBSD ; • Solaris. La liste complète des OS supportés est fournie dans les **Annexes**, dans l'Annexe A.
Autre	Pour l'installation du Serveur proxy sous les OS de la famille UNIX, les bibliothèques suivantes sont requises : `lsb` en version 3 ou supérieure. En plus, sous **FreeBSD**, la bibliothèque `compat-8x` 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	

Navigateur	Support
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 exéutables + espace disque supplémentaire pour les journaux et les fichiers temporaires.

Composant	Pré-requis
Autre	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 : • 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
drweb-esuite-server-10.01.0-<*assemblage*>-<*version_de_l'OS*>.run	Distribution principale du Serveur Dr.Web
drweb-esuite-extra-10.01.0-<*assemblage*>-<*version_de_l'OS*>.run	Distribution supplémentaire du Serveur Dr.Web
drweb-esuite-proxy-10.01.0-<*assemblage*>-<*version_de_l'OS*>.run	Serveur proxy

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

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

Pour en savoir plus sur les principes et les particularités de la licence Dr.Web Enterprise Security Suite, consultez le **Manuel administrateur**, les sous-rubriques Chapitre 2. Licence.

L'utilisation des fichiers clés de licence lors de l'installation du programme est décrite dans le p. Installer le Serveur Dr.Web.

L'utilisation des fichiers clés de lience pour un réseau antivirus déjà déployé est décrite en détails dans le **Manuel Administrateur**, p. Gestionnaire de licences.

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 **Manuel Administrateur**, 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 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 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 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 **Manuel administrateur**, le p. Centre de gestion de la sécurité Dr.Web).
7. Effectuez la configuration initiale du Serveur (vous pouvez consulter le description détaillée des paramètres du Serveur dans le **Manuel administrateur**, dans la 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 composant 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 **Manuel Administrateur**, 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 **Manuel administrateur**, la 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 **Manuel Administrateur**, 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 **Manuel administrateur**, la 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 crées. 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 :

   - Sil 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 egalement 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 **Manuel Administrateur**, 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 **Manuel administrateur**, la Chapitre 7).

3.2. Configuration des connexions réseau

Généralités

Les client 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 adresses spécifiée dans les paramètres du Serveur.
2. Les Agents lorsqu'ils recherchent le Serveur, envoient des requêtes multicast à l'adresse de groupe spéficié 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. Installation des composants Dr.Web Enterprise Security Suite

4.1. Installation du Serveur Dr.Web

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

L'installation du package complet du Serveur Dr.Web comprend deux étapes :

1. Installation de la *distribution principale*. 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 OS Windows.
2. Installation de la *distribution supplémentaire (extra)*. La distribution supplémentaire 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 installée la distribution principale du Serveur Dr.Web.

La procédure d'installation du Serveur Dr.Web varie en fonction de la version du Serveur (pour OS Windows ou pour les OS de la famille UNIX) à installer.

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

Si le logiciel du Serveur est déjà installé, consultez les paragraphes Mise à jour du Serveur Dr.Web sous OS Windows® ou Mise à jour du Serveur Dr.Web sous les OS de la famille UNIX®.

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

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

Exception : le cas où l'anglais est utilisé pour le nom du répertoire d'installation.

Le Centre de gestion de la Sécurité s'installe automatiquement avec le Serveur Dr.Web et sert à gérer le réseau antivirus et la configuration du Serveur.

Par défaut, sous Windows, le Serveur Dr.Web démarre de manière automatique après l'installation. Sous les OS de la famille UNIX le démarrage est effectué manuellement.

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

L'installation du Serveur Dr.Web pour OS Windows est décrite ci-dessous.

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

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

Les droits d'administrateur sur le poste sont requis pour installer le Serveur Dr.Web.

Après l'installation du Serveur Dr.Web, une mise à jour de tous les composants de Dr.Web Enterprise Security Suite est nécessaire (voir **Manuel Administrateur**, p. Mise à jour manuelle des composants de Dr.Web Enterprise Security Suite).

En cas d'utilisation d'une BD externe, il faut d'abord créer la BD et paramétrer ensuite le pilote correspondant (voir **Annexes**, p. Annexe B. Description des paramètres du SGBD. Paramètres de pilotes du SGBD).

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**.

La Fig. 4-1 présente un organigramme de la procédure d'installation du Serveur Dr.Web avec l'installateur. La description détaillée ci-dessous correspond aux étapes de la procédure.

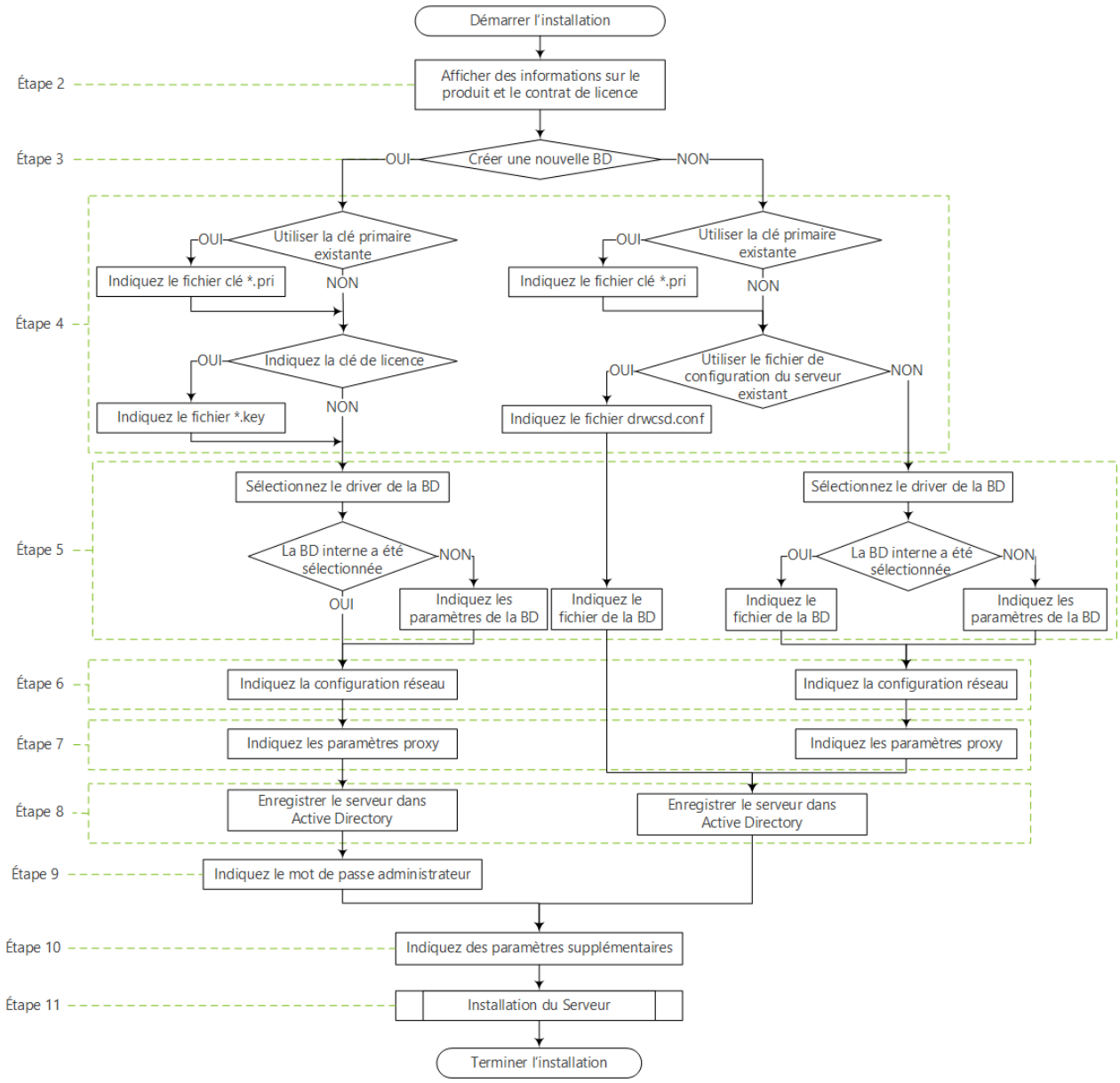

Figure 4-1. Schéma de la procédure d'installation du Serveur Dr.Web(Cliquez sur un élément de l'organigramme pour consulter la description)

Marche à suvre pour installer le Serveur Dr.Web sur un ordinateur tournant sous OS Windows :

1. Lancez le fichier de distribution.

   Par défaut, la langue du système d'exploitation est sélectionnée comme la langue de l'installateur. Si nécessaire, vous pouvez modifier la langue d'installation à toutes les étapes en sélectionnant l'élément correspondant qui se trouve dans l'angle droit supérieur de la fenêtre de l'installateur.

2. Une fenêtre affichant le texte du Contrat de licence va s'ouvrir. Après en avoir pris connaissance, cochez la case **J'accepte les termes du Contrat de licence** et cliquez sur **Suivant**.
3. Dans la fenêtre suivante sélectionnez la base qui sera utilisée pour le réseau antivirus :

- **Initialiser une nouvelle base de données** – pour créer un nouveau réseau antivirus.
- **Utiliser la base de données existante** – si vous souhaitez conserver la base de données du Serveur relative à l'installation précédente. Vous pourrez spécifier le fichier de la base de données ultérieurement (voir l'étape **5**).

4. Dans la fenêtre suivante spécifiez les paramètres de la base de données.

a) Si à l'étape **3** vous avez choisi l'option **Initialiser une nouvelle base de données** specifiez les paramètres suivants dans la fenêtre **Paramètres d'une nouvelle base de données** :

- La case **Spécifier la clé de licence** permet de specifier le fichier clé de licence de l'Agent Dr.Web lors de l'installation du Serveur.
  - Si la case est décochée, l'installation du Serveur sera effectué sans fichier clé de licence de l'Agent. Dans ce cas, les clés de licence doivent être ajoutées après l'installation du Serveur, via le Gestionnaire de licences.
  - Si la case est cochée, il faut spécifier le chemin vers le fichier clé de licence de l'Agent dans le champ correspondant.
- La case **Utiliser la clé de chiffrement privée existante** permet d'utiliser les clés de chiffrement existantes, par exemple, relatives à l'installation précédente du Serveur.
- Lors de la première installation du Serveur, décochez la case **Utiliser la clé de chiffrement privée existante**. Les nouvelles clés de chiffrement seront générées automatiquement durant l'installation.
- Si vous installez le Serveur pour un réseau déjà existant, cochez la case **Utiliser la clé de chiffrement privée existante** et spécifiez le chemin vers le fichier contenant la clé privée. Un fichier avec une clé publique sera généré automatiquement (le contenu de la clé publique va correspondre au contenu de la clé publique précédente). Ceci permet aux Agents déjà installés de se connecter à un nouveau Serveur. Sinon, après l'installation, il sera nécessaire de copier la nouvelle clé de chiffrement publique sur tous les postes sur lesquels les Agents Dr.Web ont été installés précédemment.
  Si une erreur survient lors de l'extraction de la clé publique, dans le champ **Spécifiez la clé de chiffrement publique** spécifiez manuellement le chemin vers le fichier contenant la clé publique correspondante.

Pour tester le produit, vous pouvez utiliser des fichiers clés de démonstration. Cliquez sur le bouton **Demander une clé de démonstration** pour visiter le site web de Doctor Web et obtenir les fichiers clés de démo (voir Fichiers clés de démonstration).

b) Si à l'étape **3** vous avez choisi l'option **Utiliser la base de données existante** specifiez les paramètres suivants dans la fenêtre **Paramètres de la base de données existante** :

- La case **Utiliser le fichier de configuration existant** permet de définir les paramètres du Serveur.
  - Si la case est décochée, le fichier de configuration du Serveur sera créé avec des paramètres par défaut.
  - Si la case est cochée, il faut spécifier dans le champ correspondant le chemin vers le fichier de configuration avec les paramètres du Serveur.
- La case **Utiliser la clé de chiffrement privée existante** permet d'utiliser les clés de chiffrement existantes, par exemple, relatives à l'installation précédente du Serveur.

- Lors de la première installation du Serveur, décochez la case **Utiliser la clé de chiffrement privée existante**. Les nouvelles clés de chiffrement seront générées automatiquement durant l'installation.
- Si vous installez le Serveur pour un réseau déjà existant, cochez la case **Utiliser la clé de chiffrement privée existante** et spécifiez le chemin vers le fichier contenant la clé privée. Un fichier avec une clé publique sera généré automatiquement (le contenu de la clé publique va correspondre au contenu de la clé publique précédente). Ceci permet aux Agents déjà installés de se connecter à un nouveau Serveur. Sinon, après l'installation, il sera nécessaire de copier la nouvelle clé de chiffrement publique sur tous les postes sur lesquels les Agents Dr.Web ont été installés précédemment.
  Si une erreur survient lors de l'extraction de la clé publique, dans le champ **Spécifiez la clé de chiffrement publique** spécifiez manuellement le chemin vers le fichier contenant la clé publique correspondante.

Pour tester le produit, vous pouvez utiliser des fichiers clés de démonstration. Cliquez sur le bouton **Demander une clé de démonstration** pour visiter le site web de Doctor Web et obtenir les fichiers clés de démo (voir Fichiers clés de démonstration).

5. La fenêtre **Pilote de la base de données** permet de configurer les paramètres de la base utilisée. Ces paramètres dépendent du type de base de données choisi à l'étape **3** et de la disponibilité du fichier de configuration du Serveur spécifié à l'étape **4** :
   - Si à l'étape **3** vous avez sélectionné l'option **Créer une nouvelle base de données** ou que vous n'avez pas spécifié le chemin vers le fichier de configuration du Serveur à l'étape **4** de l'option **Utiliser la base de données existante**, sélectionnez le pilote qu'il faudra utiliser. Dans ce cas :
     - Les options **SQLite** (base de données embarquée) et **IntDB** (base de données embarquée) activent l'utilisation des outils intégrés du Serveur Dr.Web. La définition de paramètres supplémentaires n'est pas requise.
     - Les autres options correspondent à l'utilisation d'une BD externe. Dans ce cas, il faut d'abord indiquer les paramètres correspondants pour la configuration d'accès à la BD. La configuration des paramètres du SGBD est décrite dans les Annexes (voir **Annexes**, p. Annexe B Paramètres nécessaire pour utiliser le SGBD. Paramètres de pilotes du SGBD).
   - Si à l'étape **3** vous avez sélectionné l'option **Utiliser la base de données existante** et vous n'avez pas spécifié le chemin vers le fichier de configuration du Serveur à l'étape **4**, spécifiez le chemin vers le fichier de la base de données qui sera utilisée conformément au fichier de configuration du Serveur spécifié.
6. Si à l'étape **3** vous avez sélectionné l'option **Créer une nouvelle base de données** ou que vous n'avez pas spécifié le chemin vers le fichier de configuration du Serveur à l'étape **4** de l'option **Utiliser la base de données existante**, la fenêtre **Configuration du réseau** va s'afficher. Dans cette fenêtre vous pouvez configurer le protocole réseau pour le fonctionnement du Serveur (il est autorisé de spécifier un seul protocole réseau, les protocoles supplémentaires vous pouvez spécifier ultérieurement).

   Pour définir les paramètres réseau depuis le jeu préétabli. Pour cela, sélectionnez un des éléments suivants dans la liste déroulante :

   - **Configuration standard** prescrit l'utilisation de paramètres par défaut à la base du service de détection du Serveur.

- **Configuration limitée** prescrit la limitation du fonctionnement du Serveur par l'interface réseau locale – `127.0.0.1`. Cette configuration permet de gérer le Serveur uniquement via le Centre de gestion ouvert sur le même poste, et de communiquer uniquement avec l'Agent lancé sur le même poste. Dès que le réglage des paramètres du Serveur est achevé, vous pouvez modifier les paramètres réseau.
- **Configuration personnalisée** signifie la modification des paramètres préétablis :
  - Dans les champs **Interface** et **Port**, spécifiez les valeurs correspondantes pour l'accès au Serveur. Par défaut, l'interface `0.0.0.0` est définie, ce qui signifie que l'accès au Serveur est possible via toutes les interfaces.

Le port `2193` est utilisé par défaut.

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

Les adresses doivent être spécifiées au format d'adresse réseau décrite dans les **Annexes**, p. Annexe E. Spécification de l'adresse réseau.

  - Pour restreindre l'accès local au Serveur, cochez la case **Restreindre l'accès au Serveur Dr.Web**. Ainsi l'accès sera interdit aux Installateurs des Agents, aux Agents et aux autres Serveurs (en cas de réseau antivirus existant créé à l'aide de Dr.Web Enterprise Security Suite). Vous pouvez modifier ces paramètres ultérieurement depuis le menu du Centre de gestion **Administration**, élément **Configuration du Serveur Dr.Web**, onglet **Modules**.
  - Cochez la case **Activer le service de détection du Serveur Dr.Web** si vous souhaitez que le Serveur réponde aux requêtes de recherche multicast ou broadcast de la part des autres Serveurs via l'adresse IP et le nom du service spécifiés dans les champs correspondants ci-dessous.

7. Si à l'étape **3** vous avez sélectionné l'option **Créer une nouvelle base de données**ou que vous n'avez pas spécifié le chemin vers le fichier de configuration du Serveur à l'étape **4** de l'option **Utiliser la base de données existante**, la fenêtre **Serveur proxy** va s'afficher. Dans la fenêtre vous pouvez configurer les paramètres d'utilisation du serveur proxy lors de la connexion au Serveur :

   Pour se connecter au Serveur via le serveur proxy cochez la case **Utiliser le serveur proxy**.

La case **Utiliser le Serveur proxy** sera disponible uniquement si le dossier d'installation du Serveur ne contient pas de fichiers de configuration de l'installation précédente.

   Définissez les paramètres suivants pour configurer la connexion au serveur proxy :

   - **Adresse du serveur proxy** – adresse IP ou nom DNS du serveur proxy (champ obligatoire),
   - **Nom d'utilisateur**, **Mot de passe** – nom d'utilisateur et mot de passe d'accès au serveur proxy, si le serveur proxy supporte la connexion authentifiée.
   - Dans la liste déroulante **Méthode d'authentification**, sélectionnez la méthode d'authentification sur le serveur proxy s'il supporte les connexions authentifiées.

8. Si l'ordinateur sur lequel l'installation du Serveur est effectuée, fait partie du domaine Active Directory, vous serez invité à enregistrer le Serveur Dr.Web dans le domaine Active Directory dans la fenêtre suivante. Lors de l'enregistrement dans le domaine Active Directory sur le serveur DNS, l'enregistrement SRV correspondant au Serveur Dr.Web sera créé. Après les clients pourront accéder au Serveur Dr.Web via cet enregistrement SRV.

   Pour enregistrer, configurez les paramètres suivants :

   - Cochez la case **Enregistrer le Serveur Dr.Web dans Active Directory**.
   - Dans le champ **Domaine** indiquez le nom du domaine Active Directory, dans lequel le Serveur sera enregistré. Si le domaine n'est pas spécifié, ce sera le domaine dans lequel est enregistré l'ordinateur que lequel l'installation est effectuée qui sera utilisé.
   - Dans les champs **Nom d'utilisateur** et **Mot de passe** entrez les identifiants de l'administrateur du domaine Active Directory.

9. Si à l'étape **3**vous avez sélectionné l'option **Créer une nouvelle base de données**, la fenêtre **Mot de passe de l'administrateur** va s'ouvrir. Spécifiez le mot de passe de l'administrateur du réseau antivirus, créé par défaut avec l'identifiant **admin** et un accès à toutes les options de gestion du réseau antivirus.

10. Dans la fenêtre suivant l'Assistant vous informera sur la disponibilité de l'installation du Serveur. Si nécessaire, vous pouvez configurer les paramètres d'installation avancés. Pour ce faire cliquez sur l'élément **Paramètres avancés** en bas de la fenêtre et définissez les paramètres suivants :

    - Dans l'onglet **Général** :
      - Dans liste déroulante **Langue d'interface du Centre de gestion de la sécurité Dr.Web**, sélectionnez la langue d'interface par défaut pour le Centre de gestion de la sécurité Dr.Web.
      - Dans la liste déroulante **Langue d'interface de l'Agent Dr.Web**, sélectionnez la langue d'interface par défaut pour l'Agent Dr.Web et pour les composants du package antivirus installés sur les postes.
      - Cochez la case **Partager le dossier d'installation de l'Agent Dr.Web** pour modifier le mode d'utilisation et le nom du dossier d'installation partagé de l'Agent (Le nom masqué des ressources partagées est défini par défaut).
      - Cochez la case **Démarrer le Serveur Dr.Web** après l'installation pour démarrer automatiquement le Serveur après l'installation.
      - Cochez la case **Mettre à jour le dépôt des produits après la fin de l'installation** pour mettre à jour automatiquement le dépôt des produits du Serveur juste après la fin de l'installation.
      - Cochez la case **Envoyer des statistiques à Doctor Web** pour autoriser l'envoi des statistiques sur les événements viraux à Doctor Web.
    - Dans l'onglet **Chemin** :
      - Dans le champ **Répertoire d'installation du Serveur Dr.Web** est spécifié le répertoire dans lequel l'installation du Serveur est effectuée. Pour modifier le répertoire spécifié par défaut cliquez sur **Parcourir** et sélectionnez le répertoire nécessaire.

- Dans le champ **Répertoire de sauvegarde du Serveur Dr.Web** est spécifié le répertoire dans lequel la sauvegarde des données critiques du Serveur est effectuée d'après les tâches du planificateur du Serveur. Pour modifier le répertoire spécifié par défaut cliquez sur **Parcourir** et sélectionnez le répertoire nécessaire.

- Dans l'onglet **Composants** sélectionnez les composants que vous souhaitez installer.

Si vous souhaitez utiliser ODBC pour Oracle en tant que base de données externe, annulez l'installation du client intégré pour SGBD Oracle (dans la rubrique **Support des bases de données → Pilote de la base de données Oracle**).

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

- Dans l'onglet **Journal**, vous pouvez configurer la journalisation de l'installation et du fonctionnement du Serveur.

Après avoir configuré les composants supplémentaires cliquez sur **OK** pour appliquer les modifications ou sur **Annuler** si vous n'avez apporté aucune modification ou pour annuler les modifications apportées.

11. Cliquez sur le bouton **Installer** afin de lancer la procédure d'installation. Les actions suivantes du logiciel ne nécessitent aucune intervention de l'utilisateur.
12. Après la fin de l'installation, cliquez sur le bouton **Terminer**.

La gestion du Serveur Dr.Web est effectuée normallement à l'aide du Centre de gestion qui sert d'interface intégrée pour le 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.

La structure du dossier d'installation du Serveur est décrite dans le **Manuel Administrateur**, à la rubrique Serveur Dr.Web.

4.1.2. Installation du Serveur Dr.Web pour les OS de la famille UNIX®

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

Installation du Serveur Dr.Web pour les OS de la famille UNIX :

1. Pour démarrer l'installation du package du Serveur, exécutez la commande suivante :

   `sh ./<fichier_de_distribution>.run`

   Pour lancer le package d'installation, vous pouvez utiliser les clés de la ligne de commande. Vous trouverez les paramètres de la commande de démarrage dans les **Annexes**, p. H11. Installateur du Serveur Dr.Web pour les OS de la famille UNIX®

   Par défaut, le nom de l'administrateur du réseau antivirus est **admin**, le mot de passe – **root**.

2. Les fenêtres suivantes contiennent le Contrat de licence. Pour procéder à l'installation, vous devez l'accepter.
3. En réponse à la requête concernant le répertoire de sauvegarde, spécifiez le chemin vers le répertoire nécessaire ou confirmez la sauvegarde dans le répertoire par défaut – `/var/tmp/drwcs`.
4. Si une distribution supplémentaire (extra) est trouvée dans le système, une notification sur la suppression de la distribution supplémentaire sera affichée avant le début de l'installation du package du Serveur. Il n'est pas possible de continuer l'installation sans supprimer la distribution supplémentaire.
5. Les composants seront ensuite installés sur votre ordinateur. Au cours de l'installation, vous pouvez être sollicités pour confirmer certaines actions en tant qu'administrateur.

   Au cours de l'installation du logiciel sous l'OS **FreeBSD** un script rc- `/usr/local/etc/rc.d/drwcsd.sh` sera créé.

   Utilisez les commandes :

   - `/usr/local/etc/rc.d/drwcsd.sh stop` – pour stopper manuellement le Serveur ;
   - `/usr/local/etc/rc.d/drwcsd.sh start` – pour démarrer manuellement le Serveur.

En cas de première installation du Serveur, la clé de licence n'est pas spécifiée. Les clés de licence doivent être ajoutées après l'installation du Serveur, via le Gestionnaire de licences.

4.1.3. Installation de la distribution supplémentaire du Serveur Dr.Web

L'installation de la distribution supplémentaire (extra) doit être effectuée sur l'ordinateur sur lequel est installée la distribution principale du Serveur Dr.Web. Vous trouverez la description de la distribution principale du Serveur dans la rubrique Installation du Serveur Dr.Web sous OS Windows® et Installation du Serveur Dr.Web sous les OS de la famille UNIX®.

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

Marche à suvre pour installer la distribution supplémentaire du Serveur Dr.Web sur un ordinateur tournant sous Windows :

1. Lancez le fichier de distribution.
2. La fenêtre **Dr.Web ESuite Extra** contenant les informations sur le produit à installer et le texte du Contrat de licence va s'ouvrir. Après avoir pris connaissance des termes de ce Contrat, sélectionnez **J'accepte les termes du Contrat de licence** et cliquez sur **Installer** pour procéder à l'installation.
3. L'installation de la distribution supplémentaire va commencer. Si aucune erreur n'est survenue lors de l'installation, l'intervention de l'utilisateur n'est pas requise.
4. Après la fin de l'installation, cliquez sur le bouton **Terminer**. Le redémarrage n'est pas requis.

Marche à suvre pour installer la distribution supplémentaire du Serveur Dr.Web sur un ordinateur tournant sous un OS de la famille UNIX :

1. Lancez le fichier de distribution à l'aide de la commande suivante :

   `sh ./<fichier_de_distribution>.run`
2. Les fenêtres suivantes contiennent le Contrat de licence. Pour procéder à l'installation, vous devez l'accepter.
3. Ensuite, le logiciel sera installé.

4.1.4. Installation de l'extension pour le Centre de gestion de la sécurité Dr.Web

> ⚠ Installation de l'extension pour le Centre de gestion de la sécurité Dr.Webpour les navigateurs web Mozilla Firefox, Opera et Chrome est possible uniquement pour leurs versions tournant sous l'OS Windows ou sous les OS de la famille Linux.

L'extension pour le Centre de gestion de la sécurité Dr.Web assure le fonctionnement complet du Centre de gestion (voir aussi Pré-requis système pour le Centre de gestion de la sécurité Dr.Web).

L'extension est fournie avec la distribution du Serveur et peut être installée d'une façon suivante :

1. Automatiquement, en réponse à une requête du navigateur web pendant l'utilisation des éléments du Centre de gestion nécessitant le chargement du module (Scanner réseau, installation à distance des composants antivirus).
2. Manuellement, à l'aide de l'installateur d'extension pour le Centre de gestion de la sécurité Dr.Web.

Installation manuelle de l'extension pour le Centre de gestion de la sécurité Dr.Web

Marche à suivre pour télécharger manuellement l'installateur d'extension pour le Centre de gestion de la sécurité Dr.Web :

1. Ouvrez le Centre de gestion. Si l'extension pour le Centre de gestion de la sécurité Dr.Web n'est pas encore installée pour le navigateur utilisé, une recommandation à installer l'extension sera affichée au-dessous du menu principal.
2. Cliquez sur le lien **Installer l'extension pour le Centre de gestion de la sécurité Dr.Web pour le navigateur**.

Figure 4-2. Rubrique de téléchargement de l'extension pour le Centre de gestion de la sécurité Dr.Web

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

   Pour les OS de la famille UNIX, il sera également proposé de sélectionner depuis la liste une version de la distribution correspondant au système d'exploitation utilisé.
4. Pour télécharger et sauvegarder le module, cliquez sur le bouton **Télécharger**. Puis vous pouvez procéder à l'installation manuelle.
5. Afin de basculer entre les différents types de plateforme, cliquez sur le lien se trouvant au-dessous du bouton de téléchargement, puis téléchargez le plugin comme décrit à l'étape **4**.

Marche à suivre pour installer l'extension pour le Centre de gestion de la sécurité Dr.Web sous OS Windows :

1. Lancez le fichier de distribution. La fenêtre de l'assistant **InstallShield Wizard** vous informant du produit installé va s'ouvrir. Cliquez sur **Suivant**.

2. La fenêtre affichant le texte du Contrat de licence va s'ouvrir. Après avoir pris connaissance des termes du Contrat, indiquez **J'accepte les termes du Contrat de licence** et cliquez sur **Suivant**.
3. La fenêtre de sélection du dossier d'installation s'ouvrira. Pour modifier le dossier d'installation spécifié par défaut, cliquez sur **Modifier** et sélectionnez un dossier. Puis cliquez sur **Suivant**.
4. Dans la fenêtre suivante, cliquez sur le bouton **Installer** afin de lancer la procédure d'installation. Les actions suivantes de l'assistant d'installation ne nécessitent aucune intervention de l'utilisateur.
5. Après la fin de l'installation, cliquez sur le bouton **Terminer**.

Marche à suivre pour installer l'extension pour le Centre de gestion de la sécurité Dr.Web sous l'OS de la famille UNIX :

Exécutez la commande suivante :

- pour les **packages** deb :

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

- pour les packages **rpm** :

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

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

  1. Déballez l'archive contenant le plugin.
  2. Créez un dossier pour les plugins si un tel dossier n'a pas encore été créé.

     Par exemple pour le navigateur Mozilla Firefox :
     ```
     mkdir /usr/lib/mozilla/plugins
     ```
  3. Copiez la bibliothèque déballée à l'étape 1 vers le dossier pour les plugins.

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

Après avoir installé l'extension pour le Centre de gestion de la sécurité Dr.Web sous un OS de la famille UNIX, redémarrez le navigateur Web, s'il a été déjà lancé.

4.2. Installation de l'Agent Dr.Web

Les droits d'administrateur sur le poste sont requis pour installer l'Agent Dr.Web.

Si l'Antivirus est déjà installé sur le poste, il faudra supprimer l'Antivirus installé avant de procéder à la nouvelle installation.

L'Agent Dr.Web peut être installé sur un 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.

Installation de l'Agent Dr.Web par-dessus le produit antivirus autonome Dr.Web pour les postes tournant sous OS Windows

Si le produit autonome Dr.Web en version 7/8/9/10/11 est déjà installé sur le poste, l'installation de l'Agent pour Dr.Web Enterprise Security Suite en version 10 d'après le schéma suivant :

- En cas de lancement de l'installateur ou du package d'installation de l'Agent en mode GUI sur le poste contenant le produit autonome installé en version 7.0/8.0/9.0/9.1/10.0 l'installateur du produit installé sera lancé. Puis, l'utilisateur sera invité à entrer le code de confirmation d'actions et à supprimer le produit. Après le redémarrage de l'OS, la version GUI de l'installateur qui a été lancé initialement pour l'installation de l'Agent pour Dr.Web Enterprise Security Suite en version 10, sera lancée.
- Si l'installateur de l'Agent est lancé en tâche de fond sur le poste contenant le produit autonome en version 7.0/8.0/9.0/9.1/10.0, cela ne va pas aboutir à l'exécution des actions quelconques. En cas de l'installation à distance, l'installateur va informer le Centre de gestion sur la disponibilité de produits autonomes de versions précédentes. Dans ce cas il est nécessaire de supprimer manuellement le produit autonome et d'installer l'Agent pour Dr.Web Enterprise Security Suite en version 10 par un des moyens possibles.
- En cas de l'installation de l'Agent sur le poste contenant le produit autonome en version 11.0, le produit installé va passer du mode autonome en mode de protection centralisée. Après la connexion et l'authentification sur le Serveur, il est possible d'obtenir des mises à jour, de nouveaux paramètres et la liste de composants à installer. Certains composants peuvent exiger le redémarrage.

Lors de l'installation des Agents Dr.Web sur les serveurs de LAN et sur les ordinateurs du cluster, il faut prendre en compte les informations suivantes :

- En cas d'installation sur les ordinateurs servant des serveurs terminaux (sous OS Windows les services **Terminal Services** sont installés), afin d'assurer le fonctionnement des Agents lors des sessions terminales des utilisateurs, l'installation des Agents doit être réalisée de manière locale avec l'assistant d'installation et de suppression des programmes depuis le **Panneau de configuration** Windows.
- Il n'est pas recommandé d'installer les composants SpIDer Gate, Office Control, 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.
- L'installation de l'Agent sur le cluster doit être réalisée séparément pour chaque nœud du cluster.

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

4.2.1. Fichiers d'installation

Packages d'installation

Package d'installation personnel

Lors de la création d'un nouveau compte pour un poste, un package d'installation personnel de l'Agent Dr.Web est généré dans le Centre de gestion. Le package d'installation personnel inclut l'installateur de l'Agent Dr.Web et le jeu de paramètres de connexion au Serveur Dr.Web ainsi que les paramètres d'authentification du poste sur le Serveur Dr.Web.

Les packages d'installation personnels sont disponibles pour les postes protégés tournant sous tous les systèmes d'exploitation supportés par Dr.Web Enterprise Security Suite. Ainsi :

- Pour les postes sous l'OS Windows, le package d'installation personnel généré dans le Centre de gestion sur la base de l'installateur réseau de l'Agent est fourni. Les paramètres de connexion au Serveur et les paramètres d'authentification du poste sur le Serveur sont inclus directement dans le package d'installation personnel.
- Pour les postes sous l'OS Android, Linux, OS X, le package d'installation personnel représente l'installateur pour l'installation de l'Agent et le fichier de configuration avec les paramètres de connexion au Serveur et les paramètres d'authentification du poste sur le Serveur.

> ⚠ Pour obtenir les packages d'installation personnels sous les OS autres que Windows, l'installation de la distribution supplémentaire (extra) du Serveur Dr.Web est requise.

Le lien de téléchargement du package d'installation personnel de l'Agent Dr.Web sur le poste particulier est disponible :

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

Installateurs

L'installateur de l'Agent se distingue du package d'installation par ce qu'il n'inclut pas les paramètres de connexion au Serveur et les paramètres d'authentification du poste sur le Serveur.

Les types suivants des installateurs de l'Agent Dr.Web sont fournis :

- Pour les postes tournant sous l'OS Windows, deux types d'installateurs sont disponibles :
  - *L'installateur réseau* `drwinst.exe` n'installe que l'Agent. Après la connexion au Serveur, l'Agent télécharge et installe les composants correspondants de ce package antivirus. À l'aide de l'installateur réseau il est possible d'effectuer l'installation de l'Agent en mode local ainsi qu'à distance.
    L'installateur réseau de l'Agent `drwinst.exe` se trouve dans le répertoire `Installer` (par défaut, c'est une ressource partagée cachée) du répertoire d'installation du Serveur Dr.Web. L'accessibilité de cette ressource via le réseau peut être configurée à l'étape 10 pendant l'installation du Serveur Dr.Web. Vous pouvez modifier cette ressource ultérieurement.
  - *L'installateur complet* `drweb-esuite-agent-full-`*<version_de_l'Agent>*`-`*<version_de_l'assemblage>*`-windows.exe` effectue l'installation de l'Agent et du package antivirus en même temps.
- L'installateur pour l'installation de l'Agent Dr.Web, équivalent à l'installateur de la version autonome, est disponible pour les postes tournant sous les OS Android, Linux, OS X.

Les installateurs pour l'installation de l'Antivirus sont disponibles depuis la page d'installation du Centre de gestion de la sécurité Dr.Web.

> ⚠ Pour obtenir les installateurs sous les OS autres que Windows et pour installer la distribution complète, l'installation de la distribution supplémentaire (extra) du Serveur Dr.Web est requise.

Page d'installation

La page d'installation du Centre de gestion de la sécurité Dr.Web vous permet de télécharger :

1. Installateur de l'Agent Dr.Web.

   Les installateurs pour tous les postes protégés sous tous les OS supportés par Dr.Web Enterprise Security Suite, se trouvent dans des répertoires avec les noms correspondant au nom de l'OS.
2. Clé de chiffrement publique `drwcsd.pub`.

La page d'installation est accessible sur n'importe quel ordinateur ayant un accès réseau au Serveur Dr.Web, à l'adresse suivante :

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

comme <*Adresse_du_Serveur*> spécifiez l'adresse IP ou le nom DNS de l'ordinateur sur lequel est installé le Serveur Dr.Web. Comme <*numéro_du_port*>, spécifiez le port `9080` (ou `9081` pour https).

4.2.2. Installation de l'Agent Dr.Web en mode local

L'installation de l'Agent Dr.Web 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.

Avant la première installation des Agents Dr.Web, il est nécessaire de mettre à jour le dépôt du Serveur (voir **Manuel Administrateur**, p. Mise à jour manuelle des composants Dr.Web Enterprise Security Suite, p. **Vérification des mises à jour**).

Postes tournant sous l'OS Android, OS Linux, OS X

Pour installer l'Agent Dr.Web sur les postes tournant sous l'OS Android, OS Linux, OS X, les moyens suivants sont disponibles :

- Package d'installation personnel créé dans le Centre de gestion.
- Installateur de l'Agent Dr.Web.

Lors de la sélection du type de package d'installation, prenez en compte les particularités suivantes :

a) Lors de la création du package d'installation personnel, l'installateur de l'Agent Dr.Web est fourni, tandis que les paramètres de connexion au Serveur et les paramètres d'authentification du poste sur le Serveur sont fournis dans le fichier de configuration.

b) En cas de l'installation à l'aide de l'installateur, l'installation de l'Agent Dr.Web est effectuée, mais les paramètres de connexion au Serveur et les paramètres d'authentification du poste sur le Serveur ne sont pas fournis.

Postes tournant sous l'OS Windows

Pour installer l'Agent Dr.Web en mode local sur les postes tournant sous l'OS Windows, les moyens suivants sont disponibles :

- Package d'installation personnel créé dans le Centre de gestion `drweb-ess-installer.exe`.
- Installateur complet de l'Agent Dr.Web `drweb-esuite-agent-full-`<*version_de_l'Agent*>`-`<*version_de_l'assemblage*>`-windows.exe`.
- Installateur réseau de l'Agent Dr.Web `drwinst.exe`.

Lors de la sélection du type de package d'installation, prenez en compte les particularités suivantes :

a) Lors de l'installation depuis le package d'installation personnel, les paramètres de connexion au Serveur et les paramètres d'authentification sur le Serveur sont inclus dans le package d'installation personnel. L'installation depuis le package d'installation personnel est effectuée à la base de l'installateur réseau depuis lequel l'Agent est installé. Après la connexion au Serveur, l'Agent télécharge et installe les composants du package antivirus.

b) En cas de l'installation à l'aide de la distribution complète, l'Agent et le package d'installation sont installés simultanément. Dans ce cas, les paramètres de connexion au Serveur et les paramètres d'authentification du poste sur le Serveur ne sont pas fournis.

c) En cas de l'installation à l'aide de l'installateur réseau, seul l'Agent est installé. Après la connexion au Serveur, l'Agent télécharge et installe les composants correspondants du package antivirus. Dans ce cas, les paramètres de connexion au Serveur et les paramètres d'authentification du poste sur le Serveur ne sont pas fournis.

Caractéristiques comparatives des fichiers d'installation

Fichier d'installation		Installation de l'Agent	Installation du package antivirus	Paramètres de connexion au Serveur	Paramètres d'authentification sur le Serveur
Package d'installation personnel		+	–	+	+
Installateur	Réseau	+	–	–	–
	Complet	+	+	–	–

Pour obtenir les packages d'installation et les installateurs sous les OS autres que Windows, ainsi que l'installateur complet sous l'OS Windows, l'installation du package d'installation supplémentaire (extra) du Serveur Dr.Web est requise.

Le lancement de fichiers d'installation de l'Agent de tout type est également possible depuis la ligne de commande à l'aide de clés mentionnées dans le document **Annexes**, p. H2. Installateur réseau.

4.2.2.1. Installation de l'Agent Dr.Web avec le package d'installation personnel

Pour installer l'Agent Dr.Web sur les postes protégés avec le package d'installation personnel, procédez comme suit :

1. Depuis le Centre de gestion créez un compte de nouvel utilisateur sur le Serveur Dr.Web.

2. Envoyez à l'utilisateur le lien vers le package d'installation peronnel de l'Agent Dr.Web pour le système d'exploitation correspondant ou l'appareil mobile si l'installation du logiciel Agent Dr.Web se fait par l'utilisateur lui-même.Si l'installation est effectuée sur le poste tournant sous un système d'exploitation autre que Windows, il est nécessaire d'envoyer à l'utilisateur le fichier de configuration avec les paramètres de connexion au Serveur Dr.Web (voir l'étape **11** de la procédure Création d'un nouveau compte du poste).

   Pour transmettre facilement le fichier d'installation et le fichier de configuration, vous pouvez utiliser la fonction **Envoi des fichiers d'installation** (pour plus d'information, consultez le **Manuel Administrateur**, p. Envoi des fichiers d'installation). Ainsi, vous pourrez envoyer un message contenant les fichiers correspondants sur l'e-mail.

3. Effectuez l'installation de l'Agent Dr.Web sur le poste de travail.

   L'installation de l'Agent Dr.Web en mode local sur le poste de travail est décrite dans le **Manuel Utilisateur** pour les OS correspondants.

   Les droits d'administrateur sur le poste sont requis pour installer l'Agent Dr.Web.

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

4. Configurez les paramètres de connexion au Serveur Dr.Web sur le poste.

Création d'un nouveau compte de poste

Afin de créer un compte ou plusieurs comptes utilisateur, utilisez le Centre de gestion de la sécurité Dr.Web.

Lors de la création d'un compte utilisateur, merci de noter le nom du Serveur indiqué dans les sections suivantes du Centre de gestion :

1. **Administration** → **Configuration du Serveur web** → champ **Serveur** (conservé dans le paramètre `<server-name />` du fichier de configuration `webmin.conf`). La valeur de ce paramètre est utilisée lors de la génération du lien vers le package d'installation de l'Agent.

   Si la valeur du paramètre n'est pas spécifiée, le nom DNS (s'il est disponible) ou l'adresse IP de l'ordinateur sur lequel le Centre de gestion est ouvert est utilisé comme le nom du Serveur pour générer le lien de téléchargement de l'installateur de l'Agent.

2. **Administration** → **Configuration du Serveur Dr.Web** → Onglet **Réseau** → onglet **Téléchargement** → champ **Serveur** (conservé dans le paramètre `<name />` du fichier de configuration `download.conf`). La valeur de ce paramètre est spécifiée dans les packages d'installation de l'Agent et définit à quel Serveur l'Agent est connecté durant l'installation.

Si la valeur du paramètres n'est pas spécifiée, lors de la création du package d'installation de l'Agent, l'adresse du Serveur auquel est connecté le Centre de gestion est spécifiée. Dans ce cas, le Centre de gestion doit être connecté au Serveur utilisant l'adresse IP du domaine pour lequel vous avez créé un compte (l'adresse du Serveur ne doit pas être spécifiée comme un loopback – `127.0.0.1`).

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

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

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

7. Dans le champ **Description**, entrez des informations supplémentaires sur l'utilisateur. Ce paramètre est facultatif.
8. Dans la rubrique **Groupe**, sélectionnez les groupes auxquels va appartenir le poste que vous créez.
   - Dans la liste **Appartenance à**, vous pouvez configurer la liste de groupes utilisateur auxquels va appartenir le poste.
     Par défaut, le poste fait partie du groupe **Everyone**. S'il existe des groupes utilisateur, vous pouvez y inclure le poste que vous créez sans aucune restriction du nombre de groupes auxquels appartient le poste. Pour ce faire, cochez les cases contre les groupes utilisateur nécessaires dans la liste **Appartenance à**.

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

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

9. Si nécessaire, spécifiez des informations dans la rubrique **Sécurité**. Pour en savoir plus sur la configuration de cette rubrique, consultez le **Manuel Administrateur** dans la rubrique Sécurité.
10. Si nécessaire, spécifiez les paramètres dans la rubrique **Emplacement**.
11. Cliquez sur le bouton **Sauvegarder** se trouvant en haut, au coin droit de la fenêtre. Une fenêtre apparaît et informe sur la création réussie du nouveau poste, cette fenêtre affiche également le numéro d'identification et les liens suivants :
    - Dans l'élément **Fichier d'installation** – un lien pour télécharger l'installateur de l'Agent.

      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 section de téléchargement de la distribution, les liens sont fournis séparément pour chaque OS pris en charge par Dr.Web Enterprise Security Suite.

      Pour obtenir les packages d'installation sous les OS autres que Windows, l'installation de la distribution supplémentaire (extra) du Serveur Dr.Web est requise.

    - 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.
    - L'élément **Mot de passe** contient le mot de passe d'accès au Serveur pour ce poste. Pour voir le mot de passe, cliquez ici.

      Les liens de téléchargement de l'installateur de l'Agent et du fichier de configuration sont également disponibles :
      - depuis l'élément Propriétés du poste après sa création,
      - dans la rubrique **Objets sélectionnés** lors de la sélection du poste créé dans l'arborescence.

    - Dans cette fenêtre le bouton **Installer** est également disponible. Ce bouton est réservé pour l'installation de l'Agent Dr.Web à distance en utilisant le Centre de gestion de la sécurité Dr.Web.
12. La marche à suivre pour installer le logiciel de l'Agent Dr.Web est décrite dans le **Manuel Utilisateur** pour les OS correspondants.

Paramètres de connexion au Serveur Dr.Web

- **Postes tournant sous l'OS Windows**

  En cas de l'installation de l'Agent Dr.Web sur les postes tournant sous OS Windows à l'aide du package d'installation personnel, la configuration supplémentaire n'est pas requise. Les paramètres de connexion au Serveur et les paramètres d'authentification du poste sur le Serveur sont inclus directement dans le package d'installation personnel. Après l'installation de l'Agent, le poste va se connecter au Serveur automatiquement.

- **Postes tournant sous OS Android**

  1. Sur l'écran principal de l'appareil mobile, ouvrez le menu de l'application Antivirus Dr.Web et sélectionnez l'élément **Paramètres**.
  2. Sur l'écran **Dr.Web – Paramètres**, dans la rubrique **Mode**, cochez la case **Agent Dr.Web**.
  3. De tels paramètres de connexion au Serveur comme l'adresse IP et les paramètres d'authentification sur le Serveur sont spécifiés automatiquement depuis le fichier de configuration `install.cfg`.

     Pour utiliser le fichier, placez-le dans un répertoire de premier niveau d'emboîtement sur la carte SD. Si le fichier est téléchargé sur l'appareil, les champs de saisie de paramètres de connexion au Serveur seront remplis automatiquement.
  4. Cliquez sur **Se connecter**.

- **Postes tournant OS X**

  1. Dans le menu de l'application Antivirus Dr.Web, cliquez sur **Paramètres** et sélectionnez la rubrique **Mode**.
  2. Cochez la case **Activer le mode de protection centralisée**.
  3. De tels paramètres de connexion au Serveur comme l'adresse IP et les paramètres d'authentification sur le Serveur sont spécifiés automatiquement depuis le fichier de configuration `install.cfg`.

  Pour utiliser le fichier :

  a) Dans le Gestionnaire de licences cliquez sur **Autres types d'activation**.

  b) Faites un glisser-déposer du fichier contenant les paramètres dans la fenêtre qui s'ouvre ou cliquez sur la zone pointillée pour ouvrir la fenêtre de sélection du fichier.

  Après la connexion du fichier, les champs de saisie de paramètres de connexion au Serveur seront remplis automatiquement.

- **Postes tournant sous OS de la famille Linux**

  1. Dans le menu de l'application Dr.Web pour Linux, cliquez sur **Paramètres** et sélectionnez la section **Mode**.
  2. Cochez la case **Activer le mode de protection centralisée**.
  3. Dans la liste déroulante, sélectionnez l'élément **Télécharger depuis le fichier** et specifiez le chemin vers le fichier de configuration `install.cfg`. Dans ce cas, les paramètres de connexion au Serveur (l'adresse IP et les paramètres d'authentification sur le Serveur) seront remplis automatiquement.
  4. Cliquez sur **Connecter**.

4.2.2.2. Installation de l'Agent Dr.Web avec l'installateur

L'installateur de l'Agent se distingue du package d'installation par ce qu'il n'inclut pas les paramètres de connexion au Serveur et les paramètres d'authentification du poste sur le Serveur.

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

Pour obtenir les installateurs sous les OS autres que Windows et pour installer la distribution complète, l'installation de la distribution supplémentaire (extra) du Serveur Dr.Web est requise.

Installation en mode local sur les postes tournant sous les OS Android, OS Linux, OS X

L'installateur pour l'installation de l'Agent Dr.Web, équivalent à l'installateur de la version autonome, est disponible pour les postes tournant sous les OS Android, Linux, OS X.

L'installation de l'Agent Dr.Web en mode local sur le poste de travail est décrite dans le **Manuel Utilisateur** pour les OS correspondants.

Si l'installation est effectuée à l'aide de l'installateur sans fichier de configuration, vous serez obligé de spécifier l'adresse du Serveur sur le poste manuellement pour que le poste soit connecté.

Vous pouvez spécifier manuellement ou ne pas spécifier les paramètres d'authentification. Les options suivantes de connexion au Serveur sont possibles :

Variante de tâche	Paramètres d'authentification
Spécifié manuellement	Une tentative d'authentification automatique d'après les paramètres d'authentification s'effectue.
Non spécifié	Le principe d'authentification sur le Serveur dépend des paramètres du Serveur pour la connexion de nouveaux postes (pour en savoir plus, voir **Manuel Administrateur**, p. Politique d'approbation des nouveaux postes).

Pour spécifier les paramètres d'authentification manuellement, il est nécessaire de créer un nouveau compte du poste dans le Centre de gestion de la Sécurité. Dans ce cas, un package d'installation contenant un fichier de configuration avec les paramètres de connexion et d'authentification sera disponible. Il est recommandé d'utiliser le package d'installation au lieu de l'installateur.

Installation en mode local sur les postes tournant sous l'OS Windows

Les types suivants des installateurs de l'Agent Dr.Web sont fournis :

- *l'installateur réseau* `drwinst.exe` n'installe que l'Agent. Après la connexion au Serveur, l'Agent télécharge et installe les composants correspondants de ce package antivirus.
- *l'installateur complet* `drweb-esuite-agent-full-`*<version_de_l'Agent>*`-`*<version_de_l'assemblage>*`-windows.exe` effectue l'installation de l'Agent et du package antivirus en même temps.

Lors de l'installation via ces installateurs, vous pouvez ne pas spécifier les paramètres de connexion au Serveur ainsi que les paramètres d'authentification ou vous pouvez les spécifier manuellement.

Pour spécifier les paramètres d'authentification manuellement, il est nécessaire de créer un nouveau compte du poste dans le Centre de gestion de la Sécurité. Dans ce cas, un package d'installation sera disponible. S'il n'y a pas de nécessité d'installer à l'aide de la distribution complète ou de l'installateur réseau, il est recommandé d'utiliser le package d'installation au lieu de l'installateur.

Les options suivantes de connexion au Serveur sont possibles :

Variante de tâche	Adresse du Serveur	Paramètres d'authentification
Spécifié manuellement	Le poste se connecte directement au Serveur spécifié.	Une tentative d'authentification automatique d'après les paramètres d'authentification s'effectue.
Non spécifié	L'Agent recherche le Serveur dans le réseau en utilisant le *Service de détection de Serveur*. Une tentative de connexion au premier Serveur trouvé s'effectue.	Le principe d'authentification sur le Serveur dépend des paramètres du Serveur pour la connexion de nouveaux postes (pour en savoir plus, voir **Manuel Administrateur**, p. Politique d'approbation des nouveaux postes).

Les options de l'installation de l'Agent Dr.Web à l'aide de l'installateur complet et du package d'installation sont décrites dans le **Manuel Utilisateur** pour l'OS Windows.

Il est recommandé que l'installation via l'installateur réseau soit effectuée par l'administrateur du réseau antivirus.

Installation en mode local avec l'installateur réseau sous l'OS Windows

L'installateur réseau de l'Agent `drwinst.exe` est fourni pour l'installation de l'Agent uniquement sur les postes tournant sous l'OS Windows.

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

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

1. *Mode Tâche de fond* est lancé si la clé du mode Tâche du fond est spécifiée.
2. *Mode Graphique* est spécifié par défaut. Il est lancé si la clé du mode Tâche du fond n'est pas spécifiée.

Vous pouvez également installer l'Agent Dr.Web sur le poste de manière distante via le Centre de gestion, (voir p. Installation à distance de l'Agent Dr.Web).

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

1. Sur le poste sur lequel vous souhaitez installer l'antivirus, ouvrez le répertoire réseau d'installation de l'Agent (en cas d'installation du Serveur, c'est le sous-répertoire `Installer` dans le répertoire d'installation du Serveur. Vous pourrez le déplacer ultérieurement) ou téléchargez le fichier exécutable de l'installateur `drwinst.exe` et la clé de chiffrement publique `drwcsd.pub` depuis la page d'installation du Centre de gestion. Lancez le fichier `drwinst.exe` avec la clé du mode Tâche de fond `/silent yes`.

   Par défaut, le fichier `drwinst.exe` lancé sans paramètres de connexion au Serveur utilise le mode *Multicast* pour scanner le réseau afin de trouver des Serveurs Dr.Web actifs et tente d'installer l'Agent depuis le premier Serveur trouvé dans le réseau.

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

   Le fichier `drwinst.exe` peut également être lancé avec les paramètres avancés de la ligne de commande suivants :

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

   ```
   drwinst /silent yes /server <nom_DNS_du_Serveur>
   ```

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

   - Vous pouvez aussi spécifier l'adresse du Serveur de façon explicite, par exemple :

   ```
   drwinst /silent yes /server 192.168.1.3
   ```

   - L'utilisation de la clé `/regagent yes` permet d'enregistrer l'Agent lors de l'installation dans la liste d'ajout/suppression de programmes.

Vous pouvez consulter la liste complète des paramètres de l'Installateur réseau dans les **Annexes**, p. H2. Installateur réseau.

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

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

Sur le poste sur lequel vous souhaitez installer l'antivirus, ouvrez le répertoire réseau d'installation de l'Agent (en cas d'installation du Serveur, c'est le sous-répertoire `Installer` dans le répertoire d'installation du Serveur. Vous pourrez le déplacer ultérieurement) ou téléchargez le fichier exécutable de l'installateur `drwinst.exe` et la clé de chiffrement publique `drwcsd.pub` depuis la page d'installation du Centre de gestion. Lancez le fichier `drwinst.exe`.

La fenêtre de l'assistant d'installation de l'Agent Dr.Web va s'ouvrir. Les actions suivantes pour installer l'Agent sur le poste à l'aide de l'installateur réseau en mode graphique sont équivalentes aux actions d'installation à l'aide du package d'installation, mais sans paramètres de connexion au Serveur, s'ils n'ont pas été spécifiés dans la clé correspondante de la ligne de commande.

L'installation de l'Agent sur les postes de travail est décrite dans le manuel **Agent Dr.Web® pour Windows. Manuel Utilisateur**.

4.2.3. Installation à distance de l'Agent Dr.Web sous OS Windows®

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

L'installation à distance peut être effectuée en modes suivants :

- Depuis le Centre de gestion.
- Avec le service Active Directory, si ce service est utilisé dans le réseau local protégé.

L'installation à distance des Agents Dr.Web n'est possible que sur les postes tournant sous un OS de la famille Windows (voir **Annexes**, p. Annexe A. Liste complète des OS supportés), sauf les éditions Starter et Home.

L'installation à distance des Agents Dr.Web est possible uniquement depuis le Centre de gestion lancé sous un OS de la famille Windows (voir **Annexes**, p. Annexe A. Liste complète des OS supportés).

Les droits d'administrateur pour les postes de travail sont requis pour pouvoir installer à distance l'Agent Dr.Web sur ces postes.

Lors de l'installation à distance depuis le Centre de gestion, il est nécessaire d'activer le partage de fichiers et d'imprimantes sur les postes (l'emplacement du paramètre sous différentes versions de Windows est indiqué dans le tableau ci-dessous) si les postes de travail font partie du domaine et le compte administrateur de domaine est utilisé pour l'installation.

Dans le cas où le poste distant n'appartient pas au domaine ou en cas d'utilisation du compte local pour l'installation, sous certaines versions de Windows, un paramétrage supplémentaire de postes distants sera nécessaire.

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

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

Après la configuration du poste distant il est recommandé de réinitialiser tous les paramètres modifiés et de reprendre les valeurs initiales pour ne pas bousculer la politique de base du système d'exploitation.

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

OS	**Configuration**	
Windows XP	Configurez le mode d'accès aux fichiers partagés	Nouveau style : **Démarrer** → **Configuration** → **Panneau de configuration** → **Apparence et thèmes** → **Options des dossiers** → Onglet **Affichage** → Décochez la case **Utiliser le partage de fichiers simple (recommandé)**
		Style classique : **Démarrer** → **Configuration** → **Panneau de configuration** → **Options des dossiers** → Onglet **Affichage** → Décochez la case **Utiliser le partage de fichiers simple (recommandé)**
	Configurez le mode d'authentification réseau	Nouveau style :

OS	Configuration	
	dans les stratégies locales	**Démarrer → Configuration → Panneau de configuration → Performances et maintenance → Outils d'administration → Stratégie de sécurité locale → Paramètres de sécurité → Stratégies locales → Options de sécurité → Accès réseau : modèle de partage et de sécurité pour les comptes locaux → Classique – les utilisateurs locaux s'authentifient eux-mêmes**.
		Style classique : **Démarrer → Configuration → Panneau de configuration → Outils d'administration → Stratégie de sécurité locale → Paramètres de sécurité → Stratégies locales → Options de sécurité → Accès réseau : modèle de partage et de sécurité pour les comptes locaux → Classique – les utilisateurs locaux s'authentifient eux-mêmes**.
	Désactiver Windows Firewall sur le poste avant l'installation à distance.	
Windows Server 2003	Désactiver Windows Firewall sur le poste avant l'installation à distance.	
Windows Vista Windows Server 2008	Activer le partage de fichiers	Nouveau style : **Démarrer → Configuration → Panneau de configuration → Réseau et Internet → Centre Réseau et partage → Partage et découverte → Partage de fichiers → Activer**.
		Style classique : **Démarrer → Configuration → Panneau de configuration → Centre Réseau et partage → Partage et découverte → Partage de fichiers → Activer**.
	Configurez le mode d'authentification réseau dans les stratégies locales	Nouveau style : **Démarrer → Configuration → Panneau de configuration → Système et maintenance → Outils d'administration → Stratégie de sécurité locale → Paramètres de sécurité → Stratégies locales → Paramètres de sécurité → Accès réseau : modèle de partage et de sécurité pour les comptes locaux → Classique – les utilisateurs locaux s'authentifient eux-mêmes**.
		Style classique : **Démarrer → Panneau de configuration → Outils d'administration → Stratégie de sécurité locale → Paramètres de sécurité → Stratégies locales → Paramètres de sécurité → Accès réseau : modèle de partage et de sécurité pour les comptes locaux → Classique – les utilisateurs locaux s'authentifient eux-mêmes**.
	Créer la clé **LocalAccountTokenFilterPolicy** :	

<table>
<tr><th>OS</th><th colspan="2">Configuration</th></tr>
<tr><td></td><td colspan="2">a) Dans l'éditeur d'enregistrement, ouvrez la branche HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System. Si l'enregistrement LocalAccountTokenFilterPolicy n'existe pas, dans le menu Editer, sélectionnez Ajouter et indiquez la valeur DWORD. Entrez la valeur LocalAccountTokenFilterPolicy et cliquez sur ENTRER.
b) Dans le menu contextuel de l'élément LocalAccountTokenFilterPolicy, sélectionnez Modifier.
c) Dans le champ Valeur, indiquez la valeur 1 et cliquez sur OK.
Le redémarrage n'est pas requis.</td></tr>
<tr><td rowspan="4">Windows 7

Windows Server 2008 R2</td><td rowspan="2">Activer le partage de fichiers et d'imprimantes</td><td>Nouveau style :

Démarrer → Panneau de configuration → Réseau et Internet → Centre Réseau et partage → Modifier les paramètres de partage avancés → Partage de fichiers et d'imprimantes → Activer le partage de fichiers et d'imprimantes.</td></tr>
<tr><td>Style classique :

Démarrer → Panneau de configuration → Centre Réseau et partage → Modifier les paramètres de partage avancés → Partage de fichiers et d'imprimantes → Activer le partage de fichiers et d'imprimantes.</td></tr>
<tr><td rowspan="2">Configurez le mode d'authentification réseau dans les stratégies locales</td><td>Nouveau style :

Démarrer → Panneau de configuration → Système et sécurité → Outils d'administration → Stratégie de sécurité locale → Paramètres de sécurité → Stratégies locales → Paramètres de sécurité → Accès réseau : modèle de partage et de sécurité pour les comptes locaux → Classique – les utilisateurs locaux s'authentifient eux-mêmes.</td></tr>
<tr><td>Style classique :

Démarrer → Panneau de configuration → Outils d'administration → Stratégie de sécurité locale → Paramètres de sécurité → Stratégies locales → Paramètres de sécurité → Accès réseau : modèle de partage et de sécurité pour les comptes locaux → Classique – les utilisateurs locaux s'authentifient eux-mêmes.</td></tr>
<tr><td colspan="2">Créer la clé LocalAccountTokenFilterPolicy :
a) Dans l'éditeur d'enregistrement, ouvrez la branche HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System. Si l'enregistrement LocalAccountTokenFilterPolicy n'existe pas, dans le menu Editer, sélectionnez Ajouter et indiquez la valeur DWORD. Entrez la valeur LocalAccountTokenFilterPolicy et cliquez sur ENTRER.</td></tr>
</table>

<table>
<tr><th>OS</th><th colspan="2">Configuration</th></tr>
<tr><td></td><td colspan="2">b) Dans le menu contextuel de l’élément LocalAccountTokenFilterPolicy, sélectionnez Modifier.
c) Dans le champ Valeur, indiquez la valeur 1 et cliquez sur OK.
Le redémarrage n’est pas requis.</td></tr>
<tr><td rowspan="4">Windows 8
Windows 8.1
Windows Server 2012
Windows Server 2012 R2
Windows 10</td><td rowspan="2">Activer le partage de fichiers et d’imprimantes</td><td>Nouveau style :
Paramètres → Panneau de configuration → Réseau et Internet → Centre Réseau et partage → Modifier les paramètres de partage avancés → Partage de fichiers et d’imprimantes → Activer le partage de fichiers et d’imprimantes.</td></tr>
<tr><td>Style classique :
Paramètres → Panneau de configuration → Centre Réseau et partage → Modifier les paramètres de partage avancés → Partage de fichiers et d’imprimantes → Activer le partage de fichiers et d’imprimantes.</td></tr>
<tr><td rowspan="2">Configurez le mode d’authentification réseau dans les stratégies locales</td><td>Nouveau style :
Paramètres → Panneau de configuration → Système et sécurité → Outils d’administration →Stratégie de sécurité locale →Paramètres de sécurité →Stratégies locales →Paramètres de sécurité →Accès réseau : modèle de partage et de sécurité pour les comptes locaux →Classique – les utilisateurs locaux s’authentifient eux-mêmes.</td></tr>
<tr><td>Style classique :
Paramètres → Panneau de configuration → Outils d’administration → Stratégie de sécurité locale → Paramètres de sécurité → Stratégies locales → Paramètres de sécurité → Accès réseau : modèle de partage et de sécurité pour les comptes locaux → Classique – les utilisateurs locaux s’authentifient eux-mêmes.</td></tr>
<tr><td colspan="2">Créer la clé LocalAccountTokenFilterPolicy :
a) Dans l’éditeur d’enregistrement, ouvrez la branche HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System. Si l’enregistrement LocalAccountTokenFilterPolicy n’existe pas, dans le menu Editer, sélectionnez Ajouter et indiquez la valeur DWORD. Entrez la valeur LocalAccountTokenFilterPolicy et cliquez sur ENTRER.
b) Dans le menu contextuel de l’élément LocalAccountTokenFilterPolicy, sélectionnez Modifier.
c) Dans le champ Valeur, indiquez la valeur 1 et cliquez sur OK.
Le redémarrage n’est pas requis.</td></tr>
</table>

Dans le cas où le compte se trouvant sur le poste local n'a pas de mot de passe, spécifiez dans les politiques locales une stratégie d'accès sans mot de passe : **Panneau de configuration → Outils d'administration → Stratégie de sécurité locale → Paramètres de sécurité → Stratégies locales → Options de sécurité → Comptes : restreindre l'utilisation de mots de passe vierge par le compte local à l'ouverture de session console → Désactiver**.

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

4.2.3.1. Installation de l'Agent Dr.Web via le Centre de gestion de la sécurité Dr.Web

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

1. Installation avec le Scanner réseau.

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

2. Installation avec l'outil Installation via réseau.

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

3. Installation sur les postes avec les ID spécifiés.

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

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

Utilisation du Scanner Réseau

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

Afin d'effectuer une installation rapide du logiciel de l'Agent sur les postes de travail, il est recommandé d'utiliser le Scanner réseau (voir **Guide d'installation**, art. Scanner réseau) qui recherche les postes par leurs adresses IP.

Pour installer l'Agent avec le Scanner réseau :

1. Ouvrez le Scanner réseau. Pour ce faire, sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion et depuis la fenêtre qui apparaît sélectionnez l'élément du menu de gestion Scanner réseau. Une fenêtre vide portant le même nom s'ouvrira.
2. 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.

   Pour une description détaillée des paramètres avancés, consultez la rubrique **Manuel Administrateur**, p. Scanner réseau.
4. Cliquez sur le bouton **Scanner**. L'arborescence dans laquelle il est indiqué pour chaque poste si l'antivirus est installé ou pas sera téléchargée dans la fenêtre.
5. 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 4-1. 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.
	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.

Icône	Description
	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.

6. Dans la fenêtre du **Scanner réseau**, sélectionnez un ordinateur non protégé (ou plusieurs ordinateurs non protégés en utilisant les boutons CTRL ou SHIFT).
7. Dans la barre d'outils, cliquez sur le bouton  **Installer l'Agent Dr.Web**.
8. La fenêtre **Installation via réseau** va s'afficher pour créer la tâche d'installation de l'Agent.
9. Dans le champ **Adresses des postes**, spécifiez les adresses IP ou les noms DNS des ordinateurs sur lesquels vous souhaitez installer l'Agent Dr.Web. Si vous spécifiez plusieurs adresses, utilisez « ; » ou « , » pour les séparer (le nombre d'espaces n'a pas d'importance).

   En cas d'installation sur les postes trouvés avec le Scanner Réseau, l'adresse du poste ou des plusieurs postes sur lesquels sera effectuée l'installation sera indiquée dans le champ **Adresses des postes**.

   En cas d'installation de l'Agent sur plusieurs postes à la fois, vous pouvez spécifier plusieurs adresses IP au format suivant :

   - espacé par un trait d'union (par exemple, `10.4.0.1-10.4.0.10`),
   - espacé par une virgule 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`).
10. Par défaut, le logiciel de l'Agent sera installé sur le poste, dans le répertoire `C:\Program Files\DrWeb`. Si nécessaire, vous pouvez spécifier un autre chemin dans le champ **Répertoire d'installation de l'Agent Dr.Web**.

    Il est recommandé de spécifier le chemin complet pour la détermination exacte de l'emplacement du répertoire d'installation. Lors de la spécification, les variables d'environnement peuvent être utilisées.
11. Par défaut, dans le champ **Serveur Dr.Web**, s'affiche l'adresse IP ou le nom DNS du Serveur Dr.Web auquel le Centre de gestion est connecté. Si nécessaire, spécifiez dans ce champ l'adresse du Serveur depuis lequel le logiciel antivirus sera installé. Utilisez « ; » ou « , » pour séparer plusieurs Serveurs (le nombre d'espaces avant et après le séparateur n'a pas d'importance). Laissez le champ vide pour utiliser le service de détection du Serveur Dr.Web.
12. Dans le champ **Clé publique de chiffrement**, spécifiez le chemin vers la clé publique de chiffrement du Serveur Dr.Web.
13. Dans le champ **Fichier exécutable de l'installateur réseau**, spécifiez le chemin vers l'Installateur réseau de l'Agent Dr.Web.

Si la clé publique de chiffrement et le fichier exécutable de l'Installateur réseau sont placés dans la ressource partagée, les chemins doivent être spécifiés au format d'adresses réseau.

14. Dans le menu déroulant **Langue**, sélectionnez la langue de l'interface de l'Antivirus Dr.Web qui sera installé sur les postes.
15. Si nécessaire, dans le champ **Paramètres avancés** saisissez les paramètres de la ligne de commande pour le lancement de l'Installateur réseau (pour en savoir plus, voir les **Annexes**, p. H2. Installateur réseau).
16. Dans le champ **Timeout d'installation (s)**, spécifiez un délai d'attente maximum avant la fin d'installation de l'Agent en secondes. Les valeurs admissibles sont les suivantes : 1-600. Par défaut, le délai de 180 secondes est spécifié. En cas de faible bande passante de la connexion entre le Serveur et l'Agent, il est recommandé d'augmenter la valeur spécifiée par défaut.
17. Si nécessaire, cochez la case **Enregistrer l'Agent Dr.Web dans la liste des logiciels installés**.
18. Dans la rubrique **Composants à installer**, sélectionnez les composants du package antivirus à installer sur les postes.
19. Dans les rubriques **Compression** et **Chiffrement**, spécifiez les paramètres de la compression et du chiffrement utilisés par l'Installateur réseau lors de l'installation de l'Agent et du package antivirus. Ces paramètres seront également utilisés pour l'interaction entre l'Agent et le Serveur lors de l'installation.
20. Dans la rubrique **Authentification sur les postes distants**, spécifiez les paramètres d'authentification nécessaires pour accéder au postes distants sur lesquels l'Agent sera installé.

    Il est possible de spécifier plusieurs comptes administrateur. Pour ajouter encore un compte, cliquez sur  et remplissez les champs relatifs à l'authentification. De façon analogique pour chaque nouvelle entrée.

    Lors de l'installation de l'Agent, c'est le premier compte de la liste qui est utilisé en premier lieu. Si l'installation sous ce compte a échoué, le compte suivant sera utilisé, etc.
21. Après avoir spécifié tous les paramètres nécessaires, cliquez sur le bouton **Installer**.

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

22. L'Agent Dr.Web sera installé sur les postes spécifiés. Après l'approbation du poste sur le Serveur (si l'approbation est requise selon la configuration du Serveur Dr.Web, voir aussi le **Manuel administrateur** p. Politique de connexion des postes), le package antivirus sera installé de manière automatique.
23. Redémarrez l'ordinateur selon la requête de l'Agent.

Utilisation de l'outil Installation via réseau

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

Pour effectuer une installation via réseau, procédez comme suit :

1. Dans le menu principal, sélectionnez l'élément **Administration** puis dans la fenêtre qui s'affiche, sélectionnez l'élément du menu de gestion **Installation via réseau**.
2. Les étapes suivantes sont équivalentes aux étapes **8-22** ci-dessus.

Installation pour les comptes avec les ID spécifiés

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

1. En cas de création d'un nouveau compte de poste :
   a) Créez un nouveau compte ou plusieurs comptes pour les postes de travail (voir Création d'un nouveau compte).
   b) Immédiatement après la création du compte, dans la partie droite de la fenêtre principale, le panneau au titre **Création d'un poste** va s'afficher. Cliquez sur **Installer**.
   c) La fenêtre du Scanner réseau va s'afficher.
   d) Les étapes suivantes sont équivalentes aux étapes **2-22** ci-dessus.
   e) Après la fin de l'installation, vérifiez que les icônes se trouvant contre les postes en question dans l'arborescence ont été changées.
2. En cas d'utilisation d'un compte de poste existant :
   a) Dans l'arborescence du réseau antivirus, sélectionnez un nouveau poste ou un groupe des postes pour lesquels les Agents n'ont pas encore été installés, vous pouvez également sélectionner le groupe **New** (pour l'installation vers tous les nouveaux comptes).
   b) Dans la barre d'outils, cliquez sur **Installer l'Agent Dr.Web**.
   c) La fenêtre du Scanner réseau va s'afficher.
   d) Les étapes suivantes sont équivalentes aux étapes **2-22** ci-dessus.
   e) Après la fin de l'installation, vérifiez que les icônes se trouvant contre les postes en question dans l'arborescence ont été changées.

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

En cas d'erreurs lors de l'installation à distance, consultez la rubrique **Annexes** Diagnostic des problèmes d'installation à distance.

4.2.3.2. Installation de l'Agent Dr.Web avec le service Active Directory

Si le service **Active Directory** est utilisé dans le réseau local protégé, vous pouvez installer l'Agent Dr.Web sur les postes de manière distante.

Il est possible d'installer l'Agent via Active Directory en utilisant le système de fichiers distribué DFS (voir les **Annexes**, p. Utilisation de DFS lors de l'installation de l'Agent via Active Directory).

Installation de l'Agent

Pour installer l'Agent avec Active Directory :

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

Lors de la mise à jour du Serveur, la mise à jour de l'installateur de l'Agent Dr.Web pour les réseaux avec Active Directory n'est pas obligatoire. Après la mise à jour du logiciel du Serveur, les Agents et le logiciel antivirus sur les postes seront mis à jour automatiquement après l'installation.

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

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

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

La clé `/a` lance le déploiement du package administrateur.

Nom du package

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

`drweb-esuite-agent-activedirectory-<version>-<date-de-sortie>.msi`

Paramètres

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

- `ESSERVERADDRESS=<nom_DNS>` – l'adresse du Serveur Dr.Web auquel l'Agent va se connecter. Pour en savoir plus sur les formats possibles, consultez les **Annexes**, p. Annexe E2.
- `ESSERVERPATH=<chemin_nom_du_fichier>` – le chemin complet vers la clé publique de chiffrement du Serveur Dr.Web et le nom du fichier (par défaut c'est le fichier `drwcsd.pub` dans le sous-dossier `Installer` du répertoire d'installation du Serveur Dr.Web).

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

  Avant l'installation en mode administrateur, il ne faut pas placer manuellement les fichiers pour l'installation dans le répertoire cible pour l'image de l'Agent (voir le paramètre TARGETDIR). L'installateur de l'Agent pour les réseaux avec Active Directory (<*nom_du_package*>.msi) et les autres fichiers requis pour l'installation des Agents sur les postes de travail seront placés automatiquement dans le répertoire cible lors de l'installation en mode administrateur. Si avant l'installation en mode administrateur, le répertoire cible contient déjà ces fichiers, par exemple, ils sont restés des installations précédentes, les fichiers portant le même nom seront réécrits.

  S'il est nécessaire d'effectuer l'installation en mode administrateur depuis les Serveurs différents, il est recommandé de spécifier les répertoires différents pour chaque Serveur.

  Après le déploiement du package administrateur, le répertoire <*répertoire_cible*>\Program Files\DrWeb ne doit contenir que le fichier README.txt.

Exemples :

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

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

Les mêmes paramètres peuvent être spécifiés dans le mode graphique de l'installateur.

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

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

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

Après le déploiement du package administrateur, le répertoire :

<*répertoire_cible*>\Program Files\DrWeb

ne doit contenir que le fichier README.txt.

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

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

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

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

3. Dans la nouvelle fenêtre, spécifiez le nom DNS ou l'adresse IP du Serveur Dr.Web (voir **Annexes**, p. Annexe E2). Spécifiez également l'emplacement de la clé publique du Serveur Dr.Web (`drwcsd.pub`). Cliquez ensuite sur le bouton **Suivant**.
4. Dans la fenêtre suivante, spécifiez le répertoire réseau vers lequel l'image de l'Agent sera enregistré. Le chemin vers l'image doit être spécifié au format adresse réseau même si le répertoire se trouve sur la machine locale ; ce répertoire doit être accessible depuis les postes ciblés. Cliquez ensuite sur **Installer**.
5. Après la fin de l'installation, la fenêtre de configuration permettant de spécifier l'installation des packages sur les postes dans le réseau sera affichée de manière automatique.

Configuration de l'installation du package sur les postes sélectionnés

1. Dans le **Panneau de configuration** (ou dans le menu **Démarrer** sous Windows Server 2003/2008/2012/2012R2, dans le menu **Démarrer** → **Tous les programmes** sous Windows Server 2000) sélectionnez **Administration** → **Active Directory – utilisateurs et ordinateurs** (en mode graphique de l'installation de l'Agent cette fenêtre s'affiche de manière automatique).
2. Dans le domaine contenant les ordinateurs sur lesquels les Agents Dr.Web seront installés, créez une nouvelle **Unité** (sous Windows Server 2000 – **Unité d'organisation**) nommée par exemple **ESS**. Pour ce faire, dans le menu contextuel, sélectionnez **Créer** → **Unité**. Dans la fenêtre qui s'affiche, entrez le nom de cette nouvelle unité et cliquez sur **OK**. Ajoutez à cette unité les ordinateurs sur lesquels vous souhaitez installer l'Agent.
3. Ouvrez la fenêtre d'édition des politiques de groupe. Pour cela, procédez comme suit :
   a) sous Windows Server 2000/2003 : dans le menu contextuel de l'unité créée **ESS**, sélectionnez l'élément **Propriétés**. Dans la fenêtre qui apparaît, passez à l'onglet **Politique de groupe**.
   b) sous Windows 2008/2012/2012R2 : cliquez sur **Démarrer** → **Administration** → **Gestion de la politique de groupe**.
4. Spécifiez une politique de groupe pour l'unité créée. Pour cela, procédez comme suit :
   a) Sous Windows 2000/2003 : double cliquez sur le bouton **Ajouter** et créez un élément de la liste avec le nom de la politique **ESS**. Double cliquez sur cet élément.
   b) Sous Windows 2008/2012/2012R2 : dans le menu contextuel de l'unité **créée ESS**, sélectionnez l'élément **Créer un objet GPO dans ce domaine, et le lier**. Dans la fenêtre qui apparaît, spécifiez le nom du nouvel objet de la politique de groupe et cliquez ensuite sur **OK**. Dans le menu contextuel de la nouvelle politique, sélectionnez l'élément **Modifier**.

5. La fenêtre **Éditeur d'objets de stratégie de groupe** sera ouverte, spécifiez les paramètres relatifs à la politique de groupe créée à l'étape **4**. Pour ce faire, procédez comme suit :
   a) Sous Windows 2000/2003 : depuis l'arborescence sélectionnez l'élément **Configuration ordinateur → Paramètres du logiciel → Installations des logiciels**.
   b) Sous Windows 2008/2012/2012R2 : depuis l'arborescence sélectionnez l'élément **Configuration ordinateur → Stratégies → Paramètres du logiciel → Installations des logiciels**.
6. Dans le menu contextuel de l'élément **Installations des logiciels**, sélectionnez l'élément **Créer → Package**.
7. Spécifiez le package d'installation de l'Agent. Pour cela, spécifiez l'adresse de la ressource réseau partagée (image de l'Agent créé lors de l'installation en mode administrateur). Le chemin vers le répertoire contenant le package doit être spécifié au format adresse réseau même si le répertoire se trouve sur la machine locale.
8. La fenêtre **Déploiement du logiciel** s'affiche. Sélectionnez l'option **Attribués**. Cliquez sur **OK**.
9. L'élément **Dr.Web Agent** sera présent dans la fenêtre de l'éditeur d'objets de stratégie de groupe. Depuis le menu contextuel de cet élément sélectionnez **Propriétés**.
10. Dans la fenêtre de propriétés du package qui apparaît, passez à l'onglet **Déploiement**. Cliquez sur le bouton **Avancé**.
11. La fenêtre **Options de déploiement avancées** sera ouverte.
    - Cochez la case **Ignorer la langue lors du déploiement**.
    - Si vous planifiez l'installation de l'Agent Dr.Web avec un package msi configurable sur les OS 64 bits, activez la case **Rendre cette application 32 bits disponible sur les ordinateurs x64**.
12. Double cliquez sur **OK**.
13. L'Agent Dr.Web sera installé sur les postes sélectionnés au prochain enregistrement dans le domaine.

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

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

1. **L'Agent Dr.Web n'est pas présent sur le poste**.

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

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

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

Afin d'installer l'Agent via Active Directory, il est nécessaire de supprimer l'Agent de manière manuelle (ou avec le Centre de gestion) et de redéterminer les stratégies Active Directory pour le poste en question.

3. **L'Agent Dr.Web est déjà installé sur le poste avec l'utilisation du service Active Directory**.

   Il est impossible de redéterminer la stratégie pour le poste avec l'Agent Dr.Web installé via le service Active Directory.

   Ainsi, la détermination des stratégies ne va pas influencer le statut du logiciel antivirus sur le poste.

4.3. Installation de NAP Validator

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

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

Marche à suivre pour installer NAP Validator :

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

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

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

4.4. Installation du Serveur proxy

Le réseau antivirus peut comprendre un ou plusieurs Serveurs proxy.

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

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

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** (voir le **Manuel Administrateur**, la rubrique Configuration du Serveur Dr.Web → Général).

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

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

1. Lancez le fichier de la distribution. La fenêtre de l'assistant **InstallShield Wizard** va s'ouvrir. Cliquez sur **Suivant**.
2. La fenêtre affichant le texte du Contrat de Licence apparaît. Après avoir pris connaissance des termes de ce Contrat, cochez la case **I accept the terms of the license agreement** et cliquez ensuite sur le bouton **Next**.
3. La fenêtre de configuration du Serveur proxy vous permet d'accéder aux paramètres suivants :
   - Dans le champ **Listen to**, spécifiez l'adresse IP « écoutée » par le Serveur proxy. Par défaut c'est – `any (0.0.0.0)` – ce qui signifie « écouter » toutes les interfaces.

     

     Les adresses doivent être spécifiées au format d'adresse réseau décrite dans les **Annexes**, p. Annexe E. Spécification de l'adresse réseau.

   - Dans le champ **Port**, spécifiez le numéro du port qui va "écouter" le Serveur proxy. Par défaut c'est le port `2193`.
   - Cochez la case **Enable discovery** afin d'activer le mode d'imitation du Serveur. Ce mode permet au Scanner réseau de détecter le Serveur proxy en tant que Serveur Dr.Web. Les paramètres suivants sont disponibles pour le mode d'imitation du Serveur :
     - Cochez la case **Enable multicasting** pour que le Serveur proxy réponde aux requêtes broadcast adressées au Serveur.
     - Dans le champ **Multicast group**, entrez l'adresse IP du groupe multi-adresses dont le Serveur proxy fera partie. L'interface spécifiée sera "écoutée" par le Serveur proxy afin d'assurer l'interaction avec les Installateurs réseau lors des recherches dans le réseau des Serveurs Dr.Web actifs. Si vous laissez le champ vide, le Serveur proxy ne sera inclus dans

aucun groupe multi-adresses. Par défaut, le Serveur appartient au groupe multi-adresses `231.0.0.1`.

- Dans la liste déroulante **Compression mode** sélectionnez le mode de compression du trafic pour les canaux entre le Serveur proxy et les clients servis : les Agents et les installateurs des Agents. Dans le champ **Level** spécifiez le niveau de compression. Les nombres entiers de 1 à 9 sont autorisés.

Après avoir spécifié les paramètres généraux cliquez sur **Next**.

4. La fenêtre de configuration de la mise en cache du Serveur proxy va s'afficher :

   Cochez la case **Enable caching** pour mettre en cache les données transmises par le Serveur proxy et spécifiez les paramètres suivants :

   - Pour modifier le répertoire de sauvegarde de données mises en cache spécifié par défaut cliquez sur **Browse** et spécifiez un nouveau répertoire dans l'explorateur.
   - Dans le champ **Maximum revision number** spécifiez le nombre maximum de révisions sauvegardées. Par défaut, les 3 dernières révisions sont sauvegardées, les révisions plus anciennes seront supprimées.
   - Dans le champ **Cleanup interval** spécifiez l'intervalle de temps en minutes entre les suppressions des anciennes révisions. La valeur spécifiée par défaut est 60 minutes.
   - Dans le champ **Unload interval** spécifiez l'intervalle de temps en minutes entre les suppressions des fichiers non utilisés de la mémoire. La valeur spécifiée par défaut est 10 minutes.
   - Dans la liste déroulante **Integrity check mode** sélectionnez le mode de vérification de l'intégrité de cache :
     - **At startup** – au démarrage du Serveur proxy (cela peut prendre un certain temps).
     - **Idle** – lors du fonctionnement du Serveur proxy en tâche de fond.

   Après avoir spécifié les paramètres de mise en cache, cliquez sur **Next**.

5. La fenêtre de configuration de la redirection des connexions va s'afficher :

   Dans le bloc **Redirection settings**, spécifiez l'adresse ou une liste d'adresses de Serveurs Dr.Web vers lesquels connexions établies par le Serveur proxy seront redirigées.

   

   Les adresses doivent être spécifiées au format d'adresse réseau décrite dans les **Annexes**, p. Annexe E. Spécification de l'adresse réseau.

   Dans les listes déroulantes **Compression mode** sélectionnez les modes de compression du trafic pour les canaux de communication entre le Serveur proxy et chaque Serveur Dr.Web.

   Après avoir spécifié les paramètres de redirection, cliquez sur **Next**.

6. La fenêtre de sélection du dossier d'installation va s'ouvrir. Pour modifier le dossier d'installation spécifié par défaut, cliquez sur **Change** et sélectionnez un dossier.

   Cliquez sur **Next**.

7. La fenêtre informant sur la disponibilité de l'installation du Serveur proxy va s'ouvrir. Cliquez alors sur le bouton **Install**.

8. Après la fin de l'installation, cliquez sur le bouton **Finish**.

Après la fin de l'installation, vous pouvez modifier les paramètres du Serveur proxy. Pour ce faire, vous pouvez utiliser le fichier de configuration `drwcsd-proxy.xml` se trouvant dans le répertoire d'installation suivant :

- OS Windows : `C:\ProgramData\Doctor Web\drwcsd-proxy\`
- sous OS Linux et OS Solaris : `/var/opt/drwcs/etc`
- sous OS FreeBSD : `/var/drwcs/etc`

Pour plus d'informations sur les paramètres du fichier de configuration, consultez les **Annexes**, p. Annexe G4.

Marche à suvre pour installer le Serveur proxy sur un ordinateur tournant sous OS de la famille UNIX :

Exécutez la commande suivante :

`sh ./<fichier_de_distribution>.run`

Lors de l'installation du logiciel sous OS **FreeBSD** le script `rc` sera crée : `/usr/local/etc/rc.d/0.dwcp-proxy.sh`.

Utilisez les commandes :

- `/usr/local/etc/rc.d/0.dwcp-proxy.sh stop` – pour arrêter manuellement le Serveur proxy ;
- `/usr/local/etc/rc.d/0.dwcp-proxy.sh start` – pour démarrer manuellement le Serveur proxy.

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

Chapitre 5. Suppression des composants Dr.Web Enterprise Security Suite

5.1. Suppression du Serveur Dr.Web

5.1.1. Suppression du Serveur Dr.Web sous OS Windows®

Afin de désinstaller le logiciel du Serveur Dr.Web (la distribution principale et supplémentaire) ou l'extension pour le Centre de gestion de la sécurité Dr.Web, lancez le package d'installation de la version correspondant à la version installée. L'installateur va détecter le produit installé de manière automatique et proposera de le supprimer. Pour désinstaller le logiciel, cliquez sur le bouton **Supprimer**.

La suppression du logiciel du Serveur Dr.Web (de la distribution principale et supplémentaire) ou de l'extension pour le Centre de gestion de la sécurité Dr.Web peut également être effectuée avec les outils standard de l'OS Windows via l'élément suivant : **Panneau de configuration** → **Ajout/Suppression de programmes**.

En cas de suppression du Serveur, la copie de réserve des fichiers de configuration, des clés de chiffrement et des bases de données est effectuée uniquement si le paramètre Sauvegarder la copie de réserve des données critiques du **Serveur Dr.Web** est activé.

5.1.2. Suppression du Serveur Dr.Web sous les OS de la famille UNIX®

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

Suppression de la distribution principale du Serveur Dr.Web

1. La procédure d'installation du Serveur varie selon le système d'exploitation installé et la version du Serveur installée.

   a) Pour supprimer le Serveur de la version 6 ou antérieure, procédez comme suit :

OS du Serveur		Action
FreeBSD		Exécutez la commande : `pkg_delete drweb-esuite`
Solaris		1. Arrêtez le Serveur : `/etc/init.d/drwcsd stop` 2. Exécutez la commande : `pkgrm DWEBesuit`
Linux	Debian	Exécutez la commande : `dpkg -r drweb-esuite`

OS du Serveur		Action
	Ubuntu	
	package rpm	Exécutez la commande : `rpm -e drweb-esuite`
	package generic	Lancez le script `/opt/drwcs/bin/drweb-esuite-uninstall.sh`

b) Pour supprimer le Serveur de la version 10 ou antérieure, procédez comme suit :

OS du Serveur		Action
FreeBSD		Lancez le script `/usr/local/etc/opt/software/drweb-esuite.remove`
Solaris		1. Arrêtez le Serveur : `/etc/init.d/drwcsd stop` 2. Exécutez la commande : `pkgrm drweb-esuite`
Linux	Debian Ubuntu	Exécutez la commande : `dpkg -P drweb-esuite`
	package rpm	Exécutez la commande : `rpm -e drweb-esuite`
	package generic	Lancez le script `/etc/opt/drweb.com/software/drweb-esuite.remove`

2. Sous l'OS **Solaris**, il est nécessaire de confirmer la suppression du logiciel ainsi que d'accepter l'exécution des scripts de suppression en mode administrateur (**root**).

Lors de la suppression du Serveur sous **FreeBSD** ou **Linux** les processus serveur seront arrêtés automatiquement, la base de données, les fichiers clés et les fichiers de configuration seront sauvegardés dans le répertoire par défaut – `/var/tmp/drwcs`.

Suppression de la distribution supplémentaire du Serveur Dr.Web

1. Pour supprimer la distribution supplémentaire du Serveur de la version 10 ou antérieure, procédez comme suit :

OS du Serveur	Action
FreeBSD	Lancez le script `/usr/local/etc/opt/software/drweb-esuite-extra.remove`
Solaris	1. Arrêtez le Serveur : `/etc/init.d/drwcsd stop` 2. Exécutez la commande : `pkgrm drweb-esuite-extra`

OS du Serveur		Action
Linux	Debian Ubuntu	Exécutez la commande : `dpkg -P drweb-esuite-extra`
	package rpm	Exécutez la commande : `rpm -e drweb-esuite-extra`
	package generic	Lancez le script `/etc/opt/drweb.com/software/drweb-esuite-extra.remove`

2. Sous l'OS **Solaris**, il est nécessaire de confirmer la suppression du logiciel ainsi que d'accepter l'exécution des scripts de suppression en mode administrateur (**root**).

Suppression de l'extension pour le Centre de gestion de la sécurité Dr.Web

Pour supprimer l'extension pour le Centre de gestion de la sécurité Dr.Web, procédez comme suit :

Type de package	Commande
package **deb**	`dpkg -P drweb-esuite-plugins`
package **rpm**	`rpm -e drweb-esuite-plugins`

autres packages (**tar.bz2** et **tar.gz**)	`rm -f <dossier_des_modules>/libnp*.so`
	Par exemple pour le navigateur Mozilla Firefox :
	`rm -f /usr/lib/mozilla/plugins/libnp*.so`

5.2. Suppression de l'Agent Dr.Web

La suppression de l'Agent Dr.Web depuis les postes protégés peut être réalisé par les moyens suivants :

- Pour les postes tournant sous l'OS Windows :
  - Via le Centre de gestion.
  - En mode local sur le poste.
  - Via le service Active Directory, si l'Agent a été installé à l'aide de ce service.
- Pour les postes tournant sous l'OS Android, l'OS Linux, OS X – en mode local sur le poste.

La suppression de l'Agent Dr.Web sur les postes de travail tournant sous l'OS Android,l'OS Linux, OS X est décrite dans le **Manuel Utilisateur** pour le système d'exploitation correspondant.

5.2.1. Suppression de l'Agent Dr.Web sous OS Windows®

Suppression de l'Agent Dr.Web et du package antivirus via réseau

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

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

Marche à suivre pour supprimer l'antivirus du poste en mode distant (uniquement pour les OS Windows) :

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

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

Suppression de l'Agent Dr.Web et du package antivirus en mode local

La suppression locale de l'Agent et du package antivirus est possible à condition que cette option soit autorisée sur le Serveur dans la rubrique **Droits** (voir **Manuel Administrateur**, p. Droits des utilisateurs du poste).

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

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

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

Suppression avec les outils standard de Windows

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

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

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

Suppression avec l'installateur

- **Module client win-es-agent-setup.exe**

  Pour désinstaller le logiciel de l'Agent et le package antivirus avec le module client qui est créé lors de l'installation de l'Agent, lancez le fichier d'installation `win-es-agent-setup.exe` avec le paramètre `/instMode remove`. Si vous souhaitez surveiller la progression du processus de suppression, utilisez le paramètre supplémentaire `/silent no`.

  Le fichier de configuration `win-es-agent-setup.exe` se trouve par défaut dans le répertoire suivant :

  - sous OS Windows XP et OS Windows Server 2003 : `%ALLUSERSPROFILE%\Application Data\Doctor Web\Setup\`
  - sous OS Windows Vista ou supérieur et OS Windows Server 2008 ou supérieur : `%ALLUSERSPROFILE%\Doctor Web\Setup\`

  Par exemple, sous Windows 7, où `%ALLUSERPROFILE%` correspond à `C:\ProgramData`:

  ```
  C:\ProgramData\Doctor Web\Setup\win-es-agent-setup.exe /instMode
  remove /silent no
  ```

- **Package d'installation drweb-ess-installer.exe**

  Pour désinstaller le logiciel de l'Agent et le package antivirus avec le package d'installation, lancez le fichier d'installation `drweb-ess-installer.exe` de la version du produit qui est installée sur votre ordinateur.

- **Installateur complet drweb-esuite-agent-full-<*version_de_l'Agent*>-<*version_de_l'assemblage*>-windows.exe**

  Pour désinstaller le logiciel de l'Agent et le package antivirus avec l'installateur complet, lancez le fichier d'installation `drweb-esuite-agent-full-`<*version_de_l'Agent*>`-`<*version_de_l'assemblage*>`-windows.exe` de la version du produit qui est installée sur votre ordinateur.

- **Installateur réseau drwinst.exe**

  Pour désinstaller le logiciel de l'Agent et le package antivirus avec l'installateur réseau en mode local, il est nécessaire de lancer depuis le répertoire d'installation de l'Agent Dr.Web (par défaut – `C:\Program Files\DrWeb`) l'installateur `drwinst.exe` accompagnée du paramètre `/instMode remove`. Si vous souhaitez surveiller la progression du processus de suppression, utilisez le paramètre `/silent no`.

  Exemple :

  ```
  drwinst /instMode remove /silent no
  ```

  

  Au lancement du package antivirus `drweb-ess-installer.exe`, de l'installateur complet `drweb-esuite-agent-full-<version_de_l'Agent>-<version_de_l'assemblage>-windows.exe` et de l'installateur réseau `drwinst.exe`, le module client `win-es-agent-setup.exe` qui effectue la suppression est lancé.

  Le module client `win-es-agent-setup.exe`, lancé sans paramètres détermine le produit installé et se lance en mode de modification/suppression. Pour le lancer aussitôt en mode de suppression utilisez la clé `/instMode remove`.

5.2.2. Suppression de l'Agent Dr.Web avec le service Active Directory

1. Dans le panneau de configuration sous Windows, sélectionnez l'élément **Administration** puis l'élément **Active Directory** - **utilisateurs et ordinateurs**.
2. Dans le domaine, sélectionnez l'unité d'organisation **ESS** que vous avez créée. Depuis le menu contextuel, sélectionnez l'élément **Propriétés**. La fenêtre **ESS Propriétés** s'ouvre.
3. Passez à l'onglet **Stratégie de groupe**. Sélectionnez l'élément **ESS Stratégies** dans la liste. Double cliquez sur cet élément. La fenêtre **Éditeur d'objets de stratégie de groupe** va s'ouvrir.
4. Dans l'arborescence, sélectionnez **Configuration ordinateur** → **Paramètres du logiciel** → **Installations des logiciels** → **Package**. Puis dans le menu contextuel du package contenant la distribution de l'Agent, sélectionnez **Toutes les tâches** → **Désinstaller** → **OK**.
5. Dans l'onglet **Stratégie de groupe**, cliquez sur **OK**.
6. Agent Dr.Web sera supprimé sur les postes lors du prochain enregistrement dans le domaine.

5.3. Suppression du Serveur proxy

Suppression du Serveur proxy sous Windows

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

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

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

OS du Serveur proxy		Action
FreeBSD		Lancez le script `/usr/local/etc/opt/software/drweb-proxy.remove`
Solaris		Exécutez la commande : `pkgrm drweb-esuite-proxy`
Linux	package deb	Exécutez la commande : `dpkg -P drweb-esuite-proxy`
	package rpm	Exécutez la commande : `rpm -e drweb-esuite-proxy`
	package generic	Lancez le script `/etc/opt/drweb.com/software/drweb-proxy.remove`

Chapitre 6. 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, prenez en compte les particularités suivantes :

- Avant de procéder à la mise à jour, 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.
- En cas de la configuration multi-serveur du réseau antivirus, il faut noter que le transfert des mises à jour entre les Serveurs de la version 10 et les Serveurs des versions 6 ne s'effectue pas et la liaison entre serveurs n'est utilisée que pour le transfert des statistiques. Pour assurer le transfert des mises à jour entre serveurs, il faut mettre à niveau tous les Serveurs. S'il est nécessaire de laisser au sein du réseau antivirus les Serveurs des versions précédentes pour la connexion des Agents installés sur les OS qui ne sont pas supportés par la version 10 (voir le p. Mise à jour des Agents Dr.Web), alors les Serveurs des versions 6 et les Serveurs de la version 10 doivent obtenir des mises à jour séparément.
- Lors de la mise à niveau du Serveur de la version 6 vers la version 10, les paramètres de fonctionnement du Serveur ne sont pas sauvegardés. Après l'installation de la version 10, il est nécessaire de spécifier manuellement les paramètres de connexion via le serveur proxy (voir le **Manuel Administrateur**, p. Proxy).
- Lors de la mise à niveau automatique des Agents, l'ancienne version des Agents est supprimée et l'installation de la nouvelle version s'effectue.La nouvelle version est installée selon la tâche de la planification du Serveur qui sera exécutée après le redémarrage du poste. Il est nécessaire de redémarrer le poste manuellement après la suppression de l'ancienne version de l'Agent.

Après la suppression de l'Agent, une notification sur la nécessité de redémarrage est affichée sur le poste. L'administrateur doit redémarrer le poste lui-même.

Après la suppression de l'ancienne version de l'Agent et jusqu'à l'installation de la nouvelle version, les postes ne sont pas protégés.

6.1. Mise à jour du Serveur Dr.Web sous OS Windows®

La mise à niveau du Serveur depuis la version 6 vers la version 10 et la mise à jour au sein de la version 10 est effectuée automatiquement via l'installateur.

Avant de supprimer le Serveur de la version précédente, merci de lire la rubrique Mise à jour de l'Agent Dr.Web.

La mise à jour du Serveur au sein de la version 10 via le Centre de gestion est également disponible. La procédure est décrite dans le **Manuel Administrateur**, dans la rubrique Mise à

jour du Serveur Dr.Web et restauration depuis une copie de sauvegarde.

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.

Sauvegarde des fichiers de configuration

En cas de suppression du Serveur de la version 6, les fichiers suivants sont sauvegardés automatiquement :

Fichier	Description	Répertoire
`agent.key` (le nom peut varier)	clé de licence de l'Agent	`etc`
`certificate.pem`	certificat SSL	
`drwcsd.conf` (le nom peur varier)	fichier de configuration du Serveur	
`drwcsd.pri`	clé de chiffrement privée	
`enterprise.key` (le nom peut varier)	clé de licence du Serveur	
`private-key.pem`	clé privée RSA	
`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	
`dbinternal.dbs`	BD intégrée	`var`
`drwcsd.pub`	clé de chiffrement publique	• `Installer` • `webmin\install`

En cas de suppression du Serveur de la version 10, les fichiers de configuration suivants sont sauvegardés :

Fichier	Description	Répertoire
`agent.key` (le nom peut varier)	clé de licence de l'Agent	`etc`
`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	
`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	
`download.conf`	paramètres réseau pour la génération de packages d'installation de l'Agent	
`drwcsd.conf` (le nom peur 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	
`openssl.cnf`	certificat du Serveur pour HTTPS	
`webmin.conf`	fichier de configuration du Centre de gestion	
`dbexport.gz`	exportation de la base de données	répertoire <*backup*>
`drwcsd.pub`	clé de chiffrement publique	• `Installer` • `webmin\install`

Si vous prévoyez d'utiliser les fichiers de configuration du Serveur d'une version précédente, notez que :

1. La clé de licence du Serveur n'est plus supportée (voir le p. Chapitre 2. Licence).

2. La base de données intégrée est mise à jour et le fichier de configuration du Serveur est converti par les moyens de l'installateur. Ces fichiers ne peuvent pas être remplacés par les copies sauvegardées automatiquement lors du passage au Serveur de la version 10.

Si nécessaire, copiez d'autres fichiers importants dans un autre répertoire, différent du répertoire d'installation du Serveur. Par exemple, les modèles de rapport sauvegardés dans le dossier `\var\templates`.

Sauvegarde de la base de données

La base de données MS SQL CE n'est plus supportée à commencer par la version du Serveur Dr.Web 10. Lors de la mise à niveau automatique du Serveur avec l'installateur, la base de données MS SQL CE est convertie automatiquement en base de données intégrée IntDB.

Avant la mise à niveau de Dr.Web Enterprise Security Suite, il est recommandé de sauvegarder la base de données.

Pour sauvegarder la base de données :

1. Arrêter le Serveur.
2. Exportez la base de données vers le fichier :

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=all exportdb <dossier_de_sauvegarde>\esbase.es
```

Pour les Serveurs utilisant une base de données externe, il est recommandé d'utiliser les outils standard fournis avec la base de données.

Assurez-vous que l'exportation de la base de données Dr.Web Enterprise Security Suite a réussi. Sans avoir une copie de sauvegarde de la BD, vous ne pourrez pas restaurer le Serveur en cas de nécessité.

Mise à jour du Serveur Dr.Web

Pour mettre à jour le Serveur Dr.Web, procédez comme suit :

1. Lancez le fichier de distribution.

Par défaut, la langue du système d'exploitation est sélectionnée comme la langue de l'installateur. Si nécessaire, vous pouvez modifier la langue d'installation à toutes les étapes en sélectionnant l'élément correspondant qui se trouve dans l'angle droit supérieur de la fenêtre de l'installateur.

2. Une fenêtre va s'ouvrir vous informant sur la présence du logiciel installé du Serveur de la version précédente et vous présentant une brève description du processus de la mise à niveau vers la nouvelle version. Pour commencer la configuration de la procédure de la mise à niveau, cliquez sur **Mettre à niveau**.
3. Une fenêtre contenant les informations sur le produit et le lien vers le texte du Contrat de licence va s'ouvrir. Après l'avoir lu, cochez la case **J'accepte les termes du Contrat de licence** et cliquez sur **Suivant**.
4. Aux étapes suivantes de l'assistant d'installation la configuration du Serveur mis à jour est effectuée de la même manière que le processus d'Installation du Serveur Dr.Web à la base des fichiers de configuration de la version précédente (voir ci-dessus). L'installateur localise automatiquement le répertoire d'installation du Serveur, les fichiers de configuration et la BD intégrée de la version précédente. Si cela est nécessaire, vous pouvez modifier le chemin vers les fichiers qui sont trouvé automatiquement par l'installateur.

   Pour la base de données externe du Serveur, sélectionnez aussi **Utiliser la base de données existante** durant la mise à niveau.

   Si vous planifiez utiliser en tant que la base de données externe la base de données Oracle ou PostgreSQL via la connexion ODBC, alors désactivez dans les paramètres de l'installateur l'installation du client intégré pour le SGBD correspondant (dans la rubrique **Support des bases de données**) lors de la mise à jour du Serveur.

   Sinon, le travail avec la BD Oracle via ODBC ne sera pas possible à cause du conflit des bibliothèques.

5. Afin de procéder à la suppression du Serveur de la version antérieure et pour lancer l'installation du Serveur en version 10, cliquez sur **Installer**.

   Une fois les Serveurs du réseau antivirus sont mis à jour, il est nécessaire de spécifier encore une fois les paramètres de chiffrement et de compression pour les Serveurs liés (voir le **Manuel Administrateur**, la rubrique Configuration des liaisons entre Serveurs Dr.Web).

Après la mise à niveau du logiciel du Serveur Dr.Web, effectuez les actions suivantes pour garantir un fonctionnement normal du Centre de gestion :

1. Videz le cache du navigateur web utilisé pour se connecter au Centre de gestion.
2. Mettez à jour l'extension du Centre de gestion de la sécurité Dr.Web.

6.2. Mise à jour du Serveur Dr.Web sous les OS de la famille UNIX®

Toutes les actions doivent être effectuées du nom de l'administrateur **root**.

La mise à niveau du logiciel du Serveur vers la version 10 par-dessus la version précédente n'est pas possible pour tous les OS de la famille UNIX. Ainsi, sous un OS UNIX ne permettant pas la mise à niveau, il est recommandé de supprimer le logiciel Serveur des versions précédentes en effectuant une copie de sauvegarde et d'installer ensuite le logiciel de version 10 d'après la copie sauvegardée.

La mise à jour du Serveur au sein de la version 10 pour les mêmes types de packages s'effectue automatiquement pour tous les OS de la famille UNIX.

Avant de supprimer le Serveur de la version précédente, merci de lire la rubrique Mise à jour de l'Agent Dr.Web.

La mise à jour du Serveur au sein de la version 10 via le Centre de gestion est également disponible. La procédure est décrite dans le **Manuel Administrateur**, dans la rubrique Mise à jour du Serveur Dr.Web et restauration depuis une copie de sauvegarde.

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.

Sauvegarde des fichiers de configuration

En cas de suppression du Serveur de la version 6, les fichiers suivants sont sauvegardés automatiquement :

Fichier	Description	Répertoire par défaut
`agent.key` (le nom peut varier)	clé de licence de l'Agent	• sous Linux et Solaris : `/var/opt/drwcs/etc` • sous FreeBSD : `/var/drwcs/etc`
`certificate.pem`	certificat SSL	
`download.conf`	paramètres réseau pour la génération de packages d'installation de l'Agent	
`drwcsd.conf` (le nom peur varier)	fichier de configuration du Serveur	
`drwcsd.pri`	clé de chiffrement privée	
`enterprise.key` (le nom peut varier)	clé de licence du Serveur	
`private-key.pem`	clé privée RSA	
`webmin.conf`	fichier de configruation du Centre de gestion	

Fichier	Description	Répertoire par défaut
common.conf	fichier de configuration (pour les OS de la famille UNIX)	
local.conf	paramètres du journal du Serveur	
dbinternal.dbs	BD intégrée	• sous Linux et Solaris : /var/opt/drwcs/ • sous FreeBSD : /var/drwcs/
drwcsd.pub	clé de chiffrement publique	• sous Linux et Solaris : /opt/drwcs/Installer /opt/drwcs/webmin/install • sous FreeBSD : /usr/local/drwcs/Installer /usr/local/drwcs/webmin/install

En cas de suppression du Serveur de la version 10, les fichiers de configuration sont automatiquement sauvegardés dans le répertoire de sauvegarde par défaut :

Fichier	Description	Répertoire par défaut
agent.key (le nom peut varier)	clé de licence de l'Agent	/var/tmp/drwcs/
certificate.pem	certificat SSL	
download.conf	paramètres réseau pour la génération de packages d'installation de l'Agent	
drwcsd.conf (le nom peur varier)	fichier de configuration du Serveur	
drwcsd.pri	clé de chiffrement privée	
enterprise.key (le nom peut varier)	clé de licence du Serveur. La clé est sauvegardée 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	
private-key.pem	clé privée RSA	
webmin.conf	fichier de configruation du Centre de gestion	
common.conf	fichier de configuration (pour les OS de la famille UNIX)	

Fichier	Description	Répertoire par défaut
local.conf	paramètres du journal du Serveur	
dbexport.gz	exportation de la base de données	
drwcsd.pub	clé de chiffrement publique	

En cas de la mise à jour automatique sous les OS **Linux** et **Solaris**, les fichiers suivants sont également sauvegardés :

Pour le Serveur de la version 6 :

Fichier	Description	Répertoire par défaut
auth-ldap.xml	fichier de configuration pour l'authentification externe des administrateurs via LDAP	/var/opt/drwcs/etc
auth-radius.xml	fichier de configuration pour l'authentification externe des administrateurs via RADIUS	

Pour le Serveur de la version 10 :

Fichier	Description	Répertoire par défaut
auth-ldap.xml	fichier de configuration pour l'authentification externe des administrateurs via LDAP	/var/tmp/drwcs/
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	

Si vous prévoyez d'utiliser les fichiers de configuration du Serveur d'une version précédente, notez que :

1. La clé de licence du Serveur n'est plus supportée (voir le p. Chapitre 2. Licence).
2. La base de données intégrée est mise à jour et le fichier de configuration du Serveur est converti par les moyens de l'installateur. Ces fichiers ne peuvent pas être remplacés par les copies sauvegardées automatiquement lors du passage au Serveur de la version 10.

Sauvegarde de la base de données

Avant la mise à niveau de Dr.Web Enterprise Security Suite, il est recommandé d'enregistrer la base de données.

Pour sauvegarder la base de données :

1. Arrêter le Serveur.
2. Exportez la base de données vers le fichier :
   - Sous FreeBSD :
     ```
     # /usr/local/etc/rc.d/drwcsd.sh exportdb /var/drwcs/etc/esbase.es
     ```
   - Sous Linux :
     ```
     # /etc/init.d/drwcsd exportdb /var/opt/drwcs/etc/esbase.es
     ```
   - Sous Solaris :
     ```
     # /etc/init.d/drwcsd exportdb /var/drwcs/etc/esbase.es
     ```

Pour les Serveurs utilisant une base de données externe, il est recommandé d'utiliser les outils standard fournis avec la base de données.

Assurez-vous que l'exportation de la base de données Dr.Web Enterprise Security Suite a réussi. Sans avoir une copie de sauvegarde de la BD, vous ne pourrez pas restaurer le Serveur en cas de nécessité.

Mise à jour automatique

En cas de mise à niveau du Serveur de la version 6 vers la version 10 sous **Linux** et **Solaris**, au lieu de supprimer la version antérieure et d'installer une nouvelle version du Serveur, il est possible d'utiliser la mise à jour automatique du Serveur. Pour cela, lancez le package correspondant du Serveur.

Tous les fichiers enregistrés de manière automatique seront placés dans les dossiers appropriés, aucune opération de remplacement manuel ne sera requise.

Mise à jour manuelle

Pour mettre à jour le Serveur Dr.Web en cas d'utilisation de la base de données intégrée, procédez comme suit :

1. Arrêter le Serveur.
2. Si vous souhaitez utiliser ultérieurement des fichiers (à part les fichiers qui seront sauvegardés automatiquement lors de la suppression du Serveur à l'étape **4**), copiez-les manuellement. Par exemple, les modèles de rapports.
3. Supprimez tout le contenu du dépôt.
4. Supprimez le logiciel du Serveur (voir le p. Suppression du Serveur Dr.Web sous les OS de la famille UNIX®). Il vous sera proposé d'enregistrer automatiquement des copies des fichiers. Pour ce faire, indiquez un dossier ou acceptez le dossier par défaut.
5. Installez le Serveur Dr.Web en version 10 d'après la procédure standard d'installation (voir le p. Installation du Serveur Dr.Web pour les OS de la famille UNIX®) basée sur la copie de sauvegarde de l'étape **4**. Tous les fichiers de configuration ainsi que la base de données intégrée

seront automatiquement convertis pour la version 10 du Serveur. Sans conversion automatique, la base de données et certains fichiers de configuration du Serveur de la version précédente ne peuvent pas être utilisés.

En cas de sauvegarde manuelle, placez les fichiers dans les mêmes dossiers où ils se trouvaient en version précédente du Serveur.

Pour tous les fichiers sauvegardés de la précédente version du Serveur (voir l'étape 6) désignez l'utilisateur sélectionné lors de l'installation de la nouvelle version du Serveur (**drwcs** par défaut) comme le propriétaire des fichiers.

6. Lancez le Serveur.
7. Configurez la mise à niveau du dépôt et effectuez-la.
8. Redémarrez le Serveur.

Pour mettre à jour le Serveur Dr.Web en cas d'utilisation de la base de données externe, procédez comme suit :

1. Arrêter le Serveur.
2. Si vous souhaitez utiliser ultérieurement des fichiers (à part les fichiers qui seront sauvegardés automatiquement lors de la suppression du Serveur à l'étape **4**), copiez-les manuellement. Par exemple, les modèles de rapports.
3. Supprimez tout le contenu du dépôt.
4. Supprimez le logiciel du Serveur (voir le p. Suppression du Serveur Dr.Web sous les OS de la famille UNIX®). Il vous sera proposé d'enregistrer automatiquement des copies des fichiers. Pour ce faire, indiquez un dossier ou acceptez le dossier par défaut.
5. Installez le Serveur Dr.Web en version 10 selon la procedure standard d'installation (voir le p. Installation du Serveur Dr.Web pour les OS de la famille UNIX®).
6. Placez les fichiers sauvegardés automatiquement (voir ci-dessus) :
   - sous **Linux** :
     pub-clé: `/opt/drwcs/Installer/` et vers `/opt/drwcs/webmin/install`
     le reste : `/var/opt/drwcs/etc`
   - sous **FreeBSD** :
     pub-clé: `/usr/local/drwcs/Installer/` et vers `/usr/local/drwcs/webmin/install`
     le reste : `/var/drwcs/etc`
   - sous **Solaris** :
     pub-clé: `/opt/drwcs/Installer/` et vers `/opt/drwcs/webmin/install`
     le reste : `/var/drwcs/etc`

   En cas de sauvegarde manuelle, placez les fichiers dans les mêmes dossiers où ils se trouvaient en version précédente du Serveur.

Pour tous les fichiers sauvegardés de la précédente version du Serveur (voir l'étape 6) désignez l'utilisateur sélectionné lors de l'installation de la nouvelle version du Serveur (**drwcs** par défaut) comme le propriétaire des fichiers.

7. Pour mettre à niveau les abses de données, exécutez les commandes ci-dessous :
   - sous **Linux** et **Solaris** :
     ```
     /etc/init.d/drwcsd upgradedb
     ```
   - sous **FreeBSD** :
     ```
     /usr/local/etc/rc.d/drwcsd.sh upgradedb
     ```
8. Lancez le Serveur.
9. Configurez la mise à niveau du dépôt et effectuez-la.
10. Redémarrez le Serveur.

Une fois les Serveurs du réseau antivirus sont mis à jour, il est nécessaire de spécifier encore une fois les paramètres de chiffrement et de compression pour les Serveurs liés (voir le **Manuel Administrateur**, la rubrique Configuration des liaisons entre Serveurs Dr.Web).

6.3. Mise à jour de l'extension pour le Centre de gestion de la sécurité Dr.Web

Pour mettre à jour l'extension du Centre de gestion de la sécurité Dr.Web (utilisé par le Centre de gestion) il est nécessaire de supprimer manuellement la version antérieure de l'extension et d'installer la nouvelle extension du Centre de gestion de la sécurité Dr.Web.

La procédure de suppression de l'extension est décrite dans le p. Suppression du Serveur Dr.Web sous OS Windows® et dans le p. Suppression du Serveur Dr.Web sous les OS de la famille UNIX®.

Pour en savoir plus sur la procédure d'installation, consultez le paragraphe Installation de l'extension pour le Centre de gestion de la sécurité Dr.Web.

6.4. Mise à jour des Agents Dr.Web

La mise à jour des Agents après la mise à jour du logiciel du Serveur est décrite pour les variantes suivantes :

1. Mise à jour des Agents Dr.Web sur les postes tournant sous Windows®,
2. Mise à jour des Agents Dr.Web pour les postes tournant sous Linux, Android et OS X.

6.4.1. Mise à jour des Agents Dr.Web sur les postes tournant sous Windows®

Mise à jour automatique

Pour la mise à jour automatique il faut satisfaire aux conditions suivantes :

1. Les Agents doivent être installés sur les ordinateurs tournant sous Windows en versions supportées pour l'installation des Agents pour Dr.Web Enterprise Security Suite de la version 10 (voir les **Annexes**, p. Annexe A. Liste complète des versions d'OS supportées).
2. En cas de la mise à jour automatique, les actions à accomplir peuvent varier en fonction des paramètres du Serveur :
   a) La mise à jour automatique s'effectue si lors de la mise à niveau du Serveur, les clés de chiffrement et les paramètres réseau du Serveur précédent ont été sauvegardés.
   b) La mise à jour automatique requiert la configuration manuelle, si lors de la mise à niveau du Serveur, les nouvelles clé de chiffrement et les nouveaux paramètres réseau du Serveur ont été spécifiés.

Lors de la mise a jour automatique, prenez en compte les particularités suivantes :

1. Après la suppression de l'Agent, une notification sur la nécessité de redémarrage est affichée sur le poste. L'administrateur doit redémarrer le poste lui-même.
2. Après la suppression de l'ancienne version de l'Agent et jusqu'à l'installation de la nouvelle version, les postes ne sont pas protégés.
3. Après la mise à jour de l'Agent sans redémarrage du poste, le fonctionnement du logiciel antivirus est limité. Dans ce cas la protection complète antivirus n'est pas fournie. Il faut que l'utilisateur effectue la mise à jour du poste selon la demande de l'Agent.

La mise à jour automatique des Agents s'effectue conformément au schéma suivant :

1. Une fois la mise à jour est lancée, l'ancienne version de l'Agent est supprimée.
2. Le redémarrage du poste s'effectue manuellement.
3. Ensuite, s'effectue l'installation de la nouvelle version de l'Agent.Pour cela, une tâche est créée automatiquement dans la planification du Serveur.
4. Après la fin de la mise à jour de l'Agent, le poste se connecte automatiquement au Serveur. Dans la rubrique **Statut** du Centre de gestion, une notification sur la nécessité de redémarrage s'affichera pour le poste mis à jour.Il est nécessaire de redémarrer le poste.

La mise à jour automatique des Agents avec la configuration manuelle s'effectue conformément au schéma suivant :

1. Configurez manuellement les paramètres de connexion au nouveau Serveur et remplacez la clé de chiffrement publique sur les postes.

2. Après la modification des paramètres sur le poste et la connexion du poste au Serveur, la mise à jour de l'Agent commencera.
3. Une fois la mise à jour est lancée, l'ancienne version de l'Agent est supprimée.
4. Le redémarrage du poste s'effectue manuellement.
5. Ensuite, s'effectue l'installation de la nouvelle version de l'Agent.Pour cela, une tâche est créée automatiquement dans la planification du Serveur.
6. Après la fin de la mise à jour de l'Agent, le poste se connecte automatiquement au Serveur. Dans la rubrique **Statut du** Centre de gestion, une notification sur la nécessité de redémarrage s'affichera pour le poste mis à jour.Il est nécessaire de redémarrer le poste.

Mise à jour manuelle

Si l'installation de la nouvelle version de l'Agent lors de la mise à niveau automatique a échoué pour une raison quelconque, les autres tentatives d'installation ne seront pas entreprises. Le logiciel antivirus ne sera pas installé sur le poste et un tel poste sera affiché dans le Centre de gestion comme désactivé.

Dans ce cas, l'utilisateur doit installer l'Agent lui-même. Après l'installation du nouvel Agent, il faudra fusionner l'ancien poste et le nouveau poste dans l'arborescence du réseau antivirus, dans le Centre de gestion.

La mise à jour n'est pas supportée

Si les Agents sont installés sur les postes avec les systèmes d'exploitation qui ne sont pas supportés pour l'installation des Agents pour Dr.Web Enterprise Security Suite de la version 10, alors aucune action de mise à jour ne sera pas exécutée.

Les Agents installés sur des OS non supportés ne peuvent pas recevoir les mises à jour (y compris les mises à jour des bases virales) du nouveau Serveur. Si vous devez maintenir les Agents sous des OS non supportés, vous devez garder au sein du réseau antivirus les Serveurs des versions précédentes, auxquels ces Agents sont connectés. Notez que les Serveurs des versions 6 et les Serveurs de la version 10 doivent obtenir des mises à jour séparément.

Les recommandations sur la mise à niveau des Agents installés sur les postes ayant des fonctions importantes de LAN, sont disponibles dans les **Annexes**, p. Mise à niveau des Agents sur les serveurs LAN.

6.4.2. Mise à jour des Agents Dr.Web pour les postes tournant sous Linux, Android et OS X

Les Agents installés sur des postes tournant sous Linux, Android et OS X seront connectés au Serveur de la version 10 avec un support complet du processus de mise à jour dans les cas suivants :

1. Les Agents doivent être installés sur les ordinateurs tournant sous les OS supportés pour l'installation des Agents pour Dr.Web Enterprise Security Suite de la version 10 (voir les **Annexes**, p. Annexe A. Liste complète des versions d'OS supportées).
2. Les clés de chiffrement et les paramètres réseau du Serveur mis à jour doivent être spécifiés sur les postes.

6.5. Mise à jour du Serveur proxy

Mise à jour du serveur proxy sous l'OS Windows

La mise à jour automatique du Serveur proxy n'est pas prise en charge.

Lors du démarrage de l'installateur sur l'ordinateur sur lequel le Serveur proxy est installé :

- Si l'installateur ayant le même type de système que le Serveur proxy installé démarre, une alerte sur l'installation impossible sera affichée.
- Si l'installateur lancé a un type de système autre que le type de plateforme du Serveur proxy, le Serveur proxy sera installé dans le répertoire autre que celui en version déjà installée.

> ⚠ Si vous installez deux Serveurs proxy sur la même machine et que vous les paramétrez de sorte qu'ils utilisent le même port, ceci met hors service les deux Serveurs proxy.

Pour mettre à jour le serveur proxy :

1. Si sur l'ordinateur avec le Serveur proxy tourne l'Agent dont la fonction d'autoprotection est activée, désactivez le composant d'autoprotection Dr.Web via les paramètres de l'Agent.
2. Supprimez le Serveur proxy conformément à la procédure standard (voir Suppression du Serveur proxy).

> ⚠ Lors de la suppression du Serveur proxy le fichier de configuration `drwcsd-proxy.xml` est supprimé (voir les **Annexes**, p. Annexe G4). Si nécessaire, sauvegardez le fichier de configuration manuellement avant la suppression du Serveur proxy.

3. Installez une nouvelle version du Serveur proxy conformément à la procédure standard (voir Installation du Serveur proxy).
4. S'il est nécessaire, remplacez le fichier de configuration par le fichier sauvegardé depuis la version antérieure.

5. Si à l'étape 1 le composant d'autoprotection Dr.Web a été désactivé, activez-le via les paramètres de l'Agent.

Mise à jour du Serveur proxy sous l'OS de la famille UNIX

Pour mettre à jour le serveur proxy :

1. Lors de la mise à jour du Serveur proxy le fichier de configuration drwcsd-proxy.xml est supprimé (voir les **Annexes**, p. Annexe G4). Si nécessaire, sauvegardez le fichier de configuration manuellement avant la mise à jour du Serveur proxy.
2. Pour lancer le processus, exécutez la commande suivante :
   `sh ./<fichier_de_distribution>.run`
3. Si nécessaire, remplacez le fichier de configuration `drwcsd-proxy.xml` par le fichier sauvegardé avant la mise à jour.

Référence

Référence

R

S