



Dr.WEB

Enterprise Security Suite

Manuel Administrateur



© **Doctor Web, 2024. Tous droits réservés**

Le présent document est un document d'information et de référence concernant le logiciel de la famille Dr.Web y spécifié. Ce document ne justifie pas les conclusions exhaustives sur la présence ou l'absence de tout paramètre fonctionnel et/ou technique dans le logiciel de la famille Dr.Web et ne peut pas être utilisé pour déterminer la conformité du logiciel de la famille Dr.Web aux exigences, tâches techniques et/ou paramètres quelconques ainsi qu'aux autres documents de tierces personnes.

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

Marques déposées

Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-Desk, KATANA et le logo Dr.WEB sont des marques déposées et des marques commerciales de Doctor Web en Russie et/ou dans d'autres pays. D'autres marques déposées, marques commerciales et noms de société utilisés dans ce document sont la propriété de leurs titulaires respectifs.

Limitation de responsabilité

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

Dr.Web Enterprise Security Suite
Version 13.0
Manuel Administrateur
07/03/2024

Doctor Web, Siège social en Russie

Adresse : 2-12A, 3e rue Yamskogo polya, 125124 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 : Introduction	9
1.1. Destination du document	9
1.2. Légende et abréviations	10
Chapitre 2 : Dr.Web Enterprise Security Suite	12
2.1. A propos du produit	12
2.2. Kit de distribution	22
Chapitre 3 : Octroi de licence	25
3.1. Politique de l'octroi de licence	26
3.2. Distributions des licences par les liaisons entre les serveurs	27
3.3. Mise à jour automatique de licences	30
Chapitre 4 : Mise en route	34
4.1. Création d'un réseau antivirus	34
4.2. Configuration des connexions réseau	38
4.2.1. Connexions directes	39
4.2.2. Service de détection du Serveur Dr.Web	40
4.2.3. Utiliser le protocole SRV	41
4.3. Assurance d'une connexion sécurisée	42
4.3.1. Chiffrement et compression du trafic	42
4.3.2. Instruments assurant une connexion sécurisée	48
4.3.3. Connexion des clients au Serveur Dr.Web	50
4.4. Intégration de Dr.Web Enterprise Security Suite avec Active Directory	52
Chapitre 5 : Composants du réseau antivirus et leur interface	55
5.1. Serveur Dr.Web	55
5.1.1. Gestion du Serveur Dr.Web sous Windows	57
5.1.2. Gestion du Serveur Dr.Web sous les OS de la famille UNIX	61
5.2. Protection de postes de travail	64
5.3. Centre de gestion de la sécurité Dr.Web	66
5.3.1. Administration	69
5.3.2. Réseau antivirus	72
5.3.3. Favoris	82
5.3.4. Barre de recherche	83
5.3.5. Événements	84
5.3.6. Paramètres	86



5.3.7. Aide	91
5.4. Composants du Centre de gestion de la sécurité Dr.Web	92
5.4.1. Scanner réseau	92
5.5. Schéma d'interaction des composants du réseau antivirus	96
Chapitre 6 : Administrateurs du réseau antivirus	100
6.1. Authentification des administrateurs	100
6.1.1. Authentification des administrateurs depuis la BD du Serveur Dr.Web	101
6.1.2. Authentification via LDAP/AD	102
6.1.3. Authentification via RADIUS	102
6.1.4. Authentification via PAM	104
6.1.5. Authentification via Active Directory	106
6.1.6. Authentification via LDAP	107
6.2. Administrateurs et groupes administrateur	109
6.2.1. Hiérarchie des administrateurs	109
6.2.2. Droits d'administrateurs	110
6.3. Gestion des comptes et des groupes administrateur	114
6.3.1. Création et suppression des comptes et des groupes administrateur	114
6.3.2. Récupération du mot de passe de l'administrateur	117
6.3.3. Éditer les comptes et les groupes administrateurs	118
Chapitre 7 : Gestion globale des postes de travail	121
7.1. Héritage de la configuration du poste de travail	122
7.2. Groupes	125
7.2.1. Groupes système et groupes utilisateur	126
7.2.2. Gestion des groupes	130
7.2.3. Placement des postes dans les groupes	133
7.2.4. Comparaison des postes et des groupes	138
7.2.5. Copie des configurations vers d'autres groupes/postes	138
7.3. Politiques	139
7.3.1. Gestion des politiques	140
7.3.2. Assignation d'une politique aux postes	141
7.4. Profils	142
7.4.1. Création et assignation de profils	144
7.4.2. Configuration des profils	145
Chapitre 8 : Gestion des postes de travail	154
8.1. Gestion des comptes des postes de travail	154
8.1.1. Politique d'approbation des postes	154



8.1.2. Suppression et restauration d'un poste	156
8.1.3. Fusionner des postes	157
8.2. Paramètres généraux du poste de travail	157
8.2.1. Propriétés du poste	157
8.2.2. Composants de protection	163
8.2.3. Matériel et logiciels des postes tournant sous Windows	164
8.3. Configuration du poste de travail	166
8.3.1. Droits des utilisateurs du poste	166
8.3.2. Planification des tâches sur un poste	168
8.3.3. Composants à installer du package antivirus	174
8.3.4. Paramètres de connexion	175
8.3.5. Clés de licence	176
8.4. Configuration des composants antivirus	179
8.5. Scan antivirus des postes de travail	184
8.5.1. Interruption des composants en cours selon leur type	184
8.5.2. Lancement de l'analyse sur le poste de travail	185
8.5.3. Configuration du Scanner	186
8.6. Consultation des statistiques sur un poste	194
8.6.1. Statistiques	194
8.6.2. Graphiques	205
8.6.3. Identificateurs de sécurité	206
8.6.4. Quarantaine	207
8.6.5. Rapports du support technique	211
8.7. Envoi des fichiers d'installation	212
8.8. Envoi de messages aux postes	214
Chapitre 9 : Gestion des postes dans les environnements virtuels	218
9.1. Connexion de postes au Serveur de scan	219
9.2. Intégration à l'infrastructure de bureau virtuel	223
Chapitre 10 : Configuration du Serveur Dr.Web	228
10.1. Gestion des licences	228
10.1.1. Gestionnaire de licences	228
10.1.2. Rapport sur l'utilisation des licences	237
10.2. Journalisation	239
10.2.1. Journal en temps réel	239
10.2.2. Journal d'audit	241
10.2.3. Journal du Serveur Dr.Web	243



10.2.4. Journal des mises à jour du référentiel	245
10.2.5. Journal de messages	247
10.3. Configuration du Serveur Dr.Web	249
10.3.1. Général	250
10.3.2. Trafic	252
10.3.3. Réseau	256
10.3.4. Statistiques	263
10.3.5. Sécurité	268
10.3.6. Cache	269
10.3.7. Base de données	270
10.3.8. Modules	273
10.3.9. Localisation	274
10.3.10. Licences	274
10.3.11. Journal	276
10.4. Accès distant au Serveur Dr.Web	277
10.5. Configuration de l'agent SNMP Dr.Web	278
10.6. Configuration de la planification du Serveur Dr.Web	279
10.7. Configuration du Serveur web	292
10.7.1. Général	293
10.7.2. Avancé	295
10.7.3. Transport	296
10.7.4. Sécurité	296
10.7.5. Modules	298
10.7.6. Gestionnaires	299
10.8. Procédures utilisateur	301
10.9. Modèles de messages	306
10.10. Configuration des notifications	307
10.10.1. Configuration des notifications	307
10.10.2. Notifications de la console Web	314
10.10.3. Notifications non envoyées	316
10.11. Gestion du référentiel du Serveur Dr.Web	317
10.11.1. Statut du référentiel	322
10.11.2. Mises à jour reportées	322
10.11.3. Configuration générale du référentiel	324
10.11.4. Configuration détaillée du référentiel	328
10.11.5. Contenu du référentiel	334



10.11.6. Hashs de menaces connus	336
10.12. Contrôle des applications	338
10.12.1. Mode de test	341
10.12.2. Applications de confiance	342
10.12.3. Répertoire d'applications	346
10.13. Options supplémentaires	349
10.13.1. Gestion de la base de données	349
10.13.2. Statistiques du Serveur Dr.Web	352
10.13.3. Copies de sauvegarde	353
10.13.4. Utilitaires	355
10.13.5. Produits d'entreprise	357
10.14. Particularités du réseau avec plusieurs Serveurs Dr.Web	358
10.14.1. Structure du réseau avec plusieurs Serveurs Dr.Web	359
10.14.2. Configuration des liaisons entre Serveurs Dr.Web	361
10.14.3. Utilisation du réseau antivirus avec plusieurs Serveurs Dr.Web	368
10.14.4. Cluster des Serveurs Dr.Web	369
Chapitre 11 : Mise à jour des composants de Dr.Web Enterprise Security Suite lors du fonctionnement du produit	375
11.1. Mise à jour du Serveur Dr.Web et restauration depuis une copie de sauvegarde	375
11.2. Mise à jour des Serveurs Dr.Web dans le cluster	377
11.3. Mise à jour manuelle du référentiel du Serveur Dr.Web	378
11.4. Mise à jour du référentiel du Serveur Dr.Web selon la planification	379
11.5. Mise à jour du référentiel du Serveur Dr.Web non connecté à Internet	380
11.5.1. Copier le référentiel d'un autre Serveur Dr.Web	381
11.5.2. Chargeur du référentiel Dr.Web	381
11.6. Restrictions de mises à jour des postes	386
11.7. Mise à jour des Agents Dr.Web en mode mobile	389
Chapitre 12 : Configuration des composants supplémentaires	390
12.1. Serveur proxy Dr.Web	390
12.1.1. Configuration distante du Serveur proxy	394
12.2. NAP Validator	399
Référence	403



Chapitre 1 : Introduction

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

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

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 et 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

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.

4. Manuel sur Web API

Il contient les informations techniques sur l'intégration de Dr.Web Enterprise Security Suite avec un tiers logiciel via Web API.

5. Manuel de la structure de la base de données du Serveur Dr.Web

Contient la description de la structure interne de la base de données du Serveur Dr.Web et des exemples de son utilisation.



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, leur dernière version est disponible sur le site officiel de Doctor Web à l'adresse <https://download.drweb.com/doc/>.

1.2. Légende et abréviations

Conventions

Les styles utilisés dans ce manuel :

Style	Commentaire
	Notice/indication importante.
	Avertissement sur des situations potentielles d'erreurs et sur les éléments importants auxquels il faut faire attention.
<i>Réseau antivirus</i>	Un nouveau terme ou l'accent mis sur un terme dans les descriptions.
<IP-address>	Champs destinés à remplacer les noms fonctionnels par leurs valeurs.
Enregistrer	Noms des boutons de l'écran, des fenêtres, des éléments de menu et d'autres éléments de l'interface du logiciel.
CTRL	Touches du clavier.



Style	Commentaire
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 :

- 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,
- -
- 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,
- MIB : base d'information pour la gestion du réseau (Management Information Base),
- 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).

Chapitre 2 : Dr.Web Enterprise Security Suite

2.1. A propos du produit

Dr.Web Enterprise Security Suite est conçu pour la mise en oeuvre d'une protection antivirus unique et 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.

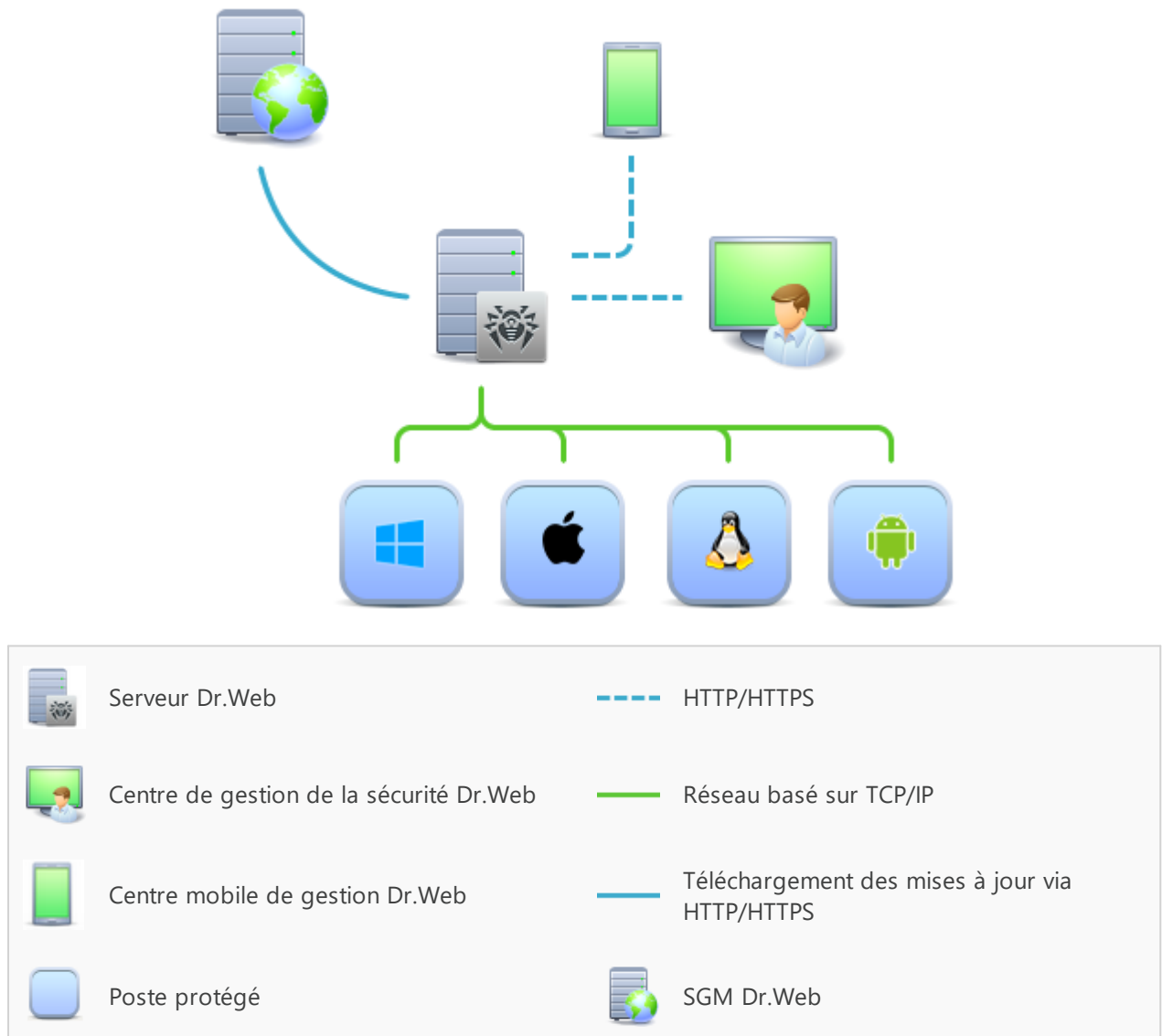


Figure 1-1. Structure logique du réseau antivirus

Le réseau antivirus Dr.Web Enterprise Security Suite a l'architecture *client-serveur*. Ses composants sont installés sur les postes. Dans ce cas, le terme poste signifie un appareils protégé dans le réseau antivirus sur lequel l'Agent Dr.Web et le package antivirus sont installés.



Cet appareil agit en tant que client et interagit avec le Serveur Dr.Web. Ce sont les ordinateurs, les appareils mobiles et virtuels d'utilisateurs et d'administrateurs, les ordinateurs exécutant les fonctions des serveurs LAN qui peuvent jouer le rôle d'un poste.

Les composants du réseau antivirus 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 (ci-après dénommé le Serveur Dr.Web) 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 **Manuel d'installation**, le p. [Pré-requis système](#).

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

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

Le Serveur Dr.Web 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 Dr.Web 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 Dr.Web qui maintiennent les postes protégés du réseau antivirus.

Le Serveur Dr.Web prend en charge la fonction de sauvegarde (backup) des données critiques (les bases de données, fichiers de configuration etc.).

Le Serveur Dr.Web effectue la journalisation des événements du réseau antivirus.

Base de données commune

La base de données commune se connecte au Serveur Dr.Web et contient les statistiques des événements du réseau antivirus, les paramètres du Serveur Dr.Web, 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 Dr.Web est fournie.

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

- MySQL, Maria DB,
- Oracle,



- PostgreSQL (PostgreSQL Pro, Jatoba et autres),
- 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 besoins tels que : la possibilité de maintenir le réseau antivirus d'une taille correspondante, les particularités de maintenance du logiciel de la 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 (ci-après dénommé le Centre de gestion de la sécurité Dr.Web) s'installe automatiquement avec le Serveur Dr.Web et fournit l'interface Web permettant la gestion à distance du Serveur Dr.Web et du réseau antivirus par le biais de la modification des configurations du Serveur Dr.Web et des postes protégés conservés sur le Serveur Dr.Web et sur les postes protégés.

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

- Windows Internet Explorer,
- Microsoft Edge,
- Mozilla Firefox,
- Google Chrome,
- Navigateur Yandex.

La liste des options d'utilisation possibles se trouve dans le **Manuel d'installation**, p. [Pré-requis système](#).

Le Centre de gestion fournit les fonctionnalités suivantes :

- Facilité d'installation de l'Antivirus sur les postes protégés, y compris la possibilité d'installation à distance avec une recherche préliminaire des ordinateurs ; création de distributions aux identifiants et aux paramètres uniques de connexion au Serveur de protection centralisée pour faciliter le processus d'installation de l'Antivirus par l'administrateur et donner la possibilité aux utilisateurs d'installer l'Antivirus eux-même.
- Facilité de gestion des postes dans le réseau antivirus, assurée par un mécanisme de groupement (pour plus d'informations, voir [Chapitre 7 : Gestion globale des postes de travail](#)).
- Possibilité de gestion centralisée de packages antivirus de postes, y compris : suppression de composants particuliers ou de l'Antivirus dans son ensemble sur les postes tournant sous 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 (pour plus d'informations, voir [Chapitre 8 : Gestion des postes de travail](#)).



- Gestion centralisée du scan antivirus de postes, y compris lancement à distance du scan antivirus selon la planification ou la requête directe de l'administrateur depuis le Centre de gestion, configuration centralisée de paramètres du scan antivirus qui sont transmis sur les postes pour lancer le scan local avec les paramètres spécifiés (pour plus d'informations voir [Scan antivirus des postes de travail](#)).
- 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 (pour plus d'informations, voir [Consultation des statistiques sur un poste](#)).
- Système flexible d'administration du Serveur de protection centralisée 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 (pour plus d'informations, voir [Chapitre 6 : Administrateurs du réseau antivirus](#)).
- Gestion de licences de protection antivirus sur les postes avec le système ramifié d'assignation de licences aux postes, groupes de postes et de transmission de licences entre plusieurs Serveurs de protection centralisée en cas de configuration réseau multi-serveurs (pour plus d'informations, voir [Gestionnaire de licences](#)).
- Un large ensemble de paramètres pour configurer le Serveur Dr.Web et ses composants, y compris : configuration de planification de maintenance ; 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 plus d'informations, voir [Chapitre 10 : Configuration du Serveur Dr.Web](#)).



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

Le Serveur web est automatiquement installé avec le Serveur Dr.Web 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 mobile de gestion (Dr.Web Mobile Control Center) est fourni en tant que composant à part tournant sous iOS et Android. La configuration requise pour l'application est décrite dans la **Manuel d'installation**, le p. [Pré-requis système](#).

Le Centre de gestion mobile se connecte au Serveur Dr.Web par un protocole crypté et utilise les identifiants de l'administrateur. Le Centre de gestion Mobile supporte les fonctions de base du Centre de gestion :

1. 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 le poste sélectionné ou sur tous les postes du groupe sélectionné.
2. 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.
 3. Gestion des postes et des groupes :
 - consultation des paramètres ;
 - consultation et gestion du contenu des composants du package antivirus ;
 - suppression de postes et de groupes ;
 - envoi de messages sur les postes ;
 - redémarrage des postes tournant sous Windows ;
 - ajout des postes et des groupes aux favoris pour l'accès rapide.
 4. 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 ;
 - prévention de la perte de notifications suite à une suppression automatique.
 5. Gestion des nouveaux postes qui attendent la connexion au Serveur Dr.Web :
 - approbation de l'accès ;
 - rejet des postes.
 6. 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.
 7. 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.
 8. Recherche des postes et des groupes sur le réseau antivirus par le nom, l'adresse ou l'ID.

Vous pouvez télécharger Dr.Web Mobile Control Center 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 Dr.Web) 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 systèmes d'exploitation suivants :

- OS Windows,
- OS de la famille UNIX,
- macOS,
- OS Android.

Les ordinateurs personnels et les serveurs LAN peuvent être considérés comme postes protégés. La protection antivirus du système de messagerie Microsoft Outlook est supportée.

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

En cas d'indisponibilité du Serveur Dr.Web 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 Windows

Protection antivirus

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

Moniteur de fichiers

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

Moniteur de courrier

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

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



Moniteur web

Analyse de toutes les requêtes vers les sites Web via le protocole HTTP. Neutralisation des menaces contenues dans le trafic HTTP (par exemple, dans les fichiers reçus/envoyés). Limitation 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 Internet. Contrôle de la connexion et de la transmission de données via Internet et blocage de connexions suspectes au niveau de paquets et d'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.

Contrôle des applications

Il surveille l'activité de tous les processus sur les postes. Il permet à l'administrateur du réseau antivirus de spécifier les applications dont le lancement sera autorisé ou bloqué sur les postes protégés.

Postes tournant sous l'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 envoie 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 créés sur les disques durs et des fichiers ouverts sur les supports amovibles.

Moniteur web

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

Quarantaine

Isolation des objets malveillants ou suspects dans un répertoire spécial.

Appareils mobiles tournant sous OS Android

Protection antivirus

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

Moniteur de fichiers

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



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 de 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 de connexions suspectes au niveau de paquets et d'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 Dr.Web et les postes protégés dans le cas où la connexion directe 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 Dr.Web et la connexion entre le Serveur Dr.Web et le Serveur proxy et pour réduire le délai 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 Dr.Web, 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 Dr.Web.

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. Le Chargeur du référentiel Dr.Web peut être utilisé pour télécharger les mises à jour de produits Dr.Web Enterprise Security Suite et pour placer les mises à jour sur le Serveur Dr.Web qui n'est pas connecté à Internet.

Serveur de scan Dr.Web

Le serveur de scan Dr.Web est fourni sous forme d'un composant à part destiné à fonctionner dans des environnements virtuels. Le serveur de scan est installé sur une machine virtuelle à part et traite les demandes de scan antivirus reçues des autres machines virtuelles.

2.2. Kit de distribution

La distribution Dr.Web Enterprise Security Suite est fournie en fonction du système d'exploitation du Serveur Dr.Web sélectionné :

1. 'Pour les OS de la famille UNIX :

- `drweb-esuite-server-<version_du_package>-<assemblage>-<version_de_l'OS>.tar.gz.run`

Distribution du Serveur Dr.Web.



- `drweb-reloader-<OS>-<nombre de bits>`
Version de console du Chargeur du référentiel Dr.Web.

2. Sous Windows :

- `drweb-esuite-server-<version_du_package>-<assemblage>-<version_de_l'OS>.exe`
Distribution du Serveur Dr.Web.
- `drweb-<version_du_package>-<assemblage>-esuite-agent-full-windows.exe`
Installateur complet de l'Agent Dr.Web.
- `drweb-reloader-windows-<nombre_de_bits>.exe`
Version de console du Chargeur du référentiel Dr.Web.
- `drweb-reloader-gui-windows-<nombre_de_bits>.exe`
Version graphique du Chargeur du référentiel Dr.Web.

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

- logiciel du Serveur Dr.Web pour le système d'exploitation correspondant ;
- données de sécurité du Serveur Dr.Web ;
- logiciel du Centre de gestion de la sécurité Dr.Web ;
- logiciel de l'Agent Dr.Web et package antivirus pour les postes sous Windows ;
- module de mise à jour de l'Agent Dr.Web pour Windows ;
- Antispam Dr.Web pour Windows ;
- bases virales, bases de filtres intégrés des composants antivirus et de l'Antispam Dr.Web pour Windows ;
- documentation ;
- actualités de Doctor Web.

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

Après l'installation du Serveur Dr.Web, vous pourrez télécharger dans le référentiel les Produits d'entreprise Dr.Web suivants se trouvant sur les serveurs du SGM :

- Produits pour l'installation sur les postes protégés tournant sous UNIX (y compris les serveurs du réseau local), Android, macOS ;
- Serveur de scan Dr.Web ;
- Dr.Web pour IBM Lotus Domino ;
- Dr.Web pour Microsoft Exchange Server ;
- Serveur proxy Dr.Web ;
- Installateur complet de l'Agent Dr.Web pour Windows ;
- Agent Dr.Web pour Active Directory ;



- Utilitaire de modification du schéma Active Directory ;
- Utilitaire de modification des attributs des objets Active Directory ;
- NAP Validator.



Pour en savoir plus sur la gestion du référentiel du Serveur Dr.Web, consultez le **Manuel Administrateur**, la rubrique [Gestion du référentiel du Serveur Dr.Web](#).



Chapitre 3 : 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/v4/>, 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 les fichiers clé de démonstration. Les fichiers clés de démo fournissent les fonctionnalités complètes des composants antivirus, mais leur durée de validité est limitée. Pour obtenir les fichiers clés de démo, vous devez remplir un formulaire se trouvant sur la page <https://download.drweb.com/demoreq/biz/>. Votre demande sera traitée à titre individuel. En cas de réponse positive, une archive contenant les fichiers clés de licence vous sera envoyée à l'adresse e-mail indiquée.



L'utilisation des fichiers clés de licence lors de l'installation du programme est décrite dans le **Manuel d'installation**, p. [Installer le Serveur Dr.Web](#).

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

3.1. Politique de l'octroi de licence

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



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

- Lors de l'installation d'un nouveau Serveur Dr.Web, un nouveau UUID est généré.
- Durant la mise à niveau du Serveur Dr.Web depuis des versions antérieures, l'IDUU est récupéré automatiquement du fichier de configuration de la précédente version et enregistré dans le fichier de configuration du Serveur Dr.Web installé.

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

2. Les clés de licence sont valables uniquement pour les postes protégés . Vous pouvez assigner une licence à des postes particuliers ou à des groupes de postes : dans ce cas, une clé de licence est valide pour tous les postes qui l'héritent de ce groupe. Pour assigner un fichier clé en même temps pour tous les postes du réseau antivirus pour lesquels aucun paramètre personnalisé de la clé de licence n'est spécifié, assignez la clé de licence au groupe **Everyone**.
3. Le fichier clé de licence peut être spécifié durant l'installation du Serveur Dr.Web (voir le **Manuel d'installation**, p. [Installer le Serveur Dr.Web](#)).

Pourtant, le Serveur Dr.Web peut être installé sans clé de licence. La licence peut être ajoutée plus tard localement ou via la communication inter-serveurs.



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



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

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

3.2. Distributions des licences par les liaisons entre les serveurs

Dans le réseau antivirus avec plusieurs Serveurs Dr.Web, il est possible de transférer un nombre optionnel des licences entre les Serveurs Dr.Web pour un certain temps.



Pour pouvoir transférer les licences entre les Serveurs Dr.Web, configurez les liaisons entre les Serveurs, comme cela est décrit dans la rubrique [Configuration des liaisons entre Serveurs Dr.Web](#).



La distribution de licences est possible uniquement pour les types des liaisons suivantes :

- Le Serveur Dr.Web principal délivre les licences, le Serveur Dr.Web subordonné accepte conformément aux paramètres de la liaison pour le transfert des licences (ne sont pas à modifier).
- Le transfert des licences entre les Serveurs Dr.Web égaux. Dans ce cas, sur le Serveur Dr.Web qui délivre les licences, la case **Envoyer** doit être cochée dans la section **Licences** des paramètres de la liaison, sur le Serveur Dr.Web qui accepte les licences, c'est la case **Accepter** qui doit être cochée.

Pour configurer le Serveur Dr.Web qui délivrera les licences

1. Ouvrez le Centre de gestion du Serveur Dr.Web du réseau antivirus qui délivrera les licences aux Serveurs voisins Dr.Web.
2. Pour ouvrir le **Gestionnaire de licences**, sélectionnez l'élément **Administration** dans le [menu de gestion](#) du Centre de gestion.
3. Ajoutez la clé de licence comme cela est décrit dans la section [Gestionnaire de licences](#), si la clé n'a pas été ajoutée auparavant. Le nombre des licences dans la clé doit correspondre au nombre total des postes servis par ce Serveur Dr.Web et par tous les Serveurs Dr.Web qui accepteront les licences de cette clé.

Dans le cas commun, une seule clé peut suffire. Les licences de cette clé seront réparties entre tous les Serveurs Dr.Web.

4. Comptez combien de licences de cette clé vous pouvez transférer aux Serveurs voisins Dr.Web. Lors du compte, notez que les Serveurs voisins Dr.Web peuvent transmettre une partie des licences aux autres Serveurs Dr.Web. Dans ce cas, le nombre total des licences que vous planifiez de diffuser le long de la chaîne est transmis de la clé du Serveur Dr.Web principal. Notez également que le Serveur Dr.Web principal ne pourra pas utiliser les licences distribuées avant le délai de distribution de ces licences et leur retour.
5. Configurez la distribution des licences depuis la clé de licence sur les Serveurs voisins Dr.Web comme cela est décrit dans la section [Gestionnaire de licences](#).

Dans le paramètre **Date d'expiration de la licence**, spécifiez la date finale de la validité du transfert des licences. Le délai de transfert peut être inférieur ou égal au délai de validité de la licence. A l'expiration du délai, toutes les licences seront rappelées du Serveur voisin Dr.Web et retourneront dans la liste des licences disponibles dans la clé de licence initiale. Si nécessaire, vous pourrez modifier ce délai à tout moment comme cela est décrit dans la section [Gestionnaire de licences](#).

6. Si nécessaire, modifiez les paramètres de distribution des licences. Pour ce faire, allez dans la section **Configuration du Serveur Dr.Web**.
7. Dans l'onglet **Licences**, spécifiez les paramètres suivants concernant le Serveur Dr.Web délivrant les licences :
 - **Période du renouvellement automatique des licences délivrées** : période de temps pour laquelle les licences sont délivrées de la clé sur ce Serveur Dr.Web. A l'expiration de cette période, les licences délivrées sont renouvelées automatiquement pour le même délai. Le renouvellement automatique sera effectué jusqu'à ce que dure le délai de



distribution des licences spécifié dans le Gestionnaire de licences à l'étape 5. Ce mécanisme assure le retour des licences sur le Serveur Dr.Web principal au cas où le Serveur Dr.Web subordonné sera désactivé et ne pourra pas retourner les licences délivrées.

- **Période de synchronisation de licences** : périodicité de synchronisation des informations sur les licences délivrées entre les Serveurs Dr.Web. La synchronisation des licences permet de déterminer que le nombre de licences délivrées par le Serveur Dr.Web principal correspond au nombre des licences reçues par le Serveur Dr.Web subordonné. Ce mécanisme permet de détecter les défaillances et les cas de falsification lors du transfert des licences.
- **Période de création du rapport** : fréquence de création des rapports sur les clés de licences utilisées. Si le rapport sur l'utilisation de licences est créé par le Serveur subordonné Dr.Web, ce rapport sera envoyé sur le Serveur principal Dr.Web juste après sa création. Les rapports créés sont également envoyés à chaque connexion (y compris chaque redémarrage) du Serveur Dr.Web, et en cas de modification du nombre de licences délivrées sur le Serveur principal Dr.Web. Le paramètre est spécifiée sur le Serveur principal Dr.Web, mais il est également utilisé par le Serveur subordonné Dr.Web lors de l'envoi des rapports.
- **Période de décompte des postes actifs** : période pendant laquelle les postes actifs seront comptés pour envoyer un rapport sur l'utilisation des licences. La valeur 0 indique d'utiliser dans le rapport tous les postes quel que soit leur statut d'activité. Le paramètre est spécifié sur le Serveur Dr.Web principal mais il est également utilisé par le Serveur Dr.Web subordonné lors de l'envoi des rapports.

8. Enregistrez les modifications apportées et redémarrez le Serveur Dr.Web.

Pour configurer le Serveur Dr.Web qui recevra les licences :

1. Ouvrez le Centre de gestion du Serveur Dr.Web du réseau antivirus qui recevra les licences du Serveur voisin Dr.Web.
2. Si nécessaire, modifiez les paramètres de distribution des licences. Pour ce faire, allez dans la section **Configuration du Serveur Dr.Web**.
3. Dans l'onglet **Licences**, spécifiez l'**Intervalle de renouvellement provisoire des licences obtenues** — délai de temps qui dure jusqu'à la fin de la période du renouvellement automatique des licences obtenues du Serveur voisin Dr.Web. A partir de ce moment ce Serveur Dr.Web demande le renouvellement automatique provisoire de ces licences.

L'utilisation de ce paramètre dépend du type de connexion sélectionné dans la section **Paramètres de connexion** lors de la configuration de la liaison entre les Serveurs Dr.Web (voir la section [Configuration des liaisons entre Serveurs Dr.Web](#)) :

- Pour la connexion périodique : si la période de reconnexion spécifiée dans le paramètre de la liaison est supérieure à la **Période du renouvellement automatique des licences délivrées** spécifiée sur le Serveur Dr.Web délivrant les licences, le renouvellement automatique de ces licences sera initié avant l'expiration de la **Période du renouvellement automatique des licences délivrées**.
- Pour la reconnexion permanente : ce paramètre n'est pas utilisé.



4. Enregistrez les modifications apportées et redémarrez le Serveur Dr.Web.

3.3. Mise à jour automatique de licences


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

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

- À l'expiration de la clé de licence, elle peut être remplacée automatiquement par une clé de licence achetée d'avance.
- La mise à jour automatique s'effectue pour une clé de licence particulière pour laquelle a été acheté le renouvellement.
- La clé de licence pour la mise à jour automatique se trouve sur les serveurs de Doctor Web jusqu'à l'expiration de sa validité.

Procédure de la mise à jour automatique des licences

La procédure de la mise à jour automatique des licences est lancée dans les cas suivants :

- Quand l'administrateur clique sur le bouton  **Vérifier la disponibilité des mises à jour et remplacer les clés de licence** dans la barre d'outils du [Gestionnaire de licences](#) du Centre de gestion.
- Quand la tâche **Mise à jour du référentiel** de la [planification du Serveur Dr.Web](#) est exécutée. Dans ce cas, la case **Mettre à jour les clés de licence** doit être cochée dans les paramètres de la tâche.



La mise à jour automatique de la clé de licence est lancée uniquement si la licence mise à jour appartient à ce Serveur Dr.Web : au départ elle est ajoutée manuellement ou obtenue lors de la mise à jour automatique. Pour les licences obtenues depuis les Serveurs voisins Dr.Web par les liaisons entre les serveurs, la procédure de la mise à jour automatique ne se lance pas.

La procédure de la mise à jour automatique de la licence comprend les étapes suivantes :

1. Vérification de la présence de la clé de licence sur les serveurs de la société Doctor Web (SGM).
2. Le chargement de la clé de licence depuis le SGM sur le Serveur Dr.Web avec l'ajout de la clé dans la base de données et le Gestionnaire de licences.
3. Distribution de la nouvelle clé de licence sur les objets de la clé précédente.

En fonction des résultats d'exécution de chaque étape, la procédure peut se terminer à chacune des étapes.



Les résultats suivants d'exécution de la mise à jour automatique sont possibles :

1. *La clé de licence pour la mise à jour automatique est introuvable dans le SGM.*

Aucune action ne sera effectuée.

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

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

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

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

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

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

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

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

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



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



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

Mise à jour manuelle des licences

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

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

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

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

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



fois par minute. En cas de disponibilité de licences disponibles, elles seront remises aux Serveurs voisins Dr.Web.

Fichier clé de licence

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

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



Chapitre 4 : Mise en route

4.1. 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, les machines virtuelles et les appareils mobiles à protéger.

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



Le Serveur de protection centralisée peut être installé sur n'importe quel ordinateur et pas uniquement sur le poste utilisé comme serveur LAN. Pour en savoir plus sur les pré-requis principaux, consultez le **Manuel d'installation**, le p. [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 Dr.Web.

Pour installer le Serveur Dr.Web et l'Agent Dr.Web une procédure d'accès unitaire aux postes 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.

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 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.

Vous pouvez consulter la description détaillée de l'ordre de gestion des groupes administratifs et des règles d'accès dans [Chapitre 6 : Administrateurs du réseau antivirus](#).



2. Déterminez quels produits pour quels systèmes d'exploitation sont 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 les postes 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 Dr.Web 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 **Manuel d'installation**, le p. [Installation du Serveur Dr.Web](#). Le Centre de gestion de la sécurité Dr.Web est installé avec le Serveur Dr.Web. Par défaut, le Serveur Dr.Web démarre de manière automatique après l'installation et après chaque redémarrage du système.
4. Si nécessaire, installez et configurez le Serveur proxy. Vous pouvez consulter la description dans le **Manuel d'installation**, le p. [Installation du Serveur proxy Dr.Web](#).
5. Si le réseau antivirus est composé de machines virtuelles, il est recommandé d'utiliser le Serveur de scan. Vous trouverez la description d'installation et de configuration dans le **Manuel d'installation**, p. [Installation du Serveur de scan Dr.Web](#).
6. Pour configurer le Serveur Dr.Web et le logiciel antivirus sur les postes, il faut se connecter au Serveur Dr.Web 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 Dr.Web. Une connexion réseau doit être établie avec l'ordinateur sur lequel le Serveur Dr.Web est installé.

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

`http://<Adresse_du_Serveur_Dr.Web>:9080`

ou

`https://<Adresse_du_Serveur_Dr.Web>:9081`

où comme valeur `<Adresse_du_Serveur_Dr.Web>` spécifiez l'adresse IP, NetBIOS 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 Dr.Web.



- pour les OS de la famille UNIX — mot de passe qui a été automatiquement créé au cours de l'installation du Serveur Dr.Web (voir aussi le **Manuel d'installation**, le p. [Installation du Serveur Dr.Web pour les OS de la famille UNIX](#)).

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

Si vous avez installé le Serveur de scan, indiquez son adresse dans les paramètres du poste (voir la description détaillée dans le **Manuel Administrateur**, p. [Connexion de postes au Serveur de scan](#)).

7. Effectuez la configuration initiale du Serveur Dr.Web (vous pouvez consulter la description détaillée des paramètres dans la [Chapitre 10 : 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 Dr.Web.
 - b. Dans la rubrique [Configuration générale du référentiel](#), spécifiez les composants du réseau antivirus à mettre à jour depuis le SGM Dr.Web. Si le réseau antivirus inclut des postes protégés sous Android, Linux, macOS, il faut télécharger les **produits d'entreprise Dr.Web**.

Dans la rubrique [Statut du référentiel](#) effectuez la mise à jour des produits du référentiel du Serveur Dr.Web. La mise à jour peut prendre un long temps. Attendez la fin de la mise à jour avant de continuer la configuration.



Lors de l'installation du Serveur Dr.Web en version 13, les mises à jour des produits de référentiel **Bases Dr.Web pour Android**, **Agent Dr.Web pour UNIX** et **Serveur proxy Dr.Web** sont téléchargées depuis le SGM uniquement en cas d'appel de ces produits depuis les postes. Pour en savoir plus, consultez le p. [Configuration détaillée du référentiel](#).

Si votre Serveur Dr.Web n'est pas connecté à Internet, les mises à jour sont téléchargées manuellement depuis un autre Serveur Dr.Web ou via le Chargeur du référentiel et que vous voulez installer ou mettre à jour les produits pour lesquels l'option **Mettre à jour à la demande uniquement** est activé dans les paramètres du référentiel, il faut d'abord télécharger ces produits manuellement dans le référentiel.

- c. Vous trouverez les informations sur la version du Serveur Dr.Web sur la page **Administration** → **Serveur Dr.Web**. Si la nouvelle version est disponible, mettez à jour le Serveur Dr.Web. La procédure est décrite dans le p. [Mise à jour du Serveur Dr.Web et restauration depuis une copie de sauvegarde](#).
- d. Si nécessaire, spécifiez la [Configuration des 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 Dr.Web. L'authentification externe des administrateurs est également possible. Pour en savoir plus, consultez la [Chapitre 6 : 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 Dr.Web (voir 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 Dr.Web et de ceux de la copie de sauvegarde.
8. Spécifiez les paramètres et la configuration du logiciel antivirus pour les postes (vous pouvez consulter la description détaillée de la configuration de groupes et de postes dans la [Chapitre 7](#) et la [Chapitre 8](#)) :
 - a. Si nécessaire, créez les groupes utilisateur de postes.
 - b. Spécifiez les paramètres du groupe **Everyone** et des groupes utilisateur créés. Notamment configurez la rubrique des composants à installer.
9. Installez le logiciel de l'Agent Dr.Web sur un poste.

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

- Si les utilisateurs installent l'antivirus eux-mêmes, utilisez les packages d'installation personnels qui sont créés via le Centre de gestion séparément pour chaque poste. Vous pouvez envoyer aux utilisateurs des e-mails avec ce type de package directement du Centre de gestion. Après l'installation, les postes se connectent automatiquement au Serveur Dr.Web.
- 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 poste ou sur plusieurs postes en même temps tournant sous Windows ou Linux. 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 Dr.Web.
- Si, lors de l'installation, il faut diminuer la charge sur le canal de communication entre le Serveur Dr.Web et les postes, vous pouvez utiliser l'installateur complet qui effectue l'installation de l'Agent Dr.Web et des composants de protection en même temps.
- L'installation sur les postes sous OS Android et macOS peut s'effectuer de manière locale conformément aux règles générales. Le produit autonome installé peut se connecter au Serveur Dr.Web conformément à la configuration correspondante.



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 Dr.Web se connectent automatiquement au Serveur Dr.Web. L'approbation des postes antivirus sur le Serveur Dr.Web est effectuée selon la politique que vous sélectionnez (les paramètres sont décrits dans le p. [Politique de connexion des postes](#)) :
- En cas d'installation depuis les packages d'installation et la configuration de l'approbation automatique sur le Serveur Dr.Web, les postes sont enregistrés automatiquement à la première connexion au Serveur Dr.Web et l'approbation supplémentaire n'est pas requise.
 - 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 Dr.Web. Dans ce cas, les nouveaux postes ne se connectent pas automatiquement, mais ils sont déplacés par le Serveur Dr.Web dans le groupe de novices.
11. Après la connexion au Serveur Dr.Web et l'obtention des paramètres, l'ensemble des composants du package antivirus est installé sur le poste. Cet ensemble est spécifié dans les paramètres du groupe primaire du poste.



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

12. La configuration des postes et du logiciel antivirus est également possible après l'installation (vous pouvez consulter la description détaillée dans la [Chapitre 8](#)).

4.2. Configuration des connexions réseau

Généralités

Les clients 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 Dr.Web 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 Dr.Web](#).

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 Dr.Web.

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

Cette approche permet de rechercher un Serveur Dr.Web par le nom d'un ordinateur ou le service de Serveur Dr.Web 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 Dr.Web 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 Dr.Web, l'installateur ajoute automatiquement les ports et les interfaces du Serveurs Dr.Web 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.

4.2.1. Connexions directes

Configuration du Serveur Dr.Web

L'adresse qu'il faut écouter pour la réception de connexions TCP entrantes doit être indiquée dans les paramètres du Serveur Dr.Web (voir le document **Annexes**, [Annexe D. Spécification de l'adresse réseau](#)).

Vous pouvez configurer ce paramètre dans la configuration du Serveur Dr.Web :

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 Dr.Web :

- **Adresse** : valeur vide — utiliser *toutes les interfaces réseau* pour cet ordinateur sur lequel le Serveur Dr.Web 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 Dr.Web « 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 Dr.Web, l'adresse du Serveur Dr.Web (l'adresse IP, NetBIOS ou le nom de domaine 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_Dr.Web>
```

Lors de l'installation de l'Agent Dr.Web, il est recommandé d'utiliser le nom du Serveur Dr.Web au format FQDN en tant qu'adresse du Serveur Dr.Web au [format FQDN](#). Cela facilitera le processus de configuration du réseau antivirus relatif à la procédure de réinstallation du Serveur Dr.Web sur un autre ordinateur. Dans ce cas, si vous voulez changer l'adresse du Serveur Dr.Web, il suffira de la changer dans les paramètres du serveur DNS pour le nom de l'ordinateur hébergeant le Serveur Dr.Web. Tous les agents se connecteront automatiquement au nouveau serveur.

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

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

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

4.2.2. 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 Dr.Web. Avant d'établir chaque connexion, une recherche du Serveur Dr.Web dans le réseau sera effectuée. Pour cela, le client envoie une requête broadcast et attend une réponse contenant l'adresse du Serveur Dr.Web. Dès que la réponse est réceptionnée, le client établit une connexion au Serveur Dr.Web.

Pour cela, le Serveur Dr.Web doit "écouter" le réseau pour réceptionner de telles requêtes.

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

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

1. Le Serveur Dr.Web s'enregistre dans le groupe multicast avec une adresse spécifiée dans les paramètres du Serveur Dr.Web.



2. Les Agents Dr.Web lorsqu'ils recherchent le Serveur Dr.Web, envoient des requêtes multicast à l'adresse de groupe spécifiée à l'étape 1.

Le Serveur Dr.Web écoute par défaut l'adresse `udp/231.0.0.1:2193` (idem pour les connexions directes).

Ce paramètre est spécifié dans les paramètres du Centre de gestion **Administration** → **Configuration du Serveur Dr.Web** → **Réseau** → **Transport** → **TCP/IP**. La valeur vide indique d'utiliser l'adresse par défaut indiquée ci-dessus.

4.2.3. Utiliser le protocole SRV

Les clients sous Windows supportent le protocole réseau client *SRV* (une description du format est donnée dans le document **Annexes**, [Annexe D. Spécification de l'adresse réseau](#)).

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

1. Durant l'installation du Serveur Dr.Web, 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 RFC2782 (voir <https://datatracker.ietf.org/doc/html/rfc2782>).

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

Par exemple, le lancement de l'installateur de l'Agent Dr.Web :

- 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 Dr.Web.



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



4.3. Assurance d'une connexion sécurisée

4.3.1. 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 Dr.Web et les clients qui comprennent:

- 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 Dr.Web) 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 Dr.Web.

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

Le [tableau 4-1](#) comprend les combinaisons des paramètres qui assurent (+) ou n'assurent pas (-) le chiffrement et la compression de la connexion entre le Serveur Dr.Web et le client ainsi que les combinaisons inappropriées (**Erreur**).

**Tableau 4-1. Compatibilité des paramètres relatifs aux politiques de chiffrement et de compression**

Paramètres de client	Paramètres du Serveur Dr.Web		
	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 Dr.Web 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 Dr.Web 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 Dr.Web et du Serveur proxy (ici, il sert du client) doivent être coordonnés selon [le tableau 4-1](#).
- Les paramètres du client et du Serveur proxy (ici, il sert du Serveur Dr.Web) doivent être coordonnés selon [le tableau 4-1](#).

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

- Si le Serveur Dr.Web et le client supportent le chiffrement TLS utilisé dans la version 13.0, 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 une version antérieure avec le chiffrement selon GOST est installée sur le Serveur Dr.Web et/ou le client, une vérification supplémentaire selon [le tableau 4-2](#) est effectuée.

**Tableau 4-2. 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 Dr.Web			
	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 Dr.Web 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 Dr.Web ou Agent Dr.Web) est en version 13, et l'autre — en version 10, le chiffrement utilisé dans la version 10 sera spécifié.
Erreur	La connexion du Serveur proxy avec le Serveur Dr.Web et le client sera interrompue.

Ainsi, si le Serveur Dr.Web et l'Agent Dr.Web sont en versions différentes : l'un est en version 13. 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 Dr.Web et avec le client sont établies sans l'utilisation de chiffrement.



- Le chiffrement sera utilisé uniquement si les deux connexions avec le Serveur Dr.Web 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 Dr.Web

Pour configurer les paramètres de compression et de chiffrement du Serveur Dr.Web

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 Dr.Web).
 - **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 Dr.Web).



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

Paramètres de chiffrement et de compression sur le Serveur proxy Dr.Web

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 **Manuel d'installation**, le p. [Connexion du Serveur proxy Dr.Web au Serveur Dr.Web](#).

1. Ouvrez le Centre de gestion pour le Serveur Dr.Web 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 Dr.Web et les installateurs des Agents Dr.Web.
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 Dr.Web 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 Dr.Web 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 Dr.Web. Dans ce cas, il faut spécifier les paramètres à distance depuis le Serveur Dr.Web ou désactiver les paramètres autorisant d'accepter la configuration de ce Serveur Dr.Web.

Le fichier de configuration `drwcsd-proxy.conf` est décrit dans les **Annexes**, [F4. Fichier de configuration du Serveur proxy Dr.Web](#).

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 Dr.Web.
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 Dr.Web est obligatoire.
 - **Possible** : le chiffrement (ou la compression) sera appliqué au trafic avec le Serveur Dr.Web, si les paramètres du Serveur Dr.Web 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 Dr.Web.

Agent Dr.Web pour Windows

Les paramètres de chiffrement et de compression peuvent être spécifiés 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, [G1. Installateur réseau](#)**).

Après l'installation de l'Agent Dr.Web, 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 Dr.Web. Pourtant les paramètres du côté de l'Agent Dr.Web 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 Dr.Web 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 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 côté 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 Dr.Web.

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

4.3.2. 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 Dr.Web `drwcsd.pri`.

Sauvegardée sur le Serveur Dr.Web 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 de chiffrement publique et le certificat sont créés automatiquement de la clé privée lors de l'installation du Serveur Dr.Web. Dans ce cas, une nouvelle clé privée peut être créée ou bien la clé existante (de la dernière installation du Serveur Dr.Web) 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 le document **Annexes**, [H7.1. 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 Dr.Web.*

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

Le Serveur Dr.Web 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 Dr.Web et les clients, les données envoyées par le client sont déchiffrées sur le Serveur Dr.Web avec la clé publique.

2. Clé publique de chiffrement du Serveur Dr.Web *.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 Dr.Web, 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 Dr.Web `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 Dr.Web 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 Dr.Web ou depuis un autre client.

La certificat est utilisé dans les cas suivants :

a) *Authentification du Serveur Dr.Web.*

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



Le Serveur Dr.Web 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 Dr.Web, c'était la clé publique qui était utilisée à cet effet.

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

b) Chiffrement des données.

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

c) Réalisation d'une session TLS entre le Serveur Dr.Web 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 Dr.Web 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 Dr.Web 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 actions 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.

4.3.3. Connexion des clients au Serveur Dr.Web

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

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



- **Agents Dr.Web.**

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

Le certificat utilisé lors de l'installation et les certificats reçus via les paramètres centralisés depuis le Serveur Dr.Web 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 Dr.Web (mais pas dans le registre) et la liste commune des certificats utilisés. Ce certificat sera utilisé pour la connexion au Serveur Dr.Web en cas d'erreur dans les paramètres centralisés.

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

- **Installeurs des Agents Dr.Web.**

Lors de l'installation de l'Agent Dr.Web sur le poste, le certificat du Serveur Dr.Web 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 Dr.Web, 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 Dr.Web (cela concerne tous les types des fichiers d'installation de l'Agent Dr.Web).

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

Si vous configurez les connexions entre les Serveurs voisins Dr.Web en version 11 ou supérieure, sur chaque Serveur Dr.Web configuré il vous faudra spécifier le certificat du Serveur Dr.Web avec lequel vous voulez établir la liaison (voir 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 Dr.Web fourni avec le Serveur Dr.Web en version 11 avec la connexion au Serveur Dr.Web en version 10 et vice-versa n'est pas recommandée.

4.4. Intégration de Dr.Web Enterprise Security Suite avec Active Directory

Si le service Active Directory est utilisé dans le réseau local protégé, vous pouvez configurer l'intégration des composants de Dr.Web Enterprise Security Suite avec ce service.



Toutes les méthodes listées ci-dessous sont autonomes et elles peuvent être appliquées ensemble ou séparément.

L'intégration de Dr.Web Enterprise Security Suite avec Active Directory s'effectue à la base de méthodes suivantes :

1. L'enregistre, du Serveur Dr.Web dans le domaine Active Directory pour appeler le Serveur Dr.Web via le protocole SRV

Lors de l'installation du Serveur Dr.Web, vous avez la possibilité d'enregistrer le Serveur dans le domaine Active Directory via l'installateur. Lors de l'enregistrement sur le serveur DNS, l'enregistrement SRV correspondant au Serveur Dr.Web sera créé. Ensuite, les clients pourront accéder au Serveur Dr.Web via cet enregistrement SRV.

Pour en savoir plus, voir le **Manuel d'installation** [Installation du Serveur Dr.Web sous Windows](#) et [Utilisation du protocole SRV](#).

2. Synchronisation de la structure du réseau antivirus avec le domaine Active Directory

Il existe une possibilité de synchroniser automatiquement les structures du réseau avec les postes du domaine Active Directory. Dans ce cas, les conteneurs Active Directory qui contiennent des ordinateurs deviennent des groupes du réseau antivirus dans lesquels les postes de travail sont placés.

Pour cela, la tâche **Synchronisation avec Active Directory** est fournie dans la planification du Serveur Dr.Web. L'administrateur doit créer cette tâche lui-même ou avec le Planificateur de tâches du Serveur Dr.Web.

Pour en savoir plus, consultez [Configuration de la planification du Serveur Dr.Web](#).



3. Authentification des utilisateurs d'Active Directory sur le Serveur Dr.Web en tant qu'administrateurs

Il existe une possibilité d'authentifier sur le Serveur Dr.Web les utilisateurs sous les comptes d'Active Directory pour la gestion du réseau antivirus. Pour ce faire, il faut utiliser l'un des moyens suivants :

- Authentification LDAP/AD. Disponible pour les Serveurs Dr.Web sur tous les OS supportés. La configuration de l'accès au Serveur Dr.Web pour tous les utilisateurs par les attributs correspondants d'Active Directory se fait via le Centre de gestion. L'accès au contrôleur du domaine et au composant logiciel enfichable Active Directory n'est requis — une configuration supplémentaire du côté d'Active Directory n'est pas effectuée.
- Microsoft Active Directory. Disponible uniquement pour les Serveurs Dr.Web sous Windows inclus dans le domaine cible. La configuration des utilisateurs et des groupes d'utilisateurs ayant accès au Serveur Dr.Web se fait directement dans le composant logiciel enfichable Active Directory. La configuration initiale avec les utilitaires supplémentaires est requise. Les packages `drweb-<version_du_package>-<assemblage>-esuite-modify-ad-schema-<version_de_l'OS>.exe` et `drweb-<version_du_package>-<assemblage>-esuite-aduac-<version de l'OS>.msi` sont disponibles dans le référentiel du Serveur Dr.Web dans les **Produits d'entreprise Dr.Web**.

La sélection de la méthode dépend du système d'exploitation du Serveur Dr.Web et du moyen de configuration des utilisateurs autorisés.

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

4. Installation à distance des Agents Dr.Web sur le poste dans le domaine Active Directory

Il est possible d'installer à distance l'Agent Dr.Web sur le poste dans le domaine Active Directory. Pour ce faire :

- a) Effectuer une installation administrative sur la ressource cible partagée avec l'installateur spécial de l'Agent pour Dr.Web Active Directory. Le package `drweb-<version_du_package>-<assemblage>-esuite-agent-activedirectory.msi` est disponible dans le référentiel du Serveur Dr.Web dans le **Produits d'entreprise Dr.Web**.
- b) Configurer les politiques correspondantes d'Active Directory pour l'installation automatique du package de poste dans le domaine.

Pour en savoir plus, voir **le Manuel d'installation** [Installation de l'Agent Dr.Web avec le service Active Directory](#).

5. Recherche des postes du domaine Active Directory

Il existe une possibilité de chercher les postes du domaine Active Directory via le Scanner du réseau. Dans ce cas, il est possible de déterminer la présence de l'Agent Dr.Web sur les postes trouvés et, s'il n'y est pas, l'installer à distance via le Centre de gestion.



Cette approche de l'installation distante des Agent Dr.Web peut être utilisée en même temps que l'installation automatique des packages avec les politiques Active Directory décrite dans le p.4.

Pour en savoir plus, voir [Scanner réseau](#).

6. Recherche des utilisateurs du domaine Active Directory

Il existe une possibilité de chercher les utilisateur du domaine Active Directory pour la création des profils utilisateur et une configuration plus précise de Office Control et du Contrôle des applications.

Pour en savoir plus, voir le **Manuel de gestion des postes sous Windows**.



Chapitre 5 : Composants du réseau antivirus et leur interface

5.1. Serveur Dr.Web

Le réseau antivirus basé sur Dr.Web Enterprise Security Suite doit comprendre au moins un Serveur Dr.Web.



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

Serveur Dr.Web est un service qui reside en permanence dans la mémoire vive. Le logiciel du Serveur Dr.Web est conçu pour divers OS (consultez la liste complète des systèmes d'exploitation pris en charge dans le **Manuel d'installation**, la rubrique [Pré-requis système](#)).

Fonctions clés

Le Serveur Dr.Web réalise les fonctions suivantes :

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

Collecte des informations sur le statut du réseau antivirus

Le Serveur Dr.Web collecte et journalise les informations sur le fonctionnement des packages antivirus. Il reçoit ces informations depuis les logiciels installés sur les postes protégés (les Agents Dr.Web décrits ci-après). La journalisation est effectuée dans un journal d'événements commun se présentant sous forme de base de données. Dans un réseau de petite taille (400–600 postes au maximum) la base de données embarquée peut être utilisée pour écrire le journal d'événements commun.



La base de données embarquée est conçue pour la connexion de 400–600 postes au Serveur Dr.Web. Si l'ordinateur sur lequel est installé le Serveur Dr.Web et la charge relative à d'autres tâches exécutées sur la même machine le permettent, il est possible de connecter jusqu'à 1000–1500 postes.



Sinon, il est nécessaire d'utiliser une BD externe. En fonction de la configuration et de la charge sur l'ordinateur exécutant les fonctions du Serveur Dr.Web, la BD externe peut être placée sur le même ordinateur ou sur un ordinateur spécial séparé.

En cas d'utilisation d'une BD externe et si le nombre de postes connectés au Serveur Dr.Web est supérieur à 10000, il est recommandé de respecter les pré-requis minimum suivants :

- processeur 3GHz,
- au moins 6 coeurs de processeur,
- mémoire vive : au moins 4 Go pour le Serveur Dr.Web, au moins 8 Go pour le Serveur de BD,
- OS de la famille UNIX.

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

- informations sur la version des packages antivirus sur les postes protégés,
- heure et date d'installation et de mise à jour du logiciel antivirus sur le poste (y compris la version du logiciel),
- heure et date de mise à jour des bases virales et leurs versions,
- information sur la version du système d'exploitation installé sur les postes protégés, sur le type de processeur, l'emplacement des répertoires système etc.,
- configuration et modes de fonctionnement des packages antivirus,
- informations sur les événements viraux et notamment les noms des virus détectés, la date de la détection, les actions réalisées, les résultats de la neutralisation, etc.

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

Serveur Web

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

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



5.1.1. Gestion du Serveur Dr.Web sous Windows

Interface et gestion du Serveur Dr.Web

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

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

- Le répertoire **Gestion du serveur** contient les commandes suivantes :
 - **Journal détaillé** : spécifier le niveau **Tous** pour la journalisation détaillée de fonctionnement du Serveur Dr.Web.
 - **Lancer** : lancer le service de Serveur Dr.Web.
 - **Stop** : arrêter le service de Serveur Dr.Web.
 - **Recharger le référentiel** : relire le référentiel du Serveur Dr.Web depuis le disque.
 - **Recharger les modèles** : relire les modèles de notifications de l'administrateur.
 - **Redémarrer** : redémarrer le service de Serveur Dr.Web.
 - **Vérifier la base de données** : lancer la vérification de la base de données intégrée.
 - **Journal standard** : établir le niveau **Informations** pour le journal de fonctionnement du Serveur Dr.Web.



Une fois les commandes **Journal détaillé** et **Journal standard** exécutées, il faut redémarrer le Serveur Dr.Web pour appliquer les modifications. Pour ce faire, exécutez la commande **Redémarrer**.



Les paramètres avancés de journalisation sont disponibles dans la section [Journal](#) du Centre de gestion.

Pour plus d'infos sur les commandes correspondantes, consultez les **Annexes**, [G3. Serveur Dr.Web](#).

- L'élément **Interface Web** permet d'ouvrir le Centre de gestion et de se connecter au Serveur Dr.Web installé sur ce poste (à l'adresse <http://localhost:9080>).
- L'élément **Documentation** sert à afficher le Manuel Administrateur au format HTML.

Le répertoire du Serveur Dr.Web a la structure suivante :

Répertoire d'installation du Serveur par défaut (peut être modifié si nécessaire) : C:\Program Files\DrWeb Server

- **bin** : fichiers exécutables du Serveur Dr.Web.



- `ds-modules` : modules script déballés.
- `etc` : fichiers de configuration principaux des composants du réseau antivirus.
- `fonts` : polices pour les documents PDF.
- `var` : le répertoire comprend les sous-répertoires suivants :
 - `backup` : copies de sauvegarde de la BD et d'autres données critiques.
 - `extensions` : scripts utilisateur destinés à automatiser l'exécution de certaines tâches.
 - `file-cache` : cache de fichiers.
 - `installers-cache` : cache de sauvegarde des packages d'installation de groupe et personnels de l'Agent Dr.Web lors de la création des postes dans le Centre de gestion. Il est créé en cas de création des paquets d'installation.
 - `plugins` : objets temporaires des plug-ins.
 - `object` : cache des objets du Centre de gestion.
 - `reports` : répertoire temporaire pour la création et la sauvegarde des rapports. Il est créé en cas de nécessité.
 - `repository` : répertoire de référentiel dans lequel sont placées les mises à jour actuelles des bases virales, des fichiers des packages antivirus et des fichiers des composants du réseau antivirus. Le répertoire comprend des sous-répertoires pour certains composants du logiciel et ces sous-répertoires à leur tour contiennent des sous-répertoires appropriés aux OS respectifs. Ce répertoire doit être accessible en écriture à l'utilisateur sous le nom duquel le Serveur Dr.Web démarre (d'habitude, c'est l'utilisateur **LocalSystem**).
 - `sessions` : sessions du Centre de gestion.
 - `tmp` : fichiers temporaires.
 - `twin-cache` : bases virales déballées pour la rétrocompatibilité avec les versions précédentes des Agents Dr.Web. Peut contenir également les autres fichiers déballés du référentiel, par exemple, l'installateur de l'Agent Dr.Web.
 - `upload` : dossier pour télécharger les fichiers temporaires spécifiés via le Centre de gestion. Il est créé lors du téléchargement de fichiers de grande taille.
- `vfs` : modules script et paquets de langue emballés.
- `webmin` : éléments du Centre de gestion.
- `websockets` : scripts pour la gestion des sockets web.

Répertoire de la copie de sauvegarde (peut être modifié en cas de suppression) :

`<disque_d'installation>:\Drweb Backup.`



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



Fichiers de configuration principaux

Fichier	Description	Répertoire par défaut
agent.key (le nom peut varier)	clé de licence de l'Agent Dr.Web	etc
certificate.pem	certificat SSL	
database.conf	modèle de configuration de la base de données avec les paramètres par défaut	
download.conf	paramètres réseau pour la génération des packages d'installation de l'Agent Dr.Web	
drwcsd.conf (le nom peut varier)	fichier de configuration du Serveur Dr.Web	
drwcsd.conf.distr	modèle du fichier de configuration du Serveur Dr.Web avec les paramètres par défaut	
drwcsd.pri	clé privée de chiffrement	
enterprise.key (le nom peut varier)	clé de licence du Serveur Dr.Web. La clé est sauvegardé uniquement si elle est présente après la mise à niveau depuis des versions antérieures. Elle n'est pas présente en cas d'installation du nouveau Serveur Dr.Web 13.0	
frontdoor.conf	fichier de configuration pour l'utilitaire du diagnostic distant du Serveur Dr.Web	
http-alerter-certs.pem	certificats pour la vérification de l'hôte <code>apple-notify.drweb.com</code> pour l'envoi de notifications push	
private-key.pem	clé privée RSA	
yalocator.apikey	Clé API pour l'extension Yandex Locator	
webmin.conf	fichier de configuration du Centre de gestion	
auth-ads.conf	fichier de configuration pour l'authentification externe des administrateurs via Active Directory	
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	





Fichier	Description	Répertoire par défaut
	simplifié	
auth-radius.conf	fichier de configuration pour l'authentification externe des administrateurs via RADIUS	
database.sqlite	BD embarquée	var
*.pub	clé publique de chiffrement	section Administration → Clés de chiffrement dans le Centre de gestion

Démarrage et arrêt du Serveur Dr.Web

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

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

- Cas général :
 - Avec la commande correspondante se trouvant dans le menu **Démarrer** → **Tous les programmes** → **Dr.Web Server**.
 - Avec les outils de gestion des services depuis la rubrique **Outils d'administration** dans le **Panneau de configuration** Windows.
- Arrêt et redémarrage via le Centre de gestion :
 - Dans la section **Administration** : le redémarrage avec le bouton , l'arrêt avec le bouton .
- Avec les commandes de console exécutées depuis le sous-répertoire `bin` du répertoire d'installation du Serveur Dr.Web (voir aussi les **Annexes**, p. [G3. Serveur Dr.Web](#)) :
 - `drwcsd start` : démarrage du Serveur Dr.Web.
 - `drwcsd restart` : redémarrage complet du service du Serveur Dr.Web.
 - `drwcsd stop` : arrêt normal du Serveur Dr.Web.



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



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

Interface et gestion du Serveur Dr.Web

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

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

`/opt/drwcs/` sous Linux et `/usr/local/drwcs` sous FreeBSD :

- `bin` : fichiers exécutables du Serveur Dr.Web.
- `doc` : fichiers de contrats de licence.
- `ds-modules` : modules script déballés.
- `fonts` : polices pour les documents PDF.
- `lib` : jeu de bibliothèques pour le fonctionnement du Serveur Dr.Web.
- `vfs` : modules script et paquets de langue emballés.
- `webmin` : éléments du Centre de gestion.
- `websockets` : scripts pour la gestion des sockets web.

`/var/opt/drwcs/` sous Linux et `/var/drwcs` sous FreeBSD :

- `backup` : copies de sauvegarde de la BD et d'autres données critiques.
- `coredump` : les dumps de crash du Serveur Dr.Web. Créé lors de l'apparition des dumps.
- `etc` : fichiers de configuration principaux des composants du réseau antivirus.
- `extensions` : scripts utilisateur destinés à automatiser l'exécution de certaines tâches.
- `installers-cache` : cache de sauvegarde des packages d'installation de groupe et personnels de l'Agent Dr.Web lors de la création des postes dans le Centre de gestion. Il est créé en cas de création des paquets d'installation.
- `file-cache` : cache de fichiers.
- `log` : fichiers de journal du Serveur Dr.Web.
- `plugins` : objets temporaires des plug-ins.
- `object` : cache des objets du Centre de gestion.
- `reports` : répertoire temporaire pour la création et la sauvegarde des rapports. Il est créé en cas de nécessité.
- `repository` : répertoire des mises à jour dans lequel sont placées les mises à jour actuelles des bases virales, des fichiers des packages antivirus et des fichiers des composants du réseau antivirus. Le répertoire comprend des sous-répertoires pour certains composants du logiciel et ces sous-répertoires à leur tour contiennent des sous-répertoires appropriés aux OS respectifs. Ce répertoire doit être accessible en écriture à



l'utilisateur sous le nom duquel le Serveur Dr.Web démarre (d'habitude, c'est l'utilisateur **drwcs**).

- `run` : ID du processus du Serveur Dr.Web.
- `sessions` : sessions du Centre de gestion.
- `tmp` : fichiers temporaires.
- `twin-cache` : bases virales déballées pour la rétrocompatibilité avec les versions précédentes des Agents Dr.Web. Peut contenir également les autres fichiers déballés du référentiel, par exemple, l'installateur de l'Agent Dr.Web.
- `upload` : dossier pour télécharger les fichiers temporaires spécifiés via le Centre de gestion. Il est créé lors du téléchargement de fichiers de grande taille.

`/etc/opt/drweb.com/` pour Linux et `/usr/local/etc/drweb.com` pour FreeBSD :

- `software/drweb-suite.remove` : script pour la suppression du Serveur Dr.Web.
- des fichiers et des répertoires supplémentaires sont possibles.

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

- `drwcsd` : script pour le démarrage et l'arrêt du Serveur Dr.Web.

`/var/tmp/drwcs` : copie de sauvegarde après la suppression du Serveur Dr.Web.

Fichiers de configuration principaux

Fichier	Description	Répertoire par défaut
<code>agent.key</code> (le nom peut varier)	clé de licence de l'Agent Dr.Web	<ul style="list-style-type: none">• sous Linux : <code>/var/opt/drwcs/etc</code>• sous FreeBSD : <code>/var/drwcs/etc</code>
<code>certificate.pem</code>	certificat SSL	
<code>common.conf</code>	fichier de configuration (pour les OS de la famille UNIX)	
<code>database.conf</code>	modèle de configuration de la base de données avec les paramètres par défaut	
<code>download.conf</code>	paramètres réseau pour la génération des packages d'installation de l'Agent Dr.Web	
<code>drwcsd.conf</code> (le nom peut varier)	fichier de configuration du Serveur Dr.Web	
<code>drwcsd.conf.distr</code>	modèle du fichier de configuration du Serveur Dr.Web avec les paramètres par défaut	
<code>drwcsd.pri</code>	clé privée de chiffrement	



Fichier	Description	Répertoire par défaut
<code>enterprise.key</code> (le nom peut varier)	clé de licence du Serveur Dr.Web. 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 Dr.Web 13.0	
<code>frontdoor.conf</code>	fichier de configuration pour l'utilitaire du diagnostic distant du Serveur Dr.Web	
<code>http-alerter-certs.pem</code>	certificats pour la vérification de l'hôte <code>apple-notify.drweb.com</code> pour l'envoi de notifications push	
<code>private-key.pem</code>	clé privée RSA	
<code>yalocator.apkey</code>	Clé API pour l'extension Yandex Locator	
<code>webmin.conf</code>	fichier de configuration du Centre de gestion	
<code>auth-ldap.conf</code>	fichier de configuration pour l'authentification externe des administrateurs via LDAP	
<code>auth-ldap-rfc4515.conf</code>	fichier de configuration pour l'authentification externe des administrateurs via LDAP selon le schéma simplifié	
<code>auth-pam.conf</code>	fichier de configuration pour l'authentification externe des administrateurs via PAM	
<code>auth-radius.conf</code>	fichier de configuration pour l'authentification externe des administrateurs via RADIUS	
<code>database.sqlite</code>	BD embarquée	<ul style="list-style-type: none">• sous Linux : <code>/var/opt/drwcs</code>• sous FreeBSD : <code>/var/drwcs</code>
<code>*.pub</code>	clé publique de chiffrement	section Administration → Clés de chiffrement dans le Centre de gestion

Démarrage et arrêt du Serveur Dr.Web

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



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

- Arrêt et redémarrage via le Centre de gestion :
 - Dans la section **Administration** : le redémarrage avec le bouton , l'arrêt avec le bouton .
- Avec la commande de console (voir aussi le document **Annexes**, [G3. Serveur Dr.Web](#)) :
 - Démarrage :
 - sous FreeBSD :

```
# /usr/local/etc/rc.d/drwcsd start
```
 - sous Linux :

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

```
# /usr/local/etc/rc.d/drwcsd restart
```
 - sous Linux :

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

```
# /usr/local/etc/rc.d/drwcsd stop
```
 - Sous Linux :

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



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

5.2. Protection de postes de travail



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

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

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

Les packages antivirus sont installés sur les postes protégés et sont connectés au Serveur Dr.Web. Chaque poste fait partie d'un ou de plusieurs groupes enregistrés sur ce Serveur Dr.Web (pour en savoir plus, consultez le paragraphe [Groupes système et groupes utilisateur](#)).



Les échanges d'information entre le poste et le Serveur Dr.Web sont effectués via le protocole utilisé dans le réseau local (TCP/IP en version 4 ou 6).

Installation

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

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



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

Gestion

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

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

Mise à jour

Serveur Dr.Web télécharge les mises à jour et les diffuse sur les postes connectés. Cela permet d'installer de manière automatique, de maintenir et de gérer la meilleure stratégie de protection antivirus quel que soit le niveau de compétence des utilisateurs des postes.

Au cas où le poste est temporairement déconnecté du réseau antivirus, l'Antivirus sur le poste utilise une copie locale de la configuration et la protection antivirus sur le poste reste donc opérationnelle (durant une période inférieure ou égale à la durée de la licence de l'utilisateur), mais le logiciel ne sera pas mis à jour. Si le fonctionnement en *Mode mobile* est autorisé pour le poste, en cas de la perte de connexion au Serveur Dr.Web, la mise à jour des bases virales s'effectuera directement depuis les serveurs du SGM.



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

5.3. Centre de gestion de la sécurité Dr.Web

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



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

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

Connexion au Serveur Dr.Web

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

`http://<Adresse_du_Serveur_Dr.Web>:9080`

ou

`https://<Adresse_du_Serveur_Dr.Web>:9081`

où comme valeur `<Adresse_du_Serveur_Dr.Web>` 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 Dr.Web.
 - pour les OS de la famille UNIX — mot de passe qui a été automatiquement créé au cours de l'installation du Serveur Dr.Web (voir aussi le **Manuel d'installation**, [Installation du Serveur Dr.Web pour les OS de la famille UNIX](#)).



Vous pouvez récupérer le mot de passe oublié, voir le p. [Récupération du mot de passe de l'administrateur](#).



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



Sous certaines versions de navigateurs web, par exemple **Firefox 3** ou supérieur, une erreur survient lors du téléchargement via HTTPS et le Centre de gestion ne sera pas téléchargé. Dans ce cas-là, il est nécessaire de sélectionner l'élément **Ajouter le site dans la liste des exclusions** (au-dessous de la notification d'erreur). Alors, l'accès au Centre de gestion sera autorisé.

Interface du Centre de gestion de la sécurité Dr.Web

Le fenêtre du Centre de gestion (voir [5-1](#)) comprend deux zones : *l'en-tête du menu principal* et *la zone de travail*.

Menu principal

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

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

Zone de travail

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

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

La langue d'interface doit être définie séparément pour chaque compte administrateur (voir le p. [Création et suppression des comptes et des groupes administrateur](#)).

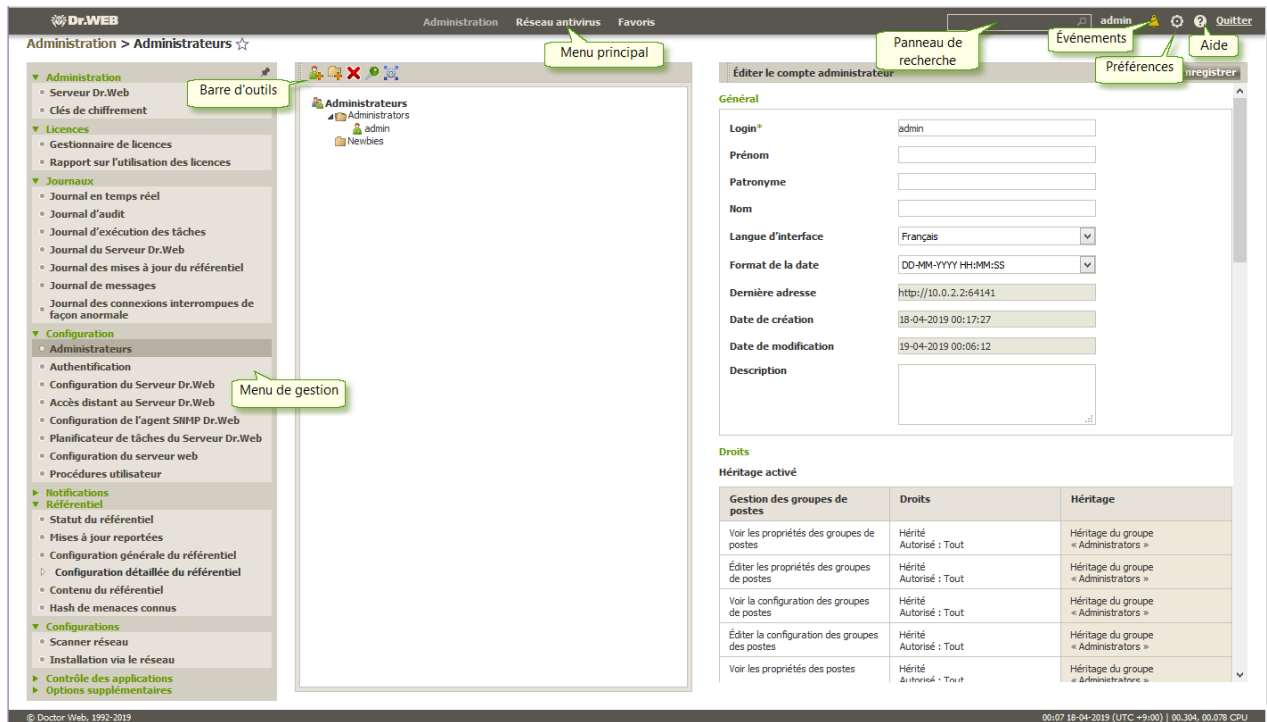


Figure 5-1. Fenêtre du Centre de gestion Dr.Web. Cliquez sur les éléments dans le cadre vert pour ouvrir la section correspondante

Menu de gestion

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

Le menu de gestion peut être réduit. Dans ce cas, seuls les noms des sections sont affichés. Si vous placez le curseur sur une section, les éléments du menu disponibles dans cette section s'affichent.

Pour configurer l'affichage du menu de gestion, utilisez les icônes dans le coin droit supérieur :

- Enlever le menu** : enlever la fixation et afficher le menu réduit.
- Fixer le menu** : fixer le menu en position déroulée.

Menu des liaisons voisines





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



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

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

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

- Le Centre de gestion du Serveur Dr.Web lié va s'ouvrir, si l'adresse IP du Centre de gestion a été indiquée lors de la configuration de la liaison.
L'action est similaire à celle du bouton  →  dans la barre d'outils lors de la gestion des liaisons.
- Si l'adresse du Centre de gestion du Serveur voisin Dr.Web n'est pas spécifiée pour cette liaison, la rubrique de configuration des liaisons va s'afficher pour que vous puissiez spécifier l'adresse IP.

5.3.1. Administration



Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion.

Menu de gestion

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

Le menu de gestion comprend les éléments suivants :

1. Administration

- **Serveur Dr.Web** : cet élément ouvre le panneau permettant de consulter les informations principales sur le Serveur Dr.Web, il permet également de redémarrer le serveur avec le bouton  ou de l'arrêter avec le bouton  se trouvant en haut dans la partie droite du panneau. En cas de disponibilité des mises à jour du Serveur Dr.Web téléchargées, vous pouvez accéder depuis cette section à la section [Mises à jour du Serveur Dr.Web](#) contenant la liste de versions du Serveur Dr.Web pour la mise à jour et la copie de sauvegarde. Pour restaurer l'intégrité du Serveur Dr.Web et revenir à l'état de la révision actuelle, cliquez sur **Restaurer le Serveur**.
- **Clés de chiffrement** : cet élément permet d'exporter (sauvegarder de manière locale) les clés de chiffrement publiques et privées, ainsi que le certificat du Serveur Dr.Web.

2. Licences

- [Gestionnaire de licences](#) : cet élément permet de gérer les fichiers clés de licence.



- [Rapport sur l'utilisation de licences](#) : contient les informations sur l'utilisation des licences, y compris les licences sur les Serveurs voisins Dr.Web.

3. Journaux

- [Journal en temps réel](#) : cet élément permet de consulter la liste des événements et des modifications liés au fonctionnement du Serveur Dr.Web, affichés en temps réel (juste au moment de l'événement).
- [Journal d'audit](#) : cet élément permet de consulter le journal des événements et des modifications effectuées via les sous-systèmes de gestion de Dr.Web Enterprise Security Suite.
- **Journal d'exécution des tâches** : cet élément comprend la liste des tâches du Serveur Dr.Web accompagnée de notes sur leur exécution ou de commentaires.
- [Journal du Serveur Dr.Web](#) : cet élément contient la liste des événements liés au fonctionnement du Serveur Dr.Web.
- [Journal des mises à jour du référentiel](#) : cet élément contient la liste de mises à jour depuis le SGM et les informations détaillées sur les révisions mises à jour de produits.
- [Journal des messages](#) : cet élément contient tous les messages qui ont été envoyés par l'administrateur sur les postes du réseau antivirus.
- **Journal des connexions interrompues de façon anormale** : cet élément contient tous les cas d'interruptions de connexions du Serveur Dr.Web aux clients : postes, installateurs des Agents Dr.Web, Serveurs voisins Dr.Web, Serveurs proxy.

4. Configuration


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



5. Notifications

- [Notification de la console web](#) : cet élément permet de consulter et gérer les notifications de l'administrateur reçues par le moyen de la **Console Web**.
- [Notifications non envoyées](#) : cet élément permet de suivre et gérer les notifications de l'administrateur dont l'envoi a échoué conformément aux paramètres de la rubrique **Configuration des notifications**.
- [Configuration des notifications](#) : cet élément permet de configurer les notifications de l'administrateur sur les événements du réseau antivirus.
- [Modèles de messages](#) : liste de modèles de messages texte aléatoires envoyés par l'administrateur sur les postes du réseau antivirus.

6. Référentiel

- [Statut du référentiel](#) : cet élément permet de contrôler le statut du référentiel : date de la dernière mise à jour des composants du référentiel et leur statut, ainsi que de mettre à jour le référentiel depuis le SGM.
- [Mises à jour reportées](#) : cet élément contient la liste des produits temporairement exclus des mises à jour dans la rubrique **Configuration détaillée du référentiel**.
- [Configuration générale du référentiel](#) : cet élément ouvre la fenêtre de configuration des paramètres de connexion au SGM et des mises à jour du référentiel pour tous les produits.
- [Configuration détaillée du référentiel](#) : cet élément permet de définir la configuration des révisions pour chaque référentiel de produit séparément.
- [Contenu du référentiel](#) : cet élément permet de consulter et de gérer le contenu actuel du référentiel au niveau de répertoires et de fichiers du référentiel.
- **Hashs de menaces connus** : permet d'effectuer la recherche par les bulletins avec les hashs de menaces connus. Pour la recherche par les marges du tableau de hashs, cliquez sur .
La section est disponible uniquement si les bulletins de hashs de menaces connus sont utilisés sous licence. La disponibilité de la licence est indiquée dans les informations sur la clé de licence que vous pouvez consulter dans la section [Gestionnaire de licences](#), le paramètre **Listes autorisées de bulletins de hashs** (il suffit d'avoir une seule licence dans une clé de licence utilisée par le Serveur Dr.Web).

7. Installations

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



8. Contrôle des applications

- [Applications de confiance](#) : liste des applications dont le lancement est toujours autorisé sur les postes avec le composant Contrôle des applications installé (les listes autorisées sont sélectionnées dans les paramètres du [profil](#) spécifié sur le poste).
- [Répertoire d'applications](#) : liste de toutes les applications installées sur les postes.

9. Options supplémentaires

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



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

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

- [Copies de sauvegarde](#) : cet élément permet de consulter et sauvegarder le contenu de copies de sauvegarde des données critiques du Serveur Dr.Web.
- [Utilitaires](#) : cet élément ouvre la rubrique de téléchargement d'utilitaires supplémentaires nécessaires pour le fonctionnement de Dr.Web Enterprise Security Suite.

5.3.2. Réseau antivirus

Dans le menu principal du Centre de gestion, sélectionnez l'élément **Réseau antivirus**.

Menu de gestion

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

Le menu de gestion comprend les éléments suivants :

1. Général

- [Graphiques](#)
- [Identificateurs de sécurité](#)



- [Composants de protection](#)
 - [Quarantaine](#)
 - [Matériel et logiciels](#)
 - **Périphériques détectés**
 - **Sessions d'utilisateurs**
 - **Postes inactifs**
 - [Propriétés](#)
 - [Règles d'appartenance au groupe](#) (lors de la sélection d'un groupe utilisateur)
 - [Serveur proxy Dr.Web](#) (en cas de sélection de Serveurs proxy ou de leur groupe)
2. [Statistiques](#)
3. **Configuration**
- [Serveur proxy Dr.Web](#) (en cas de sélection du Serveur Proxy ou du groupe **Proxies** et de ses sous-groupes)
 - [Droits](#)
 - [Planificateur des tâches](#)
 - [Composants à installer](#)
 - [Paramètres de connexion](#)
 - [Restrictions de mises à jour](#)
 - **Agent Dr.Web pour UNIX** permet de configurer la périodicité d'envoi des statistiques sur les menaces détectées pour le poste tournant sous l'OS de la famille UNIX.
 - Liste des composants antivirus pour l'OS des postes sélectionnés ou par liste d'OS lors de la sélection d'un groupe.



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

Liste hiérarchique (arborescence) du réseau antivirus

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

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

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



- cliquer sur l'icône d'un poste pour ouvrir la fiche des propriétés de ce poste.
















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

L'apparence de l'icône dépend du type et du statut de l'élément (voir le [tableau 5-1](#)).

Tableau 5-1. Icônes des éléments de la liste hiérarchique

Icône	Description
Groupes. Icônes générales	
	Groupes toujours apparents dans la liste hiérarchique.
	Les groupes ne sont pas affichés dans la liste hiérarchique si : <ul style="list-style-type: none">• pour les groupes, l'option Configurer la visibilité du groupe → Masquer si vide est activée et que les groupes ne contiennent pas de postes,• pour les groupes, l'option Configurer la visibilité du groupe → Masquer est activée et que, dans la section Paramètres de l'affichage l'arborescence, la case Afficher les groupes masqués n'est pas cochée.
	L'icône des règles d'appartenance s'affiche près de l'icône principale des groupes utilisateurs pour lesquels les règles de placement automatique de postes dans le groupe sont définies. Pour afficher l'icône, sélectionnez dans la barre d'outils l'option Paramètres d'affichage de l'arborescence → Afficher l'icône des règles d'appartenance .
Postes de travail. Icônes générales	
	Postes de travail disponibles avec l'antivirus installé.
	Poste disponible avec l'antivirus installé. L'importance de l'état du poste Moyenne . Pour déterminer les actions nécessaires à effectuer du côté de l'administrateur, précisez la situation sur ce poste dans la section Statut . Pour afficher l'icône, sélectionnez ans la barre d'outils l'option Paramètres d'affichage de l'arborescence → Afficher l'icône des paramètres personnalisés .
	Poste disponible avec l'antivirus installé. L'importance de l'état du poste Maximale ou Haute . Pour déterminer les actions nécessaires à effectuer du côté de l'administrateur, précisez la situation sur ce poste dans la section Statut . Pour afficher l'icône, sélectionnez ans la barre d'outils l'option Paramètres d'affichage de l'arborescence → Afficher l'icône des paramètres personnalisés .
	Le poste est indisponible.
	Le logiciel antivirus est désinstallé sur le poste.



Icône	Description
	Statut du poste lors de l'installation de l'Agent Dr.Web à distance. Le poste a ce statut depuis l'installation réussie de l'Agent Dr.Web sur le poste jusqu'à la première connexion au Serveur Dr.Web.
Serveurs proxy. Icônes principales	
	Serveur proxy non connecté à votre Serveur Dr.Web.
	Le Serveur proxy est connecté à votre Serveur Dr.Web, mais il n'utilise pas les paramètres spécifiés.
	Le Serveur proxy est connecté à votre Serveur Dr.Web et utilise les paramètres spécifiés.
Serveur de scan. Icônes principales	
	Serveur de scan disponible
	Serveur de scan disponible. Importance de l'état Moyenne . Pour déterminer les actions nécessaires à effectuer du côté de l'administrateur, précisez la situation sur ce Serveur de scan dans la section Statut . Pour afficher l'icône, sélectionnez ans la barre d'outils l'option  Paramètres d'affichage de l'arborescence → Afficher l'icône des paramètres personnalisés .
	Serveur de scan disponible. Importance de l'état Maximale ou Haute . Pour déterminer les actions nécessaires à effectuer du côté de l'administrateur, précisez la situation sur ce Serveur de scan dans la section Statut . Pour afficher l'icône, sélectionnez ans la barre d'outils l'option  Paramètres d'affichage de l'arborescence → Afficher l'icône des paramètres personnalisés .
	Le Serveur de scan Dr.Web n'est pas disponible.
Icônes supplémentaires pour les groupes, les postes, les Serveurs proxy et les Serveurs de scan	
	L'icône des paramètres personnels s'affiche sur les icônes principales des postes, des groupes et des Serveurs proxy et des Serveurs de scan pour lesquels les paramètres personnels sont spécifiés. Pour afficher l'icône, sélectionnez dans la barre d'outils l'option  Paramètres d'affichage de l'arborescence → Afficher l'icône des paramètres personnalisés . Par exemple, si les paramètres personnalisés sont spécifiés pour un poste en ligne avec l'antivirus installé, son icône est la suivante :  .
Politiques	
	Politique ou version de la politique avec les paramètres des composants antivirus des postes. Pour afficher l'icône, sélectionnez dans la barre d'outils l'option  Paramètres d'affichage de l'arborescence → Afficher l'icône de la politique .




Icône	Description
Profils	
	Profil de sauvegarde des paramètres du composant Contrôle des applications, mode actif.
	Profil de sauvegarde des paramètres du composant Contrôle des applications, mode test.
	Profil désactivé de sauvegarde des paramètres du composant Contrôle des applications.
	Profil de sauvegarde des paramètres du composant Contrôle des applications pour lequel est spécifié un groupe d'applications de confiance manquant dans le référentiel du Serveur Dr.Web.

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


Barre d'outils

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


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


 **Supprimer les objets sélectionnés** : supprimer les éléments de la liste hiérarchique. Sélectionnez un ou plusieurs éléments dans la liste et cliquez sur **Supprimer les objets sélectionnés**.

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


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

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


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


 **Supprimer les paramètres personnalisés** : supprimer les paramètres personnalisés de l'objet sélectionné sans la liste. Dans ce cas, les paramètres seront hérités du groupe primaire. Si un groupe est sélectionné dans la liste hiérarchique, les paramètres de tous les postes appartenant à ce groupe seront également supprimés.


 **Envoyer un messages aux postes** : envoyer un message aléatoire aux utilisateurs.


 **Redémarrer le poste** : effectuer le redémarrage du poste à distance. Dans la section [Statut](#), vous pouvez préciser si le redémarrage du poste est requis, par exemple, à la suite d'une mise à jour ou d'une modification des composants antivirus.





 **Désinstaller l'Agent Dr.Web** : supprimer l'Agent Dr.Web et le logiciel antivirus sur le poste ou le groupe de postes sélectionné.

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


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


 **Envoyer les fichiers d'installation** : envoyer les fichiers d'installation pour les postes sélectionnés dans la liste, sur les adresses e-mail spécifiées dans les paramètres de cette section.

 **Annuler l'assignation du profil aux objets** : supprimer le profil de la liste des profils assignés aux objets sélectionnés. L'élément est actif lors de la sélection des objets auxquels le profil est assigné (ils s'affichent dans l'arborescence en tant qu'objets emboîtés pour ce profil).

 **Créer un rapport pour le support technique** : créer un rapport du support technique contenant les informations système pour un poste ou un groupe de postes.


+ Ajouter un objet de réseau : créer un nouvel élément du réseau antivirus. Pour cela, sélectionnez un élément dans la liste déroulante :


 **Créer un poste** : créer un nouveau poste (voir le **Manuel d'installation**, le p. [Installation de l'Agent Dr.Web avec le package d'installation personnel](#)).

 **Créer un groupe** : créer un nouveau groupe de postes.

 **Créer une liaison** : créer une liaison avec le Serveur voisin Dr.Web.

 **Créer une politique** : créer une nouvelle politique pour spécifier les paramètres des postes.

 **Créer un Serveur proxy** : créer un nouveau compte pour la connexion du Serveur proxy (voir le **Manuel d'installation**, le p. [Création du compte du Serveur proxy Dr.Web](#)).


 **Créer un profil** : créer un profil pour la sauvegarde des paramètres des composants antivirus des postes.

 **Données et configuration** :

 **Enregistrer les données dans un fichier CSV** : enregistrer au format CSV les informations générales sur les postes sélectionnées du réseau antivirus.

 **Enregistrer les données dans un fichier HTML** : enregistrer au format HTML les informations générales sur les postes sélectionnées du réseau antivirus.

 **Enregistrer les données dans un fichier XML** : enregistrer au format XML les informations générales sur les postes sélectionnées du réseau antivirus.

 **Enregistrer les données dans un fichier PDF** : enregistrer au format PDF les informations générales sur les postes sélectionnées du réseau antivirus.



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



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



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



Exporter la configuration : enregistrer dans un fichier les statistiques de fonctionnement des composants antivirus pour les objets sélectionnés du réseau antivirus. Pour cette option, vous serez invité à sélectionner les sections de statistiques à enregistrer et le format d'exportation.



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



Assigner la politique : assigner la politique sélectionnée à un groupe ou à postes séparées. Pour cette option, il vous sera proposé de sélectionner les objets auxquels la politiques peut être assignée.



Assigner le profil : assigner le profil sélectionné dans l'arborescence du réseau antivirus aux objets : postes, utilisateurs et groupes. Pour cette option, vous serez invité à sélectionner les objets auxquels le profil sera assigné.

Paramétrer l'affichage du groupe. Cet élément permet de modifier les paramètres d'affichage des groupes. Pour cela, sélectionnez un groupe dans l'arborescence et, dans la liste déroulante, spécifiez une des variantes suivantes (l'icône du groupe va changer d'apparence, voir [le tableau 5-1](#)) :



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



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



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

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



Restaurer les composants échoués : forcer la restauration des composants fonctionnant avec des erreurs. C'est la révision installée en ce moment sur le poste qui est restaurée.




Interrompre les composants lancés : arrêter tous les composants antivirus lancés sur le poste. Vous pouvez arrêter et lancer les composants séparément dans la section [Composants de protection](#).





 **Scanner** : cet élément permet de scanner les postes dans un des modes sélectionnés dans la liste déroulante :

 **Scan rapide**. Ce mode prévoit l'analyse des objets suivants par le Scanner Dr.Web Agent :

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

 **Scan complet**. Ce mode assure l'analyse complète de tous les disques durs ainsi que des supports amovibles (y compris les secteurs d'amorçage) par le Scanner Dr.Web Agent.


 **Scan personnalisé**. Ce mode permet de choisir les dossiers et les fichiers à analyser par le Scanner Dr.Web Agent.


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


 **Approuver les postes sélectionnés et définir le groupe primaire** : approuver l'accès du poste au Serveur Dr.Web et spécifier le groupe primaire de la liste proposée.

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

 **Rejeter les postes sélectionnés** : refuser l'accès des postes au Serveur Dr.Web.

 **Paramètres de blocage**. Cet élément permet de modifier les paramètres d'accès des postes au Serveur Dr.Web. Sélectionnez un paramètre

 **Période de blocage** : spécifier une plage de date durant laquelle le poste ne sera pas autorisé à se connecter au Serveur Dr.Web.

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

- pour les groupes :
 - **Appartenance à tous les groupes** : dupliquer l'affichage du poste dans la liste s'il appartient à plusieurs groupes en même temps (uniquement pour les groupes accompagnés de l'image du dossier blanc – voir le [tableau 5-1](#)). Si la case est cochée,






toutes les appartenances seront affichées. Sinon le poste sera affiché dans la liste une seule fois.

- **Afficher les groupes masqués** : afficher tous les groupes faisant partie du réseau antivirus. Si la case est décochée, tous les groupes vides (ceux qui ne contiennent pas de postes) seront masqués. Ceci peut être pratique pour éviter d'afficher trop d'informations, par exemple en cas de nombreux groupes vides.
- **Afficher les groupes avec des postes activés uniquement** : n'afficher que les groupes avec les postes qui au moins une fois se sont connectés au Serveur Dr.Web.
- pour les clients du Serveur Dr.Web (postes, Serveurs proxy et Serveurs voisins Dr.Web) :
 - **Afficher les identifiants de clients** : afficher les identifiants uniques des clients du Serveur Dr.Web.
 - **Afficher les noms de clients** : afficher les noms des clients du Serveur Dr.Web, s'il sont disponibles.



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

- **Afficher les adresses de clients** : afficher les adresses IP de clients du Serveur Dr.Web.
- **Afficher les serveurs de postes** : afficher les noms ou les adresses IP des Serveurs Dr.Web auxquels les postes sont connectés. Cela concerne les postes inclus dans le cluster des Serveurs Dr.Web.
- **Afficher l'icône de la politique** : afficher l'icône de la politique à côté de l'icône du poste auquel la politique est assignée.
- **Afficher la gravité de l'état de postes** : afficher la gravité de statut pour les postes actifs. Dans ce cas, une gradation de couleur s'ajoute pour les postes en fonction de leurs statuts (voir le [tableau 5-1](#)). Si l'option est désactivée, une icône commune  sera affichée pour le poste dont les statuts correspondent aux icônes  et .
- **Afficher les postes bloqués** : afficher les postes dont l'accès au Serveur Dr.Web est bloqué.
- pour tous les éléments :
 - **Afficher les configurations personnalisées** : afficher le marqueur indiquant la configuration personnalisée sur les icônes des groupes et des clients de Serveur Dr.Web : postes, Serveurs proxy et Serveurs voisins Dr.Web.
 - **Afficher les descriptions** : afficher les descriptions des clients de Serveurs Dr.Web : postes, Serveurs proxy et Serveurs voisins Dr.Web (les descriptions sont spécifiées dans les propriétés de l'élément).
 - **Afficher le nombre de clients** : afficher le nombre de clients de Serveur Dr.Web : des postes, des Serveurs proxy et des Serveurs voisins Dr.Web pour tous les groupes du réseau antivirus dont ces clients font partie.
 - **Afficher l'icône des règles d'appartenance** : afficher le marqueur sur les icônes des postes qui sont ajoutés automatiquement aux groupes d'après les règles



d'appartenance, ainsi que sur les icônes des groupes dans lesquels les postes sont ajoutés automatiquement.

Paramètres de filtrage : permet de filtrer les éléments affichés de l'arborescence du réseau antivirus grâce à la recherche par les paramètres indiqués. Pour spécifier un critère de recherche, cochez les cases contre les critères nécessaires dans la liste déroulante. Dans le champ **Recherche**, saisissez la ligne de recherche. Cliquez sur **Appliquer** pour commencer la recherche par les paramètres spécifiés.

Les critères de recherche sont équivalents aux critères décrits dans la rubrique [Barre de recherche](#), sauf le critère particulier **Configuration**. Ce critère sert à rechercher les postes par les paramètres particuliers des composants antivirus installés sur les postes. Lorsque vous sélectionnez cette option, un panneau de recherche contenant les paramètres suivants s'ouvre :

- **Composant** : dans la liste déroulante sélectionnez le nom du composant antivirus dans les paramètres duquel il faut effectuer la recherche. Pour faciliter la sélection du composant dans la liste, vous pouvez utiliser la recherche : commencez à saisir dans le champ le nom du composant, le système vous proposera automatiquement les variantes contenant les caractères entrés.
- **Paramètre** : dans la liste déroulante sélectionnez le nom du paramètre par les valeurs duquel on peut effectuer la recherche. La recherche par les paramètres ayant une structure complexe des valeurs possibles n'est pas disponible.
- **Valeur** : spécifiez la valeur du paramètre sélectionné ci-dessus. En fonction des valeurs possibles de chaque paramètre, une liste déroulante ou un champ de saisie s'affiche.

Pour réinitialiser les paramètres de recherche, cliquez sur le bouton **Par défaut**.

Paramètres de tri des clients : modifier le paramètre de tri et l'ordre de tri des clients du Serveur Dr.Web : postes, Serveurs proxy et Serveurs voisins Dr.Web dans l'arborescence du réseau antivirus.

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



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

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

Panneau des propriétés

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

Pour afficher le panneau des propriétés

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



Lorsque vous sélectionnez **Réseau antivirus** dans l'arborescence, le panneau de propriétés affichera les informations sur les groupes et les postes du réseau antivirus, ainsi que les informations sur les licences disponibles.


5.3.3. Favoris

Le Centre de gestion permet d'enregistrer les pages de l'interface comme favoris pour faciliter la gestion. Par exemple, pour passer rapidement sur les pages les plus visitées du Centre de gestion.



Gérer la liste des favoris

1. Dans le menu principal du Centre de gestion, sélectionnez l'élément **Favoris**.
2. La liste des favoris du Centre de gestion va s'ouvrir.
3. Cliquez sur **Éditer**.
4. Depuis la liste des favoris, vous pouvez :
 - Ouvrir la page mise en favoris. Pour ce faire, dans la liste des favoris, cliquez sur le signet correspondant à cette page.





- Modifier l'ordre de tri des signets. Pour ce faire, cliquez sur l'icône  à gauche du signet et déplacez le signet plus haut ou plus bas.
- Supprimer tous les signets de la liste des favoris. Pour ce faire, sélectionnez le signet à supprimer ou tous les signets. Cliquez sur **Supprimer**, ensuite cliquez sur **Enregistrer**.

Ajouter un favori

1. Ouvrez la page du Centre de gestion que vous voulez ajouter aux favoris.
2. Cliquez sur l'icône  contre le nom de la page au-dessus du menu de gestion.
3. La fenêtre **Ajouter aux favoris** va s'ouvrir. Le nom de la page au format *<Élément du menu principal>* > *<Élément du menu de gestion>* est ajouté automatiquement dans le champ **Nom**. Si nécessaire, vous pouvez modifier le nom du favori.
4. Les actions suivantes sont disponibles :
 - Pour mettre la page en favoris, cliquez sur **Ajouter**. L'icône contre le nom de la page sera remplacée par l'icône .
 - Pour fermer la fenêtre sans modifier la liste de favoris, cliquez sur **Annuler**.

Édition et suppression de favoris

1. Ouvrez la page du Centre de gestion que vous voulez éditer ou supprimer des favoris.
2. Cliquez sur l'icône  contre le nom de la page au-dessus du menu de gestion.
3. La fenêtre **Édition du signet** va s'ouvrir. Les actions suivantes sont disponibles :
 - Pour éditer un signet, modifiez son nom dans le champ **Nom**. Cliquez sur **Actualiser** pour appliquer les modifications.
 - Pour supprimer la page de la liste de favoris, cliquez sur **Supprimer**. L'icône contre le nom de la page sera remplacée par l'icône .

5.3.4. Barre de recherche

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



Pour une recherche avancée par les paramètres, utilisez l'élément [Paramètres de filtrage](#) dans la barre d'outils de l'élément **Réseau antivirus**.

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

1. Dans la liste déroulante du panneau de recherche sélectionnez un critère de recherche :
 - **Poste** : pour rechercher les postes par leurs noms.
 - **Groupe** : pour rechercher les groupes par le nom.




- **ID du poste** : pour rechercher les postes par leurs identificateurs uniques.
- **ID du groupe** : pour rechercher les groupes par leurs identificateurs uniques.
- **Nom d'utilisateur** : pour rechercher les postes par le nom de l'utilisateur sur le poste.
- **Adresse IP** : pour rechercher les postes par l'adresse IP.
- **Adresse MAC** : pour rechercher les postes par l'adresse MAC.
- **Matériel** : pour rechercher les postes par le nom du hardware installé sur le poste ou par son producteur.
- **Logiciel** : pour rechercher les postes par le nom de software, installé sur le poste.
- **Description** : pour rechercher les postes et les groupes par leur description.

Pour commencer la recherche par les paramètres des composants, cliquez sur le bouton **Recherche**.

2. Entrez une ligne, conformément à laquelle la recherche sera effectuée. Dans ce cas, vous pouvez spécifier :
 - une ligne afin d'obtenir une coïncidence totale avec le paramètre de recherche,
 - un masque correspondant à la ligne recherchée : le symbole * est autorisé.
3. Pressez la touche ENTER pour commencer la recherche. L'arborescence du réseau antivirus va s'ouvrir.
4. Tous les éléments trouvés seront affichés dans l'arborescence du réseau antivirus conformément aux paramètres de recherche :
 - en cas de recherche d'un poste, toutes les appartenances à des groupes seront affichées,
 - dans le cas où aucun élément n'est trouvé, l'arborescence s'affichera vide et accompagnée du message suivant : **Rien n'est trouvé**.


5.3.5. Événements

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


L'état de l'icône peut varier :

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

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

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

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

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




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

Tableau 5-2. Liste des notifications possibles des événements sur le réseau antivirus

Événement	Importance	Rubrique du Centre de gestion	Description
Notifications sur les novices	mineure	Réseau antivirus Le groupe Newbies s'ouvre dans l'arborescence du réseau antivirus	De nouveaux postes se sont connectés au Serveur Dr.Web et attendent la confirmation d'accès par l'administrateur. Cela est possible dans le cas où la valeur Confirmation d'accès manuelle est spécifiée pour le paramètre Mode d'enregistrement de novices dans la configuration du Serveur Dr.Web .
Actualités non lues	mineure	 Support → Actualités	Les actualités non lues de Doctor Web sont disponibles.
Nouvelles notifications	mineure	Administration → Notifications de la console web	Les nouvelles notifications de l'administrateur reçues via la Console web sont disponibles.
Notifications critiques	majeure		
Les mises à jour du Serveur sont disponibles	majeure	Administration → Serveur Dr.Web	La mise à jour du Serveur Dr.Web est téléchargée dans le référentiel et elle est disponible pour l'installation.
La configuration du Serveur a été modifiée. Le redémarrage du Serveur est requis.	majeure	Administration → Configuration du Serveur Dr.Web	Les paramètres du fichier de configuration du Serveur Dr.Web ont été modifiés après le lancement du Serveur Dr.Web. Pour appliquer les nouveaux paramètres, veuillez redémarrer le Serveur Dr.Web.
La configuration du serveur web a été modifiée. Le redémarrage du Serveur est requis.	majeure	Administration → Configuration du serveur web	Les paramètres du fichier de configuration du serveur web ont été modifiés après le lancement du Serveur Dr.Web. Pour appliquer les nouveaux paramètres, veuillez redémarrer le Serveur Dr.Web.



5.3.6. Paramètres

Pour aller à la section des paramètres du Centre de gestion, cliquez sur  **Paramètres** dans le menu principal.



Tous les paramètres de cet onglet sont valables uniquement pour le compte administrateur courant.

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

- [Mon compte](#).
- [Interface](#).
- [Abonnement](#).

Mon compte

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

Général



Les valeurs des champs marqués par le symbole * doivent être obligatoirement spécifiées.

Si nécessaire, éditer les paramètres suivants :


- **Login*** de l'administrateur : login requis pour accéder au Centre de gestion.
- Nom, prénom et patronyme de l'administrateur.
- **Adresse e-mail** liée au compte.
- **Langue d'interface** utilisée par cet administrateur.



Les textes de l'interface en langue sélectionnée seront mis à jour automatiquement, une fois les paramètres de l'administrateur enregistrés. De plus, les cases seront automatiquement cochées dans les sections **Administration** → **Configuration générale du référentiel** → **Serveur Dr.Web** → **Langues du Centre de gestion de la sécurité Dr.Web** et **Administration** → **Configuration générale du référentiel** → **Serveur Dr.Web** → **Documentation**.

- **Format de la date** utilisé par l'administrateur lors de l'édition des paramètres contenant des dates. Les formats suivants peuvent être sélectionnés :
 - européen : JJ-MM-AAAA HH:MM:SS



- américain : MM/JJ/AAAA HH:MM:SS
- **Fuseau horaire** : la date et l'heure des événements seront affichées dans le navigateur selon fuseau horaire sélectionné.
- **Description du compte**.
- Pour changer de mot de passe, cliquez sur  **Changer de mot de passe** dans la barre d'outils.

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

- **Identificateur** du compte d'administrateur.
- **Type d'authentification** pour ce compte (voir [Authentification des administrateurs](#)) :
 - **Interne** : basée sur les identifiants dans la base de données du Serveur Dr.Web.
 - **Externe** : via les systèmes externes.
- Date de la création du compte et date de la dernière modification de ses paramètres.
- **Dernière adresse** : cet élément affiche les adresses réseau de la dernière connexion sous le compte actuel.


Droits

Description des droits administrateur et leur édition à l'onglet [Éditer les comptes et les groupes administrateurs](#).

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

Interface

Configuration de l'arborescence

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




- pour les groupes :
 - **Appartenance à tous les groupes** : doubler l'affichage du poste dans la liste s'il appartient à plusieurs groupes en même temps (uniquement pour les groupes accompagnés de l'image du dossier blanc – voir le [tableau 5-1](#)). Si la case est cochée, toutes les appartenances seront affichées. Sinon le poste sera affiché dans la liste une seule fois.
 - **Afficher les groupes masqués** : afficher tous les groupes faisant partie du réseau antivirus. Si la case est décochée, tous les groupes vides (ceux qui ne contiennent pas de postes) seront masqués. Ceci peut être pratique pour éviter d'afficher trop d'informations, par exemple en cas de nombreux groupes vides.



- **Afficher les groupes avec des postes activés uniquement** : n'afficher que les groupes avec les postes qui au moins une fois se sont connectés au Serveur Dr.Web.
- pour les clients du Serveur Dr.Web (postes, Serveurs proxy Dr.Web et Serveurs voisins Dr.Web) :
 - **Afficher les identifiants de clients** : afficher les identifiants uniques des clients du Serveur Dr.Web.
 - **Afficher les noms de clients** : afficher les noms des clients du Serveur Dr.Web.




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

- **Afficher les adresses de clients** : afficher les adresses IP de clients du Serveur Dr.Web.
- **Afficher les serveurs de postes** : afficher les noms ou les adresses IP des Serveurs Dr.Web auxquels les postes sont connectés. Cela concerne les postes inclus dans le cluster des Serveurs Dr.Web.
- **Afficher la gravité de l'état de postes** : afficher la gravité de statut pour les postes actifs. Dans ce cas, une gradation de couleur s'ajoute pour les postes en fonction de leurs statuts (voir le [tableau 5-1](#)). Si l'option est désactivée, une icône commune  sera affichée pour un poste dont les statuts correspondent aux icônes  et .
- **Afficher l'icône de la politique** : afficher l'icône de la politique à côté de l'icône du poste auquel la politique est assignée.
- **Afficher les postes bloqués** : afficher les postes dont l'accès au Serveur Dr.Web est bloqué.
- pour tous les éléments :
 - **Afficher les configurations personnalisées** : afficher le marqueur indiquant la configuration personnalisée sur les icônes des groupes et des clients de Serveur Dr.Web : postes, Serveurs proxy Dr.Web et Serveurs voisins Dr.Web.
 - **Afficher les descriptions** : afficher les descriptions des clients de Serveurs Dr.Web : postes, Serveurs proxy Dr.Web et Serveurs voisins Dr.Web (les descriptions sont spécifiées dans les propriétés de l'élément).
 - **Afficher le nombre de clients** : afficher le nombre de clients de Serveur Dr.Web : des postes, des Serveurs proxy Dr.Web et des Serveurs voisins Dr.Web pour tous les groupes du réseau antivirus dont ces clients font partie.
 - **Afficher l'icône des règles d'appartenance** : afficher le marqueur sur les icônes des postes qui sont ajoutés automatiquement aux groupes d'après les règles d'appartenance, ainsi que sur les icônes des groupes dans lesquels les postes sont ajoutés automatiquement.



Paramètres de tri des clients

Les paramètres de cette sous-section permettent de modifier le paramètre de tri et l'ordre de tri des clients du Serveur Dr.Web : postes, Serveurs proxy Dr.Web et Serveurs voisins Dr.Web dans l'arborescence du réseau antivirus. Ces paramètres sont similaires aux paramètres se trouvant dans la barre d'outils de l'élément  **Paramètres de tri des clients** dans la section **Réseau antivirus** du menu principal :

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

Délai de temps

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

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

Lors de la première ouverture de la page, les statistiques seront affichées conformément au délai spécifié. Si nécessaire, vous pouvez le modifier directement depuis les rubriques de statistiques.
- Afin de conserver le dernier délai spécifié dans les rubriques de statistiques, cochez la case **Sauvegarder le dernier délai d'affichage des statistiques**.

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

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

Authentification

Dans la liste déroulante **Période d'inactivité autorisée**, sélectionnez un délai après lequel la session utilisateur du Centre de gestion sera automatiquement terminée dans le navigateur.



Export au format PDF

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

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

Rapports

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

- Dans le champ **Nombre de lignes par page**, indiquez le nombre maximum de lignes sur une page de rapport pour la visualisation par page des statistiques.
- Dans le champ **Nombre de caractères après la coupure des lignes trop longues**, vous pouvez spécifier le nombre maximum des caractères qui seront visibles après la coupure des lignes trop longues dans les tableaux de journaux et de notifications.
- Cochez la case **Afficher les graphiques** pour afficher les graphiques sur les pages de rapports statistiques. Si la case est décochée, la visualisation des graphiques est désactivée.

Abonnement


Dans cet onglet, vous pouvez configurer l'abonnement aux actualités de Doctor Web. Cochez les cases pour recevoir les actualités des catégories suivantes :





- **Mises à jour** : actualités sur les mises à jour des produits Dr.Web.
- **Offres** : actualités sur les offres publicitaires de la société Doctor Web.
- **Virus** : bilans mensuels de l'activité virale et actualités sur les plus importantes menaces et attaques .
- **Produits Dr.Web** : actualités sur les produits Dr.Web.
- **Dr.Web AV-Desk** : actualités sur le service Dr.Web AV-Desk.
- **Actualités d'entreprise** : actualités sur les événement de l'entreprise Doctor Web.

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




5.3.7. Aide

Pour obtenir de l'aide pendant l'utilisation de Dr.Web Enterprise Security Suite, cliquez sur le bouton  **Aide** du menu principal. Le menu contextuel contenant les éléments suivants va s'afficher :

-  **Documentation** : afficher la rubrique du manuel administrateur correspondant à la section du Centre de gestion où vous vous trouvez en ce moment. Si dans la documentation il n'y a pas la rubrique correspondante à la section actuelle du Centre de gestion, l'élément  **Documentation** ne s'affiche pas dans le menu contextuel de l'icône .
-  **Support** : ouvrir la section **Support** du Centre de gestion (voir ci-dessous).

Support

La section **Aide** contient les éléments suivants :

1. Lien vers les ressources auxiliaires
 - **Forum** : cet élément redirige vers le forum de Doctor Web.
 - **Actualités** : cet élément redirige vers la page d'actualités de Doctor Web.
 - **Contacteur le support technique** : cet élément redirige vers la page du Support technique de Doctor Web.
 - **Envoyer un fichier suspect** : cet élément ouvre un formulaire permettant d'envoyer un virus au Laboratoire de Doctor Web.
 - **Wikipédia Doctor Web** : cet élément redirige vers la page de la base de connaissance consacrée aux produits de Doctor Web.
 - **Signaler un faux positif dans Office Control** : cet élément ouvre un formulaire permettant d'envoyer un message sur une fausse alerte ou sur un problème de non détection dans le module de Office Control.
2. Section **Documentation**. Chaque document est disponible aux formats HTML et PDF à condition que la case correspondante soit cochée dans la section **Configuration générale du référentiel** → **Serveur Dr.Web** → [Documentation](#) pour la langue sélectionnée de l'interface du Centre de gestion et qu'il soit indiqué de mettre à jour la documentation au format PDF. Pour ouvrir un document au format HTML, cliquez sur le nom du manuel nécessaire. Vous pouvez ouvrir le même document au format PDF en cliquant sur l'icône  dans la colonne **Télécharger**. Pour plus de commodité, la documentation est divisée en quelques sous-rubriques :
 - **Installation et utilisation de Dr.Web Enterprise Security Suite (documentation d'administrateur)**

Les manuels de cette sous-rubrique donne une image complète de l'organisation du service Dr.Web Enterprise Security Suite. Dans les manuels groupés ici, vous pouvez trouver les informations sur le déploiement et la configuration de la protection antivirus complète et les particularités d'interaction avec des logiciels tiers ainsi que prendre



connaissance des dernières modifications de la version de Dr.Web Enterprise Security Suite installée sur votre ordinateur.

- **Gestion des postes protégés par Dr.Web Enterprise Security Suite (documentation d'administrateur)**

Ces manuels contiennent les informations sur la configuration et la gestion centralisée de différents produits de Doctor Web faisant partie du réseau antivirus Dr.Web Enterprise Security Suite.

- **Documentation d'utilisateur**

Cette documentation contient les informations détaillées sur l'installation et la configuration de différents produits de Doctor Web ainsi que les recommandations d'utilisation et de solution de problèmes courants que les utilisateurs rencontrent.



Quand vous téléchargez la documentation via le Centre mobile de gestion Dr.Web sur un appareil tournant sous Android, le document est automatiquement enregistré dans le dossier Téléchargements.

Si le Serveur Dr.Web fonctionne via le protocole HTTPS avec un certificat autosigné, avant de télécharger la documentation sur l'appareil tournant sous Android, assurez-vous que ce certificat du Serveur Dr.Web est installé sur votre appareil.

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

5.4.1. Scanner réseau

Fonctions du Scanner réseau

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

Principe de fonctionnement du Scanner réseau

Le Scanner réseau supporte les modes de recherche suivants :

1. Recherche dans Active Directory.
2. Recherche via NetBIOS.
3. Recherche via ICMP.
4. Recherche via TCP.
5. Mode supplémentaire : détermination de la présence de l'Agent Dr.Web.



Principe de fonctionnement si tous les modes sont activés :

1. Les trois premiers modes démarrent simultanément. Les postes déjà interrogés ne seront pas interrogés de nouveau.
2. Après la fin de la recherche via ICMP, la recherche via TCP démarre pour les adresses qui n'ont pas répondu. Si la recherche via ICMP est désactivée, la recherche via TCP démarre tout de suite en parallèle avec les deux premiers modes.



La recherche via ICMP s'effectue sur la base de requêtes ping qui peuvent être bloquées à cause des stratégies de réseau (notamment à cause des paramètres du pare-feu).

Exemple :

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

3. Les postes qui sont détectés lors de la recherche dans les quatre premiers modes sont interrogés dans le but de détecter les Agents Dr.Web.



Le Scanner réseau peut détecter un Agent Dr.Web installé sur le poste s'il est en version 4.44 ou supérieure, mais il n'est pas compatible avec les Agents Dr.Web en versions antérieures.

Installé sur le poste protégé, l'Agent Dr.Web traite les requêtes du Scanner réseau reçues sur le port spécifié. Par défaut, le port `udp/2193` sera utilisé. Dans le Scanner réseau, les requêtes seront envoyées vers le même port. En fonction de la possibilité d'échange d'informations via le port indiqué (requête-réponse), le Scanner réseau détermine la présence de l'Agent Dr.Web sur le poste.



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

Lancer le Scanner réseau

Pour réaliser un scan du réseau

1. Ouvrez la fenêtre du Scanner réseau. Pour cela, 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**. La fenêtre du Scanner réseau va s'ouvrir.
2. Cochez la case **Activer la recherche via ICMP** pour rechercher les postes via le protocole ICMP à l'intérieur des adresses IP spécifiées.
3. Cochez la case **Activer la recherche via TCP** pour rechercher les postes via le protocole TCP à l'intérieur des adresses IP spécifiées.



Spécifiez les paramètres pour ce mode :

- **Scan rapide.** En mode de scan rapide du réseau, seuls les ports principaux 445, 139, 22, 80 sur les postes sont interrogés.
- **Scan avancé.** En mode de scan avancé du réseau, beaucoup de ports fréquemment utilisés sont analysés. Les ports sont scannés dans l'ordre suivant : 445, 139, 135, 1025, 1027, 3389, 22, 80, 443, 25, 21, 7, 19, 53, 110, 115, 123, 220, 464, 465, 515, 873, 990, 993, 995, 1194, 1433, 1434, 2049, 3306, 3690, 4899, 5222, 5269, 5432, 6000, 6001, 6002, 6003, 6004, 6005, 6006, 6007, 6446, 9101, 9102, 9103, 10050, 10051, 8080, 8081, 98, 2193, 8090, 8091, 24554, 60177, 60179.

- **Adresses IPv4** : liste des adresses IPv4 :

- adresses séparées : 10.4.0.10
- plage d'adresses séparées par un trait d'union : 172.16.0.1-172.16.0.123
- plage avec le préfixe de réseau : 192.168.0.0/24

Si vous spécifiez plusieurs adresses, utilisez « ; » ou « , » pour les séparer.

- **Adresses IPv6** : liste des adresses IPv6 :

- adresses séparées : fe80::9109:1808:8e44:735b%3
- plage d'adresses séparées par un trait d'union : [FC00::0001]-[FC00::ffff]
- plage avec le préfixe de réseau : [::ffff:10.0.0.1]/7

Si vous spécifiez plusieurs adresses, utilisez « ; » ou « , » pour les séparer.

4. Cochez la case **Activer la recherche via NetBIOS** pour rechercher les postes via le protocole NetBIOS.

Spécifiez les paramètres pour ce mode :

- **Domaines** : liste des domaines dans lesquels la recherche des postes sera effectuée. Utilisez la virgule pour séparer plusieurs domaines.
- Cochez la case **Scan avancé** pour effectuer le scan avancé en utilisant les informations de navigateurs web.

5. Cochez la case **Activer la recherche dans Active Directory** pour rechercher des postes dans le domaine Active Directory.



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

La recherche des postes dans le domaine Active Directory se fait uniquement via le protocole sécurisé ldaps.

Spécifiez les paramètres pour ce mode :

- **Contrôleur Active Directory** : contrôleur Active Directory, par exemple, dc.example.com.
- **Nom d'utilisateur** : nom de l'utilisateur Active Directory.



- **Mot de passe** : mot de passe de l'utilisateur Active Directory.



Pour les Serveurs Dr.Web sous Windows, la configuration de la recherche dans Active Directory n'est pas obligatoire. Les identifiants de l'utilisateur au nom de qui le processus du Serveur Dr.Web (généralement LocalSystem) est lancé sont utilisés en tant que les données d'enregistrement.

Pour les Serveurs Dr.Web sous les OS de la famille UNIX, les paramètres doivent être obligatoirement spécifiés.

- Dans la liste déroulante **Protection de la connexion**, sélectionnez le type de l'échange chiffrée de données :
 - **STARTTLS** : le passage à la connexion sécurisée s'effectue via la commande STARTTLS. L'utilisation du port 25 pour la connexion est prévue par défaut.
 - **SSL/TLS** : ouvrir une connexion sécurisée à part. L'utilisation du port 465 pour la connexion est prévue par défaut.
 - **Non** : ne pas utiliser le chiffrement. L'échange de données s'effectuera par la connexion non sécurisée.
- 6. Dans la section **Paramètres généraux**, spécifiez les paramètres utilisés par tous les modes de recherche :
 - **Délai (s)** : délai maximum de réponse du poste en secondes.
 - **Nombre maximum des requêtes à un poste** : nombre maximum des requêtes à un poste dans l'attente d'une réponse.
 - **Nombre des requêtes simultanées** : nombre maximum des postes sur lesquels les requêtes simultanées sont envoyées.
 - Cochez la case **Afficher les noms des postes** pour afficher non seulement l'adresse IP, mais aussi le nom de domaine pour les postes détectés. Si le poste n'est pas enregistré sur le serveur DNS, seule l'adresse IP est affichée.
 - Cochez la case **Déterminer la présence de l'Agent** pour déterminer la présence de l'Agent Dr.Web installé sur le poste. Si l'option est désactivée, tous les postes trouvés afficheront le statut inconnu du logiciel sur le poste.



Si l'option **Déterminer la présence de l'Agent** est désactivée, le statut 🍌 sera affiché pour tous les postes trouvés, c'est-à-dire, le statut du logiciel sur le poste est inconnu.


- **Port** : numéro du port du protocole UDP par lequel il faut s'adresser aux Agents Dr.Web lors de la recherche. La plage de valeurs doit être comprise entre 1 et 65535. Le port 2193 est utilisé par défaut.
7. Cliquez sur le bouton **Scanner**. Le scan du réseau va commencer.
 8. Pendant le scan du réseau, la liste d'ordinateurs s'affiche dans une fenêtre indiquant la présence de l'Agent Dr.Web sur ces postes.

Développez 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 la description vous trouverez ci-dessous :

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 les icônes  pour consulter l'ensemble des composants installés.

5.5. Schéma d'interaction des composants du réseau antivirus

La [figure 5-2](#) présente le schéma d'un fragment du réseau antivirus.

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

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

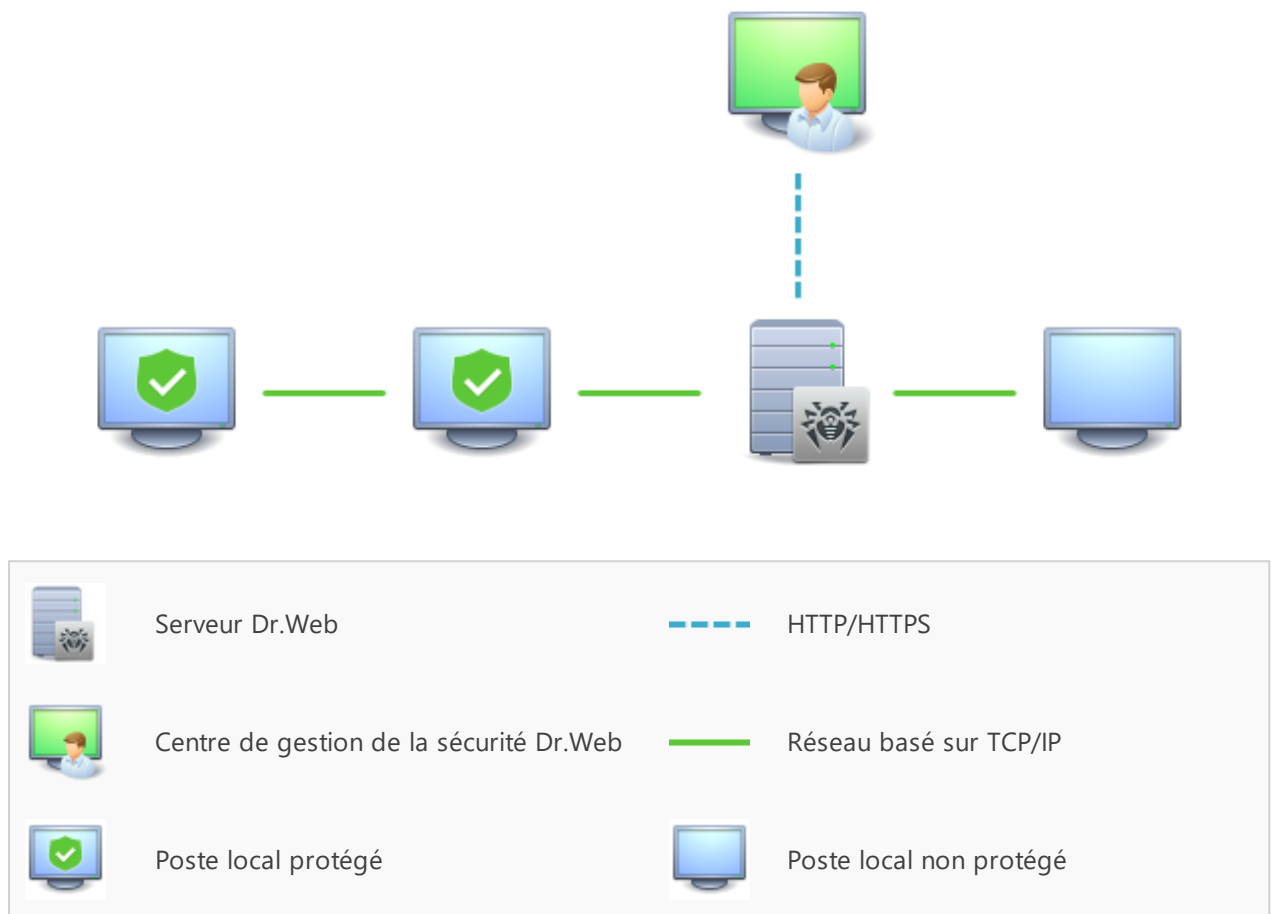


Figure 5-2. Structure du réseau antivirus

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

1. Téléchargement des fichiers du Serveur Dr.Web depuis le répertoire `bin`.
2. Téléchargement du Planificateur des tâches du Serveur Dr.Web.
3. Chargement du répertoire de mise à jour, initialisation du système de notification.
4. Vérification de l'intégrité de la BD du Serveur Dr.Web.
5. Exécution des tâches du Planificateur des tâches du Serveur Dr.Web.
6. Attente des informations depuis les Agents Dr.Web et des commandes depuis les Centres de gestion.

Tout le flux des commandes, données, informations statistiques passe obligatoirement par le Serveur Dr.Web. Le Centre de gestion échange des informations uniquement avec le Serveur Dr.Web ; les modifications de la configuration du poste et la transmission des commandes vers l'Agent Dr.Web sont effectuées par le Serveur Dr.Web selon les commandes reçues depuis le Centre de gestion.

La structure logique de ce fragment du réseau antivirus est présentée dans la [figure 5-3](#).

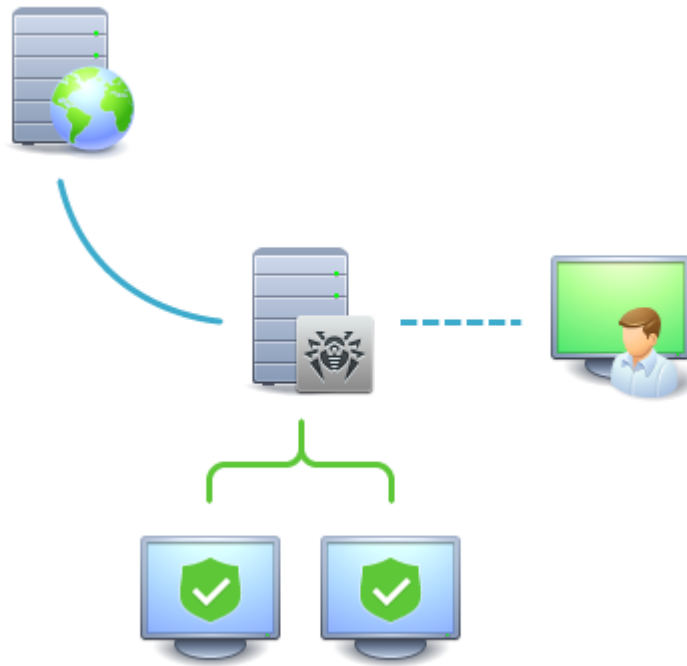


Figure 5-3. Structure logique du réseau antivirus

Entre le Serveur Dr.Web et les postes de travail (trait continu dans la [figure 5-3](#)), les informations suivantes sont transmises :

- requêtes de l'Agent Dr.Web pour la réception de la planification centralisée et la planification centralisée du poste,
- paramètres de l'Agent Dr.Web et du package antivirus,
- requêtes pour les tâches urgentes à exécuter (scan, mise à jour des bases virales, etc.),
- fichiers des packages antivirus : lorsque l'Agent reçoit des commandes relatives à leur installation,
- mises à jour du logiciel et des bases virales : lors de l'exécution de la tâche de mise à jour,
- messages de l'Agent Dr.Web relatifs à la configuration du poste,



- statistiques sur le fonctionnement de l'Agent Dr.Web et des packages antivirus à inclure dans le journal centralisé,
- messages sur les événements viraux et d'autres événements à mémoriser.

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

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

Les fichiers nécessaires à la réplication de répertoires d'installation centralisés et de mises à jour ainsi que des informations de service sur la progression de ce processus sont transmis, via le protocole HTTP, depuis le serveur web de mises à jour vers le Serveur Dr.Web (trait continu gras dans la [figure 5-3](#)). L'intégrité des informations transmises (fichiers de Dr.Web Enterprise Security Suite et de packages antivirus) est assurée par le mécanisme utilisant la somme de contrôle : un fichier endommagé lors de la transmission ou un fichier qui a été remplacé ne seront pas réceptionnés par le Serveur Dr.Web.

Entre le Serveur Dr.Web et le Centre de gestion (trait pointillé dans la [figure 5-3](#)) sont transmises les informations sur la configuration du Serveur (y compris les informations sur la topologie du réseau) et sur les configurations des postes de travail. Ces informations sont affichées dans le Centre de gestion et si les configurations sont modifiées par l'utilisateur (l'administrateur du réseau antivirus), les informations sur les modifications apportées seront transmises au Serveur Dr.Web.

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



Chapitre 6 : Administrateurs du réseau antivirus

L'administrateur du réseau antivirus doit avoir une expérience en administration des réseaux locaux et il doit être compétent en matière de protection antivirus. L'administrateur doit avoir accès aux répertoires d'installation du Serveur Dr.Web. En fonction des politiques de sécurité adoptées dans la société et selon sa structure, l'administrateur du réseau antivirus doit bénéficier des droits d'administrateur du réseau local, sinon il doit travailler en contact étroit avec l'administrateur du réseau local.



Les droits d'administrateur sur les postes faisant partie du réseau ne sont pas indispensables à l'administrateur du réseau antivirus pour sa gestion courante. Cependant, l'installation à distance ainsi que la désinstallation du logiciel de l'Agent n'est possible que dans le réseau local et nécessite les droits d'administrateur dans ce réseau, le débogage du Serveur Dr.Web requiert un accès illimité au répertoire d'installation du Serveur.

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.

6.1. Authentification des administrateurs

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

- Via la sauvegarde des données du compte administrateur dans la BD du Serveur Dr.Web.
- Avec les paramètres LDAP/AD permettant la connexion aux serveurs LDAP et à Active Directory.
- Via le protocole RADIUS.
- Via PAM (uniquement pour les OS de la famille UNIX).

Lors de la mise à niveau du Serveur Dr.Web de la version précédente, les types d'authentifications suivants sont disponibles (s'ils ont été activés dans la version précédente) :



En cas de désactivation de ces types d'authentification, leurs sections seront exclues du Centre de gestion.

Lors de la première installation du Serveur Dr.Web, ces sections ne sont pas disponibles.

- Via Active Directory (Serveurs Dr.Web sous Windows).



- Via le protocole LDAP.

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

1. L'authentification de l'administrateur depuis la BD du Serveur Dr.Web est toujours tentée en premier.
2. L'ordre d'application des méthodes d'authentification via les systèmes externes dépend de l'ordre de leur succession dans les paramètres spécifiés dans le Centre de gestion.
3. L'authentification via les systèmes externes est désactivée par défaut.

Pour modifier l'ordre de l'utilisation des modes d'authentification

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion.
2. Dans le menu de gestion, sélectionnez la section **Authentification**.
3. Dans la fenêtre qui s'ouvre, une liste des types d'authentification par ordre d'utilisation apparaît. Pour modifier l'ordre, glissez-déposez les modes d'authentification dans l'ordre dans lequel il faut effectuer l'authentification.
4. Redémarrez le Serveur Dr.Web pour appliquer les modifications.



Le login administrateur doit être unique.

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

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

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

`<nom_de_fichier>_<date_et_heure_de_création>`

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

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

6.1.1. Authentification des administrateurs depuis la BD du Serveur Dr.Web

Le mode d'authentification dans lequel les données sur les administrateurs sont conservées dans la BD du Serveur Dr.Web est utilisé par défaut.



Pour ouvrir la section de gestion des comptes administrateurs

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion.
2. Dans le menu de gestion, sélectionnez la section **Administrateurs**. La liste de tous les administrateurs du Serveur Dr.Web sera affichée.

Pour en savoir plus, consultez [Administrateurs et groupes administrateur](#).

6.1.2. Authentification via LDAP/AD

Pour activer l'authentification via LDAP/AD

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion.
2. Dans le menu de gestion, sélectionnez la section **Authentification**.
3. Dans la fenêtre qui apparaît, allez dans la section **Authentification LDAP/AD**.
4. Cochez la case **Utiliser l'authentification LDAP/AD**.
5. Cliquez sur **Enregistrer**.
6. Redémarrez le Serveur Dr.Web pour appliquer les modifications.

Il est possible de configurer l'authentification via le protocole LDAP sur n'importe quel serveur LDAP. En utilisant ce mécanisme, vous pouvez configurer le Serveur Dr.Web tournant sous l'OS de la famille UNIX pour l'authentification dans Active Directory sur le contrôleur de domaine.

Pour plus de commodité de l'utilisateur, la section a une possibilité de basculer entre les paramètres simples et avancés de l'authentification via LDAP/AD.



Les paramètres d'authentification LDAP/AD sont sauvegardés dans le fichier de configuration `auth-ldap-rfc4515.conf`.

Les fichiers de configuration avec les paramètres standard sont également fournis : `auth-ldap-rfc4515-check-group.conf`, `auth-ldap-rfc4515-check-group-novar.conf`, `auth-ldap-rfc4515-simple-login.conf`.

Pour en savoir plus sur les attributs xml principaux de l'authentification, consultez les **Annexes**, l'[Annexe B3. Authentification via LDAP/AD](#).

6.1.3. Authentification via RADIUS

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

Avant de commencer la configuration de l'authentification via RADIUS, assurez-vous que le Dictionnaire `dictionary.drweb` se trouvant dans le répertoire `etc` du Serveur



Dr.Web est copié dans le répertoire `/usr/share/freeradius`. Le dictionnaire sauvegarde l'ensemble des attributs RADIUS de la société Doctor Web (VSA — Vendor-Specific Attributes).

Avec la ligne de commande assignez les droits d'accès au fichier `dictionary.drweb` dans le répertoire `/usr/share/freeradius`. La commande ressemble à celle-ci :

```
chmod 644 /usr/share/freeradius/dictionary.drweb
```

À la fin du fichier `/etc/raddb/dictionary`, ajoutez la ligne suivante :

```
$INCLUDE/usr/share/freeradius/dictionary.drweb
```

Au début du fichier `/etc/raddb` , ajoutez les lignes suivantes :

```
<Nom_d'enregistrement> Cleartext-Password := "<mot_de_passe>"  
DrWeb-ES-Adm-Flag = 1
```

Après avoir effectué ces actions, activez l'authentification via RADIUS dans le Centre de gestion.

Pour activer l'authentification via RADIUS

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion.
2. Dans le menu de gestion, sélectionnez la section **Authentification**.
3. Dans la fenêtre qui apparaît, allez dans la rubrique **Authentification RADIUS**.
4. Cochez la case **Utiliser l'authentification RADIUS**.
5. Cliquez sur **Enregistrer**.
6. Redémarrez le Serveur Dr.Web pour appliquer les modifications.

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

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



Le fichier de configuration `auth-radius.conf` situé dans le répertoire `etc` du Serveur peut être également utilisé pour la configuration des paramètres supplémentaires de RADIUS.

Outre les paramètres spécifiés via le Centre de gestion, vous pouvez indiquer, dans le fichier de configuration, la valeur de l'identificateur NAS. Cet identificateur, d'après le RFC 2865, peut être utilisé au lieu de l'adresse IP/ nom de domaine DNS, comme un identificateur du client pour la connexion au serveur RADIUS. Il est sauvegardé dans le fichier de configuration sous cette forme :

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

6.1.4. Authentification via PAM

Pour activer l'authentification via PAM

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion.
2. Dans le menu de gestion, sélectionnez la section **Authentification**.
3. Dans la fenêtre qui apparaît, allez dans la rubrique **Authentification PAM**.
4. Cochez la case **Utiliser l'authentification PAM**.
5. Cliquez sur **Enregistrer**.
6. Redémarrez le Serveur Dr.Web pour appliquer les modifications.

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

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

- Paramètres du mode d'authentification via le Centre de gestion : dans la section **Administration** → **Authentification** → **Authentification PAM**.
- Fichier de configuration `auth-pam.xml` situé dans le répertoire `etc` du Serveur Dr.Web.
Exemple de fichier de configuration :

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




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

Élément du Centre de gestion	Éléments du fichier auth-pam.xml			Description
	Balise	Attribut	Valeurs autorisées	
Case Utiliser l'authentification PAM	<code><enabled></code>	<code>value</code>	yes no	Case qui détermine si la méthode d'authentification PAM est utilisée.
Utilisez le <i>glisser-déposer</i>	<code><order></code>	<code>value</code>	nombre entier positif, coordonné avec les valeurs des autres méthodes	Numéro de série de l'authentification PAM si plusieurs méthodes sont utilisées.
Champ Nom du Service	<code><service></code>	<code>name</code>	-	Nom du service utilisé pour créer un contexte PAM. PAM peut lire les politiques via ce service depuis <code>/etc/pam.d/<service name></code> ou depuis <code>/etc/pam.conf</code> , si le fichier n'existe pas. Si le paramètre n'est pas configuré (il n'y a pas de balise <code><service></code> dans le fichier de configuration), le nom <code>drwcs</code> est utilisé par défaut.
La case La case de contrôle est obligatoire	<code><admin-flag></code>	<code>mandatory</code>	yes no	Ce paramètre détermine si l'indicateur de contrôle permettant d'identifier un utilisateur comme administrateur est obligatoire. Par défaut — yes.
Champ Nom de la case de contrôle	<code><admin-flag></code>	<code>name</code>	-	Élément de la clé d'après lequel les modules PAM lisent la case. Par défaut — <code>DrWeb_Esuite_Admin</code> .

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



6.1.5. Authentification via Active Directory



Avant d'activer l'authentification avec l'utilisation d'Active Directory, assurez-vous que le compte pour lequel vous activez l'authentification ne fait pas partie du groupe **Utilisateurs protégés**. Vu que le Serveur Dr.Web est un service, une tentative d'authentification du compte faisant partie du groupe **Utilisateurs protégés** échouera. Pour en savoir plus sur le groupe de sécurité Utilisateurs protégés, visitez le [site officiel de Microsoft](#).

Pour activer l'authentification via Active Directory

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion.
2. Dans le menu de gestion, sélectionnez la section **Authentification**.
3. Dans la fenêtre qui apparaît, passez dans la rubrique **Microsoft Active Directory**.
4. Cochez la case **Utiliser l'authentification Microsoft Active Directory**.
5. Cliquez sur **Enregistrer**.
6. Redémarrez le Serveur Dr.Web pour appliquer les modifications.

Lors de l'authentification des administrateurs via Active Directory, dans le Centre de gestion, vous pouvez configurer uniquement l'autorisation d'utiliser ce mode d'authentification.

L'édition des propriétés des administrateurs d'Active Directory se fait de manière manuelle sur le serveur d'Active Directory.



Si l'administrateur est créé automatiquement et que l'authentification via Active Directory est activé, le compte de l'administrateur est automatiquement assigné au groupe Newbies. Pour l'assigner au groupe nécessaire, il faut le faire manuellement.

Le compte de l'administrateur peut être automatiquement transféré du groupe Newbies dans le groupe spécifié en fonction de l'appartenance aux groupes Active Directory avec la procédure utilisateur, voir le document **Annexes**, [M1. Administrateurs](#).

Pour éditer les administrateurs d'Active Directory



Les opérations listées ci-après doivent être exécutées sur un PC sur lequel est installé le composant logiciel enfichable Schéma Active Directory.

1. Pour pouvoir éditer les paramètres des administrateurs, il est nécessaire de réaliser les opérations suivantes :
 - a) Afin de modifier le schéma d'Active Directory, lancez l'utilitaire `drweb-<version_du_package>-<assemblage>-esuite-modify-ad-schema-<version_de_l'OS>.exe` (inclus dans le package d'installation du Serveur Dr.Web). La modification du schéma d'Active Directory peut prendre un certain temps. En fonction



de la configuration de votre domaine, la synchronisation et l'application du schéma modifié peuvent prendre 5 minutes au minimum.



Si auparavant vous avez déjà modifié le schéma Active Directory à l'aide de cet utilitaire du Serveur Dr.Web en version 6 ou supérieure, il n'est pas nécessaire d'effectuer la modification encore une fois à l'aide de l'utilitaire en version 13 du Serveur Dr.Web.

- b) Pour enregistrer le composant logiciel enfichable Active Directory Schema (Schéma Active Directory), exécutez la commande `regsvr32 schmmgmt.dll` en mode administrateur, puis lancez `mmc` et ajoutez le composant logiciel enfichable **Active Directory Schema**.
- c) En utilisant le composant logiciel enfichable Active Directory Schema, ajoutez à la classe **User** et (si nécessaire) à la classe **Group** la classe auxiliaire **DrWebEnterpriseUser** et l'attribut supplémentaire **DrWebAdmin**.



Si l'application du schéma modifié n'est pas encore achevée, la classe **DrWebEnterpriseUser** est introuvable. Dans ce cas, patientez un certain temps et réessayez comme décrit dans le p. c).

- d) Dans le mode administrateur, lancez le fichier `drweb-<version_du_package>-<assemblage>-esuite-aduac-<version_de_l'OS>.msi` (inclus dans le package d'installation Dr.Web Enterprise Security Suite 13.0) et attendez la fin de l'installation.
2. L'interface graphique permettant d'éditer les attributs est disponible depuis le panneau de configuration **Active Directory Users and Computers** → dans la section **Users** → dans la fenêtre d'édition des propriétés de l'utilisateur sélectionné **Administrator Properties** → dans l'onglet **Dr.Web Authentication**.
 3. Les paramètres ci-dessous sont disponibles en édition (chaque attribut peut prendre les valeurs **yes**, **no** ou **not set**) :

User is administrator signifie que l'utilisateur est administrateur ayant les droits complets.



Vous pouvez consulter les algorithmes relatifs au fonctionnement et à l'analyse des attributs lors de l'authentification dans les **Annexes**, [B1. Authentification via Active Directory](#).

Pour continuer à utiliser le compte Active Directory, il faut s'authentifier dans le Centre de gestion de la sécurité du Serveur Dr.Web avec les identifiants de l'utilisateur d'Active Directory auquel l'attribut correspondant **Dr.Web Authentication** a été désigné plus tôt. Ensuite, le compte de l'utilisateur apparaîtra dans le répertoire **Newbies**, dans la section **Administration** → **Administrateurs**.

6.1.6. Authentification via LDAP



Vous pouvez configurer cette section via le Centre de gestion uniquement lors de la mise à niveau du Serveur Dr.Web. Après la désactivation de ce type d'authentification, sa section



sera exclue des paramètres du Centre de gestion.

Lors de la première installation du Serveur Dr.Web, cette section n'est pas disponible.

Pour activer l'authentification via LDAP

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion.
2. Dans le menu de gestion, sélectionnez la section **Authentification**.
3. Dans la fenêtre qui apparaît, allez dans la section **Authentification LDAP**.
4. Cochez la case **Utiliser l'authentification LDAP**.
5. Cliquez sur **Enregistrer**.
6. Redémarrez le Serveur Dr.Web pour appliquer les modifications.

Il est possible de configurer l'authentification via le protocole LDAP sur n'importe quel serveur LDAP. En utilisant ce mécanisme, vous pouvez configurer le Serveur Dr.Web tournant sous l'OS de la famille UNIX pour l'authentification dans Active Directory sur le contrôleur de domaine.



Les paramètres de l'authentification LDAP sont sauvegardés dans le fichier de configuration `auth-ldap.conf`.

Pour en savoir plus sur les attributs xml principaux de l'authentification, consultez les **Annexes**, l'[B2. Authentification via LDAP](#).

A la différence d'Active Directory, le mécanisme peut être configuré conformément à n'importe quel schéma LDAP. Par défaut, une tentative d'utiliser les attributs de Dr.Web Enterprise Security Suite sera entreprise, comme ils sont spécifiés pour Active Directory.

Le processus d'authentification LDAP :

1. L'adresse du serveur LDAP est spécifiée via le Centre de gestion ou dans le fichier de configuration xml.
2. Pour un nom d'utilisateur spécifié, les actions suivantes sont réalisées :
 - Transformation du nom vers le nom distingué DN (Distinguished Name) à l'aide des masques de type DOS (en utilisant le symbole *) si les règles sont spécifiées.
 - Transformation du nom vers le nom distingué DN avec les expressions régulières si les règles sont spécifiées.
 - Utilisation du script utilisateur pour la transformation des noms vers les DN si ce script est spécifié dans les paramètres.
 - Si aucune règle de transformation ne correspond, le nom spécifié est utilisé tel qu'il est.



Le format dans lequel est spécifié le nom d'utilisateur n'est pas déterminé ni fixé, l'entreprise peut utiliser un format adopté, dans ce cas, aucune modification forcée du



schéma LDAP n'est requise. La transformation d'après ce schéma se fait conformément aux règles de transformation de noms vers LDAP DN.

3. Après la transformation, tout comme en cas d'Active Directory, avec le DN reçu et le mot de passe entré, une tentative d'enregistrer l'utilisateur sur le serveur LDAP sélectionné sera réalisée.
4. Puis, tout comme en cas d'Active Directory, les attributs de l'objet LDAP pour le DN reçu sont lus. Les attributs et leurs valeurs admissibles peuvent être modifiés dans le fichier de configuration.
5. S'il reste des valeurs des attributs de l'administrateur non déterminées et que l'héritage est spécifié (dans le fichier de configuration), la recherche des attributs nécessaires dans les groupes dont l'utilisateur fait partie se fait de la même manière qu'en cas d'utilisation d'Active Directory.

6.2. Administrateurs et groupes administrateur

Pour ouvrir la section de gestion des comptes administrateurs

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion.
2. Dans le menu de gestion, sélectionnez la section **Administrateurs**. La liste de tous les administrateurs du Serveur Dr.Web sera affichée.



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

Les options suivantes sont disponibles dans la barre d'outils de la section **Administrateurs** :



[Créer un compte](#)



[Créer un groupe](#)



[Supprimer les objets sélectionnés](#)



[Changer de mot de passe](#)



[Distribuer les droits d'administrateur](#)

6.2.1. Hiérarchie des administrateurs

La visualisation de la hiérarchie des administrateurs est une arborescence qui représente la structure des groupes administrateurs et des comptes administrateurs. Les groupes administrateurs et leurs membres (les comptes administrateurs) peuvent être chacun des



noeuds de cette arborescence. Chaque administrateur peut être membre d'un groupe seulement. Le niveau d'emboîtement des groupes dans l'arborescence n'est pas limité.

Groupes prédéfinis

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

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

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

Administrateurs prédéfinis

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

Paramètre	Valeur
Nom du compte	admin
Mot de passe	Le mot de passe est spécifié lors de l'installation du Serveur Dr.Web (étape 9 de la procédure d'installation).
Droits	Ensemble complet de droits.
Édition du compte	Le compte administrateur ne peut pas être supprimé.

Affichage des listes hiérarchiques

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

6.2.2. Droits d'administrateurs

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



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

- **Octroi de droits**

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

- **Héritage de droits**

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

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

- **Modification des droits**

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

La modification des droits est décrite dans le paragraphe [Modification des droits](#).

Modification des droits

Pour modifier les droits d'administrateur ou de groupe administrateur

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




  **L'héritage est activé**

  **L'héritage est désactivé**

5. Les paramètres généraux sont spécifiés dans le tableau de droits :

a) Dans la première colonne s'affichent les noms des droits. L'en-tête de la colonne dépend d'une section spécifique fusionnant les droits par types.

 Pour en savoir plus sur les droits des administrateurs et des sections du Centre de gestion qui sont responsables des droits spécifiques, consultez le document **Annexes**, [Annexe B4. Sections dépendantes de droits.](#)

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

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



Objets de gestion	Liste des paramètres de la colonne Droits	Principe de spécification du droit
		<ul style="list-style-type: none">• Interdire pour refuser le droit aux objets sélectionnés.



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

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

Fusionner les droits

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

Droit du groupe parent	Droit de l'enfant en question	Droit calculé (résultant)
Tout est accordé	Accordé pour certains objets	Accordé pour les objets de l'enfant
Accordé pour certains objets	Accordé pour certains objets	Les listes des objets autorisés sont fusionnés
Accordé pour certains objets	Tout est accordé	Tout est accordé
Les droits du parent et de l'enfant sont interdisants. L'un des droits interdit tout		Tout est refusé
Refusé pour certains objets	Refusé pour certains objets	Les listes des objets interdits sont fusionnés
Tout est refusé	Tout est accordé	Tout est accordé



Droit du groupe parent	Droit de l'enfant en question	Droit calculé (résultant)
Refusé pour certains objets	Tout est accordé	Refusé pour les objets du parent
Refusé pour certains objets	Accordé pour certains objets	Les objets autorisés sont exclus des objets interdits. Si, après cela, la liste des objets interdits n'est pas vide, les objets restants sont interdits. Sinon, tous les objets de l'enfant sont autorisés
Accordé pour certains objets	Tout est refusé	Tout est refusé
Tout est accordé	Refusé pour certains objets	Refusé pour les objets de l'enfant
Accordé pour certains objets	Refusé pour certains objets	Les objets interdits sont exclus des objets autorisés. Si, après cela, la liste des objets autorisés est vide, tous les objets sont interdits. Sinon, tous les objets restants sont autorisés.

6.3. Gestion des comptes et des groupes administrateur

6.3.1. Création et suppression des comptes et des groupes administrateur



Le login administrateur doit être unique.


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

Ajout d'un compte administrateur



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

Pour ajouter un nouveau compte administrateur

1. Sélectionnez l'élément **Administration** du menu principal du Centre de gestion, et dans la fenêtre qui s'ouvre, sélectionnez l'élément **Administrateurs** dans le menu de gestion.
2. Cliquez sur l'icône  **Créer un compte** dans la barre d'outils. Une fenêtre contenant les paramètres du compte créé va s'ouvrir.
3. Dans la sous-section **Général**, configurez les paramètres suivants :



- Dans le champ **Login**, spécifiez le login du compte administrateur pour accéder au Centre de gestion. Vous pouvez utiliser des lettres minuscules (a-z), des majuscules (A-Z), des chiffres (0-9) et des caractères « _ » et « . ».
- Dans les champs **Mot de passe** et **Confirmez le mot de passe**, spécifiez un mot de passe pour accéder au Serveur Dr.Web et au Centre de gestion.



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



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

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

- Dans les champs **Nom**, **Prénom** et **Patronyme**, vous pouvez spécifier les données personnelles de l'administrateur.
- Indiquez votre **Adresse e-mail**. Si vous ne le faites pas, vous ne pourrez pas réinitialiser le mot de passe en cas de besoin.
- Dans la liste déroulante **Langue d'interface**, sélectionnez la langue à utiliser par l'administrateur que vous créez (la langue du navigateur ou l'anglais est spécifié par défaut).



Si vous sélectionnez une langue et que les textes d'interface écrits dans cette langue ne sont pas mis à jour en ce moment, vous serez invité à activer la mise à jour pour cette langue. Pour cela, accédez à **Administration** → **Configuration générale du référentiel** → **Serveur Dr.Web** → **Langues du Centre de gestion de la sécurité Dr.Web**, cochez la case contre la langue nécessaire et cliquez sur **Enregistrer**. Lors de la prochaine mise à jour, les textes d'interface pour la langue sélectionnée seront mis à jour. Vous pouvez également lancer manuellement la mise à jour dans la section **Statut du référentiel**.

- Dans la liste déroulante **Format de la date**, sélectionnez le format qui sera utilisé par l'administrateur lors de l'édition des paramètres contenant des dates. Les formats suivants peuvent être sélectionnés :
 - européen : JJ-MM-AAAA HH:MM:SS
 - américain : MM/JJ/AAAA HH:MM:SS
- Dans le champ **Description**, vous pouvez donner une description facultative du compte.



Les valeurs des champs marqués par le symbole * doivent être obligatoirement spécifiées.

4. Dans la sous-section **Groupes**, vous pouvez indiquer le groupe parent administrateur. La liste contient les groupes auxquels un administrateur peut être assigné. La case est cochée contre le groupe auquel l'administrateur créé sera rattaché. Par défaut, les administrateurs



créés sont placés dans le groupe parent de l'administrateur actuel. Pour modifier le groupe assigné, cochez la case contre le groupe nécessaire.

Chaque administrateur peut être membre d'un seul groupe.

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

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



Pour que l'administrateur ait les informations actuelles sur les événements du réseau antivirus, il est recommandé de configurer des notifications tout de suite après la création du compte, en suivant les instructions de la section [Configuration des notifications](#). Pour pouvoir créer des rapports statistiques selon la planification, il faut activer la notification **Rapport statistique**.

Ajouter des groupes administrateur



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

Pour ajouter un nouveau compte du groupe d'administration

- Sélectionnez l'élément **Administration** du menu principal du Centre de gestion, et dans la fenêtre qui s'ouvre, sélectionnez l'élément **Administrateurs** dans le menu de gestion.
- Cliquez sur l'icône **Créer un groupe** dans la barre d'outils. Une fenêtre contenant les paramètres du groupe créé va s'ouvrir.
- Dans la sous-section **Général**, configurez les paramètres suivants :
 - Dans le champ **Groupe**, spécifiez le nom du groupe administrateur. Vous pouvez utiliser les lettres minuscules (a-z), les majuscules (A-Z), des chiffres (0-9) et les caractères « _ » et « . ».
 - Dans le champ **Description**, vous pouvez donner une description facultative du groupe.
- Dans la sous-section **Groupes**, vous pouvez indiquer le groupe administrateur parent. La liste contient les groupes qui peuvent être définis comme groupes parents. La case est cochée contre le groupe dans lequel le groupe administrateur créé sera inclus. Par défaut, les groupes créés sont placés dans le groupe parent de l'administrateur actuel. Pour modifier le groupe assigné, cochez la case contre le groupe nécessaire.
Seul un groupe parent peut être assigné.
Le groupe administrateur hérite les droits du groupe parent (voir p. [Droits d'administrateurs](#)).
- Après la configuration de tous les paramètres, cliquez sur **Enregistrer** pour créer un nouveau groupe administrateur.



Suppression des administrateurs et des groupes administrateur



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

Pour supprimer un compte administrateur ou un groupe

1. Sélectionnez l'élément **Administration** du menu principal du Centre de gestion, et dans la fenêtre qui s'ouvre, sélectionnez l'élément **Administrateurs** dans le menu de gestion.
2. Dans la liste hiérarchique des administrateurs, sélectionnez le compte ou le groupe administrateur à supprimer.
3. Dans la barre d'outils, cliquez sur l'icône **✖ Supprimer les objets sélectionnés**.
Si l'administrateur à supprimer est l'auteur des [tâches de la planification du Serveur Dr.Web](#), avant de le supprimer, attribuez les tâches à un autre administrateur dans la partie droite de la fenêtre. Ensuite, cliquez sur le bouton **Supprimer**.
4. Confirmez la suppression.

6.3.2. Récupération du mot de passe de l'administrateur

Vous pouvez récupérer le mot de passe oublié de l'administrateur de l'une des manières suivantes :

1. Réinitialiser le mot de passe lors de la connexion au Centre de gestion de la sécurité Dr.Web.
2. Spécifier un nouveau mot de passe dans la ligne de commande lors du lancement du Serveur Dr.Web.

Pour réinitialiser le mot de passe lors de la connexion au Centre de gestion de la sécurité Dr.Web

1. Ouvrez la page d'authentification (http://<Adresse_du_Serveur_Dr.Web>:9080 ou https://<Adresse_du_Serveur_Dr.Web>:9081).http://<Adresse_du_Serveur_Dr.Web>:9080 ou https://<Adresse_du_Serveur_Dr.Web>:9081) où comme valeur <Adresse_du_Serveur_Dr.Web> indiquez l'adresse IP ou le nom DNS de l'ordinateur sur lequel le Serveur Dr.Web est installé.
2. Cliquez sur **Réinitialiser le mot de passe**.
3. Dans la fenêtre qui s'ouvre, remplissez les champs **Nom d'enregistrement** et **Adresse e-mail** en saisissant les identifiants de l'administrateur dont vous voulez récupérer le mot de passe.



L'adresse e-mail saisie doit correspondre à l'adresse indiquée dans les [paramètres du compte](#) de l'administrateur.



4. Cliquez sur **Envoyer un lien**. Un message contenant le lien de réinitialisation du mot de passe sera envoyé à l'adresse e-mail indiquée.



Le message sera envoyé à condition que le Serveur SMTP soit configuré au préalable (voir la rubrique [E-mail](#)).

5. Suivez le lien indiqué et spécifiez un nouveau mot de passe sur la page qui s'ouvre. Si vous n'avez pas reçu le message, réessayez.

Pour changer le mot de passe lors du lancement du Serveur Dr.Web via la ligne de commande :

Lancez le Serveur Dr.Web depuis la ligne de commande en indiquant le paramètre nécessaire pour le changement du mot de passe, le nom de l'administrateur et le nouveau mot de passe :

```
drwcsd modexecdb set-admin-password <nom_d'administrateur> <nouveau_mot_de_passe>
```

6.3.3. Éditer les comptes et les groupes administrateurs



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

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

Les valeurs des champs marqués par le symbole * doivent être obligatoirement spécifiées.

Pour modifier un compte d'administrateur

1. Sélectionnez le compte que vous souhaitez éditer dans la liste des administrateurs. La fenêtre de ses propriétés va s'ouvrir.
2. La sous-section **Général** contient les propriétés qui ont été configurées durant la [création](#) d'un compte. Ainsi :
 - a) Pour changer de mot de passe du compte administrateur, cliquez sur l'icône **Changer de mot de passe** dans la barre d'outils.



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



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



- b) Les propriétés suivantes du compte administrateur sont en lecture seule :
- Date de la création du compte et date de la dernière modification de ses paramètres,
 - **Statut** : affiche l'adresse réseau de la dernière connexion du compte actuel.
3. Dans la sous-section **Groupes**, vous pouvez modifier un groupe administrateur. La liste contient les groupes auxquels un administrateur peut être rattaché. La case est cochée contre le groupe parent actuel de l'administrateur. Pour modifier le groupe assigné, cochez la case contre le groupe nécessaire.
- Il est obligatoire d'assigner un groupe parent à l'administrateur. Chaque administrateur peut être inclus à un seul groupe à la fois. Les droits de l'administrateur sont hérités du groupe parent assigné.
- Voir aussi la sous-section [Modifier l'appartenance](#).
4. Dans la sous-section **Droits**, vous pouvez modifier la liste des actions autorisées pour l'administrateur sélectionné.
- La modification des droits est décrite en détails dans la sous-section [Modifier les droits](#).
5. Cliquez sur **Enregistrer** pour appliquer les modifications.

Pour modifier un groupe administrateur


1. Sélectionnez le groupe que vous souhaitez éditer dans la liste des administrateurs. La fenêtre de ses propriétés va s'ouvrir.
 2. La sous-section **Général** contient les propriétés qui ont été configurées durant la [création](#).
 3. Dans la sous-section **Groupes**, vous pouvez modifier le groupe administrateur parent. La liste contient les groupes qui peuvent être définis comme groupe parent. La case est cochée près du groupe parent actuel. Pour modifier le groupe assigné, cochez la case près du groupe nécessaire.
- Il est obligatoire d'assigner un groupe parent au groupe administrateur. Le groupe hérite des droits de son groupe parent assigné.
- Voir aussi la sous-section [Modifier l'appartenance](#).
4. Dans la sous-section **Droits**, vous pouvez modifier la liste des actions autorisées pour le groupe administrateur sélectionné.
- La modification des droits est décrite en détails dans la sous-section [Modifier les droits](#).
5. Cliquez sur **Enregistrer** pour appliquer les modifications.

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

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



Pour distribuer les droits d'administrateur ou de groupe à un autre administrateur ou un groupe

1. Dans la liste des administrateurs, sélectionnez un objet dont vous voulez distribuer les droits. Cela peut être un administrateur ou un groupe d'administrateurs.
2. Dans la barre d'outils, cliquez sur le bouton  **Distribuer les droits d'administrateur**.
3. Dans la fenêtre qui s'ouvre, sélectionnez les objets auxquels vous voulez assigner les droits. Notez les particularités suivantes :
 - Un ou plusieurs objets peuvent être sélectionnés pour l'assignation des droits. Cela peut être des administrateurs ou des groupes d'administrateurs.
 - Les droits sont conservés pour les objets sélectionnés comme des droits personnels. L'héritage du groupe parent est interrompu.
 - L'assignation des droits aux objets créés par défaut (les groupes **Administrators**, **Newbies**, l'administrateur **admin**) n'est pas possible.
 - Vous pouvez distribuer les droits uniquement aux objets autorisés dans les droits **Éditer les comptes administrateurs** et **Éditer les propriétés et la configuration des groupes administrateurs**.
 - Si la distribution entraîne l'assignation des droits qui dépassent les droits de l'administrateur exécutant l'opération, une erreur sera retournée en vous informant du manque de droits pour l'exécution de l'opération.
4. Cliquez sur le bouton **Distribuer**.



Chapitre 7 : Gestion globale des postes de travail

Pour la gestion globale des postes et de leurs paramètres, les outils suivants sont fournis :

- **Groupes.**

Le poste peut faire partie d'un nombre illimité des groupes. L'appartenance aux groupes prédéfinis à partir de son statut est obligatoire. L'appartenance aux groupes utilisateurs est optionnelle. Pourtant un seul groupe est primaire.

- **Politiques.**

Une seule ou aucune politique peut être assignée pour le poste.

- **Profils.**

Les profils sont utilisés pour configurer les paramètres du composant [Contrôle des applications](#). Les profils peuvent être assignés aux postes, aux groupes de postes et aux utilisateurs particuliers.

Pour contrôler le lancement des applications sur les postes, il faut qu'au moins un profil actif soit assigné au poste ou à l'utilisateur du poste.

Types des paramètres de postes

- **Paramètres hérités.**


Lors de la création du poste, les paramètres sont toujours hérités de la politique ou du groupe primaire. Pour plus d'informations, consultez la rubrique [Héritage de la configuration du poste de travail](#).

- **Paramètres personnalisés.**

Lors du fonctionnement du poste, l'héritage peut être interrompu et les paramètres personnalisés peuvent être spécifiés.

Pour spécifier les paramètres personnalisés pour le poste, éditez la section correspondante des paramètres.

Si les paramètres personnalisés sont spécifiés pour le poste, les paramètres de la politique assignée ou du groupe primaire et toute leur modification n'auront pas d'impact sur les paramètres du poste.

Vous pouvez rétablir l'héritage de la politique ou du groupe primaire. Pour cela, cliquez sur le bouton  **Supprimer les paramètres personnalisés** se trouvant dans la barre d'outils du Centre de gestion, dans la section des paramètres correspondants ou dans la section des propriétés du poste.



Dans chaque section de paramètres des éléments de la configuration du poste s'affichent les informations sur la spécification des paramètres de cette section (s'il sont spécifiés de manière personnelle ou s'ils sont hérités de l'objet existant).



Une partie des sections contenant les paramètres peut être spécifiée et l'autre partie peut être héritée de la politique ou du groupe primaire, si la politique n'est pas spécifiée.

Vous pouvez spécifier des configurations différentes pour des [groupes](#) et des [postes](#) différents en modifiant les paramètres.

7.1. Héritage de la configuration du poste de travail

Lors de la création d'un poste ou d'un groupe, leurs paramètres sont toujours hérités :

- Le nouveau groupe hérite les paramètres de son groupe parent auquel il est inclus. S'il n'y a pas de groupe parent (le groupe créé est un groupe racine de l'arborescence), les paramètres sont hérités du groupe **Everyone**.
- Le nouveau poste hérite les paramètres de la politique qui a été assignée lors de la création du poste. Si la politique n'a pas été assignée, les paramètres sont hérités d'un des groupes auxquels il appartient. Un tel groupe s'appelle le groupe *primaire*.

Lors du fonctionnement ultérieur, l'héritage peut être interrompu et les paramètres personnalisés peuvent être spécifiés.

Pour le composant Contrôle des applications, le principe d'héritage des paramètres se distingue du principe standard. Pour en savoir plus, voir [Héritage des paramètres du composant Contrôle des applications](#).

Priorité d'application des paramètres pour les postes :

1. Si les paramètres personnalisés sont spécifiés pour le poste, on utilise les paramètres personnalisés. Dans ce cas, une politique peut être assignée au poste. Si vous spécifiez les paramètres d'une section particulière, l'héritage des paramètres de cette section est interrompu.
2. S'il n'y a pas de paramètres personnalisés, les paramètres de la politique assignée sont utilisés.
3. S'il n'y a pas de paramètres personnalisés ni de la politique assignée, le poste utilise les paramètres du groupe primaire.

Les paramètres personnalisés sont spécifiés	La politique est assignée	Paramètres utilisés
+	+	Configurations personnalisées
+	-	Configurations personnalisées
-	+	Paramètres de la politique



Les paramètres personnalisés sont spécifiés	La politique est assignée	Paramètres utilisés
–	–	Paramètres du groupe primaire



Le poste peut n'avoir aucune politique, mais il a toujours un groupe primaire.

Héritage des paramètres de postes des politiques

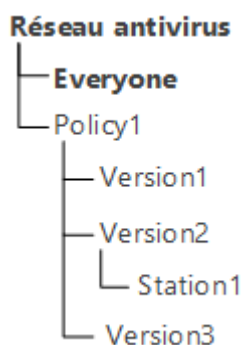
Si une politique est assignée au poste, l'héritage des paramètres de la politique est établi pour le poste.

En cas de modifications des paramètres de la politique, ces modifications sont héritées par les postes auxquels la politique est assignée, sauf les cas où les paramètres personnalisés sont spécifiés pour les postes. Lors de la création d'un poste, vous pouvez indiquer quelle politique sera assignée au poste. La politique peut être remplacée à tout moment du travail. Si aucune politique n'est assignée, les paramètres seront hérités du groupe primaire.

Les politiques n'ont pas de structure hiérarchique de l'héritage. Une fois une politique créée, ses paramètres sont copiés de l'objet spécifié (par défaut c'est la politique **Default policy**) en tant que les paramètres personnalisés. Une seule version de la politique sert de la version actuelle et ses paramètres sont les paramètres de la politique-même. Seule la version actuelle peut être assignée aux postes.

Exemple :

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



Pour le poste `Station1` la politique `Policy1` est assignée. La version `Version2` est actuelle pour la politique `Policy1`. Les paramètres de la version `Version2` sont équivalents aux paramètres de la politique `Policy1` qui sont personnalisés.



Héritage des paramètres de postes des politiques

Si une politique n'est pas assignée au poste, l'héritage des paramètres du groupe primaire est établi pour le poste.

En cas de modifications apportées dans la configuration du groupe primaire, elles seront héritées par les postes appartenant au groupe, excepté le cas où les postes possèdent des configurations personnalisées. A la création du poste, vous pouvez indiquer quel groupe sera désigné comme primaire. Par défaut, c'est le groupe **Everyone**. Le groupe primaire peut être remplacé à tout moment de travail.



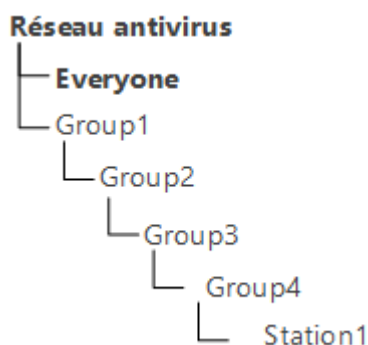
Si le groupe primaire n'est pas le groupe **Everyone** et n'a pas de configuration personnalisée, les configurations du groupe **Everyone** seront héritées.

Il est possible de créer des groupes emboîtés.

En cas de groupes emboîtés, si la configuration du poste n'est pas personnalisée, l'héritage des éléments de configuration se fait selon la structure des groupes emboîtés. La recherche se déroule vers le haut de l'arborescence à partir du groupe primaire du poste, son groupe supérieur et jusqu'à l'élément racine de l'arborescence. Dans le cas où aucune configuration personnalisée n'est trouvée, les paramètres de configuration du groupe **Everyone** seront hérités.

Exemple :

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




Le groupe `Group4` est un groupe primaire pour le poste `Station1`. Dans ce cas lors de l'héritage de paramètres le poste `Station1` va effectuer la recherche de paramètres dans l'ordre suivant : `Station1` → `Group4` → `Group3` → `Group2` → `Group1` → `Everyone`.



Par défaut, la structure du réseau est présentée de façon à ce que l'on puisse voir tous les groupes dont le poste fait partie. Si vous souhaitez afficher seulement l'appartenance aux



groupes primaires, décochez la case **Appartenance à tous les groupes** dans la rubrique  **Configuration de l'arborescence** dans la barre d'outils du Centre de gestion.

Héritage des paramètres du composant Contrôle des applications

Les paramètres des profils du Contrôle des applications peuvent être assignés non seulement aux postes et aux groupes de postes, mais aussi aux utilisateurs et aux groupes d'utilisateurs isolés.

Priorité d'application des paramètres :

1. S'il y a des paramètres utilisateurs, ils ont la plus haute priorité.
2. Si les paramètres utilisateurs sont manquants, la priorité est accordée aux paramètres du groupe d'utilisateurs.
3. Si les paramètres pour les utilisateurs et les groupes d'utilisateurs ne sont pas spécifiés, l'héritage se fait selon la [priorité d'application des paramètres pour les postes](#).

7.2. Groupes

Le mécanisme de groupes est conçu pour faciliter la gestion des postes de travail dans le réseau antivirus.

La fusion des postes en groupes permet d'effectuer les actions suivantes :

- Exécution des opérations de groupe sur tous les postes faisant partie des groupes concernés.
Pour un groupe sélectionné ainsi que pour plusieurs groupes, vous pouvez lancer, consulter et arrêter les tâches de scan sur les postes faisant partie du groupe correspondant. Vous pouvez également consulter les statistiques (y compris les infections, virus, procédures de démarrage/arrêt, erreurs de scan et d'installation, etc.) ainsi que les statistiques sommaires relatives à tous les postes du groupe ou à plusieurs groupes.
- Configuration des paramètres communs pour des postes via le groupe dont ils font partie (voir [Chapitre 7 : Gestion globale des postes de travail](#)).
- Organisations (de structuration) de la liste des postes de travail.

Il est possible de créer des groupes emboîtés.



7.2.1. Groupes système et groupes utilisateur

Groupes système

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

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



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

Everyone

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

Active Directory

Le groupe contient les utilisateurs et les groupes d'utilisateurs enregistrés dans le domaine Active Directory. Ce groupe apparaît dans l'arborescence du réseau antivirus, une fois la tâche **Synchronisation avec Active Directory** de la [planification](#) du Serveur Dr.Web accomplie.

Configured

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

Neighbors

Le groupe **Neighbors** comprend tous les Serveurs Dr.Web liés à ce Serveur Dr.Web et sert à gérer les liaisons entre les Serveurs Dr.Web dans un réseau antivirus en contenant plusieurs (voir [Particularités du réseau avec plusieurs Serveurs Dr.Web](#)).

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



Le groupe **Neighbors** comprend les groupes imbriqués affichant le statut des Serveurs voisins Dr.Web connectés à ce Serveur Dr.Web :

- Le groupe **All neighbors** comprend tous les Serveurs Dr.Web voisins connectés à ce Serveur Dr.Web.
- Le groupe **Children** comprend les Serveurs Dr.Web subordonnés.
- Le groupe **Offline** comprend les Serveurs Dr.Web inactifs en ce moment.
- Le groupe **Online** comprend les Serveurs Dr.Web actifs en ce moment.
- Le groupe **Parents** comprend les Serveurs Dr.Web principaux.
- Le groupe **Peers** comprend les Serveurs Dr.Web égaux.

Operating system

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

- Sous-groupes de la famille **Android**. Cette famille contient un jeu de groupes correspondant à une version particulière du système d'exploitation Android pour les appareils mobiles.
- Sous-groupes de la famille **macOS**. Cette famille contient un jeu de groupes correspondant à une version particulière du système d'exploitation macOS.
- Sous-groupes de la famille **UNIX**. Cette famille contient un jeu de groupes correspondant aux systèmes d'exploitation de la famille UNIX, par exemple Linux, FreeBSD, etc.
- Sous-groupes de la famille **Windows**. Cette famille contient un jeu de groupes correspondant à une version particulière du système d'exploitation Windows.
- Catégorie **Unknown OS**. Ici sont affichés les postes fonctionnant sous un système d'exploitation inconnu pour le Serveur Dr.Web.

Policies

Groupe contenant les politiques pour configuration des postes.



Le groupe **Policies** sera affiché dans l'arborescence du réseau antivirus uniquement si l'utilisation des politiques est autorisée dans la configuration du Serveur Dr.Web.

Profiles

Groupe contenant les profils de paramètres du composant Contrôle des applications pour les postes tournant sous l'OS Windows. Voir [Profils](#).



Proxies

Groupe contenant les Serveurs proxy Dr.Web pour la connexion des Agents Dr.Web et des Serveurs voisins Dr.Web.

Status

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

- Groupe **Deinstalled**. Une fois le logiciel de l'Agent Dr.Web est désinstallé, le poste passe automatiquement en groupe **Deinstalled**.
- Le groupe **Deleted** comprend les postes qui ont été précédemment supprimés depuis le Serveur Dr.Web par l'administrateur. Ces postes peuvent être restaurés (voir [Suppression et restauration d'un poste](#)).
- Le groupe **New** comprend les nouveaux postes qui ont été créés par l'administrateur via le Centre de gestion, mais on n'a pas encore installé l'Agent Dr.Web sur ces postes.
- Le groupe **Newbies** contient tous les postes dont l'enregistrement sur le Serveur Dr.Web n'est pas encore confirmé. Une fois l'enregistrement sur le Serveur Dr.Web réussi, les postes seront retirés du groupe de manière automatique (pour en savoir plus, voir [Politique d'approbation des postes](#)).
- Le groupe **Offline** comprend tous les postes inactifs en ce moment.
- Le groupe **Online** comprend tous les postes actifs en ce moment (répondant aux requêtes du Serveur Dr.Web).
- Le groupe **Update Errors** comprend tous les postes dont la mise à jour a échoué.

Transport

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

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

Ungrouped

Le groupe comprend les postes qui n'appartiennent à aucun groupe utilisateur.



Groupes utilisateurs

Ce sont les groupes déterminés par l'administrateur du réseau antivirus. L'administrateur peut créer ses propres groupes ainsi que des groupes emboîtés et y ajouter des postes. Dr.Web Enterprise Security Suite n'a aucune limitation concernant les composants ou le nom des groupes.

Pour plus de commodité, le tableau 7-1 comprend tous les groupes et les types de groupes possibles ainsi que les paramètres typiques qui sont supportés (+) ou ne sont pas supportés (-) par ces groupes.

Les paramètres suivants sont décrits :

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

Tableau 7-1. Groupes et paramètres supportés

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



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



7.2.2. Gestion des groupes

7.2.2.1. Création et suppression des groupes

Pour créer un nouveau groupe

1. Dans le menu principal du Centre de gestion, sélectionnez l'élément **Réseau antivirus**.
2. Sélectionnez l'élément **+ Ajouter un objet de réseau** dans la barre d'outils, puis dans le sous-menu qui apparaît, sélectionnez l'élément **+ Créer un groupe**.
La fenêtre de création d'un groupe va s'ouvrir.
3. Le champ de saisie **Identificateur** sera rempli automatiquement. Si nécessaire, vous pouvez l'éditer lors de la création. L'identificateur ne doit pas contenir d'espaces. Vous ne pourrez pas le modifier ultérieurement.
4. Saisissez le nom du groupe dans le champ **Nom**.
5. Pour les groupes emboîtés, dans le champ **Groupe supérieur**, sélectionnez depuis la liste déroulante un groupe à spécifier en tant que parent. Si aucune configuration personnalisée n'est spécifiée, c'est depuis ce groupe que les configurations seront héritées. Pour le groupe racine (qui n'a pas de parent) laissez ce champ vide, le groupe sera ajouté dans la racine de l'arborescence. Dans ce cas, les configurations seront héritées depuis le groupe **Everyone**.
6. Laissez un commentaire dans le champ **Description**.
7. Cliquez sur **Enregistrer**.

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

Pour supprimer un groupe existant

1. Sélectionnez le groupe dans l'arborescence Centre de gestion.
2. Dans la barre d'outils, cliquez sur **★ Général** → **✗ Supprimer les objets sélectionnés**.



Il est impossible de supprimer les groupes pré-installés.

7.2.2.2. Configuration des groupes

Pour configurer le groupe, procédez comme suit

1. Sélectionnez l'élément **Réseau antivirus** dans le menu principal du Centre de gestion, puis dans la fenêtre qui apparaît, sélectionnez un groupe dans l'arborescence.
2. Ouvrez la rubrique de configuration du groupe d'une des façons suivantes :



- a) Cliquez sur le nom du groupe dans la liste hiérarchique du réseau antivirus. La section contenant les propriétés du groupe va s'afficher automatiquement dans la partie droite du Centre de gestion.
 - b) Sélectionnez l'élément **Propriétés** [du menu de gestion](#). La fenêtre contenant les propriétés du groupe de postes va s'ouvrir.
3. La fenêtre de configuration du groupe comprend les onglets **Général** et **Configuration** dont vous trouverez la description et le paramétrage ci-après.



Lors de l'ouverture des propriétés du poste depuis la partie droite du Centre de gestion (voir p. 2.a), vous pouvez accéder à la rubrique **Informations sur les postes** affichant des informations sur les postes faisant partie du groupe en question.

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

Général

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

- **Identificateur** : identificateur unique du groupe. Il est protégé contre l'édition.
- **Nom** : nom du groupe. Si nécessaire, vous pouvez le modifier. Pour les groupes préinstallés, le champ **Nom** ne peut pas être modifié.
- **Groupe parent** : le groupe parent dont le groupe en question fait partie et duquel il hérite sa configuration à moins que les paramètres personnalisées ne soient spécifiées. Si aucun groupe supérieur n'est spécifié, les configurations seront héritées depuis le groupe **Everyone**.
- **Description** : champ facultatif contenant une description du groupe.

Informations sur les postes

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

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

Organisation

Si lors de la création du groupe vous avez désigné le groupe comme représentant d'une organisation ou d'une entreprise, la rubrique **Organisation** vous sera disponible pour modification. Dans cette rubrique vous pourrez modifier les références de l'entreprise que ce groupe représente. Le jeu de références peut varier en fonction du pays où se trouve l'organisation.



Vous pouvez désigner le groupe comme représentant de l'organisation uniquement lors de la création du groupe. Il est impossible d'annuler cette caractéristique après la création du groupe.

Configuration



Pour plus d'informations sur l'héritage des paramètres des groupes primaires par les postes, voir la rubrique [Chapitre 7 : Gestion globale des postes de travail](#).

La rubrique **Configuration** vous permet de modifier les paramètres suivants :

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

Le nombre des groupes emboîtés avec l'héritage interrompu et leurs propres paramètres personnels (s'il y en a) est indiqué dans la section **Configuration** pour les groupes dont les



paramètres personnels sont spécifiés. Si vous cliquez sur cette option, dans la fenêtre qui s'affiche, vous trouverez la liste des groupes dont les noms et les identificateurs sont indiqués.

7.2.3. Placement des postes dans les groupes

Paramétrage du groupe primaire

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

Paramétrer un groupe primaire pour un poste de travail :

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

Pour spécifier un groupe primaire pour plusieurs postes de travail :

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

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

Placement dans les groupes utilisateurs

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

1. [Placement manuel de postes dans des groupes](#).



2. [Utilisation des règles d'appartenance automatique au groupe.](#)

7.2.3.1. Placement manuel de postes dans des groupes

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

1. [Modification des paramètres du poste.](#)
2. [Glisser-déposer le poste dans la liste hiérarchique.](#)

Pour éditer la liste des groupes dont le poste fait partie via la configuration du poste, procédez comme suit :

1. Sélectionnez l'élément **Réseau antivirus** dans le menu principal, puis dans la fenêtre qui apparaît cliquez sur le nom du poste dans la liste hiérarchique.
2. Le panneau des propriétés du poste va s'ouvrir. Vous pouvez également ouvrir la rubrique des propriétés du poste en cliquant sur l'élément **Propriétés** du [menu de gestion](#).
3. Dans le panneau affiché **Propriétés du poste** passez à l'onglet **Groupes**.
La liste **Appartenance** à contient les groupes dont le poste fait déjà partie.
4. Pour ajouter un poste au groupe utilisateur, cochez la case contre ce groupe dans la liste **Appartenance**.
5. Pour supprimer un poste du groupe utilisateur, cliquez sur le nom du groupe dans la liste **Appartenance**.



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

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

Dans la rubrique **Propriétés** du poste, vous pouvez également spécifier un groupe primaire pour le poste (pour en savoir plus, voir [Héritage de la configuration du poste de travail](#)).

Pour éditer la liste des groupes dont le poste fait partie via l'arborescence, procédez comme suit :

1. Sélectionnez l'élément **Réseau antivirus** du menu principal et ouvrez l'arborescence des groupes et des postes.
2. Pour ajouter un poste au groupe utilisateur, pressez la touche CTRL et tout en maintenant la touche, glissez-déposez du poste vers le groupe choisi.
3. Pour déplacer le poste d'un groupe utilisateur vers un autre groupe, glissez-déposez le poste depuis le groupe utilisateur (duquel le poste sera supprimé) vers l'autre groupe utilisateur (où le poste sera ajouté).



En cas de déplacement du poste depuis un groupe pré-installé selon les variantes 2 ou 3, le poste sera ajouté au groupe utilisateur mais ne sera pas supprimé du groupe pré-installé.

7.2.3.2. Configuration de l'appartenance automatique au groupe

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

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

1. Sélectionnez l'élément **Réseau antivirus** du menu principal du Centre de gestion.
2. Dans la liste hiérarchique du réseau antivirus, sélectionnez le groupe utilisateur pour lequel vous voulez spécifier les règles d'appartenance.
3. Passez à la rubrique d'édition des règles d'appartenance par un des moyens suivants :
 - Dans le panneau de propriétés dans la partie droite de la fenêtre, cliquez sur **🔽 Règles d'appartenance au groupe** dans la rubrique **Configuration**.
 - Dans le [menu de gestion](#), sélectionnez l'élément **Règles d'appartenance au groupe** dans la section **Général**.
 - Dans le [menu de gestion](#), sélectionnez l'élément **Propriétés** dans la section **Général**, puis passez à l'onglet **Configuration** et cliquez sur **🔽 Règles d'appartenance au groupe**.
4. Postes en réseau : nombre de postes dans ce groupe qui sont en réseau (online) en ce moment :
 - a) Si les règles d'appartenance n'étaient pas spécifiées précédemment, cliquez sur **Ajouter une règle**.
 - b) Cochez la case **Spécifier le groupe comme primaire** pour que le groupe pour lequel la règle est créée soit désigné comme primaire pour tous les postes qui seront déplacés dans ce groupe d'après cette règle.
 - c) Sélectionnez une option déterminant comment les règles seront appliquées : **Appliquer les règles après leur enregistrement** ou **Appliquer les règles après la connexion de postes**.
 - d) Pour chaque bloc de règles spécifiez les paramètres suivants :
 - Sélectionnez une des options, déterminant le principe de regroupement de règles au sein d'un bloc : **Correspond à toutes les conditions**, **Correspond à n'importe quelle condition**, **Ne correspond à aucune condition**.
 - Dans la liste déroulante de conditions sélectionnez : un des paramètres du poste dont la conformité aux conditions sera vérifiée, le principe de conformité à cette condition, puis entrez la ligne de condition si cela est sous-entendu par le paramètre du poste. Les postes peuvent être rassemblés dans des groupes en fonction des conditions suivantes :



- **Adresse IP du poste** (un jeu de caractères contenus dans l'adresse IP, le sous-réseau dont elle fait partie ou une expression régulière) ;
- **description** (un jeu de caractères contenus dans la description ou une expression régulière) ;
- **ID du poste** (un jeu de caractères contenus dans l'ID ou une expression régulière) ;
- **novice** (les postes sont ajoutés dans le groupe en fonction de présence du statut de novice) ;
- **LDAP DN d'Active Directory** (un jeu de caractères contenus dans LDAP DN ou une expression régulière) ;





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


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

Il est possible de spécifier les expressions régulières uniquement pour la variante **correspond à l'expression régulière**. Pour les autres types, la recherche par correspondance exacte à la ligne entrée est utilisée.

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

- **système d'exploitation** installé sur le poste (Windows, UNIX, MacOS, Android et autres ; il existe également le paramètre « Inconnu ») ;
 - **numéro d'assemblage du système d'exploitation** (un jeu de caractères contenus dans le numéro ou une expression régulière) ;
 - **plateforme du poste** (version du système d'exploitation installé sur le poste ; uniquement pour Android, Windows et macOS) ;
 - **protocole de connexion** (TCP IP, TCP IPv6, UNIX) ;
 - **ID du serveur Dr.Web** (un jeu de caractères contenus dans l'ID ou une expression régulière) ;
 - **nom du poste** (un jeu de caractères contenus dans le nom ou une expression régulière) ;
 - **type de poste** (agent complet, agent virtuel, serveur de scan).
- Pour ajouter encore une condition dans ce bloc, cliquez  à droite de la ligne de condition.
- e) Pour ajouter un nouveau bloc de règles cliquez  à droite du bloc. Dans ce cas spécifiez le principe d'union de ce bloc de conditions avec d'autres blocs :
- **ET** : les conditions de blocs doivent être remplies en même temps.
 - **OU** : les conditions d'au moins un bloc doivent être remplies.






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



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

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

1. Sélectionnez l'élément **Réseau antivirus** du menu principal du Centre de gestion.
2. Dans la liste hiérarchique du réseau antivirus, sélectionnez le groupe utilisateur pour lequel vous voulez supprimer les règles d'appartenance.
3. Effectuez une des actions suivantes :
 - Dans la barre d'outils, cliquez sur le bouton  **Supprimer les règles d'appartenance**.
 - Dans le panneau de propriétés dans la partie droite de la fenêtre, cliquez sur  **Supprimer les règles d'appartenance** dans la rubrique **Configuration**.
 - Dans le [menu de gestion](#), sélectionnez l'élément **Propriétés** dans la section **Général**, puis passez à l'onglet **Configuration** et cliquez sur  **Supprimer les règles d'appartenance au groupe**.
4. Après la suppression des règles d'appartenance du groupe, tous les postes déplacés dans ce groupe conformément aux règles d'appartenance seront supprimés du groupe. Si ce groupe a désigné par l'administrateur comme primaire pour un de ces postes, c'est le groupe **Everyone** qui sera désigné comme primaire en cas de suppression des postes depuis le groupe.



7.2.4. Comparaison des postes et des groupes

Il existe une possibilité de comparer les postes et les groupes selon les paramètres principaux.

Pour comparer plusieurs objets du réseau antivirus

1. Sélectionnez l'élément **Réseau antivirus** dans le menu principal et sélectionnez ensuite depuis l'arborescence les objets que vous souhaitez comparer. Utilisez les touches CTRL et SHIFT. Les variantes ci-dessous sont possibles :
 - sélection de plusieurs postes — pour comparer les postes sélectionnés ;
 - sélection de plusieurs groupes — pour comparer les groupes sélectionnés et tous les groupes emboîtés ;
 - sélection de plusieurs postes et groupes — pour comparer tous les postes : les postes sélectionnés dans l'arborescence ainsi que ceux appartenant à tous les groupes sélectionnés et à leurs groupes emboîtés.
2. Dans le [menu de gestion](#), cliquez sur l'élément **Comparer**.
3. Le tableau comparatif pour les objets sélectionnés s'affichera.
 - Paramètres utilisés pour comparer les groupes :
 - **Postes** : total de postes appartenant à un groupe sélectionné.
 - **Postes sur réseau** : total de postes actifs au moment actuel.
 - **Groupe primaire pour** : total de postes pour lesquels ce groupe est un groupe primaire.
 - **Configuration personnalisée** : liste des composants pour lesquels les paramètres sont personnalisés et non hérités du groupe parent.
 - Paramètres utilisés pour comparer les postes :
 - **Date de création** du poste.
 - **Groupe primaire** pour le poste.
 - **Configuration personnalisée** : liste des composants pour lesquels les paramètres sont personnalisés et non hérités du groupe primaire.
 - **Composants installés** : liste des composants antivirus installés sur le poste.






7.2.5. Copie des configurations vers d'autres groupes/postes

Les configurations des outils antivirus, planifications, droits des utilisateurs ainsi que d'autres configurations de groupe ou de poste peuvent être copiées (diffusées) vers un groupe ou vers des groupes ou des postes.

Pour copier les paramètres

1. Cliquez sur le bouton **Diffuser les configurations vers un autre objet** :



-  dans la fenêtre d'édition de la configuration du composant antivirus,
-  dans la fenêtre d'édition de la planification,
-  dans la fenêtre d'édition des restrictions de mises à jour,
-  dans la fenêtre de composants à installer,
-  dans la fenêtre de configuration des droits d'utilisateurs.

L'arborescence du réseau antivirus sera affichée.

2. Sélectionnez dans l'arborescence les groupes et les postes vers lesquels vous souhaitez diffuser la configuration.
3. Afin de réaliser la modification de la configuration des groupes concernés, cliquez sur le bouton **Enregistrer**.

7.3. Politiques

La *politique* est un ensemble de tous les paramètres du poste : droits, planification des tâches, clés de licence, limitations des mises à jour, liste des composants installés, configuration des composants antivirus.



La politique peut être assignée uniquement aux postes.

Pour autoriser l'utilisation des politiques pour la configuration des postes

1. Sélectionnez l'élément **Administration** du menu principal du Centre de gestion, et dans la fenêtre qui s'ouvre, sélectionnez l'élément **Configuration du Serveur Dr.Web** du menu de gestion.
2. Dans l'onglet **Général** :
 - a) Cochez la case **Utiliser les politiques**.
 - b) Dans le champ **Nombre des versions de la politique**, spécifiez le nombre maximum des versions que l'on peut créer pour chaque politique. Si, lors de la création d'une nouvelle version de la politique, ce nombre est dépassé, la plus ancienne version de la politique sera supprimée.
3. Cliquez sur **Enregistrer** et redémarrez le Serveur Dr.Web.
4. Après l'autorisation de l'utilisation des politiques, la politique prédéfinie **Default policy** est créée. Cette politique ne peut pas être supprimée, mais vous pouvez l'éditer et l'assigner aux postes.



Pour pouvoir gérer les politiques et leurs paramètres, l'administrateur doit posséder les [droits Voir les propriétés et la configuration des politiques](#) et [Éditer les propriétés et la configuration des politiques](#).



Si les droits ne sont pas assignés, les politiques seront affichées dans l'arborescence du réseau antivirus et dans le Gestionnaire de licences, mais vous ne pouvez pas consulter leur contenu ou les gérer.

7.3.1. Gestion des politiques

Création d'une politique

Pour créer une nouvelle politique

1. Dans le menu principal du Centre de gestion, sélectionnez l'élément **Réseau antivirus**.
2. Sélectionnez l'élément **+ Ajouter un objet de réseau** dans la barre d'outils, puis dans le sous-menu qui apparaît, sélectionnez l'élément **+ Créer une politique**.
La fenêtre de création d'une politique va s'ouvrir.
3. Le champ de saisie **Identificateur** sera rempli automatiquement. Si nécessaire, vous pouvez l'éditer lors de la création. L'identificateur ne doit pas contenir d'espaces. Vous ne pourrez pas le modifier ultérieurement.
4. Spécifiez le nom de la politique dans le champ **Nom**.
5. Quand vous créez une politique, ses paramètres sont copiés par défaut de la politique **Default policy**. Pour modifier l'objet dont les paramètres seront copiés, cliquez sur la lien **Sélectionner un autre objet**. Dans la fenêtre qui s'affiche, sélectionnez un objet dans la liste déroulante. Cela peut être un groupe, un poste, une autre politique ou version de la politique. Un seul objet peut être sélectionné. Cliquez sur **Enregistrer**. Dans la fenêtre de création de la politique, l'objet sélectionné s'affichera.
6. Pour créer une politique avec les paramètres spécifiés, cliquez sur **Enregistrer**.
7. Quand vous créez une politique, une version de la politique correspondant à la date d'ajout de la politique est créée automatiquement.

Version de la politique

La politique peut contenir plusieurs versions, mais pas plus qu'indiqué dans les paramètres de la configuration du Serveur Dr.Web. Le nom de la version de la politique correspond à la date de sa création.

Pour créer une nouvelle version de la politique

1. Dans le menu principal du Centre de gestion, sélectionnez l'élément **Réseau antivirus**.
2. L'accès aux paramètres de la politique se fait par la liste hiérarchique du réseau antivirus. Éditez la configuration de la politique dont vous voulez créer une nouvelle version. Vous pouvez le faire manuellement ou avec l'importation/distribution de la configuration d'un autre objet du réseau antivirus (poste, groupe, politique).



3. Lors de l'enregistrement des modifications, la nouvelle version de la politique sera créée automatiquement à la base des paramètres de politique spécifiées. La version créée sera désignée actuelle.



Une seule version de la politique est considérée comme actuelle et peut être assignée aux postes.

Les paramètres de la version de la politique sont disponibles uniquement en lecture.

Pour modifier la version actuelle de la politique

1. Dans le menu principal du Centre de gestion, sélectionnez l'élément **Réseau antivirus**.
2. Dans la liste déroulante, sélectionnez la politique dont vous voulez modifier la version actuelle.
3. Sélectionnez la version nécessaire dans la liste déroulante **Versión actuelle**, de la section **Général** du panneau de propriétés de la politique.
4. Cliquez sur **Enregistrer**.

Suppression de la politique



Vous pouvez supprimer la version entière ou par versions.

Pour supprimer la politique ou la version de la politique

1. Dans le menu principal du Centre de gestion, sélectionnez l'élément **Réseau antivirus**.
2. Sélectionnez une politique ou une version de la politique dans la liste hiérarchique.
3. Dans la barre d'outils, cliquez sur **★ Général** → **✗ Supprimer les objets sélectionnés**.



Lors de la suppression de la politique, prenez en compte les particularités suivantes :

- Si la dernière version de la politique est supprimée, la politique même est supprimée.
- Si la version actuelle de la politique est supprimée, la dernière version (avec la date la plus récente) devient actuelle.
- La version actuelle de la politique sera assignée à tous les postes auxquels la version supprimée de la politique a été assignée.

7.3.2. Assignation d'une politique aux postes



Une seule politique peut être assignée pour le poste.



Seule la politique pour laquelle [la clé de licence est spécifiée](#) peut être assignée aux postes.

Pour assigner ou modifier la politique du poste

1. Dans le menu principal du Centre de gestion, sélectionnez l'élément **Réseau antivirus**.
2. Dans la liste hiérarchique, sélectionnez un poste pour lequel vous voulez assigner ou modifier la politique.
3. Dans le panneau affiché des propriétés du poste, dans la section **Groupes**, dans la liste **Politique**, cochez la case contre la politique à assigner.

Si une politique a été assignée auparavant, sa case sera automatiquement décochée, car une seule politique peut être assignée au poste.

Vous pouvez également décocher toutes les cases. Dans ce cas, les paramètres du postes seront restaurés dans l'état avant l'assignation de la politique.

4. Cliquez sur **Enregistrer**.

7.4. Profils

Les *Profils* déterminent les paramètres du composant [Contrôle des applications](#). C'est selon ces paramètres que les applications, les modules, les modules, les interpréteurs de scripts, les pilotes et les packages MSI seront lancés ou bloqués sur les postes .

Les profils sont créés par l'administrateur et ils sont assignés aux politiques, postes, utilisateurs, y compris aux groupes de postes et d'utilisateurs. Les profils déterminent le [mode de fonctionnement](#) du Contrôle des applications.

La configuration des profils se fait dans l'arborescence du réseau antivirus :

- Tous les profles sont placés dans le groupe prédéfini **Profils**.
- Les objets, auxquels un profil est assigné, sont placés dans l'arborescence du réseau antivirus en tant qu'éléments enfants de ce profil.

Pour configurer le Contrôle des applications

1. [Créez un nouveau profil](#).
2. [Spécifiez les paramètres du profil](#).
3. [Assignez le profil aux objets nécessaires](#).



Il est recommandé de configurer les profils en mode de test.



On distingue les mode de fonctionnement suivants :

- **Désactivé** : le profil n'est pas activé, les paramètres du profil ne s'appliquent pas.
- **Actif** : le profil est activé, les paramètres s'appliquent aux objets auxquels le profil est appliqué.
- **Test global** : le profil est activé, mais il fonctionne en mode test global. Le mode test imite le fonctionnement du Contrôle des applications avec une journalisation complète de l'activité (voir [Événements du Contrôle des applications](#)), pourtant le blocage des applications ne se fait pas.
- **Test pour les règles** : le profil est actif, mais seuls les paramètres de l'analyse fonctionnelle et des règles s'appliquent aux objets. Pourtant, les règles qui fonctionnent en mode test n'influencent pas le blocage d'applications. Le résultat du fonctionnement qu'elles imitent est enregistré dans le journal d'activité (voir [Événements du Contrôle des applications](#)). Le mode test pour les règles peut être activé ou désactivé dans la section de paramètres des règles de blocage et d'autorisation.

Le tableau ci-dessous indique quels paramètres spécifient un tel ou tel mode de fonctionnement du profil.

Mode	Désactivé	Actif	Test global	Test pour les règles
Paramètre				
Général → Activer le profil	–	+	+	+
Général → Faire basculer le profil en mode test global	non active	–	+	–
<Mode> → <Règle> → Activer la règle	non active	+/-	+/-	+
<Mode> → <Règle> → Faire basculer la règle en mode test	non active	–	+/-	+

Conventions

+	le paramètre doit être activé
–	le paramètre doit être désactivé
+/-	le paramètre n'a pas d'importance
non active	le paramètre n'est pas disponible pour la modification



7.4.1. Création et assignation de profils

Pour créer un nouveau profil

1. Dans le menu principal du Centre de gestion, sélectionnez l'élément **Réseau antivirus**.
2. Dans la fenêtre qui s'affiche, dans la barre d'outils, sélectionnez l'élément **+ Ajouter un objet de réseau** → **+ Créer un profil**.
3. Dans le panneau qui s'ouvre, spécifiez le **Nom de profil**. Plus tard, vous pourrez le modifier dans la section des paramètres [Général](#), si cela est nécessaire.
4. Cliquez sur **Enregistrer**.
5. Le nouveau profil sera créé et placé dans le groupe **Profils**.

Pour assigner le profil à un objet

1. Dans le menu principal du Centre de gestion, sélectionnez l'élément **Réseau antivirus**.
2. Dans la fenêtre qui s'affiche, sélectionnez le profil que vous voulez assigner dans la liste hiérarchique.
3. Dans la barre d'outils, cliquez sur **Données et configuration** → **Assigner le profil**.

Dans la fenêtre qui s'ouvre, sélectionnez l'objet de distribution des paramètres :

- L'onglet **Active Directory** contient les listes équivalentes à la liste de l'arborescence du réseau antivirus mise à jour selon la tâche **Synchronisation avec Active Directory** de la [planification](#) du Serveur Dr.Web. Les listes contiennent les mêmes objets mais elles se distinguent pas le type des objets auxquels le profil sera assigné :
 - Dans la liste **Postes Active Directory**, vous pouvez sélectionner les groupes de postes ou les postes isolés enregistrés dans le domaine Active Directory.
 - Dans la liste **Utilisateurs d'Active Directory**, vous pouvez sélectionner les groupes d'utilisateurs et les utilisateurs particuliers enregistrés dans le domaine Active Directory.



Les mêmes objets ne doivent pas être sélectionnés dans les listes différentes.

- Dans l'onglet **Réseau antivirus**, vous pouvez sélectionner les objets suivants :
 - Groupes de postes. Dans ce cas, les paramètres seront appliqués aux comptes de tous les utilisateurs de tous les postes inclus dans ces groupes.
 - Postes particuliers dans des groupes. Dans ce cas, les paramètres seront appliqués aux comptes de tous les utilisateurs des postes sélectionnés.
 - Politiques dans le groupe **Politiques**. Dans ce cas, les paramètres seront appliqués aux comptes de tous les utilisateurs des postes auxquels la politique sélectionnée a été assignée.



- Dans l'onglet **Utilisateurs locaux** vous pouvez sélectionner un groupe d'utilisateurs ou des utilisateurs individuels sur les postes. Dans ce cas, les paramètres seront appliqués uniquement aux comptes des utilisateurs sélectionnés sur ces postes.

Pour en savoir plus sur la priorité d'assignation des profils, voir la rubrique [Héritage de la configuration du poste de travail](#).

4. Cliquez sur le bouton **Enregistrer**. Tous les objets sélectionnés seront ajoutés dans la liste à laquelle le profil configuré s'applique (ils s'affichent dans l'arborescence en tant qu'objets emboîtés de ce profil).

Pour arrêter la distributions des paramètres du profils à l'objet

1. Dans le menu principal du Centre de gestion, sélectionnez l'élément **Réseau antivirus**.
2. Dans la fenêtre qui s'affiche, dans la liste hiérarchique, ouvrez la liste des objets emboîtés du profil et sélectionnez l'objet pour lequel vous voulez annuler l'assignation du profil.
3. Dans la barre d'outils, cliquez sur **Général** → **Annuler l'assignation du profil**.

7.4.2. Configuration des profils

Pour configurer le profil

1. Dans le menu principal du Centre de gestion, sélectionnez l'élément **Réseau antivirus**.
2. Ouvrez la rubrique de configuration du profil d'une des façons suivantes :
 - a) Cliquez sur le nom du profil dans la liste hiérarchique du réseau antivirus. Le panneau contenant les propriétés du profil va s'afficher automatiquement dans la partie droite du Centre de gestion.
 - b) Cliquez sur l'icône du profil dans l'arborescence du réseau antivirus ou sélectionnez le profil. Ensuite, sélectionnez l'élément **Propriétés du menu de gestion**. Une fenêtre contenant les propriétés du poste va s'ouvrir.
3. Dans la section **Général**, les principes de fonctionnement du profil sont spécifiés :
 - Dans le champ **Nom de profil**, vous pouvez changer le nom de profil.
 - Cochez la case **Activer le profil** pour commencer à utiliser ce profil.
 - Si la case **Faire basculer le profil en mode test global** est cochée, seule l'activité sera journalisée comme si les paramètres étaient activés. Vous pouvez utiliser ce mode pour le débogage du profil.
 - Dans la section [Analyse fonctionnelle](#) spécifiez les ensembles des règles prédéfinies selon lesquelles le lancement des applications sera autorisé ou interdit.
4. Pour appliquer les paramètres spécifiés dans la section **Général**, cliquez sur **Enregistrer** dans les paramètres du profil.
5. La section **Mode d'autorisation** contient des informations récapitulatives sur les paramètres du mode : nombre de règles d'autorisation et de groupes d'applications de confiance assignées à ce profil. Afin d'activer ou désactiver le mode ou configurer les règles et les



applications de confiance, cliquez sur le lien [Mode d'autorisation](#) pour accéder à la section correspondante.

6. La section **Mode de blocage** contient des informations récapitulatives sur les paramètres du mode : nombre de règles de blocage créées. Afin d'activer ou désactiver le mode ou configurer les règles, cliquez sur le lien [Mode de blocage](#) pour accéder à la section correspondante.

Prenez en compte les particularités suivantes du profil du **Contrôle des applications** :

- Si aucun critère de la section **Critères de l'analyse fonctionnelle** n'est activé, le profil sera désactivé.
- Si, lors de la configuration des paramètres du profil, les paramètres avancés ne sont pas spécifiés pour un critère de la section **Critères de l'analyse fonctionnelle** et que le mode de blocage et le mode d'autorisation sont désactivés, cette configuration ne sera pas sauvegardée.
- Si aucune règle d'autorisation, ni application de confiance n'est spécifiée, le mode d'autorisation sera désactivé.
- Si les règles d'autorisation ne sont pas spécifiées, le mode de blocage sera désactivé.

7.4.2.1. Analyse fonctionnelle

Analyse fonctionnelle spécifie l'ensemble des règles prédéfinies selon lesquelles le lancement des applications est autorisé ou bloqué conformément aux fonctions exécutées.

La configuration des paramètres de l'analyse fonctionnelle se fait dans la section des [propriétés](#) du profil **Général** → **Critères de l'analyse fonctionnelle**.



Si aucun critère de la section **Critères de l'analyse fonctionnelle** n'est activé, le profil sera désactivé.

Si les paramètres avancés ne sont pas spécifiés pour un critère de la section **Critères de l'analyse fonctionnelle** et que le mode de blocage et le mode d'autorisation sont désactivés, le profil sera désactivé.

Pour configurer l'analyse fonctionnelle

1. Dans la section **Critères de l'analyse fonctionnelle**, cochez les cases contre les catégories que vous voulez utiliser :
 - **Lancement d'applications,**
 - **Téléchargement et exécution des modules,**
 - **Lancement des interpréteurs de script,**
 - **Téléchargement de pilotes,**
 - **Installation des paquets MSI,**




▫ Intégrité de fichiers exécutable.



Si vous configurez le profil pour la première fois, les catégories d'autorisation sont activées automatiquement dans les paramètres avancés de chaque critère lors de son activation.

Cet outil est utilisé comme mesure de sécurité au cas où les objets du système d'exploitation nécessaires pour le fonctionnement des postes seraient bloqués après l'application des paramètres du mode de blocage ou du mode d'autorisation.

Plus tard vous pourrez désactiver ces catégories d'autorisation dans les paramètres avancés si cela est nécessaire.

2. Pour spécifier les paramètres avancés selon le critère sélectionné, cliquez sur  **Éditer** contre le critère correspondant. Une fenêtre contenant une liste de paramètres va s'afficher. La configuration de l'analyse fonctionnelle peut autoriser ou bloquer le lancement d'applications.
Cochez les cases des paramètres qui doivent être exécutés.
3. Si vous activez l'utilisation d'un critère mais ne spécifiez pas ses paramètres avancés, le contrôle de lancement sera effectué pour tous les objets selon ce critère conformément aux paramètres du mode d'autorisation ou du mode de blocage.
Exemple :
 - Si le critère **Lancement des interpréteurs de script** est spécifié, mais que ses paramètres avancés ne sont pas spécifiés, le lancement de tous les interpréteurs de script sera contrôlé conformément aux paramètres spécifiés pour le mode de blocage et le mode d'autorisation.
 - Si le critère **Lancement des interpréteurs de script** est spécifié, et que le paramètre avancé **Bloquer le lancement des scripts depuis les supports amovibles** est également configuré, seul le lancement de scripts depuis les supports amovibles sera bloqué.
4. Si vous spécifiez les paramètres avancés mais n'activez pas l'utilisation du critère, ni les paramètres avancés ni le critère ne seront réalisés.
5. Pour enregistrer les paramètres avancés, cliquez sur **Enregistrer** dans la fenêtre contenant la liste de paramètres avancés.
6. Pour enregistrer les paramètres de l'analyse fonctionnelle, cliquez sur **Enregistrer** dans la fenêtre de configuration du profil.

7.4.2.2. Mode d'autorisation

Le *Mode d'autorisation* implique que le lancement des applications de la liste des **Applications de confiance** et/ou des applications relevant des règles d'autorisation est autorisé sur tous les postes contrôlés. Les autres applications sont bloquées conformément aux critères de l'analyse fonctionnelle.

Le mode d'autorisation peut être activé même si seuls les règles d'autorisation fonctionnent. Dans ce cas, le mode d'autorisation sera un supplément de l'analyse fonctionnelle permettant de lancer certaines applications de la liste d'applications interdites. Par exemple, si le



lancement d'applications à partir du réseau et de ressources partagées est interdit dans les critères de l'analyse fonctionnelle, mais le lancement de l'application est autorisé dans les règles d'autorisation, l'application sera lancée tandis que les autres applications resteront bloquées.

Vous pouvez modifier les règles d'autorisation et les applications de confiance dans les [propriétés](#) du profil, dans l'onglet **Mode d'autorisation**.

Pour utiliser le mode d'autorisation

1. Cochez la case **Utiliser le mode d'autorisation** dans l'onglet **Mode d'autorisation**.
2. Spécifiez les paramètres dans au moins une section :
 - [Règles d'autorisation](#).
 - [Applications de confiance](#).
3. Cliquez sur **Enregistrer**.



Si aucune règle d'autorisation, ni application de confiance n'est spécifiée, le mode d'autorisation sera désactivé.

Règles d'autorisation

Vous pouvez modifier les règles d'autorisation dans la section de [propriétés](#) du profil **Mode d'autorisation** → **Règles d'autorisation**.

Pour créer une nouvelle règle d'autorisation

1. Dans la section **Règles d'autorisation** cliquez sur le bouton **+ Créer une règle** dans la barre d'outils.
2. Dans la fenêtre **Ajout d'une règle**, spécifiez **Nom de la règle** et cliquez sur **Enregistrer**.
3. Dans la liste des règles, sélectionnez la règle créée et configurez ses paramètres dans le panneau de propriétés qui s'affiche :
 - a) Cochez la case **Activer la règle** pour commencer à utiliser cette règle.
 - b) Si vous voulez tester la règle, cochez la case **Faire basculer la règle en mode test**. Les applications sur les postes ne seront pas contrôlées, pourtant l'activité sera journalisée comme si les paramètres étaient activés. Les résultats de lancements et de blocages d'applications en mode test s'afficheront dans la section [Événements du Contrôle des applications](#).
Si la case **Faire basculer la règle en mode test** est décochée, la règle fonctionnera en mode actif avec le lancement des applications sur les postes conformément aux paramètres de règle spécifiés (voir aussi les [modes de fonctionnement des profils](#)).
 - c) Dans la section **Autoriser le lancement des applications selon les critères suivants**, sélectionnez les options selon lesquelles le lancement des applications sur les postes sera



autorisé. Dans le champ **Nom de fichier**, indiquez le nom de fichier ou le répertoire. Les variables d'environnement et les masques sont pris en charge. Vous pouvez :

- Indiquer un fichier ou un dossier.
 - pour indiquer un dossier ou un fichier particulier dans ce dossier, saisissez le chemin d'accès complet au fichier ou au dossier dans le champ de saisie.
 - pour ajouter un fichier avec un nom particulier, saisissez le nom de fichier y compris l'extension dans le champ de saisie. Si le chemin n'est pas indiqué, le paramètre sera considéré comme fichier au nom indiqué quelle que soit sa localisation.
 - `C:\folder\file.exe` : ajoute le fichier `file.exe` se trouvant dans le dossier `C:\folder` aux autorisés.
 - `C:\folder` : ajoute tous les sous-dossiers et les fichiers se trouvant dans le dossier `C:\folder` aux autorisés.
 - `file.exe` : ajoute aux autorisés tous les fichiers avec le nom `file` et l'extension `.exe` dans tous les dossiers.
 - `file` : ajoute tous les fichiers avec le nom `file` sans extension dans tous les dossiers.
- Utiliser le masque qui désigne la partie commune du nom de l'objet, dans ce cas :
 - le caractère « * » remplace toute séquence (potentiellement vide) de caractères ;
 - le caractère « ? » remplace n'importe quel caractère (un seul caractère).
 - `C:\Program Files\folder*.exe` : ajoute aux autorisés les applications dans le dossier `C:\Program Files\folder`.
 - `C:\Program Files**.exe` : ajoute aux autorisés uniquement les applications dans les sous-dossiers du premier niveau d'emboîtement du dossier `C:\Program Files`.
 - `C:\Program Files***.exe` : ajoute aux autorisés les applications dans les sous-dossiers de tout niveau d'emboîtement du dossier `C:\Program Files`.
 - `C:\Program Files\folder\exam*.exe` : ajoute aux autorisés toutes les applications du dossier `C:\Program Files\folder` dont les noms commencent par `exam`.
 - `example.exe` : ajoute aux autorisés toutes les applications avec le nom `example` et l'extension `.exe` dans tous les dossiers.
 - `example*` : ajoute aux autorisés les applications de tout type dont les noms commencent par `example`, dans tous les dossiers.
 - `example.*` : ajoute aux autorisés toutes les applications avec le nom `example` et n'importe quelle extension dans tous les dossiers.
- Spécifier une application autorisée par le nom de variable, si le nom et la valeur de cette variable sont spécifiés dans les paramètres des variables système.
 - `%EXAMPLE_PATH%\example.exe` : spécifie l'application par le nom de la variable système. Vous pouvez spécifier le nom de variable et sa valeur dans les paramètres du système d'exploitation. (sous Windows : **Panneau de configuration** → **Système** →



Paramètres système avancés → **Avancé** → **Variable d'environnement** → **Variables système**).

Nom de la variable dans l'exemple : `EXAMPLE_PATH`.

Valeur de la variable dans l'exemple : `C:\Program Files\folder`.



Vous pouvez également créer des règles d'autorisation depuis les sections [Événements du Contrôle des applications](#) et [Répertoire d'applications](#) à partir des données obtenues des postes. Dans ce cas, les paramètres des applications dans les paramètres de la règle seront remplis automatiquement conformément à l'application sélectionnée.

4. Cliquez sur **Enregistrer**.

Pour dupliquer une règle d'autorisation

1. Dans la section **Règles d'autorisation**, dans le tableau de règles, sélectionnez la règle que vous voulez dupliquer pour ce profil.
2. Cliquez sur le bouton **Dupliquer la règle** dans la barre d'outils.
3. Dans le tableau de règles s'affichera une nouvelle règle dont les paramètres seront complètement copiés de la règle sélectionnée à l'étape 1. Le chiffre **1** s'ajoutera au nom de la règle.

Pour supprimer une règle d'autorisation

1. Dans la section **Règles d'autorisation**, dans le tableau de règles, sélectionnez la règle que vous voulez supprimer du profil.
2. Cliquez sur le bouton **Supprimer la règle** dans la barre d'outils.

Applications de confiance

Si vous voulez utiliser les applications de confiance, effectuez l'une des actions suivantes :

- La collecte des applications de confiance s'effectuera sur votre Serveur Dr.Web (voir aussi [Applications de confiance](#)). Activez la collecte des applications de confiance dans la section **Administration** → **Contrôle des applications** → **Applications de confiance** du Centre de gestion.
- Si les applications de confiance seront transmises sur votre Serveur Dr.Web par la liaison depuis le Serveur voisin Dr.Web, spécifiez les [paramètres correspondants](#) dans les référentiels de Serveurs Dr.Web envoyant et recevant le produit **Applications de confiance**.


La modification des applications de confiance pour chaque profil se fait dans la section des [propriétés](#) du profil **Mode d'autorisation** → **Applications de confiance**.

Le tableau de la section contient la liste de tous les groupes des applications de confiances assignées à ce profil.




Le *Groupe des applications de confiance* (ou la liste blanche d'applications) représente une liste des applications classées selon les critères spécifiés du poste ou du groupe de postes sélectionné. Ces applications sont autorisées pour le lancement sur les postes du réseau antivirus auxquels ce profil est assigné lors du fonctionnement en mode d'autorisation.



Si votre Serveur obtient les applications de confiance par la liaison depuis le Serveur voisin Dr.Web (voir [Applications de confiance](#)), le tableau de groupes peut contenir des entrées marquées par l'icône . **Le groupe d'applications de confiance est introuvable dans le référentiel du Serveur Dr.Web.** Ces entrées concernent les groupes d'applications ajoutés depuis la révision précédente du produit **Applications de confiance**. Ensuite, une nouvelle révision a été obtenue dont ce groupe ne fait pas partie. Dans ce cas, les applications peuvent être toujours opérationnelles sur les postes correspondants, mais il est recommandé de [supprimer](#) de tels groupes des paramètres du profil pour éviter des problèmes de fonctionnement.

Pour ajouter un groupe des applications de confiance au profil


1. Dans la section **Applications de confiance**, cliquez sur le bouton  **Ajouter le groupe des applications de confiance au profil** dans la barre d'outils.
2. Une fenêtre s'ouvre affichant la liste de tous les groupes d'applications de confiance disponibles.



Quand vous configurez le mode d'autorisation, les groupes d'applications de confiance sont sélectionnés dans la liste des groupes disponibles dans le [référentiel](#) du produit **Applications de confiance**.

3. Cochez les cases contre les groupes d'applications que vous voulez ajouter dans le profil.
4. Cliquez sur **Enregistrer**.

Pour supprimer un groupe des applications de confiance du profil

1. Dans la section **Applications de confiance**, cochez les cases contre les groupes que vous voulez supprimer du profil.
2. Cliquez sur le bouton  **Supprimer le groupe des applications de confiance** dans la barre d'outils.
3. Les applications de ce groupe seront supprimées de la liste des applications autorisées pour le lancement sur les postes auxquels le profil est assigné.



En cas de suppression du profil, le groupe des applications de confiance n'est pas supprimée. Le groupe reste disponible dans le référentiel et peut être ajoutée dans ce profil ou dans un autre profil.



7.4.2.3. Mode de blocage

Mode de blocage implique que le lancement des applications relevant des règles de blocage est bloqué sur tous les postes contrôlés. Les autres applications sont autorisées.

Vous pouvez modifier les règles de blocage dans les [propriétés](#) du profil, dans l'onglet **Mode de blocage**.

Pour utiliser le mode de blocage

1. Cochez la case **Utiliser le mode de blocage** dans l'onglet **Mode de blocage**.
2. Créez les règles de blocage comme cela est décrit [ci-dessous](#).
3. Cliquez sur **Enregistrer**.



Si les règles d'autorisation ne sont pas spécifiées, le mode de blocage sera désactivé.

Pour créer une nouvelle règle de blocage

1. Dans la section **Règles de blocage** cliquez sur le bouton **+ Créer une règle** dans la barre d'outils.
2. Dans la fenêtre **Ajout d'une règle**, spécifiez **Nom de la règle** et cliquez sur **Enregistrer**.
3. Dans la liste des règles, sélectionnez la règle créée et configurez ses paramètres dans le panneau de propriétés qui s'affiche :
 - a) Cochez la case **Activer la règle** pour commencer à utiliser cette règle.
 - b) Si vous voulez tester la règle, cochez la case **Faire basculer la règle en mode test**. Les applications sur les postes ne seront pas contrôlées, pourtant l'activité sera journalisée comme si les paramètres étaient activés. Les résultats de lancements et de blocages d'applications en mode test s'afficheront dans la section [Événements du Contrôle des applications](#).
Si la case **Faire basculer la règle en mode test** est décochée, la règle fonctionnera en mode actif avec le blocage des applications sur les postes conformément aux paramètres de règle spécifiés (voir aussi les [modes de fonctionnement des profils](#)).
 - c) Dans la section **Bloquer le lancement des applications selon les critères suivants**, sélectionnez les options selon lesquelles le lancement des applications sur les postes sera bloqué.




Indiquez le nom du fichier ou le répertoire dans le champ **Nom de fichier**. Les variables d'environnement et les masques sont pris en charge. Si le chemin n'est pas indiqué, le paramètre sera considéré comme fichier au nom indiqué quel que soit sa localisation. Pour en savoir plus, consultez la rubrique [Mode d'autorisation](#).




Vous pouvez également créer des règles de blocage depuis les sections [Événements du Contrôle des applications](#) et [Répertoire d'applications](#) à partir des données obtenues des postes. Dans ce cas, les paramètres d'applications dans les paramètres de la règle seront remplis automatiquement conformément à l'application sélectionnée.

4. Cliquez sur **Enregistrer**.

Pour dupliquer une règle de blocage

1. Dans la section **Règles de blocage**, dans le tableau de règles, sélectionnez la règle que vous voulez dupliquer pour ce profil.
2. Cliquez sur le bouton  **Dupliquer la règle** dans la barre d'outils.
3. Dans le tableau de règles s'affichera une nouvelle règle dont les paramètres seront complètement copiés de la règle sélectionnée à l'étape 1. Le chiffre **1** s'ajoutera au nom de la règle.

Pour supprimer la règle de blocage

1. Dans la section **Règles de blocage**, dans le tableau de règles, sélectionnez la règle que vous voulez supprimer du profil.
2. Cliquez sur le bouton  **Supprimer la règle** dans la barre d'outils.



Chapitre 8 : Gestion des postes de travail

Le réseau antivirus géré par Dr.Web Enterprise Security Suite permet de configurer les packages antivirus sur les postes de manière centralisée. Dr.Web Enterprise Security Suite permet de réaliser les paramétrages suivants :

- configuration des paramètres des outils antivirus,
- configuration de la planification des lancements de tâches de scan,
- lancement des tâches sur des postes indépendamment de la planification,
- lancement du processus de mise à jour des postes y compris le lancement d'une mise à jour après une erreur survenue, avec remise à zéro du statut d'erreur.

L'administrateur du réseau antivirus peut accorder à l'utilisateur des droits autorisant la configuration et le lancement des tâches ainsi que limiter ou enlever ces droits.

Des modifications peuvent être apportées dans la configuration du poste même lorsqu'il est temporairement inaccessible pour le Serveur Dr.Web. Ces modifications seront prises en compte sur le poste dès que la connexion au Serveur Dr.Web aura été rétablie.

8.1. Gestion des comptes des postes de travail

8.1.1. Politique d'approbation des postes



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

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

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



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



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

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

Approuver l'accès manuellement

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


Pour modifier le mode d'accès des postes non approuvés

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



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

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

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

 **Approuver les postes sélectionnés et définir le groupe primaire** : approuver l'accès du poste au Serveur Dr.Web et spécifier le groupe primaire de la liste proposée.

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

 **Rejeter les postes sélectionnés** : refuser l'accès des postes au Serveur Dr.Web.



Refus automatique de l'accès

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



Approbation automatique d'accès

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

8.1.2. Suppression et restauration d'un poste

Suppression de postes

Pour supprimer l'entrée sur un poste

1. Sélectionnez l'élément **Réseau antivirus** du menu principal.
2. Dans la fenêtre qui s'affiche, sélectionnez dans l'arborescence un ou plusieurs postes à supprimer.
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 alors sur **OK**.

Après la suppression des postes depuis l'arborescence, ils sont placés dans le tableau des postes supprimés depuis lequel ils peuvent être restaurés via le Centre de gestion.



Restauration de postes

Pour restaurer une entrée sur un poste

1. Sélectionnez l'élément du menu principal **Réseau antivirus**, puis dans la fenêtre qui apparaît, sélectionnez dans l'arborescence un ou plusieurs postes distants à restaurer.



Tous les postes supprimés se trouvent dans le sous-groupe **Deleted** du groupe **Status**.

2. Depuis la barre d'outils, sélectionnez l'élément  **Général** →  **Restaurer les postes supprimés**.



3. La rubrique relative à la restauration des postes supprimés va s'ouvrir. Vous pouvez alors configurer les paramètres du poste à spécifier lors de sa restauration :
 - **Groupe primaire** : sélectionnez un groupe primaire auquel le poste sera ajouté après la restauration. Par défaut, le groupe primaire associé au poste avant sa suppression sera spécifié.






En cas de restauration de plusieurs postes à la fois, la variante suivante est spécifiée par défaut : **Ancien groupe primaire**, ce qui signifie que pour chaque poste restauré, l'ancien groupe primaire où les postes ont figuré avant la suppression sera spécifié. En cas de sélection d'un groupe pour tous les postes restaurés, ce groupe sélectionné sera spécifié pour tous les postes restaurés.

- La rubrique **Appartenance** vous permet de modifier la liste des groupes dont le poste fait partie. Par défaut, la liste des groupes où le poste a figuré avant la suppression est spécifiée. La liste **Appartenance** contient la liste des groupes auxquels le poste peut être inclus. Cochez les cases contre les groupes auxquels le poste sera inclus.
4. Pour restaurer un poste avec les paramètres spécifiés, cliquez sur le bouton **Restaurer**.

8.1.3. Fusionner des postes

Suite aux opérations avec la base de données ou en cas de réinstallation du logiciel sur les postes, l'arborescence peut contenir plusieurs postes ayant le même nom (dont un seul correspond à un poste antivirus).

Afin de supprimer les noms de postes en doublons

1. Sélectionnez tous les doublons relatifs à un poste. Pour cela, utilisez la touche CTRL.
2.  **Général** → **Fusionner les postes**.
3. Dans la colonne  sélectionnez le poste à considérer comme principal. Tous les autres postes seront supprimés et leurs données seront associées au poste sélectionné.
4. Dans la colonne , sélectionnez le poste dont la configuration sera appliquée au poste principal sélectionné.
5. Cliquez sur **Enregistrer**.

8.2. Paramètres généraux du poste de travail

8.2.1. Propriétés du poste

Pour consulter et éditer les propriétés du poste de travail

1. Sélectionnez l'élément **Réseau antivirus** du menu principal du Centre de gestion, puis dans la fenêtre qui apparaît, sélectionnez un poste dans l'arborescence.
2. Ouvrez la rubrique de configuration du poste d'une des façons suivantes :



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

Pour supprimer les paramètres personnalisés du poste

1. Sélectionnez l'élément **Réseau antivirus** du menu principal du Centre de gestion, puis dans la fenêtre qui apparaît, sélectionnez le poste dans l'arborescence et dans la barre d'outils cliquez sur **Général** → **Supprimer les paramètres personnalisés**. La liste des paramètres du poste va s'afficher, les cases contre les paramètres personnalisés sont cochées.
2. Laissez les cases cochées contre les paramètres à supprimer. Décochez les cases contre les paramètres qui doivent rester personnels. Cliquez sur **Supprimer**. L'héritage du groupe primaire sera rétabli pour les paramètres cochés.

8.2.1.1. Général

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

- **Identificateur du poste** : identificateur unique du poste. Il est spécifié lors de la création du compte du poste et ne peut pas être modifié après.
- **Nom** : nom du poste. Il est spécifié lors de la création du compte du poste et sera automatiquement remplacé par le nom de l'ordinateur après la connexion de l'Agent Dr.Web.
- **Date de création** : date de création du compte sur le Serveur Dr.Web.
- **Identificateur de sécurité** : identificateur de sécurité unique (SID – security identifier) du compte utilisateur de Windows. Le champ est rempli automatiquement après la connexion du poste tournant sous Windows au Serveur Dr.Web.
- **LDAP DN** : nom unique (distinguished name) du poste sous Windows. Cela concerne les postes faisant partie du domaine ADS/LDAP. Le champ est rempli automatiquement après la connexion du poste au Serveur Dr.Web.
- **Adresse MAC** : adresse MAC du poste. Le champ est rempli automatiquement après la connexion du poste au Serveur Dr.Web.
- **Date du premier téléchargement de l'Agent Dr.Web** : date du premier téléchargement du package d'installation de l'Agent Dr.Web par le lien de l'élément **Fichier d'installation** (voir ci-dessous).
- **Date de la dernière connexion** : date de la dernière connexion de ce poste au Serveur Dr.Web.



- **Adresse réseau** : adresse réseau du poste.
- **Numéro de version du système d'exploitation** : numéro de version de l'OS Windows installé sur le poste.

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

- Dans le champ **Mot de passe**, spécifiez un mot de passe pour l'authentification du poste sur le Serveur Dr.Web (il sera nécessaire de ressaisir ce mot de passe dans le champ **Confirmez le mot de passe**). Pour pouvoir connecter l'Agent Dr.Web en cas de changement de mot de passe, il est nécessaire d'effectuer la même procédure dans les paramètres de la connexion de l'Agent Dr.Web sur le poste.
- Dans les champs **Début de la période de blocage** et **Fin de la période de blocage**, spécifiez la période (depuis quand et jusqu'à quelle date) durant laquelle le poste sera bloqué sur le Serveur Dr.Web. Les champs servent à suspendre temporairement l'accès du poste au Serveur Dr.Web. Si la valeur est indiquée uniquement dans le champ **Début de la période de blocage**, le poste sera bloqué pour une durée illimitée à commencer par la date spécifiée.
- Dans le champ **Description** vous pouvez entrer des informations supplémentaires sur le poste.



Les valeurs des champs marqués par le symbole * doivent être obligatoirement spécifiées.

Cette rubrique contient également les liens suivants :

- Dans l'élément **Fichier d'installation** : lien de téléchargement du package d'installation de l'Agent Dr.Web pour ce poste.
Après la création du poste et jusqu'au moment où un système d'exploitation pour le poste en question ne soit défini, les liens de téléchargement des distributions sont fournis pour tous les OS pris en charge par Dr.Web Enterprise Security Suite.
- Dans l'élément **Fichier de configuration** — un lien pour télécharger le fichier contenant les paramètres de connexion au Serveur Dr.Web pour les postes sous OS Android, macOS et Linux.

8.2.1.2. Configuration

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


Icône	Paramètres	Rubrique contenant la description
	Droits des utilisateurs du poste	Droits des utilisateurs du poste
	Planification centralisée pour lancer des tâches sur les postes	Planification des tâches sur un poste
	Fichiers clés de licence pour les postes	Clés de licence



Icône	Paramètres	Rubrique contenant la description
	Restrictions sur la diffusion des mises à jour du logiciel antivirus	Restrictions de mises à jour des postes
	Liste des composants à installer	Composants à installer du package antivirus
	Paramètres des composants du package antivirus pour ce poste	Configuration des composants antivirus

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



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

8.2.1.3. Groupes

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

Pour gérer l'appartenance d'un poste

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



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

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

8.2.1.4. Sécurité

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



Pour configurer les limitations d'accès

1. Cochez la case **Utiliser cette liste de contrôle d'accès** pour spécifier les listes d'adresses autorisées ou bloquées. Si la case est décochée, toutes les connexions seront autorisées.
2. Pour autoriser l'accès depuis une adresse TCP déterminée, ajoutez l'adresse dans la liste **TCP: autorisé** ou **TCPv6: autorisé**.
3. Pour interdire une adresse TCP, ajoutez-la dans la liste **TCP: interdit** ou **TCPv6: interdit**.
4. Les adresses non mentionnées dans aucune des listes sont autorisées ou interdites en fonction du statut de la case **Priorité de refus** : si la case est cochée, la liste **Refuser** possède une priorité plus importante que la liste **Autoriser**. Les adresses qui ne sont incluses à aucune liste ou incluses aux deux listes sont refusées. Seules les adresses appartenant à la liste **Autoriser** et non incluses à la liste **Refuser** seront autorisées.

Pour éditer la liste des adresses :

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



Les listes pour les adresses TCPv6 ne seront affichées que dans le cas où l'interface IPv6 est installée sur le poste.

Exemple d'utilisation du préfixe :

1. Le préfixe 24 désigne les réseaux ayant le masque : 255 . 255 . 255 . 0
Il contient 254 adresses.
Les adresses hôte dans les réseaux de ce type : 195 . 136 . 12 . *
2. Le préfixe 8 désigne les réseaux ayant le masque 255 . 0 . 0 . 0
Il contient jusqu'à 16777214 adresses (256*256*256-2).
Les adresses d'hôtes dans les réseaux de ce type ont le format suivant : 125 . * . * . *

8.2.1.5. Serveur proxy


Dans la section **Serveur proxy**, vous pouvez spécifier les paramètres du Serveur proxy Dr.Web installé sur ce poste.



Pour plus d'infos sur l'installation et la connexion du Serveur proxy au Serveur Dr.Web, consultez le **Manuel d'installation**, le p. [Installation du Serveur proxy](#).



Si le Serveur proxy est déjà installé sur le poste :

1. Le champ **Identificateur** contient l'identificateur du compte du Serveur proxy créé dans le Centre de gestion. Après la création du compte, l'édition de l'identificateur est impossible.
2. Dans le champ **Nom**, vous pouvez modifier le nom du compte du Serveur proxy créé dans le Centre de gestion.
3. Dans les champs **Nom** et **Confirmez le mot de passe**, vous pouvez changer de mot de passe du compte du Serveur proxy créé dans le Centre de gestion. Le mot de passe est utilisé pour la connexion du Serveur proxy au Serveur Dr.Web. En cas de changement de mot de passe, assurez-vous que le mot de passe dans les paramètres de connexion sur le Serveur proxy correspond au mot de passe modifié dans le Centre de gestion. Si les mots de passe ne correspondent pas, le Serveur proxy ne pourra pas se connecter au Serveur Dr.Web pour la gestion distante de la configuration via le Centre de gestion.
4. La section **Appartenance** contient le groupe dont le Serveur proxy fait 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.
5. Vous pouvez supprimer le Serveur proxy, lié à l'Agent Dr.Web sur le poste édité. Pour ce faire, cliquez sur  **Supprimer le Serveur proxy**.
Après un clic sur **Enregistrer**, le Serveur proxy sera désinstallé du poste. Le compte du Serveur proxy sera supprimé du Serveur Dr.Web.

Si le Serveur proxy n'est pas installé sur le poste :

1. Si vous voulez installer le Serveur proxy sur le poste sélectionné, cochez la case **Créer un Serveur proxy lié** et spécifiez les paramètres du Serveur proxy créé. Les paramètres sont équivalents aux paramètres utilisés lors de la création du Serveur proxy.
2. Une fois le bouton **Enregistrer** cliqué, le compte du Serveur proxy est 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'AgentDr.Web se connectera au Serveur Dr.Web uniquement via le Serveur proxy installé. L'utilisation du Serveur proxy sera transparente pour l'utilisateur.

8.2.1.6. Localisation

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

Vous pouvez également localiser géographiquement le poste sur une carte.

Pour voir l'emplacement du poste sur la carte

1. Dans les champs **Latitude** et **Longitude**, indiquez les coordonnées géographiques du poste au format Degrés Décimaux.



2. Cliquez sur **Sauvegarder** pour conserver les données entrées.
3. Dans l'onglet **Localisation**, la visualisation OpenStreetMap va s'ouvrir et les coordonnées indiquées seront marquées.
Si le chargement de l'aperçu est impossible, le texte **Afficher sur la carte** apparaît.
4. Pour consulter la carte au plus grand format, cliquez sur l'outil de visualisation ou sur le texte **Afficher sur la carte**.



La configuration de la localisation automatique est disponible pour les postes tournant sous l'OS Android.

Pour plus d'informations sur l'utilisation et la configuration de cette fonction, consultez les **Annexes**, la rubrique [Localisation automatique d'un poste tournant sous l'OS Android](#).

8.2.2. Composants de protection

Composants

Pour savoir quels composants du package antivirus sont installés sur le poste de travail et pour lancer ou arrêter le fonctionnement des composants

1. Sélectionnez l'élément **Réseau antivirus** dans le menu principal du Centre de gestion, puis dans la fenêtre qui apparaît, cliquez sur le nom du poste ou du groupe dans l'arborescence.
2. Dans le [menu de gestion](#), sélectionnez l'élément **Composants installés** dans la sous-rubrique **Général**.
3. Une fenêtre s'ouvre contenant les informations sur les composants installés sur les postes sélectionnés.



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

- composants autorisés pour l'utilisation dans le fichier clé de licence ;
- OS installé sur le poste de travail ;
- paramètres configurés par l'administrateur sur le Serveur Dr.Web. L'administrateur peut modifier l'ensemble de composants du package antivirus sur le poste avant l'installation de l'Agent Dr.Web ainsi qu'à tout moment après l'installation (voir [Composants à installer du package antivirus](#)).

4. Si nécessaire, vous pouvez modifier le statut de fonctionnement des composants directement du Centre de gestion. Pour ce faire, cochez les cases pour les composants dont vous voulez modifier le statut et cliquez sur le bouton correspondant dans la barre d'outils :
 - : arrêter les composants sélectionnés sur les postes.
 - : lancer les composants sélectionnés sur les postes.



Si vous arrêtez le composant, les scans en cours seront interrompus, le Scanner sera arrêté et les moniteurs seront mis en pause.

Vous pouvez également arrêter le fonctionnement des composants en fonction de type de leur lancement, comme cela est décrit dans la section [Interruption des composants en cours selon leur type](#).

5. Si nécessaire, vous pouvez exporter les données sur le matériel et les logiciels vers un fichier. Pour ce faire, cliquez sur un des boutons suivants dans la barre d'outils :



Sauvegarder les données dans un fichier CSV,



Sauvegarder les données dans un fichier HTML,



Sauvegarder les données dans un fichier XML,



Sauvegarder les données dans un fichier PDF.

Bases virales

Pour consulter les bases virales installées sur le poste

1. Sélectionnez l'élément **Réseau antivirus** dans le menu principal du Centre de gestion, puis dans la fenêtre qui apparaît, cliquez sur le nom du poste dans l'arborescence.
2. Dans le [menu de gestion](#) qui s'affiche, sélectionnez l'élément **Bases virales** depuis la sous-rubrique **Statistiques**.
3. Une fenêtre qui s'affiche contient les informations suivantes sur les bases virales installées : nom de fichier contenant la base virale, version de la base virale, date de création de la base virale, total d'entrées dans la base virale.



En cas de désactivation de l'affichage de l'élément **Bases virales**, pour l'activer, sélectionnez l'élément **Administration** du menu principal et dans la fenêtre qui apparaît, sélectionnez l'élément du menu de gestion **Configuration du Serveur Dr.Web**. Dans l'onglet **Statistiques**, cochez les cases **Statuts des postes** et **Statut des bases virales**, puis redémarrez le Serveur Dr.Web.

L'élément **Bases virales** est disponible uniquement si vous sélectionnez les postes isolés.

8.2.3. Matériel et logiciels des postes tournant sous Windows

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



Pour collecter des informations sur le matériel et les logiciels du poste

1. Activer la collecte des statistiques sur le Serveur Dr.Web :



- a) Sélectionnez l'élément **Administration** du menu principal du Centre de gestion.
 - b) Sélectionnez l'élément **Configuration du menu de gestion du Serveur Dr.Web**.
 - c) Dans les paramètres du Serveur Dr.Web, ouvrez l'onglet **Statistiques** et cochez la case **Composition de matériel et de logiciels** si cette case est décochée.
 - d) Pour appliquer les modifications apportées, cliquez sur **Sauvegarder** et redémarrez le Serveur Dr.Web.
2. Autoriser la collecte des statistiques sur les postes :
- a) Sélectionnez l'élément **Réseau antivirus** du menu principal du Centre de gestion.
 - b) Dans la liste hiérarchique du réseau antivirus, sélectionnez un poste ou un groupe de postes pour lesquels vous voulez autoriser la collecte des statistiques. En cas de la sélection d'un groupe des postes, prenez en compte l'héritage des paramètres : si les paramètres personnalisés sont spécifiés pour le groupe sélectionné, la modification des paramètres du groupe ne va pas modifier les paramètres du poste.
 - c) Dans le menu de gestion, sélectionnez la section **Configuration** → **Windows**, ensuite sélectionnez l'élément **Agent Dr.Web**.
 - d) Dans les paramètres de l'Agent Dr.Web, dans l'onglet **Général**, cochez la case **Collecter les informations sur les postes** si elle est décochée. Si, avant, vous n'avez pas autorisé la collecte des statistiques dans les paramètres du Serveur Dr.Web, ce paramètre ne sera pas disponible. Si nécessaire, éditez la valeur du paramètre **Période de la collecte des informations sur les postes (min)**.
 - e) Pour appliquer les modifications apportées, cliquez sur **Sauvegarder**. Les paramètres seront transmis sur les postes.

Pour consulter le matériel et les logiciels sur un ou plusieurs postes

1. Sélectionnez l'élément **Réseau antivirus** du menu principal du Centre de gestion.
2. Sélectionnez un poste ou un groupe de postes dans la liste hiérarchique du réseau antivirus.
3. Dans le menu de gestion, sélectionnez l'élément **Matériel et logiciels** dans la section **Général**.
4. Le tableau comprend les onglets suivants contenant les informations sur le matériel et les logiciels des postes sélectionnés :
 - **Matériel** : liste du matériel installé sur les postes.
 - **Applications** : liste des produits installés sur les postes.
 - **Mises à jour de Windows** : liste de packages de mises à jour de Windows installés sur les postes.
5. La colonne **Poste** dans chaque onglet contient le nom du poste pour lequel les informations sont affichées.
6. Pour éditer l'affichage des données dans le tableau :
 - Avec l'icône , sélectionnez les colonnes à afficher dans le tableau.
 - Avec l'icône , spécifiez la ligne aléatoire pour la recherche dans toutes les sections du tableau.



- Si nécessaire, vous pouvez exporter les données sur le matériel et les logiciels vers un fichier. Pour ce faire, cliquez sur un des boutons suivants dans la barre d'outils :

 **Sauvegarder les données dans un fichier CSV,**

 **Sauvegarder les données dans un fichier HTML,**

 **Sauvegarder les données dans un fichier XML,**

 **Sauvegarder les données dans un fichier PDF.**

8.3. Configuration du poste de travail



8.3.1. Droits des utilisateurs du poste

Pour configurer les droits des utilisateurs du poste à l'aide du Centre de gestion de la sécurité Dr.Web

- Sélectionnez l'élément **Réseau antivirus** dans le menu principal, puis cliquez sur le nom du poste dans l'arborescence. Dans le [menu de gestion](#) qui va s'ouvrir, sélectionnez l'élément **Droits**. La fenêtre de configuration des droits va s'ouvrir.
- Vous pouvez modifier les droits aux onglets correspondant au système d'exploitation du poste de travail. Pour modifier (autoriser ou refuser) tout droit, cochez ou décochez la case pour ce droit.
- Pour modifier les droits des postes sous Windows, macOS, Linux et Android, utilisez les sous-sections suivantes :
 - Composants** : configuration des droits relatifs à la gestion des composants antivirus. Par défaut, l'utilisateur conserve le droit de lancer chaque composant mais il n'est pas autorisé à éditer la configuration des composants ni à stopper des composants.
 - Général** : configuration des droits relatifs à la gestion de l'Agent Dr.Web et de ses fonctions :

Case de la rubrique Droits	Action de la case	Résultat sur le poste si la case est décochée
Postes tournant sous Windows		
Modifier la configuration de l'Agent Dr.Web	Cochez la case pour permettre aux utilisateurs d'un poste de modifier les paramètres de l'Agent Dr.Web.	Les paramètres des sous-sections suivantes ne sont pas disponibles dans la section Général des paramètres de l'Agent Dr.Web : <ul style="list-style-type: none">Notifications : aucun paramètre n'est disponible.Serveur : aucun paramètre de connexion au Serveur Dr.Web n'est disponible, ainsi que la case Synchroniser l'heure système avec l'heure du serveur et le paramètre Utiliser le Mode mobile



Case de la rubrique Droits	Action de la case	Résultat sur le poste si la case est décochée
		<p>lorsqu'il n'y a pas de connexion au serveur.</p> <ul style="list-style-type: none">• Autoprotection : les paramètres Empêcher la modification de la date et de l'heure système et Empêcher l'émulation de l'activité utilisateur ne sont pas disponibles.• Avancé : les éléments Mise à jour Dr.Web, Services Dr.Web, Créer des dumps de mémoire en cas d'erreur de scan ne sont pas disponibles dans les paramètres de la rubrique Journal.
Désactiver l'autoprotection	Cochez la case pour permettre aux utilisateurs d'un poste de désactiver l'autoprotection.	Le paramètre Activer l'autoprotection et le paramètre Activer le support de la virtualisation assistée par matériel ne sont pas disponible dans la rubrique Général > Autoprotection dans les paramètres de l'Agent Dr.Web.
Désinstaller l'Agent Dr.Web	Cochez la case pour permettre aux utilisateurs d'un poste de désinstaller l'Agent Dr.Web.	Empêche la désinstallation de l'Agent Dr.Web sur le poste via l'installateur ou via les outils standard de Windows. Dans ce cas, l'Agent Dr.Web peut être désinstallé uniquement via l'option  Général →  Désinstaller l'Agent Dr.Web dans la barre d'outils du Centre de gestion.
Postes tournant sous macOS		
Lancer en mode mobile	Cochez la case pour autoriser les utilisateurs du poste à passer en mode mobile et à utiliser le Système Global de Mise à jour Dr.Web pour les mises à jour s'il n'y a pas de connexion au Serveur Dr.Web.	Dans la fenêtre principale de l'application, la rubrique Mise à jour n'est pas disponible.
Postes tournant sous OS de la famille Linux		
Lancer en mode mobile	Cochez la case pour autoriser les utilisateurs du poste à passer en mode mobile et à utiliser le Système Global de Mise à jour Dr.Web pour les mises à jour s'il n'y a pas de	Pour le mode de console de l'application : la commande <code>drweb-ctl update</code> pour mettre à jour les bases virales depuis le SGM n'es pas disponible.



Case de la rubrique Droits	Action de la case	Résultat sur le poste si la case est décochée
	connexion au Serveur Dr.Web.	
Postes tournant sous OS Android		
Lancer en mode mobile	Cochez la case pour autoriser les utilisateurs d'appareils mobiles à passer en mode mobile et à utiliser le Système Global de Mise à jour Dr.Web pour les mises à jour s'il n'y a pas de connexion au Serveur Dr.Web.	Dans la fenêtre principale de l'application lancée sur l'appareil mobile, la rubrique Mise à jour est bloquée.



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

Vous pouvez consulter la description des actions associées aux éléments du menu dans les **Manuels Utilisateur** des produits Dr.Web pour le système d'exploitation correspondant.

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



Si lors de l'édition des paramètres du poste, le poste n'est pas connecté au Serveur Dr.Web, les paramètres seront pris en compte dès que l'Agent Dr.Web aura rétabli la connexion au Serveur Dr.Web.

8.3.2. Planification des tâches sur un poste

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

Planification des tâches : liste d'actions à exécuter de manière automatique à une heure définie sur les postes de travail. La planification sert à exécuter le scan antivirus des postes aux moments les plus opportuns pour les utilisateurs, sans nécessité de lancer manuellement le Scanner. De plus, l'Agent Dr.Web permet d'exécuter d'autres types d'actions décrits ci-dessous.



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



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

Pour les postes tournant sous Windows, la planification contient une tâche par défaut — Daily scan — scan quotidien du poste.

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

Pour modifier la planification centralisée

1. Sélectionnez l'élément **Réseau antivirus** dans le menu principal du Centre de gestion. Puis, dans l'arborescence de la fenêtre qui s'ouvre, cliquez sur le nom d'un poste ou d'un groupe. Dans le [menu de gestion](#) qui s'affiche, sélectionnez **Planificateur des tâches**. La liste contenant les tâches pour les postes va s'ouvrir.




La plupart des outils de cette section seront indisponibles si l'héritage des paramètres du groupe parent est spécifié pour le poste ou le groupe sélectionné. Les éléments suivants de la barre d'outils permettent de modifier les paramètres d'héritage au sein de la planification de tâches si cela est nécessaire :

Configurer l'héritage des paramètres de la politique ou du groupe primaire : supprimer les paramètres personnalisés de la planification de tâches et configurer l'héritage des paramètres de cette section du groupe parent.

Copier les paramètres de la politique ou du groupe primaire et les enregistrer comme personnalisés : copier les paramètres de la planification de tâches du groupe parent et les assigner aux postes sélectionnés. Dans ce cas, l'héritage sera coupé et toutes modifications postérieures de la planification de tâches seront considérées comme personnalisées.

2. Pour gérer la planification, utilisez les éléments correspondants dans la barre d'outils :
 - a) Les éléments généraux de la barre d'outils sont utilisés pour créer de nouvelles tâches et gérer la rubrique planification dans son ensemble.
 - Créer une tâche** : ajouter une nouvelle tâche. Cette action est décrite en détails ci-dessous, dans la sous-rubrique [Éditeur de tâches](#).
 - Distribuer ces paramètres à un autre objet** : copier les tâches planifiées dans d'autres objets – postes et groupes. Pour en savoir plus, voir [Copie des configurations vers d'autres groupes/postes](#).
 - Exporter les paramètres de cette rubrique vers un fichier** : exporter la planification vers un fichier au format spécial.









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







L'importation de la liste de tâches pour le Serveur Dr.Web dans le Planificateur de tâches des postes ou vice versa n'est pas autorisée.

- b) Pour gérer les tâches existantes, cochez les cases près des tâches souhaitées ou dans l'entête du tableau pour sélectionner toutes les tâches dans la liste. Les éléments de gestion des tâches sélectionnées deviennent disponibles dans la barre d'outils à condition que l'héritage des paramètres de la planification de tâches depuis le groupe parent ne soit pas spécifié pour le poste ou le groupe sélectionné :

Configuration		Action
 Type de lancement	Synchrone	Spécifier le lancement synchrone pour toutes les tâches marquées ci-dessous. La tâche avec une périodicité spécifiée sera placée dans la file d'attente commune des tâches du Planificateur. Les tâches dans cette file d'attente sont exécutées à tour de rôles.
	Asynchrone	Spécifier le lancement asynchrone pour toutes les tâches marquées ci-dessous. La tâche avec une périodicité spécifiée sera exécutée en même temps que les autres tâches hors de la file d'attente.
 Statut	Autoriser l'exécution	Activer l'exécution des tâches sélectionnées selon leur planification, si elles étaient désactivées.
	Désactiver l'exécution	Désactiver l'exécution des tâches sélectionnées. Les tâches restent dans la liste mais ne seront pas exécutées.
 Vous pouvez spécifier le même paramètre dans l'éditeur de tâches dans l'onglet Général en cochant la case Autoriser l'exécution .		
 Importance	Définir comme critique	Effectuer un lancement supplémentaire de la tâche au prochain démarrage de l'Agent Dr.Web, si l'exécution planifiée de cette tâche a été omise.
	Définir comme non critique	Exécuter la tâche uniquement au moment où elle planifiée indépendamment du fait que le lancement de la tâche ait été omis ou pas.
 Vous pouvez spécifier le même paramètre dans l'éditeur de tâches dans l'onglet Général en cochant la case Tâche critique .		
 Dupliquer des paramètres	Permet de dupliquer des tâches sélectionnées dans la liste des planifications actuelles. Lorsque vous activez l'option Dupliquer des paramètres , les nouvelles tâches créées	



Configuration	Action
	possèdent des paramètres identiques à ceux des tâches sélectionnées.
 Planifier à plusieurs reprises	Pour les tâches qui ne sont exécutées qu'une fois : exécuter la tâche de nouveau selon les horaires configurés (la modification de la répétition d'exécution d'une tâche est décrite ci-dessous, dans la rubrique Éditeur de tâches).
 Supprimer les tâches sélectionnée	Supprimer la tâche sélectionnée de la planification.
 Exécuter la tâche	Exécuter tout de suite les tâches sélectionnées dans la liste. Dans ce cas, la tâche sera lancée même si son exécution selon la planification est interdite.
 Modifier la tâche	Modifier les paramètres de la tâche. Dans ce cas, la fenêtre de l' Éditeur de tâches , décrit ci-dessous , s'ouvre.




Si vous avez besoin de la planification héritée du groupe parent, vous devez désactiver l'héritage pour le poste et laisser au moins une tâche en la désactivant .

1. Sélectionnez l'élément **Réseau antivirus** du menu principal du Centre de gestion, puis dans la fenêtre qui apparaît, sélectionnez un poste dans l'arborescence.
2. Ouvrez la rubrique de configuration du poste d'une des façons suivantes :
 - a) Cliquez sur le nom du poste dans la liste hiérarchique du réseau antivirus. La section contenant les propriétés du poste va s'afficher automatiquement dans la partie droite du Centre de gestion.
 - b) Sélectionnez l'élément **Propriétés** du menu de gestion. La fenêtre contenant les propriétés du poste va s'ouvrir.
3. Dans la section contenant les propriétés du poste, sélectionnez l'élément **Configuration -> Planificateur des tâches**.
4. Cliquez sur l'icône **Copier les paramètres de la politique ou du groupe primaire et les enregistrer comme personnalisés** et confirmez l'action sélectionnée.
5. Laissez au moins une tâche et bloquez son exécution en cliquant sur l'icône **Statut -> Interdire l'exécution**.

Éditeur de Tâches

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

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



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



Les champs dans l'interface marqués par le symbole * doivent être obligatoirement remplis.

Pour modifier les paramètres d'une tâche

1. Dans l'onglet **Général**, vous pouvez configurer les paramètres suivants :

- Dans le champ **Nom**, indiquez le nom de la tâche affichée dans la liste des planifications.
- Cochez la case **Activer l'exécution** pour activer l'exécution d'une tâche. Si la case n'est pas cochée, la tâche reste dans la liste mais elle ne sera pas exécutée.



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

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



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



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

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

- Si la case **Lancer la tâche de manière asynchrone** est décochée, la tâche sera placée dans la file d'attente des tâches du Planificateur exécutées successivement. Cochez la case pour exécuter cette tâche simultanément hors de la file d'attente.
2. Dans l'onglet **Action**, dans la liste déroulante **Action**, sélectionnez le type de tâche et configurez les paramètres nécessaires à son exécution :

Type de tâche	Paramètres et description
Écrire dans le fichier de journal	Ligne : texte du message enregistré dans le fichier de rapport.
Lancer un programme	Configurez les paramètres suivants :



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



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


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

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

Mode de lancement	Paramètres et description
Démarrage	La tâche sera lancée au démarrage de l'Agent Dr.Web. Aucun paramètre supplémentaire n'est requis pour exécuter la tâche.
Dans N minutes après la tâche initiale	Dans la liste déroulante Tâche initiale , sélectionnez la tâche par rapport à laquelle est spécifiée l'heure d'exécution de la tâche courante. Dans le champ Minute , indiquez ou choisissez dans la liste le nombre de minutes pour lancer l'exécution de la tâche éditée après l'exécution de la tâche initiale.
Chaque jour	Indiquez l'heure et les minutes — la tâche sera lancée chaque jour au moment spécifié.
Chaque mois	Choisissez la date (jour du mois) et indiquez l'heure et les minutes — la tâche sera lancée au jour spécifié au moment indiqué.
Chaque semaine	Choisissez le jour de la semaine et indiquez l'heure et les minutes — la tâche sera lancée au jour de la semaine spécifié au moment indiqué.



Mode de lancement	Paramètres et description
Chaque heure	Indiquez un chiffre entre 0 et 59 pour paramétrer la minute à laquelle sera lancée la tâche dans une heure.
Chaque N minutes	La valeur N doit être indiquée pour paramétrer l'intervalle entre l'exécution des tâches. Si N est égal à 60 ou plus, la tâche sera lancée chaque N minutes. Si N est inférieur à 60, la tâche sera lancée chaque minute de l'heure multiple de N .

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

8.3.3. Composants à installer du package antivirus



Il n'est pas recommandé d'installer les composants SplDer Gate, SplDer 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.

Pour configurer la liste des composants du package antivirus à installer, procédez comme suit :

1. Sélectionnez l'élément **Réseau antivirus** dans le menu principal du Centre de gestion. Puis, dans la fenêtre qui s'ouvre, sélectionnez un poste ou un groupe dans l'arborescence. Dans le [menu de gestion](#) qui apparaît, sélectionnez l'élément **Composants à installer**.
2. Pour installer les composants nécessaires, sélectionnez l'une des variantes dans la liste déroulante :
 - **Doit être installé** : la présence du composant sur le poste est obligatoire. Lors de la création d'un nouveau poste, le composant fait partie du package antivirus. Si la valeur **Doit être installé** est spécifiée dans la configuration du poste existant, le composant correspondant sera ajouté au package antivirus installé.
 - **Peut être installé** : détermine une possibilité d'installer le composant antivirus. C'est l'utilisateur qui décide d'installer ou de ne pas installer l'Agent Dr.Web.



- **Ne peut pas être installé** : interdit la présence du composant sur le poste. Lors de la création d'un nouveau poste, le composant n'est pas inclus au package antivirus. Si la valeur **Ne peut pas être installé** est spécifiée dans la configuration du poste existant, le composant concerné sera supprimé du package antivirus.

Le tableau 8-1 indique si le composant sera installé sur le poste (+) en fonction des paramètres spécifiés par l'utilisateur et des configurations spécifiées par l'administrateur sur le Serveur Dr.Web.


Tableau 8-1.

Utilisateur	Configuré sur le Serveur Dr.Web		
	Doit	Peut	Ne peut pas
Installer	+	+	
Ne pas installer	+		

3. Cliquez sur le bouton **Sauvegarder** pour enregistrer les paramètres et sauvegarder le jeu de composants modifié du package antivirus installé sur le poste.


8.3.4. Paramètres de connexion

L'onglet **Paramètres de connexion** présente les paramètres déterminant la configuration de l'interaction avec le Serveur Dr.Web :

- Dans le champ **Certificat**, on spécifie le certificat SSL du Serveur Dr.Web (`drwcsd-certificate.pem`). Pour sélectionner un fichier de certificat, cliquez sur .

Plusieurs certificats peuvent être sauvegardés sur le poste en même temps, par exemple, lors du déménagement d'un Serveur Dr.Web sur un autre. Notez que les certificats doivent être uniques, c'est-à-dire que vous ne pouvez pas indiquer deux certificats identiques.

Pour ajouter un certificat, cliquez sur  et sélectionnez le fichier de certificat.

Pour supprimer un certificat existant, cliquez sur  contre le certificat à supprimer.



Le certificat doit être spécifié obligatoirement.

- Dans le champ **Serveur**, spécifiez l'adresse du Serveur Dr.Web ou du Serveur proxy Dr.Web (pour en savoir plus [Serveur proxy Dr.Web](#)). Vous pouvez laisser ce champ vide. Dans ce cas, l'Agent Dr.Web va utiliser l'adresse du Serveur Dr.Web spécifiée dans les paramètres de la machine locale de l'utilisateur (l'adresse du Serveur Dr.Web depuis laquelle l'installation a été effectuée).

Vous pouvez spécifier une adresse de Serveur Dr.Web ainsi que plusieurs adresses de Serveurs Dr.Web différents. Pour ajouter encore une adresse de Serveur Dr.Web, cliquez sur



+ et entrez l'adresse dans le champ ajouté. Le format des adresses réseau du Serveur Dr.Web est décrit dans les **Annexes**, [Annexe D. Spécification de l'adresse réseau](#).

Exemple de spécification de l'adresse du Serveur Dr.Web :

tcp/10.4.0.18:2193

tcp/10.4.0.19

10.4.0.20



Si une valeur non valide/incorrecte du paramètre **Serveur** est spécifiée, les Agents Dr.Web seront déconnectés du Serveur Dr.Web et ils ne pourront plus se connecter. Si c'est le cas, il faudra spécifier l'adresse du Serveur Dr.Web directement sur le poste.

- Dans le champ **Nombre de reprises de recherche**, spécifiez une valeur déterminant le nombre de reprises de recherche du Serveur Dr.Web si le mode *Multicasting* est activé.
- Dans le champ **Délai de recherche (s)**, spécifiez un délai entre les tentatives de recherche du Serveur Dr.Web en secondes, si le mode *Multicasting* est activé.
- Les champs **Mode de compression** et **Mode de chiffrement** permettent de spécifier les paramètres de compression et de chiffrement du trafic réseau (voir aussi Chiffrement et compression du trafic).
- Dans le champ **Paramètres d'écoute du réseau** indiquez le port UDP utilisé par le Centre de gestion pour rechercher dans le réseau les Agents Dr.Web actifs. Pour interdire l'écoute des ports, entrez la valeur **NONE**.

Le paramètre est spécifié au format d'adresse réseau décrit dans le document **Annexes**, [Annexe D. Spécification de l'adresse réseau](#).


La valeur par défaut est **udp/:2193**, ceci désigne "toutes les interfaces, port 2193".

8.3.5. Clés de licence

Vous pouvez consulter et éditer la liste des clés de licences du poste ou du groupe par l'un des moyens suivants :

1. Via [Gestionnaire de licences](#).
2. Via la configuration de l'objet de licence (du poste ou du groupe) dans le réseau antivirus.

Pour éditer la liste des clés de licences via la configuration de l'objet de licence

1. Dans le menu principal du Centre de gestion, sélectionnez l'élément **Réseau antivirus**.
2. Ouvrez la section [Propriétés du poste](#) ou [Configuration des groupes](#) pour l'objet, dont vous voulez modifier les clés de licence.
3. Dans la section de configuration cliquez sur icône  **Éditer** ou sur le lien **Clés de licence**.
4. La fenêtre **Clés de licence** qui s'affiche contient la liste des clés de licence de l'objet, leur statut actuel (héritées ou spécifiées personnellement) ainsi que la liste de toutes les clés disponibles sur ce Serveur Dr.Web. Si nécessaire, vous pouvez aller directement dans le Gestionnaire de licences.




5. Les actions appliquées à la liste des clé dépendent du statut des clés de licences actuelles de l'objet :

Action	Les clés actuelles sont héritées	Les clés actuelles sont spécifiée de manière personnalisée	Aucune clé n'est spécifiée
Ajouter une clé de licence	L'héritage sera interrompu. La nouvelle clé sera ajoutée dans la liste des clés assignées et elle deviendra personnelle.	La nouvelle clé sera ajoutée dans la liste des clés assignées.	Les clé seront ajoutées dans la liste des clés de licence de l'objet en tant que personnelles.
Supprimer la clé de licence	Action indisponible.	La clé sera supprimée de la liste des clés de l'objet.	Action indisponible.
Établir l'héritage	Action indisponible.	Les clés actuelles seront supprimées de la liste des clés de l'objet, l'héritage des clés du groupe primaire/parent sera établi.	Action indisponible.
Interrompre l'héritage	L'héritage sera interrompu. La liste ne sera pas modifiée, mais elle deviendra personnelle.	Action indisponible.	Action indisponible.

Les clés actuelles sont héritées

Pour ajouter une clé de licence

1. Dans la liste **Toutes les clés** de la fenêtre **Clés de licence**, sélectionnez une ou plusieurs clés de licences que vous voulez ajouter.
2. Cliquez sur .
3. Si la liste des composants installés sur les postes ne correspond pas à celle des clés ajoutées, un avertissement correspondant s'affiche. Vous serez invité à éditer la liste résultante des composants.
4. Après toutes les modifications nécessaires, cliquez sur **Enregistrer**.
5. L'héritage sera interrompu. La nouvelle clé sera ajoutée dans la liste des clés assignées et elle deviendra personnelle.



Pour interrompre l'héritage sans modifier la liste des clés de licence

1. Dans la fenêtre **Clés de licence**, cliquez sur le bouton **Copier les paramètres du groupe primaire et les enregistrer comme personnalisés**.
2. L'héritage sera interrompu. La liste des clés sera copiée depuis le groupe primaire/parent et elle sera spécifiée pour l'objet en tant que personnelle.
3. Cliquez sur **Enregistrer**.

Les clés actuelles sont spécifiée de manière personnalisée

Pour ajouter une clé de licence

1. Dans la liste **Toutes les clés** de la fenêtre **Clés de licence**, sélectionnez une ou plusieurs clés de licences que vous voulez ajouter.
2. Cliquez sur .
3. Si la liste des composants installés sur les postes ne correspond pas à celle des clés ajoutées, un avertissement correspondant s'affiche. Vous serez invité à éditer la liste des composants.
4. Après toutes les modifications nécessaires, cliquez sur **Enregistrer**.
5. La nouvelle clé sera ajoutée dans la liste des clés assignées.

Pour supprimer une clé de licence

1. Dans la liste **Clés de l'objet** de la fenêtre **Clés de licences**, cliquez sur contre toutes les clés de licence que vous voulez supprimer.



Si toutes les clés sont supprimées, l'héritage des clés de licence du groupe primaire/parent sera établi (voir aussi [Établissement de l'héritage](#)).

2. Cliquez sur **Enregistrer**.
3. Si la liste des composants installés sur les postes ne correspond pas à celle des clés restantes, un avertissement correspondant s'affiche. Vous serez invité à éditer la liste résultante des composants.

Pour établir l'héritage

1. Vous pouvez établir l'héritage par l'un des moyens suivants :
 - Ouvrez la section [Propriétés du poste](#) ou [Configuration des groupes](#) pour l'objet, pour lequel vous voulez établir l'héritage. Dans la section de configuration, cliquez sur l'icône **Supprimer la clé**.
 - Dans la liste **Clés de l'objet** de la fenêtre **Clés de licences**, cliquez sur contre toutes les clés de licence assignées que vous voulez supprimer. Cliquez sur le bouton **Enregistrer**.




2. Les clés actuelles seront supprimées de la liste des clés de l'objet, l'héritage des clés du groupe primaire/parent sera établi.
3. Si la liste des composants installés sur les postes ne correspond pas à celle des clés héritées, un avertissement correspondant s'affiche. Vous serez invité à éditer la liste des composants.

Aucune clé n'est spécifiée



La situation est possible uniquement si aucune clé n'a été ajoutée sur le Serveur Dr.Web ou que les clés de licences ont été ajoutées sur le Serveur Dr.Web mais elles n'ont pas été distribuées sur l'objet, y compris le groupe **Everyone**.

Pour ajouter une clé de licence

1. Dans la liste **Toutes les clés** de la fenêtre **Clés de licence**, sélectionnez une ou plusieurs clés de licences que vous voulez ajouter.
2. Cliquez sur .
3. Cliquez sur **Enregistrer**.
4. Les clés seront ajoutées dans la liste des clés de licence de l'objet en tant que personnelles.

8.4. Configuration des composants antivirus



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

Composants

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

Postes tournant sous Windows

Scanner Dr.Web, Scanner Dr.Web Agent

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

SpIDer Guard

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



SpIDer Mail

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

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

SpIDer Gate

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

Office Control

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

Pare-feu

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

Elle comprend l'analyse de comportement, la protection contre les exploits et la protection contre les ransomwares.

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.



Contrôle des applications

Il surveille l'activité de tous les processus sur les postes. Il permet à l'administrateur du réseau antivirus de spécifier les applications dont le lancement sera autorisé ou bloqué sur les postes protégés.

Postes tournant sous l'OS de la famille UNIX

Dr.Web Scanning Engine

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.

Dr.Web File Checker

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 envoie 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).

Dr.Web ICAPD

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.

SpIDer Guard pour Linux (uniquement au sein des distributions conçues pour les OS de la famille 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 le 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.

SpIDer Guard pour SMB

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.

SplDer Guard pour NSS (uniquement au sein des distributions conçues pour les OS de la famille GNU/Linux)

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.

SplDer Gate (uniquement au sein des distributions conçues pour les OS de la famille GNU/Linux)

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.

Dr.Web MailD

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 SplDer Gate.



Les autres composants pour les postes tournant sous les OS de la famille UNIX sont supplémentaires et servent à configurer les paramètres internes du logiciel antivirus.

Postes tournant sous macOS

Scanner Dr.Web, Scanner Dr.Web Agent

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

SplDer Guard

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



SpIDer Gate

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

Quarantaine

Isolation des objets malveillants ou suspects dans un répertoire spécial.

Appareils mobiles tournant sous OS Android

Scanner Dr.Web, Scanner Dr.Web Agent

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

SpIDer Guard

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

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 de numéros inconnus.

Antivol

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

Cloud Checker

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

Pare-feu (les paramètres sont disponibles uniquement sur l'appareil mobile)

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

Contrôleur de sécurité (les paramètres sont disponibles uniquement sur l'appareil mobile)

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



Filtre d'applications

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

8.5. Scan antivirus des postes de travail



L'utilisateur du poste peut effectuer lui-même le scan antivirus avec le composant Scanner Dr.Web.

Le lancement et le fonctionnement du Scanner sont possibles même en cas d'Agent Dr.Web inactif, même lors du démarrage du système d'exploitation Windows en mode sans échec.

Via le Centre de gestion vous pouvez :



- Consulter la liste de tous les composants antivirus en cours d'exécution au moment spécifié.
- Interrompre des composants en cours selon leur type.
- Lancer des tâches de scan antivirus et configurer les paramètres du scan.

8.5.1. Interruption des composants en cours selon leur type



Lorsque vous utilisez cette option, les scans en cours seront interrompus, le Scanner arrêté et les moniteurs mis en pause.

Marche à suivre pour arrêter tous les composants en cours d'exécution en fonction du type spécifié :

1. Sélectionnez l'élément **Réseau antivirus** dans le menu principal du Centre de gestion. Puis dans la fenêtre qui apparaît, sélectionnez un groupe ou des postes dans l'arborescence.
2. Dans la barre d'outils du répertoire, cliquez sur le bouton  **Gestion des composants**. Dans la liste déroulante qui s'affiche, sélectionnez l'élément  **Arrêter les composants lancés**.
3. Dans la barre d'outils qui s'affiche, cochez les cases contre les types des composants que vous voulez arrêter immédiatement :
 - **Arrêter le Scanner Dr.Web Agent, lancé par le Planificateur de Tâches** : pour arrêter à l'aide du Scanner Dr.Web Agent le scan actif lancé conformément aux tâches de la planification centralisée.
 - **Arrêter le Scanner Dr.Web Agent lancé par l'administrateur** : pour arrêter à l'aide du Scanner Dr.Web Agent le scan actif lancé manuellement par l'administrateur via le Centre de gestion.
 - **Arrêter le Scanner Dr.Web lancé par l'utilisateur** : pour arrêter à l'aide du Scanner Dr.Web Agent le scan actif lancé par l'utilisateur sur le poste.




- **Arrêter SpIDer Guard, SpIDer Mail, SpIDer Gate, Office Control, le Pare-feu, l'Autoprotection et la Protection préventive** : pour suspendre le fonctionnement de ces composants.


Pour sélectionner tous les types des composants à interrompre, cochez la case contre l'entête de la barre d'outils **Interrompre les composants lancés**.

4. Cliquez sur le bouton **Interrompre**.


8.5.2. Lancement de l'analyse sur le poste de travail


Pour lancer le scan antivirus sur les postes de travail

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 groupe ou d'un poste dans la liste hiérarchique.
3. Dans la barre d'outils cliquez sur l'élément  **Scan**. Dans la liste qui va s'afficher dans la barre d'outils sélectionnez un mode de scan :

 **Scan rapide**. Ce mode assure le scan des objets suivants :

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

 **Scan complet**. Ce mode assure l'analyse complète de tous les disques durs ainsi que des supports amovibles (y compris les secteurs d'amorçage).

 **Scan personnalisé**. Dans ce mode, vous pouvez choisir des fichiers et dossiers à analyser et configurer des paramètres avancés du scan.

4. Après la sélection du type de scan, la fenêtre des paramètres du Scanner Dr.Web Agent va s'ouvrir. Modifiez les paramètres de scan si nécessaire (voir la rubrique [Configuration du Scanner](#)).
5. Cliquez sur **Scanner** pour lancer le processus de scan sur les postes sélectionnés.



Le scan des postes via le Scanner Dr.Web Agent lancé à distance est effectué en tâche de fond sans afficher aucune notification sur le poste de l'utilisateur.



8.5.3. Configuration du Scanner

Via le Centre de gestion, vous pouvez configurer les paramètres de contrôle antivirus suivants :

- Paramètres du Scanner Dr.Web. Ce Scanner est lancé par les utilisateurs sur les postes et ne peut pas être lancé à distance depuis le Centre de gestion. Mais l'administrateur peut modifier ses paramètres de façon centralisée et ces derniers seront transmis et sauvegardés sur les postes.
- Paramètres du Scanner Dr.Web Agent. Ce Scanner est lancé à distance depuis le Centre de gestion et effectue le contrôle des postes de la même façon que le Scanner Dr.Web. Les paramètres du Scanner Dr.Web Agent sont présentés comme des paramètres étendus du Scanner Dr.Web et configurés durant le lancement du contrôle antivirus des postes.

Configuration du Scanner Dr.Web

1. 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 groupe ou d'un poste dans la liste hiérarchique.
3. Dans le [menu de gestion](#) de la rubrique **Configuration**, sélectionnez l'élément **Scanner** dans la sous-rubrique du système d'exploitation nécessaire. La fenêtre des paramètres du Scanner Dr.Web va s'ouvrir.
4. Configurez les paramètres nécessaires du scan. La description des paramètres du Scanner Dr.Web est disponible dans le **Manuel de gestion des postes** pour le système d'exploitation correspondant.
5. Cliquez sur **Sauvegarder**. Les paramètres seront sauvegardés dans le Centre de gestion et transmis aux postes correspondants.

Configuration des paramètres du Scanner Dr.Web Agent

Les paramètres du Scanner Dr.Web Agent sont configurés durant le lancement du contrôle antivirus des postes comme décrit dans le paragraphe [Lancement de l'analyse sur le poste de travail](#).

La liste des paramètres du Scanner Dr.Web Agent disponibles (+) ou non disponibles (-) dépend du mode de lancement du scan sur les postes. La liste est présentée dans le tableau ci-dessous.



Tableau 8-2. Liste des sections de paramètres du Scanner Dr.Web Agent en fonction du mode de lancement du scan

Mode de lancement du scan	Paramètres par rubrique			
	Général	Actions	Limitations	Exclusions
Scan personnalisé	+	+	+	+
Scan rapide	+	+	+	-
Scan complet	+	+	+	-

En fonction du système d'exploitation du poste sur lequel le scan à distance est lancé, seule une partie des paramètres du Scanner Dr.Web Agent sera disponible. Il s'agit des paramètres pris en charge par le système d'exploitation du poste.

8.5.3.1. Général



Les paramètres qui ne sont pas supportés dans le cadre du contrôle des postes sous les OS de la famille UNIX et macOS sont mis entre crochets [].

Les paramètres qui ne sont pas supportés dans le cadre de l'analyse des postes sous Android sont mis entre parenthèses ().

Dans la rubrique **Général**, vous pouvez configurer les paramètres suivants de l'analyse antivirus effectuée par le Scanner Dr.Web Agent :

- Dans la liste déroulante, sélectionnez un mode d'analyse :
 - **Analyse de tous les disques** : effectuer une analyse antivirus sur tous les disques locaux disponibles.
 - **Analyse des chemins indiqués** : effectuer une analyse antivirus par les chemins indiqués uniquement.

Dans le champ **Chemins à scanner**, indiquez la liste des chemins à scanner (pour savoir comment indiquer les chemins, consultez [Exclusions](#)).

- Pour ajouter une nouvelle ligne à la liste, cliquez sur et indiquez le chemin nécessaire dans la ligne qui s'affiche.
 - Pour supprimer un élément de la liste, cliquez sur contre la ligne correspondante.
- Cochez la case **Analyser les secteurs d'amorçage** pour que le Scanner Dr.Web Agent effectue l'analyse des secteurs d'amorçage des disques. Les secteurs d'amorçage des disques logiques ainsi que les principaux secteurs d'amorçage des disques physiques seront scannés.
- Cochez la case **Analyser les programmes lancés automatiquement** pour scanner les programmes qui se lancent automatiquement au démarrage du système d'exploitation.



- Cochez la case **[(Scan des applications et modules téléchargés)]** permet de scanner les processus lancés dans la mémoire vive.
- Cochez la case **[(Scan anti-rootkits)]** pour activer le scan à la recherche des programmes malveillants qui masquent leur présence dans le système.
- Cochez la case **Scanner les disques durs** pour effectuer le scan des disques durs "fixes" (disques durs etc.).
- Cochez la case **Scan des supports amovibles** pour analyser tous les supports amovibles, disquettes, CD/DVD, disques flash etc.
- Cochez la case **Utiliser l'analyse heuristique** afin que le Scanner Dr.Web Agent effectue la recherche des virus inconnus avec le moteur heuristique. Ce mode n'exclut pas des faux positifs du Scanner.
- Cochez la case **Suivre les liens symboliques** pour les suivre durant le scan.
- Cochez la case **[(Interrompre le scan lors du passage sur la batterie)]** pour interrompre l'analyse lorsque l'ordinateur fonctionne sur la batterie.
- Cochez la case **Désactiver le réseau durant le scan** pour déconnecter l'ordinateur du réseau local et de l'Internet durant le scan.
- Cochez la case **Archives** pour chercher des virus dans les fichiers contenus dans des archives.
- Cochez la case **Fichiers e-mail** pour analyser les boîtes e-mail.
- Cochez la case **Packages d'installation** pour analyser les packages d'installation de logiciels.
- Dans la liste déroulante **[(Priorité de scan)]** sélectionnez la priorité du processus du scan en fonction des ressources du système d'exploitation.
- Dans la liste **[(Niveau de charge des ressources de l'ordinateur)]**, sélectionnez la charge maximum de ressources autorisée pour le Scanner Dr.Web Agent. En l'absence d'autres tâches lancées, les ressources sont utilisées au maximum.



L'option **Niveau de charge des ressources de l'ordinateur** n'a aucune influence sur la valeur de la charge des ressources lors du scan dans le système monoprocesseur à un seul noyau.

- Dans le champ **[(Coeurs de processeur utilisés (nombre))]** spécifiez le nombre maximal des coeurs de processeur utilisés par le Scanner Dr.Web Agent. Les valeurs de 0 à 32 sont possibles. La valeur 0 indique d'utiliser tous les coeurs disponibles. Lors de la configuration du groupe de postes, notez qu'une valeur absolue est spécifiée pour ce paramètre et non pas le pourcentage du nombre total de coeurs disponibles. C'est pourquoi, la même valeur spécifiée peut provoquer une charge relative différente sur les postes avec un nombre différent de coeurs de processeur.
- La liste déroulante **[(Coeurs de processeur utilisés (%))]**, choisissez le pourcentage du nombre de coeurs utilisés par rapport au nombre total de coeurs disponibles.
- Dans la liste déroulante **(Actions effectuées après le scan)**, sélectionnez une action à effectuer juste après la fin de l'analyse :
 - **ne rien faire** : n'appliquer aucune action à l'ordinateur après la fin du scan.



- **éteindre le poste** : éteindre l'ordinateur de l'utilisateur après la fin du scan. Avant cela, le Scanner Dr.Web Agent applique les actions spécifiées aux menaces détectées.
- **redémarrer le poste** : redémarrer le poste après la fin du scan. Avant le redémarrage du poste, le Scanner Dr.Web Agent applique les actions spécifiées aux menaces détectées.
- **mettre le poste en veille.**
- **mettre le poste en veille.**



8.5.3.2. Exclusions

Dans la rubrique **Exclusions**, vous pouvez configurer la liste des fichiers et dossiers à exclure de l'analyse antivirus du Scanner Dr.Web Agent.



Avant d'ajouter des exclusions, merci de prendre connaissance des recommandations sur l'utilisation des logiciels antivirus pour les ordinateurs tournant sous Windows. Vous pouvez consulter l'article contenant toutes les informations nécessaires à l'adresse suivante — <https://support.microsoft.com/en-us/topic/virus-scanning-recommendations-for-enterprise-computers-that-are-running-windows-or-windows-server-kb822158-c067a732-f24a-9079-d240-3733e39b40bc>. Cet article vous permettra d'optimiser les performances système en cas d'utilisation d'un logiciel antivirus.

Pour éditer les listes des chemins et fichiers exclus

1. Entrez un chemin ou un fichier dans la ligne **Chemins et fichiers exclus**.
2. Pour ajouter une nouvelle ligne à la liste, cliquez sur  et indiquez le chemin nécessaire dans la ligne qui s'affiche.
3. Pour supprimer un élément de la liste, cliquez sur  contre la ligne correspondante.

La liste des objets exclus peut contenir les éléments suivants :

1. Le chemin vers l'objet à exclure spécifié de manière explicite, avec :
 - Le caractère \ exclut de l'analyse tout le disque système sous l'OS Windows,
 - Le caractère / exclut de l'analyse tout le système de fichiers racine sous l'OS de la famille UNIX,
 - Un chemin qui se termine par le caractère \ (ou / dans le cas des OS de la famille Unix) — ce répertoire sera exclu de l'analyse,
 - Un chemin qui ne se termine pas par le caractère \ (ou / dans le cas des OS de la famille Unix) — tout sous-dossier dont le chemin commence par la ligne spécifiée sera exclu de l'analyse.

Exemple pour Windows : `C:\Windows` — ne pas analyser les fichiers se trouvant dans le répertoire `C:\Windows` et ses sous-répertoires.

Exemple pour les OS de la famille UNIX : `/etc` — ne pas analyser les fichiers se trouvant dans le répertoire `/etc` et ses sous-répertoires.



2. Les masques des objets à exclure du scan. Pour spécifier les masques, les symboles ? et * peuvent être utilisés.

Exemple pour Windows : `C:\Windows**.dll` — ne pas analyser tous les fichiers ayant l'extension `dll` se trouvant dans tous les sous-répertoires du répertoire `C:\Windows`.

Exemple pour les OS de la famille UNIX : `/etc/*/*.pub` — ne pas analyser tous les fichiers ayant l'extension `pub` se trouvant dans tous les sous-répertoires du répertoire `/etc`.

3. Variables d'environnement spécifiées dans le système d'exploitation au sein du chemin d'accès aux objets exclus de l'analyse.

Exemple pour Windows : `%WINDIR%\SysWOW64\` — ne pas analyser les fichiers dans le sous-répertoire `SysWOW64` du répertoire `C:\Windows`.

Exemple pour les OS de la famille UNIX : `/home/*/network` — ne pas analyser les fichiers dans le sous-répertoire `network` du répertoire `/home`.

4. L'expression régulière. Les chemins peuvent être spécifiés avec des expressions régulières. A part cela, tout fichier dont le nom complet (avec le chemin) correspond à une expression régulière sera exclu de l'analyse.

La syntaxe des expressions régulières utilisées pour spécifier les chemins exclus est la suivante :

`qr{ <expression> } <cases>`

Le paramètre le plus souvent utilisé est le caractère `i`, ce paramètre désigne « ne pas prendre en compte la casse ».

Exemples des chemins et des fichiers exclus qui sont spécifiés avec les expressions régulières

Expression régulière	Valeur
<code>qr{\\pagefile\.sys\$}i</code>	ne pas analyser les fichiers d'échange de Windows
<code>qr{\\notepad\.exe\$}i</code>	ne pas scanner les fichiers <code>notepad.exe</code>
<code>qr{^C:}i</code>	ne rien scanner sur le disque C :
<code>qr{^.:\\WINNT\\}i</code>	ne rien scanner dans les répertoires <code>WINNT</code> sur tous les disques
<code>qr{(^C:) (^.:\\WINNT\\)}i</code>	deux derniers cas sont réunis
<code>qr{^C:\\dir1\\dir2\\file\.ext\$}i</code>	ne pas scanner le fichier <code>c:\dir1\dir2\file.ext</code>
<code>qr{^C:\\dir1\\dir2\\(.+\\)?file\.ext\$}i</code>	ne pas scanner le fichier <code>file.ext</code> s'il se trouve dans le répertoire <code>c:\dir1\dir2</code> ou dans ses sous-répertoires
<code>qr{^C:\\dir1\\dir2\\}i</code>	ne pas scanner le répertoire <code>c:\dir1\dir2</code> ni ses sous-répertoires



Expression régulière	Valeur
<code>qr{dir\[^\]+}i</code>	ne pas scanner le sous-répertoire <code>dir</code> se trouvant dans n'importe quel répertoire, mais vérifier les sous-dossiers
<code>qr{dir\\}i</code>	ne pas scanner le sous-répertoire <code>dir</code> se trouvant dans n'importe quel répertoire, ni ses sous-répertoires

Les expressions régulières sont brièvement décrites dans le document **Annexes**, [Annexe I. Utilisation des expressions régulières dans Dr.Web Enterprise Security Suite](#).

8.5.3.3. Actions

Dans la rubrique **Actions**, vous pouvez configurer la réaction du Scanner Agent Dr.Web en cas de détection de fichiers infectés ou suspects, de programmes malveillants ou d'archives infectées.



Scanner Dr.Web Agent applique automatiquement les actions spécifiées pour les objets malveillants détectés.

Les actions suivantes peuvent être appliquées aux menaces détectées :

- **Désinfecter** : restaurer l'objet dans son état antérieur à l'infection. Si l'objet est incurable ou que les tentatives de désinfection ont échoué, le traitement pour les objets incurables est appliqué.
Cette action ne peut être appliquée qu'aux objets infectés par un virus connu, excepté les Trojans, supprimés dès leur détection, et les fichiers contaminés se trouvant dans des objets complexes (archives, fichiers e-mail ou conteneurs de fichiers).
- **Supprimer** : supprimer les objets infectés.
- **Déplacer en Quarantaine** : déplacer les objets infectés vers le dossier de Quarantaine du poste.
- **Informé** : envoyer une notification sur la détection d'un virus au Centre de gestion (pour en savoir plus sur le mode de notification, voir la rubrique [Configuration des notifications](#)).
- **Ignorer** : laisser passer l'objet sans lui appliquer aucune action et aucune notification n'est inscrite dans les statistiques du scan.

**Tableau 8-3. Les actions du Scanner Dr.Web Agent appliquées aux différents événements viraux**

Objet	Action				
	Désinfecter	Supprimer	Déplacer en quarantaine	Notifier	Ignorer
Infectés	+/*	+	+	disponible si l'une des clés possède l'option AllowReportAction=Yes	
Suspects		+	+/*		+
Incurables		+	+/*		
Packages d'installation		+	+/*		
Archives		+	+/*		
Fichiers e-mail			+	+/*	+
Secteurs d'amorçage	+/*			+	
Adwares		+	+/*		+
Dialers		+	+/*		+
Canulars		+	+/*		+
Riskwares		+	+/*		+
Hacktools		+	+/*		+

Conventions

- | |
|---|
| + l'action est autorisée pour ce type d'objets |
| +/* l'action est appliquée par défaut à ce type d'objets |

Pour configurer des actions appliquées aux menaces détectées, utilisez les paramètres suivants :

- La liste déroulante **Infectés** indique la réaction du Scanner Dr.Web Agent à la détection d'un fichier infecté par un virus connu.



- La liste déroulante **Suspects** indique la réaction du Scanner Dr.Web Agent à la détection d'un fichier présumé infecté par un virus (lors d'une réaction du moteur heuristique).



Si le scan inclut le dossier d'installation de l'OS, il est recommandé de choisir l'action **Notifier** pour les fichiers suspects.

- La liste déroulante **Incurables** indique la réaction du Scanner Dr.Web Agent en cas de la détection d'un fichier infecté par un virus inconnu et si la tentative de réparation a échoué.
- La liste déroulante **Packages d'installation infectés** indique la réaction du Scanner Dr.Web Agent en cas de la détection d'un fichier infecté ou suspect contenu dans package d'installation de programmes.
- La liste déroulante **Archives infectées** indique la réaction du Scanner Dr.Web Agent en cas de la détection d'un fichier infecté ou suspect contenu dans une archive.
- La liste déroulante **Fichiers e-mail infectés** indique la réaction du Scanner Dr.Web Agent en cas de la détection d'un fichier infecté ou suspect au format e-mail.



Si un code viral ou de programme malveillant est détecté au sein d'objets complexes (archives, fichiers e-mail ou conteneurs de fichiers), les actions paramétrées pour ce type de menaces s'appliquent à l'objet en entier et pas seulement à la partie infectée.

- La liste déroulante **Secteurs d'amorçage infectés** indique la réaction du Scanner en cas de la détection d'un virus ou d'un code suspect dans la zone des secteurs d'amorçage.
- Dans la liste déroulante suivante, configurez la réaction du Scanner en cas de la détection de logiciels non sollicités :
 - **Adwares** ;
 - **Dialers** ;
 - **Canulars** ;
 - **Riskware** ;
 - **Hacktools**.



Si vous choisissez **Ignorer**, aucune action n'est appliquée : aucune notification n'est envoyée au Centre de gestion, de la même façon que lorsque vous choisissez **Notifier** pour la détection de virus.

Cochez la case **Afficher la progression du scan** pour afficher une barre de progression et une barre de statut du processus de scan des postes dans le Centre de gestion.

8.5.3.4. Limitations



Les paramètres qui ne sont pas supportés dans le cadre du contrôle des postes sous les OS de la famille UNIX et macOS sont mis entre crochets [].



La rubrique **Limitations** contient les paramètres suivants de l'analyse antivirus du Scanner Dr.Web Agent :

- **Durée maximum du scan (ms)** : la durée maximum du scan d'un objet en millisecondes. A l'expiration de ce délai, le scan de l'objet sera arrêté.
- **Niveau maximum d'emboîtement d'une archive** : quantité maximum des archives emboîtées. Si le niveau d'emboîtement est supérieur à la valeur spécifiée, le scan ne sera effectué que jusqu'au niveau d'emboîtement indiqué.
- **[Taille maximum de l'archive (Ko)]** : taille maximum de l'archive à scanner en kilooctets. Si la taille de l'archive est supérieure à la valeur spécifiée, l'extraction de l'archive et son analyse ne seront pas effectuées.
- **Ratio maximum de compression d'un archive** : si le Scanner Dr.Web Agent détermine que le ratio de compression est supérieur à la valeur spécifiée, l'extraction de l'archive et son analyse ne seront pas effectuées.
- **[Taille maximum d'un objet extrait (Ko)]** : taille maximum d'un objet extrait en kilooctets. Si le Scanner Dr.Web Agent détermine que la taille de l'archive après l'extraction est supérieure à la valeur spécifiée, l'extraction de l'archive et son analyse ne seront pas effectuées.
- **[Seuil de contrôle de la compression (Ko)]** : taille minimum en kilooctets du fichier archivé à partir de laquelle la vérification du ratio de compression sera effectuée.

8.6. Consultation des statistiques sur un poste

Le menu de gestion de la rubrique **Réseau antivirus** vous permet de consulter les informations suivantes :

- **Statistiques** : statistiques relatives au fonctionnement des outils antivirus sur le poste ainsi que les informations sur le statut des postes et des outils antivirus, pour consulter et sauvegarder les rapports contenant des données statistiques récapitulatives ou des extraits de tableaux spécifiques.
- **Graphiques** : les graphiques affichant des informations sur les infections détectées sur les postes.
- **Quarantaine** : accès distant au contenu de la Quarantaine sur le poste.

8.6.1. Statistiques



Vous pouvez configurer la création automatique du rapport statistique contenant l'ensemble des tableaux statistiques dont vous avez besoin. Ce rapport peut être enregistré au format nécessaire sur le Serveur Dr.Web ou bien, il peut être envoyé par e-mail.

Pur cela, configurez la tâche **Création d'un rapport statistique** dans la [planification](#) du Serveur Dr.Web.



Pour consulter les tableaux

1. Sélectionnez l'élément **Réseau antivirus** dans le menu principal du Centre de gestion, puis dans la fenêtre qui apparaît, cliquez sur le nom du poste ou du groupe dans l'arborescence.
2. Dans le [menu de gestion](#) qui s'affiche, sélectionnez l'élément nécessaire dans la rubrique **Statistiques**.

La rubrique **Statistiques** comprend les éléments suivants :

- **Menaces** : pour consulter les informations sur la détection des menaces de sécurité sur les postes protégés : liste des objets infectés, emplacement par postes, noms de menaces, actions réalisées par l'antivirus, etc.



En cas de blocage d'URL pour les virus et les mineurs, l'action Signalé s'affiche dans le tableau.

- **Erreurs** : pour consulter la liste des erreurs de scan sur un poste sélectionné pour une période déterminée.
- [Données sommaires](#) : pour consulter et sauvegarder les rapports contenant toutes les données statistiques sommaires ou les données de synthèse sélectives selon les types de tableaux spécifiés. Cet élément ne s'affiche pas dans le menu si tous les autres éléments sont masqués dans la rubrique **Statistiques**.
- [Statistiques de scan](#) : pour obtenir les statistiques sur le fonctionnement des outils antivirus sur le poste.
- **Démarrage/Arrêt** : pour consulter la liste des composants lancés sur le poste.
- **Statistiques des menaces** : pour consulter les informations sur la détection des menaces de sécurité sur les postes. Les informations sont triées selon les types des menaces et le nombre des menaces sur les postes.
- [Statut](#) : pour consulter les informations sur un statut non-standard des postes et éventuellement nécessitant une intervention.
- **Tâches** : pour consulter la liste des tâches spécifiées pour le poste durant une période donnée.
- **Périphériques bloqués** : pour consulter la liste des périphériques bloqués par le composant Office Control sur les postes.
- **Produits** : pour consulter les informations sur les produits installés sur les postes sélectionnés. Sous produits on comprend dans ce cas les produits du [référentiel](#) du Serveur Dr.Web.
- **Bases virales** : pour consulter les informations sur les bases virales installées : nom du fichier contenant la base virale, version de la base virale ; total d'entrées dans la base ; date de création de la base. Cet élément n'est accessible qu'à condition qu'un poste soit sélectionné.
- **Modules** : pour consulter les informations détaillées sur tous les modules de l'antivirus Dr.Web : nom fonctionnel, hash MD5, version complète du module etc. Cet élément n'est accessible que lors de sélection de postes.



- **Événements de la Protection préventive** : pour consulter les événements enregistrés sur les postes par le composant Protection préventive.
- **Événements du Contrôle des applications** : pour voir les informations sur les événements enregistrés sur les postes par le composant Contrôle des applications.
- **Installations des Agents** : pour consulter la liste des installations de l'Agent Dr.Web sur le poste ou dans le groupe des postes.
- **Désinstallations des Agents** : pour consulter la liste des postes de travail sur lesquels le logiciel Dr.Web a été supprimé.



Pour afficher les éléments masqués de la rubrique **Statistiques**, sélectionnez l'élément **Administration** du menu principal, puis dans la fenêtre qui apparaît, sélectionnez l'élément du menu de gestion **Configuration du Serveur Dr.Web**. Dans l'onglet **Statistiques**, cochez les cases correspondantes (voir ci-dessous), cliquez ensuite sur le bouton **Enregistrer** et redémarrez le Serveur Dr.Web.

Tableau 8-4. Correspondance entre les éléments de la rubrique Statistiques et les cases de la rubrique Statistiques dans la configuration du Serveur Dr.Web

Éléments de la rubrique Statistiques	Cases de la rubrique Statistiques dans la configuration du Serveur Dr.Web
Menaces	Menaces de sécurité détectées
Erreurs	Erreurs de scan
Statistiques de scan	Statistiques de scan
Démarrage/Arrêt	Démarrage/arrêt des composants
Statistiques des menaces	Menaces de sécurité détectées
Statut	Statuts des postes
Tâches	Journal d'exécution des tâches sur les postes
Périphériques bloqués	Périphériques bloqués
Bases virales	Statuts des postes Statut des bases virales
Modules	Liste des modules des postes
Événements de la Protection préventive	Menaces de sécurité détectées
Événements du Contrôle des applications	Statistiques du Contrôle des applications sur l'activité des processus



Éléments de la rubrique Statistiques	Cases de la rubrique Statistiques dans la configuration du Serveur Dr.Web
	Statistiques du Contrôle des applications sur le blocage des processus
Installations des Agents	Installations des Agents


Les fenêtres affichant les résultats du fonctionnement des composants divers ainsi que des statistiques sommaires ont la même interface et les actions permettant d'entrer dans les détails de chaque fenêtre sont analogues.

Vous trouverez ci-après quelques exemples de consultation des statistiques sommaires via le Centre de gestion.

8.6.1.1. Données sommaires

Pour consulter les données sommaires


1. Sélectionnez un poste ou un groupe dans la liste hiérarchique.
2. Sélectionnez l'onglet **Statistiques sommaires** dans la rubrique **Statistiques** du [menu de gestion](#).
3. La fenêtre contenant les données de tableau du rapport va s'ouvrir.





Pour insérer les données statistiques particulières dans le tableau, cliquez sur le bouton  dans la barre d'outils et sélectionnez les types nécessaires dans la liste déroulante : **Statistiques de scan, Menaces, Tâches, Démarrage/Arrêt, Erreurs**. Les statistiques de ces rubriques sont identiques à celles de la rubrique **Tableaux**. Pour voir le rapport avec les tableaux sélectionnés, cliquez sur **Actualiser**.

4. Si le tableau avec les menaces détectés est inclus dans le rapport, les options suivantes seront disponibles dans la barre d'outils :

Option	Description
 Exclure les fichiers du scan	<p>Permet d'ajouter les objets sélectionnés dans la liste des exclusions du scan par les composants de la protection :</p> <ol style="list-style-type: none">a) Dans le tableau Menaces, cochez les cases contre un ou plusieurs objets détectés.b) Cliquez sur le bouton .c) Dans la fenêtre qui s'affiche, configurez les paramètres suivants :<ul style="list-style-type: none">• Exclure du scan et spécifier les paramètres personnalisés de SpIDer Guard : ajouter les objets sélectionnés dans la liste d'exclusions à appliquer lors du scan par le composant SpIDer Guard. Dans ce cas, si les nœuds du réseau, pour lesquels la liste d'exclusions sera modifiée, ont hérité les paramètres du composant SpIDer Guard de leurs



Option	Description
	<p>groupes primaires, l'héritage sera rompu pour ces groupes et les paramètres personnalisés seront spécifiés.</p> <ul style="list-style-type: none">• Exclure du scan et spécifier les paramètres personnalisés du Scanner Dr.Web : ajouter les objets sélectionnés dans la liste d'exclusions à appliquer lors du scan par le composant Scanner Dr.Web. Dans ce cas, si les nœuds du réseau, pour lesquels la liste d'exclusions sera modifiée, ont hérité les paramètres du composant Scanner Dr.Web de leurs groupes primaires, l'héritage sera rompu pour ces groupes et les paramètres personnalisés seront spécifiés.• Dans la liste Exclure pour les objets suivants, sélectionnez les nœuds du réseau pour lesquels l'objet sélectionné sera ajouté dans la liste d'exclusions : soit uniquement pour le poste sur lequel l'objet a été détecté, soit pour les postes et les groupes utilisateurs sélectionnés dans la liste. <p>d) Cliquez sur le bouton Exclure.</p>
 Scanner	Rescanner les objets sélectionnés. Dans le menu déroulant, sélectionnez le type de scan.

5. Pour consulter les informations relatives à une période donnée, vous pouvez sélectionner depuis la liste déroulante une période par rapport à la date courante ou choisir depuis la barre d'outils une plage de dates nécessaire. Pour spécifier une plage de dates, saisissez les dates correspondantes ou cliquez sur l'image représentant un calendrier contre le champ de date. Pour télécharger des données, cliquez sur **Actualiser**.
6. Pour sauvegarder le rapport pour l'imprimer ou le traiter plus tard, cliquez sur l'un des boutons suivants :
 -  **Sauvegarder les données dans un fichier CSV,**
 -  **Sauvegarder les données dans un fichier HTML,**
 -  **Sauvegarder les données dans un fichier XML,**
 -  **Sauvegarder les données dans un fichier PDF.**

8.6.1.2. Statistiques de scan

Pour obtenir des statistiques sur le fonctionnement des outils antivirus sur le poste





1. Sélectionnez un poste ou un groupe dans la liste hiérarchique.



Pour consulter les statistiques relatives aux plusieurs postes ou groupes, vous pouvez les sélectionner à l'aide des touches SHIFT ou CTRL.


2. Dans le [menu de gestion](#), dans la rubrique **Statistiques**, sélectionnez l'élément **Statistiques de scan**.
3. Par défaut, les statistiques relatives aux dernières vingt-quatre heures s'affichent.



4. Pour consulter les informations relatives à une période déterminée, vous pouvez indiquer dans la liste déroulante une période arbitraire par rapport à la date courante ou choisir depuis la barre d'outils une plage de dates nécessaire. Pour spécifier une plage de dates, saisissez les dates nécessaires ou cliquez sur les icônes du calendrier contre les champs des dates. Pour charger des données, cliquez sur **Actualiser**. Les tableaux statistiques seront chargés.
5. Afin de consulter les statistiques détaillées sur le fonctionnement des outils antivirus, cliquez sur le nom de poste dans le tableau. Une fenêtre (ou une rubrique de la fenêtre active) contenant le tableau avec les données détaillées va s'ouvrir.
6. Pour effectuer un tri des données contenues dans une colonne du tableau, cliquez sur la flèche correspondante (afin de trier par ordre croissant ou décroissant) dans l'en-tête respectif.
7. Afin de sauvegarder un tableau de statistiques pour l'imprimer ou le traiter plus tard, cliquez sur le bouton :
 -  **Sauvegarder les données dans un fichier CSV,**
 -  **Sauvegarder les données dans un fichier HTML,**
 -  **Sauvegarder les données dans un fichier XML,**
 -  **Sauvegarder les données dans un fichier PDF.**
8. Pour consulter les statistiques sommaires triées par événements viraux sous forme graphique, dans le [menu de gestion](#), sélectionnez l'élément **Graphiques**. Une fenêtre contenant des diagrammes statistiques va s'afficher (pour en savoir plus, consultez les informations [ci-dessous](#)).

8.6.1.3. Statut

Pour consulter les données sur l'état des postes

1. Sélectionnez un poste ou un groupe dans la liste hiérarchique.
2. Dans le [menu de gestion](#), sélectionnez l'élément **Statut** dans la rubrique **Statistiques**.
3. Les données sur le statut de postes s'affichent conformément aux paramètres du filtre. Cliquez sur l'icône  dans l'en-tête du tableau pour modifier les paramètres suivants du filtre :
 - Dans le champ **Recherche**, entrez une ligne aléatoire pour la recherche dans toutes les sections du tableau.
 - Dans la liste **Importance**, cochez les cases de niveaux nécessaires d'importance de messages : la liste de messages sur le statut va contenir uniquement les messages avec le niveau d'importance sélectionné.
 - Dans la liste **Source**, cochez les cases pour les sources des événements qui seront affichés dans la liste :
 - **Agent** : afficher les événements venus des Agents Dr.Web connectés à ce Serveur Dr.Web.



- **Serveur** : afficher les événements venus de ce Serveur Dr.Web.
- Dans la liste **Postes** cochez les cases pour les types de statut des postes dont les messages seront affichés dans la liste :
 - **Connectés** : afficher les événements pour les postes qui sont connectés à ce Serveur Dr.Web et qui sont en ligne (online) en ce moment.
 - **Déconnectés** : afficher les événements pour les postes qui sont connectés à ce Serveur Dr.Web et qui sont hors ligne (offline) en ce moment.
 - **Désinstallés** : afficher le dernier événement pour les postes sur lesquels l'antivirus Dr.Web a été supprimé.

Pour gérer les paramètres du filtre, utilisez les boutons suivants dans la liste du filtre :

- **Par défaut** : restaurer tous les paramètres par défaut du filtre.
 - **Actualiser** : appliquer les paramètres sélectionnés du filtre.
4. Les actions relatives au niveau de détails et au formatage des informations de ce tableau sont identiques aux actions pour le tableau des statistiques de scan décrites ci-dessus.



Pour consulter les rapports de fonctionnement et les statistiques de plusieurs postes, sélectionnez-les dans la liste hiérarchique réseau.

5. Pour sauvegarder le rapport pour l'imprimer ou le traiter plus tard, cliquez sur l'un des boutons suivants sur le panneau de gestion :



Sauvegarder les données dans un fichier CSV,



Sauvegarder les données dans un fichier HTML,



Sauvegarder les données dans un fichier XML,



Sauvegarder les données dans un fichier PDF.

8.6.1.4. Événements du Contrôle des applications

Configuration d'obtention des statistiques

Pour activer l'envoi des informations de postes pour la section Événements du Contrôle des applications

1. Dans la section **Réseau antivirus**, sélectionnez dans l'arborescence le poste ou le groupe de postes avec le Contrôle des applications installé depuis lequel vous voulez recevoir les informations concernant le lancement des applications.
2. Dans le menu de gestion, sélectionnez **Windows** → **Agent Dr.Web** si un groupe a été sélectionnée ou **Agent Dr.Web** si un poste a été sélectionné.
3. Dans l'onglet **Général**, cochez la case **Suivre les événements du Contrôle des applications** pour suivre l'activité des processus sur les postes enregistrée par le Contrôle des applications et envoyer les événements sur le Serveur Dr.Web. S'il n'y a pas de connexion au



Serveur Dr.Web, les événements sont accumulés et envoyés, une fois la connexion établie. Si la case est décochée, l'activité des processus est ignorée.

4. Cliquez sur **Enregistrer**.

Pour activer la collecte des informations par le Serveur Dr.Web pour la section Événements du Contrôle des applications

1. Dans la section **Administration** → **Configuration du Serveur Dr.Web**, accédez à l'onglet **Statistiques**.

2. Spécifiez l'une des options suivantes :

- **Statistiques du Contrôle des applications sur l'activité des processus** pour obtenir et enregistrer les informations sur toute activité de tous les processus dont le lancement est autorisé ou bloqué par le Contrôle des applications. Si vous choisissez cette option, les applications seront enregistrées dans le répertoire seulement après la création et l'assignation d'au moins un [profil](#) avec une ou plusieurs catégories de [critères d'analyse fonctionnelle](#) sélectionnées.

Avant la création de profils et leur assignation aux postes du réseau antivirus, le lancement de toutes les applications est autorisé.

- **Statistiques du Contrôle des applications sur l'activité des processus** pour obtenir et enregistrer les informations sur l'activité de tous les processus dont le lancement est bloqué par le Contrôle des applications. Si vous choisissez cette option, les applications seront enregistrées dans le répertoire seulement après la création des [profils](#) dont les paramètres bloqueront le lancement des applications et l'assignation de ces profils aux postes du réseau antivirus.



La case **Statistiques du Contrôle des applications sur l'activité des processus** peut augmenter considérablement la charge de la collecte des statistiques sur tout le réseau antivirus.

3. Cliquez sur **Enregistrer**.

4. Redémarrez le Serveur Dr.Web.

5. Après le redémarrage, le Serveur Dr.Web commencera à enregistrer, selon les paramètres spécifiés, toutes les statistiques de lancement des applications envoyées depuis tous les postes avec le Contrôle des applications installée.

Consultation des statistiques

Pour voir les événements enregistrés sur les postes par le composant Contrôle des applications

1. Sélectionnez un poste ou un groupe dans la liste hiérarchique.

2. Dans le [menu de gestion](#), sélectionnez l'élément **Événements du Contrôle des applications** dans la rubrique **Statistiques**.



3. La fenêtre s'ouvre affichant la liste des applications dont le lancement a été autorisé ou interdit sur les postes sélectionnés.
4. Les statistiques pour les 24 heures s'affichent par défaut. Pour consulter les informations relatives à une période déterminée, indiquez dans la liste déroulante une période arbitraire par rapport à la date courante ou choisissez depuis la barre d'outils une plage de dates nécessaire. Pour spécifier une plage de dates, saisissez les dates nécessaires ou cliquez sur les icônes du calendrier contre les champs des dates. Pour charger des données, cliquez sur **Actualiser**. Les tableaux statistiques seront chargés. Vous trouverez la description des colonnes du tableau ci-dessous.

Tableau 8-5. Description des colonnes du tableau Événements du Contrôle des applications

Nom de la colonne	Description
Identificateur	Identificateur du poste
Poste	Nom du poste
Adresse du poste	Adresse du poste
Identificateur de sécurité	Identificateur de sécurité du compte utilisateur
Utilisateur	Utilisateur du poste de travail
Type d'événement	Type de l'événement lancé sur le poste
Action appliquée	Action appliquée à l'application lancée sur le poste
Critère de l'analyse fonctionnelle	Critère selon lequel l'application est autorisée ou bloquée
Masque de l'analyse fonctionnelle	Paramètre du critère de l'analyse fonctionnelle qui détermine si l'application est autorisée à se lancer ou pas
ID du profil	Identificateur du profil
Nom du profil	Nom du profil
ID de la règle	Identificateur de la règle
Nom de la règle	Nom de la règle
Mode de fonctionnement	Mode de fonctionnement de la règle
Chemin vers le fichier de processus	Localisation du fichier de processus
Processus	Processus autorisé à se lancer sur le poste ou bloqué



Nom de la colonne	Description
Bulletin avec le hash du processus	Bulletin contenant le hash du fichier du processus lancé
Chemin du fichier de script	Localisation du fichier de script
Script	Fichier du script
Bulletin avec le hash du script	Bulletin contenant le hash de fichier du script lancé
Apparition de l'événement	Date et heure de l'apparition de l'événement
Notification de l'événement	Date et heure de notification de l'événement
Hash de fichier (SHA-256)	Valeur du hash de fichier par l'agorithme SHA-256
Description du fichier	Description du fichier
Éditeur	Éditeur du fichier
Éditeur du certificat	Centre de certification qui a délivré le certificat
Empreinte du certificat (SHA-1)	Valeur du hash de certificat par l'algorithme SHA-1
Date de début du certificat	Date de début du certificat
Date de fin du certificat	Date de fin du certificat

5. Afin de sauvegarder un tableau de statistiques pour l'imprimer ou le traiter plus tard, cliquez sur le bouton :

 **Sauvegarder les données dans un fichier CSV,**

 **Sauvegarder les données dans un fichier HTML,**

 **Sauvegarder les données dans un fichier XML,**

 **Sauvegarder les données dans un fichier PDF.**



S'il y a un profil ou une règle en [mode test](#) lancé sur les postes assignés, les applications sont analysées conformément au [schéma de fonctionnement du Contrôle des applications](#) du début à la fin. Les statistiques vont contenir les cas de concordance de l'application à tous les critères suivants : les paramètres de l'analyse fonctionnelle, les règles et le groupe



d'applications de confiance. Ainsi, une application peut avoir plusieurs enregistrements dans la colonne **Règle appliquée** qui indiquent que l'application est autorisée selon un critère et/ou elle bloquée selon un autre critère.

Création de règles

Pour créer une nouvelle règle à partir des statistiques des événements du Contrôle des applications

1. Dans la section **Statistiques** → **Événements du Contrôle des applications**, sélectionnez la ligne portant sur une tentative du lancement de l'application pour laquelle vous voulez créer une règle contrôlant le lancement.
2. Quand vous cliquez sur une ligne du tableau, une fenêtre contenant les informations sur l'événement sélectionné s'ouvre.
3. Cliquez sur le bouton **Créer une règle** (à la base des données du processus ou de l'application).
4. Une fenêtre de création d'une nouvelle règle s'ouvre. Spécifiez les paramètres suivants :
 - a) Dans la liste déroulante **Nom de profil**, sélectionnez un [profil](#) du Contrôle des applications dans lequel la règle sera créée.
 - b) Dans le champ **Nom de règle**, spécifiez un nom pour la règle créée.
 - c) Dans la section **Type de règle**, sélectionnez le type de la règle créée : une règle de [blocage](#) ou une règle d'[autorisation](#).
 - d) Pour l'option **Mode de fonctionnement**, sélectionnez un mode dans lequel la règle créée fonctionnera (cela correspond à la case **Faire basculer la règle en mode test** lors de la création de la règle depuis le profil) :

Si vous voulez tester la règle, sélectionnez le mode **Test**. Les applications sur les postes ne seront pas bloquées, pourtant l'activité sera journalisée comme si les paramètres étaient activés. Les résultats de lancements et de blocages d'applications en mode test s'afficheront dans la section **Événements du Contrôle des applications**.

En mode **Actif**, la règle fonctionnera en mode actif avec le blocage des applications sur les postes conformément aux paramètres de règle spécifiés (voir aussi les [modes de fonctionnement des profils](#)).
 - e) Dans la section **Bloquer le lancement des applications selon les critères suivants/Autoriser le lancement des applications selon les critères suivants** (en fonction du type de règle sélectionnée à l'étape 4c), les champs seront automatiquement remplis conformément à l'application sur laquelle la règle est basée. Si nécessaire, vous pouvez modifier les valeurs des paramètres.
5. Cliquez sur **Enregistrer**. La règle sera créée dans le profil spécifié du Contrôle des applications.



8.6.2. Graphiques

Graphiques et tableaux d'infections

Afin de consulter les graphiques et les tableaux communs contenant les informations sur les infections détectées

1. Sélectionnez l'élément **Réseau antivirus** dans le menu principal du Centre de gestion. Puis dans la fenêtre qui apparaît, cliquez sur le nom d'un poste ou d'un groupe dans l'arborescence. Dans le [menu de gestion](#) qui s'ouvre, sélectionnez l'élément **Graphiques** dans la section **Général**.
2. La fenêtre affichant les données graphiques et numériques suivantes va s'ouvrir :
 - **Activité virale** : le graphique présente le nombre total des virus détectés pendant une période donnée pour tous les postes et les groupes sélectionnés.
 - **Menaces les plus répandues** : le top 10 des menaces présents dans le plus grand nombre de fichiers. Le graphique présente les données numériques par objets relatifs à une menace concrète.
 - **Classes de menaces** : cet élément affiche la liste des menaces conformément à la classification des objets malveillants. Le diagramme circulaire présente le pourcentage de chaque menace détectée.
 - **Actions réalisées** : cet élément affiche la liste des actions appliquées aux objets malveillants détectés. Le diagramme circulaire présente le pourcentage de chaque action réalisée.
 - **Postes les plus attaqués** : cet élément affiche la liste des postes sur lesquels les menaces de sécurité ont été détectées. Le tableau présente le nombre total des menaces pour chaque poste.
3. Pour consulter les données relatives à une période définie, sélectionnez une période dans la liste déroulante dans la barre d'outils : le rapport pour un jour ou un mois. Vous pouvez également sélectionner n'importe quelle plage de dates, pour cela, entrez les dates nécessaires ou sélectionnez les dates dans les calendriers déroulantes. Pour afficher les données, cliquez sur le bouton **Actualiser**.

Graphiques et tableaux des statistiques totales

Les données graphiques et numériques sont présentées dans l'élément **Graphique** de la section **Général** ainsi que dans certains éléments de la section **Statistiques** du menu de gestion. Le tableau ci-dessous contient la liste de tous les graphiques et les tableaux possibles, ainsi que les sections correspondantes du menu de gestion dans lesquels ces éléments sont affichés.

**Tableau 8-6. Conformité des graphiques et tableaux aux rubriques du menu de gestion**

Graphiques et tableaux	Rubriques
Activité virale	Graphiques
Menaces les plus répandues	Graphiques Menaces Statistiques des menaces
Classes des menaces	Graphiques Statistiques des menaces
Postes les plus attaqués	Graphiques
Actions réalisées	Graphiques Menaces
Nombre d'erreurs par poste	Erreurs
Nombre d'erreurs par composant	Erreurs
Menaces par composant	Démarrage/Arrêt
Erreurs par composants	Démarrage/Arrêt

- **Nombre d'erreurs par poste** : cet élément affiche la liste des postes sur lesquels survenaient des erreurs de fonctionnement des composants antivirus. Le graphique présente le nombre total d'erreurs pour chaque poste.
- **Nombre d'erreurs par composant** : cet élément affiche la liste des composants antivirus dont le fonctionnement provoquaient des erreurs. Le diagramme circulaire présente le pourcentage d'erreurs pour chaque composant.
- **Menaces par composant** : cet élément affiche la liste des composants antivirus qui ont détecté les menaces. Le graphique présente le nombre total des menaces détectées par chaque composant.
- **Erreurs par composant** : cet élément affiche une liste des composants antivirus dont le fonctionnement provoquaient des erreurs. Le graphique présente le nombre total d'erreurs pour chaque composant.

8.6.3. Identificateurs de sécurité

Pour voir les informations sur les identificateurs de sécurité 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 d'un poste ou d'un groupe dans



l'arborescence. Ensuite, sélectionnez l'élément **Identificateurs de sécurité** dans la section **Général** du menu de gestion dans la partie gauche de la fenêtre.

2. La fenêtre affichant les données suivantes va s'ouvrir :
 - **Identificateur** : identificateur unique du poste. Il est spécifié lors de la création du compte du poste et ne peut pas être modifié après.
 - **Poste** : nom du poste. Il est spécifié lors de la création du compte du poste et sera automatiquement remplacé par le nom de l'ordinateur après la connexion de l'Agent Dr.Web.
 - **Adresse** : adresse IP du poste.
 - **Identificateur de sécurité** : identificateur de sécurité unique (SID – security identifier) de l'ordinateur. Le champ est rempli automatiquement après la connexion du poste tournant sous Windows au Serveur Dr.Web.
 - **Date de la dernière connexion** : date de la dernière tentative de connexion de ce poste au Serveur Dr.Web.
3. Pour consulter les données relatives à une période définie, sélectionnez une période dans la liste déroulante dans la barre d'outils : le rapport pour un jour ou un mois. Ensuite, cliquez sur le bouton **Actualiser**. Vous pouvez également sélectionner n'importe quelle plage de dates, pour cela, entrez les dates nécessaires ou sélectionnez les dates dans les calendriers déroulantes et cliquez sur le bouton **Actualiser**.

8.6.4. Quarantaine

Contenu de la quarantaine

Les fichiers peuvent être mis en quarantaine par un des composants antivirus, par exemple, par le Scanner.

L'utilisateur peut rescanner lui-même les fichiers se trouvant dans la quarantaine via le Centre de gestion ou via le Gestionnaire de quarantaine sur le poste.

Pour consulter et modifier le contenu de la quarantaine dans le Centre de gestion

1. Sélectionnez l'élément **Réseau antivirus** dans le menu principal du Centre de gestion, puis dans la fenêtre qui apparaît, cliquez sur le nom du poste ou du groupe dans l'arborescence. Dans le [menu de gestion](#), sélectionnez l'élément **Quarantaine** dans la rubrique **Général**.
2. La fenêtre contenant les données sur le statut actuel de la quarantaine va s'ouvrir.

Si un seul poste a été sélectionné, le tableau contenant les objets se trouvant dans la quarantaine sur ce poste sera affiché.

Si plusieurs postes ou un groupe/plusieurs groupes ont été sélectionnés, le jeu de tableaux contenant les objets se trouvant en Quarantaine sur chaque poste sera affiché.





Les statistiques du rescane de l'objet en quarantaine affichées dans la colonne **Informations** concerne uniquement le rescane lancé via le Centre de gestion.

S'il y a plusieurs menaces qui sont déplacées en quarantaine, cliquez sur le nombre d'objets déplacés dans la colonne **Informations** pour voir toute la liste de menaces dans une fenêtre pop-up.

Si l'objet placé en Quarantaine a le statut **non infecté**, cela signifie qu'après la mise en quarantaine cet objet considéré comme menace a été rescanné et il a reçu le statut sain.

Les objets de la quarantaine peuvent être restaurés seulement manuellement.









3. Pour consulter les fichiers placés en quarantaine pour une période donnée, vous pouvez sélectionner dans la liste déroulante une période par rapport à la date courante ou spécifier une plage de dates dans la barre d'outils. Pour spécifier une plage de dates, saisissez les dates nécessaires ou cliquez sur l'image représentant un calendrier contre les champs de dates. Pour consulter des données, cliquez sur **Actualiser**.
4. Pour modifier l'affichage des données, cliquez sur l'icône  dans l'en-tête du tableau :
 - Spécifiez les paramètres d'affichage de lignes (cela concerne surtout de longues lignes).
 - Sélectionnez les colonnes à afficher dans le tableau.
5. Pour filtrer les fichiers de la quarantaine, cliquez sur le bouton  dans l'en-tête du tableau et spécifiez les paramètres de filtrage suivants :
 - **Recherche** : spécifiez une ligne aléatoire pour la recherche dans toutes les sections du tableau. Seules les lignes correspondant aux résultats de recherche seront affichées dans le tableau.
 - **Composant déplaçant** : sélectionnez le composant de protection Dr.Web qui a déplacé les fichiers en quarantaine.
 - **Menace** : sélectionnez le nom de la menace détectée conformément à la classification de la société Doctor Web.
 - **Nom d'origine** : entrez le nom d'origine de l'objet avant son déplacement en Quarantaine.
 - **Taille de fichiers, en octets** : utilisez le curseur pour spécifier la plage de tailles des objets détectés en octets.

Cliquez sur **Appliquer** pour afficher les fichiers de la quarantaine conformément aux paramètres spécifiés du filtre.


Cliquez sur le bouton **Par défaut** pour réinitialiser les paramètres de filtrage.

6. Pour gérer les fichiers se trouvant en quarantaine, cochez les cases correspondantes à un fichier, un groupe de fichiers ou pour tous les fichiers placés en quarantaine (la case se trouve dans l'en-tête du tableau). Dans la barre d'outils, sélectionnez une des actions suivantes :



Option	Description
 Supprimer les fichiers	
	 Supprimer les fichiers sélectionnés Supprimer les fichiers sélectionnés de la Quarantaine et du système.
	 Supprimer tous les fichiers Supprimer de la quarantaine et du système tous les fichiers correspondant aux paramètres de filtrage sélectionnés, c'est-à-dire tous les fichiers affichés dans la fenêtre de la quarantaine.
 Exporter Copier et enregistrer le fichier sélectionné. Après avoir déplacé les fichiers suspects dans la quarantaine locale sur l'ordinateur de l'utilisateur, vous pouvez copier et enregistrer ces fichiers via le Centre de gestion/ Par exemple, pour les envoyer plus tard pour l'analyse dans le laboratoire antivirus de Doctor Web. Lors de l'exportation, le fichier est mis en archive qui reçoit le nom correspondant au hash du fichier exporté. A part de l'objet exporté, l'archive contient également un fichier CSV contenant des informations générales à propos de l'objet. L'archive est protégée par le mot de passe <code>virus</code> par défaut.	
 Restaurer les fichiers	
 N'utilisez l'option de restauration de fichiers de la quarantaine que dans le cas où vous êtes vraiment sûr que l'objet ne présente aucun danger.	
	 Restaurer les fichiers sélectionnés Restaurer l'emplacement d'origine des fichiers sélectionnés dans la fenêtre, c'est-à-dire restaurer les fichiers dans les répertoires où il se trouvait avant d'être mis en quarantaine.
	 Restaurer les fichiers selon les paramètres Dans la fenêtre qui s'affiche, configurez les paramètres suivants : <ul style="list-style-type: none">• Si un objet est sélectionné :



Option	Description
	<ul style="list-style-type: none">▫ Restaurer le fichier sous : restaurer le fichier sélectionné depuis la Quarantaine et le placer dans un chemin spécifié avec le nom spécifié. Dans le champ Restaurer le fichier dans le chemin suivant, spécifiez le chemin complet sur le poste dans lequel le fichier sélectionné sera restauré. Le nom de fichier doit être obligatoirement spécifié. L'emplacement initial du fichier (avant le déplacement) est utilisé par défaut. Si nécessaire, vous pouvez modifier ce paramètre.▫ Restaurer les fichiers selon le type de menace : restaurer tous les fichiers de la Quarantaine auxquels on a attribué le même type de menace que celui du fichier sélectionné. Le type de menace est indiqué dans le champ Restaurer les fichiers contenant la menace suivante.▫ Restaurer les fichiers dans un chemin : restaurer les fichiers de la Quarantaine déplacés depuis un répertoire particulier. Dans le champ Restaurer tous les fichiers déplacés en Quarantaine du répertoire suivant, spécifiez le chemin d'accès au répertoire sur le poste. Tous les fichiers déplacés en Quarantaine depuis ce répertoire seront restaurés, Le chemin d'accès initial (avant le déplacement) est utilisé par défaut. Si nécessaire, vous pouvez modifier ce paramètre.• Si plusieurs objets sont sélectionnés :<ul style="list-style-type: none">▫ Restaurer les fichiers : restaurer les fichiers vers leur emplacement d'origine sur l'ordinateur. C'est-à-dire restaurer les fichiers dans les répertoires où ils se trouvaient avant d'être placés en Quarantaine.▫ Restaurer les fichiers selon le type de : restaurer les fichiers de la Quarantaine auxquels on a attribué le même type de menace que celui des fichiers sélectionnés.• Dans la liste Restaurer sur les objets suivants, sélectionnez les noeuds du réseau sur lesquels l'objet sélectionné sera restauré de la Quarantaine : soit uniquement pour le poste sur lequel l'objet a été détecté, soit pour les groupes utilisateurs sélectionnés dans la liste.• Ajouter des exceptions en tant que les paramètres personnalisés de SplDer Guard : ajouter les objets sélectionnés dans la liste d'exclusions lors du scan par le composant SplDer Guard. Dans ce cas, si les noeuds du réseau pour lesquels la liste d'exclusions a été modifiée ont hérité les paramètres du composant SplDer Guard de leurs groupes primaires, alors l'héritage sera rompu et les paramètres personnalisés seront spécifiés.• Ajouter des exceptions en tant que paramètres personnalisés du Scanner Dr.Web : ajouter les objets sélectionnés dans la liste d'exclusions à appliquer lors du scan par le composant Scanner Dr.Web. Dans ce cas, si les noeuds du réseau, pour lesquels la liste d'exclusions sera modifiée, ont hérité les paramètres du composant Scanner Dr.Web de leurs groupes primaires, l'héritage sera rompu pour ces groupes et les paramètres personnalisés seront spécifiés.
	 Restaurer tous les fichiers



Option	Description
	Restaurer l'emplacement d'origine de tous les fichiers dans la fenêtre de la quarantaine, c'est-à-dire restaurer les fichiers dans les répertoires où il se trouvait avant d'être mis en quarantaine.
 Scanner les fichiers	
	 Scanner les fichiers sélectionnés Rescanner les fichiers sélectionnés dans la quarantaine.
	 Scanner tous les fichiers Rescanner tous les fichiers dans la fenêtre de la quarantaine.



Sur les postes désactivés la demande sera envoyée uniquement après la connexion des postes au Serveur Dr.Web.

7. Exporter les données sur le statut de la quarantaine vers un fichier sous un des formats suivants :



Sauvegarder les données dans un fichier CSV,



Sauvegarder les données dans un fichier HTML,




Sauvegarder les données dans un fichier XML,




Sauvegarder les données dans un fichier PDF.

8.6.5. Rapports du support technique

Collecte des informations système

1. Sélectionnez un poste ou un groupe de postes pour lesquels il faut créer un rapport.
2. Dans l'onglet **Général** de la barre d'outils, sélectionnez l'élément  **Créer un rapport pour le support technique.**
3. Confirmez le lancement de création du rapport.



Une fois la création des rapports pour un poste ou un groupe de postes lancée, l'icône  reste active, mais il devient impossible de lancer sur un poste la création de plusieurs rapports en même temps. S'il s'agit d'un groupe, la création d'un nouveau rapport sera lancé quand vous double-cliquez sur l'icône. Pourtant elle concernera uniquement les postes sur lesquels la collecte du rapport précédent est terminée ou arrêtée. Les autres postes ignoreront cette commande.



4. Pour voir le statut du rapport, cliquez sur **Détails**. Si la collecte des rapports est lancée ou reportée, un message s'affichera. Ce message comprendra le lien vers la section du tableau ou s'affiche le processus de création des rapports et des fichiers de rapports terminés.

Voir les rapports

Les informations sur le statut de la collecte des rapports et les fichiers des rapports sont disponibles dans le tableau de la section **Réseau antivirus** → **Général** → **Rapports pour le support technique**.



Le tableau peut contenir plusieurs rapports pour le même poste.

Le tableau contient les données suivantes :

- **Identificateur** : ID du poste.
- **Poste** : nom du poste.
- **Adresse du poste** : par défaut.
- **Nom du rapport** : nom du fichier de rapport.
- **Hash SHA-256** : hash SHA-256 du fichier de rapport.
- **Progression** : progression de l'exécution de la tâche (création du rapport) en pourcentage.
- **Statut** : statut de la collecte (**Création en cours**/**Téléchargement en cours**/**Terminé**/**Erreur**).
- **Erreurs** : message d'erreur.
- **Heure du début** : heure du début de la collecte.
- **Heure de la fin** : heure de la fin de la collecte.

Les boutons au-dessus du tableau permettent de lancer ou d'annuler la création du rapport, de supprimer du serveur les rapports arrêtés ou terminés (les rapports ne sont pas stockés sur le poste) et de télécharger les rapports.



Le tableau ne garde pas le statut des rapports en attente (quand l'Agent Dr.Web n'a pas encore envoyé les informations sur le statut) ou les rapports des postes qui ne prennent pas en charge cette fonction.

8.7. Envoi des fichiers d'installation

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



l'Agent Dr.Web via ce package d'installation dans le **Manuel d'installation**, la rubrique [Installation de l'Agent Dr.Web en mode local](#)).

Après avoir créé les packages d'installation, pour plus de commodité, vous pouvez envoyer les packages d'installation concrets sur les e-mails des utilisateurs.

Lors de l'envoi des packages d'installation, le contenu de la lettre est généré de la façon suivante :

1. Les pièces jointes sont interdites dans les paramètres (la case **Envoyer seulement le lien** est cochée, voir ci-dessous) : seuls les liens de téléchargement de packages sont envoyés dans le message.
2. Le système d'exploitation est connu (les pièces jointes sont autorisées) :
 - a) OS Windows : le package d'installation de l'Agent Dr.Web pour Windows est attaché en pièce jointe.
 - b) Linux, macOS, Android : le package d'installation de l'Agent Dr.Web pour le système d'exploitation correspondant et le fichier de configuration contenant les paramètres de connexion au Serveur Dr.Web sont attachés en pièces jointes.
3. Le système d'exploitation est inconnu : un nouveau compte du poste, l'Agent Dr.Web n'est pas encore installé (les pièces jointes sont autorisées) :
 - a) Si sur le Serveur Dr.Web il n'y a pas de packages d'installation sous Linux, macOS, Android (notamment, les **Produits d'entreprise Dr.Web** ne sont pas téléchargés sur le Serveur Dr.Web), le package d'installation de l'Agent Dr.Web pour Windows et le fichier de configuration contenant les paramètres de connexion au Serveur Dr.Web pour les postes sous Linux, macOS, Android sont attachés au message en pièces jointes.
 - b) Si sur le Serveur Dr.Web il y a au moins un seul package d'installation pour les postes tournant sous Windows : le package d'installation de l'Agent Dr.Web pour Windows est attaché à la lettre en pièce jointe, ainsi que le fichier de configuration avec les paramètres de connexion au Serveur Dr.Web pour les postes sous Linux, macOS Android et le lien de téléchargement des fichiers d'installation pour les postes tournant sous Linux, macOS, Android.

Pour envoyer les paquets d'installation par e-mail

1. Sélectionnez l'élément **Réseau antivirus** du menu principal du Centre de gestion, puis dans la fenêtre qui apparaît, sélectionnez les objets suivants dans l'arborescence :
 - sélectionnez le poste pour envoyer par e-mail le package d'installation généré pour ce poste.
 - sélectionnez le groupe des postes pour envoyer par e-mail tous les packages d'installation générés pour les postes de ce groupe.

Pour sélectionner plusieurs objets en même temps utilisez les boutons CTRL et SCHIFT.

2. Dans la barre d'outils, cliquez sur **Général** → **Envoyer les fichiers d'installation**.
3. Dans la rubrique **Envoyer les fichiers d'installation** qui s'affiche, configurez les paramètres suivants :



- Dans la section **Général** :
 - Cochez la case **Mettre dans une archive zip** pour mettre les fichiers d'installation dans une archive zip. L'archivage peut être utile en cas de présence des filtres e-mail du côté de l'utilisateur qui peuvent bloquer les fichiers exécutables qui se trouvent en pièces jointes.
 - Cochez la case **Envoyer seulement le lien** pour envoyer dans le message seulement le lien de téléchargement du package. Dans ce cas, le fichier du package d'installation ne sera pas joint au message. Cette option peut être utile au cas où le serveur de messagerie de client supprime automatiquement les pièces jointes des e-mails.
- Dans la section **Adresse e-mail du destinataire**, spécifiez l'adresse e-mail à laquelle le package d'installation sera envoyé. Si plusieurs postes ou groupes ont été sélectionnés, spécifiez les adresses e-mail pour chaque poste en particulier pour envoyer les packages d'installation.



Les paramètres d'envoi d'e-mails sont configurés dans le menu **Administration**, la rubrique **Configuration du Serveur Dr.Web**, l'onglet **Réseau**, l'onglet intérieur [E-mail](#).

4. Cliquez sur **Envoyer**.

8.8. Envoi de messages aux postes

L'administrateur système peut envoyer des messages aux utilisateurs, qui peuvent contenir les informations suivantes :

- texte du message ;
- hyperliens vers des ressources Internet ;
- logo de société (ou tout visuel).

L'en-tête du message comprend également la date précise de réception du message.

Les messages sont affichés du côté de l'utilisateur sous forme d'infobulles (voir [la figure 8-1](#)).

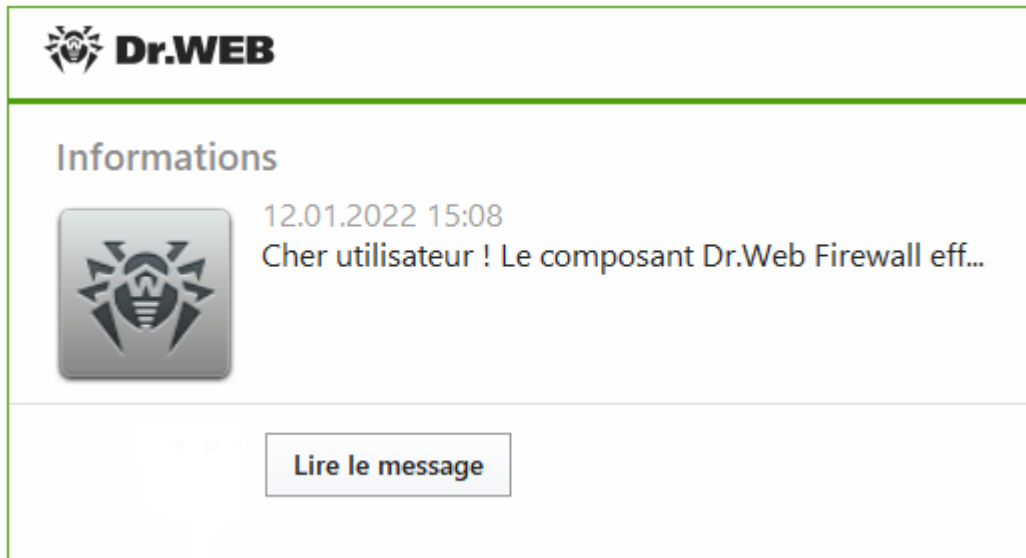



Figure 8-1. Fenêtre d'un message sur un poste tournant sous Windows

Pour envoyer un message à un utilisateur

1. Dans le menu principal du Centre de gestion, sélectionnez l'élément **Réseau antivirus**.
2. Dans la fenêtre qui apparaît, sélectionnez un groupe ou un poste dans l'arborescence, puis dans la barre d'outils cliquez sur **★ Général** → **Envoyer des messages aux postes**.
3. Dans la fenêtre qui apparaît, remplissez les champs suivants :
 - Dans le champ **En-tête du message**, vous pouvez spécifier un en-tête du message, par exemple, le nom de l'entreprise. Ce texte sera affiché dans l'en-tête de la fenêtre de message (à droite du logo). Si vous laissez ce champ vide, des informations sur le message s'afficheront au lieu du logo.
 - **Texte du message** : champ obligatoire.
 - Cochez la case **Afficher le logo dans le message** pour afficher le logo dans l'en-tête de la fenêtre de message. Spécifiez les paramètres suivants du logo :
 - A droite du champ **Fichier du logo**, cliquez sur le bouton  pour télécharger le logo depuis une ressource locale et sélectionnez ensuite l'objet nécessaire dans le fichier dans l'explorateur (voir [Format du fichier de logo](#)).
 - Cochez la case **Afficher le lien dans le message** pour insérer le lien sur les ressources web dans le message.

Pour ajouter un lien, procédez comme suit :

- a) Dans le champ **Nom du lien**, spécifiez le nom du lien : le texte à afficher à la place du lien dans le message.
- b) Dans le champ **Adresse URL pour le lien** spécifiez l'adresse URL d'une page web à ouvrir avec un clic sur le lien.
- c) Dans le champ **Texte du message**, ajoutez le marqueur `{link}` partout où vous voulez insérer le lien. Dans le message final, le lien sera inséré selon les paramètres spécifiés. Le nombre de balises `{link}` dans le texte est illimité, cependant, toutes



les balises auront les mêmes paramètres (depuis les champs **Adresse URL pour le lien** et **Nom du lien**). S'il y a un ou plusieurs marqueurs `{link}`, le lien sera inséré uniquement à la place des marqueurs.

d) Si le marqueur `{link}` n'est pas indiqué dans le champ **Texte du message**, le lien sera ajouté une fois sur une ligne distincte à la fin du message.

- Cochez la case **Envoyer seulement sur les postes sur le réseau** pour envoyer le message uniquement sur les postes qui sont sur le réseau (online). Si la case est cochée, le message ne sera pas envoyé sur les postes qui sont hors réseau. Si la case est décochée, l'envoi du message sur les postes hors réseau sera reporté jusqu'au moment de leur connexion.
- Cochez la case **Afficher le statut de l'envoi** pour afficher la notification sur le statut de l'envoi.

4. Cliquez sur **Envoyer**.

Format du fichier de logo

Le fichier contenant une image (logo) incluse dans le message doit correspondre aux critères suivants :

1. Format graphique du fichier : BMP, JPG, PNG, GIF, SVG.
2. La taille du fichier de logo ne doit pas dépasser 512 Ko.
3. Dimensions de l'image — 72x72 pixels. Les images ayant d'autres dimensions seront mises à l'échelle lors de l'envoi jusqu'aux dimensions par défaut.
4. Profondeur de couleur (bit depth) : n'importe laquelle (8 — 24 bits).



Si vous souhaitez utiliser un logo ayant un fond transparent, utilisez les fichiers au format PNG ou GIF.

Avant l'envoi du message aux utilisateurs (surtout en cas de message à plusieurs destinataires), il est recommandé de tester l'envoi en envoyant le message vers un poste avec un Agent Dr.Web installé pour être sûr que cela fonctionne correctement.



Exemple de l'envoi du message

Pour envoyer le message affiché dans la [figure 8-1](#), les paramètres suivants ont été spécifiés :

Texte du message :

```
Cher utilisateur !
```

```
Le composant Pare-feu Dr.Web a été installé sur votre ordinateur.
```

```
Pour plus d'informations sur les fonctionnalités de ce composant consultez  
{link}.
```

```
Cordialement,
```

```
Administration
```

Adresse URL pour le lien : `http://drweb.com/`

Nom du lien : `ici`



Chapitre 9 : Gestion des postes dans les environnements virtuels

Dr.Web Enterprise Security Suite peut être utilisé pour la protection de l'infrastructure virtuelle - les clusters de machines virtuelles fournissant les services aux clients (appelés ci-dessous les VM *client*) : hébergement virtuel, système de postes de travail à distance, clouds d'entreprise, etc.

Une ou plusieurs machines virtuelles du cluster reçoivent le rôle de *service* ; le logiciel spécifique est installé sur ces machines virtuelles (Serveur de scan Dr.Web) avec lequel elles traitent les demandes d'analyse antivirus de la part des machines virtuelles client.

Le Serveur de scan contient :

- le moteur de scan effectuant l'analyse pour la présence de menaces des données reçues ;
- les bases virales et les bases des filtres intégrés pour l'Office Control .

L'Agent virtuel Dr.Web est installé sur les VM client. Il est géré par le Serveur Dr.Web et transmet les demandes de scan et les fichiers à scanner sur une VM de service. Ce schéma de fonctionnement diminue considérablement la charge sur les machines virtuelles client grâce aux facteurs suivants :

- l'analyse est mise hors des VM client ;
- il n'est pas nécessaire de maintenir l'état actuel des bases virales et de la base de filtres intégrés sur chaque VM client.

La configuration avec le Serveur de scan permet :

- d'économiser la mémoire vive ;
- de baisser la charge sur le sous-système disque des machines virtuelles ;
- de baisser la charge sur le réseau.

L'approche utilisée provoque l'augmentation de la charge du processeur. Les configurations avec le Serveur de scan sont plus efficaces si le réseau antivirus est placé au sein d'un seul serveur physique L'utilisation du réseau virtuel (et non pas physique) pour la transmission des données entre les VM se trouvant sur le même serveur (hyperviseur) peut assurer une grande vitesse d'échange de données et d'analyse.

Le Serveur de scan peut être membre de tout groupe. On peut également réunir les Serveurs de scan dans un groupe à part, même automatiquement [à la base des règles d'appartenance définies](#).



L'ajout du Serveur de scan dans des groupes et la configuration des règles d'appartenance sont effectués de la même manière que pour les autres postes. Vous trouverez les informations détaillées sur la gestion des groupes dans la rubrique [Placement des postes dans les groupes](#).

Les postes interagissent avec le Serveur de scan par l'Agent Dr.Web fonctionnant en mode virtuel (Agent virtuel Dr.Web). L'Agent Dr.Web est géré par le Serveur Dr.Web et envoie des



demandes d'analyse des fichiers et des URL au Serveur de scan. Lors du passage en mode virtuel l'Agent Dr.Web cesse d'utiliser les bases virales et sans connexion au Serveur de scan reste sans protection. Ainsi, les Agents virtuels ne peuvent pas être utilisés sans installation et configuration du Serveur de scan.

9.1. Connexion de postes au Serveur de scan

Le Serveur de scan est une machine virtuelle qui a un statut particulier. Un logiciel spécial est installé sur le Serveur de scan pour le traitement de demandes de scan antivirus de la part des autres machines virtuelles.

Vous trouverez les informations détaillées sur l'installation et la configuration du Serveur de scan dans le **Manuel d'installation**, p. [Installation du Serveur de scan Dr.Web](#).



Le Serveur de scan peut être installé uniquement sous les OS de la famille Linux et FreeBSD.

Le serveur de scan et les machines virtuelles avec l'Agent Dr.Web installé qu'il dessert doivent se placer au sein d'un seul hyperviseur.



La connexion de postes au Serveur de scan est possible uniquement si c'est autorisé par les conditions de votre licence.

Pour connecter un poste au Serveur de scan

1. Dans le menu principal du Centre de gestion, sélectionnez l'élément **Réseau antivirus** (icône).
2. Sélectionnez un poste (icône ou si le poste est activé) ou un groupe de postes (icône) à connecter au Serveur de scan (icône) dans l'arborescence du réseau antivirus. Les postes connectés au Serveur de scan sont représentés dans l'arborescence sous forme d'éléments imbriqués.
3. Dans la section **Configuration**, sélectionnez **Agent virtuel**.
4. Cochez la case **Utiliser le serveur de scan** et indiquez l'adresse du Serveur de scan dans le champ **Adresse réseau du Serveur de scan**.



Vous pouvez indiquer une seule adresse du Serveur de scan pour un Agent virtuel.

S'il ne faut pas indiquer une adresse spécifique, utilisez la configuration par défaut `udp://:18008` — dans ce cas le Serveur de scan sera déterminé automatiquement quelle que soit l'adresse assignée — IPv4 ou IPv6.



L'adresse indiquée doit avoir l'un des formats suivants :

- `tcp://<adresse IP>:<port>` (on peut indiquer des adresses IPv4 et des adresses IPv6; l'adresse IPv6 doit être indiquée entre crochets, par exemple `tcp://[fd15:4ba5:5a2b:1008:edc8:733e:1dd7:789c]:7777`);
- `udp://:<port>` (seuls le protocole et le port par lequel les postes chercheront le Serveur de scan sont indiqués dans ce format)
- `srv://service@<domain>` (l'adresse et le port du serveur de service sont déterminés par la recherche de l'enregistrement SRV du domaine DNS `<domain>`; si le domaine n'est pas indiqué, il sera pris du fichier de configuration DNS, du champ `search` ou `domain` — cela dépend du champ figurant en dernier dans le fichier de configuration).

5. Cliquez sur le bouton **Enregistrer**.

Droits

Les droits suivants sont disponibles aux utilisateurs des postes tournant sous les OS de la famille UNIX :

- lancement du Serveur de scan,
- arrêt du Serveur de scan,
- modification de la configuration du Serveur de scan.

Par défaut seul le droit de lancement du Serveur de scan est accordé.

Si nécessaire, l'ensemble des droits accordés peut être modifié par l'administrateur du réseau antivirus. Pour en savoir plus sur les droits, consultez la rubrique [Droits des utilisateurs du poste](#).

Paramètres avancés

Des paramètres supplémentaires peuvent être spécifiés sur le Serveur de scan et sur les postes UNIX qui y sont connectés. Ils sont ensuite indiqués dans le fichier de configuration `drweb.ini` (section `[MeshD]`). Vous pouvez apporter des modifications dans le fichier `drweb.ini` via le Centre de gestion (dans les paramètres du poste, sélectionnez **UNIX** → **Agent Dr.Web** → **Configuration**).

Vous trouverez la description détaillée des paramètres dans le tableau ci-dessous.



Seule l'adresse du Serveur de scan peut être spécifiée pour les postes tournant sous Windows. Les autres configurations décrites dans le tableau ne sont pas supportées.

Paramètre	Description
<code>LogLevel</code> <i>{niveau de détail}</i>	Niveau de détail de journal. Il peut prendre une des valeurs suivantes :



Paramètre	Description
	<ul style="list-style-type: none">• DEBUG : le niveau le plus détaillé (de débogage). Tous les messages et toute l'information de débogage sont affichés.• INFO : tous les messages sont affichés.• NOTICE : les messages d'erreurs, les avertissements et les notifications sont affichés.• WARNING : les messages d'erreur et les avertissements sont affichés.• ERROR : seuls les messages d'erreurs sont affichés. <p>Valeur par défaut : Notice</p>
<code>-log</code> <i>{type de journal}</i>	<p>Mode de journalisation. Il peut prendre une des valeurs suivantes :</p> <ul style="list-style-type: none">• <code>Stderr[:ShowTimestamp]</code> : les messages s'affichent dans le flux d'erreurs standard <code>stderr</code>.• <code>Auto</code> : les messages à enregistrer dans le journal sont transmis au démon de gestion de configuration Dr.Web ConfigD sur le poste qui les enregistre dans un emplacement unique conformément à ses propres configurations.• <code>Syslog[:<facility>]</code> : les messages seront transmis par un composant au service de journalisation système <code>syslog</code>.• La marque supplémentaire <code><facility></code> est utilisée pour indiquer le type de journal dans lequel <code>syslog</code> enregistrera les messages. Valeurs possibles :<ul style="list-style-type: none">▫ <code>DAEMON</code> : messages de démons ;▫ <code>USER</code> : messages de processus utilisateur ;▫ <code>MAIL</code> : messages de programmes de messagerie ;▫ <code>LOCAL0</code> : messages de processus locaux 0 ;...▫ <code>LOCAL7</code> : messages de processus locaux 7.▫ <code><chemin></code> : les messages seront enregistrés directement dans le fichier de journal indiqué sur le poste. <p>Valeur par défaut : Auto</p>
<code>IdleTimeLimit</code> <i>{délai}</i>	<p>Délai maximal d'arrêt de l'Agent virtuel ou du Serveur de scan à l'issue duquel il s'arrête.</p> <p>Le paramètre peut être spécifié sur le Serveur de scan et sur Agent virtuel.</p> <p>Si la valeur <code>None</code> est spécifiée, l'Agent virtuel/le Serveur de scan fonctionnera en permanence ; en cas d'inactivité, le signal <code>SIGTERM</code> ne lui sera pas envoyé.</p>



Paramètre	Description
	<p>Valeur munumale : 10s.</p> <p>Valeur par défaut : 30s</p>
DebugSsh <i>{logique}</i>	<p>Indiqué s'il faut journaliser les messages du protocole SSH sur le poste si le niveau de détail de journal <code>LogLevel = Debug</code> est spécifié.</p> <p>Valeur par défaut : No</p>
ListenAddress <i>{<adresse IP>:<port>}</i>	<p>Socket réseau (adresse et port) de connexion client sur lequel le Serveur de scan attend des connexions des postes client.</p> <p>Le paramètre peut être spécifié uniquement sur le Serveur de scan.</p> <p>Le paramètre doit être obligatoirement spécifié pour que le Serveur de scan écoute l'interface IPv6 et puisse détecter des Agents virtuels par Ipv6.</p> <p>Les adresses Ipv6 sont indiquées entre crochets.</p> <p>Si une ligne vide est spécifiée en tant que valeur de ce paramètre, le Serveur de scan s'arrêtera.</p> <p>Pour attribuer à ce paramètre la valeur ' ' (c'est-à-dire une ligne vide), il faut posséder en même temps les droits d'arrêter le Serveur de scan et de modifier sa configuration.</p>
DnsResolverConfPath <i>{chemin}</i>	<p>Chemin d'accès au fichier de paramètres du sous-système de résolution des noms de domaine (DNS resolver).</p> <p>Le paramètre est spécifié pour l'Agent virtuel si l'enregistrement SRV est spécifié en tant qu'adresse du Serveur de scan.</p> <p>Valeur par défaut : <code>/etc/resolv.conf</code></p>
DiscoveryResponderPort <i>{port}</i>	<p>Port sur lequel le Serveur de scan répond aux demandes de clients via le protocole UDP.</p> <p>Valeur par défaut : 18008</p>
EngineChannel <i>{On Off}</i>	<p>Activation et désactivation de la possibilité de fournir des service du moteur de scan pour le serveur.</p> <p>Le paramètre peut être spécifié uniquement sur le Serveur de scan.</p> <p>Valeur par défaut : On</p> <p>Pour changer la valeur de ce paramètre en <code>Off</code>, il faut posséder en même temps les droits d'arrêter et de modifier la configuration du Serveur de scan.</p>



Paramètre	Description
EngineUplink <i>{adresse}</i>	Adresse du Serveur de scan (indiquée au même format que lors de la configuration via le Centre de gestion). Le paramètre peut être spécifié uniquement sur l'Agent virtuel. Valeur par défaut : <i>Non spécifiée</i>
EngineDebugIpc <i>{logique}</i>	Afficher dans le journal les informations de débogage pour le service de scan si le niveau de détail de journal <code>LogLevel = Debug</code> est spécifié. Valeur par défaut : <code>No</code>
UrlChannel <i>{On Off}</i>	Activation et désactivation de la possibilité de fournir des service d'analyse d'URL pour le serveur. Valeur par défaut : <code>On</code> Pour changer la valeur de ce paramètre en <code>Off</code> , il faut posséder en même temps les droits d'arrêter et de modifier la configuration du Serveur de scan.
UrlUplink <i>{adresse}</i>	Adresse du hôte supérieur utilisé pour l'analyse d'URL. Le paramètre peut être spécifié uniquement sur l'Agent virtuel. Valeur par défaut : <i>Non spécifiée</i>
UrlDebugIpc <i>{logique}</i>	Afficher dans le journal les informations de débogage pour le service d'analyse d'URL si le niveau de détail de journal <code>LogLevel = Debug</code> est spécifié. Valeur par défaut : <code>No</code>



Pour en savoir plus sur la configuration des paramètres du Serveur de scan et des Agents virtuels, consultez les **Manuels Administrateur Dr.Web pour UNIX**, la section **Dr.Web MeshD**.

9.2. Intégration à l'infrastructure de bureau virtuel

Dr.Web Enterprise Security Suite supporte l'intégration à l'infrastructure de bureau virtuel (VDI). Cette possibilité est utile lors de la gestion de *clients légers* assurant le fonctionnement en mode terminal par le protocole RDP.

Le fonctionnement du réseau antivirus est organisé de la manière suivante :

1. L'administrateur du réseau antivirus crée une *image de référence de poste virtuel* avec les logiciels préinstallés et l'Agent Dr.Web. Ensuite, il connecte la référence au Serveur Dr.Web.



2. Des postes virtuels nécessaire sont clonés depuis la référence créée.
3. Une fois le délai spécifié écoulé, les postes virtuels sont supprimés. Ensuite, les postes virtuels sont créés de nouveau depuis la référence en cas de nécessité.

Pour préparer le réseau antivirus au fonctionnement avec VDI

1. Dans le menu principal du Centre de gestion, sélectionnez l'élément **Réseau antivirus** et créez un nouveau poste qui servira de référence.
2. Installez l'Agent Dr.Web et tous les logiciels nécessaires sur le poste créé. [Connectez le poste](#) au Serveur Dr.Web.
3. Désignez un des postes comme le Serveur de scan et [installez sur ce poste le logiciel nécessaire](#).
4. Dans les paramètres des postes créés, spécifiez qu'ils doivent utiliser le [Serveur de scan](#). Indiquez l'adresse du Serveur de scan auquel les postes se connecteront.
5. Dans la même section, [créez un nouveau groupe](#) dans lequel se placeront des postes virtuels.
6. Configurez l'ordre d'enregistrement de postes virtuels. Pour ce faire, accédez à la section **Administration** → [Procédures utilisateur](#). Ajoutez une nouvelle procédure à la base de l'événement **Un novice se connecte au Serveur Dr.Web**. Dans le champ **Texte de procédure**, indiquez :

```
local args = ... -- args.id, args.address, args.station

if args.id == '<identificateur_du_poste_de_référence>' then

    return { "id", dwcore.get_uuid(), "pgroup",
            "<identificateur_du_poste_de_référence>" }

end
```

En tant que *<identificateur_du_poste_de_référence>*, il faut indiquer l'ID du poste de référence créé à l'[étape 1](#). En tant que *<identificateur_du_groupe_primaire>*, indiquez l'ID du groupe créé à l'[étape 5](#). Ces informations sont toujours disponibles dans les propriétés d'objets dans l'arborescence du **Réseau antivirus**.

Lors du clonage, chaque nouveau poste virtuel recevra un identificateur correspondant à l'identificateur du poste de référence. Selon les conditions de la procédure, un nouveau UUID est généré pour le poste au moment de connexion du poste au Serveur Dr.Web. Ensuite, le poste est enregistré dans le groupe primaire avec l'identificateur indiqué.


Lors de l'écriture de la procédure, il est recommandé de vérifier le modèle de procédure intégrée **Un novice se connecte au Serveur Dr.Web**. Pour préciser les informations, y compris les paramètres alternatifs et les valeurs retournés possibles, sélectionnez **Examples of the hooks** → **Novices** → **Un novice se connecte au Serveur Dr.Web** dans l'arborescence de procédures du Centre de gestion.



Suppression planifiée de postes virtuels inactifs

Pour une distribution rationnelle de licences et pour éviter l'accumulation dans la base de données des informations sur les postes virtuels distants, il faut configurer la tâche de suppression automatique de postes inactifs. Les postes inactifs, ce sont des postes qui ne sont pas connectés au Serveur Dr.Web pendant le délai spécifié.

Pour préparer la tâche de suppression automatique de postes inactifs

1. Dans le Centre de gestion, accédez à la section **Administration** → **Planificateur de tâches du Serveur Dr.Web**.
2. Créez une nouvelle tâche, en cliquant sur le bouton  **Créer une tâche** dans la barre d'outils.



3. Sélectionnez **Exécution du script** dans la liste déroulante de l'onglet **Action**. Ensuite, importez le script lua suivant d'un fichier ou entrez-le manuellement dans le champ ci-dessous :

```
local adminName = 'admin'
-- on indique l'ID du groupe
local gid        = '<identificateur_du_groupe_primaire>'
-- on indique la période d'inactivité (en secondes)
local interval  = 86400

require('st-db-state')
require('core/datetime')
require('core/admins/admins')

local lastseen = Datetime.timeUnixstampToDBFormat(Datetime.nowTimestamp()
- interval)

local stations = {}
-- on envoie une requête à la base de données
local res, err1 = DBuilder()
    :select('id, lastseenat')
    :from('stations')
    :where('gid', gid)
    :where('lastseenat '..dwcore.base64_decode('PA=='), lastseen)
    :where('state !=', st_db_state.st_db_state_logged_in)
    :get()

if res and next(res) then
    for i = 1, #res do
        table.insert(stations, res[i][1])
    end
end

-- on supprime les postes inactifs
local function delete_stations(ids)
    local admin, err = Admin:initWithLogin(adminName)
    require 'core/admins/admins'
    require('core/stations/stations')
    local status, results_stations = Stations:delete(ids, admin)
    return ''
end

return delete_stations(stations)
```

En tant que *<identificateur_du_groupe_primaire>*, indiquez l'ID du groupe créé à l'[étape 5](#), lors de la préparation à la gestion de VDI.



Ce script accède à la base de données, reçoit l'ID de postes qui ne sont pas connectés au Serveur Dr.Web pendant les dernières 24 heures (86400 secondes) et supprime les postes du groupe avec l'ID indiqué.



Il est recommandé de mettre à jour l'image de référence chaque fois après la mise à jour des composants antivirus nécessitant un redémarrage du système d'exploitation. Après la mise à jour, vérifiez et corrigez l'identificateur du poste de référence dans le texte de la procédure, si cela est nécessaire.



Chapitre 10 : Configuration du Serveur Dr.Web

Cette chapitre contient la description de fonctionnalités suivantes de configuration du réseau antivirus et du Serveur Dr.Web :

- [Gestion des licences](#) : paramètres de licence ;
- [Journalisation](#) : consulter et gérer l'accès aux journaux du Serveur Dr.Web, consulter les statistiques détaillées sur le fonctionnement du Serveur Dr.Web ;
- [Configuration du Serveur Dr.Web](#) : configurer les paramètres du Serveur Dr.Web ;
- [Configuration de la planification du Serveur Dr.Web](#) : configurer la planification de tâches pour maintenir le Serveur Dr.Web ;
- [Configuration du Serveur web](#) : configurer les paramètres du Serveur web ;
- [Procédures utilisateur](#) : activer et configurer les procédures utilisateur ;
- [Configuration des notifications](#) : configurer le système de notification de l'administrateur sur les événements du réseau antivirus par les différents moyens de notification ;
- [Gestion du référentiel du Serveur Dr.Web](#) : configurer le référentiel pour la mise à jour de tous les composants du réseau antivirus depuis le SGM et la diffusion ultérieure des mises à jour sur les postes ;
- [Gestion de la base de données](#) : maintenir la base de données du Serveur Dr.Web ;
- [Particularités du réseau avec plusieurs Serveurs Dr.Web](#) : configurer le réseau antivirus multi-serveurs et les connexions entre serveurs ;
- [Intégration à l'infrastructure de bureau virtuel](#) : configurer le Serveur Dr.Web pour la gestion de l'infrastructure de bureau virtuel (VDI).

10.1. Gestion des licences

10.1.1. Gestionnaire de licences



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

Interface du Gestionnaire de Licences

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

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



Liste hiérarchique des clés

La fenêtre principale du Gestionnaire de licences contient l'arborescence des clés — la liste hiérarchique dont les nœuds sont les clés de licence, ainsi que les postes, les groupes et les politiques auxquels ces clés de licence sont assignées.

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

Option	Description	Disponibilité dans l'arborescence
 Ajouter une clé de licence	Enregistrement d'une nouvelle clé de licence.	Cette option est toujours disponible. Les fonctionnalités dépendent de la sélection de l'objet dans l'arborescence des clés (voir Ajouter une nouvelle clé de licence).
 Supprimer les objets sélectionnés	Supprimer la connexion entre la clé et l'objet soumis à licence.	L'option est disponible si un objet soumis à licence (poste, groupe ou politique) ou une clé de licence est sélectionnée dans l'arborescence.
 Distribuer la clé aux groupes et postes	Remplacer ou ajouter la clé sélectionnée à un objet soumis à licence.	L'option est disponible si une clé de licence est sélectionnée dans l'arborescence.
 Exporter la clé	Sauvegarder une copie locale du fichier clé de licence.	
 Vérifier la disponibilité des mises à jour et remplacer les clés de licence	Vérifier la disponibilité des mises à jour se trouvant dans le SGM pour toutes les clés. Si les mises à jour sont disponibles, télécharger les clés et remplacer (voir Mise à jour automatique de licences).	Cette option est toujours disponible. L'action affecte toutes les clés de licence dans l'arborescence.
 Distribuer la clé sur les Serveurs voisins Dr.Web	Distribuer les licences de la clé sélectionnée aux Serveurs voisins Dr.Web.	L'option est disponible si une clé de licence est sélectionnée dans l'arborescence.

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

- La case **Afficher le nombre de licences** active/désactive l'affichage du nombre total de licences fournies par les fichiers clés de licence.
- Pour modifier la structure de l'arborescence, utilisez les options suivantes :
 - L'option **Clés** permet d'afficher toutes les clés de licence du réseau antivirus en tant que nœuds à la racine de la liste hiérarchique. Ainsi, tous les groupes, les postes et les politiques auxquels ces clés sont assignées se présentent comme des éléments imbriqués



dans les clés de licence (éléments « enfants »). Ce mode de visualisation de l'arborescence est une vue d'ensemble et permet de gérer les objets soumis à licence et les clés de licence.

- L'option **Groupes** permet d'afficher les groupes contenant des objets auxquels les clés sont assignées directement en tant que noeuds à la racine de la liste hiérarchique. Ainsi, les postes et les politiques inclus à ces groupes et les clés de licence assignées à ces groupes se présentent comme des éléments "enfants" des groupes. Ce mode de visualisation permet d'obtenir des informations sur la licence mais ne permet pas de gérer les objets de l'arborescence.
- Pour modifier l'affichage de l'arborescence, utilisez les options suivantes :
 - **Afficher les identificateurs de clients** : active/désactive l'affichage des identificateurs uniques de postes.
 - **Afficher les noms de clients** : active/désactive l'affichage des noms de postes.
 - **Afficher les adresses de clients** : active/désactive l'affichage des adresses IP des postes.
 - **Afficher les descriptions** : active/désactive l'affichage des descriptions de postes et de groupes de postes.

Gestion des licences

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

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

Accéder aux données concernant une licence

Pour voir le récapitulatif sur une clé de licence, dans la fenêtre principale du Gestionnaire de licences, sélectionnez le compte de la clé dont vous voulez consulter les informations (cliquez sur le nom du compte de la clé). Dans le panneau qui s'ouvre, les informations suivantes s'affichent :

- Nombre de licences fournis et utilisés de ce fichier clé de licence.
- Utilisateur de la licence.
- Partenaire qui a vendu la licence.



- Numéro d'identification et numéro de série de la licence.
- Date d'expiration de la licence.
- Support du module Antispam par cette licence.
- Hash MD5 de la clé de licence.
- Listes autorisées de bulletins de hashes pour informer de l'appartenance des menaces détectées. Si la fonctionnalité n'est pas autorisée, le paramètre n'est pas présent.




L'absence d'une licence pour les bulletins de hashes ne baisse pas le niveau de protection antivirus. Cette licence permet d'ajouter une notification d'administrateur sur la présence de la menace détectée dans les bulletins spécialisés des hashes de menaces connus.

- La liste des composants antivirus pouvant être utilisés par cette licence.

Ajout d'une nouvelle clé de licence

Pour ajouter une nouvelle clé de licence

1. Dans la fenêtre principale du Gestionnaire de licences cliquez sur **+** **Ajouter une clé de licence** dans la barre d'outils.
2. Dans le panneau qui s'ouvre, cliquez sur  et sélectionnez le fichier clé de licence.
3. Cochez la case :
 - **Assigner la clé de licence au groupe Everyone**, si c'est la première clé de licence dans le réseau antivirus. La clé ajoutée sera automatiquement assignée au groupe **Everyone**.
 - **Remplacer la clé de licence du groupe Everyone**, si ce n'est pas la première clé de licence dans le réseau antivirus. La clé de licence actuelle du groupe **Everyone** sera remplacée par la clé de licence ajoutée.



S'il y a plusieurs clés de licence qui sont assignées au groupe **Everyone**, c'est la première clé de la liste qui sera remplacée.

Si vous voulez remplacer une clé de licence particulière du groupe **Everyone**, utilisez la procédure [Mise à jour de la clé de licence](#).

4. Cliquez sur **Enregistrer**.
5. La clé de licence sera ajoutée dans l'arborescence des clés.

Si à l'étape 3, vous n'avez pas coché la case correspondante, la clé de licence ajoutée ne sera assignée à aucun objet. Dans ce cas, pour spécifier les objets soumis à licence, appliquez les procédures [Remplacer la clé de licence](#) ou [Étendre la liste des clés de licence de l'objet](#) décrites ci-dessus.


Mettre à jour la clé de licence

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



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


Pour mettre à jour une clé de licence

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

Remplacer la clé de licence

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

Pour remplacer la clé de licence actuelle

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



Pour assigner une clé à la politique, il faut sélectionner la politique ou la version actuelle de cette politique (la clé est assignée automatiquement à la politique lors de la sélection de sa version actuelle ou vice-versa).

La clé de licence peut être assignée à n'importe quelle version de la politique qui n'est pas une politique actuelle. Dans ce cas, la clé sera assignée uniquement à cette version, mais pas à la politique. Une telle clé ne sera pas appliquée aux postes jusqu'à ce que la version actuelle de la politique ne soit remplacée par la politique à laquelle la clé a été assignée.

Il faut assigner la clé de licence directement aux politiques et leurs versions.


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



Étendre la liste des clés de licence de l'objet

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

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

1. Dans le menu principal du Gestionnaire de licences, dans l'arborescence des clés, sélectionnez la clé que vous souhaitez ajouter à la liste des clés de l'objet : groupe de postes, poste ou politique.
2. Cliquez sur  **Distribuer la clé aux groupes et postes** dans la barre d'outils. Une fenêtre contenant la liste hiérarchique du réseau antivirus s'ouvre.
3. Sélectionnez les objets dans la liste. Pour sélectionner plusieurs objets, utilisez les touches CTRL et SHIFT.



Pour assigner une clé à la politique, il faut sélectionner la politique ou la version actuelle de cette politique (la clé est assignée automatiquement à la politique lors de la sélection de sa version actuelle ou vice-versa).

La clé de licence peut être assignée à n'importe quelle version de la politique qui n'est pas une politique actuelle. Dans ce cas, la clé sera assignée uniquement à cette version, mais pas à la politique. Une telle clé ne sera pas appliquée aux postes jusqu'à ce que la version actuelle de la politique ne soit remplacée par la politique à laquelle la clé a été assignée.

Il faut assigner la clé de licence directement aux politiques et leurs versions.

4. Cliquez sur **Ajouter une clé de licence**. Une fenêtre contenant les paramètres des composants à installer décrits dans la sous-rubrique [Paramètres de modification d'une clé de licence](#), va s'ouvrir.
5. Cliquez sur **Enregistrer** pour ajouter la clé de licence.

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




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

La clé de licence doit être assignée aux postes sans paramètres personnels de la clé de licence.

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

1. Dans le menu principal du Gestionnaire de Licences, dans l'arborescence des clés, sélectionnez la clé de licence que vous souhaitez supprimer, ou l'objet (poste, groupe ou




politique) auquel cette clé est assignée, et cliquez sur  **Supprimer les objets sélectionnés** dans la barre d'outils. Ainsi :

- Si un groupe ou un poste a été sélectionné, il sera supprimé de la liste des objets pour lesquels la clé assignée est active. L'héritage de la clé de licence est établi pour le groupe ou le poste dont la clé de licence personnelle est supprimée.
 - Si une politique a été sélectionnée, la version actuelle de la politique sera supprimée de la liste des objets auxquels la clé de licence est assignée. Si la version actuelle de la politique a été sélectionnée, la politique-même sera également supprimée. Pourtant en cas de suppression d'une version non actuelle de la politique, la politique et la version actuelle ne seront pas supprimées.
 - Si la clé de licence a été sélectionnée, le compte de cette clé est supprimé du réseau antivirus. L'héritage de la clé de licence est établi pour tous les groupes et les postes auxquels cette clé de licence a été assignée.
2. Une fenêtre donnant les paramètres d'installation des composants, décrits dans [Paramètres de modification d'une clé de licence](#), va s'ouvrir.
 3. Cliquez sur **Enregistrer** pour supprimer l'objet sélectionné.

Distribuer des licences au Serveur voisin Dr.Web

Lors de la distribution des licences disponibles au Serveur voisin Dr.Web depuis la clé de licence de ce Serveur Dr.Web, les licences distribuées ne pourront pas être utilisées sur ce Serveur Dr.Web avant la fin de leur propagation.

Pour distribuer des licences au Serveur voisin Dr.Web

1. Dans la fenêtre principale du Gestionnaire de Licences, dans l'arborescence des clés, sélectionnez la clé d'après laquelle vous souhaitez distribuer des licences disponibles à un Serveur voisin Dr.Web.
2. Cliquez sur  **Distribuer la clé aux Serveurs voisins Dr.Web** dans la barre d'outils. Une fenêtre donnant l'arborescence des Serveurs voisins Dr.Web s'ouvre.
3. Sélectionnez dans la liste les Serveurs Dr.Web auxquels vous souhaitez distribuer les licences.
4. Configurez les paramètres suivants près de chaque Serveur Dr.Web :
 - **Nombre de licences** : nombre des licences disponibles que vous souhaitez distribuer depuis cette clé à un Serveur voisin Dr.Web.
 - **Date d'expiration de la licence** : durée de validité de la transmission de licences. À la fin de cette période, toutes les licences seront rappelées du Serveur voisin Dr.Web et retourneront dans la liste des licences disponibles de cette clé de licence.
5. Cliquez sur l'un des boutons :
 - **Ajouter une clé de licence** : pour ajouter des licences à la liste des licences des Serveurs voisins Dr.Web. Une fenêtre s'ouvre contenant les paramètres d'installation des



composants, décrits dans la sous-rubrique [Paramètres pour ajouter une clé de licence à la liste de clés](#).

- **Remplacer la clé de licence** : pour supprimer les licences en cours des Serveurs voisins Dr.Web et traiter uniquement les licences distribuées. Une fenêtre s'ouvre contenant les paramètres d'installation des composants, décrits dans la sous-rubrique [Paramètres de modification d'une clé de licence](#).

Modifier les licences distribuées à un Serveur voisin Dr.Web

Pour modifier les licences distribuées à un Serveur voisin Dr.Web

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

Modifier les listes des composants installés

Paramètres de modification d'une clé de licence

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

- Mettre à jour la clé de licence.
- Remplacer la clé de licence.
- Supprimer la clé de licence.
- Distribuer des licences au Serveur voisin Dr.Web avec remplacement de clé.

Pour configurer les composants à installer lors de l'exécution de ces procédures

1. Dans la fenêtre de configuration de l'installation des composants, les objets suivants sont listés :
 - Postes, groupes et politiques avec leur liste de composants à installer.
 - Dans la colonne **Clé en cours**, vous pouvez trouver la liste des clés de l'objet et les paramètres d'installation des composants associés à l'objet.
 - Dans la colonne **Clé assignée**, vous pouvez trouver la clé et les paramètres d'installation des composants spécifiés dans la clé que vous souhaitez assigner aux objets sélectionnés.



- Si nécessaire, cochez la case **Afficher seulement si différent** pour voir dans la liste uniquement les paramètres des composants qui diffèrent dans les clés assignées et en cours.
2. Pour configurer la liste des composants installés :
- a) Dans la colonne **Clé assignée**, vous pouvez configurer la liste finale des composants à installer.
- Les paramètres d'installation des composants dans la colonne **Clé assignée** sont définis d'après l'utilisation autorisée (+) ou non autorisée (-) du composant dans les paramètres actuels et dans ceux de la clé, comme suit :

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

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

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

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

- Étendre la liste des clés de licence de l'objet.
- Distribuer des licences au Serveur voisin Dr.Web avec ajout de clé.

Pour configurer les composants à installer lors de l'exécution de ces procédures

1. Dans la fenêtre de configuration de l'installation des composants, les objets suivants sont listés :
- Postes, groupes et politiques avec leur liste de composants à installer.
 - Dans la colonne **Clé en cours**, vous pouvez trouver la liste des clés de l'objet et les paramètres d'installation des composants associés à l'objet.



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

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

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

10.1.2. Rapport sur l'utilisation des licences

Le rapport sur l'utilisation des licences contient les informations sur toutes les licences utilisées par ce Serveur Dr.Web et les Serveurs voisins Dr.Web, y compris lors du transfert de la licence par la liaison entre les serveurs.



Les rapports sont créés (et envoyés en cas de Serveurs voisins Dr.Web) conformément aux paramètres spécifiés dans la section **Configuration du Serveur Dr.Web** → **Licences**, section **Paramètres du rapport sur l'utilisation des licences**.

Pour consulter le rapport, sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique [Rapport sur l'utilisation des licences](#) dans le **menu de gestion**.



Cette section contient les informations suivantes :

- Rapport sur toutes les licences gérées par ce Serveur Dr.Web. Il y aura un rapport même si aucune liaison avec les Serveurs voisins Dr.Web n'est pas établie.
- Rapports sur les licences qui sont gérées par les Serveurs voisins Dr.Web subordonnés à ce Serveur Dr.Web, y compris ceux qui reçoivent de ce Serveur les licences par les liaisons entre les serveurs. Dans ce cas, il y aura les rapports de tous les Serveurs voisins Dr.Web de l'arborescence de liaisons entre les serveurs.

Chaque rapport représente un tableau et contient les informations sur les licences d'un seul Serveur Dr.Web — auteur du rapport.

L'en-tête du tableau contient les informations suivantes :

- **Serveur Dr.Web** : nom du Serveur Dr.Web — auteur du rapport.
- **Total de licences reçues par les liaisons** : nombre total de licences que le Serveur Dr.Web a obtenues par la liaison entre les serveurs.

Le tableau du rapport contient les données suivantes :

- **Utilisateur** : utilisateur de la clé de licence. Les informations sur les licences de la clé se trouvent dans une ligne du rapport.
- **Total de licences** : nombre total de licences fournies par cette clé de licence sur ce Serveur Dr.Web.
- **Licences disponibles** : nombre de licences disponibles et non utilisées dans cette clé.
- **Total de licences utilisées** : nombre total des licences qui ont été utilisées (délivrées aux postes ou aux Serveurs voisins Dr.Web) au moment de création du rapport.
- **Licences utilisées par les postes** : nombre de licences qui sont utilisées par les postes connectés au Serveur Dr.Web — auteur du rapport.
- **En attente** : nombre de licences dont l'auteur du rapport attend la réception. Notamment, si le Serveur Dr.Web ayant utilisé un nombre quelconque de licences (ou qu'il les a assignées à ces postes ou transmises par les liaisons entre les serveurs) a perdu une partie de ces licences. Par exemple, la clé de licence a été remplacée par une clé ayant moins de licences ou le nombre de licences reçues du Serveur Dr.Web parent a été diminué.
- **Licences réservées** : nombre de licence qui sont transmises par les liaisons entre les serveurs, mais le destinataire n'a pas encore récupéré les licences qui lui sont assignées : les Serveurs voisins Dr.Web n'ont pas été connectés pour recevoir les licences. Ces licences sont réservées dans la clé de licence et ne peuvent pas être transmises aux autres postes ou Serveurs Dr.Web.
- **Licences délivrées par les liaisons** : nombre de licences que le Serveur Dr.Web, auteur du rapport, a délivré à ses Serveurs voisins Dr.Web par les liaisons entre les serveurs.
- **Licences reçues par les liaisons** : nombre de licences que le Serveur Dr.Web, auteur du rapport, a reçu de ces Serveurs voisins Dr.Web par les liaisons entre les serveurs.
- **Date du rapport** : date de création du rapport.



Les informations supplémentaires sont disponibles pour les licences utilisées par les postes du Serveur Dr.Web, auteur du rapport. Pour les consulter, cliquez sur le nombre de licences dans la colonne **Licences utilisées par les postes** (le nombre de licences doit être supérieur à zéro). Dans le tableau **Utilisation des licences par les groupes** qui s'affiche, vous trouverez les informations suivantes :

- **Nom de groupe** : nom du groupe auquel les licences ont été diffusées.
- **Licences diffusées** : nombre total de licences diffusées au groupe de postes.
- **Postes actifs** : nombre de postes actifs dans le groupe. Les postes actifs sont les postes qui ont été en ligne durant la période indiquée dans les paramètres de génération du rapport sur le Serveur Dr.Web, titulaire de la clé de licence.

10.2. Journalisation

10.2.1. Journal en temps réel

Le journal en temps réel permet de consulter la liste des événements et des modifications liés au fonctionnement du Serveur Dr.Web, affichés tout de suite au moment de l'événement.



Le journal en temps réel affiche les informations uniquement dans le Centre de gestion et n'enregistre pas les événements dans un fichier. Le fichier [journal du Serveur Dr.Web](#) est écrit séparément, avec ses propres paramètres et il ne dépend pas du journal en temps réel et ses paramètres.

Si vous passez dans une autre section, toutes les informations affichées dans le journal en temps réel s'effacent.



Le tableau du journal contient les données suivantes :

- **N°** : numéro d'entrée. Le numéro est attribué selon l'ordre de réception des messages du Serveur Dr.Web.
- **Heure au format du journal** : l'heure d'apparition de l'événement affichée au format du journal du Serveur Dr.Web. Peut être utilisée lors de la recherche de l'événement dans le fichier journal du Serveur Dr.Web.
- **Heure** : l'heure d'apparition de l'événement affichée dans un format convivial.
- **Niveau** : niveau de journalisation selon lequel l'événement a eu lieu.
- **PID** : identificateur du processus au sein duquel l'événement a eu lieu.
- **TID** : identificateur du flux au sein duquel l'événement a eu lieu.
- **Flux** : nom du flux au sein duquel l'événement a eu lieu.
- **Sous-système** : nom du sous-système au sein duquel l'événement a eu lieu.
- **Message** : texte du message informant de l'événement survenu. Cliquez sur le message dans le tableau pour ouvrir la fenêtre contenant le texte complet du message. Si le texte représente le code HTML, cochez la case **Formater comme un texte HTML** pour l'affichage




correct des informations. Notez que si le texte du message contient JavaScript, il sera exécuté.


Pour modifier l'affichage des données dans le tableau :



- Avec l'icône  :
 - Spécifiez les paramètres d'affichage de lignes (cela concerne surtout de longues lignes).
 - Sélectionnez les colonnes à afficher dans le tableau.
- Avec l'icône  :
 - Spécifiez la ligne aléatoire pour la recherche dans toutes les sections du tableau. Seules les lignes correspondant aux résultats de recherche seront affichées dans le tableau.
 - Pour afficher seulement les niveaux particuliers, cochez les cases contre les niveaux nécessaires.
 - Pour afficher seulement les sous-systèmes particuliers, cochez les cases contre les sous-systèmes nécessaires.



Pour écrire enregistrer dans le journal les messages des niveaux et des sous-systèmes particuliers, spécifiez les [paramètres de journalisation](#).

La barre d'outils contient les éléments suivants de gestion du journal :


 **Configurer l'affichage des données** : ouvrir la fenêtre de [configuration du journal](#).

 **Vider le tableau** : effacer toutes les données affichées dans le tableau. L'opération est irréversible.


 **Arrêter la collecte des données** : arrêter l'affichage des informations sur les événements dans le tableau. Le bouton est actif, quand la collecte des données est en cours. Si vous cliquez dessus, le bouton change en bouton  **Lancer la collecte des données**.

 **Lancer la collecte des données** : commencer l'affichage des informations sur les événements dans le tableau. Le bouton est actif, quand la collecte des données est arrêtée. Si vous cliquez dessus, le bouton change en bouton  **Arrêter la collecte des données**.

Configuration de journalisation en temps réel

1. Dans le panneau de configuration, cliquez sur  **Configurer l'affichage des données**. La fenêtre **Paramètres d'affichage des données** va s'ouvrir.
2. Le champ **Nombre maximal d'entrées** limite le nombre d'entrées affichées dans le tableau de journal. Quand le nombre spécifié est atteint, les anciennes entrées sont supprimées au fur et à mesure que les nouvelles entrées sont créés.
3. Le champ **Périodicité de mises à jour, s** détermine la fréquence d'affichage de nouvelles entrées dans le journal, en secondes.
4. Le champ **Recherche par les sous-systèmes** permet de rechercher par les noms des sous-systèmes listés ci-dessous. Il peut être utilisé afin de spécifier un niveau de détail d'écriture du journal d'un sous-système en cas de grand nombre de sous-systèmes dans la liste.




5. Le tableau de sous-systèmes permet de configurer la liste des données affichées et leur niveau de détail :
 - a) Cochez les cases contre les sous-systèmes dont les événements seront affichés dans le tableau.
 - b) Sélectionnez le niveau de détails d'écriture du journal pour les sous-systèmes sélectionnés.
 - c) Pour afficher tous les sous-systèmes, cochez la case dans l'en-tête du tableau.
 - d) Pour spécifier le niveau égal de détail de la journalisation pour tous les sous-systèmes, sélectionnez une valeur dans la liste déroulante contre le sous-système **all**. Dans ce cas, seuls les messages des sous-systèmes cochés seront affichés dans le tableau.
6. Cliquez sur **Appliquer** pour commencer à s'afficher les données selon les paramètres spécifiés.
7. Cliquez sur  **Fermer** pour fermer la fenêtre sans modifier les paramètres d'affichage du journal.

10.2.2. Journal d'audit

Le journal d'audit permet de consulter la liste des événements et des modifications effectuées via les sous-systèmes de gestion de Dr.Web Enterprise Security Suite.

Pour consulter le journal d'audit

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion.
2. Dans la fenêtre qui s'ouvre, sélectionnez l'élément **Journal d'audit** du menu de gestion.
3. Le tableau contenant les événements enregistrés va s'ouvrir. Pour configurer l'affichage du journal, spécifiez une période d'actions dans la barre d'outils. Pour cela, vous pouvez sélectionner une des périodes proposées dans la liste déroulante ou spécifier les dates aléatoires dans des calendriers qui s'affichent quand vous cliquez sur les champs de dates. Cliquez sur **Actualiser** pour afficher le journal pour les dates sélectionnés.
4. Pour configurer l'affichage du tableau, cliquez sur l'icône  dans le coin droit de l'en-tête du tableau. Dans la liste déroulante, vous pouvez configurer les options suivantes :
 - Activer ou désactiver le retour à la ligne pour de longs messages.
 - Sélectionner les colonnes à afficher dans le tableau (cases cochées contre le nom). Pour activer/désactiver une colonne, cliquez sur la ligne portant son nom.
 - Choisir l'ordre des colonnes dans le tableau. Pour modifier l'ordre, glissez-déposez une colonne de la liste dans l'endroit nécessaire.
5. Le tableau du journal contient les données suivantes :
 - **Heure** : la date et l'heure de la réalisation de l'action.
 - **Statut** : le résultat de l'exécution de l'action en bref :
 - **OK** : l'opération est effectuée avec succès.



- **échoué** : une erreur est survenue lors de l'exécution de l'opération. L'opération n'est pas effectuée.
- **initié** : l'opération a été initiée. Vous allez apprendre le résultat uniquement après la fin de l'opération.
- **pas de droits** : l'administrateur qui a lancé l'opération ne possède pas des droits nécessaires pour son exécution.
- **reporté** : l'opération est reportée pour un délai déterminé ou jusqu'à un certain événement.
- **interdit** : l'exécution de l'action est bloquée. Par exemple, la suppression des groupes système.



Pour les actions échouées (la valeur **échoué** dans la colonne **Statut**), les lignes sont marquées en rouge.

- **Message / Erreur** : description détaillée de l'action effectuée ou de l'erreur survenue.
 - **Login** : le nom d'enregistrement de l'administrateur du Serveur Dr.Web. Il est indiqué si c'est l'administrateur qui a initié l'action ou que la connexion au Serveur Dr.Web s'effectue avec les identifiants de l'administrateur.
 - **Adresse** : l'adresse IP depuis laquelle l'action a été initiée. Elle est indiquée uniquement en cas de connexion externe au Serveur Dr.Web, notamment lors de la connexion via le Centre de gestion ou via Web API.
 - **Sous-système** : le nom du sous-système par lequel ou via lequel l'action a été initiée. L'enregistrement d'audit s'effectue pour les sous-systèmes suivants :
 - **Centre de gestion** : l'action a été réalisée via le Centre de gestion de la sécurité Dr.Web, notamment par l'administrateur.
 - **Web API** : l'action a été réalisée via Web API, par exemple depuis une application externe connectée avec les identifiants de l'administrateur (voir aussi les **Annexes**, p. [Annexe K. Intégration de Web API et de Dr.Web Enterprise Security Suite](#)).
 - **Serveur** : l'action a été réalisée par le Serveur Dr.Web, par exemple selon sa planification.
 - **Utilitaires** : l'action a été initiée via les utilitaires externes, notamment via l'utilitaire de diagnostic distant du Serveur Dr.Web.
6. Si nécessaire, vous pouvez exporter les données pour une période sélectionnée vers un fichier. Pour ce faire, cliquez sur un des boutons suivants dans la barre d'outils :



Sauvegarder les données dans un fichier CSV,



Sauvegarder les données dans un fichier HTML,



Sauvegarder les données dans un fichier XML,



Sauvegarder les données dans un fichier PDF.



10.2.3. Journal du Serveur Dr.Web

Le Serveur Dr.Web effectue la journalisation des événements relatifs à son fonctionnement.



Le journal du Serveur Dr.Web est utilisé pour le débogage et pour la détection des problèmes en cas de dysfonctionnement des composants du réseau antivirus.

Par défaut, le fichier de journal a le nom `drwcsd.log` et se place dans :

- Sous **UNIX** :
 - sous Linux : `/var/opt/drwcs/log/drwcsd.log` ;
 - sous FreeBSD : `/var/drwcs/log/drwcsd.log`.
- Sous **Windows** : dans le sous-répertoire `var` du répertoire d'installation du Serveur Dr.Web.

Le fichier est au format texte simple (voir le document **Annexes**, [Annexe J. Format des fichiers de journal](#)).

Pour consulter le journal du Serveur Dr.Web via le Centre de gestion :

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion.
2. Dans la fenêtre qui s'ouvre, sélectionnez l'élément **Journal du Serveur Dr.Web** du menu de gestion.
3. Une fenêtre affichant la liste des journaux du Serveur Dr.Web va s'ouvrir. Le format suivant des noms des fichiers de journal du Serveur Dr.Web est utilisé en fonction des paramètres du mode de rotation : `<file_name> . <N> . log` ou `<file_name> . <N> . log . gz`, où `<N>` est un numéro d'ordre : 1, 2, etc. Par exemple, si le nom du fichier de journal est `drwcsd`, la liste des fichiers de journal est la suivante :
 - `drwcsd.log` — fichier de journal actuel (dans lequel s'effectue l'écriture),
 - `drwcsd.1.log.gz` — précédent,
 - `drwcsd.2.log.gz` et ainsi de suite — plus le nombre est élevé, plus la version est ancienne.
4. Pour gérer les fichiers du journal, cochez la case contre un fichier ou plusieurs fichiers nécessaires. Pour sélectionner tous les fichiers de journal, cochez la case dans l'en-tête du tableau. Dans la barre d'outils, les boutons suivants seront disponibles :



Exporter les fichiers de journal sélectionnés : sauvegarder la copie locale des fichiers de journal sélectionnés. La sauvegarde des copies de journal peut être utilisée, par exemple, pour consulter le contenu du fichier de journal depuis l'ordinateur distant.



Supprimer les fichiers de journal sélectionnés : pour supprimer les fichiers de journal sélectionnés sans possibilité de restauration.



Pour modifier le mode de tenue du journal du Serveur Dr.Web via le Centre de gestion, utilisez la section [Journal](#).



Gestion du niveau de détail du journal

En fonction des paramètres spécifiés, le journal du Serveur Dr.Web peut avoir un niveau de détails différent. L'activation du niveau plus détaillé pour une source particulière ou pour toutes les sources peut aider en cas de débogage et résolution de problème et peut être nécessaire en cas d'appel au support technique. Il existe plusieurs façons de configurer ce paramètre :

- Via le Centre de gestion dans la section **Administration** → **Configuration du Serveur Dr.Web** → **Journal**. Vous pouvez spécifier le niveau de détails de messages du journal pour toutes les sources possibles.
- Via la clé `-verbosity` lors du lancement du Serveur Dr.Web depuis la ligne de commande. Cette façon est plus flexible et permet de spécifier le niveau de détails pour une ou plusieurs sources séparées. Le format d'indication de la clé est décrit dans le document **Annexes**, [G3.8. Description des clés](#).
- A l'aide du fichier de configuration `logging.conf`. Pour cela, il est nécessaire de créer un fichier portant ce nom dans le répertoire `etc` dans le répertoire d'installation du Serveur Dr.Web. Ensuite il faut indiquer dans le fichier les sources de messages et les niveaux de détails au format `<sources_de_messages> : <niveau>`. La clé au format `-verbosity=all:all` est équivalent à la clé `-verbosity=all`. Les niveaux de détails spécifiés via `logging.conf` ont une priorité devant les niveaux spécifiés d'autres façons.

Exemple du contenu de fichier `logging.conf` :

```
Alert:all, Server:err, SQLite3:inf
```

A part la virgule vous pouvez utiliser en tant que séparateur tout symbole d'espace, y compris l'espace, la tabulation, le saut de ligne, etc. Vous pouvez préciser la liste de sources de messages directement dans le fichier de journal du Serveur Dr.Web ou via le Centre de gestion, en exécutant la commande `drwcs.log_subsystems()` dans la section **Administration** → **Console Lua**. Les niveaux de détails possibles sont mentionnés dans le document **Annexes**, [Annexe J. Format de fichiers du journal](#).



Les niveaux de détail spécifiés de telle façon sont hérités par les sous-systèmes. C'est-à-dire, si vous spécifiez en même temps les paramètres `Socket/Client:inf` et `Socket:all`, le sous-système `Socket/Client` en suivant les indications au niveau de parent enregistrera dans le journal toutes les informations sur tous les événements et non seulement les messages à caractère informatif.

- Pour les Serveurs Dr.Web fonctionnant sous les OS de la famille UNIX - à l'aide d'une clé spéciale dans le fichier de configuration `local.conf`. L'ordre de gestion de ce fichier est décrit ci-dessous.



Configuration du journal de fonctionnement sous UNIX

Sur les Serveurs Dr.Web tournant sous les OS de la famille UNIX, il existe une possibilité d'écrire le journal de fonctionnement du Serveur Dr.Web via un fichier de configuration spécifique :

- sous Linux : `/var/opt/drwcs/etc/local.conf` ;
- sous FreeBSD : `/var/drwcs/etc/local.conf`.

Contenu du fichier `local.conf` :

```
# Log level.  
  
DRWCS_LEV=info  
  
# Log rotation.  
  
DRWCS_ROT=10z,10m
```

Les valeurs des paramètres correspondent aux valeurs des clés de la ligne de commande pour le lancement du Serveur Dr.Web :

- `-verbosity=<niveau_de_détail>` : niveau de détail du journal du Serveur Dr.Web.
- `-rotate=<N><f>, <M><u>` : mode de rotation du journal de fonctionnement du Serveur Dr.Web.

Vous trouverez la description détaillée des clés dans le document **Annexes**, rubrique [G3.8. Description des clés](#).



Si le fichier `local.conf` a été édité lors du fonctionnement du Serveur Dr.Web, il faut redémarrer le Serveur Dr.Web pour que les modifications apportées aux paramètres d'écriture du journal entrent en vigueur. Le redémarrage doit être lancé par des moyens du système d'exploitation.

Les copies de sauvegarde du fichier `local.conf` sont créées lors de la mise à jour et la suppression du Serveur Dr.Web. Cela permet de gérer le niveau d'écriture du journal lors de la mise à jour de paquets du Serveur Dr.Web.


10.2.4. Journal des mises à jour du référentiel

Journal des mises à jour du référentiel : cet élément contient la liste de mises à jour depuis le SGM et les informations détaillées sur les révisions mises à jour de produits.

Pour consulter le journal des mises à jour du référentiel

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion.
2. Dans la fenêtre qui s'ouvre, sélectionnez l'élément **Journal des mises à jour du référentiel**.



3. Le tableau contenant les événements enregistrés va s'ouvrir. Pour configurer l'affichage du journal, spécifiez une période d'actions dans la barre d'outils. Pour cela, vous pouvez sélectionner une des périodes proposées dans la liste déroulante ou spécifier les dates aléatoires dans des calendriers qui s'affichent quand vous cliquez sur les champs de dates. Cliquez sur **Actualiser** pour afficher le journal pour les dates sélectionnés.
4. Pour afficher dans le tableau les événement d'un type particulier, cliquez sur l'icône  dans la barre d'outils. Dans la liste déroulante, vous pouvez sélectionner les paramètres de filtrage nécessaires :
 - **Nom du produit** : tous les événements liés aux produits sélectionnés dans la liste seront affichés dans le tableau du journal.
 - **Résultat de la mise à jour** : toutes les séances de mise à jour et leurs résultats seront affichés dans le tableau du journal. Vous pouvez filtrer les séances par les résultats suivants :
 - **Le produit requis est introuvable sur les serveurs du SGM ;**
 - **La clé de licence est introuvable sur les serveurs du SGM ;**
 - **Mise à jour désactivée ;**
 - **Mise à jour terminée avec succès.**
 - **Initiateur** : les séances de mises à jour initiées par les systèmes suivants seront affichées dans le tableau du journal :
 - **Lancée depuis la ligne de commande** : la mise à jour est initiée par l'administrateur avec la commande correspondante de console.
 - **Lancée par le Planificateur de tâches** : la mise à jour est lancée selon la tâche de la [planification du Serveur Dr.Web](#).
 - **Mise à jour entre serveurs** : la mise à jour a été obtenue via la liaison entre serveurs depuis le Serveur Dr.Web principal. Cet initiateur est présent uniquement en cas de [configuration multi-serveurs](#) du réseau antivirus avec la diffusion des mises à jour par les liaisons entre serveurs.
 - **Lancée depuis le Centre de gestion** : la mise à jour est lancé par l'administrateur via le Centre de gestion de la sécurité Dr.Web, dans la rubrique [Statut du référentiel](#).
 - **Importation du référentiel** : la mise à jour a été téléchargée par l'administrateur via la rubrique [Contenu du référentiel](#) du Centre de gestion.
5. Le tableau du journal contient les données suivantes :
 - **Administrateur** : nom d'enregistrement de l'administrateur du Serveur Dr.Web. Il est indiqué si c'est l'administrateur qui a initié l'action.
 - **Adresse réseau** : l'adresse IP depuis laquelle l'action a été initiée. Elle est indiquée uniquement en cas de connexion externe au Serveur Dr.Web, notamment lors de la connexion via le Centre de gestion ou via Web API.
 - **Initiateur** : système qui a initié le processus de la mise à jour.
 - **Répertoire dans le référentiel** : nom du répertoire du référentiel du Serveur Dr.Web qui a été modifié selon le processus de la mise à jour.



- **Nom du produit** : nom du produit du référentiel qui a été téléchargé ou dont le téléchargement a été sollicité.
- **Début** : date et heure du début du téléchargement des mises à jour depuis le SGM pour un produit concret.
- **Fin** : date et heure de la fin du téléchargement des mises à jour depuis le SGM pour un produit concret.
- **Résultat de la mise à jour** : résultat de la mise à jour du référentiel. Vous pouvez consulter une brève information sur la fin réussie de la mise à jour ou sur la raison de l'erreur.



Pour les actions échouées, les cases **Code de terminaison** sont marquées en rouge.

- **Révision initiale** : numéro de la révision (les révisions sont numérotées selon la date de leur création) qui était la dernière pour ce produit avant le début de la mise à jour.
 - **Révision reçue** : numéro de la révision (les révisions sont numérotées selon la date de leur création) qui était téléchargée lors de la mise à jour.
 - **Fichiers mis à jour** : brève information sur les fichiers mis à jour au format suivant : *<nombre des fichiers> – <action sur les fichiers>*.
6. Si nécessaire, vous pouvez exporter les données pour une période sélectionnée vers un fichier. Pour ce faire, cliquez sur un des boutons suivants dans la barre d'outils :



Sauvegarder les données dans un fichier CSV,



Sauvegarder les données dans un fichier HTML,



Sauvegarder les données dans un fichier XML,



Sauvegarder les données dans un fichier PDF.

10.2.5. Journal de messages

Le journal des messages contient tous les messages qui ont été envoyés par l'administrateur sur les postes du réseau antivirus. (voir [Envoi de messages aux postes](#)).


Le journal des messages envoyés contient les informations suivantes :


- **Date de l'envoi.**
- **Expéditeur** : login de l'administrateur authentifié dans le Centre de gestion lors de l'envoi du message.
- **Statut** : nombre des messages envoyés par l'administrateur et nombre des messages délivrés sur les postes. Si le nombre des messages envoyés et délivrés correspondent, les informations sur les messages sont marquées par la couleur grise.
- **Message** : texte du message envoyé. Les informations sur les autres paramètres configurés lors de l'envoi s'affichent en supplément.



Quand vous cliquez sur un message particulier dans le tableau, une fenêtre s'affiche contenant les détails de l'envoi : liste de tous les destinataires et date de délivrance du message si l'opération a réussi ou message **N'est pas délivré** si l'opération a échoué.


Pour gérer le journal de messages, utilisez les options suivantes dans la barre d'outils :

 **Envoyer les messages sélectionnés encore une fois** : l'opération est disponible si vous sélectionnez un ou plusieurs messages envoyés dans le journal (voir les procédures ci-dessous).


 **Enregistrer le message sélectionné en tant que modèle** : créer un modèle à partir du message sélectionné pour pouvoir l'utiliser plus tard. L'option est disponible si vous sélectionnez un message dans le journal. Vous pouvez gérer les modèles enregistrés dans la section [Modèles de messages](#).

Dans la liste déroulante sélectionnez la période pendant laquelle les messages à afficher ont été envoyés. Vous pouvez sélectionner la même période dans les champs de dates qui sont spécifiés via le calendrier déroulant. Pour appliquer la période sélectionnée, cliquez sur **Actualiser**.

Pour envoyer encore un message

1. Cochez la case contre le message à envoyer.
2. Cliquez sur le bouton  **Envoyer les messages sélectionnés encore une fois**.
3. La fenêtre **Envoi du message** s'ouvre. Spécifiez les paramètres suivants :
 - a) Dans l'arborescence **Réseau antivirus**, seront sélectionnés les postes sur lesquels ce message a été envoyé. Vous pouvez utiliser les anciens destinataires ou sélectionner les utilisateurs aléatoires de la liste : cela peut être les postes ou les groupes de postes.
 - b) Les paramètres du messages sont équivalents aux paramètres de la section [Envoi de messages aux postes](#).
4. Cliquez sur **Envoyer**.

Pour envoyer encore quelques messages

1. Cochez les cases contre les messages à envoyer.
2. Cliquez sur le bouton  **Envoyer les messages sélectionnés encore une fois**.
3. La fenêtre **Envoi de plusieurs messages** s'ouvre. Dans la section **Liste des messages**, vous trouverez tous les messages qui ont été sélectionnés pour être envoyés encore une fois. Les noms de messages correspondent aux dates de leur envoi précédent sur les postes.
4. Cliquez sur **Envoyer tout** pour envoyer tous les messages de la liste.
5. Pour modifier un message, sélectionnez-le dans la section **Liste des messages**. Dans la section **Paramètres du message**, spécifiez les paramètres suivants :
 - a) Dans l'arborescence **Réseau antivirus**, seront sélectionnés les postes sur lesquels ce message a été envoyé. Vous pouvez utiliser les anciens destinataires ou sélectionner les utilisateurs aléatoires de la liste : cela peut être les postes ou les groupes de postes.



- b) Les paramètres du messages sont équivalents aux paramètres de la section [Envoi de messages aux postes](#).
- c) Pour supprimer le message sélectionnés de la liste, cliquez sur le bouton **Supprimer**.

10.3. Configuration du Serveur Dr.Web



A chaque enregistrement des modifications de la section **Configuration du Serveur Dr.Web**, une copie de sauvegarde de la version précédente du fichier de configuration du Serveur Dr.Web est automatiquement enregistrée. 10 dernières copies sont sauvegardées.

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

`drwcsd.conf_<date_et_heure_de_création>`

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

Pour configurer les paramètres du Serveur Dr.Web

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion.
2. Dans la fenêtre qui s'affiche, sélectionnez l'élément **Configuration du Serveur Dr.Web** du menu de gestion. Une fenêtre permettant de configurer le Serveur Dr.Web va s'ouvrir.



Les valeurs des champs marqués par le symbole * doivent être obligatoirement spécifiées.

3. Les boutons suivants de gestion des paramètres sont disponibles dans la barre d'outils :
 - Redémarrer le Serveur Dr.Web** : redémarrer le Serveur Dr.Web pour appliquer les modifications apportées dans cette rubrique. Le bouton est activé après la modification des paramètres de la rubrique et l'appui sur le bouton **Enregistrer**.
 - Restaurer la configuration de la copie de sauvegarde** : liste déroulante contenant les copies de sauvegarde des paramètres de la rubrique entière que l'on peut restaurer après les modifications apportées. Le bouton est activé après la modification des paramètres de la rubrique et l'appui sur le bouton **Sauvegarder**.
 - Restaurer tous les paramètres à leur valeur initiale** : restaurer les valeurs données à tous les paramètres de cette rubrique avant modification (dernières valeurs sauvegardées).
 - Restaurer tous les paramètres à leur valeur par défaut** : restaurer les valeurs par défaut de tous les paramètres de la rubrique.
4. Pour appliquer les paramètres apportées dans les paramètres de la rubrique, cliquez sur **Sauvegarder**. Ensuite, le redémarrage du Serveur Dr.Web est requis. Pour ce faire, cliquez sur le bouton **Redémarrer le Serveur Dr.Web** dans la barre d'outils de cette rubrique.



10.3.1. Général

Dans l'onglet **Général**, vous pouvez configurer les paramètres suivants du Serveur Dr.Web :

- **Nom du Serveur** : nom de ce Serveur Dr.Web. Si aucun nom n'est spécifié, le nom du poste sur lequel est installé le Serveur Dr.Web est utilisé.
- **Langue du Serveur Dr.Web** : langue utilisée par défaut par les composants et les systèmes du Serveur Dr.Web, si les paramètres de langue n'ont pas été reçus de la base de données du Serveur Dr.Web. Notamment, elle est utilisée pour le Centre de gestion de la sécurité Dr.Web et le système de notifications de l'administrateur si la base de données a été endommagée et qu'il est impossible d'obtenir les paramètres de la langue.



Si vous sélectionnez une langue et que les textes d'interface écrits dans cette langue ne sont pas mis à jour en ce moment, vous serez invité à activer la mise à jour pour cette langue. Pour cela, accédez à **Administration** → **Configuration générale du référentiel** → **Serveur Dr.Web** → **Langues du Centre de gestion de la sécurité Dr.Web**, cochez la case contre la langue nécessaire et cliquez sur **Enregistrer**. Lors de la prochaine mise à jour, les textes d'interface pour la langue sélectionnée seront mis à jour. Vous pouvez également lancer manuellement la mise à jour dans la section **Statut du référentiel**.

- **Nombre de requêtes parallèles des clients** : nombre de flux de traitement des données reçues des clients : Agents Dr.Web, installeurs des Agents, Serveurs voisins Dr.Web, Serveurs proxy Dr.Web. Ce paramètre influence les performances du Serveur Dr.Web. Si vous utilisez la base de données embarquée, il n'est pas recommandé de modifier la valeur par défaut. Si vous utilisez la base de données externe, une valeur supérieure peut être requise (voir **Annexes**, rubrique [Charge sur le Serveur Dr.Web et paramètres de configuration recommandés](#)). Si vous gérez un réseau avec un grand nombre de connexions des clients au Serveur Dr.Web, il est recommandé de consulter le support technique de la société Doctor Web avant de modifier le paramètre.



A partir de la version 10, la modification du paramètre **File d'attente pour l'authentification** via le Centre de gestion n'est plus disponible.

Par défaut, la valeur de ce paramètre spécifiée lors de l'installation du nouveau Serveur Dr.Web est de 50. En cas de la mise à niveau de la version antérieure avec la sauvegarde du fichier de configuration, la valeur de la file d'attente pour l'authentification est sauvegardée de la configuration de la version antérieure.

S'il est nécessaire de modifier la longueur de la file d'attente pour l'authentification éditez la valeur du paramètre suivant dans le fichier de configuration du Serveur Dr.Web :

```
<!-- Maximum authorization queue length -->  
<maximum-authorization-queue size='50' />
```

- Dans la liste déroulante **Mode d'enregistrement des novices**, sélectionnez le mode d'enregistrement des nouveaux postes (voir [Politique d'approbation des postes](#)).



- La liste déroulante **Groupe primaire par défaut**, détermine le groupe primaire dans lequel les postes seront placés lorsque l'accès des postes au Serveur Dr.Web est autorisé automatiquement.
- Cochez la case **Redéfinir les non approuvés comme novices** pour réinitialiser les paramètres d'accès au Serveur Dr.Web pour les postes qui n'ont pas correctement passé l'authentification. Cette option peut être utile si vous modifiez les paramètres du Serveur Dr.Web (comme la clé de chiffrement publique) ou que vous modifiez la BD. Dans ces cas, les postes ne seront pas en mesure de se connecter et auront besoin des nouveaux paramètres pour accéder au Serveur Dr.Web.
- Cochez la case **Créer des comptes de postes automatiquement** pour créer automatiquement les comptes de postes manquants dans le Centre de gestion, lors de l'installation des Agents Dr.Web depuis le package d'installation de groupe. Si la case est décochée, l'installation est possible seulement par le nombre de comptes déjà créés dans le groupe dont le package d'installation est lancé.
- Dans le champ **Différence autorisée entre l'heure du Serveur Dr.Web et celle de l'Agent**, indiquez la différence autorisée entre l'heure système sur le Serveur Dr.Web et celle des Agents Dr.Web en minutes. Si la différence est supérieure à la valeur indiquée, ce sera noté dans le statut du poste sur le Serveur Dr.Web. 3 minutes sont autorisées par défaut. La valeur 0 indique que la vérification est désactivée.
- Cochez la case **Remplacer les adresses IP** pour remplacer les adresses IP par les noms DNS dans le fichier de journal du Serveur Dr.Web.
- Dans la liste **Nom du poste**, vous pouvez spécifier le format d'affichage des noms de postes dans le répertoire du réseau antivirus du Centre de gestion.
- Grâce à la liste **Remplacer le nom du poste**, vous pouvez, si nécessaire, remplacer les noms affichés des postes par le nom de domaine complet ou partiellement qualifié (s'il est impossible de déterminer les noms DNS, les adresse IP s'affichent) .



La case **Remplacer les adresses IP** est décochée par défaut et les noms ne sont pas remplacés. En cas de paramétrage incorrect du service DNS, l'activation de ces fonctions peut ralentir considérablement le Serveur Dr.Web. En cas d'activation d'un de ces deux modes, il est recommandé d'autoriser la mise en cache des noms sur le serveur DNS.



Si une des options est sélectionné dans la liste **Remplacer le nom du poste** et que le Serveur proxy Dr.Web est utilisé dans le réseau antivirus, le nom de l'ordinateur sur lequel le Serveur proxy Dr.Web est installé sera affiché en tant que nom du poste dans le Centre de gestion pour tous les postes connectés au Serveur Dr.Web via le Serveur proxy Dr.Web.

- Cochez la case **Synchroniser les descriptions des postes** pour synchroniser la description de l'ordinateur de l'utilisateur (champ **Description** sur la page **Propriétés système**) avec celle du poste dans le Centre de gestion. Si la description du poste n'est pas présent dans le Centre de gestion, c'est la description de l'ordinateur du côté de l'utilisateur qui sera inscrite dans ce champ. Si les descriptions sont différentes, les données du Centre de gestion seront remplacées par les données utilisateur.



- Cochez la case **Synchroniser la géolocalisation** pour permettre la synchronisation de la géolocalisation des postes entre les Serveurs Dr.Web dans le réseau antivirus multi-serveurs. Si la case est cochée, vous pouvez configurer le paramètre suivant :
 - **Synchronisation au démarrage** : nombre de postes sans coordonnées géographiques, les informations sur lesquels sont requis lors de l'établissement d'une connexion entre les Serveurs Dr.Web.
- Cochez la case **Utiliser les politiques** pour autoriser à utiliser les politiques pour la configuration des postes protégés (voir [Politiques](#)).
 - **Nombre des versions de la politique** : nombre maximum des versions que l'on peut créer pour chaque politique.
- Dans le champ **Nombre maximal des copies de sauvegarde du Serveur Dr.Web**, spécifiez le nombre maximal des copies de sauvegarde, créés lors du passage à la nouvelle révision du Serveur Dr.Web via le Centre de gestion (voir la section [Mise à jour du Serveur Dr.Web et restauration depuis une copie de sauvegarde](#)). La valeur 0 prescrit de garder toutes les copies de sauvegarde.
- Cochez la case **Utiliser l'extension du protocole de l'Agent pour transmettre les données de fichiers** pour autoriser le transfert des données de fichiers par le protocole SFTP de l'Agent Dr.Web au Serveur Dr.Web. Si la case est décochée, les données ne sont pas transmises.
- Dans le champ **Nombre de machines virtuelles Lua** spécifiez le nombre maximal des machines virtuelles Lua préchargées pour les besoins du serveur web.
- Dans le champ **Script pour la création d'une machine virtuelle Lua**, entrez le script exécuté lors de la création en tâche de fond d'une machine virtuelle Lua pour les besoins du serveur Web.

10.3.2. Trafic

10.3.2.1. Mises à jour

Dans l'onglet **Mises à jour** sont spécifiées les limitations du volume de trafic lors de la transmission des mises à jour entre le Serveur Dr.Web et les Agents Dr.Web.

Pour en savoir plus, voir [Limitation du trafic des postes de travail](#).



Pour spécifier les limitations du trafic des mises à jour des Agents Dr.Web

1. Dans le champ **Nombre de processus d'installation simultanés**, spécifiez le nombre maximum des sessions de distribution des mises à jour lancées en même temps depuis ce Serveur Dr.Web. Si le nombre maximum est atteint, les requêtes des Agents Dr.Web sont placées dans une file d'attente. La taille de la file d'attente n'est pas limitée. Spécifiez la valeur **0** pour enlever les limitation du nombre des processus simultanés.
2. Cochez la case **Limiter le trafic des mises à jour** pour limiter l'utilisation de la bande passante lors de la transmission des mises à jour du Serveur Dr.Web aux Agents Dr.Web.



Si la case est décochée, les mises à jour des Agents Dr.Web seront transmises sans aucune limitation de la bande passante.

3. Si la case est cochée, dans le champ **Vitesse maximale du transfert (Ko/s)**, indiquez la vitesse maximale du transfert des mises à jour. Les mises à jour seront transmises par tranches de bande passante allouée au trafic réseau total relatif aux mises à jour de tous les Agents Dr.Web.

Il est possible de spécifier cinq limitations de la vitesse de transmission de données pour le transfert des mises à jour au maximum. Pour ajouter encore un champ de limitation de vitesse cliquez sur le bouton . Pour supprimer une limitation de vitesse, cliquez sur  contre la limitation qu'il faut supprimer.

4. Dans le tableau de planification, les limitations sont définies séparément pour chaque 30 minutes de chaque jour de la semaine.

Pour modifier le mode de limitation de transmission de données, cliquez sur le bloc correspondant dans le tableau. La sélection de plusieurs blocs temporaires à l'aide du principe glisser-déposer est aussi prise en charge.

La couleur des cases varient cycliquement conformément au schéma en couleurs présentés au dessous du tableaux à commencer par la variante qui marque l'autorisation de transmettre des mises à jour sans aucune limitation de trafic jusqu'à la variante qui marque l'interdiction de transmettre des mises à jour.

5. Après avoir apporté les modifications, cliquez sur **Sauvegarder** pour les appliquer.

10.3.2.2. Installations

Dans l'onglet **Installations** sont spécifiées les limitations du volume de trafic lors du transfert de données pendant l'installation des Agents Dr.Web sur les postes.

Pour en savoir plus, voir [Limitation du trafic des postes de travail](#).

Pour spécifier les limitations du trafic lors de l'installation des Agents Dr.Web

1. Dans le champ **Nombre de processus d'installation simultanés**, spécifiez le nombre maximum des sessions d'installation de l'Agent Dr.Web lancées en même temps depuis ce Serveur Dr.Web. Si le nombre maximum est atteint, les requêtes des Agents Dr.Web sont placées dans une file d'attente. La taille de la file d'attente n'est pas limitée. Spécifiez la valeur **0** pour enlever les limitation du nombre des processus simultanés.
2. Cochez la case **Limiter le trafic lors de l'installation des Agents** pour limiter le volume du trafic réseau lors du transfert de données du Serveur Dr.Web aux postes pendant l'installation des Agents Dr.Web.

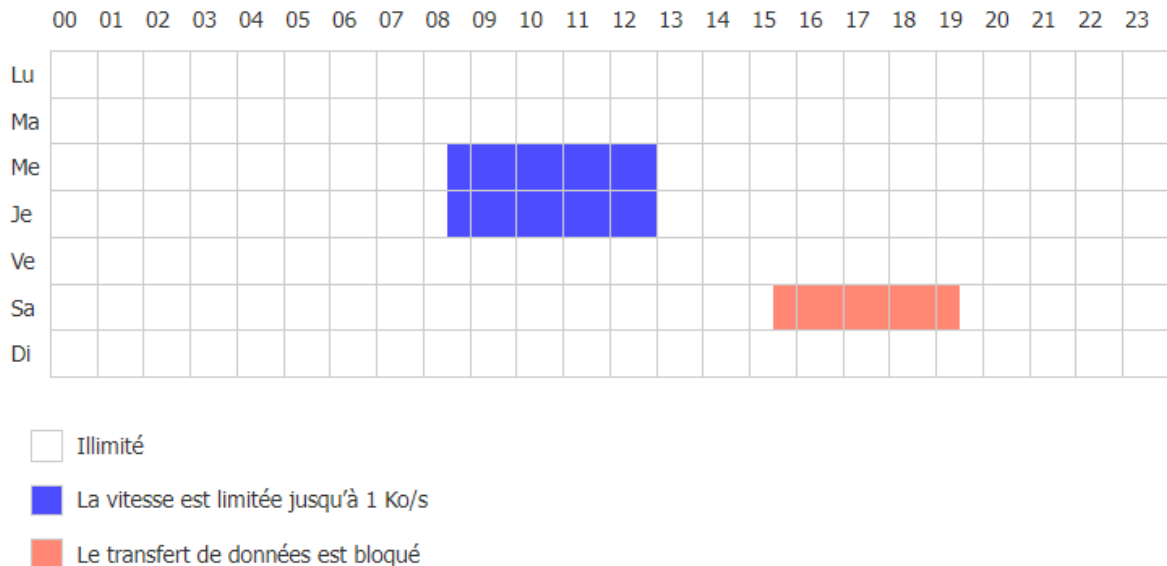
Si la case n'est pas cochée, les données seront transmises lors de l'installation des Agents sans aucune limitation de la bande passante.

3. Si la case est cochée, dans le champ **Vitesse maximale du transfert (Ko/s)**, indiquez la vitesse maximale du transfert des données. Dans ce cas, les données de l'installation des Agents Dr.Web seront transmises par tranches de bande passante allouée au trafic réseau total de tous les Agents Dr.Web.



Il est possible de spécifier cinq limitations de la vitesse de transmission de données pour l'installation des Agents Dr.Web au maximum. Pour ajouter encore un champ de limitation de vitesse cliquez sur le bouton **+**. Pour supprimer une limitation de vitesse, cliquez sur **-** contre la limitation qu'il faut supprimer.

4. Dans le tableau de planification, les limitations sont définies séparément pour chaque 30 minutes de chaque jour de la semaine.



Pour modifier le mode de limitation de transmission de données, cliquez sur le bloc correspondant dans le tableau. La sélection de plusieurs blocs temporaires à l'aide du principe glisser-déposer est aussi prise en charge.

La couleur des cases varie cycliquement conformément au schéma en couleurs présentés au dessous du tableaux à commencer par la variante qui marque l'autorisation de transmettre des données sans aucune limitation de trafic jusqu'à la variante qui marque l'interdiction de transmettre des données.

5. Après avoir apporté les modifications, cliquez sur **Sauvegarder** pour les appliquer.

10.3.2.3. Limitation du trafic des postes de travail

Dans le réseau antivirus Dr.Web Enterprise Security Suite, vous pouvez limiter la vitesse de transfert de données entre le Serveur Dr.Web et les Agents Dr.Web. Les paramètres comportent les limitations de transfert des mises à jour et les limitations de transfert des données en cas d'installations de l'Agent Dr.Web.

Les options suivantes de limitation du trafic sont disponibles :

1. Limiter la vitesse commune de transfert de données pour tous les postes.

Vous pouvez configurer cette option dans la section de configuration du Serveur Dr.Web : l'élément **Administration** du menu principal du Centre de gestion → l'élément **Configuration du Serveur Dr.Web** du menu de gestion → l'onglet **Trafic** → l'onglet



intérieur **Mises à jour** ou **Installations** → le paramètre **Limiter le trafic des mises à jour** ou **Limiter le trafic lors de l'installation des Agents**.

2. Limiter de manière personnalisée la vitesse de transfert de données sur les postes particuliers ou les groupes de postes.

Vous pouvez configurer cette option dans la section de configuration des postes : l'élément **Réseau antivirus** du menu principal → sélectionnez le poste ou le groupe de postes dans l'arborescence → l'élément **Restrictions de mises à jour** du menu de gestion → le paramètre **Limiter le trafic des mises à jour**.

Le trafic est limité selon le principe suivant :

1. Si la limitation est activée pour la vitesse commune de transfert des données dans les paramètres du Serveur Dr.Web, la vitesse sommaire de transfert des données du Serveur Dr.Web vers tous les postes n'excèdera pas la valeur indiquée. Ainsi :
 - a) Quelle que soit la différence de largeur des bandes passantes entre le Serveur Dr.Web et les postes, la vitesse de transfert est répartie à parts égales entre tous les postes.
 - b) Si la largeur de bande passante entre le Serveur Dr.Web et un poste est inférieure à la valeur moyenne octroyée à un poste, calculée d'après le point a), le trafic de transfert des données pour ce poste est limité à la largeur de bande passante maximum pour le canal vers ce poste. La valeur restante de la limitation est partagée de manière identique au point a), et pour tous les autres postes.
2. Si une limitation personnalisée est définie pour la vitesse de transfert des données pour un poste en particulier ou pour un groupe de postes, la vitesse de transfert des données pour ce groupe ou ce poste n'excèdera pas la valeur indiquée. Cette limitation n'affecte pas les autres postes et les données sont transférées vers eux à la vitesse maximum.
3. Si la limitation de vitesse commune pour le transfert des données est activée dans les paramètres du Serveur Dr.Web, ainsi que la limitation personnalisée pour un groupe ou un poste en particulier, dans ce cas :
 - a) La vitesse de transfert des données vers les groupes et postes ayant une limitation personnalisée n'excèdera pas la valeur spécifiée dans leurs paramètres.
 - b) La vitesse de transfert des données vers le reste des postes est calculé comme suit : la limitation commune de la vitesse de transfert des données, après la soustraction des limitations définies au point a), est égale pour tous les autres postes.
 - c) Si la largeur de bande passante entre le Serveur Dr.Web et un poste, qui ne possède pas de limite personnalisée, est inférieure à la largeur moyenne obtenue conformément au point b), le trafic, pour ce poste, est limité à la largeur de bande passante maximum pour le canal vers ce poste. La valeur restante de la limitation est répartie de manière identique au point b), à parts égales entre les autres postes qui n'ont pas de limitation personnalisée.



10.3.3. Réseau

10.3.3.1. DNS

Dans l'onglet **DNS**, vous pouvez configurer les paramètres suivants d'utilisation du serveur DNS :

- **Délai des requêtes DNS (s)** : délai, en secondes, pour répondre aux requêtes DNS directes/inverses. Indiquez la valeur 0 pour désactiver la restriction sur le temps d'attente de la résolution de la requête DNS.
- **Nombre de requêtes DNS répétées** : nombre maximum de requêtes DNS répétées en cas d'échec durant la résolution de la requête DNS.
- Cochez la case **Indiquer la durée de stockage des réponses du serveur DNS** pour indiquer la durée de stockage des réponses du serveur DNS dans le cache (TTL).
 - **Pour les réponses positives (min)** : la durée de stockage dans le cache (TTL) des réponses positives du serveur DNS en minutes.
 - **Pour les réponses négatives (min)** : la durée de stockage dans le cache (TTL) des réponses négatives du serveur DNS en minutes.
- **Adresse du serveur DNS-over-HTTPS** : adresse du serveur DNS-over-HTTPS compatible.



Pour un fonctionnement correct, il faut indiquer la valeur **Tous** dans la section **Administration** → **Configuration générale du référentiel** → **SGM Dr.Web** → **Certificats autorisés**.

- **Serveurs DNS** : liste des serveurs DNS qui remplace la liste système utilisée par défaut.
- **Suffixes DNS** : liste des suffixes DNS qui remplace la liste système utilisée par défaut.

10.3.3.2. Proxy

Dans l'onglet **Proxy**, vous pouvez configurer les paramètres du serveur proxy.

Cochez la case **Utiliser le serveur proxy** pour paramétrer les connexions avec le Serveur Dr.Web via le serveur proxy. Les paramètres suivants sont disponibles :

- **Serveur proxy** : adresse IP ou nom DNS du serveur proxy. Si cela est nécessaire, il est possible de spécifier le port au format `<adresse>:<port>` dans la ligne d'adresse. Par défaut, le port 3128 est utilisé.
- Pour utiliser l'authentification pour l'accès au serveur proxy, selon les méthodes choisies, cochez la case **Utiliser l'authentification** et indiquez les paramètres suivants :
 - Remplissez les champs **Utilisateur du serveur proxy** et **Mot de passe de l'utilisateur du serveur proxy**.
 - Choisissez une des méthodes d'authentification suivantes :



Option	Description	
Toute méthode supportée	Utilisez n'importe quelle méthode d'authentification supportée par le serveur proxy. Si le serveur proxy supporte plusieurs méthodes, la méthode la plus fiable est utilisée.	
Toute méthode sécurisée supportée	Utilisez n'importe quelle méthode d'authentification sécurisée supportée par le serveur proxy. Dans ce mode, la méthode d'authentification Standard n'est pas supportée. Si le serveur proxy supporte plusieurs méthodes d'authentification, la plus sûre est utilisée.	
Les méthodes suivantes :	Authentification Basic	Utiliser l'authentification Basic. Il n'est pas recommandé d'utiliser cette méthode car le transfert des données d'authentification n'est pas crypté.
	Authentification Digest	Utiliser l'authentification Digest. Méthode d'authentification cryptographique.
	Authentification Digest avec le support d'IE	Utiliser l'authentification Digest. La méthode d'authentification est basée sur la cryptographie. Active le support du navigateur Internet Explorer en version 6 ou antérieure.
	Authentification NTLM	Utiliser l'authentification NTLM. Méthode d'authentification cryptographique. Le protocole NTLM de Microsoft est utilisé pour l'authentification.
	Authentification NTLM via winbind	Utiliser l'authentification NTLM via l'application externe winbind. Méthode cryptographique d'authentification.
	Authentification GSS-Negotiate	Utiliser l'authentification GSS-Negotiate. Méthode d'authentification cryptographique.

10.3.3.3. Transport

L'onglet **Transport** permet de configurer les protocoles de transport utilisés par le Serveur Dr.Web pour se connecter aux clients.

- Dans la liste déroulante **Chiffrement**, choisissez la politique de chiffrement du trafic entre le Serveur Dr.Web et les clients connectés : les Agents Dr.Web, les Serveurs voisins Dr.Web et les Installateurs réseau.
- Dans la liste déroulante **Compression**, choisissez le mode de compression du trafic entre le Serveur Dr.Web et les clients connectés : les Agents Dr.Web, les Serveurs voisins Dr.Web et les Installateurs réseau.

Pour en savoir plus sur ces paramètres, voir la rubrique [Chiffrement et compression du trafic](#).

- Lorsque vous choisissez **Oui** ou **Possible** pour la compression du trafic, la liste déroulante **Niveau de compression** est disponible. Dans cette liste, vous pouvez indiquer le niveau



de compression des données de 1 à 9, où 1 est le niveau minimum et 9 le niveau maximum de compression.



Pour en savoir plus, voir la rubrique [Chiffrement et compression du trafic](#).

- Dans le champ **Clé de chiffrement pour les tickets de session TLS**, spécifiez le chemin vers le fichier de la clé de chiffrement pour les tickets de sessions TLS. Utilisé pour reprendre la séance TLS à la base des tickets de sessions qui sont chiffrés avec la clé spécifiée.

Dans la sous-rubrique **TCP/IP** sont configurés les paramètres de connexion au Serveur Dr.Web via les protocoles TCP/IP :

- **Adresse** et **Port** : l'adresse IP correspondante et le numéro du port de l'interface réseau à laquelle ce protocole de transport est lié. Le Serveur Dr.Web écoute l'interface avec les paramètres configurés pour communiquer avec les Agents Dr.Web installés sur les postes de travail.
- Cochez la case **Détecter** pour activer le service de détection du Serveur Dr.Web.
- Cochez la case **Multicast** pour utiliser le mode *Multicast over UDP* pour la détection du Serveur Dr.Web.
- **Groupe multicast** : adresse IP du groupe multicast dans lequel le Serveur Dr.Web est enregistré. Il est utilisé pour la communication avec des Agents Dr.Web et des Installateurs réseau lors de la recherche des Serveurs Dr.Web actifs dans le réseau. Si le champ n'est pas rempli, le groupe 231.0.0.1 est utilisé par défaut.
- **Nom** : nom du Serveur Dr.Web. Si aucun nom n'est indiqué, le nom indiqué à l'onglet **Général** est utilisé (voir ci-dessus, si aucun nom n'est indiqué dans cet onglet, le nom de l'ordinateur est utilisé). Si un autre nom est indiqué pour le protocole que le nom spécifié dans l'onglet **Général**, le nom inscrit dans la description du protocole est utilisé. Ce nom est utilisé par le service de détection du Serveur par les Agents Dr.Web, etc.
- Uniquement sous les OS de la famille UNIX : dans le champ **Chemin** indiquez le chemin d'accès au socket de communication, par exemple, de la communication avec l'Agent Dr.Web.



Pour en savoir plus, voir la rubrique [Configuration des connexions réseau](#).

Ces paramètres sont spécifiés au format d'adresse réseau décrit dans le document **Annexes**, [Annexe D. Spécification de l'adresse réseau](#).



10.3.3.4. E-mail

Dans l'onglet **E-mail** sont configurés les paramètres d'envoi d'e-mails depuis le Centre de gestion, par exemple en tant que les [notifications](#) de l'administrateur, lors de l'[envoi de packages d'installation de postes](#) ou pour la récupération du mot de passe de l'administrateur :

- **E-mail de l'expéditeur** : adresse e-mail de laquelle les e-mails seront envoyés.
- **Adresse du serveur** : adresse du serveur SMTP qui sera utilisée pour envoyer des e-mails.
- **Port** : port pour la connexion au serveur SMTP. C'est le port 465 qui est utilisé par défaut en cas d'ouverture d'une connexion TLS sécurisée à part, sinon, c'est le port 25.
- **Utilisateur, Mot de passe** : si nécessaire, spécifiez le nom de l'utilisateur et le mot de passe de l'utilisateur du serveur SMTP, si le serveur SMTP exige l'authentification.
- **Délai de connexion au serveur SMTP** : délai en secondes pour l'établissement de la connexion au serveur SMTP. La valeur est un nombre entier positif égal ou supérieur à 1.
- Dans la liste déroulante **Protection de la connexion**, sélectionnez le type de l'échange chiffrée de données :
 - **STARTTLS** : le passage à la connexion sécurisée s'effectue via la commande `STARTTLS`. L'utilisation du port 25 pour la connexion est prévue par défaut.
 - **SSL/TLS** : ouvrir une connexion sécurisée à part. L'utilisation du port 465 pour la connexion est prévue par défaut.
 - **Non** : ne pas utiliser le chiffrement. L'échange de données s'effectuera par la connexion non sécurisée.
- Cochez la case **Utiliser l'authentification CRAM-MD5** pour utiliser l'authentification *CRAM-MD5* sur le serveur de messagerie.
- Cochez la case **Utiliser l'authentification DIGEST-MD5** pour utiliser l'authentification *DIGEST-MD5* sur le serveur de messagerie.
- Cochez la case **Utiliser l'authentification LOGIN** pour utiliser l'authentification *LOGIN* sur le serveur de messagerie.
- Cochez la case **Utiliser l'authentification AUTH-NTLM** pour utiliser l'authentification *AUTH-NTLM* sur le serveur de messagerie.
- Cochez la case **Utiliser l'authentification standard** pour utiliser l'authentification *plain text* sur le serveur de messagerie.
- Cochez la case **Vérifier le certificat du serveur** pour vérifier le certificat TLS du serveur de messagerie. Spécifiez le chemin d'accès aux certificats TLS dans le champ **Certificats TLS**.
- Cochez la case **Mode de débogage** pour consulter le journal détaillé de la session SMTP.
- Dans le champ **Adresses e-mail des destinataires**, vous pouvez spécifier les adresses des boîtes e-mail pour vérifier l'envoi de courriel. Cliquez sur **Envoyer un message texte** pour envoyer un message texte (équivalent à la [notification](#) du Serveur Dr.Web) par e-mail conformément aux paramètres configurés dans cette section.



10.3.3.5. Cluster

Dans l'onglet **Cluster**, vous pouvez configurer les paramètres du cluster des Serveurs Dr.Web pour l'échange de données en cas de configuration du réseau antivirus multi-serveurs.

Pour utiliser le cluster, indiquez les paramètres suivants :

- **Groupe multicast** : adresse IP du groupe multicast via lequel les Serveurs Dr.Web vont échanger des informations.
- **Port** : numéro de port de l'interface réseau à laquelle le protocole de transport est lié pour transmettre des informations au groupe multicast.
- **Durée de vie** : durée de vie du datagramme lors du transfert de données dans le cluster des Serveurs Dr.Web.
- **Interface** : adresse IP de l'interface réseau à laquelle le protocole de transport est lié pour transmettre des informations au groupe multicast.



Vous pouvez consulter les particularités de la création du cluster des Serveurs Dr.Web dans la rubrique [Cluster des Serveurs Dr.Web](#).

10.3.3.6. Téléchargement

Dans l'onglet **Télécharger**, vous pouvez configurer les paramètres du Serveur Dr.Web utilisés pour générer les fichiers d'installation de l'Agent Dr.Web sur les postes du réseau antivirus. Ensuite, ces paramètres sont utilisés pour connecter l'installateur de l'Agent Dr.Web au Serveur Dr.Web :

- **Adresse du Serveur Dr.Web** : adresse IP ou nom de domaine du Serveur Dr.Web. Si l'adresse du Serveur Dr.Web n'est pas indiquée, le nom de l'ordinateur retourné par le système d'exploitation est utilisé.



Il est recommandé d'utiliser le nom du Serveur Dr.Web au [format FQDN](#) en tant qu'adresse du Serveur Dr.Web.

- **Port** : numéro du port utilisé lors de la connexion de l'installateur de l'Agent Dr.Web au Serveur Dr.Web.

Si le numéro de port n'est pas indiqué, le port 2193 est utilisé (ceci est configuré dans le Centre de gestion, dans la rubrique **Administration** → **Configuration du Serveur Dr.Web** → l'onglet **Réseau** → l'onglet **Transport**).

Les paramètres de la rubrique **Télécharger** sont sauvegardés dans le fichier de configuration `download.conf` (voir le document **Annexes**, [F3. Fichier de Configuration download.conf](#)).



10.3.3.7. Mises à jour de groupes

Dans l'onglet **Mises à jour Multicast**, vous pouvez configurer la transmission des mises à jour aux postes de travail via le protocole multicast.

Cochez la case **Activer les mises à jour de groupe** pour permettre la transmission des mises à jour aux postes via le protocole multicast.

Principes essentiels de fonctionnement des mises à jour de groupe :

1. Si les mises à jour de groupes sont activées, pour tous les postes connectés à ce Serveur Dr.Web, la mise à jour s'effectue en deux étapes :
 - a) Les postes écoutent les groupes multicast dont le Serveur Dr.Web fait partie. Si de nouvelles mises à jour de groupe apparaissent, les postes les téléchargent via *multicast over UDP*.
 - b) Après avoir transmis les mises à jour, le Serveur Dr.Web envoie une notification standard aux postes pour les informer des mises à jour disponibles. Tout ce que les postes n'ont pas pu télécharger via les mises à jour de groupe, ils téléchargent via le protocole TCP comme si c'était une mise à jour standard.
2. Si les mises à jour de groupes sont désactivées, la mise à jour de tous les postes est effectuée uniquement en mode général — via le protocole TCP.

Pour paramétrer les mises à jour multicast, utilisez les paramètres suivants :

- **Taille du datagramme UDP (octets)** : taille des datagrammes UDP utilisés par le protocole multicast, en octets.

L'intervalle autorisé est 512–8192. Pour éviter la fragmentation, il est recommandé d'indiquer une valeur inférieure au MTU (Maximum Transmission Unit) du réseau utilisé.

- **Délai de transmission du fichier (ms)** : durant cet intervalle de temps, le fichier de mise à jour unique est transmis, après quoi le Serveur Dr.Web commence à envoyer le fichier suivant.

Tous les fichiers qui n'ont pu être transmis à l'étape de la mise à jour via le protocole multicast seront transmis lors du processus standard de mise à jour via le protocole TCP.

- **Durée des mises à jour multicast (ms)** : durée du processus de mise à jour via le protocole multicast.

Tous les fichiers qui n'ont pu être transmis à l'étape de la mise à jour via le protocole multicast seront transmis lors du processus standard de mise à jour via le protocole TCP.

- **Intervalle de transmission des packages (ms)** : intervalle de transmission des packages à un groupe multicast.

Un intervalle faible peut provoquer des pertes significatives durant le transfert des packages et une surcharge du réseau. Il est recommandé de modifier ce paramètre.

- **Intervalle entre les demandes de retransmission (ms)** : avec cet intervalle, les Agents Dr.Web envoient des demandes de retransmission des paquets perdus.

Le Serveur Dr.Web accumule ces requêtes puis renvoie les blocs perdus.



- **Intervalle de "Silence" sur la ligne (ms)** : lorsqu'une transmission d'un fichier est terminée avant que la durée allouée ait expiré, si, durant l'intervalle de "silence" indiqué, aucune requête n'est envoyée par l'Agent Dr.Web pour la retransmission de packages perdus, le Serveur Dr.Web considère que tous les Agents Dr.Web ont reçu les fichiers de mise à jour et commence à envoyer le fichier suivant.
- **Intervalle d'accumulation des requêtes de retransmission (ms)** : durant cet intervalle, le Serveur Dr.Web accumule les requêtes des Agents Dr.Web pour la retransmission des packages perdus.

Les Agents Dr.Web redemandent les packages perdus. Le Serveur Dr.Web accumule ces requêtes durant un délai de temps spécifié, après quoi il envoie les blocs perdus.

Pour indiquer la liste des groupes multicast depuis lesquels les mises à jour multicast sont disponibles, configurez les paramètres suivants dans la sous-rubrique **Groupes multicast** :

- **Groupe multicast** : adresse IP du groupe multicast via lequel les postes recevront des mises à jour multicast.
- **Port** : numéro de port de l'interface réseau du Serveur Dr.Web à laquelle le protocole multicast de transport est lié pour transmettre des mises à jour.



Pour les mises à jour multicast, il faut spécifier n'importe quel port libre, autre que le port spécifié dans les paramètres pour le fonctionnement du protocole de transport du Serveur Dr.Web.

- **Durée de vie** : durée de vie du datagramme lors du transfert des données durant les mises à jour de groupe.
- **Interface** : adresse IP de l'interface réseau du Serveur Dr.Web à laquelle le protocole multicast de transport est lié pour transmettre des mises à jour.

Chaque ligne contient la configuration d'un groupe multicast. Pour ajouter un groupe multicast supplémentaire, cliquez sur .

En cas de sélection de plusieurs groupes multicast, prenez en compte les particularités suivantes :

- Pour les Serveurs Dr.Web différents qui diffuseront les mises à jour multicast, il faut spécifier les groupes multicast différents.
- Pour les Serveurs Dr.Web différents qui diffuseront les mises à jour multicast, il faut spécifier les paramètres différents **Interface** et **Port**.
- En cas d'utilisation de plusieurs groupes multicast, les ensembles des postes inclus dans ces groupes ne doivent pas se croiser. Ainsi, chaque poste du réseau antivirus peut entrer dans un seul groupe multicast.

Dans la section **Liste de contrôle d'accès** sont spécifiées les limitations des adresses réseau des postes qui recevront les mises à jour de groupe :

- Les postes qui sont autorisés de recevoir des mises à jour de groupe écouteront les groupes multicast spécifiés et recevront des mises à jour selon la procédure habituelle (voir [procédure 1](#)).



- Les postes qui ne sont pas autorisés de recevoir des mises à jour de groupe n'écoutent pas les groupes multicast spécifiés pour la présence des mises à jour, mais ils téléchargent toutes les mises à jour via TCP (voir [procédure 2](#)).

Les listes sont configurées de la même manière que les listes de la section [Sécurité](#).

10.3.4. Statistiques

L'onglet **Statistiques** permet de spécifier les informations statistiques à écrire dans le journal du protocole ainsi que dans la base de données du Serveur Dr.Web. Vous pourrez consulter ces informations plus tard dans la section de [statistiques](#) du Centre de gestion.

Pour ajouter des informations correspondantes dans la BD, cochez les cases suivantes :

- **Statut de la quarantaine** : permet de surveiller le statut de la Quarantaine sur les postes et d'enregistrer les informations dans la base de données.
- **Composition de matériel et de logiciels** : permet de surveiller la composition de matériel et de logiciels sur les postes et d'enregistrer les informations dans la base de données.
- **Liste des modules de postes** : permet de surveiller la liste des modules de l'Antivirus et d'enregistrer les informations dans la base de données.
- **Liste des composants installés** : permet de surveiller la liste des composants de l'Antivirus (Scanner, moniteurs etc.) installés sur le poste et d'enregistrer les informations dans la base de données.
- **Sessions des utilisateurs des postes** : permet de surveiller des sessions utilisateur sur les postes et de sauvegarder dans la base de données les logins des utilisateurs connectés au système depuis un ordinateur avec un Agent Dr.Web installé.
- **Démarrage/arrêt des composants** : permet de surveiller les informations sur le lancement et l'arrêt des composants de l'Antivirus (Scanner, moniteurs etc.) et d'enregistrer les informations dans la base de données.
- **Menaces de sécurité détectées** : permet de surveiller les menaces détectées sur les postes et d'enregistrer les informations dans la base de données.

Si la case **Menaces de sécurité détectées** est cochée, vous pouvez également configurer les paramètres supplémentaires des statistiques sur les menaces.

- Cochez la case **Suivre les épidémies** pour activer le mode de notification de l'administrateur en cas d'épidémie virale. Si la case n'est pas cochée, les notifications des infections virales sont effectuées en mode standard. Si la case est cochée, vous pouvez configurer les paramètres de suivi des épidémies :
 - **Période de blocage d'envoi des notifications** : délai en secondes après l'envoi de la notification portant sur une épidémie. Pendant ce délai, les notifications portant sur des infections isolées des postes ne seront pas envoyées.
 - **Délai de décompte des postes infectés** : délai en secondes pendant lequel un nombre spécifié de messages portant sur des postes infectés doit être reçu pour envoyer un rapport sommaire sur une épidémie.



- **Nombre de messages** : nombre de messages portant sur des infections devant être reçus dans le délai indiqué afin que le Serveur Dr.Web envoie à l'administrateur une notification d'une épidémie relative à tous les cas d'infection (notification **Épidémie dans le réseau**).
- **Nombre de menaces les plus répandues** : nombre des menaces les plus répandues à inclure dans le rapport sur les épidémies.
- Cochez la case **Regrouper les rapports de la Protection préventive** pour envoyer un seul rapport sommaire sur plusieurs événements de la Protection préventive. Si la case est décochée, les événements de la Protection préventive seront reçus dans de différentes notifications indépendamment de leur nombre. Si la case est cochée, vous pouvez également spécifier les paramètres suivants de groupement des rapports :
 - **Période de blocage d'envoi des notifications** : délai en secondes après l'envoi du rapport sommaire portant sur les événements de la Protection préventive. Pendant ce délai, les notifications portant sur des événements isolés ne seront pas envoyées.
 - **Délai de décompte des événements** : délai en secondes pendant lequel un nombre spécifié des événements de la Protection préventive doit se produire pour envoyer un rapport sommaire.
 - **Nombre d'événements** : nombre des événements de la Protection préventive qui doivent être reçus dans le délai indiqué afin que le Serveur Dr.Web envoie à l'administrateur un rapport sommaire sur ces événements (notification **Rapport sommaire de la Protection préventive**).
 - **Nombre des processus les plus actifs** : nombre des processus les plus répandues exécutant une action suspecte à inclure dans le rapport de la Protection préventive.
- Cochez la case **Envoyer des statistiques à Doctor Web** pour activer l'envoi des statistiques sur les menaces détectées à Doctor Web. Les champs suivants seront disponibles :
 - **Intervalle** : intervalle, en minutes, pour l'envoi des statistiques ;
 - **Identificateur** : une clé MD5 (située dans le fichier de configuration du Serveur Dr.Web).

Le champ **Intervalle** de l'envoi des statistiques est le seul champ obligatoire.

- **Interruptions anormales des connexions** : autorise à surveiller les connexions aux clients interrompues de façon anormale et à avoir la possibilité d'envoyer les notifications correspondantes à l'administrateur.

Spécifiez les paramètres suivants des interruptions anormales des connexions :

- **Période de blocage d'envoi des notifications** : délai en secondes après l'envoi de la notification portant sur de nombreuses interruptions de connexions. Pendant ce délai, les notifications portant sur des interruptions isolées des connexions ne seront pas envoyées.
- **Délai de décompte des connexions terminées** : délai en secondes pendant lequel un nombre spécifié d'interruptions de connexions aux clients doit se produire pour envoyer une notification correspondante.
- **Nombre de connexions pour une notification des interruptions isolées** : nombre minimum des connexions à une adresse qui doivent être interrompues pendant le



décompte pour qu'une notification d'une interruption anormale soit envoyée (notification **Interruption anormale de la connexion**).

- **Nombre de connexions pour une notification de nombreuses interruptions** : nombre minimum des connexions qui doivent être interrompues pendant le décompte pour qu'une notification unique de nombreuses interruptions anormales soit envoyée (notification **Un grand nombre de connexions interrompues de façon anormale est enregistré**).
- **Durée de courtes connexions** : si la durée d'une connexion au client terminée est inférieure à la durée indiquée, une notification d'interruptions isolées de connexions (notification **Arrêt d'urgence de la connexion**) sera envoyée lorsque le nombre spécifié de connexions sera atteint, quelle que soit la période de décompte. Dans ce cas, la connexion ne doit pas être interrompue plus tard par des connexions plus longues et une notification de nombreuses interruptions anormales de connexions ne doit pas être envoyée (notification **Un grand nombre de connexions interrompues de façon anormale est enregistré**).
- **Erreurs de scan** : permet de surveiller les erreurs de scan sur les postes et d'enregistrer les informations dans la base de données.
- **Statistiques de scan** : permet de surveiller les statistiques de scan et d'enregistrer les informations dans la base de données.
- **Installations des Agents** : permet de surveiller les informations sur les installations des Agents Dr.Web sur les postes et d'enregistrer les informations dans la base de données.
- **Périphériques bloqués** : autorise le suivi des informations sur les périphériques bloqués par le composant Office Control et l'enregistrement des informations dans la base de données.
- **Statistiques du Contrôle des applications sur l'activité de processus** : autorise le suivi des informations sur l'activité des processus sur les postes enregistrée par le Contrôle des applications et l'enregistrement des informations dans la base de données.
- **Statistiques du Contrôle des applications sur le blocage de processus** : autorise le suivi des informations sur le blocage des processus sur les postes par le Contrôle des applications et l'enregistrement des informations dans la base de données.
- **Nombreux blocages du Contrôle des applications** : autorise à surveiller de nombreux blocages de processus faits par le Contrôle des applications et à avoir la possibilité d'envoyer les notifications correspondantes à l'administrateur.

Spécifiez les paramètres suivants des événements :

- **Période de blocage d'envoi des notifications** : délai en secondes après l'envoi du rapport sommaire portant sur les processus bloqués par le Contrôle des applications. Pendant ce délai, les notifications portant sur des blocages isolés ne seront pas envoyées.
- **Période de décompte des processus bloqués** : délai en secondes pendant lequel un nombre spécifié de processus doit être bloqué pour envoyer un rapport sommaire.
- **Nombre de blocages** : nombre des événements des processus bloqués par le Contrôle des applications qui doivent être reçus dans le délai indiqué afin que le Serveur Dr.Web envoie à l'administrateur un rapport sommaire sur tous ces événements (notification **Un grand nombre de blocages faits par le Contrôle des applications est enregistré**).



- **Nombre des profils les plus répandus** : nombre des profils les plus répandus par lesquels le blocage a été fait et qu'il faut inclure dans la notifications de nombreux blocages.
- **Journal d'exécution des tâches sur les postes** : permet de surveiller les résultats de l'exécution des tâches sur les postes et d'enregistrer les informations dans la base de données.
- **Surveillance des statuts des postes** : permet de surveiller les modifications intervenues sur les postes et d'enregistrer les informations dans la base de données.
 - **Statut des bases virales** : permet de surveiller les modifications du statut et du contenu des bases virales sur le poste et d'enregistrer les informations dans la base de données. La case est disponible seulement si la case **Statut du poste** est cochée.
- **Données de localisation** : permet de recevoir des informations sur la localisation de postes et enregistrer les informations dans la base de données.
- **Espace disque sur les postes** : permet de recevoir des informations sur l'espace disque sur les postes et d'enregistrer les informations dans la base de données.
- **Collecter les informations sur les périphériques** : permet au Serveur Dr.Web de collecter les informations sur les périphériques connectés aux postes.
- **Collecter les informations sur les utilisateurs** : permet au Serveur Dr.Web de collecter les informations sur les utilisateurs du poste.



L'Agent Dr.Web a les mêmes paramètres de collecte d'informations qui lui permettent d'envoyer les données sur le Serveur Dr.Web. Les paramètres ci-dessus déterminent si le Serveur Dr.Web gardera et traitera les données envoyées par l'Agent Dr.Web

Pour consulter les informations statistiques

1. Sélectionnez l'élément **Réseau antivirus** du menu principal.
2. Sélectionnez un poste ou un groupe dans la liste hiérarchique.
3. Ouvrez la rubrique correspondante du menu de gestion (voir le tableau ci-dessous).



Pour en savoir plus sur les données statistiques, voir la rubrique [Consultation des statistiques sur un poste](#).

Le tableau ci-dessous présente la correspondance entre les cases de la rubrique **Statistiques** dans les paramètres du Serveur Dr.Web et les éléments du menu de gestion sur la page **Réseau antivirus**.

Si les cases de l'onglet **Statistiques** sont décochées, les éléments correspondants seront masqués dans le menu de gestion.

**Tableau 10-1. Correspondance entre les paramètres du Serveur Dr.Web et les éléments du menu de gestion**

Paramètres du Serveur Dr.Web	Éléments du menu
Statut de la quarantaine	Général → Quarantaine Configuration → Windows → Agent Dr.Web → case Autoriser la gestion de la Quarantaine à distance
Composition de matériel et de logiciels	Général → Composition de matériel et de logiciels Général → Périphériques détectés
Liste des modules du poste	Statistiques → Modules
Listes des composants installés	Général → Composants installés
Sessions des utilisateurs des postes	Général → Sessions utilisateurs
Démarrage/arrêt des composants	Statistiques → Démarrage/Arrêt
Menaces de sécurité détectées	Statistiques → Menaces Statistiques → Statistiques des menaces Statistiques → Événements de la Protection préventive
Erreurs de scan	Statistiques → Erreurs
Statistiques de scan	Statistiques → Statistiques de scan
Installations des Agents	Statistiques → Installations des Agents
Périphériques bloqués	Statistiques → Périphériques bloqués
Statistiques du Contrôle des applications sur l'activité des processus	Statistiques → Événements du Contrôle des applications
Statistiques du Contrôle des applications sur le blocage des processus	Administration → Contrôle des applications → Répertoire d'applications
Journal de l'exécution des tâches sur les postes	Statistiques → Tâches
Statuts des postes	Statistiques → Statut Statistiques → Bases virales
Statut des bases virales	Statistiques → Bases virales



10.3.5. Sécurité

L'onglet **Sécurité** permet de spécifier des limitations pour les adresses réseau depuis lesquelles les Agents Dr.Web, les installateurs réseau et d'autres Serveurs Dr.Web (voisins) pourront accéder au Serveur Dr.Web spécifié.

Les cases ci-dessous permettent de gérer le journal d'audit du Serveur Dr.Web :

- **Audit des opérations de l'administrateur** autorise l'écriture dans le journal d'audit des opérations de l'administrateur avec le Centre de gestion ainsi que l'écriture du journal dans la BD.
- **Audit des opérations internes du serveur** autorise l'écriture dans le journal d'audit des opérations internes du Serveur Dr.Web ainsi que l'écriture du journal dans la BD.
- **Audit des opérations de l'API Web** permet l'écriture des opérations effectuées via l'API XML ainsi que l'écriture du journal dans la BD.



Pour consulter le journal d'audit, sélectionnez l'élément **Journal d'audit** dans le menu principal **Administration**.

L'onglet **Sécurité** comprend les onglets supplémentaires permettant de configurer des limitations pour les types correspondants de connexions :



- **Agents** : listes de restrictions des adresses IP depuis lesquelles les Agents Dr.Web peuvent se connecter à ce Serveur Dr.Web.
- **Installateurs** : listes de restrictions des adresses IP depuis lesquelles les installateurs des Agents Dr.Web peuvent se connecter à ce Serveur Dr.Web.
- **Liaisons** : listes de restrictions des adresses IP depuis lesquelles les Serveurs Dr.Web peuvent se connecter à ce Serveur Dr.Web.
- **Service de détection** : liste de restrictions des adresses IP depuis lesquelles les requêtes de recherche broadcast sont reçues par le [service de détection du Serveur Dr.Web](#).

Pour configurer les limitations d'accès (elles sont spécifiées séparément pour les Agents, les Installations, les Serveurs voisins Dr.Web ou les Services de détection) :

1. Cochez la case **Utiliser cette liste de contrôle d'accès** pour spécifier les listes d'adresses autorisées ou bloquées. Si la case est décochée, toutes les connexions seront autorisées.
2. Pour autoriser l'accès depuis une adresse TCP déterminée, ajoutez l'adresse dans la liste **TCP: autorisé** ou **TCPv6: autorisé**.
3. Pour interdire une adresse TCP, ajoutez-la dans la liste **TCP: interdit** ou **TCPv6: interdit**.
4. Les adresses non mentionnées dans aucune des listes sont autorisées ou interdites en fonction du statut de la case **Priorité de refus** : si la case est cochée, la liste **Refuser** possède une priorité plus importante que la liste **Autoriser**. Les adresses qui ne sont incluses à aucune liste ou incluses aux deux listes sont refusées. Seules les adresses appartenant à la liste **Autoriser** et non incluses à la liste **Refuser** seront autorisées.



Pour éditer la liste des adresses :

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



Les listes pour les adresses TCPv6 ne seront affichées que dans le cas où l'interface IPv6 est installée sur le poste.


Exemple d'utilisation du préfixe :

1. Le préfixe 24 désigne les réseaux ayant le masque : `255 . 255 . 255 . 0`
Il contient 254 adresses.
Les adresses hôte dans les réseaux de ce type : `195 . 136 . 12 . *`
2. Le préfixe 8 désigne les réseaux ayant le masque `255 . 0 . 0 . 0`
Il contient jusqu'à 16777214 adresses ($256*256*256-2$).
Les adresses d'hôtes dans les réseaux de ce type ont le format suivant : `125 . * . * . *`

10.3.6. Cache

Dans l'onglet **Cache**, vous pouvez spécifier les paramètres de nettoyage du cache :

- **Période de nettoyage du cache** : fréquence de nettoyage complet du cache.
- **Fichiers de quarantaine** : périodicité de suppression des fichiers de quarantaine du côté du Serveur Dr.Web.
- **Fichiers du référentiel** : périodicité de suppression des fichiers dans le référentiel.
- **Cache de fichiers** : fréquence de nettoyage du cache de fichiers.
- **Packages d'installation** : périodicité de suppression des packages d'installation personnels et des packages d'installation de groupe.

Cliquez sur le bouton  **Supprimer tous les packages d'installation maintenant** pour supprimer tous les packages personnels et les packages de groupe créés précédemment et se trouvant dans le répertoire `installers-cache` du répertoire `var`. Notez qu'en cas de téléchargement des packages, ils seront créés de nouveau, ce qui peut prendre un certain temps.



Lors de l'indication des valeurs numériques, vous pouvez utiliser les listes déroulantes d'unités de mesure de périodicité.



10.3.7. Base de données

Dans l'onglet **Base de données**, vous pouvez sélectionner la BD requise pour le fonctionnement du Serveur Dr.Web.



La structure de la base de données du Serveur voisin est disponible sous forme d'un manuel éponyme à part. Vous pouvez ouvrir le document dans la section **Support** dans le Centre de gestion de la sécurité Dr.Web.

Pour configurer les paramètres de travail avec la base de données

1. Dans le champ **Nombre de connexions**, indiquez le nombre maximum des connexions du Serveur Dr.Web à la base de données.

Si vous utilisez la base de données embarquée, il n'est pas recommandé de modifier la valeur par défaut. Si vous utilisez la base de données externe, une valeur supérieure peut être requise. (Pour en savoir plus sur la sélection d'une valeur optimale, voir le document **Annexes**, rubrique [Charge sur le Serveur Dr.Web et paramètres de configuration recommandés](#)).



La base de données embarquée est conçue pour la connexion de 400-600 postes au Serveur Dr.Web. Si l'ordinateur sur lequel est installé le Serveur Dr.Web et la charge relative à d'autres tâches exécutées sur la même machine le permettent, il est possible de connecter jusqu'à 1000-1500 postes.

Sinon, il est nécessaire d'utiliser une BD externe. En fonction de la configuration et de la charge sur l'ordinateur exécutant les fonctions du Serveur Dr.Web, la BD externe peut être placée sur le même ordinateur ou sur un ordinateur spécial séparé.

En cas d'utilisation d'une BD externe et si le nombre de postes connectés au Serveur Dr.Web est supérieur à 10000, il est recommandé de respecter les pré-requis minimum suivants :

- processeur 3GHz,
- au moins 6 coeurs de processeur,
- mémoire vive : au moins 4 Go pour le Serveur Dr.Web, au moins 8 Go pour le Serveur de BD,
- OS de la famille UNIX.

Si vous gérez un réseau avec un grand nombre de connexions des clients au Serveur Dr.Web, il est recommandé de consulter le support technique de la société Doctor Web avant de modifier le paramètre.

2. Cochez la case **Nettoyer automatiquement la base de données après les procédures de maintenance** pour effectuer automatiquement le nettoyage automatique de la base de données après son initialisation, sa mise à jour et son importation. Si la case est décochée, le nettoyage automatique ne se fait pas. Dans ce cas, il est recommandé de configurer la tâche **Nettoyage de la base de données** dans la planification du Serveur Dr.Web ou nettoyer manuellement via la section [Gestion de la base de données](#).



Pour exécuter un nettoyage automatique une tâche masquée est créée dans la planification du Serveur Dr.Web. La tâche est réalisée la nuit prochaine après les procédures de maintenance, à 01h17, heure locale du Serveur Dr.Web. La tâche est exécutée uniquement s'il n'y a pas d'autre tâche **Nettoyage de la base de données** dans la planification du Serveur Dr.Web dans les 24 heures qui suivent après les procédures de maintenance mentionnées.

3. Dans la liste déroulante **Base de données**, choisissez le type de la BD :

- **MySQL** : BD externe,
- **ODBC** : pour utiliser une BD externe via la connexion ODBC,



Si un avertissement ou une erreur survient lors du travail du Serveur Dr.Web avec SGBD Microsoft SQL Server via ODBC, il faut s'assurer que vous utilisez la dernière version disponible de SGBD de cette rédaction.

Pour savoir comment vous pouvez vérifier la disponibilité des corrections, consultez la page suivante de Microsoft :

<https://learn.microsoft.com/troubleshoot/sql/general/determine-version-edition-update-level>.

- **Oracle** : BD externe pour toutes les plateformes sauf FreeBSD,



Si un SGBD externe Oracle est utilisé via une connexion ODBC, il est nécessaire d'installer la dernière version du pilote ODBC fourni avec ce SGBD. Il est fortement recommandé de ne pas utiliser le pilote ODBC Oracle fourni par Microsoft.

- **PostgreSQL** : BD externe,
- **SQLite3** : BD intégrée (composant du Serveur Dr.Web).

4. Configurez les paramètres requis pour le fonctionnement de la BD :

- Pour une BD embarquée, indiquez, si nécessaire, le chemin d'accès complet au fichier de la base de données dans le champ **Nom du fichier** et spécifiez la taille du cache et le mode d'enregistrement des données.
- Les paramètres des BD externes sont décrits dans le document **Annexes, Annexe A. Paramètres d'utilisation du SGBD. Paramètres des pilotes du SGBD.**

5. Pour appliquer les paramètres spécifiés, cliquez sur **Enregistrer**.



Le kit de distribution du Serveur Dr.Web contient des clients intégrés pour les SGBD supportés, veuillez donc noter :

- Si vous prévoyez d'utiliser des clients SGBD intégrés qui sont fournis avec le Serveur Dr.Web, durant l'installation (mise à niveau) du Serveur Dr.Web, dans les paramètres de l'installateur, sélectionnez l'installation Personnalisée et dans la fenêtre suivante, vérifiez que l'installation du client correspondant pour le SGBD intégré est activée dans la rubrique **Support des Bases de données**.
- Si vous 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 Dr.Web). Sinon, l'interaction avec la BD via ODBC sera impossible à cause du conflit des bibliothèques.

L'installateur du Serveur Dr.Web 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 Dr.Web et de choisir **Modifier**.

L'utilisation d'une BD interne est spécifiée par défaut. Ce mode accroît beaucoup la charge sur le Serveur Dr.Web. Dans de grands réseaux antivirus il est recommandé d'utiliser une BD externe. La procédure de changement du type de BD est décrite dans les **Annexes**, la rubrique [Changement du type de BD Dr.Web Enterprise Security Suite](#).



Il est possible de nettoyer la base de données utilisée par le Serveur Dr.Web, notamment supprimer des enregistrements d'événements et de données sur les postes qui n'ont pas visité le Serveur Dr.Web depuis un certain temps. Pour nettoyer la base de données, ouvrez la rubrique de la [planification du Serveur Dr.Web](#) et créez la tâche correspondante.

10.3.7.1. Restauration des bases de données

En cas d'échec de la base de données **SQLite3** il est possible de restaurer la base endommagée à l'aide des outils standard.

En cas d'endommagement de la base de données, il faut effectuer les actions suivantes :

1. Si la base de données est endommagée, le Serveur Dr.Web ne démarre pas et ne fonctionne pas :
 - a) Si, pendant le fonctionnement du Serveur Dr.Web, un échec survient lors de l'interaction standard avec la base de données, le Serveur Dr.Web s'arrête automatiquement.
 - b) Si au démarrage du Serveur Dr.Web, l'option **Rapide** ou **Compète** est sélectionnée dans la liste déroulante **Vérifier l'intégrité de l'image** des paramètres de la base de données **SQLite3**, l'image de la base de données est automatiquement vérifiée. En cas de détection d'un défaut, le Serveur Dr.Web ne démarre pas.
2. Pour pouvoir démarrer le Serveur Dr.Web, il est nécessaire de restaurer la base de données endommagée :
 - a) Si la case **Restaurer l'image corrompue automatiquement** est cochée dans les paramètres de la base de données **SQLite3**, la restauration automatique de l'image endommagée s'effectue au démarrage du Serveur Dr.Web.
 - b) Si la restauration automatique de l'image de la base de données est désactivée, vous pouvez utiliser la clé `repairdb` lors du démarrage du Serveur Dr.Web depuis la ligne de commande (voir aussi le document **Annexes**, [H3.3. Commandes de gestion de la base de données](#)).



10.3.8. Modules

Dans l'onglet **Modules**, vous pouvez configurer le mode d'interaction du Serveur Dr.Web avec d'autres composants de Dr.Web Enterprise Security Suite :

- Cochez la case **Protocole de l'Agent Dr.Web** pour activer le protocole qui permet l'interaction du Serveur Dr.Web avec les Agents Dr.Web.
- Cochez la case du **Protocole Microsoft NAP Health Validator** pour activer le protocole qui permet l'interaction du Serveur Dr.Web avec le composant de vérification de l'état de santé du système NAP Validator de Microsoft.
- Cochez la case **Protocole de l'installateur de l'Agent Dr.Web** pour activer le protocole qui permet l'interaction du Serveur Dr.Web avec les installateurs des Agents Dr.Web.
- Cochez la case **Protocole du cluster des Serveurs Dr.Web** pour activer le protocole permettant l'interaction entre les Serveurs Dr.Web dans le système de cluster.
- Cochez la case **Protocole du Serveur Dr.Web** pour activer le protocole qui permet l'interaction d'un Serveur Dr.Web avec d'autres Serveurs Dr.Web. Le protocole est désactivé par défaut. Si vous utilisez une configuration réseau multi-serveurs (voir [Particularités du réseau avec plusieurs Serveurs Dr.Web](#)), cochez la case **Protocole du Serveur Dr.Web** pour l'activer.
- Cochez la case **Protocole du Serveur proxy Dr.Web** pour activer le protocole d'interaction du Serveur Dr.Web avec les Serveurs proxy Dr.Web.
- Cochez la case **Extension pour le Centre de gestion de la sécurité Dr.Web** pour la gestion du Serveur Dr.Web et du réseau antivirus via le Centre de gestion.



Si vous décochez la case **Extension pour le Centre de gestion de la sécurité Dr.Web**, le Centre de gestion de la sécurité Dr.Web ne sera pas disponible après le redémarrage du Serveur Dr.Web. Dans ce cas, vous pourrez gérer le Serveur Dr.Web et le réseau antivirus uniquement via l'utilitaire de diagnostic distant, si la case **Extension Dr.Web Server FrontDoor** est cochée.

- Cochez la case du **Extension Dr.Web Server FrontDoor** pour utiliser l'extension Dr.Web Server FrontDoor qui autorise la connexion de l'utilitaire de diagnostic distant du Serveur Dr.Web (voir aussi [Accès distant au Serveur Dr.Web](#)).
- Cochez la case **Extension de l'agent SNMP Dr.Web** pour autoriser le Serveur Dr.Web à échanger les informations avec les systèmes de gestion réseau via le protocole SNMP (voir aussi [Configuration de l'agent SNMP Dr.Web](#)).
- Cochez la case **Extension Yandex Locator** pour autoriser l'utilisation de l'extension Yandex Locator pour localiser les appareils mobiles connectés au Serveur Dr.Web.
 - Dans le champ **Clé API**, entrez la clé API obtenue depuis le service correspondant de Yandex.



Si vous activez l'extension Yandex Locator, mais vous ne spécifiez pas la clé API, l'extension ne sera pas activée.



Pour plus d'informations sur l'utilisation et la configuration de l'extension Yandex.Locator, consultez les **Annexes**, la rubrique [Localisation automatique d'un poste tournant sous l'OS Android](#).

10.3.9. Localisation

L'onglet **Localisation** vous permet de consulter des informations supplémentaires sur l'emplacement de l'ordinateur sur lequel le logiciel du Serveur Dr.Web est installé.

Dans cet onglet, vous pouvez également voir la localisation du Serveur Dr.Web sur une carte.

Pour voir la localisation du Serveur Dr.Web sur la carte

1. Dans les champs **Latitude** et **Longitude**, indiquez les coordonnées géographiques du Serveur Dr.Web au format Degrés décimaux.
2. Cliquez sur **Enregistrer** pour conserver ces données dans le fichier de configuration du Serveur Dr.Web.
Pour consulter la carte, vous n'avez pas besoin de redémarrer le Serveur Dr.Web. Mais pour appliquer des changements dans les coordonnées géographiques, vous devez le redémarrer.
3. Dans l'onglet **Localisation**, un aperçu de la carte OpenStreetMap va s'ouvrir et les coordonnées indiquées seront marquées.
Si le chargement de l'aperçu est impossible, le texte **Afficher sur la carte** apparaît.
4. Pour consulter la carte au plus grand format, cliquez sur l'outil de visualisation ou sur le texte **Afficher sur la carte**.

10.3.10. Licences

Dans l'onglet **Licences** sont spécifiés les paramètres de la distribution des licences entre les Serveurs Dr.Web, ainsi que les paramètres de création des rapports sur l'utilisation des licences.

Paramètres de la notification portant sur la limitation du nombre de licences dans la clé de licence

- **Nombre des licences restantes** : nombre maximal des licences restantes qui déclenchera l'envoi de la notification **Limitation du nombre de licences dans la clé de licence**.
- **Taux des licences restantes** : taux maximal des licences restantes qui déclenchera l'envoi de la notification **Limitation du nombre de licences dans la clé de licence**.



Paramètres du rapport sur l'utilisation des licences



Lors de l'envoi des rapports entre les Serveurs Dr.Web, ces paramètres doivent être spécifiés sur le Serveur Dr.Web principal, pourtant ils seront utilisés par les Serveurs Dr.Web subordonnés.

Si les liaisons avec les Serveurs voisins Dr.Web ne sont pas configurées, ces options sont utilisées uniquement par le Serveur courant Dr.Web pour ses rapports personnels.

- **Période de création du rapport** : fréquence de création des rapports sur le Serveur Dr.Web portant sur les clés de licence utilisées.
Si le rapport sur l'utilisation de licences est créé par le Serveur Dr.Web subordonné, ce rapport sera envoyé sur le Serveur principal Dr.Web juste après sa création.
Les rapports créés sont également envoyés à chaque connexion (y compris chaque redémarrage) du Serveur Dr.Web, et en cas de modification du nombre de licences délivrées sur le Serveur principal Dr.Web.
- **Période de décompte des postes actifs** : période pendant laquelle les postes actifs seront comptés pour envoyer un rapport sur l'utilisation des licences. La valeur 0 indique d'utiliser dans le rapport tous les postes quel que soit leur statut d'activité.

Paramètres pour le Serveur Dr.Web délivrant la licence

- **Période du renouvellement automatique des licences délivrées** : période de temps pour laquelle les licences sont délivrées de la clé sur ce Serveur Dr.Web. A l'expiration de cette période, les licences délivrées sont renouvelées automatiquement pour le même délai. Le renouvellement automatique sera effectué jusqu'à ce que dure le délai de distribution des licences spécifié dans le Gestionnaire de licences à l'étape 5.
Ce mécanisme assure le retour des licences sur le Serveur Dr.Web principal au cas où le Serveur Dr.Web subordonné sera désactivé et ne pourra pas retourner les licences délivrées.
- **Période de synchronisation de licences** : périodicité de synchronisation des informations sur les licences délivrées entre les Serveurs Dr.Web. La synchronisation des licences permet de déterminer que le nombre de licences délivrées par le Serveur Dr.Web principal corresponde au nombre des licences reçues par le Serveur Dr.Web subordonné. Ce mécanisme permet de détecter les défaillances et les cas de falsification lors du transfert des licences.

Paramètres pour le Serveur Dr.Web recevant la licence

- **Intervalle de renouvellement provisoire des licences obtenues** : délai de temps qui dure jusqu'à la fin de la période du renouvellement automatique des licences obtenues du Serveur voisin Dr.Web. A partir de ce moment ce Serveur Dr.Web demande le renouvellement automatique provisoire de ces licences.



L'utilisation de ce paramètre dépend du type de connexion sélectionné dans la section **Paramètres de connexion** lors de la configuration de la liaison entre les Serveurs Dr.Web (voir la section [Configuration des liaisons entre Serveurs Dr.Web](#)) :

- Pour la connexion périodique : si la période de reconnexion spécifiée dans le paramètre de la liaison est supérieure à la **Période du renouvellement automatique des licences délivrées** spécifiée sur le Serveur Dr.Web délivrant les licences, le renouvellement automatique de ces licences sera initié avant l'expiration de la **Période du renouvellement automatique des licences délivrées**.
- Pour la reconnexion permanente : ce paramètre n'est pas utilisé.



Pour plus d'informations sur la distribution des licences entre les Serveurs Dr.Web, consultez la rubrique [Distributions des licences par les liaisons entre les serveurs](#).

10.3.11. Journal

Dans l'onglet **Journal**, vous pouvez spécifier les paramètres de tenue du journal du Serveur Dr.Web :

- Dans la liste déroulante **Niveau de détails du fichier journal du Serveur Dr.Web**, sélectionnez le niveau de détails du journal de fonctionnement du Serveur Dr.Web.
- **Nombre maximal de fichiers** : nombre maximal des fichiers journaux (y compris le fichier actuel et les fichiers archivés) à sauvegarder.
- **Mode de rotation du journal du Serveur Dr.Web** : mode de rotation du journal de fonctionnement du Serveur Dr.Web. Sélectionnez l'une des valeurs présentées :
 - **rotation par taille** détermine la limitation de la taille pour chaque fichier du journal.
Taille maximale de chaque fichier : taille maximale autorisée de chaque fichier du journal. Quand le fichier actuel atteint la taille spécifiée, il est archivé, son nom change et le nouveau fichier de journal est créé.
 - **rotation par période** détermine la durée d'enregistrement de chaque fichier du journal.
Délai maximum d'enregistrement du fichier : délai maximum d'enregistrement de chaque fichier du journal. Quand le délai d'enregistrement du fichier atteint la durée spécifiée, le fichier est mis en archive, son nom est modifié et un nouveau fichier du journal est créé.
- Cochez la case **Archiver les fichiers du journal** pour mettre en archive les anciens fichiers du journal lors de la rotation.



Pour appliquer les modifications apportées, vous devez redémarrer le Serveur Dr.Web.

Vous pouvez redémarrer le Serveur soit via le Centre de gestion, soit avec la commande de console correspondante.



Pour plus d'infos sur le journal du Serveur Dr.Web, consultez la section [Journal du Serveur Dr.Web](#).

10.4. Accès distant au Serveur Dr.Web



Pour la connexion de l'utilitaire du diagnostic distant du Serveur Dr.Web, il est nécessaire d'activer l'extension Dr.Web Server FrontDoor. Pour ce faire cochez la case **Extension Dr.Web Server FrontDoor** dans l'onglet [Modules](#) de la section **Configuration du Serveur Dr.Web**.


Pour la connexion de l'utilitaire du diagnostic distant du Serveur Dr.Web, il faut que l'administrateur qui se connecte via l'utilitaire possède le droit **Utilisation des fonctionnalités supplémentaires**. Sinon, l'accès au Serveur Dr.Web via l'utilitaire du diagnostic distant sera interdit.


Pour configurer les paramètres de connexion de l'utilitaire du diagnostic distant du Serveur Dr.Web

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion. Dans la fenêtre qui s'ouvre, sélectionnez l'élément du menu de gestion **Accès distant au Serveur Dr.Web**.
2. Spécifiez le protocole de connexion :
 - Cochez la case **Utiliser TLS** pour autoriser la connexion de l'utilitaire de diagnostic distant au Serveur Dr.Web via le protocole TLS. Si la case est décochée, la connexion sera possible uniquement via le protocole TCP.
Pour la connexion via le protocole TLS, spécifiez les paramètres suivants :
 - **Certificat** : fichier du certificat qui sera vérifié lors de la connexion. Dans la liste déroulante sont présentés les certificats disponibles du répertoire du Serveur Dr.Web.
 - **Clé privée SSL** : fichier de la clé privée SSL qui sera vérifiée lors de la connexion. Dans la liste déroulante sont présentées les clés privées disponibles du répertoire du Serveur Dr.Web.
 - Dans le champ **Clé de chiffrement pour les tickets de session TLS**, spécifiez le chemin vers le fichier de la clé de chiffrement pour les tickets de sessions TLS. Utilisé pour reprendre la séance TLS à la base des tickets de sessions qui sont chiffrés avec la clé spécifiée.
 - **Liste de chiffrements autorisés** : ligne déterminant la liste de chiffrements du package OpenSSL autorisés à être utilisés dans les connexions aux clients. Si vous laissez le champ vide, la valeur `DEFAULT` sera utilisée ce qui signifie `ALL:!EXPORT:!LOW:!aNULL:!eNULL:!SSLv2`.
3. Spécifiez les paramètres de l'interface pour la connexion :



- **Adresse** : adresse IP écoutée du côté du Serveur Dr.Web pour la connexion de l'utilitaire de diagnostic distant.
- **Port** : port écouté du côté du Serveur Dr.Web pour la connexion de l'utilitaire de diagnostic distant du Serveur. Le port 10101 est utilisé par défaut.

Pour ajouter encore une interface pour la connexion, cliquez sur  et spécifiez les valeurs des champs ajoutés.

Pour interdire la connexion via une interface spécifiée avant, supprimez-la de la liste en cliquant sur  contre la ligne portant cette adresse.

4. Cliquez sur **Enregistrer**.



L'utilisation de la version de console de l'utilitaire du diagnostic distant du Serveur Dr.Web est décrite en détails dans les **Annexes**, [H7.3. Utilitaire du diagnostic distant du Serveur Dr.Web](#).

10.5. Configuration de l'agent SNMP Dr.Web

L'agent SNMP est conçu pour l'intégration de Dr.Web Enterprise Security Suite avec les systèmes de gestion réseau via le protocole SNMP. Une telle intégration permet de surveiller le fonctionnement des composants Dr.Web et collecter les statistiques de détection et de neutralisation de menaces.

Les systèmes de surveillance ou tous les gestionnaires SNMP peuvent s'adresser au Serveur Dr.Web qui fournit les informations nécessaires via l'extension de l'agent SNMP Dr.Web.



Pour consulter les informations qui peuvent être fournies par l'agent SNMP Dr.Web, vous pouvez utiliser MIB fourni avec le Serveur Dr.Web. Le fichier `DRWEB-ESUITE-STAT-MIB.txt` se trouve dans le sous-répertoire `etc` du répertoire d'installation du Serveur Dr.Web.




Pour autoriser le Serveur à échanger les informations avec les systèmes de gestion réseau via le protocole SNMP, il est nécessaire d'activer l'extension de l'agent SNMP Dr.Web. Pour ce faire, cochez la case **Extension de l'agent SNMP Dr.Web** dans l'onglet [Modules](#) de la section **Configuration du Serveur Dr.Web**.


Pour configurer les paramètres de connexion à l'agent SNMP Dr.Web

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion. Dans la fenêtre qui s'ouvre, sélectionnez l'élément **Configuration de l'agent SNMP Dr.Web** du menu de gestion.
2. Dans le champ **Communauté**, spécifiez le nom de la communauté SNMPv2c. Par défaut, c'est **public**.
3. Spécifiez les paramètres de l'interface pour la connexion des systèmes de gestion réseau :



- **Interface** : adresse IP écoutée du côté du Serveur Dr.Web pour les connexions entrantes des systèmes de gestion réseau.
- **Port** : port écouté du côté du Serveur Dr.Web pour les connexions entrantes des systèmes de gestion réseau.

Pour ajouter encore une interface pour la connexion, cliquez sur  et spécifiez les valeurs des champs ajoutés.

Pour interdire la connexion via une interface spécifiée avant, supprimez-la de la liste en cliquant sur  contre la ligne portant cette adresse.

4. Cochez la case **Autoriser l'accès depuis les réseaux locaux uniquement** pour autoriser la connexion à l'agent SNMP Dr.Web uniquement depuis les réseaux locaux.


Dans ce cas, remplissez la **Liste des adresses locales** depuis lesquelles la connexion des systèmes de gestion réseau à l'agent SNMP Dr.Web est autorisée.


5. Cliquez sur **Enregistrer**.

10.6. Configuration de la planification du Serveur Dr.Web

Pour configurer la planification du Serveur Dr.Web, effectuez les actions suivantes


1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion. Dans la fenêtre qui s'affiche, sélectionnez l'élément du menu de gestion **Planification des tâches du Serveur Dr.Web**. La liste des tâches du Serveur Dr.Web va s'ouvrir.
2. Pour gérer la planification, utilisez les éléments correspondants dans la barre d'outils :
 - a) Les éléments généraux de la barre d'outils sont utilisés pour créer de nouvelles tâches et gérer la rubrique planification dans son ensemble. Ces éléments sont toujours disponibles dans la barre d'outils.

 **Ajouter les tâches par défaut** : ajouter dans la planification actuelle toutes les tâches de la planification par défaut. Dans ce cas, toutes les tâches actuelles sont enregistrées dans la liste et toutes les tâches de la planification par défaut sont ajoutées. Les tâches de la planification par défaut sont ajoutées dans tous les cas, même si la planification actuelle contient déjà ces tâches (dans leur état initial ou modifié), y compris, les cas où la planification actuelle est identique à la planification par défaut.

 **Spécifier la planification par défaut** : supprimer toutes les tâches de la planification actuelle et spécifier la planification de tâches par défaut.




Planification par défaut : liste des tâches créées lors de l'installation initiale du Serveur Dr.Web. Cette planification ne peut pas être modifiée.

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

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









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






L'importation de la liste de tâches pour le Serveur Dr.Web dans le Planificateur de tâches des postes ou vice versa n'est pas autorisée.

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

Configuration		Action
 Type de lancement	Synchrone	Spécifier le lancement synchrone pour toutes les tâches marquées ci-dessous. La tâche avec une périodicité spécifiée sera placée dans la file d'attente commune des tâches du Planificateur. Les tâches dans cette file d'attente sont exécutées à tour de rôles.
	Asynchrone	Spécifier le lancement asynchrone pour toutes les tâches marquées ci-dessous. La tâche avec une périodicité spécifiée sera exécutée en même temps que les autres tâches hors de la file d'attente.
 Statut	Autoriser l'exécution	Activer l'exécution des tâches sélectionnées selon leur planification, si elles étaient désactivées.
	Désactiver l'exécution	Bloquer l'exécution des tâches sélectionnées. Les tâches restent dans la liste mais ne seront pas exécutées.
 Vous pouvez spécifier le même paramètre dans l'éditeur de tâches dans l'onglet Général en cochant la case Autoriser l'exécution .		
 Importance	Définir comme critique	Effectuer un lancement supplémentaire de la tâche, si l'exécution planifiée de cette tâche a été omise.
	Définir comme non critique	Exécuter la tâche uniquement au moment où elle planifiée indépendamment du fait que le lancement de la tâche ait été omis ou pas.
 Vous pouvez spécifier le même paramètre dans l'éditeur de tâches dans l'onglet Général en cochant la case Tâche critique .		
 Dupliquer des paramètres	Permet de dupliquer des tâches sélectionnées dans la liste des planifications actuelles. Lorsque vous activez l'option Dupliquer des paramètres , les nouvelles tâches créées possèdent des paramètres identiques à ceux des tâches sélectionnées.	




Configuration	Action
 Planifier à plusieurs reprises	Pour les tâches qui ne sont exécutées qu'une fois : exécuter la tâche de nouveau selon les horaires configurés (la modification de la répétition d'exécution d'une tâche est décrite ci-dessous, dans la rubrique Éditeur de tâches).
 Supprimer les tâches sélectionnée	Supprimer la tâche sélectionnée de la planification.
 Exécuter la tâche	Exécuter tout de suite les tâches sélectionnées dans la liste. Dans ce cas, la tâche sera lancée même si son exécution selon la planification est interdite.

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

Éditeur de Tâches

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

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

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



Les valeurs des champs marqués par le symbole * doivent être obligatoirement spécifiées.

Pour modifier les paramètres d'une tâche

1. Dans l'onglet **Général**, configurez les paramètres suivants :
 - Spécifiez le nom de la tâche à afficher dans le champ **Nom**.
 - Cochez la case **Activer l'exécution** pour activer l'exécution d'une tâche. Si la case n'est pas cochée, la tâche reste dans la liste mais elle ne sera pas exécutée.



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




- Cochez la case **Tâche critique** pour effectuer un lancement supplémentaire de la tâche si l'exécution planifiée de cette tâche à l'heure prévue a été omise. Le Planificateur parcourt la liste des tâches à chaque minute et s'il détecte une tâche critique omise, il la lance. Si au moment de lancement, une tâche a été omise plusieurs fois, elle sera exécutée seulement une fois.




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


- Si la case Lancer la tâche de manière asynchrone est décochée, la tâche sera placée dans la file d'attente des tâches du Planificateur exécutées successivement. Cochez la case pour exécuter cette tâche simultanément hors de la file d'attente.
2. Dans l'onglet **Action**, dans la liste déroulante **Action**, sélectionnez le type de tâche et configurez les paramètres nécessaires à son exécution :

Type de tâche	Paramètres et description
	<p>Le Serveur Dr.Web est en cours d'arrêt</p> <p>La tâche consiste à fermer le Serveur Dr.Web.</p> <p>Aucun paramètre supplémentaire n'est requis pour exécuter la tâche.</p>
	<p>Copie de sauvegarde des données critiques du Serveur</p> <p>La tâche consiste à sauvegarder les données critiques suivantes du Serveur Dr.Web :</p> <ul style="list-style-type: none">• base de données,• fichier clé de licence,• clé privée de chiffrement. <p>Indiquez les paramètres suivants :</p> <ul style="list-style-type: none">• Chemin : chemin vers le répertoire dans lequel les données seront sauvegardées (un champ vide signifie que le répertoire par défaut sera utilisé).• Nombre maximum de copies : nombre maximum de copies de sauvegarde (la valeur 0 indique qu'il n'y a pas de limitation). <p>Pour en savoir plus, voir le document Annexes, p. Annexe G3.5.</p> <div style="background-color: #fff9c4; padding: 10px; border: 1px solid #ccc;"><p> Le répertoire de copie de sauvegarde doit être vide. Sinon, le contenu du répertoire sera supprimé lors de la copie de sauvegarde.</p></div>
	<p>Création d'un rapport statistique</p> <p>La tâche consiste à créer un rapport avec les statistiques sur le réseau antivirus.</p>




Type de tâche	Paramètres et description
	<p>Pour pouvoir créer un rapport, il est obligatoire d'activer la notification Rapport statistique (voir Configuration des notifications) dans un des profils de notification actif. Le rapport généré est sauvegardé sur l'ordinateur sur lequel le Serveur Dr.Web est installé. Le type de l'obtention du rapport dépend du type de notification :</p> <ul style="list-style-type: none">• Pour envoyer des messages E-mail : un message avec le rapport en pièce jointe ainsi que le lien vers l'emplacement du rapport sont envoyés sur l'adresse e-mail indiquée dans les paramètres des notifications.• Pour toute autre méthode de fourniture : envoi d'une notification avec un lien vers l'emplacement du rapport. <p>Pour créer une tâche dans le planificateur, vous devez configurer les paramètres suivants :</p> <ul style="list-style-type: none">• Langue du rapport : langue des données dans le rapport.• Format de la date : format d'affichage des données statistiques contenant des dates. Les formats suivants sont disponibles :<ul style="list-style-type: none">▫ européen : JJ-MM-AAAA HH:MM:SS▫ américain : MM/JJ/AAAA HH:MM:SS• Format du rapport : format du document de sauvegarde des rapports statistiques.• Période du rapport : période pour laquelle les données statistiques seront intégrées au rapport.• Groupes : liste des groupes des postes du réseau antivirus dont les données seront intégrées au rapport. Pour sélectionner plusieurs groupes, utilisez les touches CTRL ou SHIFT.• Tableaux de rapports : liste des tableaux statistiques dont les données seront intégrées au rapport. Pour sélectionner plusieurs tableaux, utilisez les touches CTRL ou SHIFT.• Délai de conservation du rapport : délai de conservation du rapport sur l'ordinateur avec le Serveur Dr.Web installé, du moment de la génération du rapport.
Lancer un programme	<p>La tâche consiste à lancer un programme personnalisé.</p> <div data-bbox="448 1688 1437 1809"> Les programmes lancés dans le cadre de cette tâche sont exécutés en tâche de fond.</div> <p>Indiquez les paramètres suivants :</p> <ul style="list-style-type: none">• Champ Chemin : nom complet (avec le chemin) du fichier exécutable du programme qui doit être lancé.



Type de tâche	Paramètres et description
	<ul style="list-style-type: none">• Dans le champ Arguments : paramètres de la ligne de commande pour le programme à lancer.• Cochez la case Attendre la fin du programme pour attendre la fin du programme lancé par cette tâche. Dans ce cas, le Serveur Dr.Web enregistre le lancement du programme, le code de retour et l'heure de la fin du programme. Si la case Attendre la fin du programme est décochée, la tâche est considérée comme achevée dès le lancement du programme et le Serveur Dr.Web n'enregistre que le lancement du programme.
	<p>Envoi du message sur le poste</p> <p>La tâche consiste à envoyer un message aux utilisateurs du poste ou du groupe de postes.</p> <p>Vous pouvez consulter les paramètres dans la rubrique Envoi de messages aux postes.</p>
	<p>Exécution du script</p> <p>La tâche consiste à exécuter le script Lua indiqué dans le champ Script.</p> <div style="background-color: #fff9c4; padding: 10px;"><p> L'exécution simultanée de plusieurs tâches de type Exécuter le script sur plusieurs Serveurs Dr.Web utilisant une seule base de données peut entraîner des erreurs.</p><hr/><p>Lors de l'exécution des scripts Lua, l'administrateur obtient l'accès à tout le système de fichiers à l'intérieur du répertoire du Serveur Dr.Web et aux certaines commandes sur l'ordinateur avec le Serveur Dr.Web installé.</p><p>Pour interdire l'accès à la planification, désactivez le droit Éditer la planification du Serveur Dr.Web pour l'administrateur correspondant (voir le p. Administrateurs et groupes administrateur).</p></div>
	<p>Expiration de la clé de licence</p> <p>La tâche consiste à générer des rappels sur l'expiration de la licence du produit Dr.Web.</p> <p>Vous devez indiquer la période précédant l'expiration de la licence à partir de laquelle les rappels seront générés.</p>
	<p>Écrire dans le fichier de journal</p>




Type de tâche	Paramètres et description
	<p>La tâche consiste à écrire la ligne spécifiée dans le fichier de rapport du Serveur Dr.Web.</p> <p>Ligne : texte du message enregistré dans le fichier de rapport.</p>
	<p>Le poste n'a pas été connecté depuis longtemps</p> <p>La tâche consiste à envoyer une notifications lorsque les postes n'ont pas été connectés au Serveur actuel Dr.Web depuis longtemps.</p> <p>L'affichage de notification peut être paramétré dans la section Configuration des notifications à l'aide de l'élément Le poste n'a pas été connecté au serveur depuis longtemps.</p> <p>Dans le champ Jours, indiquez un délai après lequel le poste sera considéré comme non connecté depuis longtemps.</p>
	<p>Le Serveur voisin Dr.Web n'a pas été connecté depuis longtemps</p> <p>La tâche consiste à envoyer une notifications lorsque les Serveurs voisins Dr.Web n'ont pas été connectés au Serveur actuel Dr.Web depuis longtemps.</p> <p>L'affichage des notifications peut être paramétré dans la rubrique Configuration des notifications en utilisant l'onglet Le serveur voisin n'a pas été connecté depuis longtemps.</p> <p>Indiquez les valeurs appropriées dans les champs Heures et Minutes pour définir le moment où le Serveur voisin Dr.Web sera considéré comme non connecté depuis longtemps.</p>
	<p>Les licences disponibles seront bientôt épuisées</p> <p>La tâche est destinée à envoyer la notification Le nombre de postes dans le groupe va atteindre la limite de licence si le nombre de licences par toutes les clés assignées aux groupes de postes va bientôt expirer.</p> <div style="background-color: #e6f2e6; padding: 10px; border: 1px solid #ccc;"><p> Les clés de licence assignées aux groupes sélectionnés peuvent également être assignées aux autres objets de la licence.</p></div> <p>Indiquez les paramètres suivants :</p> <ul style="list-style-type: none">• Nombre des licences disponibles : nombre maximum des licences restantes dans les clés de licence assignées aux groupes sélectionnés. Une fois ce nombre atteint, une notification sera envoyée à l'administrateur.• Taux de licences disponibles : taux maximum des licences restantes dans les clés de licence assignées aux groupes sélectionnés. Une fois ce taux atteint, une




Type de tâche	Paramètres et description
	<p>notification sera envoyée à l'administrateur</p> <ul style="list-style-type: none">• Groupes : liste des groupes dont le nombre de licences restants sera vérifié. Pour sélectionner plusieurs groupes, utilisez les touches CTRL ou SHIFT.
	<p>Mettre à jour le référentiel</p> <p>La tâche consiste à lancer les mises à jour des produits du référentiel depuis le SGM.</p> <p>Indiquez les paramètres suivants :</p> <ul style="list-style-type: none">• Dans la liste Produit, cochez les cases près des produits du référentiel à mettre à jour via cette tâche.• Cochez la case Mettre à jour les clés de licence pour activer la procédure de la mise à jour automatique des clés de licence lors de la mise à jour du référentiel. Pour plus d'informations, consultez la rubrique Mise à jour automatique de licences.
	<p>Nettoyer la base de données</p> <p>La tâche consiste à recueillir et supprimer les enregistrements non utilisés dans la base de données du Serveur Dr.Web en utilisant la commande <code>vacuum</code>.</p> <p>Aucun paramètre supplémentaire n'est requis pour exécuter la tâche.</p>
	<p>Redémarrage du Serveur Dr.Web</p> <p>La tâche consiste à redémarrer le Serveur Dr.Web.</p> <p>Aucun paramètre supplémentaire n'est requis pour exécuter la tâche.</p>
	<p>Remplacer la clé de chiffrement</p> <p>La tâche consiste à remplacer périodiquement les outils suivants assurant le chiffrement entre les composants :</p> <ul style="list-style-type: none">• la clé privée <code>drwcsd.pri</code> sur le Serveur Dr.Web,• la clé publique <code>*.pub</code> sur les postes de travail,• le certificat <code>drwcsd-certificate.pem</code> sur les postes de travail. <p>Sachant que les postes peuvent être éteints au moment du remplacement, la procédure est divisée en deux étapes. Vous devez créer deux tâches pour exécuter chacune de ces étapes, il est recommandé d'effectuer la seconde étape après la première, lorsque certains postes seront probablement connectés au Serveur Dr.Web.</p>



Type de tâche	Paramètres et description
	<p>Lors de la création d'une tâche, choisissez l'étape correspondant dans la liste déroulante :</p> <ul style="list-style-type: none">• Ajouter une nouvelle clé : première étape de la procédure lorsque une nouvelle paire de clés de chiffrement inactive et un certificat sont créés. Les postes obtiennent une nouvelle clé publique et un certificat au moment de la connexion au Serveur Dr.Web.• Supprimer l'ancienne clé et passer à la nouvelle : la seconde étape quand les postes sont informés du passage aux nouvelles clés de chiffrement et au nouveau certificat, suivi du remplacement des outils existants par des nouveaux : les clés publiques et le certificat sur les postes et la clé privée sur le Serveur Dr.Web. <p>Les postes qui n'ont pas reçu de nouvelles clés et de nouveau certificat ne pourront pas se connecter au Serveur Dr.Web. Pour résoudre ce problème, il faut installer manuellement la nouvelle clé publique et le nouveau certificat sur les postes (vous pouvez consulter la procédure de remplacement de la clé sur le poste dans les Annexes, la rubrique Connexion de l'Agent Dr.Web à un autre Serveur).</p>
	<h3>Réveiller les postes</h3> <p>La tâche consiste à réveiller les postes qui sont en veille, par exemple avant de lancer un scan.</p> <p>Les paramètres suivants définissent quels postes seront activés :</p> <ul style="list-style-type: none">• Réveiller tous les postes : réveiller tous les postes connectés au Serveur Dr.Web.• Réveiller les postes en fonction des paramètres indiqués : seuls les postes possédant les paramètres suivants seront réveillés :<ul style="list-style-type: none">▫ Adresses IP : la liste des adresses IP des postes à activer. La liste est spécifiée au format suivant : 10.3.0.127, 10.4.0.1-10.4.0.5, 10.5.0.1/30. Lors de la création d'une liste, utilisez la virgule ou le saut de ligne pour séparer les différentes adresses. Vous pouvez également utiliser les noms DNS des postes au lieu de leurs adresses IP.▫ Adresses MAC : la liste des adresses MAC des postes à activer. Les octets des adresses-MAC doivent être séparés par le symbole ':'. Utilisez la virgule ou le saut de ligne pour séparer plusieurs adresses.▫ Groupes : liste des groupes dont il faut activer les postes. Pour modifier la liste de groupes, cliquez sur le bouton Éditer (ou sur les identificateurs de groupes si les groupes sont déjà spécifiés) et sélectionnez les groupes nécessaires dans la fenêtre qui s'ouvre. Pour sélectionner plusieurs groupes, utilisez les touches CTRL ou SHIFT. <div data-bbox="448 1771 1437 1989" style="background-color: #fff9c4; padding: 10px;"><p> Pour lancer cette tâche, tous les postes qui seront activés doivent être équipés de cartes réseau supportant Wake-on-LAN.</p><p>Pour vérifier si votre carte réseau supporte Wake-on-LAN, consultez sa documentation ou ses propriétés (Panneau de configuration →</p></div>





Type de tâche	Paramètres et description
	<p style="text-align: center;">Internet et Réseau → Connexions Réseau → Modifier les paramètres de connexion → Configurer → Avancé, spécifiez Valeur → Activé pour la propriété Paquet magique Wake on).</p>
	<h3>Sauvegarder le référentiel</h3> <p>La tâche consiste à effectuer des sauvegarde régulières du référentiel.</p> <p>Indiquez les paramètres suivants :</p> <ul style="list-style-type: none">• Chemin : chemin complet vers le répertoire dans lequel la copie de sauvegarde sera stockée.• Nombre maximum de copies : nombre maximum de copies de sauvegarde du référentiel sauvegardés dans le répertoire spécifié. Si le nombre maximum de copies est atteint, la copie la plus ancienne sera effacée pour pouvoir sauvegarde la nouvelle.• Zone du référentiel indique quelles informations sur un composant antivirus seront sauvegardées :<ul style="list-style-type: none">▫ Référentiel entier : sauvegarder toutes les révisions du référentiel pour les composants sélectionnés dans la liste ci-dessous.▫ Révisions critiques seulement : seules les révisions marquées comme importantes seront sauvegardées pour les composants sélectionnés dans la liste ci-dessous.▫ Fichiers de configuration seulement : seuls les fichiers de configuration seront sauvegardés pour les composants choisis dans la liste.• Cochez les cases près des zones que vous souhaitez sauvegarder pour les composants. <div style="background-color: #fff9c4; padding: 10px; margin-top: 10px;"> Le répertoire de copie de sauvegarde doit être vide. Sinon, le contenu du répertoire sera supprimé lors de la copie de sauvegarde.</div>
	<h3>Supprimer les enregistrements obsolètes</h3> <p>La tâche consiste à supprimer les informations obsolètes de la base de données. Vous pouvez consulter les types des entrées supprimées dans les paramètres de la tâche.</p> <p>Vous devez indiquer le nombre de jours après lequel les entrées statistiques dans la base de données sont considérées comme obsolètes et supprimées du Serveur Dr.Web.</p> <p>Le délai de suppression de données doit être spécifié séparément pour chaque type d'entrée.</p>




Type de tâche	Paramètres et description
	<p>Supprimer les événements non envoyés</p> <p>La tâche consiste à supprimer les événements non envoyés de la base de données.</p> <p>Vous devez indiquer un délai de stockage des événements non envoyés après lequel ils seront supprimés.</p> <p>Cette tâche fait référence aux événements qu'un Serveur Dr.Web secondaire envoie à un Serveur principal Dr.Web. Si l'envoi d'un message échoue, il est déplacé vers la liste des messages non envoyés. Le Serveur secondaire Dr.Web continue ses tentatives d'envoi du message selon l'intervalle spécifié. Lorsque la tâche Supprimer les événements non envoyés est lancée, les événements seront supprimés si leur durée de stockage a été atteinte ou dépassée.</p>
	<p>Suppression des messages périmés</p> <p>La tâche consiste à supprimer les messages suivants de la base de données :</p> <ul style="list-style-type: none">• notifications de l'agent,• notifications pour la console web,• rapports créés d'après la planification. <p>La tâche permet également de supprimer les messages marqués comme obsolètes, c'est-à-dire dont la période de conservation a expiré. Vous pouvez spécifier la période de conservation :</p> <ul style="list-style-type: none">• pour les notifications : via la méthode d'envoi appropriée durant la création d'une notification (voir Configuration des notifications).• pour les rapports : dans la tâche de création de rapports. <p>Aucun paramètre supplémentaire n'est requis pour exécuter la tâche.</p>
	<p>Supprimer les postes non activés</p> <p>Indiquez la période après laquelle les comptes non utilisés seront supprimés.</p> <p>Vous pouvez consulter la liste des comptes non utilisés dans l'arborescence du réseau antivirus, dans le groupe Status → New (pour en savoir plus, consultez la rubrique Politique d'approbation des postes).</p>
	<p>Supprimer les anciens postes</p> <p>La tâche consiste à supprimer les postes obsolètes.</p> <p>Il faut indiquer le délai (par défaut, c'est 90 jours) pendant lequel les postes qui n'ont pas visité le Serveur Dr.Web sont considérés comme obsolètes et ils sont</p>



Type de tâche	Paramètres et description
	<p>déplacés dans le groupe Deleted du réseau antivirus. Les postes seront définitivement supprimés de la base de données du Serveur Dr.Web lors de l'exécution de la tâche Suppression des entrées obsolètes (le délai de suppression des postes du groupe Deleted est spécifié dans les paramètres de la tâche Suppression des entrées obsolètes pour le type Postes supprimés et commence au moment du déplacement dans le groupe Deleted).</p> <div data-bbox="264 546 1439 797" style="background-color: #e6f2e6; padding: 10px;"><p> L'information obsolète est supprimée de la base de données pour libérer de l'espace disque. Le délai par défaut indiqué dans les onglets Supprimer les enregistrements obsolètes et Supprimer les anciens postes est de 90 jours. Si vous réduisez ce délai, les statistiques sur le fonctionnement des composants du réseau antivirus seront moins représentatives. De plus, le Serveur Dr.Web pourrait avoir besoin de beaucoup plus de ressources.</p></div>
	<h3 data-bbox="264 869 735 902">Synchronisation avec Active Directory</h3> <p data-bbox="448 936 1382 1032">La tâche consiste à synchroniser les structures du réseau : les conteneurs Active Directory qui contiennent des ordinateurs deviennent des groupes du réseau antivirus dans lesquels les postes de travail sont placés.</p> <p data-bbox="448 1070 847 1104">Indiquez les paramètres suivants :</p> <ul data-bbox="448 1126 1318 1283" style="list-style-type: none">• Contrôleur Active Directory : contrôleur Active Directory, par exemple, <code>dc.example.com</code>.• Nom d'utilisateur : nom de l'utilisateur Active Directory.• Mot de passe : mot de passe de l'utilisateur Active Directory. <div data-bbox="448 1305 1439 1592" style="background-color: #e6f2e6; padding: 10px;"><p> Pour les Serveurs Dr.Web sous Windows, la configuration n'est pas obligatoire. On utilise en tant que les données d'enregistrement les identifiants de l'utilisateur au nom de qui le processus du Serveur Dr.Web (généralement LocalSystem) est lancé.</p><p>Pour les Serveurs Dr.Web sous les OS de la famille UNIX, les paramètres doivent être obligatoirement spécifiés.</p></div> <ul data-bbox="448 1619 1433 1921" style="list-style-type: none">• Dans la liste déroulante Protection de la connexion, sélectionnez le type de l'échange chiffrée de données :<ul data-bbox="488 1697 1433 1921" style="list-style-type: none">▫ STARTTLS : le passage à la connexion sécurisée s'effectue via la commande STARTTLS. L'utilisation du port 25 pour la connexion est prévue par défaut.▫ SSL/TLS : ouvrir une connexion sécurisée à part. L'utilisation du port 465 pour la connexion est prévue par défaut.▫ Non : ne pas utiliser le chiffrement. L'échange de données s'effectuera par la connexion non sécurisée.



Type de tâche	Paramètres et description
	<p> Cette tâche est désactivée par défaut. Pour activer l'exécution de cette tâche, activez l'option Autoriser l'exécution dans les paramètres de tâche ou dans la basse d'outils comme décrit ci-dessus.</p> <p>Une fois la tâche exécutée, la configuration des paramètres avancés de l'Office Control pour les utilisateurs et les groupes d'Active Directory devient disponible (Office Control -> Paramètres de groupes -> Paramètres d'accès -> Paramètres particuliers).</p>


3. Dans l'onglet **Heure**, spécifiez les paramètres suivants :

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

Mode de lancement	Paramètres et description
Fermeture	La tâche sera lancée à la fermeture du Serveur Dr.Web. Aucun paramètre supplémentaire n'est requis pour exécuter la tâche.
Démarrage	La tâche sera lancée au démarrage du Serveur Dr.Web. Aucun paramètre supplémentaire n'est requis pour exécuter la tâche.
Dans N minutes après la tâche initiale	Dans la liste déroulante Tâche initiale , sélectionnez la tâche par rapport à laquelle est spécifiée l'heure d'exécution de la tâche courante. Dans le champ Minute , indiquez ou choisissez dans la liste le nombre de minutes pour lancer l'exécution de la tâche éditée après l'exécution de la tâche initiale.
Chaque jour	Indiquez l'heure et les minutes — la tâche sera lancée chaque jour au moment spécifié.
Chaque mois	Choisissez la date (jour du mois) et indiquez l'heure et les minutes — la tâche sera lancée au jour spécifié au moment indiqué.
Chaque semaine	Choisissez le jour de la semaine et indiquez l'heure et les minutes — la tâche sera lancée au jour de la semaine spécifié au moment indiqué.
Chaque heure	Indiquez un chiffre entre 0 et 59 pour paramétrer la minute à laquelle sera lancée la tâche dans une heure.
Chaque N minutes	La valeur N doit être indiquée pour paramétrer l'intervalle entre l'exécution des tâches. Si N est égal à 60 ou plus, la tâche sera lancée chaque N minutes. Si N est inférieur à 60, la tâche sera lancée chaque minute de l'heure multiple de N .



- Cochez la case **Interdire après la première exécution** pour exécuter la tâche une seule fois conformément à la périodicité spécifiée. Si la case n'est pas cochée, la tâche sera exécutée plusieurs fois selon la périodicité indiquée.

Pour répéter le lancement d'une tâche déjà exécutée, utilisez le bouton  **Planifier à plusieurs reprises** dans la barre d'outils de la section Planification.

4. Lorsque tous les paramètres sont indiqués pour une tâche, cliquez sur **Sauvegarder** pour appliquer les modifications des paramètres modifiés si vous avez modifié une tâche existante, ou pour créer une nouvelle tâche avec les paramètres spécifiés si vous avez créé une nouvelle tâche.

Les résultats d'exécution des tâches sont enregistrés dans la section **Administration** → **Journal d'exécution des tâches**

10.7. Configuration du Serveur web



A chaque enregistrement des modifications de la section **Configuration du serveur web**, une copie de sauvegarde de la version précédente du fichier de configuration du serveur web est automatiquement enregistrée. 10 dernières copies sont sauvegardées.

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

```
webmin.conf_<date_et_heure_de_création>
```



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

Pour configurer les paramètres du Serveur Web

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion.
2. Cliquez sur **Configuration du Serveur Web** dans le menu de gestion. Une fenêtre permettant de configurer le Serveur Web va s'ouvrir.




Les valeurs des champs marqués par le symbole * doivent être obligatoirement spécifiées.

3. Les boutons suivants de gestion des paramètres sont disponibles dans la barre d'outils :
 -  **Redémarrer le Serveur Dr.Web** : redémarrer le Serveur Dr.Web pour appliquer les modifications apportées dans cette rubrique. Le bouton est activé après la modification des paramètres de la rubrique et l'appui sur le bouton **Enregistrer**.
 -  **Restaurer la configuration de la copie de sauvegarde** : liste déroulante contenant les copies de sauvegarde des paramètres de la rubrique entière que l'on peut restaurer après les modifications apportées. Le bouton est activé après la modification des paramètres de la rubrique et l'appui sur le bouton **Sauvegarder**.



 **Restaurer tous les paramètres à leur valeur initiale** : restaurer les valeurs données à tous les paramètres de cette rubrique avant modification (dernières valeurs sauvegardées).

 **Restaurer tous les paramètres à leur valeur par défaut** : restaurer les valeurs par défaut de tous les paramètres de la rubrique.

4. Pour appliquer les paramètres apportées dans les paramètres de la rubrique, cliquez sur **Sauvegarder**. Ensuite, le redémarrage du Serveur Dr.Web est requis. Pour ce faire, cliquez sur le bouton  **Redémarrer le Serveur Dr.Web** dans la barre d'outils de cette rubrique.

10.7.1. Général

Dans l'onglet **Général**, indiquez les paramètres du Serveur Web :

- **Adresse du Serveur Dr.Web** : adresse IP ou nom DNS du Serveur Dr.Web.

Spécifié au format suivant :

Adresse IP ou nom DNS du Serveur Dr.Web > [: <port >]

Si l'adresse du Serveur Dr.Web n'est pas spécifiée, le nom de l'ordinateur retourné par le système d'exploitation ou l'adresse réseau du Serveur Dr.Web : nom de domaine, si disponible, sinon l'adresse IP, sont utilisés.



Il est recommandé d'utiliser le nom du Serveur Dr.Web au [format FQDN](#) en tant qu'adresse du Serveur Dr.Web.

Si le numéro de port n'est pas indiqué, le port spécifié dans la requête est utilisé (par exemple, lors de l'accès au Serveur Dr.Web depuis le Centre de gestion ou via **Web API**). Notez que pour les requêtes depuis le Centre de gestion, c'est le port indiqué dans la ligne d'adresse lors de la connexion du Centre de gestion au Serveur Dr.Web.

- **Nombre de requêtes parallèles des clients** : nombre de requêtes parallèles traitées par le Serveur Web. Ce paramètre affecte les performances du serveur. Il n'est pas recommandé de modifier ce paramètre sans nécessité.
- **Nombre de flux d'entrée/sortie** : nombre de flux traitant les données transmises via le réseau. Ce paramètre affecte les performances du Serveur Dr.Web. Il n'est pas recommandé de modifier ce paramètre sans nécessité.
- **Délai de la session via HTTP/1 (s)** : délai de la session pour le protocole HTTP en version 1. En cas d'utilisation des connexions permanentes, le Serveur Dr.Web interrompt la connexion si, pendant le délai spécifié, il n'y a aucune demande client. Le délai est valable avant l'échange des données au cours de la session.
- **Vitesse minimale de l'envoi via HTTP/1 (O/s)** : vitesse minimum de l'envoi des données via le protocole HTTP en version 1. Si la vitesse entrante de transfert est inférieure à cette valeur, la connexion sera rejetée. Indiquez la valeur 0 pour enlever cette limitation.
- **Vitesse minimale de réception via HTTP/1 (O/s)** : vitesse minimum de la réception des données via le protocole HTTP en version 1. Si la vitesse entrante de transfert est inférieure à cette valeur, la connexion sera rejetée. Indiquez la valeur 0 pour enlever cette limite.



- **Délai d'envoi via HTTP/1 (s)** : délai d'envoi des données via le protocole HTTP en version 1 au cours d'une session ouverte. Si vous n'arrivez pas à envoyer les données pendant le délai indiqué, la session se ferme.
- **Délai de réception via HTTP/1 (s)** : délai de réception des données via le protocole HTTP en version 1 au cours de la session ouverte. Si, pendant le délai spécifié, il n'y a aucune demande client, la session se ferme. Le délai est valable après le début de l'échange des données au cours de la session.
- **Taille du tampon d'envoi (Ko)** : la taille des mémoires tampon utilisées pour envoyer des données. Ce paramètre affecte les performances du Serveur Dr.Web. Il n'est pas recommandé de le modifier sans nécessité.
- **Taille du tampon d'envoi (Ko)** : la taille des mémoires tampon utilisées pour recevoir des données. Ce paramètre affecte les performances du Serveur Dr.Web. Il n'est pas recommandé de le modifier sans nécessité.
- **Longueur maximum de la requête (Ko)** : taille autorisée maximum pour une requête HTTP.
- **Activer la protection contre les attaques flood** : cochez la case pour prendre les mesures de protection contre les attaques flood. Spécifiez les paramètres suivants de détection d'une attaque :
 - **Période (s)** : période de temps en secondes pendant laquelle un certain nombre de requêtes doit être reçu pour prouver l'attaque flood de la part de client.
 - **Nombre de requêtes** : nombre minimum de requêtes qui doivent être reçues pendant une certaine période de temps pour prouver l'attaque flood de la part de client.
 - **Durée de blocage (s)** : les connexions avec le client seront interdites pendant le nombre de secondes spécifié.

Dans la section **Compression**, sont spécifiés les paramètres de la compression du trafic pour la transfert de données au Serveur Web via HTTP/HTTPS :

- **Taille maximum des réponses à compresser (Ko)** : taille maximum des réponses HTTP qui seront compressées. Indiquez 0 pour désactiver la restriction de taille maximum de réponses HTTP à compresser.
- **Taille minimum d'une réponse à compresser (o)** : taille minimum des réponses HTTP qui seront compressées. Indiquez 0 pour désactiver la restriction de la taille minimum de réponses HTTP à compresser.
- **Ordre d'utilisation des types de compression** :
 - **Déterminé par le client** : l'ordre d'utilisation des types de compression est déterminé par le client en fonction des types de compression autorisés.
 - **Déterminé par le serveur** : l'ordre d'utilisation des types de compression est déterminé par le serveur en fonction des types de compression autorisés. Dans ce cas, spécifiez l'ordre des types de compression dans la liste ci-dessous. Pour modifier l'ordre, glissez-déposez le bloc correspondant par le ruban.

Vous pouvez activer ou désactiver (ainsi que spécifier l'ordre si l'ordre est déterminé par le Serveur Dr.Web) les types de compression suivants :



- **Utiliser la compression GZIP** : cochez la case pour utiliser ce type de compression. Dans le champ **Niveau de compression GZIP**, spécifiez une valeur dans la plage de 0 à 9. La valeur 0 désactive la compression.
- **Utiliser la compression Deflate** : cochez la case pour utiliser ce type de compression. Dans le champ **Niveau de compression Deflate**, spécifiez une valeur dans la plage de 0 à 9. La valeur 0 désactive la compression.
- **Utiliser la compression Brotli** : cochez la case pour utiliser ce type de compression. Dans le champ **Niveau de compression Brotli**, spécifiez une valeur dans la plage de 0 à 11. La valeur 0 désactive la compression.
- **Remplacer les adresses IP** : cochez la case pour remplacer les adresses IP par les noms d'ordinateurs dans le fichier de journal du Serveur Dr.Web.
- **Activer le support HTTP/2** : cochez la case pour supporter la connexion au serveur web via le protocole HTTP en version 2.
 - **Délai de la session via HTTP/2 (s)** : délai de la session pour le protocole HTTP en version 2. En cas d'utilisation des connexions permanentes, le serveur interrompt la connexion si pendant le délai spécifié il n'y a aucune demande client.
- **Maintenir la session TLS active** : cochez la case pour utiliser une connexion permanente pour TLS. Les anciennes versions de navigateurs peuvent ne pas fonctionner correctement avec des connexions TLS permanentes. Désactivez cette option si vous avez des problèmes de fonctionnement via le protocole TLS.
- **Certificat** : chemin vers le fichier du certificat TLS. Dans la liste déroulante sont présentés les certificats disponibles du répertoire du Serveur Dr.Web.
- **Clé privée SSL** : chemin vers le fichier de la clé privée TLS. Dans la liste déroulante sont présentées les clés privées TLS disponibles du répertoire du Serveur Dr.Web.
- **Clé de chiffrement pour les tickets de session TLS** : chemin vers le fichier de la clé de chiffrement pour les tickets de sessions TLS. Utilisé pour reprendre la séance TLS à la base des tickets de sessions qui sont chiffrés avec la clé spécifiée.
- **Liste de chiffrements autorisés** : ligne déterminant la liste de chiffrements du package OpenSSL autorisés à être utilisés dans les connexions aux clients. Si vous laissez le champ vide, la valeur `DEFAULT` sera utilisée ce qui signifie `ALL:!EXPORT:!LOW:!aNULL:!eNULL:!SSLv2`.

10.7.2. Avancé

A l'onglet **Avancé**, indiquez les paramètres du Serveur Web suivants :

- Cochez la case **Afficher les erreurs de script** pour afficher les erreurs de scripts dans le navigateur. Ce paramètre est utilisé par le support technique et les développeurs de la société Doctor Web. Il n'est pas recommandé de le modifier sans besoin.
- Cochez la case **Suivre les scripts** pour effectuer un tracing des scripts. Ce paramètre est utilisé par le support technique et les développeurs de la société Doctor Web. Il n'est pas recommandé de le modifier sans besoin.



- Cochez la case **Autoriser l'arrêt des scripts** pour annuler l'exécution des scripts. Ce paramètre est utilisé par le support technique et les développeurs de la société Doctor Web. Il n'est pas recommandé de le modifier sans besoin.
- En utilisant les champs dans la zone **En-têtes HTTP d'utilisateur**, vous pouvez ajouter vos propres en-têtes HTTP de la réponse du serveur Web avec les valeurs nécessaires. Le serveur Web utilise par défaut trois en-têtes de sécurité prédéfinis : `X-XSS-Protection`, `X-Content-Type-Options` et `X-Frame-Options`. Vous pouvez consulter et modifier leur valeurs via le fichier de configuration `webmin.conf` se trouvant dans le sous-répertoire `etc` du répertoire d'installation du Serveur Dr.Web.

10.7.3. Transport



Dans l'onglet **Transport**, sont configurées les adresses réseau « écoutées » depuis lesquelles le serveur web reçoit les connexions entrantes, par exemple, pour la connexion du Centre de gestion ou pour l'exécution des requêtes via Web API :

Dans la section **Adresses écoutées** est configurée la liste des interfaces qui seront écoutées pour recevoir des connexions via le protocole HTTP :

- **Adresse IP** : adresse IP de l'interface réseau depuis laquelle la réception des connexions est autorisée.
- **Port HTTP** : numéro de port de l'interface réseau depuis laquelle la réception des connexions via le protocole HTTP est autorisée.
- **Port HTTPS** : numéro de port de l'interface réseau depuis laquelle la réception des connexions via le protocole HTTPS est autorisée.

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

- **Adresse** : `0.0.0.0` : utiliser « toutes les interfaces réseau » pour cet ordinateur sur lequel le Serveur web est installé.
- **Port HTTP** : `9080` : utiliser le port standard `9080` pour le protocole HTTP.
- **Port HTTPS** : `9081` : utiliser le port standard `9081` pour le protocole HTTPS.

Pour ajouter une nouvelle ligne d'adresse, cliquez sur le bouton . Pour supprimer la ligne d'adresse, cliquez sur le bouton  contre l'adresse à supprimer.

10.7.4. Sécurité

A l'onglet **Sécurité**, vous pouvez paramétrer les restrictions pour les adresses réseau depuis lesquelles le Serveur Web reçoit les requêtes HTTP et HTTPS.

Général

- Cochez la case **Rediriger vers la connexion sécurisée** pour rediriger automatiquement toutes les connexions HTTP vers HTTPS.



- Cochez la case **Retourner l'en-tête détaillé** pour que le serveur web retourne les détails de l'environnement dans l'en-tête « Server ».
- Cochez la case **Convertir URI en minuscules** pour convertir en minuscules tous les URI dans les requêtes au serveur web. Seul le fragment de la partie hiérarchique de l'URI contenant le chemin est converti.
- Cochez la case **Activer le contrôle d'accès pour les applications clients** pour interdire l'accès de bots et d'autres applications clients mentionnées dans la liste ci-dessous à l'interface du Centre de gestion

Déterminez la liste des applications clients bloquées :

- Dans le champ **Nom de l'application client**, spécifiez le nom de l'application client à laquelle l'accès à l'interface du Centre de gestion sera bloqué. Sensible à la casse. Si le nom n'est pas spécifié, l'URI de l'application est utilisé
- Dans le champ **Expression régulière déterminante**, spécifiez l'expression régulière déterminant l'application à laquelle l'accès à l'interface du Centre de gestion sera bloqué.

Limitation d'accès

Pour configurer les limitations d'accès pour tout type de connexion

1. Pour autoriser l'accès via HTTP ou HTTPS depuis des adresses définies, ajoutez-les aux listes **HTTP: Autorisé** ou **HTTPS: Autorisé**.
2. Pour refuser l'accès via HTTP ou HTTPS depuis des adresses définies, ajoutez-les aux listes **HTTP: Refusé** ou **HTTPS: Refusé**.
3. Les adresses qui ne sont incluses dans aucune des listes sont autorisées ou refusées en fonction du statut des cases **Priorité de refus pour HTTP** et **Priorité de refus pour HTTPS** : si la case est cochée, les adresses qui ne sont incluses dans aucune des listes (ou incluses dans les deux listes) sont refusées. Sinon, ces adresses sont autorisées.

Pour éditer la liste des adresses

1. Entrez l'adresse réseau dans le champ correspondant et cliquez ensuite sur le bouton **Sauvegarder**.
2. L'adresse réseau doit être spécifiée au format suivant : *<adresse IP>* / [*<préfixe>*].



Les listes pour les adresses TCPv6 ne seront affichées que dans le cas où l'interface IPv6 est installée sur le poste.

3. Pour ajouter un nouveau champ d'adresse, cliquez sur le bouton **+** dans la rubrique correspondante.
4. Pour supprimer un champ, cliquez sur **-**.



Exemple d'utilisation du préfixe :

1. Le préfixe 24 désigne les réseaux ayant le masque : 255.255.255.0
Il contient 254 adresses.
Les adresses hôte dans les réseaux de ce type : 195.136.12.*
2. Le préfixe 8 désigne les réseaux ayant le masque 255.0.0.0
Il contient jusqu'à 16387064 adresses (256*256*256).
Les adresses d'hôtes dans les réseaux de ce type ont le format suivant : 125.*.*.*

10.7.5. Modules



Il n'est pas recommandé de modifier les paramètres de cette section sans indications du support technique.

Dans la section **Modules**, les scripts Lua sont configurés. Ils sont téléchargés au fur et à mesure de l'exécution des autres scripts de l'interface Web.

- La liste déroulante **Répertoire du script dans les chemins de recherche** détermine l'endroit de la liste de la section **Chemins** où il faut placer le répertoire actuel (le répertoire dans lequel se trouve le script exécuté en ce moment) :
 - **premier** — au début de la liste,
 - **dernier** — à la fin de la liste,
 - **ne pas utiliser** : ne pas ajouter du tout.
- La section **Masques** détermine plusieurs masques par lesquels les modules Lua sont détectés. On cherche les modules par les chemins indiqués dans la section **Chemin**.
- La section **Chemins** spécifie les chemins par lesquels on cherche les modules Lua de la section **Masques**. Les chemins sont spécifiés relativement au répertoire racine du serveur Web.

Exemple :

Le script se trouvant dans `var-root/webmin/esuite/include/head.ds` ne sera pas détecté sans spécification des paramètres supplémentaires dans la section **Modules**.

Les modules des répertoires `ds-modules` ou `webmin/vfs` seront détectés sans paramètres dans la section **Modules** car ce ne sont pas les modules globaux mais les modules de l'interface Web.



10.7.6. Gestionnaires



Il n'est pas recommandé de modifier les paramètres de cette section, sauf les sous-sections **Accès** et **Authentification** sans indications du support technique.

Dans la section **Gestionnaires** le mode et l'environnement du traitement de la requête reçue du client Web sont configurés.

Général

Les paramètres disponibles varient en fonction du type du gestionnaire.

Pour les sockets Web, le gestionnaire nécessaire est choisi en fonction de l'attribut **Protocole**.

Pour les autres types de gestionnaires, le gestionnaire nécessaire est choisi en fonction de l'attribut **Préfixe**.

Les types de gestionnaires utilisés sont sélectionnés dans la liste déroulante **Type** :

• Gestionnaires

Exécution du script indiqué qui reçoit le chemin d'URL en tant que paramètre. S'il n'y a pas de chemin, le chemin du champ **Répertoire** est transmis.

- **Préfixe** : préfixe des chemins dans l'URL de la requête HTTP.
- **Répertoire** : répertoire dans la racine du serveur Web par rapport auquel les chemins vers les fichiers transmis sont pris en compte.
- **Script** : gestionnaire script.

• Gestionnaires mixtes

En fonction du type de fichier demandé, il se comporte comme type **Fichiers statiques** ou comme type **Scripts**.

- **Préfixe** : préfixe des chemins dans l'URL de la requête HTTP.
- Liste des fichiers index. Détermine quels fichiers seront téléchargés et dans quel ordre si le client Web demande l'index du répertoire.
- **Script** : liste des extensions de fichiers qu'il faut considérer comme scripts Lua.

• Scripts

Un fichier demandé est exécuté comme script Lua.

- **Préfixe** : préfixe des chemins dans l'URL de la requête HTTP.
- **Répertoire** : répertoire dans la racine du serveur Web par rapport auquel les chemins vers les fichiers transmis sont pris en compte.



- **Fichiers statiques**

Le contenu de fichiers est transmis tel qu'il est.

- **Préfixe** : préfixe du chemins dans l'URL de la requête HTTP.
- **Répertoire** : répertoire dans la racine du serveur Web par rapport auquel les chemins vers les fichiers transmis sont pris en compte.
- Liste des fichiers index. Détermine quels fichiers seront téléchargés et dans quel ordre si le client Web demande l'index du répertoire.

- **Système de fichiers virtuel**

Équivalent de type **Fichiers statiques**. Seuls les fichiers sont téléchargés de l'archive au format intérieur `dar` indiquée dans le champ **Répertoire**.

- **Préfixe** : préfixe du chemins dans l'URL de la requête HTTP.
- **Répertoire** : répertoire dans la racine du serveur Web par rapport auquel les chemins vers les fichiers transmis sont pris en compte.

- **Sockets web prédéfinis**

L'application Websocket réalisée par la bibliothèque partagée fournie avec le serveur (`dll` ou `elf shared object`). Le nom du script correspond au protocole du socket Web, les fichiers sont placés dans `lib-root/websockets`.

- **Script d'authentification** : nom du fichier du script Lua qui authentifie l'utilisateur.
- **Protocole** : valeur du champ `WebSocket-Protocol` transmise dans la requête HTTP de connexion au socket Web.

- **Sockets web d'utilisateur**

L'application Websocket réalisée par le script Lua. Le nom du script correspond au protocole du socket Web, les fichiers sont placés dans `home-root/websockets`.

- **Script d'authentification** : nom du fichier du script Lua qui authentifie l'utilisateur.
- **Protocole** : valeur du champ `WebSocket-Protocol` transmise dans la requête HTTP de connexion au socket Web.

Accès

Les listes du contrôle d'accès (ALC) spécifient des limitations pour les adresses réseau depuis lesquelles les clients pourront accéder au Serveur Web.

Les paramètres sont équivalents aux [paramètres de sécurité du Serveur Dr.Web](#).

Si les paramètres ne sont pas spécifiés, on considère que toutes les adresses sont autorisées.



Authentification

Disponibles pour tous les types de gestionnaires, sauf les sockets Web.

Les paramètres de la section déterminent une liste de ressources. Pour accéder à ces ressources il faut demander l'authentification basic http du client Web.

- **Zone d'action** : valeur que le serveur Web transmettra au client dans le paramètre `WWW-Authenticate: Basic realm="ADMIN"`. En fait, une brève description de celui qui doit s'authentifier. Elle n'a aucun rapport avec le nom d'enregistrement.

Pour configurer les limitations d'accès pour tout type de connexion

1. Pour autoriser un accès libre en cas de connexion des clients par HTTP ou par HTTPS aux chemins particuliers, ajoutez ces chemins dans les listes respectives **HTTP : accès libre** ou **HTTPS : accès libre**.
2. Pour demander l'authentification en cas de connexion des clients par HTTP ou par HTTPS aux chemins particuliers, ajoutez ces chemins dans les listes respectives **HTTP : demande d'authentification** ou **HTTPS : demande d'authentification**.
3. En cas d'accès par les chemins non inclus dans une liste, l'authentification est requise en fonction du statut de la case **Priorité de demande de l'authentification** : si vous avez coché la case pour la connexion aux chemins non inclus dans une des listes (ou inclus dans les deux listes), l'authentification est requise. Sinon, un accès libre est autorisé pour ces chemins.

Pour éditer la liste des adresses

1. Entrez dans le champ l'expression régulière déterminant le chemin par rapport au répertoire spécifié dans le champ **Répertoire**.
2. Pour ajouter un nouveau champ d'adresse, cliquez sur le bouton dans la rubrique correspondante.
3. Pour supprimer un champ, cliquez sur .

10.8. Procédures utilisateur



Lors de l'exécution des scripts Lua, l'administrateur obtient l'accès à tout le système de fichiers à l'intérieur du répertoire du Serveur Dr.Web et aux certaines commandes sur l'ordinateur avec le Serveur Dr.Web installé.

Pour interdire l'accès aux procédures utilisateur, désactivez le droit **Éditer la configuration du Serveur Dr.Web et du référentiel** pour l'administrateur correspondant (voir le p. [Administrateurs et groupes administrateur](#)).

Pour faciliter et automatiser l'exécution de certaines tâches du Serveur Dr.Web, il est possible d'utiliser les procédures utilisateur effectuées en tant que scripts Lua.



Les procédures utilisateur sont placées dans le sous-répertoire suivant du répertoire d'installation du Serveur Dr.Web :

- sous Windows : `var\extensions`
- sous FreeBSD : `/var/drwcs/extensions`
- sous Linux : `/var/opt/drwcs/extensions`

Après l'installation du Serveur Dr.Web, dans ce sous-répertoire sont placées les procédures utilisateur préinstallées.

Il est recommandé d'éditer les procédures utilisateur via le Centre de gestion.



Avant de mettre à niveau le Serveur Dr.Web, il faut sauvegarder les procédures et les scripts utilisateur. Notez que lors de la migration vers une version plus récente du Serveur Dr.Web, les procédures utilisateur et les scripts qui ont fonctionné dans la version précédente peuvent ne pas fonctionner dans la version actuelle. Si un problème survient, contactez le [support technique](#).

Pour configurer l'exécution des procédures utilisateur

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion.
2. Dans la fenêtre qui s'ouvre, choisissez **Procédures utilisateur** dans le menu de gestion. Une autre fenêtre va s'ouvrir.



La description détaillée des procédures utilisateur et de leurs paramètres est disponible dans le document **Annexes**, [Annexe M. Procédures utilisateur](#).

Arborescence des procédures

La liste hiérarchique des procédures affiche une arborescence, dont les noeuds sont des groupes de procédures et des procédures utilisateur appartenant à ces groupes.

Initialement, l'arborescence des procédures contient des groupes pré-installés suivants :

- **Examples of the hooks** contient des modèles de toutes les procédures utilisateur disponibles. Sur la base de ces modèles, vous pouvez créer vos propres procédures utilisateur. La modification et l'exécution des procédures de modèles ne sont pas disponibles.
- **IBM Syslog** contiennent de modèles des procédures utilisateur utilisées lors de l'intégration avec le système IBM Tivoli. Les événements correspondant aux procédures activées sont enregistrés au format *Syslog*.

Tous les événements sont enregistrés dans le même fichier par le chemin suivant :

- sous Windows :
`var\export\tivoli\syslog\drwcs_syslog.log`



- sous OS FreeBSD :
`/var/drwcs/export/tivoli/syslog/drwcs_syslog.log`
- sous Linux :
`/var/opt/drwcs/export/tivoli/syslog/drwcs_syslog.log`
- **IBM W7Log** contiennent de modèles des procédures utilisateur utilisées lors de l'intégration avec le système IBM Tivoli. Les événements correspondant aux procédures activées sont enregistrés au format *IBM W7Log XML*.

Pour chaque événement in fichier à part est créé par le chemin suivant :

- sous Windows :
`var\export\tivoli\w7log\<nom_de_l'événement>_<unix_timestamp>`
- sous FreeBSD :
`/var/drwcs/export/tivoli/w7log/<nom_de_l'événement>_<unix_timestamp>`
- sous Linux :
`/var/opt/drwcs/export/tivoli/w7log/<nom_de_l'événement>_<unix_timestamp>`

L'apparence de l'icône dépend du type et du statut de cet élément (voir le [tableau 10-7](#)).

Tableau 10-7. Icônes des éléments de l'arborescence de procédures

Icône	Description
Groupes de procédures	
	Groupe de procédures pour lequel l'exécution des procédures est autorisée.
	Groupe de procédures pour lequel l'exécution des procédures est interdite.
Procédures	
	Procédure pour laquelle l'exécution est autorisée.
	Procédure pour laquelle l'exécution est interdite.

Gestion de l'arborescence des procédures

Pour gérer les objets de l'arborescence, utilisez les éléments suivants de la barre d'outils :

+ : liste déroulante pour l'ajout d'un élément à l'arborescence des procédures :

Ajouter une procédure : ajouter une nouvelle procédure utilisateur.

Ajouter un groupe de procédures : ajouter un nouveau groupe utilisateur pour y placer des procédures.

✗ Supprimer les objets sélectionnés : supprimer une procédure utilisateur ou un groupe de procédures sélectionné dans l'arborescence.



▶ Autoriser l'exécution de la procédure : la même action est effectuée via l'éditeur de procédures si vous cochez la case **Autoriser l'exécution de la procédure**. Voir aussi [Activation des procédures](#).



❑ Désactiver l'exécution de la procédure : la même action est effectuée via l'éditeur de procédures si vous décochez la case **Activer l'exécution de la procédure**. Voir aussi [Activation des procédures](#).

Gestion des groupes de procédures

Pour créer un nouveau groupe

1. Dans la barre d'outils, sélectionnez  →  **Ajouter un groupe de procédures**.
2. Dans la fenêtre qui s'affiche, configurez les paramètres suivants :
 - Cochez la case **Autoriser l'exécution de la procédure** pour activer les procédures qui seront incluses dans ce groupe. Voir aussi [Activation des procédures](#).
 - Dans le champ **Nom de groupe**, spécifiez un nom pour le groupe créé.
3. Cliquez sur **Enregistrer**.

Pour modifier l'ordre de l'utilisation des groupes



1. Dans l'arborescence, glissez-déposez un groupe de procédures et mettez-le dans le bon ordre par rapport aux autres groupes.
2. Si vous modifiez l'ordre des groupes, l'ordre de l'utilisation des procédures va changer automatiquement : les procédures des groupes qui sont placés plus haut dans l'arborescence seront exécutées les premières.

Pour déplacer une procédure dans un autre groupe

1. Sélectionnez dans l'arborescence la procédure que vous voulez déplacer.
2. Dans le panneau de propriétés qui s'affiche, sélectionnez dans la liste déroulante **Groupe supérieur** le groupe dans lequel il faut placer la procédure.
3. Cliquez sur **Enregistrer**.

Gestion des procédures

Pour ajouter une nouvelle procédure

1. Dans la barre d'outils, sélectionnez  →  **Ajouter une procédure**.
2. Dans la fenêtre qui s'affiche, configurez les paramètres suivants :
 - Cochez la case **Autoriser l'exécution de la procédure** pour activer la procédure créée. Voir aussi [Activation des procédures](#).
 - Dans la liste déroulante **Groupe parent**, sélectionnez le groupe dans lequel la procédure sera placée. Plus tard, vous pourrez déplacer la procédure dans un autre groupe — voir [ci-dessus](#).
 - Dans la liste déroulante **Procédure**, sélectionnez le type de la procédure. Le type de la procédure désigne l'action pour laquelle cette procédure sera appelée.



- Dans le champ **Texte de procédure**, entrez le script lus qui sera exécuté lors de l'appel de cette procédure.
Dans la sous-rubrique **Information sur la procédure** vous pouvez consulter l'événement pour lequel cette procédure sera appelée, ainsi que les informations sur la disponibilité de la base de données du Serveur Dr.Web pour cette procédure et les listes des paramètres d'entrée et des valeurs de retour pour ce type de la procédure.

3. Cliquez sur **Enregistrer**.


Pour éditer une procédure

1. Sélectionnez dans l'arborescence la procédure que vous voulez éditer.
2. Dans la partie droite de la fenêtre, un panneau des propriétés de cette procédure va s'afficher automatiquement. Vous pouvez modifier tous les paramètres spécifiés lors de la création de la procédure, sauf le paramètre **Procédure**. Ce paramètre désigne l'événement pour lequel cette procédure est appelée et il n'est pas modifiable après la création de la procédure.
3. Cliquez sur **Enregistrer**.

Activer une procédure

L'activation des procédures et des groupes détermine si les procédures seront exécutées quand l'événement correspondant a eu lieu ou non.

Pour activer une procédure ou un groupe de procédures

1. Sélectionnez dans l'arborescence la procédure ou le groupe que vous voulez activer.
2. Effectuez une des actions suivantes :
 - Dans la barre d'outils, cliquez sur le bouton  **Autoriser l'exécution de la procédure**.
 - A droite de la fenêtre, dans le panneau de propriétés de l'objet sélectionné, cochez la case **Autoriser l'exécution de la procédure**, si la case est décochée. Cliquez sur le bouton **Enregistrer**.

Particularités de l'activation des procédures :

Pour que la procédure soit exécutée si l'événement correspondant a eu lieu, il faut que :

- a) la procédure soit activée ;
- b) le groupe qui contient cette procédure soit activé.



Si le groupe de procédures est désactivé, les procédures qui y sont incluses ne seront pas exécutées même si elles sont activées.

Si vous activez un groupe, notez que seules les procédures activées seront exécutées.



10.9. Modèles de messages

Dans la section **Modèles de messages**, vous trouverez la liste de modèles de messages texte aléatoires envoyés par l'administrateur sur les postes du réseau antivirus (voir [Envoi de messages aux postes](#)).


Les messages peuvent entrer dans la liste de modèles par l'un des moyens suivants :


1. Le modèle peut être créé à la base d'un message déjà envoyé par l'administrateur. Un tel modèle est créé dans la section [Journal de messages](#).
2. Un nouveau modèle peut être créé. Pour ce faire, cliquez sur **+ Créer un modèle** dans la barre d'outils dans la section **Modèles de messages**. Les configurations du messages sont équivalentes aux configurations de la section [Envoi de messages aux postes](#).

Pour gérer les modèles de messages, utilisez les options suivantes dans la barre d'outils :


 **Supprimer** : supprimer les modèles de messages sélectionnés.

 **Créer un modèle** : créer un nouveau modèle de message (voir [ci-dessus](#)).


 **Éditer** : éditer les paramètres d'un modèle existant. L'option est disponible uniquement lorsqu'un message est sélectionné dans la liste.

 **Envoyer un message aux postes** : envoyer un ou plusieurs messages aux postes à la base se modèles sélectionnés dans la liste (voir ci-dessous).

Pour envoyer un message

1. Cochez la case contre le modèle du message à envoyer.
2. Cliquez sur  **Envoyer le message aux postes**.
3. La fenêtre **Envoi du message** s'ouvre. Spécifiez les paramètres suivants :
 - a) Dans l'arborescence **Réseau antivirus**, sélectionnez les destinataires du message dans la liste affichée : cela peut être les postes ou les groupes de postes.
 - b) Les paramètres du messages sont équivalents aux paramètres de la section [Envoi de messages aux postes](#).
4. Cliquez sur **Envoyer**.

Pour envoyer plusieurs messages

1. Cochez les cases contre les modèles des messages à envoyer.
2. Cliquez sur  **Envoyer le message aux postes**.
3. La fenêtre **Envoi de plusieurs messages** s'ouvre. Dans la section **Liste des messages**, vous trouverez tous les messages qui ont été sélectionnés pour être envoyés. Les noms des messages correspondent aux noms de leurs modèles.
4. Cliquez sur **Envoyer tout** pour envoyer tous les messages de la liste.




5. Pour modifier un message, sélectionnez-le dans la section **Liste des messages**. Dans la section **Paramètres du message**, spécifiez les paramètres suivants :
 - a) Dans l'arborescence **Réseau antivirus**, sélectionnez les destinataires du message dans la liste affichée : cela peut être les postes ou les groupes de postes.
 - b) Les paramètres du messages sont équivalents aux paramètres de la section [Envoi de messages aux postes](#).
 - c) Pour supprimer le message sélectionnés de la liste, cliquez sur le bouton **Supprimer**.


10.10. Configuration des notifications



Dr.Web Enterprise Security Suite supporte l'envoi des notifications sur les attaques virales, sur les statuts des composants du réseau antivirus et sur d'autres événements aux administrateurs du réseau antivirus Dr.Web Enterprise Security Suite.


10.10.1. Configuration des notifications

Pour configurer les notifications sur les événements du réseau antivirus

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion. Dans la fenêtre qui s'ouvre, sélectionnez l'élément du menu de gestion **Configuration des notifications**.
2. La configuration des notifications est paramétrée séparément pour chaque administrateur du Centre de gestion. Le nom de l'administrateur pour qui sont spécifiés les paramètres affichés est mentionné dans le champ **Administrateur recevant des notifications**. Pour configurer les notifications pour un autre administrateur, cliquez sur le bouton  et sélectionnez l'administrateur dans la fenêtre qui s'affiche.
3. Un bloc (profil) de notifications est ajouté par défaut pour l'administrateur principal **admin** lors de la configuration initiale. Si la liste de notifications de l'administrateur est vide, cliquez sur **Ajouter une notification** dans la section **Liste de notifications**.
4. Pour activer l'envoi des notifications, basculez l'interrupteur à gauche de l'en-tête du bloc des notifications :

  : l'envoi des notifications pour ce bloc est activé.

  : les notifications pour ce bloc ne seront pas envoyées.

5. Vous pouvez créer plusieurs blocs (profils) des notifications, par exemple, pour les différents modes d'envoi. Pour ajouter encore un bloc, cliquez sur  à droite des paramètres du bloc des notifications. Un bloc de notifications sera ajouté en bas de la page. La configuration de différents blocs de notifications s'effectue séparément.
6. Dans le champ **En-tête**, spécifiez le nom du bloc des notifications ajouté. Ce nom sera utilisé, par exemple, pour configurer la tâche **Création d'un rapport statistique** dans la planification du Serveur Dr.Web. Ensuite, pour éditer l'en-tête, cliquez avec le bouton gauche de la souris sur l'en-tête et entrez le nom nécessaire. S'il y a plus qu'un seul bloc



des notifications, une liste déroulante des en-têtes des blocs des notifications existants vous sera proposée.

7. Pour configurer l'envoi des notifications, sélectionnez le type nécessaire d'envoi des notifications dans la liste déroulante **Mode d'envoi du message** :
 - [Agent Dr.Web](#) : envoyer des notifications via le protocole de l'Agent Dr.Web.
 - [Console web](#) : envoyer des notifications pour les consulter dans la [console web](#).
 - [E-mail](#) : envoyer des notifications par e-mail.
 - [Notifications push](#) : envoyer des notifications push dans le Centre mobile de gestion de la sécurité Dr.Web. Cette option sera disponible dans la liste déroulante **Mode d'envoi du message** après la connexion du Centre mobile de gestion de la sécurité à ce Serveur Dr.Web.
 - [SNMP](#) : envoyer des notifications via le protocole SNMP.
 - [Syslog](#) : envoyer des notifications via le protocole Syslog.
8. Dans la liste des notifications, cochez les cases contre les notifications qui seront envoyées conformément au mode d'envoi de ce bloc des notifications.
9. Les textes des modèles prédéfinis sont utilisés dans les notifications.



Vous pouvez consulter la description des notification préconfigurées et de leurs paramètres dans le document **Annexes**, [C2. Paramètres des modèles de notifications](#).

Pour modifier le modèle d'une notification particulière :

- a) Cliquez sur **Basculer en mode d'édition des notifications** dans l'en-tête de la section.
- b) Cliquez sur la notification à éditer. Le modèle de notification va s'ouvrir.
- c) Si cela est nécessaire, éditez le texte de la notification à envoyer. Dans le texte de la notification, vous pouvez utiliser les variables du modèle (entre accolades). Pour ajouter les variables, les listes déroulantes dans la partie supérieure de la notification sont fournies. Lors de la préparation du message, le système des notification remplace les variables du modèle par le texte concret qui dépend de la configuration actuelle du système de notification. Vous pouvez consulter la liste des variables disponibles dans le document **Annexes**, [Annexe C2. Paramètres des modèles de notifications](#).


Pour réinitialiser les valeurs par défaut du modèle de notification, cliquez sur le bouton **Modèle par défaut**.

- d) Après avoir apporté toutes les modifications nécessaires, cliquez sur **Quitter le mode d'édition de notifications** dans l'en-tête de la section.




Pour le mode d'envoi **SNMP**, les textes des modèles de notifications sont spécifiés du côté du destinataire (*station de gestion* en termes de RFC 1067), c'est pourquoi il est impossible de les modifier via le Centre de gestion.



10. Pour les notifications de la sous-section **Postes**, vous pouvez spécifier les groupes de postes dont les événements seront indiqués dans les notifications :
 - a) Cliquez sur  à gauche de la notification.
 - b) Dans l'arborescence **Groupes des postes contrôlés**, sélectionnez les groupes de postes dont les événements seront surveillés et une notification correspondante sera envoyée. Pour sélectionner plusieurs groupes, utilisez les touches CTRL ou SHIFT.
 - c) Une fois les groupes nécessaires sélectionnés, cliquez sur **Enregistrer**.
11. Cliquez sur **Enregistrer** pour appliquer toutes les modifications apportées.

Notifications via le protocole de l'Agent Dr.Web

Pour les notifications via le protocole de l'Agent Dr.Web, spécifiez les paramètres suivants :

- Dans la section **Nouvel envoi par le Serveur Dr.Web**, spécifiez les paramètres de nouveaux envois de notifications qui seront effectués par le Serveur Dr.Web en cas d'échec :
 - **Nombre** : nombre de tentatives d'envoi faites par le Serveur Dr.Web en cas d'échec d'envoi du message. Par défaut 10.
 - **Délai** : période en secondes à l'expiration de laquelle le Serveur Dr.Web fait une nouvelle tentative d'envoyer le message. Par défaut 300 secondes.
- **Postes** : liste des postes et des groupes sur lesquels les notifications seront envoyés. Pour modifier la liste, cliquez sur **Modifier** , sélectionnez dans l'arborescence les postes et les groupes de postes nécessaires et cliquez sur **Appliquer**.
- **Envoyer un message test** : envoyer un message test conformément aux paramètres configurés du système de notifications.

Notifications affichées dans la console web

Pour les notifications affichées dans la Console Web, spécifiez les paramètres suivants :



- Dans la section **Nouvel envoi par le Serveur Dr.Web**, spécifiez les paramètres de nouveaux envois de notifications qui seront effectués par le Serveur Dr.Web en cas d'échec :
 - **Nombre** : nombre de tentatives d'envoi faites par le Serveur Dr.Web en cas d'échec d'envoi du message. Par défaut 10.
 - **Délai** : période en secondes à l'expiration de laquelle le Serveur Dr.Web fait une nouvelle tentative d'envoyer le message. Par défaut 300 secondes.
- **Durée de sauvegarde du message** : durée pendant laquelle il faut sauvegarder la notification, à partir du moment de sa réception. Par défaut c'est 1 jour. A la fin de cette période, la notification est considérée comme obsolète et supprimée conformément à la tâche **Supprimer les messages obsolètes** dans les paramètres du Serveur Dr.Web.

Pour les notifications reçues en ce mode d'envoi, vous pouvez spécifier dans la rubrique [Notifications de la console Web](#) un délai de sauvegarde illimité.
- **Envoyer un message test** : envoyer un message test conformément aux paramètres configurés du système de notifications.



Notifications par e-mail

Pour notifier par e-mail, spécifiez les paramètres suivants :

- Dans la section **Nouvel envoi par le Serveur Dr.Web**, spécifiez les paramètres de nouveaux envois de notifications qui seront effectués par le Serveur Dr.Web en cas d'échec :
 - **Nombre** : nombre de tentatives d'envoi faites par le Serveur Dr.Web en cas d'échec d'envoi du message. Par défaut 10.
 - **Délai** : période en secondes à l'expiration de laquelle le Serveur Dr.Web fait une nouvelle tentative d'envoyer le message. Par défaut 300 secondes.
- **Adresses e-mail du destinataire** : adresses e-mails des destinataires de la notification. Vous pouvez entrer une seule adresse du destinataire dans chaque champ de saisie. Pour ajouter encore un champ du destinataire, cliquez sur le bouton . Pour supprimer un champ, cliquez sur .






Les paramètres d'envoi d'e-mails sont configurés dans le menu **Administration**, la rubrique **Configuration du Serveur Dr.Web**, l'onglet **Réseau**, l'onglet intérieur [E-mail](#).

- **Envoyer un message test** : envoyer un message test conformément aux paramètres configurés du système de notifications.

Vous pouvez également ajouter les en-têtes utilisateur aléatoires dans la section avancée **En-têtes** de l'éditeur de modèle (voir [l'art. 9a ci-dessus](#)) pour chaque notification e-mail. Notamment les en-têtes des notifications e-mail peuvent être utilisées pour la configuration des filtres de messagerie. Les en-têtes doivent être formés conformément aux normes RFC 822, RFC 2822 et de ne pas interférer avec les champs spécifiés dans les normes pour les messages e-mail. Ainsi, la norme RFC 822 garantit l'absence des en-têtes commençant par X- dans la spécification, c'est pourquoi il est recommandé de spécifier les noms au format X-*<nom-de-l'en-tête>*. Par exemple, X-Template-Language: French.

Pour ajouter ou modifier l'en-tête d'une notification particulière

1. Cliquez sur  **Basculer en mode d'édition des notifications** dans l'en-tête de la section.
2. Dans la liste déroulante **Mode d'envoi de notifications** sélectionnez **E-mail**.
3. Cliquez sur la notification à éditer. Le modèle de notification va s'ouvrir.
4. Dans le champ **En-têtes**, saisissez un ou plusieurs en-têtes au format X-*<nom>*: *<valeur>*. En tant que valeur vous pouvez utiliser les variables de modèle (entre accolades) disponibles dans les listes déroulantes en haut de la fenêtre. Les en-têtes doivent se séparer par une ligne vide.
5. Cliquez sur **Enregistrer**.
6. Cliquez sur  pour fermer la fenêtre de l'éditeur de modèles.
7. Après avoir apporté toutes les modifications nécessaires, cliquez sur  **Quitter le mode d'édition de notifications** dans l'en-tête de la section.



8. Cliquez sur **Enregistrer** pour appliquer toutes les modifications apportées.

Vous pouvez également spécifier les en-têtes communs pour les notifications e-mail.



Les en-têtes communs sont ajoutés à tous les modèles de notifications e-mail. Une fois ajoutés, les en-têtes communs ne se distinguent pas des autres en-têtes utilisateur de notifications. C'est pourquoi ensuite il sera impossible d'éditer les en-têtes communs en masse en les séparant des autres. Vous pouvez éditer ou supprimer les en-têtes communs ajoutées uniquement avec les autres en-têtes utilisateur en modifiant le modèle de chaque notification particulier.

Pour ajouter un en-tête commun

1. Cliquez sur le bouton **Modifier les en-têtes communs** dans n'importe quel bloc de notifications.
2. Dans la fenêtre **En-têtes communs pour tous les modèles** qui s'affiche, saisissez un ou plusieurs en-têtes au format `X-<nom> : <valeur>`. En tant que valeur vous pouvez utiliser les variables de modèle (entre accolades) disponibles dans les listes déroulantes de l'en-tête du message. Les en-têtes doivent se séparer par une ligne vide.
3. Cliquez sur le bouton **Ajouter**. Une fois ajouté, le texte saisi disparaît du champ de saisie.
4. Cliquez sur **✕** pour fermer la fenêtre de l'éditeur de modèles.
5. Cliquez sur **Enregistrer** pour appliquer toutes les modifications apportées.

Exemple :

- Pour la notification A l'en-tête `X-Header-A` : A est spécifié.
- Pour la notification B l'en-tête `X-Header-B` : B est spécifiée.

Après l'ajout de l'en-tête commun `X-Header-C` : C :

- Pour informer A les en-têtes `X-Header-A` : A, `X-Header-C` : C seront ajoutés.
- Pour la notification B les en-têtes `X-Header-B` : B, `X-Header-C` : C seront spécifiés.

Pour supprimer l'en-tête `X-Header-C` : C de tous les modèles de notifications, il est nécessaire d'éditer les modèles de notifications A et B séparément (voir [l'art. 9a ci-dessus](#))

Pour supprimer ou remplacer tous les en-têtes de toutes les notifications

1. Cliquez sur le bouton **Modifier les en-têtes communs** dans n'importe quel bloc de notifications.
2. Dans la fenêtre **En-têtes communs pour tous les modèles** qui s'affiche, saisissez un ou plusieurs en-têtes au format `X-<nom> : <valeur>`. Les nouveaux en-têtes remplaceront tous les en-têtes de toutes les notifications e-mail spécifiés auparavant. En tant que valeur vous pouvez utiliser les variables de modèle (entre accolades) disponibles dans les listes déroulantes de l'en-tête du message. Les en-têtes doivent se séparer par une ligne vide.
Pour supprimer tous les en-têtes spécifiés auparavant, laissez le champ de saisie vide.



3. Cliquez sur le bouton **Ajouter**. Une fois ajouté, le texte saisi disparaît du champ de saisie.
4. Cliquez sur **x** pour fermer la fenêtre de l'éditeur de modèles.
5. Cliquez sur **Enregistrer** pour appliquer toutes les modifications apportées.

Exemple :

- Pour informer A les en-têtes `X-Header-A: A`, `X-Header-C: C` seront spécifiés.
- Pour informer B les en-têtes `X-Header-B: B`, `X-Header-C: C` sont spécifiés.

Si vous saisissez `X-Header-D: D` dans le champ de saisie et cliquez sur **Remplacer** :

- Pour informer A l'en-tête `X-Header-D: D` sera ajouté. Les en-têtes précédents seront supprimés.
- Pour la notification B l'en-tête `X-Header-D: D` sera ajouté. Les en-têtes précédents seront supprimés.

Si vous laissez le champ de saisie vide et cliquez sur **Remplacer** :

- Pour la notification A tous les en-têtes seront supprimés.
- Pour la notification B tous les en-têtes seront supprimés.

Notifications push

Pour les notifications push envoyées au Centre mobile de gestion, configurez les paramètres suivants :



- Dans la section **Nouvel envoi par le Serveur Dr.Web**, spécifiez les paramètres de nouveaux envois de notifications qui seront effectués par le Serveur Dr.Web en cas d'échec :
 - **Nombre** : nombre de tentatives d'envoi faites par le Serveur Dr.Web en cas d'échec d'envoi du message. Par défaut 10.
 - **Délai** : période en secondes à l'expiration de laquelle le Serveur Dr.Web fait une nouvelle tentative d'envoyer le message. Par défaut 300 secondes.
- **Envoyer un message test** : envoyer un message test conformément aux paramètres configurés du système de notifications.

Notifications via le protocole SNMP

Pour notifier via le protocole de SNMP spécifiez les paramètres suivants :

- Dans la section **Nouvel envoi par le Serveur Dr.Web**, vous pouvez configurer les paramètres de nouveaux envois de notifications qui seront effectués par le Serveur Dr.Web en cas d'échec :
 - **Nombre** : nombre de tentatives d'envoi faites par le Serveur Dr.Web en cas d'échec d'envoi du message. Par défaut, c'est 10.
 - **Délai** : période en secondes à l'expiration de laquelle le Serveur Dr.Web fait une nouvelle tentative d'envoyer la notification. Par défaut 300 secondes.



- Dans la section **Nouvel envoi par le sous-système SNMP**, vous pouvez configurer les paramètres de nouvelles tentatives d'envoi de notifications qui seront effectuées par le système SNMP en cas d'échec :
 - **Nombre** : nombre de tentatives d'envoi faites par le sous-système SNMP en cas d'échec d'envoi de la notification. Par défaut, c'est 5.
 - **Délai** : période en secondes à l'expiration de laquelle le sous-système SNMP fait une nouvelle tentative d'envoyer la notification. Par défaut 5 secondes.
- **Destinataire** : entité de réception SNMP, par exemple, l'adresse IP ou le nom DNS de l'ordinateur. Vous pouvez entrer un seul utilisateur dans chaque champ de saisie. Pour ajouter encore un champ, cliquez sur . Pour supprimer un champ, cliquez sur .
- **Expéditeur** : l'entité envoyant la requête SNMP. Par exemple, l'adresse IP ou le nom DNS de l'ordinateur (doit être reconnu par le serveur DNS). La valeur vide est utilisée par défaut.
- **Communauté** : communauté SNMP ou contexte. Par défaut `public`.
- **Envoyer un message test** : envoyer un message test conformément aux paramètres configurés.



Pour obtenir les descriptions d'OID lors de l'analyse de SNMP trap, vous pouvez utiliser MIB fourni avec le Serveur. Les fichiers `DRWEB-ESUITE-NOTIFICATIONS-MIB.txt` et `DRWEB-MIB.txt` sont placés dans le sous-répertoire `etc` du répertoire d'installation du Serveur Dr.Web.

Notifications via le protocole Syslog

Pour les notifications via le protocole Syslog spécifiez les paramètres suivants :

- Dans la section **Nouvel envoi par le Serveur Dr.Web**, vous pouvez configurer les paramètres de nouveaux envois de notifications qui seront effectués par le Serveur Dr.Web en cas d'échec :
 - **Nombre** : nombre de tentatives d'envoi faites par le Serveur Dr.Web en cas d'échec d'envoi du message. Par défaut, c'est 10.
 - **Délai** : période en secondes à l'expiration de laquelle le Serveur Dr.Web fait une nouvelle tentative d'envoyer la notification. Par défaut 300 secondes.
- **Destinataire** : adresse du destinataire de la notification via le protocole Syslog. Protocole de transmission TCP ou UDP. Par défaut, c'est le protocole UDP, le port 514.
- **Format** : format de notification: RFC 5424 ou CEF (Common Event Format). Par défaut, c'est RFC 5424.
- **Délai de connexion au destinataire (s)** : délai en secondes pendant lequel le Serveur Dr.Web tente de se connecter au destinataire de la notification via le protocole TCP. Par défaut, c'est 5 secondes
- **Facility** : c'est la catégorie du processus qui a généré la notification (par exemple, le moteur, le système de messagerie). Elle peut prendre des valeurs de 0 à 23. Par défaut, c'est 14.



- **Expéditeur** : identificateur du Serveur Dr.Web (nom de domaine complet, nom d'hôte, adresse IP). La valeur vide est utilisée par défaut.
- **Envoyer un message test** : envoyer un message test conformément aux paramètres configurés.

10.10.2. Notifications de la console Web


Via le Centre de gestion, vous pouvez consulter et gérer les notifications de l'administrateur reçues par le moyen **Console web** (l'envoi des notifications de l'administrateur est décrit dans la rubrique [Configuration des notifications](#)).

Pour consulter et gérer les notifications de la console web

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion, puis, dans la fenêtre qui apparaît, sélectionnez l'élément du menu de gestion **Notifications de la console Web**. La liste des notifications envoyées sur la console Web va s'afficher.
2. Pour consulter la notification, cliquez sur la ligne correspondante du tableau. Une fenêtre contenant le texte du message va s'ouvrir. Dans ce cas, la notification sera marquée comme lue.
3. Pour gérer la liste des notifications à l'aide des options fournies dans la barre d'outils :
 - a) Pour afficher les notifications reçues pendant le délai spécifié, utilisez un des moyens suivants :
 - Sélectionnez un des délais préconfigurés dans la liste déroulante de la barre d'outils.
 - Sélectionnez dans les calendriers déroulants les dates aléatoires du début et de la fin du délai.


Après avoir modifié les valeurs de ces paramètres, cliquez sur **Actualiser** pour afficher la liste des notifications conformément aux paramètres spécifiés.

- b) Pour gérer les notifications particulières, cochez les cases contre les notifications nécessaires ou cochez la case commune dans l'en-tête du tableau pour sélectionner toutes les notifications dans la liste. Dans ce cas, les éléments suivants de la barre d'outils deviennent disponibles :


 **Supprimer les notifications** : supprimer toutes les notifications sans possibilité de restauration.


 **Marquer les notifications comme lues** : marquer toutes les notifications comme lues.

- c) Pour gérer les types de notifications particuliers, cochez les cases contre les notifications de types nécessaires. Dans ce cas, les éléments suivants de la barre d'outils deviennent disponibles :

 **Postes non approuvés** : l'option est disponible uniquement lorsque vous sélectionnez les notifications du type **Le poste attend l'approbation**. Dans la liste déroulante, vous pouvez confirmer l'enregistrement ou refuser l'accès au Serveur Dr.Web pour les postes des notifications sélectionnées.



 **Scanner** : l'option est disponible uniquement lorsque vous sélectionnez les notifications du type **Épidémie sur réseau**, **Erreur de scan**, **Menace de sécurité détectée**. Dans la liste déroulante, vous pouvez spécifier les paramètres de lancement du Serveur Dr.Web sur les postes des notifications sélectionnées.

 **Gestion des composants** : l'option est disponible uniquement lorsque vous sélectionnez les notifications du type **Erreur critique de la mise à jour du poste**. Dans la liste déroulante, vous pouvez spécifier les paramètres de lancement des composants du logiciel antivirus sur les postes des notifications sélectionnées.

 **Redémarrer le poste** : l'option est disponible uniquement lorsque vous sélectionnez les notifications du type **Le redémarrage du poste est requis pour appliquer les mises à jour**. L'option lance le redémarrage des postes des notifications sélectionnées.

- d) Si nécessaire, vous pouvez exporter les notifications dans un fichier. Il est possible d'exporter toutes les notifications affichées en ce moment dans le tableau conformément aux paramètres de la plage de temps et aux filtres de tableau (voir p. 4.b).



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

 **Sauvegarder les données dans un fichier CSV,**

 **Sauvegarder les données dans un fichier HTML,**

 **Sauvegarder les données dans un fichier XML,**

 **Sauvegarder les données dans un fichier PDF.**


4. Pour gérer les notifications à l'aide des options fournies par le tableau de notifications :
- a) Placez l'icône  **Sauvegarder le message sans suppression automatique** contre les notifications qui ne doivent pas être supprimées après l'expiration du délai spécifié (le délai de sauvegarde est spécifié avant l'envoi des notifications dans la section [Configuration des notifications](#) dans les paramètres du moyen d'envoi **Console Web**). Ces notifications seront gardées jusqu'à ce que vous les supprimiez manuellement dans la section **Notifications de la console web** ou n'enleviez l'icône  contre ces notifications.
- b) Pour afficher des notifications particulières, dans la colonne, cliquez sur l'en-tête de la colonne que vous voulez filtrer. Dans le menu qui s'affiche, cochez les cases contre les paramètres de notifications à afficher dans le tableau.

Les sections suivantes sont disponibles pour le filtrage :

Colonne	Paramètre	Action
Importance	Critique	Afficher seulement les notifications avec le niveau d'importance sélectionné. Pour afficher toutes les notifications, cochez toutes les cases.
	Haute	
	Moyenne	
	Basse	
	Minimum	



Colonne	Paramètre	Action
Source	Agent	Afficher les notifications liées aux événements sur les postes.
	Serveur Dr.Web	Afficher les notifications liées aux événements sur le Serveur Dr.Web.

- c) Pour configurer l'affichage du tableau, cliquez sur l'icône  dans le coin droit de l'en-tête du tableau. Dans la liste déroulante, vous pouvez configurer les options suivantes :
- Activer ou désactiver le retour à la ligne pour de longs messages.
 - Sélectionner les colonnes à afficher dans le tableau (cases cochées contre le nom). Pour activer/désactiver une colonne, cliquez sur la ligne portant son nom.
 - Choisir l'ordre des colonnes dans le tableau. Pour modifier l'ordre, glissez-déposez une colonne de la liste dans l'endroit nécessaire.

10.10.3. Notifications non envoyées

Via le Centre de gestion, vous pouvez suivre et gérer les notifications de l'administrateur dont l'envoi a échoué conformément aux paramètres de la rubrique [Configuration des notifications](#).

Pour consulter et gérer les notifications non envoyées

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion. Dans la fenêtre qui s'ouvre, sélectionnez l'élément **Notifications non envoyées** du menu de gestion. La liste des notifications non envoyées de ce Serveur Dr.Web va s'ouvrir.
2. Dans la liste des notifications non envoyées sont placées les notifications dont l'envoi aux destinataires a échoué, mais le nombre de tentative d'envoi spécifié dans les paramètres de cette notification n'est pas encore dépassé.
3. Le tableau des notifications non envoyées contient des informations suivantes :
 - **Notification** : nom de la notification de la liste des notifications préinstallées.
 - **En-tête** : nom du bloc des notifications. L'envoi de notifications est effectué conformément aux paramètres de ce bloc.
 - **Nombre d'envois restants** : nombre d'envois réitérées restantes en cas d'échec d'envoi de la notification. Le nombre initial des tentatives d'envoi est spécifié lors de la configuration des notifications dans la rubrique [Configuration des notifications](#). Après l'envoi d'une notification, il n'est pas possible de modifier le nombre de tentatives de l'envoi pour cette notification.
 - **Heure du prochain envoi** : date et heure de la prochaine tentative de l'envoi de la notification. La périodicité des tentatives d'envoi est spécifiée lors de la configuration des notifications dans la rubrique [Configuration des notifications](#). Après l'envoi d'une notification, il n'est pas possible de modifier la périodicité de tentatives de l'envoi pour cette notification.
 - **Destinataire** : adresses de destinataires de la notification.



- **Erreur** : erreur qui empêche l'envoi de la notification.
4. Pour gérer les notifications non envoyées :
- a) Cochez les cases contre les notifications concrètes ou la case dans l'en-tête du tableau des notifications pour sélectionner toutes les notifications de la liste.
 - b) Utilisez les boutons suivants de la barre d'outils :
 - ➡ **Envoyer encore une fois** : envoyer immédiatement les notifications sélectionnées. Dans ce cas, une tentative supplémentaire d'envoi de la notification sera entreprise. En cas d'échec d'envoi, le nombre des tentatives restantes va diminuer d'une tentative et l'heure de la prochaine va être calculée du moment de l'envoi actuel avec la périodicité spécifiée dans la section [Configuration des notifications](#).
 - ✖ **Supprimer** : supprimer toutes les notifications non envoyées sans possibilité de restauration.
5. Les notifications non envoyées sont supprimées de la liste sans les cas suivants :
- a) La notification a été envoyée avec succès au destinataire.
 - b) La notification a été supprimée manuellement par l'administrateur avec le bouton ✖ **Supprimer** dans la barre d'outils.
 - c) Nombre de tentatives d'envoi est dépassé et la notification n'a pas été envoyée.
 - d) Dans la section [Configuration des notifications](#) le bloc des notifications a été supprimé selon paramètres duquel les notifications ont été envoyées.

10.11. Gestion du référentiel du Serveur Dr.Web

Le *référentiel* du Serveur Dr.Web est destiné à sauvegarder les échantillons standard du logiciel ainsi que leurs mises à jour depuis les Serveurs du SGM.

Pour cela, le référentiel manipule des jeux de fichiers dits *produits*. Chaque produit se trouve dans un sous-répertoire du répertoire `var/repository` du Serveur Dr.Web. Les fonctions du référentiel et sa gestion s'effectuent séparément pour chaque produit.

Dans la gestion de la mise à jour, le référentiel utilise la notion de *révision* du produit. La révision correspond à un statut correct des fichiers du produit à un moment donné. Ce statut comprend les noms de fichiers et les sommes de contrôle correspondantes. Chaque révision possède un numéro unique.

Mise à jour des produits du référentiel

La mise à jour des produits peut s'effectuer dans les directions suivantes :

a) Téléchargement des mises à jour sur le Serveur Dr.Web depuis le SGM Dr.Web.

La mise à jour du référentiel du Serveur Dr.Web depuis le SGM se fait automatiquement selon les tâches de la planification du Serveur Dr.Web.



- Pour consulter les tâches de mise à jour du référentiel, accédez à [Configuration générale du référentiel](#) de l'onglet **Planificateur des tâches**.
- Pour modifier la planification des mises à jour depuis le SGM accédez à [Configuration de la planification du Serveur Dr.Web](#).
- Pour vérifier la disponibilité des mises à jour et les télécharger manuellement, accédez à [Statut du référentiel](#) et cliquez sur **Vérifier les mises à jour**.



Voir aussi [Mise à jour du référentiel du Serveur Dr.Web non connecté à Internet](#).

b) Diffusion des mises à jour entre les divers Serveurs Dr.Web dans une configuration multi-serveurs.

Si plusieurs Serveurs Dr.Web sont installés sur votre réseau antivirus, vous pouvez configurer les liaisons entre les serveurs pour transmettre les mises à jour du référentiel :

- En cas de liaison de type supérieur-subordonné, les Serveurs Dr.Web recevant les mises à jour depuis le SGM seront les principaux, les Serveurs Dr.Web subordonnés recevront les mises à jour depuis les Serveurs Dr.Web principaux automatiquement.
- En cas de Serveurs Dr.Web égaux, n'importe lequel peut être assigné en tant que Serveur recevant les mises à jour depuis le SGM. Dans ce cas, les autres Serveurs Dr.Web en recevront toutes les mises à jour automatiquement.

Dans la rubrique [Particularités du réseau avec plusieurs Serveurs Dr.Web](#), vous pouvez consulter la description de la configuration des liaisons entre les serveurs.



Si les liaisons entre les serveurs sont configurées sur le réseau, et que les Serveurs voisins Dr.Web obtiennent des mises à jour depuis ce Serveur Dr.Web, il faut également activer sur votre Serveur Dr.Web la mise à jour des systèmes et des langues d'interfaces de ces Serveurs voisins Dr.Web.

c) Distribution des mises à jour depuis le Serveur Dr.Web sur les postes de travail.

La vérification, le téléchargement depuis le Serveur Dr.Web et l'installation des mises à jour sur les postes se font automatiquement à chaque connexion des Agents Dr.Web au Serveur Dr.Web, et, avec une certaine périodicité, lors du fonctionnement des Agents Dr.Web (cela n'est pas configurable, se fait de manière transparente pour l'administrateur).

Si nécessaire, vous pouvez configurer les limitations de temps et de trafic de mises à jour des Agents Dr.Web dans la section [Restrictions de mises à jour des postes](#).



Configuration des paramètres du référentiel

Le référentiel permet à l'Administrateur du réseau antivirus de configurer les paramètres suivants :

- **Liste des sites de mise à jour lors des opérations de type a).**

Les paramètres de connexion au SGM sont configurés dans la section [Configuration générale du référentiel](#).

- **Limitation de la composition des produits à synchroniser de type a).**

La composition des produits téléchargés depuis le SGM est configurée dans les sections [Configuration générale du référentiel](#) et [Configuration détaillée du référentiel](#).

Ainsi, l'administrateur a la possibilité de surveiller uniquement les modifications nécessaires des catégories de produits.

- **Limitation des composants du produit nécessitant une synchronisation de type c).**

L'administrateur du Serveur Dr.Web peut sélectionner les composants à installer sur les postes. La sélection des composants antivirus se fait dans la section [Composants à installer du package antivirus](#).

- **Contrôle de migrations vers les nouvelles révisions.**

Dans la section [Configuration détaillée du référentiel](#), vous pouvez configurer les révisions pour chaque produit du référentiel séparément.

Dans ce cas, vous pouvez tester vous-même le produit avant leur mise en place.

- **Gestion du contenu du référentiel au niveau de répertoires et de fichiers du référentiel.**

La section [Contenu du référentiel](#) permet de consulter et de gérer le contenu actuel du référentiel au niveau de répertoires et de fichiers du référentiel ainsi que d'exporter et d'importer les produits isolés ou le référentiel entier et ses paramètres.

Contenu des produits du référentiel

A l'heure actuelle, les produits suivants sont disponibles :

- **Utilitaires de gestion Dr.Web**

Utilitaires pour tous les systèmes d'exploitation supportés :

- Chargeur du référentiel Dr.Web (versions graphique et console),
- Centre mobile de gestion Dr.Web (liens vers App Store et Google Play),
- Utilitaire Dr.Web de collecte des informations sur le système,
- Utilitaire de génération des clés numériques et des certificats,



- Utilitaire du diagnostic distant du Serveur Dr.Web,
- Utilitaire du diagnostic distant du Serveur Dr.Web pour la gestion des scripts,
- Utilitaire de suppression de Dr.Web pour Windows,
- Utilitaire d'installation à distance de l'Agent Dr.Web pour UNIX,
- Utilitaire d'installation à distance de l'Agent Dr.Web pour Windows.



Tous les utilitaires sont disponibles pour le téléchargement dans la section du Centre de gestion **Administration** → **Utilitaires**.

- **Agent Dr.Web pour UNIX**

Bases de filtres intégrés et de l'Antispam Dr.Web pour Windows, moteur de l'Antispam Dr.Web pour UNIX.

- **Agent Dr.Web pour Windows**

Logiciels des composants antivirus pour les postes tournant sous Windows.

- **Bases Dr.Web pour Android**

Bases virales pour les postes tournant sous Android.

- **Bases de SplDer Gate**

Bases de filtres intégrés des composants antivirus pour Windows.

- **Bases de l'Antispam Dr.Web**

Bases de l'Antispam Dr.Web pour Windows.

- **Bases virales Dr.Web**

Bases virales, moteurs antivirus pour les postes tournant sous Windows et les OS de la famille UNIX.

- **Données de sécurité du Serveur Dr.Web**

Ensemble des clés, des scripts et des certificats assurant la sécurité lors de la mise à jour des composants du réseau antivirus et l'échange de données entre le Serveur Dr.Web et les Agents Dr.Web.

- **Applications de confiance**

Groupes des applications de confiance pour le composant Contrôle des applications pour les postes tournant sous Windows.



Le produit **Applications de confiance** n'est pas mis à jour depuis le SGM. La distribution de ce produit est possible uniquement par les liaisons entre les Serveurs voisins Dr.Web.



Pour en savoir plus sur la configuration du référentiel pour le produit **Applications de confiance**, voir la section [Applications de confiance](#).

- **Documentation**

Ensemble de manuels et de documents de références disponibles via la section **Support** dans le Centre de gestion.

- **Hashs de menaces connus**

Liste des hashs de menaces connus.

- **Produits d'entreprise Dr.Web**

Packages d'installation des produits suivants :

- Produits pour l'installation sur les postes protégés tournant sous UNIX, Android, macOS,
- Dr.Web pour IBM Lotus Domino,
- Dr.Web pour Microsoft Exchange Server,
- Serveur proxy Dr.Web : package d'installation personnelle du Serveur proxy non lié à l'Agent Dr.Web pour Windows,
- Installateur complet de l'Agent Dr.Web pour Windows,
- Agent Dr.Web pour Active Directory,
- Utilitaire de la modification du schéma Active Directory,
- Utilitaire de la modification des attributs des objets Active Directory,
- NAP Validator.



Tous les packages d'installation des produits d'entreprise sont disponibles pour le téléchargement sur la page à l'adresse :

`http://<Adresse_du_Serveur_Dr.Web>:<numéro_du_port>/install/`

comme `<Adresse_du_Serveur_Dr.Web>` 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).

- **Module de mise à jour Dr.Web**

Module de mise à niveau de l'Agent Dr.Web pour Windows depuis la version 6 vers la version actuelle.

- **Actualités de l'entreprise Doctor Web**

Flux d'actualités de Doctor Web.

- **Serveur proxy Dr.Web**

Logiciels d'installation du Serveur proxy lié à l'Agent Dr.Web pour Windows.



- **Serveur Dr.Web**

- logiciel du Serveur Dr.Web,
- logiciel du Centre de gestion de la sécurité Dr.Web.

10.11.1. Statut du référentiel

Pour voir l'état du référentiel ou mettre à jour les composants du réseau antivirus

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion. Dans la fenêtre qui s'ouvre, sélectionnez l'élément du menu de gestion **Statut du référentiel**.
2. Dans la fenêtre qui s'ouvre, vous pouvez voir la liste des produits du référentiel, la date de la révision utilisée, la date de la dernière révision téléchargée et le statut des produits.



Dans la colonne **Statut** vous pouvez consulter le statut des produits du référentiel du Serveur Dr.Web au moment de la dernière mises à jour.

3. Pour gérer le contenu du référentiel, utilisez les boutons suivants de la barre d'outils :
 - Cliquez sur **Vérifier les mises à jour** pour vérifier la disponibilité des mises à jour des tous les produits dans le SGM. Si le composant analysé est obsolète, il sera mis à jour automatiquement.
 - Pour télécharger le journal des mises à jour du référentiel, cliquez sur un des boutons suivants dans la barre d'outils :



Sauvegarder les données dans un fichier CSV,



Sauvegarder les données dans un fichier HTML,



Sauvegarder les données dans un fichier XML,



Sauvegarder les données dans un fichier PDF.

- Cliquez sur  **Recharger le référentiel depuis le disque**, pour charger la version actuelle du référentiel du disque.

Au démarrage, le Serveur Dr.Web charge les contenus du référentiel en mémoire. Si durant le fonctionnement du Serveur Dr.Web, l'administrateur a modifié les contenus sans tenir compte du Centre de gestion, par ex, en mettant à jour le référentiel avec un utilitaire externe ou manuellement, rechargez le référentiel pour utiliser la version téléchargée.

10.11.2. Mises à jour reportées

Dans la rubrique **Mises à jour reportées**, vous pouvez voir la liste des produits dont la mise à jour est temporairement désactivée sur la page suivante **Configuration détaillée du référentiel** → <Produit> → [Mises à jour reportées](#). Une révision différée est considérée comme *gelée*.



Le tableau des produits gelés contient les informations suivantes :

- **Répertoire du référentiel** : nom du répertoire dans lequel se trouve un produit gelé :
 - 05-drwmeta : données de sécurité du Serveur Dr.Web,
 - 10-drwbases : bases virales,
 - 10-drwgatedb : bases SplDer Gate,
 - 10-drwspamdb : bases de l'Antispam,
 - 10-drwupgrade : Module de mise à jour Dr.Web,
 - 15-drwhashdb : hashes de menaces connus,
 - 20-drwagent : Agent Dr.Web pour Windows,
 - 20-drwandroid11 : bases Dr.Web pour Android,
 - 20-drwcs : Serveur Dr.Web,
 - 20-drwunix : Agent Dr.Web pour UNIX,
 - 25-drwcsdoc : documentation,
 - 40-drwproxy : Serveur proxy Dr.Web,
 - 70-drwextra : produits d'entreprise Dr.Web,
 - 70-drwutils : utilitaires de gestion Dr.Web,
 - 80-drwnews : actualités de Doctor Web.
- **Révision** : numéro de la révision gelée.
- **Reportée à** : Temps auquel la mise à jour du produit est reportée.

Lorsque vous cliquez sur une ligne du tableau, un autre tableau donnant des informations détaillées sur les mises à jour gelées des produits correspondants s'ouvre.

L'option de report des mises à jour est utile si vous devez temporairement annuler la distribution de la dernière mise à jour d'un produit sur tous les postes du réseau antivirus, par ex, si vous souhaitez d'abord tester cette mise à jour sur un nombre limité de postes.


Pour utiliser les fonctions de report de mises à jour, effectuez les actions décrites à la section **Configuration détaillée du référentiel** → [Mises à jour reportées](#).

Pour reporter les mises à jour reportées

1. Cochez les cases près des produits pour lesquels vous souhaitez indiquer des actions sur les mises à jour reportées. Pour sélectionner tous les produits, cochez la case dans le titre du tableau des produits gelés.
2. Dans la barre d'outils, choisissez les actions souhaitées :
 - ✔ **Exécuter immédiatement** : désactiver l'état « gelé » du produit et ajouter la mise à jour à la liste des révisions à distribuer sur les postes d'après la [Procédure](#) générale.
 - ✘ **Annuler la mise à jour** : désactiver l'état « gelé » du produit et empêcher la mise à jour. La mise à jour via le SGM sera restaurée. La révision non gelée sera supprimée de la liste des



mises à jour du produit. Au moment de la réception de la prochaine révision, la révision gelée sera supprimée du disque.



 **Modifier le délai de mise à jour** : indiquez un nouveau délai de report de la mise à jour du produit. La révision est gelée du moment de la réception de la prochaine révision du SGM.

3. Si vous n'avez spécifié aucune action de suppression du statut "gelé", la révision devient "dégelée" lorsque le délai spécifié dans la liste **Délai d'attente de mises à jour** s'écoule. Alors la révision est débloquée automatiquement et elle est incluse à la liste des révisions distribuées aux postes d'après la [Procédure](#) générale.

10.11.3. Configuration générale du référentiel

Dans la rubrique **Configuration générale du référentiel**, vous pouvez indiquer les paramètres de connexion au SGM et de mise à jour des référentiels de tous les produits.

Pour modifier la configuration du référentiel

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion.
2. Dans la fenêtre qui s'ouvre, choisissez l'onglet **Configuration générale du référentiel** dans le menu de gestion.
3. Configurez tous les paramètres nécessaires pour la mise à jour depuis le SGM comme décrit [ci-dessous](#).
4. Si durant la modification des paramètres vous devez annuler toutes les modifications effectuées, utilisez les boutons suivants contre tous les paramètres :
 -  **Restaurer la valeur initiale** : réinitialiser la valeur du paramètre qu'il avait avant la modification actuelle.
 -  **Réinitialiser la valeur par défaut** : réinitialiser la valeur du paramètre par défaut enregistrée dans le fichier de configuration du Serveur Dr.Web.
5. Cliquez sur le bouton **Enregistrer** pour enregistrer toutes les modifications apportées dans les fichiers de configuration du référentiel. Ainsi, la version actuelle du référentiel est rechargée depuis le disque.



L'application de nouveaux paramètres de la configuration du référentiel peut prendre un certain temps. En cas de mise à jour immédiate du référentiel depuis le SGM juste après la modification de la configuration, les paramètres précédents peuvent être utilisés.

10.11.3.1. SGM Dr.Web

Dans l'onglet **SGM Dr.Web**, vous pouvez configurer les paramètres de connexion au Système Global de Mise à jour Dr.Web. Les mises à jour sont téléchargées à l'aide des protocoles dont la liste figure dans la liste déroulante **Protocole de réception des mises à jour** :





Type de protocole	Description
HTTP/HTTPS	Protocoles de réception des mises à jour depuis le serveur Web
FTP/FTPS	Protocoles de réception des mises à jour depuis le serveur FTP
FILE	Protocole de réception de mise à jour depuis le référentiel local sur un ordinateur avec le Serveur Dr.Web installé
SMB/SMBS	Protocoles de réception des mises à jour depuis le système de fichiers unifié (disponibles uniquement sous les OS de la famille UNIX)
SCP/SFTP	Protocoles de réception des mises à jour par la connexion sécurisée

Pour modifier la connexion au SGM

- Dans la liste déroulante **Protocole de la réception des mises à jour**, sélectionnez le type du protocole pour obtenir des mises à jour depuis les serveurs de mises à jour. Pour tous les protocoles, les mises à jour sont téléchargées d'après les paramètres de la rubrique **Liste des Serveurs du Système Global de Mise à jour Dr.Web**.
- **URI de base** : répertoire se trouvant sur les serveurs de mises à jour contenant les mises à jour des produits Dr.Web. En cas de mise à jour depuis les serveurs du SGM Dr.Web, il ne faut pas modifier ce paramètre sans nécessité.
- Si un des protocoles sécurisés supportant le chiffrement est sélectionné dans la liste **Protocole de réception des mises à jour**, alors sélectionnez dans la liste déroulante **Certificats autorisés**, le type des certificats TLS qui seront appliqués automatiquement lors de la connexion au protocole sélectionné.
- Si dans la liste déroulante **Certificats autorisés**, l'option **Personnalisé** est sélectionnée, il faut spécifier dans le champ **Certificat** le chemin d'accès au fichier contenant votre certificat TLS.
- **Login** : nom d'utilisateur utilisé pour l'authentification sur le Serveur des mises à jour, si le serveur exige l'authentification.
- **Mot de passe** : mot de passe d'utilisateur utilisé pour l'authentification sur le Serveur des mises à jour, si le serveur exige l'authentification.
- Dans la liste déroulante **Méthode d'authentification**, sélectionnez la méthode d'authentification sur le serveur de mises à jour.
- Dans le champ **Nombre des révisions stockées temporairement**, vous pouvez spécifier le nombre de révisions stockées temporairement sur le disque pour chaque produit, sans compter les révisions marquées dans l'onglet **Liste des révisions** dans la section **Configuration détaillée du référentiel**.

Si nécessaire, vous pouvez spécifier ce paramètre séparément pour chaque produit dans la section [Synchronisation](#), mais après l'enregistrement des modifications de la configuration générale, le paramètre sera remplacé par une valeur générale.



- Cochez la case **Utiliser CDN** pour autoriser l'utilisation de Content Delivery Network lors du chargement du référentiel.
- Si cela est nécessaire, éditez la liste des serveur du SGM depuis lesquels la mises à jour du référentiel s'effectue dans la section Liste des serveurs du **Système global de mise à jour Dr.Web** :
 - Pour ajouter un serveur SGM à la liste des serveurs utilisés pour les mises à jour, cliquez sur  et indiquez l'adresse du serveur SGM dans le champ qui apparaît.
 - Pour supprimer un serveur SGM de la liste, cliquez sur  contre le serveur que vous souhaitez supprimer.
 - Les serveurs SGM sont listés dans l'ordre dans lequel le Serveur Dr.Web les contacte lors de la mise à jour du référentiel. Pour modifier l'ordre des serveurs SGM, déplacez un serveur nécessaire en faisant glisser la ligne racine de gauche du serveur.

Au moment de l'installation du Serveur Dr.Web, seuls les serveurs de Doctor Web sont présents dans la liste. Si cela est nécessaire, vous pouvez configurer vos propres zones de mises à jour et les ajouter dans la liste des serveurs pour obtenir les mises à jour.

10.11.3.2. Planificateur des tâches

Dans l'onglet **Planificateur des tâches**, vous pouvez consulter toutes les tâches de mise à jour du référentiel créées dans la planification du Serveur Dr.Web.



Vous pouvez créer, supprimer et modifier des tâches de mise à jour du référentiel dans la section [Configuration de la planification du Serveur Dr.Web](#).

10.11.3.3. Agent Dr.Web

- Dans l'onglet **Agent Dr.Web pour UNIX**, sélectionnez les OS UNIX pour lesquels vous voulez mettre à jour les composants installés sur les postes.



Pour désactiver complètement la réception des mises à jour depuis le SGM pour l'Agent pour UNIX, passez dans la rubrique **Configuration détaillée du référentiel**, l'élément **Agent Dr.Web pour UNIX**, l'onglet **Synchronisation** et cochez la case **Désactiver la mise à jour du produit**.

- Dans l'onglet **Agent Dr.Web pour Windows**, indiquez si vous souhaitez mettre à jour tous les composants qui seront installés sur les postes sous Windows ou mettre à jour uniquement les bases virales.
- Dans l'onglet **Langues de l'Agent Dr.Web pour Windows**, spécifiez la liste des langues de l'interface de l'Agent Dr.Web et du package antivirus pour Windows qui seront téléchargées depuis le SGM.



10.11.3.4. Serveur Dr.Web

- Dans l'onglet **Serveur Dr.Web**, indiquez les OS pour lesquels vous voulez mettre à jour les fichiers du Serveur Dr.Web :
 - Pour recevoir les mises à jour des Serveurs Dr.Web sous tous les OS supportés, cochez la case **Mettre à jour toutes les plateformes disponibles sur le SGM**.
 - Pour recevoir les mises à jour du Serveur Dr.Web uniquement sous certains OS supportés, cochez les cases contre ces OS.




Pour désactiver complètement la réception des mises à jour depuis le SGM pour le Serveur Dr.Web, passez dans la rubrique **Configuration détaillée du référentiel**, l'élément **Serveur Dr.Web**, l'onglet **Synchronisation** et cochez la case **Désactiver la mise à jour du produit**.

- Dans l'onglet **Langues du Centre de gestion de la sécurité Dr.Web**, spécifiez la liste des langues de l'interface du Centre de gestion et qui seront téléchargées depuis le SGM.
 - La sous-rubrique **Langues utilisées** contient la liste des langues assignées, dans les paramètres, à au moins un administrateur.
 - La sous-rubrique **Langues non utilisées** contient la liste des langues qui ne sont assignées, dans les paramètres, à aucun administrateur.
- Dans l'onglet **Documentation** sélectionnez les langues en lesquelles les manuels seront disponibles dans la section [Aide](#) → **Documentation**.
 - La division de la documentation en **Langues utilisées/non utilisées** est réalisée de la même manière que dans l'onglet **Langues du Centre de gestion de la sécurité Dr.Web**.
 - Pour avoir l'accès aux manuels au format PDF, cochez la case **Actualiser la documentation** dans la sous-section **Documentation au format PDF** en dessous de la sélection de langues.

10.11.3.5. Actualités de l'entreprise Doctor Web

Dans l'onglet **Actualités de Doctor Web**, indiquez la liste des langues pour le flux d'actualités.

Vous pouvez configurer les paramètres d'abonnement aux actualités dans la section [Paramètres](#) → **Abonnement**.

Vous pouvez consulter les actualités téléchargées de Doctor Web dans le menu principal du Centre de gestion, dans la section  **Support** → **Actualités**.

10.11.3.6. Packages d'installation Dr.Web

- Dans l'onglet **Produits d'entreprise Dr.Web**, sélectionnez dans la liste déroulante les produits qui seront mis à jour depuis le SGM :
 - **Mettre à jour tous les produits** : en cas de mise à jour depuis le SGM, tous les produits d'entreprise disponibles seront mis à jour.



- **Mettre à jour les produits sélectionnés uniquement** : en cas de mise à jour depuis le SGM, seuls les produits cochés dans la liste ci-dessous seront mis à jour.

Après le téléchargement depuis le SGM, les produits d'entreprise seront disponibles dans la section **Administration** → **Options supplémentaires** → [Produits d'entreprise](#) et sur la page d'installation à l'adresse :

`https://<Adresse_du_Serveur_Dr.Web>:<numéro_du_port>/install/`

où `<Adresse_du_Serveur_Dr.Web>` est l'adresse IP ou le nom DNS de l'ordinateur sur lequel est installé le Serveur Dr.Web, `<numéro_du_port>` est le port 9081 (ou 9080 pour http).

- Dans l'onglet **Utilitaires de gestion Dr.Web**, sélectionnez dans la liste déroulante les utilitaires qui seront mis à jour depuis le SGM :
 - **Mettre à jour tous les produits** : en cas de mise à jour depuis le SGM, tous les utilitaires d'administration disponibles seront mis à jour.
 - **Mettre à jour les produits sélectionnés uniquement** : en cas de mise à jour du référentiel depuis le SGM, seuls les utilitaires cochés dans la liste ci-dessous seront mis à jour.

Après le téléchargement depuis le SGM, les utilitaires de gestion deviendront disponibles dans la section **Administration** → **Options supplémentaires** → [Utilitaires](#).

10.11.3.7. Serveur proxy Dr.Web

Dans l'onglet **Serveur proxy Dr.Web**, indiquez les OS pour lesquels vous voulez mettre à jour les fichiers du Serveur proxy Dr.Web :

- Pour recevoir les mises à jour des Serveurs proxy Dr.Web sous tous les OS pris en charge, cochez la case **Mettre à jour toutes les plateformes disponibles sur le SGM**.
- Pour recevoir les mises à jour du Serveur proxy Dr.Web uniquement sous certains OS pris en charge, cochez les cases contre ces OS.

10.11.4. Configuration détaillée du référentiel

La rubrique **Configuration détaillée du référentiel** offre des options de configuration des mises à jour de chaque référentiel de produit séparément.

Pour modifier la configuration du référentiel

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion.
2. Dans la fenêtre qui s'ouvre, sélectionnez la sous-section **Configuration détaillée du référentiel** du menu de gestion, puis sélectionnez le produit que vous souhaitez modifier.
3. Configurez les paramètres du référentiel nécessaires, décrits [ci-dessous](#).
4. Les options suivantes permettant de supprimer le référentiel du produit sont disponibles dans la barre d'outils :
 - **Supprimer le produit du référentiel** : supprimer entièrement le produit du référentiel. Dans ce cas, toutes les révisions du produit seront supprimées et la mise à jour depuis le SGM sera désactivée. Le bouton est disponible si le produit n'a pas été supprimé. Après la



suppression du produit, le bouton change son nom en **Restaurer l'objet dans le référentiel**.



Après la suppression du produit du référentiel, l'onglet **Liste des révisions** sera vide, les autres onglets de cette section garderont leur état habituel, pourtant leurs paramètres ne seront pas appliqués car le produit est absent dans le référentiel.

- **Restaurer le produit dans le référentiel** : restaurer le produit dans le référentiel s'il a été supprimé par un clic sur le bouton **Supprimer le produit du référentiel**. Dans ce cas, la mise à jour du produit depuis le SGM sera activée. La version la plus récente disponible dans le SGM sera téléchargée dans le référentiel. Vous pouvez configurer le téléchargement des mises à jour dans la section [Configuration générale du référentiel](#). Après la restauration du produit, le bouton change son nom en **Supprimer le produit du référentiel**.
- **Enregistrer et recharger depuis le disque** : enregistrer toutes les modifications apportées. Ainsi, la version actuelle du référentiel est rechargée depuis le disque (voir aussi la rubrique [Statut du référentiel](#)).

10.11.4.1. Liste des révisions

Dans l'onglet **Liste des révisions**, vous pouvez voir toutes les révisions disponibles sur le Serveur Dr.Web pour un produit.

Pour supprimer quelques révisions, cochez les cases contre ces révisions et cliquez sur **Supprimer les révisions sélectionnées** dans la barre d'outils.



Vous ne pouvez pas supprimer toutes les révisions. Le produit doit contenir au moins une révision.








Pour supprimer le produit entier, utilisez le bouton **Supprimer le produit du référentiel**.

La suppression des révisions est une opération irréversible.

Le tableau des révisions contient les colonnes suivantes :

Nom de la colonne	Description
Distribuée	<p>Un marqueur automatique, dans cette colonne, définit l'état des mises à jour des produits. Deux types de marqueurs sont disponibles :</p> <p> : <i>Révision distribuée</i>. La révision est utilisée pour la mise à jour des Agents Dr.Web et du logiciel antivirus sur les postes.</p> <p>La révision à distribuer est sélectionnée comme suit :</p>



Nom de la colonne	Description
	<p>1. La révision accompagnée du marqueur  dans la colonne Actuelle est distribuée. Une seule révision peut être marquée.</p> <p>2. Si aucune révision n'est marquée dans la colonne Actuelle, la dernière révision sera distribuée.</p> <p>Le marqueur automatique désigne toujours la révision distribuée.</p> <p>  : <i>Révision gelée</i>. Cette révision n'est pas distribuée aux postes, les nouvelles révisions ne sont pas téléchargées du Serveur Dr.Web. Pour plus d'information sur les actions en cas de révision gelée, voir la sous-rubrique Mises à jour reportées.</p> <p>Si une révision est gelée, la révision à distribuer est sélectionnée comme suit :</p> <ol style="list-style-type: none">1. Si le marqueur  est sélectionné dans la colonne Actuelle, la révision actuelle est distribuée aux postes.2. Si le marqueur  n'est pas sélectionné dans la colonne Actuelle, c'est la révision précédent la révision actuelle qui est distribuée aux postes.
Actuelle	<p>Sélectionnez le marqueur  pour indiquer la révision utilisée pour la mise à jour des Agents Dr.Web et du logiciel antivirus sur les postes de travail.</p> <p>Une seule révision peut être spécifiée.</p> <p>De même, un marqueur indiquant la révision actuelle peut ne pas être inséré.</p> <p>Voir aussi Restauration de la version précédente de la révision du produit.</p>
Stockée	<p>Sélectionnez le marqueur  pour sauvegarder la révision lorsque le référentiel est nettoyé automatiquement (voir aussi Synchronisation).</p> <p>Le marqueur peut être sélectionné pour différentes révisions simultanément.</p> <p>De même, un marqueur peut n'être sélectionné pour aucune révision.</p> <p>Si la révision du produit est stable, vous pouvez la marquer comme stockée et si une nouvelle révision, téléchargée du SGM, est instable, vous pourrez revenir à la révision stockée précédente.</p>
Retenue	<p>Le marqueur automatique détermine que les composants de cette révision sont installés sur les postes avec les mises à jour limitées (les options Mettre à jour uniquement les bases ou Interdire toutes les mises à jour sont spécifiées dans la section Restrictions de mises à jour des postes).</p> <p>Une telle révision n'est pas supprimée lors du nettoyage automatique du référentiel et elle peut être utilisée s'il faudra réinstaller les composants échoués sur le poste ou installer les composants supplémentaires de cette révision.</p>
Révision	<p>La date de réception de la révision du produit.</p> <p>Si la révision est bloquée, le statut de blocage s'affiche dans cette colonne.</p>



Restauration de la version précédente de la révision du produit

La possibilité de restauration des versions précédentes des produits installés sur les postes est déterminée par les dispositions suivantes :

- Vous pouvez toujours restaurer la version précédente des produits avec les bases de composants (bases virales, bases SplDer Gate, bases de l'Antispam, bases Dr.Web pour Android).
- Pour restaurer la version précédente de l'Agent Dr.Web pour Windows, il faut autoriser l'option **Autoriser le passage aux révisions précédentes** dans la section [Restrictions de mises à jour des postes](#).



En cas de restauration de la révision précédente de l'Agent Dr.Web pour Windows (pour l'installation sur les postes de l'Agent Dr.Web en version antérieure), le redémarrage forcé des postes 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.

- La version précédente des autres produits (notamment, les Applications de confiance du composant Contrôle des applications) sera restaurée si la case **Recevoir les dernières mises à jour** est cochée dans la section [Restrictions de mises à jour des postes](#) ou que c'est la révision marquée comme **Actuelle** dans la configuration détaillée du répertoire qui est restaurée. Dans les autres cas, la restauration ne se fait pas. Le Serveur Dr.Web attend la sortie d'une révision plus récente.

10.11.4.2. Synchronisation

Dans l'onglet **Synchronisation**, vous pouvez configurer les paramètres de mise à jour du référentiel du Serveur Dr.Web depuis le SGM :

- Dans le champ **Nombre de révisions temporairement stockées**, vous pouvez spécifier le nombre de révisions temporairement stockée sur le disque. La valeur indiquée n'inclut pas les révisions marquées au moins dans une colonne dans l'onglet **Liste des révisions**. Lorsqu'une nouvelle révision est réceptionnée et que le nombre de révisions stockées a atteint son maximum, la plus ancienne révision est supprimée. Les révisions marquées comme **Actuelle**, **Stockée**, **Distribuée** et **Retenue** ne sont pas supprimées automatiquement et elles ne sont pas prises en considération lors du décompte des révisions temporairement stockées.

En cas de modification de la section [SGM Dr.Web](#), ce paramètre sera remplacé par la valeur générale pour tous les produits.

- Cochez la case **Désactiver la mise à jour du produit** pour ne plus recevoir de mises à jour des serveurs SGM pour ce produit. Les Agents Dr.Web seront mis à jour vers la révision actuelle sur le Serveur Dr.Web (ou selon la [procédure](#) utilisée pour sélectionner la révision distribuée).
- Cochez la case **Mettre à jour à la demande uniquement** pour mettre à jour le produit depuis le SGM uniquement en cas de demande de ce produit de postes. Sinon, les mises à jour du produit ne sont pas téléchargés depuis le SGM.



Si votre Serveur Dr.Web est connecté à Internet pour la réception automatique des mises à jour depuis le SGM, aucune intervention de l'administrateur n'est requise : les mises à jour seront téléchargées automatiquement aussitôt qu'un poste aura demandé des mises à jour de ce produit depuis le Serveur Dr.Web.

Si votre Serveur Dr.Web n'est pas connecté à Internet, les mises à jour sont téléchargées manuellement [depuis un autre Serveur Dr.Web](#) ou via [Chargeur du référentiel Dr.Web](#) et que vous voulez installer ou mettre à jour les produits pour lesquels est activé l'option **Mettre à jour à la demande uniquement**, il faudra d'abord télécharger ces produits manuellement dans le référentiel.



Lors de l'installation du Serveur Dr.Web en version 13 ou juste après la mise à niveau du Serveur Dr.Web vers la version 13, les mises à jour des produits de référentiel **Bases Dr.Web pour Android, Agent Dr.Web pour UNIX et Serveur proxy Dr.Web** sont téléchargées depuis le SGM uniquement en cas d'appel de ces produits depuis les postes.

- Dans la sous-section **Distribution par les liens entre serveurs**, les paramètres suivants sont configurés :
 - Cochez la case **Bloquer la transmission des mises à jour aux Serveurs voisins Dr.Web** pour bloquer la transmission des mises à jour du produit par les liaisons entre serveurs. Cette option n'affecte pas les paramètres de mise à jour du produit depuis le SGM.
 - Cocher la case **Bloquer la réception des mises à jour des Serveurs voisins Dr.Web** pour bloquer la transmission des mises à jour du produit par les liaisons entre serveurs. Cette option n'affecte pas les paramètres de mise à jour du produit depuis le SGM.

Pour certains produits, les paramètres suivants sont disponibles :

- Cochez la case **Mettre à jour uniquement les fichiers suivants** pour recevoir les mises à jour du SGM uniquement pour les fichiers listés.
- Cochez la case **Ne pas mettre à jour uniquement les fichiers suivants** pour désactiver la mise à jour depuis le SGM uniquement pour les fichiers listés.

Les fichiers peuvent être sélectionnés dans un format d'expressions régulières.

Si les deux cases sont cochées, les fichiers à mettre à jour sont sélectionnés comme suit :

1. Dans la liste complète des fichiers des produits, seuls sont sélectionnés les fichiers indiqués dans la liste **Mettre à jour uniquement les fichiers suivants**.
2. Depuis la sélection à l'étape 1, les fichiers indiqués dans la liste **Ne pas mettre à jour uniquement les fichiers suivants** sont supprimés.
3. Les fichiers résultant de la sélection à l'étape 2 sont mis à jour depuis le SGM.



10.11.4.3. Notifications

Dans l'onglet **Notifications**, vous pouvez configurer les notifications concernant les mises à jour du référentiel :

- Cochez la case **Ne pas notifier uniquement sur ces fichiers**, pour désactiver les notifications sur les événements liés aux fichiers listés ci-dessous.
- Cochez la case **Notifier uniquement sur ces fichiers** pour activer les notifications sur les événements liés aux fichiers listés.

Les fichiers peuvent être sélectionnés dans un format d'expressions régulières.

Si aucune liste d'exceptions n'est dressée, toutes les notifications activées à la rubrique [Configuration des notifications](#) sont envoyées.

Les paramètres des notifications sur les mises à jour du référentiel sont configurés à la page Notifications, à la rubrique **Référentiel**.

10.11.4.4. Mises à jour reportées

Dans l'onglet **Mises à jour reportées**, vous pouvez reporter la distribution des mises à jour sur les postes pour un certain délai. Une révision reportée est considérée comme gelée.

Cette fonctionnalité est utile si vous avez besoin d'annuler temporairement la distribution de la dernière révision du produit sur tous les postes du réseau antivirus, par exemple, si vous souhaitez tester au préalable cette révision sur un nombre limité de postes.



L'utilisation du blocage des révisions lors du passage entre les version majeures n'est pas recommandée. Après l'enlèvement du blocage, vous pouvez rencontrer des problèmes de mise à jour du logiciel sur les postes.

Pour utiliser les fonctions de mises à jour reportées



1. Si vous souhaitez geler une mise à jour pour un produit, configurez les mises à jour reportées comme décrit [ci-dessous](#).
2. Pour anuler la distribution de la dernière révision, indiquez une des révisions précédentes comme actuelle dans l'onglet [Liste des révisions](#).
3. Pour un groupe de postes qui recevra la dernière révision, cochez la case **Recevoir les dernières mises à jour** dans la section **Réseau antivirus** → [Restrictions de mises à jour des postes](#). Les autres postes recevront les révisions que vous avez indiquées comme actuelles à l'étape 2.
4. La prochaine révision téléchargée du SGM qui satisfait aux conditions requises à l'option **Reporter les mises à jour uniquement pour les fichiers suivants**, sera bloquée et reportée dans le délai indiqué dans la liste **Délai de report des mises à jour**.



Pour configurer les mises à jour reportées

1. Cochez la case **Différer les mises à jour** pour désactiver temporairement le téléchargement des mises à jour des serveurs SGM pour le produit.
2. Dans la liste déroulante **Période de report des mises à jour**, sélectionnez la période à laquelle reporter le téléchargement des mises à jour, à partir de leur réception des serveurs SGM.
3. Si nécessaire, cochez la case **Différer les mises à jour uniquement pour les fichiers suivants** pour reporter la distribution des mises à jour contenant des fichiers correspondant aux masques spécifiés. Les masques sont indiqués au format d'expressions régulières.
Si la case n'est pas cochée, toutes les mises à jour du SGM sont bloquées.

Pour enlever le blocage

- Dans l'onglet **Liste des révisions**, cliquez sur  **Exécuter immédiatement** pour désactiver le blocage du produit et ajouter la révision à la liste des révisions distribuées aux postes conformément à la [procédure](#) générale.
- Dans l'onglet **Liste des révisions**, cliquez sur  **Annuler la mise à jour** pour désactiver le blocage du produit et empêcher la révision. La mise à jour depuis le SGM sera restaurée. La révision non bloquée sera supprimée de la liste des révisions du produit. Après la réception de la prochaine révision, la révision non bloquée sera supprimée du disque.
- Lorsque la période indiquée dans la liste **Heure de report des mises à jour** est dépassée, la révision sera débloquée et est incluse à la liste des révisions distribuées aux postes selon la [procédure](#) générale.

Vous pouvez gérer les révisions gelées pour tous les produits à la page [Mises à jour reportées](#).

10.11.5. Contenu du référentiel

La rubrique **Contenu du référentiel** permet de consulter et gérer le contenu actuel du référentiel au niveau de répertoires et de fichiers du référentiel.

La fenêtre principal de la rubrique **Contenu du référentiel** contient l'arborescence du référentiel représentant tous les répertoires et les fichiers de la version actuelle du référentiel avec la liste de toutes les révisions existantes pour chaque produit.

Voir les informations sur le référentiel

Pour consulter les informations sur les objets du référentiel sélectionnez un objet dans l'arborescence du contenu du référentiel. Le panneau de propriété contenant les informations suivantes va s'ouvrir :

- La section **Objets sélectionnés** contient des informations détaillées sur l'objet sélectionné dans l'arborescence du contenu du référentiel : **Type**, **Taille** (pour les objets particuliers), **Date de création** et **Date de modification**.



- La sous-rubrique **Contenu du référentiel** contient les informations générales sur tous les objets du référentiel : liste courante des objets et date de leur dernière modification.

Gestion du référentiel

Pour gérer le contenu du référentiel, utilisez les boutons suivants de la barre d'outils :





 [Exporter des fichiers de référentiel vers une archive,](#)

 [Importer une archive avec des fichiers de référentiel,](#)

 **Supprimer les objets sélectionnés** : supprimer les objets sélectionnés dans l'arborescence du contenu du référentiel sans possibilité de restauration.

Exportation du référentiel

Pour enregistrer les fichiers du référentiel en archive zip

- Pour mettre en archive le référentiel entier, cliquez sur le bouton  **Exporter des fichiers de référentiel vers une archive** → **Tout le contenu du référentiel** dans la barre d'outils. Dans ce cas, le référentiel entier sera exporté quel que soit l'objet sélectionné dans l'arborescence.
- Pour mettre en archive les dernières révisions de tous les produits, cliquez sur le bouton  **Exporter des fichiers de référentiel vers une archive** → **Dernières révisions de tous les produits** dans la barre d'outils.
- Pour mettre en archive tous les fichiers de configuration du référentiel, cliquez sur le bouton  **Exporter des fichiers de référentiel vers une archive** → **Fichiers de configuration** dans la barre d'outils. Dans ce cas, tous les fichiers se trouvant dans le répertoire racine du référentiel et de tous les produits seront exportés.
- Pour mettre en archive certains objets du référentiel, sélectionnez-les dans l'arborescence en utilisant les touches CTRL ou SHIFT et cliquez sur le bouton  **Exporter des fichiers de référentiel vers une archive** → **Objets sélectionnés** dans la barre d'outils.



En cas de grande quantité de données, le délai d'exportation peut dépasser la durée de la session. Si la durée de la session s'écoule avant la fin de l'exportation, l'exportation sera automatiquement arrêtée et l'archive de données d'exportation ne sera pas générée.

Lors de l'exportation des objets du référentiel, prenez en compte les types principaux des objets exportés :

- a) Archives zip des produits du référentiel. Les archives pareilles contiennent un des types suivants des objets du référentiel :
 - Référentiel entier.
 - Produit entier.
 - Révision entière du produit.



Les archives obtenues lors de l'exportation des données des objets peuvent être [importées](#) via la rubrique **Contenu du référentiel**. Les noms de ces archives ont le préfixe `repository_`.



b) Archives zip des fichiers particuliers du référentiel.

Les archives obtenues lors de l'exportation des fichiers particuliers et des répertoire se trouvant dans l'arborescence au-dessous des objets du p. **a)** ne peuvent pas être importées via la rubrique **Contenu du référentiel**. Les noms de ces archives ont le préfixe `files_`.

Ces archives peuvent être utilisées en tant que copies de sauvegarde des fichiers pour le remplacement manuel. Pourtant il est recommandé de ne pas remplacer les fichier du référentiel manuellement sans faire recours à la rubrique **Contenu du référentiel**.

Importation du référentiel

Pour charger les fichiers du référentiel depuis une archive zip

1. Cliquez sur  **Importer une archive avec des fichiers de référentiel** dans la barre d'outils.
2. Dans la fenêtre qui s'ouvre dans la section **Sélection d'un fichier**, spécifiez l'archive zip avec les fichiers du référentiel. Pour sélectionner un fichier, utilisez le bouton .

On peut importer seulement les archives zip obtenues lors de l'exportation d'un des types suivants des objets du référentiel :

- Référentiel entier.
- Produit entier.
- Révision entière du produit.

Lors de l'exportation, le nom des archives pareilles contient le préfixe `repository_`.

3. Dans la rubrique **Importer les paramètres**, configurez les paramètres suivants :
 - **Ajouter uniquement les révisions manquantes** : dans ce mode d'importation, seules les révisions du référentiel manquantes dans la version actuelle seront ajoutées. Les autres révisions demeurent inchangées.
 - **Remplacer le référentiel entièrement** : dans ce mode d'importation, le référentiel est entièrement remplacé par le référentiel importé.
 - Cochez la case **Importer les fichiers de configuration** pour importer les fichiers de configuration lors de l'importation du référentiel.
4. Cliquez sur le bouton **Importer** pour commencer l'importation.

10.11.6. Hashs de menaces connus

La section **Hashs de menaces connus** permet d'effectuer la recherche par le bulletin des hashs de menaces connus qui est fourni par le centre FinCERT et est inclus dans le produit 15-drwhashdb.



Cette section est disponible uniquement si les bulletins de hashes de menaces connus sont utilisés sous licence. La disponibilité de la licence est indiquée dans les informations sur la clé de licence que vous pouvez consulter dans la section [Gestionnaire de licences](#), le paramètre **Listes autorisées de bulletins de hashes** (il suffit d'avoir une seule licence dans une clé de licence utilisée par le Serveur Dr.Web).



L'absence d'une licence pour les bulletins de hashes ne baisse pas le niveau de protection antivirus. Cette licence permet d'ajouter une notification d'administrateur sur la présence de la menace détectée dans les bulletins spécialisés des hashes de menaces connus.



Le produit 15-drwhashdb est géré depuis la section **Administration > Configuration détaillée du référentiel > Hashs de menaces connus**.

Le tableau de la section contient les données suivantes :

- **Hash de menace** : hash de menace connu.
- **Nom du bulletin** : FinCERT_IOC.

Pour la recherche par les marges du tableau de hashes, cliquez sur .

En cas de détection d'une menace sur le poste (par le contrôle des applications, la protection préventive ou lors du scan) et lors de l'envoi des informations sur cette menace au Serveur Dr.Web, le Serveur compare son hash avec le hash de la liste FinCERT. S'ils sont identiques, le Serveur Dr.Web la marque comme présente dans le bulletin FinCERT. Ces informations sont présentes dans les tableaux des statistiques de menaces détectées, quand vous activez l'affichage de la colonne **Bulletin** dans la section **Réseau antivirus > Statistiques**.

La base de données contenant les hashes se trouve dans le fichier unique `hash-db` dans le répertoire suivant :

- sous Windows : `C:\Program Files\DrWeb Server\var\hash-db\,`
- sous Linux : `/var/opt/drwcs/hash-db/<numéro de révision>/hash.db`,
- sous FreeBSD : `/var/drwcs/hash-db/<numéro de révision>/hash.db`.

Notifications de détection de menaces par les hashes de menaces connus

Dans la section [Configuration des notifications](#), vous pouvez configurer l'envoi des notifications sur les correspondances détectées avec les hashes de menaces.

Les notifications suivantes sont disponibles :

- **Le Contrôle des applications a bloqué le processus de la liste des hashes de menaces connus**,
- **Menace détectée par les hashes de menaces connus**,



- **Erreur de scan lors de la détection d'une menace par les hashes de menaces connus,**
- **Rapport de la Protection préventive sur la détection de menaces par les hashes de menaces connus.**

Si vous gérez plusieurs Serveurs Dr.Web, cochez la case **Envoyer les notifications des événements du Serveur voisin Dr.Web en cas de détection de menaces par les hashes connus** pour envoyer à l'administrateur les notifications des événements reçus du Serveur subordonné Dr.Web configuré en cas de détection de menaces de sécurité par les hashes de menaces connus. Si la case est décochée, l'administrateur recevra les notifications des événements de son Serveur Dr.Web uniquement.

La case est disponible uniquement si l'utilisation des bulletins de hashes de menaces connus est autorisée par la licence.

Vous pouvez également configurer les notifications à l'aide des [procédures utilisateur](#).



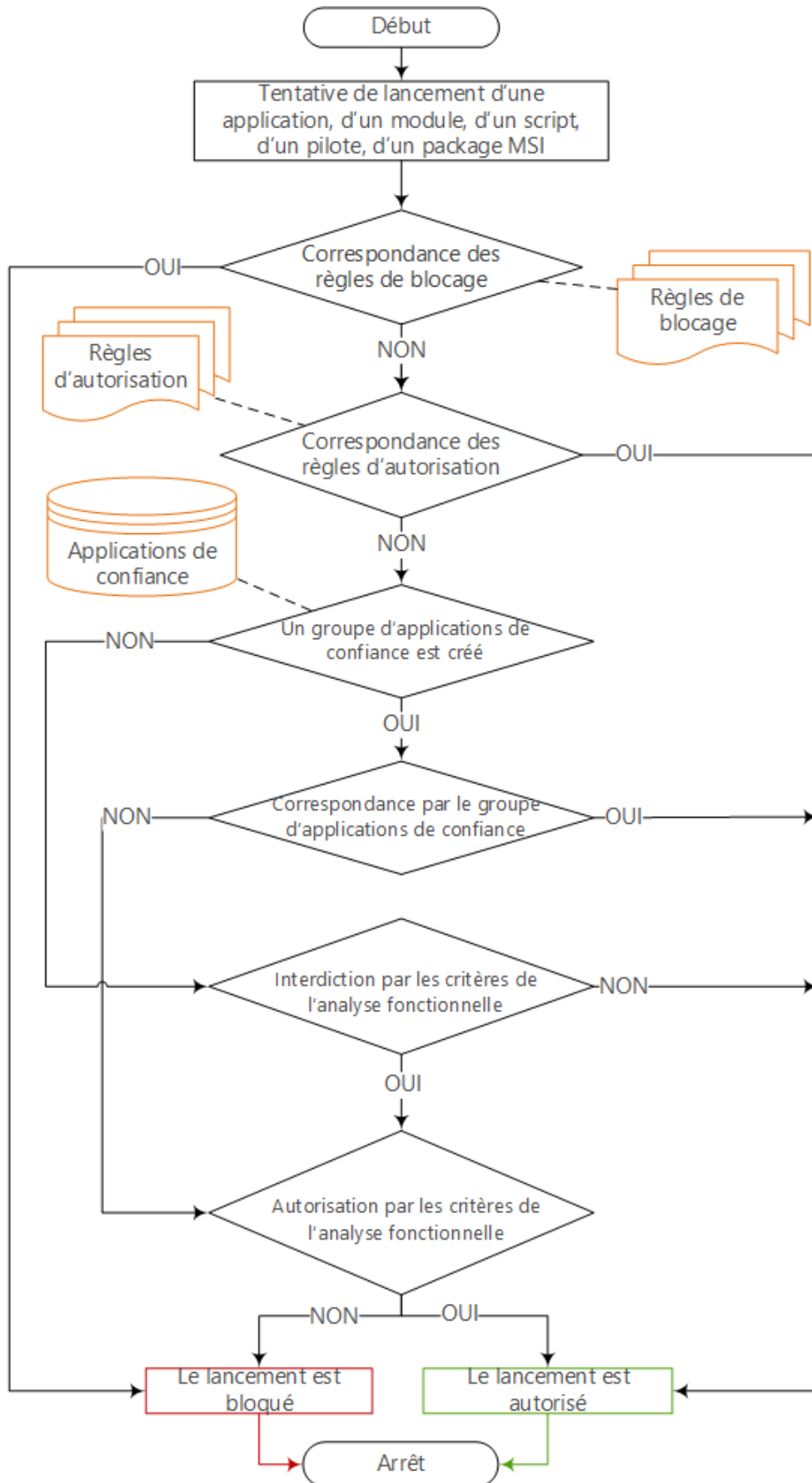
Si la licence du produit est manquante, les notifications sont automatiquement désactivées.

10.12. Contrôle des applications

Avec le composant Contrôle des applications, vous pouvez régler les applications, modules, interpréteurs de scripts, pilotes et packages MSI qui seront autorisés et ceux qui seront bloqués sur les postes du réseau antivirus sur lesquels l'Agent Dr.Web pour Windows est installé.



Vous trouverez le schéma de fonctionnement du Contrôle des applications ci-dessous.





Outils principaux du Contrôle des applications :

- **Profils** : ce sont des listes de règles qui déterminent lesquelles des applications peuvent être lancées sur les postes et lesquelles sont bloquées. Les profils sont créés par l'administrateur et ils sont assignés aux politiques, aux postes et aux utilisateurs, y compris aux groupes de postes et d'utilisateurs. Les profils déterminent le **mode de fonctionnement** du Contrôle des applications.

La configuration des profils se fait dans l'arborescence du réseau, dans la section **Réseau antivirus**.

- Liste des applications :
 - **Applications de confiance** : liste des applications qui est rédigée conformément aux règles spécifiées et obtenue depuis les postes sélectionnés par l'administrateur. Quand vous travaillez en **mode d'autorisation**, le lancement de ces applications sera toujours autorisé. Les groupes particuliers des applications de confiance sont sélectionnés dans les paramètres séparément pour chaque profil.
 - **Répertoire d'applications** : liste de toutes les applications installées sur les postes protégés. Le répertoire est créé automatiquement en tâche de fond et ne peut pas être modifié par l'administrateur.

La configuration de listes des applications se fait dans la section **Administration**.

- **Événements du Contrôle des applications** : informations sur les événements enregistrés sur les postes par le composant Contrôle des applications.

Vous pouvez consulter les événements du Contrôle des applications dans la section **Réseau antivirus** → **Statistiques**.

Modes principaux de fonctionnement du Contrôle des applications :

- **Analyse fonctionnelle** : ensemble des règles prédéfinies selon lesquelles le lancement des applications est autorisé ou bloqué conformément aux fonctions exécutées.
- **Mode d'autorisation** : ce mode implique que le lancement des applications de la liste des **Applications de confiance** et des applications relevant des règles d'autorisation est autorisé sur tous les postes contrôlés. Les autres applications sont bloquées.
- **Mode de blocage** : ce mode implique que le lancement des applications relevant des règles de blocage est bloqué sur tous les postes contrôlés. Les autres applications sont autorisées.



Vous pouvez activer ou désactiver les modes d'autorisation et de blocage ensemble ou séparément.

L'analyse fonctionnelle doit être toujours activée. Si toutes les règles de l'analyse fonctionnelle sont désactivées, le contrôle de lancement des applications ne s'effectue pas.

Pour configurer le Contrôle des applications

1. **Créer un nouveau profil**.



2. [Assignez les postes, les utilisateurs et les groupes](#) sur lesquels seront diffusés les paramètres du profil créé.
3. [Spécifiez les paramètres du profil.](#)




Il est recommandé de configurer les profils en mode de test.


10.12.1. Mode de test

Pour vous assurer des performances d'un profil ou d'une règle configuré, vous pouvez utiliser le *mode test* dans lequel le Contrôle des applications imite son fonctionnement. Dans ce mode, les applications ne sont pas bloqués mais le l'activité est journalisée (voir [Événements du Contrôle des applications](#)) comme si le profil ou la règle fonctionne de manière ordinaire. Le mode de test est pratique pour la configuration du Contrôle des applications effectuée par l'administrateur lors du déploiement du réseau de l'entreprise.

Pour activer le mode de test pour le profil

1. Dans la section **Général** des propriétés du profil, cochez la case **Activer le profil** pour commencer à utiliser ce profil (par défaut désactivé).
2. Cochez la case **Faire basculer le profil en mode de test global.**
3. Cliquez sur **Enregistrer.**

Dans le mode de test, le profil correspondant du groupe **Profiles** aura l'icône  dans l'arborescence du réseau. Sur les postes auxquels ce profil est assigné, les applications lancées ne seront pas bloquées selon les critères de l'analyse fonctionnelle, les règles d'autorisation et de blocage. Au lieu de cela, les statistiques seront collectées dans la section **Réseau antivirus** → **Statistiques** → **Événements du Contrôle des applications**. Ce journal contient les informations détaillées sur chaque application lancée. En analysant ces informations, vous pouvez configurer les paramètres du profil selon vos besoins.

Une fois assuré, que le profil testé fonctionne comme correctement, vous devez le passer du mode de test en mode actif. Le profil actif a l'icône  dans le groupe **Profiles** dans l'arborescence du réseau antivirus.

Pour désactiver le mode de test pour le profil

1. Dans la section **Général** de propriétés du profil, décochez la case **Faire basculer le profil en mode de test global.**
2. Cliquez sur **Enregistrer.**

Le mode test peut être utilisé pour la vérification de certaines règles d'autorisation et de blocage dans le profil, sans passer entièrement en mode test du profil.



Pour activer le mode test pour une règle d'autorisation ou de blocage au sein du profil

1. Dans la section **Règles d'autorisation** ou **Règles de blocage** de propriétés du profil, sélectionnez une règle créée dont vous voulez tester le fonctionnement.
2. Dans les paramètres de règle qui s'ouvrent, cochez la case **Activer la règle** et **Faire basculer la règle en mode de test**.
3. Cliquez sur **Enregistrer**.

Dans ce mode, les logiciels lancés sur les postes **seront bloqués**, mais seulement selon les critères d'analyse fonctionnelle et les règles qui ne sont pas passées en mode test. Les règles d'autorisation et de blocage en mode test fonctionnent comme les profils dans ce mode : leur configurations n'affectent pas le blocage de logiciels, mais le résultat de chaque déclenchement est enregistré dans le journal d'activité dans la section *Événements du Contrôle des applications*.



A la différence du mode test de profils, la présence de règles dans le mode test n'affecte pas l'icône du profil concerné dans l'arborescence de réseau antivirus. Le profil actif avec les règles en mode test aura l'icône

Une fois assuré que la règle testée fonctionne correctement, passez-la du mode test au mode actif.

Pour désactiver le mode test pour une règle d'autorisation ou de blocage au sein du profil

1. Dans la section **Règles d'autorisation** ou **Règles de blocage** de propriétés du profil, sélectionnez la règle testée.
2. Dans les paramètres qui s'ouvrent, décochez la case **Faire basculer la règle en mode de test**.
3. Cliquez sur **Enregistrer**.

10.12.2. Applications de confiance

Gestion des applications de confiance

Le *Groupe des applications de confiance* (ou la liste blanche d'applications) représente une liste des applications classées selon les critères spécifiés du poste ou du groupe de postes sélectionné. Ces applications sont autorisées pour le lancement sur les postes du réseau antivirus pour lesquels il sont ajoutées dans le [profil](#) du composant Contrôle des applications lors du fonctionnement en [mode d'autorisation](#).

La collecte d'informations pour la formation d'un groupe d'applications de confiance est un processus principal qui, en fonction de critères spécifiés, peut ralentir considérablement l'ordinateur utilisé. Pour diminuer la charge sur les postes du réseau antivirus, il faut collecter les informations sur un ou plusieurs *postes de références* - les ordinateurs sélectionnés spécialement



pour cette tâche. Un candidat idéal pour ce rôle est ordinateur avec le système d'exploitation qui vient d'être installé, les dernières mises jour et tous le logiciels nécessaires.

Pour gérer les applications de confiance sur les Serveurs Dr.Web collectant les informations, accédez à la section **Administration** → **Contrôle des applications** → **Applications de confiance**.

La table de la section contient la liste de tous les groupes des applications de confiances.

Les boutons suivants de gestion sont disponibles dans la barre d'outils :

- + [Créer un groupe des applications de confiance](#)
- ↻ [Redémarrez la création du groupe des applications de confiance](#)
- 🗑️ [Supprimer un groupe des applications de confiance](#)

Pour créer un nouveau groupe des applications de confiance

1. Dans la section **Applications de confiance**, cliquez sur le bouton **+ Créer un groupe des applications de confiance** dans la barre d'outils.
2. Dans la fenêtre **Général**, spécifiez les paramètres suivants :
 - **Non de groupe** : nom du groupe des applications de confiance créé.
 - **Description** : une description arbitraire et non obligatoire du groupe créé.Cliquez sur le bouton **Suivant**.
3. Dans la fenêtre **Paramètres d'ajout des applications aux applications de confiance**, spécifiez les paramètres selon lesquels les applications sur les postes seront ajoutées dans le groupe des applications de confiance créé (au moins un paramètre doit être sélectionné dans chaque catégorie) :

Cochez la case **Attribuer une priorité basse au processus de collecte des informations** si la collecte d'informations pour le groupe créée d'applications de confiance aura lieu sur le poste dont les ressources système ne doivent pas être entièrement occupées par cette tâche.



L'activation de ce paramètre aidera à économiser les ressources de l'ordinateur utilisées pour la collecte des informations. Pourtant, la durée d'exécution de cette opération peut augmenter de manière considérable.

- **Zone de recherche** : cochez les cases des zones dans lesquelles seront collectées les informations sur les applications.



Dans l'option **Chercher dans les chemins spécifiés**, vous pouvez spécifier plusieurs chemins pour chercher les applications. Utilisez « ; » pour les séparer.

- **Types de hashes ajoutés** : cochez les cases des objets dont les hashes seront enregistrés dans le groupe d'applications de confiance créé.
- **Catégories de fichiers** : cochez les cases des fichiers à ignorer lors de la recherche.



Cliquez sur le bouton **Suivant**.

4. Dans l'arborescence du réseau, sélectionnez les postes et les groupes de postes pour lesquels les informations sur les applications seront collectées pour les inclure dans la liste des applications de confiance. Pour sélectionner plusieurs groupes et postes, utilisez les boutons CTRL et SHIFT.

Cochez la case **Ignorer les groupes emboîtés** pour collecter les informations sur les postes du groupe sélectionné uniquement. Si la case est décochée, les informations de tous les postes du groupe sélectionné et de ses sous-groupes sont collectées.

5. Cliquez sur **Enregistrer**.
6. Une collecte des informations sur les applications de poste va commencer selon les paramètres spécifiés. Ce processus peut prendre beaucoup de temps.


Vous pouvez consulter les informations sur l'état et la mise à jour du groupe des applications de confiance :

- dans le tableau principal de la section **Applications de confiance**,
- dans les informations supplémentaires sur le groupe qui s'ouvrent quand vous cliquez sur la ligne correspondant au groupe dans le tableau principal de la section **Applications de confiance**.




Les informations sur les applications sont collectées au cours de la séance courante sur le poste utilisé. Si la collecte d'informations n'a pas terminé, mais le poste a été arrêté ou redémarré, l'opération poursuivra après la mise en route. Les données sur les applications collectées partiellement ne sont pas enregistrées.

Pour lancer une mise à jour d'un groupe des applications de confiance

1. Dans la section **Applications de confiance** du tableau de section, cochez les cases contre les groupes que vous voulez mettre à jour.
2. Cliquez sur le bouton  **Redémarrez la création du groupe des applications de confiance** dans la barre d'outils.

Pour supprimer un groupe des applications de confiance

1. Dans la section **Applications de confiance** du tableau de section, cochez les cases contre les groupes que vous voulez supprimer du profil.
2. Cliquez sur le bouton  **Supprimer le groupe des applications de confiance** dans la barre d'outils.
3. Les applications de ce groupe seront supprimées de la liste des applications autorisées pour le lancement sur les postes et la collecte des applications pour la liste des applications de confiance selon les critères de ce groupe sera arrêtée.




Impossible de supprimer le groupe d'applications de confiance assigné aux profils du Contrôle des applications.



Quand vous supprimez des groupes d'applications de confiance, une nouvelle révision est créée dans le référentiel pour le produit **Applications de confiance**. Cette révision est distribuée aux Serveurs voisins Dr.Web. Cela peut perturber le fonctionnement des profils du Contrôle des applications auxquels ce groupe est assigné sur les Serveurs voisins Dr.Web.

Pour supprimer les informations sur les applications sur un poste particulier du groupe des applications de confiance

1. Dans la section **Applications de confiance** du tableau de section, cliquez sur la ligne du groupe d'application depuis lequel vous voulez supprimer les informations sur les applications du poste.
2. Dans la fenêtre qui s'ouvre, cochez les cases des postes sur lesquels vous voulez supprimer les informations sur les applications.
3. Cliquez sur le bouton  **Supprimer les postes sélectionnés** dans la barre d'outils.



En cas de suppression de tous les postes, le groupe d'applications de confiance sera supprimé.

Référentiel des applications de confiance



Quand vous configurez le mode d'autorisation pour le [profil](#) du Contrôle des applications, les groupes d'applications de confiance sont sélectionnés dans la liste des groupes disponibles dans le référentiel du produit **Applications de confiance**.

Si votre réseau antivirus comprend plusieurs Serveurs Dr.Web unis par une liaison entre serveurs, vous avez la possibilité de partager la charge entre vos Serveurs Dr.Web pour faciliter la collecte des informations :

- Sur l'un des Serveurs Dr.Web, l'administrateur collecte les informations concernant les postes protégés. Les informations sont placées automatiquement dans le référentiel du Serveur Dr.Web, dans le produit **Applications de confiance** et elles sont distribuées par la liaison entre les serveurs [selon les paramètres spécifiés](#).
Les informations sur les applications de confiance peuvent être collectées sur plusieurs Serveurs Dr.Web du réseau, mais les segments du réseau traité par ces Serveurs Dr.Web doivent être isolés l'un de l'autre.
- Les autres Serveurs Dr.Web obtiennent la mise à jour du produit **Applications de confiance** par la liaison entre serveurs conformément aux [paramètres spécifiés](#). Il n'est pas nécessaire de configurer la collecte des informations sur les applications de confiance sur ces Serveurs Dr.Web car les révisions de produit obtenues du Serveur voisin Dr.Web seront placées dans le référentiel.



Le produit **Applications de confiance** n'est pas mis à jour depuis le SGM. La distribution de ce produit est possible uniquement par les liaisons entre les Serveurs voisins Dr.Web.

Avant la collecte des Applications de confiance, déterminez les Serveurs Dr.Web qui collecteront les informations et les enverront aux Serveurs voisins Dr.Web et les Serveurs Dr.Web qui recevront ces informations par la liaison entre serveurs. C'est en fonction de cela qu'il faut configurer chaque Serveur Dr.Web.

Pour configurer les Serveurs Dr.Web collectant et obtenant les applications de confiance

1. Ouvrez la section **Administration**.
2. Accédez à la section **Configuration détaillée du référentiel** → **Applications de confiance**.
3. Dans l'onglet **Synchronisation**, décochez la case **Bloquer la transmission des mises à jour aux Serveurs voisins Dr.Web** et cochez la case **Bloquer la réception des mises à jour des Serveurs voisins Dr.Web**.
4. Cliquez sur **Enregistrer**.
5. Accédez à la section **Administration** → **Contrôle des applications** → **Applications de confiance** et configurez la collecte des applications de confiance, comme cela est décrit [ci-dessous](#).
6. La nouvelle révision du produit **Applications de confiance** est enregistrée dans le référentiel après la réception des informations de tous les postes indiqués dans les paramètres de collecte des groupes d'applications de confiance. Après l'enregistrement de la révision dans le référentiel, elle est distribuée par la liaisons aux Serveurs voisins Dr.Web.

Pour configurer les Serveurs Dr.Web obtenant les applications de confiance

1. Ouvrez la section **Administration**.
2. Accédez à la section **Configuration détaillée du référentiel** → **Applications de confiance**.
3. Dans l'onglet **Synchronisation**, décochez la case **Bloquer la réception des mises à jour des Serveurs voisins Dr.Web**.
Si le Serveur Dr.Web doit transmettre le produit **Applications de confiance** aux autres Serveurs Dr.Web par la liaison entre serveurs, décochez la case **Bloquer la transmission des mises à jour aux Serveurs voisins Dr.Web**.
4. Cliquez sur **Enregistrer**.

10.12.3. Répertoire d'applications

Pour consulter le répertoire d'applications, accédez à la section **Administration** → **Contrôle des applications** → **Répertoire d'applications**.

Le répertoire d'applications contient les informations sur les applications installées sur les postes protégés tournant sous Windows, connectés au Serveur Dr.Web.



Le répertoire est créé automatiquement en tâche de fond et ne peut pas être modifié par l'administrateur après la collecte. Les informations sur chaque application sont envoyées par l'Agent Dr.Web sur le Serveur Dr.Web une seule fois, après la première activité de cette application.

Le répertoire peut être utilisé dans les cas suivants :

- Pour obtenir les informations sur les applications installées sur les postes du réseau.
- Pour créer les règles d'[autorisations](#) et les règles de [blocage](#). L'utilisation du répertoire facilite la création des règles car toutes les informations sur une applications sont remplies automatiquement à partir de données sur l'application connue sélectionnée.

Remplissage du répertoire des applications

Pour activer l'envoi des informations du poste pour le répertoire d'applications

1. Dans la section **Réseau antivirus**, sélectionnez dans l'arborescence un poste ou un groupe de postes avec le Contrôle des applications installé depuis lequel vous voulez recevoir les informations concernant les applications installées.
2. Dans le menu de gestion, sélectionnez **Windows** → **Agent Dr.Web** si un groupe a été sélectionnée ou **Agent Dr.Web** si un poste a été sélectionné
3. Dans l'onglet **Général**, cochez la case **Suivre les événements du Contrôle des applications** pour suivre toute l'activité des processus sur les postes enregistrée par le Contrôle des applications et envoyer les événements sur le Serveur Dr.Web. S'il n'y a pas de connexion au Serveur, les événements sont accumulés et envoyés, une fois la connexion établie. Si la case est décochée, seuls les événements de blocages peuvent être envoyés (en fonction des paramètres dans la configuration du Serveur Dr.Web).
4. Cliquez sur **Enregistrer**.

Pour activer la collecte des informations par le Serveur Dr.Web pour le répertoire d'applications

1. Ouvrez la section **Administration** → **Configuration du Serveur Dr.Web**.
2. Ouvrez l'onglet **Statistiques** et spécifiez l'une des options suivantes :
 - **Statistiques du Contrôle des applications sur l'activité des processus** pour obtenir et enregistrer les informations sur toute activité de tous les processus dont le lancement est autorisé ou bloqué par le Contrôle des applications. Si vous choisissez cette option, les applications seront enregistrées dans le répertoire seulement après la création et l'assignation d'au moins un [profil](#) avec une ou plusieurs catégories de [critères d'analyse fonctionnelle](#) sélectionnées.
Avant la création de profils et leur assignation aux postes du réseau antivirus, le lancement de toutes les applications est autorisé.



- **Statistiques du Contrôle des applications sur l'activité des processus** pour obtenir et enregistrer les informations sur l'activité de tous les processus dont le lancement est bloqué par le Contrôle des applications. Si vous choisissez cette option, les applications seront enregistrées dans le répertoire seulement après la création des [profils](#) dont les paramètres bloqueront le lancement des applications et l'assignation de ces profils aux postes du réseau antivirus.



La case **Statistiques du Contrôle des applications sur l'activité des processus** peut augmenter considérablement la charge de la collecte des statistiques sur tout le réseau antivirus.

3. Cliquez sur **Enregistrer**.
4. Redémarrez le Serveur Dr.Web.
5. Après le redémarrage, le Serveur Dr.Web commencera à enregistrer, selon les paramètres spécifiés, les statistiques de lancement des applications envoyées depuis tous les postes avec le Contrôle des applications installé.

Création des règles du répertoire d'applications

Pour créer une nouvelle règle à partir de données du répertoire d'applications

1. Dans la section **Répertoire d'applications**, sélectionnez la ligne de l'application pour laquelle vous voulez créer une règle contrôlant le lancement.
2. Quand vous cliquez sur une ligne de la table, une fenêtre contenant les informations sur l'application sélectionnée s'ouvre.
3. Cliquez sur le bouton **Créer une règle**.
4. Une fenêtre de création d'une nouvelle règle s'ouvre. Spécifiez les paramètres suivants :
 - a) Dans la liste déroulante **Nom de profil**, sélectionnez un [profil](#) du Contrôle des applications dans lequel la règle sera créée.
 - b) Dans le champ **Nom de règle**, spécifiez un nom pour la règle créée.
 - c) Pour l'option **Type de règle**, sélectionnez le type de la règle créée : une règle de [blocage](#) ou une règle d'[autorisation](#).
 - d) Pour l'option **Mode de fonctionnement**, sélectionnez un mode dans lequel la règle créée fonctionnera (cela correspond à la case **Faire basculer la règle en mode test** lors de la création de la règle depuis le profil) :

Si vous voulez tester la règle, sélectionnez le mode **Test**. Les applications sur les postes ne seront pas contrôlées, pourtant l'activité sera journalisée comme si les paramètres étaient activés. Les résultats de lancements et de blocages d'applications en mode test s'afficheront dans la section [Événements du Contrôle des applications](#).

En mode **Actif**, la règle fonctionnera en mode actif avec le blocage des applications sur les postes conformément aux paramètres de règle spécifiés (voir aussi les [modes de fonctionnement des profils](#)).



- e) Dans la section **Bloquer le lancement des applications selon les critères suivants/Autoriser le lancement des applications selon les critères suivants** (en fonction du type de règle sélectionnée à l'étape 4c), les champs seront automatiquement remplis conformément à l'application sur laquelle la règle est basée. Si nécessaire, vous pouvez modifier les valeurs des paramètres.
5. Cliquez sur **Enregistrer**. La règle sera créée dans le profil spécifié du Contrôle des applications.

10.13. Options supplémentaires

10.13.1. Gestion de la base de données

La rubrique **Gestion de la base de données** permet de maintenir la base de données avec laquelle fonctionne le Serveur Dr.Web.

La section **Général** contient les paramètres suivants :

- Le champ **Dernière maintenance de la BD** — la date de la dernière exécution de commandes de maintenance de la base de données de cette rubrique.
- La liste de commandes de maintenance de la base de données contient :
 - Commandes analogues aux tâches de la [planification du Serveur Dr.Web](#). Les noms de commandes correspondent aux noms de tâches de la rubrique **Actions** dans la planification du Serveur Dr.Web (les tâches correspondantes de la planification sont décrites dans le tableau [Types de tâches et leurs paramètres](#)).
 - Commande **Analyse de la base de données**. Cette commande est destinée à optimiser la base de données du Serveur Dr.Web via l'exécution de la commande `analyze`.
 - Commande **Suppression des postes non activés**. Elle est destinée à supprimer les comptes des postes qui ont été créés dans le réseau antivirus mais qui n'ont jamais été connectés au Serveur Dr.Web. Il faut indiquer la période à l'issue de laquelle les comptes seront supprimés.
Vous pouvez consulter la liste des comptes non utilisés dans l'arborescence du réseau antivirus, dans le groupe **Status** → **New**.

Pour exécuter les commandes de maintenance de la base de données

1. Dans la liste de commandes cochez les cases contre les commandes que vous voulez exécuter.
Si nécessaire, modifiez les délais de temps pour les commandes d'effacement de la base de données, après lesquels l'information sauvegardée est considérée comme obsolète et doit être supprimée du Serveur Dr.Web.
2. Cliquez sur **Appliquer maintenant**. Toutes les commandes seront exécutées tout de suite.
Pour l'exécution automatique reportée et/ou périodique de ces commandes (sauf la commande **Analyse de la base de données**), utiliser le [Planificateur des tâches du Serveur Dr.Web](#).




Pour gérer la base de données, utilisez les boutons situés dans la barre d'outils :

 [Importer](#),

 [Exporter](#).

Exportation de la base de données

Pour enregistrer l'information de la base de données dans un fichier

1. Dans la barre d'outils , cliquez sur le bouton **Exporter**.
2. Dans la fenêtre des paramètres d'exportation, sélectionnez une des variantes :
 - **Exporter toute la base de données** pour enregistrer toute l'information de la base de données dans l'archive gz. Le fichier XML obtenu lors de l'exportation est analogue au fichier d'exportation de la base de données obtenu lors du lancement du fichier exécutable du Serveur Dr.Web depuis la ligne de commande avec la clé `modexecdb database-export-xml`. Ce fichier d'exportation peut être importé lors du lancement du fichier exécutable du Serveur Dr.Web depuis la ligne de commande avec la clé `modexecdb database-import`. Ces commandes sont décrites en détails dans les **Annexes**, [G3.3. Commandes de gestion de la BD](#).
 - **Exporter les informations sur les postes et les groupes** pour enregistrer les informations sur les objets du réseau antivirus dans une archive zip. En cas d'exécution de cette opération, toute l'information sur les groupes de postes et les comptes des postes du réseau antivirus maintenu par ce Serveur Dr.Web est sauvegardée dans un fichier au format spécial. Le fichier d'exportation comprend les informations suivantes sur les postes : propriétés, configuration des composants, droits, paramètres de limitations de mises à jour, planification, liste des composants à installer, statistiques, informations sur les postes supprimés, sur les groupes : propriétés, configuration des composants, droits, paramètres de limitations de mises à jour, planification, liste des composants à installer, statistiques, identificateur du groupe parent. Ensuite le fichier d'exportation peut être [importé](#) via la rubrique **Gestion de la base de données**.
 - Dans l'arborescence **Réseau antivirus**, vous pouvez sélectionner un ou plusieurs groupes utilisateurs. Dans ce cas, seules les informations sur les groupes sélectionnés et les postes pour lesquels les groupes sélectionnés sont primaires sont exportées. Si aucun groupe n'est sélectionné, les informations sur tous les postes et les groupes utilisateurs du réseau antivirus seront exportées.
3. Cliquez sur le bouton **Exporter**.
4. La spécification du chemin de sauvegarde de l'archive avec la base de données s'effectue conformément aux paramètres du navigateur web dans lequel le Centre de gestion est ouvert.



En cas de grande quantité de données, le délai d'exportation peut dépasser la durée de la session. Si la durée de la session s'écoule avant la fin de l'exportation, l'exportation sera automatiquement arrêtée et le fichier de données d'exportation ne sera pas généré.

Importer la base de données

La procédure de l'importation du fichier de la base de données contenant les informations sur les objets du réseau antivirus peut être utilisée pour transmettre les informations sur un nouveau Serveur Dr.Web, ainsi que sur un Serveur Dr.Web qui fonctionne déjà au sein du réseau antivirus, notamment pour fusionner les listes de postes maintenus de deux Serveurs Dr.Web.



Tous les postes, les informations sur lesquels sont importées, peuvent se connecter au Serveur Dr.Web sur lequel l'importation est effectuée. En cas d'importation, prenez en compte la nécessité d'avoir une quantité suffisante des licences disponibles pour la connexion des postes transférés. Par exemple, si nécessaire, dans la section [Gestionnaire de licences](#) ajoutez une clé de licence depuis le Serveur duquel les informations sur les postes sont transférés.

Pour charger une base de données depuis un fichier

1. Dans la barre d'outils, cliquez sur le bouton **Importer**.
2. Dans la fenêtre d'importation, spécifiez l'archive zip avec le fichier de la base de données. Pour sélectionner un fichier, utilisez le bouton .

On peut importer seulement les archives zip obtenus lors de l'exportation de la base de données pour la variante **Exporter les informations sur les postes et les groupes**.

3. Cliquez sur le bouton **Importer** pour commencer l'importation.
4. Si lors de l'import sont détectés les postes et/ou les groupes ayant le même identificateur, inclus dans les données à importer et ainsi que dans la base de données du Serveur Dr.Web actuel, la rubrique **Collisions** va s'afficher pour déterminer les actions à appliquer sur les objets doublés.

Les listes des groupes et des postes sont présentés dans des tableaux différents.

Sélectionnez une variante de résolution d'une collision dans la liste déroulante **Mode de l'importation des groupes** ou **Mode de l'importation des postes** pour le tableau des objets correspondant :

- **Enregistrer les données de l'importation pour tous** : supprimer de la base de données du Serveur actuel Dr.Web toutes les informations sur les objets doublés et réécrire la base de données avec les informations de la base de données importée. L'action s'applique à tous les objets doublés de ce tableau en même temps.
- **Enregistrer les données actuelles pour tous** : sauvegarder dans la base de données du Serveur actuel Dr.Web toutes les informations sur les objets doublés. Les informations sur les objets doublés de la base de données importée seront ignorées. L'action s'applique à tous les objets doublés de ce tableau en même temps.



- **Sélectionnez manuellement** : spécifier manuellement une action pour chaque objet doublé en particulier. Dans ce mode, vous pourrez éditer la liste des objets doublés. Spécifiez les options contre les objets qui seront sauvegardés.

Cliquez sur **Enregistrer**.

10.13.2. Statistiques du Serveur Dr.Web

A l'aide du Centre de gestion vous pouvez consulter les statistiques du fonctionnement du Serveur Dr.Web au niveau de l'utilisation des ressources système de l'ordinateur sur lequel le Serveur Dr.Web est installé et de l'interaction avec les composant du réseau antivirus et les ressources externes comme SGM.

Pour consulter les statistiques du fonctionnement du Serveur Dr.Web :

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion.
2. Dans la fenêtre qui s'affiche, sélectionnez l'élément du menu de gestion **Statistiques du Serveur Dr.Web**.
3. Dans la fenêtre qui s'affiche, sont présentées les rubriques suivantes de données statistiques :
 - **Activité des clients** : les données relatives à la quantité des clients servis qui sont connectés à ce Serveur Dr.Web : des Agents Dr.Web, des Serveurs voisins Dr.Web et des installateurs des Agents Dr.Web.
 - **Trafic réseau** : paramètres du trafic entrant et sortant lors de l'échange des données avec le Serveur Dr.Web.
 - **Utilisation des ressources système** : paramètres d'utilisation des ressources système de l'ordinateur sur lequel le Serveur Dr.Web est installé.
 - **Microsoft NAP** : paramètres de fonctionnement de [NAP Validator](#).
 - **Utilisation de la base de données** : paramètres de connexion à la base de données du Serveur Dr.Web.
 - **Utilisation du cache de fichiers** : paramètres de l'appel au cache de fichiers de l'ordinateur sur lequel le Serveur Dr.Web est installé.
 - **Utilisation du cache DNS** : paramètres de l'appel au cache qui sauvegarde les requêtes au serveurs DNS de l'ordinateur sur lequel le Serveur Dr.Web est installé.
 - **Notifications** : paramètres de fonctionnement du sous-système de [notifications](#) de l'administrateur.
 - **Référentiel** : paramètres de l'échange de données du référentiel du Serveur Dr.Web avec les serveurs du SGM.
 - **Statistiques Web** : paramètres de l'envoi des statistiques des infections sur les serveurs de Doctor Web.
 - **Statistiques du serveur web** : paramètres de l'appel au Serveur Web.
 - **Cluster** : paramètres d'appels via le protocole de synchronisation entre les serveurs en cas d'utilisation du cluster de Serveurs Dr.Web dans la configuration multi-serveurs du réseau.



- **Transmission des mises à jour de groupe** : paramètres d'échange de données lors de la transmission des [mises à jour de groupe](#) aux postes de travail via le protocole multicast.
4. Pour consulter les données statistiques d'une rubrique en particulier, cliquez sur le nom de la rubrique nécessaire.
 5. Dans la liste qui s'affiche sont présentés les paramètres de la rubrique avec les compteurs dynamiques de valeurs.
 6. En même temps, quand la rubrique de statistiques ouvre, la représentation graphique des modifications pour chaque paramètre est activée. Dans ce cas :
 - Pour désactiver la représentation graphique, cliquez sur le nom de la rubrique nécessaire. En cas de désactivation de la représentation graphique, la valeur numérique de paramètres sera actualisée d'une façon dynamique.
 - Pour réactiver la représentation graphique de données, cliquez encore une fois sur le nom de la rubrique nécessaire.
 - Les noms des rubriques et de leurs paramètres pour lesquels la représentation graphique est activée sont en gras.
 7. Pour modifier la fréquence de mise à jour de données, sélectionnez l'intervalle souhaité dans la liste déroulante **Périodicité de mises à jour**. Le nouvel intervalle sera automatiquement appliqué aux données numériques et graphiques.
 8. Si vous passez la souris sur les données graphiques, une valeur numérique du point sélectionné s'affiche sous forme de :
 - **Abs** : valeur absolue du paramètre.
 - **Delta** : accroissement de la valeur du paramètre par rapport à sa valeur précédente conformément à la périodicité de la mise à jour de données.
 9. Pour masquer les paramètres de la rubrique, cliquez sur la flèche à droite du nom de la rubrique. Quand les paramètres de la rubrique sont masqués, la représentation graphique des statistiques se vide et n'apparaît qu'en cas d'une nouvelle ouverture.

10.13.3. Copies de sauvegarde

La rubrique **Copies de sauvegarde** permet de consulter les copies de sauvegarde au niveau de répertoires et de fichiers et d'enregistrer en mode local le contenu de copies de sauvegarde des données critiques du Serveur Dr.Web.

Les objets suivants sont sauvegardés : paramètres du référentiel, fichiers de configuration, clés de chiffrement, certificats, copie de sauvegarde de la base de données interne.

Les copies de données critiques du Serveur Dr.Web sont sauvegardées dans les cas suivants :

- En cas d'exécution de la tâche **Copie de sauvegarde des données critiques du Serveur** selon la [planification](#) du Serveur Dr.Web.
- En cas de lancement du fichier exécutable du Serveur Dr.Web depuis la ligne de commande avec la clé `backup`. Vous pouvez consulter la description détaillée de cette commande dans les **Annexes**, [G3.5. Copie de sauvegarde des données critiques du Serveur Dr.Web](#).



Consulter les informations sur les copies de sauvegarde

Pour consulter les informations sur la copie de sauvegarde, sélectionnez dans l'arborescence l'objet relatif à la copie nécessaire. Les copies de sauvegarde se placent dans l'arborescence conformément aux répertoires de stockage :

- pour le Serveur Dr.Web sous OS Linux : `/var/opt/drwcs/backup`,
- pour le Serveur Dr.Web sous OS FreeBSD : `/var/drwcs/backup`,
- pour le Serveur Dr.Web sous OS Windows : `C:\DrWeb Backup`,
- et tous les chemins d'accès aux copies de sauvegarde indiqués dans les tâches de la planification du Serveur Dr.Web.

Si le chemin vide est indiqué dans les tâches du Serveur Dr.Web sous Windows, le répertoire `C:\Program Files\DrWeb Server\var\backup` sera utilisé par défaut. Vous pouvez voir les informations seulement sur les copies de sauvegarde qui sont stockées dans les répertoires du Serveur Dr.Web.




En cas de modification du répertoire d'enregistrement de la copie de sauvegarde dans une tâche déjà créée, le répertoire créé précédemment ne s'affichera pas dans l'interface Web. Dans ce cas, il vous faudra créer une nouvelle tâche pour le nouveau répertoire.


Quand vous sélectionnez les répertoires et les fichiers des copies de sauvegarde, le panneau de propriétés va s'afficher. Ce panneau contient les informations suivantes sur l'objet : **Type**, **Taille** (seulement pour les fichiers particuliers), **Date de création** et **Date de modification**.

Gérer de copies de sauvegarde

Pour gérer les copies de sauvegarde, utilisez les options situées dans la barre d'outils :

 **Exporter** : sauvegarder la copie de l'objet sélectionné sur l'ordinateur sur lequel le Centre de gestion est lancé.

 **Copie de sauvegarde** : sauvegarder les données critiques du Serveur Dr.Web.

 **Supprimer les objets sélectionnés** : supprimer les objets sélectionnés dans l'arborescence sans possibilité de restauration.


Exporter la copie de sauvegarde

Pour sauvegarder la copie en mode local


1. Dans l'arborescence sélectionnez les copies de sauvegarde nécessaires (pour sélectionner une copie entière il suffit de sélectionner dans l'arborescence le répertoire correspondant à cette copie de sauvegarde) ou les fichiers particuliers de copies de sauvegarde. Pour sélectionner plusieurs objets utilisez les boutons CTRL ou SHIFT.



Lors de l'exportation, prenez en compte les types principaux des objets exportés :

- a) Les archives zip de copies sont sauvegardés pour les objets sélectionnés suivants :
 - Une ou plusieurs copies entières (si vous sélectionnez les répertoires correspondant aux copies de sauvegarde).
 - Plusieurs fichiers particuliers inclus dans les copies de sauvegarde.
 - b) Fichiers particuliers inclus dans les copies de sauvegarde. Si vous avez sélectionné un seul fichier à exporter, il sera sauvegardé dans son état initial sans être archivé.
2. Cliquez sur  **Exporter** dans la barre d'outils.
 3. La spécification du chemin de sauvegarde des objets sélectionnés s'effectue conformément aux paramètres du navigateur web dans lequel le Centre de gestion est ouvert.

Copie de sauvegarde

Pour créer une copie de sauvegarde de données critiques du Serveur Dr.Web, cliquez sur  **Copie de sauvegarde** dans la barre d'outils. Les données seront sauvegardées dans une archive gz. Les fichiers obtenus lors de la copie de sauvegarde sont analogues aux fichiers obtenus lors du lancement du fichier exécutable du Serveur Dr.Web depuis la ligne de commande avec la clé `backup`.

Vous pouvez consulter la description détaillée de cette commande dans le document **Annexes**, [G3.5. Copie de sauvegarde des données critiques du Serveur Dr.Web](#).

10.13.4. Utilitaires



L'ensemble d'utilitaires dépend des paramètres du référentiel du Serveur Dr.Web. Pour activer ou désactiver la réception des mises à jour depuis le SGM pour les utilitaires disponibles dans cette section, accédez à la section **Administration** → **Configuration générale du référentiel** → **Packages d'installation Dr.Web** → [Utilitaires de gestion Dr.Web](#).

Dans la section **Utilitaires**, vous pouvez télécharger les utilitaires supplémentaires nécessaires pour le fonctionnement de Dr.Web Enterprise Security Suite :

- [Chargeur du référentiel Dr.Web](#)

Il sert à télécharger les produits de Dr.Web Enterprise Security Suite depuis le Système global de mise à jour. La version graphique du Chargeur du Référentiel Dr.Web est disponible uniquement sous Windows.

- **Utilitaire Dr.Web de collecte des informations sur le système**

L'utilitaire sert à créer un rapport sur l'état du système et tous les programmes installés, y compris les solutions antivirus Dr.Web pour les postes protégés et le logiciel du Serveur



Dr.Web. L'archive de rapport peut être utilisée pour le diagnostic par l'administrateur du réseau antivirus. Elle peut également être envoyée au support technique de Doctor Web.

- **Utilitaire de génération des clés numériques et des certificats**

Il permet de générer les clés de chiffrement et les certificats numériques, ainsi que créer et vérifier la signature numérique des fichiers. C'est un outil important assurant la sécurité des connexions entre les composants du réseau antivirus.

- **Utilitaire du diagnostic distant pour le Serveur Dr.Web**

Il permet de se connecter au Serveur Dr.Web à distance pour la gestion de base et la consultation des statistiques de fonctionnement. La version graphique de l'utilitaire est disponible uniquement sous Windows. Voir aussi le p. [Accès distant au Serveur Dr.Web](#).

- **Utilitaire du diagnostic distant du Serveur Dr.Web pour la gestion des scripts**

Il permet de se connecter au Serveur Dr.Web à distance pour la gestion de base et la consultation des statistiques de fonctionnement. Cette version de l'utilitaire est adaptée pour l'utilisation dans des scripts. Voir aussi le p. [Accès distant au Serveur Dr.Web](#).

- **Utilitaire de suppression de Dr.Web pour Windows**

Outil d'urgence qui sert à supprimer des installations incorrectes/corrompues du logiciel des Agents Dr.Web pour Windows dans les cas où l'utilisation des outils standard serait impossible ou ne marcherait pas. L'utilitaire n'est pas conçu pour être l'outil principal de désinstallation de Dr.Web.

- **Utilitaire d'installation à distance de l'Agent Dr.Web pour UNIX**

L'utilitaire sert à installer à distance l'Agent Dr.Web sur les postes tournant sous les systèmes d'exploitation de la famille UNIX.

- **Utilitaire d'installation à distance de l'Agent Dr.Web pour Windows**

L'utilitaire sert à installer à distance l'Agent Dr.Web sur les postes tournant sous Windows.

- **Centre mobile de gestion Dr.Web**

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



Pour avoir les informations sur les clés de ligne de commande pour la gestion des utilitaires, consultez le document **Annexes**, la rubrique **G7. Utilitaires**.



10.13.5. Produits d'entreprise



L'ensemble de produits disponibles dépend des paramètres du référentiel du Serveur Dr.Web. Pour activer ou désactiver la réception des mises à jour depuis le SGM pour les produits, accédez à la section **Administration** → **Configuration générale du référentiel** → **Packages d'installation Dr.Web** → [Produits d'entreprise Dr.Web](#).

Dans la section **Produits d'entreprise**, vous pouvez télécharger les packages d'installation pour certains logiciels utilisées dans le réseau antivirus Dr.Web Enterprise Security Suite :

- **Dr.Web pour Android**

Package d'installation de l'Agent Dr.Web pour Android sur les postes protégés.

- **Dr.Web pour IBM Lotus Domino**

Package d'installation de Dr.Web pour IBM Lotus Domino sur un serveur de messagerie d'entreprise.

- **Dr.Web pour Linux**

Package d'installation de l'Agent Dr.Web pour Linux sur les postes protégés.

- **Dr.Web pour macOS**

Package d'installation de l'Agent Dr.Web pour macOS sur les postes protégés.

- **Dr.Web pour Microsoft Exchange Server**

Package d'installation de Dr.Web pour Microsoft Exchange Server sur le serveur de messagerie d'entreprise.

- **Dr.Web pour les passerelles Internet UNIX**

Package d'installation de Dr.Web pour les passerelles Internet UNIX sur une passerelle Internet d'entreprise ou un serveur proxy.

- **Dr.Web pour les serveurs de messagerie UNIX**

Package d'installation de Dr.Web pour les serveurs de messagerie UNIX sur un serveur de messagerie d'entreprise.

- **Dr.Web pour les serveurs de fichiers UNIX**

Package d'installation de Dr.Web pour les serveurs de fichiers UNIX sur un serveur de fichiers d'entreprise.



- **Serveur proxy Dr.Web**

Package d'installation du Serveur proxy Dr.Web sur l'ordinateur au sein du réseau antivirus d'entreprise utilisé en tant que serveur proxy.

- **Serveur de scan Dr.Web**

Package d'installation du Serveur de scan Dr.Web destiné à traiter les demandes de scan antivirus reçues des machines virtuelles dans les environnements virtuels.

- **Dr.Web NAP Validator**

Package d'installation de Dr.Web NAP Validator sur l'ordinateur au sein du réseau antivirus d'entreprise utilisé en tant que serveur de protection d'accès au réseau.

- **Agent Dr.Web pour Active Directory**

Outil d'installation de l'Agent Dr.Web avec le service Active Directory.

- **Installeur complet de l'Agent Dr.Web**

Package d'installation complet de l'Agent Dr.Web pour Windows et du package antivirus sur les postes protégés.

- **Utilitaire de la modification des attributs des objets Active Directory**

Outil d'édition des attributs d'objets pour l'authentification avec le service Active Directory.

- **Utilitaire de la modification du schéma Active Directory**

Outil de création d'une nouvelle classe d'objets et de description de ses attributs pour l'authentification avec le service Active Directory.

10.14. Particularités du réseau avec plusieurs Serveurs Dr.Web

Dr.Web Enterprise Security Suite permet de créer un réseau antivirus avec plusieurs Serveur Dr.Web. Ainsi, chaque poste est associé à un certain Serveur Dr.Web ce qui permet de répartir la charge entre eux.

Les liaisons entre les Serveurs Dr.Web peuvent avoir une structure hiérarchique assurant une répartition optimale de la charge sur le Serveur Dr.Web.

Pour les échanges d'information entre les Serveurs Dr.Web le *protocole spécial de synchronisation entre serveurs* est utilisé.



Fonctionnalités fournies par le protocole de la synchronisation entre serveurs :

- Distribution des mises à jour entre les Serveurs Dr.Web au sein d'un réseau antivirus.
- Rapidité de diffusion des mises à jour après leur réception des serveurs du SGM Dr.Web.
- Transfert des statistiques sur le statut des postes protégés entre les Serveurs Dr.Web liés.
- Transfert des licences pour les postes protégés entre les Serveurs voisins Dr.Web.

10.14.1. Structure du réseau avec plusieurs Serveurs Dr.Web

Le réseau antivirus permet d'installer plusieurs Serveurs Dr.Web. Ainsi, chaque Agent Dr.Web se connecte à un des Serveurs Dr.Web. Chaque Serveur Dr.Web avec des postes antivirus connectés représente un réseau antivirus, comme il est décrit ci-dessus.

Dr.Web Enterprise Security Suite permet de lier ces réseaux antivirus afin d'établir des échanges d'information entre les Serveurs Dr.Web.

Le Serveur Dr.Web peut transmettre à un autre serveur Dr.Web les informations suivantes :

- mises à jour du logiciel et des bases virales. Seul un des deux serveurs va recevoir des mises à jour depuis les Serveurs du SGM Dr.Web ;
- informations sur les événements viraux, statistiques relatives au fonctionnement etc. ;
- licences pour les postes protégés (le transfert des licences entre les Serveurs Dr.Web est configuré dans le [Gestionnaire de licences](#)).

Dr.Web Enterprise Security Suite comprend deux types de liaisons entre les Serveurs Dr.Web :

- *liaison de type supérieur-subordonné*, dans ce cas-là, le supérieur transfère les mises à jour au subordonné et reçoit des informations sur les événements,
- *liaison entres les égaux*, dans ce cas, les directions de la transmission ainsi que les types d'information à transmettre sont paramétrés de manière personnalisée.

La [figure 10-1](#) présente un exemple de la structure réseau avec plusieurs Serveurs Dr.Web.

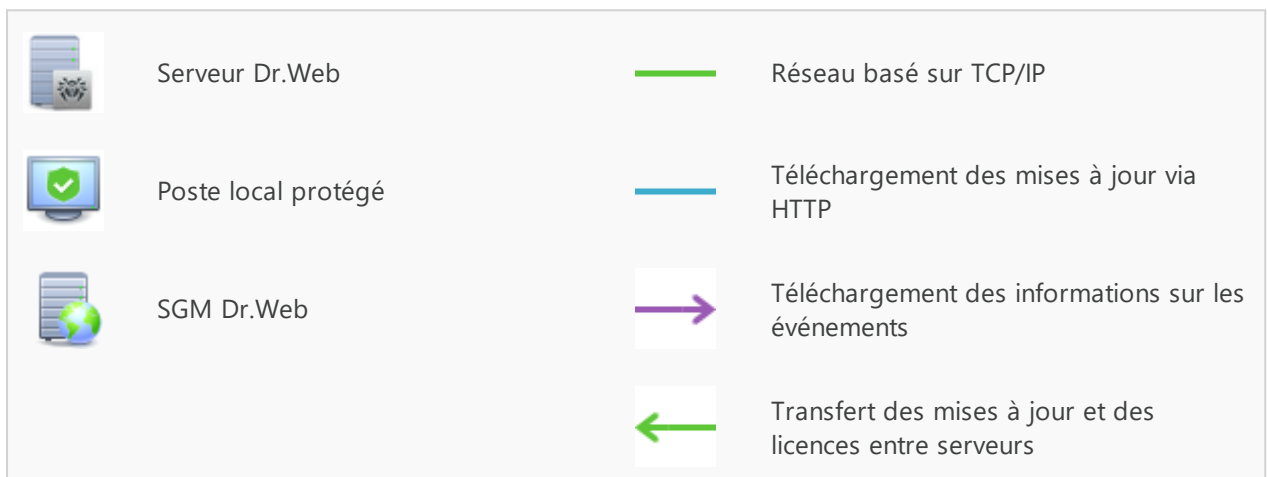
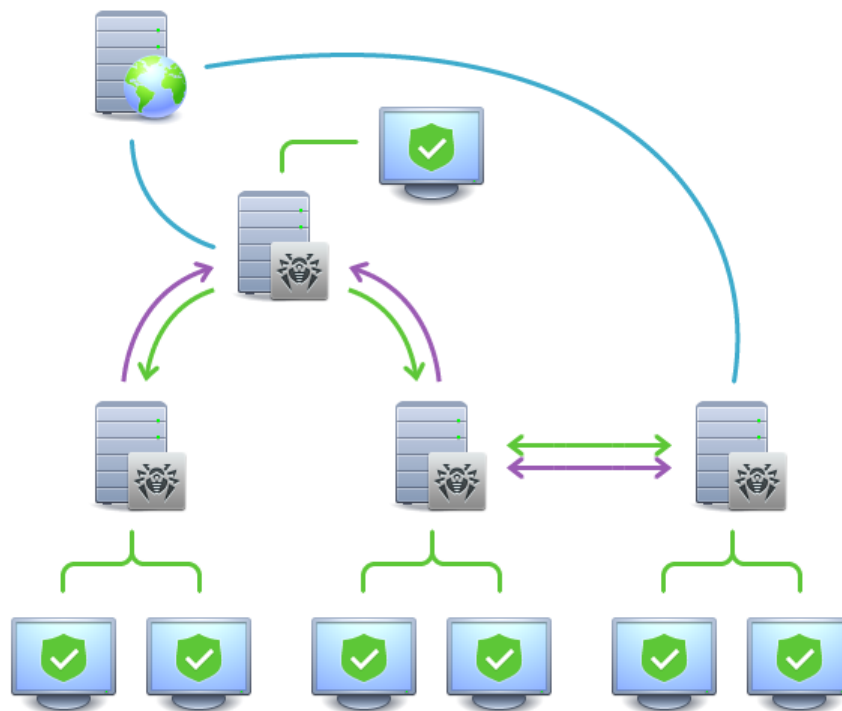


Figure 10-1. Réseau avec plusieurs Serveurs Dr.Web

Certains avantages du réseau avec plusieurs Serveurs Dr.Web :

1. Possibilité de recevoir les mises à jour depuis les Serveurs du SGM Dr.Web via l'un des Serveurs Dr.Web afin de les transmettre plus tard directement vers d'autres Serveurs Dr.Web ou par intermédiaires.



Les Serveurs Dr.Web recevant les mises à jour du Serveur supérieur Dr.Web ne reçoivent pas les mises à jour depuis le SGM même si cette tâche est spécifiée dans la planification.



Pourtant, il est recommandé de laisser la tâche de mise à jour depuis les serveurs du SGM dans la planification du Serveur Dr.Web subordonné pour le cas où le Serveur Dr.Web principal serait temporairement indisponible. Cela permettra aux Agents Dr.Web connectés au Serveur Dr.Web subordonné, de recevoir la mise à jour des bases virales et des modules du logiciel (voir aussi, le p. [Configuration générale du référentiel](#)).



Dans la tâche de mise à jour depuis le SGM sur le Serveur Dr.Web principal qui distribue les mises à jour, il est nécessaire de spécifier la réception des mises à jour du logiciel de serveur pour tous les systèmes d'exploitation installés sur tous les Serveurs Dr.Web subordonnés qui reçoivent les mises à jour depuis le Serveur Dr.Web principal (voir le p. [Configuration générale du référentiel](#)).

2. Possibilité de répartir les postes de travail sur plusieurs Serveurs Dr.Web afin de diminuer la charge sur chacun d'entre eux.
3. Stockage des informations provenant de plusieurs Serveurs Dr.Web sur un seul serveur, ce qui permet d'afficher ces informations sur ce Serveur Dr.Web via le Centre de gestion de manière consolidée.



Dr.Web Enterprise Security Suite surveille la communication des informations en évitant les échanges répétitifs des mêmes informations.

4. Possibilité de transmettre les licences disponibles pour la protection des postes sur le Serveur voisin Dr.Web. Dans ce cas, la clé de licence reste en disposition du Serveur de distribution Dr.Web. Les licences disponibles sont distribuées au Serveur voisin Dr.Web pour un délai de temps spécifié, après l'expiration duquel elles sont révoquées.

10.14.2. Configuration des liaisons entre Serveurs Dr.Web

Pour configurer un réseau avec plusieurs Serveurs Dr.Web, il est nécessaire de configurer des liaisons entre eux.

Il est recommandé, tout d'abord, de planifier la structure du réseau antivirus ainsi que de bien déterminer tous les flux d'information et de désigner les liaisons de type « entre les égaux » et ceux de type « principal-subordonné ». Puis pour chaque Serveur Dr.Web faisant partie du réseau, il est nécessaire de configurer des liaisons avec les Serveurs « voisins » Dr.Web (les Serveurs « voisins » Dr.Web sont liés au moins par un flux d'information).

S'il y a des liaisons voisines entre les Serveurs Dr.Web, les [nouvelles fonctions](#) seront ajoutées dans le menu principal pour le login de l'administrateur.



Exemple de configuration d'une connexion entre serveurs supérieur et subordonné Serveur Dr.Web :



Les valeurs des champs marqués par le symbole * doivent être obligatoirement spécifiées.

1. Assurez-vous que les deux Serveurs Dr.Web sont opérationnels.
2. Attribuez à chaque Serveur Dr.Web un nom mnémonique afin d'éviter d'éventuelles erreurs lors de la configuration de la connexion et de la gestion des Serveurs Dr.Web. Pour ce faire, ouvrez le menu du Centre de gestion **Administration** → **Configuration du Serveur Dr.Web**, l'onglet **Général**, le champ **Nom du Serveur Dr.Web**. Dans cet exemple, le nom du Serveur Dr.Web principal est `MAIN`, le nom du serveur subordonné est `AUXILIARY`.



Les noms spécifiés lors de la configuration seront automatiquement remplacés par les nom des ordinateurs après la connexion des Serveurs Dr.Web par la liaison créée.

3. Activez le protocole serveur sur les deux Serveurs Dr.Web. Pour cela, dans le menu du Centre de gestion, sélectionnez l'élément **Administration** → **Configuration du Serveur Dr.Web**, puis dans l'onglet **Modules**, cochez la case **Protocole du Serveur Dr.Web** (voir [Modules](#)).
4. Redémarrez les deux Serveur Dr.Web.
5. Via le Centre de gestion du Serveur subordonné Dr.Web (`AUXILIARY`), ajoutez le Serveur principal Dr.Web (`MAIN`) dans la liste des Serveurs voisins Dr.Web.


Pour cela, sélectionnez l'élément **Réseau antivirus** dans le menu principal. La fenêtre affichant l'arborescence du réseau antivirus s'ouvrira. Pour ajouter le Serveur voisin Dr.Web, dans la barre d'outils, sélectionnez **+ Ajouter un objet de réseau** → **+ Créer une liaison**.

La fenêtre de configuration de la liaison entre le Serveur existant et le Serveur Dr.Web ajouté va s'ouvrir. Spécifiez les paramètres suivants :

- **Type** du réseau créé — **Principal**.
- **Nom** : nom du Serveur Dr.Web principal (`MAIN`).
- **Mot de passe*** : mot de passe aléatoire pour accéder au Serveur Dr.Web principal.
- **Certificats propres du Serveur Dr.Web** : liste des certificats SSL du Serveur Dr.Web à configurer. Cliquez sur le bouton et sélectionnez le fichier de certificat `drwcsd-certificate.pem` correspondant au Serveur Dr.Web actuel. Pour ajouter encore un certificat, cliquez sur et ajoutez le certificat dans le nouveau champ.
- **Certificats du Serveur voisin Dr.Web*** : liste des certificats SSL du Serveur principal connecté Dr.Web. Cliquez sur le bouton et sélectionnez le certificat `drwcsd-certificate.pem` correspondant au Serveur principal Dr.Web. Pour ajouter encore un certificat, cliquez sur et ajoutez le certificat dans le nouveau champ.
- **Adresse*** : adresse réseau du Serveur Dr.Web principal et port de connexion. Spécifiée au format `<adresse_du_Serveur_Dr.Web> : <port>`.



Il est possible de rechercher la liste des Serveurs Dr.Web disponibles dans le réseau. Pour cela :

- a) Cliquez sur la flèche se trouvant à droite du champ **Adresse**.
 - b) Dans la fenêtre qui apparaît, spécifiez une liste des réseaux au format suivant : séparés par un trait d'union (par exemple, 10.4.0.1-10.4.0.10), par une virgule ou un espace (par exemple, 10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90), en utilisant le préfixe réseau (par exemple, 10.4.0.0/24).
 - c) Cliquez sur le bouton . La recherche des Serveurs Dr.Web disponibles dans le réseau va commencer.
 - d) Sélectionnez un Serveur Dr.Web dans la liste des Serveurs Dr.Web disponibles. Son adresse sera enregistrée dans le champ **Adresse** pour créer une liaison.
- **Adresse du Centre de gestion de la sécurité Dr.Web** : vous pouvez saisir l'adresse de la page d'accueil du Centre de gestion pour le Serveur Dr.Web principal (voir [Centre de gestion de la sécurité Dr.Web](#)).
 - Dans la liste déroulante **Paramètres de connexion**, le principe de la connexion des Serveurs Dr.Web du réseau créé est spécifié.
 - Dans la liste déroulante **Chiffrement** et **Compression**, spécifiez les paramètres du chiffrement et de la compression du trafic entre les Serveurs Dr.Web connectés (voir [Chiffrement et compression du trafic](#)).
 - **Période du renouvellement automatique des licences délivrées** : période de temps pour laquelle les licences sont délivrées de la clé sur ce Serveur Dr.Web. A l'expiration de cette période, les licences délivrées sont renouvelées automatiquement pour le même délai. Le renouvellement automatique sera effectué jusqu'à ce que dure le délai de distribution des licences. Le paramètre est utilisé si le Serveur Dr.Web principal délivre les licences au Serveur Dr.Web actuel.
 - **Délai pour le renouvellement provisoire de licences** : ce paramètre n'est pas utilisé lors de la création de la liaison du Serveur Dr.Web principal.
 - **Période de synchronisation de licences** : périodicité de synchronisation des informations sur les licences délivrées entre les Serveurs Dr.Web.
 - Les cases dans les rubriques **Licences**, **Mises à jour** et **Événements** sont configurées conformément au principe de liaison *principal-subordonné* et ne doivent pas être modifiées :
 - Le Serveur Dr.Web principal envoie les licences vers le Serveur Dr.Web subordonné ;
 - Le Serveur Dr.Web principal envoie les mises à jour vers le Serveur Dr.Web subordonné ;
 - Le Serveur Dr.Web subordonné reçoit des informations sur les événements du Serveur Dr.Web principal.
 - Configurez la réception de notifications par l'administrateur :
 - Cochez la case **Envoyer les notifications des événements du Serveur voisin Dr.Web** pour envoyer à l'administrateur les notifications des événements reçus du Serveur subordonné Dr.Web configuré. Si la case est décochée, l'administrateur recevra des notifications des événements de son Serveur Dr.Web uniquement. Vous pouvez



configurer l'envoi des notifications particulières dans la section [Configuration des notifications](#).

- Cochez la case **Envoyer les notifications des événements du Serveur voisin Dr.Web en cas de détection de menaces par les hashes connus** pour envoyer à l'administrateur les notifications des événements reçus du Serveur subordonné Dr.Web configuré en cas de détection de menaces de sécurité par les hashes de menaces connus. Si la case est décochée, l'administrateur recevra des notifications des événements de son Serveur Dr.Web uniquement. Vous pouvez configurer l'envoi des notifications particulières dans la section [Configuration des notifications](#). La case est disponible uniquement si les bulletins de hashes de menaces connus sont utilisés sous licence. La disponibilité de la licence est indiquée dans les informations sur la clé de licence que vous pouvez consulter dans la section [Gestionnaire de licences](#), le paramètre **Listes autorisées de bulletins de hashes** (il suffit d'avoir une seule licence dans une clé de licence utilisée par le Serveur Dr.Web).
- Cochez la case **Synchroniser les informations sur le matériel et les logiciels sur les postes via les liaisons entre les serveurs** pour envoyer au Serveur subordonné Dr.Web les informations collectées sur le matériel, le logiciel et les packages de mises à jour de Windows sur les postes connectés. Les données seront envoyées juste après la création d'une liaison et la connexion au Serveur principal Dr.Web. Ensuite, les données seront mises à jour en cas de changement du matériel et du logiciel sur les postes. Ces statistiques sont collectées uniquement pour les postes sur lesquels l'Agent Dr.Web pour Windows est installé et uniquement si l'option correspondante est activée dans la configuration du Serveur Dr.Web et de l'Agent Dr.Web, comme cela est décrit dans la section [Matériel et logiciels des postes tournant sous Windows](#).



Si ces options sont activées, le nombre de notifications reçues peut augmenter considérablement.

Lors de la configuration des Serveurs Dr.Web égaux, ces options seront disponibles uniquement au cas où la case **Accepter** serait cochée dans la section **Événements**.

Les notifications suivantes des événements du Serveur voisin Dr.Web sont disponibles : **Menace de sécurité détectée, Rapport de la protection préventive, Erreur de scan, Statistiques de scan.**

Les notifications particulières suivantes s'affichent en cas de détection de menaces de sécurité par les hashes de menaces connus sur le Serveur voisin Dr.Web : **Une menace de sécurité est détectée par les hashes de menaces connus, Erreur de scan en cas de détection d'une menace par les hashes de menaces connus, Rapport de la Protection préventive sur la détection de menaces par les hashes de menaces connus.**

- Dans la section **Restrictions de mise à jour** → **Événements**, vous pouvez spécifier la planification de transfert des événements du Serveur Dr.Web actuel au Serveur principal (l'édition du tableau **Restrictions de mises à jour** est effectuée de la même manière que l'édition du tableau de planification dans la section [Restrictions de mises à jour des postes](#)).



Cliquez sur **Enregistrer**.

Ainsi, le Serveur Dr.Web principal (MAIN) sera inclus dans les dossiers **Parents** et **Offline** (voir la [fig.10-2](#)).

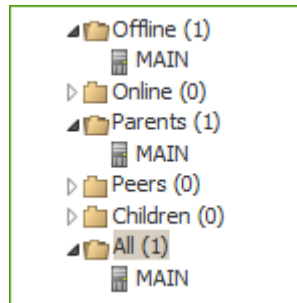






Figure 10-2.

6. Ouvrez le Centre de gestion du Serveur Dr.Web principal (MAIN) et ajoutez le Serveur Dr.Web subordonné (AUXILIARY) dans la liste des Serveurs voisins Dr.Web.

Pour cela, sélectionnez l'élément **Réseau antivirus** dans le menu principal. La fenêtre affichant l'arborescence du réseau antivirus s'ouvrira. Pour ajouter le Serveur voisin Dr.Web, dans la barre d'outils, sélectionnez **+ Ajouter un objet de réseau** → **+ Créer une liaison**.

La fenêtre de configuration de la liaison entre le Serveur existant et le Serveur Dr.Web ajouté va s'ouvrir. Spécifiez les paramètres suivants :

- **Type** du réseau créé — **Subordonné**.
- **Nom** : nom du Serveur Dr.Web subordonné (AUXILIARY).
- **Mot de passe*** : entrez le même mot de passe que celui indiqué dans le p. 5.
- **Certificats propres du Serveur Dr.Web** : liste des certificats SSL du Serveur Dr.Web à configurer. Cliquez sur le bouton  et sélectionnez le fichier de certificat `drwcsd-certificate.pem` correspondant au Serveur Dr.Web actuel. Pour ajouter encore un certificat, cliquez sur  et ajoutez le certificat dans le nouveau champ.
- **Certificats du Serveur voisin Dr.Web*** : liste des certificats SSL du Serveur Dr.Web subordonné connecté. Cliquez sur le bouton  et sélectionnez le fichier de certificat `drwcsd-certificate.pem` correspondant au Serveur Dr.Web subordonné. Pour ajouter encore un certificat, cliquez sur  et ajoutez le certificat dans le nouveau champ.
- **Adresse du Centre de gestion de la sécurité Dr.Web** : vous pouvez saisir l'adresse de la page d'accueil du Centre de gestion pour le Serveur Dr.Web subordonné (voir [Centre de gestion de la sécurité Dr.Web](#)).
- Dans la liste déroulante **Paramètres de connexion**, le principe de la connexion des Serveurs Dr.Web du réseau créé est spécifié.
- Dans la liste déroulante **Chiffrement** et **Compression**, spécifiez les paramètres du chiffrement et de la compression du trafic entre les Serveurs Dr.Web connectés (voir [Chiffrement et compression du trafic](#)).
- **Période de renouvellement automatique des licences délivrées** : ce paramètre n'est pas utilisé lors de la création d'une liaison du Serveur Dr.Web subordonné.



- **Intervalle de renouvellement provisoire des licences obtenues** : délai de temps qui dure jusqu'à la fin de la période du renouvellement automatique des licences. A partir de ce moment ce Serveur Dr.Web subordonné demande le renouvellement automatique provisoire de ces licences. Le paramètre est utilisé si le Serveur Dr.Web subordonné obtient des licences du Serveur Dr.Web actuel.
- **Période de synchronisation de licences** : ce paramètre n'est pas utilisé lors de la création d'une liaison du Serveur Dr.Web subordonné.
- Les cases dans les rubriques **Licences**, **Mises à jour** et **Événements** sont configurées conformément au principe de liaison *principal-subordonné* et ne doivent pas être modifiées :
 - Le Serveur Dr.Web subordonné reçoit les licences du Serveur Dr.Web principal ;
 - Le Serveur subordonné Dr.Web reçoit les mises à jour du Serveur principal Dr.Web ;
 - Le Serveur Dr.Web subordonné envoie des informations sur les événements sur le Serveur Dr.Web principal.
- Les options **Envoyer les notifications des événements du Serveur voisin Dr.Web**, **Envoyer les notifications des événements du Serveur voisin Dr.Web en cas de détection de menaces par les hashes connus** et **Synchroniser les informations sur le matériel et les logiciels sur les postes via les liaisons entre les serveurs** sont désactivées et ne peuvent pas être modifiées car le Serveur Dr.Web subordonné ne reçoit pas d'événements du Serveur Dr.Web principal.
- Dans la section **Restrictions de mise à jour** → **Mises à jour**, vous pouvez spécifier la planification de transfert des mises à jour du Serveur Dr.Web actuel au Serveur Dr.Web subordonné (l'édition du tableau **Restrictions de mises à jour** est effectuée de la même manière que l'édition du tableau de planification dans la rubrique [Restrictions de mises à jour des postes](#)).

Cliquez sur **Enregistrer**.

Ainsi, le Serveur Dr.Web subordonné (AUXILIARY) sera inclus dans les dossiers **Children** et **Offline** (voir la [fig.10-3](#)).

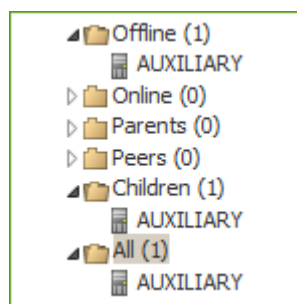


Figure 10-3.

7. Attendez que la connexion entre les Serveurs Dr.Web s'établisse (cela prend une minute au maximum). Pour vérifier la connexion, actualisez de temps en temps l'arborescence des Serveurs Dr.Web avec la touche F5. Dès que la connexion est établie, le Serveur Dr.Web subordonné (AUXILIARY) passe du dossier **Offline** vers le dossier **Online** (voir la [fig. 10-4](#)).

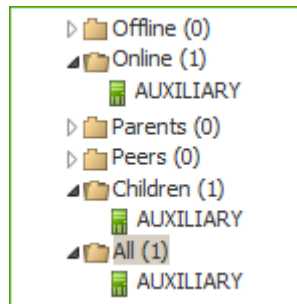


Figure 10-4.

8. Ouvrez le Centre de gestion du Serveur Dr.Web subordonné (AUXILIARY) et assurez-vous que le Serveur Dr.Web principal (MAIN) est bien connecté au serveur subordonné (AUXILIARY) (voir la [fig.10-5](#)).

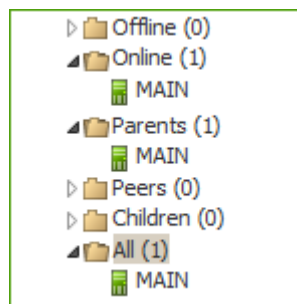


Figure 10-5.



Il est impossible de lier plusieurs Serveurs Dr.Web ayant la même paire de paramètres : mot de passe et Certificat SSL.



Lors de la création d'une liaison entre les Serveurs Dr.Web égaux, il est recommandé de spécifier l'adresse du Serveur Dr.Web à ajouter uniquement dans la configuration de l'un des deux serveurs. Cela n'a pas d'impact sur l'interaction entre les Serveurs Dr.Web mais permet d'éviter les entrées de type **Link with the same key id is already activated** dans le journal du fonctionnement des Serveurs Dr.Web.

Pourtant, il est obligatoire de spécifier l'adresse du Serveur Dr.Web connecté d'un des côtés.

Il est impossible d'établir une connexion entre les Serveurs Dr.Web Server dans les cas suivants :

- Problème de connexion via le réseau.
- Adresse invalide du Serveur Dr.Web principal spécifiée lors de la configuration de la connexion.
- Les certificats publics spécifiés sur un des Serveurs Dr.Web sont invalides.
- Mot de passe invalide sur un des Serveurs Dr.Web (les mots de passe ne correspondent pas sur les Serveurs Dr.Web à lier).



S'il est nécessaire d'établir une nouvelle liaison entre les Serveurs Dr.Web en versions 10 et 13, effectuez les actions suivantes :

1. Lors de la création de la liaison, indiquez la clé publique du Serveur Dr.Web en version 13 sur le Serveur Dr.Web en version 10.
2. Générez le certificat de la clé privée du Serveur Dr.Web en version 10 avec l'utilitaire `drwsign` (commande `gencert`) fourni avec le Serveur Dr.Web en version 13 (voir les **Annexes**, [H7.1. Utilitaire de génération des clés numériques et des certificats](#)). Indiquez ce certificat lors de la création de la liaison sur le Serveur Dr.Web en version 13.

10.14.3. Utilisation du réseau antivirus avec plusieurs Serveurs Dr.Web

Une des particularités du réseau à plusieurs Serveurs Dr.Web consiste en l'obtention des mises à jour depuis le SGM Dr.Web via une partie des Serveurs Dr.Web (en général, un ou plusieurs Serveurs Dr.Web principaux). Dans ce cas, la planification de la tâche de mise à jour ne doit être configurée que sur les Serveurs concernés (voir le p. [Configuration de la planification du Serveur Dr.Web](#)). Tout Serveur recevant des mises à jour depuis les Serveurs du SGM Dr.Web ou depuis un autre Serveur, les transmet immédiatement à tous les Serveurs pour lesquels cette option est configurée (vers tous les serveurs subordonnés ainsi que vers les serveurs égaux pour lesquels l'option permettant de recevoir les mises à jour est configurée de manière explicite).



Dr.Web Enterprise Security Suite surveille de manière automatique les situations où une planification incorrecte de la topologie du réseau ainsi que des erreurs de configuration des Serveurs Dr.Web peuvent entraîner un double envoi de la même mise à jour (déjà réceptionnée depuis d'autres sources) vers le même Serveur Dr.Web à la place d'une nouvelle mise à jour.

L'administrateur peut également recevoir des informations récapitulatives sur les événements viraux importants survenant sur les fragments du réseau liés à tel ou tel Serveur Dr.Web, via des liaisons entre serveurs.

Pour consulter les informations sur les événements viraux sur tous les Serveurs Dr.Web liés à ce serveur

1. Dans le menu principal du Centre de gestion, sélectionnez l'élément **Réseau antivirus**. Dans l'arborescence du réseau antivirus, dans le groupe **Neighbors**, sélectionnez le Serveur voisin Dr.Web, dont vous voulez consulter les informations.
2. Sélectionnez l'élément **Général** → **Matériel et logiciels** du menu gérant pour voir les statistiques du matériel et des logiciels sur les postes protégés connectés au Serveur voisin Dr.Web sélectionné.

Les informations affichées dans cette section sont similaires à celles de la section pour les postes connectés à votre Serveur Dr.Web (voir [Matériel et logiciels des postes tournant sous Windows](#)).



3. Pour voir les statistiques des composants antivirus sur les postes protégés connectés au Serveur voisin Dr.Web sélectionné, sélectionnez l'élément correspondant dans la section **Statistiques** du menu gérant.

Les informations affichées dans cette section sont similaires à celles de la section pour les postes connectés à votre Serveur Dr.Web (voir [Statistiques](#)).

10.14.4. Cluster des Serveurs Dr.Web



Pour en savoir plus sur la mise à jour des Serveurs Dr.Web au sein d'un cluster, consultez la rubrique [Mise à jour des Serveurs Dr.Web dans le cluster](#).

Pour plus d'informations sur la restauration du noeud du cluster après un échec fatal du Serveur Dr.Web, voir le document **Annexes**, la rubrique [Restauration du noeud du cluster des Serveurs Dr.Web](#).

Lors de la création du cluster des Serveurs Dr.Web dans le réseau antivirus, il faut respecter les conditions suivantes :

1. Fichiers de configuration

`webmin.conf` : l'unification sur tous les serveurs du cluster n'est pas requis.

`drwcsd.conf` : certains paramètres nécessitent l'unification :

- Disponibles uniquement dans le fichier de configuration :

Paramètres	Valeurs
<pre><!-- Password encryption salt, keep it in safe place --></pre> <p>Valeur du salage cryptographique pour le chiffrement du mot de passe de l'administrateur dans la base de données</p>	identiques
<pre><!-- The server self id from license key. --></pre> <p>Identificateur unique du Serveur Dr.Web</p>	différents

- Peut être modifié dans le Centre de gestion (**Configuration du Serveur Dr.Web**) :

Onglets	Paramètres	Valeurs
Général	Nom du Serveur Dr.Web	vide ou différent
	Langue du Serveur Dr.Web, Nombre de requêtes parallèles des clients, Nombre des copies de sauvegarde pour les versions du Serveur Dr.Web	n'a pas d'importance



Onglets	Paramètres	Valeurs
	autres	identiques
Trafic	Mises à jour, Configurations	identiques
Réseau	DNS, Proxy	n'a pas d'importance
	Transport : Chiffrement et Compression ; paramètres liés au mode Multicasting	identiques
	Transport: autres	n'a pas d'importance
	E-mail, Cluster, Téléchargement	identiques
	Mises à jour de groupes	il est recommandé de laisser sur un seul serveur du cluster et déconnecter sur les autres
Statistiques, Sécurité, Cache, Modules, Licences	tous	identiques
Localisation, Journal	tous	n'a pas d'importance
Base de données	Nombre de connexions, Restaurer l'image corrompue automatiquement	n'a pas d'importance
	autres	identiques

2. Clés de chiffrement et certificat du Serveur Dr.Web

Tous les Serveurs Dr.Web doivent avoir la même clé de chiffrement publique (*.pub) et la même clé de chiffrement privée `drwcd.pri`, ainsi que le certificat du Serveur Dr.Web `drwcd-certificate.pem`.

Si les clés de chiffrement et le certificat n'ont pas été créés avant, ils seront générés automatiquement lors de l'installation du premier Serveur Dr.Web du cluster.

Vous pouvez obtenir les clés de chiffrement nécessaires et le certificat pour l'installation des Serveurs Dr.Web suivants du cluster via le Centre de gestion : menu **Administration** → **Clés de chiffrement**. Dans ce cas, la clé privée et le certificat peuvent être requis plus tard : lors de la spécification de la clé privée `drwcd.pri` pendant l'installation du Serveur Dr.Web, la clé publique *.pub et le certificat `drwcd-certificate.pem` sont générés automatiquement, pourtant une nouvelle version du certificat est créée lors de sa génération, c'est pourquoi le certificat doit être remplacé par la même version sur tous les Serveurs Dr.Web du cluster (voir [Instruments assurant une connexion sécurisée](#)).



3. Nom unique du Serveur Dr.Web

Le même nom DNS doit être spécifié pour tous les Serveur Dr.Web. Ce nom est utilisé pour générer les fichiers d'installation de l'Agent sur les postes du réseau antivirus.

Ce nom est spécifié via le Centre de gestion : **Administration** → **Configuration du Serveur Dr.Web** → onglet **Réseau** → onglet [Téléchargement](#) → champ **Adresse du Serveur Dr.Web**. Les paramètres de cette section sont sauvegardés dans le fichier de configuration `download.conf` (vous pouvez consulter la description du fichier dans les **Annexes**, [E3. Fichier de Configuration download.conf](#)).

4. Configuration de l'utilisation du cluster

Le nom commun du cluster doit être enregistré sur le Serveur DNS dans le réseau pour chaque Serveur Dr.Web séparément et la méthode de répartition de la charge doit être spécifiée.

Pour appliquer automatiquement les paramètres dans le cluster des Serveurs Dr.Web, il faut utiliser le protocole spécial du cluster.

Pour configurer le protocole de cluster pour chaque Serveur Dr.Web dans le Centre de gestion, ouvrez le menu **Administration** → **Configuration du Serveur Dr.Web** et spécifiez les paramètres suivants :

- a) Pour activer le protocole du cluster, cochez la case **Protocole du cluster des Serveurs Dr.Web** dans l'onglet [Modules](#).
- b) Pour configurer les paramètres d'interaction des Serveurs Dr.Web au sein d'un cluster, spécifiez les paramètres suivants dans l'onglet [Cluster](#).

Exemple :

- **Groupe multicast** : 232.0.0.1
- **Port** : 11111
- **Interface** : 0.0.0.0

Dans cet exemple, les transports pour toutes les interfaces sont configurés pour tous les Serveurs Dr.Web du cluster. Dans les autres cas, par exemple, quand un des réseaux est externe par rapport au cluster et les Agents Dr.Web se connectent via ce réseau et le deuxième réseau est interne, il vaut mieux ouvrir le protocole du cluster uniquement pour les interfaces du réseau interne. Dans ce cas, il faut spécifier les adresses du type 192.168.1.1, ..., 192.168.1.N en tant qu'interfaces.

Après avoir spécifié tous les paramètres nécessaires, cliquez sur le bouton **Enregistrer** et redémarrez les Serveurs Dr.Web.

5. Base de données commune



Pour pouvoir fonctionner avec une seule base de données, tous les Serveurs Dr.Web doivent avoir la même version.



Tous les Serveurs Dr.Web au sein d'un cluster doivent fonctionner avec la seule base de données.

Comme dans le cas de l'utilisation de la base de données sans l'organisation du cluster, chaque Serveur Dr.Web s'adresse à la base de données indépendamment et toutes les données des Serveurs Dr.Web sont sauvegardées séparément. Là où cela est valable, le Serveur Dr.Web prend dans la base de données seulement les entrées liées à son ID qui est unique pour chaque Serveur Dr.Web. L'utilisation d'une base de données unique permet aux Serveurs Dr.Web d'utiliser les Agents Dr.Web qui ont été d'abord enregistrés sur d'autres Serveurs Dr.Web du cluster.

Lors de la création d'un cluster des Serveurs Dr.Web avec la base de données unique, veuillez prendre en compte les particularités suivantes :

- La base de données peut être installée séparément de tous les Serveurs Dr.Web ou sur un des ordinateurs sur lequel est installé le Serveur Dr.Web du cluster.
- La base de données doit être créée avant l'installation du premier Serveur Dr.Web du cluster ou avant la connexion du premier Serveur Dr.Web à la base de données.
- Lors de l'ajout de nouveaux nœuds au cluster (excepté le premier Serveur Dr.Web) pendant l'installation des Serveurs Dr.Web, il n'est recommandé de spécifier la base de données unique qui est utilisée dans ce cluster. Sinon les informations qui sont déjà sauvegardées dans ce cluster peuvent être supprimées. Il est recommandé d'installer les Serveurs Dr.Web avec la base de données interne et, après l'installation, les connecter à la base de données externe unique.

Vous pouvez connecter les Serveurs Dr.Web à la base de données externe via le Centre de gestion : menu **Administration** → **Configuration du Serveur Dr.Web** → onglet [Base de données](#) ou via le fichier de configuration des Serveurs Dr.Web `drwcsd.conf`.

- Il n'est pas recommandé d'ajouter à un cluster des Serveurs Dr.Web qui fonctionnent déjà dans le réseau antivirus avec une autre base de données interne ou externe (excepté le premier Serveur Dr.Web du cluster). Cela peut provoquer la perte de données : des informations sur les postes, sur les statistiques et sur les paramètres (sauf les paramètres sauvegardés dans les fichiers de configuration), car les données dans la base sont complètement supprimées lors de l'importation. Dans ce cas, seule l'importation partielle de certains paramètres est possible.
- Par défaut, lors de l'installation ou la migration de Serveurs Dr.Web des versions précédentes, une valeur de salage aléatoire est générée dans le fichier de configuration `drwcsd.conf` pour le chiffrement du mot de passe de l'administrateur dans la base de données. Pour éviter des problèmes d'authentification, il faut spécifier manuellement la même valeur de salage sur tous les Serveurs Dr.Web faisant partie du cluster. Le paramètre nécessaire est décrit dans le document **Annexes**, [F1. Fichier de configuration du Serveur Dr.Web](#).

6. Une version du référentiel

Sur tous les Serveurs Dr.Web du cluster, les référentiels doivent contenir les mises à jours de la même version.

Vous pouvez satisfaire à cette condition d'une des façons suivantes :



- Mettre à jour tous les Serveurs Dr.Web du cluster depuis le SGM en même temps. Dans ce cas, tous les Serveurs Dr.Web auront la dernière version des mises à jour. Vous pouvez configurer la mise à jour des référentiels de tous les Serveurs Dr.Web depuis la zone locale des mises à jour (le miroir du SGM). Dans ce cas, une version approuvée des mises à jour sera diffusée depuis la zone locale ou, en cas de création du miroir du SGM, ce sera la dernière version des mises à jour.
- Il est possible de créer la structure hybride associant le cluster des Serveurs Dr.Web et la structure hiérarchique à la base des liaisons voisines. Ainsi, un des Serveurs Dr.Web (un Serveur Dr.Web du cluster ou un Serveur non inclus au cluster) est désigné comme principal et il obtient les mises à jour depuis le SGM. Les autres Serveurs Dr.Web du cluster sont considérés comme subordonnés et ils obtiennent les mises à jour par les liaisons voisines depuis le Serveur principal Dr.Web.

En cas de configuration de la mise à jour des Serveurs Dr.Web du cluster depuis la zone locale ou depuis le Serveur Dr.Web principal, il est nécessaire de surveiller le fonctionnement de cette zone ou du Serveur Dr.Web principal. Si le nœud diffusant les mises à jour tombe en panne, il est nécessaire de reconfigurer un des Serveurs Dr.Web et le désigner Serveur Dr.Web principal ou créer une nouvelle zone des mises à jour pour obtenir des mises à jour depuis le SGM.

7. Particularités de la diffusion des licences sur les postes

Pour diffuser les licences sur les Serveurs Dr.Web du cluster vous pouvez agir d'une des façons suivantes :

- a) La structure hiérarchique de Serveurs Dr.Web n'est pas configurée au sein du cluster. Il suffit d'ajouter une clé de licence (ou plusieurs clés) sur un des Serveurs Dr.Web du cluster. Les informations sur cette clé de licence seront enregistrées dans la base de données commune. Ainsi, tous les Serveurs Dr.Web du cluster utiliseront en même temps la clé de licence. Le nombre total des licences sauvegardées dans la base de données commune doit correspondre au nombre total des postes servis par tous les Serveurs Dr.Web du cluster.



Pour pouvoir utiliser la clé de licence sur tous les Serveurs Dr.Web du cluster, et non seulement sur celui qui contient la clé ajoutée, il faut redémarrer les autres Serveurs Dr.Web du cluster après avoir ajouté la clé.

- b) Il est possible de créer une structure hybride associant le cluster des Serveurs Dr.Web et la structure hiérarchique à la base des liaisons voisines. Cette structure sera utile si, pendant la maintenance des Agents Dr.Web les Serveurs inclus dans cluster et les Serveurs Dr.Web non inclus dans le cluster sont utilisés. Dans ce cas, le nombre nécessaire des licences est distribué depuis le fichier de licence par les liaisons voisines pendant le travail :
 - Depuis un Serveur Dr.Web non inclus dans le cluster sur un des Serveurs Dr.Web du cluster. Les licences distribuées seront utilisées par tous les Serveurs Dr.Web du cluster, comme cela est décrit dans le p. a).



- Depuis un des Serveurs Dr.Web du cluster (c'est-à-dire, depuis une clé utilisée par tous les Serveurs Dr.Web du cluster) sur le Serveur Dr.Web non inclus dans le cluster.

La configuration de la distribution du nombre nécessaire des licences pour un délai nécessaire se fait manuellement par l'administrateur du réseau antivirus (pour plus d'informations, voir la rubrique [Distributions des licences par les liaisons entre les serveurs](#)).

Par exemple, vous pouvez configurer la structure hiérarchique des Serveurs Dr.Web et déterminer le Serveur Dr.Web principal (cela peut être un Serveur Dr.Web du cluster ou un Serveur non inclus dans le cluster) qui va distribuer les mises à jour du référentiel et les licences depuis le fichier de licence.

8. Tâches dans la planification des Serveurs Dr.Web

Pour exclure la duplication des requêtes à la BD, il est recommandé d'exécuter les tâches suivantes de la planification du Serveur Dr.Web seulement sur un des Serveurs Dr.Web : **Purge old records (Suppression des entrées obsolètes)**, **Back up critical Dr.Web Server data (Copie de sauvegarde des données critiques du Serveur Dr.Web)**, **Purge old stations (Suppression des postes obsolètes)**, **Purge unsent events (Suppression des événements non envoyés)**. Par exemple, elle peuvent être exécutées sur le Serveur Dr.Web qui est placé sur le même ordinateur que la base de données externe. Il est recommandé d'exécuter les tâches sur le plus puissant ordinateur du cluster, si les configurations des Serveurs Dr.Web sont différentes et la base de données est installée sur un ordinateur à part.



Chapitre 11 : Mise à jour des composants de Dr.Web Enterprise Security Suite lors du fonctionnement du produit

Ce chapitre contient la description de la mise à jour des composants de Dr.Web Enterprise Security Suite qui est effectuée lors du fonctionnement du produit et qui ne permet pas d'effectuer la mise à niveau.

La mise à niveau du produit et de ses composants vers une nouvelle version est décrite dans le **Manuel d'installation**, dans la [Chapitre 7 : Mise à jour des composants de Dr.Web Enterprise Security Suite](#).



Avant de procéder à la mise à jour de Dr.Web Enterprise Security Suite et de ses composants, il est fortement recommandé de vérifier les paramètres du protocole TCP/IP relatifs à l'accès à Internet. Le service DNS doit notamment être actif et correctement configuré.

Avant la mise à jour du logiciel, il est recommandé de configurer le référentiel y compris l'accès au SGM Dr.Web (voir [Configuration générale du référentiel](#)).

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

Le Centre de gestion fournit les fonctionnalités suivantes de gestion du logiciel du Serveur Dr.Web :

- Mise à niveau du logiciel du Serveur Dr.Web vers une des versions disponibles, téléchargées depuis le SGM et stockées dans le référentiel du Serveur Dr.Web. Les paramètres de la mise à jour du référentiel depuis le SGM sont décrits dans la rubrique [Gestion du référentiel du Serveur Dr.Web](#).
- Recul du logiciel du Serveur Dr.Web vers la copie de sauvegarde. Les copies de sauvegarde du Serveur Dr.Web sont créés automatiquement lors du passage vers la nouvelle version dans la rubrique **Mises à jour du Serveur Dr.Web** (étape 4 dans la procédure ci-dessous).



Vous pouvez également mettre à jour le Serveur Dr.Web avec la distribution du Serveur Dr.Web. La procédure est décrite dans le **Manuel d'installation**, dans la rubrique [Mise à jour du Serveur Dr.Web sous OS Windows](#) ou [Mise à jour du Serveur Dr.Web sous les OS de la famille UNIX](#).

Pas toutes les mises à jour du Serveur Dr.Web contiennent le fichier de distribution. Certaines d'entre elles peuvent être installées uniquement via le Centre de gestion.



Lors de la mise à jour du Serveur Dr.Web sous OS de la famille UNIX via le Centre de gestion, la version du Serveur Dr.Web dans le gestionnaire de paquets de l'OS ne changera pas.

Pour gérer le logiciel du Serveur Dr.Web :

1. Sélectionnez l'élément **Administration** du menu principal du Centre de gestion, et dans la fenêtre qui s'ouvre, sélectionnez l'élément **Serveur Dr.Web** du menu de gestion.
2. Pour accéder à la liste des versions du Serveur Dr.Web, suivez le lien **Voir la liste des versions**.
3. La rubrique **Mises à jour du Serveur Dr.Web** va s'afficher contenant la liste des mises à jour disponibles et des copies de sauvegarde du Serveur Dr.Web. Ainsi :
 - Dans la liste **Version actuelle** est indiquée la version du Serveur Dr.Web utilisée en ce moment. La rubrique **Liste des modifications** contient la brève liste des nouvelles fonctionnalités et la liste des erreurs corrigées dans cette version par rapport à la version précédente.
 - La liste **Mises à jour disponibles** contient la liste des mises à jour pour ce Serveur Dr.Web téléchargées depuis le SGM. La section **Liste des modifications** contient la brève liste des nouvelles fonctionnalités et des erreurs corrigées pour chaque composant. Pour la version qui précède l'installation initiale du Serveur Dr.Web depuis le package d'installation, la rubrique **Liste des modifications** est vide.
 - La liste **Copies de sauvegarde** contient la liste des copies de sauvegarde, faites pour ce Serveur Dr.Web. Dans la rubrique **Date** sont indiquées les informations sur la date de la copie de sauvegarde.
4. Pour *mettre à niveau* le logiciel du Serveur Dr.Web, placez l'option contre la version nécessaire du Serveur Dr.Web dans la liste **Mises à jour disponibles** et cliquez sur **Appliquer**.



Vous pouvez faire la mise à niveau uniquement vers la version plus récente du Serveur Dr.Web par rapport à la version utilisée en ce moment.

En cours de la mise à niveau du Serveur Dr.Web la version actuelle est sauvegardée en tant que copie de sauvegarde (placée dans la section **Copies de sauvegarde**), et la version, vers laquelle vous migrez est déplacée de la section **Mises à jour disponibles** vers la section **Version actuelle**.

Les copies de sauvegarde sont sauvegardées dans le répertoire suivant :

```
var → update → backup → <ancienne_version>-<nouvelle_version>
```

Lors de la mise à niveau, le fichier de journal `var → dwupdater.log` est créé, complété.

5. Pour *restaurer* la copie de sauvegarde du logiciel du Serveur Dr.Web, placez l'option contre la version nécessaire du Serveur Dr.Web dans la liste **Copies de sauvegarde** et cliquez sur



Appliquer. Lors de la restauration du logiciel du Serveur Dr.Web, la copie de sauvegarde vers laquelle le passage s'effectue, est placée dans la section **Version actuelle**.

6. *Pour restaurer l'état de la révision actuelle du logiciel du Serveur Dr.Web, cliquez sur le bouton **Restaurer le Serveur**. L'intégrité du logiciel du Serveur Dr.Web sera restaurée sans sauvegarde d'une copie, la mise à jour de la base de données et des fichiers de configuration. Si cette révision est manquante dans le référentiel, la restauration est impossible.*

11.2. Mise à jour des Serveurs Dr.Web dans le cluster

Vous pouvez effectuer une mise à jour des Serveurs Dr.Web au sein d'un cluster de deux façons :

Depuis les packages d'installation

Dans ce cas, il faut arrêter tous les Serveurs Dr.Web et les mettre à jour l'un après l'autre.



La procédure est décrite dans le **Manuel d'installation**, dans la [Chapitre 7 : Mise à jour des composants de Dr.Web Enterprise Security Suite](#).

Via le Centre de gestion

Ce moyen consiste à déconnecter les noeuds du cluster un par un, ensuite les reconnecter à la base de données embarquée et les mettre à jour à tour de rôle. Après la mise à jour, il faut connecter de nouveau les noeuds au cluster commun. Pour ce faire :

1. Déconnectez tous les Serveurs Dr.Web du cluster sauf un seul qui effectuera la mise à jour de la BD operante : sur tous les Serveurs Dr.Web sauf un seul, accédez à la section **Administration** → **Configuration du Serveur Dr.Web** → l'onglet **Modules** et décochez la case **Protocole du cluster des Serveurs Dr.Web**. Cliquez sur **Enregistrer** et redémarrez le poste.
2. Connectez les Serveurs Dr.Web déconnectés du cluster à une autre BD, par exemple la base de données embarquée : accédez à la section **Administration** → **Configuration du Serveur Dr.Web** → l'onglet **Base de données** et sélectionnez **SQLite3** dans la liste déroulante **Base de données**. Pour en savoir plus sur la connexion à la base de données, voir la rubrique [Base de données](#).
3. Bloquez toutes les connexions des Agents Dr.Web à ces Serveurs Dr.Web : accédez à la section **Administration** → **Configuration du Serveur Dr.Web** → l'onglet **Modules** et décochez la case **Protocole de l'Agent Dr.Web**. Cliquez sur le bouton **Enregistrer** et redémarrez le poste.
4. [Arrêtez](#) tous les Serveurs Dr.Web déconnectés du cluster.
5. [Effectuez une mise à jour](#) du Serveur Dr.Web avec la BD du cluster.



6. Lancez et effectuez à tour de rôle une mise à jour des autres Serveurs Dr.Web via le Centre de gestion. Après la mise à jour du dernier serveur, connectez-les à la base de données du cluster : accédez à la section **Administration** → **Configuration du Serveur Dr.Web** → **l'onglet Base de données** et sélectionnez la BD du cluster dans la liste déroulante **Base de données**. Pour en savoir plus sur la connexion à la base de données, voir la rubrique [Base de données](#).
7. Bloquez les connexions des Agents Dr.Web : accédez à la section **Administration** → **Configuration du Serveur Dr.Web** → l'onglet **Modules** et cochez la case **Protocole de l'Agent Dr.Web**. Cliquez sur le bouton **Enregistrer** et redémarrez le poste.
8. Reconnectez tous les Serveur Dr.Web au cluster: accédez à la section **Administration** → **Configuration du Serveur Dr.Web** → l'onglet **Modules** et cochez la case **Protocole du cluster des Serveurs Dr.Web**. Cliquez sur **Enregistrer** et redémarrez le poste.



S'il y a beaucoup de Serveurs Dr.Web, leur mise à jour peut prendre un temps considérable. Pour maintenir le fonctionnement permanent vous pouvez effectuer la mise à jour d'une partie de Serveurs Dr.Web et les assembler dans un cluster à part pendant que les autres sont en cours de la mise à jour.

Vous pouvez consulter la description de la procédure dans la rubrique [Mise à jour du Serveur Dr.Web et restauration depuis une copie de sauvegarde](#).

11.3. Mise à jour manuelle du référentiel du Serveur Dr.Web

Pour voir l'état du référentiel ou mettre à jour les composants du réseau antivirus

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion. Dans la fenêtre qui s'ouvre, sélectionnez l'élément du menu de gestion **Statut du référentiel**.
2. Dans la fenêtre qui s'ouvre, vous pouvez voir la liste des produits du référentiel, la date de la révision utilisée, la date de la dernière révision téléchargée et le statut des produits.



Dans la colonne **Statut** vous pouvez consulter le statut des produits du référentiel du Serveur Dr.Web au moment de la dernière mises à jour.

3. Pour gérer le contenu du référentiel, utilisez les boutons suivants de la barre d'outils :
 - Cliquez sur **Vérifier les mises à jour** pour vérifier la disponibilité des mises à jour des tous les produits dans le SGM. Si le composant analysé est obsolète, il sera mis à jour automatiquement.
 - Pour télécharger le journal des mises à jour du référentiel, cliquez sur un des boutons suivants dans la barre d'outils :



Sauvegarder les données dans un fichier CSV,




Sauvegarder les données dans un fichier HTML,



Sauvegarder les données dans un fichier XML,



Sauvegarder les données dans un fichier PDF.


- Cliquez sur  **Recharger le référentiel depuis le disque**, pour charger la version actuelle du référentiel du disque.

Au démarrage, le Serveur Dr.Web charge les contenus du référentiel en mémoire. Si durant le fonctionnement du Serveur Dr.Web, l'administrateur a modifié les contenus sans tenir compte du Centre de gestion, par ex, en mettant à jour le référentiel avec un utilitaire externe ou manuellement, rechargez le référentiel pour utiliser la version téléchargée.

11.4. Mise à jour du référentiel du Serveur Dr.Web selon la planification

Vous pouvez configurer la configuration des tâches sur le Serveur Dr.Web afin d'effectuer des mises à jour régulières du logiciel (pour en savoir plus sur la planification, voir le p. [Configuration de la planification du Serveur Dr.Web](#)).

Pour configurer la planification pour la mise à jour du référentiel du Serveur Dr.Web

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion. Puis dans la fenêtre qui s'affiche, sélectionnez l'élément du menu de gestion **Planificateur des tâches du Serveur Dr.Web**. La liste actuelle des tâches du Serveur Dr.Web va s'ouvrir.
2. Pour ajouter une nouvelle tâche, cliquez sur le bouton  **Créer une nouvelle tâche** dans la barre d'outils. Une fenêtre d'édition de la tâche va s'ouvrir.
3. Dans l'onglet **Général**, configurez les paramètres suivants :
 - Spécifiez le nom de la tâche à afficher dans le champ **Nom**.
 - Cochez la case **Activer l'exécution** pour activer l'exécution d'une tâche. Si la case n'est pas cochée, la tâche reste dans la liste mais elle ne sera pas exécutée.
 - Cochez la case **Tâche critique** pour effectuer un lancement supplémentaire de la tâche si l'exécution planifiée de cette tâche à l'heure prévue a été omise. Le Planificateur parcourt la liste des tâches à chaque minute et s'il détecte une tâche critique omise, il la lance. Si au moment de lancement, une tâche a été omise plusieurs fois, elle sera exécutée seulement une fois.
 - Si la case **Lancer la tâche de manière asynchrone** est décochée, la tâche sera placée dans la file d'attente des tâches du Planificateur exécutées successivement. Cochez la case pour exécuter cette tâche simultanément hors de la file d'attente.
4. Dans l'onglet **Action**, configurez les paramètres suivants :
 - Dans la liste **Action** sélectionnez le type de tâche **Mettre à jour le référentiel**.
 - Dans la liste **Produit**, cochez les cases près des produits du référentiel à mettre à jour via cette tâche.
 - Cochez la case **Mettre à jour les clés de licence** pour activer la procédure de la mise à jour automatique des clés de licence lors de la mise à jour du référentiel. Pour plus d'informations, consultez la rubrique [Mise à jour automatique de licences](#).



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

- Dans la liste déroulante **Périodicité**, sélectionnez le mode de lancement de la tâche et configurez l'heure en fonction de la périodicité indiquée :
- Cochez la case **Interdire après la première exécution** pour exécuter la tâche une seule fois conformément à la périodicité spécifiée. Si la case n'est pas cochée, la tâche sera exécutée plusieurs fois selon la périodicité indiquée.

6. Pour créer une tâche avec les paramètres spécifiés, cliquez sur **Enregistrer**.

11.5. Mise à jour du référentiel du Serveur Dr.Web non connecté à Internet

Si le Serveur Dr.Web n'est pas connecté à Internet pour obtenir des mises à jour du référentiel depuis les serveurs du SGM, il existe les variantes suivantes de configuration de la mise à jour :

- Si, sur le réseau, il y a un autre Serveur Dr.Web connecté à Internet pour obtenir des mises à jour, configurez une liaison avec ce serveur de type égaux ou principal-subordonné où le Serveur Dr.Web non connecté à Internet sera subordonné. Dans ce cas, le Serveur Dr.Web non connecté à Internet recevra automatiquement toutes les mises à jour du Serveur principal Dr.Web.

Dans la rubrique [Particularités du réseau avec plusieurs Serveurs Dr.Web](#), vous pouvez consulter la description de la configuration des liaisons entre les serveurs.

- Si vous ne pouvez pas configurer une mise à jour automatique de l'autre Serveur Dr.Web via une liaison entre les serveurs, vous pouvez mettre à jour manuellement le référentiel du Serveur Dr.Web non connecté.
 - Si, sur le réseau, il y a un autre Serveur Dr.Web connecté à Internet pour obtenir des mises à jour, transférez manuellement le contenu du référentiel depuis le Serveur Dr.Web mis à jour, comme cela est décrit dans la section [Copier le référentiel d'un autre Serveur Dr.Web](#).
 - S'il n'y a pas de possibilité de connecter un des Serveurs Dr.Web à Internet pour obtenir des mises à jour, vous pouvez télécharger le référentiel depuis le SGM sans utiliser le logiciel du Serveur Dr.Web. Pour ce faire, l'utilitaire standard [Chargeur du référentiel Dr.Web](#) inclus dans les produits du référentiel est fourni.



La [version graphique](#) de l'utilitaire est disponible uniquement sous Windows et peut être téléchargée des l'une des manières suivantes :

- depuis le site <https://download.drweb.com>. Une fois le numéro de série saisi et le type de produits sélectionné, le tableau d'**Assistant de téléchargement** s'affiche ou vous pouvez choisir le chargeur du référentiel Dr.Web nécessaire.
- depuis le Centre de gestion, la section **Administration** → **Utilitaires**. L'utilitaire se trouve dans le répertoire `webmin\utilities` du répertoire d'installation du Serveur Dr.Web (fichier exécutable `drweb-reloader-gui-windows-<nombre_de_bits>.exe`). S'il n'est pas disponible, il faut le télécharger selon l'[instruction](#).



La version [console](#) de l'utilitaire est également disponible.

11.5.1. Copier le référentiel d'un autre Serveur Dr.Web

Si le Serveur Dr.Web n'est pas connecté à Internet, vous pouvez mettre à jour le référentiel manuellement en copiant le référentiel d'un autre Serveur mis à jour.



Cette manipulation n'est pas destinée à la migration du Serveur Dr.Web vers une nouvelle version.

Pour transférer les mises à jour du référentiel d'un autre Serveur Dr.Web

1. Mettez à jour le référentiel du Serveur Dr.Web connecté à Internet depuis la section **Administration** → [Statut du référentiel](#) du Centre de gestion.
2. Depuis la rubrique [Contenu du référentiel](#) exportez le référentiel ou sa partie (les produits nécessaires) à l'aide du Centre de gestion. Dans ce cas, il est nécessaire de n'exporter que les types d'objets dont l'importation postérieure est supportée.
3. Copiez l'archive avec le référentiel exporté sur l'ordinateur avec le Serveur Dr.Web nécessitant les mises à jour.

Importez le référentiel téléchargé sur le Serveur Dr.Web via le Centre de gestion, depuis la rubrique **Administration** → [Contenu du référentiel](#).



Si vous utilisez les paramètres particuliers du référentiel, comme, par exemple, le blocage des révisions ou la mise à jour des Agents Dr.Web avec la révision spécifiée (pas la dernière), lors de l'importation du référentiel il est nécessaire d'activer l'option **Ajouter les révisions manquantes seulement** et désactivez l'option **Importer les fichiers de configuration**.

11.5.2. Chargeur du référentiel Dr.Web

S'il n'y a pas de possibilité de connecter un des Serveurs Dr.Web à Internet vous pouvez télécharger le référentiel depuis le SGM sans utiliser le logiciel du Serveur Dr.Web. Pour ce faire, l'utilitaire standard Chargeur du Référentiel Dr.Web est fourni.

Particularités de l'utilisation

- Pour télécharger le référentiel du SGM, vous avez besoin de la clé de licence de Dr.Web Enterprise Security Suite ou de son hash MD5 que vous pouvez trouver dans le Centre de gestion, dans la rubrique **Administration** → **Gestionnaire de licences**.
- Le Chargeur du référentiel Dr.Web est disponible dans les versions suivantes :
 - [version graphique](#) de l'utilitaire (uniquement au sein de la version sous Windows),



- [version console](#) de l'utilitaire.
- Pour télécharger le référentiel depuis le SGM, vous pouvez utiliser un serveur proxy.



Vous pouvez consulter l'ensemble de produits du référentiel dans la section [Gestion du référentiel du Serveur Dr.Web](#).

Si vous chargez la version du Serveur Dr.Web, la liste des produits disponibles pour téléchargement change également. Cliquez sur le bouton **Actualiser la liste** dans la liste des produits et assurez-vous que tous les produits nécessaires sont sélectionnés.

Moyens d'utilisation possibles

Téléchargement avec le remplacement manuel du référentiel

1. Téléchargez le référentiel du Serveur Dr.Web depuis le SGM en utilisant l'utilitaire Chargeur du référentiel Dr.Web.

Lors du téléchargement, créez une archive du référentiel :

- a) Pour l'utilitaire graphique : sélectionnez le mode **Télécharger le référentiel** et cochez la case **Archiver le référentiel** dans la fenêtre principale de l'utilitaire.
 - b) Pour l'utilitaire de console : utilisez la clé `--archive`.
2. Copiez l'archive avec le référentiel téléchargé sur l'ordinateur avec le Serveur Dr.Web nécessitant les mises à jour.

Importez le référentiel téléchargé sur le Serveur Dr.Web via le Centre de gestion, depuis la rubrique **Administration** → [Contenu du référentiel](#).



Si vous utilisez les paramètres particuliers du référentiel, comme, par exemple, le blocage des révisions ou la mise à jour des Agents Dr.Web avec la révision spécifiée (pas la dernière), lors de l'importation du référentiel il est nécessaire d'activer l'option **Ajouter les révisions manquantes seulement** et désactivez l'option **Importer les fichiers de configuration**.

Création du miroir du référentiel sur le Serveur du réseau local

1. Téléchargez le référentiel du Serveur Dr.Web depuis le SGM en utilisant l'utilitaire graphique Chargeur du référentiel Dr.Web.

Lors du téléchargement, sélectionnez le mode **Synchroniser le miroir de mise à jour** dans la fenêtre principale de l'utilitaire.

2. Envoyez le référentiel téléchargé sur le serveur web de votre réseau local qui servira pour le partage des mises à jour du référentiel.
3. Dans la rubrique **Administration** → [Configuration générale du référentiel](#), configurez l'obtention des mises à jour par le Serveur Dr.Web depuis votre miroir local et non pas depuis les serveurs du SGM Dr.Web. La sélection du protocole pour le téléchargement des



mises à jour dépendra du type du serveur de l'étape 2 : HTTP/HTTPS pour le serveur web, FTP/FTPS pour le serveur FTP, etc. Le protocole FILE fait exception, il n'est pas disponible pour l'utilisation via le réseau (voir [Création du miroir du référentiel sur le Serveur Dr.Web](#)).

Création du miroir du référentiel sur le Serveur Dr.Web

1. Téléchargez le référentiel du Serveur Dr.Web depuis le SGM en utilisant l'utilitaire Chargeur du référentiel Dr.Web.

Lors du téléchargement, sélectionnez le mode **Synchroniser le miroir de mise à jour** dans la fenêtre principale de l'utilitaire.

2. Placez le miroir téléchargé dans un répertoire aléatoire sur l'ordinateur avec le Serveur Dr.Web installé.
3. Dans la rubrique **Administration** → [Configuration générale du référentiel](#), configurez l'obtention des mises à jour avec l'utilisation du protocole FILE.

Dans le champ **URI de base**, il est nécessaire de spécifier le chemin local complet vers le répertoire dans lequel se trouve le miroir. Dans ce cas, le paramètre **Liste des serveurs du Système global de mise à jour Dr.Web** n'est pas utilisé.



Assurez-vous que le miroir est placé dans le répertoire portant le nom 13.00. Dans ce cas, dans le champ **URI de base**, vous devez indiquer le chemin d'accès au répertoire sans indiquer le répertoire même.

11.5.2.1. Utilitaire graphique

La version graphique de l'utilitaire Chargeur du référentiel Dr.Web est disponible uniquement sous Windows et peut être téléchargée via le Centre de gestion, depuis la rubrique **Administration** → **Utilitaires**. Vous pouvez lancer cette version de l'utilitaire sur n'importe quel ordinateur tournant sous Windows et ayant l'accès à Internet.

L'utilitaire se trouve dans le répertoire `webmin\utilities` du répertoire d'installation du Serveur Dr.Web. Fichier exécutable `drweb-reloader-gui-windows-<nombre de bits>.exe`.

Pour télécharger le référentiel via la version graphique du Chargeur du référentiel Dr.Web

1. Lancez la version graphique de l'utilitaire Chargeur du référentiel Dr.Web.
2. Dans la fenêtre principale de l'utilitaire, configurez les paramètres suivants :
 - a) **Clé de licence ou MD5 de la clé** : indiquez le fichier clé de licence Dr.Web. Pour ce faire, cliquez sur **Parcourir** et sélectionnez le fichier clé de licence valide. A la place de la clé de licence vous pouvez spécifier le hash MD5 de la clé de licence qui est visible dans le Centre de gestion, dans la rubrique **Administration** → **Gestionnaire de licences**.
 - b) **Répertoire de téléchargement** : spécifiez le répertoire dans lequel le référentiel sera téléchargé.



- c) Dans la liste **Mode**, sélectionnez un des modes de téléchargement des mises à jour :
- **Télécharger le référentiel** : le référentiel est téléchargé sous forme du référentiel du Serveur Dr.Web. Les fichiers téléchargés peuvent être importés via le Centre de gestion en tant que la mise à jour du référentiel du Serveur Dr.Web.
 - **Synchroniser le miroir de mise à jour** : le référentiel est téléchargé sous forme de la zone des mises à jour du SGM. Les fichiers téléchargés peuvent être placés en miroir de mise à jour dans votre réseau local. Ensuite, les Serveurs Dr.Web peuvent être configurés pour recevoir des mises à jours directement depuis ce miroir de mise à jour contenant la dernière version du référentiel et non pas depuis les serveurs du SGM.
- d) Cochez la case **Archiver** pour mettre automatiquement le référentiel téléchargé en archive zip. Cette option permet d'obtenir une archive du référentiel téléchargé prête à importer sur le Serveur Dr.Web avec le Centre de gestion de la rubrique **Administration** → [Contenu du référentiel](#).
3. Si vous voulez modifier les paramètres supplémentaires de connexion au SGM et du téléchargement des mises à jour, cliquez sur **Paramètres avancés**. Dans la fenêtre qui s'affiche, les onglets suivants sont disponibles :
- a) Dans l'onglet **Produits**, vous pouvez modifier la liste des produits téléchargés. Dans la fenêtre de paramètre, vous pouvez consulter la liste de tous les produits du référentiel disponibles pour le téléchargement depuis le SGM :
- Pour actualiser la liste des produits disponibles en ce moment dans le SGM, cliquez sur **Actualiser**.
 - Cochez les cases contre les produits que vous voulez télécharger depuis le SGM ou la case dans l'en-tête du tableau pour sélectionner tous les produits de la liste.
- b) Dans l'onglet **SGM Dr.Web**, vous pouvez configurer les paramètres des serveurs de mises à jour :
- Les serveurs SGM sont listés dans l'ordre dans lequel l'utilitaire les contacte lors du téléchargement du référentiel. Pour modifier l'ordre des serveurs SGM, utilisez les boutons **En haut** et **En bas**.
 - Pour ajouter un serveur SGM dans la liste des serveurs utilisés lors du téléchargement, entrez l'adresse du Serveur SGM dans le champ au-dessus de la liste de serveurs et cliquez sur **Ajouter**.
 - Pour supprimer un serveur SGM de la liste de serveurs utilisés lors du téléchargement, sélectionnez le serveur à supprimer et cliquez sur **Supprimer**.
 - Dans le champ **URL de base**, est indiqué le répertoire se trouvant sur les serveurs SGM contenant les mises à jour des produits Dr.Web.
 - Dans la liste déroulante **Protocole**, sélectionnez le type de protocole pour obtenir les mises à jour depuis les Serveurs de mises à jour. Le téléchargement des mises à jour s'effectue conformément à la liste des serveurs du SGM pour tous les protocoles.
 - Dans la liste déroulante **Certificats autorisés**, sélectionnez le type des certificats SSL qui seront appliqués automatiquement. Ce paramètre est utilisé uniquement pour les protocoles sécurisés supportant le chiffrement.



- **Login** et **Mot de passe** : identifiants de l'utilisateur utilisé pour l'authentification sur le Serveur des mises à jour, si le serveur exige l'authentification.
 - Cochez la case **Utiliser CDN** pour autoriser l'utilisation de Content Delivery Network lors du chargement du référentiel.
- c) Dans l'onglet **Proxy**, vous pouvez spécifier les paramètres de connexion au SGM via le serveur proxy :
- **Adresse du serveur proxy** et **Port** : adresse réseau et numéro du port du serveur proxy utilisé.
 - **Nom d'utilisateur** et **Mot de passe** : paramètres de l'authentification sur le serveur proxy, si ce serveur exige l'authentification.
- d) Dans l'onglet **Planificateur**, vous pouvez configurer la planification des mises à jour périodiques. Pour exécuter la planification, le planificateur de tâches Windows est utilisé. Dans ce cas, vous n'avez pas besoin de lancer l'utilitaire manuellement, le chargement du référentiel sera effectué automatiquement conformément à la périodicité spécifiée.
- e) Dans l'onglet **Journal**, vous pouvez configurer la journalisation des téléchargements des mises à jour.

Cliquez sur **OK** pour appliquer les modifications apportées et retourner dans la fenêtre principal du Chargeur de référentiel Dr.Web.

4. Après avoir modifié tous les paramètres, cliquez sur **Télécharger** dans la fenêtre principale du Chargeur du référentiel Dr.Web pour se connecter au SGM et commencer le téléchargement du référentiel.

11.5.2.2. Utilitaire console

Il existe les versions suivantes de l'utilitaire de console Chargeur du référentiel Dr.Web :

Fichier exécutable	Localisation	Description
drweb-reloader- <OS>-<nombre de bits>	Centre de gestion, section Administration → Utilitaires	Version indépendante de l'utilitaire. Elle peut être lancée d'un répertoire aléatoire ou sur n'importe quel ordinateur ayant le système d'exploitation correspondant.
	Répertoire du Serveur Dr.Web webmin/utilities	
drwreloader	Répertoire du Serveur Dr.Web bin	La version de l'utilitaire dépend de la présence des bibliothèques de serveur. Elle peut être lancée uniquement du répertoire de son emplacement.



Vous pouvez trouver la description des clés de ligne de commande pour la version de console de l'utilitaire du Chargeur de référentiels dans les **Annexes**, [H7.5. Chargeur du référentiel Dr.Web](#).



11.6. Restrictions de mises à jour des postes




Le Centre de gestion vous permet de configurer la limitation du trafic lors du transfert des mises à jour entre le Serveur Dr.Web et les Agents Dr.Web sur les postes protégés dans des délais spécifiés.

Pour en savoir plus, voir le p. [Limitation du trafic des postes de travail](#).



Les limitations de vitesse ne sont pas acceptées lors de l'installation supplémentaire des nouveaux composants ainsi que lors de la mise à jour lancée par l'administrateur avec l'option **Restaurer les composants échoués** de la barre d'outils.

Pour configurer le mode de limitation du trafic

1. Sélectionnez l'élément **Réseau antivirus** du menu principal et dans la fenêtre qui apparaît, cliquez sur le nom du poste ou du groupe dans la liste hiérarchique. Dans le [menu de gestion](#), sélectionnez l'élément **Restrictions de mise à jour**.
2. Dans la liste déroulante **Restrictions de mise à jour**, sélectionnez un mode de restriction :
 - **Mettre à jour tous les produits** : ne pas appliquer les limitations à la distribution des mises à jour sur les postes.
 - **Interdire toutes les mises à jour** : interdire la distribution de toutes les mises à jour sur les postes durant le délai spécifié dans le tableau ci-dessous **Planification des mises à jour des postes**.
 - **Mettre à jour seulement les bases** : interdire la distribution des mises à jour uniquement pour les modules du logiciel durant le délai spécifié dans le tableau **Planification des mises à jour des postes** ci-dessous. Les mises à jour des bases virales seront effectuées sans modification dans un mode normal.
3. Cochez la case **Baisser l'importance de l'obsolescence des bases virales** pour réduire l'importance du statut des postes ayant des bases virales obsolètes. Si la case est cochée, les postes ayant les bases virales obsolètes seront affichés dans le réseau antivirus avec l'icône commune , et dans la section **Importance**, les postes auront le statut **Basse**. Si la case est décochée, les postes ayant les bases virales obsolètes seront affichés dans le réseau antivirus avec l'icône  (si l'option est activée dans la barre d'outils  **Configuration de l'arborescence** → **Afficher l'importance de l'état de postes**), et dans la section **Statut**, les postes auront l'importance **Maximale**. ou **haute**.
4. Dans le champ **Délai de validité des révisions**, vous pouvez spécifier un délai pendant lequel les révisions des produits installés sur les postes seront considérées comme valides en cas d'apparition des révisions plus récentes dans le référentiel du Serveur Dr.Web.
5. Cochez la case **Recevoir les dernières mises à jour** pour que le poste reçoive toutes les mises à jour des composants sans tenir compte des limitations indiquées à la rubrique [Configuration détaillée du référentiel](#).



Si la case est décochée, le poste reçoit uniquement les mises à jour marquées comme actuelles.

6. Cochez la case **Autoriser le passage aux révisions précédentes** pour autoriser à remplacer les nouvelles versions des composants antivirus sur les postes par les révisions précédentes provenant du référentiel du Serveur Dr.Web conformément aux paramètres de diffusion. Voir aussi [Restauration de la version précédente de la révision du produit](#).

7. Cochez la case **Limiter le trafic des mises à jour**, pour limiter le volume du trafic réseau pour le transfert des mises à jour entre le Serveur Dr.Web et les Agents Dr.Web.

Si la case est décochée, les mises à jour des Agents Dr.Web seront transmises sans aucune limitation de la bande passante.

Si la case est cochée, spécifiez les champs suivants :

- Dans le champ **Vitesse par défaut**, indiquez la valeur de la vitesse maximum du transfert des mises à jour utilisée par défaut, c'est-à-dire si aucune autre limitation n'est spécifiée (les cases blanches dans le tableau de planification). La valeur de la vitesse par défaut est également utilisée pour les périodes quand le transfert de données est interdit, mais le processus de la mise à jour a été déjà lancé (voir ci-dessous).
- Dans le champ **Vitesse maximale du transfert (Ko/s)** indiquez la vitesse maximale du transfert des mises à jour. Les mises à jour seront transmises par tranches de bande passante allouée au trafic réseau total relatif aux mises à jour de tous les Agents Dr.Web.. Il est possible de spécifier cinq limitations de la vitesse de transmission de données pour le transfert des mises à jour au maximum. Pour ajouter encore un champ de limitation de vitesse cliquez sur le bouton **+**. Pour supprimer une limitation de vitesse, cliquez sur **-** contre la limitation qu'il faut supprimer.



Pour les champs **Vitesse par défaut** et **Vitesse maximum du transfert (Ko/s)**, il existe les limitations suivantes :

- Il est interdit de spécifier la valeur 0. La valeur minimum de la limitation — 1 Ko/s.
- La valeur vide (le champ n'est pas rempli) enlève toutes les limitations du trafic des mises à jour pour un délai de temps correspondant.

Dans le tableau de planification, les limitations sont définies séparément pour chaque 30 minutes de chaque jour de la semaine.



	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Lu																								
Ma																								
Me																								
Je																								
Ve																								
Sa																								
Di																								

- Illimité
- La vitesse est limitée jusqu'à 1 Ko/s
- Le transfert de données est bloqué

Pour modifier le mode de limitation de transmission de données, cliquez sur le bloc correspondant dans le tableau. La sélection de plusieurs blocs temporaires à l'aide du principe glisser-déposer est aussi prise en charge.

La couleur des cases varie cycliquement conformément au schéma de couleurs en dessous du tableau.



Dans les délais de temps correspondant à la valeur **Transfert des données interdit**, il est interdit de commencer le transfert des mises à jour. Si au moment du commencement de ce délai, le transfert de mises à jour a été déjà lancé, il ne sera pas interrompu, mais la vitesse maximum sera limitée par la valeur spécifiée dans le champ **Vitesse par défaut**.

8. Après avoir apporté les modifications, cliquez sur **Sauvegarder** pour les appliquer.

Les options suivantes de gestion de la rubrique sont disponibles dans la barre d'outils :

Restaurer tous les paramètres à leur valeur initiale : restaurer les valeurs données à tous les paramètres de cette rubrique avant modification (dernières valeurs sauvegardées).

Restaurer tous les paramètres à leur valeur par défaut : restaurer les valeurs par défaut de tous les paramètres de la rubrique.

Diffuser les paramètres vers un autre objet : copier les paramètres de cette rubrique sur un autre poste, un autre groupe ou plusieurs groupes et postes.

Configurer l'héritage des paramètres d'une politique ou d'un groupe primaire : supprimer les paramètres personnalisés du poste et configurer l'héritage des paramètres du groupe primaire.

Copier les paramètres d'une politique ou d'un groupe primaire et les définir comme personnalisés : copier les paramètres de cette rubrique du groupe primaire et les assigner à des postes sélectionnés. L'héritage n'est pas défini et les paramètres des postes sont considérés comme personnalisés.



 **Exporter les paramètres de cette section vers un fichier** : sauvegarder tous les paramètres de cette rubrique dans un fichier au format spécifique.

 **Importer les paramètres dans cette section depuis un fichier** remplacer tous les paramètres de cette rubrique par les paramètres du fichier au format spécifique.

11.7. Mise à jour des Agents Dr.Web en mode mobile

Si votre ordinateur, ordinateur portable ou l'appareil mobile ne sera pas connecté au Serveur Dr.Web pendant beaucoup de temps, afin de pouvoir recevoir les mises à jour depuis des Serveurs du SGM Dr.Web, il est recommandé d'installer sur le poste le *Mode mobile* de l'Agent Dr.Web.



L'activation du Mode mobile sera disponible dans les paramètres de l'Agent Dr.Web uniquement si l'utilisation du Mode mobile est autorisé dans le Centre de gestion, dans la section **Réseau antivirus** → **Droits** → `<ystème_d'exploitation>` → **Général** → **Modifier la configuration de l'Agent Dr.Web** (pour les OS Windows) ou **Lancer en mode mobile** (pour les autres systèmes d'exploitation).

En Mode mobile, l'Agent Dr.Web fait trois tentatives de se connecter au Serveur Dr.Web et en cas d'échec, il effectue une mise à jour depuis les serveurs du SGM via HTTP. Les tentatives de trouver le Serveur Dr.Web sont effectuées chaque minute.

Lorsque l'Agent Dr.Web fonctionne en Mode mobile, la connexion de l'Agent Dr.Web avec le Serveur Dr.Web est interrompue. Toutes les modifications pouvant être apportées sur le Serveur Dr.Web pour le poste concerné entreront en vigueur dès que le Mode mobile de l'Agent Dr.Web aura été désactivé et que la connexion entre l'Agent Dr.Web et le Serveur Dr.Web aura été rétablie.



Seules les bases virales sont mises à jour lorsque le mode mobile est activé.

En Mode mobile, le fonctionnement de l'Agent Dr.Web n'est pas limité dans le temps, pourtant la mise à jour des bases virales depuis le SGM est effectuée uniquement jusqu'à la fin de validité de la clé de licence du poste. Les informations sur la clé de licence ont été enregistrées par l'Agent Dr.Web lors de la dernière connexion au Serveur Dr.Web (la clé de licence se trouve sur le Serveur Dr.Web).

La configuration des paramètres du mode mobile du côté de l'Agent Dr.Web est décrite dans le **Manuel Utilisateur**.



Chapitre 12 : Configuration des composants supplémentaires

12.1. Serveur proxy Dr.Web

Le réseau antivirus peut comprendre un ou plusieurs Serveurs proxy Dr.Web.

L'objectif principal du Serveur proxy Dr.Web est d'assurer la connexion entre le Serveur Dr.Web et les Agents Dr.Web dans le cas où l'accès direct devient impossible (par exemple si le Serveur Dr.Web et les Agents Dr.Web se trouvent dans des réseaux différents entre lesquels il n'y a pas de routage de paquets).

Le Serveur proxy Dr.Web 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 Dr.Web et la connexion entre le Serveur Dr.Web et le Serveur proxy Dr.Web et pour réduire le délai 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 Dr.Web, 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 Dr.Web.

Fonctions clés

Le Serveur proxy Dr.Web remplit les fonctions suivantes :

1. Écoute du réseau et réception des connexions conformément au protocole et au port spécifiés.
2. Relais des protocoles (les protocoles TCP/IP sont supportés).
3. Envoi de données entre le Serveur Dr.Web et les Agents Dr.Web conformément à la configuration du Serveur proxy Dr.Web.
4. Mise en cache des mises à jour de l'Agent Dr.Web et du package antivirus transmis par le Serveur Dr.Web. La répartition des mises à jour depuis le cache du Serveur proxy Dr.Web offre les avantages suivants :
 - diminution du trafic réseau,
 - minimisation de la durée de réception des mises à jour par les Agents Dr.Web.
5. Chiffrement du trafic entre les Serveurs Dr.Web et les Agents Dr.Web.



Il est possible de créer une hiérarchie des Serveurs proxy Dr.Web.

Le schéma général du réseau antivirus en cas d'utilisation du Serveur proxy Dr.Web est représenté sur la [fig. 12-1](#).

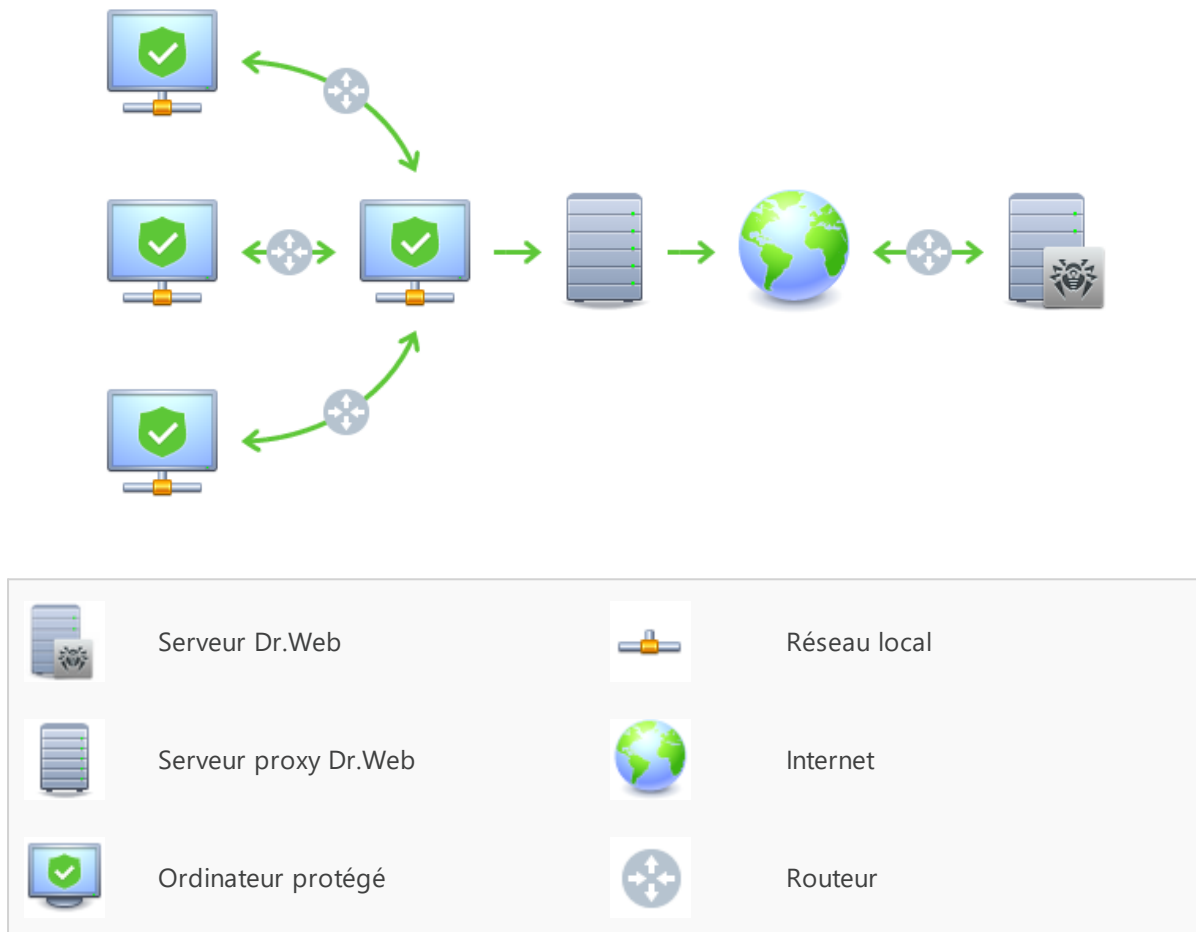


Figure 12-1. Schéma du réseau antivirus en cas d'utilisation du Serveur proxy Dr.Web

Principe de fonctionnement

Les instructions à suivre en cas d'utilisation du Serveur proxy Dr.Web :

1. Si l'adresse du Serveur Dr.Web n'est pas spécifiée dans les paramètres de l'Agent Dr.Web, l'Agent Dr.Web envoie une requête multi-adresses conformément au protocole réseau dans lequel il se trouve.
2. Si le Serveur proxy Dr.Web est configuré pour le relais des connexions (le paramètre `discovery="yes"`), un message sera envoyé vers l'Agent Dr.Web pour l'informer de la présence du Serveur proxy Dr.Web opérationnel.
3. L'Agent Dr.Web spécifie les paramètres reçus du Serveur proxy Dr.Web en tant que paramètres du Serveur Dr.Web. L'interaction ultérieure se fait de manière transparente pour l'Agent Dr.Web.



4. Conformément aux paramètres du fichier de configuration, le Serveur proxy Dr.Web écoute les ports spécifiés afin de contrôler les connexions entrantes via les protocoles spécifiés.
5. Pour chaque connexion entrante depuis l'Agent Dr.Web, le Serveur proxy Dr.Web établit une connexion avec le Serveur Dr.Web.

Algorithme de redirection en cas de présence d'une liste des Serveurs Dr.Web :

1. Le Serveur proxy Dr.Web télécharge la liste des Serveurs Dr.Web dans la mémoire vive depuis le fichier de configuration `drwcsd-proxy.conf` (voir le document **Annexes, F4. Fichier de configuration du Serveur proxy Dr.Web**).
2. L'Agent Dr.Web se connecte au Serveur proxy Dr.Web.
3. Le Serveur proxy Dr.Web redirige le trafic de l'Agent Dr.Web vers le premier Serveur Dr.Web mentionné dans la liste dans la mémoire vive.
4. Le Serveur proxy Dr.Web effectue une rotation de la liste chargée dans la mémoire vive en déplaçant le Serveur Dr.Web de la première place vers la fin de la liste.



Le Serveur proxy Dr.Web ne conserve pas l'ordre modifié des Serveurs Dr.Web dans son fichier de configuration. Au redémarrage du Serveur proxy Dr.Web, la liste des Serveurs Dr.Web est chargée dans la mémoire vive dans son état initial dans lequel elle est enregistrée dans le fichier de configuration.

5. Lorsque l'Agent Dr.Web suivant se connecte au Serveur proxy Dr.Web, la procédure se reproduit à partir de l'étape 2.
6. Si le Serveur Dr.Web se déconnecte du réseau antivirus (par exemple, en cas d'arrêt ou refus de service), l'Agent Dr.Web se connecte à nouveau au Serveur proxy Dr.Web et la procédure se reproduit à partir de l'étape 2.



Lancé sur l'ordinateur depuis un réseau externe par rapport aux Agents du réseau, le [Scanner réseau](#) ne pourra pas détecter les Agents installés Dr.Web.



Si la case **Remplacer les noms NetBIOS** est cochée dans les paramètres du Serveur Dr.Web et que le Serveur proxy Dr.Web est utilisé dans le réseau antivirus, le nom de l'ordinateur sur lequel est installé le Serveur proxy Dr.Web sera affiché à la place du nom du poste dans le Centre de gestion pour tous les postes connectés au Serveur Dr.Web via le Serveur proxy Dr.Web.

Chiffrement et compression du trafic

Le Serveur proxy Dr.Web prend en charge la compression du trafic. Les informations transférées seront traitées selon la compression/non compression du trafic.

Le Serveur proxy Dr.Web supporte le chiffrement du trafic. Pour assurer le chiffrement, le Serveur proxy Dr.Web doit se connecter au Serveur Dr.Web (voir le **Manuel d'installation, Connexion du Serveur proxy Dr.Web au Serveur Dr.Web**) et signer son certificat par le certificat



et la clé privée du Serveur Dr.Web. Le chiffrement du trafic entre le Serveur proxy Dr.Web et le Serveur Dr.Web s'effectue à la base du certificat du Serveur Dr.Web ; le chiffrement du trafic entre le Serveur proxy Dr.Web et les Agents Dr.Web s'effectue à la base du certificat du Serveur proxy Dr.Web signé par le certificat et la clé privée du Serveur Dr.Web.

Mise en cache

Le Serveur proxy Dr.Web prend en charge la mise en cache du trafic.

La mise en cache des produits se fait selon les révisions. Chaque révision se trouve dans un dossier séparé. Le dossier de chaque révision suivante contient des *liens matériels (hard links)* vers les fichiers existants des révisions antérieures ainsi que vers les originaux des fichiers modifiés. Ainsi, les fichiers de chaque version sont sauvegardés sur le disque dur en un seul exemplaire, tous les dossiers relatifs aux révisions postérieures ne contiennent que des liens vers les fichiers non modifiés.

Les paramètres spécifiés dans le fichier de configuration permettent de configurer les actions suivantes lors de la mise en cache :

- Nettoyer périodiquement les révisions périmées. Par défaut — 1 fois par heure.
- Sauvegarder les dernières révisions. Toutes les autres révisions sont considérées comme périmées et elles sont supprimées. Seules les trois dernières révisions sont conservées par défaut.
- Télécharger périodiquement les fichiers *memory mapped* non utilisés. Par défaut — toutes les 10 minutes.

Paramètres

Le Serveur proxy Dr.Web n'a pas d'interface graphique. Les paramètres sont configurés par l'un des moyens suivants :

1. A distance, via le Centre de gestion, si le Serveur proxy Dr.Web est connecté au Serveur Dr.Web (voir [Configuration distante du Serveur proxy](#)).
2. En mode local à l'aide du fichier de configuration. Le format du fichier de configuration du Serveur proxy Dr.Web est affiché dans le document **Annexes**, [Connexion du Serveur proxy Dr.Web au Serveur Dr.Web](#).



Pour modifier les paramètres (éditer le fichier de configuration) du Serveur proxy Dr.Web, les droits d'administrateur sur la machine sont requis.

Pour un fonctionnement correct du Serveur Proxy Dr.Web sous OS de la famille Linux, après un redémarrage de l'ordinateur, un paramétrage système du réseau sans utiliser le Gestionnaire de réseau sera requis.



Démarrage et arrêt

Sous Windows, le démarrage et l'arrêt du Serveur proxy Dr.Web s'effectuent avec les outils standard depuis l'élément **Panneau de configuration** → **Outils d'administration** → **Services** → dans la liste des services, double-cliquez sur **drwcsd-proxy**, puis dans la fenêtre qui apparaît, sélectionnez l'action nécessaire.

Sous les OS de la famille Unix, le démarrage et l'arrêt du Serveur proxy Dr.Web s'effectuent avec les commandes `start` et `stop` via les scripts créés lors de l'installation du Serveur proxy (voir le **Manuel d'installation**, [Installation du Serveur proxy Dr.Web](#)).

Pour démarrer le Serveur proxy Dr.Web sous Windows et les OS de la famille Unix, vous pouvez également lancer le fichier exécutable `drwcsd-proxy` avec les paramètres correspondants (voir [G5. Serveur proxy Dr.Web](#)).

12.1.1. Configuration distante du Serveur proxy

Après la connexion du Serveur proxy Dr.Web au Serveur Dr.Web, vous avez la possibilité de configurer à distance les paramètres du Serveur proxy Dr.Web via le Centre de gestion.



Pour en savoir plus sur les paramètres de connexion et sur la connexion rapide à l'aide de la ligne de commande, consultez le **Manuel d'installation**, la rubrique [Connexion du Serveur proxy Dr.Web au Serveur Dr.Web](#).



Le Serveur proxy Dr.Web peut recevoir les paramètres uniquement depuis un ensemble particulier des Serveurs Dr.Web connectés qui sont marqués comme gérants. Si aucun Serveur Dr.Web n'est marqué comme gérant, la connexion se fait à tous les Serveurs Dr.Web à tour de rôle jusqu'à la première obtention d'une configuration valide (non vide).

Si le Serveur Dr.Web n'est pas marqué comme gérant (la valeur du paramètre **Serveur Dr.Web gérant** est **Non**), le Serveur proxy Dr.Web ne peut en recevoir aucun paramètre. Cela signifie également que depuis ce Serveur Dr.Web il est impossible de l'affecter à distance comme gérant pour le Serveur proxy Dr.Web. Dans ce cas, il est nécessaire de modifier manuellement la valeur du paramètre `<forward to="" master="">` du fichier de configuration du Serveur proxy Dr.Web (voir le document **Annexes**, [F6. Fichier de configuration du Serveur proxy Dr.Web](#)).


Pour configurer les paramètres du Serveur proxy Dr.Web :

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 Serveur proxy Dr.Web ou du groupe **Proxies** dans l'arborescence.
2. Dans le [menu de gestion](#) qui s'affiche, sélectionnez l'élément **Serveur proxy Dr.Web**. La section des paramètres va s'ouvrir.



3. Dans l'onglet **Certificat**, vous pouvez spécifier la liste des certificats Dr.Web. Il faut que les certificats de tous les Serveurs auxquels le Serveur proxy Dr.Web se connecte et sur lesquels le trafic client est redirigé soient disponibles.
 - Le certificat du Serveur Dr.Web est requis pour la connexion au Serveur Dr.Web afin de gérer à distance les paramètres et chiffrer le trafic entre le Serveur Dr.Web et le Serveur proxy Dr.Web.
 - Le certificat du Serveur proxy Dr.Web signé par le certificat et la clé privée du Serveur Dr.Web (la procédure se fait automatiquement sur le Serveur Dr.Web après la connexion et elle ne nécessite pas l'intervention de l'administrateur) est requis pour la connexion des Agents Dr.Web et le support du chiffrement entre les Agents Dr.Web et le Serveur proxy Dr.Web.
4. Dans l'onglet **Écoute**, vous pouvez configurer les paramètres de réception et de redirection du trafic du Serveur proxy Dr.Web.

Pour les paramètres uniques d'écoute du réseau, vous pouvez spécifier les paramètres uniques de connexion de tous les clients et les paramètres spécifiés séparément pour chaque Serveur Dr.Web.

Pour ajouter encore un bloc de paramètres, cliquez sur le bouton .

Pour supprimer un bloc de paramètres, cliquez sur  près du bloc à supprimer.

Vous pouvez configurer les paramètres du Serveur proxy Dr.Web séparément pour chaque bloc :

a) Dans la section de paramètres d'écoute :

- Dans le champ **Adresse d'écoute**, spécifiez l'adresse IP écoutée par le Serveur proxy Dr.Web. La valeur 0.0.0.0 indique d'écouter toutes les interfaces.



Les adresses sont spécifiées au format d'adresse réseau décrit dans le document [Annexes, Annexe D. Spécification de l'adresse réseau](#).

- Dans le champ **Port**, spécifiez le numéro du port qui sera « écouté » par le Serveur proxy Dr.Web. Par défaut c'est le port 2193.
- Cochez la case **Détection** pour activer le mode d'imitation du Serveur Dr.Web. Ce mode permet aux clients de détecter le Serveur proxy Dr.Web en tant que Serveur Dr.Web lors de sa recherche par les requêtes broadcast.
- Cochez la case **Multicasting** pour que le Serveur proxy Dr.Web réponde aux requêtes broadcast adressées au Serveur Dr.Web.
- Dans le champ **Groupe Multicast**, entrez l'adresse IP du groupe de multidiffusion dont le Serveur proxy Dr.Web fera partie. L'interface spécifiée sera "écoutée" par le Serveur proxy Dr.Web 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 Dr.Web ne sera inclus dans aucun groupe de multidiffusion. Par défaut, le Serveur Dr.Web appartient au groupe de multidiffusion 231.0.0.1.




b) 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 Dr.Web et les clients servis : les Agents Dr.Web et les installateurs des Agents Dr.Web.
 - Dans la liste déroulante **Compression**, sélectionnez le mode de compression du trafic pour les canaux entre le Serveur proxy Dr.Web et les clients servis : les Agents Dr.Web et les installateurs des Agents Dr.Web. Dans le champ **Niveau de compression**, spécifiez le niveau de compression (de 1 à 9).
- c) Dans la section **Paramètres de connexion avec les Serveurs Dr.Web**, vous pouvez spécifier la liste des Serveurs Dr.Web vers lesquels le trafic sera redirigé.

L'ordre de redirection du trafic client et l'ordre de connexion du Serveur proxy Dr.Web aux Serveurs Dr.Web pour l'obtention des paramètres dépend de l'ordre des Serveurs Dr.Web dans la liste. Pour modifier l'ordre des Serveurs Dr.Web, glissez-déposez les lignes nécessaires avec le souris.

Pour gérer les Serveurs Dr.Web, utilisez les boutons situés dans la barre d'outils de la liste des Serveurs Dr.Web :

-  éditer les paramètres de connexion avec le Serveur Dr.Web sélectionné,
-  ajouter les paramètres de connexion avec le Serveur Dr.Web,
-  supprimer les paramètres de connexion avec le Serveur Dr.Web sélectionné.

Lors de l'édition ou la création des paramètres de connexion avec les Serveurs Dr.Web, la fenêtre de paramètres s'ouvre contenant les options suivantes :

- Dans la liste déroulante **Serveur gérant Dr.Web**, sélectionnez une des options pour désigner le Serveur Dr.Web comme gérant :
 - Oui** : le Serveur Dr.Web sera gérant sans condition. Vous pouvez désigner n'importe quel nombre de Serveurs Dr.Web comme gérants. Dans ce cas, la connexion se fait à tous les Serveurs Dr.Web gérants dans l'ordre spécifié dans les paramètres du Serveur proxy Dr.Web jusqu'à la première obtention d'une configuration valide (non vide).
 - Non** : Le Serveur Dr.Web ne sera pas gérant en aucun cas. Vous pouvez également ne désigner aucun Serveur Dr.Web comme gérant. Dans ce cas, la configuration des paramètres du Serveur proxy Dr.Web (y compris la désignation des Serveurs gérants Dr.Web) se fait uniquement via le fichier de configuration du Serveur proxy Dr.Web, de manière locale (voir le document **Annexes**, la rubrique [F4. Fichier de configuration du Serveur proxy Dr.Web](#)).
 - Possible** : le Serveur Dr.Web sera gérant uniquement s'il n'y a pas de Serveurs gérants sans condition (avec la valeur **Oui** spécifiée pour ce paramètre).
- Dans le champ **Adresse de redirection**, spécifiez l'adresse du Serveur Dr.Web vers lequel les connexions établies par le Serveur proxy Dr.Web seront redirigées. Il est recommandé d'utiliser le nom du Serveur Dr.Web au [format FQDN](#) en tant qu'adresse du Serveur Dr.Web.



Si l'adresse n'est pas spécifiée dans le champ **Rediriger vers** ou que la valeur `udp/` est indiquée, le Serveur proxy Dr.Web tentera de trouver le Serveur Dr.Web via le service de détection - l'envoi de requêtes broadcast (voir l'étape 9).



Les adresses sont spécifiées au format d'adresse réseau décrit dans le document [Annexes, Annexe D. 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 Dr.Web 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 Dr.Web et le Serveur Dr.Web spécifié. Dans la liste déroulante **Niveau de compression**, sélectionnez le niveau de compression (de 1 à 9).

Dans le tableau, vous pouvez spécifier les paramètres de limitation du trafic transmis de la même manière que les paramètres du Serveur Dr.Web figurant dans les sections [Mises à jour](#) et [Installations](#).

5. Dans l'onglet **Cache**, configurez les paramètres suivants de la mise en cache du Serveur proxy Dr.Web :

Cochez la case **Activer la mise en cache** pour mettre en cache les données transmises par le Serveur proxy Dr.Web 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.
- Cochez la case **Utiliser la mise en cache proactive** pour télécharger de nouvelles révisions des produits sélectionnés sur le Serveur proxy Dr.Web depuis le Serveur Dr.Web conformément à la planification ci-dessus. Pendant cette période, les révisions sont téléchargées sur le Serveur proxy Dr.Web tout de suite après que le Serveur Dr.Web les a reçues du SGM. Si la case est décochée, le téléchargement de nouvelles révisions sur le Serveur proxy Dr.Web se fait uniquement si l'Agent Dr.Web demande ces révisions du Serveur Dr.Web.
 - Dans la liste ci-dessous, cochez les case pour les produits à synchroniser.
 - Dans la section **Planification de synchronisation des référentiels**, spécifiez la planification selon laquelle les mises à jour des produits sélectionnés seront téléchargées.

Pour modifier le mode de limitation de transmission de données, cliquez sur le bloc correspondant dans le tableau. La sélection de plusieurs blocs temporaires à l'aide du principe glisser-déposer est aussi prise en charge.

La couleur des cases varient cycliquement conformément au schéma en couleurs



figurant au-dessous du tableau : le transfert de données est autorisé sans aucune limitation de trafic ou le transfert de données est complètement interdit.

6. Dans l'onglet **Événements**, spécifiez les paramètres suivants de transfert de données :
 - Cochez la case **Mettre en cache les événements** pour mettre en cache les événements reçus des Agents Dr.Web. Dans ce cas, les événements seront envoyés sur le Serveur Dr.Web toutes les 15 minutes pendant la période autorisée pour l'envoi des événements selon la planification ci-dessous. Si la mise en cache est désactivée, les événements seront envoyés sur le Serveur Dr.Web tout de suite après leur réception par le Serveur proxy Dr.Web.
 - Dans la section **Planification de synchronisation des événements**, spécifiez la planification selon laquelle les événements reçus des Agents Dr.Web seront transmis. Pour modifier le mode de limitation de transmission de données, cliquez sur le bloc correspondant dans le tableau. La sélection de plusieurs blocs temporaires à l'aide du principe glisser-déposer est aussi prise en charge.
La couleur des cases varie cycliquement conformément au schéma en couleurs figurant au-dessous du tableau : le transfert des événements est autorisé sans aucune limitation de trafic ou le transfert des événements est complètement interdit.
7. Dans l'onglet **Dump**, spécifiez les paramètres suivants :
 - Cochez la case **Créer des dumps de mémoire** pour créer des dumps de mémoire en cas d'erreurs critiques lors du fonctionnement du Serveur proxy Dr.Web.
 - Dans le champ **Nombre maximal de dumps**, spécifiez le nombre maximal de dumps de mémoire. Si le nombre spécifié est atteint, les plus anciens dumps seront supprimés lors de la création de nouveaux dumps. La configuration des dumps de mémoire est possible uniquement sous Windows.
8. Dans l'onglet **DNS**, vous pouvez configurer les paramètres d'appel au serveur DNS. Les paramètres sont équivalents aux [paramètres DNS pour le Serveur Dr.Web](#).
9. Dans l'onglet **Détection**, vous pouvez configurer les paramètres de stockage des réponses aux requêtes broadcast lors de la recherche des Serveurs Dr.Web pour la redirection de clients (voir l'étape 4c).
 - **Pour les réponses positives, s** : durée de stockage (en secondes) de la liste des Serveurs Dr.Web ayant répondu à la requête broadcast lors de la recherche des Serveurs Dr.Web. A l'issue de ce délai, la requête est envoyée encore une fois.
 - **Pour les réponses négatives, s** : durée de stockage (en secondes) des informations sur l'absence de Serveurs Dr.Web ayant répondu à la requête broadcast. A l'issue de ce délai, la requête est envoyée encore une fois.
10. Dans l'onglet **Mises à jour**, vous pouvez configurer les paramètres de la mise à jour automatique du logiciel du Serveur proxy Dr.Web depuis le Serveur Dr.Web :
 - Cochez la case **Activer la mise à jour automatique**, pour télécharger et installer automatiquement de nouvelles révisions du Serveur proxy Dr.Web depuis le Serveur Dr.Web. La planification de la mise à jour dépend des paramètres de la mise en cache proactive du Serveur proxy Dr.Web (voir l'étape 5) :



- a) Si le Serveur proxy Dr.Web 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 Dr.Web seront téléchargées et installées automatiquement conformément à la planification de la mise à jour automatique.
 - b) Si le Serveur proxy Dr.Web est inclus dans la liste de la mise en cache proactive, les mises à niveau du Serveur proxy Dr.Web seront automatiquement téléchargées conformément à la planification de la mise en cache proactive. Si une nouvelle révision du Serveur proxy Dr.Web est reçue, la mise à niveau vers cette révision sera effectuée conformément à la planification automatique.
- Dans la section **Planification de mises à jour**, spécifiez la planification selon laquelle la mise à jour automatique sera effectuée.
Pour modifier le mode de limitation de transmission de données, cliquez sur le bloc correspondant dans le tableau. La sélection de plusieurs blocs temporaires à l'aide du principe glisser-déposer est aussi prise en charge.
La couleur des cases varie cycliquement conformément au schéma en couleurs figurant au-dessous du tableau : le transfert de mises à jour est autorisé sans aucune limitation de trafic ou le transfert de mises à jour est complètement interdit.
11. Dans l'onglet **Journal**, vous pouvez changer le niveau de détail du journal du Serveur proxy Dr.Web. Les niveaux suivants sont disponibles :
 - **Erreur critique** : messages sur des erreurs critiques relatives au fonctionnement ;
 - **Erreur** : messages des erreurs de fonctionnement ;
 - **Avertissement** : avertissements sur les erreurs ;
 - **Notification** : messages d'information importants ;
 - **Informations** : messages d'information ;
 - **Trace (0–3)** : trace des actions réalisées de divers niveaux de détail (**Trace3** : niveau de détail maximum) ;
 - **Débogage (0–3)** : message de débogage de divers niveau de détail (**Débogage3** : niveau de détail maximum) ;
 - **Tous** : tous les messages (équivalent à la valeur **Débogage 3**).
 12. Après avoir apporté les modifications, cliquez sur **Enregistrer**.

12.2. NAP Validator

Généralités

Microsoft Network Access Protection (NAP) est une plateforme de politique intégrée dans les systèmes d'exploitation Windows afin de renforcer la sécurité du réseau. Le niveau de sécurité est assuré grâce à la capacité de répondre aux exigences opérationnelles relatives aux systèmes dans le réseau.



En cas d'utilisation de la technologie NAP, il est possible de créer des politiques utilisateur permettant d'évaluer le niveau de performance de l'ordinateur. Les évaluations obtenues sont prises en compte dans les cas suivants :

- avant d'autoriser l'accès ou l'interaction,
- pour réaliser une mise à jour automatique des ordinateurs se conformant aux exigences spécifiées afin d'assurer leur compatibilité de manière permanente,
- pour réaliser l'intégration des ordinateurs afin de respecter les exigences établies.

Pour en savoir plus sur la technologie NAP, consultez le [site de Microsoft Docs](#).

Utilisation de NAP dans Dr.Web Enterprise Security Suite

Dr.Web Enterprise Security Suite permet d'utiliser la technologie NAP pour vérifier la performance du logiciel antivirus sur les postes protégés. Cette fonction est assurée par le composant Dr.Web NAP Validator.

Les moyens utilisés lors de la vérification de la performance :

- Le Serveur NAP destiné à vérifier la performance (installé et configuré de façon appropriée).
- Dr.Web NAP Validator est un moyen d'évaluation de la performance du logiciel antivirus sur le système protégé (System Health Validator — SHV) via les politiques utilisateur ajoutables Dr.Web. Il doit être installé sur l'ordinateur avec le Serveur NAP.
- Agent d'intégrité système (System Health Agent — SHA). L'agent s'installe sur le poste de travail de manière automatique avec le logiciel de l'Agent Dr.Web.
- Le Serveur Dr.Web sert de serveur de correction assurant le fonctionnement de l'antivirus sur les postes.

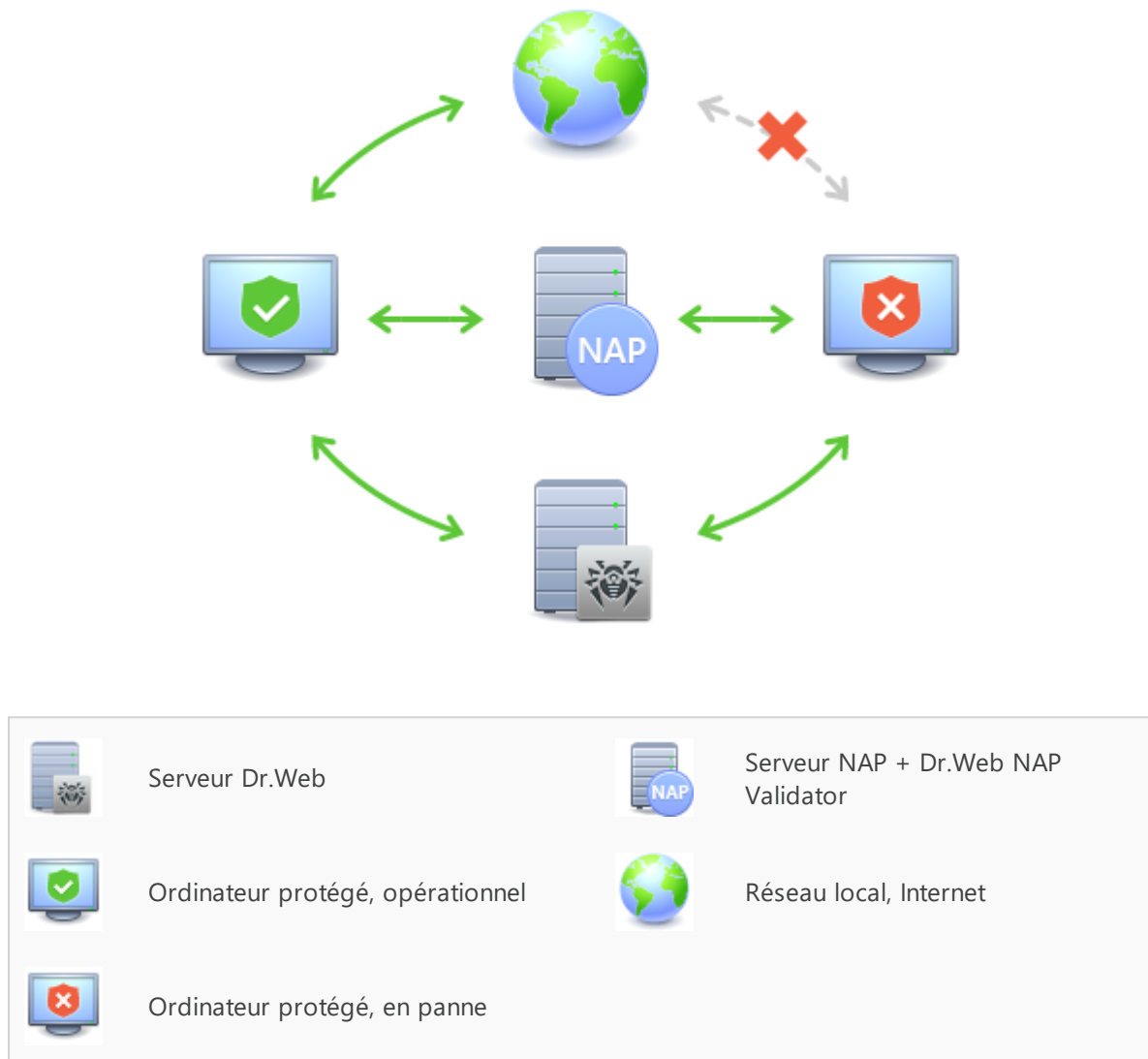


Figure 12-2. Schéma du réseau antivirus en cas d'utilisation de NAP

Marche à suivre pour effectuer la procédure de vérification :

1. Pour activer la vérification, il faut configurer les paramètres correspondants de l'Agent Dr.Web.
2. L'agent SHA se trouvant sur le poste de travail se connecte au composant Dr.Web NAP Validator installé sur le Serveur NAP.
3. Dr.Web NAP Validator effectue une vérification des politiques de performance (voir [ci-dessous](#)). La vérification des politiques est une procédure durant laquelle NAP Validator réalise une évaluation des outils antivirus en prenant en compte l'exécution des règles définies pour ces outils et donne l'état courant du système :
 - les postes en conformité avec les éléments de la politique de sécurité sont considérés comme opérationnels et approuvés pour le fonctionnement au sein du réseau.



- les postes non conformes au moins à un élément de la politique seront considérés comme non opérationnels. Ces postes ne peuvent que se connecter au Serveur Dr.Web, mais ils sont déconnectés de l'autre partie du réseau. La performance du poste peut être rétablie à l'aide du Serveur Dr.Web, puis le poste doit repasser une procédure de vérification.

Pré-requis pour le fonctionnement :

1. Statut de l'Agent Dr.Web (actif et opérationnel).
2. Le statut des bases virales qui doivent être à jour (les bases correspondent aux bases se trouvant sur le Serveur).

Configuration de NAP Validator

Après l'installation de Dr.Web NAP Validator (voir **Guide d'installation**, [Installation de NAP Validator](#)) sur la machine où tourne le serveur NAP, il est nécessaire de réaliser les opérations suivantes :

1. Ouvrez le composant de la configuration du serveur NAP (avec la commande `nps .msc`).
2. Dans la section **Policies**, sélectionnez l'élément **Health Policies**.
3. Dans la fenêtre qui sera affichée, ouvrez les propriétés des éléments suivants :
 - **NAP DHCP Compliant**. Dans la fenêtre de configuration, cochez la case **Dr.Web System Health Validator** qui détermine l'utilisation des politiques du composant Dr.Web NAP Validator. Dans la liste déroulante, sélectionnez l'élément **Client passed all SHV checks**. Conformément à cette option, le poste sera considéré comme opérationnel s'il correspond à tous les éléments de la politique adoptée.
 - **NAP DHCP Noncompliant**. Dans la fenêtre de configuration, cochez la case **Dr.Web System Health Validator** qui détermine l'utilisation des politiques du composant Dr.Web NAP Validator. Dans la liste déroulante, sélectionnez l'élément **Client fail one or more SHV checks**. Conformément à cette option, le poste sera considéré comme non opérationnel s'il n'est pas conforme à au moins un élément de la politique adoptée.



Référence

A

- Active Directory
 - authentification de l'administrateur 106
 - généralités 52
- administrateurs
 - authentification 100
 - droits 110
 - gestion 109
 - groupes 109
- Agent
 - fonctions 64
 - mise à jour 389
 - mode mobile 389
- approbation des postes 154
- authentification
 - Active Directory 106
 - automatique 89
 - externe 100
 - interne 101
 - LDAP 107
 - LDAP/AD 102
 - PAM 104
 - RADIUS 102
- authentification automatique 89

C

- Centre de gestion
 - barre d'outils 76
 - description 66
 - liste hiérarchique 73
 - menu principal 67
 - panneau des propriétés 82
- certificat 48
- chargeur du référentiel 381
- chiffrement
 - généralités 42
- clé privée 48
- clé publique 48
- clés
 - chiffrement 48
 - de licence 25
 - démo 26
- clés de démo 26
- clés de licence
 - distribution entre les Serveurs 27

- gestion 176, 228
- mise à jour automatique 30
- réception 25
- composant antivirus 179
- composants
 - antivirus 179
 - du réseau 96
- compression du trafic 42
- configuration
 - Serveur 249
 - serveur Web 292
- contrôle des applications 338
 - analyse fonctionnelle 146
 - applications de confiance 147, 342
 - mode d'autorisation 147
 - mode de blocage 152
 - mode de test 341
 - poste de référence 342
 - profils 142
 - règles d'autorisation 147
 - règles de blocage 152
 - répertoire d'applications 346
- copie de sauvegarde
 - Serveur, création 353
 - Serveur, restauration 375
- création
 - groupe 130

D

- démarrage
 - Serveur Dr.Web, UNIX 63
 - Serveur Dr.Web, Windows 60
- distribution 22
- droits, administrateurs 110

E

- enregistrement
 - postes sur le Serveur 154
 - produit Dr.Web 25

F

- fonctions
 - Agent 64
 - Serveur 55



Référence

G

- Gestionnaire de licences 228
- groupes 126
 - ajout des postes 133
 - configuration, héritage 122
 - paramètres, copie 138
 - primaires 122
 - suppression de postes 133
- groupes prédéfinis 126
- groupes primaires 122
- groupes système 126

I

- icônes
 - procédures utilisateur 303
 - réseau antivirus 74
- interface
 - Centre de gestion 66
 - Serveur, UNIX 61
 - Serveur, Windows 57

J

- journal du Serveur 243
- journal du Serveur en temps réel 239

L

- langue du Centre de gestion 86, 115
- liaisons, entre serveurs
 - configuration 361
 - types 359

M

- messages
 - envoi à l'utilisateur 214
 - journal 247
 - modèles 306
- mise à jour
 - Agent 389
 - Dr.Web Enterprise Security Suite 375
 - forcée 378
 - manuelle 378
 - mode mobile 389
 - référentiel 378
 - selon planification 379
- mise à jour forcée 378

- mise à jour manuelle du référentiel 378
- mode mobile de l'Agent 389

N

- NAP Validator 399
 - configuration 402
- notifications
 - configuration 307
 - console Web 314
- novice 154

O

- octroi de licence 25
 - particularités 26

P

- paramètres
 - postes, copie 138
 - Serveur 249
 - serveur Web 292
- Planificateur des tâches
 - postes 168
 - Serveur 279
- planification
 - des mises à jour 379
 - Du Serveur 279
 - postes 168
- politiques
 - approbations des postes 154
 - paramètres de postes 139
- poste 168
 - ajout vers le groupe 133
 - appartenance à un groupe 135
 - approbation 154
 - configuration, héritage 122
 - gestion 154
 - non approuvé 154
 - novice 154
 - paramètres, copie 138
 - planification 168
 - restauration 156
 - scan 168, 184
 - statistiques 194
 - suppression 156
 - suppression depuis le groupe 133
- postes non approuvés 154



Référence

pouvoirs, administrateurs 110
Protocole SRV 41

Q

quarantaine 207

R

récupération
 du mot de passe de l'administrateur 117
référentiel
 configuration détaillée 328
 configuration générale 324
 contenu 334
 mise à jour 378
 statut 322, 378
répertoire du Serveur, composition 61
répertoire du Serveur, composition, Windows 57
réseau antivirus 358
 composants 96
 configuration des liaisons 361
 création 34
 événements viraux 368
 structure 96, 359
restauration
 postes 156

S

scan
 automatique 168
 manuel 184
scan antivirus 184
scanner
 antivirus 184
 réseau 92
scanner antivirus
 démarrage 185
Serveur Dr.Web
 composition du répertoire, UNIX 61
 composition du répertoire, Windows 57
 configuration des liaisons 361
 démarrage, UNIX 63
 démarrage, Windows 60
 fonctions 55
 interface, UNIX 61
 interface, Windows 57
 journal 243

journal en temps réel 239
paramètres 249
planification 279
types de liaisons 359
Serveur proxy
 configuration à distance 394
 démarrage, arrêt 394
 fonctionnalité 390
serveur Web 292
 paramètres 292
service de détection du Serveur Dr.Web 40
SGM
 mise à jour manuelle 378
statistiques
 Du Serveur 352
 postes 194
suppression
 groupes 130
 poste, depuis le groupe 133
 postes 156

T

trafic
 chiffrement 42
 composition 98
 compression 42

V

VDI 223

