Dr.WEB

pour Linux

Manuel utilisateur

Dr.Web pour Linux
Version 11.1
Manuel utilisateur
01/11/2023

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

Introduction 7

Légende et abréviations 8

A propos de ce produit 9

- **Fonctionnalités principales** 9
- **Structure de Dr.Web pour Linux** 12
- **Placement de la quarantaine** 14
- **Permissions et privilèges des fichiers** 15
- **Modes de fonctionnement** 16

Pré-requis système et compatibilité 20

Octroi de la licence 25

Installation et suppression 26

- **Installation de Dr.Web pour Linux** 27
  - Installation du package universel 27
    - Installation en mode graphique 30
    - Installation en ligne de commande 31
  - Installation depuis le référentiel 32
- **Mise à jour de Dr.Web pour Linux** 36
  - Obtention des mises à jour 36
  - Mise à niveau vers une nouvelle version 38
- **Suppression de Dr.Web pour Linux** 42
  - Suppression du paquet universel 42
    - Suppression en mode graphique 43
    - Suppression en mode de ligne de commande 44
  - Suppression de Dr.Web pour Linux installé depuis le référentiel 45
- **Avancé** 49
  - Emplacement des fichiers de Dr.Web pour Linux 49
  - Installation et suppression personnalisées des composants 49
- **Configuration des sous-systèmes de sécurité** 53
  - Configuration des politiques de sécurité SELinux 54
  - Configuration des autorisations de PARSEC 57
  - Configuration du lancement en mode ELF (Astra Linux SE en versions 1.6 et 1.7) 61

Mise en marche 63

- **Enregistrement et activation** 63

Fichier clé 66
Fichier de configuration de la connexion 67
Tester les capacités de fonctionnement 67
Modes de surveillance des fichiers 68
Utilisation de Dr.Web pour Linux 71
Gestion via l'interface graphique 72
Intégration avec l'environnement graphique du bureau 77
Démarrer et arrêter l'interface graphique 80
Détection et neutralisation des menaces 81
Scan à la demande 81
Scan des objets selon la planification 85
Gérer les tâches de scan 86
Surveillance du système de fichiers 88
Surveillance des connexions réseau 91
Voir les menaces détectées 93
Gérer la quarantaine 96
Mise à jour de la protection antivirus 99
Gestionnaire de licences 100
Consultation de messages du serveur de protection centralisée 110
Gestion des privilèges du logiciel 113
Aide et références 115
Configurer les paramètres de fonctionnement 115
Paramètres principaux 116
Paramètres du scan de fichiers 119
Paramètres du contrôle du système de fichiers 121
Configuration de la surveillance des connexions réseau 122
Exclusions 126
Exclusion des fichiers et des répertoires 127
Exclusion des connexions réseau des applications 128
Listes noire et blanche de sites web 129
Configuration du scan selon la planification 130
Configuration de la protection contre les menaces transmises via le réseau 131
Paramètres du mode 134
Configuration de l'utilisation de Dr.Web Cloud 137
Avancé 138
Arguments de la ligne de commande 138
Lancement de la copie autonome 139

Gestion via la ligne de commande **140**
Format d'appel 142
Exemples d'utilisation 166

Annexes **171**
Annexe A. Types de menaces informatiques **171**
Annexe B. Neutralisation des menaces **176**
Annexe C. Support technique **178**
Annexe D. Erreurs connues **180**
Annexe E. Créer un module noyau pour SplDer Guard **226**
Application F. Liste d'abréviations **228**

Référence **230**

Introduction

Merci d'avoir acheté Dr.Web pour Linux. Il fournit une protection fiable de votre ordinateur contre différents types de menaces informatiques en utilisant les technologies les plus avancées de détection et de neutralisation des virus.

Ce manuel est destiné à aider les utilisateurs dont les ordinateurs tournent sous les OS de la famille GNU/Linux (ci-après dénommé UNIX) à installer et utiliser Dr.Web pour Linux en version 11.1.

Si Dr.Web pour Linux en version antérieure est déjà installé sur votre ordinateur et que vous souhaitez mettre à niveau Dr.Web pour Linux vers la version 11.1, effectuez la mise à niveau vers la nouvelle version (voir la rubrique Mise à niveau vers une nouvelle version).

Légende et abréviations

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.
Réseau antivirus	Un nouveau terme ou l'accent mis sur un terme dans les descriptions.
<IP-address>	Champs destinés à remplacer les noms fonctionnels par leurs valeurs.
Enregistrer	Noms des boutons de l'écran, des fenêtres, des éléments de menu et d'autres éléments de l'interface du logiciel.
CTRL	Touches du clavier.
`/home/user`	Noms de fichiers/dossiers ou fragments de programme.
Annexe A	Liens vers les autres chapitres du manuel ou liens vers des ressources externes.

Dans le Manuel, les commandes à saisir par le clavier dans la ligne de commande du système d'exploitation (dans le terminal ou l'émulateur de terminal) sont introduites par le caractère `$` ou `#` qui détermine les privilèges requis pour l'exécution de cette commande. Pour les systèmes UNIX :

`$` : l'exécution de la commande requiert les privilèges ordinaires de l'utilisateur.

`#` : l'exécution de la commande requiert les privilèges de super-utilisateur (d'habitude - *root*). Pour élever les privilèges, on peut utiliser la commande `su` ou la commande `sudo`.

Vous pouvez consulter les abréviations dans la rubrique Application F. Liste d'abréviations.

A propos de ce produit

Cette section contient les informations suivantes dur le produit :

- Désignation.
- Fonctionnalités principales.
- Structure de Dr.Web pour Linux.
- Placement de la quarantaine.
- Permissions et privilèges des fichiers.
- Modes de fonctionnement.

Désignation

Dr.Web pour Linux est créé pour protéger les ordinateurs tournant sous les OS de la famille GNU/Linux contre les virus et d'autres types de logiciels malveillants conçus pour les différentes plateformes.

Les principaux composants du logiciel (le moteur antivirus et les bases virales) ne sont pas uniquement très efficaces et économes en ressources, mais également multiplateforme, ce qui permet aux experts de Doctor Web de créer des solutions antivirus fiables assurant la protection des ordinateurs et des appareils mobiles tournant sous les OS les plus répandus contre les menaces destinés aux différentes plateformes. En ce moment, outre Dr.Web pour Linux, la société Doctor Web a élaboré des solutions antivirus fiables pour les OS de la famille UNIX (comme, par exemple, FreeBSD), IBM OS/2, Novell NetWare, macOS et Windows. De plus, on a créé des solutions antivirus assurant la sécurité des appareils mobiles tournant sous les OS Andorid, Symbian, BlackBerry.

Les composants de Dr.Web pour Linux sont constamment mis à jour et les bases virales Dr.Web s'enrichissent régulièrement de nouvelles signatures pour garantir un niveau actuel de la protection de l'ordinateur, des logiciels et des données de l'utilisateur. De plus, pour fournir une protection supplémentaire contre les virus inconnus on utilise des méthodes d'analyse heuristique réalisées dans le moteur antivirus et la connexion au service Dr.Web Cloud collectant l'information la plus actuelle sur les menaces, empêchant les utilisateurs d'accéder à des sites web indésirables et protégeant les OS contre les fichiers infectés.

Fonctionnalités principales

Fonctionnalités principales de Dr.Web pour Linux :

1. **Détection et neutralisation de menaces**. Détection et neutralisation de tout type de programmes malveillants (par exemple, les virus, y compris ceux qui infectent les boîtes de réception et les enregistrements d'amorçage, les Trojans, les vers de mail, etc.) et des logiciels non sollicités (par exemple, les adwares, les canulars, les dialers, etc.). Pour en savoir plus sur les types de menaces, voir Annexe A. Types de menaces informatiques.

Dr.Web pour Linux utilise plusieurs méthodes de détection des logiciels malveillants simultanément :

- *Analyse par signature*. Méthode qui permet la détection des menaces connues, les informations sur ces menaces sont contenues dans des bases virales.
- *Analyse heuristique*. Ensemble de méthodes qui permettent la détection des menaces qui ne sont pas encore connues.
- *Technologie cloud de détection de menaces*. Une connexion au service Dr.Web Cloud est effectuée qui collecte les informations les plus actuelles sur les menaces, envoyées par les produits antivirus différents de Dr.Web.

Notez que l'analyseur heuristique peut signaler les faux positif. Comme un objet peut être considéré à tort comme malveillant, toutes les menaces détectées par l'analyseur heuristique sont traitées comme suspectes. Ainsi, il est recommandé de placer ces fichiers en quarantaine et de les envoyer pour analyse au laboratoire antivirus de Doctor Web. Pour en savoir plus sur les méthodes de neutralisation des menaces, voir Annexe B. Neutralisation des menaces.

Les objets système sont scannés sur demande de l'utilisateur ou automatiquement, selon la planification. L'utilisateur peut lancer un scan de tous les objets du système de fichiers (les fichiers et les enregistrements d'amorçage) accessibles ou bien sélectionner le scan personnalisé pour que seuls les fichiers, répertoires et enregistrements d'amorçage spécifiés soient scannés. Il est également possible de lancer uniquement un scan des fichiers exécutables binaires contenant le code des processus en cours d'exécution. Si une menace est détectée dans ce cas de figure, l'objet malveillant est neutralisé et le processus actif est stoppé.

Pour les systèmes à l'environnement de bureau graphique, il existe la possibilité d'intégrer les fonctions de scan de fichiers à l'aide de la barre de tâches ou bien à l'aide de gestionnaire de fichiers graphique. Dans les systèmes utilisant les modèles de contrôle d'accès obligatoire avec de différents niveaux d'accès, les fichiers inaccessibles sur le niveau d'accès actuel peuvent être analysées en mode de copie autonome.

Tous les objets contenant des menaces détectés dans le système de fichiers sont enregistrés dans le registre de menaces stocké en permanence sauf les menaces qui sont détectées en mode de copie autonome.

L'utilitaire de gestion à partir de la ligne de commande inclus dans Dr.Web pour Linux permet d'analyser les systèmes de fichiers des hôtes distants du réseau qui fournissent un accès distant via SSH ou Telnet.

Vous pouvez utiliser le scan à distance uniquement pour détecter les fichiers suspects ou malveillants sur l'hôte distant. Pour neutraliser les menaces détectées sur le nœud distant, utilisez les outils de gestion fournis par ce nœud. Par exemple, pour les routeurs et d'autres dispositifs intelligents, vous pouvez mettre à jour le firmware, pour l'ordinateur — on peut s'y connecter (y compris en mode terminal distant) et effectuer les opérations nécessaire dans le système de fichiers (supprimer ou déplacer les fichiers, etc.) ou lancer un logiciel antivirus installé sur cet ordinateur.

2. **Surveillance des requîtes aux fichiers**. Surveillance de l'accès aux fichiers contenant des données et tentatives de lancement des fichiers exécutables. Cette fonction permet de détecter et de neutraliser des programmes malveillants juste au moment d'une tentative d'infecter l'ordinateur. En dehors du mode de surveillance standard, il existe la possibilité d'activer le mode renforcé (« paranoïde ») dans lequel l'accès aux fichiers sera bloqué par le moniteur jusqu'à la fin de leur analyse (cela permet de prévenir les cas d'accès au fichier contenant une menace, quand le résultat de l'analyse est connu après l'accès de l'application au fichier). Le mode de surveillance renforcé augmente le niveau de sécurité mais ralentit l'accès des applications aux fichiers non analysés.
3. **Surveillance des connexions réseau**. Surveillance des tentatives d'accéder aux serveurs sur Internet (serveurs Web, serveurs de fichiers) via les protocoles HTTP et FTP pour le blocage d'accès d'utilisateurs aux sites Web et aux hôtes dont les adresses sont marquées comme indésirables et la prévention de téléchargement de fichiers malveillants.
4. **Analyse des messages e-mail** pour prévenir la réception et l'envoi des messages e-mail contenant des fichiers infectés, des liens indésirables, ainsi que des messages classés comme spam.

   L'analyse des messages e-mail et des fichiers téléchargés sur le réseau se fait « à la volée ». En fonction de la fourniture, Dr.Web pour Linux peut ne pas contenir Dr.Web Anti-Spam. Dans ce cas, l'analyse antispam de messages e-mail n'est pas effectuée.

   Pour déterminer les liens indésirables, on utilise la base de données de catégories de ressources Web fournie avec Dr.Web pour Linux et mise à jour automatiquement, ainsi que les listes blanche et noire créées par l'utilisateur. De plus, Dr.Web pour Linux peut s'adresser au service Dr.Web Cloud pour vérifier si le site que l'utilisateur veut visiter ou le lien dans un message est marqué comme malveillant par d'autres produits Dr.Web.

   

   Si certains messages ne sont pas correctement reconnus par le composant Dr.Web Anti-Spam, il est recommandé de les envoyer aux adresses e-mail spéciales pour l'analyse et l'amélioration de fonctionnement du filtre antispam. Pour cela, enregistrez chaque message dans un fichier de type `.eml`. Veuillez joindre les fichiers sauvegardes à un message e-mail, et envoyez ce message à l'adresse service correspondante.

   - nonspam@drweb.com : si le message contient les fichiers *classés par erreur comme spam* ;
   - spam@drweb.com : si le message contient les fichiers *non classés par erreur comme spam*.

5. **Isolation fiable des objets infectés ou suspects**. Ces objets sont déplacés dans un dossier de stockage spécial, la quarantaine, pour prévenir tout endommagement du système. Lors du déplacement en quarantaine, les objets sont renommés selon des règles spécifiques et, si nécessaire, ils peuvent être restaurés dans leur emplacement d'origine sur simple requête de l'utilisateur.
6. **Mise à jour automatique** des bases virales de Dr.Web et du moteur antivirus pour permettre à Dr.Web pour Linux d'utiliser les données les plus récentes à propos des logiciels malveillants connus.
7. **Collecte des statistiques** sur les analyses et les événements viraux ; journalisation des menaces détectées (le journal est disponible uniquement depuis l'utilitaire de gestion dans

la ligne de commande) ; envoi des statistiques sur les événements de viraux dans le service cloud Dr.Web Cloud.

8. **Fonctionnement en mode Protection centralisée** (s'il y a une connexion au serveur de protection centralisée, comme avec Dr.Web Enterprise Server ou dans le service Dr.Web AV-Desk). Ce mode permet d'implémenter une politique de sécurité unifiée sur les ordinateurs du réseau protégé. Cela peut être un réseau d'entreprise, un réseau privé (VPN), ou le réseau d'un fournisseur de services (par exemple, accès à Internet).

Vu que l'utilisation de l'information stockée sur le service Dr.Web Cloud, requiert la transmission de données concernant l'activité de l'utilisateur (notamment – la transmission des adresses de sites web à vérifier), la connexion à Dr.Web Cloud est effectuée seulement après l'autorisation de l'utilisateur. Si cela est nécessaire, vous pouvez interdire l'utilisation de Dr.Web Cloud à tout moment.

Structure de Dr.Web pour Linux

Dr.Web pour Linux contient les composants suivants :

Composant	Description
Scanner	Composant effectuant le scan des objets du système de fichiers (fichiers, répertoires, enregistrements d'amorçage) à la demande ou selon la planification. L'utilisateur peut lancer un scan depuis le mode graphique et la ligne de commande.
SpIDer Guard	Le composant fonctionne en mode résident et surveille les opérations avec des fichiers (telles que création, ouverture, fermeture et lancement d'un fichier). Il envoie au Scanner les requêtes d'analyse du contenu de nouveaux fichiers ou de fichiers modifiés, ainsi que de fichiers exécutables au moment du lancement de logiciels. Il fonctionne avec le système de fichiers de l'OS via le mécanisme système fanotify ou via le module spécifique de noyau (*LKM — Linux Kernel Module*) créé par Doctor Web. En cas de fonctionnement via le mécanisme système fanotify, le moniteur peut fonctionner en mode renforcé et bloquer l'accès aux fichiers (de tous les types ou aux fichiers exécutables uniquement) qui ne sont pas encore analysés, jusqu'à la fin de leur analyse. Le mode de surveillance renforcé est désactivé par défaut.
SpIDer Gate	Composant fonctionnant en mode résidant et surveillant toutes les connexions réseau. • Il vérifie si les URL demandées se trouvent dans les bases des catégories de ressources web et dans les listes noires de l'utilisateur, il bloque l'accès aux sites, si les URL qui y mènent sont enregistrés dans la liste noire de l'utilisateur ou dans les catégories marquées comme indésirables. • Bloque l'envoie et la réception d'e-mails s'ils contiennent des objets malveillants ou des liens indésirables. • Il envoie les requêtes au Scanner pour scanner les fichiers téléchargés sur Internet (depuis les serveurs autorisés) et bloque leur téléchargement s'ils contiennent des menaces.

Composant	Description
	En plus, si l'utilisateur l'autorise, il envoie les URL requises pour les vérifier au service Dr.Web Cloud.
Moteur antivirus	Composant central de la protection antivirus utilisé par le Scanner pour la recherche et la détection des menaces, ainsi que pour l'analyse du comportement des objets suspects.
Dr.Web Anti-Spam	Composant de l'analyse de messages e-mail pour la présence de spam. Le composant n'est pas présent dans les versions pour les architectures ARM64 et E2K.
Bases de données virales	Bases de données mises à jour automatiquement utilisées par le moteur antivirus et contenant des informations pour la détection et la neutralisation des menaces connues.
Bases des catégories des ressources web	Base de données mise à jour automatiquement contenant la liste des ressources web classées par catégories et utilisée par SpIDer Gate afin de bloquer l'accès aux sites non sollicités.
Module de mise à jour	Composant responsable du téléchargement automatique des mises à jour des bases virales, du moteur antivirus et des bases des catégories de ressources web depuis les serveurs de mise à jour de Doctor Web (automatiquement selon la planification ou sur demande de l'utilisateur).
Interface graphique de gestion	Composant représentant l'interface graphique de gestion de Dr.Web pour Linux à fenêtre. Il permet à l'utilisateur de lancer le scan des objets du système de fichiers en mode graphique, de gérer les moniteurs SpIDer Guard et SpIDer Gate, de consulter le contenu de la quarantaine, de lancer l'obtention des mises à jour et de configurer Dr.Web pour Linux.
Agent de notifications	Composant fonctionnant en tâche de fond. Il affiche les pop-ups informant des événements et l'indicateur de l'application Dr.Web pour Linux dans la zone de notifications, lance les scans selon la planification. Par défaut, le composant est lancé au début de la session de l'utilisateur dans l'environnement de bureau.
Gestionnaire de licences	Il aide les utilisateurs à gérer leurs licences et effectue les actions suivantes : activer une licence et une période de démo, fournir de l'information sur la licence en cours, renouveler la licence, ainsi qu'installer ou supprimer un fichier clé de licence.

A part les composants décrits dans le tableau, Dr.Web pour Linux inclut des composants de service qui opèrent en tâche de fond et ne requièrent pas l'intervention de l'utilisateur.

SpIDer Guard, le moniteur du système de fichiers, peut opérer dans un des modes suivants :

- *FANOTIFY* : en utilisant l'interface de gestion fanotify (pas tous les OS basés sur GNU/Linux supportent fanotify).
- *LKM* : fonctionnement avec l'utilisation du module noyau chargeable UNIX créé par l'entreprise Doctor Web (compatible avec n'importe quel OS de la famille GNU/Linux ayant le noyau 2.6.x et supérieur). L'utilisation de LKM n'est pas prise en charge par les architectures ARM64 et E2K.

Par défaut, le moniteur du système de fichiers choisit automatiquement le mode opératoire approprié selon l'environnement. Si SpIDer Guard ne peut pas démarrer, créez et installez un module noyau chargeable en utilisant les codes source fournis.

Placement de la quarantaine

La quarantaine de Dr.Web pour Linux est un système de répertoires qui servent à isoler les fichiers contenant des menaces qui ne peuvent pas être désinfectées en ce moment. Par exemple, une menace détectée peut être incurable car elle est encore inconnue à Dr.Web pour Linux (par exemple, elle a été détectée par l'analyseur heuristique mais sa signature et la méthode de traitement ne sont pas présentes dans les bases virales) ou bien, elle provoque une erreur durant la désinfection. De plus, un fichier peut être placé en quarantaine sur demande de l'utilisateur s'il a sélectionné cette action dans la liste des menaces détectées ou qu'il a spécifié cette action comme réaction du Scanner ou du moniteur de système de fichiers SpIDer Guard face à une menace d'un type particulier.

Lorsqu'un fichier est placé en quarantaine, il est renommé selon des règles spécifiques. Le renommage des fichiers isolés empêche les utilisateurs et les applications d'accéder à ces fichiers s'ils outrepassent les outils de gestion de la quarantaine implémentés dans Dr.Web pour Linux. En outre, quand un fichier est placé en quarantaine, le bit d'exécution est réinitialisé à empêcher une tentative d'exécution de ce fichier.

Les répertoires de la quarantaine sont situés dans :

- *le répertoire racine Utilisateur* (si plusieurs comptes utilisateurs existent sur l'ordinateur, un répertoire de quarantaine séparé peut être créé pour chaque utilisateur).
- *le répertoire racine de chaque volume logique* monté dans le système de fichiers de l'OS.

Les répertoires de quarantaine de Dr.Web pour Linux portent toujours le nom `.com.drweb.quarantine` et ne sont pas créés qu'au moment d'application de l'action *« Déplacer en quarantaine » (Quarantaine)* à une menace, c'est-à-dire, les répertoires de la quarantaine ne sont pas créés jusqu'à ce qu'une menace ne soit détectée. Ainsi, seul un répertoire requis pour l'isolation d'un objet concret est créé. Lors de la sélection d'un répertoire, le nom du propriétaire du fichier est utilisé. Si lors du mouvement vers la racine du système de fichiers `/` depuis le répertoire contenant le répertoire personnel, le répertoire racine du propriétaire est atteint, le dossier de stockage de quarantaine créé est utilisé. Sinon, le fichier est isolé dans la quarantaine créée dans le répertoire racine du volume (qui n'est pas toujours

le même que le répertoire racine du système de fichiers). Ainsi, n'importe quel fichier infecté déplacé en quarantaine réside toujours sur le volume où il a été détecté. Cela assure un fonctionnement correct de la quarantaine au cas où plusieurs supports de stockage amovibles et d'autres volumes sont créés dans les différents emplacements du système.

Les utilisateurs peuvent gérer les objets en quarantaine soit en mode graphique soit avec la ligne de commande. Chaque action est appliquée à la quarantaine consolidée qui réunit tous les répertoires de la quarantaine disponibles en ce moment. Du point de vue de l'utilisateur, le répertoire de quarantaine situé dans le répertoire source de l'utilisateur est considéré comme la Quarantaine *utilisateur* et les autres répertoires sont considérés comme la Quarantaine *système*.

> Travailler avec des objets de quarantaine est autorisé uniquement si aucune licence active n'est trouvée. Cependant, les objets isolés ne peuvent pas être traités dans ce cas.

Permissions et privilèges des fichiers

Pour scanner les objets du système de fichiers et neutraliser les menaces, Dr.Web pour Linux (ou plutôt l'utilisateur sous lequel Dr.Web pour Linux fonctionne) requiert les permissions suivantes :

Action	Permissions requises
Afficher la liste de toutes les menaces détectées	Illimité. Aucune permission spécifique n'est requise.
Afficher le contenu du conteneur (archive, fichier de messagerie, etc.) (uniquement les éléments malveillants ou corrompus)	Illimité. Aucune permission spécifique n'est requise.
Déplacer en quarantaine	Illimité. L'utilisateur peut placer en quarantaine tous les fichiers infectés quelles que soient les permissions de lecture ou d'écriture les concernant.
Supprimer une menace	L'utilisateur doit avoir la permission d'écrire sur le fichier supprimé. Si la menace est détecté dans un fichier se trouvant dans un conteneur (archive, message, etc.), le conteneur n'est pas supprimé mais il est mise en quarantaine.
Réparer	Illimité. Les permissions et la propriété d'un fichier réparé demeurent les mêmes.

Action	Permissions requises
	Le fichier peut être supprimé du système si la suppression est le moyen le plus efficace de traitement de la menace détectée.
Restaurer un fichier de la quarantaine	L'utilisateur doit avoir les permissions de lecture du fichier et d'écriture dans le répertoire restauré.
Supprimer un fichier de la quarantaine	L'utilisateur doit avoir les permissions sur le fichier qui a été déplacé en quarantaine.

Pour élever temporairement les privilèges de Dr.Web pour Linux en mode graphique, cliquez sur le bouton correspondant dans la fenêtre de Dr.Web pour Linux (le bouton est disponible dans le cas où l'augmentation des privilèges est requise pour l'exécution réussie de certaines opérations). Pour activer le fonctionnement de Dr.Web pour Linux en mode graphique ou l'utilitaire de gestion de la ligne de commande avec les privilèges de super-utilisateur, vous pouvez utiliser la commande `su` qui permet de changer d'utilisateur, ou la commande `sudo` qui permet d'exécuter une commande au nom d'un autre utilisateur.

Le Scanner ne peut pas vérifier les fichiers dont la taille dépasse 4 Go (en cas de tentative de scanner de tels fichiers, un message d'erreur s'affiche : « *Fichier trop volumineux* »).

Modes de fonctionnement

Dr.Web pour Linux peut fonctionner en mode autonome ou bien comme partie d'un *réseau antivirus* d'entreprise ou privé géré par un *serveur de protection centralisée*. Ce mode s'appelle le *mode de protection centralisée* Le fonctionnement en mode Protection centralisée ne requiert pas l'installation d'un logiciel supplémentaire ou bien la réinstallation ou la suppression de Dr.Web pour Linux.

- *En mode standalone (standalone mode)*, l'ordinateur protégé n'est pas inclus dans le réseau antivirus et il est géré d'une manière locale. Dans ce mode, le fichier clé de configuration et celui de licence se trouvent sur les disques locaux et Dr.Web pour Linux est entièrement géré depuis l'ordinateur protégé. Les mises à jour des bases sont obtenues depuis des serveurs de mises à jour de Doctor Web.
- *En mode de protection centralisée (centralized protection mode)*, la protection de l'ordinateur est gérée par le serveur de protection centralisée. Dans ce mode, certaines fonctionnalités et paramètres de Dr.Web pour Linux peuvent être configurés en accord avec la politique générale (d'entreprise) de protection antivirus mise en œuvre dans le réseau antivirus. Le fichier clé de licence utilisé pour le mode Protection centralisée est reçu du serveur de protection centralisée auquel Dr.Web pour Linux est connecté. Le fichier clé de licence ou celui de démo conservé sur un ordinateur local, s'il en existe un, n'est pas utilisé. Les statistiques de Dr.Web pour Linux, y compris les statistiques sur les événements viraux sont

envoyées au serveur de protection centralisée. Les mises à jour des bases virales sont également reçues du serveur de protection centralisée.

- *En mode mobile (mobile mode),* Dr.Web pour Linux obtient les mises à jour depuis les serveurs de Doctor Web. Pourtant Dr.Web pour Linux utilise les paramètres sauvegardés localement et le fichier clé de licence spécial obtenu du serveur de protection centralisée.

Lorsque Dr.Web pour Linux fonctionne en mode Protection centralisée ou Mobile, les options suivantes sont bloquées :

1. Suppression d'un fichier clé de licence dans le Gestionnaire de licences.
2. Démarrage manuel d'un processus de mise à jour et configuration des paramètres de mise à jour.
3. Configuration des paramètres de scan du système de fichiers.

La configuration des paramètres de SpIDer Guard et l'option permettant de l'activer ou désactiver lors du fonctionnement de Dr.Web pour Linux opérant sous gestion du serveur de protection centralisée sont autorisées en fonction des permissions spécifiées sur le serveur.

L'analyse des fichiers selon la planification spécifiée n'est pas autorisée en mode de protection centralisée.

Si le lancement du scan sur demande de l'utilisateur n'est pas autorisé sur le serveur de protection centralisée, la page de lancement du scan et le bouton **Scanner** de la fenêtre de Dr.Web pour Linux seront désactivés.

Principes de la protection centralisée

Les solutions de Doctor Web pour l'organisation de la protection centralisée utilisent un modèle client-serveur (voir l'image ci-dessous).

Les postes de travail et les serveurs sont protégés par des *composants antivirus locaux* (dans ce cas, Dr.Web pour Linux) qui fournissent une protection antivirus des ordinateurs distants et permettent la connexion entre les postes de travail et le serveur de protection centralisée.

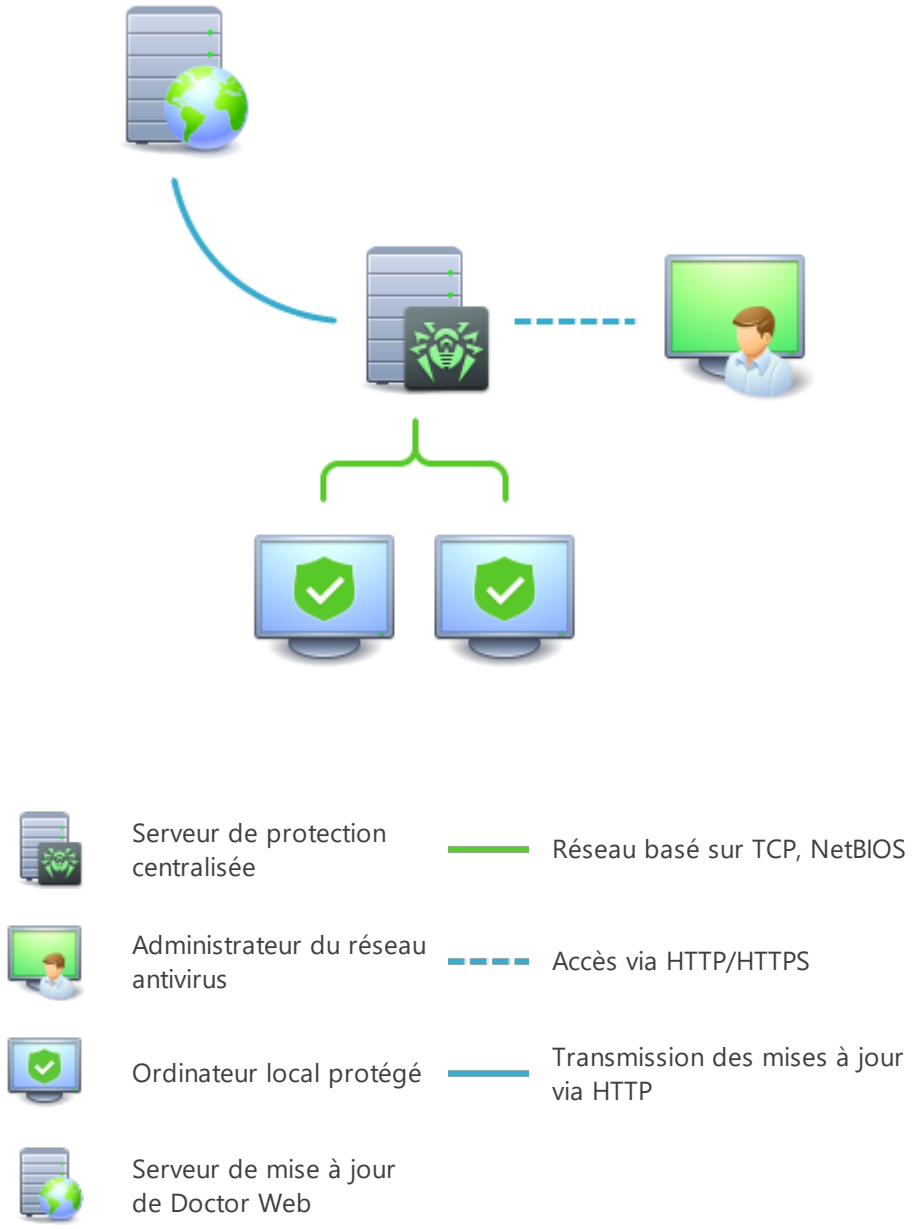

Image 1. Structure logique du réseau antivirus.

Les ordinateurs locaux sont mis à jour et configurés depuis le *serveur de protection centralisée*. Le flux d'instructions, données et statistiques dans le réseau antivirus passe également par le serveur de protection centralisée. Le volume de trafic entre les ordinateurs protégés et le serveur central peut être assez important, c'est pourquoi nos solutions fournissent des options de compression de trafic. Pour prévenir la fuite de données sensible ou la substitution de logiciels téléchargés sur des ordinateurs protégés, le chiffrement est également supporté.

Toutes les mises à jour nécessaires sont téléchargées sur le serveur de protection centralisée depuis les serveurs de mise à jour de Doctor Web.

Les composants antivirus locaux sont configurés et gérés depuis le serveur de protection centralisée d'après les commandes des administrateurs du réseau antivirus. Les administrateurs gèrent les serveurs de protection centralisée et la topologie du réseau antivirus (par exemple, valider les connexions des ordinateurs distants au serveur de protection centralisée) et configurent les composants antivirus locaux si nécessaire.

Les composants antivirus locaux ne sont pas compatibles avec les produits antivirus d'autres éditeurs ou des produits Dr.Web si cette dernière ne supporte pas un fonctionnement en mode Protection centralisée (par exemple, la version 5.0 de Dr.Web pour Linux). L'installation de deux produits antivirus sur le même ordinateur peut provoquer le crash du système et une importante perte de données.

En mode de protection centralisée, on peut exporter et sauvegarder les rapports sur le fonctionnement de Dr.Web pour Linux à l'aide du serveur de protection centralisée. L'exportation et la sauvegarde des rapports au formats HTML, CVS, PDF et XML sont supportées.

Connexion au réseau antivirus

Dr.Web pour Linux peut être connecté à un réseau antivirus d'une des façons suivantes :

- Dans l'onglet **Mode** surpage des paramètres de la fenêtre de Dr.Web pour Linux.
- Utiliser la commande `esconnect` de l'utilitaire de gestion de la ligne de commande – `drweb-ctl`.

Se déconnecter du réseau antivirus

Dr.Web pour Linux peut être déconnecté du réseau antivirus d'une des façons suivantes :

- Dans l'onglet **Mode** surpage des paramètres de la fenêtre de Dr.Web pour Linux.
- Avec la commande `esdisconnect` de l'utilitaire de gestion de la ligne de commande `drweb-ctl`.

Pré-requis système et compatibilité

Dans cette section :

- Pré-requis système.
- Liste des distributions supportées par l'OS.
- Composants et paquets supplémentaires requis.
- Compatibilité avec les composants de systèmes d'exploitation.
- Compatibilité avec les sous-systèmes de sécurité.

Pré-requis système

Vous pouvez utiliser Dr.Web pour Linux sur un ordinateur répondant aux pré-requis suivants :

Composant	Pré-requis
Plateforme	Les processeurs avec les architectures et les systèmes de commandes suivants sont pris en charge : • Intel/AMD : 32 bits (*IA-32, x86*) ; 64 bits (*x86-64, x64, amd64*) • ARM64 • E2K (*Elbrus*) • IBM POWER (*ppc64el*)
Mémoire vive (RAM)	500 Mo au minimum (il est recommandé d'avoir 1 Go et plus).
Espace disque	Au moins 2 Go d'espace disque libre sur le volume qui contient les répertoires de Dr.Web pour Linux.
Système d'exploitation	UNIX basé sur le noyau 2.6.37 ou une version supérieure, utilisant PAM et la bibliothèque `glibc` en version 2.13 ou une version supérieure. La liste des distributions UNIX prises en charge se trouve ci-dessous.
Autre	Les connexions réseau suivantes sont requises : • Connexion Internet pour télécharger les mises à jour et pour se connecter à Dr.Web Cloud (à condition que l'utilisateur l'ait autorisé). • En mode de protection centralisée, il suffit d'avoir une connexion au serveur via un réseau local ; une connexion Internet n'est pas requise.

Pour le fonctionnement correct du composant SplDer Gate, le noyau de système d'exploitation doit être compilé avec les options suivantes :

- *CONFIG_NETLINK_DIAG, CONFIG_INET_TCP_DIAG;*
- *CONFIG_NF_CONNTRACK_IPV4, CONFIG_NF_CONNTRACK_IPV6, CONFIG_NF_CONNTRACK_EVENTS;*
- *CONFIG_NETFILTER_NETLINK_QUEUE, CONFIG_NETFILTER_NETLINK_QUEUE_CT, CONFIG_NETFILTER_XT_MARK.*

L'ensemble des options nécessaires de la liste indiquée peut dépendre de la distribution utilisée de l'OS GNU/Linux.

Pour un fonctionnement correct de Dr.Web pour Linux, les ports suivants doivent être ouverts :

Usage	Direction	Numéros de ports
Pour obtenir des mises à jour	sortant	80
Pour la connexion au service cloud Dr.Web Cloud	sortant	2075 (y compris pour UDP), 3010 (TCP), 3020 (TCP), 3030 (TCP), 3040 (TCP)

Dr.Web pour Linux n'est pas compatible avec d'autres logiciels antivirus. L'installation de plusieurs logiciels antivirus sur le même ordinateur peut entraîner un crash système et une perte de données. Si vous avez déjà un autre antivirus installé sur votre ordinateur, supprimez-le avant d'installer Dr.Web pour Linux.

Liste des distributions prises en charge

Les distributions suivantes de UNIX sont prises en charge :

Plateforme	Versions GNU/Linux prises en charge
x86_64	• Astra Linux Special Edition 1.5 (avec le correctif cumulatif 20201201SE15), 1.6 (avec le correctif cumulatif 20200722SE16), 1.7 ; • Astra Linux Common Edition (Orel) 2.12 ; • Debian 9, 10 ; • Fedora 31, 32 ; • CentOS 7, 8 ; • Ubuntu 18.04, 20.04, 22.04 ; • Alt Poste de travail 9, 10 ; • Alt Serveur 9, 10 ;

Plateforme	Versions GNU/Linux prises en charge
	• Alt 8 SP ; • RED OS 7.2 MUROM, RED OS 7.3 MUROM ; • Goslinux IC6 ; • SUSE Linux Enterprise Server 12 SP3 ; • Red Hat Enterprise Linux 7, 8
x86	• CentOS 7 ; • Debian 10 ; • Alt Poste de travail 9, 10 ; • Alt 8 SP
ARM64	• Ubuntu 18.04 ; • CentOS 7, 8 ; • Alt Poste de travail 9, 10 ; • Alt Serveur 9, 10 ; • Alt 8 SP ; • Astra Linux Special Edition (Novorossiysk) 4.7
E2K	• Astra Linux Special Edition (Leningrad) 8.1 (avec le correctif cumulatif 20200429SE81) ; • Alt 8 SP ; • Elbrus-D MCST 1.4 ; • GS CS Elbrus 8.32 TVGI.00311-28
ppc64el	• CentOS 8 ; • Ubuntu 20.04 ;

Sous les OS Alt SP et Goslinux 7.1, le contrôle d'accès obligatoire n'est pas supporté.

Une compatibilité complète de Dr.Web pour Linux avec d'autres distributions de UNIX qui répondent aux pré-requis n'est pas garantie. En cas de problème de compatibilité avec votre distribution, contactez le support technique.

Composants et paquets supplémentaires requis

- Pour le fonctionnement de Dr.Web pour Linux en mode graphique et le démarrage du logiciel pour l'installation et la suppression en mode graphique, le sous-système X Window System et un gestionnaire de fenêtre sont requis. De plus, pour l'affichage correct de l'indicateur dans l'environnement graphique Ubuntu Unity, une bibliothèque supplémentaire (par défaut, la bibliothèque `libappindicator1`) peut être requise.
- Pour le fonctionnement en mode graphique du programme d'installation et de désinstallation en ligne de commande, un émulateur de terminal (comme xterm, xvt, etc.) est requis.

- Pour élever les privilèges des logiciels d'installation ou de désinstallation, un des utilitaires suivants est requis : `su`, `sudo`, `gksu`, `gksudo`, `kdesu`, `kdesudo`. Pour le fonctionnement correct de Dr.Web pour Linux, il faut que le système utilise le mécanisme d'authentification PAM.

Pour travailler correctement avec Dr.Web pour Linux en ligne de commande, vous pouvez activer la saisie semi-automatique de commandes dans l'interface de commande utilisée (si elle est désactivée).

Si vous rencontrez un problème avec l'installation de paquets ou composants supplémentaires, référez-vous aux Manuels Utilisateur concernant la distribution utilisée pour le système d'exploitation installé.

Compatibilité avec les composants de systèmes d'exploitation

- Le moniteur SpIDer Guard utilise par défaut le mécanisme système fanotify, tandis que dans les OS où le composant fanotify n'est pas réalisé ou il n'est pas disponible par d'autres raisons – il utilise le *module de noyau chargeable (module LKM)*, fourni déjà assemblé. Les modules LKM de tous les systèmes GNU/Linux mentionnés ci-dessus sont fournis avec Dr.Web pour Linux. En cas de nécessité, vous avez la possibilité d'assembler le module de noyau manuellement à partir des codes initiaux fournis pour tous les OS utilisant le noyau GNU/Linux en version 2.6.x et supérieure.
  L'utilisation de LKM n'est pas supportée pour les architectures ARM64 et E2K.

Les OS lancés dans l'environnement de l'hyperviseur Xen ne prennent pas en charge le fonctionnement de SpIDer Guard via le module de noyau GNU/Linux (module LKM). Une tentative de charger le module de noyau utilisé par SpIDer Guard lors du fonctionnement de l'OS dans l'environnement Xen peut provoquer une erreur critique du noyau (appelé l'erreur « *Kernel panic* »).

Le fonctionnement de SpIDer Guard en mode renforcé (paranoïde) avec le blocage préalable de l'accès aux fichiers non analysés est possible uniquement via fanotify, si le noyau du système est compilé avec l'option `CONFIG_FANOTIFY_ACCESS_PERMISSIONS` active.

- Le moniteur SpIDer Gate peut avoir des problèmes de compatibilité avec les autres pare-feux installés sur votre système d'exploitation :
  - Conflit avec Shorewall et SuseFirewall2 (dans l'OS SUSE Linux Enterprise Server). En cas de conflit avec ces pare-feux, un message d'erreur de SpIDer Gate avec le code `x109` s'affiche. La méthode de la résolution du conflit est décrite dans la rubrique Erreurs connues.
  - Conflit avec FirewallD (dans l'OS Fedora, CentOS, Red Hat Enterprise Linux). En cas de conflit avec ce pare-feu, un message d'erreur de SpIDer Gate avec le code `x102` s'affiche. La méthode de la résolution du conflit est décrite dans la rubrique Erreurs connues.

- Dans le cas où le système d'exploitation contient NetFilter de la version *précédant la version 1.4.15*, le problème suivant lié à une erreur interne de réalisation de NetFilter peut survenir : en cas de désactivation de SpIDer Gate, le fonctionnement du réseau est perturbé. Il est recommandé de mettre à niveau le système vers la version incluant NetFilter de la version 1.4.15 ou supérieure. La méthode de la résolution de ce problème est décrite dans la rubrique Erreurs connues.
- Dans un fonctionnement normal, le moniteur SpIDer Gate est compatible avec toutes les applications utilisateur utilisant le réseau, y compris les navigateurs web et les clients de messagerie. Pour l'analyse correcte des connexions sécurisées, il est nécessaire d'ajouter le certificat Dr.Web pour Linux à la liste des certificats fiables des applications utilisant des connexions sécurisées (par exemple, des navigateurs et des clients de messagerie).
- Après la modification de fonctionnement du moniteur SpIDer Gate (l'activation du moniteur désactivé, la modification du mode d'analyse des connexions sécurisées), il est nécessaire de *redémarrer les clients de messagerie* utilisant le protocole IMAP pour recevoir des messages entrants du serveur de messagerie.

Compatibilité avec les sous-systèmes de sécurité

Avec les paramètres par défaut, Dr.Web pour Linux n'est pas compatible avec le sous-système d'amélioration de sécurité SELinux. De plus, Dr.Web pour Linux fonctionne par défaut en mode de fonctionnalité réduite dans les systèmes GNU/Linux utilisant les modèles de contrôle d'accès obligatoire (par exemple, dans les système ayant le sous-système d'accès obligatoire PARSEC, basé sur l'attribution des niveaux de privilèges (niveaux d'accès obligatoire) aux utilisateurs et aux fichiers).

S'il est nécessaire d'installer Dr.Web pour Linux dans les systèmes avec SELinux et dans les systèmes utilisant les modèles de contrôle d'accès obligatoire, la configuration supplémentaire des sous-systèmes de sécurité peut être requise pour enlever les limitations dans le fonctionnement de Dr.Web pour Linux. Pour plus d'infos, voir la section Configuration des sous-systèmes de sécurité.

Octroi de la licence

Les permissions pour utiliser Dr.Web pour Linux sont accordées par la licence achetée auprès de Doctor Web ou auprès ses partenaires. Les paramètres de la licence déterminant les droits utilisateur sont définis conformément au Contrat de licence (voir https://license.drweb.com/agreement/) que l'utilisateur accepte durant l'installation de Dr.Web pour Linux. Le Contrat de licence contient des informations concernant l'utilisateur et le vendeur comme les paramètres d'utilisation du produit acheté, incluant :

- La liste des composants autorisés pour l'utilisateur.
- La durée de la licence de Dr.Web pour Linux.
- D'autres conditions (par exemple, le nombre d'ordinateurs sur lequel Dr.Web pour Linux acheté peut être utilisé).

Vous avez également la possibilité d'activer la *période de démo* pour tester le produit. Dans ce cas, l'utilisateur obtient le droit d'utiliser l'ensemble des fonctionnalités de Dr.Web pour Linux pendant toute la durée de validité de la période de démo.

Chaque licence pour les produits de Doctor Web possède un numéro de série unique associé à un fichier spécifique conservé sur l'ordinateur. Ce fichier régule le fonctionnement des composants de Dr.Web pour Linux en conformité avec les paramètres de la licence et est nommé fichier clé *de licence. Lors de l'activation d'une version démo, un fichier clé spécifique, nommé fichier clé de démo*, est généré automatiquement.

Si l'utilisateur ne possède aucune licence active, ni la période de démonstration activée (y compris les cas où la licence achetée ou la période de démonstration a expiré), les fonctions antivirus de Dr.Web pour Linux sont bloquées. De plus, le service de mise à jour des bases virales de Dr.Web depuis les serveurs des mises à jour de Doctor Web est indisponible. Mais vous pouvez activer Dr.Web pour Linux en le connectant au serveur de protection centralisée du réseau antivirus administré par l'entreprise ou le fournisseur de services Internet. Dans ce cas, la gestion des fonctions antivirus et des mises à jour du produit est effectuée par le serveur de protection centralisée.

Installation et suppression

Cette section décrit les procédures d'installation et de suppression de Dr.Web pour Linux en version 11.1. Dans ce chapitre, vous trouverez également la description de la réception des mises à jour et de la mise à niveau vers une nouvelle version, si Dr.Web pour Linux de la version antérieure est déjà installé sur votre ordinateur.

De plus, cette section contient la description de la procédure d'installation et de suppression personnalisée des composants de Dr.Web pour Linux (par exemple, pour réparer des erreurs survenues dans le fonctionnement ou pour installer avec l'ensemble de fonctions limité) et la description de la configuration des sous-systèmes de sécurité (tels que SELinux), ce qui peut être nécessaire lors de l'installation et l'utilisation de Dr.Web pour Linux.

- Installation de Dr.Web pour Linux.
- Mise à jour de Dr.Web pour Linux.
- Suppression de Dr.Web pour Linux.
- Configuration des sous-systèmes de sécurité.
- Paramètres avancés :
  - Emplacement des fichiers de Dr.Web pour Linux.
  - Installation et suppression personnalisées des composants.

Ces opérations peuvent être effectuées uniquement par un utilisateur possédant les privilèges de super-utilisateur (utilisateur *root*). Pour élever les privilèges, utilisez la commande `su` pour changer d'utilisateur ou la commande d'exécution au nom d'un autre utilisateur `sudo` .

La compatibilité de Dr.Web pour Linux avec des logiciels antivirus d'autres fabricants *n'est pas garantie*. L'installation de deux logiciels antivirus sur le même ordinateur peut entraîner *des erreurs de fonctionnement du système d'exploitation et une perte de données importantes*, c'est pourquoi, avant d'installer Dr.Web pour Linux, *il est fort recommandé* de supprimer de l'ordinateur les logiciels antivirus d'autres fabricants.

Si un autre produit antivirus Dr.Web *est déjà installé* sur votre ordinateur depuis le package universel (`.run`) et que vous voulez installer encore un produit antivirus Dr.Web (par exemple, Dr.Web pour les serveurs de fichiers UNIX est installé depuis un package universel et vous voulez installer en supplément Dr.Web pour Linux), il faut d'abord s'assurer que la version du produit installé est *identique* à celle de Dr.Web pour Linux que vous voulez installer. Si la version que vous voulez installer est supérieure à celle du produit déjà installé sur votre ordinateur, *avant l'installation*, il faut mettre à niveau le produit installé vers la version du produit Dr.Web que vous voulez installer en supplément.

Installation de Dr.Web pour Linux

Pour installer Dr.Web pour Linux, effectuez une des actions suivantes :

1. Téléchargez le fichier d'installation grâce au package universel pour les systèmes UNIX sur le site officiel de Doctor Web. Le paquet est fourni avec les installateurs (graphique et console) démarrant en fonction de l'environnement.
2. Installez Dr.Web pour Linux sous forme de l'ensemble des paquets natifs (pour ce faire, connectez vous au dépôt correspondant de Doctor Web).

Dans les distributions utilisant des versions obsolètes du gestionnaire de paquets (par exemple, Alt 8 SP), il est recommandé d'installer Dr.Web pour Linux depuis le package universel.

Après la fin de l'installation de Dr.Web pour Linux par un des moyens indiqués, vous devez activer la licence ou installer le fichier clé. De plus, vous pouvez connecter Dr.Web pour Linux au serveur de protection centralisée. Tant que vous n'aurez pas fait cela, les *fonctions de la protection antivirus seront désactivées.*

Si un client de messagerie (tel que Mozilla Thunderbird) utilisant le protocole IMAP pour la réception des messages est lancé dans le système, il faut le redémarrer après l'installation de l'antivirus pour assurer l'analyse des messages entrants.

Dr.Web pour Linux installé par un des moyens décrit dans cette rubrique peut être supprimé ou mis à jour si les composants inclus ont été modifiés ou en cas de sortie d'une nouvelle version. Si nécessaire, configurez les sous-systèmes de sécurité de UNIX pour le fonctionnement correct de Dr.Web pour Linux installé. En cas des problèmes de fonctionnement de certains composants, vous pouvez les reinstaller ou supprimer sans supprimer Dr.Web pour Linux entier.

Installation du package universel

Dr.Web pour Linux est distribué sous forme de fichier d'installation nommé `drweb-<version>-av-linux-<plateforme>.run` où <*plateforme*> est une ligne qui indique le type de plateforme pour laquelle le produit est prévu (`x86` pour les plateformes 64-bits, `amd64`, `arm64` et `e2s` pour les plateformes 64-bits). Par exemple :

```
drweb-11.1-av-linux-amd64.run
```

Le nom du fichier d'installation sera indiqué ci-après comme <*nom_du_fichier*>`.run`.

Pour installer les composants de Dr.Web pour Linux :

1. Téléchargez l'archive sur le site officiel de Doctor Web.
2. Enregistrez-le sur le disque dur, dans un des répertoires (par exemple, `/home/`<*username*>, où <*username*> est le nom de l'utilisateur actuel).

3. Passez dans le répertoire contenant le fichier enregistré et autorisez son exécution, par exemple avec la commande :

```
# chmod +x <nom_du_fichier>.run
```

4. Exécutez l'archive en utilisant la commande suivante :

```
# ./<nom_du_fichier>.run
```

ou utilisez le gestionnaire de fichier standard de l'interface graphique pour modifier les propriétés du fichier et exécuter le fichier.

En cas d'installation de Dr.Web pour Linux dans l'environnement Astra Linux SE en versions 1.6 et 1.7 fonctionnant en mode *ELF* (environnement logiciel fermé), vous pouvez échouer à lancer l'installateur si la clé publique de la société Doctor Web n'est pas présente dans la liste des clés de confiance. Dans ce cas il faut préconfigurer le mode ELF (voir Configuration du lancement en mode ELF (Astra Linux SE en versions 1.6 et 1.7)) et redémarrer l'installateur.

D'abord, l'intégrité de l'archive d'installation est vérifiée puis un ensemble de fichiers sont extraits de cette archive et placés dans un dossier temporaire et la procédure d'installation est lancée automatiquement. S'il n'est pas lancé avec les privilèges de super-utilisateur, le programme d'installation tente d'élever les privilèges en utilisant `sudo`. Si cette étape échoue, l'installation s'arrête.

Si une partie du système de fichiers, contenant le répertoire local, manque d'espace libre pour extraire la distribution, le processus d'installation sera achevé après avoir notifié l'utilisateur. Dans ce cas, réessayez à extraire la distribution après avoir modifié la valeur de la variable système d'environnement `TMPDIR` de manière qu'elle indique un répertoire ayant assez d'espace libre. Vous pouvez également utiliser la clé pour extraire dans le répertoire spécifié `--target` (voir la rubrique Installation et suppression personnalisées des composants).

En fonction de l'environnement dans lequel la distribution est lancée, un des installateurs inclus dans le kit de distribution s'exécute :

- Installateur pour le mode graphique.
- Installateur pour le mode de ligne de commande.

Ainsi, l'installateur pour le mode de ligne de commande sera lancé automatiquement si l'installateur pour le mode graphique échoue à démarrer.

5. Suivez les instructions de l'installateur.

Il existe la possibilité de lancer l'installateur en mode complètement automatique en exécutant la commande :

```
# ./<nom_du_fichier>.run -- --non-interactive
```

Dans ce cas, le programme d'installation sera lancé en mode complètement automatique sans afficher l'interface de l'utilisateur (y compris les dialogues du programme d'installation pour le mode de ligne de commande).

Notez que :

- L'utilisation de cette option signifie que vous *acceptez* les termes du Contrat de licence de Dr.Web. Vous pouvez prendre connaissance du texte du Contrat de licence après l'installation en lisant le fichier `/opt/drweb.com/share/doc/LICENSE`. L'extension du fichier indique la langue dans laquelle le texte du Contrat de licence est écrit. Le fichier `LICENSE` sans extension contient le texte du Contrat de licence de Dr.Web en anglais. Si vous *n'acceptez pas* les termes du Contrat de licence, vous devez supprimer Dr.Web pour Linux après l'installation.
- Le lancement de l'installation en mode complètement automatique requiert les privilèges de super-utilisateur. Pour élever les privilèges, vous pouvez utiliser les commandes `su` et `sudo`.

Si votre distribution de UNIX inclut SELinux, le processus d'installation peut être interrompu par le sous-système de sécurité. Si une telle situation arrive, mettez SELinux en mode de *permission (Permissive)*. Pour cela, entrez la commande suivante :

```
# setenforce 0
```

Ensuite, redémarrez l'installateur. Après la fin de l'installation, configurez les politiques de sécurité de SELinux pour assurer un fonctionnement correct des composants antivirus.

Tous les fichiers d'installation extraits seront automatiquement supprimés à la fin de l'installation.

Il est recommandé de sauvegarder le fichier téléchargé *<nom_du_fichier>*`.run` depuis lequel l'installation a été lancée pour pouvoir réinstaller Dr.Web pour Linux ou ses composants plus tard sans mettre à niveau sa version.

Une fois l'installation achevée, le groupe **Dr.Web** s'affiche dans le menu **Annexes** dans l'interface graphique du bureau. Ce groupe contient deux éléments :

- **Dr.Web pour Linux** pour démarrer Dr.Web pour Linux en mode graphique.
- **Supprimer les composants de Dr.Web** pour le supprimer.

L'icône de l'indicateur de statut du programme est affichée automatiquement dans la zone de notifications du bureau après la reconnexion de l'utilisateur au système.

L'installation des paquets, indiqués dans la rubrique Pré-requis système et compatibilité peut être requise pour le fonctionnement correct de Dr.Web pour Linux (par exemple, l'installation de la bibliothèque de support des applications 32-bits pour la plateforme 64-bits ou la bibliothèque `libappindicator1` pour l'affichage correct de l'indicateur de statut du programme dans la zone de notifications du bureau).

Installation en mode graphique

Si, au début de son fonctionnement, le programme d'installation détecte des problèmes qui pourraient mettre Dr.Web pour Linux en état non opérationnel complet ou partiel, une liste de problèmes détectés sera affichée dans une fenêtre correspondante. Pour résoudre les problèmes détectés avant l'installation, veuillez interrompre l'installation en cliquant sur **Quitter**. Dans ce cas vous devez relancer le programme d'installation après la résolution des problèmes détectés (installation des bibliothèques supplémentaires, désactivation temporaire de SELinux, etc.). Pour ne pas interrompre l'installation de Dr.Web pour Linux, cliquez sur **Continuer**. Dans ce cas, l'installation sera poursuivie et la fenêtre de l'Assistant d'installation sera affichée. Cependant il vous faudra résoudre les problèmes détectés plus tard, après la fin d'installation ou en cas de détection d'erreurs de fonctionnement de Dr.Web pour Linux.

Après le démarrage du programme d'installation en mode graphique, la fenêtre de l'Assistant d'Installation s'affiche.

Image 2. Page de bienvenue de l'assistant d'installation

Pour installer Dr.Web pour Linux sur l'ordinateur, effectuez les actions suivantes :

1. Lisez le Contrat de licence de Doctor Web. Pour cela, cliquez sur le lien correspondant sur la page d'accueil de l'Assistant d'installation. Une page contenant le Contrat de Licence et les informations sur le droit d'auteur pour les composants installés va s'ouvrir.

   Si nécessaire, vous pouvez imprimer le Contrat de licence et les informations sur le droit d'auteur. Pour ce faire, ouvrez l'onglet souhaité sur la page du Contrat de licence et cliquez sur **Imprimer**.

   Pour fermer la page du Contrat de licence, cliquez sur **OK**.
2. Pour démarrer l'installation, vous pouvez autoriser la connexion automatique au service Dr.Web Cloud après l'installation de Dr.Web pour Linux. Pour ce faire cochez la case correspondante (la case est cochée par défaut au moment de lancement de l'Assistant d'Installation). Si vous ne voulez pas autoriser Dr.Web pour Linux à utiliser le service Dr.Web

Cloud, décochez la case. Vous pouvez interdire ou autoriser à Dr.Web pour Linux d'utiliser le service Dr.Web Cloud à tout moment dans les paramètres du logiciel.

3. Pour lancer l'installation, cliquez sur **Installer**. Ainsi vous acceptez les conditions du Contrat de licence de Doctor Web. Si vous choisissez de ne pas installer Dr.Web pour Linux sur votre ordinateur, cliquez sur **Annuler**. Une fois le bouton cliqué, l'Assistant d'installation s'arrête.
4. Après le démarrage de l'installation, une page de l'Assistant contenant la barre de progression s'ouvre. Si vous voulez consulter le journal d'installation, cliquez sur **En savoir plus**.
5. Une fois les fichiers du logiciel copiés avec succès et les réglages de paramètres système effectués, la dernière page de l'assistant contenant les résultats de l'installation s'affiche.
6. Pour quitter l'Assistant d'installation, cliquez sur **OK**. Si cette opération est supportée par l'ordinateur, à l'étape finale une page s'affichera proposant de lancer Dr.Web pour Linux en mode graphique. Pour lancer, cochez la case **Lancez Dr.Web pour Linux maintenant** et cliquez sur **OK**.

Si le processus d'installation échoue à cause d'une erreur, la dernière page de l'Assistant d'installation contiendra un message correspondant. Dans ce cas, quittez l'Assistant d'installation en cliquant sur **OK**, résolvez le problème qui a provoqué l'erreur et redémarrez l'installation.

Installation en ligne de commande

Lorsque le programme d'installation pour la ligne de commande démarre, l'invite de commandes s'affiche sur l'écran.

1. Pour démarrer l'installation, entrez *Yes* ou *Y* en réponse à la question « Voulez-vous continuer ? ». Pour quitter l'installateur, entrez *No* ou *N*. Dans ce cas, l'installation sera terminée.
2. Ensuite, vous devez lire le Contrat de licence de Doctor Web qui s'affiche sur l'écran. Appuyez sur ENTREE pour descendre ligne par ligne ou sur LA BARRE D'ESPACE pour passer à la page suivante. En consultant le Contrat de licence, notez que la fonctionnalité de retour (en haut) n'est pas prévue.
3. Après avoir lu le Contrat de Licence, vous êtes invité à l'accepter. Tapez *Yes* ou *Y* si vous acceptez les termes du contrat. Si vous refusez de l'accepter, tapez *No* ou *N*. Dans ce cas, l'installation s'arrête automatiquement.
4. Après avoir accepté le Contrat de licence, l'installation des composants de Dr.Web pour Linux démarre automatiquement. Durant la procédure, des informations sur le processus d'installation (journal d'installation), incluant la liste des composants installés, seront affichées sur l'écran.
5. Une fois l'installation effectuée avec succès, l'installateur quitte automatiquement. Si une erreur survient, un message la décrivant s'affiche et l'installateur quitte.
6. Pour commencer à travailler avec Dr.Web pour Linux installé, lancez le produit dans un des modes disponibles.

Si le processus d'installation a échoué à cause d'une erreur, résolvez les problèmes qui l'ont provoquée et démarrez une nouvelle procédure d'installation.

Installation depuis le référentiel

Les paquets natifs de Dr.Web pour Linux sont stockés dans le référentiel officiel de Dr.Web à la page https://repo.drweb.com. Après avoir ajouté le référentiel Dr.Web à la liste de ceux utilisés par le gestionnaire de paquet de votre système d'exploitation, vous pouvez installer le produit depuis les paquets natifs comme vous installez n'importe quel autre programme depuis les référentiels du système d'exploitation. Les dépendances requises sont automatiquement résolues. De plus, dans ce cas, la procédure de détection des mises à jours est supportée. Le gestionnaire de paquets de l'OS détecte les mises à jours de tous les composants Dr.Web installés du référentiel connecté et propose d'installer les mises à jour détectées.

Pour accéder au référentiel de Dr.Web, une connexion Internet est requise.

Toutes les commandes mentionnées ci-dessous pour la connexion des référentiels, l'importation des clés d'installation, l'installation et la suppression des paquets, doivent être effectuées avec les privilèges de super-utilisateur (utilisateur *root*). Pour élever les privilèges, utilisez la commande `su` (modifier l'utilisateur en cours) ou la commande `sudo` (exécuter la commande indiquée du nom d'un autre utilisateur).

Vous trouverez ci-dessous les procédures pour les OS suivants (les gestionnaires de paquets) :

- Debian, Mint, Ubuntu (apt).
- ALT Linux, PCLinuxOS (apt-rpm).
- Mageia, OpenMandriva Lx (urpmi).
- Red Hat Enterprise Linux, Fedora, CentOS (yum, dnf).
- SUSE Linux (zypper).

Debian, Mint, Ubuntu (apt)

1. Le référentiel pour ces OS est protégé par la signature numérique de Doctor Web. Pour accéder au référentiel, importez la clé de signature numérique et ajoutez-la dans le dossier du gestionnaire de paquets en exécutant la commande :

```
# apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys
8C42FC58D8752769
```

2. Pour vous connecter au référentiel, ajoutez la ligne suivante au fichier `/etc/apt/sources.list` :

```
deb https://repo.drweb.com/drweb/debian 11.1 non-free
```

Vous pouvez effectuer les étapes 1 et 2 en téléchargeant du référentiel et en installant un paquet DEB spécifique.
Lien de téléchargement de paquet : https://repo.drweb.com/drweb/drweb-repo11.1.deb.

3. Pour installer Dr.Web pour Linux depuis le référentiel, utilisez les commandes suivantes :

```
# apt-get update
# apt-get install drweb-workstations
```

Vous pouvez également utiliser des gestionnaires de paquets alternatifs (par exemple, Synaptic ou aptitude) pour installer le produit. De plus, il est recommandé d'utiliser des gestionnaires alternatifs, comme aptitude, pour résoudre un conflit de paquets s'il survient.

ALT Linux, PCLinuxOS (apt-rpm)

1. Pour vous connecter au référentiel, ajoutez la ligne suivante au fichier `/etc/apt/sources.list` :

```
rpm https://repo.drweb.com/drweb/altlinux 11.1/<arch> drweb
```

où <*arch*> désigne l'architecture des paquets utilisée :

- Pour la version 32-bits: `i386` ;
- pour l'architecture AMD64 : `x86_64` ;
- pour l'architecture ARM64 : `aarch64` ;
- pour l'architecture E2K : `e2s`.

2. Pour installer Dr.Web pour Linux depuis le référentiel, utilisez les commandes suivantes :

```
# apt-get update
# apt-get install drweb-workstations
```

Vous pouvez également utiliser des gestionnaires de paquets alternatifs (par exemple, Synaptic ou aptitude) pour installer le produit.

Mageia, OpenMandriva Lx (urpmi)

1. Connectez le référentiel avec la commande :

```
# urpmi.addmedia drweb https://repo.drweb.com/drweb/linux/11.1/<arch>/
```

où <*arch*> désigne l'architecture des paquets utilisée :

- Pour la version 32-bits: `i386` ;
- Pour la version 64-bits: `x86_64`.

2. Pour installer Dr.Web pour Linux depuis le référentiel, utilisez la commande suivante :

```
# urpmi drweb-workstations
```

Vous pouvez également utiliser des gestionnaires de paquets alternatifs (par exemple, rpmdrake) pour installer le produit.

Red Hat Enterprise Linux, Fedora, CentOS (yum, dnf)

1. Ajoutez au répertoire `/etc/yum.repos.d` le fichier `drweb.repo` au contenu suivant :

```
[drweb]
name=DrWeb - 11.1
baseurl=https://repo.drweb.com/drweb/linux/11.1/$basearch/
gpgcheck=1
enabled=1
gpgkey=https://repo.drweb.com/drweb/drweb.key
```

Si vous voulez enregistrer le contenu indiqué ci-dessus dans un fichier à l'aide de la commande de type `echo` avec la redirection, utilisez `\$` comme caractère d'échappement pour le caractère `$`.

Vous pouvez effectuer l'étape 1 en téléchargeant du référentiel et en installant un paquet RPM spécifique.
Lien de téléchargement de paquet : https://repo.drweb.com/drweb/drweb-repo11.1.rpm.

2. Pour installer Dr.Web pour Linux depuis le référentiel, utilisez la commande suivante :

```
# yum install drweb-workstations
```

Dans l'OS Fedora, depuis la version 22, il est recommandé d'utiliser le gestionnaire `dnf` au lieu du gestionnaire `yum`, par exemple :

```
# dnf install drweb-workstations
```

Vous pouvez également utiliser des gestionnaires de paquets alternatifs (par exemple, PackageKit or Yumex) pour installer le produit.

SUSE Linux (zypper)

1. Pour vous connecter au référentiel, utilisez la commande suivante :

```
# zypper ar https://repo.drweb.com/drweb/linux/11.1/\$basearch/ drweb
```

2. Pour installer Dr.Web pour Linux depuis le référentiel, utilisez les commandes suivantes :

```
# zypper refresh
# zypper install drweb-workstations
```

Vous pouvez également utiliser des gestionnaires de paquets alternatifs (par exemple, YaST) pour installer le produit.

Mise à jour de Dr.Web pour Linux

Il existe deux mode de mise à jour de Dr.Web pour Linux :

1. Obtention des mises à jour des paquets et des composants sortis au sein de la version actuelle de Dr.Web pour Linux (en général, ces mises à jour contiennent des correction des erreurs, des améliorations mineures de fonctionnement des composants) ;
2. Mise à niveau vers une nouvelle version du produit. Ce moyen est utilisé si l'entreprise Doctor Web crée une nouvelle version de Dr.Web pour Linux utilisé possédant de nouvelles fonctionnalités.

Obtention des mises à jour

Dans cette section :

- Mise à jour par Internet.
- Mise à jour sans connexion Internet.

Mise à jour par Internet

Après l'installation de Dr.Web pour Linux par un des moyens décrits dans la rubrique correspondante, le gestionnaire de paquets se connecte automatiquement au dépôt de correspondant de Dr.Web :

- Si l'installation a été effectuée depuis un package universel (fichier `.run`), et les packages au format DEB sont utilisés dans le système (par exemple, OS Debian, Mint, Ubuntu), alors une version particulière de gestionnaire de paquets `zypper` installée automatiquement lors de l'installation de Dr.Web pour Linux est requise pour la gestion des packages Dr.Web.

  Pour obtenir et installer les paquets de Dr.Web mis à jour par ce gestionnaire, passez dans le répertoire <*opt_dir*>`/bin` (pour GNU/Linux — `/opt/drweb.com/bin`) et exécutez les commandes suivantes :

  ```
  # ./zypper refresh
  # ./zypper update
  ```

- Dans tous les autres cas, utilisez les commandes de mise à jour du gestionnaire de paquets utilisé dans votre OS, par exemple :
  - Dans Red Hat Enterprise Linux et CentOS utilisez la commande `yum`
  - Dans Fedora utilisez la commande `yum` ou `dnf`
  - Dans SUSE Linux, utilisez la commande `zypper`
  - Dans Mageia, OpenMandriva Lx, utilisez la commande `urpmi`
  - Dans Alt Linux, PCLinuxOS, Debian, Mint, Ubuntu utilisez la commande `apt-get`.

Vous pouvez également utiliser les gestionnaires de paquets alternatifs créés pour votre système d'exploitation. Si nécessaire, consultes le guide du gestionnaire de paquets utilisé.

En cas de sortie d'une nouvelle version de Dr.Web pour Linux, les paquets contenant ses composants sont placés dans la section du dépôt Dr.Web correspondant à la nouvelle version du produit. Dans ce cas, il faut changer de section du dépôt Dr.Web dans le gestionnaire de paquets (voir Mise à niveau vers une nouvelle version).

Mise à jour sans connexion Internet

En cas de sécurité renforcée, quand il n'y a pas de connexion Interner ou qu'elle est limitée, il est possible de mettre à jour les bases virales et le moteur antivirus sans connexion Internet. Dans ce cas, les mises à jour sont téléchargées sur un ordinateur connecté à Internet, ensuite elles sont copiées sur une clé USB ou un disque réseau. Enfin, elles sont installées sur un autre ordinateur qui n'est pas connecté à Internet.

La mise à jour est effectuée via la ligne de commande.

Pour obtenir les mises à jour :

1. Sur l'ordinateur connecté à Internet, exécutez la commande suivante:

```
$ drweb-ctl update --Path <chemin d'accès au répertoire où les mises à jour seront téléchargées>
```

2. Copiez les mises à jour sur la clé USB ou le disque réseau.

3. Montez un disque réseau ou un lecteur sur l'ordinateur sur lequel il faut installer les mises à jour. Si vous recevez les mises à jour depuis un lecteur USB, il faut effectuer les commandes suivantes :

```
# mkdir /mnt/usb
# mount <chemin d'accès au périphérique> /mnt/usb
```

4. Installez les mises à jour avec la commande :

```
$ drweb-ctl update --From /mnt/usb
```

Mise à niveau vers une nouvelle version

Remarques préalables

La mise à niveau des versions précédentes de Dr.Web pour Linux vers la version 11.1 est supportée. Notez que Dr.Web pour Linux doit être mis à niveau de la même façon dont la version précédente de Dr.Web pour Linux a été installée :

- Si la version actuelle de Dr.Web pour Linux a été installée depuis le référentiel, la mise à niveau requiert la mise à jour des paquets depuis le référentiel.
- Si la version actuelle de Dr.Web pour Linux a été installée depuis le package universel, la mise à niveau requiert l'installation du package universel contenant la nouvelle version.

Pour identifier la façon dont Dr.Web pour Linux a été installé, vérifiez que le répertoire de fichiers exécutables de Dr.Web pour Linux contient le script du programme de suppression `remove.sh`. Si c'est le cas, la version actuelle de Dr.Web pour Linux a été installée depuis le package universel ; sinon, elle a été installée depuis le référentiel.

Si vous ne pouvez pas mettre à niveau Dr.Web pour Linux comme vous l'avez installé, supprimez la version actuelle du produit, puis installez une nouvelle version en utilisant la méthode qui vous convient. Les procédures d'installation et de suppression des versions antérieures de Dr.Web pour Linux sont les mêmes que les procédures d'installation et de suppression décrites dans le manuel actuel pour la version 11.1. Pour en savoir plus, consultez le Manuel Utilisateur correspondant à votre version de Dr.Web pour Linux.

Notez que la migration de Dr.Web pour Linux 6.0.2 et antérieure vers la version 11.1 est possible *uniquement* si vous supprimez l'ancienne version de Dr.Web pour Linux et installez la version 11.1.

Si la version de Dr.Web pour Linux à mettre à niveau fonctionne sous le serveur de protection centralisée, alors il est recommandé avant de commencer la mise à niveau de sauvegarder l'adresse du serveur de protection centralisée auquel Dr.Web pour Linux est connecté. Pour obtenir l'adresse du serveur de protection centralisée auquel Dr.Web pour Linux est connecté, utilisez la commande (uniquement pour le produit avec la version plus récente que 6.0.2) :

```
$ drweb-ctl appinfo
```

lors de la sortie de la commande, dans la ligne du type suivant

```
ESAgent; <PID>; RUNNING 1; Connected <adresse>, on-line
```

sauvegardez la partie *<adresse>* (elle peut ressembler à la ligne du type `tcp://<adresse IP>:<port>`, par exemple : `tcp://10.20.30.40:1234`). De plus, il est recommandé de sauvegarder le fichier du certificat du serveur.

En cas de difficultés d'obtention des paramètres de la connexion actuelle, consultez le Manuel administrateur de votre version de Dr.Web pour Linux et contactez l'administrateur de votre réseau antivirus.

Mise à niveau de la version 9.0 et supérieure

Mise à niveau par l'installation du package universel

Installez Dr.Web pour Linux en version 11.1 depuis le package universel. Durant l'installation, vous serez invité à supprimer automatiquement l'ancienne version de Dr.Web pour Linux si c'est nécessaire.

Mettre à niveau depuis le référentiel

Pour mettre à niveau votre version actuelle de Dr.Web pour Linux installée depuis le référentiel de Doctor Web, en fonction des types de paquets, effectuez les actions suivantes :

- **Si vous utilisez des paquets RPM (yum)** :
  1. Changez du référentiel utilisé (de la version actuelle du référentiel de paquets vers le référentiel en version 11.1).

     Nom du référentiel qui sauvegarde les paquets en version <%PRODUCTVERSION%>, voir la rubrique Installation depuis le référentiel. Pour préciser la façon de changement de référentiels, consultez les manuels de la distribution de l'OS que vous utilisez.

  2. Installez la nouvelle version de Dr.Web pour Linux depuis le référentiel en utilisant la commande :

     ```
     # yum update
     ```

     si vous utilisez le gestionnaire `dnf` (comme, par exemple, dans l'OS Fedora en version 22 ou supérieure) :

     ```
     # dnf update
     ```

     Si une erreur survient lors de la mise à jour des paquets, supprimez et, ensuite, installez Dr.Web pour Linux. Si nécessaire, voir les sections Suppression de Dr.Web pour Linux installé depuis le référentiel et Installation depuis le référentiel (les éléments correspondant à votre OS et au gestionnaire de paquets).

- **Si vous utilisez des paquets DEB (apt-get)** :
  1. Changez du référentiel utilisé (de la version actuelle du référentiel de paquets vers le référentiel en version 11.1).
  2. Reinstallez les paquets de Dr.Web pour Linux, en exécutant les commandes :

```
# apt-get update
# apt-get dist-upgrade
```

Notez que dans l'OS Ubuntu 14.04 (version 64 bits), l'application de la commande `apt-get dist-upgrade` pour la mise à jour des distributions peut échouer. Dans ce cas, utilisez le gestionnaire de paquets aptitude (pour mettre à jour la distribution, utilisez la commande aptitude `dist-upgrade`).

Transfert du fichier clé de licence

Quelle que soit la méthode de mise à niveau de Dr.Web pour Linux, le fichier clé de licence est installé automatiquement dans l'emplacement nécessaire pour l'utilisation de la nouvelle version de Dr.Web pour Linux.

En cas de problèmes liés à l'installation automatique du fichier clé de licence, vous pouvez l'installer manuellement. A partir de la version 9.0 Dr.Web pour Linux sauvegarde le fichier clé de licence dans le répertoire `/etc/opt/drweb.com`. En cas de la perte du fichier clé de licence actuel, contactez le support technique de la société Doctor Web.

Reconnexion au serveur de protection centralisée

Si c'est possible, après la mise à niveau (si la version mise à niveau a été connectée au serveur de protection centralisée), la connexion sera rétablie automatiquement. Si la connexion n'est pas rétablie automatiquement, utilisez un des moyens suivants pour connecter la version mise à niveau de Dr.Web pour Linux au réseau antivirus (notez que vous devrez spécifier l'adresse et le fichier de la clé publique du serveur sauvegardés précédemment) :

- Cochez la case dans l'onglet **Mode** de la fenêtre de paramètres de Dr.Web pour Linux.
- Utilisez la commande :

```
$ drweb-ctl esconnect <adresse> --Certificate <chemin d'accès au fichier de certificat du serveur>
```

En cas de difficultés de connexion, contactez l'administrateur de votre réseau antivirus.

Caractéristiques du processus de mise à niveau

- Si la version actuelle de Dr.Web pour Linux est activée au moment de la mise à niveau, les processus de l'ancienne version de Dr.Web pour Linux continuent à être exécutés jusqu'à ce que l'utilisateur quitte le système après l'installation des paquets de la nouvelle version de Dr.Web pour Linux. Ainsi, si Dr.Web pour Linux fonctionne en mode graphique, l'icône de l'indicateur de l'ancienne version de Dr.Web pour Linux peut s'afficher dans la zone de notifications.

- Après la mise à niveau de Dr.Web pour Linux, les paramètres de SpIDer Gate peuvent être réinitialisés aux valeurs par défaut.
- Si un client de messagerie (tel que Mozilla Thunderbird) utilisant le protocole IMAP pour la réception des messages est lancé dans le système, redémarrez-le après la mise à jour pour assurer l'analyse des messages entrants.

Mise à niveau de la version 6.0.2 et les versions antérieures

la migration de Dr.Web pour Linux 6.0.2 et antérieure vers la version 11.1 est possible uniquement si vous supprimez l'ancienne version de Dr.Web pour Linux et installez la version 11.1. Pour plus d'informations sur la suppression de l'ancienne version de Dr.Web pour Linux, consultez le Manuel Utilisateur correspondant à votre version de Dr.Web pour Linux.

Transfert du fichier clé de licence

Le fichier clé de l'ancienne version de Dr.Web pour Linux que vous possédez ne sera pas installé automatiquement afin d'être utilisé par la nouvelle licence, mais vous pouvez l'installer manuellement. Dr.Web pour Linux de la version 6.0.2 ou antérieure réside dans le répertoire `/home/<user>/.drweb` (le répertoire est caché). Si le fichier clé valide est perdu, contactez le support technique de Doctor Web.

Dr.Web pour Linux en version 11.1 ne supporte pas la quarantaine de Dr.Web pour Linux en versions antérieures à 9.0. Si des fichiers isolés demeurent dans la quarantaine de cette version, vous pouvez récupérer ou supprimer ces fichiers manuellement. Dr.Web pour Linux en version 6.0.2 (et antérieure) utilise en tant que quarantaine les répertoires suivants :

- `/var/drweb/infected` : quarantaine système ;
- `/home/<user>/.drweb/quarantine` — quarantaine de l'utilisateur (où *<user>* — nom d'utilisateur).

Pour simplifier le traitement des fichiers placés en quarantaine, il est recommandé de revoir le contenu de la quarantaine avec Dr.Web pour Linux de la version plus ancienne avant de commencer la mise à niveau.

Suppression de Dr.Web pour Linux

En fonction de la méthode d'installation, vous pouvez supprimer Dr.Web pour Linuxpar l'un des moyens suivants :

1. Démarrer le programme de suppression du paquet universel (pour les modes graphique ou le mode de ligne de commande, en fonction de l'environnement).
2. Supprimer les paquets installés depuis le référentiel de Doctor Web via le gestionnaire de paquets système.

Suppression du paquet universel

Vous pouvez supprimer Dr.Web pour Linux installé grâce à la distribution du paquet universel pour les systèmes UNIX via le menu de l'application de l'environnement de bureau, ou via la ligne de commande.

Notez que le programme de suppression va supprimer non seulement Dr.Web pour Linux, mais aussi *tous les autres* produits Dr.Web installés sur votre ordinateur.

S'il y a d'autres produits Dr.Web qui sont installés sur votre ordinateur à part Dr.Web pour Linux, à la place du lancement automatique de la suppression, utilisez la procédure d'installation et de suppression sélective des composants pour supprimer uniquement Dr.Web pour Linux.

Supprimer Dr.Web pour Linux via le menu de l'application

Dans le menu d'applications, sélectionnez le groupe **Dr.Web** et choisissez **Supprimer les composants de Dr.Web**. L'assistant de suppression pour le mode graphique va s'ouvrir.

Supprimer Dr.Web pour Linux via la ligne de commande

Le programme de suppression est lancé par le script `remove.sh` qui réside dans le répertoire `/opt/drweb.com/bin`. Alors, pour lancer la suppression de Dr.Web pour Linux, il faut exécuter la commande suivante :

```
# /opt/drweb.com/bin/remove.sh
```

Puis un programme de désinstallation démarre (en mode graphique ou en ligne de commande selon l'environnement).

Pour lancer le programme de désinstallation directement depuis la ligne de commande, utilisez la commande suivante :

```
# /opt/drweb.com/bin/uninst.sh
```

La suppression de Dr.Web pour Linux est décrite dans les chapitres suivants :

- Suppression en mode graphique,
- Suppression en mode de ligne de commande.

Il existe la possibilité de lancer le programme de suppression en mode complètement automatique en exécutant la commande :

```
# /opt/drweb.com/bin/remove.sh --non-interactive
```

Dans ce cas, le programme de suppression sera lancé en mode complètement automatique sans afficher l'interface de l'utilisateur (y compris les dialogues du programme de suppression pour le mode de ligne de commande). Le lancement de suppression en mode complètement automatique requiert les privilèges de super-utilisateur. Pour élever les privilèges, vous pouvez utiliser les commandes `su` et `sudo`.

Sous Alt 8 СП, les messages du type suivant peuvent s'afficher dans la console :

```
/etc/init.d/drweb-configd : Fichier ou répertoire inexistant
```

Ces messages n'influencent pas le fonctionnement du système. La procédure de suppression s'effectue correctement.

Suppression en mode graphique

Après le démarrage du programme de suppression en mode graphique, la fenêtre de l'Assistant de suppression s'affiche.

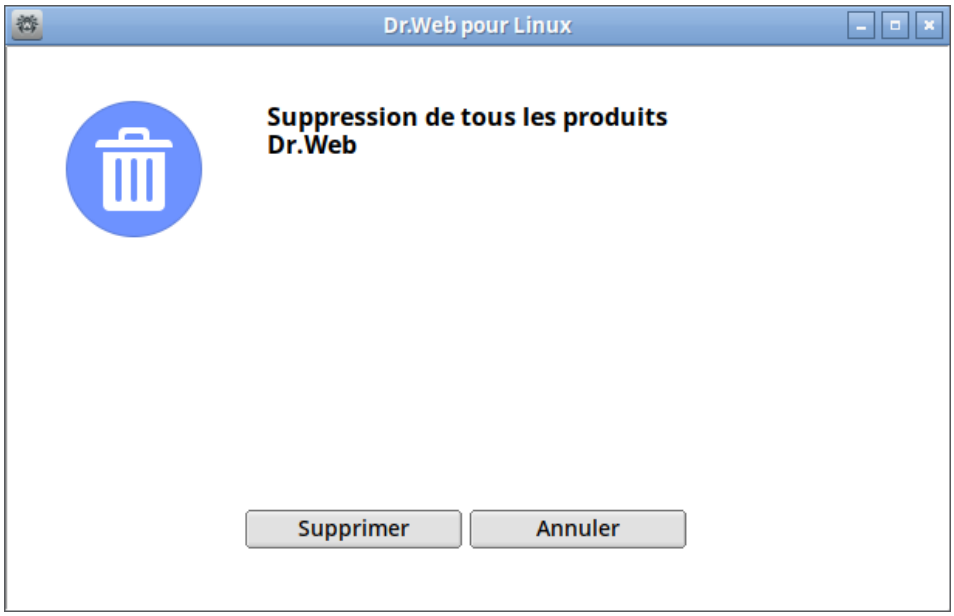

Image 3. Page de bienvenue de l'assistant de suppression

1. Pour désinstaller les produits de Dr.Web, cliquez sur **Supprimer**. Pour fermer l'Assistant de suppression et annuler la suppression des produits Dr.Web de votre ordinateur, cliquez sur **Annuler**.
2. Après le démarrage de la suppression, une page avec une barre de progression s'ouvre. Pour voir les messages du journal de suppression, cliquez sur **En savoir plus**.
3. Une fois que les fichiers de Dr.Web pour Linux sont supprimés avec succès et que toutes les modifications nécessaires sont appliquées aux paramètres système, la dernière page de l'Assistant de suppression s'affiche pour annoncer le succès de l'opération.
4. Pour fermer l'Assistant de Suppression, cliquez sur **OK**.

Suppression en mode de ligne de commande

Lorsque le programme de suppression pour le mode ligne de commande démarre, l'invite de commande s'affiche sur l'écran.

1. Pour démarrer la suppression, entrez *Yes* ou *Y* en réponse à la question « Voulez-vous continuer ? ». Pour refuser de supprimer les produits Dr.Web de votre ordinateur, entrez *No* ou *N*. Dans ce cas, la suppression sera terminée.

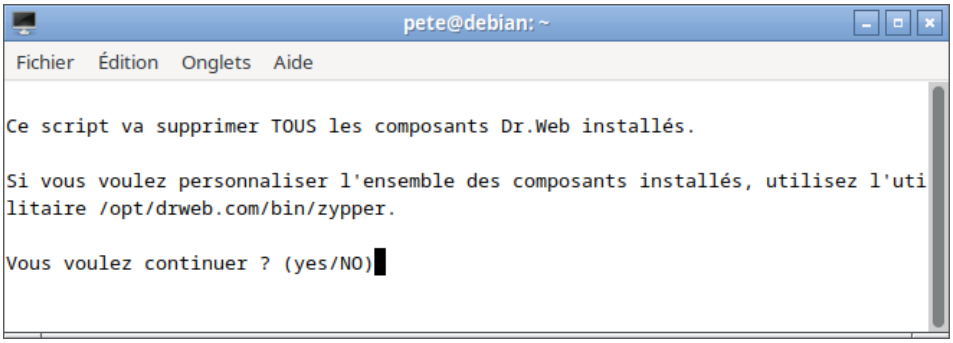

Image 4. Invite de commande pour la suppression

2. Après la confirmation de la suppression, la procédure de suppression de tous les paquets installés Dr.Web se lance. Dans ce cas, les messages sur le processus de suppression s'affichent sur l'écran et sont journalisés.
3. A la fin de processus, le programme de suppression s'arrête automatiquement.

Suppression de Dr.Web pour Linux installé depuis le référentiel

> Toutes les commandes mentionnées ci-dessous pour le paquet de suppression requièrent les privilèges de super-utilisateur (root). Pour élever les privilèges, utilisez la commande `su` (modifier l'utilisateur en cours) ou la commande `sudo` (exécuter la commande indiquée avec les privilèges d'un autre utilisateur).

Vous trouverez ci-dessous les procédures pour les OS suivants (les gestionnaires de paquets) :

- Debian, Mint, Ubuntu (apt),
- ALT Linux, PCLinuxOS (apt-rpm),
- Mageia, OpenMandriva Lx (urpmi),
- Red Hat Enterprise Linux, Fedora, CentOS (yum, dnf),
- SUSE Linux (zypper).

Debian, Mint, Ubuntu (apt)

Pour supprimer le métapaquet racine de Dr.Web pour Linux, entrez la commande suivante :

```
# apt-get remove drweb-workstations
```

Pour supprimer le métapaquet racine avec toutes les dépendances, exécutez la commande suivante :

```
# apt-get remove drweb-workstations --autoremove
```

Pour supprimer automatiquement tous les paquets qui ne sont plus utilisés, entrez la commande suivante :

```
# apt-get autoremove
```

Veuillez noter quelques aspects spécifiques de la suppression avec la commande `apt-get` :

1. La première commande supprime uniquement le métapaquet `drweb-workstations` ; tous les autres paquets qui pourraient être installés automatiquement pour résoudre les dépendances restent dans le système.
2. La deuxième commande supprime tous les paquets dont le nom commence par « `drweb` » (préfixe du nom standard pour les produits Dr.Web). Notez que cette commande supprime tous les paquets portant ce préfixe, et non seulement ceux de Dr.Web pour Linux.
3. La troisième commande supprime tous les paquets qui ont été automatiquement installés pour résoudre les dépendances d'autres paquets et ne sont plus nécessaires (par exemple, suite à la suppression du paquet initial). Notez que cette commande supprime tous les paquets qui ne sont pas utilisés, et non seulement ceux de Dr.Web pour Linux.

Vous pouvez également utiliser des gestionnaires alternatifs (par exemple Synaptic ou aptitude) pour supprimer les paquets.

ALT Linux, PCLinuxOS (apt-rpm)

Dans ce cas, la suppression de Dr.Web pour Linux est la même que sur les OS Debian, Ubuntu (voir ci-dessus).

Vous pouvez également utiliser des gestionnaires alternatifs (par exemple Synaptic ou aptitude) pour supprimer les paquets.

Sous Alt 8 СП, les messages du type suivant peuvent s'afficher dans la console :

```
/etc/init.d/drweb-configd : Fichier ou répertoire inexistant
```

Ces messages n'influencent pas le fonctionnement du système. La procédure de suppression s'effectue correctement.

Mageia, OpenMandriva Lx (urpme)

Pour supprimer Dr.Web pour Linux, entrez la commande suivante :

```
# urpme drweb-workstations
```

Pour supprimer automatiquement tous les paquets qui ne sont plus utilisés, entrez la commande suivante :

```
# urpme --auto-orphans drweb-workstations
```

Veuillez noter quelques aspects spécifiques de la suppression avec la commande `urpme` :

1. La première commande supprime uniquement le métapaquet `drweb-workstations` ; tous les autres paquets qui pourraient être installés automatiquement pour résoudre les dépendances restent dans le système.
2. La seconde commande supprime le paquet racine de `drweb-workstations` et tous les paquets qui ont été automatiquement installés pour résoudre les dépendances d'autres paquets et qui ne sont plus nécessaires (par exemple, suite à la suppression du paquet initial). Notez que cette commande supprime tous les paquets qui ne sont pas utilisés, et non seulement ceux de Dr.Web pour Linux.

Vous pouvez également utiliser des gestionnaires alternatifs (par exemple rpmdrake) pour supprimer les paquets.

Red Hat Enterprise Linux, Fedora, CentOS (yum, dnf)

Pour supprimer tous les paquets installés de Dr.Web, entrez la commande suivante (dans certains systèmes d'exploitation, le symbole '`*`' doit être évité : '`\*`') :

```
# yum remove drweb*
```

Dans l'OS Fedora, depuis la version 22, il est recommandé d'utiliser le gestionnaire `dnf` au lieu du gestionnaire `yum`, par exemple :

```
# dnf remove drweb*
```

Veuillez noter quelques aspects spécifiques de la suppression avec la commande `yum` (`dnf`) :

La commande indiquée supprime tous les paquets dont le nom commence par « `drweb` » (préfixe du nom standard pour les produits Dr.Web). Notez que cette commande supprime tous les paquets portant ce préfixe, et non seulement ceux de Dr.Web pour Linux.

Vous pouvez également utiliser des gestionnaires alternatifs (par exemple PackageKit ou Yumex) pour supprimer les paquets.

SUSE Linux (zypper)

Pour supprimer Dr.Web pour Linux, entrez la commande suivante :

```
# zypper remove drweb-workstations
```

Pour supprimer tous les paquets installés de Dr.Web, entrez la commande suivante (dans certains systèmes d'exploitation, le symbole '*' doit être évité : '*') :

```
# zypper remove drweb*
```

Veuillez noter quelques aspects spécifiques de la suppression avec la commande `zypper` :

1. La première commande supprime uniquement le métapaquet `drweb-workstations` ; tous les autres paquets qui pourraient être installés automatiquement pour résoudre les dépendances restent dans le système.
2. La deuxième commande supprime tous les paquets dont le nom commence par « `drweb` » (préfixe du nom standard pour les produits Dr.Web). Notez que cette commande supprime tous les paquets portant ce préfixe, et non seulement ceux de Dr.Web pour Linux.

Vous pouvez également utiliser des gestionnaires alternatifs (par exemple YaST) pour supprimer les paquets.

Avancé

Emplacement des fichiers de Dr.Web pour Linux

Après l'installation de Dr.Web pour Linux, ses fichiers résident dans les répertoires `/opt`, `/etc`, et `/var` du système de fichiers.

La structure des répertoires utilisés se présente comme suit :

Répertoire	Contenu
`/opt/drweb.com`	Fichiers exécutables des composants et bibliothèques de base requis pour le fonctionnement de Dr.Web pour Linux.
`/etc/opt/drweb.com`	Fichiers contenant les paramètres de composants (par défaut) et fichier clé de licence requis pour le fonctionnement de Dr.Web pour Linux en mode standalone.
`/var/opt/drweb.com`	Bases de données virales, moteur antivirus, fichiers temporaires et bibliothèques additionnelles requis pour le fonctionnement de Dr.Web pour Linux.

Installation et suppression personnalisées des composants

Si nécessaire, vous pouvez effectuer l'installation et la suppression personnalisées de certains composants de Dr.Web pour Linux en installant ou en supprimant les paquets correspondants. L'installation et la suppression personnalisées doivent s'effectuer de la même façon que l'installation de Dr.Web pour Linux.

Pour réinstaller un certain composant, vous pouvez tout d'abord le supprimer et, ensuite, l'installer de nouveau.

Installation et suppression personnalisées des composants de Dr.Web pour Linux :

- installé depuis le référentiel ;
- installé depuis le paquet universel.

1. Installation et suppression des composants de Dr.Web pour Linux installé depuis le référentiel

Si Dr.Web pour Linux n'a pas été installé depuis le référentiel, pour installer ou supprimer un composant, utilisez la commande correspondante du gestionnaire de paquets utilisé dans votre OS. Par exemple :

1. Pour supprimer le composant SpIDer Gate (le paquet `drweb-gated`) de Dr.Web pour Linux installé dans l'OS CentOS, utilisez la commande :

```
# yum remove drweb-gated
```

2. Pour ajouter le composant SpIDer Gate (le paquet `drweb-gated`) dans Dr.Web pour Linux installé dans l'OS Ubuntu Linux, utilisez la commande :

```
# apt-get install drweb-gated
```

   Si cela est nécessaire, consultez l'aide du gestionnaire de paquets, utilisé dans votre OS.

2. Installation et suppression des composants de Dr.Web pour Linux installé depuis le paquet universel

Si Dr.Web pour Linux a été installé depuis le paquet universel et que vous voulez ajouter ou réinstaller le paquet d'un certain composant, il vous faut le fichier d'installation (avec l'extension `.run`) depuis lequel Dr.Web pour Linux a été installé. Si vous n'avez pas sauvegardé ce fichier, téléchargez-le sur le site de Doctor Web.

Décompression du fichier d'installation

Au lancement du fichier run, vous pouvez utiliser les paramètres suivants de la ligne de commande :

`--noexec` : au lieu de lancer l'installation, décompressez tout simplement les fichiers d'installation de Dr.Web pour Linux. Les fichiers seront décompressés dans le répertoire indiqué dans le variable système `TMPDIR` (d'habitude, c'est le répertoire `/tmp`).

`--keep` : ne pas supprimer les fichiers d'installation de Dr.Web pour Linux et le journal d'installation à la fin de l'installation.

`--target` <*répertoire*> : décompresser les fichiers d'installation de Dr.Web pour Linux dans le répertoire indiqué <*répertoire*>.

Vous pouvez consulter la liste complète des paramètres de la ligne de commande qui peuvent être utilisés pour le fichier d'installation, en exécutant la commande :

```
$ ./<nom_du_fichier>.run --help
```

Pour l'installation sélective des composants de Dr.Web pour Linux, accédez au répertoire contenant les fichiers de paquets décompressés de Dr.Web pour Linux. Si ce répertoire n'est pas présent, exécutez la commande :

```
$ ./<nom_du_fichier>.run --noexec --target <répertoire>
```

Alors, le répertoire <*nom_du_fichier*>, contenant des fichiers de paquets décompressés de Dr.Web pour Linux apparaît dans le répertoire <*répertoire*>.

Installation personnalisée de composants

Le fichier d'installation run contient les paquets de tous les composants dont le logiciel Dr.Web pour Linux est composé (au format RPM), ainsi que les fichiers auxiliaires. Les fichiers de chaque composant ont l'aspect :

```
<nom_du_composant>_<version>~linux_<plateforme>.rpm
```

où <*version*> est la ligne qui contient la version et la date de sortie du paquet et <*plateforme*> est la ligne indiquant le type de plateforme à laquelle Dr.Web pour Linux est destiné. Les noms de tous les paquets contenant les composants de Dr.Web pour Linux commencent par le préfixe « drweb ».

Le gestionnaire de paquets `zypper` est inclus dans l'ensemble d'installation pour l'installation des paquets. Pour l'installation personnalisée, utilisez le script `installpkg.sh`. Pour cela, décompressez d'avance le contenu du paquet d'installation dans le répertoire de votre choix.

L'installation de paquets peut être effectuée uniquement par un utilisateur possédant les privilèges de super-utilisateur (utilisateur *root*). Pour élever les privilèges, utilisez la commande de changement d'utilisateur `su` ou la commande d'exécution du nom d'un autre utilisateur`sudo`.

Pour installer le paquet d'un composant, il est nécessaire d'ouvrir le répertoire contenant d'ensemble d'installation décompressé et d'exécuter dans la console (ou dans l'émulateur de console qui est un terminal pour le mode graphique) la commande :

```
# ./scripts/installpkg.sh <nom_du_paquet>
```

Par exemple :

```
# ./scripts/installpkg.sh drweb-gated
```

S'il faut lancer le programme d'installation de Dr.Web pour Linux entier, il faut lancer le script d'installation automatique en exécutant la commande :

```
$ ./install.sh
```

De plus, vous pouvez installer tous les paquets de Dr.Web pour Linux (y compris pour installer les composants manquants ou les composants supprimés par erreur) en lançant l'installation du metapaquet racine du produit :

```
# ./scripts/installpkg.sh drweb-workstations
```

Suppression personnalisée des composants

Pour la suppression personnalisée du paquet d'un composant, utilisez la commande de suppression correspondante du gestionnaire de paquets de votre système d'exploitation, si votre OS emploie le format de paquets RPM :

- Dans Red Hat Enterprise Linux et CentOS, utilisez la commande `yum remove` <*nom_du_paquet*>
- Dans Fedora, utilisez la commande `yum remove` <*nom_du_paquet*> ou `dnf remove` <*nom_du_paquet*>
- Dans SUSE Linux, utilisez la commande `zypper remove` <*nom_du_paquet*>
- Dans Mageia, OpenMandriva Lx , utilisez la commande `urpme` <*nom_du_paquet*>
- Dans Alt Linux et PCLinuxOS, utilisez la commande `apt-get remove` <*nom_du_paquet*>.

Par exemple, (pour Red Hat Enterprise Linux) :

```
# yum remove drweb-gated
```

Si votre OS emploie les paquets au format DEB, pour la suppression personnalisée, utilisez le gestionnaire de paquets `zypper` installé automatiquement lors de l'installation de Dr.Web pour Linux. Pour ce faire, allez dans le répertoire `/opt/drweb.com/bin` et exécutez la commande suivante :

```
# ./zypper rm <nom_du_paquet>
```

Par exemple :

```
# ./zypper rm drweb-gated
```

Si vous voulez supprimer Dr.Web pour Linux tout entier, lancez le script de suppression automatique en exécutant la commande suivante :

```
# ./uninst.sh
```

Pour réinstaller un certain composant, vous pouvez tout d'abord le supprimer et puis installer en lançant l'installation personnalisée ou complète depuis l'ensemble d'installation.

Configuration des sous-systèmes de sécurité

Le sous-système de la sécurité supplémentaire SELinux au sein de l'OS et l'utilisation des systèmes de contrôle d'accès obligatoire (à la différence du modèle classique discrétionnaire UNIX) comme PARSEC peuvent provoquer des problèmes de fonctionnement de Dr.Web pour Linux avec les paramètres par défaut. Dans ce cas, pour assurer le fonctionnement correct de Dr.Web pour Linux, il faut apporter des modifications supplémentaires dans les paramètres du sous-système de sécurité et/ou dans les paramètres de Dr.Web pour Linux.

Cette rubrique est consacrée aux paramètres assurant un fonctionnement correct de Dr.Web pour Linux :

- Configuration des politiques de sécurité SELinux.
- Configuration des autorisations pour le système de contrôle d'accès obligatoire PARSEC (OS Astra Linux).
- Configuration du lancement en mode ELF (environnement logiciel fermé) (OS Astra Linux SE en versions 1.6 et 1.7).

La configuration des autorisations du système de contrôle d'accès obligatoire PARSEC pour Dr.Web pour Linux permet aux composants de l'antivirus de contourner les restrictions des politiques de sécurité spécifiées et d'obtenir l'accès aux fichiers des différents niveaux de privilèges.

Notez que même si vous n'avez pas configuré les autorisations du système de contrôle d'accès obligatoire PARSEC pour les composants de Dr.Web pour Linux, vous pouvez lancer l'analyse des fichiers en utilisant l'interface graphique Dr.Web pour Linux en mode de copie autonome. Pour ce faire, exécutez la commande `drweb-gui` avec le paramètre `--Autonomous`. Vous pouvez également lancer l'analyse des fichiers depuis la ligne de commande. Pour ce faire, exécutez la commande `drweb-ctl` avec le même paramètre (`--Autonomous`). Dans ce cas, il sera possible d'analyser les fichiers, pour accéder auxquels il faut avoir un niveau égal ou inférieur à celui de l'utilisateur qui a lancé l'analyse. Ce mode a les particularités suivantes :

- Pour le lancement en mode de copie autonome, le fichier clé valide est requis, la gestion par le serveur de protection centralisée n'est pas supportée (il y a une possibilité d'installer le fichier clé exporté du serveur de protection centralisée). Dans ce cas, même si Dr.Web pour Linux est connecté au serveur de protection centralisée, la copie autonome *n'avertit pas* le serveur de protection centralisée des menaces détectées lors de l'analyse en mode de copie autonome.
- Tous les composants auxiliaires qui servent la copie autonome seront lancés de nom de l'utilisateur courant et fonctionneront avec le fichier de configuration formé spécialement.
- Tous les fichiers temporaires et les sockets UNIX utilisés pour l'interaction des composants seront crées uniquement dans le répertoire portant un nom unique créé par la copie autonome lancée dans le répertoire des fichiers temporaires (indiqué dans la variable système d'environnement `TMPDIR`).

- La copie autonome lancée de l'interface graphique de gestion *ne lance pas* les moniteurs SpIDer Guard et SpIDer Gate. Ce sont seulement le fonctions d'analyse de fichiers et de gestion de quarantaine prises en charge par le Scanner qui sont en marche.
- Les chemins vers les fichiers de bases virales, le moteur antivirus et les fichiers exécutables des composants de service sont spécifiés par défaut, ou ils sont tirés des variables d'environnement spéciales.
- Le nombre des copies autonomes fonctionnant en même temps n'est pas limité.
- Si la copie lancée d'une manière autonome arrête le fonctionnement, l'ensemble des composants de service qui la sert est également arrêté.

Configuration des politiques de sécurité SELinux

Si la distribution utilisée de UNIX inclut le sous-systeme de sécurité SELinux (*ecurity-Enhanced UNIX — UNIX avec la sécurité améliorée*), vous devrez probablement configurer les politiques de sécurité de SELinux pour assurer un fonctionnement correct des composants de l'application (par exemple, du moteur de scan) après leur installation.

1. Problèmes d'installation du paquet universel

Si SELinux est activé sous forme d'un paquet universel, l'installation depuis le fichier d'installation (`.run`) peut échouer parce que la tentative de création de l'utilisateur *drweb*, sous lequel les composants de Dr.Web pour Linux fonctionnent, peut être bloquée.

Si la tentative d'installer Dr.Web pour Linux depuis le fichier exécutable (`.run`) a échoué suite à l'impossibilité de créer l'utilisateur *drweb*, vérifiez le mode de fonctionnement SELinux. Pour ce faire, exécutez la commande `getenforce`. Cette commande affiche sur l'écran le mode actuel de la protection :

- *Permissive* : la protection est active mais une stratégie permissive est mise en place : les actions qui violent la politique de sécurité ne sont pas rejetées mais les informations sur ces actions sont journalisées.
- *Enforced* : la protection est active et une stratégie restrictive est mise en place : les actions qui violent les politiques de sécurité sont bloquées et les informations sur ces actions sont journalisées.
- *Désactivé* : SELinux est installé mais non actif.

Si SELinux opère en mode *Enforced*, passez en mode *Permissive* pour le délai d'installation. Pour cela, exécutez la commande :

```
# setenforce 0
```

qui met SELinux temporairement (jusqu'au prochain redémarrage) en mode *Permissive*.

Notez que quel que soit le mode opératoire autorisé via la commande `setenforce`, le redémarrage du système d'exploitation replace SELinux dans le mode opératoire indiqué dans les paramètres de SELinux (le fichier des paramètres de SELinux se trouve généralement dans le répertoire `/etc/selinux`).

Après l'installation réussie de Dr.Web pour Linux depuis un fichier d'installation, activez de nouveau le mode *Enforced* avant de lancer et activer le produit. Pour ce faire, exécutez la commande :

```
# setenforce 1
```

2. Problèmes de fonctionnement de Dr.Web pour Linux

Dans certains cas, lorsque SELinux est activé, certains modules auxiliaires de Dr.Web pour Linux (par exemple `drweb-se` et `drweb-filecheck` utilisés par le Scanner et SpIDer Guard) ne peuvent pas démarrer. Si c'est le cas, le scan des objets et la surveillance du système de fichiers deviennent indisponibles. Lorsqu'un module auxiliaire échoue à démarrer, la fenêtre principale de Dr.Web pour Linux affiche des messages sur les erreurs *119 et 120 et des informations sur ces erreurs sont également enregistrées dans le journal système* `syslog` (d'habitude placé dans le répertoire `/var/log/`).

Les messages de SELinux sont enregistrés dans le journal système d'audit. En général, lorsque le daemon audit est utilisé dans le système, le journal audit se trouve dans le fichier `/var/log/audit/audit.log`. Sinon, les messages sur les opérations bloquées sont sauvegardés dans le fichier journal général `/var/log/messages` ou `/var/log/syslog`.

S'il est déterminé que les modules auxiliaires ne fonctionnent pas car ils sont bloqués par SELinux, compilez pour eux des politiques de sécurité spéciales.

Certaines distributions de UNIX ne fournissent pas les utilitaires mentionnés ci-dessous. Si c'est le cas, vous pouvez avoir besoin de paquets supplémentaires pour ces utilitaires.

Pour créer les politiques requises :

1. Créez un nouveau fichier avec le code source de la politique SELinux (fichier avec l'extension `.te`). Ce fichier définit les restrictions appliquées au module. Le code source de la politique peut être indiqué d'une des façons suivantes :
   1) En utilisant l'utilitaire `audit2allow` qui est la méthode la plus simple. L'utilitaire génère des règles permissives depuis les messages de déni d'accès dans les fichiers de journaux système. Vous pouvez paramétrer de rechercher les messages automatiquement ou indiquer un chemin vers le fichier de journal manuellement.

      Notez que vous pouvez utiliser cette méthode uniquement si les composants de Dr.Web pour Linux ont violé les politiques de sécurité de SELinux et que ces événements sont

enregistrés dans le fichier de journal d'audit. Si ce n'est pas le cas, attendez qu'un incident survienne lors du fonctionnement de Dr.Web pour Linux ou créez de force des politiques permissives en utilisant l'utilitaire `policygentool` (voir ci-dessous).

L'utilitaire `audit2allow` réside dans le paquet `policycoreutils-python` ou `policycoreutils-devel` (pour les systèmes d'exploitation Red Hat Enterprise Linux, CentOS, Fedora en fonction de la version) ou dans le paquet `python-sepolgen` (pour les OS Debian, Ubuntu).

Exemple de l'utilisation de `audit2allow` :

```
# grep drweb-se.real /var/log/audit/audit.log | audit2allow -M drweb-se
```

Dans l'exemple donné, l'utilitaire `audit2allow` effectue une recherche dans le fichier `audit.log` pour trouver les messages de déni d'accès pour le module `drweb-se`.

Les deux fichiers suivants sont créés : le fichier source de la politique `drweb-se.te` et le module de la politique `drweb-se.pp` prêt à l'installation.

Si aucun incident de violation de la sécurité n'est trouvé dans le journal système, l'utilitaire remonte un message d'erreur.

Dans la plupart des cas, vous n'avez pas besoin de modifier le fichier de la politique créé par l'utilitaire `audit2allow`. Par conséquent, il est recommandé d'aller à l'étape 4 pour installer le module de la politique `drweb-se.pp`. Notez que l'utilitaire `audit2allow` affiche l'appel à la commande `semodule` en tant que résultat de son fonctionnement. En copiant ce qui s'affiche en ligne de commande et en l'exécutant, vous terminez l'étape 4. Allez à l'étape 2 seulement si vous souhaitez modifier les politiques de sécurité qui ont été automatiquement générées pour les composants de Dr.Web pour Linux.

2) En utilisant l'utilitaire `policygentool`. Pour cela, indiquez le nom du module avec lequel vous souhaitez configurer et le chemin complet vers le fichier exécutable.

Notez que l'utilitaire `policygentool`, inclus au paquet `selinux-policy` pour les OS Red Hat Enterprise Linux et CentOS peut ne pas fonctionner correctement. Si c'est le cas, utilisez l'utilitaire `audit2allow`.

Exemple de création de politique via `policygentool` :

- Pour `drweb-se` :

```
# policygentool drweb-se /opt/drweb.com/bin/drweb-se.real
```

- Pour `drweb-filecheck` :

```
# policygentool drweb-filecheck /opt/drweb.com/bin/drweb-filecheck.real
```

Vous serez invité à indiquer plusieurs caractéristiques du domaine commun. Ensuite, trois fichiers déterminant la politique seront créés pour chacun des modules :

<module_name>.te, *<module_name>.fc* et *<module_name>.if*.

2. Si nécessaire, modifiez le fichier source de la politique généré *<nom_de_module>.te* puis utilisez l'utilitaire `checkmodule` pour créer un mappage binaire du fichier source de la politique locale (fichier `.mod`).

   Notez que pour le fonctionnement réussi de la commande, le paquet `checkpolicy` doit être installé dans le système.

   Exemple d'utilisation :

   ```
   # checkmodule -M -m -o drweb-se.mod drweb-se.te
   ```

3. Créez un module de politique à installer (fichier avec l'extension `.pp`) avec l'utilitaire `semodule_package`.

   Exemple :

   ```
   # semodule_package -o drweb-se.pp -m drweb-se.mod
   ```

4. Pour installer le module de politique créé, utilisez l'utilitaire `semodule`.

   Exemple :

   ```
   # semodule -i drweb-se.pp
   ```

Pour en savoir plus sur le fonctionnement et la configuration de SELinux, consultez la documentation sur la distribution de UNIX utilisée.

Configuration des autorisations de PARSEC

Dans les distributions Linux possédant le sous-système de sécurité PARSEC, l'accès d'applications aux fichiers dépend du niveau de privilèges. C'est pourquoi SpIDer Guard peut intercepter les événements d'accès aux fichiers dans la mesure où son niveau de privilèges le permet.

De plus, si l'utilisateur bénéficie du niveau de privilèges différent de zéro, l'interface d'utilisateur de Dr.Web pour Linux ne peut pas interagir avec SpIDer Guard et les composants service de l'antivirus fonctionnant aux autres niveaux de privilèges. Il se peut que l'utilisateur ne soit pas capable d'accéder à la quarantaine consolidée.

Si l'OS utilise PARSEC et qu'il y a des comptes d'utilisateurs fonctionnant aux niveaux de privilèges différents de zéro, il faut effectuer une configuration spéciale de Dr.Web pour Linux pour assurer l'interaction de ses composants lancés aux niveaux de privilèges différents.

Cette rubrique est consacrée aux paramètres de PARSEC assurant un fonctionnement correct de Dr.Web pour Linux :

- Configuration de l'interaction des composants lancés aux niveaux différents de privilèges.
- Configuration du lancement automatique de composants de Dr.Web pour Linux au niveau de privilèges de l'utilisateur.

- Configuration de SpIDer Guard pour intercepter les événements d'accès aux fichiers.

> Ces opérations peuvent être effectuées uniquement par un utilisateur possédant les privilèges de super-utilisateur (utilisateur *root*). Pour élever les privilèges, utilisez la commande `su` pour changer d'utilisateur ou la commande d'exécution au nom d'un autre utilisateur `sudo` .

Configuration de l'interaction des composants lancés aux niveaux différents de privilèges

Sous Astra Linux SE en version 1.6

Modifiez le fichier système `/etc/parsec/privsock.conf` en dotant le démon de gestion de la configuration Dr.Web pour Linux (`drweb-configd`) du droit d'utiliser le mécanisme *privsock*. `drweb-configd` : le composant service de Dr.Web pour Linux qui assure l'interaction de tous les composants antivirus. Le mécanisme *privsock* est destiné à assurer le fonctionnement des services réseau système qui ne traitent pas les informations avec le contexte obligatoire mais qui interagissent avec les processus fonctionnant dans le contexte obligatoire du sujet d'accès. Pour cela, faites le suivant :

1. Ouvrez le fichier `/etc/parsec/privsock.conf` dans un éditeur de texte. Ajoutez les lignes indiquées dans ce fichier :

```
/opt/drweb.com/bin/drweb-configd
/opt/drweb.com/bin/drweb-configd.real
```

2. Enregistrez le fichier et redémarrez le système.

Sous Astra Linux SE en version 1.5 ou antérieure

Modifiez le script de lancement du démon de gestion de la configuration de Dr.Web pour Linux (`drweb-configd`). Pour ce faire, faites le suivant :

1. Connectez-vous sous le compte ayant le niveau zéro de privilèges.
2. Ouvrez le fichier de script `/etc/init.d/drweb-configd` dans un éditeur de texte.
3. Trouvez dans ce fichier la description de la fonction `start_daemon()` et remplacez la ligne

```
"$DAEMON" -d -p "$PIDFILE" >/dev/null 2>&1
```

   par la ligne

```
execaps -c 0x100 -- "$DAEMON" -d -p "$PIDFILE" >/dev/null 2>&1
```

4. Dans certains OS (par exemple, Astra Linux SE 1.3), il peut être nécessaire d'indiquer la dépendance du lancement du composant à l'égard du sous-système PARSEC. Dans ce cas, il faut également modifier la ligne suivante dans ce fichier :

```
# Required-Start: $local_fs $network
```

Modifiez cette ligne de la manière suivante :

```
# Required-Start: $local_fs $network parsec
```

5. Enregistrez le fichier modifié et redémarrez le système.

Configuration du lancement automatique de composants au niveau de privilèges de l'utilisateur

Pour que les composants de Dr.Web pour Linux, avec lesquels l'utilisateur interagit, soient disponibles dans son environnement (en cas de travail au niveau de privilèges différent de zéro), modifiez les fichiers de paramètres de PAM pour le lancement automatique des composants nécessaires de Dr.Web pour Linux au début de la session et leur arrêt à la fin de la session (le module PAM spécial `pam_drweb_session.so` est utilisé. Ce module est crée par Doctor Web et il lance le composant intermédiaire `drweb-session` reliant les copies locales des composants lancés dans l'environnement de l'utilisateur aux composants fonctionnant au niveau de privilèges différent de zéro et démarrant automatiquement lors du chargement de l'OS).

Pour modifier les paramètres de PAM, vous pouvez utiliser l'utilitaire de configuration `drweb-configure` inclus à Dr.Web pour Linux (recommandé) ou modifier les fichiers de configuration nécessaires manuellement.

1. Utilisation de l'utilitaire drweb-configure

Pour faciliter la configuration de certains paramètres compliqués assurant le fonctionnement de Dr.Web pour Linux, on a créé l'utilitaire spécial `drweb-configure`.

1. Pour activer ou désactiver le lancement automatique des composants nécessaires de Dr.Web pour Linux dans l'entourage de l'utilisateur lors de son travail au niveau de privilèges différent de zéro, utilisez la commande suivante :

   ```
   $ sudo drweb-configure session <mode>
   ```

   où <*mode*> peut prendre l'une des valeurs suivantes :

   - `enable` : activer le mode de lancement automatique des composants nécessaires au cours de la session de l'utilisateur à son niveau de privilèges.
   - `disable` : désactiver le mode de lancement automatique des composants nécessaires au cours de la session de l'utilisateur au niveau de privilèges (dans ce cas, les fonctions de Dr.Web pour Linux seront indisponibles).
2. Redémarrez le système.

Pour avoir l'aide d'utilisation de `drweb-configure` pour la configuration de PAM, utilisez la commande :

```
$ drweb-configure --help session
```

2. Modification manuelle des fichiers de la configuration PAM

Pour Astra Linux et d'autres distributions utilisant le module PAM pam_parsec_mac.so

1. Pour modifier les paramètres PAM, il faut éditer les fichiers de configuration stockés dans le dossier `/etc/pam.d` dans lesquels le module PAM`pam_parsec_mac.so` est appelé. Pour obtenir la liste complète de tels fichiers, exécutez la commande suivante :

   ```
   # grep -R pam_parsec_mac.so /etc/pam.d
   ```

   Dans chaque fichier de la liste ajoutez les entrées suivantes de type *session*:

   - Avant le premier enregistrement de type *session* :

   ```
   session optional pam_drweb_session.so type=close
   ```

   - Après le dernier enregistrement de type *session* :

   ```
   session optional pam_drweb_session.so type=open
   ```

2. Enregistrez les fichier modifiés.
3. Créez un lien symbolique vers le fichier `pam_drweb_session.so` du répertoire système contenant des modules PAM. Le fichier `pam_drweb_session.so` se trouve dans le répertoire de bibliothèques Dr.Web pour Linux `/opt/drweb.com/lib/` (par exemple, pour les OS 64-bits — dans le répertoire `/opt/drweb.com/lib/x86_64-linux-gnu/pam/`).
4. Redémarrez le système.

Pour Alt 8 SP et d'autres distributions utilisant le module pam_parsec_mac.so

1. Pour modifier les paramètres PAM, il faut éditer les fichiers de configuration stockés dans le répertoire `/etc/pam.d` dans lesquels le module PAM `pam_namespace.so` est appelé. Pour obtenir la liste complète de tels fichiers, exécutez la commande suivante :

   ```
   # grep -R pam_namespace.so /etc/pam.d
   ```

2. Dans chaque fichier ajoutez les mêmes entrées de type *session* que pour les distributions utilisant le module `pam_parsec_mac.so` (voir le paragraphe précédent).

Configuration de SpIDer Guard pour intercepter les événements d'accès aux fichiers

Pour accorder au moniteur de fichiers SpIDer Guard, la possibilité de détecter l'accès aux fichiers ayant tout niveau de privilèges d'accès, il est nécessaire de mettre SpIDer Guard en mode *Fanotify*.

Pour mettre SpIDer Guard en mode *Fanotify*, exécutez la commande suivante :

```
# drweb-ctl cfset LinuxSpider.Mode Fanotify
```

Pour plus d'informations, exécutez la commande suivante :

```
$ man drweb-spider
```

Configuration du lancement en mode ELF (Astra Linux SE en versions 1.6 et 1.7)

L'OS Astra Linux SE prend en charge un mode particulier d'*environnement logiciel fermé* (ELF) dans lequel sont lancées les applications dont les fichiers exécutables sont signés par la signature numérique du développeur dont la clé publique est ajoutée dans la liste de clés de confiance de l'OS.

Par défaut, les composants de Dr.Web pour Linux fournis pour être exécutés dans l'environnement Astra Linux SE sont signés par la signature numérique de la société Doctor Web et la clé publique de cette signature est automatiquement ajoutées dans la liste de confiance lors de l'installation du logiciel. C'est pourquoi, Dr.Web pour Linux doit fonctionner correctement lors de l'activation du mode d'environnement logiciel fermé sous Astra Linux SE en version 1.5 ou antérieure.

Pourtant, vu que le mécanisme de signature a été modifié dans la version 1.6 de Astra Linux SE, il faut effectuer les configurations préalables du système pour assurer le lancement de Dr.Web pour Linux en mode d'environnement logiciel fermé sous les OS en versions 1.6 et 1.7.

Configuration d'Astra Linux SE en version 1.6. et 1.7 pour le lancement de Dr.Web pour Linux en mode ELF

1. Installez le paquet `astra-digsig-oldkeys` depuis le disque d'installation de l'OS s'il n'est pas encore installé.

2. Placez la clé publique de Doctor Web dans le répertoire `/etc/digsig/keys/legacy/keys` (si le répertoire n'existe pas, il faut le créer) :

```
# cp /opt/drweb.com/share/doc/digsig.gost.gpg /etc/digsig/keys/legacy/keys
```

3. Exécutez la commande suivante :

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

4. Redémarrez le système.

Mise en marche

1. Effectuez l'activation de Dr.Web pour Linux.
2. Vérifiez les capacités de fonctionnement.
3. Spécifiez le mode de surveillance de fichiers.
4. Déterminez les exclusions, s'il y en a.

Enregistrement et activation

Dans cette section :

- Achat et enregistrement de licences.
- Activation de Dr.Web pour Linux :
  - Période de démonstration.
  - Installation du fichier clé.
  - Connexion au serveur de protection centralisée.
- Enregistrement réitéré.

Achat et enregistrement de licences

Après l'achat d'une licence, l'utilisateur peut bénéficier des mises à jour des bases de données virales et des composants qui sont régulièrement téléchargées depuis les serveurs de mises à jour de Doctor Web et de l'assistance technique fournie par Doctor Web ou ses partenaires.

Vous pouvez acheter n'importe quel produit Dr.Web ainsi qu'obtenir un numéro de série pour un produit via la boutique en ligne https://estore.drweb.com/ ou auprès de nos partenaires à l'adresse https://partners.drweb.com/. Pour en savoir plus sur les options possibles de licence, visitez le site officiel de Doctor Web à la page https://license.drweb.com/.

L'enregistrement de la licence garantit que vous êtes un utilisateur légal de Dr.Web pour Linux et active ses fonctionnalités, y compris la mise à jour des bases de données virales. Il est recommandé d'enregistrer le produit et d'activer la licence juste après l'installation.

Activation de Dr.Web pour Linux

La licence achetée peut être activée d'une des façons suivantes :

- Via l'Assistant d'enregistrement intégré dans le Gestionnaire de licences.
- Sur le site officiel de Doctor Web à la page https://products.drweb.com/register/.

Durant l'activation ou le renouvellement de la licence, il est requis d'entrer le numéro de série. Le numéro de série peut être fourni avec Dr.Web pour Linux ou par email lors de l'achat ou du renouvellement de la licence en ligne.

Si vous avez utilisé Dr.Web pour Linux par le passé, vous pouvez bénéficier d'une extension de votre nouvelle licence de 150 jours. Pour activer le bonus, entrez votre numéro de série enregistré ou fournissez le fichier clé de licence. Attention, si vous choisissez le renouvellement de licence mais que vous ne fournissez pas les données de la licence précédente, la durée de validité de la nouvelle licence sera amputée de 150 jours.

Si vous possédez plusieurs licences pour utiliser Dr.Web pour Linux sur plusieurs ordinateurs, mais que vous choisissez d'utiliser Dr.Web pour Linux sur un seul ordinateur, vous pouvez l'indiquer et la durée de validité de la licence sera automatiquement étendue.

Période de démonstration

Les utilisateurs des produits Dr.Web peuvent bénéficier de la période de démonstration d'un mois. Vous pouvez l'obtenir dans la fenêtre de l'Assistant d'enregistrement du Gestionnaire de licences sans indiquer des données personnelles.

L'assistant d'enregistrement du Gestionnaire de licences s'ouvre au premier démarrage de Dr.Web pour Linux (en général, l'assistant d'enregistrement s'ouvre à la fin de l'installation). Vous pouvez démarrer l'enregistrement depuis la fenêtre du Gestionnaire de licences à n'importe quel moment en cliquant sur **Obtenir une nouvelle licence** sur la page contenant les informations sur la licence actuelle.

Pour activer une licence en utilisant le numéro de série, une connexion Internet est requise.

Lorsqu'une période de démonstration ou une licence est activée via le Gestionnaire de licences, le fichier clé (licence ou démo) sera automatiquement généré sur l'ordinateur local dans le dossier cible. En cas d'enregistrement sur le site web, le fichier clé est envoyé par e-mail. Installez-le manuellement.

Si vous n'avez pas la possibilité d'utiliser l'assistant d'enregistrement (par exemple suite à l'absence de l'interface graphique de l'OS), vous pouvez utiliser la commande de gestion de la licence de l'utilitaire de la ligne de commande `drweb-ctl` qui permet d'obtenir automatiquement le fichier clé de licence pour le numéro de série de la licence enregistrée. Vous trouverez la description de l'utilitaire `drweb-ctl` dans le Manuel Utilisateur.

La version complète du Manuel Utilisateur Dr.Web pour Linux est disponible :

- Sur le site de Doctor Web http://download.drweb.com/doc/ (une connexion Internet est requise).
- En version PDF dans le répertoire `/opt/drweb.com/share/doc` (le suffixe du nom du fichier indique la langue du Manuel).

Installation du fichier clé

Si vous possédez un fichier clé correspondant à une licence valide (par exemple, si vous avez obtenu le fichier clé par e-mail ou que vous souhaitez utiliser Dr.Web pour Linux sur un autre ordinateur), vous pouvez activer Dr.Web pour Linux en indiquant le chemin vers le fichier clé. Vous pouvez le faire de la façon suivante :

- Dans le Gestionnaire de licences en cliquant sur **Autres modes d'activation** à la première étape de la procédure d'enregistrement et en indiquant le chemin vers le fichier clé ou l'archive zip qui le contient.
- Manuellement. Pour cela :
  1. Décompressez le fichier clé s'il est dans une archive.
  2. Copiez le fichier dans le répertoire `/etc/opt/drweb.com` et renommez-le en `drweb32.key`, si nécessaire.
  3. Exécutez la commande suivante :

     ```
     # drweb-ctl reload
     ```

     pour appliquer les modifications apportées.

Vous pouvez également utiliser la commande suivante :

```
# drweb-ctl cfset Root.KeyPath <chemin d'accès au fichier clé>
```

Dans ce cas, le fichier clé ne sera pas copié dans le répertoire `/etc/opt/drweb.com` et restera à son emplacement d'origine.

> ⚠ Si le fichier clé n'a pas été copié dans le répertoire `/etc/opt/drweb.com`, l'utilisateur doit s'assurer que le fichier est protégé contre la corruption ou la suppression. Cette méthode d'installation n'est pas recommandée car le fichier clé peut être accidentellement supprimé du système (par exemple, si le répertoire où le fichier clé réside est régulièrement nettoyé). N'oubliez pas que vous pouvez demander de nouveau le fichier clé en cas de perte, mais le nombre de demandes de réception est limité.

Connexion au serveur de protection centralisée

Si le fournisseur de service Internet ou l'administrateur réseau a fourni un fichier contenant les paramètres de connexion au serveur de protection centralisée, vous pouvez activer Dr.Web pour Linux en indiquant le chemin vers ce fichier. Vous pouvez le faire de la façon suivante :

- Dans la fenêtre de configuration du logiciel, dans l'onglet **Mode**, cochez la case **Activer le mode de protection centralisée**, sélectionnez dans la fenêtre qui s'affiche l'élément *Télécharger du fichier*, spécifiez le chemin vers le fichier existant de paramètres de connexion et cliquez sur **Connecter**.

Enregistrement réitéré

Si vous avez perdu le fichier clé mais que la licence n'a pas expiré, vous devez vous enregistrer à nouveau en entrant les données que vous aviez fournies lors du premier enregistrement. Vous pouvez utiliser une adresse email différente. Dans ce cas, le fichier clé de licence sera envoyé sur la nouvelle adresse indiquée.

Le nombre de demandes d'un fichier clé est limité. Un numéro de série ne peut pas être enregistré *plus de 25 fois*. Si le nombre de requêtes dépasse cette limite, le fichier clé ne sera pas délivré. Dans ce cas, contactez le support technique (décrivez votre problème en détails, et indiquez les données que vous avez fournies au moment de l'enregistrement du numéro de série). Le fichier clé de licence sera envoyé par e-mail.

Fichier clé

Le fichier clé est un fichier spécifique conservé sur l'ordinateur local. Il correspond à la licence achetée ou à la version démo activée pour Dr.Web pour Linux. Le fichier clé contient les paramètres d'utilisation de Dr.Web pour Linux conformément à la licence achetée ou la version démo activée.

Le fichier clé comporte l'extension `.key` et est valide s'il répond aux critères suivants :

- La licence ou la version démo n'a pas expiré.
- La version démo ou la licence s'applique à tous les composants antivirus requis par le produit.
- L'intégrité du fichier clé n'a pas été violée.

Si une de ces conditions est violée, le fichier clé de licence devient invalide.

Durant le fonctionnement de Dr.Web pour Linux, le fichier clé doit résider par défaut dans le répertoire `/etc/opt/drweb.com` et avoir le nom `drweb32.key`.

Les composants de Dr.Web pour Linux vérifient régulièrement que le fichier clé est disponible et valide. Le fichier clé comporte une signature digitale afin de prévenir sa modification. Ainsi, un fichier clé modifié devient invalide. Il n'est pas recommandé d'ouvrir le fichier clé dans des traitements de texte afin d'éviter son invalidation accidentelle.

Si aucun fichier clé valide (licence ou démo) n'est trouvé, ou si la licence a expiré, le fonctionnement des composants antivirus est bloqué jusqu'à ce qu'un fichier clé valide soit installé.

Il est recommandé de conserver le fichier clé de licence jusqu'à son expiration, et de l'utiliser pour réinstaller Dr.Web pour Linux ou l'installer sur une autre ordinateur. Dans ce cas, vous devez utiliser le même numéro de série de produit et les mêmes données utilisateur que celles fournies lors de l'enregistrement.

D'habitude, les fichiers clés Dr.Web sont envoyés par e-mail dans des archives zip. L'archive contenant le fichier clé pour activer Dr.Web pour Linux a le nom `agent.zip` (notez que si le message contient *plusieurs* archives, il faut utiliser l'archive `agent.zip`). Dans le gestionnaire d'enregistrement, vous pouvez spécifier le chemin vers l'archive sans l'avoir décompressée. Avant d'installer le fichier clé vous pouvez également décompresser l'archive comme vous le souhaitez, extraire le fichier clé et l'enregistrer dans un répertoire (par exemple, dans le répertoire personnel ou sur un support amovible USB flash).

Fichier de configuration de la connexion

Le fichier de configuration de la connexion est un fichier spécifique qui conserve les paramètres de configuration de la connexion entre Dr.Web pour Linux et le serveur de protection centralisée. Ce fichier est fourni par l'administrateur du réseau antivirus ou le fournisseur de service Internet (si ce dernier fournit le support du service de protection antivirus centralisée).

Vous pouvez utiliser ce fichier pour activer Dr.Web pour Linux au moment de sa connexion avec le serveur de protection centralisée (dans ce cas, vous ne pouvez pas utiliser Dr.Web pour Linux en mode autonome sans acheter une licence supplémentaire).

Tester les capacités de fonctionnement

Le test *EICAR (European Institute for Computer Anti-Virus Research*) permet de tester les performances des programmes antivirus utilisant la méthode de détection par signatures. Ce test a été spécialement conçu par l'organisation éponyme pour que les utilisateurs puissent tester les capacités de détection des outils antivirus nouvellement installés sans compromettre la sécurité de leur ordinateur.

Bien que le programme utilisé pour le test *EICAR* ne soit pas malveillant, il est traité par la plupart des antivirus comme un virus. Au moment de la détection de ce « virus », les produits antivirus Dr.Web affichent l'information suivante : EICAR Test File (NOT a Virus!). D'autres outils antivirus alertent les utilisateurs de la même façon. Le fichier test EICAR est un fichier COM de 68 octets pour MS DOS/MS Windows. Une fois exécuté, il affiche sur l'écran du terminal ou dans l'émulateur de la console le message suivant :

```
EICAR-STANDARD-ANTIVIRUS-TEST-FILE!
```

Le test contient la chaîne de caractères suivante seulement :

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Pour créer votre propre fichier test avec le « virus », vous devez créer un nouveau fichier contenant la ligne susmentionnée.

Si Dr.Web pour Linux fonctionne correctement, le fichier test EICAR est détecté durant le scan du système de fichiers quel que soit le mode de scan, et l'utilisateur est prévenu que la menace EICAR Test File (Not a Virus!) a été détectée.

Exemple de la commande pour tester les performances de Dr.Web pour Linux avec le programme de test EICAR depuis la ligne de commande :

```
$ tail /opt/drweb.com/share/doc/drweb-se/readme.eicar | grep X50 > testfile
&& drweb-ctl scan testfile && rm testfile
```

Cette commande trouve dans le fichier `/opt/drweb.com/share/doc/drweb-se/readme.eicar` (fourni avec Dr.Web pour Linux) la ligne qui représente le corps du programme de test EICAR et l'enregistre dans le fichier `testfile` dans le répertoire actuel. Ensuite elle analyse le fichier reçu et supprime le fichier créé.

Pour réussir ce test, vous devez avoir les droits d'enregistrement dans le répertoire actuel. De plus, assurez-vous que dans ce répertoire il n'y a pas de fichier avec le nom `testfile` (si nécessaire, modifiez le nom du fichier dans la commande).

En cas de détection réussie du virus de test, le message suivant s'affiche sur l'écran :

```
<chemin d'accès au répertoire actuel>/testfile - infected with EICAR Test File (NOT a
Virus!)
```

Si lors de l'analyse, vous recevez un message d'erreur, consultez la description des erreurs connues.

Si le moniteur du système de fichiers SpIDer Guard fonctionne dans le système, le fichier peut être supprimé tout de suite ou déplacé en quarantaine en cas de détection d'une menace (en fonction de la configuration du composant). Dans ce cas, juste après le message sur la détection d'une menace, la commande `rm` notifie l'absence du fichier. Cette situation n'est pas une erreur, elle signale le fonctionnement correct du moniteur.

Modes de surveillance des fichiers

Informations générales

Le moniteur du système de fichiers SpIDer Guard contrôlant l'accès aux fichiers peut utiliser trois modes de surveillance :

- *Standard* (défini par défaut) : surveillance d'accès aux fichiers (création, ouverture, fermeture, lancement d'un fichier). Requête de l'analyse du fichier auquel une tentative d'accès a été effectuée. Si une menace est détectée dans le fichier, des actions de neutralisation peuvent y être appliquées. L'accès des applications au fichier en cours d'analyse n'est pas restreint.

- *Surveillance renforcée des fichiers exécutables* : la surveillance des fichiers non exécutable est la même que dans le mode standard. En cas de tentative d'accès aux fichiers exécutables, SpIDer Guard bloque cette opération jusqu'à l'obtention des résultats de l'analyse pour la présence de menaces ;

  Les fichiers exécutables désignent les fichiers binaires aux formats PE et ELF et les fichiers texte de scripts contenant la préambule « `#!` ».

- *Mode paranoïde* : en cas de tentative d'accès à un fichier, SpIDer Guard bloque cette opération jusqu'à l'obtention des résultats de l'analyse du fichier pour la présence de menaces.

Pendant un temps déterminé, le Scanner enregistre les résultats de l'analyse des fichiers dans un cache spécial. C'est pourquoi en cas d'accès à ce fichier, il ne sera pas rescanné si le cache contient les informations nécessaires. Dans ce cas, le résultat tiré du cache sera utilisé en tant que le résultat de l'analyse. Pourtant, l'utilisation du mode «paranoïde» ralentit le travail lors de l'accès aux fichiers.

Changement de mode de surveillance de fichiers

Les modes de surveillance renforcées avec leur blocage préalable sont disponible uniquement si SpIDer Guard fonctionne en mode `FANOTIFY` et que le noyau de l'OS est compilé avec l'option `CONFIG_FANOTIFY_ACCESS_PERMISSIONS` activée.

Le changement de modes de fonctionnement de SpIDer Guard est effectué avec la commande `cfset` de l'utilitaire `drweb-ctl`.

Le mode de fonctionnement de SpIDer Guard peut être changé uniquement par un utilisateur possédant les droits de super-utilisateur. Pour obtenir les droits de super-utilisateur, utilisez la commande de changement d'utilisateur `su` ou la commande d'exécution au nom d'un autre utilisateur `sudo`.

- Pour mettre SpIDer Guard en mode `FANOTIFY`, exécutez la commande suivante :

```
$ sudo drweb-ctl cfset LinuxSpider.Mode FANOTIFY
```

- Pour changer de mode de surveillance, utilisez la commande suivante :

```
$ sudo drweb-ctl cfset LinuxSpider.BlockBeforeScan <mode>
```

où <*mode*> détermine le mode de blocage :

  - `Off` : l'accès n'est pas bloqué, SpIDer Guard effectue une surveillance en mode standard (pas en mode de blocage) ;
  - `Executables` : l'accès aux fichiers exécutables est bloqué, SpIDer Guard effectue une surveillance renforcée des fichiers exécutables ;

- `All` : l'accès à tous les fichiers est bloqué, SpIDer Guard effectue une surveillance en mode « paranoïde ».

- Pour modifier la durée de validité des résultats de l'analyse de fichiers stockés par le Scanner dans le cache, exécutez la commande suivante :

```
$ sudo drweb-ctl cfset FileCheck.RescanInterval <période>
```

où <*période*> détermine la période de validité des résultats d'analyse précédents se trouvant dans le cache. Valeurs autorisées : de `0s` à `1m` inclusivement. Si vous indiquez une période inférieure à 1 seconde, le fichier sera analysé à chaque appel.

Utilisation de Dr.Web pour Linux

L'utilisateur peut gérer Dr.Web pour Linux en mode graphique à l'aide du composant qui fournit l'interface graphique de gestion ou depuis la ligne de commande (y compris la gestion via les émulateurs de terminal en mode graphique).

- Pour démarrer l'interface graphique de gestion de Dr.Web pour Linux, sélectionnez l'élément **Dr.Web pour Linux** dans le menu système **Annexes** ou entrez la commande suivante dans la ligne de commande du système d'exploitation :

  ```
  $ drweb-gui
  ```

  Dans ce cas, si l'environnement de bureau est disponible, l'interface graphique de gestion de Dr.Web pour Linux démarre. Pour lancer l'analyse au démarrage de l'interface graphique ou pour le lancer en mode de copie autonome, vous pouvez utiliser cette commande avec les arguments.
- Pour en savoir plus sur la gestion de Dr.Web pour Linux depuis la ligne de commande, consultez la rubrique Gestion via la ligne de commande.
- Pour les environnements graphiques du bureau, le lancement du scan de fichiers depuis la barre de tâches (telle que Unity Launcher dans OS Ubuntu) et depuis le gestionnaire graphique de fichiers (tel que Nautilus) est également supporté. De plus, dans la zone de notifications du bureau, un indicateur d'état est affiché. Cet indicateur est utilisé pour afficher les notifications pop-up et pour accéder au menu contextuel de l'application. L'indicateur est affiché par l'agent de notifications qui est lancé automatiquement, ainsi que les autres composants de service de l'application, et ne nécessite aucune intervention manuelle. Pour plus d'informations, consultez la rubrique Intégration avec l'environnement graphique du bureau.
- L'activation du mode de surveillance renforcée des fichiers par le moniteur SpIDer Guard est décrite dans la section Modes de surveillance des fichiers.

Après l'installation de Dr.Web pour Linux par l'un des moyens décrits dans ce manuel, au début de travail, il vous faudra activer la licence, installer un fichier clé si vous en avez un ou connecter Dr.Web pour Linux au serveur de protection centralisée (voir la rubrique Enregistrement et activation). Tant que vous n'aurez pas fait cela, les *fonctionnalités de la protection antivirus seront désactivées.*

Notez que le protocole de messagerie IMAP utilisé, dans la plupart des cas, par les clients de messagerie (tel que Mozilla Thunderbird) pour la réception de messages du serveur de messagerie est un protocole de session. C'est pourquoi, après la modification de fonctionnement du moniteur SpIDer Gate (l'activation du moniteur désactivé, la modification du mode d'analyse des connexions sécurisées), il est nécessaire de redémarrer le client de messagerie pour que le moniteur SpIDer Gate puisse analyser les messages entrants après la modification de son fonctionnement.

Gestion via l'interface graphique

Dans cette section :

- Informations générales.
- Agent de notifications.
- Interface graphique de gestion.

Informations générales

Deux composants sont responsables du fonctionnement de Dr.Web pour Linux dans un environnement de bureau :

- Agent de notifications : composant lancé automatiquement au début de session dans un environnement de bureau. Ce composant affiche les pop-ups informant des événements de Dr.Web pour Linux et l'indicateur de l'état de Dr.Web pour Linux dans la zone de notifications système, ainsi que le menu principal de gestion.
- Interface graphique de Dr.Web pour Linux : composant fonctionnant dans un environnement de bureau graphique et représentant une interface à fenêtre utilisée pour la gestion de Dr.Web pour Linux.

Agent de notifications

L'Agent de notifications est destiné à :

1. L'affichage de l'indicateur de l'état de Dr.Web pour Linux.
2. La gestion des moniteurs et de la mise à jour, le lancement de l'interface graphique de gestion.
3. L'affichage des pop-ups d'événements.
4. Le lancement des scans selon la planification spécifiée.

Interface graphique de gestion

L'interface graphique de Dr.Web pour Linux permet de résoudre les tâches suivantes :

1. Voir le statut du fonctionnement de Dr.Web pour Linux, y compris le statut des bases virales et la durée de validité de la licence.
2. Démarrage et arrêt du moniteur du système de fichiers SpIDer Guard.
3. Démarrage et arrêt du moniteur de connexions réseau SpIDer Gate.
4. Lancer un scan à la demande dans l'un des modes suivants :
   - *Scan rapide* pour analyser les fichiers système et les objets systèmes les plus critiques.
   - *Scan complet* pour analyser tous les fichiers du système.

- *Scan personnalisé* pour analyser uniquement les fichiers et dossiers indiqués par l'utilisateur, ou des objets spécifiques (secteurs d'amorçage des disques, processus actifs).

Vous pouvez également indiquer des fichiers à scanner en sélectionnant des fichiers et dossiers avant le démarrage du scan ou en les *glissant/déposant* de la fenêtre de gestion de fichier vers la page principale (voir ci-dessous) ou vers la page de **Scanner** de la fenêtre de Dr.Web pour Linux.

5. Voir toutes les menaces détectées par Dr.Web pour Linux durant son fonctionnement en mode graphique, y compris les menaces neutralisées et sautées et les objets placés en quarantaine.
6. Voir les objets placés en quarantaine, les supprimer définitivement ou les restaurer.
7. Configurer les paramètres des composants de Dr.Web pour Linux y compris les paramètres suivants :
   - Les actions que le Scanner et SpIDer Guard vont appliquer aux menaces détectées (en fonction de leur type).
   - La liste des fichiers et dossiers qui ne seront pas analysés par le Scanner ou contrôlés par le moniteur du système de fichiers SpIDer Guard.
   - Les listes noires et blanches des sites web et des catégories indésirables des ressources web utilisées par SpIDer Gate et les paramètres d'analyse des fichiers téléchargés depuis Internet ou reçus par e-mail.
   - Planification des tâches de scan du système de fichiers, incluant la périodicité et le type de scan effectué, ainsi que la liste des objets à scanner selon la planification établie.
   - Mode de fonctionnement (connexion au serveur de protection centralisée et déconnexion du serveur).
   - Les paramètres de surveillance de l'activité réseau, y compris l'analyse du trafic chiffré.
   - Autorisation d'utiliser le service Dr.Web Cloud.
8. Gestion de licences (effectuée via le Gestionnaire de licences).
9. Consultation de messages sur l'état du réseau antivirus envoyés par le serveur de protection centralisée (uniquement si Dr.Web pour Linux fonctionne au sein du réseau antivirus et que l'administrateur du réseau antivirus spécifie le paramètre correspondant sur le serveur de protection centralisée).

Pour assurer un fonctionnement correct de Dr.Web pour Linux, il faut que tous ses composants service soient lancés avant le démarrage de Dr.Web pour Linux, sinon, il s'arrête immédiatement après le démarrage après avoir affiché une alerte correspondante. Dans le cadre d'un fonctionnement normal, tous les composants requis sont démarrés automatiquement et ne nécessitent pas l'intervention de l'utilisateur.

Apparence de l'interface graphique de gestion

L'apparence de la fenêtre principale de l'interface graphique de gestion de Dr.Web pour Linux est présentée dans la figure ci-dessous.

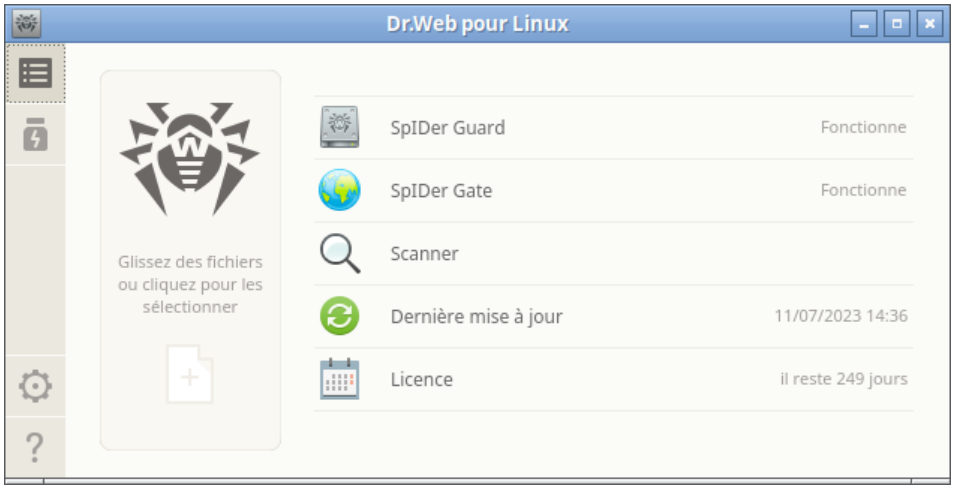

Image 5. Interface graphique de gestion de Dr.Web pour Linux

Le volet gauche de la fenêtre affiche les boutons de navigation qui permettent d'effectuer les actions suivantes.

Bouton	Description
1. Activés en continu	
	Ouvre la page principale où vous pouvez : • Activer ou désactiver le moniteur du système de fichiers SpIDer Guard. • Activer ou désactiver le moniteur de connexions réseau SpIDer Gate. • Lancer le scan des objets du système de fichiers (fichiers, secteurs d'amorçage) et des processus en cours. • Voir le statut de la base virale et la mettre à jour si nécessaire. • Lancer le Gestionnaire de licences pour voir le statut de la licence en cours et enregistrer une nouvelle licence si nécessaire.
	Ouvre la page de gestion de la quarantaine permettant de voir les fichiers mis en quarantaine, ainsi que de les supprimer ou les restaurer.
	Ouvre la fenêtre des paramètres de Dr.Web pour Linux, notamment : • du Scanner des objets du système de fichiers. • du moniteur du système de fichiers SpIDer Guard. • du moniteur de connexions réseau SpIDer Gate. • du lancement des scan selon la planification. De plus, sur cette page, vous pouvez configurer les paramètres du mode protection centralisée.

Bouton	Description
	Fournit un accès aux documents de référence et aux ressources de Doctor Web : • A propos de ce produit. • Manuel utilisateur. • Forum Dr.Web. • Support technique. • Page personnelle de l'utilisateur **Mon Dr.Web**. Tous les liens ouvrent des pages web dans le navigateur installé sur votre ordinateur.
2. Visibles sous certaines conditions	
	Ouvre la page contenant la liste des tâches de scan des fichiers dans laquelle il y a des tâches incomplètes (exécutées). *Le bouton est visible dans le panneau uniquement si au moins une analyse est lancée.*
	Ouvre la page avec les résultats des tâches de scan accomplies Le bouton change de couleur en fonction des résultats du scan : 1) Vert : toutes les tâches de scan ont été accomplies avec succès ; Toutes les menaces détectées, s'il y en avait, ont été neutralisées. 2) Rouge : certaines menaces détectées n'ont pas été neutralisées. 3) Jaune : au moins une des tâches de scan a échoué. *Le bouton est visible dans le panneau uniquement si au moins une analyse a été lancée.*
	Ouvre la page des menaces détectées par le Scanner ou par le moniteur du système de fichiers SpIDer Guard. *Le bouton est visible sur le volet si au moins une menace a été détectée.*
	Le bouton est visible sur le volet uniquement si la page de lancement du scan est ouverte et active. *Lors du passage à une autre page de la fenêtre principale ou lors du lancement du scan, la page de lancement du scan sera fermée automatiquement et le bouton sur le volet ne sera plus visible.*
	Le bouton est visible sur le volet uniquement si la page de gestion de SpIDer Guard est ouverte et active. *Lors du passage à une autre page de la fenêtre principale, la page de gestion de SpIDer Guard sera fermée automatiquement et le bouton sur le volet ne sera plus visible.*
	Le bouton est visible sur le volet uniquement si la page de gestion de SpIDer Gate est ouverte et active. *Lors du passage à une autre page de la fenêtre d'accueil, la page de gestion de SpIDer Gate sera fermée automatiquement et le bouton sur le volet ne sera plus visible.*

Bouton	Description
	Le bouton est visible sur le volet uniquement si la page de gestion des mises à jour est ouverte et active. *Lors du passage à une autre page de la fenêtre principale, la page de gestion des mises à jour sera fermée automatiquement et le bouton sur le volet ne sera plus visible.*
	Le bouton est visible sur le volet uniquement si la page de gestion du Gestionnaire de licence est ouverte et active. *Lors du passage à une autre page de la fenêtre principale, la page de gestion du Gestionnaire de licence sera fermée automatiquement et le bouton sur le volet ne sera plus visible.*
	Ouvre la page de consultation de messages du serveur de protection centralisée. *Le bouton est visible sur le volet uniquement si Dr.Web pour Linux fonctionne en mode de protection centralisée et que l'administrateur du réseau antivirus a configuré l'envoi de messages sur ce poste.*

Page d'accueil

Sur la page d'accueil de la fenêtre de l'interface graphique de gestion de Dr.Web pour Linux, vous pouvez trouver le volet où vous pouvez glisser/déposer des fichiers et dossiers à scanner. Sur le volet apparaît la mention **Faites-glisser les fichiers ici ou cliquez pour selectionner**. Une fois les objets glissés/déposés depuis le gestionnaire de fichiers vers la page d'accueil de la fenêtre Dr.Web pour Linux, leur analyse personnalisée démarre (si le Scanner analyse déjà d'autres objets, la nouvelle tâche de scan est mise en file d'attente).

Sur la page d'accueil de la fenêtre, les boutons suivants sont disponibles :

- **SpIDer Guard** affiche le statut en cours de SpIDer Guard. Cliquez sur ce bouton pour ouvrir la page de SpIDer Guard donnant accès aux paramètres du composant et sur laquelle vous pouvez lancer ou arrêter SpIDer Guard ainsi que consulter les statistiques sur son fonctionnement
- **SpIDer Gate** affiche le statut en cours de SpIDer Gate. Cliquez sur ce bouton pour ouvrir la page de SpIDer Gate donnant accès aux paramètres du composant et sur laquelle vous pouvez lancer ou arrêter SpIDer Guard ainsi que consulter les statistiques sur son fonctionnement.
- **Scanner** : permet d'ouvrir la page sur laquelle vous pouvez lancer le scan de fichiers et autres objets système (par exemple, les secteurs d'amorçage).
- **Dernière mise à jour** : affiche le statut en cours des bases virales Cliquez sur ce bouton pour ouvrir la page indiquant le statut de la mise à jour et sur laquelle vous pouvez lancer une mise à jour si nécessaire.
- **Licence** : affiche le statut de la licence en cours. Cliquez sur ce bouton pour ouvrir la page du Gestionnaire de Licences sur laquelle vous pouvez trouver des informations détaillées sur la licence en cours ainsi qu'acheter et enregistrer une nouvelle licence si nécessaire.

Intégration avec l'environnement graphique du bureau

Dr.Web pour Linux supporte quatre moyens d'intégration avec l'environnement graphique du bureau :

- Affichage dans la zone de notification du bureau de l'icône de l'application qui sert de l'indicateur de l'état permettant d'ouvrir le menu de l'application ;
- Un clic droit sur l'icône de l'application dans la barre de tâches appelle le menu contextuel avec les commandes principales du scan des fichiers ;
- Les commandes du menu contextuel dans le gestionnaire de fichiers graphique lancent le scan des fichiers et des répertoires ;
- Le glisser-déposer des fichiers et des répertoires dans la page principale de la fenêtre Dr.Web pour Linux lance le scan.

Indicateur de l'application dans la zone de notification

Après la connexion de l'utilisateur, l'agent de notifications affiche dans la zone de notifications un indicateur de l'état sous forme d'une icône avec le logo de Dr.Web pour Linux (si cela est supporté par l'environnement graphique utilisé). L'indicateur affiche l'état du logiciel et fournit un accès au menu contextuel de Dr.Web pour Linux. Si un problème survient (les bases virales ne sont pas à jour ou la licence est sur le point d'expirer), l'indicateur affiche un point d'exclamation par-dessus de l'icône de Dr.Web pour Linux :  .

Outre l'indicateur de l'état, l'agent de notifications affiche également des pop-up qui informent l'utilisateur des événements importants dans le fonctionnement de Dr.Web pour Linux comme :

- Menaces détectée (y compris celles détectées par SpIDer Guard et SpIDer Gate).
- La durée de validité de la licence est sur le point d'expirer.

Un clic sur l'icône de l'indicateur ouvre sur l'écran le menu contextuel de Dr.Web pour Linux.

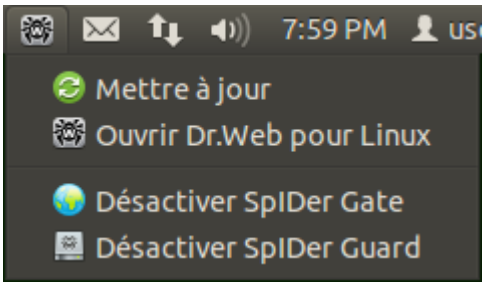

Image 6. Menu contextuel de l'indicateur Dr.Web pour Linux

Lorsque vous choisissez l'onglet **Ouvrir Dr.Web pour Linux**, la fenêtre de l'interface graphique de Dr.Web pour Linux apparaît sur l'écran ; c'est-à-dire Dr.Web pour Linux est lancé. La sélection des onglets **Activer SpIDer Gate/Désactiver SpIDer Gate** et **Activer SpIDer Guard/Désactiver SpIDer Guard** démarre ou arrête les moniteurs correspondants. Notez que vous devez vous authentifier en tant qu'utilisateur ayant les privilèges administrateur pour

désactiver tout moniteur (consultez la section Gestion des privilèges du logiciel). La sélection de l'onglet **Mettre à jour** lance une procédure de mise à jour.

Si l'indicateur signale un problème dans le fonctionnement de Dr.Web pour Linux, l'icône du composant qui a provoqué le problème s'affiche avec un point d'exclamation, par exemple : 
.

Problèmes de fonctionnement de l'indicateur de l'application

1. Si l'indicateur affiche la marque d'une erreur critique  , et que le menu déroulant ne contient qu'un seul sujet affiché **Démarrer**, cela signifie que Dr.Web pour Linux ne peut pas démarrer parce que certains composants du noyau ne sont pas disponibles. Si cet état est permanent, essayez de résoudre l'erreur manuellement ou contactez le Support technique.
2. Si après la connexion de l'utilisateur au système, l'indicateur n'a pas été affiché dans la zone de notifications du bureau, essayez de résoudre cette erreur ou contactez le Support technique.

> Selon l'environnement de bureau, l'apparence et le comportement de l'indicateur peuvent être différents de celui décrit plus haut ; Par exemple, les icônes peuvent ne pas s'afficher dans le menu déroulant.

Menu contextuel de l'icône de la barre de tâches

Si l'environnement du bureau supporte l'utilisation de la barre de tâches, telle que, par exemple, Unity Launcher dans l'OS Ubuntu, un bouton avec l'icône de l'application apparaîtra dans la barre de tâches au démarrage de l'interface graphique Dr.Web pour Linux. Pour cela, il est recommandé de lancer l'application par sélection de l'élément **Dr.Web pour Linux** dans le menu **Annexes**. Un clic droit sur le bouton de l'application lancée affichera sur l'écran le menu contextuel. Vous pouvez voir ci-dessous l'image approximative du menu contextuel (menu pour Unity Launcher dans l'OS Ubuntu).

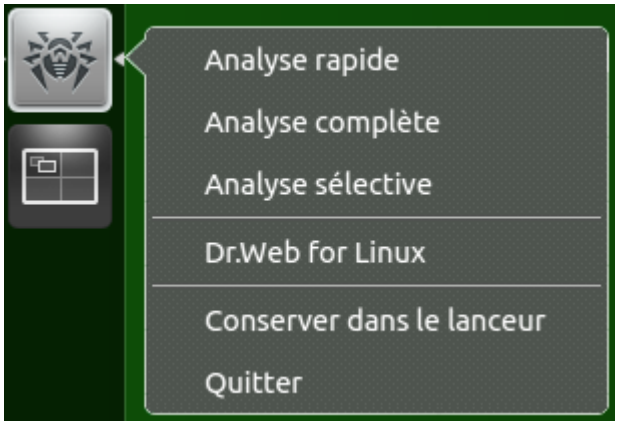

Image 7. Menu contextuel Dr.Web pour Linux dans la barre de tâches

- La sélection des éléments de menu **Scan rapide**, **Scan complet** et **Scan personnalisé** permet de lancer la tâche de scan correspondante (pour **Scan personnalisé** — ouvrir la page de sélection des objets à analyser).
- La sélection de l'élément de menu **Dr.Web pour Linux** lance l'interface graphique (si elle n'est pas encore lancée), la sélection de l'élément **Se déconnecter** — arrête le fonctionnement de l'interface graphique (si elle est lancée en ce moment).
- La sélection de l'élément de menu **Épingler au panneau** permet d'ajouter le bouton de l'application dans la barre de tâches pour accéder rapidement au lancement de l'interface graphique et de tâches principales de scan.

Si dans la file d'attente, il y a des tâches d'analyse du système de fichiers en train d'exécution, un identificateur de l'exécution cumulée des tâches d'analyse actives s'affiche par-dessus de l'icône de l'application dans la barre des tâches.

Dans les environnements différents du bureau, l'aspect de la barre de tâches et du menu contextuel peut varier. Le comportement des éléments différents de **Scan rapide**, **Scan complet** et **Scan personnalisé** peut également différer de ce qui est décrit.

Problèmes de fonctionnement de l'icône dans la barre de tâches

Si l'icône de l'interface graphique lancé s'affiche dans la barre de tâches mais le menu déroulant ne contient pas d'éléments de lancement de tâches de scan, essayez de lancer l'application graphique en sélectionnant l'élément **Dr.Web pour Linux** du menu **Annexes** (au lieu de lancer avec la commande `drweb-gui` dans l'émulateur de terminal ou au lieu de sélectionner l'élément **Ouvrir Dr.Web pour Linux** dans le menu de l'indicateur de l'application dans la zone de notification).

Analyse des fichiers et des répertoires via le menu contextuel du gestionnaire de fichiers

Dr.Web pour Linux permet d'effectuer le scan de fichiers et de répertoires depuis la fenêtre de parcours de fichiers et de répertoires du gestionnaire de fichiers (tel que Nautilus). Pour scanner les fichiers et les répertoires, il faut :

1. Les sélectionner dans la fenêtre du gestionnaire de fichiers et cliquer droit.
2. Sélectionner l'élément **Ouvrir dans un autre logiciel** dans le menu contextuel qui s'affiche.
3. Trouver **Dr.Web pour Linux** dans la liste des applications installées.

D'habitude, après la première utilisation de Dr.Web pour Linux en tant qu'application pour ouvrir des fichiers, le gestionnaire de fichiers enregistre cette association et ensuite, l'élément **Ouvrir dans Dr.Web pour Linux** sera disponible dans le menu contextuel.

Dans des gestionnaires de fichiers différents, le nom de l'élément du menu contextuel pour sélectionner les applications et le moyen de sélection de l'application dans la liste des applications installées peuvent varier.

Problèmes d'utilisation du menu contextuel du gestionnaire de fichiers

Certains environnements graphiques pour GNU/Linux peuvent configurer automatiquement l'association de fichiers et de répertoires (selon le type MIME de ces objets) avec **Dr.Web pour Linux** sélectionné dans le gestionnaire de fichiers pour l'analyse avec l'élément du menu contextuel **Ouvrir dans un autre logiciel**. Dans ce cas, pour ces fichiers et les répertoires un double clic gauche lancera **Dr.Web pour Linux**. Pour remédier à la situation, annulez l'association configurée entre les fichiers et **Dr.Web pour Linux**.

Glisser-déposer des fichiers et des répertoires dans la fenêtre de l'interface graphique de gestion

Dr.Web pour Linux permet d'effectuer le scan de fichiers et de répertoires en les glissant-déposant de la fenêtre de parcours de fichiers et de répertoires du gestionnaire de fichiers graphique à la fenêtre de l'interface graphique de gestion de Dr.Web pour Linux. Pour commencer le scan de fichiers et de répertoires glissés-déposés dans la fenêtre de l'application, il faut que la fenêtre de l'interface soit ouverte sur la page principale de l'application ou la page de sélection de type de scan. Vous pouvez glisser-déposer les fichiers et les répertoires à scanner dans la fenêtre de l'interface de gestion de Dr.Web pour Linux si la page contient une cible et l'inscription **Faites-glisser les fichiers ici ou cliquez pour selectionner**.

Démarrer et arrêter l'interface graphique

Lancement de l'interface graphique de gestion Dr.Web pour Linux

Pour lancer l'interface graphique de gestion de Dr.Web pour Linux, il faut :

- Sélectionnez dans le menu système **Annexes**, l'élément **Dr.Web pour Linux**.

ou

- Cliquez droit sur l'icône de l'indicateur de Dr.Web pour Linux dans la zone de notification du bureau et choisissez **Ouvrir Dr.Web pour Linux** dans le menu déroulant.

Vous pouvez également démarrer l'interface graphique de gestion de Dr.Web pour Linux depuis la ligne de commande en utilisant la commande `drweb-gui`. Vous pouvez utiliser cette option uniquement si l'environnement graphique est accessible en mode ligne de commande, par exemple, dans l'émulateur de terminal.

Arrêt de l'interface graphique de gestion de Dr.Web pour Linux

Pour arrêter l'interface graphique de gestion de Dr.Web pour Linux, fermez sa fenêtre via le bouton classique fermer sur la barre de titre.

Notez que les composants service, y compris l'agent de notifications, les moniteurs SpIDer Guard et SpIDer Gate, continuent à fonctionner après l'arrêt de l'interface graphique de Dr.Web pour Linux (à moins qu'ils ne soient stoppés par l'utilisateur).

Dans un fonctionnement normal, le fonctionnement des composants service ne requiert pas l'intervention de l'utilisateur.

Détection et neutralisation des menaces

La recherche et la neutralisation des menaces sont effectuées par le Scanner (à la demande de l'utilisateur ou selon la planification) et par le moniteur du système de fichiers SpIDer Guard et le moniteur des connexions réseau SpIDer Gate pendant que vous travaillez.

- Pour activer ou désactiver SpIDer Guard et SpIDer Gate, utilisez le menu de la zone de notifications et les pages de configuration correspondantes (voir Surveillance du système de fichiers et Surveillance des connexions réseau).
- Pour voir les tâches en cours du Scanner ou les gérer, ouvrez la page de gestion des tâches.
- Toutes les menaces détectées par le Scanner ou par le moniteur du système de fichiers SpIDer Guard s'affichent sous forme d'une liste sur la page de consultation des menaces détectées.
- Pour gérer les menaces placées en quarantaine, ouvrez la page de la Quarantaine.
- Pour configurer les réactions de Dr.Web pour Linux face aux menaces détectées, ouvrez la fenêtre des paramètres. Sur cette page, vous pouvez également définir une planification pour lancer le scan et configurer l'analyse de connexions chiffrées.

Si Dr.Web pour Linux opère en mode de protection centralisée et que le lancement du scan à la demande de l'utilisateur n'est pas autorisé sur le serveur de protection centralisée, la page **Scanner** de la fenêtre de Dr.Web pour Linux sera indisponible. De plus, dans ce cas, l'agent de notifications et l'interface graphique ne lanceront pas les scans selon la planification.

Scan à la demande

Dans cette section :

- Types de scans exécutés.
- Démarrer le scan.
- Ajouter et supprimer les objets dans la liste de scan personnalisé.

- Lancer le scan personnalisé des objets listés.

Types de scans exécutés

À la demande de l'utilisateur, le scan dans un des modes suivants peut être lancé :

- *Scan rapide* : scan des objets systèmes critiques exposés à un fort risque de compromission (secteurs d'amorçage, système de fichiers, etc.).
- *Scan complet* : scan de tous les objets du système de fichiers accessibles à l'utilisateur du nom duquel a été lancé Dr.Web pour Linux.
- *Scan personnalisé* : scan des objets du système de fichiers ou d'autres objets spécifiques indiqués par l'utilisateur.

Si Dr.Web pour Linux fonctionne en mode Protection centralisée et que le lancement d'un scan à la demande de l'utilisateur n'est pas autorisé sur le serveur de protection centralisée, cette page de Dr.Web pour Linux sera indisponible.

Le scan peut augmenter la charge du processeur, ce qui peut provoquer un déchargement rapide de la batterie. Ainsi, il est recommandé d'effectuer le scan d'un ordinateur portable lorsqu'il est branché.

Démarrer le scan

Pour démarrer le scan, cliquez sur **Scanner** sur la page d'accueil de la fenêtre.

La page avec les différents types de scan s'ouvre Pour démarrer un scan *Rapide* ou *Complet*, cliquez sur le bouton correspondant. Après avoir cliqué sur l'un de ces boutons, le scan démarre automatiquement.

Image 8. Page de sélection du type de l'analyse

Le scan est effectué avec les privilèges actuels du logiciel. Si le logiciel ne possède pas de privilèges élevés, tous les fichiers et les répertoires qui ne sont pas accessibles à l'utilisateur qui a lancé Dr.Web pour Linux ne peuvent pas être scannés. Pour permettre le scan de tous les fichiers souhaités pour lesquels vous n'avez pas de permissions de propriétaire, élevez les privilèges de l'application avant le lancement du scan. Pour en savoir plus, consultez la section Gestion des privilèges du logiciel.

Pour démarrer un scan *Scan personnalisé* de certains fichiers et répertoires, faites une des actions suivantes :

- **Glissez/déposez les objets souhaités**.

  Glissez/déposez les fichiers et répertoires souhaités depuis la fenêtre du Gestionnaire du système de fichiers vers la zone portant la mention **Faites-glisser les fichiers ici ou cliquez pour selectionner**. Vous pouvez également glisser/déposer les objets vers la Page d'accueil de la fenêtre de Dr.Web pour Linux.

  Lorsque vous glissez des objets sur la page, elle se modifie pour afficher le message **Faites-glisser les fichiers ici**. Pour démarrer le scan, déposez les objets glissés dans la zone appropriée. Le scan démarre automatiquement.

Image 9. Zone où les objets sont glissés pour être scannés

- **Formation de la liste des objets pour le scan personnalisé**.

  Pour sélectionner les objets à scanner, cliquez sur la zone dédiée La fenêtre dans laquelle vous pouvez sélectionner les objets système pour un scan Personnalisé s'ouvre.

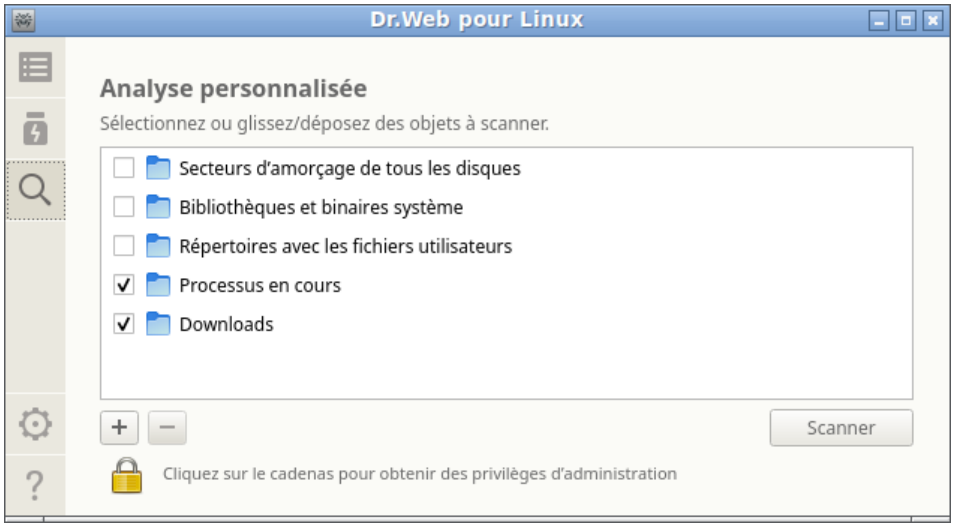

Image 10. Liste des objets à scanner

La liste des objets pour un scan Personnalisé contient quatre parties prédéfinies :

- *Entrées de démarrage de tous les disques*. Si vous cochez cette case, tous les secteurs d'amorçage de tous les disques disponibles sont sélectionnés pour être scannés.
- *Fichiers exécutables et bibliothèques système*. Si vous cochez cette case, tous les répertoires avec des exécutables systèmes sont sélectionnés pour être scannés (`/bin`, `/sbin`, etc.).
- *Répertoires avec les fichiers d'utilisateur*. Si vous cochez cette case, tous les répertoires contenant des fichiers utilisateurs et les fichiers de la session en cours sont sélectionnés pour être scannés (répertoire `/home/`<*username*> (`~`), `/tmp`, `/var/mail`, `/var/tmp`).
- *Processus lancés*. Si vous cochez cette case, les fichiers exécutables contenant le code des processus en cours sont sélectionnés pour être scannés. Dans ce cas, si une menace est détectée, non seulement l'objet malveillant est neutralisé, mais le processus actif est également arrêté.

Ajouter et supprimer les objets dans la liste de scan personnalisé

Si nécessaire, vous pouvez ajouter des chemins personnalisés vers une liste d'objets à scanner. Pour cela, glissez/déposez les objets souhaités (les chemins vers les objets sont automatiquement ajoutés à la liste) ou cliquez sur `+` sous la liste. Dans ce cas, une fenêtre de dialogue standard s'ouvre où vous pouvez sélectionner les objets (un fichier ou un répertoire). Après avoir sélectionné les objets, cliquez sur **Ouvrir**.

Les fichiers et répertoires masqués ne sont pas affichés par défaut dans le sélecteur de fichiers. Pour voir ces objets, cliquez sur ✱ dans le panneau d'instruments de la fenêtre de sélection de fichiers et de répertoires.

Pour supprimer tous les chemins sélectionnés de la liste, cliquez sur `–` sous la liste. Le chemin est sélectionné, si la ligne de liste contenant ce chemin est sélectionnée. Pour choisir plusieurs chemins, sélectionnez les éléments dans la liste avec la touche SHIFT ou CTRL appuyée. Notez que les quatre premiers éléments de la liste sont prédéfinis et ne peuvent pas être supprimés.

Lancer le scan Personnalisé des objets listés

Pour lancer un scan personnalisé, cochez tous les objets à analyser et cliquez sur **Analyser**. Après cela, le scan des objets démarre.

Après le démarrage du scan, la tâche est mise en file d'attente, qui contient toutes les tâches de scan de la session en cours : tâches terminées, tâches en cours, tâches en attente. Vous pouvez voir la liste des tâches et les gérer sur la page de gestion des tâches de scan.

Scan des objets selon la planification

Dr.Web pour Linux peut lancer automatiquement des scans périodiques de la liste d'objets du système de fichiers selon la planification spécifiée.

> Si Dr.Web pour Linux fonctionne en mode Protection centralisée et que le lancement d'un scan à la demande de l'utilisateur n'est pas autorisé sur le serveur de protection centralisée, cette fonction de Dr.Web pour Linux sera indisponible.

Types de scans exécutés

Les types suivants de scans peuvent être lancés selon la planification :

- *Scan rapide* : scan des objets systèmes critiques exposés à un fort risque de compromission (secteurs d'amorçage, système de fichiers, etc.).
- *Scan complet* : scan de tous les objets du système de fichiers accessibles à l'utilisateur du nom duquel a été lancé Dr.Web pour Linux.
- *Scan personnalisé* : scan des objets du système de fichiers ou d'autres objets spécifiques indiqués par l'utilisateur.

Démarrer le scan

Les scans sont lancés automatiquement selon la planification spécifiée. Le lancement du scan est effectué :

1. Par l'interface graphique si elle est lancée au moment du démarrage du scan.
2. Par l'Agent de notifications si au moment du démarrage du scan, l'interface graphique n'est pas disponible.

Au démarrage du scan selon la planification, l'interface graphique de gestion est lancée automatiquement (si elle n'est pas encore lancée) la tâche créée est mise en file d'attente qui contient toutes les tâches de scan de la session en cours : tâches terminées, tâches en cours, tâches en attente. Vous pouvez voir la liste des tâches et les gérer sur la page de gestion de la liste de tâches de scan.

Gérer les tâches de scan

Vous pouvez voir la liste des tâches créées et des tâches en cours sur une page spécifique de Dr.Web pour Linux. Si au moins une tâche est en attente, un bouton qui ouvre la page de la liste des tâches devient visible sur le panneau de navigation. En fonction du statut des tâches en attente, le bouton présente les icônes suivantes :

	Au moins une des tâches n'est pas terminée (l'icône est animée).
	Toutes les tâches de scan dans la liste sont terminées ou arrêtées par l'utilisateur ; aucune menace n'a été détectée ou toutes les menaces détectées ont été neutralisées avec succès.
	Toutes les tâches de scan dans la liste sont terminées ou arrêtées par l'utilisateur ; certaines des menaces détectées n'ont pas été neutralisées.
	Toutes les tâches de scan dans la liste sont terminées ou arrêtées par l'utilisateur. Certaines tâches ont échoué.

Les tâches sont triées par heure (depuis la dernière jusqu'à la première).

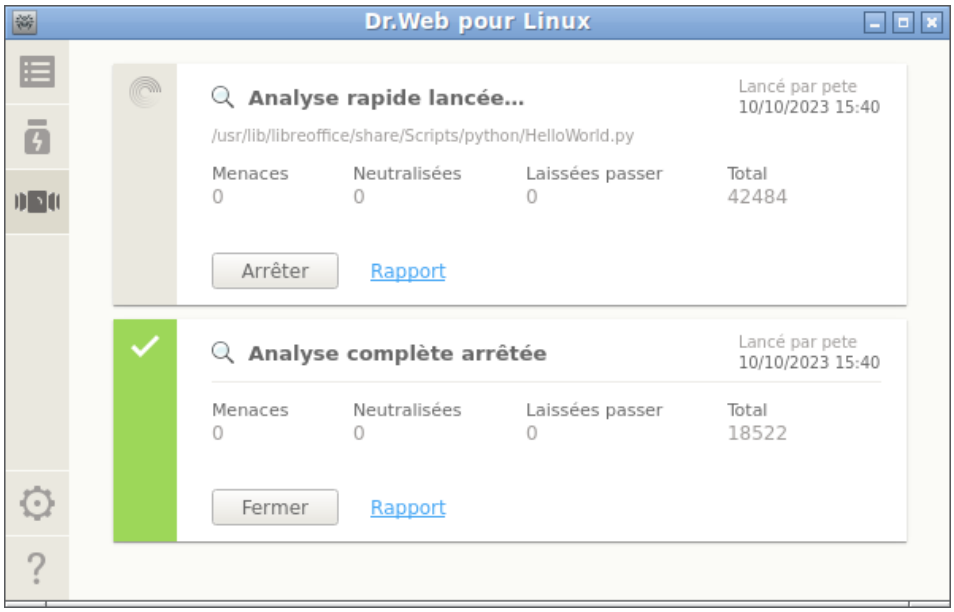

Image 11. Page de consultation de la liste des scans

Pour chaque tâche listée, les informations suivantes sont disponibles :

- Type de scan (non seulement *Scan rapide, Scan complet* et *Scan personnalisé* peuvent figurer dans la liste, mais aussi d'autres types de scan. Pour en savoir plus, voir ci-dessous).
- Nom de l'utilisateur qui a lancé le scan (s'il est inconnu, son identificateur système *UID* s'affiche).
- Date de la création et de la fin de la tâche (si elle est terminée).

- Nombre de menaces détectées, menaces neutralisées, fichiers passés et nombre total d'objets scannés.

Le statut de la tâche est indiqué grâce à la couleur assignée à la tâche dans la liste. Les couleurs suivantes sont utilisées :

	Le scan n'est pas terminé ou est en attente.
	Le scan est terminé ou arrêté par l'utilisateur. Aucune menace n'a été détectée ou toutes les menaces ont été neutralisées.
	Le scan s'est arrêté à cause d'une erreur.
	Le scan est terminé ou arrêté par l'utilisateur. Au moins une des menaces détectées n'a pas été neutralisée.

Notez que la liste contient uniquement les scans exécutés par le Scanner et lancés par l'utilisateur dans la fenêtre de Dr.Web pour Linux et les scans lancés automatiquement selon la planification spécifiée.

Dans la zone de description de la tâche, l'un des boutons suivants est disponible :

- **Annuler** : annuler la tâche en attente. Le bouton est disponible si la tâche est en attente. Après avoir cliqué dessus, la tâche se termine. L'information sur la tâche demeure dans la liste.
- **Arrêter** : arrêter la tâche en cours. Après un clic sur ce bouton, la tâche stoppée ne peut pas être relancée. Le bouton est disponible si la tâche est en cours. L'information sur la tâche stoppée demeure dans la liste.
- **Fermer** : fermer les données sur la tâche terminée et supprimer la tâche de la liste. Le bouton est disponible si la tâche n'est pas terminée et si toutes les menaces détectées ont été neutralisées.
- **Neutraliser** : neutraliser les menaces. Le bouton est disponible si la tâche est terminée et que certaines menaces n'ont pas été neutralisées.
- **En savoir plus** : ouvrir la liste des menaces détectées et les neutraliser. Le bouton est disponible si la tâche est terminée et que certaines menaces n'ont pas été neutralisées.

Cliquez sur **Rapport** pour afficher le rapport du scan incluant des données détaillées sur la tâche et la liste des menaces détectées, s'il y en a.

Image 12. Information détaillée sur les résultats du scan

Les systèmes de fichiers UNIX, tels que GNU/Linux, peuvent contenir des objets spéciaux qui apparaissent comme des noms de fichiers mais ne sont pas des fichiers contenant des données (ce sont, par exemple, des liens symboliques, des sockets, des canaux nommés et des fichiers de périphérique). Ils sont appelés fichiers *spéciaux*, à la différence des fichiers *usuels* (*réguliers*). Dr.Web pour Linux saute *toujours* les fichiers spéciaux durant le scan.

Un clic sur le lien portant le nom de la menace détectée ouvre dans le navigateur une page contenant les informations sur cette menace (vous passez sur le site de Doctor Web, une connexion Internet est requise).

Cliquer sur **Exportation** si vous voulez enregistrer le rapport de scan dans un fichier texte. Pour fermer la fenêtre contenant les informations sur le scan, cliquez sur **Fermer**.

Pour chaque menace détectée par le Scanner durant le scan lancé via la fenêtre de Dr.Web pour Linux (y compris un scan planifié) applique des actions définies dans les paramètres à l'onglet **Scanner**.

Les paramètres de neutralisation des menaces définis à l'onglet **Scanner** ne sont pas utilisés pour le scan *centralisé* et le scan *en ligne de commande*.

Pour voir toutes les menaces détectées, ouvrez la page avec la liste des menaces détectées.

Surveillance du système de fichiers

Dans cette section :

- Informations générales.
- Gérer le moniteur du système de fichiers.

- Configurer le moniteur du système de fichiers.
- Problèmes de SpIDer Guard.

Informations générales

SpIDer Guard est un moniteur du système de fichiers qui contrôle en permanence tous les objets du système de fichiers.

L'interface graphique de gestion de Dr.Web pour Linux permet de gérer SpIDer Guard, notamment :

- Lancer et arrêter le moniteur du système de fichiers.
- Voir les statistiques sur le fonctionnement du composant et la liste des menaces détectées.
- Configurer les paramètres suivants :
  - Réaction face à la détection d'une menace.
  - Liste des exclusions.

Gérer le moniteur du système de fichiers

Vous pouvez lancer et arrêter le moniteur du système de fichiers SpIDer Guard ainsi que consulter ses statistiques sur une page spécifique dans la fenêtre de Dr.Web pour Linux. Pour ouvrir la page de gestion de la surveillance, cliquez sur **SpIDer Guard** sur la page d'accueil.

Image 13. Page de gestion de SpIDer Guard

Sur la page des paramètres du moniteur, les informations suivantes sont fournies :

- Statut du moniteur du système de fichiers SpIDer Guard (activé ou desactivé) et, probablement, données sur l'erreur survenu lors de son fonctionnement.
- Statistiques de fonctionnement de SpIDer Guard :
  - Vitesse moyenne du scan de fichiers.
  - Nombre de menaces détectées et neutralisées.

Pour activer la surveillance (si elle est désactivée), cliquez sur **Activer**. Pour arrêter la surveillance, cliquez sur **Désactiver**.

Pour désactiver la surveillance du système de fichiers, le logiciel doit posséder des privilèges élevés. Pour en savoir plus, consultez la section Gestion des privilèges du logiciel.

Si Dr.Web pour Linux est géré par le serveur de protection centralisée, l'option activer/désactiver le moniteur du système de fichiers SpIDer Guard peut être bloquée, si cela est interdit par le serveur.

Le statut de SpIDer Guard (activé ou désactivé) est indiqué par l'indicateur :

	Le moniteur du système de fichiers SpIDer Guard est activé et protège le système de fichiers.
	SpIDer Guard a été désactivé par l'utilisateur ou stoppé à cause d'une erreur et ne protège pas le système de fichiers.

Pour fermer la page des paramètres du moniteur du système de fichiers, il suffit de passer à une autre page à l'aide des boutons sur le volet de navigation.

La liste des menaces détectées par SpIDer Guard durant la session en cours de Dr.Web pour Linux s'affiche sur la page des menaces listées (la page est disponible seulement s'il y a des menaces détectées).

Configurer le moniteur du système de fichiers

Pour configurer les paramètres du moniteur du système de fichiers SpIDer Guard, ouvrez la page des paramètres :

- Dans l'onglet **SpIDer Guard** : réactions face aux menaces détectées.
- Dans l'onglet **Exclusions** : exclusion des objets du contrôle.

L'activation du mode de surveillance renforcé des fichiers par le moniteur SpIDer Guard est décrite dans la section Modes de surveillance des fichiers.

Problèmes de SpIDer Guard

Si un échec de SpIDer Guard est détecté, les informations sur l'erreur survenue s'affichent sur la page de gestion. Pour résoudre le problème, consultez l'Annexe D, où vous pouvez trouver une description détaillée des erreurs connues.

Surveillance des connexions réseau

Dans cette section :

- Informations générales.
- Gestion du moniteur de connexions réseau.
- Configuration de SpIDer Gate.
- Problèmes de SpIDer Gate.

Informations générales

SpIDer Gate effectue un contrôle permanent des connexions réseau établies. Le moniteur permet de prévenir l'accès aux sites ajoutés dans les listes noires de l'utilisateur ou concernant les catégories des sites indiqués en tant que sites non recommandés pour la visite. De plus, SpIDer Gate analyse :

- les messages e-mail envoyés et reçus (y compris pour la présence du spam).
- les fichiers téléchargés sur Internet.

En cas de détection de menaces dans l'objet analysé, SpIDer Gate bloque la réception ou la transmission

L'interface graphique de gestion Dr.Web pour Linux permet de gérer SpIDer Gate :

- Lancer et arrêter le moniteur de connexions réseau.
- Voir le nombre des objets vérifiés et bloqués et des tentatives d'accès aux sites.
- Configurer les paramètres de surveillance des connexions réseau :
  - Sélectionner le type de trafic analysé (trafic Web, trafic FTP).
  - Liste des catégories de sites et de hôtes l'accès auxquels est bloqué.
  - Listes noire et blanche personnalisées contenant des sites et des hôtes.
  - Paramètres d'analyse des fichiers téléchargés sur Internet.

Les menaces que contiennent les e-mails peuvent être détectées par le moniteur actif du système de fichiers SpIDer Guard au moment de leur enregistrement dans le système de fichiers local par le client de messagerie sous forme de fichiers.

Gestion du moniteur de connexions réseau

Vous pouvez lancer et arrêter le moniteur de connexions réseau SpIDer Gate ainsi que consulter ses statistiques sur une page spécifique dans la fenêtre de Dr.Web pour Linux. Pour ouvrir la page de gestion de la surveillance des connexions réseau, il faut cliquer sur **SpIDer Gate** sur la page d'accueil.

Image 14. Page de gestion de SpIDer Gate

Sur la page de gestion de la surveillance des connexions réseau, les informations suivantes sont affichées :

- Statut du moniteur de connexions réseau SpIDer Gate (activé/désactivé) et informations sur une erreur survenu lors du démarrage.
- Statistiques de surveillance :
  - Vitesse moyenne d'analyse des e-mails et des fichiers téléchargés sur Internet.
  - Nombre des objets analysés (e-mails, fichiers téléchargés sur Internet, URL).
  - Nombre des messages, des appels aux sites et des objets contenant des menaces bloquées.

Pour activer la surveillance (si elle est désactivée), cliquez sur **Activer**. Pour arrêter la surveillance, cliquez sur **Désactiver**.

Pour désactiver la surveillance de connexions réseau, le logiciel doit posséder des privilèges élevés. Pour en savoir plus, consultez la section Gestion des privilèges du logiciel.

Si Dr.Web pour Linux est géré par le serveur en mode de protection centralisée, l'option d'activation/désactivation du moniteur de connexions réseau SpIDer Gate peut être bloquée si cela est interdit par le serveur.

Le statut du moniteur de connexions réseau SpIDer Gate (activé ou désactivé) est indiqué par un indicateur :

	SpIDer Gate est activé et contrôle les connexions réseau (l'envoi et la réception d'e-mails et l'accès à Internet).
	SpIDer Gate ne contrôle pas les connexions réseau (l'accès aux sites web n'est pas restreint et les e-mails ne sont pas analysés au moment de leur envoi et leur réception, ainsi que les fichiers téléchargés sur Internet) car il a été désactivé par l'utilisateur ou stoppé à cause d'une erreur.

Si un client de messagerie (tel que Mozilla Thunderbird) utilisant le protocole IMAP pour la réception des messages est lancé dans le système, il faut le redémarrer après l'activation du moniteur SpIDer Gate pour assurer l'analyse des messages entrants.

Pour fermer la page de gestion de la surveillance des connexions réseau, il suffit de passer à une autre page à l'aide des boutons sur le panneau de navigation.

Configuration de SpIDer Gate

Vous pouvez configurer le moniteur de connexions réseau SpIDer Gate dans la fenêtre de paramètres :

- dans l'onglet **SpIDer Gate** : définition de la liste des catégories bloquées de sites et réaction sur la détection des menaces.
- dans l'onglet **Exclusions** : gestion de la liste blanche et de la liste noire de sites et l'exclusion de l'activité réseau d'une application de la surveillance.
- dans l'onglet **Réseau** : gestion de la vérification des connexions réseau (SSL/TLS).

Problèmes de SpIDer Gate

Si un échec du moniteur de connexions réseau est détecté, les informations sur l'erreur survenue s'affichent sur la page de gestion. Pour résoudre le problème, consultez la rubrique Annexe D. Erreurs connues, où vous pouvez trouver une description détaillée des erreurs connues.

En fonction de la fourniture, Dr.Web pour Linux peut ne pas contenir le composant Dr.Web Anti-Spam. Dans ce cas, l'analyse antispam de messages n'est pas effectuée.

Si certains messages ne sont pas correctement reconnus par le composant Dr.Web Anti-Spam, il est recommandé de les envoyer aux adresses e-mail spéciales pour l'analyse et l'amélioration de fonctionnement du filtre antispam. Pour cela, enregistrez chaque message dans un fichier de type `.eml`. Veuillez joindre les fichiers sauvegardes à un message e-mail, et envoyez ce message à l'adresse service correspondante.

- nonspam@drweb.com : si le message contient les fichiers *classés par erreur comme spam* ;
- spam@drweb.com : si le message contient les fichiers *non classés par erreur comme spam*.

Voir les menaces détectées

Dans cette section :

- Informations générales.
- Neutraliser les menaces détectées.
- Voir les données sur les menaces.

Informations générales

La liste des menaces détectées par le Scanner et par SplDer Guard durant la session en cours de Dr.Web pour Linux s'affiche sur une page spéciale disponible seulement si au moins une menace a été détectée.

Si des menaces sont détectées, vous pouvez ouvrir cette page en cliquant sur  sur le panneau de navigation.

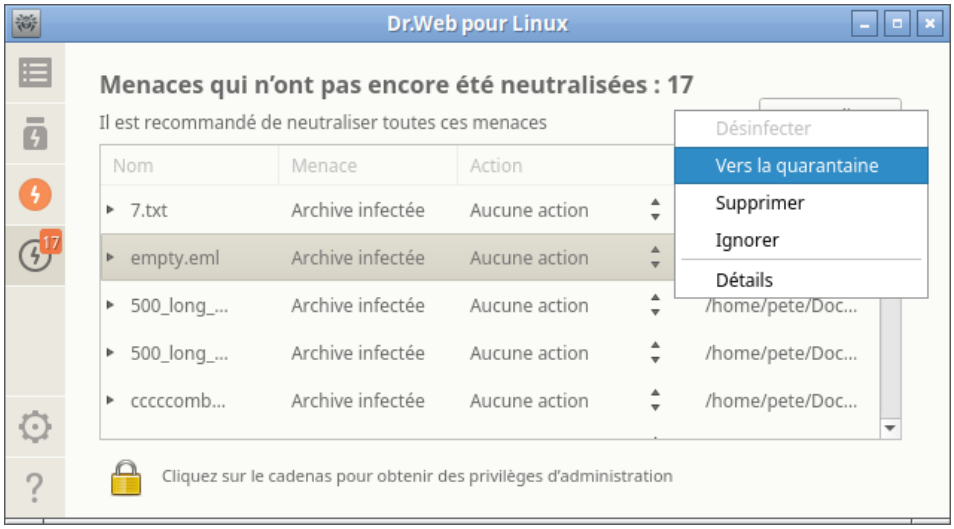

Image 15. Page de consultation des menaces

Dans la liste, les informations suivantes sont disponibles pour chaque menace détectée :

- Nom de l'objet infecté.
- Nom de la menace (d'après la classification de Doctor Web).
- Action appliquée (ou à appliquer) à la menace.
- Chemin vers l'objet malveillant.

Les menaces neutralisées s'affichent en grisé dans la liste.

Neutraliser les menaces détectées

Si certaines des menaces listées ne sont pas neutralisées, le bouton **Neutraliser** devient disponible au-dessus de la liste. Après un clic sur le bouton, les actions définies dans le champ **Action** seront appliquées à toutes les menaces listées. Si la neutralisation d'une menace est réussie, la ligne contenant cette menace devient inactive. Si une tentative de neutralisation d'une menace échoue, elle s'affiche en rouge et un message d'erreur apparaît dans le champ **Action**.

Par défaut, une action à appliquer à une menace est choisie d'après les paramètres du composant qui a détecté la menace. Vous pouvez configurer les actions appliquées aux

menaces d'un certain type par le Scanner et par SpIDer Guard. Pour cela, ouvrez l'onglet correspondant sur la Page des paramètres et définissez les paramètres.

> Si, dans les paramètres du Scanner ou SpIDer Guard, l'action *Signaler* a été sélectionnée pour un type de menaces quelconque, toutes les menaces de ce type seront affichés dans la liste de menaces avec l'action *Aucune action*. Pour neutraliser de telles menaces, il faut indiquer une action pour chaque menace dans le champ **Action**.

S'il est nécessaire d'appliquer une action différente de celle définie dans la liste, cliquez sur le champ **Action** et sélectionnez une autre action dans le menu qui s'affiche.

> Si la menace est détecté dans un fichier se trouvant dans un conteneur (archive, message, etc.), le conteneur n'est pas supprimé mais il est mise en quarantaine.

Vous pouvez choisir plusieurs menaces en même temps dans la liste. Pour cela, sélectionnez les menaces avec la souris tout en maintenant appuyées les touches CTRL ou SHIFT :

- Lorsque vous maintenez appuyée la touche CTRL, les menaces sont sélectionnées une par une.
- Lorsque vous maintenez appuyée la touche SHIFT, les menaces sont sélectionnées toutes en même temps.

Après avoir sélectionné des menaces, vous pouvez leur appliquer l'action requise en cliquant droit sur la sélection puis en cliquant sur l'action dans le menu qui s'est affiché. L'action sélectionnée dans le menu est appliquée à toutes les menaces sélectionnées.

> Notez que :
>
> - Si une menace est détectée dans un objet complexe (archive, message e-mail, etc), l'action sélectionnée est appliquée au conteneur entier (et pas uniquement à l'objet infecté).
> - L'action *Désinfecter* ne peut pas être appliquée à tous les types de menaces.
>
> Si nécessaire, élevez les privilèges du logiciel pour permettre une neutralisation réussie des menaces.

Les menaces auxquelles l'action *Ignorer* a été appliquée seront affichées dans la liste jusqu'au redémarrage de l'interface graphique de gestion.

Voir les informations sur les menaces

Pour des informations détaillées sur une menace, cliquez droit sur l'article avec les données sur la menace puis cliquez sur **En savoir plus** dans le menu qui s'est affiché. Ensuite, une fenêtre s'ouvre contenant des informations détaillées sur la menace et les objets qui contenaient la menace. Pour consulter les données sur plusieurs menaces en même temps, sélectionnez les articles correspondants avec la souris tout en maintenant appuyée la touche CTRL.

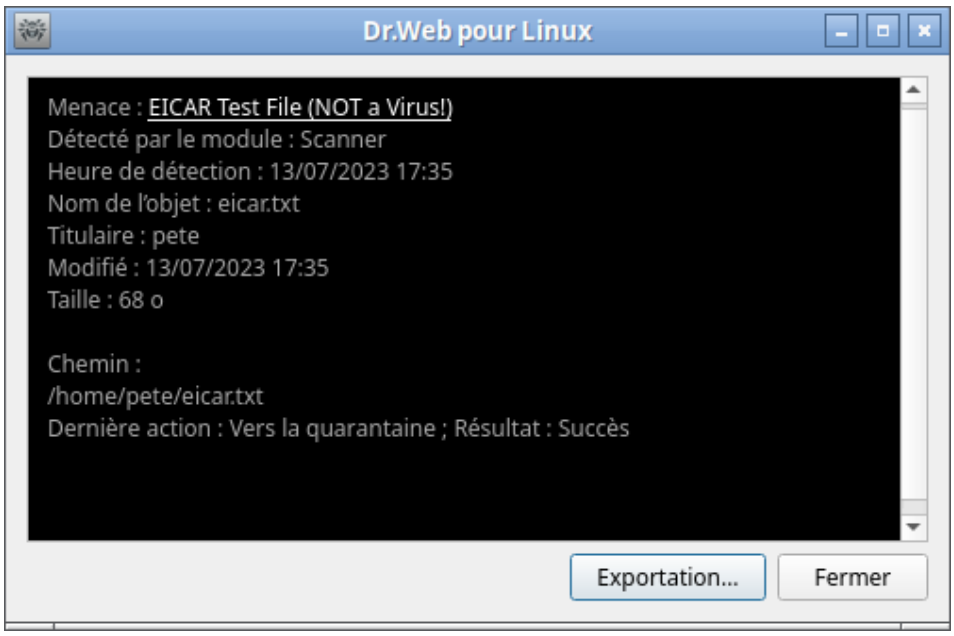

Image 16. Informations sur la menace

Dans cette fenêtre, les informations suivantes sont fournies :

- Nom de la menace (selon la classification de Doctor Web).
- Nom du composant Dr.Web pour Linux qui a détecté la menace.
- Date et heure de la détection.
- Information sur l'objet du système de fichiers dans lequel la menace a été détectée : nom de l'objet, propriétaire, date de la dernière modification et chemin vers l'objet dans le système de fichiers.
- Dernière action à être appliquée à la menace et son résultat (si l'application automatique des actions est spécifiée dans les paramètres du composant qui a détecté la menace. Par exemple une action peut être spécifiée pour le Scanner dans l'onglet correspondant de la fenêtre de configuration).

Un clic sur le lien portant le nom de la menace ouvre dans le navigateur une page contenant la description de cette menace (vous passez sur le site de Doctor Web, une connexion Internet est requise).

Cliquer sur **Exportation** si vous voulez enregistrer dans un fichier texte les informations affichées dans la fenêtre (une fenêtre s'ouvre dans laquelle vous pouvez sélectionner un fichier pour l'enregistrement des informations). Pour fermer la fenêtre contenant les informations sur la menace et l'objet infecté, cliquez sur **Fermer**.

Gérer la quarantaine

Dans cette section :

- Informations générales.
- Appliquer des actions aux objets isolés.

- Voir les données sur les objets isolés.

Informations générales

La liste de fichiers déplacés en quarantaine par le composant de Dr.Web pour Linux s'affiche sur une page spécifique. Pour ouvrir la page, cliquez sur le bouton  dans le panneau de navigation.

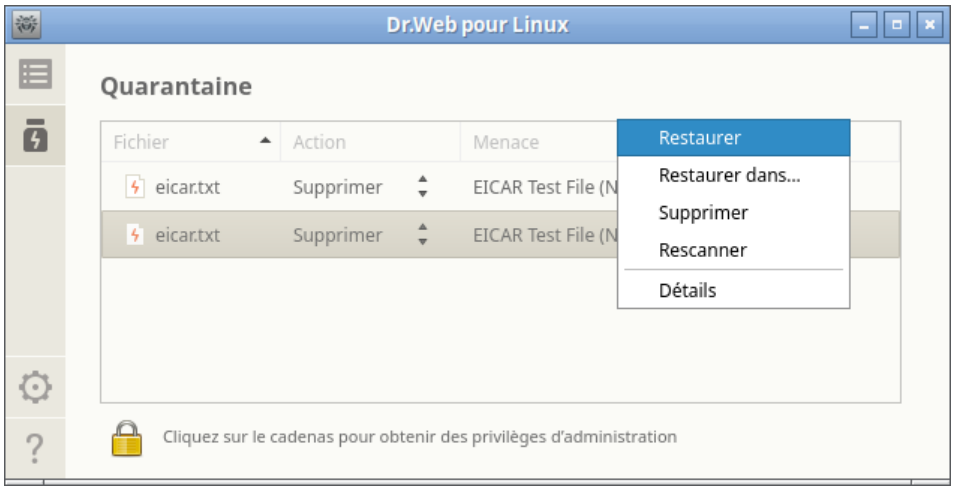

Image 17. Page de gestion de la quarantaine

Si la quarantaine n'est pas vide, les informations suivantes s'affichent pour chaque menace détectée :

- Nom de l'objet infecté.
- Action à appliquer à l'objet placé en quarantaine.
- Nom de la menace (d'après la classification de Doctor Web).

Appliquer des actions aux objets isolés

Pour appliquer une action à un objet en quarantaine, cliquez droit sur la ligne contenant les informations sur l'objet et sélectionnez une action dans le menu qui s'affiche. Pour appliquer une action à plusieurs objets isolés, sélectionnez-les avec la souris en maintenant appuyées les touches CTRL ou SHIFT :

- Lorsque vous maintenez appuyée la touche CTRL, les objets isolés sont ajoutés dans la liste un par un.
- Lorsque vous maintenez appuyée la touché SHIFT, les objets isolés sont sélectionnés tous ensemble.

Les actions suivantes sont disponibles pour les objets isolés :

- **Restaurer** : récupérer l'objet isolé dans son emplacement d'origine.
- **Restaurer sur** : récupérer les objets sélectionnés dans l'endroit sélectionné du système de fichiers (la fenêtre de sélection du répertoire de récupération va s'ouvrir).

- **Supprimer** : supprimer définitivement les objets sélectionnés.
- **Revérifier** : effectuer le scan de l'objet isolé encore une fois et désinfecter cet objet si cela est possible.

Si l'action choisie est appliquée avec succès à l'objet, il est supprimé du tableau. Si la tentative d'appliquer une action échoue, la ligne dans la liste des objets en quarantaine s'affiche en rouge et un message d'erreur apparaît dans le champ **Action**.

Pour l'application réussie des actions aux objets isolés, les privilèges élevés de l'application peuvent être requis. Par exemple, l'augmentation de privilèges est nécessaire pour appliquer les actions aux objets placés en quarantaine par un des utilisateurs.

Voir les données sur les objets isolés

Pour des informations détaillées sur un objet isolé, cliquez droit sur la ligne contenant les informations sur l'objet et sélectionnez l'élément **En savoir plus** dans le menu contextuel. Ensuite, une fenêtre s'ouvre contenant des informations détaillées sur l'objet. Pour consulter les données sur plusieurs objets isolés en même temps, sélectionnez-les dans la liste avant d'ouvrir le menu contextuel.

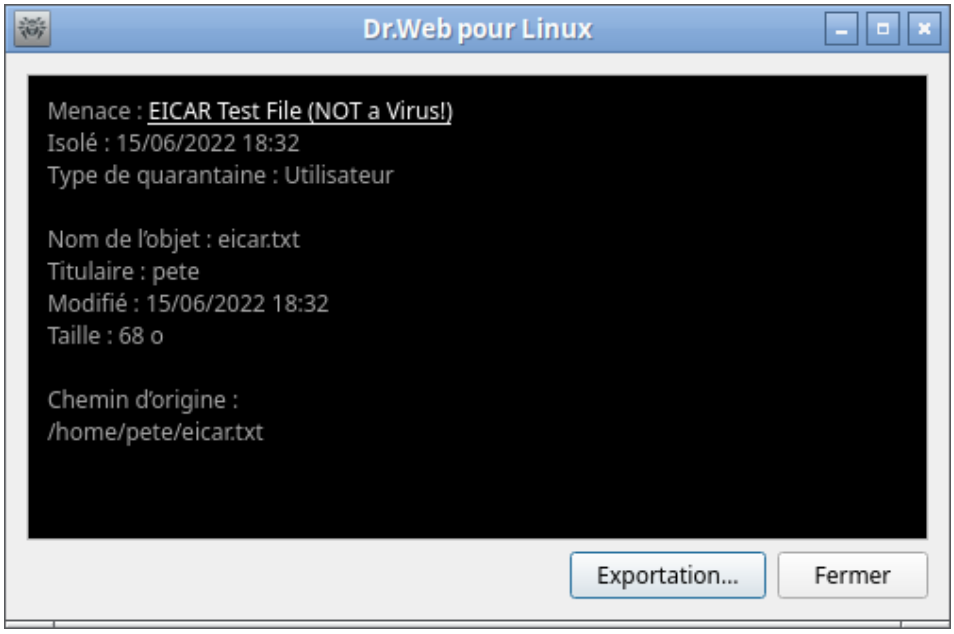

Image 18. Information sur un objet placé en quarantaine

Dans cette fenêtre, les informations suivantes sont fournies :

- Nom de la menace (selon la classification de Doctor Web).
- Date et heure du déplacement de l'objet en quarantaine.
- Type de quarantaine dans lequel l'objet a été déplacé.
- Dernière action appliquée à l'objet et résultat de cette action.

- Détails sur l'objet isolé : nom de l'objet, nom du propriétaire, dernière date de modification et chemin vers l'objet dans le système de fichiers.

Un clic sur le lien portant le nom de la menace ouvre dans le navigateur une page contenant la description de cette menace (vous passez sur le site de Doctor Web, une connexion Internet est requise).

Cliquer sur **Exportation** si vous voulez enregistrer dans un fichier texte les informations affichées dans la fenêtre (une fenêtre s'ouvre dans laquelle vous pouvez sélectionner un fichier pour l'enregistrement des informations). Pour fermer la fenêtre contenant les informations sur la menace et l'objet infecté, cliquez sur **Fermer**.

Mise à jour de la protection antivirus

Dans cette section :

- Informations générales.
- Configurer les mises à jour.
- Problèmes du composant de mise à jour.
- Mise à jour de la protection antivirus sans connexion Internet.

Informations générales

Des mises à jour régulières des bases virales, du moteur antivirus et des bases des catégories de ressources web sont téléchargées et installées par l'Updater automatiquement Vous pouvez consulter les statistiques des bases virales et forcer leur mise à jour sur une page spéciale de la fenêtre de Dr.Web pour Linux. Pour ouvrir la page, cliquez sur **Dernière mise à jour** sur la page d'accueil.

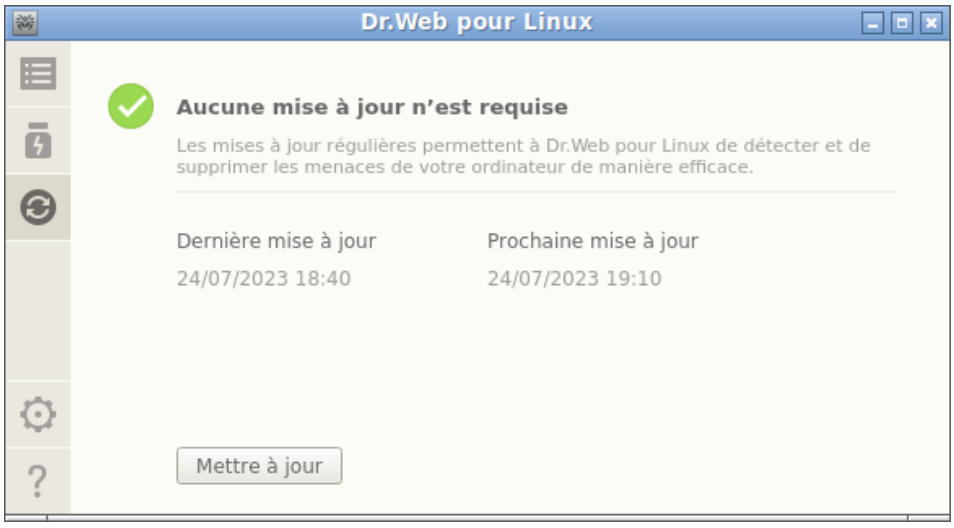

Image 19. Page de gestion de la mise à jour

La page affiche les informations suivantes :

- Statut des bases virales, du moteur antivirus et des bases des catégories de ressources web.

- Données sur la dernière mise à jour et heure de la prochaine mise à jour planifiée.

Pour forcer une mise à jour de la base, cliquez sur **Mettre à jour**. Pour fermer la page de gestion des mises à jour, il suffit de passer à une autre page à l'aide des boutons sur le volet de navigation.

Si Dr.Web pour Linux fonctionne en mode de protection centralisée, cette page sera bloquée.

Configurer les mises à jour

Vous pouvez configurer les paramètres de mise à jour de Dr.Web pour Linux dans la fenêtre des paramètres à l'onglet **Général**.

Problèmes du composant de mise à jour

Si un échec de l'Updater est constaté, une alerte d'erreur s'affiche sur la page de gestion des mises à jour. Pour résoudre le problème, consultez la rubrique Annexe D. Erreurs connues, où vous pouvez trouver une description détaillée des erreurs connues.

Gestionnaire de licences

Dans cette section :

- Informations générales.
- Lancement du Gestionnaire de licence.
- Activation de la licence.
- Supprimer le fichier clé de licence.

Informations générales

En mode graphique, le Gestionnaire de Licences permet de consulter les informations sur la licence actuelle délivrée à l'utilisateur de Dr.Web pour Linux Les données de licence sont stockées dans un fichier clé de licence qui permet le fonctionnement de Dr.Web pour Linux sur l'ordinateur de l'utilisateur. Si aucun fichier clé de licence ni fichier clé de démo n'est trouvé sur l'ordinateur, toutes les fonctionnalités de Dr.Web pour Linux (y compris la vérification des fichiers, le contrôle du système de fichiers et la mise à jour de la base virale) sont bloquées.

Lancement du Gestionnaire de licences

La page du Gestionnaire de licences est disponible dans la fenêtre de Dr.Web pour Linux. Pour ouvrir la page du Gestionnaire de licences, cliquez sur **Licence** sur la page d'accueil de la fenêtre.

Si un fichier clé de démo ou de licence pour Dr.Web pour Linux est déjà installé sur l'ordinateur, la page de démarrage du Gestionnaire de licences affiche les informations sur la licence, y compris le numéro de licence, le nom de propriétaire et la durée de validité. Ces informations sont tirées du fichier clé correspondant.

L'image ci-dessous montre l'apparence de la page du Gestionnaire de Licences.

Image 20. Informations sur la licence

Pour supprimer un fichier clé de licence, cliquez sur ✕ à droite du numéro de la licence.

Vous pouvez fermer le Gestionnaire de Licences à tout moment, il suffit de passer à une autre page à l'aide des boutons sur le volet de navigation.

Activation de la licence

Pour activer une licence via le Gestionnaire de Licences et obtenir le fichier clé correspondant fournissant les fonctionnalités de Dr.Web pour Linux (incluant l'achat d'une nouvelle licence ou le renouvellement de la licence en cours) ou obtenir une version démo, cliquez sur **Obtenir une nouvelle licence**. L'assistant d'enregistrement s'ouvre. Notez que l'assistant d'enregistrement s'ouvre automatiquement uniquement au premier démarrage de Dr.Web pour Linux après son installation.

A la première étape d'activation, choisissez le type d'activation. Trois modes sont disponibles :

1. Activation d'une licence ou d'une démo en utilisant un numéro de série.
2. Obtention d'une version démo.

3. Installation d'un fichier clé obtenu précédemment.

> Pour enregistrer un numéro de série et obtenir un fichier clé de démo, une connexion Internet valide est requise.

1. Activation d'une licence ou d'une démo en utilisant un numéro de série

Pour activer une licence ou une version démo en utilisant un numéro de série, entrez les caractères du numéro de série reçu à l'achat du produit dans le champ et cliquez sur **Activer**.

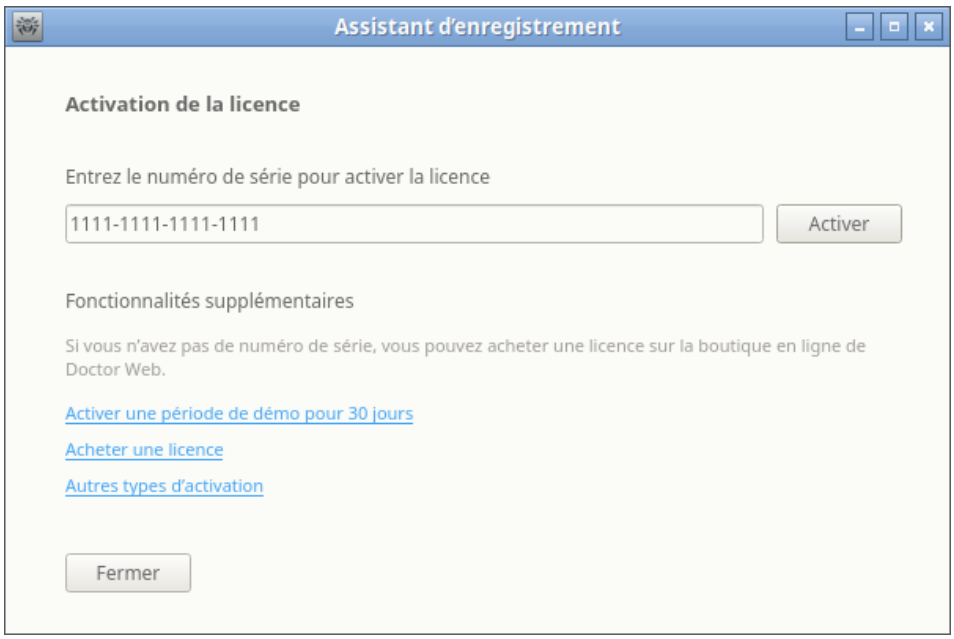

Image 21. Enregistrement avec le numéro de série

> Si vous ne possédez pas de numéro de série ou de fichier clé valide, vous pouvez acheter une licence sur le site officiel de Doctor Web Pour ouvrir la page de la boutique en ligne, cliquez sur **Acheter une licence**.
>
> ---
>
> Pour en savoir plus sur les autres moyens d'acheter une licence pour les produits Dr.Web, consultez la section Enregistrement et activation.

Après un clic sur **Activer**, la connexion avec le serveur d'enregistrement de Doctor Web est établie.

Si le numéro de série indiqué correspond à une licence pour utiliser le produit sur deux ordinateurs, vous devez indiquer sur combien d'ordinateurs vous souhaitez utiliser Dr.Web pour Linux. Si vous choisissez **Sur deux ordinateurs**, vous pouvez activer le deuxième numéro de série de ce kit sur un autre ordinateur et obtenir le deuxième fichier clé. Dans ce cas la durée de validité des licences sur les deux ordinateurs sera la même (par exemple, un an). Si vous choisissez **Sur un ordinateur**, vous serez invité d'indiquer le deuxième numéro de série du kit. Vous ne pourrez plus utiliser ce numéro de série sur un autre ordinateur (ainsi

que la copie du fichier clé de licence, reçu après l'activation de la licence unie), mais la durée de validité de licence sera doublée (par exemple, jusqu'à deux ans si votre licence est valide pour un an).

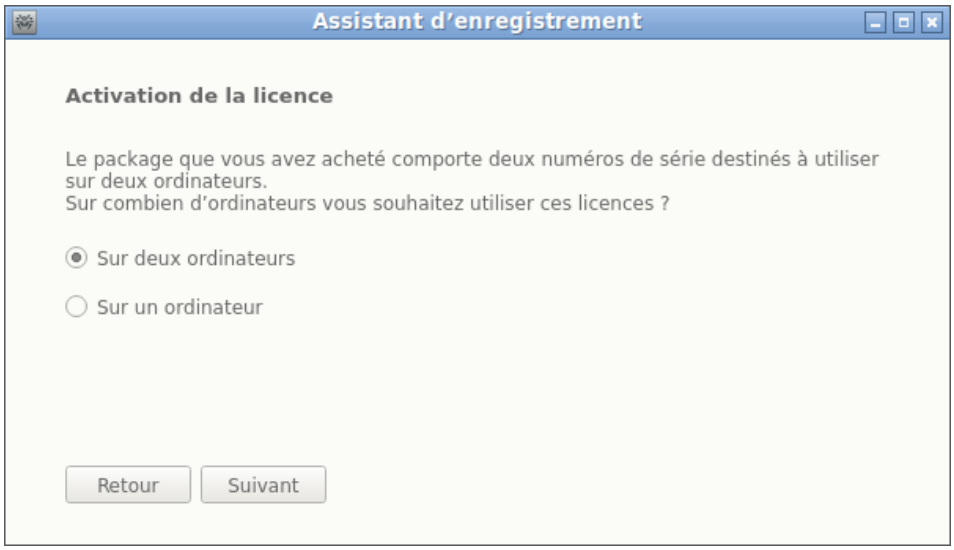

Image 22. Sélectionner le nombre d'ordinateurs

Après avoir sélectionné le nombre d'ordinateurs sur lesquels vous souhaitez activer la licence, cliquez sur **Suivant**. Si vous avez choisi **Sur un ordinateur**, indiquez le deuxième numéro de licence du kit sur la page affichée de l'Assistant. Ensuite cliquez sur **Suivant**.

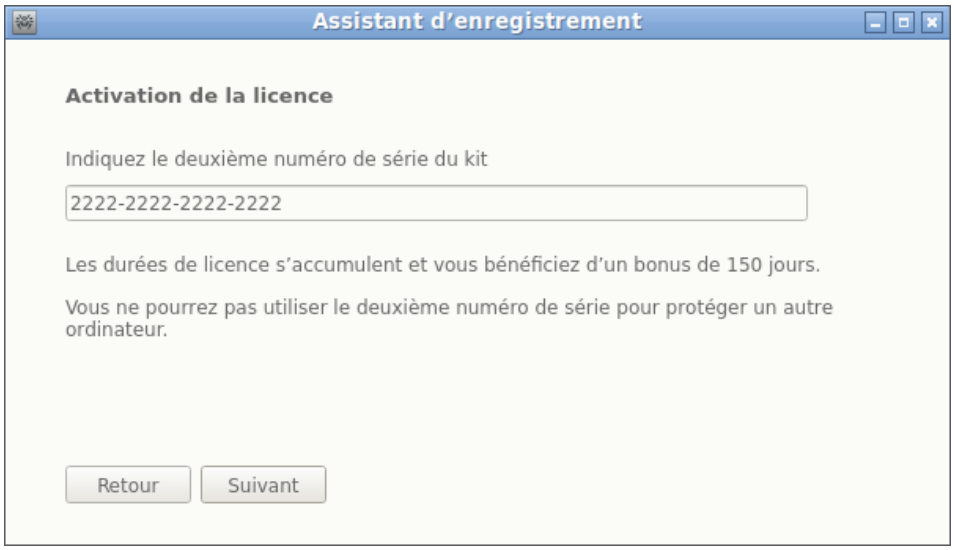

Image 23. Indication du deuxième numéro de licence

Puis vous serez invité à obtenir le bonus de 150 jours ajoutés à la durée de validité de votre nouvelle licence. Pour ce faire, veuillez indiquer des informations concernant la licence précédente si vous en possédez une. Si vous voulez obtenir le bonus, sélectionnez **Indiquer la licence précédente**, si vous ne voulez pas obtenir le bonus ou vous n'avez pas de licence précédente, sélectionnez **Je n'ai pas la licence précédente** et cliquez sur **Suivant**.

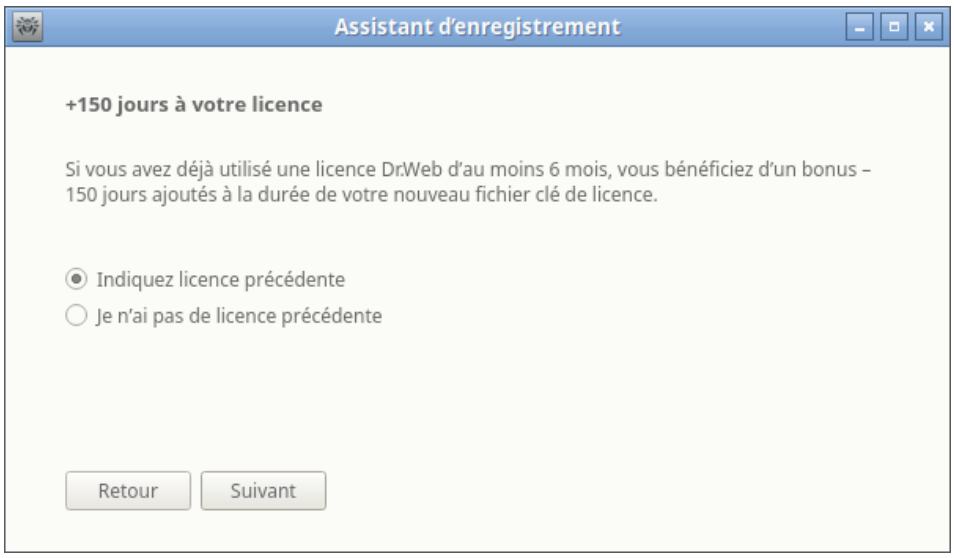

Image 24. Réception du bonus

Si à la première étape vous avez indiqué le *numéro spécial de renouvellement,* vous serez invité d'indiquer la licence précédente pour ne pas perdre le bonus de 150 jours ajoutés à la nouvelle licence. Si, dans ce cas, vous sélectionnez **Je n'ai pas la licence précédente**, vous diminuerez de 150 jours la durée de validité de votre nouvelle licence.

Image 25. Renouvellement de la licence

Si vous avez sélectionné l'élément **Indiquer la licence précédente**, veuillez indiquer le numéro de série de la licence précédente et le chemin vers le fichier clé dans la fenêtre qui s'affiche.

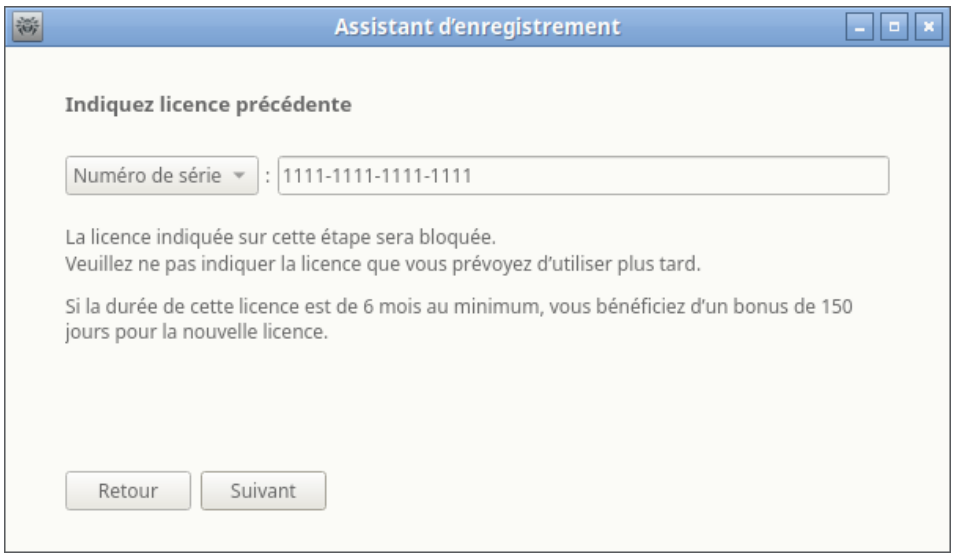

Image 26. Indication de la licence précédente

Si vous indiquez une licence qui n'a pas expiré, la durée de la licence activée sera prolongée par la durée de validité restante de la licence précédente. Si vous activez un kit de deux numéros de série, le bonus sera appliqué en fonction de l'option que vous avez sélectionnée à l'étape précédente de l'assistant d'enregistrement :

- **Sur deux ordinateurs**, *et cet ordinateur est premier*. Pour activer le bonus de 150 jours pour le premier ordinateur, indiquez à cette étape la licence précédente délivrée pour cet ordinateur (s'il y en a une). *N'indiquez pas le second numéro de série du kit ici*.
- **Sur deux ordinateurs**, *et cet ordinateur est second*. Pour activer le bonus de 150 jours pour le second ordinateur, indiquez à cette étape la licence précédente délivrée pour cet ordinateur (s'il y en a une). *N'indiquez pas le premier numéro de série du kit ici*.
- **Sur un ordinateur**. Dans ce cas, non seulement la durée de la licence activée est doublée, mais elle est également étendue de 150 jours (le premier numéro de série apporte un bonus au deuxième numéro). De plus, si à cette étape, vous indiquez la licence précédente délivrée pour cet ordinateur (s'il y en a une), 150 jours de bonus et le reste de validité de la licence indiquée s'ajoutent à la durée doublée de la licence activée.

Pour indiquer la licence précédente, vous pouvez soit entrer son numéro de série dans le champ correspondant, soit donner son fichier clé. Sélectionnez le type de l'information concernant la licence précédente dans la liste déroulante située à gauche du champ d'entrée. Pour indiquer le fichier clé, faites une des actions suivantes :

- Indiquez le chemin vers le fichier dans le champ de saisie.
- Utilisez le sélecteur de fichiers standard en cliquant sur **Parcourir**.
- Glissez/déposez le fichier depuis la fenêtre du gestionnaire de fichiers dans la fenêtre de l'Assistant d'enregistrement.

A la place du fichier clé, vous pouvez indiquer l'archive zip contenant le fichier clé sans la décompresser.

Pour continuer l'enregistrement, cliquez sur **Suivant**.

A l'étape suivante, indiquez vos données d'enregistrement incluant :

- Nom d'enregistrement.
- Votre région (pays) sélectionnée dans la liste.
- Adresse e-mail valide.

Tous les champs du formulaire d'enregistrement sont obligatoires.

Image 27. Page d'information de l'utilisateur

Après avoir rempli tous les champs correctement, cliquez sur **Terminé** pour établir une connexion serveur et obtenir un fichier clé de licence. Si nécessaire, vous pouvez utiliser le fichier clé de licence sur un autre ordinateur après l'avoir supprimé de cet ordinateur.

2. Obtenir une version démo

Si vous souhaitez activer une version démo qui fournit les fonctionnalités complètes des composants Dr.Web pour Linux pour une période de 30 jours, cliquez sur **Activer la période de démo de 30 jours** à la première étape.

Lors de l'activation de la période de démonstration pour un mois via le Gestionnaire de licences, vous ne devez pas fournir des données personnelles.

3. Installation d'un fichier clé obtenu antérieurement

Si vous possédez déjà une licence valide et le fichier clé qui lui est lié (par exemple, obtenu de Doctor Web ou des partenaires de Doctor Web par e-mail), vous pouvez activer Dr.Web pour Linux en installant ce fichier clé. Pour cela, cliquez sur le lien **Autres modes d'activation** à la première étape et indiquez le chemin vers le fichier clé dans le champ qui s'affiche.

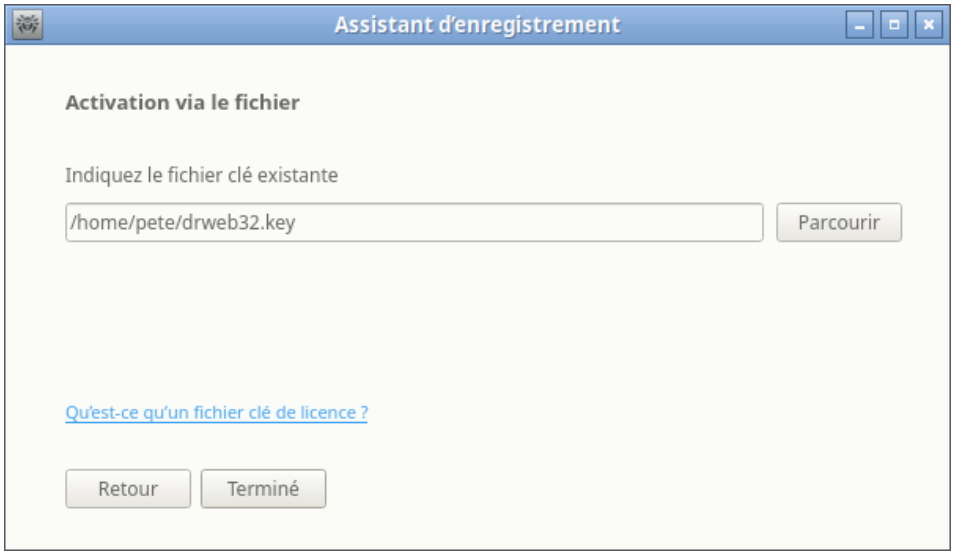

Image 28. Activation en utilisant le fichier clé

Pour spécifier un fichier clé, vous pouvez :

- Indiquez le chemin vers le fichier dans le champ de saisie.
- Utilisez le sélecteur de fichiers standard en cliquant sur **Parcourir**.
- Glissez/déposez le fichier depuis la fenêtre du gestionnaire de fichiers dans la fenêtre de l'Assistant d'enregistrement.

A la place du fichier clé, vous pouvez indiquer l'archive zip contenant le fichier clé sans la décompresser.

Après avoir indiqué le chemin vers le fichier clé (ou le chemin vers l'archive contenant le fichier clé), cliquez sur **Terminer** pour installer le fichier clé automatiquement Si nécessaire, le fichier clé est automatiquement décompressé et copié dans le répertoire des fichiers de Dr.Web pour Linux. Une connexion Internet n'est pas requise.

Après la fin de la procédure de l'activation (quel que soit le type d'activation choisi), la dernière page de l'Assistant avec les notifications correspondantes s'affiche. Cliquez sur **OK** pour quitter l'Assistant d'enregistrement et ouvrez la page principale de Dr.Web pour Linux.

Image 29. Message d'activation réussie

Si une erreur est survenue à n'importe quelle étape de la procédure, une page avec une notification décrivant rapidement l'erreur s'affiche. L'image ci-dessous en montre un exemple.

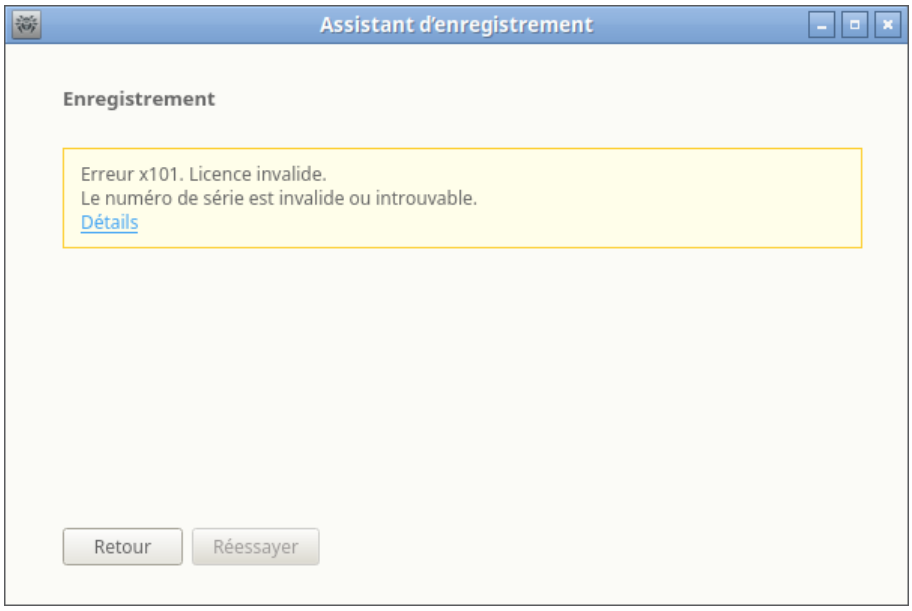

Image 30. Message d'erreur

Si une erreur survient, vous pouvez retourner à l'étape précédente et faire des corrections (par exemple, corriger le numéro de série ou indiquer un chemin correct). Pour retourner à l'étape précédente, cliquez sur **Retour**.

Si l'erreur est due à un problème temporaire (par exemple, un échec réseau temporaire), vous pouvez tenter de recommencer l'opération en cliquant sur **Réessayer**. Si nécessaire, vous pouvez cliquer sur **Fermer** pour annuler l'enregistrement et quitter l'Assistant. Dans ce cas, vous devez recommencer l'enregistrement ultérieurement. Si l'Assistant d'enregistrement ne pourra pas se connecter au serveur d'enregistrement de Doctor Web pour vérifier le numéro de série, un message d'erreur sera affiché.

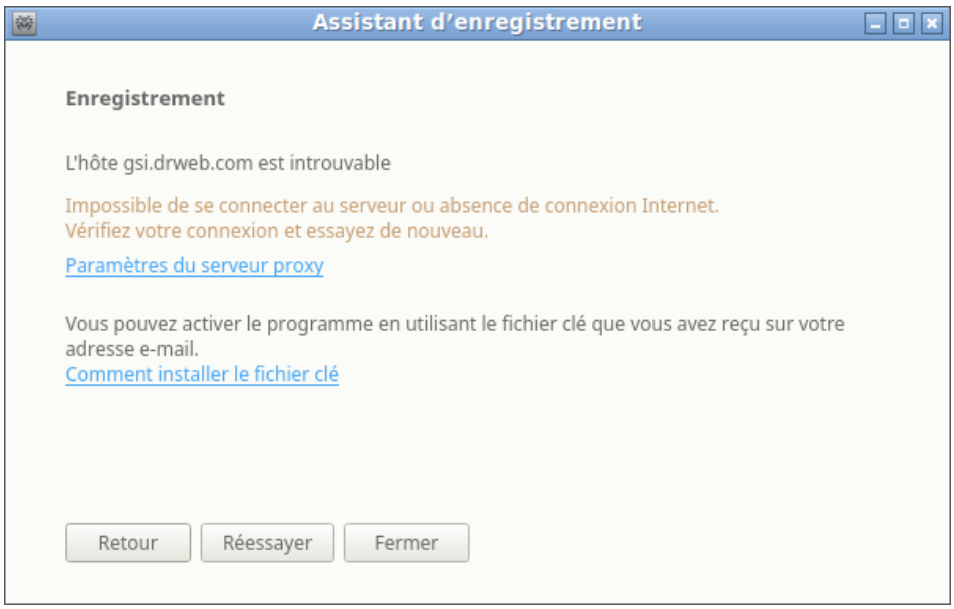

Image 31. Erreur de connexion au serveur d'enregistrement

Si l'erreur est liée à l'impossibilité de vous connecter via Internet, mais vous pouvez vous connecter via le serveur proxy, le passage par le lien **Paramètres du serveur proxy** affiche la fenêtre de paramètres du serveur-proxy :

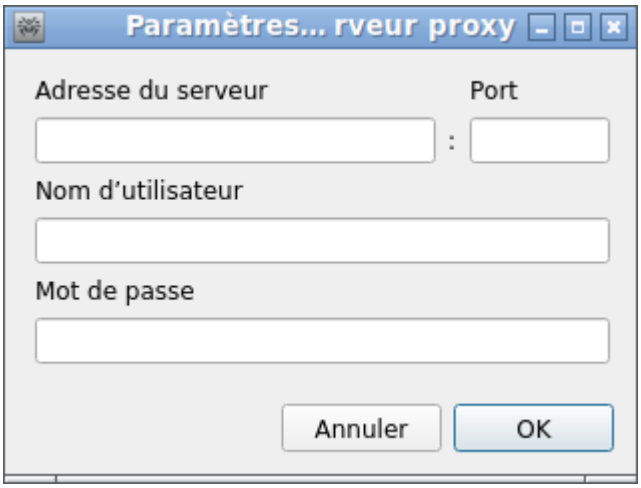

Image 32. Paramètres du serveur proxy

Dans cette fenêtre, spécifiez les paramètres d'accès au serveur proxy et cliquez sur **OK** Puis, réessayez de vous connecter au serveur d'enregistrement de Doctor Web, en cliquant sur **Réessayer**.

Lors de l'activation d'une nouvelle licence et la génération d'un nouveau fichier clé, le fichier clé précédent utilisé par Dr.Web pour Linux, est automatiquement sauvegardé comme copie de sauvegarde dans le répertoire `/etc/opt/drweb.com`. Si nécessaire, vous pouvez réutiliser ce fichier clé en l'installant.

Supprimer le fichier clé de licence

Si nécessaire (par exemple si vous décidez d'utiliser Dr.Web pour Linux sur un autre ordinateur), vous pouvez supprimer un fichier clé de licence installé gérant le fonctionnement de Dr.Web pour Linux. Pour cela, ouvrez la page d'information sur la licence (la page de démarrage du Gestionnaire de Licences) et cliquez sur l'icône ✕ à droite du numéro de la licence en cours.

Ensuite, confirmez la suppression du fichier clé de licence dans la fenêtre qui s'ouvre en cliquant sur **Oui**. Si vous souhaitez annuler la suppression du fichier clé de licence depuis cet ordinateur, cliquez sur **Non**.

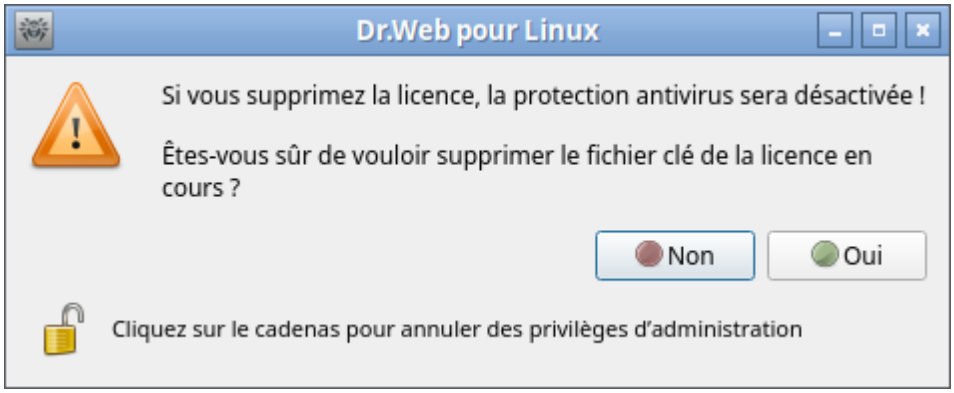

Image 33. Fenêtre de confirmation de la suppression du fichier clé de licence

Pour supprimer un fichier clé de licence, le logiciel doit être démarré avec les privilèges de root. Si au moment de la tentative de suppression du fichier clé, le logiciel ne possède pas de privilèges élevés, le bouton **Oui** n'est pas disponible. Si nécessaire, vous pouvez élever les privilèges et, si cela fonctionne, le bouton **Oui** devient accessible.

La suppression d'un ficher clé de licence n'affecte pas la durée de validité de la licence. Si la licence n'a pas expiré, vous pouvez obtenir un nouveau fichier clé pour cette licence pour la durée de validité restante.

Après la suppression du fichier clé de licence, toutes les fonctionnalités antivirus de Dr.Web pour Linux (analyse de fichiers, mise à jour des bases virales, du moteur antivirus et des bases des catégories de ressources web, surveillance du système de fichiers) sont bloquées jusqu'à ce qu'une nouvelle licence ou version démo soit activée.

Consultation de messages du serveur de protection centralisée

Dans cette section :

- Informations générales.
- Application des actions aux messages.
- Filtrage des messages.

Informations générales

Si Dr.Web pour Linux est géré par le serveur de protection centralisée, l'interface de consultation de messages est disponible. Les messages portent sur l'état du réseau antivirus et ils sont envoyés par le serveur sur les postes qu'il gère. L'administrateur du réseau antivirus peut utiliser cet outil pour surveiller l'état du réseau et des événements importants du serveur de protection centralisée.

> Les messages sur l'état et les événements du réseau antivirus seront reçus uniquement si l'administrateur du réseau antivirus a configuré sur le serveur de protection centralisée auquel Dr.Web pour Linux est connecté l'envoi de messages sur votre poste. Sinon, l'affichage de messages est indisponible et la page correspondante ne s'affiche pas dans la fenêtre d'accueil de Dr.Web pour Linux.

L'interface de consultation de messages du serveur s'affiche sur une page spéciale. Pour ouvrir la page, cliquez sur le bouton  dans le panneau de navigation.

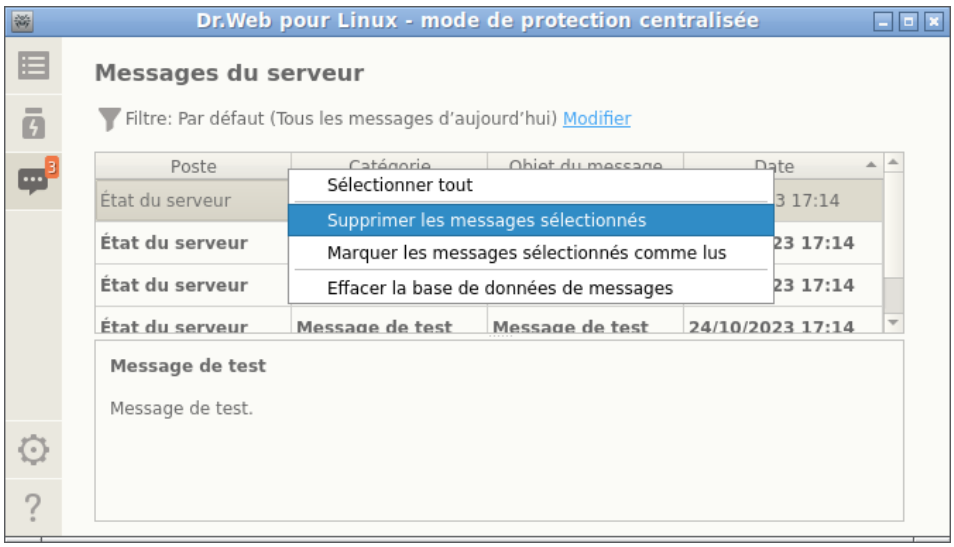

Image 34. Page de consultation de messages du serveur de protection centralisée

Dans la liste, les informations suivantes sont disponibles pour chaque message :

- Nom (adresse) du poste décrit dans le message.
- Catégorie de message.
- En-tête (objet) du message.
- Date et heure de l'envoi du message par le serveur.

Pour consulter un message, il faut le sélectionner dans la liste. Ensuite, le texte du message sélectionné sera affiché dans le panneau sous la liste de messages. Les messages non vus sont en caractères gras.

Le texte de messages sur l'état et les événements du réseau antivirus est rédigé en langue spécifiée dans les paramètres du serveur de protection centralisée.

Application des actions aux messages

Pour appliquer une action à un message, cliquez droit sur la ligne contenant les informations sur le message et sélectionnez une action dans le menu qui s'affiche. Pour appliquer une action à plusieurs messages, sélectionnez-les avant d'ouvrir le menu. Vous pouvez les sélectionner avec la souris en maintenant appuyées les touches CTRL ou SHIFT :

- Si vous maintenez appuyée la touche CTRL, les messages s'ajouteront à la liste de sélection un par un.
- Si vous maintenez appuyée la touche SHIFT, les messages seront sélectionnés comme une liste continue.

Pour sélectionner tous les messages, utilisez la combinaison de touches CTRL+A.

Les actions suivantes sont disponibles pour les objets isolés :

- Sélectionner dans la liste tous les messages concernés par le filtre actuel.
- Supprimer les messages sélectionnés.
- Marquer les messages sélectionnés comme lus.
- Nettoyer la base de données de messages.

Lors du nettoyage de la base de données de messages, tous les messages reçus seront supprimés (y compris les messages non lus).

Notez que pour les messages reçus du serveur de protection centralisée il existe une durée maximale de stockage dans la base de données qui est spécifiée dans les paramètres. A l'issue de cette période, les messages sont supprimés automatiquement.

Filtrage des messages

Vu que le nombre de messages du serveur peut être assez élevé, il existe une possibilité de filtrer les messages par l'adresse du serveur expéditeur, par le nom du poste du réseau antivirus, par la catégorie de messages ou la période de réception. Le filtre par défaut affiche dans la liste les messages de toutes les catégories reçus depuis tous les serveur au cours de cette journée.

Si nécessaire, vous pouvez modifier le filtre d'affichage de messages. Pour ce faire, cliquez sur le lien **Modifier**. Ensuite, dans la partie supérieure, un panneau de modification du filtre s'affichera.

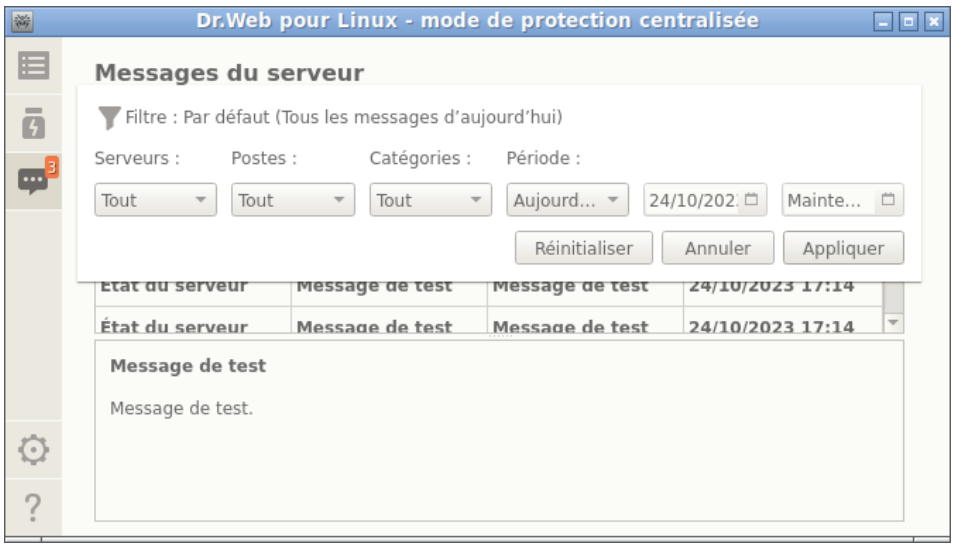

Image 35. Panneau du filtre de messages

Dans le panneau du filtre, vous pouvez indiquer les paramètres suivants de filtrage de messages :

- **Serveurs** : liste des serveurs dont les messages seront affichés.
- **Postes** : liste des postes, les messages sur lesquels seront affichés.
- **Catégories** : liste des catégories de messages à afficher.
- **Période** : période de création de messages à afficher (à part la sélection de la période dans la liste, vous pouvez indiquer le début et la fin de la période de création de messages par le serveur).

Pour enregistrer les modifications apportées dans le filtre, cliquez sur **Appliquer**. Pour fermer le panneau du filtre sans appliquer les modifications, cliquez sur **Annuler**. Pour réinitialiser les valeurs par défaut, cliquez sur **Réinitialiser**.

Gestion des privilèges du logiciel

Certaines actions avec Dr.Web pour Linux peuvent être effectuées en mode graphique uniquement si l'application possède des privilèges élevés (*privilèges d'administrateur*) qui correspondent aux droits du *super-utilisateur* (utilisateur *root*). Pour élever les privilèges, les fonctions suivantes sont requises :

1. Gestion des objets déplacés en quarantaine (c'est-à-dire dans le répertoire de quarantaine qui n'appartient pas à l'utilisateur qui a lancé Dr.Web pour Linux).
2. Analyse de fichiers et dossiers d'autres utilisateurs (notamment ceux de super-utilisateur).
3. Désactivation du moniteur du système de fichiers SpIDer Guard.
4. Désactivation du moniteur de connexions réseau SpIDer Gate.
5. Suppression du fichier clé de licence, connexion et déconnexion du serveur de protection centralisée.

Même si le logiciel est lancé par le super-utilisateur (par exemple, avec les commandes `su` ou `sudo`), il *ne reçoit pas* de privilèges élevés par défaut.

Toutes les pages de Dr.Web pour Linux qui permettent des actions requérant des privilèges élevés présentent un bouton spécifique avec l'icône d'un cadenas. L'icône indique si le logiciel Dr.Web pour Linux possède ou pas des privilèges élevés :

	Le logiciel ne possède pas de privilèges élevés. Cliquez sur le cadenas pour élever les privilèges jusqu'aux privilèges de super-utilisateur.
	Les privilèges du logiciel sont élevés jusqu'aux privilèges de super-utilisateur. Cliquez sur l'icône pour baisser les privilèges ; c'est-à-dire pour passer des privilèges de super-utilisateur aux droits d'utilisateur.

Lorsque vous cliquez sur l'icône pour élever les privilèges, la fenêtre d'authentification de l'utilisateur s'ouvre.

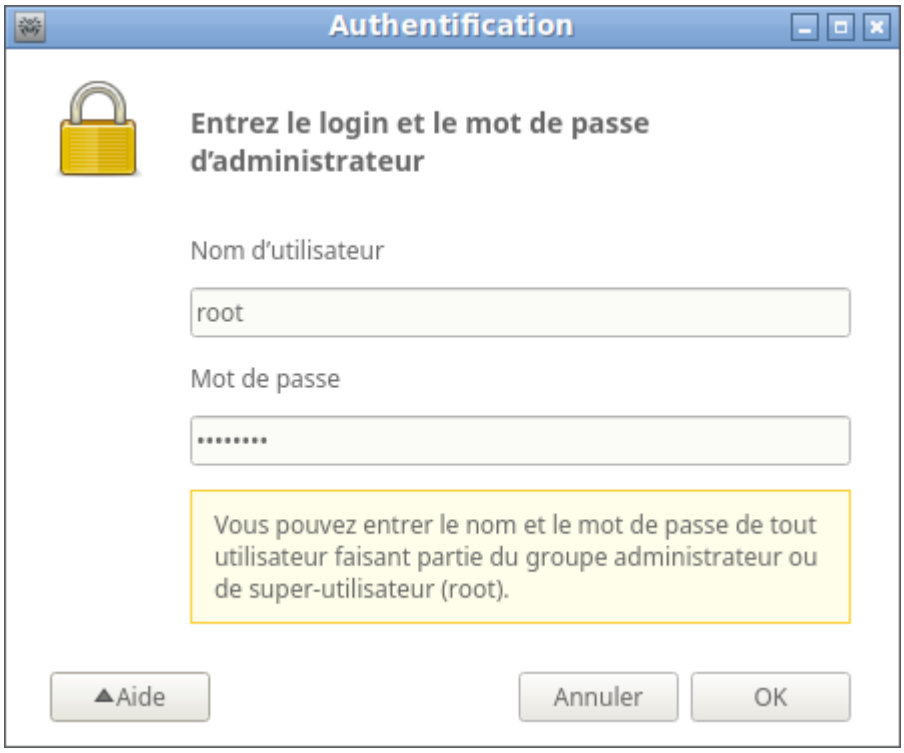

Image 36. Fenêtre d'authentification

Pour attribuer au logiciel des privilèges de super-utilisateur, indiquez le nom (login) et le mot de passe d'un utilisateur dont le compte est inclus au groupe d'utilisateurs de Dr.Web pour Linux en tant que *groupe d'administrateurs* ou le login et le mot de passe de super-utilisateur (compte *root*) et cliquez sur **OK**. Pour annuler l'augmentation de privilèges, fermez la fenêtre en cliquant sur **Annuler**. Pour afficher ou masquer un court texte d'aide, cliquez sur le bouton **Aide**.

Durant l'installation de Dr.Web pour Linux, un groupe d'utilisateurs qui peut élever ses droits jusqu'aux privilèges de super-utilisateur (par exemple, le groupe *sudo*) est choisi comme groupe d'administrateurs. Si la tentative de recherche de ce groupe échoue, vous pouvez entrer le login et le mot de passe de super-utilisateur (*root*) dans la fenêtre d'authentification pour élever les droits du logiciel.

Le passage des privilèges administrateur aux droits utilisateur ne requiert pas d'authentification.

Aide et références

Pour accéder aux documents de référence, cliquez sur  sur le panneau de navigation de la fenêtre Dr.Web pour Linux.

Un menu déroulant contenant les éléments suivants va s'ouvrir sur l'écran :

- **Aide** : ouvrir le Manuel utilisateur de Dr.Web pour Linux.
- **Forum Dr.Web** : ouvrir la page web du forum officiel de Doctor Web (une connexion Internet est requise).
- **Support technique** : ouvrir la page web du support technique de Doctor Web (une connexion Internet est requise).
- **Mon Dr.Web** : ouvrir votre page web personnelle sur le site officiel de Doctor Web (une connexion Internet est requise).
- **À propos du programme** : ouvrir une fenêtre contenant de brèves informations sur Dr.Web pour Linux et sa version.

De plus, lorsqu'une des pages de la fenêtre principale de Dr.Web pour Linux affiche un message d'erreur, vous pouvez cliquer sur le lien **En savoir plus** pour obtenir des informations sur l'erreur et les conseils pour résoudre le problème.

Configurer les paramètres de fonctionnement

Dans la fenêtre des paramètres, vous pouvez configurer les paramètres du logiciel suivants :

- Périodicité des mises à jour.
- Réactions de Dr.Web pour Linux aux menaces détectées lors d'un scan à la demande effectué par le Scanner et par le moniteur du système de fichiers SpIDer Guard.
- Liste des objets à exclure de l'analyse du Scanner et de SpIDer Guard.
- Paramètres du contrôle de connexions réseau.
- Planification pour lancer des scans réguliers effectués par le Scanner.
- Mode de protection (autonome, protection centralisée).
- Utilisation du service Dr.Web Cloud.

est exécuté dans la fenêtre des paramètres de Dr.Web pour Linux.

Pour ouvrir la fenêtre des paramètres, cliquez  sur le panneau de navigation.

Dans la fenêtre des paramètres, les onglets suivants sont disponibles :

- Général : permet de configurer les notifications et la fréquence des mises à jour automatiques.
- Scanner : permet de configurer les réactions de Dr.Web pour Linux face aux menaces détectées durant le scan à la demande ou planifié.
- SpIDer Guard : permet de configurer les réactions de Dr.Web pour Linux aux menaces détectées par le moniteur du système de fichiers SpIDer Guard.
- SpIDer Gate : permet de configurer les paramètres du contrôle de connexions réseau effectué par le moniteur SpIDer Gate.
- Exclusions : perment de définir la liste des objets à exclure du scan à la demande, du scan d'après la planification, ou de la liste des objets surveillés par SpIDer Guard et contrôlés par SpIDer Gate.
- Planificateur : permet de configurer la planification pour lancer les scans.
- Réseau : permet d'activer ou de désactiver le mode de vérification des connexions réseau (basées sur SSL/TLS, comme, par exemple, HTTPS) pour SpIDer Gate, ainsi que de sauvegarder dans un fichier le certificat Dr.Web utilisé pour intercepter les connexions réseau sécurisées.
- Mode : permet de sélectionner le mode de protection de Dr.Web pour Linux (autonome, protection centralisée).
- Dr.Web Cloud : permet d'interdire ou d'autoriser à Dr.Web pour Linux l'utilisation du service Dr.Web Cloud.

Pour accéder à Aide, cliquez  sur la page correspondante de la fenêtre de paramètres.

Toutes les modifications apportées dans ces onglets sont appliquées immédiatement.

Notez que lorsque Dr.Web pour Linux opère en mode Protection centralisée, certains paramètres peuvent ne pas être disponibles.

Paramètres principaux

Dans cette section :

- Informations générales.
- Configurer le serveur proxy utilisé pour obtenir des mises à jour.

Informations générales

Dans l'onglet **Général**, vous pouvez configurer les paramètres principaux du logiciel.

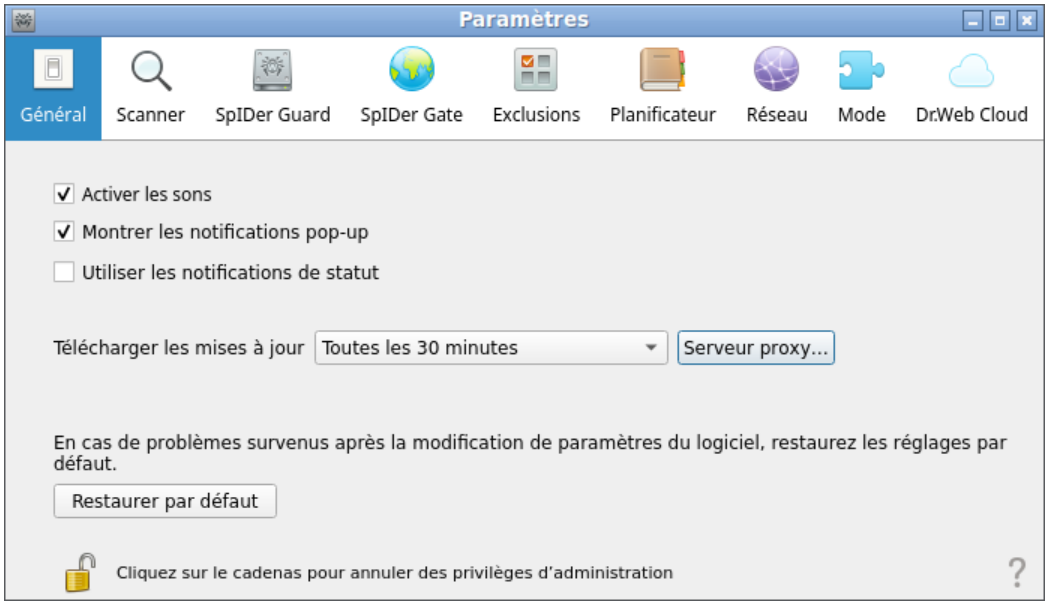

Image 37. Onglet des paramètres principaux

Option	Action
Case **Sons pour les événements**	Cochez cette case si vous souhaitez que Dr.Web pour Linux utilise les notifications sonores pour des événements particuliers comme : • détection d'une menace (par le Scanner et par SpIDer Guard) ; • erreur de scan de l'objet ; • etc.
Case **Afficher des pop-ups d'événements**	Cochez cette case si vous souhaitez que Dr.Web pour Linux affiche des notifications pop-up pour des événements particuliers comme : • détection de menaces ; • erreur de scan ; • etc.
Case **Utiliser les notifications sur le statut**	La définition de cette case indique à Dr.Web pour Linux d'afficher les notifications pop-up en cas de changement de statut des composants (par exemple, en cas de leur activation ou désactivation).
Liste déroulante **Télécharger les mises à jour**	Choisissez la fréquence à laquelle l'Updater vérifiera la disponibilité de mises à jour pour les bases virales, les bases des catégories de ressources web et le moteur antivirus.
Bouton **Serveur proxy**	Cliquez pour configurer les paramètres du serveur proxy pour la réception des mises à jour (l'Updater utilise un serveur proxy si le contact avec des serveurs externes est interdit par la politique de sécurité réseau).

Option	Action
Bouton **Réinitialiser les paramètres**	Cliquez pour restaurer les paramètres par défaut.

Pour gérer les paramètres de mise à jour et les réinitialiser par défaut, le logiciel doit posséder des privilèges de super-utilisateur. Pour en savoir plus, consultez la section Gestion des privilèges du logiciel.

Configurer le serveur proxy pour les mises à jour

Dans la fenêtre des paramètres permettant de configurer l'utilisation d'un serveur proxy par l'Updater, vous pouvez :

- Activer ou désactiver l'utilisation du serveur proxy pour recevoir les mises à jour.
- Adresse du serveur proxy utilisé pour recevoir les mises à jour.
- Port utilisé pour la connexion au serveur proxy.
- Indiquer le nom et mot de passe de l'utilisateur utilisé pour l'authentification sur le serveur proxy.

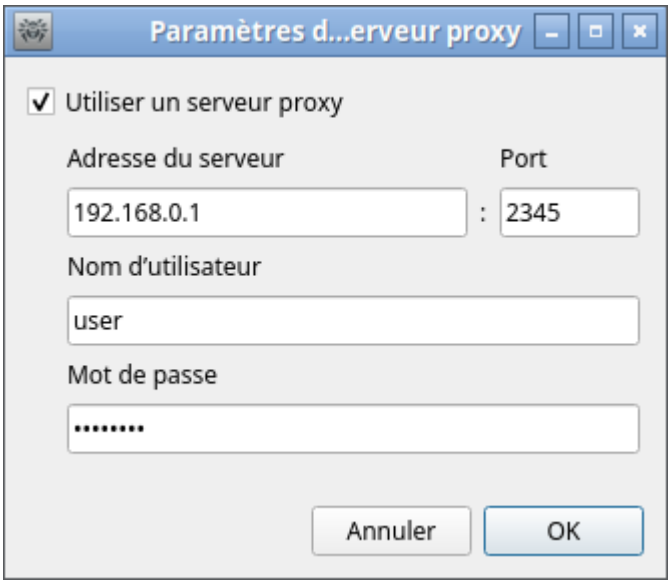

Image 38. Paramètres du serveur proxy

On peut indiquer en tant qu'adresse l'adresse IP ou FQDN du nœud sur lequel fonctionne le serveur proxy. L'adresse et le port sont obligatoires à indiquer. Puisque la mise à jour s'effectue via le protocole HTTP, il est nécessaire d'utiliser le serveur proxy HTTP. Le nom et le mot de passe sont obligatoires à indiquer seulement au cas où le serveur proxy HTTP exige l'authentification.

Pour appliquer les modifications et fermer la fenêtre, cliquez sur **OK**. Pour rejeter les modifications et fermer la fenêtre, cliquez sur **Annuler**.

Paramètres du scan de fichiers

Dans cette section :

- Informations générales.
- Paramètres avancés du scan de fichiers.

Informations générales

Dans l'onglet **Scanner**, vous pouvez définir les actions que Dr.Web pour Linux applique aux menaces détectées lors du scan de fichiers à la demande de l'utilisateur ou selon la planification.

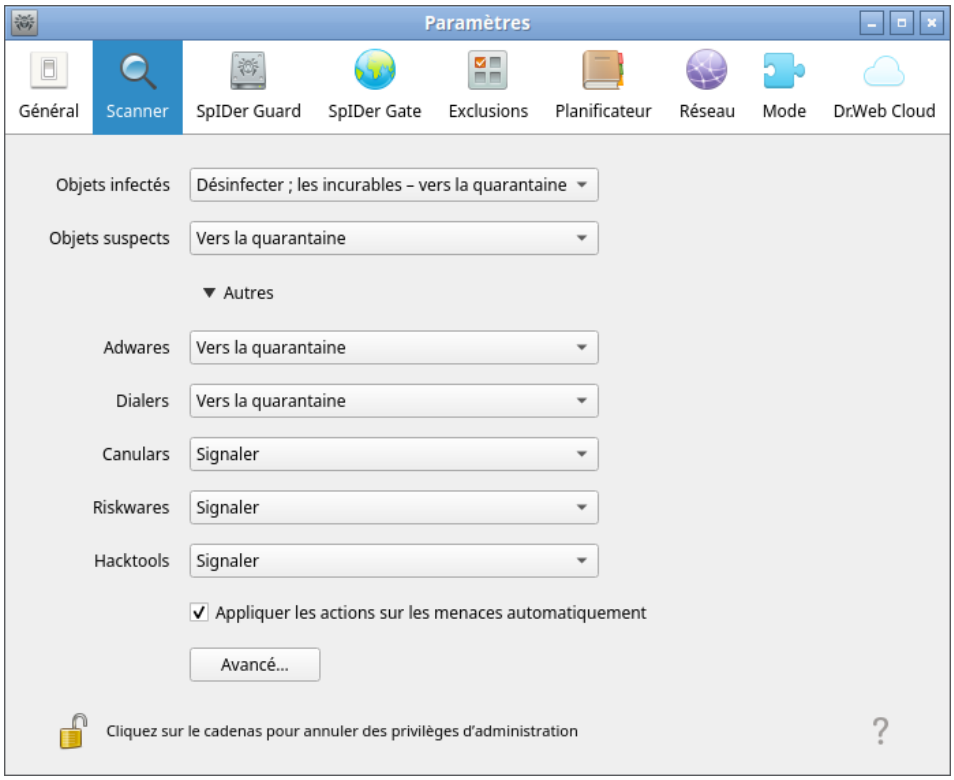

Image 39. Onglet des paramètres du scan des fichiers par le Scanner

Dans les listes déroulantes, sélectionnez les actions que Dr.Web pour Linux appliquera aux objets en cas de détection d'une menace de type correspondant.

Si la menace est détecté dans un fichier se trouvant dans un conteneur (archive, message, etc.), le conteneur n'est pas supprimé mais il est mise en quarantaine.

Cochez la case **Appliquer automatiquement les actions aux menaces**, si vous souhaitez que Dr.Web pour Linux applique des actions spécifiques aux menaces au moment de leur détection par le Scanner lors de l'analyse sur demande ou selon la planification. Dans ce cas, l'utilisateur est notifié de la neutralisation et les informations sur la menace neutralisée sont ajoutées à liste des menaces. Si la case n'est pas cochée, le Scanner ajoute la menace détectée à la liste de

menaces détectées et l'utilisateur sélectionne manuellement l'action à appliquer à l'objet contenant la menace détectée.

Pour ouvrir la fenêtre de paramètres de l'analyse de fichiers, cliquez sur **Avancé**.

Remarques :

- Vous pouvez exclure les fichiers et les répertoires de l'analyse du Scanner dans l'onglet **Exclusions**.
- Les réactions à la détection des menaces, y compris l'application automatique des actions spécifiées pour le Scanner, n'influencent pas le comportement du moniteur SpIDer Guard. Ses réactions à la détection des menaces sont spécifiées dans la page correspondante.

Pour modifier les réactions du Scanner sur les menaces et pour accéder aux paramètres avancés, il faut que l'application possède des privilèges élevés. Voir Gestion des privilèges du logiciel.

La configuration du Scanner lors du fonctionnement de Dr.Web pour Linux sous la gestion du serveur de protection centralisée peut être bloquée si cela est interdit par le serveur.

Paramètres avancés du scan de fichiers

Dans la fenêtre des paramètres avancés, vous pouvez configurer les paramètres du Scanner comme :

- Activer ou désactiver le scan du contenu des conteneurs :
  - Archives.
  - Fichiers e-mail.
- Définir la durée maximum de scan d'un fichier.

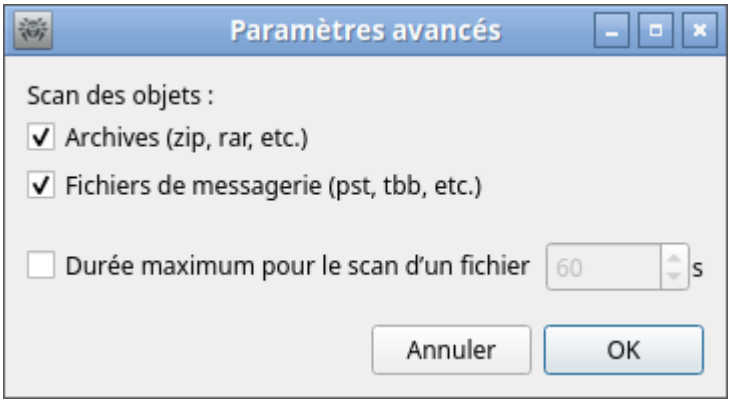

Image 40. Paramètres avancés du scan de fichiers

Si les cases ne sont pas cochées, les conteneurs seront également scannés, mais uniquement comme des objets globaux, sans analyse de leur structure interne.

Pour appliquer les modifications et fermer la fenêtre, cliquez sur **OK**. Pour rejeter les modifications et fermer la fenêtre, cliquez sur **Annuler**.

Paramètres du contrôle du système de fichiers

Dans l'onglet **SpIDer Guard**, vous pouvez définir des actions que Dr.Web pour Linux doit appliquer aux menaces détectées par le moniteur SpIDer Guard.

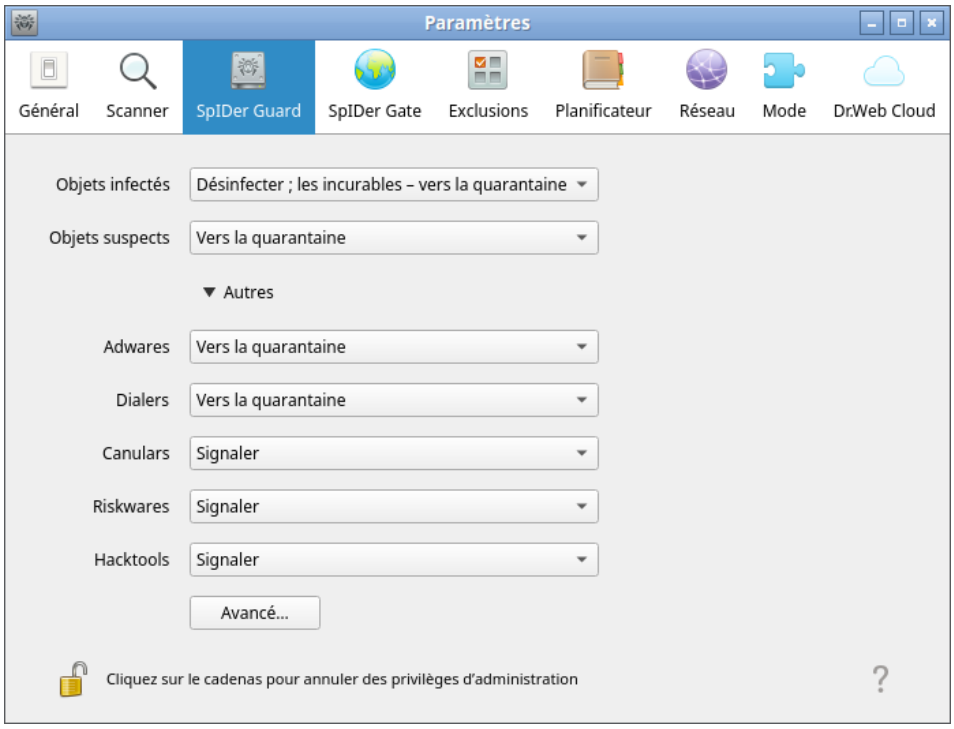

Image 41. Onglet de la configuration de la surveillance du système de fichiers

Cet onglet y compris la fenêtre des paramètres avancés est identique à celui de configuration du scan de fichiers (onglet **Scanner**).

Si la menace est détecté dans un fichier se trouvant dans un conteneur (archive, message, etc.), le conteneur n'est pas supprimé mais il est mise en quarantaine.

Remarques :

- Vous pouvez exclure les fichiers et les répertoires de la surveillance du moniteur SpIDer Guard dans l'onglet **Exclusions**.
- L'activation du mode de surveillance renforcé des fichiers par le moniteur SpIDer Guard est décrite dans la section Modes de surveillance des fichiers.
- Les réactions à la détection des menaces, spécifiées pour le moniteur SpIDer Guard, n'influencent pas le comportement du Scanner. Ses réactions à la détection des menaces sont spécifiées dans la page correspondante.

Le réglage des paramètres de SpIDer Guard demande que le logiciel possède des privilèges élevés. Pour en savoir plus, voir Gestion des privilèges du logiciel.

La configuration de SpIDer Guard lors du fonctionnement de Dr.Web pour Linux sous la gestion du serveur de protection centralisée peut être bloquée si cela est interdit par le serveur.

Configuration de la surveillance des connexions réseau

Dans cette section :

- Informations générales.
- Sélection des catégories de sites Web.
- Gestion des paramètres des fichiers.

Informations générales

Dans l'onglet **SpIDer Gate**, vous pouvez configurer les politiques de sécurité que le moniteur de connexions réseau SpIDer Gate va utiliser lors du contrôle de l'accès à Internet.

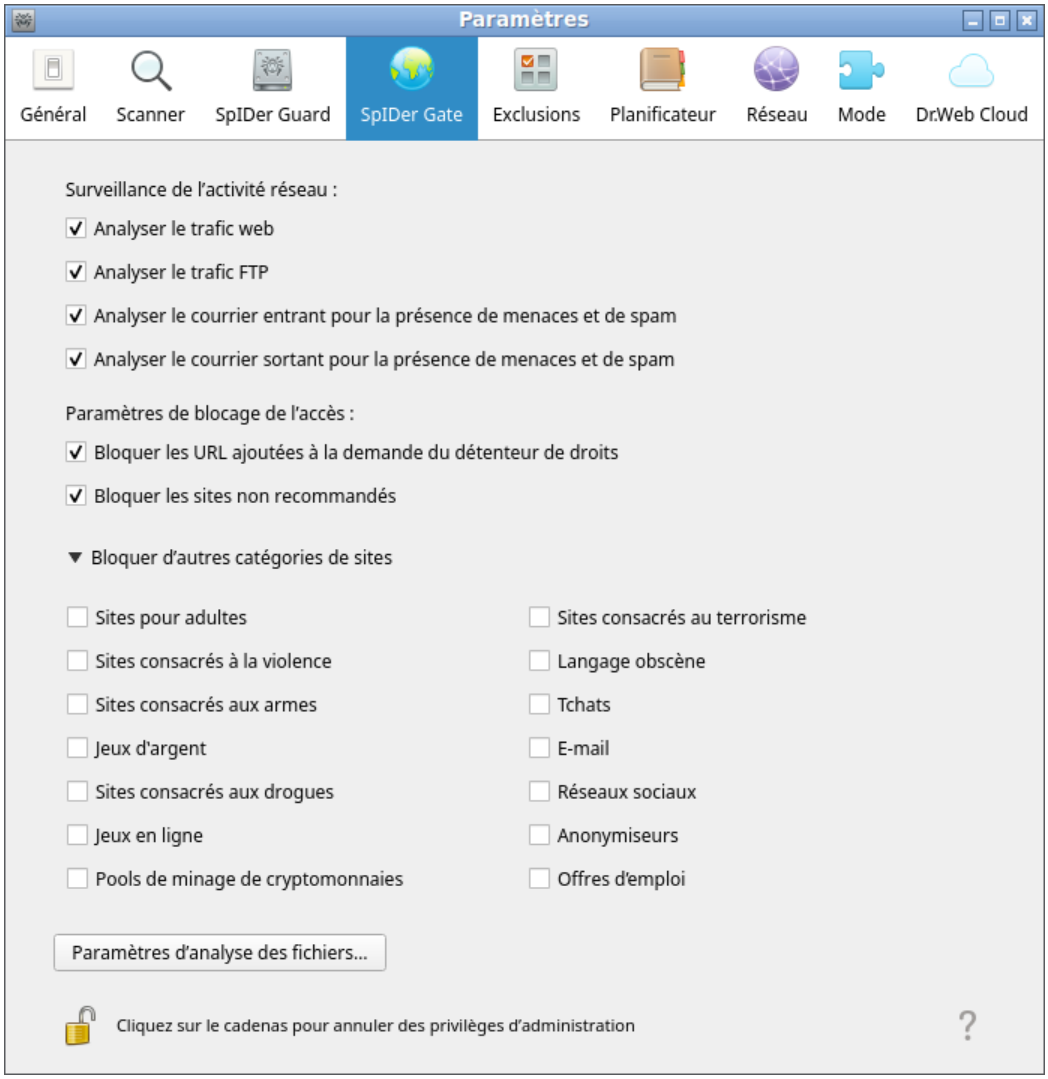

Image 42. Onglet des paramètres du contrôle d'accès au réseau

En basculant les interrupteur dans la section **Surveillance de l'activité réseau**, vous pouvez déterminer quels types de l'activité réseau sont contrôlés par le moniteur, s'il est activé.

Sélection des catégories de sites Web

Les interrupteurs dans la section **Paramètres de surveillance** déterminent les catégories de sites et de hôtes auxquelles l'accès est bloqué (cela concerne non seulement les tentatives d'accès via le navigateur, mais aussi les tentatives d'accès aux serveurs FTP). En basculant les interrupteurs correspondants, vous pouvez interdire ou autoriser l'accès à des sites web et des noeuds des catégories suivantes :

Catégorie	Description
URL listées suite à une requête d'un propriétaire de copyright	Les sites Web dont le contenu viole le copyright (d'après son propriétaire), par exemple, les sites pirates, les répertoires de liens de fichiers, les sites de partage de fichiers, etc.

Catégorie	Description
Sites non recommandés	Les sites web au contenu douteux (suspecté de phishing ou de vol de mot de passé, etc.).
Sites pour adultes	Sites web avec du contenu pour adultes
Violence	Sites web dont le contenu traite d'actes violents (par exemple actes de terrorisme, images de scènes de guerre, etc.)
Armes	Sites dont le contenu donne des informations sur les armes et les explosifs
Jeux d'argent	Sites web de jeux de hasard, jeux d'argent et casinos en ligne
Drogues	Sites web dont le contenu traite de production, distribution et consommation de drogues
Langage obscène	Sites web dont le contenu emploie un langage obscène
Tchats	Sites web de chat
Terrorisme	Sites à caractère terroriste
E-mail	Sites web proposant la création d'email gratuit
Réseaux sociaux	Sites web de réseaux sociaux
Jeux en ligne	Sites de jeux nécessitant la connexion Internet permanente.
Anonymiseurs	Sites permettant aux utilisateurs de masquer leurs informations personnelles et donnant accès à des sites bloqués.
Pools de minage de cryptomonnaies	Sites donnant accès aux services rassemblant les utilisateurs pour le minage de cryptomonnaies.
Offres d'emploi	Sites de recherche d'emploi

La base des catégories de ressources web est fournie avec Dr.Web pour Linux et elle est mise à jour automatiquement lors de la mise à jour des bases virales. L'utilisateur ne peut pas modifier le contenu de la base des catégories de ressources web.

Le même site web peut appartenir à plusieurs catégories. Le moniteur de connexions réseau SpIDer Gate va bloquer l'accès au site web ou à l'hôte s'il est inclus au moins dans une des catégories des sites auxquelles l'accès est bloqué. Cliquez sur l'inscription **Bloquer les autres catégories de sites** pour afficher ou masquer la liste des catégories disponibles.

S'il faut bloquer l'accès à un site web ou à un hôte qui n'appartient pas à ces catégories, ajoutez-le à la liste noire. Si, en revanche, il faut autoriser l'accès à un site web ou à un hôte même s'il est inclus dans une des catégories non recommandées, ajoutez-le à la liste blanche.

De plus, vous pouvez configurer la liste des applications dont les connexions réseau ne sont pas contrôlées par le moniteur SpIDer Gate.

Vous pouvez configurer la liste blanche et noire des sites web et des applications exclus de la surveillance du moniteur SpIDer Gate dans l'onglet **Exclusions**.

> Il existe une catégorie particulière de sites web — *Sources de propagation de virus*. L'accès aux sites et aux hôtes de cette catégorie sera interdit dans tous les cas, même s'ils sont inclus dans la liste blanche.

Gestion des paramètres des fichiers

Pour configurer les paramètres que SpIDer Gate va utiliser lors de l'analyse des fichiers téléchargés sur Internet, cliquez sur **Paramètres du scan de fichiers**.

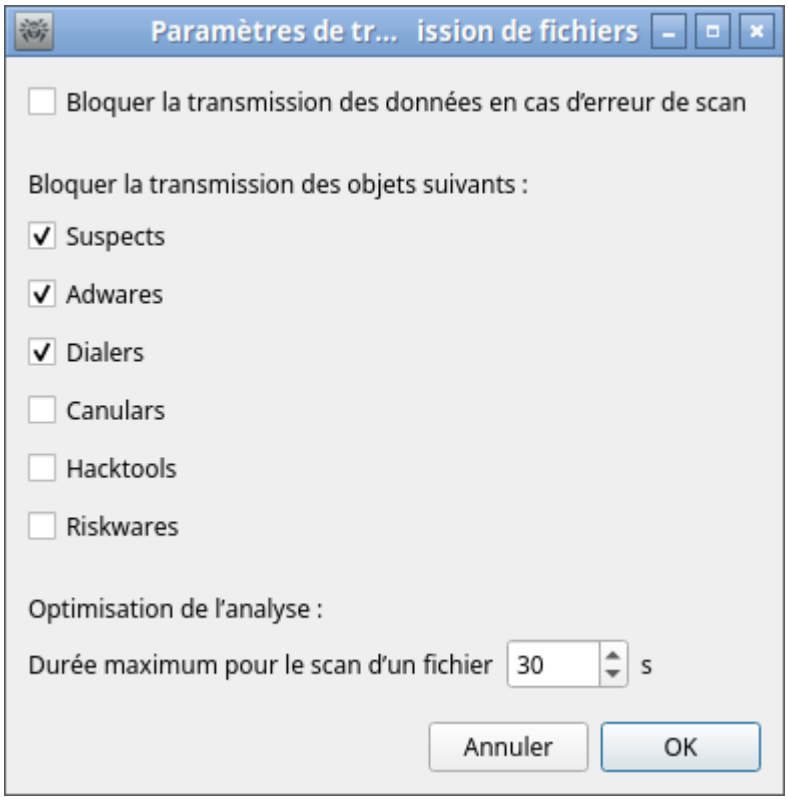

Image 43. Fenêtre de la gestion des paramètres de scan de fichiers

Dans la fenêtre qui s'ouvre, vous pouvez choisir les catégories des objets malveillants à bloquer lors d'une tentative de les transmettre. Si une case est cochée, les fichiers contenant une menace de type correspondant seront rejetés lors d'une tentative de les télécharger sur l'ordinateur. Si la case n'est pas cochée, les fichiers contenant des menaces de ce type seront téléchargés par Internet. Vous pouvez également indiquer la durée maximum d'analyse de fichiers téléchargés (et d'e-mails). Si l'option **Bloquer la transmission des données en cas d'erreur d'analyse** est activée, les fichiers qui ne sont pas analysés à cause d'une erreur sont

bloqués et ne peuvent pas être téléchargés. Pour autoriser le téléchargement des fichiers et des e-mails non analysés, décochez la case (non recommandé).

> Si le scan d'un fichier téléchargé a échoué parce que le délai d'analyse a expiré, ce fichier *ne sera pas* traité comme non vérifié et ne sera pas bloqué même si la case **Bloquer la transmission des données en cas d'erreur d'analyse** est cochée.

Pour appliquer les modifications et fermer la fenêtre, cliquez sur **OK**. Pour rejeter les modifications et fermer la fenêtre, cliquez sur **Annuler**.

> Pour modifier les paramètres du moniteur de connexions réseau SpIDer Gate, l'application doit avoir des privilèges élevés. Voir Gestion des privilèges du logiciel.

Exclusions

Dans l'onglet **Exclusions**, les boutons suivants sont disponibles et permettent de configurer les exclusions suivantes :

- **Fichiers et répertoires** : ouvrir la fenêtre contenant la liste des chemins d'accès aux objets du système de fichiers exclus de l'analyse du Scanner et du moniteur du système de fichiers SpIDer Guard.
- **Sites Web** : ouvrir la fenêtre de gestion des listes blanches et noires de sites web. L'accès à ces sites sera réglé indépendamment des stratégies de blocage spécifiées pour le moniteur de connexions réseau SpIDer Gate.
- **Annexes** : ouvrir la fenêtre contenant la liste des applications dont les connexions réseau ne seront pas contrôlées par le moniteur de connexions réseau SpIDer Gate.

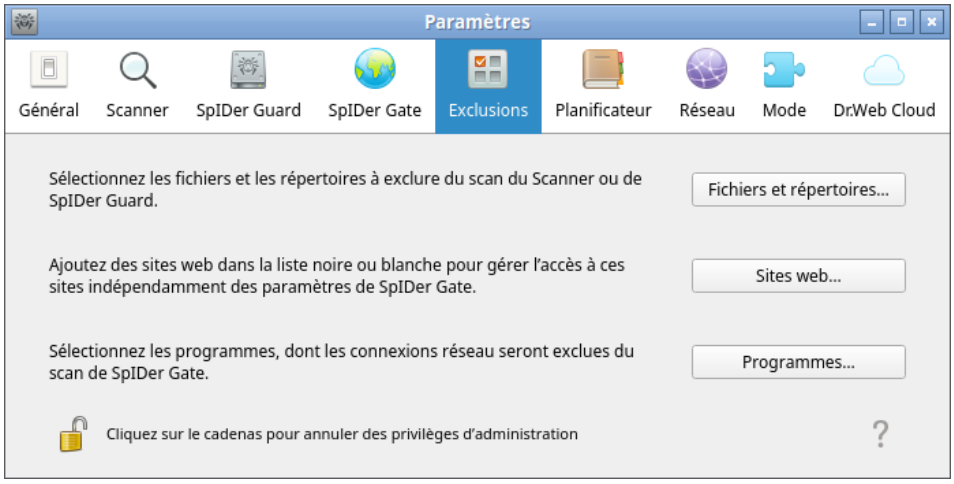

Image 44. Onglet de la configuration des exclusions

> Pour ajouter et supprimer des objets de la liste des exclusions, il faut que l'application possède des privilèges élevés. Voir Gestion des privilèges du logiciel.

Exclusion des fichiers et des répertoires

Dans cette section :

- Informations générales.
- Ajouter et supprimer les objets des listes d'exclusions.

Informations générales

Dans la fenêtre **Fichiers et répertoires**, vous pouvez exclure les fichiers et les répertoires du scan. Pour ouvrir cette fenêtre, cliquez sur **Fichiers et répertoires** dans l'onglet **Exclusions**.

Ici, vous pouvez indiquer les chemins d'accès aux objets qu'il faut exclure de l'analyse du Scanner sur demande de l'utilisateur et/ou selon la planification ou exclure de la surveillance du moniteur du système de fichiers SpIDer Guard.

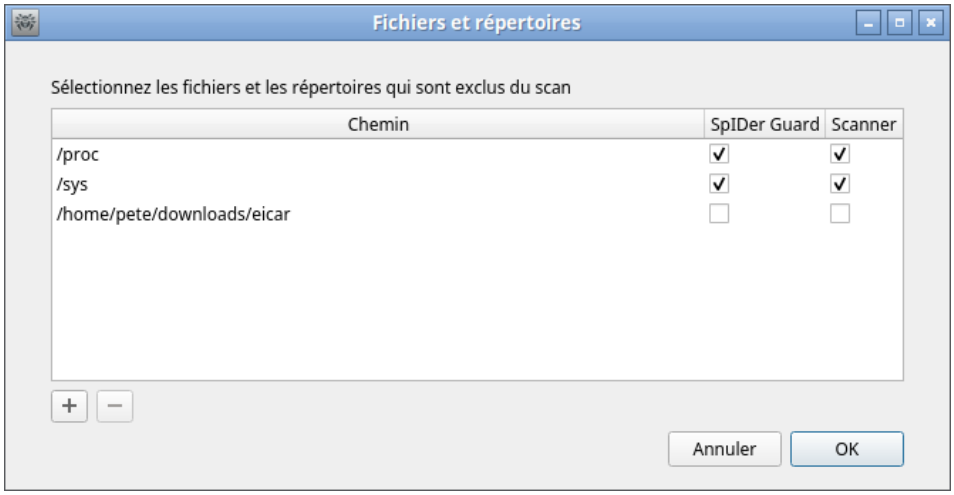

Image 45. Configuration de l'exclusion des fichiers et des répertoires

Vous pouvez ajouter le même objet à deux listes d'exclusions et désactiver son contrôle par le Scanner (sur demande et/ou selon la planification) et par le moniteur du système de fichiers SpIDer Guard. Si un objet est ajouté à une liste d'exclusions, il est coché dans la colonne correspondante du tableau.

Ajouter et supprimer les objets des listes d'exclusions

- Pour exclure un objet listé de l'analyse du Scanner ou de SpIDer Guard, cochez la case correspondante dans la ligne de l'objet. Pour exclure un objet de la liste d'exclusions du Scanner et de SpIDer Guard, décochez la case dans la ligne de l'objet.
- Pour ajouter un nouvel objet, cliquez sur + au-dessous de la liste des objets et sélectionnez l'objet dans la fenêtre qui apparaît. Vous pouvez également ajouter des objets à la liste en glissant/déposant des objets depuis la fenêtre du Gestionnaire de fichiers.
- Pour supprimer un objet de la liste, sélectionnez sa ligne dans la liste et cliquez sur − au-dessous de la liste.

Pour appliquer les modifications et fermer la fenêtre, cliquez sur **OK**. Pour rejeter les modifications et fermer la fenêtre, cliquez sur **Annuler**.

Exclusion des connexions réseau des applications

Dans cette section :

- Informations générales.
- Ajouter et supprimer les applications de la liste des exclusions.

Informations générales

Dans la fenêtre **Annexes**, vous pouvez exclure les connexions réseau des applications de la surveillance du moniteur d'accès à Internet SpIDer Gate. Pour ouvrir cette fenêtre, cliquez sur **Annexes** dans l'onglet **Exclusions**.

Ici vous pouvez spécifier la liste des chemins vers les fichiers exécutables des applications dont les connexions réseau ne doivent pas être contrôlées par le moniteur de connexions réseau SpIDer Gate.

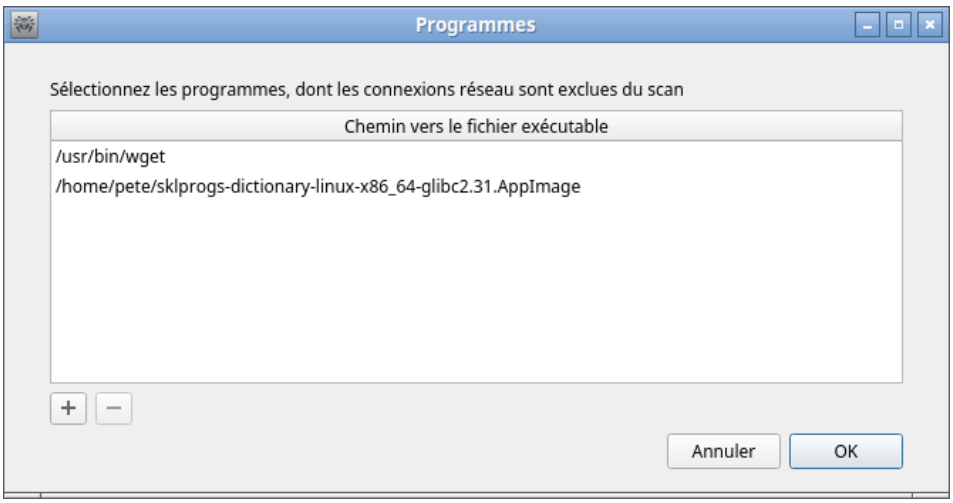

Image 46. Configuration des exclusions des connexions réseau des applications

Ajouter et supprimer les applications de la liste des exclusions

- Pour ajouter une nouvelle application à la liste, cliquez sur + au-dessous de la liste des applications, ensuite, sélectionnez dans la fenêtre qui s'affiche le fichier exécutable nécessaire. Vous pouvez également ajouter des applications à la liste en glissant/déposant des fichiers exécutables depuis la fenêtre du Gestionnaire de Fichiers.
- Pour supprimer une application de la liste, sélectionnez sa ligne dans la liste et cliquez sur − au-dessous de la liste.

Pour appliquer les modifications et fermer la fenêtre, cliquez sur **OK**. Pour rejeter les modifications et fermer la fenêtre, cliquez sur **Annuler**.

Listes noire et blanche de sites web

Dans cette section :

- Informations générales.
- Ajouter et supprimer les sites web de la liste noire et blanche.

Informations générales

Dans la fenêtre **Gestion des listes**, vous pouvez gérer les listes blanche et noire du scan. Pour ouvrir cette fenêtre, cliquez sur **Sites Web** dans l'onglet **Exclusions**.

Ici, vous pouvez indiquer la liste des sites web. L'accès à ces sites sera toujours autorisé ou, au contraire, toujours interdit par le moniteur de connexions réseau SpIDer Gate.

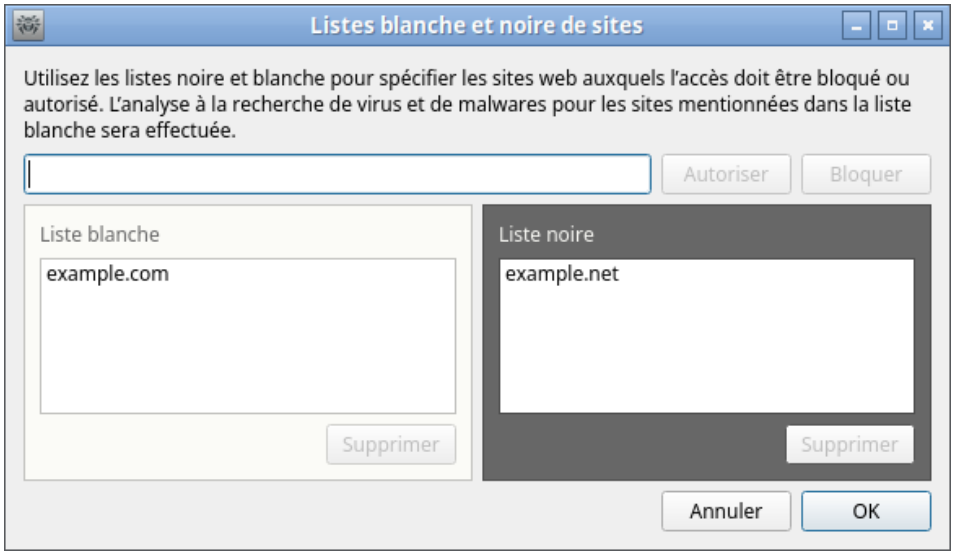

Image 47. Fenêtre de gestion des listes noire et blanche

Il existe une catégorie particulière de sites web — *Sources de propagation de virus*. L'accès à ces sites sera interdit dans tous les cas, même s'ils sont inclus dans la liste blanche de l'utilisateur.

Ajouter et supprimer les sites web de la liste noire et blanche

- Pour ajouter un site à une liste noire ou blanche, entrez l'adresse du domaine dans le champ de saisie et cliquez sur le bouton approprié :
  - **Autoriser** pour ajouter l'adresse indiquée à la liste *blanche*.
  - **Interdire** pour ajouter l'adresse indiquée à la liste *noire*.
- L'ajout d'une adresse de domaine à la liste noire ou blanche bloque ou autorise l'accès à toutes les ressources de ce domaine.
- Pour supprimer un site web de la liste blanche ou noire, sélectionnez-le dans la liste et cliquez sur **Supprimer**.

Pour appliquer les modifications et fermer la fenêtre, cliquez sur **OK**. Pour rejeter les modifications et fermer la fenêtre, cliquez sur **Annuler**.

Configuration du scan selon la planification

Dans cette section :

- Informations générales.
- Configuration du scan selon la planification.

Informations générales

Dans l'onglet **Planificateur**, vous pouvez activer le lancement automatique des scans selon la planification, ainsi que configurer cette planification et choisir le type de scan.

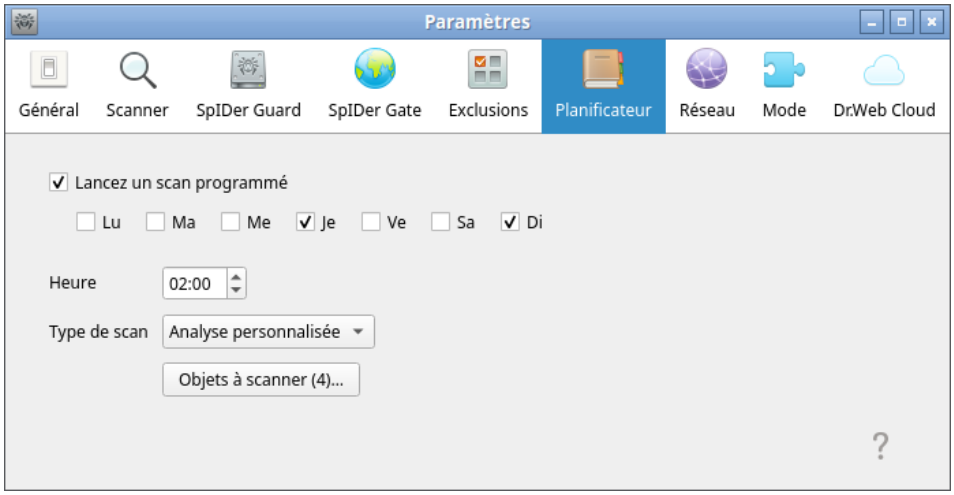

Image 48. Onglet de la configuration de la planification

Pour activer le scan automatique selon la planification, cochez la case **Effectuer un scan selon la planification** Dans ce cas, Dr.Web pour Linux crée une planification de lancement des scans périodiques de type choisi.

Les scans selon la planification seront lancés par l'agent de notifications aux intervalles indiqués ou bien, par l'interface graphique de gestion si elle est lancée au moment du démarrage du scan. que Dr.Web pour Linux soit lancé ou pas. Les scans selon la planification ne sont pas lancés si Dr.Web pour Linux est géré par le serveur de protection centralisée ou que la licence active est introuvable.

Les scans programmés ainsi que les scans à la demande sont configurés via les paramètres définis à l'onglet **Scanner**.

Configuration du scan selon la planification

Si le scan programmé est activé, vous pouvez configurer les paramètres suivants :

- Sélectionner les jours de la semaine pour le lancement de l'analyse (pour cela, cochez les cases correspondantes).
- Spécifier l'heure (heures et minutes) de démarrage du scan.
- Spécifier le mode d'analyse (*Scan rapide, Scan complet* ou *Scan personnalisé*).
- Si vous choisissez *Scan personnalisé*, vous pouvez indiquer la liste des objets à scanner. Pour cela, cliquez sur **Analyser les objets** (le nombre d'objets sélectionnés est indiqué entre parenthèses).

  Ensuite, choisissez un objet dans la fenêtre qui s'est ouverte et qui est similaire au sélecteur de fichiers pour le scan personnalisé à la demande. Vous pouvez ajouter des objets à la liste soit en cliquant sur `+`, soit en les glissant/déposant depuis la fenêtre du gestionnaire de fichiers.

Pour désactiver le scan automatique selon la planification, décochez la case **Effectuer un scan selon la planification**. La tâche correspondante de l'agent de notifications sera supprimée automatiquement.

Configuration de la protection contre les menaces transmises via le réseau

Dans cette section :

- Informations générales.
- Configuration de la vérification des connexions sécurisées.
- Ajouter le certificat Dr.Web dans les listes de certificats fiables d'applications.
- Ajout du certificat Dr.Web à la liste des certificats de confiance via la ligne de commande.

Informations générales

Dans l'onglet **Réseau**, vous pouvez activer pour le moniteur de connexions réseau SpIDer Gate le mode d'analyse du trafic transmis via les connexions réseau sécurisées qui utilisent les protocoles basés sur SSL et TLS.

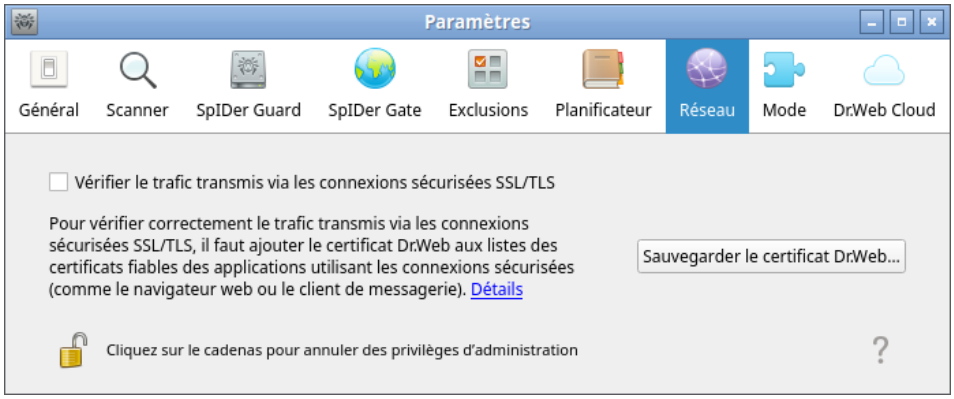

Image 49. Onglet de la configuration de la protection contre les menaces transmises via le réseau

Configuration de la vérification des connexions sécurisées

Pour autoriser le moniteur SpIDer Gate à analyser le trafic transmis via les connexions réseau sécurisées qui utilisent les protocoles basés sur SSL et TLS, cochez la case **Analyser le trafic transmis via les connexions sécurisées SSL/TLS**. Pour désactiver l'analyse du trafic sécurisé, décochez la case.

Pour gérer la vérification du trafic sécurisé, il faut que l'application possède des privilèges élevés. Voir Gestion des privilèges du logiciel.

Si un client de messagerie (tel que Mozilla Thunderbird) est lancé dans le système, il faut le redémarrer après l'activation du mode **Analyser le trafic transmis via les connexions sécurisées SSL/TLS**.

Pour le fonctionnement correct du mécanisme de vérification du trafic transmis via les connexions réseau sécurisées, exporter le certificat spécial Dr.Web vers un fichier. Ensuite, il faut ajouter manuellement le certificat exporté dans les listes de certificats fiables des applications utilisant les connexions sécurisées. Tout d'abord, ce sont les navigateurs web et les clients de messagerie. Si vous n'ajoutez pas le certificat Dr.Web dans la liste de certificats fiables du navigateur web, les données seront affichées d'une manière incorrecte. Il s'agit des données obtenues des sites l'accès auxquels s'effectue via le protocole sécurisé HTTPS (par exemple, les sites de systèmes de banking en ligne ou d'interfaces des services de messagerie). Si le certificat Dr.Web ne sera pas ajouté dans la liste de certificats fiables du client de messagerie, il sera impossible de s'authentifier sur les serveurs de messagerie utilisant les protocoles sécurisés pour la transmission des messages (tels que SMTPS).

Pour exporter le certificat Dr.Web vers un fichier, cliquez sur **Enregistrer le certificat Dr.Web**, ensuite, dans la fenêtre qui apparaît, indiquez l'emplacement de sauvegarde. Par défaut le fichier reçoit le nom `SpIDer Gate Trusted Root Certificate.pem` que vous pouvez modifier, si nécessaire.

Ensuite, ajoutez manuellement le fichier sauvegardé du certificat Dr.Web dans la liste de certificats fiables des applications dont le fonctionnement a été perturbé lors de l'établissement des connexions sécurisées. Il suffit d'ajouter une seule fois le certificat dans la liste pour une application. Plus tard, si vous cochez et décochez la case **Analyser le trafic transmis via les connexions sécurisées SSL/TLS** sur la page des paramètres **Réseau**, vous ne serez plus obligé de sauvegarder et ajouter le certificat Dr.Web dans la liste des fiables encore une fois.

Ajouter le certificat Dr.Web dans les listes de certificats fiables d'applications

Navigateur web Mozilla Firefox

1) Sélectionnez l'élément **Paramètres** dans le menu principal, ensuite, sur la page de paramètres qui s'affiche, sélectionnez l'élément **Supplémentaires**, et sur la page qui s'ouvre — la section **Certificats**.
2) Cliquez sur **Consulter les certificats**, dans la fenêtre qui apparaît, sélectionnez l'onglet **Centres de certification** et cliquez sur **Importer**.
3) Dans la fenêtre qui s'affiche, indiquez le chemin vers le fichier du certificat Dr.Web (par défaut, c'est le fichier `SpIDer Gate Trusted Root Certificate.pem`) et cliquez sur **Ouvrir**.
4) Ensuite dans la fenêtre qui s'affiche, indiquez à l'aide des cases à cocher le niveau de fiabilité du certificat. Il est recommandé de cocher toutes les trois cases (pour identifier des sites web, pour identifier les utilisateurs d'e-mail, pour identifier le logiciel). Ensuite, cliquez sur **OK**.
5) Dans la liste des certificats fiables, une rubrique *DrWeb*, va apparaître. Cette rubrique contient le certificat ajouté (par défaut *SpIDer Gate Trusted Root Certificate*) en tant que certificat.
6) Fermez la fenêtre contenant la liste de certificats en cliquant sur **OK**. Puis, fermez la page des paramètres du navigateur (fermez l'onglet correspondant dans la barre du navigateur).

Client de messagerie Mozilla Thunderbird

1) Sélectionnez l'élément **Paramètres** dans le menu principal, ensuite, dans la fenêtre de paramètres qui s'affiche, sélectionnez la section **Supplémentaires**, et sur la page qui s'ouvre — l'onglet **Certificats**.
2) Cliquez sur **Consulter les certificats**, dans la fenêtre qui apparaît, sélectionnez l'onglet **Centres de certification** et cliquez sur **Importer**.
3) Dans la fenêtre qui s'affiche, indiquez le chemin vers le fichier du certificat Dr.Web (par défaut, c'est le fichier `SpIDer Gate Trusted Root Certificate.pem`) et cliquez sur **Ouvrir**.
4) Ensuite dans la fenêtre qui s'affiche, indiquez à l'aide des cases à cocher le niveau de fiabilité du certificat. Il est recommandé de cocher toutes les trois cases (pour identifier des

sites web, pour identifier les utilisateurs d'e-mail, pour identifier le logiciel). Ensuite, cliquez sur **OK**.

5) Dans la liste des certificats fiables, une rubrique *DrWeb*, va apparaître. Cette rubrique contient le certificat ajouté (par défaut *SpIDer Gate Trusted Root Certificate*) en tant que certificat.
6) Fermez la fenêtre contenant la liste des certificats en cliquant sur **OK**, puis fermez la fenêtre de configuration du client de messagerie en cliquant sur **Fermer**.
7) Redémarrez le client de messagerie.

Ajout du certificat Dr.Web à la liste des certificats de confiance via la ligne de commande

Vous pouvez ajouter le certificat non seulement via l'interface graphique, mais aussi via la ligne de commande. Pour générer le certificat, exécutez la commande suivante (il faudra indiquer le nom du fichier vers lequel sera enregistré le fichier au format PEM) :

```
$ drweb-ctl certificate > <cert_name>.pem
```

Ensuite, ajoutez le certificat au stockage système. Dans de différentes distributions de Linux, cette operation est effectuée à l'aide des commandes différentes.
Dans Ubuntu, Debian, Mint :

```
# cp <cert_name>.pem /etc/ssl/certs/
# c_rehash
```

Dans CentOS et Fedora :

```
# cp <cert_name>.pem /etc/pki/ca-trust/source/anchors/
# update-ca-trust extract
```

Paramètres du mode

Dans cette section :

- Informations générales.
- Connexion au serveur de protection centralisée.
- Paramètres avancés.

Informations générales

Dans l'onglet **Mode**, vous pouvez connecter Dr.Web pour Linux au serveur de protection centralisée (en le basculant en mode de protection centralisée) ou vous déconnecter du serveur de protection centralisée (dans ce cas, Dr.Web pour Linux va fonctionner en mode standalone).

Image 50. Onglet Mode

Pour connecter ou déconnecter Dr.Web pour Linux du serveur de protection centralisée, cochez ou décochez la case correspondante.

Pour connecter Dr.Web pour Linux au serveur de protection centralisée ou l'en déconnecter, le logiciel doit posséder des privilèges élevés. Pour en savoir plus, consultez la section Gestion des privilèges du logiciel.

Connexion au serveur de protection centralisée

Lors d'une tentative de connexion au serveur de protection centralisée, une fenêtre s'affiche. Il vous faudra y indiquer les paramètres de connexion au serveur :

Image 51. Fenêtre de la connexion au serveur de protection centralisée

Dans la liste déroulante située en dessus de la fenêtre, sélectionnez le mode de connexion au serveur. Trois modes sont disponibles :

- *Télécharger du fichier.*
- *Indiquer manuellement.*
- *Déterminer automatiquement.*

Si vous choisissez l'option *Télécharger du fichier*, il suffit d'indiquer dans le champ correspondant le chemin vers le fichier contenant les paramètres de connexion au serveur fourni par l'administrateur du réseau antivirus. Si vous choisissez les options *Indiquer manuellement* et *Déterminer automatiquement* , spécifiez l'adresse et le port pour la connexion au serveur de protection centralisée ainsi que le chemin vers le fichier de certificat du serveur (normalement, ce fichier est fourni par l'administrateur du réseau antivirus ou le fournisseur de service Internet).

De plus, dans la rubrique **Authentification**, vous pouvez entrer l'identificateur du poste et le mot de passe pour l'authentification sur le serveur (si vous les connaissez). La connexion sera réussie uniquement si vous indiquez le bon couple identifiant/mot de passe. Si les champs sont vides, la connexion sera établie uniquement au cas où elle serait approuvée sur le serveur (automatiquement ou par l'administrateur du réseau antivirus, en fonction des configurations du serveur).

Vous pouvez également cocher la case **Se connecter en tant que novice**. Si c'est autorisé sur le serveur, une paire login/mot de passe unique sera automatiquement générée après l'approbation de la connexion et, ensuite elle sera utilisée pour la connexion de votre ordinateur à cette serveur. Notez que si cette case n'est pas cochée, un nouveau compte est générée pour votre ordinateur même si le poste possède déjà un compte sur ce serveur.

Spécifiez les paramètres de connexion conformément aux instructions fournies par l'administrateur réseau ou votre fournisseur de service Internet.

Pour vous connecter au serveur, configurez tous les paramètres, cliquez sur **Connecter** et attendez que la connexion s'établisse. Pour fermer la fenêtre sans établir une connexion avec le serveur, cliquez sur **Annuler**.

Après avoir connecté Dr.Web pour Linux au serveur de protection centralisée, Dr.Web pour Linux est administré par le serveur jusqu'au passage en mode standalone. Une connexion serveur est automatiquement établie à chaque démarrage du système d'exploitation. Pour en savoir plus, consultez la section Modes de fonctionnement.

Si le lancement du scan sur demande de l'utilisateur n'est pas autorisé sur le serveur de protection centralisée, la page de lancement du scan et le bouton **Scanner** de la fenêtre de Dr.Web pour Linux seront désactivés. De plus, dans ce cas, le Scanner ne lancera pas des scans planifiés.

Paramètres avancés

Dans la liste déroulante **Délai maximum de stockage des messages du serveur**, vous pouvez indiquer la durée maximale de stockage des messages sur le statut et les événements du réseau antivirus envoyés sur ce poste par le serveur de protection centralisée auquel Dr.Web pour Linux est connecté. A l'issue de la période indiquée, les messages seront supprimés automatiquement, même s'ils ne sont pas lus.

Les messages sur l'état et les événements du réseau antivirus seront reçus uniquement si l'administrateur du réseau antivirus a configuré sur le serveur de protection centralisée auquel Dr.Web pour Linux est connecté l'envoi de messages sur votre poste. Sinon, l'affichage de messages sera indisponible et la liste déroulante **Délai maximum de stockage des messages du serveur** ne s'affichera pas sur la page de configuration du mode de protection.

Configuration de l'utilisation de Dr.Web Cloud

Dr.Web Cloud – ici, vous pouvez interdire ou autoriser à Dr.Web pour Linux l'utilisation du service Dr.Web Cloud.

La connexion à Dr.Web Cloud permet à Dr.Web pour Linux d'utiliser des informations actuelles sur les menaces. Ces informations sont mises a jour sur les serveurs de Doctor Web en temps réel. En fonction des paramètres de mise à jour, les informations sur les menaces utilisées par les composants de la protection antivirus peuvent devenir obsolètes. L'utilisation des services cloud permet de restreindre de façon fiable l'accès des utilisateurs de votre ordinateur aux sites au contenu non désirable ainsi que protéger contre les fichiers infectée.

Image 52. Onglet de gestion de Dr.Web Cloud

Pour autoriser ou interdire à Dr.Web pour Linux l'utilisation du service Dr.Web Cloud, cochez ou décochez la case correspondante.

Pour accéder au service Dr.Web Cloud, la connexion Internet est requise.

Pour autoriser ou interdire à Dr.Web pour Linux l'utilisation du service Dr.Web Cloud, il faut que le logiciel possède des privilèges élevés. Pour en savoir plus, consultez Gestion des privilèges du logiciel.

Avancé

Arguments de la ligne de commande

Pour démarrer Dr.Web pour Linux en mode graphique depuis la ligne de commande, la commande suivante est utilisée :

```
$ drweb-gui [<chemin>[ <chemin> ...] | <paramètres>]
```

où <*chemin*> est le chemin à vérifier. Vous pouvez indiquer la liste des chemins séparés par les espaces.

Vous pouvez utiliser également les paramètres de commande suivants (<*paramètres*>) :

- `--help (-h)` : afficher de brèves informations sur les paramètres de la ligne de commande et arrêter l'interface graphique.

- `--version (-v)` : afficher les informations sur la version de l'interface graphique.
- `--Autonomous (-a)` : lancer l'interface graphique de Dr.Web pour Linux en mode de copie autonome.
- `--FullScan` : lancer le scan complet au démarrage de l'interface graphique Dr.Web pour Linux.
- `--ExpressScan` : lancer le scan rapide au démarrage de l'interface graphique de Dr.Web pour Linux.
- `--CustomScan` : lancer le scan personnalisé au démarrage de l'interface graphique de Dr.Web pour Linux (ouvrir la page de sélection des objets à scanner).

Exemple :

```
$ drweb-gui /home/user/
```

Cette commande va lancer l'interface graphique Dr.Web pour Linux, après quoi, le Scanner va scanner les fichiers à l'emplacement indiqué (la tâche correspondante sera affichée dans la liste de scans courants).

Lancement de la copie autonome

Dr.Web pour Linux supporte le fonctionnement en mode particulier — en mode de *copie autonome*.

Si on lance l'interface graphique de gestion Dr.Web pour Linux en mode de copie autonome, l'interface fonctionnera avec l'ensemble particulier des composants de service (le *daemon de gestion de la configuration de Dr.Web pour Linux* fonctionnant en fond (`drweb-configd`), le Scanner et le moteur antivirus utilisé par le Scanner) lancé spécialement pour maintenir la capacité de travail.

Particularités de fonctionnement de Dr.Web pour Linux en mode de copie autonome :

- Pour le lancement de l'interface graphique de gestion de Dr.Web pour Linux en mode de copie autonome, le fichier clé valide est requis, la gestion par le serveur de protection centralisée n'est pas supportée (il y a une possibilité d'installer le fichier clé exporté du serveur de protection centralisée). Dans ce cas, même si Dr.Web pour Linux est connecté au serveur de protection centralisée, la copie autonome *n'avertit pas* le serveur de protection centralisée des menaces détectées lors de l'analyse en mode de copie autonome.
- Tous les composants auxiliaires qui servent la copie autonome seront de l'interface graphique lancés de nom de l'utilisateur courant et fonctionneront avec le fichier de configuration formé spécialement.
- Tous les fichiers temporaires et les sockets UNIX utilisés pour l'interaction des composants seront crées uniquement dans le répertoire portant un nom unique créé par la copie autonome lancée dans le répertoire des fichiers temporaires (indiqué dans la variable système d'environnement `TMPDIR`).

- La copie autonome lancée de l'interface graphique de gestion *ne lance pas* les moniteurs SpIDer Guard et SpIDer Gate. Ce sont seulement le fonctions d'analyse de fichiers et de gestion de quarantaine prises en charge par le Scanner qui sont en marche.
- Les chemins vers les fichiers de bases virales, le moteur antivirus et les fichiers exécutables des composants de service sont spécifiés par défaut, ou ils sont tirés des variables d'environnement spéciales.
- Le nombre des copies autonomes de l'interface graphique fonctionnant en même temps n'est pas limité.
- Si la copie de l'interface graphique lancée d'une manière autonome arrête le fonctionnement, l'ensemble des composants de service qui la sert est également arrêté.

Gestion via la ligne de commande

Dans cette section :

- Informations générales.
- Analyse des hôtes distants.

Informations générales

Il existe la possibilité de gérer Dr.Web pour Linux depuis la ligne de commande du système d'exploitation. Pour cela, il contient l'utilitaire spécial Dr.Web Ctl (`drweb-ctl`). Avec cet utilitaire vous pouvez effectuer les actions suivantes depuis la ligne de commande :

- Lancer l'analyse des fichiers, des secteurs d'amorçage des disques et des fichiers exécutables des processus actifs.
- Lancer l'analyse des fichiers sur les hôtes distants du réseau (voir la note ci-dessous).
- Lancer la mise à jour des composants antivirus (des bases virales, du moteur antivirus, etc. en fonction de la distribution).
- Voir et modifier les paramètres de configuration de Dr.Web pour Linux.
- Voir le statut des composants de Dr.Web pour Linux et les statistiques sur les menaces détectées.
- Voir la quarantaine et gérer les objets placés en quarantaine.
- Vous connecter ou vous déconnecter du serveur de protection centralisée.

Les commandes utilisateur pour la gestion de Dr.Web pour Linux ont un effet seulement si les composants de Dr.Web pour Linux sont en cours d'exécution (par défaut, ils sont automatiquement lances au démarrage du système).

Notez que certaines commandes de gestion requièrent les privilèges de super-utilisateur.

Pour élever les privilèges, utilisez la commande de changement d'utilisateur `su` ou la commande d'exécution au nom d'un autre utilisateur `sudo`.

L'utilitaire `drweb-ctl` supporte la saisie semi-automatique des commandes de gestion de Dr.Web pour Linux si cette option est activée dans l'interface de commande utilisée. Si l'interface de commande n'autorise pas la saisie semi-automatique, vous pouvez configurer cette option. Pour cela, consultez le manuel correspondant à la distribution du système d'exploitation utilisé.

A la fin du fonctionnement, l'utilitaire retourne le code de sortie conformément à l'accord pour les systèmes compatibles POSIX : 0 (zéro) — si l'opération est exécutée avec succès et, le code de sortie différent de zéro — dans les cas contraires.

Notez que le code de sortie différent de zéro est retourné uniquement en cas d'erreur interne (par exemple, l'utilitaire n'a pas pu se connecter à un certain composant, l'opération demandée ne peut pas être exécutée, etc.). Si l'utilitaire détecte (et, probablement) neutralise une menace, il retourne le code de sortie 0, car l'opération demandée (par exemple, `scan`, etc.) est exécutée avec succès. S'il est nécessaire d'établir une liste des menaces détectées et des actions appliquées, analysez les messages affichés par l'utilitaire dans la console.

Vous trouverez les codes de toutes les erreurs disponibles dans la section Annexe D. Erreurs connues.

Analyse distante des hôtes

Dr.Web pour Linux permet d'analyser des fichiers se trouvant sur les hôtes distants du réseau. Les machines (les postes et les serveurs), les routeurs, les consoles TV et d'autres dispositifs intelligents constituant le soi-disant Internet des objets peuvent représenter des hôtes. Pour l'analyse distante, il faut que l'hôte distant fournisse la possibilité d'accès distant via *SSH* (*Secure Shell*) ou *Telnet*. De plus, il faut connaître l'adresse IP ou le nom de domaine de l'hôte distant, le nom et le mot de passe de l'utilisateur qui peut accéder à distance au système via *SSH* ou *Telnet*. Cette personne doit avoir le droit d'accéder aux fichiers analysés (au moins, le droit de les lire).

Cette fonction peut être utilisée uniquement pour détecter les fichiers suspects ou malveillants sur l'hôte distant. Il est impossible de neutraliser les menaces (mettre en quarantaine ou désinfecter les objets malveillants) avec les outils de l'analyse distante. Pour neutraliser les menaces détectées sur le nœud distant, utilisez les outils de gestion fournis par ce nœud. Par exemple, pour les routeurs et d'autres dispositifs intelligents, on peut utiliser le mécanisme de mise à jour de leur firmware, pour l'ordinateur — on peut s'y connecter (y compris en mode terminal distant) et effectuer les opérations nécessaire dans le système de fichiers (supprimer ou déplacer les fichiers, etc.) ou lancer un logiciel antivirus installé sur cet ordinateur.

L'analyse distante s'effectue uniquement via l'utilitaire de gestion depuis la ligne de commande `drweb-ctl` (la commande `remotescan` est utilisée).

Format d'appel

1. Format d'appel de l'utilitaire de gestion depuis la ligne de commande

L'utilitaire de gestion de Dr.Web pour Linux a le format suivant :

```
$ drweb-ctl [<options générales> | <commande> [<argument>] [<options de la commande>]]
```

Où :

- <*options générales*> : options qui peuvent être appliquées au démarrage lorsque la commande n'est pas spécifiée ou à n'importe quelle commande. Non obligatoire pour le démarrage.
- <*commande*> : commande devant être effectuée par Dr.Web pour Linux (par exemple, démarrage du scan, sortie de la liste des objets en quarantaine, etc.).
- <*argument*> : argument de commande. Dépend de la commande indiquée. Peut être absent pour certaines commandes.
- <*options de la commande*> : options gérant le fonctionnement de la commande. Dépend de la commande. Peut être absent pour certaines commandes.

2. Options générales

Les options générales suivantes sont disponibles :

Option	Description
`--help`	Afficher les informations d'aide résumées et sortir. Pour des informations sur une commande en particulier, entrez la ligne suivante : `$ drweb-ctl <commande> -h`
`-v, --version`	Afficher les informations sur la version du module et arrêter
`-d, --debug`	Indique d'afficher les messages de diagnostic après l'exécution de la commande spécifiée. Cela n'a pas d'effet si une commande n'est pas spécifiée. Pour appeler une commande, entrez la ligne suivante : `$ drweb-ctl <commande> -d`

3. Commandes

Les commandes de gestion de Dr.Web pour Linux peuvent être divisées en groupes :

- Commandes de scan antivirus.
- Commandes degestion des mises à jour et du fonctionnement en mode de protection centralisée.
- Commandes de gestion de la configuration.
- Commandes pour gérer les menaces détectées et la quarantaine.
- Commandes d'affichage d'informations.

> Pour obtenir de l'aide pour le composant de la ligne de commande, utilisez la commande `man 1 drweb-ctl`

3.1. Commandes de scan antivirus

Les commandes suivantes pour gérer le scan antivirus sont disponibles :

Commande	Description
`scan` <*chemin*>	Fonction : Lancer l'analyse du fichier ou du répertoire spécifiés par le Scanner. Arguments : <*chemin*> : chemin vers le fichier ou le répertoire à analyser (le chemin peut être relatif). *Cet argument peut être omis si l'option* `--stdin` *ou* `--stdin0` *est activée. Pour vérifier la liste des fichiers sélectionnés selon certains critères, utilisez l'utilitaire* `find` *(voir* Exemples d'utilisation*) et l'option* `--stdin` *ou* `--stdin0`. Options : `-a [--Autonomous]` : lancer une instance séparée du moteur antivirus et du Scanner pour effectuer un scan spécifié et les arrêter après la fin de scan. Notez que les menaces détectées durant un scan autonome ne sont pas affichées dans la liste commune des menaces qui s'affiche par la commande `threats` (voir ci-dessous). De plus, le serveur de protection centralisée ne sera pas notifié de ces menaces, si Dr.Web pour Linux fonctionne sous sa gestion. `--stdin` : obtenir la liste des chemins à scanner depuis la chaîne de saisie standard (*stdin*). Les chemins dans la liste doivent être séparés par le caractère de la nouvelle ligne ('`\n`').

Commande	Description
	`--stdin0` : obtenir la liste des chemins à scanner depuis la chaîne de saisie standard (*stdin*). Les chemins dans la liste doivent être séparés par le caractère NUL ('`\0`'). En cas d'utilisation des options `--stdin` et `--stdin0` les chemins dans la liste ne doivent pas contenir de templates. L'utilisation recommandée des options `--stdin` et `--stdin0` est de générer une liste de chemins (générée par un utilitaire externe, par exemple `find`), dans la commande `scan` (voir Exemples d'utilisation). `--Exclude` <*chemin*> : chemin à exclure de l'analyse. Il peut être relatif et inclure le masque de fichiers (contenant les caractères '`?`' et '`*`', ainsi que les classes de caractères '`[ ]`', '`[! ]`', '`[^ ]`'). *L'option non obligatoire peut être indiquée plus d'une fois.* `--Report` <*type*> : spécifier le type de rapport de l'analyse. Valeurs autorisées : • `BRIEF` : bref rapport. • `DEBUG` : rapport détaillé. • `JSON` : rapport sérialisé au format JSON. Valeur par défaut : *BRIEF* `--ScanTimeout` <*nombre*> : indiquer la valeur de la durée de scan d'un fichier, en ms. Si la valeur est égale à *0*, la durée de scan d'un fichier n'est pas limitée. Valeur par défaut *: 0* `--PackerMaxLevel` <*nombre*> : indiquer le niveau d'emboîtement maximum lors de l'analyse d'objets empaquetés. Si la valeur est égale à *0*, les objets emboîtés ne sont pas vérifiés. Valeur par défaut : *8* `--ArchiveMaxLevel` <*nombre*> : indiquer le niveau d'emboîtement maximum lors du scan des archives (zip, rar, etc.). Si la valeur est égale à *0*, les objets emboîtés ne sont pas vérifiés. Valeur par défaut : *8* `--MailMaxLevel` <*nombre*> : indiquer le niveau d'emboîtement maximum lors de l'analyse de fichiers de messagerie (pst, tbb, etc.). Si la valeur est égale à *0*, les objets emboîtés ne sont pas vérifiés. Valeur par défaut : *8* `--ContainerMaxLevel` <*nombre*> : indiquer le niveau d'emboîtement maximum lors du scan de conteneurs d'un autre type (HTML et autres). Si la valeur est égale à *0*, les objets emboîtés ne sont pas vérifiés. Valeur par défaut : *8*

Commande	Description
	`--MaxCompressionRatio` <*ratio*> : indiquer le taux de compression maximum pour les objets scannés. Le ratio doit être au moins égal à *2*. `--MaxSizeToExctract` <size> — spécifier la limitation de la taille de fichiers dans l'archive. Les fichiers dont la taille surpasse ce paramètre seront sautés lors de l'analyse. La taille est indiquée par un nombre avec un suffixe (b, kb, mb, gb). S'il n'y a pas de suffixe indiqué, le nombre est interprété comme la taille en octets. Valeur par défaut : *non* `--Cure` <*Yes*|*No*> : activer ou désactiver les tentatives de désinfection des menaces détectées. Si la valeur est égale à *No*, seule la notification est émise. Valeur par défaut *: No* Valeur par défaut : *3000* `--HeuristicAnalysis` <*On*|*Off*> : activer ou désactiver l'analyse heuristique lors du scan. Valeur par défaut : *On* `--OnKnownVirus` <*action*> : action appliquée à une menace connue détectée à l'aide de l'analyse par signatures. Actions possibles : *Signaler*, *Désinfecter*, *Quarantaine*, *Supprimer*. Valeur par défaut : *Signaler* `--OnIncurable` <*action*> : action appliquée en cas d'échec de traitement (`Désinfecter`) d'une menace détectée ou si la menace est incurable. Actions possibles : *Signaler*, *Quarantaine*, *Supprimer*. Valeur par défaut : *Signaler* `--OnSuspicious` <*action*> : action appliquée si l'analyse heuristique détecte un objet suspect. Actions possibles : *Signaler*, *Quarantaine*, *Supprimer*. Valeur par défaut : *Signaler* `--OnAdware` <*action*> : action appliquée en cas de détection d'un adware. Actions possibles : *Signaler*, *Quarantaine*, *Supprimer*. Valeur par défaut : *Signaler* `--OnAdware` <*action*> : action appliquée en cas de détection d'un dialer. Actions possibles : *Signaler*, *Quarantaine*, *Supprimer*. Valeur par défaut : *Signaler* `--OnJokes` <*action*> : action appliquée en cas de détection d'un canular. Actions possibles : *Signaler*, *Quarantaine*, *Supprimer*. Valeur par défaut : *Signaler*

Commande	Description
	`--OnRiskware` <*action*> : action appliquée en cas de détection d'un riskware. Actions possibles : *Signaler*, *Quarantaine*, *Supprimer*. Valeur par défaut : *Signaler* `--OnAdware` <*action*> : action appliquée en cas de détection d'un hacktool. Actions possibles : *Signaler*, *Quarantaine*, *Supprimer*. Valeur par défaut : *Signaler* Si la menace est détecté dans un fichier se trouvant dans un conteneur (archive, message, etc.), le conteneur n'est pas supprimé (*Supprimer*) mais il est mise en quarantaine (*Quarantaine*). `--FollowSymlinks` : autoriser automatiquement des liens symboliques
`bootscan` <*appareil*> `|` `ALL`	Fonction : Démarrer le scan des secteurs d'amorçage sur les disques indiqués par le Scanner. Les secteurs MBR et VBR sont scannés. Arguments : <*disque*> : chemin vers un fichier bloc du disque dont le secteur d'amorçage doit être scanné. Vous pouvez indiquer plusieurs disques en les séparant par les espaces. Argument obligatoire. Si vous indiquez la valeur `ALL`, tous les secteurs d'amorçage de tous les disques disponibles seront scannés. Options : `-a [--Autonomous]` : lancer une instance séparée du moteur antivirus et du Scanner pour effectuer un scan spécifié et les arrêter après la fin de scan. Notez que les menaces détectées durant un scan autonome ne sont pas affichées dans la liste commune des menaces qui s'affiche par la commande `threats` (voir ci-dessous). De plus, le serveur de protection centralisée ne sera pas notifié de ces menaces, si Dr.Web pour Linux fonctionne sous sa gestion. `--Report` <*type*> : spécifier le type de rapport de l'analyse. Valeurs autorisées : • `BRIEF` : bref rapport. • `DEBUG` : rapport détaillé. • `JSON` : rapport sérialisé au format JSON. Valeur par défaut : *BRIEF* `--ScanTimeout` <*nombre*> : indiquer la valeur de la durée de scan d'un fichier, en ms. Si la valeur est égale à *0*, la durée de scan d'un fichier n'est pas limitée. Valeur par défaut : *0*

Commande	Description
	`--HeuristicAnalysis` <*On*|*Off*> : activer ou désactiver l'analyse heuristique lors du scan. Valeur par défaut : *On* `--Cure` <*Yes*|*No*> : activer ou désactiver les tentatives de désinfection des menaces détectées. Si la valeur est égale à *No*, seule la notification est émise. Valeur par défaut : *No* `--ShellTrace` : activer l'émission d'informations de débogage supplémentaires lors du scan d'amorçage.
`procscan`	Fonction : démarrer l'analyse par le Scanner des fichiers exécutables contenant le code des processus en cours d'exécution. Si une menace est détectée, le fichier exécutable malveillant est neutralisé et tous les processus actifs lances de ce fichier sont arrêtés de force. Arguments : Non. Options : `-a [--Autonomous]` : lancer une instance séparée du moteur antivirus et du Scanner pour effectuer un scan spécifié et les arrêter après la fin de scan. Notez que les menaces détectées durant un scan autonome ne sont pas affichées dans la liste commune des menaces qui s'affiche par la commande `threats` (voir ci-dessous). De plus, le serveur de protection centralisée ne sera pas notifié de ces menaces, si Dr.Web pour Linux fonctionne sous sa gestion. `--Report` <*type*> : spécifier le type de rapport de l'analyse. Valeurs autorisées : • `BRIEF` : bref rapport. • `DEBUG` : rapport détaillé. • `JSON` : rapport sérialisé au format JSON. Valeur par défaut : *BRIEF* `--ScanTimeout` <*nombre*> : indiquer la valeur de la durée de scan d'un fichier, en ms. Si la valeur est égale à *0*, la durée de scan d'un fichier n'est pas limitée. Valeur par défaut : *0* `--HeuristicAnalysis` <*On*|*Off*> : activer ou désactiver l'analyse heuristique lors du scan. Valeur par défaut : *On* `--PackerMaxLevel` <*nombre*> : indiquer le niveau d'emboîtement maximum lors de l'analyse d'objets empaquetés. Si la valeur est égale à *0*, les objets emboîtés ne sont pas vérifiés. Valeur par défaut : *8* `--OnKnownVirus` <*action*> : action appliquée à une menace connue détectée à l'aide de l'analyse par signatures.

Commande	Description
	Actions possibles : *Signaler*, *Désinfecter*, *Quarantaine*, *Supprimer*. Valeur par défaut : *Signaler* `--OnIncurable` <*action*> : action appliquée en cas d'échec de traitement (`Désinfecter`) d'une menace détectée ou si la menace est incurable. Actions possibles : *Signaler*, *Quarantaine*, *Supprimer*. Valeur par défaut : *Signaler* `--OnSuspicious` <*action*> : action appliquée si l'analyse heuristique détecte un objet suspect. Actions possibles : *Signaler*, *Quarantaine*, *Supprimer*. Valeur par défaut : *Signaler* `--OnAdware` <*action*> : action appliquée en cas de détection d'un adware. Actions possibles : *Signaler*, *Quarantaine*, *Supprimer*. Valeur par défaut : *Signaler* `--OnAdware` <action> : action appliquée en cas de détection d'un dialer. Actions possibles : *Signaler*, *Quarantaine*, *Supprimer*. Valeur par défaut : *Signaler* `--OnJokes` <*action*> : action appliquée en cas de détection d'un canular. Actions possibles : *Signaler*, *Quarantaine*, *Supprimer*. Valeur par défaut : *Signaler* `--OnRiskware` <*action*> : action appliquée en cas de détection d'un riskware. Actions possibles : *Signaler*, *Quarantaine*, *Supprimer*. Valeur par défaut : *Signaler* `--OnAdware` <*action*> : action appliquée en cas de détection d'un hacktool. Actions possibles : *Signaler*, *Quarantaine*, *Supprimer*. Valeur par défaut : *Signaler*  En cas de détection d'une menace dans le fichier exécutable, tous les processus lancés depuis ce fichier sont arrêté par Dr.Web pour Linux.
`remotescan` <*hôte*> <*chemin*>	Fonction : lancer l'analyse du fichier ou du répertoire spécifié sur l'hôte distant spécifié en s'y connectant via *SSH* ou via *Telnet*.

Commande	Description
	 Notez que les menaces détectées durant un scan distant ne seront pas neutralisées et ne seront pas affichées dans la liste commune des menaces qui est affichée par la commande `threats` (voir ci-dessous). Vous pouvez utiliser cette commande uniquement pour détecter les fichiers suspects ou malveillants sur l'hôte distant. Pour neutraliser les menaces détectées sur le nœud distant, il faut utiliser les outils de gestion fournis par ce nœud. Par exemple, pour les routeurs, les consoles TV et d'autres dispositifs intelligents, vous pouvez utiliser le mécanisme de mise à jour du firmware, pour l'ordinateur — on peut s'y connecter (y compris en mode terminal distant) et effectuer les opérations nécessaire dans le système de fichiers (supprimer ou déplacer les fichiers, etc.) ou lancer un logiciel antivirus installé sur cet ordinateur. Arguments : <*hôte*> : adresse IP ou nom de domaine de l'hôte auquel il faut se connecter pour l'analyse. <*chemin*> : chemin vers le fichier ou le répertoire à analyser (le chemin doit être absolu). Options : `-m [--Method]` <*SSH*|*Telnet*> : méthode (protocole) de connexion à un hôte distant. *Si la méthode n'est pas indiquée, SSH sera utilisé.* `-l [--Login]` <*nom*> : login (nom d'utilisateur) utilisé pour l'authentification sur l'hôte distant via le protocole choisi. *Si le nom d'utilisateur n'est pas spécifié, une tentative de se connecter à l'hôte distant s'effectuera au nom de l'utilisateur qui a lancé la commande.* `-i [--Identity]` <*chemin vers le fichier*> : fichier de la clé privée utilisé pour l'authentification de l'utilisateur indiqué via le protocole choisi. `-p [--Port]` <*nombre*> : numéro de port sur l'hôte distant pour la connexion via le protocole choisi. Valeur par défaut : *port par défaut pour le protocole choisi (22 — pour SSH, 23 — pour Telnet).* `--ForceInteractive` : utiliser la session interactive SSH (uniquement pour la méthode de connexion *SSH*). *Option non obligatoire.* `--TransferListenAddress` <*adresse*> : adresse écoutée pour la réception des fichiers à analyser, transmis par un périphérique distant.

Commande	Description
	Option non obligatoire. Si elle n'est pas indiquée, on utilise une adresse aléatoire. `--TransferListenPort` <*port*> : port écouté pour la réception des fichiers à analyser transmis par l'appareil distant. *Option non obligatoire. Si elle n'est pas indiquée, on utilise un port aléatoire.* `--TransferExternalAddress` <*adresse*> : adresse pour la transmission de fichiers à analyser, communiquée à l'appareil distant. *Option non obligatoire. Si elle n'est pas indiquée, on utilise la valeur de l'option* `--TransferListenAddress` *ou l'adresse sortante de la session établie.* `--TransferExternalAddress` <*port*> : port pour la transmission de fichiers à analyser, communiqué à l'appareil distant. *Option non obligatoire. Si elle n'est pas indiquée, on utilise le port déterminé automatiquement.* `--Password` <*mot de passe* > : mot de passe utilisé pour l'authentification de l'utilisateur indiqué via le protocole choisi. *Notez que le mot de passe est transmis en clair.* `--Exclude` <*chemin*> : chemin à exclure de l'analyse. Il peut inclure le masque de fichiers (contenant les caractères '`?`' et '`*`', ainsi que les classes de caractères '`[ ]`', '`[! ]`', '`[^ ]`'). Le chemin (y compris celui contenant le masque) doit être absolu. *L'option non obligatoire peut être indiquée plus d'une fois.* `--Report` <*type*> : spécifier le type de rapport de l'analyse. Valeurs autorisées : • `BRIEF` : bref rapport. • `DEBUG` : rapport détaillé. • `JSON` : rapport sérialisé au format JSON. Valeur par défaut : *BRIEF* `--ScanTimeout` <*nombre*> : indiquer la valeur de la durée de scan d'un fichier, en ms. Si la valeur est égale à *0*, la durée de scan d'un fichier n'est pas limitée. Valeur par défaut *: 0* `--PackerMaxLevel` <*nombre*> : indiquer le niveau d'emboîtement maximum lors de l'analyse d'objets empaquetés. Si la valeur est égale à *0*, les objets emboîtés ne sont pas vérifiés. Valeur par défaut : *8* `--ArchiveMaxLevel` <*nombre*> : indiquer le niveau d'emboîtement maximum lors du scan des archives (zip, rar, etc.). Si la valeur est égale à *0*, les objets emboîtés ne sont pas vérifiés. Valeur par défaut : *8*

Commande	Description
	`--MailMaxLevel` <*nombre*> : indiquer le niveau d'emboîtement maximum lors de l'analyse de fichiers de messagerie (pst, tbb, etc.). Si la valeur est égale à *0*, les objets emboîtés ne sont pas vérifiés. Valeur par défaut : *8* `--ContainerMaxLevel` <*nombre*> : indiquer le niveau d'emboîtement maximum lors du scan de conteneurs d'un autre type (HTML et autres). Si la valeur est égale à *0*, les objets emboîtés ne sont pas vérifiés. Valeur par défaut : *8* `--MaxCompressionRatio` <*ratio*> : indiquer le taux de compression maximum pour les objets scannés. Le ratio doit être au moins égal à *2*. `--MaxSizeToExctract` <size> — spécifier la limitation de la taille de fichiers dans l'archive. Les fichiers dont la taille surpasse ce paramètre seront sautés lors de l'analyse. La taille est indiquée par un nombre avec un suffixe (b, kb, mb, gb). S'il n'y a pas de suffixe indiqué, le nombre est interprété comme la taille en octets. Valeur par défaut : *non* `--Cure` <*Yes*|*No*> : activer ou désactiver les tentatives de désinfection des menaces détectées. Si la valeur est égale à *No*, seule la notification est émise. Valeur par défaut *: No* Valeur par défaut : *3000* `--HeuristicAnalysis` <*On*|*Off*> : activer ou désactiver l'analyse heuristique lors du scan. Valeur par défaut : `On`
`checkmail` <*chemin d'accès au fichier*>	Fonction : analyser (avec le composant d'analyse de messagerie) le message enregistré dans un fichier pour la présence de menaces, de traces de spam ou de la non-conformité aux règles de traitement de messages. Dans le flux de sortie de la console (*stdout*), les résultats de l'analyse du message seront retournés, ainsi que les informations sur l'action appliquée au message lors de son analyse par le composant d'analyse de messages. Arguments : <*chemin d'accès au fichier*> : chemin d'accès au fichier de message e-mail à analyser. Argument obligatoire. Options : `--Report` <*type*> : spécifier le type de rapport de l'analyse. Valeurs autorisées : • *BRIEF* : bref rapport. • *DEBUG* : rapport détaillé. • *JSON* : rapport sérialisé au format JSON.

Commande	Description

	Valeur par défaut : *BRIEF*
	`-r [--Rules]` <*liste de règles*> : spécifier l'ensemble des règles à appliquer au message lors de son analyse.
	Si les règles ne sont pas spécifiées, l'ensemble de règles par défaut sera utilisé, notamment :
	`threat_category in (KnownVirus, VirusModification, UnknownVirus, Adware, Dialer) : REJECT`
	`total_spam_score gt 0.80 : REJECT`
	`url_category in (InfectionSource, NotRecommended, CopyrightNotice) : REJECT`
	Dans ce cas, si le composant Dr.Web Anti-Spam n'est pas installé, la règle d'analyse pour la présence de spam (la deuxième ligne) sera automatiquement exclue de l'ensemble.
	`-c [--Connect]` <*IP*>:<*port*> : indiquer le socket réseau à utiliser en tant qu'adresse depuis lequel s'est connecté l'expéditeur du message analysé.
	`-e [--Helo]` <*nom*> : indiquer l'identificateur du client qui a envoyé le message (adresse IP ou FQDN de l'hôte comme pour la commande SMTP HELO/EHLO).
	`-f [--From]` <*email*> : indiquer l'adresse e-mail de l'expéditeur (comme pour la commande SMTP MAIL FROM).
	Si l'adresse n'est pas indiquée, l'adresse correspondante du message sera utilisée.
	`-t [--Rcpt]` <*email*> : indiquer l'adresse e-mail de destinataire (comme pour la commande SMTP RCPT TO).
	Si l'adresse n'est pas indiquée, l'adresse correspondante du message sera utilisée.
	Si le composant de l'analyse de messages n'est pas installé, l'appel de cette commande retournera une erreur.

Outre les commandes listées dans le tableau, l'utilitaire `drweb-ctl` supporte les commandes de vérification supplémentaires. Vous pouvez consulter leur description dans la documentation `man 1 drweb-ctl`.

3.2. Commandes de gestion de la mise à jour du fonctionnement en mode de protection centralisée

Les commandes suivantes pour la gestion des mises à jour et le fonctionnement en mode Protection centralisée sont disponibles :

Commande	Description
`update`	Fonction : initier une mise à jour des composants antivirus (des bases virales, du moteur antivirus, et des autres composants en fonction de la distribution) depuis les serveurs de mise à jour de Doctor Web ou du cloud local, terminer le processus de mise à jour en cours ou restaurer les résultats de la dernière mise à jour en restaurant les anciennes versions des fichiers mis à jour. La commande n'a pas d'effet si Dr.Web pour Linux est connecté au serveur de protection centralisée. Arguments : Non. Options : `-l [--local-cloud]` : utiliser le service cloud local auquel est connecté Dr.Web pour Linux pour le téléchargement des mises à jour. Si l'option n'est pas indiquée, les mises à jour sont téléchargées depuis les serveurs de mises à jour de l'entreprise Doctor Web (le comportement par défaut). `--From` <*chemin*> : effectuer une mise à jour depuis le répertoire indiqué sans connexion Internet. `--Path` <*chemin*> : enregistrer dans le répertoire indiqué les fichiers qui seront utilisés pour la mise à jour sans connexion Internet. Si les fichiers ont été déjà téléchargés dans ce répertoire, ils seront mis à jour. `--Rollback` : restaurer la dernière mise à jour et les dernières copies sauvegardées des fichiers mis à jour. `--Stop` : terminer le processus de mise à jour en cours.
`esconnect` <*serveur*>`[:`<*port*>`]`	Fonction : connecter Dr.Web pour Linux au serveur de protection centralisée spécifié (par exemple, Dr.Web Enterprise Server). Pour en savoir plus sur les modes de fonctionnement, voir la rubrique Modes de fonctionnement. Arguments : • <*serveur*> : adresse IP ou nom de l'hôte sur lequel se trouve le serveur de protection centralisée. L'argument est obligatoire. • <*port*> : nom du port utilisé par le serveur de protection centralisée. L'argument est optionnel. Indiquez l'argument uniquement si le serveur de protection centralisée utilise un port non standard.

Commande	Description
	Options : `--Certificate` <*chemin*> : chemin vers le fichier de certificat du serveur de protection centralisée auquel Dr.Web pour Linux est connecté. `--Login` <*ID*> : login (identificateur du poste de travail) utilisé pour la connexion au serveur de protection centralisée. `--Password` <*mot de passe*> : mot de passe utilisé pour la connexion au serveur de protection centralisée. `--Group` <*ID*> : identificateur du groupe auquel le poste de travail est relié lors de la connexion. `--Rate` <*ID*> : identificateur du groupe tarifaire appliqué à un poste de travail lorsqu'il est inclus à l'un des groupes du serveur de protection centralisée (peut être indiqué uniquement en même temps que l'option `--Group`). `--Compress` <*On*|*Off*> : activer (*On*) ou désactiver (*Off*) la compression forcée des données transmises. Lorsque rien n'est indiqué, l'utilisation de la compression est déterminée par le serveur. `--Encrypt` <*On*|*Off*> : activer (*On*) ou désactiver (*Off*) le chiffrement forcé des données transmises. Lorsque rien n'est indiqué, le chiffrement est déterminé par le serveur. `--Newbie` : se connecter comme « novice » (obtenir un nouveau compte sur le serveur). Notez que cette commande nécessite que `drweb-ctl` soit lancé avec les privilèges de super-utilisateur (utilisateur *root*). Si cela est nécessaire, utilisez les commandes `su` ou `sudo`.
`esdisconnect`	Fonction : déconnecter Dr.Web pour Linux du serveur de protection centralisée et le mettre en mode standalone. La commande n'a pas d'effet si Dr.Web pour Linux fonctionne déjà en mode standalone. Arguments : Non. Options : Non. Notez que cette commande nécessite que `drweb-ctl` soit lancé avec les privilèges de super-utilisateur (utilisateur *root*). Si cela est nécessaire, utilisez les commandes `su` ou `sudo`.

3.3. Commandes de gestion de la configuration

Les commandes suivantes pour gérer la configuration sont disponibles :

Commande	Description
`cfset` <*section*>`.`<*paramètre*> <*valeur*>	Fonction : modifier la valeur active du paramètre indiqué dans la configuration actuelle de Dr.Web pour Linux. Arguments : • <*section*> : nom de la section du fichier de configuration où le paramètre réside. L'argument est obligatoire. • <*paramètre*> : nom du paramètre modifié. L'argument est obligatoire. • <*valeur*> : nouvelle valeur du paramètre. Argument obligatoire. Le format suivant est utilisé pour spécifier la valeur de paramètres <*section*>.<*paramètre*> <*valeur*>, le signe d'affectation '=' n'est pas utilisé. Si vous voulez spécifier plusieurs valeurs du paramètre, il faut répéter l'appel de la commande `cfset` autant de fois que vous voulez les valeurs de paramètres à ajouter. Dans ce cas, il faut utiliser l'option `-a` (voir ci-dessous) pour ajouter une nouvelle valeur dans la liste de valeurs du paramètre. Il ne faut pas indiquer la séquence <*paramètre*> <*valeur 1*>, <*valeur 2*> en tant qu'argument car la ligne <*valeur 1*>, <*valeur 2*> sera considérée comme valeur unique du paramètre <*paramètre*>. Pour une description du fichier de configuration, consultez le document `man 5 drweb.ini`. Options : `-a [--Add]` : ne pas remplacer la valeur actuelle du paramètre mais ajouter la valeur indiquée à la liste (autorisé uniquement pour les paramètres qui peuvent avoir plusieurs valeurs, indiqués dans une liste). Il faut également utiliser cette option pour ajouter de nouveaux groupes de paramètres avec une balise. `-e [--Erase]` : ne pas remplacer la valeur actuelle du paramètre mais supprimer la valeur indiquée de la liste (autorisé uniquement pour les paramètres qui peuvent avoir plusieurs valeurs, indiqués dans une liste). `-r [--Reset]` : restaurer la valeur du paramètre par défaut. Ainsi, <*valeur*> n'est pas requis dans la commande et est ignoré si indiqué. Les options ne sont pas obligatoires Si elles ne sont pas activées, la valeur actuelle du paramètre (ou la liste des valeurs si plusieurs sont indiquées) est remplacée par la valeur indiquée.

Commande	Description
	 Notez que cette commande nécessite que `drweb-ctl` soit lancé avec les privilèges de super-utilisateur. Si cela est nécessaire, utilisez les commandes `su` ou `sudo`.
`cfshow [<section>[.<paramètre>]]`	Fonction : afficher sur l'écran les paramètres de la configuration actuelle de Dr.Web pour Linux. La commande pour afficher les paramètres se présente comme ceci <*section*>.<*paramètre*> = <*valeur*>. Les sections et paramètres des composants qui ne sont pas installés ne sont pas affichés. Arguments : • <*section*> : nom de la section du fichier de configuration dont les paramètres doivent être affichés. L'argument est optionnel. S'il n'est pas spécifié, les paramètres de toutes les sections du fichier de configuration sont affichés. • <*paramètre*> : nom du paramètre affiché. L'argument est optionnel. S'il n'est pas spécifié, tous les paramètres de la section sont affichés. Sinon, seul ce paramètre est affiché. Si un paramètre est indiqué sans le nom de la section, tous les paramètres portant ce nom pour toutes les sections du fichier de configuration sont affichés. Options : `--Uncut` : afficher tous les paramètres de configuration (et non seulement ceux utilisés avec l'ensemble des composants actuellement installés). Si l'option n'est pas spécifiée, seuls les paramètres utilisés pour la configuration des composants installés s'affichent. `--Changed` : afficher les paramètres dont les valeurs se distinguent des valeurs par défaut. `--Ini` : afficher les valeurs du paramètre au format INI : tout d'abord, le nom de la section est indiqué entre crochets, puis les paramètres de la section sont listés par paires <*paramètre*> = <*valeur*> (une paire par ligne). `--Value` : afficher uniquement la valeur du paramètre indiqué. Dans ce cas, l'argument <*paramètre*> est obligatoire.
`reload`	Fonction : Redémarrer les composants Dr.Web pour Linux. Dans ce cas, les journaux ouvrent de nouveau, le fichier de configuration est relu et on tente de redémarrer les composants après un arrêt anormal. Arguments : Non. Options : Non.

3.4. Commandes pour gérer les menaces détectées et la quarantaine

Les commandes suivantes pour gérer les menaces détectées et la quarantaine sont disponibles :

Commande	Description
`threats [<action> <objet>]`	Fonction : Appliquer l'action spécifiée aux menaces détectées par leurs identificateurs. Le type d'action est configuré via l'option de commande indiquée. Si aucune action n'est spécifiée, des informations sur les menaces détectées sont affichées mais pas sur les menaces neutralisées. Les informations sur les menaces sont affichées au format spécifié par l'option non obligatoire `--Format`. Si l'option `--Format` n'est pas spécifiée, les informations suivantes sont affichées pour chaque menace : • Identificateur attribué à la menace (numéro d'ordre). • Chemin complet vers le fichier infecté. • Informations sur la menace (nom, type selon la classification de Doctor Web). • Informations sur le fichier : taille, utilisateur propriétaire, date de la dernière modification. • Historiques des actions sur le fichier infecté : détection, actions appliquées, etc. Arguments : Non. Options : `--Format "<ligne_de_format>"` : afficher les informations sur les menaces au format spécifié. Vous trouverez la description de la ligne de format ci-dessous. *Si cette option est indiquée ensemble avec une option-action, elle sera ignorée.* `-f [--Follow]` : attendre de nouveaux messages sur de nouvelles menaces et afficher les messages dès leur réception (interrompre l'attente par CTRL+C). *Si cette option est indiquée ensemble avec une option-action, elle sera ignorée.* `--Directory <liste de répertoires>` : afficher uniquement les menaces détectées dans les fichiers des répertoires de la *<liste de répertoires>*. *Si cette option est indiquée ensemble avec une des options affichées ci-dessous, elle sera ignorée.* `--Cure <liste de menaces>` : essayer de traiter les menaces listées (les identificateurs des menaces sont indiqués dans une liste et séparés par des virgules). `--Quarantine <liste de menaces>` : déplacer les menaces listées en quarantaine (les identificateurs des menaces sont indiqués dans une liste et séparés par des virgules).

Commande	Description
	`--Delete` <*liste de menaces*> : supprimer les menaces listées (les identificateurs des menaces sont indiqués dans une liste et séparés par des virgules). `--Ignore` <*liste de menaces*> : ignorer les menaces listées (les identificateurs des menaces sont indiqués dans une liste et séparés par des virgules). S'il est nécessaire d'appliquer une action à toutes les menaces détectées, indiquez `All` au lieu de <*liste_de_menaces*>. Par exemple, la commande suivante : `$ drweb-ctl threats --Quarantine All` déplace tous les objets malveillants détectés en quarantaine.
`quarantine [`<*action*> <*objet*>`]`	Fonction : Appliquer une action à l'objet indiqué en quarantaine. Si aucune action n'est spécifiée, les informations suivantes s'affichent : identificateurs des objets en quarantaine et courtes informations sur les fichiers source. Les informations sur les objets isolés sont affichées au format spécifié par l'option non obligatoire `--Format`. Si l'option `--Format` n'est pas spécifiée, les informations suivantes sont affichées pour chaque objet isolé : • Identificateur attribué à l'objet isolé en quarantaine. • Chemin initial vers le fichier déplacé en quarantaine. • Date du déplacement des fichiers en quarantaine. • Informations sur le fichier : taille, utilisateur propriétaire, date de la dernière modification. • Informations sur la menace (nom, type selon la classification de Doctor Web). Arguments : Non. Options : `-a [--Autonomous]` : lancer une instance séparée du Scanner pour appliquer une action à la quarantaine et arrêter son fonctionnement de l'instance après l'exécution de l'action. *Cette option peut être appliquée ensemble avec une des options indiquées ci-dessous.* `--Format "`<*ligne_de_format*>`"` : afficher les informations sur les objets mis en quarantaine au format spécifié. Vous trouverez la description de la ligne de format ci-dessous. *Si cette option est indiquée ensemble avec une option-action, elle sera ignorée.* `-f [--Follow]` : attendre de nouveaux messages sur de nouvelles menaces et afficher les messages dès leur réception (interrompre l'attente par CTRL+C).

Commande	Description

	Si cette option est indiquée ensemble avec une option-action, elle sera ignorée.
	`--Discovery [`<*liste_des_répertoires*>`]` : rechercher les répertoires de la quarantaine dans la liste des répertoires indiquée et les ajouter à la quarantaine consolidée en cas de détection. Si <*liste_des_répertoires*> n'est pas indiquée, rechercher les répertoire dans les endroits standard du système de fichiers (les points de montages de volume et les répertoires personnels des utilisateurs).
	Cette option peut être indiquée ensemble non seulement avec l'option `-a` *(*`--Autonomous`*) (voir ci-dessus), mais aussi avec une des options-actions listées ci-dessous. De plus, si la commande* `quarantine` *est lancée en mode de copie autonome, c'est-à-dire avec l'option* `-a` *(*`--Autonomous`*), mais sans l'option* `--Discovery`*, cela est équivalent à l'appel :*
	`quarantine --Autonomous --Discovery`
	`--Delete` <*objet*> : supprimer l'objet indiqué de la quarantaine.
	Notez que la suppression de la quarantaine est une opération irréversible.
	`--Cure` <*objet*> : essayer de désinfecter l'objet indiqué en quarantaine.
	Notez que même en cas de désinfection, l'objet restera en quarantaine. Pour retirer l'objet désinfecté de la quarantaine utilisez l'option de restauration `--Restore`.
	`--Restore` <*objet*> : restaurer l'objet indiqué de la quarantaine vers sont emplacement d'origine.
	Notez que l'exécution de cette action peut exiger le lancement de `drweb-ctl` *par le super-utilisateur. Le fichier peut être restauré de la quarantaine même s'il est infecté.*
	`--TargetPath` <*chemin*> : restaurer l'objet de la quarantaine vers l'emplacement spécifié : en tant que fichier avec le nom spécifié si <*chemin*> est le chemin vers le fichier ou dans le répertoire spécifié (si <*chemin*> est le chemin vers le répertoire). Vous pouvez indiquer un chemin absolu ou relatif (par rapport au répertoire actuel).
	Notez que l'option est appliquée seulement avec l'option de restauration `--Restore`.
	L'identificateur de l'objet en quarantaine est utilisé en tant qu'<*object*>. Pour appliquer une commande à tous les objets placés en quarantaine, indiquez `All` à la place d'<*object*>. Par exemple, la commande suivante :
	`$ drweb-ctl quarantine --Restore All --TargetPath test`
	restaure tous les objets de la quarantaine, en les plaçant dans le sous-répertoire `test` se trouvant dans le répertoire actuel depuis lequel la commande `drweb-ctl` a été exécutée.

Commande	Description
	Notez que pour la variante `--Restore All`*, l'option supplémentaire* `--TargetPath` *(si elle est spécifiée) doit indiquer le chemin vers un répertoire et pas vers un fichier.*

Affichage formaté de données pour les commandes threats et quarantine

Le format de l'affichage est spécifié par la ligne de format indiquée en tant que l'argument de l'option non obligatoire `--Format`. La ligne de format doit être obligatoirement indiquées entre guillemets. La ligne de format peut contenir des caractères ordinaires (qui seront affichés tels qu'ils sont) ou les marqueurs spécifiques qui seront remplacés par les informations correspondantes. Les marqueurs suivants sont disponibles :

1. Les éléments communs pour les commandes `threats` et `quarantine` :

Marqueur	Description
`%{n}`	Saut de ligne
`%{t}`	Tabulation
`%{threat_name}`	Nom de la menace (virus) détectée selon la classification de Doctor Web
`%{threat_type}`	Type de menace (« known virus », etc.) selon la classification de Doctor Web
`%{size}`	Taille du fichier initial
`%{origin}`	Nom complet du fichier initial avec le chemin
`%{path}`	Synonyme pour `%{origin}`
`%{ctime}`	Date/heure de la modification du fichier initial au format "*%Y-%b-%d %H:%M:%S*" (par exemple, `"2018-Jul-20 15:58:01"`)
`%{timestamp}`	La même que `%{ctime}`, mais au format *UNIX timestamp*
`%{owner}`	Utilisateur propriétaire du fichier initial
`%{rowner}`	Utilisateur distant - propriétaire du fichier initial (si c'est inapplicable ou que la valeur est inconnue, elle est remplacée par `?`)

2. Éléments spécifiques pour la commande `threats` :

Marqueur	Description
`%{hid}`	Identificateur de l'enregistrement de la menace dans le registre des événements liés à la menace
`%{tid}`	Identificateur de menace
`%{htime}`	Date/heure de l'événement lié à la menace

Marqueur	Description
`%{app}`	Identificateur du composant Dr.Web pour Linux ayant traité la menace
`%{event}`	Dernier événement lié à la menace : • `FOUND` : la menace a été détectée ; • `Désinfecter` : la menace a été désinfectée ; • `Quarantaine` : le fichier contenant une menace a été mis en quarantaine ; • `Supprimer` : le fichier contenant une menace a été supprimé ; • `Ignorer` : la menace a été ignorée ; • `RECAPTURED` : la menace a été détectée de nouveau par un autre composant.
`%{err}`	Texte du message d'erreur (s'il n y a pas d'erreur, il est remplacé par chaîne vide)

3. Éléments spécifiques pour la commande `quarantine` :

Marqueur	Description
`%{qid}`	Date et heure du déplacement de l'objet en quarantaine
`%{qtime}`	Date/heure de la mise de l'objet en quarantaine
`%{curetime}`	Date et heure de la tentative de désinfecter l'objet mis en quarantaine (si c'est inapplicable ou que la valeur est inconnue, elle est remplacée par `?`)
`%{cureres}`	Résultat de la tentative de désinfecter l'objet mis en quarantaine : • `cured` : la menace est neutralisée ; • `not cured` : la menace n'est pas neutralisée ou il n y a pas eu de tentatives de la neutraliser.

Exemple

```
$ drweb-ctl quarantine --Format "{%{n} %{origin}: %{threat_name} - %{qtime}%{n}}"
```

Cette commande affichera le contenu de la quarantaine sous forme d'enregistrements au format suivant :

```
{
 <chemin d'accès au fichier> : <nom de menace> - <date de mise en quarantaine>
}
...
```

3.5. Commandes d'affichage d'informations

Les commandes d'affichage d'informations suivantes sont disponibles :

Commande	Description
`appinfo`	Fonction : afficher sur l'écran les informations sur les composants actifs de Dr.Web pour Linux. Les informations suivantes sont affichées pour chaque composant lancé : • Nom interne. • Identificateur du processus GNU/Linux (PID). • Statut (lancé, arrêté, etc.). • Code d'erreur, si le fonctionnement du composant a échoué. • Information supplémentaire (en option). Les informations suivantes sont affichées pour le démon de gestion de la configuration (`drweb-configd`) : • Liste des composants installés — *Installed*. • Liste des composants dont le lancement doit être assuré par le daemon — *Should run*. Arguments : Non. Options : `-f [--Follow]` : attendre les nouveaux messages sur le changement de statut du module et les afficher dès leur réception (interrompre l'attente par CTRL+C).
`baseinfo`	Fonction : Afficher des informations sur la version actuelle du moteur antivirus et le statut des bases virales. Les informations suivantes sont affichées : • Version du moteur antivirus. • Date et heure de la sortie des bases utilisées. • Nombre d'entrées virales disponibles. • Moment de la dernière mise à jour des bases virales et du moteur antivirus. • Moment de la mise à jour automatique suivante. Arguments : Non. Options : `-l [--List]` : afficher la liste complète des fichiers téléchargés des bases virales et le nombre d'entrées virales dans chaque fichier.
`certificate`	Fonction : Afficher sur l'écran le contenu du certificat fiable Dr.Web qui est utilisé par Dr.Web pour Linux pour accéder aux connexions sécurisées dans le but de les vérifier, si cette vérification est activée dans les

Commande	Description
	paramètres. Pour sauvegarder le certificat dans le fichier <*cert_name*>.pem, vous pouvez utiliser la commande suivante : `$ drweb-ctl certificate > <cert_name>.pem` Arguments : Non. Options : Non.
events	Désignation : Voir les événements de Dr.Web pour Linux. De plus, la commande permet de gérer les événements (marquer comme « lus », supprimer). Arguments : Non. Options : `--Report` <*type*> : spécifier le type de rapport des événements. Valeurs autorisées : • `BRIEF` : bref rapport. • `DEBUG` : rapport détaillé. • `JSON` : rapport sérialisé au format JSON. `-f [--Follow]` : attendre les nouveaux événements et les afficher dès leur réception (interrompre l'attente par CTRL+C). `-s [--Since]` <*date, heure*> : afficher les événements qui ont eu lieu après le moment indiqué (<*date, heure*> est indiquée au format « `YYYY-MM-DD hh:mm:ss` »). `-u [--Until]` <*date, heure*> : afficher les événements qui ont eu lieu avant le moment indiqué (<*date, heure*> est indiquée au format « `YYYY-MM-DD hh:mm:ss` »). `-t [--Types]` <*liste de types*> : afficher les événements de types listes uniquement (les types d'événements sont séparés par des virgules). Les types d'événements suivants sont disponibles : • `Mail` : une menace est détecte dans le message e-mail ; • `UnexpectedAppTermination` : arrêt d'urgence d'un composant. Pour afficher les événements de tous les types, utilisez `All`. `--ShowSeen` : afficher également les événements déjà lus. `--Delete` <*liste d'événements*> : afficher tous les événements listés (les identificateurs sont séparés par des virgules). `--Delete` <*liste d'événements*> : supprimer tous les événements listés (les identificateurs sont séparés par des virgules). `--MarkAsSeen` <*liste d'événements*> : marquer les événements listés comme « lus » (les identificateurs sont séparés par des virgules).

Commande	Description
	S'il faut marquer comme « lus » ou supprimer tous les événements, indiquez `All` à la place de <*liste d'événements*>. Par exemple, la commande suivante : `$ drweb-ctl events --MarkAsSeen All` marque tous les événements comme « lus ».
`report` <*type*>	Fonction : créer un rapport sur les événements de Dr.Web pour Linux sous forme d'une page HTML (le corps de la page est affiché dans le fichier spécifié). Arguments : <*type*> : type des événements pour lesquels le rapport est créé (un seul type est indiqué). Voir les valeurs possibles dans la description de l'option `--Types` de la commande `events` ci-dessus. Argument obligatoire. Options : `-o [--Output]` <*chemin d'accès au fichier*> : enregistrer le rapport dans le fichier indiqué. Option obligatoire. `-s [--Since]` <*date, heure*> : afficher dans le rapport les événements qui ont eu lieu après le moment indiqué (<*date, heure*> est indiquée au format « `YYYY-MM-DD hh:mm:ss` »). `-u [--Until]` <*date, heure*> : afficher dans le rapport les événements qui ont eu lieu avant le moment indiqué (<*date, heure*> est indiquée au format « `YYYY-MM-DD hh:mm:ss` »). `--TemplateDir` <*chemin vers le répertoire* > : chemin vers le répertoire dans lequel se trouvent les fichiers des modèles de la page HTML du rapport. Les options `-s`, `-u` et `--TemplateDir` ne sont pas obligatoires. Par exemple, la commande : `$ drweb-ctl report Mail -o report.html` crée le rapport sur tous les événements de détection de menaces dans des messages e-mail à la base du modèle par défaut et enregistre le résultat dans le fichier `report.html` dans le répertoire actuel.
`license`	Fonction : Afficher sur l'écran les informations sur la licence actuelle, obtenir la licence de démo ou obtenir un fichier clé pour la licence enregistrée (par exemple, sur le site de la société). Si aucune licence n'est spécifiée, les informations suivantes sont affichées (si vous utilisez la licence pour le mode standalone) : • Numéro de licence. • Date et heure de l'expiration de la licence.

Commande	Description
	Si vous utilisez la licence délivrée par le serveur de protection centralisée (pour le fonctionnement en mode de protection centralisée ou en mode mobile), les informations suivantes sont affichées. Arguments : Non. Options : `--GetDemo` : demander le fichier clé de démo pour un mois et l'obtenir si les conditions d'obtention de la période de démo sont respectées. `--GetRegistered` <*numéro de série*> : obtenir le fichier clé de licence pour le numéro de série indiqué si les conditions d'obtention de la période de démo sont respectées (par exemple, le programme n'est pas en mode de protection centralisé quand le serveur de protection centralisée gère la licence). `--Proxy` *nom d'utilisateur*>:<*mot de passe*>@<*adresse du serveur*>:<*numéro du port*> : obtenir une clé de licence via le serveur proxy (utilisé uniquement en parallèle avec l'une des options précédentes — `--GetDemo` ou `--GetRegistered`). *Si le numéro de série n'est pas un numéro de série pour la période de démo, il doit être enregistré sur le site de la société.* Pour en savoir plus sur la licence pour les produits Dr.Web, consultez la rubrique Octroi de la licence. Pour enregistrer un numéro de série et obtenir un fichier clé de démo, une connexion Internet valide est requise.
`log`	Fonction : afficher sur l'écran de la console (dans le flux *stdout*) les dernières entrées du journal de Dr.Web pour Linux (analogue à la commande `tail`). Arguments : Non. Options : `-s [--Size]` <*nombre*> : nombre de dernières entrées du journal à afficher sur l'écran. `-c [--Components]` <*liste de composants*> : liste des identificateurs des composants dont les entrées seront affichées. Les identificateurs sont séparés par des virgules. Si le paramètre n'est pas spécifié, toutes les entrées disponibles, envoyées dans le journal par les composants, sont affichées. *Vous pouvez consulter les identificateurs actuels des composants installés (c'est-à-dire, les noms de composants affichés dans le journal) avec la commande* `appinfo` *(voir ci-dessus).*

Commande	Description
	`-f [--Follow]` : attendre les nouvelles entrées dans le journal et afficher ces entrées dès leur réception (l'appui sur les touches CTRL+C interrompt l'attente).

Exemples d'utilisation

Cette section contient des exemples d'utilisation de l'utilitaire Dr.Web Ctl `drweb-ctl` :

- Analyse d'objets :
  - Commandes simples de l'analyse.
  - Analyse des fichiers sélectionnés selon des critères.
  - Analyse des objets supplémentaires.
- Gestion de la configuration.
- Gestion de menaces.
- Exemple de fonctionnement en mode de copie autonome.

1. Analyse d'objets

1.1. Commandes simples de l'analyse

1. Lancer l'analyse du répertoire `/home` avec les paramètres par défaut :

```
$ drweb-ctl scan /home
```

2. Chemins du scan listés dans le fichier `daily_scan` (un chemin par ligne) :

```
$ drweb-ctl scan --stdin < daily_scan
```

3. Lancer l'analyse du secteur d'amorçage du dispositif de disque *sda* :

```
$ drweb-ctl bootscan /dev/sda
```

4. Lancer l'analyse des processus en cours :

```
$ drweb-ctl procscan
```

1.2. Analyse des fichiers sélectionnés selon des critères

В нижеприведенных примерах для формирования выборки файлов, подлежащих проверке, используется результат работы утилиты `find`. Полученный перечень файлов передается команде `drweb-ctl scan` с параметром `--stdin` или `--stdin0`.

1. Lancer l'analyse de la liste des fichiers retournés par l'utilitaire `find` et séparés par le symbole UL ('`\0`') :

```
$ find -print0 | drweb-ctl scan --stdin0
```

2. Scanner tous les fichiers dans tous les répertoires, en commençant par le répertoire racine, dans la même partition du système de fichiers :

```
$ find / -xdev -type f | drweb-ctl scan --stdin
```

3. Scanner tous les fichiers dans tous les répertoires, en commençant par le répertoire racine, excepté les fichiers `/var/log/messages` et `/var/log/syslog` :

```
$ find / -type f ! -path /var/log/messages ! -path /var/log/syslog |
drweb-ctl scan --stdin
```

4. Scanner tous les fichiers de l'utilisateur *root* dans tous les répertoires en commençant par le répertoire racine :

```
$ find / -type f -user root | drweb-ctl scan --stdin
```

5. Scanner les fichiers de l'utilisateur *root* et *admin* dans tous les répertoires, en commençant par le répertoire racine :

```
$ find / -type f \( -user root -o -user admin \) | drweb-ctl scan --stdin
```

6. Scanner les fichiers des utilisateurs avec un UID dans la fourchette 1000–1005 dans tous les répertoires, en commençant par le répertoire racine :

```
$ find / -type f -uid +999 -uid -1006 | drweb-ctl scan --stdin
```

7. Scanner les fichiers dans tous les répertoires en commençant par le répertoire racine avec un niveau d'emboîtement inférieur ou égal à 5 :

```
$ find / -maxdepth 5 -type f | drweb-ctl scan --stdin
```

8. Scanner les fichiers dans un répertoire racine en ignorant les fichiers dans les sous-répertoires :

```
$ find / -maxdepth 1 -type f | drweb-ctl scan --stdin
```

9. Scanner les fichiers dans tous les répertoires en commençant par le répertoire racine en suivant tous les liens symboliques :

```
$ find -L / -type f | drweb-ctl scan --stdin
```

10. Scanner les fichiers dans tous les répertoires en commençant par le répertoire racine sans suivre les liens symboliques :

```
$ find -P / -type f | drweb-ctl scan --stdin
```

11. Analyser les fichiers créés au plus tard le 1 mai 2017 dans tous les répertoires en commençant par le répertoire racine :

```
$ find / -type f -newermt 2017-05-01 | drweb-ctl scan --stdin
```

1.3. Analyse des objets supplémentaires

1. Analyse des objets se trouvant dans le répertoire `/tmp` sur l'hôte distant *192.168.0.1* lors de la connexion via SSH en tant que l'utilisateur *user* avec le mot de passe *passw* :

```
$ drweb-ctl remotescan 192.168.0.1 /tmp --Login user --Password passw
```

2. Analyse du message e-mail enregistré dans le fichier `email.eml` avec l'utilisation de l'ensemble de règles par défaut :

```
$ drweb-ctl checkmail email.eml
```

2. Gestion de la configuration

1. Afficher sur l'écran toutes les informations sur le contenu actuel de Dr.Web pour Linux, y compris les informations sur les composants lancés :

```
$ drweb-ctl appinfo
```

2. Afficher tous les paramètres de la configuration active depuis la section `[Root]` :

```
$ drweb-ctl cfshow Root
```

3. Indiquer `'No'` comme valeur du paramètre `Start` dans la section `[LinuxSpider]` de la configuration active (ce paramètre désactive SpIDer Guard – moniteur du système de fichiers) :

```
# drweb-ctl cfset LinuxSpider.Start No
```

   Notez que les privilèges de super-utilisateur sont requis pour cela. Exemple de la même commende exécutée avec `sudo` pour élever temporairement les privilèges :

```
$ sudo drweb-ctl cfset LinuxSpider.Start No
```

4. Forcer la mise à jour des composants antivirus de Dr.Web pour Linux :

```
$ drweb-ctl update
```

5. Redémarrez la configuration pour les composants de Dr.Web pour Linux :

```
# drweb-ctl reload
```

   Notez que les privilèges de super-utilisateur sont requis pour cela. Exemple de la même commende exécutée avec `sudo` pour élever temporairement les privilèges :

```
$ sudo drweb-ctl reload
```

6. Connecter Dr.Web pour Linux au serveur de protection centralisée fonctionnant sur le nœud *192.168.0.1*, à condition que le certificat du serveur se trouve dans le fichier `/home/user/cscert.pem` :

```
$ drweb-ctl esconnect 192.168.0.1 --Certificate /home/user/cscert.pem
```

7. Pour connecter Dr.Web pour Linux au serveur de protection centralisée à l'aide du fichier de configuration de la connexion settings.cfg :

```
$ drweb-ctl esconnect --cfg <chemin d'accès au fichier settings.cfg>
```

8. Déconnecter Dr.Web pour Linux du serveur de protection centralisée :

```
# drweb-ctl esdisconnect
```

Notez que les privilèges de super-utilisateur sont requis pour cela. Exemple de la même commende exécutée avec `sudo` pour élever temporairement les privilèges :

```
$ sudo drweb-ctl esdisconnect
```

9. Consulter les derniers enregistrements faits par les composants `drweb-update` et `drweb-configd` dans le journal de Dr.Web pour Linux :

```
# drweb-ctl log -c Update,ConfigD
```

3. Gestion de menaces

1. Afficher sur l'écran les informations sur les menaces détectées :

```
$ drweb-ctl threats
```

2. Déplacer en quarantaine tous les fichiers contenant des menaces non neutralisées :

```
$ drweb-ctl threats --Quarantine All
```

3. Afficher sur l'écran la liste des fichiers mis en quarantaine :

```
$ drweb-ctl quarantine
```

4. Restaurer tous les fichiers de la quarantaine :

```
$ drweb-ctl quarantine --Restore All
```

4. Exemple de fonctionnement en mode de copie autonome

1. Analyser les fichiers et traiter la quarantaine en mode de copie autonome :

```
$ drweb-ctl scan /home/user -a --OnKnownVirus=Quarantaine
$ drweb-ctl quarantine -a --Delete All
```

La première commande analysera les fichiers dans le répertoire `/home/user` en mode de copie autonome et les fichiers contenant les virus connus seront mis en quarantaine. La deuxième commande traitera tout le contenu de la quarantaine (également en mode de copie autonome) et supprimera les objets qu'elle contient.

Annexes

Annexe A. Types de menaces informatiques

Par le terme *« menace »* nous comprenons tout logiciel pouvant potentiellement ou directement endommager l'ordinateur ou le réseau, ou porter atteinte aux données ou aux droits de l'utilisateur (logiciels malveillants ou indésirables). Dans le sens le plus large du terme, « menace » peut indiquer tout type de danger potentiel pour la sécurité de l'ordinateur ou du réseau (ainsi, une vulnérabilité peut être utilisée pour des attaques de pirates).

Tous les types de logiciels décrits ci-dessous peuvent présenter un danger pour les données de l'utilisateur et pour son droit à la confidentialité. Les logiciels qui ne dissimulent pas leur présence dans le système (par exemple, certains logiciels pour diffusion de spam ou analyseurs du trafic), ne sont normalement pas considérés comme menaces, mais peuvent l'être sous certaines conditions.

Virus informatiques

Ce type de menaces informatiques se caractérise par sa capacité à introduire son code dans le code d'exécution d'autres logiciels. Cette pénétration porte le nom d'*infection*. Dans la plupart des cas, le fichier infecté devient lui-même porteur du virus et le code introduit n'est plus conforme à l'original. La majeure partie des virus est conçue pour détériorer ou détruire les données du système.

Dans la classification de Doctor Web, les virus sont triés par le type d'objets qu'ils infectent :

- *Virus de fichiers* : virus infectant les fichiers système (fichiers exécutables, bibliothèques dynamiques) et qui s'activent au lancement du fichier infecté.
- *Macrovirus* infectant les fichiers utilisés par les applications Microsoft® Office et d'autres programmes utilisant des commandes macros (généralement écrits en Visual Basic). *Macros*, ce sont des logiciels internes, écrits dans un langage de programmation totalement fonctionnel. Par exemple, dans Microsoft® Word, les macros se lancent automatiquement lorsque vous ouvrez, (fermez, sauvegardez etc) un document.
- *Virus script* : virus écrits en langages de script qui infectent dans la plupart des cas d'autres scripts (par exemple, les fichiers du système d'exploitation). Ils peuvent également infecter d'autres formats de fichiers qui supportent l'exécution des scripts, tout en se servant des scripts vulnérables des applications Web.
- *Virus de boot* : ils infectent les secteurs d'amorçage des disques et des partitions aussi bien que les principaux secteurs boot des disques durs. Ils occupent peu de mémoire et restent prêts à remplir leurs fonctions jusqu'à ce qu'un déchargement, un redémarrage ou un arrêt du système ne soient effectués.

La plupart des virus possèdent des mécanismes de protection contre leur détection. Leurs méthodes de protection contre la détection s'améliorent sans cesse, de même que les moyens pour les contrer. On peut également classer les virus selon le moyen de protection contre la détection qu'ils utilisent :

- *Virus chiffrés* : ils chiffrent leur code à chaque infection afin de rendre leur détection dans un fichier, un secteur d'amorçage ou en mémoire, plus difficile. Toutes les variantes de ce type de virus contiennent uniquement un petit fragment de code en commun (la procédure de déchiffrement) qui peut être utilisé comme la signature du virus.
- *Virus polymorphes* : ce sont des virus qui chiffrent également leur code mais qui, en plus, utilisent un algorithme de déchiffrement spécifique différent à chaque nouvelle variante du virus. Ceci implique que ces types de virus n'ont pas de signature virale.
- *Virus furtifs* : ils agissent de telle façon qu'ils masquent leur activité et cachent leur présence dans les objets infectés. Ces virus captent les caractéristiques d'un objet avant de l'infecter et présentent ensuite ces caractéristiques « modèles » au scanner antivirus cherchant, lui, à dépister des fichiers modifiés.

On peut également classer les virus d'après le langage de programmation dans lequel ils sont écrits (la plupart sont écrits en Assembleur, en langages de haut niveau de programmation et en langages de scripts, etc.) ainsi que selon les systèmes d'exploitation ciblés.

Vers informatiques

Récemment, les vers sont devenus plus fréquents que les virus ou d'autres logiciels malveillants. Tout comme les virus, ils sont capables de s'autorépliquer et de diffuser leurs copies, mais n'affectent pas d'autres logiciels ni fichiers (ils n'ont pas besoin des fichiers host pour se répandre). Les vers pénètrent dans un ordinateur du réseau (souvent via une pièce jointe dans un email ou via Internet) et ils envoient massivement leurs propres copies à d'autres ordinateurs du réseau. Au départ, pour se propager, les vers peuvent profiter des actions de l'utilisateur ou choisir le poste à attaquer de manière automatique.

Les vers ne sont pas forcément composés d'un seul fichier (le corps du ver). Plusieurs d'entre eux possèdent également une partie infectieuse (le shellcode), qui se charge dans la mémoire vive (RAM) de l'ordinateur puis télécharge le corps du ver sous forme de fichier exécutable via le réseau. Si seul le shellcode est présent dans le système, le ver peut être supprimé en redémarrant simplement l'ordinateur (et la mémoire vive est déchargée et remise à zéro). Mais aussitôt que le corps du ver entre dans le système, seul l'antivirus peut le désinfecter.

A cause de leur propagation intense, les vers peuvent paralyser des réseaux entiers, même s'ils n'endommagent pas directement le système.

Doctor Web classifie les vers d'après leur mode de propagation :

- *Les vers de réseau* se propagent à l'aide de différents protocoles réseau ou d'échanges de fichiers.
- *Les vers de courrier* se propagent via les protocoles de courrier électronique (POP3, SMTP, etc.).

- *Les vers de tchat* se propagent en utilisant les messageries instantanées (ICQ, IM, IRC, etc.).

Chevaux de Troie (Trojans)

Ce type de logiciels malicieux n'est pas capable de s'autorépliquer ni d'infecter d'autres logiciels. Les chevaux de Troie se substituent à des programmes très utilisés, effectuent les mêmes actions qu'eux ou en imitent le fonctionnement. Dans le même temps, ils effectuent des actions malveillantes dans le système (suppriment ou endommagent des fichiers ou des données, envoient les données confidentielles de l'utilisateur, etc.) ou donnent aux cybercriminels un accès à l'ordinateur pour, par exemple, porter atteinte au propriétaire de l'ordinateur touché.

Les capacités de camouflage et d'endommagement d'un cheval de Troie sont les mêmes que celles d'un virus. Un Trojan peut représenter lui-même un module de virus. Mais dans la plupart des cas, les Trojans se diffusent comme des fichiers exécutables isolés (via les serveurs d'échange de fichiers, les supports amovibles ou dans les pièces jointes des emails) qui sont exécutés par l'utilisateur lui-même ou par les tâches système.

Il est difficile de classifier les Trojans car ils sont souvent diffusés par des virus ou des vers mais également parce que beaucoup d'actions malveillantes pouvant être effectuées par d'autres types de menaces sont imputées aux Trojans uniquement. Certains types de Trojans sont classés à part par les spécialistes de Doctor Web :

- *Backdoors* : ce sont des Trojans qui offrent un accès privilégié au système, contournant le mécanisme existant d'accès et de protection. Les backdoors n'infectent pas les fichiers, mais ils s'inscrivent dans le registre, modifiant les clés de registre.
- *Rootkits* : ils sont destinés à intercepter les fonctions de l'API du système d'exploitation pour dissimuler leur présence dans le système. En outre, le rootkit peut masquer les processus d'autres logiciels (par ex, d'autres menaces), les clés de registre, des fichiers et des dossiers. Le rootkit se propage comme un logiciel indépendant ou comme le composant d'un autre logiciel malveillant. Selon leur mode de fonctionnement, il existe deux types de rootkits : *User Mode Rootkits (UMR)* qui fonctionnent dans le mode utilisateur (interception des fonctions des bibliothèques du mode utilisateur), et *Kernel Mode Rootkits (KMR)* qui fonctionnent dans le mode noyau (interception des fonctions au niveau du noyau système, ce qui rend la détection plus difficile).
- *Keyloggers* : ils sont utilisés pour enregistrer les données entrées par l'utilisateur sur le clavier. Le but de ces actions est le vol des données personnelles (mots de passe, logins, numéros de cartes bancaires, etc.).
- *Cliqueurs* : ils redirigent les liens quand on clique sur eux. D'ordinaire, l'utilisateur est redirigé vers des adresses déterminées avec le but d'augmenter le trafic publicitaire des sites web ou pour organiser des attaques DDoS.
- *Trojans proxy* : ils offrent aux cybercriminels un accès anonyme à Internet via l'ordinateur de leur victime.

Les Trojans peuvent accomplir d'autres actions malveillantes comme, par exemple, changer la page d'accueil du navigateur web ou supprimer certains fichiers. Mais ces actions peuvent

également être exécutées par les menaces d'autres types (par exemple, par des virus et des vers).

Hacktools

Les hacktools sont créés pour aider les hackers. Les logiciels de ce type les plus répandus sont des scanners de ports sachant détecter les vulnérabilités des pare-feux (firewalls) et d'autres composants qui assurent la sécurité du système de l'ordinateur. A part les pirates, les administrateurs peuvent utiliser ce type d'outils pour vérifier la sécurité de leurs réseaux. Certains logiciels utilisés pour le hacking ou ceux qui utilisent l'ingénierie sociale sont considérés comme des hacktools.

Adwares

Sous ce terme, on désigne le plus souvent un code interne aux logiciels gratuits qui impose l'affichage d'une publicité sur l'ordinateur de l'utilisateur. Mais parfois, ce code peut être diffusé par d'autres logiciels malveillants et afficher des publicités dans les navigateurs web. Très souvent, ces adwares fonctionnent en utilisant des données collectées par des logiciels espions.

Canulars

Ce type de logiciels malveillants, comme les adwares, ne détériorent pas le système. Ils génèrent le plus souvent des messages sur des erreurs inexistantes et effraient l'utilisateur pour effectuer des actions qui peuvent mener à la perte de données. Leur but est d'intimider l'utilisateur ou de l'irriter.

Dialers

Ce sont de petites applications installées sur les ordinateurs, élaborées spécialement pour scanner un certain spectre de numéros de téléphone. Par la suite, les cybercriminels utiliseront les numéros trouvés pour prélever de l'argent à leur victime ou pour connecter l'utilisateur à des services téléphoniques surtaxés et coûteux.

Riskwares

Ces logiciels ne sont pas créés pour détériorer le système, mais peuvent être utilisés pour paralyser la sécurité du système grâce à certaines fonctionnalités. C'est pourquoi ils sont classés parmi les menaces mineures. Ces logiciels peuvent non seulement détériorer les données ou les supprimer par hasard, mais ils peuvent également être utilisés par des crackers ou par d'autres logiciels pirates pour nuire au système. Parmi ce type de logiciels, on peut trouver les tchats et les outils d'administration à distance, les serveurs FTP, etc.

Objets suspects

Ce sont des menaces potentielles dépistées à l'aide de l'analyse heuristique. Ces objets peuvent s'avérer appartenir à un des types de menaces informatiques (même encore inconnues) ou être absolument inoffensifs, en cas de faux positif. Dans tous les cas, il est recommandé de placer les objets suspects en quarantaine et de les envoyer pour analyse au laboratoire antivirus de Doctor Web.

Annexe B. Neutralisation des menaces

Toutes les solutions antivirus créées par Dr.Web utilisent un ensemble de méthodes de détection, ce qui leur permet d'effectuer des analyses en profondeur des fichiers suspects et de contrôler le comportement des logiciels.

- Méthode de détection des menaces.
- Actions appliquées aux menaces.

Méthode de détection des menaces

Analyse par signature

C'est la première méthode de détection appliquée. Le scan commence par l'analyse de l'objet à la recherche des signatures des virus connus. Une *signature* est une séquence continue et finie d'octets qui est nécessaire et suffisante pour identifier une menace. Pour réduire la taille de la base de signatures, les solutions antivirus Dr.Web utilisent des sommes de contrôle de signatures au lieu de séquences complètes de signatures. Les sommes de contrôle identifient les signatures de manière unique, ce qui garantit l'exactitude de la détection de virus et leur neutralisation. Les bases de données virales Dr.Web sont faites de telle sorte que certaines entrées peuvent être utilisées pour détecter non seulement un virus, mais une famille entière de menaces.

Origins Tracing™

C'est une technologie unique qui permet de détecter de nouveaux virus ou des virus modifiés utilisant des mécanismes d'infection connus. Appliquée à la fin de l'analyse par signatures, elle assure la protection des utilisateurs des solutions antivirus Dr.Web contre des menaces telles que le Trojan.Encoder.18 (également connu sous le nom gpcode). En outre, l'utilisation de la technologie Origins Tracing™ peut réduire considérablement le nombre de faux positifs de l'analyseur heuristique. Les objets détectés grâce à Origins Tracing™ obtiennent l'extension `.Origin`.

Émulation d'exécution

La méthode d'émulation d'exécution de code est utilisée pour détecter les virus polymorphes et cryptés si la recherche à l'aide des sommes de contrôle des signatures est inapplicable ou considérablement compliquée en raison de l'impossibilité de construire des signatures fiables. La méthode consiste à simuler l'exécution du code en utilisant un *émulateur* — un modèle de programmation du processeur et de l'environnement d'exécution. L'Émulateur fonctionne avec un espace mémoire protégé (tampon d'émulation), dans lequel l'exécution du logiciel analysé est modélisée instruction par instruction. Cependant, les instructions ne sont pas transmises à un processeur central (CPU) pour exécution réelle. Lorsque l'émulateur reçoit un fichier infecté par

un virus polymorphe, le résultat de l'émulation donne le corps décrypté du virus, qui est ensuite facilement trouvable via une recherche par les sommes de contrôles de signatures.

Analyse heuristique

Le fonctionnement de l'analyseur heuristique est fondé sur un ensemble d'*heuristiques* (hypothèses, dont la signification statistique est confirmée par l'expérience) sur les signes caractéristiques des codes malveillants et, inversement, sur les caractéristiques qui sont extrêmement rares dans les virus. Chaque attribut ou caractéristique du code possède un *score* indiquant le niveau de dangerosité et de fiabilité. Le score peut être positif si le signe indique la présence d'un comportement de code malveillant, et négatif si le signe ne correspond pas à une menace informatique. En fonction du score total du fichier, l'analyseur heuristique calcule la probabilité de la présence d'un objet malveillant inconnu. Si cette probabilité dépasse une certaine valeur de seuil, l'objet analysé est considéré comme malveillant.

L'analyseur heuristique utilise également la technologie FLY-CODE™ — un algorithme universel pour l'extraction des fichiers. Ce mécanisme permet de construire des hypothèses heuristiques sur la présence d'objets malveillants dans les objets, de logiciels compressés par des outils de compression (emballeurs), non seulement par des outils connus des développeurs des produits Dr.Web, mais également par des outils de compression nouveaux et inexplorés. Lors du contrôle des objets emballés, les solutions antivirus Dr.Web utilisent également l'analyse par entropie structurale. La technologie détecte les menaces en assemblant des parties de code ; ainsi, une entrée dans la base de données permet l'identification de plusieurs menaces emballées par le même emballeur polymorphe.

Comme tout système basé sur des hypothèses, l'analyseur heuristique peut commettre des erreurs de type I ou II (omettre une menace ou faire un faux positif). Par conséquent, les objets détectés par l'analyseur heuristique reçoivent le statut « suspects ».

Au cours de toute analyse, tous les composants des produits antivirus Dr.Web utilisent l'information la plus récente sur tous les programmes malveillants connus. Dès que les spécialistes du laboratoire antivirus Doctor Web découvrent une nouvelle menace, les informations sur ses propriétés et les caractéristiques de comportement sont tout de suite ajoutées dans les bases virales. Parfois, les mises à jour sont publiées plusieurs fois par heure. Ainsi, même si un nouveau programme malveillant passe à travers la protection résidente Dr.Web et pénètre dans le système, il sera détecté et neutralisé après la mise à jour des bases virales.

Technologie cloud de détection de menaces

Les méthodes cloud de détection permettent d'analyser tout objet (fichier, application, extension pour le navigateur, etc) par sa *somme de contrôle*. Elle représente une séquence de chiffres et de lettres d'une longueur spécifiée. Lors de l'analyse par la somme de contrôle, les objets sont analysés par la base existante et ensuite sont classés dans les catégories suivantes : sains, suspects, malveillants, etc.

Une telle technologie réduit le temps de l'analyse des fichiers et économise les ressources de l'appareil. Vu que c'est la somme de contrôle unique qui est analysée et non pas l'objet, la décision est prise tout de suite. S'il n'y a pas de connexion aux serveurs Dr.Web Cloud, les fichiers sont analysés de manière locale et l'analyse cloud est reprise après la restauration de la connexion.

Ainsi, le service Dr.Web Cloud collecte les informations de plusieurs utilisateurs et met a jour rapidement les données sur les menaces inconnues auparavant. Grâce à cela, l'efficacité de la protection d'appareils augmente.

Actions appliquées aux menaces

Les produits antivirus Dr.Web peuvent appliquer des actions spécifiques aux objets détectés pour neutraliser les menaces informatiques. L'utilisateur peut laisser le logiciel appliquer automatiquement les actions paramétrées par défaut, indiquer les actions à appliquer automatiquement, ou choisir manuellement une action spécifique pour chaque objet dépisté. Les actions disponibles sont :

- **Ignorer** *(Ignorer, sauter)* : ignorer la menace détectée sans appliquer aucune action ;
- **Signaler** *(Informer)* : informer de la présence d'une menace mais n'appliquer aucune action ;
- **Désinfecter** *(Désinfecter)* : essayer de désinfecter l'objet infecté en supprimant le contenu malveillant et en gardant l'intégrité du contenu utile. Notez que cette action ne s'applique pas à tous les types de menaces ;
- **Quarantaine** *(Déplacer en quarantaine, Isoler)* : déplacer un objet infecté (s'il admet cette opération) dans un répertoire spécial de quarantaine pour l'isoler ;
- **Supprimer** *(Supprimer)* : supprimer définitivement l'objet infecté.

Si la menace est détecté dans un fichier se trouvant dans un conteneur (archive, message, etc.), le conteneur n'est pas supprimé mais il est mise en quarantaine.

Annexe C. Support technique

En cas de problèmes liés à l'installation ou au fonctionnement des produits de la société, avant de contacter le support technique, essayez de trouver la solution par un des moyens suivants :

- consultez les dernières versions des descriptions et des manuels à l'adresse https://download.drweb.fr/doc/ ;
- lisez la rubrique de questions fréquentes à l'adresse https://support.drweb.com/show_faq/ ;
- visitez des forums de Doctor Web à l'adresse https://forum.drweb.com/.

Si après avoir tout essayé, vous n'avez pas résolu le problème, utilisez un des moyens suivants pour contacter le support technique de Doctor Web :

- remplissez le formulaire de question dans la section correspondante de la rubrique

https://support.drweb.com/ ;

- appelez le numéro : 0 825 300 230.

Vous pouvez trouver les informations sur les bureaux régionaux de Doctor Web sur le site officiel à l'adresse https://company.drweb.com/contacts/offices/.

Pour faciliter le travail de l'analyse de votre problème pour le support technique, il est recommandé de former le paquet d'informations sur le produit installé, ses paramètres et l'environnement système. Pour cela, utilisez l'utilitaire spécial inclus dans Dr.Web pour Linux.

Pour collecter les informations pour le support technique, entrez la commande suivante :

```
# /opt/drweb.com/bin/support-report.sh
```

Pour collecter les informations pour le support technique, il est recommandé de lancer l'utilitaire avec les privilèges de super-utilisateur (utilisateur *root*). Pour élever les privilèges, utilisez la commande de changement d'utilisateur `su` ou la commande d'exécution du nom d'un autre utilisateur `sudo`.

Durant son fonctionnement, l'utilitaire collecte et met en archive les informations suivantes :

- Informations sur l'OS (nom, architecture, sortie de la commande `uname -a`) ;
- Liste des paquets installés dans le système, y compris les paquets d'Doctor Web ;
- Contenu des journaux :
  - les journaux de Dr.Web pour Linux (s'ils sont configurés pour les composants particuliers) ;
  - le journal rédigé par le démon de journalisation `syslog` (`/var/log/syslog`, `/var/log/messages`) ;
  - le journal du gestionnaire de paquets système (`apt`, `yum`, etc.) ;
  - journal `dmesg`;
- Résultats de l'exécution des commandes suivantes : `df`, `ip a` (`ifconfig -a`), `ldconfig -p`, `iptables-save`, `nft export xml`.
- Informations sur les paramètres et la configuration de Dr.Web pour Linux :
  - liste des bases virales téléchargées (`drweb-ctl baseinfo -l`) ;
  - liste des fichiers des répertoires de Dr.Web pour Linux et leurs hashs MD5 ;
  - version et hash MD5 du fichier du moteur antivirus Dr.Web Virus-Finding Engine ;
  - paramètres de configuration de Dr.Web pour Linux (y compris : le contenu du fichier `drweb.ini`, les règles et les fichiers de valeurs utilisés dans les règles, les procédures Lua, etc.) ;
  - Informations sur l'utilisateur et les autorisations extraites du fichier clé, si Dr.Web pour Linux ne fonctionne pas en mode de protection centralisée.

L'archive créée contenant les informations sur le produit et l'environnement système sera enregistrée dans le répertoire de base de l'utilisateur ayant lancé l'utilitaire et portera le nom

suivant :

```
drweb.report.<timestamp>.tgz
```

où <*timestamp*> est un horodatage complet de l'heure de création du rapport, incluant les millisecondes, par exemple : `20190618151718.23625`.

Annexe D. Erreurs connues

Cette section contient :

- Recommandations sur l'identification des erreurs
- Codes d'erreurs
- Erreurs sans code

> Si vous ne trouvez pas la description de l'erreur survenue, il est recommandé de contacter le Support technique. Indiquez le code d'erreur et décrivez les conditions de son apparition.

Recommandations sur l'identification des erreurs

- Pour préciser la raison et les circonstances de l'erreur, consultez le journal de Dr.Web pour Linux (par défaut il se trouve dans le fichier `/var/log/syslog` ou `/var/log/messages` en fonction de l'OS utilisé). Vous pouvez également utiliser la commande `drweb-ctl log`.
- Pour faciliter l'identification d'une erreur, il est recommandé de configurer la sortie du journal vers un fichier particulier et d'autoriser l'affichage des informations de débogage détaillées. Pour ce faire, exécutez les commandes suivantes :

```
# drweb-ctl cfset Root.Log <chemin d'accès au fichier de journal>
# drweb-ctl cfset Root.DefaultLogLevel DEBUG
```

- Pour réinitialiser les paramètres de journalisation par défaut, exécutez les commandes suivantes :

```
# drweb-ctl cfset Root.Log -r
# drweb-ctl cfset Root.DefaultLogLevel -r
```

Codes d'erreurs

Message d'erreur	*Erreur de connexion à l'écran*
Code d'erreur	x1

Description	Erreur de connexion d'un ou de plusieurs composants au démon de gestion de la configuration Dr.Web ConfigD.

Résoudre l'erreur :

1. Redémarrez le démon de gestion de la configuration, en exécutant la commande

   ```
   # service drweb-configd restart
   ```

2. Assurez-vous que le mécanisme d'authentification PAM est installé dans le système, qu'il est configuré et qu'il fonctionne correctement. Si ce n'est pas le cas, installez le mécanisme et configurez-le (pour plus d'informations, consultez les manuels d'administration de votre distribution de l'OS).
3. Si le démon de gestion de la configuration est redémarré, PAM est correctement configuré mais l'erreur persiste, essayez de réinitialiser les paramètres par défaut de Dr.Web pour Linux.

   Pour ce faire, nettoyez le fichier *<etc_dir>*`/drweb.ini` (dans ce cas, il est recommandé de sauvegarder la copie du fichier de configuration), par exemple, en exécutant la commande :

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   Ensuite, redémarrez le démon de gestion de la configuration.
4. Si vous n'arrivez pas à lancer le démon de gestion de la configuration, essayez de réinstaller le package `drweb-configd`.

   Pour en savoir plus sur l'installation et la suppression du produit ou de ses composants, consultez les rubriques Installation de Dr.Web pour Linux et Suppression de Dr.Web pour Linux.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*L'opération est déjà en exécution*
Code d'erreur	`x2`
Description	L'opération demandée est déjà en exécution.

Résoudre l'erreur :

1. Attendez la fin de l'opération et, si nécessaire, recommencez l'action nécessaire plus tard.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*L'opération attend l'exécution*
Code d'erreur	`x3`
Description	L'opération demandée attend l'exécution (il est possible que la connexion réseau s'établisse en ce moment ou qu'un composant de soit en train de télécharger ou de s'initialiser. Cela peut prendre un certain temps).

Résoudre l'erreur : 1. Attendez le début de l'exécution de l'opération et, si nécessaire, recommencez l'action nécessaire plus tard.
Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Interrompu par l'utilisateur*
Code d'erreur	x4
Description	L'action a été interrompue par l'utilisateur.
Résoudre l'erreur : 1. Recommencez l'action nécessaire plus tard.	
Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.	

Message d'erreur	*L'opération est annulée*
Code d'erreur	x5
Description	L'action a été annulée.
Résoudre l'erreur : 1. Répétez l'action nécessaire.	
Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.	

Message d'erreur	*La connexion IPC est interrompue*
Code d'erreur	x6
Description	La connexion IPC à un composant de Dr.Web pour Linux est interrompue (il est probable que le composant s'est arrêté à cause de l'inactivité ou suite à une commande de l'utilisateur).
Résoudre l'erreur : 1. Si l'opération exécutée a échoué, recommencez-la. Sinon la déconnexion n'est pas une erreur.	
Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.	

Message d'erreur	*Taille de message IPC invalide*
Code d'erreur	x7

Description	Lors de l'échange de données entre les composants, un message de taille inacceptable est reçu.

Résoudre l'erreur :

1. Redémarrez Dr.Web pour Linux, en exécutant la commande suivante :

```
# service drweb-configd restart
```

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Format de message IPC invalide*
Code d'erreur	x8
Description	Lors de l'échange de données entre les composants, un message au format inacceptable est reçu.

Résoudre l'erreur :

1. Redémarrez Dr.Web pour Linux, en exécutant la commande suivante :

```
# service drweb-configd restart
```

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Non prêt*
Code d'erreur	x9
Description	L'action nécessaire ne peut pas être effectuée car le composant ou l'appareil requis n'est pas encore initialisé.

Résoudre l'erreur :

1. Recommencez l'action nécessaire plus tard.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Le composant n'est pas installé*
Code d'erreur	x10
Description	Le composant nécessaire pour l'exécution de la fonction requise n'est pas installé.

Résoudre l'erreur :

1. Installez à part ou réinstallez le paquet avec le composant en question :
   - `drweb-filecheck`, si le Scanner n'est pas installé.

- `drweb-spider`, si SpIDer Guard n'est pas installé.
- `drweb-gated`, si SpIDer Gate n'est pas installé.
- `drweb-update`, si l'Updater n'est pas installé.

2. Si l'erreur persiste, ou que vous ne pouvez pas déterminer quel composant est manquant, supprimez Dr.Web pour Linux et réinstallez-le.

   Pour en savoir plus sur l'installation et la suppression du produit ou de ses composants, consultez les rubriques Installation de Dr.Web pour Linux et Suppression de Dr.Web pour Linux.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Message IPC inattendu*
Code d'erreur	`x11`
Description	Lors de l'échange de données entre les composants, un message inacceptable est reçu.

Résoudre l'erreur :

1. Redémarrez Dr.Web pour Linux, en exécutant la commande suivante :

```
# service drweb-configd restart
```

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Violation du protocole IPC*
Code d'erreur	`x12`
Description	Lors de l'échange de données entre les composants, le protocole a été violé.

Résoudre l'erreur :

1. Redémarrez Dr.Web pour Linux, en exécutant la commande suivante :

```
# service drweb-configd restart
```

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Statut de sous-système inconnu*
Code d'erreur	`x13`
Description	Le sous-système de Dr.Web pour Linux nécessaire pour l'exécution de l'opération est en état inconnu.

Résoudre l'erreur :

1. Répétez l'opération.
2. Redémarrez Dr.Web pour Linux, en exécutant la commande suivante :

   ```
   # service drweb-configd restart
   ```

   ensuite, répétez l'opération.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Le chemin doit être absolu*
Code d'erreur	`x20`
Description	Vous avez indiqué le chemin relatif pour accéder à un fichier ou un répertoire au lieu du chemin absolu.

Résoudre l'erreur :

1. Modifiez le chemin vers le fichier ou le répertoire d'une façon qu'il soit absolu, et répétez l'opération.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Pas assez de mémoire pour terminer l'opération*
Code d'erreur	`x21`
Description	Pas assez de mémoire pour exécuter l'opération nécessaire.

Résoudre l'erreur :

1. Essayez d'augmenter la taille de la mémoire disponible pour les processus de Dr.Web pour Linux (par exemple, en modifiant les limites à l'aide de la commande `ulimit`), de redémarrer le logiciel et de répéter l'opération.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Erreur d'entrée-sortie*
Code d'erreur	`x22`
Description	Une erreur d'entrée/sortie s'est produite (par exemple, le lecteur n'est pas encore initialisé ou que la section du système de fichiers n'est plus disponible).

Résoudre l'erreur :

1. Vérifiez la disponibilité de l'appareil d'entrée/sortie nécessaire ou de la section du système de fichiers. Exécutez le montage et recommencez l'opération, si cela est nécessaire.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Fichier ou répertoire inexistant*
Code d'erreur	x23
Description	Tentative d'accès à un fichier ou un répertoire inexistant.

Résoudre l'erreur :

1. Vérifiez si le chemin indiqué est correct. Modifiez le chemin, si cela est nécessaire, et répétez l'opération.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Accès refusé*
Code d'erreur	x24
Description	Pas assez de droits pour accéder à l'objet indiqué (fichier ou répertoire),

Résoudre l'erreur :

1. Vérifiez la justesse du chemin indiqué et la présence des droits requis du composant. S'il est nécessaire d'accéder à l'objet, modifiez les droits d'accès ou augmentez les privilèges du composant et répétez l'opération.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*N'est pas un répertoire*
Code d'erreur	x25
Description	L'objet indiqué du système de fichiers n'est pas un répertoire.

Résoudre l'erreur :

1. Modifiez le chemin et répétez l'opération.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Le fichier de données est endommagé*
Code d'erreur	x26
Description	Les données requises sont endommagées.

Résoudre l'erreur :

1. Répétez l'opération.
2. Redémarrez Dr.Web pour Linux, en exécutant la commande suivante :

```
# service drweb-configd restart
```

ensuite, répétez l'opération.
Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Le fichier existe déjà*
Code d'erreur	x27
Description	Le nom du fichier existe déjà.
Résoudre l'erreur : 1. Modifiez le chemin et répétez l'opération.	
Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.	

Message d'erreur	*Le système de fichiers est accessible seulement en lecture*
Code d'erreur	x28
Description	Le système de fichiers est accessible seulement en lecture.
Résoudre l'erreur : 1. Vérifiez si le chemin indiqué est correct. Corrigez le chemin de façon qu'il mène à la section du système de fichiers accessible en écriture et répétez l'opération.	
Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.	

Message d'erreur	*Erreur de réseau*
Code d'erreur	x29
Description	Erreur de réseau (il est probable que l'hôte distant a cessé de répondre ou qu'il est impossible d'établir la connexion nécessaire).
Résoudre l'erreur : 1. Vérifiez la disponibilité du réseau et la justesse des paramètres réseau. Corrigez les paramètres réseau, si cela est nécessaire, et répétez l'opération.	
Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.	

Message d'erreur	*N'est pas un lecteur*
Code d'erreur	x30
Description	Tentative d'accès à un appareil d'entrée/sortie qui n'est pas un lecteur.
Résoudre l'erreur :	

1. Vérifiez la justesse du nom d'appareil indiqué. Corrigez le chemin de façon qu'il mène au lecteur et répétez l'opération.
Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Fin de fichier inattendue*
Code d'erreur	`x31`
Description	La fin de fichier inattendue a été atteinte lors de la lecture de données.
Résoudre l'erreur : 1. Vérifiez la justesse du nom de fichier indiqué. Corrigez le chemin de façon qu'il mène au fichier juste et répétez l'opération.	
Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.	

Message d'erreur	*Le fichier a été modifié*
Code d'erreur	`x32`
Description	Le fichier analysé a été modifié.
Résoudre l'erreur : 1. Répétez l'opération de scan.	
Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.	

Message d'erreur	*Fichier spécial*
Code d'erreur	`x33`
Description	L'objet demandé du système de fichiers n'est pas un fichier régulier (cela peut être un répertoire, un socket ou un autre objet).
Résoudre l'erreur : 1. Vérifiez la justesse du nom de fichier indiqué. Corrigez le chemin de façon qu'il mène au fichier régulier et répétez l'opération.	
Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.	

Message d'erreur	*Ce nom est déjà utilisé*
Code d'erreur	`x34`
Description	Le nom de l'objet existe déjà.

Résoudre l'erreur : 1. Modifiez le chemin et répétez l'opération.
Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*L'hôte est désactivé*
Code d'erreur	x35
Description	L'hôte distant n'est pas accessible par le réseau.
Résoudre l'erreur : 1. Vérifiez la disponibilité de l'hôte de réseau nécessaire. Corrigez l'adresse de l'hôte et répétez l'opération, si cela est nécessaire.	
Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.	

Message d'erreur	*La limite d'utilisation de la ressource est atteinte*
Code d'erreur	x36
Description	La limite d'utilisation de la ressource est atteinte.
Résoudre l'erreur : 1. Vérifiez la disponibilité de la ressource nécessaire. Augmentez la limite d'utilisation de la ressource et répétez l'opération.	
Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.	

Message d'erreur	*Différents points de montage*
Code d'erreur	x37
Description	La restauration du fichier signifie le déplacement entre deux points de montage différents
Résoudre l'erreur : 1. Sélectionnez un autre chemin pour la restauration du fichier et répétez l'opération.	
Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.	

Message d'erreur	*Erreur de décompression*
Code d'erreur	x38

Description	Impossible de décompresser l'archive (il est possible qu'elle soit protégée par un mot de passe ou endommagée)

Résoudre l'erreur :

1. Assurez-vous que le fichier n'est pas endommagé. Si l'archive est protégée par un mot de passe, enlevez la protection en entrant le mot de passe correct et répétez l'opération.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*La base virale est endommagée*
Code d'erreur	`x40`
Description	Les bases virales sont endommagées.

Résoudre l'erreur :

1. Vérifiez si le chemin d'accès au répertoire des bases virales est correct et corrigez-le, si cela est nécessaire (le paramètre `VirusBaseDir` dans la section `[Root]` du fichier de configuration).

   Pour consulter et modifier le chemin, utilisez les commandes de l'utilitaire de gestion depuis la ligne de commande :

   - Pour consulter la valeur actuelle d'un paramètre, entrez la commande :

     ```
     $ drweb-ctl cfshow Root.VirusBaseDir
     ```

   - Pour définir une nouvelle valeur de paramètre, entrez la commande :

     ```
     # drweb-ctl cfset Root.VirusBaseDir <nouveau chemin>
     ```

   - Pour réinitialiser la valeur d'un paramètre, entrez la commande :

     ```
     # drweb-ctl cfset Root.VirusBaseDir -r
     ```

2. Mettez à jour les bases virales d'une des façons suivantes :

   - Cliquez sur **Mettre à jour** sur la page de gestion des mises à jour de la fenêtre principale de l'application.
   - Sélectionnez l'élément **Mettre à jour** dans le menu contextuel de l'indicateur de l'application dans la zone de notification du bureau.
   - Exécutez la commande suivante :

     ```
     $ drweb-ctl update
     ```

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Version des bases virales non prise en charge*
Code d'erreur	`x41`

Description	Les bases virales existantes correspondent à l'ancienne version du logiciel.

Résoudre l'erreur :

1. Vérifiez si le chemin d'accès au répertoire des bases virales est correct et corrigez-le, si cela est nécessaire (le paramètre `VirusBaseDir` dans la section `[Root]` du fichier de configuration).

   Pour consulter et modifier le chemin, utilisez les commandes de l'utilitaire de gestion depuis la ligne de commande :

   - Pour consulter la valeur actuelle d'un paramètre, entrez la commande :

     ```
     $ drweb-ctl cfshow Root.VirusBaseDir
     ```

   - Pour définir une nouvelle valeur de paramètre, entrez la commande :

     ```
     # drweb-ctl cfset Root.VirusBaseDir <nouveau chemin>
     ```

   - Pour réinitialiser la valeur d'un paramètre, entrez la commande :

     ```
     # drweb-ctl cfset Root.VirusBaseDir -r
     ```

2. Mettez à jour les bases virales d'une des façons suivantes :

   - Cliquez sur **Mettre à jour** sur la page de gestion des mises à jour de la fenêtre principale de l'application.
   - Sélectionnez l'élément **Mettre à jour** dans le menu contextuel de l'indicateur de l'application dans la zone de notification du bureau.
   - Exécutez la commande suivante :

     ```
     $ drweb-ctl update
     ```

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*La base virale est vide*
Code d'erreur	`x42`
Description	Les bases virales sont vides.

Résoudre l'erreur :

1. Vérifiez si le chemin d'accès au répertoire des bases virales est correct et corrigez-le, si cela est nécessaire (le paramètre `VirusBaseDir` dans la section `[Root]` du fichier de configuration).

   Pour consulter et modifier le chemin, utilisez les commandes de l'utilitaire de gestion depuis la ligne de commande :

   - Pour consulter la valeur actuelle d'un paramètre, entrez la commande :

     ```
     $ drweb-ctl cfshow Root.VirusBaseDir
     ```

   - Pour définir une nouvelle valeur de paramètre, entrez la commande :

```
# drweb-ctl cfset Root.VirusBaseDir <nouveau chemin>
```

- Pour réinitialiser la valeur d'un paramètre, entrez la commande :

```
# drweb-ctl cfset Root.VirusBaseDir -r
```

2. Mettez à jour les bases virales d'une des façons suivantes :
   - Cliquez sur **Mettre à jour** sur la page de gestion des mises à jour de la fenêtre principale de l'application.
   - Sélectionnez l'élément **Mettre à jour** dans le menu contextuel de l'indicateur de l'application dans la zone de notification du bureau.
   - Exécutez la commande suivante :

```
$ drweb-ctl update
```

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*L'objet ne peut pas être désinfecté*
Code d'erreur	`x43`
Description	L'action Désinfecter a été appliquée à un objet incurable

Résoudre l'erreur :

1. Sélectionnez une action possible pour cet objet et répétez l'opération.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Combinaison des bases virales non prise en charge*
Code d'erreur	`x44`
Description	L'ensemble de bases virales est incompatible.

Résoudre l'erreur :

1. Vérifiez si le chemin d'accès au répertoire des bases virales est correct et corrigez-le, si cela est nécessaire (le paramètre `VirusBaseDir` dans la section `[Root]` du fichier de configuration).

   Pour consulter et modifier le chemin, utilisez les commandes de l'utilitaire de gestion depuis la ligne de commande :
   - Pour consulter la valeur actuelle d'un paramètre, entrez la commande :

```
$ drweb-ctl cfshow Root.VirusBaseDir
```

   - Pour définir une nouvelle valeur de paramètre, entrez la commande :

```
# drweb-ctl cfset Root.VirusBaseDir <nouveau chemin>
```

- Pour réinitialiser la valeur d'un paramètre, entrez la commande :

```
# drweb-ctl cfset Root.VirusBaseDir -r
```

2. Mettez à jour les bases virales d'une des façons suivantes :
   - Cliquez sur **Mettre à jour** sur la page de gestion des mises à jour de la fenêtre principale de l'application.
   - Sélectionnez l'élément **Mettre à jour** dans le menu contextuel de l'indicateur de l'application dans la zone de notification du bureau.
   - Exécutez la commande suivante :

```
$ drweb-ctl update
```

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*La limite de l'analyse est atteinte*
Code d'erreur	`x45`
Description	Les limitation spécifiées sont dépassées lors du scan de l'objet (par exemple, la limitation de la taille du fichier décompressé, la limitation du niveau d'emboîtement, etc.).

Résoudre l'erreur :

1. Modifiez les limitations de scan des objets (dans les paramètres du composant correspondant) par tout moyen à votre convenance :
   - En utilisant la page de paramètres de ce composant dans la fenêtre de gestion des paramètres de l'application.
   - Avec les commandes `drweb-ctl cfshow` et `drweb-ctl cfset`.
2. Après avoir modifié les paramètres, répétez l'opération.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Identifiants d'utilisateur incorrects*
Code d'erreur	`x47`
Description	Tentative d'authentification avec les identifiants d'utilisateur incorrects.

Résoudre l'erreur :

1. Répétez la tentative d'authentification en indiquant les identifiants corrects de l'utilisateur possédant les privilèges requis.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*L'utilisateur ne possède pas les droits requis*

Code d'erreur	`x48`
Description	L'utilisateur actuel n'a pas les droits d'exécuter l'opération requise.
Résoudre l'erreur : 1. Répétez la tentative d'authentification en indiquant les identifiants corrects de l'utilisateur possédant les privilèges requis.	
Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.	

Message d'erreur	*Jeton d'accès invalide*
Code d'erreur	`x49`
Description	Un composant de Dr.Web pour Linux a présenté un identificateur d'authentification incorrect lors d'une tentative d'accès à l'opération requérant des privilèges élevés.
Résoudre l'erreur : 1. Authentifiez-vous en indiquant les identifiants corrects de l'utilisateur possédant les privilèges requis et répétez l'opération.	
Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.	

Message d'erreur	*Argument invalide*
Code d'erreur	`x60`
Description	La commande ne peut pas être exécutée car vous avez indiqué un argument invalide.
Résoudre l'erreur : 1. Répétez l'action nécessaire en indiquant l'argument valide.	
Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.	

Message d'erreur	*Opération invalide*
Code d'erreur	`x61`
Description	Tentative d'exécuter une commande invalide.
Résoudre l'erreur : 1. Répétez l'action nécessaire en indiquant la commande valide.	
Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.	

Message d'erreur	*Les privilèges de super-utilisateur sont requis*
Code d'erreur	`x62`
Description	Les droits de super-utilisateur sont requis pour l'exécution de l'action nécessaire.

Résoudre l'erreur :

1. Augmentez les privilèges pour passer en mode Super-utilisateur et répétez l'action nécessaire. Pour augmenter les privilèges, vous pouvez utiliser les commandes `su` et `sudo`.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*N'est pas autorisé en mode de protection centralisée*
Code d'erreur	`x63`
Description	L'action nécessaire peut être exécutée uniquement si Dr.Web pour Linux fonctionne en mode standalone.

Résoudre l'erreur :

1. Basculez Dr.Web pour Linux en mode standalone et répétez l'opération.
2. Pour cela :
   - Décochez la case **Activer le mode de protection centralisée** sur la page de paramètres **Mode**.
   - Ou exécutez la commande suivante :

```
# drweb-ctl esdisconnect
```

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*OS non pris en charge*
Code d'erreur	`x64`
Description	Le système d'exploitation installé sur l'hôte n'est pas supporté par Dr.Web pour Linux.

Résoudre l'erreur :

1. Installez un système d'exploitation de la liste spécifiée dans les pré-requis système.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*La fonctionnalité n'est pas implémentée*
Code d'erreur	`x65`

Description	Les fonctions demandées du composant ne sont pas disponibles dans la version actuelle.

Résoudre l'erreur :

1. Réinitialisez les paramètres par défaut de Dr.Web pour Linux en effaçant le contenu du fichier de configuration `/etc/opt/drweb.com/drweb.ini`. Il est recommandé de faire une copie de sauvegarde du fichier avant la procédure. Par exemple :

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

2. Après le nettoyage du fichier de configuration, redémarrez Dr.Web pour Linux en exécutant la commande :

   ```
   # service drweb-configd restart
   ```

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Paramètre inconnu*
Code d'erreur	`x66`
Description	Le fichier de configuration contient les paramètres qui sont inconnus ou non supportés dans la version actuelle de Dr.Web pour Linux.

Résoudre l'erreur :

1. Ouvrez le fichier `/etc/opt/drweb.com/drweb.ini` dans un éditeur de texte et supprimez la ligne contenant le paramètre invalide. Après cela, enregistrez le fichier et redémarrez Dr.Web pour Linux en exécutant la commande :

   ```
   # service drweb-configd restart
   ```

2. Si cela n'a pas aidé, essayez de réinitialiser les paramètres de Dr.Web pour Linux par défaut.

   Pour ce faire, nettoyez le fichier `/etc/opt/drweb.com/drweb.ini` (dans ce cas, il est recommandé de sauvegarder la copie du fichier de configuration), par exemple, en exécutant la commande :

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   Après le nettoyage du fichier de configuration, redémarrez Dr.Web pour Linux en exécutant la commande.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Section inconnue*
Code d'erreur	`x67`

Description	Le fichier de configuration contient les sections qui sont inconnues ou non supportées dans la version actuelle de Dr.Web pour Linux.

Résoudre l'erreur :

1. Ouvrez le fichier `/etc/opt/drweb.com/drweb.ini` dans un éditeur de texte et supprimez la section inconnue. Après cela, enregistrez le fichier et redémarrez Dr.Web pour Linux en exécutant la commande :

   ```
   # service drweb-configd restart
   ```

2. Si cela n'a pas aidé, essayez de réinitialiser les paramètres de Dr.Web pour Linux par défaut.

   Pour ce faire, nettoyez le fichier `/etc/opt/drweb.com/drweb.ini` (dans ce cas, il est recommandé de sauvegarder la copie du fichier de configuration), par exemple, en exécutant la commande :

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   Après le nettoyage du fichier de configuration, redémarrez Dr.Web pour Linux en exécutant la commande.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Valeur de paramètre invalide*
Code d'erreur	`x68`
Description	Les valeurs invalides sont spécifiées pour un ou plusieurs paramètres dans le fichier de configuration.

Résoudre l'erreur :

1. Modifiez la valeur du paramètre par tout moyen à votre convenance :
   - En utilisant la page de paramètres de ce composant dans la fenêtre de gestion des paramètres de l'application.
   - Avec les commandes `drweb-ctl cfshow` et `drweb-ctl cfset`.

   Si vous ne savez pas quelle valeur du paramètre est valide, consultez l'aide sur le composant utilisant ce paramètre ou essayez de réinitialiser ce paramètre par défaut.
2. De plus, vous pouvez éditer directement le fichier de configuration `/etc/opt/drweb.com/drweb.ini`. Pour ce faire, ouvrez-le dans un éditeur de texte, trouvez la ligne contenant la valeur invalide du paramètre, spécifiez la valeur valide et redémarrez Dr.Web pour Linux en exécutant la commande suivante :

   ```
   # service drweb-configd restart
   ```

3. Si les étapes précédentes n'ont pas résolu le problème, essayez de réinitialiser les paramètres de Dr.Web pour Linux par défaut.

Pour ce faire, nettoyez le fichier `/etc/opt/drweb.com/drweb.ini` (dans ce cas, il est recommandé de sauvegarder la copie du fichier de configuration), par exemple, en exécutant la commande :

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

Après le nettoyage du fichier de configuration, redémarrez Dr.Web pour Linux en exécutant la commande.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Statut invalide*
Code d'erreur	`x69`
Description	Un composant ou Dr.Web pour Linux entier sont en état non valide pour l'exécution de l'opération demandée.

Résoudre l'erreur :

1. Recommencez l'action nécessaire plus tard.
2. Redémarrez Dr.Web pour Linux, en exécutant la commande suivante :

```
# service drweb-configd restart
```

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Une seule valeur est autorisée*
Code d'erreur	`x70`
Description	Une valeur sous forme d'un liste est spécifiée pour le paramètre qui ne peut avoir qu'une seule valeur dans le fichier de configuration.

Résoudre l'erreur :

1. Modifiez la valeur du paramètre par tout moyen à votre convenance :
   - En utilisant la page de paramètres de ce composant dans la fenêtre de gestion des paramètres de l'application.
   - Avec les commandes `drweb-ctl cfshow` et `drweb-ctl cfset`.

   Si vous ne savez pas quelle valeur du paramètre est valide, consultez l'aide sur le composant utilisant ce paramètre ou essayez de réinitialiser ce paramètre par défaut.
2. De plus, vous pouvez éditer directement le fichier de configuration `/etc/opt/drweb.com/drweb.ini`. Pour ce faire, ouvrez-le dans un éditeur de texte, trouvez la ligne contenant la valeur invalide du paramètre, spécifiez la valeur valide et redémarrez Dr.Web pour Linux en exécutant la commande suivante :

```
# service drweb-configd restart
```

3. Si les étapes précédentes n'ont pas résolu le problème, essayez de réinitialiser les paramètres de Dr.Web pour Linux par défaut.

   Pour ce faire, nettoyez le fichier `/etc/opt/drweb.com/drweb.ini` (dans ce cas, il est recommandé de sauvegarder la copie du fichier de configuration), par exemple, en exécutant la commande :

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   Après le nettoyage du fichier de configuration, redémarrez Dr.Web pour Linux en exécutant la commande.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Entrée introuvable*
Code d'erreur	`x80`
Description	Aucune information sur la menace détectée (il est probable que la menace a été déjà traitée par un autre composant).

Résoudre l'erreur :

1. Actualisez la liste de menaces plus tard.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*L'enregistrement est traité en ce moment*
Code d'erreur	`x81`
Description	La menace est déjà traitée par un autre composant.

Résoudre l'erreur :

1. Actualisez la liste de menaces plus tard.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Le fichier est déjà mis en quarantaine*
Code d'erreur	`x82`
Description	Le fichier est déjà mis en quarantaine. Il est probable que la menace a été déjà traitée par un autre composant.

Résoudre l'erreur :

1. Actualisez la liste de menaces plus tard.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Impossible d'enregistrer la copie de sauvegarde avant la mise à jour*
Code d'erreur	`x89`
Description	Impossible d'enregistrer la copie de sauvegarde des fichiers à mettre à jour avant le téléchargement des mises à jour depuis le serveur de mises à jour,

Résoudre l'erreur :

1. Vérifiez la justesse du chemin d'accès au répertoire où sont stockées les copies de sauvegarde des fichiers exécutables et corrigez-le, si cela est nécessaire (le paramètre `BackupDir` dans la section `[Update]` du fichier de configuration).

   Pour consulter et modifier le chemin, vous pouvez utiliser les commandes de l'utilitaire de gestion depuis la ligne de commande.

   - Pour consulter la valeur actuelle d'un paramètre, entrez la commande :

     ```
     $ drweb-ctl cfshow Update.BackupDir
     ```

   - Pour définir une nouvelle valeur de paramètre, entrez la commande :

     ```
     # drweb-ctl cfset Update.BackupDir <nouveau chemin>
     ```

   - Pour réinitialiser la valeur d'un paramètre, entrez la commande :

     ```
     # drweb-ctl cfset Update.BackupDir -r
     ```

2. Mettez à jour les bases virales d'une des façons suivantes :
   - Cliquez sur **Mettre à jour** sur la page de gestion des mises à jour de la fenêtre principale de l'application.
   - Sélectionnez l'élément **Mettre à jour** dans le menu contextuel de l'indicateur de l'application dans la zone de notification du bureau.
   - Exécutez la commande suivante :

     ```
     $ drweb-ctl update
     ```

3. Si l'erreur persiste, assurez-vous que l'utilisateur qui lance le Module de mise à jour possède les droits d'écrire dans le répertoire spécifié dans le paramètre `BackupDir`. Le nom d'utilisateur est indiqué dans le paramètre `RunAsUser`. Si cela est nécessaire, vous pouvez modifier le nom d'utilisateur en modifiant la valeur du paramètre `RunAsUser` ou accorder les droits manquants dans les propriétés du répertoire.
4. Si l'erreur persiste, essayez de réinstaller le package `drweb-update`.

   Pour en savoir plus sur l'installation et la suppression du produit ou de ses composants, consultez les rubriques Installation de Dr.Web pour Linux et Suppression de Dr.Web pour Linux.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Fichier DRL invalide*

Code d'erreur	`x90`
Description	La structure d'un fichier de listes de serveurs de mises à jour est endommagée.

Résoudre l'erreur :

1. Vérifiez si le chemin d'accès au fichier de la liste de serveurs est correct et corrigez-le, si cela est nécessaire (les paramètres avec le nom de type `*DrlDir` dans la section `[Update]` du fichier de configuration). Pour ce faire, utilisez les commandes de l'utilitaire de gestion depuis la ligne de commande.
   - Pour consulter la valeur actuelle d'un paramètre, entrez la commande (il faut remplacer <*DrlDir> par le nom du paramètre. Si le nom du paramètre est inconnu, regardez la valeur de tous les paramètres dans la section en omettant la partie de la commande placée entre crochets) :

     ```
     $ drweb-ctl cfshow Update[.<*DrlDir>]
     ```

   - Pour définir une nouvelle valeur de paramètre, entrez la commande (il faut remplacer <*DrlDir> par le nom du paramètre) :

     ```
     # drweb-ctl cfset Update.<*DrlDir> <nouveau chemin>
     ```

   - Pour réinitialiser la valeur d'un paramètre, entrez la commande (il faut remplacer <*DrlDir> par le nom du paramètre) :

     ```
     # drweb-ctl cfset Update.<*DrlDir> -r
     ```

2. Mettez à jour les bases virales d'une des façons suivantes :
   - Cliquez sur **Mettre à jour** sur la page de gestion des mises à jour de la fenêtre principale de l'application.
   - Sélectionnez l'élément **Mettre à jour** dans le menu contextuel de l'indicateur de l'application dans la zone de notification du bureau.
   - Exécutez la commande suivante :

     ```
     $ drweb-ctl update
     ```

3. Si l'erreur persiste, installez ou réinstallez les paquets `drweb-bases` et `drweb-dws`, puis lancez une mise à jour.
4. Si l'erreur persiste, supprimez Dr.Web pour Linux, puis réinstallez-le.

   Pour en savoir plus sur l'installation et la suppression du produit ou de ses composants, consultez les rubriques Installation de Dr.Web pour Linux et Suppression de Dr.Web pour Linux.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Fichier LST invalide*
Code d'erreur	`x91`
Description	La structure d'un fichier contenant la liste des bases virales mises à jour est endommagée.

Résoudre l'erreur :

1. Mettez à jour les bases virales d'une des façons suivantes :
   - Cliquez sur **Mettre à jour** sur la page de gestion des mises à jour de la fenêtre principale de l'application.
   - Sélectionnez l'élément **Mettre à jour** dans le menu contextuel de l'indicateur de l'application dans la zone de notification du bureau.
   - Exécutez la commande suivante :

     ```
     $ drweb-ctl update
     ```
2. Si l'erreur persiste, essayez de réinstaller le package `drweb-update`.
3. Si l'erreur persiste, supprimez Dr.Web pour Linux, puis réinstallez-le.

   Pour en savoir plus sur l'installation et la suppression du produit ou de ses composants, consultez les rubriques Installation de Dr.Web pour Linux et Suppression de Dr.Web pour Linux.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Fichier compressé invalide*
Code d'erreur	`x92`
Description	La structure du fichier téléchargé contenant des mises à jour est rompue.

Résoudre l'erreur :

1. Mettez à jour les bases virales d'une des façons suivantes :
   - Cliquez sur **Mettre à jour** sur la page de gestion des mises à jour de la fenêtre principale de l'application.
   - Sélectionnez l'élément **Mettre à jour** dans le menu contextuel de l'indicateur de l'application dans la zone de notification du bureau.
   - Exécutez la commande suivante :

     ```
     $ drweb-ctl update
     ```

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Erreur d'authentification sur le proxy*
Code d'erreur	`x93`
Description	Impossible de se connecter au serveur de mises à jour via le serveur proxy spécifié dans les paramètres.

Résoudre l'erreur :

1. Vérifiez la justesse des paramètres de connexion au serveur proxy (spécifiés dans le paramètre avec le nom `Proxy` dans la section `[Update]` du fichier de configuration). Si nécessaire, changez de serveur proxy utilisé ou refusez l'utilisation du serveur proxy.

Pour consulter et spécifier les paramètres de connexion, ouvrez la page des paramètres généraux.

Vous pouvez également utiliser les commandes de l'utilitaire de gestion depuis la ligne de commande.

- Pour consulter la valeur actuelle d'un paramètre, entrez la commande :

```
$ drweb-ctl cfshow Update.Proxy
```

- Pour définir une nouvelle valeur de paramètre, entrez la commande :

```
# drweb-ctl cfset Update.Proxy <nouveaux paramètres>
```

- Pour réinitialiser la valeur d'un paramètre, entrez la commande :

```
# drweb-ctl cfset Update.Proxy -r
```

2. Mettez à jour les bases virales d'une des façons suivantes :
   - Cliquez sur **Mettre à jour** sur la page de gestion des mises à jour de la fenêtre principale de l'application.
   - Sélectionnez l'élément **Mettre à jour** dans le menu contextuel de l'indicateur de l'application dans la zone de notification du bureau.
   - Exécutez la commande suivante :

```
$ drweb-ctl update
```

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Aucun serveur de mise à jour disponible*
Code d'erreur	`x94`
Description	Impossible de se connecter à aucun serveur de mises à jour.

Résoudre l'erreur :

1. Vérifiez la disponibilité du réseau et corrigez les paramètres réseau, si cela est nécessaire.
2. Si l'accès au réseau est possible uniquement via le serveur proxy, spécifiez les paramètres de connexion au serveur proxy (déterminés dans le paramètre avec le nom `Proxy` dans la section `[Update]` du fichier de configuration). Si nécessaire, changez de serveur proxy utilisé ou refusez l'utilisation du serveur proxy.

   Pour consulter et spécifier les paramètres de connexion, ouvrez la page des paramètres généraux.

   Vous pouvez également utiliser les commandes de l'utilitaire de gestion depuis la ligne de commande.

   - Pour consulter la valeur actuelle d'un paramètre, entrez la commande :

```
$ drweb-ctl cfshow Update.Proxy
```

   - Pour définir une nouvelle valeur de paramètre, entrez la commande :

```
# drweb-ctl cfset Update.Proxy <nouveaux paramètres>
```

- Pour réinitialiser la valeur d'un paramètre, entrez la commande :

```
# drweb-ctl cfset Update.Proxy -r
```

3. Si les paramètres de la connexion réseau (y compris la connexion utilisée par le serveur proxy) sont corrects, mais l'erreur persiste, assurez-vous que vous utilisez la liste disponible des serveurs de mise à jour. La liste des serveurs utilisés est indiquée dans les paramètres de type `*DrlDir` dans la section `[Update]` du fichier de configuration. Notez que si les paramètres de type `*CustomDrlDir` indiquent le fichier correct de la liste de serveurs, les serveur qui y sont indiqués seront utilisés à la place des serveurs de la zone de mise à jour standard (la valeur spécifiée dans le paramètre correspondant `*DrlDir` est ignorée).

   Pour consulter et modifier les paramètres de connexion, vous pouvez utiliser les commandes de l'utilitaire de gestion depuis la ligne de commande.

   Pour consulter la valeur actuelle d'un paramètre, entrez la commande (il faut remplacer *<*DrlDir>* par le nom du paramètre. Si le nom du paramètre est inconnu, regardez la valeur de tous les paramètres dans la section en omettant la partie de la commande placée entre crochets) :

```
$ drweb-ctl cfshow Update[.<*DrlDir>]
```

   Pour définir une nouvelle valeur de paramètre, entrez la commande (il faut remplacer *<*DrlDir>* par le nom du paramètre) :

```
# drweb-ctl cfset Update.<*DrlDir> <nouveau chemin>
```

   Pour réinitialiser la valeur d'un paramètre, entrez la commande (il faut remplacer *<*DrlDir>* par le nom du paramètre) :

```
# drweb-ctl cfset Update.<*DrlDir> -r
```

4. Mettez à jour les bases virales d'une des façons suivantes :
   - Cliquez sur **Mettre à jour** sur la page de gestion des mises à jour de la fenêtre principale de l'application.
   - Sélectionnez l'élément **Mettre à jour** dans le menu contextuel de l'indicateur de l'application dans la zone de notification du bureau.
   - Exécutez la commande suivante :

```
$ drweb-ctl update
```

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Format de fichier clé invalide*
Code d'erreur	x95
Description	Format de fichier clé corrompu.

Résoudre l'erreur :

1. Vérifiez la présence du fichier clé et la justesse du chemin vers ce fichier. Le chemin d'accès au fichier clé est spécifié dans le paramètre `KeyPath` de la section `[Root]` du fichier de configuration.

   Pour consulter les paramètres de la licence et spécifier le chemin d'accès au fichier clé, passez à la page du Gestionnaire de licences de la fenêtre principale de l'application.

   Vous pouvez également utiliser les commandes de l'utilitaire de gestion depuis la ligne de commande.

   - Pour consulter la valeur actuelle d'un paramètre, entrez la commande :

     ```
     $ drweb-ctl cfshow Root.KeyPath
     ```

   - Pour définir une nouvelle valeur de paramètre, entrez la commande :

     ```
     # drweb-ctl cfset Root.KeyPath <chemin d'accès au fichier>
     ```

   - Pour réinitialiser la valeur d'un paramètre, entrez la commande :

     ```
     # drweb-ctl cfset Root.KeyPath -r
     ```

2. Si vous n'avez pas de fichier clé ou que le fichier clé utilisé est endommagé, achetez et installez-le. Dans la rubrique Octroi de la licence, vous pouvez consulter la description du fichier clé, les moyens de l'acheter et d'installer.
3. Pour installer le fichier clé disponible, vous pouvez utiliser le Gestionnaire de licences.
4. Vous pouvez également consulter les paramètres de la licence actuelle dans l'espace personnel **Mon Dr.Web** sur https://support.drweb.com/get+cabinet+link/.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*La licence a expiré*
Code d'erreur	`x96`
Description	La licence a expiré.

Résoudre l'erreur :

1. Achetez une nouvelle licence et installez le fichier clé obtenu. Dans la rubrique Octroi de la licence, vous pouvez consulter les moyens d'acheter une licence et d'installer le fichier clé.
2. Pour installer le fichier clé acheté, vous pouvez utiliser le Gestionnaire de licences.
3. Vous pouvez également consulter les paramètres de la licence actuelle dans l'espace personnel **Mon Dr.Web** sur https://support.drweb.com/get+cabinet+link/.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Le délai de l'opération réseau a expiré*
Code d'erreur	`x97`

Description	Le délai d'attente de la connexion réseau a expiré (il est probable que l'hôte distant a cessé de répondre ou qu'il est impossible d'établir la connexion nécessaire).

Résoudre l'erreur :

1. Vérifiez la disponibilité du réseau et la justesse des paramètres réseau. Corrigez les paramètres réseau, si cela est nécessaire, et répétez l'opération.
2. Si l'erreur survient lors de la réception de mises à jour, vérifiez les paramètres d'utilisation du Serveur proxy. Et, si cela est nécessaire, changez de serveur proxy utilisé ou refusez son utilisation.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Somme de contrôle incorrecte*
Code d'erreur	`x98`
Description	La somme de contrôle du fichier téléchargé contenant des mises à jour est endommagée.

Résoudre l'erreur :

1. Réessayez la mise à jour plus tard d'une des façons suivantes :
   - Cliquez sur **Mettre à jour** sur la page de gestion des mises à jour de la fenêtre principale de l'application.
   - Sélectionnez l'élément **Mettre à jour** dans le menu contextuel de l'indicateur de l'application dans la zone de notification du bureau.
   - Exécutez la commande suivante :

     ```
     $ drweb-ctl update
     ```

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Fichier clé de démo invalide*
Code d'erreur	`x99`
Description	Le fichier clé de démo est invalide (par exemple, il a été obtenu pour un autre ordinateur).

Résoudre l'erreur :

1. Demandez une nouvelle période de démo pour cet ordinateur ou achetez une nouvelle licence et installez le fichier clé obtenu. Dans la rubrique Octroi de la licence, vous pouvez consulter les moyens d'acheter une licence et d'installer le fichier clé.
2. Pour installer le fichier clé acheté, vous pouvez utiliser le Gestionnaire de licences.
3. Vous pouvez également consulter les paramètres de la licence actuelle dans l'espace personnel **Mon Dr.Web** sur https://support.drweb.com/get+cabinet+link/.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Le fichier clé de licence est bloqué*
Code d'erreur	`x100`
Description	La licence actuelle est bloquée (il est probable que les termes du Contrat de licence d'utilisation de Dr.Web pour Linux ont été violés).

Résoudre l'erreur :

1. Achetez une nouvelle licence et installez le fichier clé obtenu. Dans la rubrique Octroi de la licence, vous pouvez consulter les moyens d'acheter une licence et d'installer le fichier clé.
2. Pour installer le fichier clé acheté, vous pouvez utiliser le Gestionnaire de licences.
3. Vous pouvez également consulter les paramètres de la licence actuelle dans l'espace personnel **Mon Dr.Web** sur https://support.drweb.com/get+cabinet+link/.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Licence invalide*
Code d'erreur	`x101`
Description	La licence que vous utilisez est destinée à un autre produit ou elle ne contient pas les autorisations nécessaires pour le fonctionnement des composants de Dr.Web pour Linux .

Résoudre l'erreur :

1. Achetez une nouvelle licence et installez le fichier clé obtenu. Dans la rubrique Octroi de la licence, vous pouvez consulter les moyens d'acheter une licence et d'installer le fichier clé.
2. Pour installer le fichier clé acheté, vous pouvez utiliser le Gestionnaire de licences.
3. Vous pouvez également consulter les paramètres de la licence actuelle dans l'espace personnel **Mon Dr.Web** sur https://support.drweb.com/get+cabinet+link/.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Configuration incorrecte*
Code d'erreur	`x102`
Description	Le composants de Dr.Web pour Linux ne peut pas fonctionner à cause des paramètres de configuration incorrects.

Résoudre l'erreur :

1. Si le nom de composant provoquant l'erreur est inconnu, essayez de le définir en consultant le contenu du journal.

2. Si l'erreur est provoquée par le composant SpIDer Guard, il est probable que le mode de fonctionnement non supporté par le système d'exploitation est spécifié. Vérifiez le mode de fonctionnement de composant spécifié et corrigez-le, si cela est nécessaire en indiquant la valeur `AUTO` (le paramètre `Mode` dans la section `[LinuxSpider]` du fichier de configuration).

   Pour consulter et modifier le mode de fonctionnement, vous pouvez utiliser les commandes de l'utilitaire de gestion depuis la ligne de commande.

   - Pour définir la valeur `AUTO`, entrez la commande

   ```
   # drweb-ctl cfset LinuxSpider.Mode AUTO
   ```

   - Pour réinitialiser la valeur d'un paramètre, entrez la commande

   ```
   # drweb-ctl cfset LinuxSpider.Mode -r
   ```

   Si l'erreur persiste, créez et installez manuellement le module noyau pour le composant SpIDer Guard.

   

   Notez que le fonctionnement de SpIDer Guard et du module noyau chargeable est garanti uniquement si le système d'exploitation que vous utilisez fait partie de la liste des distributions prises en charge UNIX (voir Pré-requis système et compatibilité).

3. Si l'erreur est provoquée par le composant SpIDer Gate, cela veut dire qu'il y a sans doute un problème de compatibilité avec un autre pare-feu. Par exemple, on sait que SpIDer Gate rentre en conflit avec le pare-feu FirewallD dans l'OS Fedora, CentOS, Red Hat Enterprise Linux (à chaque redémarrage, FirewallD perturbe les règles de routage de trafic spécifiées par SpIDer Gate). Pour résoudre le problème, redémarrez Dr.Web pour Linux en exécutant la commande

   ```
   # service drweb-configd restart
   ```

   ou

   ```
   # drweb-ctl reload
   ```

   

   Notez que si vous ne bloquez pas le fonctionnement de FirewallD, cette erreur de SpIDer Gate peut survenir à chaque redémarrage de FirewallD, y compris les redémarrages de l'OS. Vous pouvez résoudre cette erreur en désactivant FirewallD (consultez le guide de FirewallD dans le manuel de votre OS).

4. Si l'erreur est provoquée par un autre composant, essayez de réinitialiser les paramètres du composant par défaut par tout moyen à votre convenance :
   - Avec les commandes `drweb-ctl cfshow` et `drweb-ctl cfset`.
   - En éditant le fichier de configuration manuellement, en supprimant tous les paramètres de la section du composant.
5. Si les étapes précédentes n'ont pas résolu le problème, essayez de réinitialiser les paramètres de Dr.Web pour Linux par défaut.

   Pour ce faire, nettoyez le fichier `/etc/opt/drweb.com/drweb.ini` (dans ce cas, il est recommandé de sauvegarder la copie du fichier de configuration), par exemple, en exécutant la commande :

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

Après le nettoyage du fichier de configuration, redémarrez Dr.Web pour Linux en exécutant la commande

```
# service drweb-configd restart
```

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Fichier exécutable invalide*
Code d'erreur	x104
Description	Impossible de lancer le composant. Le fichier exécutable est endommagé ou le chemin d'accès au fichier est incorrect.

Résoudre l'erreur :

1. Si le nom de composant provoquant l'erreur est inconnu, essayez de le définir en consultant le contenu du journal.
2. Vérifiez la valeur du chemin vers le fichier exécutable du composant dans la configuration de Dr.Web pour Linux (le paramètre `ExePath` dans la section du composant) en exécutant la commande (remplacez *<section du composant>* par le nom de la section correspondante du fichier de configuration)

   ```
   $ drweb-ctl cfshow <section du composant>.ExePath
   ```

3. Essayez de réinitialiser le chemin par défaut en exécutant la commande (remplacez *<section du composant>* par le nom de la section correspondante du fichier de configuration)

   ```
   # drweb-ctl cfset <section du composant>.ExePath -r
   ```

4. Si les étapes précédentes n'ont pas résolu le problème, essayez de réinstaller le paquet du composant correspondant.
   - `drweb-filecheck` si le fichier exécutable du composant Scanner est endommagé.
   - `drweb-spider`, si le fichier exécutable de SpIDer Guard est endommagé.
   - `drweb-gated`, si le fichier exécutable de SpIDer Gate est endommagé.
   - `drweb-update`, si le fichier exécutable de l'Updater est endommagé.
5. Si l'erreur persiste, ou que vous ne pouvez pas déterminer quel fichier exécutable de quel composant est endommagé, supprimez Dr.Web pour Linux et réinstallez-le.

   Pour en savoir plus sur l'installation et la suppression du produit ou de ses composants, consultez les rubriques Installation de Dr.Web pour Linux et Suppression de Dr.Web pour Linux.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Le moteur Virus-Finding Engine n'est pas disponible*

Code d'erreur	`x105`
Description	Le fichier du moteur antivirus Dr.Web Virus-Finding Engine est manquant ou indisponible.

Résoudre l'erreur :

1. Vérifiez si le chemin d'accès au moteur antivirus `drweb32.dll` est correct et corrigez-le, si cela est nécessaire (le paramètre `CoreEnginePath` dans la section `[Root]` du fichier de configuration).

   Pour consulter et modifier le chemin, vous pouvez utiliser les commandes de l'utilitaire de gestion depuis la ligne de commande.

   - Pour consulter la valeur actuelle d'un paramètre, entrez la commande

   ```
   $ drweb-ctl cfshow Root.CoreEnginePath
   ```

   - Pour définir une nouvelle valeur de paramètre, entrez la commande

   ```
   # drweb-ctl cfset Root.CoreEnginePath <nouveau chemin>
   ```

   - Pour réinitialiser la valeur d'un paramètre, entrez la commande

   ```
   # drweb-ctl cfset Root.CoreEnginePath -r
   ```

2. Mettez à jour les bases virales d'une des façons suivantes :
   - Cliquez sur **Mettre à jour** sur la page de gestion des mises à jour de la fenêtre principale de l'application.
   - Sélectionnez l'élément **Mettre à jour** dans le menu contextuel de l'indicateur de l'application dans la zone de notification du bureau.
   - Exécutez la commande suivante :

   ```
   $ drweb-ctl update
   ```

3. Si le chemin est correct et que l'erreur persiste après la mise à jour des bases virales, réinstallez le paquet `drweb-bases`.
4. Si l'erreur persiste, supprimez Dr.Web pour Linux, puis réinstallez-le.

   Pour en savoir plus sur l'installation et la suppression du produit ou de ses composants, consultez les rubriques Installation de Dr.Web pour Linux et Suppression de Dr.Web pour Linux.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Les bases virales n'existent pas*
Code d'erreur	`x106`
Description	Les bases virales sont introuvables.

Résoudre l'erreur :

1. Vérifiez si le chemin d'accès au répertoire des bases virales est correct et corrigez-le, si cela est nécessaire (le paramètre `VirusBaseDir` dans la section `[Root]` du fichier de configuration).

Pour consulter et modifier le chemin, vous pouvez utiliser les commandes de l'utilitaire de gestion depuis la ligne de commande.

- Pour consulter la valeur actuelle d'un paramètre, entrez la commande

```
$ drweb-ctl cfshow Root.VirusBaseDir
```

- Pour définir une nouvelle valeur de paramètre, entrez la commande

```
# drweb-ctl cfset Root.VirusBaseDir <nouveau chemin>
```

- Pour réinitialiser la valeur d'un paramètre, entrez la commande

```
# drweb-ctl cfset Root.VirusBaseDir -r
```

2. Mettez à jour les bases virales d'une des façons suivantes :
   - Cliquez sur **Mettre à jour** sur la page de gestion des mises à jour de la fenêtre principale de l'application.
   - Sélectionnez l'élément **Mettre à jour** dans le menu contextuel de l'indicateur de l'application dans la zone de notification du bureau.
   - Exécutez la commande suivante :

```
$ drweb-ctl update
```

3. Si l'erreur persiste, installez le paquet `drweb-bases` contenant les bases virales et le fichier exécutable du moteur antivirus.
4. Si l'erreur persiste, supprimez Dr.Web pour Linux, puis réinstallez-le.

   Pour en savoir plus sur l'installation et la suppression du produit ou de ses composants, consultez les rubriques Installation de Dr.Web pour Linux et Suppression de Dr.Web pour Linux.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Le processus est terminé à réception d'un signal*
Code d'erreur	`x107`
Description	Le composant s'est arrêté (peut-être, à cause de l'inactivité ou suite à une commande de l'utilisateur).

Résoudre l'erreur :

1. Sinon l'arrêt du fonctionnement n'est pas une erreur.Si l'opération exécutée a échoué, redémarrez-la.
2. Si le composant s'arrête tout le temps, essayez de réinitialiser les paramètres du composant par défaut par tout moyen à votre convenance :
   - Avec les commandes `drweb-ctl cfshow` et `drweb-ctl cfset`.
   - En éditant le fichier de configuration manuellement (en supprimant tous les paramètres de la section du composant).
3. Si cela n'a pas aidé, essayez de réinitialiser les paramètres de Dr.Web pour Linux par défaut.

Pour ce faire, nettoyez le fichier `/etc/opt/drweb.com/drweb.ini` (dans ce cas, il est recommandé de sauvegarder la copie du fichier de configuration), par exemple, en exécutant la commande :

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

Après le nettoyage du fichier de configuration, redémarrez Dr.Web pour Linux en exécutant la commande :

```
# service drweb-configd restart
```

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Fin de processus inattendue*
Code d'erreur	x108
Description	Le composant s'est arrêté brusquement suite à une panne.

Résoudre l'erreur :

1. Essayez de refaire l'opération.
2. Si le composant tombe en panne tout le temps, essayez de réinitialiser les paramètres du composant par défaut par tout moyen à votre convenance :
   - Avec les commandes `drweb-ctl cfshow` et `drweb-ctl cfset`.
   - En éditant le fichier de configuration manuellement (en supprimant tous les paramètres de la section du composant).
3. Si cela n'a pas aidé, essayez de réinitialiser les paramètres de Dr.Web pour Linux par défaut.

   Pour ce faire, nettoyez le fichier `/etc/opt/drweb.com/drweb.ini` (dans ce cas, il est recommandé de sauvegarder la copie du fichier de configuration), par exemple, en exécutant la commande :

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   Après le nettoyage du fichier de configuration, redémarrez Dr.Web pour Linux en exécutant la commande :

   ```
   # service drweb-configd restart
   ```
4. Si l'erreur persiste après la réinitialisation des paramètres de Dr.Web pour Linux, essayez de réinstaller le paquet du composant.
5. Si l'erreur persiste, supprimez Dr.Web pour Linux, puis réinstallez-le.

   Pour en savoir plus sur l'installation et la suppression du produit ou de ses composants, consultez les rubriques Installation de Dr.Web pour Linux et Suppression de Dr.Web pour Linux.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Logiciel incompatible détecté*
Code d'erreur	`x109`
Description	Le composant de Dr.Web pour Linux ne peut pas fonctionner car un logiciel incompatible a été détecté.

Résoudre l'erreur :

1. Si l'erreur est provoquée par le composant SpIDer Gate, il est probable que dans le système il y a un logiciel qui génère pour le pare-feu système NetFilter des règles empêchant le fonctionnement correct de SpIDer Gate. Par exemple, cela peut être Shorewall ou SuseFirewall2 (dans l'OS SUSE Linux). La cause principale du conflit de SpIDer Gate avec d'autres applications configurant le pare-feu système NetFilter consiste en ce que ces applications vérifient de temps en temps l'intégrité du système de règles qu'elles ont spécifié et elles le réécrivent.

   Configurez le logiciel provoquant un conflit de telle façon qu'il n'empêche pas le fonctionnement de SpIDer Gate. Si vous n'arrivez pas à configurer le logiciel en conflit de telle façon qu'il n'empêche pas le fonctionnement de SpIDer Gate, désactivez ce logiciel et interdisez son lancement au démarrage de l'OS. Vous pouvez essayer de configurer l'application SuseFirewall2 (dans l'OS SUSE Linux) de la manière suivante :

   1) Ouvrez le fichier de configuration de SuseFirewall2 (par défaut, c'est le fichier `/etc/sysconfig/SuSEfirewall2`).
   2) Trouvez dans le fichier le bloc de texte suivant :

```
# Type: yesno
#
# Install NOTRACK target for interface lo in the raw table. Doing so
# speeds up packet processing on the loopback interface. This breaks
# certain firewall setups that need to e.g. redirect outgoing
# packets via custom rules on the local machine.
#
# Defaults to "yes" if not set
#
FW_LO_NOTRACK=""
```

   3) Spécifiez la valeur `no` pour le paramètre :

```
FW_LO_NOTRACK="no"
```

   4) Redémarrez SuseFirewall2, en exécutant la commande suivante :

```
# rcSuSEfirewall2 restart
```

   > ⚠ Notez que si le paramètre `FW_LO_NOTRACK n'est pas présent dans les paramètres de SuseFirewall2`, il est nécessaire de désactiver l'application et interdire son lancement au démarrage de l'OS pour résoudre le conflit (par exemple, il faut le faire dans l'OS SUSE Linux Enterprise Server 11).

   5) Après avoir modifié les paramètres ou désactivé l'application en conflit, redémarrez SpIDer Gate (désactivez-le, puis activez-le sur la page correspondante).

2. Si l'erreur est provoquée par un autre composant, désactivez ou reconfigurez le logiciel en conflit afin de prévenir une perturbation du fonctionnement de Dr.Web pour Linux.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Bibliothèque incompatible*
Code d'erreur	`x110`
Description	Le fichier de la bibliothèque antispam (requise pour l'analyse d'e-mail) est manquant, indisponible ou endommagé.

Résoudre l'erreur :

1. Vérifiez si le chemin d'accès au fichier de la bibliothèque est correct et corrigez-le, si cela est nécessaire (le paramètre `AntispamCorePath` dans la section `[Root]` du fichier de configuration).

   Pour consulter et modifier le chemin, vous pouvez utiliser les commandes de l'utilitaire de gestion depuis la ligne de commande.

   - Pour consulter la valeur actuelle d'un paramètre, entrez la commande

   ```
   $ drweb-ctl cfshow Root.AntispamCorePath
   ```

   - Pour définir une nouvelle valeur de paramètre, entrez la commande

   ```
   # drweb-ctl cfset Root.AntispamCorePath <nouveau chemin>
   ```

   - Pour réinitialiser la valeur d'un paramètre, entrez la commande

   ```
   # drweb-ctl cfset Root.AntispamCorePath -r
   ```

2. Mettez à jour les bases virales d'une des façons suivantes :
   - Cliquez sur **Mettre à jour** sur la page de gestion des mises à jour de la fenêtre principale de l'application.
   - Sélectionnez l'élément **Mettre à jour** dans le menu contextuel de l'indicateur de l'application dans la zone de notification du bureau.
   - Exécutez la commande suivante :

   ```
   $ drweb-ctl update
   ```

3. Si le chemin est correct et que l'erreur persiste après la mise à jour des bases virales, réinstallez le paquet `drweb-maild`.
4. Si l'erreur persiste, supprimez Dr.Web pour Linux, puis réinstallez-le.

   Pour en savoir plus sur l'installation et la suppression du produit ou de ses composants, consultez les rubriques Installation de Dr.Web pour Linux et Suppression de Dr.Web pour Linux.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Les bases des catégories de ressources web sont introuvables*

Code d'erreur	`x112`
Description	Les bases des catégories de ressources web sont introuvables.

Résoudre l'erreur :

1. Vérifiez si le chemin d'accès au répertoire de la base de données des catégories de ressources web est correcte et corrigez-le, si cela est nécessaire (le paramètre `DwsDir` dans la section `[Root]` du fichier de configuration).
   - Pour consulter et modifier le chemin, vous pouvez utiliser les commandes de l'utilitaire de gestion depuis la ligne de commande.

   Pour consulter la valeur actuelle d'un paramètre, entrez la commande

   ```
   $ drweb-ctl cfshow Root.DwsDir
   ```

   Pour définir une nouvelle valeur de paramètre, entrez la commande

   ```
   # drweb-ctl cfset Root.DwsDir <nouveau chemin>
   ```

   Pour réinitialiser la valeur d'un paramètre, entrez la commande

   ```
   # drweb-ctl cfset Root.DwsDir -r
   ```
2. Mettez à jour les bases virales d'une des façons suivantes :
   - Cliquez sur **Mettre à jour** sur la page de gestion des mises à jour de la fenêtre principale de l'application.
   - Sélectionnez l'élément **Mettre à jour** dans le menu contextuel de l'indicateur de l'application dans la zone de notification du bureau.
   - Exécutez la commande suivante :

   ```
   $ drweb-ctl update
   ```
3. Si l'erreur persiste, installez le composant séparément ou réinstallez le paquet `drweb-dws` contenant les bases des catégories de ressources web.
4. Si l'erreur persiste, supprimez Dr.Web pour Linux, puis réinstallez-le.

   Pour en savoir plus sur l'installation et la suppression du produit ou de ses composants, consultez les rubriques Installation de Dr.Web pour Linux et Suppression de Dr.Web pour Linux.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Le module noyau Linux pour SplDer Guard n'est pas disponible*
Code d'erreur	`x113`
Description	Le module noyau manquant Linux est requis pour le fonctionnement de SplDer Guard.

Résoudre l'erreur :

1. Vérifiez le mode de fonctionnement spécifié pour le composant et corrigez-le, si cela est nécessaire en indiquant la valeur `AUTO` (le paramètre `Mode` dans la section `[LinuxSpider]` du fichier de configuration).

   Pour consulter et modifier le mode, vous pouvez utiliser les commandes de l'utilitaire de gestion depuis la ligne de commande.

   - Pour définir la valeur `AUTO`, entrez la commande

   ```
   # drweb-ctl cfset LinuxSpider.Mode AUTO
   ```

   - Pour réinitialiser la valeur d'un paramètre, entrez la commande

   ```
   # drweb-ctl cfset LinuxSpider.Mode -r
   ```

2. Si l'erreur persiste, créez et installez manuellement le module noyau pour le composant SplDer Guard.

   > ⚠ Notez que le fonctionnement de SplDer Guard et du module noyau chargeable est garanti uniquement si le système d'exploitation que vous utilisez fait partie de la liste des distributions prises en charge UNIX (voir Pré-requis système et compatibilité).

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*SplDer Gate n'est pas disponible*
Code d'erreur	`x117`
Description	Le composant SplDer Gate est manquant (nécessaire pour l'analyse de connexions réseau).

Résoudre l'erreur :

1. Vérifiez si le chemin d'accès au fichier exécutable `drweb-gated` est correct et corrigez-le, si cela est nécessaire (le paramètre `ExePath` dans la section `[GateD]` du fichier de configuration).

   Vous pouvez utiliser les commandes de l'utilitaire de gestion depuis la ligne de commande.

   - Pour consulter la valeur actuelle d'un paramètre, entrez la commande :

   ```
   $ drweb-ctl cfshow GateD.ExePath
   ```

   - Pour définir une nouvelle valeur de paramètre, entrez la commande :

   ```
   # drweb-ctl cfset GateD.ExePath <nouveau chemin>
   ```

   - Pour réinitialiser la valeur d'un paramètre, entrez la commande :

   ```
   # drweb-ctl cfset GateD.ExePath -r
   ```

2. Si les paramètres du composant SplDer Gate sont manquants dans la configuration ou qu'une erreur se produit lors de l'indication du chemin correct, installez ou réinstallez le paquet `drweb-gated`.

3. Si l'erreur persiste, supprimez Dr.Web pour Linux, puis réinstallez-le.

   Pour en savoir plus sur l'installation et la suppression du produit ou de ses composants, consultez les rubriques Installation de Dr.Web pour Linux et Suppression de Dr.Web pour Linux.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Le composant MailD n'est pas disponible*
Code d'erreur	`x118`
Description	Le composant Dr.Web MailD est manquant (nécessaire pour l'analyse d'e-mail).

Résoudre l'erreur :

1. Vérifiez si le chemin d'accès au fichier exécutable `drweb-maild` est correct et corrigez-le, si cela est nécessaire (le paramètre `ExePath` dans la section `[MailD]` du fichier de configuration).

   Vous pouvez utiliser les commandes de l'utilitaire de gestion depuis la ligne de commande.

   - Pour consulter la valeur actuelle d'un paramètre, entrez la commande :

     ```
     $ drweb-ctl cfshow MailD.ExePath
     ```

   - Pour définir une nouvelle valeur de paramètre, entrez la commande :

     ```
     # drweb-ctl cfset MailD.ExePath <nouveau chemin>
     ```

   - Pour réinitialiser la valeur d'un paramètre, entrez la commande :

     ```
     # drweb-ctl cfset MailD.ExePath -r
     ```

2. Si les paramètres du composant Dr.Web MailD sont manquants dans la configuration ou qu'une erreur se produit lors de l'indication du chemin correct, installez ou réinstallez le paquet `drweb-maild`.
3. Si l'erreur persiste, supprimez Dr.Web pour Linux, puis réinstallez-le.

   Pour en savoir plus sur l'installation et la suppression du produit ou de ses composants, consultez les rubriques Installation de Dr.Web pour Linux et Suppression de Dr.Web pour Linux.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Scanning Engine n'est pas disponible*
Code d'erreur	`x119`
Description	Le composant Dr.Web Scanning Engine est introuvable ou ne peut pas être lancé.

Résoudre l'erreur :

1. Vérifiez si le chemin d'accès au fichier exécutable `drweb-se` est correct et corrigez-le, si cela est nécessaire (le paramètre `ExePath` dans la section `[ScanEngine]` du fichier de configuration).

Vous pouvez utiliser les commandes de l'utilitaire de gestion depuis la ligne de commande.

- Pour consulter la valeur actuelle d'un paramètre, entrez la commande :

```
$ drweb-ctl cfshow ScanEngine.ExePath
```

- Pour définir une nouvelle valeur de paramètre, entrez la commande :

```
# drweb-ctl cfset ScanEngine.ExePath <nouveau chemin>
```

- Pour réinitialiser la valeur d'un paramètre, entrez la commande :

```
# drweb-ctl cfset ScanEngine.ExePath -r
```

2. En cas d'erreur lorsque vous spécifiez un chemin d'accès correct :
   - Exécutez la commande

```
$ drweb-ctl rawscan /
```

   si la ligne `Error: No valid license provided` s'affiche sur l'écran, cela signifie que le fichier clé valide est manquant. Enregistrez Dr.Web pour Linux et obtenez la licence. Si vous avez obtenu la licence, vérifiez la disponibilité du fichier clé et installez-le si cela est nécessaire.

   - Si votre OS utilise le sous-système de sécurité SELinux, configurez la politique de sécurité pour le module `drweb-se` (voir la rubrique Configuration des politiques de sécurité SELinux).
3. Si les paramètres du composant sont manquants dans la configuration ou que les étapes précédentes n'ont pas aidé, installez ou réinstallez le paquet `drweb-se`.
4. Si l'erreur persiste, supprimez Dr.Web pour Linux, puis réinstallez-le.

   Pour en savoir plus sur l'installation et la suppression du produit ou de ses composants, consultez les rubriques Installation de Dr.Web pour Linux et Suppression de Dr.Web pour Linux.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Le Scanner n'est pas disponible*
Code d'erreur	`x120`
Description	Le composant Dr.Web File Checker est introuvable ou ne peut pas être lancé.

Résoudre l'erreur :

1. Vérifiez si le chemin d'accès au fichier exécutable `drweb-filecheck` est correct et corrigez-le, si cela est nécessaire (le paramètre `ExePath` dans la section `[FileCheck]` du fichier de configuration).

   Vous pouvez utiliser les commandes de l'utilitaire de gestion depuis la ligne de commande.

   Pour consulter la valeur actuelle d'un paramètre, entrez la commande :

```
$ drweb-ctl cfshow FileCheck.ExePath
```

   Pour définir une nouvelle valeur de paramètre, entrez la commande :

```
# drweb-ctl cfset FileCheck.ExePath <nouveau chemin>
```

Pour réinitialiser la valeur d'un paramètre, entrez la commande :

```
# drweb-ctl cfset FileCheck.ExePath -r
```

2. En cas d'erreur lorsque vous spécifiez un chemin d'accès correct :
   - Si votre OS utilise le sous-système de sécurité SELinux, configurez la politique de sécurité pour le module `drweb-filecheck` (voir la rubrique Configuration des politiques de sécurité SELinux).
3. Si les paramètres du composant sont manquants dans la configuration ou que les étapes précédentes n'ont pas aidé, installez ou réinstallez le paquet `drweb-filecheck`.
4. Si l'erreur persiste, supprimez Dr.Web pour Linux, puis réinstallez-le.

   Pour en savoir plus sur l'installation et la suppression du produit ou de ses composants, consultez les rubriques Installation de Dr.Web pour Linux et Suppression de Dr.Web pour Linux.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*ES Agent n'est pas disponible*
Code d'erreur	`x121`
Description	Le composant Dr.Web ES Agent est manquant (nécessaire pour la connexion au serveur de protection centralisée).

Résoudre l'erreur :

1. Vérifiez si le chemin d'accès au fichier exécutable `drweb-esagent` est correct et corrigez-le, si cela est nécessaire (le paramètre `ExePath` dans la section `[ESAgent]` du fichier de configuration).

   Vous pouvez utiliser les commandes de l'utilitaire de gestion depuis la ligne de commande.
   - Pour consulter la valeur actuelle d'un paramètre, entrez la commande :

```
$ drweb-ctl cfshow ESAgent.ExePath
```

   - Pour définir une nouvelle valeur de paramètre, entrez la commande :

```
# drweb-ctl cfset ESAgent.ExePath <nouveau chemin>
```

   - Pour réinitialiser la valeur d'un paramètre, entrez la commande :

```
# drweb-ctl cfset ESAgent.ExePath -r
```

2. Si les paramètres du composant sont manquants dans la configuration ou qu'une erreur se produit lors de l'indication du chemin correct, installez ou réinstallez le paquet `drweb-esagent`.
3. Si l'erreur persiste, supprimez Dr.Web pour Linux, puis réinstallez-le.

   Pour en savoir plus sur l'installation et la suppression du produit ou de ses composants, consultez les rubriques Installation de Dr.Web pour Linux et Suppression de Dr.Web pour Linux.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Le composant Firewall pour Linux n'est pas disponible*
Code d'erreur	`x122`
Description	Le composant Dr.Web Firewall pour Linux est manquant (nécessaire pour l'analyse de connexions réseau).

Résoudre l'erreur :

1. Vérifiez si le chemin d'accès au fichier exécutable `drweb-firewall` est correct et corrigez-le, si cela est nécessaire (le paramètre `ExePath` dans la section `[LinuxFirewall]` du fichier de configuration).

   Vous pouvez utiliser les commandes de l'utilitaire de gestion depuis la ligne de commande.

   - Pour consulter la valeur actuelle d'un paramètre, entrez la commande :

     ```
     $ drweb-ctl cfshow LinuxFirewall.ExePath
     ```

   - Pour définir une nouvelle valeur de paramètre, entrez la commande :

     ```
     # drweb-ctl cfset LinuxFirewall.ExePath <nouveau chemin>
     ```

   - Pour réinitialiser la valeur d'un paramètre, entrez la commande :

     ```
     # drweb-ctl cfset LinuxFirewall.ExePath -r
     ```

2. Si les paramètres du composant Dr.Web Firewall pour Linux sont manquants dans la configuration ou qu'une erreur se produit lors de l'indication du chemin correct, installez ou réinstallez le paquet `drweb-firewall`.
3. Si l'erreur persiste, supprimez Dr.Web pour Linux, puis réinstallez-le.

   Pour en savoir plus sur l'installation et la suppression du produit ou de ses composants, consultez les rubriques Installation de Dr.Web pour Linux et Suppression de Dr.Web pour Linux.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Network Checker n'est pas disponible*
Code d'erreur	`x123`
Description	Le composant Dr.Web Network Checker nécessaire pour l'analyse des fichiers par réseau est manquant.

Résoudre l'erreur :

1. Vérifiez si le chemin d'accès au fichier exécutable `drweb-netcheck` est correct et corrigez-le, si cela est nécessaire (le paramètre `ExePath` dans la section `[NetCheck]` du fichier de configuration).

   Vous pouvez utiliser les commandes de l'utilitaire de gestion depuis la ligne de commande.

   - Pour consulter la valeur actuelle d'un paramètre, entrez la commande :

     ```
     $ drweb-ctl cfshow Netcheck.ExePath
     ```

- Pour définir une nouvelle valeur de paramètre, entrez la commande :

```
# drweb-ctl cfset NetCheck.ExePath <nouveau chemin>
```

- Pour réinitialiser la valeur d'un paramètre, entrez la commande :

```
# drweb-ctl cfset Netcheck.ExePath -r
```

2. Si les paramètres du composant sont manquants dans la configuration ou qu'une erreur se produit lors de l'indication du chemin correct, installez ou réinstallez le paquet `drweb-netcheck`.
3. Si l'erreur persiste, supprimez Dr.Web pour Linux, puis réinstallez-le.

   Pour en savoir plus sur l'installation et la suppression du produit ou de ses composants, consultez les rubriques Installation de Dr.Web pour Linux et Suppression de Dr.Web pour Linux.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Le composant CloudD n'est pas disponible*
Code d'erreur	`x124`
Description	Le composant Dr.Web CloudD est manquant (nécessaire pour accéder à Dr.Web Cloud).

Résoudre l'erreur :

1. Vérifiez si le chemin d'accès au fichier exécutable `drweb-cloud` est correct et corrigez-le, si cela est nécessaire (le paramètre `ExePath` dans la section `[CloudD]` du fichier de configuration).

   Vous pouvez utiliser les commandes de l'utilitaire de gestion depuis la ligne de commande.

   - Pour consulter la valeur actuelle d'un paramètre, entrez la commande :

```
$ drweb-ctl cfshow CloudD.ExePath
```

   - Pour définir une nouvelle valeur de paramètre, entrez la commande :

```
# drweb-ctl cfset CloudD.ExePath <nouveau chemin>
```

   - Pour réinitialiser la valeur d'un paramètre, entrez la commande :

```
# drweb-ctl cfset CloudD.ExePath -r
```

2. Si les paramètres du composant sont manquants dans la configuration ou qu'une erreur se produit lors de l'indication du chemin correct, installez ou réinstallez le paquet `drweb-cloudd`.
3. Si l'erreur persiste, supprimez Dr.Web pour Linux, puis réinstallez-le.

   Pour en savoir plus sur l'installation et la suppression du produit ou de ses composants, consultez les rubriques Installation de Dr.Web pour Linux et Suppression de Dr.Web pour Linux.

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Message d'erreur	*Erreur inattendue*

Code d'erreur	`x125`
Description	Une erreur imprévue s'est produite lors du fonctionnement d'un ou de plusieurs composants

Résoudre l'erreur :

1. Essayez de redémarrez Dr.Web pour Linux, en exécutant la commande suivante :

```
# service drweb-configd restart
```

Si l'erreur persiste, contactez le Support technique et indiquez le code d'erreur.

Erreurs sans code

Symptômes : Après l'installation du module de noyau de SpIDer Guard, le système d'exploitation s'arrête avec l'erreur de noyau « *Kernel panic* ».

Description : Le fonctionnement du module noyau de SpIDer Guard est impossible dans l'environnement d'exécution du noyau de l'OS (par exemple, l'OS fonctionne dans l'environnement de l'hyperviseur Xen).

Résolution de l'erreur

1. Annulez le chargement du module de noyau de SpIDer Guard (le module de noyau porte le nom `drweb`) en ajoutant dans le chargeur grub la ligne :

```
drweb.blacklist=yes
```

   dans la ligne des paramètres de chargement du noyau de l'OS.
2. Après le chargement de l'OS, supprimez le module de noyau `drweb.ko` du répertoire des modules supplémentaires de noyau `/lib/modules/`uname -r`/extra`.
3. Spécifiez pour SpIDer Guard le mode *AUTO* en exécutant les commandes suivantes :

```
# drweb-ctl cfset LinuxSpider.Mode Auto
# drweb-ctl reload
```

4. Si l'OS utilisé ne prend pas en charge le mécanisme *fanotify* ou que l'utilisation de ce mode ne permet pas d'utiliser SpIDer Guard pour un contrôle complet du système de fichiers et que l'utilisation du mode *LKM* devient obligatoire, refusez l'utilisation de l'hyperviseur Xen.

Si vous n'arrivez pas à résoudre l'erreur, contactez le Support technique.

Symptômes : La fenêtre principale de Dr.Web pour Linux est désactivée, l'indicateur dans la zone de notifications indique une erreur critique, et le menu déroulant contient un seul élément désactivé **Démarrer**.

Description : Dr.Web pour Linux ne peut pas démarrer car le composant de service principal `drweb-configd` n'est pas disponible.

Résolution de l'erreur

1. Redémarrez Dr.Web pour Linux, en exécutant la commande suivante :

   ```
   # service drweb-configd restart
   ```

2. Si cette commande remonte un message d'erreur, ou n'a pas d'effet, installez le composant `drweb-configd` (package) séparément.

   Notez que cela peut signifier que PAM n'est pas utilisé pour l'authentification d'utilisateurs dans le système. Si c'est le cas, installez et configurez-le.

3. Si l'erreur persiste, supprimez Dr.Web pour Linux, puis réinstallez-le.

   Pour en savoir plus sur l'installation et la suppression du produit ou de ses composants, consultez les rubriques Installation de Dr.Web pour Linux et Suppression de Dr.Web pour Linux.

Si vous n'arrivez pas à résoudre l'erreur, contactez le Support technique.

Symptômes

1. L'indicateur dans la zone de notification du bureau ne s'affiche pas après la connexion au système.
2. La tentative d'exécuter la commande du lancement de l'interface graphique :

   ```
   $ drweb-gui
   ```

   ouvre la fenêtre principale de Dr.Web pour Linux.

Description : Il est probable que cette erreur est liée à l'absence de la bibliothèque supplémentaire `libappindicator1` dans votre système.

Résolution de l'erreur

1. Vérifiez la présence du paquet `libappindicator1` dans votre système en exécutant la commande suivante :

   ```
   # dpkg -l | grep libappindicator1
   ```

2. Si la commande n'affiche aucun résultat, installez ce paquet en utilisant n'importe quel gestionnaire de paquet du système. Après, ouvrez une nouvelle session système (*log in*).

   Notez que cela peut signifier que PAM n'est pas utilisé pour l'authentification d'utilisateurs dans le système. Si c'est le cas, installez et configurez-le.

3. Si l'erreur persiste, supprimez Dr.Web pour Linux, puis réinstallez-le.

   Pour en savoir plus sur l'installation et la suppression du produit ou de ses composants, consultez les rubriques Installation de Dr.Web pour Linux et Suppression de Dr.Web pour Linux.

Si vous n'arrivez pas à résoudre l'erreur, contactez le Support technique.

Symptômes

1. Après la désactivation de SpIDer Gate, les connexions réseau (sortantes et probablement entrantes – via les protocoles SSH, FTP) s'arrêtent.
2. Recherche dans les règles de NetFilter (`iptables`) avec la commande :

```
# iptables-save | grep "comment --comment --comment"
```

vous obtenez le résultat non vide.

Description : Cette erreur est liée au fonctionnement incorrect de NetFilter (`iptables`) en version plus ancienne que 1.4.15. Les règles au marqueur (commentaire) unique sont ajoutées incorrectement de sorte que SpIDer Gate lors de son arrêt ne peut pas supprimer les règles de redirection des connexions réseau ajoutées par lui-même.

Résolution de l'erreur

1. Réactivez SpIDer Gate pour qu'il effectue le scan.
2. S'il faut laisser SpIDer Gate désactivé, supprimez les règles incorrectes de NetFilter (`iptables`) à l'aide de la commande :

   ```
   # iptables-save | grep -v "comment --comment --comment" | iptables-restore
   ```

   Notez que les droits root sont requis pour exécuter les commandes `iptables-save` et `iptables-restore`. Pour obtenir les droits de super-utilisateur, vous pouvez utiliser les commandes `su` et `sudo`. Notez aussi que la commande indiquée va supprimer de la liste de règles toutes les règles avec le commentaire ajouté incorrectement, par exemple les règles ajoutées par d'autres applications exécutant la correction de l'acheminement des connexions.

Informations supplémentaires

- Pour éviter cette erreur à l'avenir, veuillez mettre à niveau le système d'exploitation (ou au moins NetFilter vers la version 1.4.15 ou supérieure).
- De plus, vous pouvez activer le mode manuel d'acheminement des connexions pour SpIDer Gate en spécifiant les règles nécessaires manuellement à l'aide de l'utilitaire `iptables` (non recommandé).
- Pour plus d'information, voir la documentation `man`: `drweb-firewall(1)`, `drweb-gated(1)`, `iptables(8)`.

Si vous n'arrivez pas à résoudre l'erreur, contactez le Support technique.

Symptômes : Un double-clic sur l'icône d'un fichier ou d'un répertoire dans le gestionnaire graphique de fichiers ne les ouvre pas mais il lance l'analyse dans Dr.Web pour Linux**.**

Description :L'interface graphique a fait l'association automatique des fichiers d'un certain type et/ou des répertoires avec l'action **Ouvrir dans Dr.Web pour Linux**.

Résolution de l'erreur

1. Annulez l'association entre les fichiers de ce type et l'application Dr.Web pour Linux. Les associations configurées sont fixées dans le fichier `mimeapps.list` ou `defaults.list`. Les fichiers déterminant les paramètres locaux modifiés dans le profil utilisateur sont enregistrés dans le répertoire `~/.local/share/applications/` ou `~/.config/` (d'habitude ces répertoires ont l'attribut caché).
2. Ouvrez le fichier `mimeapps.list` ou `defaults.list` dans un éditeur de texte (notez que les privilèges de super-utilisateur sont requis pour l'édition du fichier système. Si nécessaire, utilisez les commandes `su` ou `sudo`).

3. Trouvez dans le fichier, la section `[Default Applications]`, dans cette section, trouvez les ligne d'associations de type`<type MIME>=drweb-gui.desktop`, par exemple :

```
[Default Applications]
inode/directory=drweb-gui.desktop
text/plain=drweb-gui.desktop;gedit.desktop
```

4. Si dans la partie droite (après l'égalité) de la ligne de l'association, outre `drweb-gui.desktop`, il y a des liens vers d'autres applications, supprimez de la ligne uniquement le lien vers l'application `drweb-gui` (`drweb-gui.desktop`). Si l'association ne contient que le lien vers l'application `drweb-gui`, supprimez la ligne entière de l'association.
5. Enregistrez le fichier modifié.

Informations supplémentaires

- Pour vérifier les associations actuelles, vous pouvez utiliser les utilitaires `xdg-mime`, `xdg-open` et `xdg-settings` (inclus dans le paquet `xdg-utils`).
- Pour plus d'informations sur le fonctionnement des utilitaires xdg voir la documentation `man`: `xdg-mime(1)`, `xdg-open(1)`, `xdg-settings(1)`.

Si vous n'arrivez pas à résoudre l'erreur, contactez le Support technique.

Annexe E. Créer un module noyau pour SpIDer Guard

Dans cette section :

- Informations générales.
- Instruction d'assemblage du module noyau.
- Erreurs de création possibles.

Informations générales

Si le système d'exploitation ne fournit pas le mécanisme fanotify utilisé par SpIDer Guard pour la surveillance des actions avec les objets du système de fichiers, il peut utiliser un module chargeable spécial fonctionnant dans l'espace noyau (module LKM).

Par défaut, SpIDer Guard est fourni avec un module noyau compilé pour les OS qui ne fournissent pas le service fanotify. De plus, vous pouvez construire un module noyau chargeable manuellement en utilisant les codes source fournis dans une archive au format `tar.bz2`.

> Le module LKM utilisé par SpIDer Guard est conçu pour fonctionner avec les noyaux GNU/Linux en version 2.6 * et supérieure.

> L'utilisation de LKM n'est pas supportée pour les architectures ARM64 et E2K.

L'archive contenant les codes source est situé dans le sous-répertoire `share/drweb-spider-kmod/src du répertoire de base de` Dr.Web pour Linux (par défaut `/opt/drweb.com`). Le nom de l'archive est construit comme suit : `drweb-spider-kmod-`*<version>*`-`*<date>*`.tar.bz2`. Le répertoire `drweb-spider-kmod` contient également le script de test `check-kmod-install.sh`. Exécutez le script pour vérifier si l'OS utilisé prend en charge les versions compilées des modules noyau inclus dans Dr.Web pour Linux. Si ce n'est pas le cas, un message vous invitant à créer manuellement le module s'affiche sur l'écran.

Si le répertoire spécifié `drweb-spider-kmod` est introuvable, installez le paquet `drweb-spider-kmod`.

> Pour créer le module noyau chargeable manuellement d'après les codes source, il faut avoir les privilèges de super-utilisateur (root). Pour cela, vous pouvez utiliser la commande `su` pour passer à un autre utilisateur ou la commande `sudo` pour créer le module en tant qu'autre utilisateur.

Instruction d'assemblage du module noyau

1. Décompressez l'archive contenant les codes source dans n'importe quel répertoire. Par exemple, la commande

   ```
   # tar -xf drweb-spider-kmod-<version>-<date>.tar.bz2
   ```

   décompresse les codes source dans le répertoire créé. Ce répertoire comporte le nom de l'archive et est créé au même endroit que celui où réside l'archive (notez que les privilèges de super-utilisateur sont requis pour écrire dans un répertoire contenant une archive).
2. Allez au dossier créé et exécutez la commande suivante :

   ```
   # make
   ```

   Si une erreur survient à l'étape *make*, réparez-la (voir ci-dessous) et relancez la compilation.
3. Une fois la commande *make* exécutée avec succès, entrez les commandes suivantes :

   ```
   # make install
   # depmod
   ```
4. Une fois le module noyau compilé avec succès et enregistré dans le système, effectuez les paramétrages supplémentaires de SpIDer Guard. Paramétrez le composant afin qu'il fonctionne avec le module noyau en exécutant la commande suivante :

   ```
   # drweb-ctl cfset LinuxSpider.Mode LKM
   ```

   Vous pouvez également indiquer `AUTO` au lieu de `LKM`. Dans le dernier cas, SpIDer Guard tentera d'utiliser non seulement le module noyau, mais aussi le mécanisme systeme fanotify. Pour en savoir plus, consultez la documentation `man : drweb-spider(1)`.

Erreurs de création possibles

Durant l'exécution de la commande *make*, des erreurs peuvent survenir. Si c'est le cas, vérifiez les éléments suivants :

- Pour garantir une création réussie du module, Perl et le compilateur GCC sont requis. S'ils ne sont pas présents dans le système, installez-les.
- Sur certains OS, vous pouvez avoir besoin d'installer le paquet `kernel-devel` avant de lancer la procédure.
- Sur certains OS, la procédure peut échouer parce que le chemin vers le répertoire contenant les codes source a été indiqué de manière incorrecte. Si c'est le cas, utilisez la commande `make` avec le paramètre `KDIR=<chemin vers les codes source de noyau>`. D'habitude, les codes source sont situés dans le répertoire `/usr/src/kernels/<version du noyau>`.

Notez que la version du noyau remontée par la commande `uname -r` peut différer du nom de répertoire <*version du noyau*>.

Application F. Liste d'abréviations

Les termes suivants seront utilisés dans ce manuel sans explication :

Terme	Description
FQDN	Fully Qualified Domain Name
GNU	Projet GNU (GNU is Not Unix)
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure (via SSL/TLS)
ID	Identifiant
IMAP	Internet Message Access Protocol (protocole de messagerie)
IP	Internet Protocol
MBR	Master Boot Record
NSS	Novell Storage Services
PID	Process ID (identifiant de processus)
PAM	Pluggable Authentication Modules
POP	Post Office Protocol (protocole de messagerie)
RPM	RedHat Package Manager (format de paquets)
SMTP	Simple Mail Transfer Protocol (protocole de messagerie)
SP	Service Pack
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UID	User ID (identifiant d'utilisateur)
URL	Uniform Resource Locator
VBR	Volume Boot Record

Terme	Description
OS	Système d'exploitation

Référence

A

A propos de ce produit 9
A propos du produit 9
Abréviations 228
Acheter une licence 100
Activer l'antivirus 100
Aide 115
Analyse de SSL/TLS, HTTPS 131
Analyse des connexions cryptées 131
Analyse des fichiers du gestionnaire de fichiers 77
annexe
  neutralisation des menaces informatiques 176
  types de menaces informatiques 171
Annexes 171
Arguments de la ligne de commande de l'interface graphique 138
Assistance 115
Augmentation des privilèges 113

B

Baisse des privilèges 113

C

Composants 12
Configuration d'ELF 61
Configuration de la planification 130
Configuration de la surveillance des connexions réseau 122
Configuration de PARSEC 57
Configuration des sous-systèmes de sécurité 53
Configurer SELinux 54
Connexion à Dr.Web Cloud 137
Connexion au serveur de protection centralisée 67, 134
Consulter l'aide 115
Consulter les messages 110
Contrôle des connexions réseau 91
Créer un module noyau 226

D

Déconnexion de Dr.Web Cloud 137
Démarrer le GUI 80
Dr.Web Cloud 137
Droits des fichiers 15
drweb-ctl 140
drweb-gui 80

E

EICAR 67
Enregistrement 63
Enregistrement réitéré 63
Enregistrer la licence 100
Entrer le numéro de série 100
Erreurs connues 180
Exclusion de l'analyse 126
Exclusion des connexions réseau des applications 128
Exclusion des fichiers et des répertoires 127
Exclusions 126
Exemples de l'appel depuis la ligne de commande 166

F

Fichier clé 66, 100
Fichier clé de licence 66
Fichier de configuration de la connexion 67
Fichiers de Dr.Web pour Linux 49
Fonctionnement autonome de l'interface graphique 139
Fonctions 9

G

Gérer la quarantaine 96
Gestion des fichiers clé 63
Gestion des licences 63
Gestion des privilèges 113
Gestion via la ligne de commande 140
Gestionnaire de Licences 100

I

Icône de la barre d'outils 77
Installateur en ligne de commande 31
Installateur graphique 30
Installation de Dr.Web pour Linux 26, 27
Installation depuis la distribution 27
Installation depuis le package .run 27
Installation depuis le référentiel 32
Installation depuis les packages universels 27
Installation depuis les paquets natifs 32
Installation personnalisée 49
Interface graphique de gestion 72
Interfaces de gestion 71
Introduction 7
Isolement 14

Référence

L

Lancement du logiciel de suppression 42
Lancer l'utilitaire de ligne de commande 142
Lancer la mise à jour 99
Légende 8
Licence 25
Liste des exclusions 126
Liste des menaces 93
Liste des scans 86
Listes noire et blanche de sites web 129

M

Menaces 93
menaces informatiques 171
Menu contextuel du logiciel 77
Mettre à jour 99
Mettre à jour les bases 99
Mise à jour de Dr.Web pour Linux 36
Mise à jour des composants 36
Mise à jour du produit 36
Mise à niveau vers une nouvelle version 38
Mise en marche 63
Mode de fonctionnement 134
Mode de surveillance paranoïde 68
Mode de surveillance renforcé 68
Mode mobile 16
Mode standalone 16
Modes d'installation de Dr.Web pour Linux 27
Modes d'utilisation de Dr.Web pour Linux 71
Modes de fonctionnement 16
Modes de suppression de Dr.Web pour Linux 42
Modules 12

N

neutralisation des menaces informatiques 176
Neutraliser les menaces 93
Notifications 77

O

Ouvrir l'aide 115

P

Paramètres 115
Paramètres d'analyse 119
Paramètres de SpIDer Gate 122
Paramètres de SpIDer Guard 121
Paramètres du contrôle du système de fichiers 121
Paramètres du Scanner 119
Paramètres principaux 116
Planification 130
Pré-requis système 20
Privilèges de super-utilisateur 113
Privilèges des fichiers 15
Problèmes de SELinux 54
Protection centralisée 16, 110, 134

Q

Quarantaine 14, 96
Quitter le GUI 80

R

Recherche de menaces 81
Répertoires de la quarantaine 14

S

Scan complet 81
Scan de fichiers 81
Scan personnalisé 81
Scan rapide 81
Scan selon la planification 85, 130
Sécurité SELinux 54
SpIDer Gate 91
SpIDer Guard 88
Structure du produit 12
Support technique 178
Suppression de Dr.Web pour Linux 26, 42
Suppression en mode de ligne de commande 44
Suppression en mode graphique 43
Suppression via l'interface graphique 43
Supprimer de la ligne de commande 44
Supprimer des paquets natifs 45
Supprimer du dépôt 45
Supprimer la distribution 42
Surveillance du système de fichiers 88
Systèmes d'exploitation 20

T

Tâches 9
Tâches de scan 86
Tester l'antivirus 67

Référence

U

Utilisation de Dr.Web Cloud 137

V

Voir la quarantaine 96