Dr.WEB

Enterprise Security Suite

Manuel d'Installation

Dr.Web Enterprise Security Suite
Version 11.0.2
Manuel d'Installation
31/07/2020

Doctor Web, Siège social en Russie

Adresse : 2-12A, 3e rue Yamskogo polya, 125040 Moscou, Russie

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

Téléphone : +7 (495) 789-45-87

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

Doctor Web

Doctor Web — éditeur russe de solutions de sécurité informatique.

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

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

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

Nous remercions tous nos clients pour leur soutien !

Contenu

Chapitre 1. Dr.Web Enterprise Security Suite 6
1.1. Introduction 6
1.1.1. Destination du document 6
1.1.2. Légende et abréviations 8
1.2. A propos du produit 9
1.3. Pré-requis système 19
1.4. Kit de distribution 24
Chapitre 2. Octroi de licence 27
Chapitre 3. Mise en route 29
3.1. Création d'un réseau antivirus 29
3.2. Configuration des connexions réseau 33
3.2.1. Connexions directes 34
3.2.2. Service de détection du Serveur Dr.Web 35
3.2.3. Utiliser le protocole SRV 35
3.3. Assurance d'une connexion sécurisée 36
3.3.1. Chiffrement et compression du trafic 36
3.3.2. Instruments assurant une connexion sécurisée 42
3.3.3. Connexion des clients au Serveur Dr.Web 44
Chapitre 4. Installation des composants Dr.Web Enterprise Security Suite 47
4.1. Installation du Serveur Dr.Web 47
4.1.1. Installation du Serveur Dr.Web sous OS Windows® 48
4.1.2. Installation du Serveur Dr.Web pour les OS de la famille UNIX® 55
4.1.3. Installation de la distribution supplémentaire du Serveur Dr.Web 57
4.2. Installation de l'Agent Dr.Web 57
4.2.1. Fichiers d'installation 59
4.2.2. Installation de l'Agent Dr.Web en mode local 61
4.2.3. Installation à distance de l'Agent Dr.Web sous OS Windows® 72
4.3. Installation de NAP Validator 86
4.4. Installation du Serveur proxy 86
4.4.1. Connexion du Serveur proxy au Serveur Dr.Web 87
4.4.2. Création du compte du Serveur proxy 89
4.4.3. Installation du Serveur proxy lors de l'installation de l'Agent Dr.Web pour Windows 91

4.4.4. Installation du Serveur proxy avec l'installateur 92

Chapitre 5. Suppression des composants Dr.Web Enterprise Security Suite 97

5.1. Suppression du Serveur Dr.Web 97

5.1.1. Suppression du Serveur Dr.Web sous OS Windows® 97

5.1.2. Suppression du Serveur Dr.Web sous les OS de la famille UNIX® 97

5.2. Suppression de l'Agent Dr.Web 98

5.2.1. Suppression de l'Agent Dr.Web sous OS Windows® 99

5.2.2. Suppression de l'Agent Dr.Web avec le service Active Directory 101

5.3. Suppression du Serveur proxy 102

5.3.1. Suppression locale du Serveur proxy 102

5.3.2. Suppression à distance du Serveur proxy 103

Chapitre 6. Mise à jour des composants de Dr.Web Enterprise Security Suite 104

6.1. Mise à jour du Serveur Dr.Web sous OS Windows® 104

6.2. Mise à jour du Serveur Dr.Web sous les OS de la famille UNIX® 111

6.3. Mise à jour des Agents Dr.Web 117

6.3.1. Mise à jour des Agents Dr.Web sur les postes tournant sous Windows® 118

6.3.2. Mise à niveau des Agents Dr.Web sur les postes tournant sous l'OS Android 120

6.3.3. Mise à niveau des Agents Dr.Web sur les postes tournant sous l'OS Linux® et macOS® 121

6.4. Mise à jour du Serveur proxy Dr.Web 122

6.4.1. Mise à jour du Serveur proxy Dr.Web lors de son fonctionnement 122

6.4.2. Mise à jour du Serveur proxy Dr.Web via l'installateur 123

Référence 126

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 contient les parties suivantes :

1. **Manuel d'installation** (fichier **drweb-11.0-esuite-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-11.0-esuite-admin-manual-fr.pdf**)

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

   L'administrateur du réseau antivirus doit posséder les privilèges administrateur sur le système ou collaborer avec l'administrateur du réseau local, savoir mettre en place la politique de protection antivirus et connaître en détails les packages antivirus Dr.Web pour tous les systèmes d'exploitation utilisés dans le réseau.
3. **Annexes** (fichier **drweb-11.0-esuite-appendices-fr.pdf**)

   Les Annexes fournissent des informations techniques, décrivent les paramètres de configuration des composants Antivirus, ainsi que la syntaxe et les valeurs utilisées pour leur gestion.

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 se trouvent dans le même dossier et portent leurs noms initiaux.

De plus, les Manuels suivants sont fournis :

1. **Instructions de déploiement du réseau antivirus**

   Les instructions contiennent de brèves informations sur l'installation et la configuration initiale des composants du réseau antivirus. Pour des informations détaillées, consultez la documentation de l'administrateur.

2. **Manuels de gestion des postes**

   Ces manuels contiennent les informations sur la configuration centralisée des composants du logiciel antivirus sur les postes effectuée par l'administrateur du réseau antivirus via le Centre de gestion de la sécurité Dr.Web.

3. **Manuels Utilisateur**

   Les manuels utilisateur contiennent les informations sur la configuration de la solution antivirus Dr.Web effectuée directement sur les postes protégés.

Tous les Manuels listés sont fournis au sein du produit Dr.Web Enterprise Security Suite et vous pouvez les ouvrir via le Centre de gestion de la sécurité Dr.Web.

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

1.1.2. Légende et abréviations

Conventions

Les styles de texte utilisées dans ce manuel :

Styles	Utilisés
	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 peuvent être utilisées dans le Manuel :

- ACL : listes de contrôle d'accès (Access Control List),
- CDN : réseau de distribution de contenu (Content Delivery Network),
- DFS : système de fichiers distribués (Distributed File System),
- DNS : système de noms de domaine (Domain Name System),
- FQDN : nom de domaine complètement qualifié (Fully Qualified Domain Name),
- GUI : interface graphique utilisateur (Graphical User Interface), une version GUI du logiciel est une version utilisant des outils GUI,
- MTU : taille maximale de l'unité de transmission (Maximum Transmission Unit),
- NAP : Protection d'accès réseau (Network Access Protection),
- 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 du réseau antivirus et pas uniquement sur le 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®).

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. La base de données SQLite3 embarquée directement dans le Serveur de protection centralisée est fournie.

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

- MySQL,
- 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 référentiel 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®,
- Microsoft Edge®,
- 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 l'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 l'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, 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 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 référentiel du Serveur Dr.Web :
   - consulter le statut des produits dans le référentiel ;
   - lancer la mise à jour du référentiel 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®,
- macOS®,

- OS Android.

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

Moteur de scan. Il effectue l'analyse des données (contenu des fichiers, enregistrements de démarrage des périphériques de disques et autres données reçues des autres composants de Dr.Web pour UNIX). Il crée une file d'attente de l'analyse. Il désinfecte les menaces curables.

Analyse antivirus, gestion de la quarantaine

Composant de l'analyse des objets du système de fichiers et gestionnaire de la quarantaine. Il reçoit les tâches d'analyse de fichiers des autres composants de Dr.Web pour UNIX. Il contourne les répertoires du système de fichiers conformément à la tâche. il envoi des fichiers pour l'analyse du moteur de scan. Il supprime les fichiers infectés, les déplace en quarantaine, les restaure de la quarantaine et gère les répertoires de la quarantaine. Il organise et tient à jour le cache stockant les informations sur les fichiers analysés précédemment et le registre de menaces détectées.

Il est utilisé par tous les composants analysant les objets du système de fichiers, tel que SpIDer Guard (pour Linux, SMB, NSS).

Analyse du trafic web

Serveur ICAP exécutant l'analyse de requêtes et du trafic passant par les serveurs proxy HTTP. Il empêche le transfert des fichiers infectés et l'accès aux hôtes du réseau listés

dans les catégories indésirables de ressources web et les listes noires créées par l'administrateur système.

Moniteur de fichiers pour les systèmes GNU/Linux

Moniteur du système de fichiers Linux. Il fonctionne en tâche de fond et suit les opérations avec les fichiers (telles que la création, l'ouverture, la fermeture et le lancement du fichier) dans les système de fichiers GNU/Linux. Il envoie au composant de l'analyse de fichiers les requêtes pour l'analyse du contenu de nouveaux fichiers et de fichiers modifiés, ainsi que des fichiers exécutables au moment du lancement de programmes.

Moniteur de fichiers pour les répertoires Samba

Moniteur des répertoires partagés Samba. Il fonctionne en tâche de fond et suit les opérations du système de fichiers (telles que la création, l'ouverture, la fermeture du fichier et les opérations de lecture et écriture) dans les répertoires servant des stockages de fichiers du serveur SMB de Samba. Il envoie au composant de l'analyse de fichiers le contenu de nouveaux fichiers et de fichiers modifiés.

Moniteur de fichiers NSS

Moniteur des volumes NSS (Novell Storage Services). Il fonctionne en tâche de fond et suit les opérations du système de fichiers (telles que la création, l'ouverture, la fermeture du fichier et les opérations d'écriture) sur les volumes NSS créés dans le point indiqué du système de fichiers. Il envoie au composant de l'analyse de fichiers le contenu de nouveaux fichiers et de fichiers modifiés.

Analyse des connexions réseau

Composant de l'analyse du trafic réseau d'URL. Il est conçu pour analyser pour la présence de menaces les données téléchargées depuis le réseau sur un hôte local et transmises de cet hôte dans le réseau externe. Il sert à empêcher la connexion avec les hôtes de réseau qui sont inscrits dans les catégories indésirables de ressources web ou bien, dans des listes noires créées par l'administrateur du réseau.

Moniteur de courrier

Composant de l'analyse des messages e-mail. Il analyse les messages des protocoles, trie les messages e-mail et les prépare à l'analyse pour la présence de menaces. Il peut fonctionner en deux modes :

1. Filtre pour les serveurs de messagerie (Sendmail, Postfix, etc), connecté via l'interface Milter, Spamd ou Rspamd.
2. Proxy transparent de protocoles de messagerie (SMTP, POP3, IMAP). Dans ce mode, il utilise SpIDer Gate.

Postes tournant sous macOS®

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.

Filtre des appels et des SMS

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.

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 inclus 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 l'accès direct de l'organisation deviendrait impossible.

Le Serveur proxy permet d'utiliser tout ordinateur faisant partie du réseau antivirus dans les buts suivants :

- Comme le centre de retransmission des mises à jour pour réduire la charge réseau sur le Serveur et la connexion entre le Serveur et le Serveur proxy et pour réduire le délais de réception de mises à jour par les postes grâce à l'utilisation de la fonction de mise en cache.
- Comme le centre de transmission des événements viraux des postes protégés vers le Serveur, ce qui aussi réduit la charge système et permet de gérer les cas où, par exemple, le groupe de postes se trouve dans le segment isolé du segment dans lequel se trouve le Serveur.

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 Référentiel

Chargeur du Référentiel 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 mises 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

Pour l'installation et le fonctionnement de Dr.Web Enterprise Security Suite il faut que :

- Les ordinateurs du réseau antivirus aient un accès au Serveur Dr.Web ou au Serveur proxy.
- Pour assurer l'interaction entre les composants antivirus, les ports suivants doivent être ouverts sur les ordinateurs utilisés :

Numéros de ports	Protocoles	Direction des connexions	Utilisation
2193	TCP	• entrantes, sortantes pour le Serveur et le Serveur proxy • sortantes pour l'Agent	Pour la connexion des composants antivirus au Serveur et les liaisons entre Serveurs. Le Serveur proxy est également utilisé pour établir la connexion aux clients.
	UDP	entrantes, sortantes	Pour le fonctionnement du Scanner réseau.
139, 445	TCP	• entrantes pour le Serveur • entrantes, sortantes pour l'Agent • sortantes pour l'ordinateur sur lequel le Centre de gestion est ouvert	Pour le fonctionnement de l'Installateur réseau.
	UDP	entrantes, sortantes	
9080	HTTP	• entrantes pour le Serveur • sortantes pour l'ordinateur sur lequel le Centre de	Pour le fonctionnement du Centre de gestion de la sécurité Dr.Web.
9081	HTTPS		

Numéros de ports	Protocoles	Direction des connexions	Utilisation
10101	TCP		Pour l'utilitaire de diagnostique à distance du Serveur.
80	HTTP	sortantes	Pour obtenir des mises à jour depuis SGM.
443	HTTPS		

Le fonctionnement du Serveur Dr.Web requiert :

Composant	Pré-requis
CPU	CPU supportant les instructions SSE2 et ayant la fréquence d'horloge de 1,3 Ghz ou supérieure.
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 embarquée (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 17 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 4,3 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).
Système d'exploitation	• Windows ; • Linux ; • FreeBSD. La liste complète des OS supportés est fournie dans les **Annexes**, dans l'Annexe A.
Support des environnements virtuels et cloud	Le fonctionnement est supporté sous les systèmes d'exploitation qui satisfont les pré-requis ci-dessus, dans les environnements virtuels et cloud, y compris : • VMware ; • Hyper-V ; • Xen ;

Composant	Pré-requis
	• KVM.
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 l'utilisation de la BD **Oracle**, la bibliothèque `Linux kernel AIO access library` (`libaio`) est requise.

Les utilitaires supplémentaires fournis avec le Serveur Dr.Web (disponibles pour le téléchargement via le Centre de gestion, section **Administration** → **Utilitaires**) doivent être lancés sur l'ordinateur qui satisfait les pré-requis système du Serveur Dr.Web.

Le fonctionnement du Serveur proxy Dr.Web requiert :

Composant	Pré-requis
CPU	CPU supportant les instructions SSE2 et ayant la fréquence d'horloge de 1,3 Ghz ou supérieure.
Mémoire vive	Pas moins de 1 Go.
Espace disque	Pas moins de 1 Go.
Système d'exploitation	• Windows ; • Linux ; • FreeBSD. 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.

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

a) Navigateur :

Navigateur	Support
Windows Internet Explorer 11	Supporté.
Microsoft Edge 0.10 ou supérieur	
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**.
- Pour l'interaction correcte avec le Centre de gestion via le navigateur web Windows Internet Explorer par le protocole sécurisé `https`, il faut installer toutes les dernières mises à jour du navigateur web.
- La gestion du Centre de gestion via le navigateur Windows Internet Explorer n'est pas supportée en mode de compatibilité.

b) 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 8 ou 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 Go pour les fichiers exécutables + espace disque supplémentaire pour les journaux et les fichiers temporaires.
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.

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

Le fonctionnement de l'Agent Dr.Web est supporté sous les systèmes d'exploitation qui satisfont aux pré-requis ci-dessus, dans les environnements virtuels et cloud, y compris :

- VMware ;
- Hyper-V ;
- Xen ;
- KVM.

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 :
   - `drweb-11.00.2-<assemblage>-esuite-server-<version_de_l'OS>.tar.gz.run`
     Distribution principale du Serveur Dr.Web
   - `drweb-11.00.2-<assemblage>-esuite-extra-<version_de_l'OS>.tar.gz.run`
     Distribution supplémentaire du Serveur Dr.Web
   - `drweb-11.00.2-<assemblage>-esuite-proxy-<version_de_l'OS>.tar.gz.run`
     Serveur proxy Dr.Web
   - `drweb-reploader-<OS>-<nombre de bits>`
     Version de console du Chargeur du référentiel Dr.Web
2. Sous Windows :
   - `drweb-11.00.2-<assemblage>-esuite-server-<version_de_l'OS>.exe`
     Distribution principale du Serveur Dr.Web
   - `drweb-11.00.2-<assemblage>-esuite-extra-<version_de_l'OS>.exe`
     Distribution supplémentaire du Serveur Dr.Web
   - `drweb-11.00.2-<assemblage>-esuite-proxy-<version_de_l'OS>.exe`
     Serveur proxy Dr.Web

- `drweb-11.05.4-<assemblage>-esuite-agent-activedirectory.msi`

  Agent Dr.Web pour Active Directory
- `drweb-11.00.1-<assemblage>-esuite-modify-ad-schema-<version_de_l'OS>.exe`

  Utilitaire de la modification du schéma Active Directory
- `drweb-11.00.1-<assemblage>-esuite-aduac-<version_de_l'OS>.msi`

  Utilitaire de la modification des attributs des objets Active Directory
- `drweb-11.00.1-<assemblage>-esuite-napshv-<version_de_l'OS>.msi`

  NAP Validator
- `drweb-11.05.2-<assemblage>-esuite-agent-full-windows.exe`

  Installateur complet de l'Agent Dr.Web. Inclus dans la distribution supplémentaire du Serveur Dr.Web.
- `drweb-reploader-windows-<nombre_de_bits>.exe`

  Version de console du Chargeur du référentiel Dr.Web
- `drweb-reploader-gui-windows-<nombre_de_bits>.exe`

  Version graphique du Chargeur du référentiel 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 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. Octroi de 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 (https://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 licence 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**, le p. Particularités du réseau avec plusieurs Serveurs Dr.Web.

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

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

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

   Quand vous planifiez un réseau antivirus, pensez à créer une liste des personnes qui doivent avoir accès au Centre de gestion en fonction de leurs responsabilités. Préparez, également, une liste de rôles avec les responsabilités associées à chaque rôle. Il faut créer un groupe administratif pour chaque rôle. Pour associer les administrateurs aux rôles, placez les comptes d'administrateurs dans les groupes administratifs. Si nécessaire, vous pouvez hiérarchiser les groupes (rôles) dans un système à plusieurs niveaux et configurer les droits d'accès administratifs pour chaque niveau séparément.

   Pour en savoir plus sur la gestion des groupes administratifs et des règles d'accès, consultez le **Manuel d'installation**, la Chapitre 5 : Administrateurs du réseau antivirus

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.com/.

   Les Agents Dr.Web pour le poste sous OS Android, OS Linux, macOS 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 des Agents dans les **Manuels utilisateur** correspondants.

3. Installez la distribution principale du Serveur Dr.Web sur un ou plusieurs ordinateurs. L'installation est décrite dans 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, macOS, 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 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_du_Serveur>:9080`

   ou

   `https://<adresse_du_Serveur>:9081`

   où comme valeur <*adresse_du_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 nom et le mot de passe administrateur. Par défaut, les identifiants de l'administrateur ayant tous les droits sont :

   - Nom – **admin**.
   - Mot de passe :
     - sous Windows – le mot de passe a été spécifié lors de l'installation du Serveur.
     - pour les OS de la famille UNIX – mot de passe qui a été automatiquement créé au cours de l'installation du Serveur (voir aussi le p. Installation du Serveur Dr.Web pour les OS de la famille UNIX®).

   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 référentiel, spécifiez les composant du réseau antivirus à mettre à jour depuis le SGM Dr.Web. Dans la rubrique Statut du référentiel effectuez la mise à jour des produits du référentiel 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.

- S'il est nécessaire d'installer l'antivirus sur plusieurs postes d'un seul groupe utilisateur, vous pouvez utiliser le package d'installation de groupe créé en un seul exemplaire via le Centre de gestion pour plusieurs postes d'un groupe spécifique.
- Utilisez l'installateur réseau pour l'installation à distance sur un ou plusieurs postes en même temps (uniquement pour les postes tournant sous Windows). L'installation s'effectue via le Centre de gestion.
- Il est également possible d'installer l'antivirus à distance par réseau à l'aide du service Active Directory sur un ou plusieurs postes en même temps. Pour ce faire, il faut utiliser l'installateur de l'Agent Dr.Web pour les réseaux Active Directory fourni avec la distribution Dr.Web Enterprise Security Suite, mais séparément de l'installateur du Serveur.
- Si, lors de l'installation, il faut diminuer la charge sur le canal de communication entre le Serveur et les postes, vous pouvez utiliser l'installateur complet qui effectue l'installation de l'Agent et des composants de protection en même temps.
- Installation sur les postes sous OS Android, OS Linux et macOS peut s'effectuer de manière locale conformément aux règles générales. Le produit autonome installé peut se connecter au Serveur conformément à la configuration correspondante.

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.

Pour un fonctionnement correct de l'Agent Dr.Web sur l'OS de serveur Windows à partir de Windows Server 2016, il faut désactiver Windows Defender manuellement en utilisant les politiques de groupe.

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**, le p. Politique de connexion des postes) :
    a. En cas d'installation depuis les packages d'installation et la configuration de l'approbation automatique sur le Serveur, les postes de travail sont enregistrés automatiquement à la première connexion au Serveur et l'approbation supplémentaire n'est pas requise.
    b. En cas d'installation depuis les installateurs et la configuration de l'approbation manuelle, l'administrateur doit approuver manuellement de nouveaux postes pour les enregistrer sur le Serveur. Dans ce cas, les nouveaux postes ne se connectent pas automatiquement, mais ils sont déplacés par le Serveur dans le groupe de novices.
11. Après la connexion au Serveur et l'obtention des paramètres, l'ensemble des composants du package antivirus est installé sur le poste. Cet ensemble est spécifié dans les paramètres du groupe primaire du poste.

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

12. La configuration des postes et du logiciel est également possible après l'installation (vous pouvez consulter la description détaillée dans le **Manuel administrateur**, dans la Chapitre 7).

3.2. Configuration des connexions réseau

Généralités

Les client suivants se connectent au Serveur Dr.Web :

- Agents Dr.Web.
- Installateurs des Agents Dr.Web.
- Les Serveurs voisins Dr.Web.
- Serveurs proxy Dr.Web.

La connexion est toujours initiée par le client.

Les schémas suivants de connexion au Serveur sont disponibles :

1. Via les connexions directes.

   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`.

> Le port 2193 est enregistré pour Dr.Web Enterprise Management Service dans IANA.

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 lequel le Serveur Dr.Web est lancé) peut être indiquée directement dans les paramètres d'installation :

`drwinst /server` *<Adresse_du_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`.

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 de l'adresse 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 recherché 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.

3.3. Assurance d'une connexion sécurisée

3.3.1. Chiffrement et compression du trafic

Le mode de chiffrement est utilisé pour assurer la protection des données transmises par un canal non sécurisé et permet d'éviter la divulgation des données importantes et la substitution des logiciels téléchargés sur les postes protégés.

Le réseau antivirus Dr.Web Enterprise Security Suite utilise les outils cryptographiques suivants :

- Signature numérique (GOST R 34.10-2001).
- Chiffrement asymétrique (VKO GOST R 34.10-2001 – RFC 4357).
- Chiffrement symétrique (GOST 28147-89).
- Fonction de hachage cryptographique (GOST R 34.11-94).

Le réseau antivirus Dr.Web Enterprise Security Suite permet de chiffrer le trafic entre le Serveur et les clients qui comprennent:

- Les Agents Dr.Web.
- Installateurs des Agents Dr.Web.
- Les Serveurs voisins Dr.Web.
- Les Serveurs proxy Dr.Web.

Compte tenu du fait que le trafic entre les composants (surtout entre les Serveurs) peut être assez important, le réseau antivirus permet de compresser le trafic. La politique de compression et la compatibilité des paramètres des divers clients sont équivalents aux paramètres de chiffrement.

Politique de concordance des paramètres

La politique de chiffrement et de compression peut être configurée séparément sur chaque composant du réseau antivirus, la configuration d'autres composants doit être conforme à celle du Serveur.

Pour assurer une concordance entre les politiques de chiffrement et de compression sur le Serveur et sur un client, il faut noter qu'il existe des paramètres incompatibles dont la sélection entraîne l'échec de connexion entre le Serveur et le client concerné.

Le tableau 3-1 comprend les combinaisons des paramètres qui assurent (**+**) ou n'assurent pas (**–**) le chiffrement et la compression de la connexion entre le Serveur et le client ainsi que les combinaisons inappropriées (**Erreur**).

Tableau 3-1. Compatibilité des paramètres relatifs aux politiques de chiffrement et de compression

Paramètres de client	Paramètres du Serveur		
	Oui	**Possible**	**Non**
Oui	+	+	Erreur
Possible	+	+	–
Non	Erreur	–	–

Le chiffrement du trafic entraîne une charge importante sur les ordinateurs dont les performances sont proches de la limite inférieure des pré-requis relatifs aux composants installés. Dans le cas où le chiffrement du trafic n'est pas indispensable pour la sécurité, il est possible de ne pas l'utiliser.

Pour désactiver le mode de chiffrement, il faut d'abord basculer les paramètres du Serveur et des composants vers le statut **Possible** afin d'éviter l'apparition de paires de paramètres incompatibles client-Serveur.

L'utilisation de la compression diminue le trafic mais augmente considérablement l'utilisation de la mémoire vive et la charge sur les ordinateurs, beaucoup plus que le chiffrement.

Connexion via le Serveur proxy Dr.Web

Lors de la connexion des clients au Serveur via le Serveur proxy Dr.Web, il faut tenir compte des paramètres de chiffrement et de compression de tous les trois composants. Dans ce cas,

- Les paramètres du Serveur et du Serveur proxy (ici, il sert du client) doivent être coordonnés selon le tableau 3-1.
- Les paramètres du client et du Serveur proxy (ici, il sert du Serveur) doivent être coordonnés selon le tableau 3-1.

La possibilité de connexion via le Serveur proxy dépend de la version du Serveur et celle du client supportant des technologies de chiffrement particulières :

- Si le Serveur et le client supportent le chiffrement TLS utilisé dans la version 11.0.2, il suffit de satisfaire aux conditions décrites ci-dessus pour établir une connexion fonctionnelle.
- Si un des composants ne supporte pas le chiffrement TLS : la version 10 ou inférieure avec le chiffrement selon GOST est installée sur le Serveur et/ou le client, une vérification supplémentaire selon le tableau 3-2 est effectuée.

Tableau 3-2. Compatibilité des paramètres relatifs aux politiques de chiffrement et de compression en cas d'utilisation du Serveur proxy

Paramètres de connexion avec le client	Paramètres de connexion avec le Serveur			
	Rien	**Compression**	**Chiffrement**	**Tout**
Rien	Mode standard	Mode standard	Erreur	Erreur
Compression	Mode standard	Mode standard	Erreur	Erreur
Chiffrement	Erreur	Erreur	Mode transparent	Erreur
Tout	Erreur	Erreur	Erreur	Mode transparent

Conventions

Paramètres de connexion avec le Serveur et le client	
Rien	Ni la compression, ni le chiffrement n'est supporté.
Compression	Seule la compression est supportée.
Chiffrement	Seul le chiffrement est supporté.
Tout	La compression et le chiffrement sont supportés.
Résultat de la connexion	
Mode standard	La connexion établie signifie le fonctionnement en mode standard avec le traitement de commandes et la mise en cache.
Mode transparent	La connexion établie signifie le fonctionnement en mode transparent : sans traitement de commandes et la mise en cache. Le version sélectionnée du protocole de chiffrement est minimale : si un des composants (Serveur ou Agent) a la version 11, et l'autre – version 10, le chiffrement utilisé dans version 10 est spécifié.
Erreur	La connexion du Serveur proxy avec le Serveur et le client sera interrompue.

Ainsi, si le Serveur et l'Agent sont en versions différentes : l'un est en version 11. L'autre – en version 10 ou antérieure, les restrictions suivantes sont appliquées pour les connexions établies via le Serveur proxy.

- La mise en cache des données du Serveur proxy est possible uniquement si les deux connexions – avec le Serveur et avec le client sont établies sans l'utilisation de chiffrement.
- Le chiffrement sera utilisé uniquement si les deux connexions avec le Serveur et le client sont établies avec l'utilisation de chiffrement et les mêmes paramètres de compression (la compression est utilisée ou n'est pas utilisée pour les deux connexions).

Paramètres de chiffrement et de compression sur le Serveur

Pour configurer les paramètres de compression et de chiffrement du Serveur :

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion.
2. Dans la fenêtre qui s'affiche, sélectionnez l'élément du menu de gestion **Configuration de Serveur Dr.Web**.
3. Dans l'onglet **Réseau** → **Transport**, sélectionnez dans les listes déroulantes **Chiffrement** et **Compression** l'une des variantes suivantes :
   - **Oui** : le chiffrement (ou la compression) du trafic entre tous les clients est obligatoire (la valeur est spécifiée par défaut pour le chiffrement, si le paramètre n'a pas été modifié lors de l'installation du Serveur).
   - **Possible** : le chiffrement (ou la compression) sera appliqué au trafic relatif aux clients dont les paramètres le permettent.
   - **Non** : le chiffrement (ou la compression) n'est pas supporté (la valeur est spécifiée par défaut pour la compression si le paramètre n'a pas été modifié lors de l'installation du Serveur).

Quand vous configurer le chiffrement et la compression du côté du Serveur, prenez en compte les particularités de clients que vous projetez de connecter à ce Serveur. Pas tous les clients supportent le chiffrement et la compression du trafic.

Paramètres de chiffrement et de compression sur le Serveur proxy

Pour configurer de manière centralisée les paramètres de chiffrement et de compression pour le Serveur proxy :

Si le Serveur proxy n'est pas connecté au Serveur Dr.Web, pour pouvoir gérer les paramètres à distance, configurez la connexion, comme cela est décrit dans le le p. Connexion du Serveur proxy au Serveur Dr.Web.

1. Ouvrez le Centre de gestion pour le Serveur qui gère le serveur proxy.

2. Sélectionnez l'élément **Réseau antivirus** dans le menu principal du Centre de gestion, puis dans la fenêtre qui apparaît, dans la liste hiérarchique, cliquez sur le nom du Serveur proxy dont vous voulez éditer les paramètres ou sur le nom de son groupe primaire si les paramètres du Serveur proxy sont hérités.
3. Dans le menu de gestion qui s'affiche, sélectionnez l'élément **Serveur proxy Dr.Web**. La section des paramètres va s'ouvrir.
4. Ouvrez l'onglet **Écoute**.
5. Dans la liste déroulante **Paramètres de connexion avec les clients**, dans les listes déroulantes **Chiffrement** et **Compression**, sélectionnez le mode de chiffrement et de compression du trafic pour les canaux entre le Serveur proxy et les clients servis : les Agents et les installateurs des Agents.
6. Dans la section **Paramètres de connexion avec les Serveurs Dr.Web**, la liste des Serveurs vers lesquels le trafic sera redirigé est spécifiée. Sélectionnez le Serveur nécessaire dans la liste et cliquez sur le bouton dans la barre d'outils de cette section pour modifier les paramètres de connexion au Serveur Dr.Web sélectionné. Dans la fenêtre qui s'affiche, dans les listes déroulantes **Chiffrement** et **Compression**, sélectionnez le mode de chiffrement et de compression du trafic pour le canal entre le Serveur proxy et le Serveur sélectionné.
7. Pour sauvegarder les paramètres spécifiés, cliquez sur **Enregistrer**.

Pour configurer de manière locale les paramètres de chiffrement et de compression pour le Serveur proxy :

Si le Serveur proxy est connecté au Serveur Dr.Web gérant pour la configuration à distance, le fichier de configuration du Serveur proxy sera réécrit conformément aux paramètres reçus du Serveur. Dans ce cas, il faut spécifier les paramètres à distance depuis le Serveur ou désactiver le paramètres autorisant d'accepter la configuration de ce Serveur.

Le fichier de configuration `drwcsd-proxy.conf` est décrit dans les **Annexes**, l'Annexe G4.

1. Ouvrez le fichier de configuration `drwcsd-proxy.conf` sur l'ordinateur, sur lequel le Serveur proxy est installé.
2. Éditez les paramètres responsables de compression et de chiffrement pour les connexions avec les clients et les Serveurs.
3. Redémarrez le Serveur proxy :
   - Sous Windows :
     - Si le Serveur proxy est lancé en tant que service de l'OS Windows, le redémarrage s'effectue avec des outils standard du système.
     - Si le Serveur proxy est lancé dans la console, cliquez sur CTRL+BREAK pour le redémarrer.
   - Pour les OS de la famille UNIX :
     - Envoyez le signal `SIGHUP` au daemon du Serveur proxy.

- Exécutez la commande suivante :

Sous Linux :

```
/etc/init.d/dwcp_proxy restart
```

Sous FreeBSD :

```
/usr/local/etc/rc.d/dwcp_proxy restart
```

Paramètres de chiffrement et de compression sur les postes

Pour configurer de manière centralisée les paramètres de chiffrement et de compression sur les postes :

1. Sélectionnez l'élément **Réseau antivirus** dans le menu principal du Centre de gestion, puis dans la fenêtre qui apparaît, cliquez sur le nom du poste ou du groupe dans l'arborescence.
2. Dans le menu de gestion qui s'affiche, sélectionnez l'élément **Paramètres de connexion**.
3. Dans l'onglet **Général**, sélectionnez dans les listes déroulantes **Mode de chiffrement** et **Mode de compression** l'une des variantes suivantes :
   - **Oui** : le chiffrement (ou la compression) du trafic avec le Serveur est obligatoire.
   - **Possible** : le chiffrement (ou la compression) sera appliqué au trafic avec le Serveur, si les paramètres du Serveur le permettent.
   - **Non** : le chiffrement (ou la compression) n'est pas supporté.
4. Cliquez sur **Enregistrer**.
5. Les modifications seront appliquées dès que les paramètres auront été transmis sur les postes. Si les postes sont désactivés au moment de la modification des paramètres, les modifications seront transmises sur les postes juste après leur connexion au Serveur.

Agent Dr.Web pour Windows

Les paramètres de chiffrement et de compression peuvent être spécifiez lors de l'installation de l'Agent :

- En cas d'installation distante depuis le Centre de gestion, le mode de chiffrement et de compression est spécifié directement dans les paramètres de la section **Installation via le réseau**.
- En cas d'installation locale, l'installateur graphique n'accorde pas la possibilité de modifier le mode de chiffrement et de compression, pourtant ces paramètres peuvent être spécifiés à l'aide des clés de la ligne de commande lors du lancement de l'installateur (voir le document **Annexes**, le p. H2. Installateur réseau).

Après l'installation de l'Agent, la possibilité de modifier les paramètres de chiffrement ou de compression sur le poste de manière locale n'est pas accordée. Le mode **Possible** est spécifié par défaut (si une autre valeur n'a pas été spécifiée), cela veut dire que l'utilisation du

chiffrement et de la compression dépend des paramètres du côté du Serveur. Pourtant les paramètres du côté de l'Agent peuvent être modifiés via le Centre de gestion (voir ci-dessus).

Antivirus Dr.Web pour Android

L'Antivirus Dr.Web pour Android ne supporte ni chiffrement, ni compression. La connexion est impossible si la valeur **Oui** est spécifiée pour le chiffrement et/ou la compression du côté du Serveur ou du Serveur proxy (en cas de connexion via le Serveur proxy).

Antivirus Dr.Web pour Linux

Lors de l'installation de l'antivirus le mode de chiffrement et de compression ne peut pas être modifié. Le mode **Possible** est spécifié par défaut.

Après l'installation de l'antivirus, vous avez la possibilité de modifier les paramètres de chiffrement et de compression sur le poste uniquement en mode de la ligne de commande. Pour en savoir plus sur le ce mode et les clés correspondantes de la ligne de commande, consultez le **Manuel utilisateur Dr.Web pour Linux**.

Les paramètres peuvent également être spécifiés du côte du poste via le Centre de gestion (voir ci-dessus).

Antivirus Dr.Web pour macOS

La possibilité de modifier les paramètres de chiffrement ou de compression sur le poste de manière locale n'est pas accordée. Le mode **Possible** est spécifié par défaut, cela veut dire que l'utilisation du chiffrement et de la compression dépend des paramètres de côté du Serveur.

Les paramètres du côté du poste peuvent être modifiés via le Centre de gestion (voir ci-dessus).

3.3.2. Instruments assurant une connexion sécurisée

Lors de l'installation du Serveur Dr.Web, les outils suivants sont créés assurant la connexion sécurisées entre les composants du réseau antivirus :

1. **Clé privée de chiffrement du Serveur** `drwcsd.pri`**.**

   Sauvegardée sur le Serveur et n'est pas transmise aux autres composants du réseau antivirus.

   Si la clé privée est perdue, il faut rétablir manuellement la connexion entre les composants du réseau antivirus (créer tous les clés et les certificats et les distribuer sur tous les composants du réseau antivirus).

   La clé privée est utilisée dans les cas suivants :

   a) Création des clés publiques et des certificats.

La clé publique de chiffrement et le certificat sont créés automatiquement depuis la clé privée lors de l'installation du Serveur. Une nouvelle clé privée peut être créée ou bien la clé existante (de la dernière installation du Serveur) peut être utilisée. Les clés de chiffrement et les certificats peuvent être créés à tout moment à l'aide de l'utilitaire de serveur `drwsign` (voir les **Annexes**, p. H9.1. Utilitaire de génération des clés et des certificats).

Vous trouverez les informations sur les clés publiques et les certificats ci-dessous.

b) Authentification du Serveur.

L'authentification du Serveur par les clients distants s'effectue à la base de la signature numérique (une fois pour chaque connexion).

Le Serveur effectue la signature numérique du message avec la clé privée et envoie le message au client. Le client vérifie la signature du message à l'aide du certificat.

c) Déchiffrement des données.

En cas de chiffrement du trafic entre le Serveur et les clients, les données envoyées par le client sont déchiffrées sur le Serveur avec la clé publique.

2. **Clé publique de chiffrement du Serveur** `drwcsd.pub`**.**

Disponible pour tous les composants du réseau antivirus. La clé publique peut toujours être générée de la clé privée (voir ci-dessus). A chaque génération depuis la même clé privée, vous obtenez la même clé publique.

A partir de la version 11 du Serveur, la clé publique est utilisée pour la communication avec les clients des versions précédentes. Les autres fonctions sont transférées au certificat qui en même temps contient la clé publique de chiffrement.

3. **Certificat du Serveur** `drwcsd-certificate.pem`**.**

Disponible pour tous les composants du réseau antivirus. Le certificat contient la clé publique de chiffrement. Le certificat peut être généré de la clé privée (voir ci-dessus). A chaque génération depuis la même clé privée, vous obtenez un nouveau certificat.

Les clients connectés au Serveurs sont rattaché à un certificat particulier, c'est pourquoi en cas de perte du certificat sur le client vous pourrez le restaurer uniquement au cas où le même certificat est utilisé par un autre composant réseau : dans ce cas on peut copier sur le client depuis le Serveur ou depuis un autre client.

La certificat est utilisé dans les cas suivants :

a) Authentification du Serveur.

L'authentification du Serveur par les clients distants s'effectue à la base de la signature numérique (une fois pour chaque connexion).

Le Serveur effectue la signature numérique du message avec la clé privée et envoie le message au client. Le client vérifie la signature du message à l'aide du certificat (notamment, à l'aide de la clé publique indiquée dans le certificat). Dans les versions précédentes du Serveur, c'était la clé publique qui était utilisée à cet effet.

Pour cela, il faut qu'un ou plusieurs certificats fiables des Serveurs auxquels le client peut se connecter soient disponibles sur le client.

b) *Chiffrement des données*.

En cas de chiffrement du trafic entre le Serveur et les Clients, les données sont chiffrées par le client avec la clé publique.

c) *Réalisation d'une session TLS entre le Serveur et les clients distants*.

d) *Authentification du Serveur proxy*.

L'authentification des Serveurs proxy Dr.Web par les clients distants s'effectue à la base de la signature numérique (une fois pour chaque connexion).

Le Serveur proxy signe ses certificats par la clé privée et le certificat du Serveur Dr.Web. Le client qui fait confiance au certificat du Serveur Dr.Web aura confiance aux certificats qu'il a signés.

4. **Clé privée de chiffrement du serveur web.**

   Sauvegardée sur le Serveur et n'est pas transmise aux autres composants du réseau antivirus. Pour plus d'informations, voir ci-dessous.

5. **Certificat du serveur web.**

   Disponible pour tous les composants du réseau antivirus.

   Utilisé pour réaliser une session TLS entre le serveur web et le navigateur (via HTTPS).

   Lors de l'installation du Serveur à la base de la clé privée du serveur web, un certificat auto-signé est généré qui ne sera pas accepté par les navigateurs web car il n'a pas été délivré par un centre de certification connu.

   Pour que la connexion sécurisée (HTTPS) soit disponible, effectuez l'une des action suivantes :

   - Ajouter le certificat auto-signé aux fiables ou aux exclusions pour tous les postes et les navigateurs sur lesquels le Centre de gestion est ouvert.
   - Obtenir le certificat signé par le centre de certification connu.

3.3.3. Connexion des clients au Serveur Dr.Web

Pour pouvoir se connecter au Serveur Dr.Web le certificat du Serveur doit être présent du côté de client que le trafic entre le Serveur et le client soit chiffré ou non.

Les client suivants peuvent se connecter au Serveur Dr.Web :

- **Agents Dr.Web.**

  Pour le fonctionnement de l'Agent en mode centralisé avec la connexion au Serveur Dr.Web, il faut qu'un ou plusieurs certificats fiables des Serveurs auxquels l'Agent peut se connecter soient disponibles.

Le certificat utilisé lors de l'installation et les certificats reçus via les paramètres centralisés depuis le Serveur sont sauvegardés dans le registre, mais les fichiers de certificats ne sont pas utilisés.

Le fichier de certificat en seul exemplaire peut être ajouté à l'aide de la clé de la ligne de commande dans le répertoire de l'Agent (mais pas dans le registre) et la liste commune des certificats utilisés. Ce certificat sera utilisé pour la connexion au Serveur en cas d'erreur dans les paramètres centralisés.

Si le certificat est introuvable ou invalide, l'Agent ne pourra pas se connecter au Serveur, mais il continuera à fonctionner et effectuer les mises à jour en Mode mobile s'il est autorisé pour ce poste.

- **Installateurs des Agents Dr.Web.**

  Lors de l'installation de l'Agent sur le poste, le certificat du Serveur doit être présent, tout comme le fichier d'installation sélectionné.

  Si vous lancez le package d'installation créé dans le Centre de gestion, le certificat est inclus dans le package d'installation. Dans ce cas, il ne faut pas indiquer en outre le fichier de certificat.

  Après l'installation de l'Agent, les données du certificat sont inscrit dans le registre, le fichier du certificat n'est plus utilisé.

  Si le certificat est introuvable ou indisponible, l'installateur ne pourra pas installer l'Agent (cela concerne tous les types des fichiers d'installation de l'Agent).

- **Les Serveurs voisins Dr.Web.**

  Si vous configurez les connexions entre les Serveurs voisins Dr.Web en version 11, sur chaque Serveur configuré il vous faudra spécifier le certificat du Serveur avec lequel vous voulez établir la liaison (voir le **Manuel Administrateur**, le p. Configuration des liaisons entre les Serveurs Dr.Web).

  Si au moins un certificat est introuvable ou invalide, l'établissement de la liaison entre serveurs sera impossible.

- **Serveurs proxy Dr.Web.**

  Pour la connexion du Serveur proxy au Serveur Dr.Web avec la possibilité de la configuration distante via le Centre de gestion, il faut que le certificat soit présent sur le poste avec le Serveur proxy installé. Dans ce cas, le Serveur proxy pourra supporter le chiffrement.

  Si le certificat est introuvable, le Serveur proxy continuera à fonctionner, mais la gestion à distance, le chiffrement et la mise en cache seront indisponibles.

En cas de mise à niveau standard de tout le réseau antivirus de la version précédente qui utilisait les clés publiques vers la nouvelle version qui utilise les certificats, aucune action supplémentaire n'est requise.

L'installation de l'Agent fourni avec le Serveur en version 11 avec la connexion au Serveur en version 10 et vice-versa n'est pas recommandée.

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 référentiel sera supprimé et une nouvelle version du référentiel sera installée. Si pour une raison quelconque le référentiel 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 référentiel.

Le nom du répertoire dans lequel le Serveur est installé doit être spécifié dans la langue indiquée dans les paramètres de 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 du référentiel du Serveur Dr.Web).

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.

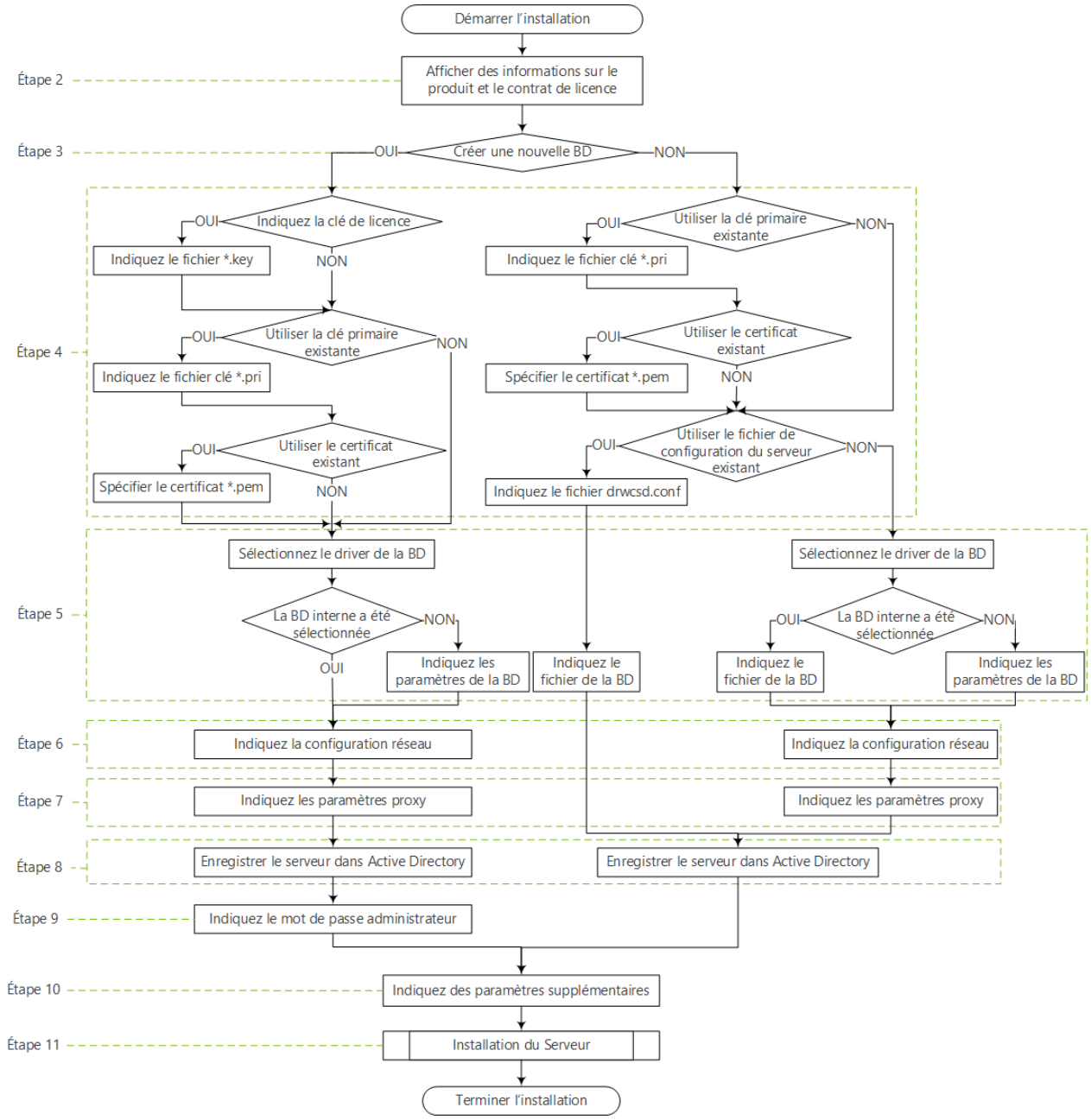

Figure 4-1. Schéma de la procédure d'installation du Serveur Dr.Web (Cliquez sur un élément de l'organigramme pour consulter la description)

Marche à suivre 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** spécifiez les paramètres suivants dans la fenêtre **Paramètres d'une nouvelle base de données** :

   - La case **Spécifier la clé de licence** permet de spécifier 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 privée de chiffrement 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 privée de chiffrement existante**. Les nouvelles clés de chiffrement et le certificat seront générées automatiquement durant l'installation.
     - Si vous installez un Serveur pour un réseau déjà existant, cochez la case **Utiliser la clé de chiffrement privée existante** et contenant une clé publique (le contenu de la clé publique correspondra au contenu de la clé publique précédente) et le certificat (à chaque génération de la même clé privée, un nouveau certificat est créé) sera généré automatiquement.
     - Si vous installez un Serveur pour un réseau déjà existant et que vous utilisez la clé de chiffrement privée existante, cochez la case **Utiliser le certificat existant** pour spécifier le fichier de certificat qui a été utilisé auparavant. Ceci permettra aux Agents déjà installés de se connecter au nouveau Serveur car les clients connectés au Serveur sont liés à un certificat particulier (à chaque génération de la même clé privée, un nouveau certificat est créé). Sinon, après l'installation, il sera nécessaire de copier le nouveau certificat 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, spécifiez le chemin vers le fichier contenant la clé publique correspondante dans le champ **Clé publique de chiffrement**.

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** spécifiez 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 privée de chiffrement 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 privée de chiffrement existante**. Les nouvelles clés de chiffrement et le certificat seront générées automatiquement durant l'installation.
  - Si vous installez un Serveur pour un réseau déjà existant, cochez la case **Utiliser la clé de chiffrement privée existante** et contenant une clé publique (le contenu de la clé publique correspondra au contenu de la clé publique précédente) et le certificat (à chaque génération de la même clé privée, un nouveau certificat est créé) sera généré automatiquement.
  - Si vous installez un Serveur pour un réseau déjà existant et que vous utilisez la clé de chiffrement privée existante, cochez la case **Utiliser le certificat existant** pour spécifier le fichier de certificat qui a été utilisé auparavant. Ceci permettra aux Agents déjà installés de se connecter au nouveau Serveur car les clients connectés au Serveur sont liés à un certificat particulier (à chaque génération de la même clé privée, un nouveau certificat est créé). Sinon, après l'installation, il sera nécessaire de copier le nouveau certificat 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, spécifiez le chemin vers le fichier contenant la clé publique correspondante dans le champ **Clé publique de chiffrement**.

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 :

- L'option **SQLite (base de données embarquée)** active 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.

     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 référentiel après la fin de l'installation** pour mettre à jour automatiquement le référentiel 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.

Les plateformes supportées par Oracle Client sont listées sur le site de l'éditeur.

- 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 normalement 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 **Dr.Web Server** 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 :

   `./<fichier_de_distribution>.tar.gz.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. H8. Installateur du Serveur Dr.Web pour les OS de la famille UNIX®.

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

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.

6. Lors de l'installation un mot de passe aléatoire est généré pour l'administrateur principal. Après la fin de l'installation, ce mot de passe s'affiche via la console dans les résultats de l'installation du Serveur.

Le mot de passe de l'administrateur est sauvegardé dans la base de données du Serveur. S'il est nécessaire, vous pouvez consulter ce mot de passe à l'aide des outils de gestion de la base de données (en cas d'utilisation de la base de données externe) ou à l'aide de l'utilitaire `drwidbsh` pour la base de données intégrée (pour plus d'informations, voir les **Annexes**, le p. Récupération de mot de passe de l'administrateur Dr.Web Enterprise Security Suite).

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

Utilisez les commandes :

- `/usr/local/etc/rc.d/drwcsd stop` : pour l'arrêt manuel du Serveur ;
- `/usr/local/etc/rc.d/drwcsd start` : pour le lancement manuel du 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.

Configuration d'Astra Linux en version 1.6 pour l'installation du Serveur Dr.Web en mode ELF

En cas d'installation du Serveur dans l'environnement Astra Linux en version 1.6 fonctionnant en mode ELF (environnement logiciel fermé), vous pouvez échouer à lancer l'installateur si la clé publique de chiffrement du Serveur Dr.Web n'est pas présente dans la liste des clés de confiance. Dans ce cas il faut préconfigurer le mode ELF et redémarrer l'installateur.

Pour préconfigurer le mode ELF :

1. Installez le paquet `astra-digsig-oldkeys` depuis le disque de l'OS s'il n'est pas encore installé.
2. Placez la clé publique de chiffrement du Serveur Dr.Web dans le répertoire `/etc/digsig/keys/legacy/keys` (s'il n y a pas le répertoire, il faut le créer).
3. Exécutez la commande suivante :

```
# update-initramfs -k all -u
```

4. Redémarrez le système.

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 suivre 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 Server 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 suivre 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 :

   `./<fichier_de_distribution>.tar.gz.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.

4.2. 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.

Pour un fonctionnement correct de l'Agent Dr.Web sur l'OS de serveur Windows à partir de Windows Server 2016, il faut désactiver Windows Defender manuellement en utilisant les politiques de groupe.

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 11.0.2 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 11.0.2, 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 11.0.2 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, il est recommandé d'effectuer l'installation des Agents de manière locale avec l'assistant d'installation et de suppression des programmes depuis le **Panneau de configuration** Windows. L'installation distante dans ce cas peut provoquer des erreurs de fonctionnement du protocole Remote Desktop.
- Il n'est pas recommandé d'installer les composants SpIDer Gate, Office Control, SpIDer Mail et le Pare-feu Dr.Web sur les serveurs exécutant des fonctions réseau importantes (contrôleurs de domaine, serveurs de distribution des licences etc.) afin d'éviter d'éventuels conflits entre les services réseau et les composants intérieurs de l'antivirus Dr.Web.
- L'installation de l'Agent sur le cluster doit être réalisée séparément pour chaque nœud du cluster.
- Les principes de fonctionnement de l'Agent et des composants du package antivirus sur un nœud du cluster sont pareils aux principes relatifs à un serveur LAN, il n'est pas recommandé d'installer sur les nœuds du cluster les composants 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. Le package d'installation personnel est créé dans le Centre de gestion à la base de l'installateur de l'Agent. 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 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 un 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.

Package d'installation de groupe

Le package d'installation de groupe de l'Agent est généré dans le Centre de gestion pour l'installation sur le poste d'un groupe utilisateur particulier. Dans ce cas, l'Agent est installé sur tous les postes tournant sous le même OS du même package d'installation de groupe.

Le package d'installation de groupe inclut l'installateur de l'Agent, les paramètres de connexion au Serveur, ainsi que l'identificateur et le mot de passe du groupe utilisateur dans lequel le poste sera inclus après l'installation de l'Agent. Pourtant les paramètres d'authentification du poste sur le Serveur et les composants antivirus ne sont pas inclus dans le package d'installation de groupe.

Le lien de téléchargement du package d'installation de groupe est disponible dans la rubrique de paramètres du groupe utilisateur.

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 `webmin/install` (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-11.05.2-<assemblage>-esuite-agent-full-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, macOS.

Les installateurs pour l'installation de l'Antivirus sont disponibles sur 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 publique de chiffrement `drwcsd.pub`.
3. Certificat du Serveur `drwcsd-certificate.pem`.

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 référentiel du Serveur (voir **Manuel Administrateur**, p. Mise à jour manuelle des composants Dr.Web Enterprise Security Suite, p. **Vérification des mises à jour**).

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

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

- Package d'installation personnel créé dans le Centre de gestion.
- Package d'installation de groupe 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) L'installateur de l'Agent Dr.Web est fourni lors de la création du package d'installation personnel, ainsi que les paramètres de connexion au Serveur et les paramètres d'authentification du poste sur le Serveur.

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_<OS>_<poste>.exe`.
- Package d'installation de groupe créé dans le Centre de gestion `drweb_ess_<OS>_<groupe>.exe`.
- Installateur complet de l'Agent Dr.Web `drweb-11.05.2-<assemblage>-esuite-agent-full-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) Lors de l'installation depuis le package d'installation de groupe, les paramètres de connexion au Serveur, ainsi que l'identificateur et le mot de passe du groupe utilisateur dans lequel le poste sera inclus après l'installation de l'Agent, sont inclus dans le package d'installation. Pourtant les paramètres d'authentification du poste sur le Serveur et les composants antivirus ne sont pas inclus dans le package d'installation de groupe. Après

l'installation de l'Agent, il établit la connexion au Serveur lors de laquelle l'Agent détermine la disponibilité de postes libres dans le groupe utilisateur, dont le package d'installation de groupe a été utilisé. Si les postes libres sont disponibles, les paramètres d'authentification du poste sur le Serveur sont fournis automatiquement.

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.

d) 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.

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	+	–	+	+
	de groupe	+	–	+	–
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. Si l'utilisateur effectue l'installation de l'Agent Dr.Web lui-même, envoyez-lui le lien vers le package d'installation personnel de l'Agent Dr.Web pour le système d'exploitation correspondant de l'ordinateur ou de l'appareil mobile.

   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. Pour les postes sous macOS, configurez les paramètres de connexion au Serveur Dr.Web de manière locale.

   En cas de l'installation de l'Agent Dr.Web à l'aide du package d'installation personnel pour les autres systèmes supportés, 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.

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 **Adresse du Serveur Dr.Web**. 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 **Adresse du Serveur Dr.Web**. 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 à l'aide du Centre de gestion Dr.Web :

1. Dans le menu principal du Centre de gestion, sélectionnez l'élément **Réseau antivirus**.
2. Dans la barre d'outils, cliquez sur le bouton **Ajouter un objet de réseau** → **Créer un poste**. Le panneau de création du compte du poste sera affiché dans la partie droite de la fenêtre du Centre de gestion.
3. Spécifiez le nombre des comptes 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 remplis de manière automatique et il sera impossible de les modifier durant la création des postes.

7. Dans le champ **Description**, entrez des informations supplémentaires sur le poste. 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 d'exclure le poste du groupe **Everyone** ou du 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.

- Dans la liste **Politiques**, vous pouvez spécifier la politique dont les paramètres seront utilisés pour le poste créé.
  Par défaut, la politique n'est pas assignée. Pour assigner la politique, cochez la case contre la politique nécessaire. Les paramètres du poste seront hérités des paramètres de la version actuelle de cette politique. Pas plus d'une seule politique peut être assignée au poste.

9. Dans la section **Serveur proxy**, vous pouvez spécifier les paramètres du Serveur proxy Dr.Web lié à ce poste.
   Si vous voulez installer le Serveur proxy sur le poste créé, cochez la case **Créer un Serveur proxy lié** et spécifiez les paramètres du Serveur proxy. Les paramètres sont équivalents aux paramètres utilisés lors de la création du Serveur proxy.

   Lors de la création du compte du poste, le compte du Serveur proxy sera créé dans le Centre de gestion. Après le transfert des paramètres sur le poste, le Serveur proxy sera installé sur ce poste en tâche de fond. L'Agent se connectera au Serveur uniquement via le Serveur proxy installé. L'utilisation du Serveur proxy sera transparente pour l'utilisateur.

10. 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.
11. Si nécessaire, spécifiez les paramètres dans la rubrique **Emplacement**.
12. Cliquez sur le bouton **Enregistrer** 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.
    - 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, macOS et Linux.

    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.

    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.

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.

- L'élément **Mot de passe** contient le mot de passe pour l'accès de ce poste au Serveur. Pour voir le mot de passe, cliquez sur .
- L'élément **Mot de passe du Serveur proxy** contient le mot de passe pour l'accès du Serveur proxy au Serveur si le poste a été créé avec le Serveur proxy lié (voir l'étape 9).
- 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.

13. 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 pour un poste tournant sous macOS

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` situé à l'intérieur du package d'installation personnel.

   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.

4.2.2.2. Installation de l'Agent Dr.Web avec le package d'installation de groupe

Pour installer l'Agent Dr.Web avec le package d'installation de groupe, procédez comme suit :

1. A l'aide du Centre de gestion créez un nouveau groupe utilisateur sur le Serveur Dr.Web (pour en savoir plus sur la procédure de la création de groupes consultez le **Manuel Administrateur**, p. Création et suppression de groupes). Vous pouvez également utiliser un groupe existant que vous avez créé précédemment.
2. Si nécessaire, spécifiez dans le Gestionnaire de licence la clé de licence personnelle pour le groupe. Sinon, le groupe va hériter la clé de licence du groupe parent.

3. A l'aide du Centre de gestion créez des comptes pour de nouveaux postes sur le Serveur Dr.Web. Aoutez les nouveaux comptes de postes dans le groupe utilisateur de l'étape 1 et spécifiez ce groupe comme primaire. Dans le groupe utilisateur, il est possible de créer autant de nouveaux postes qu'il y a des licences libres disponibles dans ce groupe.
4. Le lien vers le package d'installation de groupe sera disponible dans les paramètres du groupe. Les packages d'installation seront partagés selon les tarifs correspondants : un package d'installation pour un tarif pour chaque système d'exploitation.
5. Si les utilisateurs effectuent l'installation de l'Agent Dr.Web eux-mêmes, envoyez-leur le lien vers le package d'installation de l'Agent Dr.Web pour le système d'exploitation correspondant de l'ordinateur ou de l'appareil mobile. Dans ce cas, le même package d'installation de groupe pour le système d'exploitation correspondant sera envoyé à tous les utilisateurs.
6. 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.

7. Après l'installation de l'Agent, l'Agent se connecte au Serveur indiqué dans le package d'installation de groupe. Lors de la première connexion au Serveur, la disponibilité de postes libres dans le réseau utilisateur, dont le package d'installation a été utilisé pour l'installation de l'Agent. La quantité de postes libres est déterminée d'après le nombre de comptes dans ce groupe dont le délai d'accès n'a pas expiré. A chaque connexion du package d'installation de groupe, le nombre de postes libres est recompté pour fournir des informations actuelles.
   a) En cas de disponibilité de postes libres. Les paramètres d'authentifications de poste pour la connexion au Serveur sont attribués automatiquement. Cette procédure s'effectue de manière transparente pour l'Administrateur et ne nécessite aucune intervention de l'utilisateur.
   b) En cas d'absence de postes libres dans ce groupe, l'installation s'interrompe et le message adressé à l'utilisateur s'affiche.

4.2.2.3. 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, macOS

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, macOS.

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-11.05.2-<assemblage>-esuite-agent-full-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 `webmin/install` dans le répertoire d'installation du Serveur. Vous pourrez le déplacer ultérieurement) ou téléchargez le fichier exécutable de l'installateur `drwinst.exe` et le certificat `drwcsd-certificate.pem` depuis la page d'installation du Centre de gestion. Lancez le fichier `drwinst.exe` avec la clé du mode de 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 publique de chiffrement 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).

   S'il faut installer l'Agent sur l'ordinateur sur lequel le Serveur est installé, il faut spécifier l'adresse du Serveur directement dans les paramètres de lancement de l'installateur, car le Serveur risque de ne pas être détecté lors de la recherche via une requête multicast.

   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 `webmin/install` dans le répertoire d'installation du Serveur. Vous pourrez le déplacer ultérieurement) ou téléchargez le fichier exécutable de l'installateur `drwinst.exe` et le certificat `drwcsd-certificate.pem` 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'utilisation de ces paramètres avant d'apporter des modifications dans le système ou de refuser l'installation à distance et d'installer l'Agent manuellement.

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)**

OS	Configuration	
		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 dans les stratégies locales	Nouveau style : **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 :

OS	Configuration	
		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** : 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.	
Windows 7 Windows Server 2008 R2	Activer le partage de fichiers et d'imprimantes	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**.
		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**.
	Configurez le mode d'authentification réseau dans les stratégies locales	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**.
		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 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.</td></tr>
</table>

OS	Configuration
	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.

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**.

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 antivirus.

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**, p. 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. Dans la fenêtre qui apparaît sélectionnez l'élément du menu de gestion **Scanner réseau**. Une fenêtre vide portant le même nom s'ouvrira.
2. Spécifiez les paramètres de recherche des postes sur le réseau. Pour une description détaillée des paramètres, consultez le **Manuel Administrateur**, p. Scanner réseau.
3. 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.
4. 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	
	Postes actif avec l'antivirus installé.
	Poste actif avec le statut non approuvé du logiciel : il n'y a pas de logiciel antivirus sur l'ordinateur ou la disponibilité de l'antivirus n'est pas vérifiée.

   Vous pouvez ouvrir les éléments du répertoire correspondant aux postes ayant l'icône  pour consulter l'ensemble des composants installés.
5. Dans la fenêtre du **Scanner réseau**, sélectionnez un ordinateur non protégé (ou plusieurs ordinateurs non protégés en utilisant les boutons CTRL ou SHIFT).
6. Dans la barre d'outils, cliquez sur le bouton  **Installer l'Agent Dr.Web**.
7. La fenêtre **Installation via réseau** va s'afficher pour créer la tâche d'installation de l'Agent.
8. 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**.

9. 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.

10. 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 (mode *Multicast*).

   

   S'il faut installer l'Agent sur l'ordinateur sur lequel le Serveur est installé, il faut spécifier l'adresse directement dans le champ **Serveur Dr.Web**, car le Serveur risque de ne pas être détecté lors de la recherche via une requête multicast.

11. Dans le menu déroulant **Langue**, sélectionnez la langue de l'interface de l'Antivirus Dr.Web qui sera installé sur les postes.
12. Dans le champ **Nombre des installations simultanées**, spécifiez le nombre maximum des postes sur lesquels l'installation distante est possible.
13. Dans le champ **Délai d'installation (s)**, spécifiez un délai d'attente maximum en secondes avant la fin d'installation de l'Agent. Les valeurs admissibles sont les suivantes : 1-600. Le délai de 180 secondes est spécifié par défaut. 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.
14. Si nécessaire, cochez la case **Enregistrer l'Agent Dr.Web dans la liste des logiciels installés**.
15. Dans la rubrique **Composants à installer**, sélectionnez les composants du package antivirus à installer sur les postes.
16. 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.
17. 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.

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

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

Pour lancer l'installation, on utilise l'installateur réseau du Serveur actuel se trouvant dans le répertoire `webmin\install\windows` du répertoire d'installation du Serveur et le certificat SSL `drwcsd-certificate.pem` se trouvant dans le répertoire `etc` du répertoire d'installation du Serveur.

19. 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.
20. 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 **8-21** de la procédure 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 **2-21** de la procédure 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 le bouton **Installer l'Agent Dr.Web**.
   c) La fenêtre du Scanner réseau va s'afficher.
   d) Les étapes suivantes sont équivalentes aux étapes **2-21** de la procédure 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 sur le site https://download.drweb.com/ 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-11.05.4-<assemblage>-esuite-agent-activedirectory.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 F.
- `ESSERVERPATH=<nom_complet_du_fichier>` : le chemin complet vers le certificat du Serveur Dr.Web et le nom de fichier (par défaut c'est le fichier `drwcsd-certificate.pem` dans le sous-répertoire `webmin/install` 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-certificate.pem TARGETDIR=\\comp\share
```

```
msiexec /a ES_Agent.msi /qn ESSERVERADDRESS=192.168.14.1 ESSERVERPATH="C:
\Program Files\DrWeb Server\webmin\install\drwcsd-certificate.pem"
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_l'installateur>\<nom_du_package>.msi
   ```

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

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

3. Dans la nouvelle fenêtre, spécifiez le nom DNS ou l'adresse IP du Serveur Dr.Web (voir **Annexes**, p. Annexe E). Spécifiez également l'emplacement du certificat du Serveur Dr.Web (drwcsd-certificate.pem). 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** apparaît et vous informe sur le produit en cours d'installation. Cliquez sur le bouton **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 appliquer 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.

Vous pouvez installer le Serveur proxy sous Windows par l'un des moyens suivants :

- Automatiquement lors de l'installation de l'Agent Dr.Web pour Windows

  L'installation s'effectue depuis le package d'installation personnel de l'Agent Dr.Web pendant la création duquel les paramètres pour l'installation du Serveur proxy lié ont été spécifiés. Dans ce cas, l'installation du Serveur proxy se fait automatiquement en tâche de fond.
- Automatiquement sur le poste avec l'Agent Dr.Web pour Windows installé

  Dans le Centre de gestion du poste sélectionné, configurez la création du Serveur proxy lié. Le Serveur proxy sera installé sur le poste automatiquement en tâche de fond.
- Manuellement avec l'installateur graphique

  L'administrateur effectue l'installation manuellement sur tout poste approprié du réseau. Aucun autre composant du réseau antivirus ne peut être installé sur ce poste.

L'installation du Serveur proxy sous l'OS de la famille UNIX ne se fait que manuellement à l'aide de l'installateur.

4.4.1. Connexion du Serveur proxy au Serveur Dr.Web

A partir de la version 11, il existe la possibilité de connexion du Serveur proxy Dr.Web au Serveur Dr.Web pour la gestion distante des paramètres et le support du chiffrement du trafic.

Paramètres de connexion

Pour la connexion du Serveur proxy au Serveur Dr.Web, il faut :

- **Certificat du Serveur** `drwcsd-certificate.pem`**.**

  Il faut que les certificats de tous les Serveurs auxquels le Serveur proxy se connecte et vers lesquels le trafic client est redirigé soient disponibles.
  - Le certificat du Serveur est requis pour la connexion au Serveur afin de gérer à distance les paramètres et chiffrer le trafic entre le Serveur et le Serveur proxy.
  - Le certificat du Serveur proxy signé par le certificat et la clé privée du Serveur (la procédure se fait automatiquement sur le Serveur après la connexion et elle ne nécessite pas l'intervention de l'administrateur) est requis pour la connexion des Agents et le support du chiffrement entre les Agents et le Serveur proxy.

  Tous les certificats des Serveurs sont stockés sur le Serveur proxy dans le fichier de configuration `drwcsd-proxy-trusted.list` au format suivant (les entrées des certificats sont séparées par une ou plusieurs lignes vides) :

```
[<certificat_1>]
```

```
[<certificat_2>]


[<certificat_3>]

...
```

- **Adresse du Serveur.**

  Le Serveur proxy se connecte à tous les Serveurs Dr.Web qui sont indiqués dans son fichier de configuration pour la redirection du trafic client. Pourtant, la réception des paramètres est autorisée seulement depuis un ensemble particulier des Serveurs qui sont marqués comme gérants. Si plusieurs Serveurs sont marqués comme gérants, la connexion se fait à tous les Serveurs à tour de rôle jusqu'à l'obtention d'une configuration valide (non vide).

- **Identificateur et mot de passe pour l'accès au Serveur.**

  Les identifiants sont disponibles après la création du compte du Serveur proxy via le Centre de gestion (voir Création du compte du Serveur proxy).

  > L'identificateur et le mot de passe du Serveur proxy sont utilisés en unique exemplaire. Sur tous les Serveurs auxquels le Serveur proxy se connecte, vous devez créer des comptes du Serveur proxy avec les mêmes identifiants.

  Les identifiants sont sauvegardés sur le Serveur proxy, dans le fichier de configuration `drwcsd-proxy.auth` au format suivant :

```
[<ID_du_Serveur_proxy>]

[<Mot_de_passe_du_Serveur_proxy>]
```

Connexion du Serveur proxy au Serveur Dr.Web

> Pour pouvoir connecter le Serveur proxy Dr.Web, il faut activer le protocole nécessaire du coté du Serveur Dr.Web. Pour ce faire, dans le Centre de gestion, dans la section **Administration → Configuration du Serveur Dr.Web → Modules**, cochez la case **Protocole du Serveur proxy Dr.Web**, enregistrez les paramètres et redémarrez le Serveur.

Automatiquement lors de l'installation sous l'OS Windows

- Si le Serveur proxy a été installé durant l'installation de l'Agent ou sur un poste avec l'Agent installé, la connexion au Serveur se fait automatiquement.
- Si le Serveur proxy a été installé via l'installateur graphique sous Windows, la connexion au Serveur se fait automatiquement avec les paramètres de connexion indiqués par l'administrateur dans les paramètres de l'installateur.

Après l'installation du Serveur proxy, les fichiers de connexion au Serveur se trouvent par défaut dans le répertoire : `%ALLUSERSPROFILE%/Doctor Web/drwcs/etc`.

Manuellement lors de l'installation sous l'OS de la famille UNIX :

1. Installez le Serveur proxy pour les OS de la famille UNIX conformément à la procédure décrite dans la rubrique Installation du Serveur proxy avec l'installateur.
2. Créez un compte du Serveur proxy à l'aide du Centre de gestion de la sécurité Dr.Web, comme cela est décrit dans la rubrique Création du compte du Serveur proxy.
3. Copiez le certificat du Serveur sur l'ordinateur sur lequel le Serveur proxy est installé.
4. Dans le fichier de configuration `drwcsd-proxy-trusted.list`, indiquez le certificat, copié sur l'ordinateur à l'étape 3 : copiez le contenu du fichier de certificat et insérez-le dans le fichier de configuration conformément au format décrit ci-dessus.
5. Dans le fichier de configuration `drwcsd-proxy.auth`, spécifiez les paramètres de connexion au Serveur pour le compte créé à l'étape 2 conformément au format décrit ci-dessus.

   Les fichiers `drwcsd-proxy-trusted.list` et `drwcsd-proxy.auth` doivent se trouver dans les répertoires suivants :

   - sous Linux : `/var/opt/drwcs/etc`
   - sous FreeBSD : `/var/drwcs/etc`

   Pour les fichiers, il faut spécifier les droits suivants :

```
drwcsd-proxy-trusted.list 0644 drwcs:drwcs

drwcsd-proxy.auth 0600 drwcs:drwcs
```

4.4.2. Création du compte du Serveur proxy

L'administrateur doit créer les comptes du Serveur proxy sur tous les Serveurs auxquels le Serveur proxy se connectera (vers lesquels le trafic sera redirigé).

Marche à suivre pour créer un compte du Serveur proxy à l'aide du Centre de gestion de la sécurité Dr.Web :

1. Spécifiez les paramètres pour le groupe parent dans lequel vous allez créer le Serveur proxy. La procédure de configuration des paramètres est décrite dans le **Manuel Administrateur**, dans la rubrique Configuration distante du Serveur proxy. Dans ce cas, les paramètres spécifiés seront hérités par le Serveur proxy lors de la connexion. Vous pouvez également spécifier ces paramètres après la création du compte du Serveur proxy (tant pour le groupe parent en cas d'héritage que personnellement pour le Serveur proxy) mais avant la connexion du Serveur proxy au compte.

Si les paramètres n'ont pas été spécifiés avant la connexion du Serveur proxy, le fichier de configuration ne sera pas téléchargé. Le Serveur proxy utilisera les paramètres actuels jusqu'à ce que les paramètres soient spécifiés sur le Serveur connecté, à condition qu'il soit autorisé à gérer la configuration.

2. Dans le menu principal du Centre de gestion, sélectionnez l'élément **Réseau antivirus**.
3. Les actions nécessaires pour la création du Serveur proxy dépendront du fait que vous vouliez installer le Serveur proxy sur le poste existant avec l'Agent Dr.Web ou installer le Serveur prozy séparément :

№	Actions	Installer avec l'Agent	Installer séparément
a)	1. Dans l'arborescence du réseau antivirus, sélectionnez le poste pour l'installation du Serveur proxy lié. 2. Dans le panneau de propriétés du poste sélectionné, ouvrez la section **Serveur proxy**.	+	–
b)	1. Dans l'arborescence du réseau antivirus, sélectionnez le poste pour l'installation du Serveur proxy lié. 2. Dans la barre d'outils, sélectionnez l'option **Ajouter un objet de réseau** → **Créer un Serveur proxy**.	+	+
c)	1. Assurez-vous qu'aucun poste n'est sélectionné dans l'arborescence du réseau antivirus. 2. Dans la barre d'outils, sélectionnez l'option **Ajouter un objet de réseau** → **Créer un Serveur proxy**.	+	+

Si vous créez un compte du Serveur proxy pour l'installation sur les postes avec l'Agent, l'installation du Serveur proxy s'effectuera automatiquement via l'Agent en tâche de fond, juste après la création du Serveur proxy (voir aussi Installation du Serveur proxy lors de l'installation de l'Agent Dr.Web pour Windows).

Si vous créez un compte du Serveur proxy pour l'installation particulière (sans liaison à l'Agent), l'administrateur devra installer le Serveur proxy manuellement depuis le package d'installation fourni avec la distribution du Serveur.

4. L'identificateur unique du compte créé est généré automatiquement dans le champ **Identificateur**. Si nécessaire, vous pouvez le modifier.
5. Dans le champ **Nom**, spécifiez le nom du Serveur proxy qui sera affiché dans l'arborescence du réseau antivirus.
6. Dans les champs **Mot de passe** et **Confirmez le mot de passe**, entrez le mot de passe pour que le Serveur proxy puisse accéder au Serveur. Si le mot de passe n'est pas spécifié, il sera généré automatiquement.

L'identificateur et le mot de passe du Serveur proxy sont utilisés en unique exemplaire. Sur tous les Serveurs auxquels le Serveur proxy se connecte, vous devez créer des comptes du Serveur proxy avec les mêmes identifiants (voir Connexion des clients au Serveur Dr.Web).

Après la création du compte du Serveur proxy, l'édition de l'identificateur sera impossible.

7. Pour le étapes 3.b) et 3.c) dans le champ **Poste**, spécifiez un poste existant avec l'Agent installé auquel ce Serveur proxy sera lié.

   Pour l'étape 3.b), l'identificateur du poste sélectionné sera automatiquement ajouté dans le champ **Poste**.

   Pour l'étape 3.c), le champ **Poste** reste vide.

   - Pour spécifier un poste sur lequel le Serveur proxy sera installé, cliquez sur  et, dans la fenêtre qui s'affiche, sélectionnez un poste existant dans l'arborescence du réseau antivirus.
   - Laissez le champ **Poste** vide pour ne pas lier le Serveur proxy à un poste et connecter le Serveur proxy installé manuellement. Si le champ **Poste** est déjà rempli, cliquez sur  pour supprimer le poste lié.

8. La section **Appartenance** contient le groupe dont le Serveur proxy créé fera partie. Pour modifier le groupe, cochez la case contre le groupe nécessaire dans la liste affichée.

   Chaque Serveur proxy peut appartenir à un seul groupe.

   Il est possible de sélectionner un groupe prédéfini **Proxies** ou ses sous-groupes.

9. Cliquez sur **Enregistrer**.

   La fenêtre annonçant la création réussie du compte du Serveur proxy va s'afficher. Cette fenêtre contiendra également le mot de passe d'accès au Serveur. Pour afficher le mot de passe, cliquez  .

L'administrateur a besoin de l'identificateur et du mot de passe du compte du Serveur proxy créé via le Centre de gestion pour la connexion du Serveur proxy au Serveur :

- Lors de l'installation du Serveur proxy via l'installateur graphique.
- Manuellement après l'installation du Serveur proxy (uniquement pour les OS de la famille UNIX).

4.4.3. Installation du Serveur proxy lors de l'installation de l'Agent Dr.Web pour Windows

Pour installer le Serveur proxy ensemble avec l'Agent Dr.Web pour Windows :

1. Spécifiez les paramètres du Serveur proxy dans le Centre de gestion comme cela est décrit dans le **Manuel Administrateur**, le p. Configuration distante du Serveur proxy. Les paramètres doivent être spécifiés pour le groupe dans lequel vous allez créer le Serveur proxy. Dans ce cas, les paramètres spécifiés seront hérités par le Serveur proxy au moment de la création. Vous pouvez également spécifier ces paramètres après la création du Serveur proxy (tant pour le groupe en cas d'héritage que personnellement pour le Serveur proxy) mais avant la connexion du Serveur proxy au compte créé.

Si les paramètres n'ont pas été spécifiés avant la connexion du Serveur proxy, les paramètres transmis au Serveur proxy par l'installateur seront utilisés. Ces paramètres impliquent seulement la connexion au Serveur depuis lequel l'installation a été effectuée.

2. Créez le compte du poste à l'aide du Centre de gestion comme cela est décrit dans la rubrique Installation de l'Agent Dr.Web avec le package d'installation personnel. Lors de la création du compte, cochez la case **Créer un Serveur proxy lié** et spécifiez les paramètres. Notamment, indiquez le groupe pour le placement du Serveur proxy pour lequel vous avez spécifié les paramètres à l'étape 1.

   Vous pouvez modifier l'identificateur du Serveur proxy uniquement lors de la création du compte.

3. Sur le poste, lancez l'installation de l'Agent depuis le package d'installation personnel créé à l'étape 2.
4. Après l'installation, l'Agent télécharge automatiquement l'installateur du Serveur proxy depuis le Serveur et lance l'installateur en tâche de fond sur le même poste. Le certificat et l'adresse du Serveur, ainsi que les identifiants utilisés pour la connexion au Serveur seront automatiquement inscrits dans les fichiers de configuration du Serveur proxy. Seul le Serveur depuis lequel l'installation a été effectuée est indiqué dans les paramètres du Serveur proxy pour la redirection du trafic.
5. Après l'installation, le Serveur proxy se connectera au Serveur depuis lequel l'installation a été effectuée pour la réception du fichier de configuration valide. Si les paramètres n'ont pas été spécifiés à l'étape 1, le fichier de configuration ne sera pas téléchargé. La configuration spécifiée par l'installateur sera utilisée jusqu'à ce que la configuration sur le Serveur connecté soit spécifiée.
6. L'Agent se connectera au Serveur uniquement via le Serveur proxy installé. L'utilisation du Serveur proxy sera transparente pour l'utilisateur.

4.4.4. Installation du Serveur proxy avec l'installateur

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

Installation du Serveur proxy sous Windows

1. Créez un compte du Serveur proxy à l'aide du Centre de gestion de la sécurité Dr.Web, comme cela est décrit dans la rubrique Création du compte du Serveur proxy.
2. Sur le poste sur lequel vous voulez effectuer l'installation, copiez le certificat du Serveur auquel le Serveur proxy se connectera (voir Connexion des clients au Serveur Dr.Web) et l'installateur du Serveur proxy fourni avec la distribution du Serveur.

3. Lancez l'installateur du Serveur proxy. La fenêtre de l'assistant **InstallShield Wizard** apparaît et vous informe sur le produit en cours d'installation. Cliquez sur le bouton **Suivant**.
4. Dans la fenêtre des paramètres du Serveur proxy dans l'onglet **Général**, spécifiez les paramètres principaux suivants :
   - Si cela est nécessaire, dans le champ **Chemin vers les données du logiciel** modifiez le chemin de placement des fichiers utilisés par le Serveur proxy : les journaux de fonctionnement, les fichiers de configuration, le cache. Le chemin `%PROGRAMDATA %/Doctor Web/drwcs` est utilisé par défaut. Pour sélectionnez un autre chemin, cliquez sur **Parcourir**.
   - Dans le champ **Adresse d'écoute**, 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 sera « écouté » par le Serveur proxy. Par défaut c'est le port `2193`.
   - Cochez la case **Activer la détection** pour activer le mode d'imitation du Serveur. Ce mode permet au clients de détecter le Serveur proxy en tant que Serveur Dr.Web lors de sa recherche par les requêtes broadcast.
   - Cochez la case **Activer le multicasting** pour que le Serveur proxy réponde aux requêtes broadcast adressées au Serveur.
     - Dans le champ **Groupe Multicast**, entrez l'adresse IP du groupe de multidiffusion dont le Serveur proxy fera partie. L'interface spécifiée sera "écoutée" par le Serveur proxy afin d'assurer l'interaction avec les clients lors de la recherche des Serveurs Dr.Web actifs. Si vous laissez le champ vide, le Serveur proxy ne sera inclus dans aucun groupe de multidiffusion. Par défaut, le Serveur appartient au groupe de multidiffusion `231.0.0.1`.
   - Dans la section **Paramètres de connexion avec les clients** :
     - Dans la liste déroulante **Chiffrement**, sélectionnez le mode de chiffrement du trafic pour les canaux entre le Serveur proxy et les clients servis : les Agents et les installateurs des Agents.
     - Dans la liste déroulante **Compression**, 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 **Niveau**, spécifiez le niveau de compression (de 1 à 9).
5. Dans l'onglet **Cache**, configurez les paramètres suivants de la mise en cache du Serveur proxy :

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

   - Dans le champ **Périodicité de suppression des anciennes révisions (min)**, spécifiez la périodicité de suppression des anciennes révisions du cache au cas où leur nombre

dépasserait le nombre maximum autorisé des révisions stockés. La valeur est spécifiée en minutes. Par défaut c'est 60 minutes.

- Dans le champ **Nombre de révisions stockées**, spécifiez le nombre maximal des révisions de chaque produit à stocker dans le cache après le nettoyage. Par défaut, les 3 dernières révisions sont sauvegardées, les révisions plus anciennes sont supprimées.

- Dans le champ **Période de déchargement des fichiers non utilisés (min)**, spécifiez l'intervalle de temps en minutes entre les déchargements des fichiers non utilisés de la mémoire vive. La valeur spécifiée par défaut est de 10 minutes.
- Dans la liste déroulante **Mode de l'analyse de l'intégrité**, sélectionnez le mode de vérification de l'intégrité des données mises en cache :
  - **Au démarrage** : au démarrage du Serveur proxy (cela peut prendre un certain temps).
  - **En cas d'inactivité** : lors de l'inactivité du Serveur proxy.

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

6. La fenêtre de configuration de la redirection des connexions va s'afficher :
   - Dans le champ **Adresse de redirection**, spécifiez l'adresse du Serveur Dr.Web vers lequel les connexions établies par le Serveur proxy seront redirigées. Vous devez indiquer en premier le Serveur auquel le Serveur proxy devra se connecter pour obtenir le configuration. Le certificat de ce Serveur a été copié sur le poste à l'étape 2.

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

   - Dans la liste déroulante **Chiffrement**, sélectionnez le mode de chiffrement du trafic pour les canaux de communication entre le Serveur proxy et le Serveur Dr.Web spécifié.
   - Dans la liste déroulante **Compression** sélectionnez le mode de compression du trafic pour les canaux de communication entre le Serveur proxy et le Serveur Dr.Web spécifié. Dans la liste déroulante **Niveau**, sélectionnez le niveau de compression (de 1 à 9).

Pour ajouter encore un Serveur dans la liste de redirection du trafic, cliquez sur le bouton  et spécifiez les paramètres conformément à la liste ci-dessus.

Pour supprimer un Serveur de la liste de redirection du trafic, cliquez sur  contre le Serveur que vous souhaitez supprimer.

Après la fin de l'installation le Serveur proxy se connectera au premier Serveur spécifié dans cette section pour obtenir les paramètres.

Au cas où la configuration du Serveur proxy serait spécifiée sur le Serveur, tous les paramètres spécifiés dans l'installateur seront réécrits pour la nouvelle configuration obtenue du Serveur.

Après avoir édité les paramètres de redirection, cliquez sur **Suivant**.

7. La fenêtre de configuration de la connexion au Serveur Dr.Web s'ouvrira pour la gestion à distance.

La connexion se fait au premier Serveur spécifié à l'étape 6 pour la redirection du trafic.

- Dans le champ **Certificat du Serveur**, spécifiez le fichier du certificat copié sur le poste à l'étape 2. Pour sélectionner le fichier, cliquez sur **Parcourir**.
- Dans les champs **Identificateur** et **Mot de passe**, spécifiez les identifiants du compte créé sur le Serveur à l'étape 1.

8. La fenêtre informant sur la disponibilité de l'installation du Serveur proxy va s'ouvrir.

   S'il faut modifier les paramètres supplémentaires de l'installation, notamment le répertoire d'installation du Serveur proxy, cliquez sur **Paramètres avancés**.

   Pour commencer l'installation du Serveur proxy, cliquez sur le bouton **Installer**.

9. Après la fin de l'installation, cliquez sur le bouton **Quitter**.

10. Après l'installation, le Serveur proxy se connectera au Serveur spécifié à l'étape 6 pour la réception du fichier de configuration valide. Si les paramètres n'ont pas été spécifiés, le fichier de configuration ne sera pas téléchargé. La configuration spécifiée par l'installateur sera utilisée jusqu'à ce que la configuration sur le Serveur connecté soit spécifié.

Installation du Serveur proxy sous les OS de la famille UNIX

1. Lancez l'installateur du Serveur proxy à l'aide de la commande suivante :

   `./<`*fichier_de_distribution*`>.tar.gz.run`

2. Pour continuer l'installation, veuillez accepter le contrat de licence.
3. Indiquez le chemin vers le certificat du Serveur. Vous pouvez également ajouter le certificat après l'installation du Serveur proxy (voir Connexion des clients au Serveur Dr.Web).
4. Si nécessaire, vous pouvez utiliser les fichiers de configuration de l'installation précédente du Serveur proxy :
   - Pour utiliser la copie de sauvegarde enregistrée par défaut dans le dossier `/var/tmp/drwcsd-proxy`, cliquez sur ENTRER.
   - Pour utiliser une copie de sauvegarde se trouvant dans un autre dossier, indiquez le chemin d'accès manuellement.
   - Vous pouvez également installer le Serveur proxy avec les paramètres par défaut sans utiliser la copie de sauvegarde de la configuration de l'installation précédente. Pour ce faire, cliquez sur 0.
5. Après l'installation du Serveur proxy, vous pouvez éditer les fichiers de configuration correspondants si cela est nécessaire (voir Connexion des clients au Serveur Dr.Web).

Démarrage et arrêt

Au cours de l'installation du logiciel sous l'OS **FreeBSD** le script `rc /usr/local/etc/rc.d/dwcp_proxy` est créé. Utilisez les commandes :

- `/usr/local/etc/rc.d/dwcp_proxy stop` : pour arrêter manuellement le Serveur proxy ;

- `/usr/local/etc/rc.d/dwcp_proxy start` : pour démarrer manuellement le Serveur proxy.

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

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

Pour supprimer le Serveur en version 10 ou supérieure, procédez comme suit :

OS du Serveur	Action
FreeBSD	Lancez le script : `/usr/local/etc/drweb.com/software/drweb-esuite.remove`
Linux	Lancez le script : `/etc/opt/drweb.com/software/drweb-esuite.remove`

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` (vous trouverez la liste de fichiers pour la copie de sauvegarde dans la rubrique Mise à jour du Serveur Dr.Web sous les OS de la famille UNIX®).

Pour annuler la copie de sauvegarde, il est nécessaire de spécifier la variable d'environnement `SKIP_BACKUP`. La variable peut prendre n'importe quelle valeur. Par exemple : `SKIP_BACKUP="x"`

Vous pouvez également ajouter la définition de la variable dans le fichier `common.conf`.

Suppression de la distribution supplémentaire du Serveur Dr.Web

Pour supprimer la distribution supplémentaire du Serveur en version 10 ou supérieure, procédez comme suit :

OS du Serveur	Action
FreeBSD	Lancez le script : `/usr/local/etc/drweb.com/software/drweb-esuite-extra.remove`
Linux	Lancez le script : `/etc/opt/drweb.com/software/drweb-esuite-extra.remove`

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, macOS – 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, macOS 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 à distance de l'Agent Dr.Web et du package antivirus

L'installation et la suppression du logiciel de l'Agent à distance 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. Dans le menu principal du Centre de gestion, sélectionnez l'élément **Réseau antivirus**.
2. Dans la fenêtre qui apparaît du 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.

En cas de suppression de l'Agent à distance (la suppression sur le poste est effectuée en tâche de fond), le redémarrage forcé du poste sera effectué dans un délai de cinq minutes. Il est impossible de modifier le délai et annuler le redémarrage. Les utilisateurs seront informés du redémarrage par une notification pop-up.

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

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 Dr.Web 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 personnel drweb_ess_<*OS*>_<*poste*>.exe**

  Pour désinstaller le logiciel de l'Agent et le package antivirus à l'aide du package d'installation, lancez le fichier d'installation `drweb_ess_<OS>_<poste>.exe` de la version du produit qui est installée sur votre ordinateur.

- **Installateur complet drweb-11.05.2-<*assemblage*>-esuite-agent-full-windows.exe**

  Pour désinstaller le logiciel de l'Agent et le package antivirus à l'aide de l'installateur complet, lancez le fichier d'installation `drweb-11.05.2-<assemblage>-esuite-agent-full-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_<OS>_<poste>.exe`, de l'installateur complet `drweb-11.05.2-<assemblage>-esuite-agent-full-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

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

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 **Propriétés** de **ESS** s'ouvre.
3. Passez à l'onglet **Stratégie de groupe**. Sélectionnez l'élément **Stratégies ESS** 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

Le Serveur proxy peut être supprimé par un des moyens suivants :

1. En mode local.

   La suppression locale est effectuée par l'administrateur sur l'ordinateur sur lequel le Serveur proxy est installé.
2. À distance.

   Le Serveur proxy est géré à distance depuis le Centre de gestion via LAN. La gestion à distance est disponible si le Serveur proxy est connecté au Serveur.

5.3.1. Suppression locale du Serveur proxy

Sous Windows

Lors de la suppression du Serveur proxy, le fichier de configuration `drwcsd-proxy.conf` (`drwcsd-proxy.xml` pour la version 10 ou antérieure) est supprimé. Si nécessaire, sauvegardez le fichier de configuration manuellement avant la suppression du 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 et supérieur).

Pour les OS de la famille UNIX

Lors de la suppression du Serveur proxy, la copie de sauvegarde des fichiers de configuration est automatiquement enregistrée dans le répertoire `/var/tmp/drwcsd-proxy`.

OS du Serveur proxy	Action
FreeBSD	Lancez le script : `/usr/local/etc/drweb.com/software/drweb-esuite-proxy.remove`
Linux	Lancez le script :

OS du Serveur proxy	Action
	`/etc/opt/drweb.com/software/drweb-proxy.remove`

5.3.2. Suppression à distance du Serveur proxy

La suppression du Serveur proxy à distance est disponible uniquement si le Serveur proxy est connecté au Serveur (voir Connexion des clients au Serveur Dr.Web).

> Quand vous supprimez le compte du Serveur proxy du Centre de gestion, le Serveur proxy est supprimé du poste.

Pour supprimer un Serveur proxy :

1. Dans le menu principal du Centre de gestion, sélectionnez l'élément **Réseau antivirus**.
2. Dans la fenêtre qui apparaît, cliquez sur le nom d'un ou de plusieurs Serveurs proxy à supprimer dans la liste hiérarchique.
3. Dans la barre d'outils, cliquez sur **Général** → **Supprimer les objets sélectionnés**.
4. La fenêtre de confirmation de la suppression va s'ouvrir. Cliquez sur **OK**.

Pour supprimer un Serveur proxy installé sur un poste lié :

1. Dans le menu principal du Centre de gestion, sélectionnez l'élément **Réseau antivirus**.
2. Ouvrez la section de propriétés du poste sur lequel le Serveur proxy est installé d'une des façons suivantes :
   a) Cliquez sur le nom du poste dans la liste hiérarchique du réseau antivirus. La section contenant les propriétés du poste va s'afficher automatiquement dans la partie droite du Centre de gestion.
   b) Sélectionnez l'élément **Propriétés** du menu de gestion. La fenêtre contenant les propriétés du poste va s'ouvrir.
3. De la fenêtre de propriétés du poste, allez à l'onglet **Serveur proxy**.
4. Cliquez sur **Supprimer le Serveur proxy**.
5. Cliquez sur **Enregistrer**. Le Serveur proxy sera désinstallé du poste. Le compte du Serveur proxy sera supprimé du Serveur.

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 en version 11 et les Serveurs en 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 11 (voir le p. Mise à jour des Agents Dr.Web), alors les Serveurs en versions 6 et les Serveurs en version 11.0.2 doivent obtenir des mises à jour séparément.
- Pour le réseau antivirus dans lequel le Serveur proxy Dr.Web est utilisé, il faut également mettre à niveau le Serveur proxy vers la version 11.0.2 en cas de mise à niveau des composants vers la version 11.0.2. Sinon, la connexion des Agents fournis avec la version 11.0.2 au Serveur en version 11.0.2 sera impossible. Il est recommandé d'effectuer la mise à niveau dans l'ordre suivant : Serveur Dr.Web → Serveur proxy Dr.Web → Agent Dr.Web.
- Lors de la migration du Serveur en version 6 vers la version 11, les paramètres de fonctionnement du Serveur via le Serveur proxy ne sont pas sauvegardés. Après l'installation de la version 11, il est nécessaire de spécifier manuellement les paramètres de connexion via le serveur proxy (voir le **Manuel Administrateur**, p. Proxy).
- Lors de la suppression du Serveur, tous les paramètres du référentiel ne sont pas transférés dans la nouvelle version (ils sont réinitialisés aux valeurs par défaut), pourtant une copie de sauvegarde est créée. Si nécessaire, spécifiez manuellement les paramètres du référentiel après la mise à niveau du Serveur.

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

Lors de la mise à niveau du Serveur Dr.Web tournant sous Windows depuis la version 10 ou antérieure, les paramètres des sections suivantes du Centre de gestion ne seront pas transférés dans la version 11 :

- **Configuration du Serveur Dr.Web** → **Réseau** → **Téléchargement** (fichier `download.conf`),
- **Accès distant au Serveur Dr.Web** (fichier `frontdoor.conf`),
- **Configuration du serveur web** (fichier `webmin.conf`).

Les paramètres de ces sections seront réinitialisés par défaut. Si vous voulez utiliser les paramètres de la version précédente, spécifiez-les manuellement après la mise à niveau du Serveur dans les sections correspondantes du Centre de gestion à partir des données des copies de sauvegarde de fichiers de configuration.

La mise à niveau du Serveur depuis la version 6 ou 10 vers la version 11 et la mise à jour au sein de la version 11 est effectuée automatiquement via l'installateur.

Avant de mettre à niveau le Serveur, merci de lire la rubrique Mise à jour de l'Agent Dr.Web.

La mise à jour du Serveur au sein de la version 11 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 11 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 mise à niveau du Serveur vers la version 11 via l'installateur, les fichiers de configuration sont enregistrés dans le répertoire de sauvegarde par défaut :

- En cas de la mise à niveau depuis la version 6 : dans le répertoire <*disque_d'installation*>: `\DrWeb Backup`.
- En cas de la mise à niveau depuis la version 10 ou la mise à jour au sein de la version 11 : dans le répertoire spécifié lors de la mise à jour dans le paramètre **Sauvegarde des données critiques du Serveur Dr.Web** (par défaut, c'est <*disque_d'installation*>: `\DrWeb Backup`).

En cas de mise à niveau du Serveur depuis la version 6, les fichiers de configuration suivants sont sauvegardés :

Fichier	Description
`agent.key` (le nom peut varier)	clé de licence de l'Agent
`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

Fichier	Description
`auth-radius.xml`	fichier de configuration pour l'authentification externe des administrateurs via RADIUS
`drwcsd.conf` (le nom peur varier)	fichier de configuration du Serveur
`dbinternal.dbs`	BD embarquée
`drwcsd.pri`	clé privée de chiffrement
`drwcsd.pub`	clé publique de chiffrement
`enterprise.key` (le nom peut varier)	clé de licence du Serveur
`webmin.conf`	fichier de configuration du Centre de gestion

En cas de mise à niveau du Serveur depuis la version 10, les fichiers de configuration suivants sont sauvegardés :

Fichier	Description
`agent.key` (le nom peut varier)	clé de licence de l'Agent
`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
`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 11.0.2
`drwcsd.conf` (le nom peur varier)	fichier de configuration du Serveur
`drwcsd.conf.distr`	modèle du fichier de configuration du Serveur avec les paramètres par défaut
`drwcsd.pri`	clé privée de chiffrement
`drwcsd.pub`	clé publique de chiffrement

Fichier	Description
download.conf	paramètres réseau pour la génération de packages d'installation de l'Agent
frontdoor.conf	fichier de configuration pour l'utilitaire du diagnostic distant du Serveur
webmin.conf	fichier de configuration du Centre de gestion
openssl.cnf	certificat du Serveur pour HTTPS

En cas de la mise à jour du Serveur au sein de la version 11, les fichiers de configuration suivants sont sauvegardés :

Fichier	Description
agent.key (le nom peut varier)	clé de licence de l'Agent
auth-ads.conf	fichier de configuration pour l'authentification externe des administrateurs via Active Directory
auth-radius.conf	fichier de configuration pour l'authentification externe des administrateurs via RADIUS
auth-ldap.conf	fichier de configuration pour l'authentification externe des administrateurs via LDAP
auth-ldap-rfc4515.conf	fichier de configuration pour l'authentification externe des administrateurs via LDAP selon le schéma simplifié
auth-ldap-rfc4515-check-group.conf	modèle du fichier de configuration pour l'authentification externe des administrateurs via LDAP selon le schéma simplifié avec la vérification d'appartenance au groupe Active Directory
auth-ldap-rfc4515-check-group-novar.conf	modèle du fichier de configuration pour l'authentification externe des administrateurs via LDAP selon le schéma simplifié avec la vérification d'appartenance au groupe Active Directory avec l'utilisation des variables
auth-ldap-rfc4515-simple-login.conf	modèle du fichier de configuration pour l'authentification externe des administrateurs via LDAP selon le schéma simplifié
auth-pam.conf	fichier de configuration pour l'authentification externe des administrateurs via PAM
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 11.0.2
drwcsd-certificate.pem	certificat de Serveur

Fichier	Description
`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`	modèle du fichier de configuration du Serveur avec les paramètres par défaut
`drwcsd.pri`	clé privée de chiffrement
`dbexport.gz`	exportation de la base de données
`drwcsd.pub`	clé publique de chiffrement
`frontdoor.conf`	fichier de configuration pour l'utilitaire du diagnostic distant du Serveur
`openssl.cnf`	certificat du Serveur pour HTTPS
`webmin.conf`	fichier de configuration du Centre de gestion
`yalocator.apikey`	Clé API pour l'extension Yandex.Locator

Si vous prévoyez d'utiliser les fichiers de configuration du Serveur de la version 6, notez que :

1. La clé de licence du Serveur n'est plus supportée (voir le p. Chapitre 2. Licence).
2. La base de données embarquée est mise à niveau 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 du Serveur de la version 6.

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 `SQLite`.

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 niveau le Serveur Dr.Web, lancez le fichier de distribution. Les étapes suivantes dépendent de la version mise à niveau.

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.

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

Si vous projetez d'utiliser la BD Oracle via la connexion ODBC comme base de données externe, refusez l'installation du client intégré pour le SGBD Oracle dans les paramètres de l'installateur (dans la section **Support des bases de données – Pilote de la base de données Oracle**) lors de l'installation (mise à jour) du Serveur.

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

En cas de la mise à niveau depuis la version 6

1. 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**.

2. 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**.
3. Aux étapes suivantes, la configuration du Serveur 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. L'installateur détermine automatiquement le répertoire d'installation du Serveur et localise les fichiers de configuration et la BD intégrée de la version précédente. Si cela est nécessaire, vous pouvez modifier les chemins vers les fichiers qui sont trouvé automatiquement par l'installateur.
4. Afin de procéder à la suppression du Serveur de la version antérieure et pour lancer l'installation du Serveur en version 11.0.2, cliquez sur **Installer**.

   Lors de la suppression du Serveur, les fichiers de configuration sont sauvegardés automatiquement dans le répertoire <*disque_d'installation*>:\DrWeb Backup.

En cas de la mise à niveau depuis la version 10.0

1. 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**.
2. 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**.
3. Aux étapes suivantes, la configuration du Serveur 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. L'installateur détermine automatiquement le répertoire d'installation du Serveur et localise les fichiers de configuration et la BD intégrée de la version précédente. Si cela est nécessaire, vous pouvez modifier les chemins vers les fichiers qui sont trouvé automatiquement par l'installateur.
4. Afin de procéder à la suppression du Serveur de la version antérieure et pour lancer l'installation du Serveur en version 11.0.2, cliquez sur **Installer**.
5. Lors de la mise à niveau, une fenêtre de configuration va s'ouvrir vous proposant de créer une copie de sauvegarde des données critiques avant la suppression du Serveur de la version précédente. Il est recommandé de cocher la case **Sauvegarde des données critiques du Serveur Dr.Web**. S'il est nécessaire, vous pouvez modifier le répertoire de copie de sauvegarde spécifié par défaut <*disque_d'installation*>:\DrWeb Backup.

En cas de la mise à niveau depuis les versions 10.0.1, 10.1 ou la mise à jour au sein de la version 11

1. 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**.

2. Une fenêtre va s'ouvrir vous proposant de créer une copie de sauvegarde des données critiques avant la suppression du Serveur de la version précédente. Il est recommandé de cocher la case **Sauvegarde des données critiques du Serveur Dr.Web**. S'il est nécessaire, vous pouvez modifier le répertoire de copie de sauvegarde spécifié par défaut (<*disque_d'installation*>`:\DrWeb Backup`). Pour commencer la suppression de la version précédente du Serveur, cliquez sur **Supprimer**.
3. Après la fin de la suppression de la version précédente du Serveur, l'installation de la nouvelle version commence. 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, la configuration du Serveur 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. L'installateur détermine automatiquement le répertoire d'installation du Serveur et localise les fichiers de configuration et la BD intégrée de la version précédente. Si cela est nécessaire, vous pouvez modifier les chemins vers les fichiers qui sont trouvé automatiquement par l'installateur.
5. Pour commencer l'installation du Serveur de la version 11.0.2, cliquez sur le bouton **Installer**.

Après la fin de la mise à jour des Serveurs du réseau antivirus, il est nécessaire :

1. Spécifier de nouveau les paramètres de chiffrement et de compression pour les Serveurs liés (voir le **Manuel Administrateur**, la rubrique Configuration des liaisons entre Serveurs Dr.Web).
2. Vider le cache du navigateur web utilisé pour se connecter au Centre de gestion.

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

Lors de la mise à niveau du Serveur Dr.Web tournant sous un OS de la famille UNIX depuis la version 10 ou antérieure, les paramètres de la section **Configuration du serveur web** du Centre de gestion (le fichier `webmin.conf`) ne seront pas transférés dans la version 11.0.2.

Les paramètres de cette section seront réinitialisés aux valeurs par défaut. Si vous voulez utiliser les paramètres de la version précédente, spécifiez-les manuellement après la mise à niveau du Serveur dans la section correspondante du Centre de gestion à partir des données de la copie de sauvegarde du fichier de configuration.

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

La mise à niveau du Serveur vers la version 11 dépend de la version initiale :

- La mise à niveau de la version 6.0.4 vers la version 11 ne se fait que manuellement.
- La mise à niveau automatique de la version 10 vers la version 11 par-dessus la version installée n'est pas possible sous tous les OS de la famille UNIX. Ainsi, sous un OS de la famille

UNIX ne permettant pas la mise à niveau automatique par-dessus le package installé, il faut effectuer la mise à niveau manuelle.

- Si vous voulez, vous pouvez effectuer la mise à jour manuellement. La mise à jour du Serveur au sein de la version 11 pour les mêmes types de packages s'effectue automatiquement pour tous les OS de la famille UNIX.

Avant de mettre à niveau le Serveur, merci de lire la rubrique Mise à jour de l'Agent Dr.Web.

La mise à jour du Serveur au sein de la version 11 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 11 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 et la mise à niveau vers la version 11, les fichiers de configuration sont enregistrés dans le répertoire de sauvegarde par défaut : `/var/tmp/drwcs/`

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

Fichier	Description
`agent.key` (le nom peut varier)	clé de licence de l'Agent
`certificate.pem`	certificat SSL
`common.conf`	fichier de configuration (pour les OS de la famille UNIX)
`dbinternal.dbs`	BD embarquée
`drwcsd.conf` (le nom peur varier)	fichier de configuration du Serveur
`drwcsd.pri`	clé privée de chiffrement
`drwcsd.pub`	clé publique de chiffrement
`enterprise.key` (le nom peut varier)	clé de licence du Serveur

Fichier	Description
private-key.pem	clé privée RSA
webmin.conf	fichier de configuration du Centre de gestion

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

Fichier	Description
agent.key (le nom peut varier)	clé de licence de l'Agent
auth-ldap.xml	fichier de configuration pour l'authentification externe des administrateurs via LDAP
auth-pam.xml	fichier de configuration pour l'authentification externe des administrateurs via PAM
auth-radius.xml	fichier de configuration pour l'authentification externe des administrateurs via RADIUS
certificate.pem	certificat SSL
common.conf	fichier de configuration (pour les OS de la famille UNIX)
dbexport.gz	exportation de la base de données (créé lors de la suppression du Serveur avec la commande drwcs.sh xmlexportdb)
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 privée de chiffrement
drwcsd.pub	clé publique de chiffrement
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 11.0.2
frontdoor.conf	fichier de configuration pour l'utilitaire du diagnostic distant du Serveur
local.conf	paramètres du journal du Serveur
private-key.pem	clé privée RSA
webmin.conf	fichier de configuration du Centre de gestion

Fichier	Description
`*.dbs` `*.sqlite`	BD embarquée

En cas de suppression du Serveur en version 11, les fichiers de configuration suivants sont sauvegardés :

Fichier	Description
`agent.key` (le nom peut varier)	clé de licence de l'Agent
`auth-ldap.conf`	fichier de configuration pour l'authentification externe des administrateurs via LDAP
`auth-ldap-rfc4515.conf`	fichier de configuration pour l'authentification externe des administrateurs via LDAP selon le schéma simplifié
`auth-pam.conf`	fichier de configuration pour l'authentification externe des administrateurs via PAM
`auth-radius.conf`	fichier de configuration pour l'authentification externe des administrateurs via RADIUS
`certificate.pem`	certificat SSL
`common.conf`	fichier de configuration (pour les OS de la famille UNIX)
`dbexport.gz`	exportation de la base de données (créé lors de la suppression du Serveur avec la commande `drwcs.sh xmlexportdb`)
`download.conf`	paramètres réseau pour la génération de packages d'installation de l'Agent
`drwcsd-certificate.pem`	certificat de Serveur
`drwcsd.conf` (le nom peur varier)	fichier de configuration du Serveur
`drwcsd.pri`	clé privée de chiffrement
`drwcsd.pub`	clé publique de chiffrement
`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 11.0.2
`frontdoor.conf`	fichier de configuration pour l'utilitaire du diagnostic distant du Serveur

Fichier	Description
local.conf	paramètres du journal du Serveur
private-key.pem	clé privée RSA
webmin.conf	fichier de configuration du Centre de gestion
yalocator.apikey	Clé API pour l'extension Yandex.Locator

En cas de la mise à niveau automatique, les fichiers suivants sont stockés dans le répertoire de copie de sauvegarde :

Pour le Serveur version 10 :

Fichier	Description
auth-ldap.xml	fichier de configuration pour l'authentification externe des administrateurs via LDAP
auth-pam.xml	fichier de configuration pour l'authentification externe des administrateurs via PAM
auth-radius.xml	fichier de configuration pour l'authentification externe des administrateurs via RADIUS
db.backup.gz	exportation de la base de données (créé lors de la mise à niveau du Serveur avec la commande drwcs.sh exportdb)

Pour le Serveur en version 11 :

Fichier	Description
auth-ldap.conf	fichier de configuration pour l'authentification externe des administrateurs via LDAP
auth-ldap-rfc4515.conf	fichier de configuration pour l'authentification externe des administrateurs via LDAP selon le schéma simplifié
auth-pam.conf	fichier de configuration pour l'authentification externe des administrateurs via PAM
auth-radius.conf	fichier de configuration pour l'authentification externe des administrateurs via RADIUS
db.backup.gz	exportation de la base de données (créé lors de la mise à niveau du Serveur avec la commande drwcs.sh exportdb)

Si vous prévoyez d'utiliser les fichiers de configuration du Serveur de la version 6, notez que :

1. La clé de licence du Serveur n'est plus supportée (voir le p. Chapitre 2. Licence).
2. La base de données embarquée est mise à niveau 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 du Serveur de la version 6.

Sauvegarde de la base de données

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 :
   - Sous FreeBSD :
     ```
     # /usr/local/etc/rc.d/drwcsd exportdb /var/tmp/esbase.es
     ```
   - Sous Linux :
     ```
     # /etc/init.d/drwcsd exportdb /var/tmp/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 depuis la version 10 vers la version 11 (sauf les Serveurs installés sous **Linux** depuis les packages, `*.rpm.run` et `*.deb.run`), au lieu de supprimer la version précédente et d'installer une nouvelle version du Serveur, vous pouvez utiliser la mise à niveau automatique du Serveur. Pour cela, lancez le package correspondant du Serveur.

La mise à jour du Serveur au sein de la version 11 pour les mêmes types de packages s'effectue automatiquement pour tous les OS de la famille UNIX.

Dans ce cas, les fichiers de configuration seront convertis automatiquement et placés dans les répertoires appropriés. Certains fichiers de configuration sont également sauvegardés dans le répertoire de copie de sauvegarde.

Mise à jour manuelle

Si la mise à niveau du Serveur en version 6.0.4 ou supérieure par-dessus le package installé n'est pas possible, il faut supprimer les versions précédentes du logiciel de Serveur en créant une copie de sauvegarde et installer ensuite le logiciel en version 11 d'après la copie sauvegardée.

Pour mettre à niveau le Serveur Dr.Web, faites la procédure suivante :

1. Arrêter le Serveur.
2. Si vous souhaitez utiliser plus tard des fichiers (à part les fichiers qui seront sauvegardés automatiquement lors de la suppression du Serveur à l'étape **3**), créez des copies de sauvegarde de ces fichiers manuellement. Par exemple, les modèles de rapports, etc.
3. 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.
4. Installez le Serveur Dr.Web en version 11.0.2 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 **3**. Tous les fichiers de configuration ainsi que la base de données embarquée (en cas d'utilisation de la base de données embarquée) seront automatiquement convertis pour la version 11.0.2 du Serveur. Sans conversion automatique, la base de données (en cas d'utilisation de la base de données embarquée) et certains fichiers de configuration du Serveur de versions précédentes 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 4) désignez l'utilisateur sélectionné lors de l'installation de la nouvelle version du Serveur (**drwcs** par défaut) comme le propriétaire des fichiers.

5. Lancez le Serveur.
6. Configurez la mise à niveau du référentiel et effectuez-la.

   

   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 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 niveau des Agents Dr.Web sur les postes tournant sous l'OS Android,
3. Mise à niveau des Agents Dr.Web sur les postes tournant sous l'OS Linux® et macOS®.

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

Mise à niveau des Agents fournis avec Dr.Web Enterprise Security Suite 10

La mise à niveau des Agents fournis avec la version Enterprise Security Suite 10 se fait manuellement.

Après le redémarrage automatique, une notification de la nécessité de redémarrage s'affiche sur le poste ; la nécessité de redémarrage est marquée dans le statut du poste après la mise à niveau. Pour terminer la mise à niveau, veuillez redémarrer le poste de manière locale ou distante via le Centre de gestion.

Au cas où le poste se connecterait au Serveur via le Serveur proxy Dr.Web en version 10 ou une version antérieure, avant la mise à niveau de l'Agent il faut mettre à niveau le Serveur proxy vers la version 11 ou supprimer le Serveur proxy.

Mise à niveau automatique des Agents fournis avec Dr.Web Enterprise Security Suite 6

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 11.0.2 (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 se fait 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 section **Statut** du Centre de gestion, une notification de 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 publique de chiffrement 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 se fait 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 section **Statut** du Centre de gestion, une notification de la nécessité de redémarrage s'affichera pour le poste mis à jour. Il est nécessaire de redémarrer le poste.

Mise à jour manuelle des Agents fournis avec Dr.Web Enterprise Security Suite 6

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 11.0.2, alors aucune action de mise à jour ne sera pas exécutée.

Les Agents installés sur les 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 laisser les Serveurs des versions précédentes, auxquels ces Agents sont connectés, dans le réseau antivirus. Notez que les Serveurs des versions 6 et les Serveurs de la version 11.0.2 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.

6.3.2. Mise à niveau des Agents Dr.Web sur les postes tournant sous l'OS Android

La mise à niveau des Agents Dr.Web pour Android pour le travail avec Dr.Web Enterprise Security Suite en version 11.0.2 doit être faite manuellement sur les appareils mobiles.

Dr.Web Enterprise Security Suite en version 11.0.2 supporte le fonctionnement uniquement avec les Agents Dr.Web pour Android en version 12.2 ou une version supérieure.

En cas de mise à niveau standard des Agents Dr.Web pour Android, la protection d'appareils mobiles sera désactivée à cause d'une erreur de version incompatible des bases virales.

Pour la mise à niveau locale des Agents Dr.Web pour Android vous pouvez utiliser l'un des moyens suivants :

1. Si vous avez la possibilité de télécharger séparément le package d'installation de le version autonome de l'Agent.

   Avant la mise à niveau du Serveur Dr.Web, mettez à niveau manuellement les Agents Dr.Web pour Android vers la version 12.2 ou supérieure sur les appareils mobiles. Vous pouvez télécharger une nouvelle version sur le site de Doctor Web à l'adresse : https://download.drweb.com/android/. Le nouvel Agent se connectera au Serveur de la version précédente, après quoi, vous pouvez mettre à niveau le Serveur vers la version 11.0.2 conformément à la procédure commune.
2. Si vous n'avez pas la possibilité de télécharger séparément le package d'installation de le version autonome de l'Agent.

Après la mise à niveau du Serveur Dr.Web, les Agents Dr.Web pour Android se connecteront automatiquement au Serveur mis à niveau. Après une tentative de mise à jour, la protection sur les appareils mobiles sera désactivée à cause d'une erreur d'incompatibilité des version des bases virales. Mettez à niveau les Agents manuellement sur les appareils mobiles. Vous pouvez télécharger le package d'installation d'une nouvelle version dans le Centre de gestion, dans les propriété du poste ou sur la page d'installation.

3. Si vous n'avez pas la possibilité de télécharger séparément le package d'installation de le version autonome de l'Agent et que l'erreur sur l'appareil mobile est indesirable.

   Avant la mise à niveau du Serveur, déconnectez du Serveur les Agents Dr.Web pour Android. Dans ce cas, les appareils mobiles ne pourront pas se connecter au nouveau Serveur pour télécharger les mise à jour incompatibles. Mettez à niveau le Serveur vers la version 11.0.2 selon la procédure commune. Téléchargez le package d'installation de la nouvelle version de l'Agent dans le Centre de gestion dans les propriétés du poste ou sur la page d'installation. Mettez à niveau les Agents manuellement sur les appareils mobiles. Connectez les Agents mis à niveau au nouveau Serveur.

6.3.3. Mise à niveau des Agents Dr.Web sur les postes tournant sous l'OS Linux® et macOS®

Les Agents installés sur les postes tournant sous les OS de la famille Linux et macOS seront connectés au Serveur en version 11.0.2, si les conditions suivantes sont satisfaites :

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 11.0.2 (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.

Après la connexion du poste au Serveur mis à jour :

1. Sur les postes, seules les bases virales seront mises à jour. La mise à jour automatique du logiciel antivirus ne se fait pas.
2. Si la dernière version du logiciel est installée sur les postes, aucune action supplémentaire n'est requise.
3. Si le logiciel est obsolète, téléchargez le package d'installation de la nouvelle version de l'Agent dans le Centre de gestion, dans les paramètres du poste ou sur la page d'installation. Mettez à niveau manuellement le logiciel des postes comme cela est décrit dans les **Manuels utilisateur** correspondants.

6.4. Mise à jour du Serveur proxy Dr.Web

6.4.1. Mise à jour du Serveur proxy Dr.Web lors de son fonctionnement

La mise à jour du Serveur proxy peut être effectuée automatiquement au cours de son fonctionnement.

La planification de la mise à jour dépend des paramètres de la mise en cache proactive du Serveur proxy :

1. Si le Serveur proxy n'est pas inclus dans la liste de la mise en cache proactive (même si la mise en cache n'est pas utilisée), les mises à jour du Serveur proxy seront téléchargées et installées automatiquement conformément à la planification de la mise à jour automatique.
2. Si le Serveur proxy est inclus dans la liste de la mise en cache proactive, les mises à niveau du Serveur proxy seront automatiquement téléchargés conformément à la planification de la mise en cache proactive. Si une nouvelle révision du Serveur proxy est reçue, la mise à niveau vers cette révision sera effectuée conformément à la planification automatique.

Vous pouvez configurer la mise à jour automatique par l'un des moyens suivants :

- Via les paramètres du Serveur proxy, dans le Centre de gestion du Serveur gérant, dans la section **Mises à jour**. Pour en savoir plus, consultez le **Manuel Administrateur**, la rubrique Configuration distante du Serveur proxy.
- Via le fichier de configuration du Serveur proxy `drwcsd-proxy.conf`. Pour en savoir plus, consultez les **Annexes**, p. Annexe G4.

6.4.2. Mise à jour du Serveur proxy Dr.Web via l'installateur

Fichiers de configuration du Serveur proxy

Fichier de configuration du Serveur proxy en version 10 ou antérieure :

Fichier	Description
`drwcsd-proxy.xml`	fichier de configuration du Serveur proxy (voir les **Annexes**, p. Annexe G4)

Fichiers de configuration du Serveur proxy en version 11 et supérieure :

Fichier	Description
`drwcsd-proxy.conf`	fichier de configuration du Serveur proxy (voir les **Annexes**, p. Annexe G4)
`drwcsd-proxy.auth`	données d'identification (ID et mot de passe) pour l'accès au Serveur Dr.Web
`drwcsd-proxy-trusted.list`	liste des certificats de confiance des Serveurs Dr.Web
`drwcsd-proxy-signed.list`	liste des certificats signés du Serveur proxy
`drwcsd-proxy.pri`	clé privée de chiffrement du Serveur proxy

Mise à niveau du Serveur proxy sous Windows

La mise à niveau se fait automatiquement à l'aide de l'installateur.

Pour mettre à niveau le Serveur proxy depuis la version 10 ou antérieure :

1. Lancez le fichier de distribution du Serveur proxy.
2. Une fenêtre va s'ouvrir vous informant sur la présence du logiciel installé du Serveur de la version précédente et vous proposant la mise à niveau vers la nouvelle version. Pour commencer la suppression de la version précédente et l'installation de la nouvelle version, cliquez sur **Upgrade**.
3. Une fenêtre d'informations sur le produit s'ouvre. Cliquez sur le bouton **Next**.
4. Aux étapes suivantes, la configuration du Serveur proxy est effectuée de la même manière que le processus d'Installation du Serveur proxy Dr.Web à la base du fichier de configuration de la version précédente. L'installateur détermine automatiquement le répertoire d'installation du Serveur proxy et localise le fichier de configuration de la version

précédente. Si cela est nécessaire, vous pouvez modifier les paramètres du fichier qui sont trouvés automatiquement par l'installateur.

5. Pour commencer l'installation du Serveur proxy de la version 11.0.2, cliquez sur le bouton **Install**.

Pour mettre à niveau le Serveur proxy depuis la version 11 ou supérieure:

1. Lancez le fichier de distribution du Serveur proxy.
2. Une fenêtre va s'ouvrir vous informant sur la présence du logiciel installé du Serveur de la version précédente et vous proposant la mise à niveau vers la nouvelle version. Pour commencer la configuration de la procédure de la mise à niveau, cliquez sur **Upgrade**.
3. Une fenêtre s'affiche vous informant de la suppression du Serveur proxy de la version précédente. Pour commencer la suppression, cliquez sur **Uninstall**.
4. Après la fin de la suppression de la version précédente du Serveur proxy, l'installation d'une nouvelle version commence. Une fenêtre d'informations sur le produit s'ouvre. Cliquez sur **Next**.
5. Aux étapes suivantes, la configuration du Serveur proxy est effectuée de la même manière que le processus d'Installation du Serveur proxy Dr.Web à la base des fichiers de configuration de la version précédente. L'installateur détermine automatiquement le répertoire d'installation du Serveur proxy et localise les fichiers de configuration de la version précédente. Si cela est nécessaire, vous pouvez modifier les paramètres de fichiers qui sont trouvés automatiquement par l'installateur.
6. Pour commencer l'installation du Serveur proxy de la version 11.0.2, cliquez sur le bouton **Install**.

Mise à niveau du Serveur proxy sous les OS de la famille UNIX

Pour mettre à niveau le Serveur proxy depuis la version 11.0 ou antérieure :

Lors de la mise à niveau du Serveur proxy, les fichiers de configuration sont supprimés. Si nécessaire, sauvegardez les fichiers de configuration manuellement avant la mise à niveau.

1. Pour lancer la mise à niveau, lancez le fichier de distribution du Serveur proxy : `./<fichier_de_distribution>.tar.gz.run`
2. Après la mise à niveau, transférez manuellement les paramètres de fichiers de configuration sauvegardés avant la mise à niveau vers les nouveaux fichiers de configuration, si cela est nécessaire.

Pour mettre à niveau le Serveur proxy de la version 11.0.1 :

1. Pour lancer la mise à niveau, lancez le fichier de distribution du Serveur proxy : `./<fichier_de_distribution>.tar.gz.run`

2. Lors de la suppression de la version précédente, les fichiers de configuration du Serveur proxy seront sauvegardés automatiquement.
3. Si nécessaire, vous pouvez utiliser les fichiers de configuration de l'installation précédente du Serveur proxy, enregistrés lors de la sauvegarde :
   - Pour utiliser la copie de sauvegarde enregistrée par défaut dans le dossier `/var/tmp/drwcsd-proxy`, cliquez sur ENTRER.
   - Pour utiliser une copie de sauvegarde se trouvant dans un autre dossier, indiquez le chemin d'accès manuellement.
   - Vous pouvez également installer le Serveur proxy avec les paramètres par défaut sans utiliser la copie de sauvegarde de la configuration de l'installation précédente. Pour ce faire, cliquez sur 0.

Référence

A

Active Directory
- installation de l'Agent 81
- suppression de l'Agent 101

Agent
- installation 57, 68
- installation, à distance 72, 77, 81
- installation, Active Directory 81
- installation, en mode local 61
- mise à jour 117
- suppression, Active Directory 101
- suppression, sous OS Windows 99

C

chiffrement
- trafic 36

clés
- démo 28

clés de démo 28

composition du kit de distribution 24

compression du trafic 36

comptes
- poste, création 63

D

distribution 24

distribution principale du Serveur Dr.Web
- composition 24
- installation, pour les OS UNIX 55
- installation, sous OS Windows 48
- suppression, sous OS UNIX 97
- suppression, sous OS Windows 97

distribution supplémentaire du Serveur Dr.Web
- composition 24
- installation 57
- suppression, sous OS UNIX 98
- suppression, sous OS Windows 97

E

extension pour le Centre de gestion de la sécurité Dr.Web
- mise à jour, sous OS Windows 104
- suppression, sous OS Windows 97

I

icônes
- scanner réseau 78

installateur
- composition 59
- installation 68
- suppression, sous OS Windows 100
- types 59

installateur de groupe
- installation 67

installation
- NAP Validator 86
- package antivirus 57
- serveur proxy 86

installation de l'Agent 57
- à distance 72, 77, 81
- Active Directory 81
- en mode local 61
- installateur 68
- installateur de groupe 67
- package d'installation 63

installation du Serveur Dr.Web
- distribution principale, pour OS Windows 48
- distribution principale, sous OS UNIX 55
- distribution supplémentaire 57

M

mise à jour
- Agent 117
- extension pour le Centre de gestion de la sécurité Dr.Web 104
- Serveur, pour les OS UNIX 111
- Serveur, sous OS Windows 104

N

NAP Validator
- installation 86

P

package antivirus
- installation 57, 81
- suppression 99

package d'installation
- composition 59
- installation 63
- suppression, sous OS Windows 100

page d'installation 59

poste
- création d'un compte 63

Référence

pré-requis système 19

R

réseau antivirus
- planification 29

S

scanner réseau 77

Serveur Dr.Web
- installation, pour les OS UNIX 55
- installation, sous OS Windows 48
- mise à jour, sous OS UNIX 111
- mise à jour, sous OS Windows 104
- suppression, sous OS UNIX 97
- suppression, sous OS Windows 97

serveur proxy
- installation 86
- suppression 102

suppression
- composants 99
- extension pour le Centre de gestion de la sécurité Dr.Web, sous OS Windows 97
- package antivirus 99
- serveur proxy 102

suppression de l'Agent
- Active Directory 101
- installation, sous OS Windows 100
- package d'installation, sous Windows 100
- sous Windows 99

suppression du Serveur Dr.Web
- distribution principale, pour OS Windows 97
- distribution principale, sous OS UNIX 97
- distribution supplémentaire, sous OS UNIX 98
- distribution supplémentaire, sous OS Windows 97

T

trafic
- chiffrement 36
- compression 36