Dr.WEB

Enterprise Security Suite

Annexes

Dr.Web Enterprise Security Suite
Version 13.0
Annexes
12/07/2024

Doctor Web, Siège social en Russie

Adresse : 2-12A, 3e rue Yamskogo polya, 125124 Moscou, Russie

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

Téléphone : +7 (495) 789-45-87

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

Doctor Web

Doctor Web — éditeur russe de solutions de sécurité informatique.

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

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

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

Nous remercions tous nos clients pour leur soutien !

Contenu

Chapitre 1 : Introduction

Destination du document

La documentation de l'administrateur du réseau antivirus Dr.Web Enterprise Security Suite décrit les principes généraux ainsi que les détails concernant la mise en oeuvre de la protection antivirus des ordinateurs d'entreprise avec Dr.Web Enterprise Security Suite.

La documentation de l'administrateur du réseau antivirus contient les parties suivantes :

1. **Manuel d'installation**

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

   Le Manuel d'installation explique comment construire un réseau antivirus et installer ses composants.

2. **Manuel Administrateur**

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

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

3. **Annexes**

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

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

De plus, les manuels suivants sont fournis :

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

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

2. **Manuels de gestion des postes**

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

3. **Manuels Utilisateur**

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

4. **Manuel sur Web API**

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

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

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

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

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

Légende et abréviations

Conventions

Les styles utilisés dans ce manuel :

Style	Commentaire
	Notice/indication importante.
	Avertissement sur des situations potentielles d'erreurs et sur les éléments importants auxquels il faut faire attention.
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.

Style	Commentaire
`C:\Windows\`	Noms de fichiers/dossiers ou fragments de programme.
Annexe A	Liens vers les autres chapitres du manuel ou liens vers des ressources externes.

Abréviations

Les abréviations suivantes peuvent être utilisées dans le manuel :

- BD, SGBD : base de données, système de gestion de base de données,
- SGM Dr.Web : Système Global de Mises à jour Dr.Web,
- LAN : réseau local,
- OS : système d'exploitation,
- -
- ACL : listes de contrôle d'accès (Access Control List),
- CDN : réseau de distribution de contenu (Content Delivery Network),
- DFS : système de fichiers distribués (Distributed File System),
- DNS : système de noms de domaine (Domain Name System),
- FQDN : nom de domaine complètement qualifié (Fully Qualified Domain Name),
- GUI : interface graphique utilisateur (Graphical User Interface), une version GUI du logiciel est une version utilisant des outils GUI,
- MIB : base d'information pour la gestion du réseau (Management Information Base),
- MTU : taille maximale de l'unité de transmission (Maximum Transmission Unit),
- NAP : Protection d'accès réseau (Network Access Protection),
- TTL : durée de Vie (Time To Live),
- UDS : socket du domaine UNIX (UNIX Domain socket).

Chapitre 2 : Annexes

Annexe A. Configuration du SGBD. Paramètres des pilotes du SGBD

La structure de la base de données du Serveur voisin est disponible sous forme d'un manuel éponyme à part. Vous pouvez ouvrir le document dans la section **Support** dans le Centre de gestion de la sécurité Dr.Web.

En tant que base de données du Serveur Dr.Web les bases suivantes peuvent être utilisées :

- BD embarquée ;
- SGBD externe.

BD embarquée

Lors de la configuration de l'accès à la BD pour la sauvegarde et le traitement de données, utilisez les paramètres décrits dans le tableau **A-1**.

Tableau A-1. BD embarquée

Nom	Valeur par défaut	Description
`DBFILE`	`database.sqlite`	Chemin vers le fichier de la base de données
`CACHESIZE`	`2048`	La taille de la mémoire cache de la base de données en pages
`PRECOMPILEDCACHE`	`1048576`	Taille du cache des opérateurs SQL précompilés en octets
`MMAPSIZE`	• sous UNIX — `10485760`, • sous Windows — `0`	Taille maximum du fichier de la base de données (en octets) qui peut être mappé en espace d'adresse du processus en une fois.
`CHECKINTEGRITY`	`QUICK`	Vérifier l'intégrité de l'image de la base de données au démarrage du Serveur Dr.Web : • `FULL` : analyse complète pour la présence des erreurs liées aux restrictions de type UNIQUE, CHECK et NOT NULL, enregistrements incorrects, pages sautées et index incohérents, • `QUICK` : variante rapide de l'analyse sans détection d'erreurs de restrictions et d'index incohérents,

		• NO : l'analyse n'est pas effectuée.
AUTOREPAIR	NO	Restauration automatique de l'image corrompue de la base de données au démarrage du Serveur Dr.Web : • YES : restauration de l'intégrité de l'image de la base de données à chaque démarrage du Serveur Dr.Web, • NO : la restauration automatique est désactivée.
WAL	YES	Utilisation de la journalisation préventive (Write-Ahead Logging) : • YES : la journalisation est activée, • NO : la journalisation n'est pas utilisée.
WAL-MAX-PAGES	1000	Nombre maximum de pages de modifications à atteindre pour que toutes les pages soient écrites sur le disque.
WAL-MAX-SECONDS	30	Délai maximum pour retarder l'écriture des pages sur le disque (en secondes).
SYNCHRONOUS	FULL	Mode d'enregistrement synchrone des modifications apportées dans la base de données sur le disque : • FULL : enregistrement complètement synchrone sur le disque, • NORMAL : enregistrement synchrone des données critiques, • OFF : enregistrement asynchrone.

SQLite3 (BD prise en charge par le Serveur Dr.Web, à commencer par la version 10) est fourni en tant que BD embarquée.

SGBD externe

Les SGBD suivants peuvent être utilisés en tant que la base de données externe du Serveur Dr.Web :

- SGBD MySQL, MariaDB. Les paramètres sont décrits dans A4. Utilisation du SGBD MySQL.
- SGBD Oracle. La configuration est décrite dans A2. Configuration du pilote de BD pour Oracle.
- SGBD PostgreSQL. Les paramètres sont décrits dans A3. Utilisation du SGBD PostgreSQL.

  Les SGBD basés sur PostgreSQL sont pris en charge (PostgreSQL Pro, Jatoba et autres).

- Microsoft SQL Server/Microsoft SQL Server Express. Pour accéder à ce SGBD, le pilote ODBC peut être utilisé (la configuration du pilote ODBC pour Windows est décrite dans l'Annexe A1. Configuration du pilote ODBC).

Microsoft SQL Server 2008 ou une version supérieure est supporté. Il est recommandé d'utiliser Microsoft SQL Server 2014 ou une version supérieure.

La BD Microsoft SQL Server Express n'est pas recommandée en cas de déploiement d'un réseau antivirus avec un grand nombre de postes (100 et plus).

Si Microsoft SQL Server est utilisé comme BD externe pour le Serveur Dr.Web sous un OS de la famille UNIX, le fonctionnement correct via ODBC avec FreeTDS n'est pas garanti.

Si un avertissement ou une erreur survient lors du travail du Serveur Dr.Web avec SGBD Microsoft SQL Server via ODBC, il faut s'assurer que vous utilisez la dernière version disponible de SGBD de cette rédaction.

Pour savoir comment vérifier la disponibilité des mises à jour, consultez la page suivante de Microsoft : https://learn.microsoft.com/en-US/troubleshoot/sql/releases/download-and-install-latest-updates.

Pur diminuer le nombre de blocages lors de l'utilisation du SGBD Microsoft SQL Server avec le niveau d'isolation des transactions par défaut (READ COMMITTED), il est recommandé d'activer le paramètre READ_COMMITTED_SNAPSHOT, en exécutant la commande SQL suivante :

```
ALTER DATABASE <nom_de_la_base_de_données>
SET READ_COMMITTED_SNAPSHOT ON;
```

Il faut exécuter la commande en mode de transactions implicites et avec une seule connexion existante à la base de données.

Caractéristiques comparatives de la BD embarquée et des SGBD externes

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

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

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

- processeur 3GHz,

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

Pour choisir entre une base de données embarquée ou externe, prenez en compte les paramètres particuliers de chaque BD :

- Dans les grands réseaux antivirus (comptant plus de 400–600 postes) il est recommandé d'utiliser une BD externe qui est plus résistante aux échecs qu'une BD interne.
- Le SGBD intégré est beaucoup plus rapide que son homologue externe et il est recommandé principalement pour une utilisation standard de la base de donnée.
- La base de données embarquée ne requiert pas d'expérience en administration de SGBD et constitue un bon choix pour les petits ou moyens réseaux.
- Il est recommandé d'utiliser une base externe si vous devez travailler via un SGBD et accéder directement à la BD. Pour faciliter l'accès, il est possible d'utiliser les API standard comme OLE DB, ADO.NET ou ODBC.

A1. Configuration du pilote ODBC

Lors de la configuration de la connexion au SGBD externe pour le stockage et le traitement de données, les paramètres listés dans le tableau **A-2** sont utilisés (les valeurs concrètes sont utilisées à titre d'exemple).

Tableau A-2. Paramètres de la connexion ODBC

Nom	Valeur	Description
`DSN`	`drwcs`	Nom du jeu de données
`USER`	`drwcs`	Nom d'utilisateur
`PASS`	`fUqRbrmlvI`	Mot de passe
`TRANSACTION`	`DEFAULT`	Valeurs possibles du paramètre `TRANSACTION` : • `SERIALIZABLE` • `READ_UNCOMMITTED` • `READ_COMMITTED` • `REPEATABLE_READ` • `DEFAULT` La valeur déterminée par défaut `DEFAULT` signifie : "utiliser les valeurs par défaut relatives à la configuration du Serveur SQL". Pour

Nom	Valeur	Description
		plus d'informations sur les niveaux d'isolation des transactions, consultez la documentation de la base de données correspondant.

Afin d'éviter d'éventuels problèmes concernant le codage, il est nécessaire de désactiver les paramètres suivants du pilote ODBC :

- **Utiliser les paramètres régionaux lors de l'affichage des devises, des nombres, des dates et de l'heure** : cela peut entraîner des erreurs lors du formatage des valeurs numériques.
- **Traduire les données de type caractère** : cela peut entraîner l'affichage incorrect des symboles dans les paramètres provenant de la base de données dans le Centre de gestion. Ce paramètre établit une correspondance entre l'affichage des symboles et le paramètre de langue pour les programmes n'utilisant pas Unicode.

Quand vous créez une nouvelle base de données dans le SGBD Microsoft SQL, il faut indiquer le tri en respectant la casse (le suffixe `_CS`) et les signes diacritiques (le suffixe `_AS`).

L'utilisation des caractères suivants est indésirable: espace, `{`, `;` et `}`. Pour en savoir plus, consultez https://learn.microsoft.com/en-us/sql/odbc/reference/syntax/sqldriverconnect-function?redirectedfrom=MSDN&view=sql-server-ver15.

La base de données est créée préalablement sur le Serveur SQL avec les paramètres ci-dessus.

Il est nécessaire de configurer également les paramètres du pilote ODBC pour l'ordinateur sur lequel est installé Serveur Dr.Web.

Vous pouvez consulter les informations sur la configuration du pilote ODBC sous les OS de la famille UNIX sur le site https://www.unixodbc.org/, dans la rubrique **Manuals**.

Configuration du pilote ODBC pour Windows

Pour configurer les paramètres du pilote ODBC

1. Dans le **Panneau de configuration Windows**, sélectionnez l'élément **Outils d'administration**, puis dans la fenêtre qui apparaît, faites un double clic sur l'icône **Sources de données (ODBC)**. La fenêtre **Administrateur de sources de données ODBC** va s'ouvrir. Passez à l'onglet **Sources de données système**.
2. Cliquez sur le bouton **Ajouter**. La fenêtre de sélection de pilote va s'ouvrir.

3. Sélectionnez dans la liste l'élément correspondant au pilote ODBC pour la BD sélectionnée et cliquez ensuite sur le bouton **Terminer**. La première fenêtre de configuration d'accès au Serveur de BD va s'ouvrir.

   

   En cas d'utilisation d'un SGBD externe, il faut installer la dernière version du pilote ODBC fournie avec ce SGBD. Il n'est pas recommandé d'utiliser le pilote ODBC fourni avec l'OS Windows (SQL Server Native Client).

   Les BD fournies par Microsoft sans pilote ODBC font exception. Si vous utilisez un SGBD MS SQL, il faut installer et utiliser la version actuelle du pilote ODBC depuis le site Microsoft.

4. Spécifiez les paramètres d'accès à la source de données correspondant aux paramètres spécifiés dans la configuration du Serveur Dr.Web. Si le Serveur de BD se trouve sur un ordinateur autre que celui sur lequel tourne le Serveur Dr.Web, spécifiez son adresse IP ou le nom du serveur de BD dans le champ de saisie **Serveur**. Cliquez sur le bouton **Suivant**.
5. Sélectionnez l'option **Vérifier l'authenticité du compte SQL Server** et spécifiez les identifiants nécessaire de l'utilisateur pour accéder à la BD. Cliquez sur **Suivant**.
6. Dans la liste déroulante **Utiliser la base de données par défaut**, sélectionner la base de données utilisée par le Serveur Dr.Web. Dans ce cas, c'est le nom de la base de données du Serveur Dr.Web qui doit être indiquée et non la valeur **Default**.

   Assurez-vous que les cases suivantes sont cochées : **Identificateurs entre guillemets au format ANSI**, **Valeurs null, Modèles et notifications au format ANSI** sont cochées. Cliquez ensuite sur le bouton **Suivant**.

   

   S'il est possible de changer la langue des messages système lors de la configuration du pilote ODBC, il est nécessaire de spécifier l'anglais.

7. A la fin de l'édition cliquez sur **Terminer**. La fenêtre contenant le tableau des paramètres configurés va s'afficher.
8. Pour vérifier les paramètres, cliquez sur le bouton **Tester la source de données**. Après avoir reçu un message de réussite de la vérification, cliquez sur le bouton **OK**.

A2. Configuration du pilote de BD pour Oracle

Généralités

Oracle Database (ou SGBD Oracle) est un SGBD objet-relationnel. Oracle peut être utilisé en tant que base de données externe pour Dr.Web Enterprise Security Suite.

Serveur Dr.Web peut utiliser le SGBD Oracle en tant que base externe sur toutes les plateformes excepté FreeBSD (voir le p. Installation et versions supportées).

Pour utiliser le SGBD Oracle

1. L'installation d'une BD Oracle avec le codage `AL32UTF8`. Vous pouvez également utiliser la BD existante avec ce codage.
2. La configuration du pilote de BD afin de pouvoir utiliser la base de données externe. Vous pouvez le configurer dans le fichier de configuration ou via le Centre de gestion : menu **Configuration du Serveur Dr.Web**, onglet **Base de données**.

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

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

La connexion à la BD Oracle au nom des utilisateurs systèmes SYS et SYSTEM est interdite, même avec les privilèges SYSDBA et SYSOPER.

Installation et versions supportées

Pour pouvoir utiliser la BD Oracle en tant que base externe, il est nécessaire de configurer, pour la base, le codage `AL32UTF8` (`CHARACTER SET AL32UTF8 / NATIONAL CHARACTER SET AL16UTF16`). Ceci peut être réalisé par les moyens suivants :

1. Avec l'installateur de la BD Oracle (utilisez le mode avancé d'installation et de configuration de la BD).
2. Avec la commande SQL `CREATE DATABASE`.

Pour en savoir plus sur la création et la configuration de la BD, consultez la documentation relative à la BD Oracle.

En cas d'utilisation d'un codage autre que le codage indiqué, les symboles nationaux ne seront pas affichés correctement.

Le client d'accès à la BD (Oracle Instant Client) fait partie du package d'installation de Dr.Web Enterprise Security Suite.

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

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

Dr.Web Enterprise Security Suite supporte le SGBD Oracle en version 11 ou supérieure.

Notez également les pré-requis système du Serveur Dr.Web lors du travail avec la base de données externe Oracle (voir le **Manuel d'installation**, p. Pré-requis système).

Paramètres

Lors de la configuration de la connexion au SGBD Oracle, les paramètres décrits dans le tableau **A-3** sont utilisés.

Tableau A-3. Paramètres du SGBD Oracle

Paramètre	Description
`drworacle`	Nom du pilote
`User`	Nom de l'utilisateur de la BD (obligatoire)
`Password`	Mot de passe utilisateur (obligatoire)
`ConnectionString`	Ligne de connexion à la BD (obligatoire)

Format de la ligne de connexion au SGBD Oracle :

//<host>:<port>/<service name>

où :

- *<host>* : adresse IP ou nom du serveur Oracle ;
- *<port>* : port écoutant le Serveur ;
- *<service name>* : nom de la BD à laquelle il faut se connecter.

Exemple :

```
//myserver111:1521/bjava21
```

où :

- `myserver111` : nom du serveur Oracle.
- `1521` : port écoutant le serveur.
- `bjava21` : nom de la BD à laquelle il faut se connecter.

Configuration du pilote de SGBD Oracle

Si vous utilisez SGBD Oracle, il est nécessaire de modifier le mode de détection et les paramètres du pilote de base de données d'une des manières suivantes :

- Dans le Centre de gestion : l'élément **Administration** du menu principal → l'élément **Configuration du Serveur Dr.Web** du menu de gestion → l'onglet **Base de données** →

sélectionnez dans la liste déroulante **Base de données** type **Oracle**, configurez les paramètres selon le format indiqué ci-dessus.

- Dans le fichier de configuration du Serveur Dr.Web.

A3. Utilisation du SGBD PostgreSQL

Généralités

PostgreSQL est un SGBD objet-relationnel. C'est une alternative aux SGBD commercialisés (tels que Oracle Database, Microsoft SQL Server etc.). Dans les grands réseaux, le SGBD PostgreSQL peut être utilisé en tant que BD externe pour Dr.Web Enterprise Security Suite.

Pour utiliser PostgreSQL en tant que BD externe

1. Installer le Serveur PostgreSQL ou Postgres Pro.
2. Configurer le Serveur Dr.Web conformément à l'utilisation de la base externe. Ceci peut être effectué dans le fichier de configuration ou via le Centre de gestion : dans le menu **Configuration** du **Serveur Dr.Web**, dans l'onglet **Base de données**.

Pour vous connecter à la BD PostgreSQL vous pouvez utiliser uniquement une authentification trust, password et MD5.

Installation et versions supportées

1. Téléchargez la dernière version du produit gratuit PostgreSQL (le serveur PostgreSQL et le pilote ODBC correspondant, si c'est nécessaire) ou, au moins, n'utilisez pas une version plus ancienne que **8.4** ou 11.4.1 pour Postgres Pro.
2. Créez la base de données PostgreSQL d'une des façons suivantes :
   a) Avec l'interface graphique `pgAdmin`.
   b) Avec la commande SQL `CREATE DATABASE`.

La base doit être créée dans le codage UTF8.

Pour migrer vers la BD externe, consultez le paragraphe Changement du type de la BD Dr.Web Enterprise Security Suite.

Notez également les pré-requis système pour le Serveur Dr.Web lors du travail avec la base de données externe PostgreSQL (voir le **Manuel d'installation**, p. Pré-requis système).

Paramètres

Lors de la configuration de la connexion à la BD PostgreSQL, les paramètres décrits dans le tableau **A-4** sont utilisés.

Tableau A-4. PostgreSQL

Nom	Valeur par défaut	Description
`host`	*<Socket local UNIX>*	Hôte du Serveur PostgreSQL
`port`		Port du Serveur PostgreSQL ou extension du nom de fichier du socket
`dbname`	`drwcs`	Nom de la base de données
`user`	`drwcs`	Nom d'utilisateur
`password`	`drwcs`	Mot de passe
`options`		Options de débogage/traçage à envoyer au Serveur
`requiressl`		• 1 pour la demande de connexion SSL • 0 pour ne pas demander
`temp_tablespaces`		Nom de l'espace pour les tableaux temporaires
`default_transaction_isolation`		Mode d'isolation de la transaction (voir la documentation PostgreSQL)

Pour plus d'information technique, visitez le lien https://www.postgresql.org/docs/.

Interaction entre le Serveur Dr.Web et la BD PostgreSQL via UDS

Lors de l'installation du Serveur Dr.Web et de la BD PostgreSQL sur la même machine, leur interaction peut être configurée via UDS (socket du domaine UNIX).

Pour configurer le fonctionnement via UDS

1. Dans le fichier de configuration de la BD PostgreSQL `postgresql.conf`, indiquez le dossier suivant pour UDS :

   ```
   unix_socket_directory = '/var/run/postgresql'
   ```

2. Redémarrez PostgreSQL.

Configuration de la base de données PostgreSQL

Pour augmenter les performances lors de la gestion de la base de données, il est recommandé d'effectuer la configuration basée sur les informations reçues des manuels officiels sur la base de données.

En cas d'utilisation d'une base de données de grande taille et en cas de disponibilité des ressources de calculs correspondants, il est recommandé de configurer les paramètres suivants dans le fichier de configuration `postgresql.conf` :

Configuration minimale :

```
shared_buffers = 256Mo

temp_buffers = 64Mo

work_mem = 16Mo
```

Configuration avancée :

```
shared_buffers = 1Go

temp_buffers = 128Mo

work_mem = 32Mo

fsync = off

synchronous_commit = off

wal_sync_method = fdatasync

commit_delay = 1000

max_locks_per_transaction = 256

max_pred_locks_per_transaction = 256
```

Le paramètre `fsync = off` augmente considérablement les performances, pourtant cela peut amener à la perte complète des données en cas de coupure de courant ou d'échec du système. Il est recommandé de désactiver le paramètre `fsync` uniquement s'il y a une copie de sauvegarde de la base de données pour pouvoir la restaurer complètement.

La configuration du paramètre `max_locks_per_transaction` peut être utile pour l'assurance de travail continu en cas d'appel de masse aux tables de la base de données, notamment en cas de la mise à niveau de la base de données.

A4. Utilisation du SGBD MySQL

Généralités

MySQL est un SGBD libre, multiplateforme et relationnel. MySQL peut être utilisé en tant que base de données externe pour Dr.Web Enterprise Security Suite.

Pour utiliser MySQL en tant que BD externe

1. Installer le Serveur MySQL.
2. Configurer le Serveur Dr.Web conformément à l'utilisation de la base externe. Ceci peut être effectué dans le fichier de configuration ou via le Centre de gestion : dans le menu **Configuration du Serveur Dr.Web**, dans l'onglet **Base de données**.

Installation et versions supportées

Dr.Web Enterprise Security Suite supporte les versions suivantes du SGBD MySQL :

- MySQL : toutes les versions, à commencer par 8.0.12,

> ⚠ Assurez-vous que le type d'authentification correspond à caching_sha2_password pour l'utilisateur par lequel la connexion à MySQL en version 8.X est établie. Ce paramètre est spécifié lors de l'installation et devient le paramètre par défaut pour chaque utilisateur ou bien, il doit être configuré manuellement pour chaque utilisateur.

- MariaDB — 10.2.2, 10.3, 10.4.

Après l'installation du SGBD, avant la création d'une nouvelle base de données, il est nécessaire de spécifier les paramètres suivants dans le fichier de configuration (pour en savoir plus, consultez la documentation de votre SGBD) :

Pour MySQL en versions 8.X :

```
[mysqld]

innodb_file_per_table = true

max_allowed_packet = 64M
```

Si la version du SGBD MariaDB est plus ancienne que 10.2.4, il faut indiquer le suivant dans le fichier de configuration :

```
binlog_format = mixed
```

Paramètres

Lors de la configuration de la connexion au SGBD MySQL, les paramètres décrits dans le tableau **A-5** sont utilisés.

Tableau A-5. Paramètres du SGBD MySQL

Nom	Valeur par défaut	Description
HOST	localhost	• En cas de connexion à la base de données via TCP/IP — adresse du serveur de la base de données. • En cas d'utilisation d'UDS — chemin d'accès au fichier de socket UNIX. Si le chemin n'est pas spécifié, le Serveur Dr.Web essaie de trouver le fichier dans les répertoires standard de mysqld.
PORT	3306	• En cas de connexion à la base de données via TCP/IP — numéro de port pour la connexion à la base de données. • En cas d'utilisation d'UDS — nom du fichier de socket UNIX.
DBNAME		Nom de la base de données
USER		Nom d'utilisateur de la base de données
PASSWORD	QUICK	Mot de passe d'utilisateur de la base de données
PRECOMPILEDCACHE	1048576	Taille du cache des opérateurs sql précompilés en octets
SSL	NO	N'utiliser que les connexions SSL : • YES : se connecter à la base de données à condition que le protocole SSL soit utilisé, • NO : le protocole SSL n'est pas obligatoire lors de la connexion à la base de données.

Annexe B. Authentification des administrateurs

> Vous pouvez consulter les informations standard sur l'authentification des administrateurs sur le Serveur Dr.Web dans le **Manuel Administrateur**, p. Authentification des administrateurs.

B1. Authentification via Active Directory

Seuls l'autorisation d'utilisation et l'ordre dans la liste des authentificateurs doivent être configurés : balises `<enabled/>` et `<order/>` dans `auth-ads.conf`.

Principe de fonctionnement :

1. L'administrateur définit le nom d'utilisateur et le mot de passe à l'un des formats suivants :
   - `username`,
   - `domain\username`,
   - `username@domain`,
   - LDAP DN de l'utilisateur.
2. Le Serveur Dr.Web s'enregistre sur le contrôleur de domaine par défaut avec ce nom d'utilisateur et ce mot de passe (ou sur un contrôleur de domaine pour le domaine spécifié dans le nom d'utilisateur).
3. En cas d'authentification échouée, le mécanisme d'authentification suivant sera essayé.
4. Puis LDAP DN de l'utilisateur enregistré sera déterminé.
5. L'attribut `DrWebAdmin` est lu depuis l'objet ayant le DN déterminé. Si l'attribut prend la valeur `FALSE`, la tentative est considérée comme échouée et le mécanisme d'authentification suivant sera appliqué.
6. Si lors de cette étape, certains attributs ne sont pas déterminés, ils seront recherchés dans les groupes dont l'utilisateur fait partie. Les groupes parent de chaque groupe seront vérifiés (stratégie de recherche — en profondeur).

> En cas de n'importe quel erreur, le mécanisme d'authentification suivant sera appliqué.

L'utilitaire `drweb-<version_du_package>-<assemblage>-esuite-modify-ad-schema-<version_de_l'OS>.exe` (fourni séparément du package d'installation du Serveur Dr.Web) crée une nouvelle classe d'objets `DrWebEnterpriseUser` pour Active Directory et décrit de nouveaux attributs pour cette classe.

Dans l'espace Enterprise, les attributs ont les OID suivants :

```
DrWeb_enterprise_OID "1.3.6.1.4.1" // iso.org.dod.internet.private.enterprise
DrWeb_DrWeb_OID DrWeb_enterprise_OID ".29690" // DrWeb
DrWeb_EnterpriseSuite_OID DrWeb_DrWeb_OID ".1" // EnterpriseSuite
DrWeb_Alerts_OID DrWeb_EnterpriseSuite_OID ".1" // Alerts
DrWeb_Vars_OID DrWeb_EnterpriseSuite_OID ".2" // Vars
DrWeb_AdminAttrs_OID DrWeb_EnterpriseSuite_OID ".3" // AdminAttrs

// 1.3.6.1.4.1.29690.1.3.1 (AKA
iso.org.dod.internet.private.enterprise.DrWeb.EnterpriseSuite.AdminAttrs.Admin)

DrWeb_Admin_OID DrWeb_AdminAttrs_OID ".1" // R/W admin
DrWeb_AdminReadOnly_OID DrWeb_AdminAttrs_OID ".2" // R/O admin
DrWeb_AdminGroupOnly_OID DrWeb_AdminAttrs_OID ".3" // Group admin
DrWeb_AdminGroup_OID DrWeb_AdminAttrs_OID ".4" // Admin's group
DrWeb_Admin_AttrName "DrWebAdmin"
DrWeb_AdminReadOnly_AttrName "DrWebAdminReadOnly"
DrWeb_AdminGroupOnly_AttrName "DrWebAdminGroupOnly"
DrWeb_AdminGroup_AttrName "DrWebAdminGroup"
```

La modification des propriétés des utilisateurs d'Active Directory se fait manuellement sur le serveur Active Directory (voir le **Manuel Administrateur**, p. Authentification des administrateurs).

Assigner des droits aux administrateurs se fait selon le principe général d'héritage dans la structure hiérarchique des groupes auxquels appartient l'administrateur.

B2. Authentification via LDAP

Les paramètres sont écrits dans le fichier de configuration `auth-ldap.conf`.

Les balises principales du fichier de configuration :

- `<enabled/>` et `<order/>` — comme dans le cas d'Active Directory.
- `<server/>` spécifie l'adresse du serveur LDAP. Il est possible d'indiquer plusieurs balises `<server/>` avec les adresses de serveurs LDAP différents. Ainsi, une liste de serveurs depuis lesquels on peut s'authentifier sera créée. L'adresse du serveur principal qui assumera la charge essentielle doit être indiqué en premier. Ensuite, vous pouvez indiquer les adresses de serveurs en réserve. En cas de connexion de l'administrateur, le premier serveur LDAP disponible est utilisé. En cas d'échec, l'authentification aura lieu sur le serveur suivant et, ensuite, dans l'ordre dans lequel les adresses des serveurs LDAP sont indiquées dans le fichier de configuration.
- `<user-dn/>` détermine les règles de transformation des noms vers DN à l'aide des masque de type DOS.

  La balise `<user-dn/>` permet d'utiliser les caractères de substitution :

  - `*` remplace une séquence de n'importe quels caractères sauf `. , = @ \` et des espaces ;
  - `#` remplace une séquence de n'importe quels caractères.
- `<user-dn-expr/>` détermine les règles de transformation des noms vers DN à l'aide des expressions régulières.

  Pour l'exemple, la même règle dans deux variantes :

```
<user-dn user="*@example.com" dn="CN=\1,DC=example,DC=com"/>
<user-dn-expr user="(.*)@example.com" dn="CN=\1,DC=example,DC=com"/>
```

`\1` .. `\9` déterminent la place de substitution dans le modèle des valeurs *, # ou des expressions entre parenthèses.

Selon ce principe, si le nom d'utilisateur est spécifié au format `login@example.com`, après la traduction, le DN a le format suivant : "`CN=login,DC=example,DC=com`".

- `<user-dn-extension-enabled/>` autorise l'exécution du script Lua `ldap-user-dn-translate.ds` (depuis le dossier `extensions`) pour traduire le nom d'utilisateur en DN. Ce script est exécuté après les tentatives d'appliquer toutes les règles `user-dn`, `user-dn-expr` ou si aucune règle correspondante n'est trouvée. Le script a un seul paramètre – le nom d'utilisateur saisi. Le script retourne la ligne contenant DN, sinon il retourne la ligne vide. Si aucune règle ne correspond et que le script n'est pas autorisé ou qu'il n'a rien retourné, le nom d'utilisateur saisi sera utilisé tel qu'il est.
- L'attribut de l'objet LDAP pour DN reçu suite à la transformation et ses valeurs possibles peuvent être remplacés à l'aide de la balise suivante (les valeurs par défaut sont indiquées) :

```
 <!-- DrWebAdmin attribute equivalent (OID 1.3.6.1.4.1.29690.1.3.1) -->
 <admin-attribute-name value="DrWebAdmin" true-value="^TRUE$" false-
value="^FALSE$"/>
```

  En tant que les valeurs de paramètres `true-value`/`false-value` des expressions régulières sont spécifiées.
- S'il reste des valeurs des attributs de l'administrateur non déterminées et que dans le fichier de configuration, la balise `<group-reference-attribute-name value="memberOf"/>` est spécifiée, la valeur de l'attribut `memberOf` sera comprise comme une liste de DN des groupes dont l'administrateur fait partie. Dans ce cas, la recherche des attributs nécessaires sera effectuée par groupes tout comme c'est le cas d'Active Directory.

B3. Authentification via LDAP/AD

Fichier de configuration

Les paramètres sont écrits dans le fichier de configuration `auth-ldap-rfc4515.conf`.

Les fichiers de configuration avec les paramètres standard sont également fournis :

- `auth-ldap-rfc4515-check-group.conf` : modèle du fichier de configuration pour l'authentification externe des administrateurs via LDAP selon le schéma simplifié avec la vérification d'appartenance au groupe Active Directory.
- `auth-ldap-rfc4515-check-group-novar.conf` : modèle du fichier de configuration pour l'authentification externe des administrateurs via LDAP selon le schéma simplifié avec la vérification d'appartenance au groupe Active Directory avec l'utilisation des variables.
- `auth-ldap-rfc4515-simple-login.conf` : modèle du fichier de configuration pour l'authentification externe des administrateurs via LDAP selon le schéma simplifié.

Balises principales du fichier de configuration auth-ldap-rfc4515.conf :

- `<server />` : détermination du serveur LDAP.

Attribut	Description	Valeur par défaut
`base-dn`	DN de l'objet par rapport auquel la recherché est effectuée.	Valeur de l'attribut `rootDomainNamingContext` de l'objet `Root DSE`
`cacertfile`	Fichier des certificats racine (uniquement UNIX).	–
`host`	Adresse du serveur LDAP.	• Contrôleur de domaine pour un serveurs sous Windows. • `127.0.0.1` pour un serveur sous les OS de la famille UNIX. • Il est possible d'indiquer plusieurs balises `<server />` avec les adresses de serveurs LDAP différents. L'adresse du serveur principal qui assumera la charge essentielle doit être indiqué en premier. En cas d'échec, l'authentification aura lieu sur le serveur suivant et, ensuite, dans l'ordre indiqué.
`scope`	Zone de recherche. Valeurs autorisées : • `sub-tree` : toute la zone au-dessous de DN de base, • `one-level` : descendants directs de DN de base, • `base` : DN de base.	`sub-tree`
`tls`	Établir TLS pour la connexion à LDAP.	`no`
`ssl`	Utiliser le protocole LDAPS lors de la connexion à LDAP.	`no`

- `<set />` : spécifier les variables par la recherche dans LDAP.

Attribut	Description	Valeur par défaut
`attribute`	Nom de l'attribut dont la valeur est attribuée à la variable. Il ne peut pas être absent.	–
`filter`	Filtre RFC4515 de recherche dans LDAP.	–

Attribut	Description	Valeur par défaut
scope	Zone de recherche. Valeurs autorisées : • sub-tree : toute la zone au-dessous de DN de base, • one-level : descendants directs de DN de base, • base : DN de base.	sub-tree
search	DN de l'objet par rapport auquel la recherché est effectuée.	En cas d'absence base-dn de la balise <server /> est utilisé
variable	Nom de variable. Il doit commencer par une lettre et ne contenir que des lettres et des chiffres. Il ne peut pas être absent.	–

Les variables peuvent être utilisées dans les valeurs de l'attribut add des balises <mask /> et <expr />, dans la valeur de l'attribut value de la balise <filter /> sous forme de \varname, et dans la valeur de l'attribut search de la balise <set />. Le niveau maximal autorisée de la récursivité dans les variables est 16.

Si la recherche retourne plusieurs objets trouvés, c'est seulement le premier qui est utilisé.

- <mask /> : modèles de nom d'utilisateur.

Attribut	Description
add	Ligne ajoutée au filtre de recherche utilisant l'opération ET avec des éléments de substitution.
user	Masque du nom de l'utilisateur avec l'utilisation des métacaractères de type DOS * et #. Il ne peut pas être absent.

Exemple :

```
<mask user="*@#"  add="sAMAccountName=\1" />

<mask user="*\*"  add="sAMAccountName=\2" />
```

\1 et \2 : liens vers les masques correspondants dans l'attribut user.

- <expr /> : modèles de nom d'utilisateur avec l'utilisation des expressions régulières (les attributs sont équivalents <mask />).

Exemple :

```
<expr user="^(.*)@([^.,=@\s\\]+)$"  add="sAMAccountName=\1" />

<expr user="^(.*)\\(.*)"            add="sAMAccountName=\2" />
```

Correspondance des masques et des expressions régulières :

Masque	Expression régulière
*	.*
#	[^.,=@\s\\]+

- `<filter />` : filtre de recherche dans LDAP.

Attribut	Description
value	Ligne ajoutée au filtre de recherche utilisant l'opération ET avec des éléments de substitution.

Concaténation de filtres

```
<set variable="admingrp"  filter="&amp;(objectclass=group)(cn=ESuite Admin)"
attribute="dn" />
<mask user="*\*" add="sAMAccountName=\2" />
<filter value="&amp;(objectClass=user)(memberOf=\admingrp)" />
```

Si suite à la recherche `admingrp` prend la valeur "`CN=ESuite Admins,OU=some name,DC=example,DC=com`", et l'utilisateur a saisi `domain\user`, vous aurez le filtre suivant :

```
"(&(sAMAccountName=user)(&(objectClass=user)(memberOf=CN=ESuite
Admins,OU=some name,DC=example,DC=com)))"
```

Exemple de la configuration de l'authentification LDAP/AD

Vous trouverez ci-dessous l'exemple de configuration de base pour l'authentification avec LDAP. Les paramètres sont spécifiés dans le Centre de gestion, la section **Administration** → **Authentification** → **Authentification LDAP/AD** (pour le mode **Paramètres simplifiés**).

Les paramètres initiaux des administrateur qui doivent s'authentifier :

- domaine : `dc.test.local`
- groupe dans Active Directory : `DrWeb_Admins`

Paramètres du Centre de gestion :

Nom du paramètre		Valeur
Type du serveur		Microsoft Active Directory
Adresse du serveur		dc.test.local
Modèles de noms d'utilisateurs pour la confirmation de	Masque du compte	test* ou *@test.local

Nom du paramètre		Valeur
l'authentification	Nom d'utilisateur	\1
Appartenance d'utilisateurs pour la confirmation de l'authentification	Nom	DrWeb_Admins
	Type	groupe

B4. Sections de droits dépendantes

Tableau B-1. Liste des droits administrateurs et leurs particularités

Code	Droit	Description	Rubrique du Centre de gestion
Gestion des groupes de postes			
1*	**Voir les propriétés des groupes de postes**	Liste des groupes utilisateur que l'administrateur voit dans le réseau antivirus. Tous les groupes système sont affichés dans l'arborescence, mais on y voit uniquement les postes de la liste indiquée des groupes utilisateur. Si le droit est accordé à certains groupes et non pas à tout le réseau antivirus, l'élément du menu **Administration** → **Configurations** → **Installation via le réseau** ne sera pas disponible.	Réseau antivirus Réseau antivirus → Général → Propriétés
2*	**Modifier les propriétés des groupes de postes**	Liste des groupes utilisateur, dont les propriétés peuvent être éditées par l'administrateur. Doit contenir des groupes de la liste du droit 1.	
3	**Voir la configuration des groupes de postes**	Liste des groupes utilisateur, dont la configuration et visible pour l'administrateur. L'administrateur peut également consulter la configuration des postes sur lesquels les postes de la liste sont primaires.	Réseau antivirus Réseau antivirus → Général → Composants en cours d'exécution Réseau antivirus → Général → Quarantaine

Code	Droit	Description	Rubrique du Centre de gestion
		Doit contenir des groupes de la liste du droit 1.	Pages de la rubrique **Configuration** du menu de gestion
4	**Éditer la configuration des groupes de postes**	De la même manière que le droit 3, mais avec la possibilité d'édition. Doit contenir des groupes de la liste du droit 3.	
5	**Voir les propriétés des postes**	Liste des groupes utilisateur qui sont primaires pour les postes, dont les propriétés sont visibles pour l'administrateur. Doit contenir des groupes de la liste du droit 1.	Réseau antivirus Réseau antivirus → Général → Propriétés
6	**Modifier les propriétés des postes**	Y compris ACL, blocage, accès, etc. De la même manière que le droit 5, mais avec la possibilité d'édition. Doit contenir des groupes de la liste du droit 5.	
8*	**Placer des postes dans des groupes et retirer des postes des groupes**	Liste des groupes utilisateur. Doit contenir des groupes de la liste du droit 1.	Réseau antivirus
9	**Suppression de postes**	Liste des groupes utilisateur qui sont primaires pour les postes que l'administrateur peut supprimer. Doit contenir des groupes de la liste du droit 1.	
10	**Installation et désinstallation des Agents à distance**	Liste des groupes utilisateurs sur les postes depuis lesquels l'administrateur peut lancer l'installation distante des Agents Dr.Web avec les ID sélectionnés. Ces groupes doivent être primaires pour les postes installés. Doit contenir des groupes de la liste du droit 1.	

Code	Droit	Description	Rubrique du Centre de gestion
		L'élément du menu n'est pas affiché s'il y a des objets interdits. L'installation réseau est possible depuis le fichier /esuite/network/index.ds uniquement si le droit 16 est accordé.	
11	**Fusionner des postes**	Liste des groupes utilisateur dont les postes peuvent être fusionnés. Ces groupes doivent être primaires pour les postes. L'icône de fusion des postes est disponible dans la barre d'outils. Doit contenir des groupes de la liste du droit 1.	
12*	**Voir les tableaux statistiques**	Liste des groupes utilisateur dont les statistiques sont disponibles à l'administrateur. Le droit donne la possibilité de créer la tâche de réception des rapports périodiques dans la planification du Serveur Dr.Web. La liste des groupes utilisateur que l'administrateur peut mentionner dans cette tâche (groupes, pour les postes desquels les rapports seront reçus) est spécifiée. Si le groupe Everyone est spécifié, vous recevrez les rapports sur tous les groupes de la liste. Doit contenir des groupes de la liste du droit 1.	Réseau antivirus pages de la rubrique **Statistiques** du menu de gestion
23	**Modifier la gestion des licences**	Liste des groupes utilisateur pour lesquels l'administrateur peut ajouter/remplacer/supprimer la clé de licence. Ces groupes doivent être primaires pour les postes. Doit contenir des groupes de la liste du droit 1.	Réseau antivirus → Configuration → Clés de licence
40	**Lancer et arrêter les composants**	Lancer et arrêter les composants installés sur le poste.	Réseau antivirus → Configuration → Droits

Code	Droit	Description	Rubrique du Centre de gestion
48	**Consulter les rapports pour le support technique**	Création et affichage des journaux système des composants de protection installés sur le poste.	Réseau antivirus → Général → Rapports pour le support technique
Gestion par les administrateurs			
18	**Voir la planification du Serveur Dr.Web**	Voir le tableau **Journal d'exécution des tâches**. Vous pouvez consulter les tâches créées par l'administrateur et les administrateurs du groupe sélectionné. Si les droits 12 et 18 ne sont pas accordés, la consultation de la page de planification du Serveur Dr.Web est interdite. Si le droit 12 est accordé mais pas le droit 18, la consultation de la planification des statistiques est disponible. La tâche d'envoi de rapports pour l'administrateur s'affiche selon la présence du droit 12 et de la notification **Rapport périodique**, même si le droit 18 n'est pas accordé.	Administration → Configuration → Planificateur de Tâches du Serveur Dr.Web Administration →Journaux → Journal d'exécution des tâches
19	**Éditer la planification du Serveur Dr.Web**	Vous pouvez modifier les tâches créées par l'administrateur et les administrateurs du groupe sélectionné.	Administration → Configuration → Planificateur de Tâches du Serveur Dr.Web
24	**Modifier la configuration des notifications**		Administration → Notifications → Configuration des notifications Administration → Notifications → Notifications non envoyées Administration → Notifications → Notifications de la console web

Code	Droit	Description	Rubrique du Centre de gestion
25	**Créer des administrateurs, des groupes administrateurs**	L'icône correspondante dans la barre d'outils est masquée.	Administration → Configuration → Administrateurs
26	**Modifier des comptes administrateurs**	L'administrateur du groupe **Newbies** voit l'arborescence dont la racine est le groupe dont il fait partie. C'est-à-dire, il voit les administrateurs de son groupe et de ses sous-groupes. L'administrateur du groupe **Administrators** voit tous les administrateurs indépendamment de leurs groupes. L'administrateur peut éditer les comptes des administrateurs des groupes indiqués. Dans ce cas, l'icône correspondante devient disponible dans la barre d'outils.	
27	**Supprimer des comptes administrateurs**	De la même manière que le droit 26.	
28	**Voir les propriétés et la configuration des groupes administrateurs**	Y compris les administrateurs dans les groupes et les sous-groupes. L'administrateur peut sélectionner uniquement depuis le sous-groupe de son propre groupe parent.	
29	**Modifier les propriétés et la configuration des groupes administrateurs**	Y compris les administrateurs dans les groupes et les sous-groupes. L'administrateur peut sélectionner uniquement depuis le sous-groupe de son propre groupe parent. Si ce droit est refusé, même si le droit 26 est accordé pour ce groupe, l'administrateur ne peut pas désactiver l'héritage et élever les droits de l'administrateur dans le groupe.	

Code	Droit	Description	Rubrique du Centre de gestion
39	**Affichage du groupe d'administrateurs « Newbies »**	Autoriser l'administrateur à voir le groupe prédéfini **Newbies** dans l'arborescence des administrateurs. Si l'administrateur n'a pas le droit de consulter le groupe **Newbies** et qu'il se trouve dans ce groupe, il ne verra que lui-même.	
41	**Éditer les notifications administrateur**	Édition de la configuration des notifications d'administrateurs.	
Avancé			
7	**Créer des postes**	Lors de la création d'un poste, seule la liste de groupes ayant le droit 8 est disponible (le groupe dans lequel les postes sont placés doivent avoir le droit 8). Lors de la création d'un poste, un des groupes utilisateur disponibles doit devenir primaire.	Réseau antivirus
13	**Voir l'audit**	L'audit est accessible à l'administrateur ayant les plein-droits et aux objets possédant le droit 4.	Administration → Journaux → Journal d'audit
16	**Lancer le Scanner réseau**	Si le droit n'est pas accordé, l'installation par le réseau pour /esuite/network/index.ds n'est pas disponible.	Réseau antivirus Administration → Scanner réseaux
17	**Approuver des novices**	La liste des groupes du droit 8 est disponible. Ce droit ne peut pas être accordé si l'administrateur a l'autorisation de gérer certains groupes mais qu'il n'est pas autorisé à gérer tous les objets du réseau antivirus. Cela veut dire que pour le droit 1 (**Consulter les propriétés des groupes de postes**), l'ensemble de groupes est spécifié.	Réseau antivirus

Code	Droit	Description	Rubrique du Centre de gestion
20	**Voir la configuration du Serveur Dr.Web et la configuration du référentiel**		Administration → Configuration → Configuration du serveur web
21	**Éditer la configuration du Serveur Dr.Web et la configuration du référentiel**		Administration → Référentiel des produits → Statut du référentiel des produits Administration → Référentiel → Mises à jour reportées Administration → Référentiel → Configuration générale du référentiel Administration → Référentiel → Configuration détaillée du référentiel Administration → Référentiel → Contenu du référentiel Administration → Journaux → Journal des mises à jour du référentiel Administration → Configuration → Procédures utilisateur Administration → Serveur Dr.Web → Liste des versions
22	**Voir les données sur la licence**		Administration → Administration → Gestionnaire de licences
30	**Opération via Web API**		-

Code	Droit	Description	Rubrique du Centre de gestion
31	**Voir les liaisons voisines**		Liaisons
32	**Modifier les connexion voisines**		Liaisons
33	**Utiliser des fonctionnalités supplémentaires**	Limite l'accès à toutes les rubriques de la section **Options supplémentaires**, sauf la rubrique **Utilitaires** qui est toujours disponible.	Administration → Options supplémentaires
34	**Mettre à jour le référentiel**	Mise à jour du référentiel du Serveur Dr.Web depuis le SGM.	Bouton **Mettre à jour le référentiel** dans la rubrique **Statut du référentiel**
42	**Modifier vos propres paramètres**	Droit de modifier les paramètres personnels du compte administrateur.	Administration → Configuration → Administrateurs
43	**Consulter les Serveurs proxy Dr.Web**	Droit de consulter les paramètres des Serveurs proxy Dr.Web (si l'affichage est désactivé, l'édition se désactive automatiquement).	Réseau antivirus → Proxy
44	**Modifier les Serveurs proxy Dr.Web**	Droit de modifier les paramètres des Serveurs proxy Dr.Web.	Réseau antivirus → Proxy
45	**Voir les propriétés et la configuration des politiques**	Si l'affichage est désactivé, l'édition se désactive automatiquement.	Réseau antivirus → Politiques
46	**Éditer les propriétés et la configuration des politiques**		Réseau antivirus → Politiques
47	**Éditer les règles d'appartenance**	Droit de modifier les règles d'appartenance des groupes utilisateur.	Réseau antivirus

* Les droits 1, 2, 8, 12 sont déterminés pour un poste selon la liste des groupes auxquels il fait partie et pas selon le groupe primaire du poste.

Si un poste fait partie d'un groupe et quelques-uns de ces droits sont accordés à ce groupe, l'ensemble de fonctions correspondant à ces droits sera disponible pour l'administrateur, peu importe si le groupe autorisé est primaire pour le poste ou non. Dans ce cas, l'autorisation est

prioritaire : si un poste fait partie d'un groupe autorisé et interdit en même temps, les fonctionnalités correspondant aux droits du groupe autorisé sera disponible pour l'administrateur.

Annexe C. Système de notification

Vous pouvez consulter les informations standard sur la configuration des notifications de l'administrateur dans le **Manuel Administrateur**, p. Configuration des notifications.

C1. Descriptions des paramètres du système de notifications

Le système de notification des événements liés au fonctionnement des composants du réseau antivirus utilise les types suivants d'envoi des notifications :

- notifications par e-mail,
- notifications via la console web,
- notifications via SNMP,
- notifications via le protocole de l'Agent Dr.Web,
- notifications push,
- notifications via le protocole Syslog.

En fonction du mode de notifications, les jeux de paramètres différents au format clé → valeur sont requis. Pour chaque mode, les paramètres suivants sont spécifiés :

Tableau C-1. Paramètres généraux

Paramètre	Description	Valeur par défaut	Obligatoire
`TO`	Plusieurs destinataires de notifications séparés par le symbole |		oui
`ENABLED`	Activer ou désactiver les notifications	`true` ou `false`	oui
`_TIME_TO_LIVE`	Nombre de tentatives d'envoi en cas d'envoi échoué	10 tentatives	non
`_TRY_PERIOD`	Délai en secondes entre deux tentatives d'envoi de notification	5 min, (l'envoi s'effectue une seule fois pour 5 minutes)	non

Les tableaux avec les listes des paramètres pour les modes d'envoi différents sont disponibles ci-dessous.

Tableau C-2. Notifications par e-mail

Paramètre	Description	Valeur par défaut
FROM	Adresse e-mail de l'expéditeur	drwcsd@${nom de l'hôte}
TO	Adresses e-mail de destinataires	-
HOST	Adresse du serveur SMTP	127.0.0.1
PORT	Numéro du port du Serveur SMTP	• 25, si le paramètre SSL prend la valeur no • 465, si le paramètre SSL prend la valeur yes
USER	Utilisateur du serveur SMTP	"" si l'utilisateur est spécifié, il est nécessaire d'activer au moins un mode d'autorisation, sinon les e-mails ne seront pas transmis.
PASS	Mot de passe de l'utilisateur du serveur SMTP	""
STARTTLS	Pour l'échange chiffré de données. Dans ce cas, le passage à la connexion sécurisée s'effectue via la commande STARTTLS. L'utilisation du port 25 pour la connexion est prévue par défaut.	yes
SSL	Pour l'échange chiffré de données. Dans ce cas, une connexion TLS sécurisée sera ouverte à part. L'utilisation du port 465 pour la connexion est prévue par défaut.	no
AUTH-CRAM-MD5	Utiliser l'authentification CRAM-MD5	no
AUTH-PLAIN	Utiliser l'authentification PLAIN	no
AUTH-LOGIN	Utiliser l'authentification LOGIN	no
AUTH-NTLM	Utiliser l'authentification NTLM	no
SSL-VERIFYCERT	Vérifier la correction du certificat du serveur SSL	no

Paramètre	Description	Valeur par défaut
DEBUG	Activer le mode de débogage, par exemple pour analyser la situation avec l'autorisation impossible	-

Tableau C-3. Notifications via la console Web

Paramètre	Description	Valeur par défaut
TO	UUID des administrateurs à qui ce message sera envoyé	-
SHOW_PERIOD	Délai de conservation du message en secondes, à commencer par le moment de réception du message	86400 secondes, c'est-à-dire un jour.

Tableau C-4. Notifications via SNMP

Paramètre	Description	Valeur par défaut
TO	Entité de réception SNMP, par exemple, l'adresse IP	-
DOMAIN	Domaine	• `localhost` sous OS Windows, • "" : pour les OS de la famille UNIX.
COMMUNITY	généralité SNMP ou contexte	`public`
RETRIES	Nombre de tentatives d'envoi de la notification, effectuées par API	5 tentatives
TIMEOUT	Délai en secondes, après lequel API va tenter d'envoyer la notification encore une fois	5 secondes

Tableau C-5. Notifications via le protocole de l'Agent

Paramètre	Description	Valeur par défaut
TO	UUID des postes de réception	-
SHOW_PERIOD	Délai de conservation du message en secondes, à commencer par le moment de réception du message	86400 secondes, c'est-à-dire un jour.

Tableau C-6. Notifications Push

Paramètre	Description	Valeur par défaut
TO	Les jetons d'authentifications que les applications reçoivent au moment de l'enregistrement sur le serveur de l'éditeur, par exemple Apple	-
SERVER_URL	URL du serveur relay via lequel les notifications sont envoyées sur le serveur de l'éditeur	-

Tableau C-7. Notifications via le protocole Syslog

Paramètre	Description	Valeur par défaut
TO	Adresse du destinataire de la notification via le protocole Syslog. Protocole de transmission TCP ou UDP.	UDP, port 514
FORMAT	Format de notification : RFC 5424 ou CEF (Common Event Format).	RFC 5424
TIMEOUT	Délai en secondes pendant lequel le Serveur Dr.Web tente de se connecter au destinataire de la notification via le protocole TCP.	5 s
FACILITY	Catégorie du processus qui a généré la notification (par exemple, le moteur, le système de messagerie). Elle peut prendre les valeurs de 0 à 23.	14
HOSTNAME	Expéditeur. Identificateur du Serveur Dr.Web (nom de domaine complet, nom d'hôte, adresse IP).	-

C2. Paramètres des modèles de notifications

Les textes de messages sont générés depuis les fichiers de modèles par un composant du Serveur Dr.Web appelé processeur de modèles.

Le système de notifications via le réseau Windows fonctionne uniquement sous OS Windows supportant le service Windows Messenger (Net Send).

Windows Vista et les versions supérieures ne supportent pas le service Windows Messenger.

Le fichier de modèle comprend un texte et des variables entre accolades. Lors de l'édition des fichiers de modèles, utilisez les variables listées ci-dessous.

Les variables sont écrites sous un des formats suivants :

- {<*VAR*>} : mettre la valeur de la variable <*VAR*>.
- {<*VAR*>:<*N*>} : les <*N*> premiers caractères de la variable <*VAR*>.
- {<*VAR*>:<*first*>:<*N*>} – <*N*> caractères de la variable <*VAR*> suivante après les <*first*> premiers caractères (à partir du <*first*>+1er caractère), si le reste est inférieur à ce nombre, il est complété par des espaces à droite.
- {<*VAR*>:<*first*>:-<*N*>} – <*N*> caractères de la variable <*VAR*>, suivante après les <*first*> premiers caractères (à partir du <*first*>+1er caractère), si le reste est inférieur à ce nombre, il est complété par des espaces à gauche.
- {<*VAR*>/<*original1*>/<*replace1*>[/<*original2*>/<*replace2*>]} – les caractères spécifiés seront remplacés par la valeur <*VAR*> *afin d'attribuer les valeurs données* : les symboles <*original1*> seront remplacés par les symboles <*replace1*>, si les symboles <*original2*> sont présents, ils seront remplacés par les symboles <*replace2*> etc.

  Le nombre de paires de substitution est illimité.
- {<*VAR*>/<*original1*>/<*replace1*[{<*SUB_VAR*>}]>[/<*original2*>/<*replace2*>]} : équivalent aux remplacements par les valeurs spécifiées décrits ci-dessus mais avec l'utilisation de la valeur intégrée <*SUB_VAR*>. Les actions avec les valeurs intégrées sont équivalentes à toutes les actions avec les valeurs parent.

  La profondeur d'imbrication en cas de substitutions récursives est illimitée.
- {<*VAR*>/<*original1*>/<*replace1*>/<*original2*>/<*replace2*>/*/<*replace3*>} : équivalent aux remplacements par les valeurs spécifiées décrits ce-dessus, mais la complétion par la valeur spécifiée dans <*replace3*>, est autorisée si aucune valeur initiale ne correspond. De plus, si dans <*VAR*>, il n'y a pas de <*original1*> ou <*original2*>, toutes les valeurs seront remplacées par <*replace3*>.

Tableau C-8. Format des variables

Variable	Valeur	Expression	Résultat
SYS.TIME	10:35:17:456	{SYS.TIME:5}	10:35
SYS.TIME	10:35:17:456	{SYS.TIME:3:5}	35:17
SYS.TIME	10:35:17:456	{SYS.TIME:3:-12}	°°°35:17:456
SYS.TIME	10:35:17:456	{SYS.TIME:3:12}	35:17:456°°°
SYS.TIME	10:35:17:456	{SYS.TIME/10/99/35/77}	99:77:17:456

Conventions

° : espace.

Variables d'environnement

Pour générer les textes de messages, vous pouvez utiliser les variables d'environnement du processus du Serveur Dr.Web (utilisateur **System**).

Les variables d'environnement sont disponibles dans l'éditeur de messages du Centre de gestion, dans la liste déroulante **ENV**. Notez qu'il est nécessaire d'indiquer les variables en ajoutant le préfixe `ENV.` (le préfixe se termine par un point).

Variables système

- `SYS.BRANCH` : version des Agents Dr.Web et du Serveur Dr.Web,
- `SYS.BUILD` : date de l'assemblage du Serveur Dr.Web,
- `SYS.DATE` : date système courante,
- `SYS.DATETIME` : date et heure système courantes,
- `SYS.HOST` : nom DNS du Serveur Dr.Web,
- `SYS.MACHINE` : adresse réseau de l'ordinateur avec le Serveur Dr.Web installé,
- `SYS.OS` : nom du système d'exploitation avec le Serveur Dr.Web installé,
- `SYS.PLATFORM` : plateforme du Serveur Dr.Web,
- `SYS.PLATFORM.SHORT` : variante abrégée de `SYS.PLATFORM`,
- `SYS.SERVER` : nom du produit (Dr.Web Server),
- `SYS.TIME` : heure système courante,
- `SYS.VERSION` : version du Serveur Dr.Web.

Variables communes pour les postes

- `GEN.LoginTime` : heure de connexion du poste,
- `GEN.StationAddress` : adresse du poste,
- `GEN.StationDescription` : description du poste,
- `GEN.StationID` : identificateur unique du poste,
- `GEN.StationLDAPDN` : nom unique (distinguished name) du poste sous Windows. Cela concerne les postes faisant partie du domaine ADS/LDAP,
- `GEN.StationMAC` : adresse MAC du poste,
- `GEN.StationName` : nom du poste,
- `GEN.StationPrimaryGroupID` : identificateur du groupe primaire du poste,
- `GEN.StationPrimaryGroupName` : nom du groupe primaire du poste,
- `GEN.StationSID` : identificateur de sécurité du poste.

Variables communes pour le référentiel

- `GEN.CurrentRevision` : identificateur courant de version,
- `GEN.Folder` : répertoire d'emplacement du produit,
- `GEN.NextRevision` : identificateur de la version mise à jour,
- `GEN.Product` : description du produit.

Paramètres et variables de notifications par types

Administrateurs

Administrateur inconnu

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée en cas de tentative d'authentification de l'administrateur au login inconnu dans le Centre de gestion.	
Configuration supplémentaire	N'est pas requise.	
Variables	`MSG.Login`	nom du compte
	`MSG.Address`	adresse réseau du Centre de gestion

Erreur d'authentification de l'administrateur

Paramètre	Valeur	
Raison de l'envoi de notification	En cas d'erreur d'authentification de l'administrateur dans le Centre de gestion. La raison de l'erreur est indiquée dans le texte de notification.	
Configuration supplémentaire	N'est pas requise.	
Variables	`MSG.Login`	nom du compte
	`MSG.Address`	adresse réseau du Centre de gestion
	`MSG.LoginErrorCode`	code numérique d'erreur

Autre

Erreur de rotation du journal du Serveur Dr.Web

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée en cas d'erreur survenue lors de rotation du journal de Serveur Dr.Web. La raison de l'erreur de rotation du journal est indiquée dans le texte de notification.	
Configuration supplémentaire	N'est pas requise.	
Variables	`MSG.Error`	texte d'erreur

Erreur d'écriture du journal du Serveur Dr.Web

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyé en cas d'erreur survenue lors de rotation du journal de Serveur Dr.Web. La raison de l'erreur de rotation du journal est indiquée dans le texte de notification.	
Configuration supplémentaire	N'est pas requise.	
Variables	`MSG.Error`	texte d'erreur

Épidémie sur le réseau

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée en cas de détection d'une épidémie du réseau antivirus. Cela signifie que le nombre de menaces détectés dans le réseau pendant le délai indiqué dépasse le nombre de menaces spécifié.	
Configuration supplémentaire	Pour envoyer une notification sur les épidémies, il faut cocher la case **Suivre les épidémies** dans la section **Administration** → **Configuration du Serveur Dr.Web** → **Configuration du Serveur Dr.Web** → **Statistiques**. Les paramètres de détermination de l'épidémie sont spécifiés dans la même section.	
Variables	`MSG.Infected`	nombre total de menaces détectées
	`MSG.Virus`	menaces les plus répandues

Le Serveur voisin Dr.Web n'a pas été connecté depuis longtemps

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée conformément à la tâche de planification du Serveur Dr.Web. Notifie que le Serveur voisin Dr.Web n'a pas été connecté depuis longtemps à ce Serveur Dr.Web. La date de la dernière connexion est mentionnée dans le texte de message.	
Configuration supplémentaire	La durée de la période lors de laquelle le Serveur voisin Dr.Web n'a pas été connecté. A l'issue de cette période une notification est envoyée. La durée est spécifiée dans la tâche **Le serveur voisin n'a pas été connecté depuis longtemps** dans la planification du Serveur Dr.Web configurée dans la rubrique **Administration** → **Planificateur de tâches du Serveur Dr.Web**.	
Variables	`MSG.LastDisconnectTime`	heure de la dernière connexion du Serveur Dr.Web
	`MSG.StationName`	nom du serveur voisin

Rapport statistique

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyé après la génération d'un rapport conformément à la tâche de planification du Serveur Dr.Web. En outre, dans la notification est indiqué le chemin par lequel on peut télécharger le fichier de rapport.	
Configuration supplémentaire	Le rapport est généré conformément à la tâche **Création d'un rapport statistique** dans la planification du Serveur Dr.Web configurée dans la section **Administration** → **Planificateur de tâches du Serveur Dr.Web**.	
Variables	`MSG.Attachment`	chemin vers le rapport
	`MSG.AttachmentType`	type MIME
	`GEN.File`	nom du fichier de rapport

Rapport sommaire de la protection préventive

Paramètre	Valeur
Raison d'envoi de la notification	Envoyée si un grand nombre de rapports est reçu des postes de réseau par le composant Protection préventive.

Paramètre	Valeur	
Configuration avancée	Pour envoyer une notification unique sur le rapport de la Protection préventive, il faut cocher la case **Grouper les rapports de la Protection préventive** dans la section **Administration → Configuration du Serveur Dr.Web → Configuration du Serveur Dr.Web → Statistiques**. Les paramètres de groupement des rapports sont spécifiés dans la même section.	
Variables	`MSG.AutoBlockedActCount`	nombre de processus ayant une activité suspecte bloqués automatiquement
	`MSG.AutoBlockedProc`	processus ayant une activité suspecte bloqué automatiquement
	`MSG.HipsType`	type de l'objet protégé
	`MSG.IsShellGuard`	division par types de réaction de la Protection préventive lors du blocage automatique : • blocage de l'exécution du code non autorisé • contrôle d'accès aux objets protégés
	`MSG.ShellGuardType`	la cause la plus répandue de blocage de l'exécution du code non autorisé lors du blocage automatique de l'événement
	`MSG.Total`	nombre total d'événements de Protection préventive enregistrés sur le réseau
	`MSG.UserAllowedActCount`	nombre de processus ayant une activité suspecte autorisés par l'utilisateur
	`MSG.UserAllowedHipsType`	type des objets le plus souvent protégés l'accès auxquels est autorisé par l'utilisateur
	`MSG.UserAllowedIsShellGuard`	division par types de réaction de la Protection préventive lors de l'autorisation de l'accès par l'utilisateur : • blocage de l'exécution du

Paramètre	Valeur	
		code non autorisé • contrôle d'accès aux objets protégés
	MSG.UserAllowedProc	processus ayant une activité suspecte autorisé par l'utilisateur
	MSG.UserAllowedShellGuard	la cause la plus répandue de blocage de l'exécution du code non autorisé lors de l'autorisation de l'événement par l'utilisateur
	MSG.UserBlockedActCount	nombre de processus ayant une activité suspecte bloqués par l'utilisateur
	MSG.UserBlockedHipsType	type des objets le plus souvent protégés l'accès auxquels est interdit par l'utilisateur
	MSG.UserBlockedIsShellGuard	division par types de réaction de la Protection préventive lors du blocage de l'accès par l'utilisateur : • blocage de l'exécution du code non autorisé • contrôle d'accès aux objets protégés
	MSG.UserBlockedProc	processus ayant une activité suspecte bloqué par l'utilisateur
	MSG.UserBlockedShellGuard	la cause la plus répandue de blocage de l'exécution du code non autorisé lors du blocage de l'événement par l'utilisateur

Un grand nombre de blocages faits par le Contrôle des applications est enregistré

Paramètre	Valeur
Raison d'envoi de la notification	Envoyée si le Contrôle des applications a bloqué beaucoup d'applications sur le poste.
Configuration avancée	Pour envoyer des notifications sur de nombreuses applications

Paramètre	Valeur	
	bloquées, il faut cocher la case **Nombreux blocages par le Contrôle des applications** dans la section **Administration → Configuration du Serveur Dr.Web → Statistiques**. Les paramètres correspondants sont spécifiés dans la même section.	
Variables	`MSG.Total`	nombre total des blocages
	`MSG.Profile`	les profils les plus répandus par lesquels le blocage a été fait

Un grand nombre de connexions interrompues de façon anormale est enregistré

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée en cas de grand nombre d'interruptions anormales des connexions avec les clients : postes, installateurs de l'Agent, Serveurs voisins Dr.Web, Serveurs proxy.	
Configuration supplémentaire	Pour envoyer des notifications sur de nombreuses connexions interrompues de façon anormale, il faut cocher la case **Interruptions anormales des connexions** dans la section **Administration → Configuration du Serveur Dr.Web → Statistiques**. Les paramètres correspondants sont spécifiés dans la même section.	
Variables	`MSG.Total`	nombre de connexions interrompues
	`MSG.AddrsCount`	nombre d'adresses dont les connexions ont été interrompues

Installations

Les variables communes pour les postes disponibles pour les messages de ce groupe sont listées ci-dessus.

L'installation sur le poste n'est pas effectuée

Paramètre	Valeur
Raison d'envoi de la notification	Envoyée en cas d'erreur survenant lors de l'installation de l'Agent sur le poste. La raison précise de l'erreur est indiquée dans le texte de message.
Configuration	N'est pas requise.

Paramètre	Valeur	
supplémentaire		
Variables	`MSG.Error`	message d'erreur

L'installation sur le poste s'est terminée avec succès

Paramètre	Valeur
Raison d'envoi de la notification	Envoyée en cas de l'installation réussie de l'Agent sur le poste.
Configuration supplémentaire	N'est pas requise.
Variables	Absentes.

Licences

Expiration de la clé de licence

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée si la clé de licence va expirer et la mise à jour automatique de la licence n'est pas disponible.	
Configuration supplémentaire	N'est pas requise.	
Variables	`MSG.ExpirationDate`	date d'expiration de la licence
	`MSG.Expired`	• 1 : le délai d'expiration est atteint • 0 : le délai d'expiration n'est pas encore atteint
	`MSG.KeyId`	identificateur de la clé de licence
	`MSG.KeyName`	nom de la clé de licence

La clé de licence ne peut pas être mise à jour automatiquement

Paramètre	Valeur
Raison d'envoi de la	Envoyée si la clé de licence ne peut pas être mise à jour

Paramètre	Valeur	
notification	automatiquement car les composants soumis à la licence de l'ancienne clé sont différents de ceux de la clé actuelle. Dans ce cas, la nouvelle clé est téléchargée avec succès mais elle n'est pas diffusée sur tous les objets de l'ancienne clé de licence. Il est nécessaire de remplacer la clé de licence manuellement.	
Configuration avancée	Pour en savoir plus sur la mise à jour automatique des licences, consultez le **Manuel Administrateur**, le p. Mise à jour automatique de licences.	
Variables	`MSG.ExpirationDate`	date d'expiration de la licence
	`MSG.Expired`	• 1 : le délai d'expiration est atteint • 0 : le délai d'expiration n'est pas encore atteint
	`MSG.KeyDifference`	Raison par laquelle le remplacement automatique de la clé est impossible : • 1 : les composants de la clé de licence actuelle sont différents de ceux de la nouvelle clé • 2 : la nouvelle clé a moins de licences que la clé de licence actuelle
	`MSG.KeyId`	identificateur de l'ancienne clé de licence
	`MSG.KeyName`	nom de l'ancienne clé de licence
	`MSG.NewKeyId`	identificateur de la nouvelle clé de licence
	`MSG.NewKeyName`	nom de la nouvelle clé de licence

La clé de licence est mise à jour automatiquement

Paramètre	Valeur
Raison d'envoi de la notification	Envoyé si la clé de licence a été mise à jour automatiquement. Dans ce cas, une nouvelle clé est téléchargée avec succès et diffusée sur tous les objets de l'ancienne clé de licence.
Configuration avancée	Pour en savoir plus sur la mise à jour automatique des licences,

Paramètre	Valeur	
	consultez le **Manuel Administrateur**, le p. Mise à jour automatique de licences.	
Variables	`MSG.KeyId`	identificateur de l'ancienne clé de licence
	`MSG.KeyName`	nom de l'ancienne clé de licence
	`MSG.NewKeyId`	identificateur de la nouvelle clé de licence
	`MSG.NewKeyName`	nom de la nouvelle clé de licence

La clé de licence est bloquée

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée si lors de la mise à jour du référentiel depuis le Système global de mises à jour Dr.Web, il s'est avéré que la clé de licence est bloquée. L'utilisation de cette clé n'est plus possible.	
Configuration avancée	Pour plus d'infos sur la raison de blocage, veuillez contacter le service de support technique.	
Variables	`MSG.KeyId`	ID de la clé de licence
	`MSG.KeyName`	nom d'utilisateur de la clé de licence

La limite du nombre de postes sur le réseau est atteint

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée si, lors de la connexion du poste au Serveur Dr.Web, il a été révélé que le nombre de postes dans un groupe auquel appartient le poste connecté a atteint la limite dans la clé de licence assignée pour ce groupe. Dans ce cas, le nouveau poste ne peut pas être enregistré sur le Serveur Dr.Web.	
Configuration supplémentaire	N'est pas requise.	
Variables	`MSG.ID`	UUID du poste

Paramètre	Valeur	
	`MSG.StationName`	nom du poste
	Les variables communes pour les postes sont listées ci-dessus.	

La limite du nombre de licences transmises est atteinte

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée si le nombre de licences requises par le Serveur voisin Dr.Web dépasse le nombre de licences disponibles dans la clé de licence.	
Configuration supplémentaire	N'est pas requise.	
Variables	`MSG.ObjId`	ID de la clé de licence

Le délai de transmission de licences est écoulé

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée si le délai de distribution des licences au Serveur voisin Dr.Web depuis la clé de licence de ce Serveur Dr.Web a expiré.	
Configuration supplémentaire	Le délai de distribution des licences aux Serveurs voisins Dr.Web est spécifié dans la section **Administration** → **Configuration du Serveur Dr.Web** → **Licences**.	
Variables	`MSG.ObjId`	ID de la clé de licence
	`MSG.Server`	nom du Serveur voisin Dr.Web

Le nombre de postes dans le groupe va atteindre la limite de licence

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée si le nombre de postes dans le groupe va atteindre la limite de licence spécifiée dans la clé assignée pour ce groupe.	
Configuration avancée	Dans la clé auprès de laquelle s'effectue la notification, il y a moins de trois licences disponibles ou moins de 5% du nombre total des licences dans la clé.	
Variables	`MSG.Free`	nombre des licences disponibles restantes

Paramètre	Valeur	
	MSG.Licensed	nombre de postes utilisant les licences de ce groupe
	MSG.Total	nombre total des licences par toutes les clés assignées au groupe. notez que les clés de licence du groupe peuvent également être assignées aux autres objets de la licence.
	GEN.StationPrimaryGroupID	ID du groupe primaire
	GEN.StationPrimaryGroupName	nom du groupe primaire

Limitation du nombre de licences dans la clé de licence

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée si, lors de l'activation du Serveur Dr.Web, il a été révélé que le nombre de postes dans un groupe a déjà dépassé le nombre de licences dans la clé de licence assignée pour ce groupe.	
Configuration supplémentaire	N'est pas requise.	
Variables	MSG.KeyId	ID de la clé de licence
	MSG.KeyName	nom d'utilisateur de la clé de licence
	MSG.Licensed	nombre des licences autorisées
	MSG.LicenseLimit	statuts des licences : • 1 : le nombre des licences disponibles dans la clé de licence va atteindre sa limite, • 2 : le nombre des licences disponibles dans la clé de licence a atteint sa limite, • 3 : la clé de licence a été assignée à plus d'objets que cela est autorisé dans

Paramètre	Valeur	
		cette clé.
	`MSG.Licensed`	nombre d'objets auxquels la clé a été assignée
	`MSG.Total`	nombre de licences dans la clé

Novices

Les variables communes pour les postes disponibles pour les messages de ce groupe sont listées ci-dessus.

Le poste attend l'approbation

Paramètre	Valeur
Raison d'envoi de la notification	Envoyée si le nouveau poste a demandé une connexion au Serveur Dr.Web et que l'administrateur a besoin d'approuver ou de refuser l'accès du poste manuellement.
Configuration supplémentaire	Cette situation peut survenir si la valeur **Confirmation d'accès manuelle** est spécifiée pour le paramètre **Mode d'enregistrement de novices** dans la rubrique **Administration** → **Configuration du Serveur Dr.Web** → **Général**.
Variables	Absentes.

Le poste est rejeté automatiquement

Paramètre	Valeur
Raison d'envoi de la notification	Envoyée si le nouveau poste a demandé une connexion au Serveur Dr.Web et que le Serveur Dr.Web l'a rejeté automatiquement.
Configuration supplémentaire	Cette situation peut survenir si la valeur **Toujours refuser l'accès** est spécifiée dans la rubrique **Administration** → **Configuration du Serveur Dr.Web** → **Général** pour le paramètre **Mode d'enregistrement de novices**.
Variables	Absentes.

Le poste est rejeté par l'administrateur

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée si le nouveau poste a demandé une connexion au Serveur Dr.Web et que l'administrateur l'a rejeté manuellement.	
Configuration supplémentaire	Cette situation peut survenir si la valeur **Confirmation manuelle d'accès** est spécifiée pour le paramètre **Mode d'enregistrement de novices** dans la rubrique **Administration → Configuration du Serveur Dr.Web → Général** et que l'administrateur a sélectionné pour le poste l'option **Réseau antivirus →**  **Postes non approuvés →**  **Refuser l'accès aux postes sélectionnés**.	
Variables	`MSG.AdminAddress`	adresse réseau du Centre de gestion
	`MSG.AdminName`	nom de l'administrateur

Référentiel

Les variables communes pour le référentiel, disponibles pour les messages de ce groupe sont listées ci-dessus.

Erreur de la mise à jour du référentiel

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée si une erreur est survenue lors de la mise à jour du référentiel ou d'un des produits du référentiel depuis le SGM. Le nom du produit et la raison concrète de l'erreur sont mentionnés dans le texte de notification.	
Configuration supplémentaire	N'est pas requise.	
Variables	`MSG.Error`	message d'erreur
	`MSG.ExtendedError`	description détaillée de l'erreur

La mise à jour du produit dans le référentiel est bloquée

Paramètre	Valeur
Raison d'envoi de la notification	Envoyée si le produit dans le référentiel a été bloqué par l'administrateur. La mise à jour depuis le SGM n'est pas effectué.

Paramètre	Valeur
Configuration avancée	La gestion des produits du référentiel y compris le blocage et le déblocage est effectué dans la rubrique **Administration** → **Configuration détaillée du référentiel**.
Variables	Absentes.

La mise à jour du produit du référentiel est lancée

Paramètre	Valeur
Raison d'envoi de la notification	Envoyée si, lors de vérification des mises à jour du référentiel, il a été révélé que les produits requis nécessitent une mise à jour. Dans ce cas, la mise à jour depuis le SGM est lancée automatiquement.
Configuration supplémentaire	N'est pas requise.
Variables	Absentes.

La mise à jour du référentiel est déjà lancée

Paramètre	Valeur
Raison d'envoi de la notification	Envoyée si une mise à jour a été lancée encore une fois au cours de la mise à jour du Serveur Dr.Web.
Configuration supplémentaire	N'est pas requise.
Variables	Absentes.

Statut actuel du produit dans le référentiel

Paramètre	Valeur
Raison d'envoi de la notification	Envoyée si, lors de vérification des mises à jour du référentiel, il a été révélé que le produit requis est en état actuel. La mise à jour de ce produit depuis le SGM n'est pas requise.
Configuration supplémentaire	N'est pas requise.
Variables	Absentes.

Les variables du modèle **Statut actuel du produit dans le référentiel** ne comprennent pas les fichiers marqués comme **ignorés lors des notifications** dans le fichier de configuration du produit, voir E1. Fichiers de configuration généraux.

Le produit dans le référentiel est mis à jour

Message	Valeur	
Raison d'envoi de la notification	Envoyée en cas de la mise à jour réussie du référentiel depuis le SGM.	
Configuration supplémentaire	N'est pas requise.	
Variables	`MSG.Added`	liste des fichiers ajoutés (chaque nom à la ligne)
	`MSG.AddedCount`	nombre de fichiers ajoutés
	`MSG.Deleted`	liste des fichiers supprimés (chaque nom à la ligne)
	`MSG.DeletedCount`	nombre de fichiers supprimés
	`MSG.Replaced`	liste des fichiers remplacés (chaque nom à la ligne)
	`MSG.ReplacedCount`	nombre de fichiers remplacés

Pas assez d'espace libre sur le disque

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée si l'espace libre sur le disque sur lequel est placé le répertoire du Serveur Dr.Web `var` avec les données dynamiques est presque épuisé.	
Configuration supplémentaire	L'espace libre sur le disque est considéré comme insuffisant s'il reste moins de 315 Mo ou moins de 1000 inodes (pour les OS de la famille UNIX) si ces valeurs ne sont pas préconfigurées par les variables d'environnement.	
Variables	Les variables communes pour le référentiel listées ci-dessus sont indisponibles.	
	`MSG.FreeInodes`	nombre de descripteurs de fichiers inodes disponibles

Paramètre	Valeur	
		(s'applique uniquement pour certains systèmes de la famille UNIX)
	`MSG.FreeSpace`	espace libre en octets
	`MSG.Path`	chemin vers le répertoire de petit volume de mémoire
	`MSG.RequiredInodes`	nombre d'inodes disponibles requis (s'applique uniquement pour certains système de la famille UNIX)
	`MSG.RequiredSpace`	volume de mémoire requis

Postes

Les variables communes pour les postes disponibles pour les messages de ce groupe sont listées ci-dessus.

Dans le réseau multi-serveurs, on peut recevoir des notifications des événements produits sur les postes de Serveurs voisins Dr.Web. L'activation de cette option se fait lors de la configuration des liaisons avec les Serveurs voisins Dr.Web (voir le **Manuel administrateur**, la rubrique Configuration des liaisons entre Serveurs Dr.Web).

Les notifications suivantes des événements du Serveur voisin Dr.Web sont disponibles : **Menace de sécurité détectée**, **Rapport de la protection préventive**, **Erreur de scan**, **Statistiques de scan**.

Arrêt d'urgence de la connexion

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée en cas de connexion interrompue avec le client : poste, installateur de l'Agent, Serveur voisin Dr.Web, Serveur proxy.	
Configuration supplémentaire	Pour envoyer des notifications sur des connexions interrompues de façon anormale, il faut cocher la case **Interruptions anormales des connexions** dans la section **Administration → Configuration du Serveur Dr.Web → Statistiques**. Les paramètres correspondants sont spécifiés dans la même section.	
Variables	`MSG.Total`	nombre de connexions interrompues

Paramètre	Valeur	
	`MSG.Type`	type de client

Erreur d'authentification du poste

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée, si le poste a fourni les identifiants incorrects lors de la tentative de connexion au Serveur Dr.Web. Les actions ultérieures dépendant de la politique de connexion de postes sont également mentionnées dans la notification.	
Configuration supplémentaire	La politique de la connexion de poste est spécifiée dans le paramètre **Mode d'enregistrement de novices**, dans la rubrique **Administration → Configuration du Serveur Dr.Web → Général**.	
Variables	`MSG.ID`	UUID du poste
	`MSG.Rejected`	valeurs : • `rejected` : accès au poste refusé • `newbie` : tentative de basculer le poste vers le statut « novice »
	`MSG.StationName`	nom du poste

Erreur de création du compte de poste

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée s'il est impossible de créer un nouveau compte du poste sur le Serveur Dr.Web. Tous les détails sur l'erreur sont mentionnés dans le fichier de journal du Serveur Dr.Web.	
Configuration supplémentaire	N'est pas requise.	
Variables	`MSG.ID`	UUID du poste
	`MSG.StationName`	nom du poste

Erreur de scan

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée si une notification sur une erreur survenue lors du scan est reçue depuis le poste.	
Configuration supplémentaire	N'est pas requise.	
Variables	`MSG.Component`	nom du composant
	`MSG.Error`	message d'erreur
	`MSG.ObjectName`	nom de l'objet
	`MSG.ObjectOwner`	propriétaire de l'objet
	`MSG.RunBy`	utilisateur au nom duquel le composant est lancé
	`MSG.ServerTime`	heure de la réception de l'événement, GMT
	`GEN.ServerRecvLinkID`	UUID du dernier Serveur voisin Dr.Web depuis lequel on a obtenu les informations sur l'erreur de scan des postes connectés (valeur vide, si l'erreur de scan a eu lieu sur les postes connectés à ce Serveur Dr.Web)
	`GEN.ServerRecvLinkName`	nom du dernier Serveur voisin Dr.Web depuis lequel on a obtenu les informations sur l'erreur de scan des postes connectés (valeur vide, si l'erreur de scan a eu lieu sur les postes connectés à ce Serveur Dr.Web)
	`GEN.ServerOriginatorID`	UUID du Serveur Dr.Web auquel est connectée le poste sur lequel une erreur de scan s'est produite
	`GEN.ServerOriginatorName`	nom du Serveur Dr.Web auquel est connecté le poste sur lequel une erreur de scan s'est produite

Erreur critique de mise à jour du poste

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée si une notification sur une erreur survenue lors du scan des composants antivirus est reçue depuis le Serveur Dr.Web.	
Configuration supplémentaire	N'est pas requise.	
Variables	`MSG.Product`	produit à mettre à jour
	`MSG.ServerTime`	heure de la réception de l'événement, GMT

Erreur de scan lors de la détection d'une menace par les hashs de menaces connus

Paramètre	Valeur	
Raison de l'envoi de notification	Envoyée si une erreur de scan s'est produite en cas de détection d'une menaces de la liste de hashs de menaces connus.	
Configuration supplémentaire	La notification de détection par la liste des hashs de menaces connus est possible uniquement si l'utilisation des bulletins de hashs de menaces connus est autorisée (il suffit d'avoir une licence dans une des clés de licences utilisées par le Serveur Dr.Web). La disponibilité de la licence est indiquée dans les informations sur la clé de licence que vous pouvez consulter dans la section **Gestionnaire de licences**, le paramètre **Listes autorisées de bulletins de hashs** (si la fonctionnalité n'est pas autorisée, le paramètre n'est pas présent).	
Variables	`MSG.Component`	nom du composant
	`MSG.Document`	bulletin contenant le hash de la menace détectée
	`MSG.Error`	message d'erreur
	`MSG.ObjectName`	nom de l'objet
	`MSG.ObjectOwner`	propriétaire de l'objet
	`MSG.RunBy`	utilisateur au nom duquel le composant est lancé
	`MSG.SHA1`	hash SHA-1 de l'objet trouvé

Paramètre	Valeur	
	MSG.SHA256	hash SHA-256 de l'objet trouvé
	MSG.ServerTime	heure de la réception de l'événement, GMT
	GEN.ServerRecvLinkID	UUID du dernier Serveur voisin Dr.Web depuis lequel on a obtenu les informations sur l'erreur de scan des postes connectés (valeur vide, si l'erreur de scan a eu lieu sur les postes connectés à ce Serveur Dr.Web)
	GEN.ServerRecvLinkName	nom du dernier Serveur voisin Dr.Web depuis lequel on a obtenu les informations sur l'erreur de scan des postes connectés (valeur vide, si l'erreur de scan a eu lieu sur les postes connectés à ce Serveur Dr.Web)
	GEN.ServerOriginatorID	UUID du Serveur Dr.Web auquel est connectée le poste sur lequel une erreur de scan s'est produite
	GEN.ServerOriginatorName	nom du Serveur Dr.Web auquel est connecté le poste sur lequel une erreur de scan s'est produite

L'appareil est bloqué

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée si une notification a été reçue depuis le poste et elle informe du blocage d'un périphérique connecté au poste par le composant antivirus Dr.Web.	
Configuration supplémentaire	N'est pas requise.	
Variables	MSG.Capabilities	caractéristiques de l'appareil
	MSG.Class	classe de l'appareil (nom du groupe parent)
	MSG.Description	description de l'appareil

Paramètre	Valeur	
	`MSG.FriendlyName`	nom convivial de l'appareil
	`MSG.InstanceId`	identificateur de l'appareil
	`MSG.User`	nom d'utilisateur

Le Contrôle des applications a bloqué le processus de la liste des hashs de menaces connus

Paramètre	Valeur	
Raison de l'envoi de notification	Envoyée si le Contrôle des applications a bloqué sur le poste une application de la liste des hashs de menaces connus.	
Configuration supplémentaire	La notification de détection par la liste des hashs de menaces connus est possible uniquement si l'utilisation des bulletins de hashs de menaces connus est autorisée (il suffit d'avoir une licence dans une des clés de licences utilisées par le Serveur Dr.Web). La disponibilité de la licence est indiquée dans les informations sur la clé de licence que vous pouvez consulter dans la section **Gestionnaire de licences**, le paramètre **Listes autorisées de bulletins de hashs** (si la fonctionnalité n'est pas autorisée, le paramètre n'est pas présent).	
Variables	`MSG.AppCtlAction`	action appliquée : • 0 : inconnu, • 2 : bloqué, • 3 : bloqué (introuvable dans la liste des applications de confiance), • 5 : bloqué par les règles de blocage, • 7 : bloqué par les paramètres des politique.
	`MSG.AppCtlType`	type de l'événement : • 0 : inconnu, • 1 : lancement du processus, • 2 : lancement du processus hôte, • 3 : lancement de l'interpréteur de script, • 4 : chargement du module,

Paramètre	Valeur	
		• 5 : chargement du pilote, • 6 : lancement de l'installateur MSI, • 7 : création d'un nouveau du fichier exécutable sur le disque, • 8 : modification du fichier exécutable sur le disque.
	`MSG.Document`	bulletin contenant le hash
	`MSG.Path`	chemin ver le processus bloqué
	`MSG.Profile`	nom du profil par lequel le blocage a été fait
	`MSG.Rule`	nom de la règle par laquelle le blocage a été fait
	`MSG.SHA256`	hash du processus bloqué (SHA-256)
	`MSG.StationTime`	heure sur le poste quand le processus a été bloqué
	`MSG.Target`	chemin vers le script bloqué en cas du processus hôte
	`MSG.TargetSHA256`	hash du script bloqué en cas du processus hôte (SHA-256)
	`MSG.TestMode`	si mode test est activé
	`MSG.User`	utilisateur au nom duquel l'objet bloqué a été lancé

Le Contrôle des applications a bloqué le processus

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée si le Contrôle des applications a bloqué une application sur le poste.	
Configuration supplémentaire	N'est pas requise.	
Variables	`MSG.AppCtlAction`	action appliquée :

Paramètre	Valeur	
		• 0 : inconnu, • 2 : bloqué, • 3 : bloqué (introuvable dans la liste des applications de confiance), • 5 : bloqué par les règles de blocage, • 7 : bloqué par les paramètres des politique.
	`MSG.AppCtlType`	type de l'événement : • 0 : inconnu, • 1 : lancement du processus, • 2 : lancement du processus hôte, • 3 : lancement de l'interpréteur de script, • 4 : chargement du module, • 5 : chargement du pilote, • 6 : lancement de l'installateur MSI, • 7 : création d'un nouveau du fichier exécutable sur le disque, • 8 : modification du fichier exécutable sur le disque.
	`MSG.Path`	chemin ver le processus bloqué
	`MSG.Profile`	nom du profil par lequel le blocage a été fait
	`MSG.Rule`	nom de la règle par laquelle le blocage a été fait
	`MSG.SHA256`	hash du processus bloqué (SHA-256)
	`MSG.StationTime`	heure sur le poste quand le processus a été bloqué
	`MSG.Target`	chemin vers le script bloqué en cas du processus hôte
	`MSG.TargetSHA256`	hash du script bloqué en cas du

Paramètre	Valeur	
		processus hôte (SHA-256)
	MSG.TestMode	si mode test est activé
	MSG.User	utilisateur au nom duquel l'objet bloqué a été lancé

Le poste est déjà enregistré

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée en cas de tentative de connexion au Serveur Dr.Web du poste à l'identificateur qui ne correspond pas à l'identificateur du poste déjà connecté à ce Serveur Dr.Web.	
Configuration supplémentaire	N'est pas requise.	
Variables	MSG.ID	UUID du poste
	MSG.Server	ID du Serveur Dr.Web sur lequel est enregistré le poste
	MSG.StationName	nom du poste

Le poste n'a pas été connecté au Serveur Dr.Web depuis longtemps

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée conformément à la tâche de planification du Serveur Dr.Web. Notifie que le poste n'a pas été connecté depuis longtemps à ce Serveur Dr.Web. La date de la dernière connexion est mentionnée dans le texte de message.	
Configuration supplémentaire	La durée de la période lors de laquelle le poste n'a pas été connecté. A l'issue de cette période une notification est envoyée. La durée est spécifiée dans la tâche **Le poste n'a pas été connecté depuis longtemps** dans la planification du Serveur Dr.Web configurée dans la rubrique **Administration** → **Planificateur de tâches du Serveur Dr.Web**.	
Variables	Les variables communes pour les postes listées ci-dessus sont indisponibles.	
	MSG.DaysAgo	nombre de jours écoulés depuis la dernière connexion au Serveur

Paramètre	Valeur	
		Dr.Web
	MSG.LastSeenFrom	adresse depuis laquelle le poste s'est connectée la dernière fois au Serveur Dr.Web
	MSG.StationDescription	description du poste
	MSG.StationID	UUID du poste
	MSG.StationMAC	adresse MAC du poste
	MSG.StationName	nom du poste
	MSG.StationSID	identificateur de sécurité du poste

Le redémarrage du poste est requis

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée si un redémarrage du poste est requis par l'une des raisons suivantes : • pour terminer la désinfection, • pour appliquer les mises à jour, • pour modifier le statut de la virtualisation matérielle, • pour terminer la désinfection et appliquer les mises à jour, • pour terminer la désinfection et modifier le statut de la virtualisation matérielle, • pour appliquer les mises à jour et modifier le statut de la virtualisation matérielle, • pour terminer la désinfection, appliquer les mises à jour et modifier le statut de la virtualisation matérielle.	
Configuration supplémentaire	N'est pas requise.	
Variables	MSG.Reason	cause du redémarrage les causes possibles sont listées dans le modèle préinstallé

Le poste est approuvé automatiquement

Paramètre	Valeur
Raison d'envoi de la notification	Envoyée si un nouveau poste a demandé une connexion au Serveur Dr.Web et que l'administrateur l'a approuvé manuellement ou qu'il a été approuvé automatiquement par le Serveur Dr.Web.
Configuration supplémentaire	Cette situation peut survenir si la valeur **Autoriser l'accès automatiquement** est spécifiée pour le paramètre **Mode d'enregistrement de novices** dans la rubrique **Administration** → **Configuration du Serveur Dr.Web** → **Général**.
Variables	Absentes.

Le poste est approuvé par l'administrateur

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée si un nouveau poste a demandé une connexion au Serveur Dr.Web et que l'administrateur l'a approuvé manuellement.	
Configuration supplémentaire	Cette situation peut survenir si la valeur **Confirmation d'accès manuelle** est spécifiée pour le paramètre **Mode d'enregistrement de novices** dans la rubrique **Administration** → **Configuration du Serveur Dr.Web** → **Général** et que l'administrateur a sélectionné pour le poste l'option **Réseau antivirus** → **Postes non approuvés** → **Autoriser l'accès aux postes sélectionnés et spécifier le groupe primaire**.	
Variables	`MSG.AdminAddress`	adresse réseau du Centre de gestion
	`MSG.AdminName`	nom de l'administrateur

Menace de sécurité détectée

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée si une notification sur la détection de menaces a été reçue du poste. Les informations détaillées sur les menaces détectées sont également mentionnées dans la notification de l'administrateur.	
Configuration supplémentaire	N'est pas requise.	
Variables	`MSG.Action`	action appliquée en cas de

Paramètre	Valeur	
		détection
	MSG.Component	nom du composant
	MSG.InfectionType	type de menace
	MSG.ObjectName	nom de l'objet infecté
	MSG.ObjectOwner	propriétaire de l'objet infecté
	MSG.RunBy	utilisateur au nom duquel le composant est lancé
	MSG.ServerTime	heure de la réception de l'événement, GMT
	MSG.Virus	nom de menace
	GEN.ServerRecvLinkID	UUID du dernier Serveur voisin Dr.Web depuis lequel on a obtenu ce message informant d'une menace détectée sur les postes connectés (valeur vide, si la menace est détectée sur les postes connectés à ce Serveur Dr.Web)
	GEN.ServerRecvLinkName	nom du dernier Serveur voisin Dr.Web depuis lequel on a obtenu le message informant d'une menace détectée sur les postes connectés (valeur vide, si la menace est détectée sur les postes connectés à ce Serveur Dr.Web)
	GEN.ServerOriginatorID	UUID du Serveur Dr.Web auquel est connectée le poste sur lequel la menace a été détectée
	GEN.ServerOriginatorName	nom du Serveur Dr.Web auquel est connectée le poste sur lequel la menace a été détectée

Menace détectée par les hashs de menaces connus

Paramètre	Valeur	
Raison de l'envoi de notification	Envoyée si une notification sur la détection de menaces de la liste de hashs de menaces connus a été reçue du poste. Les informations détaillées sur les menaces détectées sont également mentionnées dans la notification de l'administrateur.	
Configuration supplémentaire	La notification de détection par la liste des hashs de menaces connus est possible uniquement si l'utilisation des bulletins de hashs de menaces connus est autorisée (il suffit d'avoir une licence dans une des clés de licences utilisées par le Serveur Dr.Web). La disponibilité de la licence est indiquée dans les informations sur la clé de licence que vous pouvez consulter dans la section **Gestionnaire de licences**, le paramètre **Listes autorisées de bulletins de hashs** (si la fonctionnalité n'est pas autorisée, le paramètre n'est pas présent).	
Variables	`MSG.Action`	action appliquée en cas de détection
	`MSG.Component`	nom du composant
	`MSG.Document`	bulletin contenant le hash de la menace détectée
	`MSG.InfectionType`	type de menace
	`MSG.ObjectName`	nom de l'objet infecté
	`MSG.ObjectOwner`	propriétaire de l'objet infecté
	`MSG.RunBy`	utilisateur au nom duquel le composant est lancé
	`MSG.SHA1`	hash SHA-1 de l'objet trouvé
	`MSG.SHA256`	hash SHA-256 de l'objet trouvé
	`MSG.ServerTime`	heure de la réception de l'événement, GMT
	`MSG.Virus`	nom de menace
	`GEN.ServerRecvLinkID`	UUID du dernier Serveur voisin Dr.Web depuis lequel on a obtenu ce message informant d'une menace détectée sur les postes

Paramètre	Valeur	
		connectés (valeur vide, si la menace est détectée sur les postes connectés à ce Serveur Dr.Web)
	`GEN.ServerRecvLinkName`	nom du dernier Serveur voisin Dr.Web depuis lequel on a obtenu le message informant d'une menace détectée sur les postes connectés (valeur vide, si la menace est détectée sur les postes connectés à ce Serveur Dr.Web)
	`GEN.ServerOriginatorID`	UUID du Serveur Dr.Web auquel est connectée le poste sur lequel la menace a été détectée
	`GEN.ServerOriginatorName`	nom du Serveur Dr.Web auquel est connectée le poste sur lequel la menace a été détectée

Poste inconnu

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée si le poste a demandé une connexion au Serveur Dr.Web mais il a été rejeté avant la confirmation ou le refus de l'enregistrement.	
Configuration supplémentaire	N'est pas requise.	
Variables	`MSG.ID`	UUID du poste inconnu
	`MSG.Rejected`	valeurs : • `rejected` : accès au poste refusé • `newbie` : tentative de basculer le poste vers le statut « novice »
	`MSG.StationName`	nom du poste

Rapport de la Protection préventive

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée en cas de réception du rapport du composant Protection préventive du poste de ce Serveur ou du Serveur voisin Dr.Web.	
Configuration supplémentaire	N'est pas requise.	
Variables	`MSG.AdminName`	administrateur qui a initié l'action appliquée au processus suspect
	`MSG.Denied`	action appliquée au processus suspect : • interdit • autorisé
	`MSG.HipsType`	type de l'objet protégé
	`MSG.IsShellGuard`	division par types de réaction de la Protection préventive : • blocage de l'exécution du code non autorisé • contrôle d'accès aux objets protégés
	`MSG.Path`	chemin vers le processus ayant une activité suspecte
	`MSG.Pid`	identificateur du processus ayant une activité suspecte
	`MSG.ShellGuardType`	cause de blocage de l'exécution du code non autorisé
	`MSG.StationTime`	l'heure de l'apparition de l'événement sur le poste
	`MSG.Target`	chemin vers l'objet protégé auquel une tentative d'accès a été faite
	`MSG.Total`	nombre de blocages en cas de réaction automatique de la Protection préventive
	`MSG.User`	utilisateur au nom de qui le processus ayant une activité

Paramètre	Valeur	
		suspecte a été lancé
	MSG.UserAction	initiateur de l'action appliquée au processus suspect : • utilisateur • réaction automatique de la Protection préventive
	GEN.ServerRecvLinkID	UUID du dernier Serveur voisin Dr.Web depuis lequel on a obtenu le rapport de la Protection préventive des postes connectés (valeur vide, s'il s'agit du rapport des postes connectés à ce Serveur Dr.Web)
	GEN.ServerRecvLinkName	nom du dernier Serveur voisin Dr.Web depuis lequel on a obtenu le rapport de la Protection préventive des postes connectés (valeur vide, s'il s'agit du rapport des postes connectés à ce Serveur Dr.Web)
	GEN.ServerOriginatorID	UUID du Serveur Dr.Web auquel est connecté le poste depuis lequel le rapport de la Protection préventive a été envoyé
	GEN.ServerOriginatorName	nom du Serveur Dr.Web auquel est connecté le poste depuis lequel le rapport de la Protection préventive a été envoyé

Rapport de la Protection préventive sur la détection de menaces par les hashs de menaces connus

Paramètre	Valeur
Raison d'envoi de la notification	Envoyée en cas de réception du rapport du composant Protection préventive du poste de ce Serveur ou du Serveur voisin Dr.Web si une menace de la liste de hashs de menaces connus est détectée.
Configuration supplémentaire	La notification de détection par la liste des hashs de menaces connus est possible uniquement si l'utilisation des bulletins de hashs de menaces connus est autorisée (il suffit d'avoir une licence dans

Paramètre	Valeur	
	une des clés de licences utilisées par le Serveur Dr.Web). La disponibilité de la licence est indiquée dans les informations sur la clé de licence que vous pouvez consulter dans la section **Gestionnaire de licences**, le paramètre **Listes autorisées de bulletins de hashs** (si la fonctionnalité n'est pas autorisée, le paramètre n'est pas présent).	
Variables	`MSG.AdminName`	administrateur qui a initié l'action appliquée au processus suspect
	`MSG.Denied`	action appliquée au processus suspect : • interdit • autorisé
	`MSG.Document`	bulletin contenant le hash de la menace détectée
	`MSG.HipsType`	type de l'objet protégé
	`MSG.IsShellGuard`	division par types de réaction de la Protection préventive : • blocage de l'exécution du code non autorisé • contrôle d'accès aux objets protégés
	`MSG.Path`	chemin vers le processus ayant une activité suspecte
	`MSG.Pid`	identificateur du processus ayant une activité suspecte
	`MSG.SHA1`	hash SHA-1 de l'objet trouvé
	`MSG.SHA256`	hash SHA-256 de l'objet trouvé
	`MSG.ShellGuardType`	cause de blocage de l'exécution du code non autorisé
	`MSG.StationTime`	l'heure de l'apparition de l'événement sur le poste
	`MSG.Target`	chemin vers l'objet protégé auquel une tentative d'accès a été faite

Paramètre	Valeur	
	MSG.Total	nombre de blocages en cas de réaction automatique de la Protection préventive
	MSG.User	utilisateur au nom de qui le processus ayant une activité suspecte a été lancé
	MSG.UserAction	initiateur de l'action appliquée au processus suspect : • utilisateur • réaction automatique de la Protection préventive
	GEN.ServerRecvLinkID	UUID du dernier Serveur voisin Dr.Web depuis lequel on a obtenu le rapport de la Protection préventive des postes connectés (valeur vide, s'il s'agit du rapport des postes connectés à ce Serveur Dr.Web)
	GEN.ServerRecvLinkName	nom du dernier Serveur voisin Dr.Web depuis lequel on a obtenu le rapport de la Protection préventive des postes connectés (valeur vide, s'il s'agit du rapport des postes connectés à ce Serveur Dr.Web)
	GEN.ServerOriginatorID	UUID du Serveur Dr.Web auquel est connecté le poste depuis lequel le rapport de la Protection préventive a été envoyé
	GEN.ServerOriginatorName	nom du Serveur Dr.Web auquel est connecté le poste depuis lequel le rapport de la Protection préventive a été envoyé

Statistiques de scan

Paramètre	Valeur
Raison d'envoi de la notification	Envoyée si une notification sur la fin du scan est reçue depuis le poste. Les brèves statistiques du scan sont également mentionnées

Paramètre	Valeur	
	dans la notification de l'administrateur.	
Configuration supplémentaire	N'est pas requise.	
Variables	`MSG.Component`	nom du composant qui effectue le scan
	`MSG.Cured`	nombre d'objets désinfectés
	`MSG.DeletedObjs`	nombre d'objets supprimés
	`MSG.Errors`	nombre d'erreurs du scan
	`MSG.Infected`	nombre d'objets infectés
	`MSG.Locked`	nombre d'objets bloqués
	`MSG.Modifications`	nombre d'objets infectés par des modifications de virus
	`MSG.Moved`	nombre d'objets déplacés en quarantaine
	`MSG.Renamed`	nombre d'objets renommés
	`MSG.RunBy`	utilisateur au nom duquel le composant est lancé
	`MSG.Scanned`	nombre d'objets scannés
	`MSG.ServerTime`	heure de la réception de l'événement, GMT
	`MSG.Speed`	vitesse de traitement en Ko/s
	`MSG.Suspicious`	nombre de fichiers suspects
	`MSG.VirusActivity`	nombre de virus détectés
	`GEN.ServerRecvLinkID`	UUID du dernier Serveur voisin Dr.Web depuis lequel on a obtenu les statistiques de scan des postes connectés (valeur vide, s'il s'agit des statistiques de postes connectés à ce Serveur Dr.Web)
	`GEN.ServerRecvLinkName`	nom du dernier Serveur voisin Dr.Web depuis lequel on a obtenu

Paramètre	Valeur	
		les statistiques de scan des postes connectés (valeur vide, s'il s'agit des statistiques de postes connectés à ce Serveur Dr.Web)
	`GEN.ServerOriginatorID`	UUID du Serveur Dr.Web auquel est connecté le poste depuis lequel les statistiques ont été envoyées
	`GEN.ServerOriginatorName`	nom du Serveur Dr.Web auquel est connecté le poste depuis lequel les statistiques ont été envoyées

Un redémarrage du poste est requis pour appliquer les mises à jour

Paramètre	Valeur	
Raison d'envoi de la notification	Envoyée si une notification a été reçue depuis le poste et elle informe sur l'installation ou la mise à jour du produit effectuée et le redémarrage du poste requis.	
Configuration supplémentaire	N'est pas requise.	
Variables	`MSG.Product`	produit à mettre à jour
	`MSG.ServerTime`	heure de la réception de l'événement, GMT

Annexe D. Spécification de l'adresse réseau

La spécification présente comprend les termes suivants :

- les variables (les champs à remplacer par des valeurs spécifiées) sont à mettre entre < > et en italique,
- le texte permanent (qui reste après les substitutions) doit utiliser une police non proportionnelle (largeur fixe),
- les éléments facultatifs sont à mettre entre crochets,
- à gauche de la séquence des symboles `::=` se trouve une notion à déterminer, à droite — sa détermination (comme dans la forme de Backus-Naur).

D1. Format général de l'adresse

L'adresse réseau est au format suivant :

`[`<*protocol*>`://][`<*protocol-specific-part*>`]`

Par défaut, <*protocol*> reçoit la valeur `TCP`. Les valeurs par défaut <*protocol-specific-part*> sont déterminées par l'application.

L'ancien format d'adresses est également autorisé :

`[`<*protocol*>`/][`<*protocol-specific-part*>`]`.

Adresses de la famille IP

- <*interface*>`::=`<*ip-address*>

  <*ip-address*> peut être un nom DNS ou une adresse IP espacée par des points (exemple `127.0.0.1`).

- <*socket-address*>`::=`<*interface*>`:`<*port-number*>

  <*port-number*> doit être un nombre décimal.

Quand vous spécifiez l'adresse du Serveur Dr.Web et l'adresse de l'Agent Dr.Web, vous pouvez indiquer la version du protocole utilisé. Les variantes suivantes sont possibles :

- <*protocol*>`://`<*interface*>`:`<*port-number*> : utiliser IPv4 et IPv6.
- <*protocol*>`://(`<*interface*>`)`<*port-number*> : utiliser uniquement IPv4.
- <*protocol*>`://[`<*interface*>`]:`<*port-number*> : utiliser uniquement IPv6.

Exemple :

`1. tcp://127.0.0.1:2193`

désigne le protocole `TCP`, le port `2193` sur l'interface `127.0.0.1`.

2. `tcp://(examle.com):2193`

   désigne le protocole `TCP`, le port `2193` sur l'interface IPv4 `example.com`.

3. `tcp://[::]:2193`

   désigne le protocole `TCP`, le port `2193` sur l'interface IPv6 `0000.0000.0000.0000.0000.0000.0000.0000`

4. `localhost:2193`

   idem.

5. `tcp://:9999`

   valeur pour le Serveur : l'interface par défaut qui est fonction de l'application (en général, toutes les interfaces disponibles), le port `9999` ; valeur pour le client : connexion avec l'hôte par défaut, en fonction de l'application (en général `localhost`), le port `9999`.

6. `tcp://`

   le protocole TCP, le port est déterminé par défaut.

Protocole orienté connexion

<protocol>`://`*<socket-address>*

où *<socket-address>* détermine l'adresse locale du socket pour le Serveur ou un Serveur distant pour le client.

Protocole orienté datagramme

<protocol>`://`*<endpoint-socket-address>*`[-`*<interface>*`]`

Exemple :

1. `udp://231.0.0.1:2193`

   désigne l'utilisation du groupe muticast `231.0.0.1:2193` sur l'interface par défaut qui est fonction de l'application.

2. `udp://[ff18::231.0.0.1]:2193`

   désigne l'utilisation du groupe muticast `[ff18::231.0.0.1]` sur l'interface par défaut qui est fonction de l'application.

3. `udp://`

   l'interface en fonction de l'application et le point final.

4. `udp://255.255.255.255:9999-myhost1`

   l'utilisation des messages broadcast sur le port `9999` et sur l'interface `myhost1`.

Adresses de la famille UDS

- Le protocole orienté connexion :

  `unx://`*<file_name>*

- Protocole orienté datagramme :

udx://<*file_name*>

Exemple :

1. unx://tmp/drwcsd:stream
2. udx://tmp/drwcsd:datagram

Adresses SRV

srv://[<*server name*>][@<*domain name/dot address*>]

D2. Adresses de l'Agent Dr.Web/ de l'Installateur

Connexion directe au Serveur Dr.Web

[<*connection-protocol*>]://[<*remote-socket-address*>]

Par défaut, en fonction de <*connection-protocol*> :

- tcp://127.0.0.1:2193

  où 127.0.0.1 — loopback, 2193 — port ;
- tcp://[::1]:2193

  où [::1] — loopback (IPv6), 2193 — port.

Recherche du Serveur Dr.Web <drwcs-name> utilisant la famille spécifiée de protocoles et le point final

[<*drwcs-name*>]@<*datagram-protocol*>://[<*endpoint-socket-address*>[-<*interface*>]]

Par défaut, en fonction de <*datagram-protocol*> :

- drwcs@udp://231.0.0.1:2193-0.0.0.0

  recherche du Serveur Dr.Web avec le nom drwcs pour la connexion TCP en utilisant le groupe muticast 231.0.0.1:2193 sur toutes les interfaces.

Annexe E. Gestion du référentiel

Il est recommandé de gérer le référentiel via les paramètres correspondants du Centre de gestion. Pour en savoir plus, voir le **Manuel Administrateur**, p. Gestion du référentiel du Serveur Dr.Web.

Les paramètres du référentiel sont sauvegardés dans les fichiers de configuration du référentiel suivants :

- Les fichiers de configuration généraux se placent dans la racine du répertoire du référentiel et spécifient les paramètres des serveurs des mises à jour.
- Les fichiers de configuration des produits se placent dans la racine des répertoires correspondant aux produits concrets du référentiel et spécifient le contenu des fichiers et les paramètres des mises à jour du produit dans le répertoire duquel ils se placent.

Après l'édition des fichiers de configuration, le redémarrage du Serveur Dr.Web est requis.

Lors de la configuration des liaisons entre serveurs (voir le **Manuel Administrateur**, p. Particularités du réseau avec plusieurs Serveurs Dr.Web), pour répartir en miroir les produits, il est à noter que les fichiers de configuration ne font pas partie du produit et ne sont pas traités par le système de répartition en miroir. Afin d'éviter des failles du système de mises à jour, veuillez respecter les instructions suivantes :

- pour les Serveurs Dr.Web égaux, sauvegardez la configuration identique,
- pour les Serveurs Dr.Web subordonnés, désactivez la synchronisation des composants via le protocole HTTP ou sauvegardez la configuration identique.

E1. Fichiers de configuration généraux

.servers

Le fichier `.servers` contient une liste des serveurs pour la mise à jour des composants Dr.Web Enterprise Security Suite se trouvant dans le répertoire du Serveur Dr.Web depuis les serveurs du SGM.

Les Serveurs se trouvant dans la liste seront interrogés successivement. Après une mise à jour réussie, la procédure se termine.

Exemple :

```
esuite.geo.drweb.com
```

.url

Le fichier `.url` contient URI de base de la zone de mise à jour — du répertoire qui se place sur les serveurs des mises à jour et qui contient les mises à jour pour un produit concret Dr.Web.

Exemple :

```
update
```

.proto

Le fichier `.proto` contient le nom du protocole via lequel on reçoit les mises à jour depuis les serveurs des mises à jour.

Il peut prendre une des valeurs suivantes : `http | https | ftp | ftps | sftp | scp | smb | smbs | file`.

> ⚠ Les protocoles `smb` et `smbs` sont disponibles uniquement pour les Serveurs Dr.Web sous les OS de la famille Unix.

Exemple :

```
https
```

.auth

Le fichier `.auth` contient les paramètres d'authentification de l'utilisateur sur le serveur des mises à jour.

Les paramètres d'authentification sont spécifiés au format suivant :

```
<nom d'utilisateur>
<mot de passe>
```

Nom d'utilisateur — paramètre obligatoire, mot de passe — paramètre facultatif.

Exemple :

```
admin
root
```

.version

Le fichier `.version` contient la version de serveur de la zone duquel les mises à jour doivent être téléchargées. Il est utilisé lors du debogage, par défaut il correspond à la version actuelle du serveur au format MM.mm.

.max-retry

Le fichier `.max-retry` contient le nombre maximal de tentatives en cas d'erreurs de téléchargement de chaque serveur de mise à jour.

.cdn-mode

Le fichier `.cdn-mode` contient les paramètres d'utilisation de Content Delivery Network (CDN) lors du chargement du référentiel.

Il peut prendre une des valeurs suivantes :

- `on` : utiliser CDN,
- `off` : ne pas utiliser CDN.

.cert-mode

Le fichier `.cert-mode` contient les configurations pour les certificats SSL des serveurs des mises à jour qui seront automatiquement acceptés :

Il peut prendre une des valeurs suivantes :

- `drweb` : accepter uniquement les certificats SSL de Doctor Web,
- `valid` : accepter uniquement les certificats SSL valides,
- `any` : accepter tous les certificats,
- `custom` : accepter le certificat désigné par l'utilisateur.

.cert-file

Le fichier `.cert-file` contient le chemin au certificat utilisateur, si le mode `custom` est spécifié pour le paramètre `cert`.

.ssh-mode

Le fichier `.ssh-mode` contient les paramètres du mode d'authentification en cas d'utilisation des protocoles SCP et SFTP (basés sur SSH2).

Il peut prendre une des valeurs suivantes :

- `pwd` : authentification par le login et le mot de passe de l'utilisateur,
- `pubkey` : authentification par les clés de chiffrement.

.ssh-pubkey

Le fichier `.ssh-pubkey` contient le chemin d'accès à la clé SSH publique du serveur des mises à jour.

.ssh-prikey

Le fichier `.ssh-prikey` contient le chemin d'accès à la clé SSH privée du serveur des mises à jour.

E2. Fichiers de configuration des produits

.description

Le fichier `description` désigne le nom du produit. Si le fichier est introuvable, le nom du répertoire du produit sera utilisé comme nom du produit.

Exemple :

```
Dr.Web Server
```

..languages

Le fichier `..languages` contient la liste des codes de langues pour lesquelles la mise à jour est configurée. Si le fichier est manquant ou vide, la mise à jour n'est configurée pour aucune langue et ne sera pas effectuée.

..platforms

Le fichier `..platforms` contient les codes complets des plateformes utilisées dans le produit pour lesquelles la mise à jour est configurée. Si le fichier est manquant ou vide, la mise à jour n'est configurée pour aucune plateforme et ne sera pas effectuée.

..formats

Le fichier `..formats` contient les formats des fichiers pour lesquels la mise à jour est configurée, par exemple, les formats de documents (html, pdf). Si le fichier est manquant ou vide, la mise à jour n'est configurée pour aucun format et ne sera pas effectuée.

..items

Le fichier `..items` détermine les utilitaires d'administration et les produits d'entreprises à mettre à jour. Si le fichier est manquant ou vide, la mise à jour n'est configurée pour aucun utilitaire et aucun produit et ne sera pas effectuée.

.sync-off

Le fichier `.sync-off` désactive la mise à jour du produit. Le contenu n'a pas d'importance.

.deleted

Le fichier `.deleted` marque le produit comme supprimé. Toutes les révisions seront supprimées du fichier, la synchronisation avec le SGM est désactivée.

Fichiers d'exclusions lors de la mise à jour du référentiel du Serveur Dr.Web depuis le SGM

.sync-only

Le fichier `.sync-only` contient les expressions régulières déterminant la liste des fichiers du référentiel qui seront synchronisées lors de la mise à jour du référentiel depuis le SGM. Les fichiers du référentiel non spécifiés dans fichier `.sync-only` ne seront pas synchronisés. Si le fichier `.sync-only` est introuvable, tous les fichiers du référentiel seront synchronisés excepté les fichiers exclus conformément aux paramètres du fichier `.sync-ignore`.

.sync-ignore

Le fichier `.sync-ignore` contient les expressions régulières qui déterminent la liste des fichiers du référentiel à exclure de la synchronisation lors de la mise à jour du référentiel depuis le SGM.

Exemple d'un fichier aux exclusions

```
^windows-nt-x64/

^windows-nt/

^windows/
```

L'ordre d'utilisation des fichiers de configuration

Si les deux fichiers `.sync-only` et `.sync-ignore` sont présents pour le produit, alors le schéma d'actions suivant est utilisé :

1. D'abord s'applique `.sync-only`. Les fichiers non mentionnés dans `.sync-only` ne seront pas traités.
2. Ensuite, `.sync-ignore` s'applique aux fichiers restants.

Fichiers d'exclusions lors de la mise à jour des Agents Dr.Web depuis le Serveur Dr.Web

.state-only

Le fichier `.state-only` contient les expressions régulières déterminant la liste des fichiers qui seront synchronisées lors de la mise à jour des Agents Dr.Web depuis le Serveur Dr.Web. Les fichiers du référentiel non spécifiés dans fichier `.state-only` ne seront pas synchronisés. Si le fichier `.state-only` est introuvable, tous les fichiers du référentiel seront synchronisés excepté les fichiers du référentiel exclus conformément aux paramètres du fichier `.state-ignore`.

.state-ignore

Le fichier `.state-ignore` contient les expressions régulières déterminant la liste des fichiers qui seront exclus de la synchronisation lors de la mise à jour des Agents Dr.Web depuis le Serveur Dr.Web.

Exemple :

- il n'est pas requis de télécharger les langues d'interface allemande, chinoise et espagnole (les autres langues doivent être téléchargées),
- il n'est pas requis de recevoir les composants conçus pour les OS Windows 64-bits.

```
;^common/ru-.*\.dwl$ cela sera mis à jour

^common/de-.*\.dwl$

^common/cn-.*\.dwl$

^common/es-.*\.dwl$

^win/de-.*

^win/cn-.*

^windows-nt-x64\.*
```

L'ordre d'application de `.state-only` et de `.state-ignore` est équivalent à `.sync-only` et `.sync-ignore`.

Paramètres de l'envoi des notifications

Les fichiers du groupe `notify` permettent de créer le système de notifications en cas de la mise à jour réussie des produits correspondants du référentiel.

> Ces paramètres ne concernent que la notification **Le produit est mis à jour**. Les exclusions ne concernent pas les autres types de notifications.
>
> Les paramètres du système de notification sont décrits dans le **Manuel Administrateur**, p. Configuration des notifications.

.notify-only

Le fichier `.notify-only` contient la liste des fichiers du référentiel. En cas de modification de ces fichiers, une notification est envoyée.

.notify-ignore

Le fichier `.notify-ignore` contient la liste des fichiers du référentiel. En cas de modification de ces fichiers une notification n'est pas envoyée.

L'ordre d'utilisation des fichiers de configuration

Si les fichiers `.notify-only` et `.notify-ignore` sont présents pour le produit, alors le schéma d'actions suivant est utilisé :

1. En cas de mise à jour du produit, les fichiers mis à jour depuis le SGM sont comparés avec les listes des exclusions.
2. D'abord sont exclus les fichiers figurant dans la liste `.notify-ignore`.
3. Ensuite ce sont des fichiers qui ne figurent pas dans la liste `.notify-only` qui sont exclus.
4. S'il reste des fichiers qui ne sont pas exclus aux étapes précédentes, les notifications sont envoyées.

Si les fichiers `.notify-only` et `.notify-ignore` ne sont pas présents, alors les notifications seront toujours envoyées (si elles sont actives sur la page **Configuration des notifications** dans le Centre de gestion).

Exemple :

Si l'exclusion `^.vdb.lzma$` est spécifiée dans le fichier `.notify-ignore` et que seuls les fichiers des bases virales sont mis à jour, la notification ne sera pas envoyée. Si, outre les bases virales, le noyau `drweb32.dll` est également mis à jour, alors la notification sera envoyée.

Paramètres du blocage

.delay-config

Le fichier `.delay-config` contient les paramètres qui interdisent de basculer le produit vers une nouvelle révision. Le référentiel continue à diffuser la révision antérieure, la synchronisation ne s'effectue plus (le statut du produit est « bloqué »). Si l'administrateur considère la révision acceptée comme valable pour la diffusion, il doit autoriser sa diffusion dans le Centre de gestion (voir **Manuel Administrateur**, p. Gestion du référentiel du Serveur Dr.Web).

Le fichier contient deux paramètres qui ne sont pas sensibles à la casse et qui sont séparés par un point-virgule.

Format du fichier :

```
Delay [ON|OFF|APPROVAL]; UseFilter [YES|NO]
```

Paramètre	Valeurs possibles	Description
`Delay`	`ON|OFF|APPROVAL`	• `ON` : le blocage des mises à jour est activé. • `OFF` : le blocage des mises à jour est désactivé. • `APPROVAL` : blocage des mises à jour du produit jusqu'à ce que l'administrateur les approuve.
`UseFilter`	`YES|NO`	• `Yes` : bloquer les mises à jour uniquement si les fichiers mis à jour correspondent à la liste des exclusions dans le fichier `.delay-only`. • `No` : bloquer les mises à jour en tout cas.

Exemple :

```
Delay ON; UseFilter NO
```

.delay-only

Le fichier `.delay-only` contient la liste des fichiers dont la modification entraîne une interdiction de basculer le produit vers la nouvelle révision. La liste des fichiers est spécifiée au format des expressions régulières.

Si le fichier de la mise à jour du référentiel correspond aux masques indiqués et le paramètre `UseFilter` est activé dans le fichier `.sync-only`, la révision sera bloquée.

.rev-to-keep

Le fichier `.rev-to-keep` contient le nombre de révisions stockées.

Exemple :

```
3
```

.on-demand

La présence du fichier signifie que la synchronisation du produit sur demande est activée, c'est-à-dire s'il y a des clients demandant ce produit.

.is-sync-off-in

La présence du fichier indique que la réception des mises à jour du produit par les liaisons entre serveurs est désactivée.

.is-sync-off-out

La présence du fichier indique que la distribution des mises à jour du produit par les liaisons entre serveurs est désactivée.

.no-platform

La présence du fichier indique que les dossiers du haut niveau de la révision du produit ne sont pas considérés comme plateformes, c'est-à-dire, la révision concerne toute plateforme.

Annexe F. Format des fichiers de configuration

Ce paragraphe vous propose une description du format des fichiers suivants :

Fichier	Description
drwcsd.conf	Fichier de configuration du Serveur Dr.Web.
webmin.conf	Fichier de configuration du Centre de gestion de la sécurité Dr.Web.

Fichier	Description
download.conf	Fichier de configuration des données téléchargées du Serveur Dr.Web.
drwcsd-proxy.conf	Fichier de configuration du Serveur proxy Dr.Web.
drwreploader.conf	Fichier de configuration du Chargeur du référentiel.

Si l'Agent tourne sur le poste sur lequel est installé un de ces composants et que l'option d'autoprotection est activée, il est nécessaire de désactiver le composant d'autoprotection Dr.Web Self-protection via les paramètres de l'Agent Dr.Web avant de procéder à la modification des fichiers de configuration.

Après l'enregistrement de toutes les modifications apportées, il est recommandé de réactiver le composant Dr.Web Self-protection.

F1. Fichier de configuration du Serveur Dr.Web

Le fichier de configuration du Serveur Dr.Web `drwcsd.conf` se trouve par défaut dans le sous-répertoire `etc` du répertoire racine du Serveur Dr.Web. Au démarrage du Serveur Dr.Web, il est possible de spécifier un emplacement non standard du fichier de configuration ainsi que son nom avec une clé de la ligne de commande (pour en savoir plus, consultez l'Annexe G3. Serveur Dr.Web).

Pour éditer manuellement le fichier de configuration du Serveur Dr.Web

1. Arrêtez le Serveur Dr.Web (voir le **Manuel administrateur**, p. Serveur Dr.Web).
2. Désactivez l'autoprotection (si l'Agent Dr.Web tourne sur l'ordinateur avec l'autoprotection activée, utilisez le menu contextuel de l'Agent Dr.Web).
3. Apportez les modifications nécessaires dans le fichier de configuration du Serveur Dr.Web.
4. Lancez le Serveur Dr.Web (voir le **Manuel administrateur**, p. Serveur Dr.Web).

Format du fichier de configuration du Serveur Dr.Web

Le fichier de configuration du Serveur Dr.Web est fourni au format XML.

Description des paramètres du fichier de configuration du Serveur Dr.Web :

- `<version value="" />`

  Version actuelle du fichier de configuration.

- `<name value="" />`

  Nom du Serveur Dr.Web ou du cluster des Serveurs Dr.Web via lequel les Agents Dr.Web, les installateurs des Agents Dr.Web et le Centre de gestion vont envoyer les requêtes de recherches.

Laissez la valeur du paramètre vide ("" — utilisé par défaut) pour utiliser le nom de l'ordinateur sur lequel le Serveur Dr.Web est installé.

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

1. Si le serveur DNS local fonctionne dans le réseau, il faut y créer un nom à part pour le Serveur Dr.Web et pour le Serveur proxy Dr.Web (par exemple, `drwebes.company.lan`).
2. Dans les paramètres des Agents Dr.Web, il faut indiquer le nom du Serveurs Dr.Web au format FQDN.
3. En plus du nom au format FQDN, il est recommandé d'ajouter dans les paramètres de l'Agent Dr.Web l'adresse du Serveur Dr.Web et maintenir cette adresse à jour en cas de son changement. Dans ce cas, s'il est impossible d'utiliser le nom du serveur, l'agent tentera de se connecter par l'adresse du serveur.

- `<id value="" />`

  Identificateur unique du Serveur Dr.Web. Dans les versions précédentes, il a été stocké dans une clé de licence du Serveur Dr.Web. Depuis la version 10, il est sauvegardé dans le fichier de configuration du Serveur Dr.Web.

- `<passwd-salt value="" />`

  Salage. Ligne de données aléatoires qui est ajoutée au mot de passe de l'administrateur. Ensuite la valeur unie est traitée par une fonction de hachage et sauvegardée dans la base de données pour protéger le mot de passe contre les attaques par force brute. Il est généré par défaut lors de l'installation et la mise à niveau du Serveur Dr.Web.

  Outre le salage statique, le salage dynamique est généré pour chaque mot de passe. La norme de génération de clé à la base du mot de passe PBKDF2 est utilisée en tant que code d'authentification HMAC lors du calcul de l'empreinte du mot de passe salé. Ainsi le mot de passe est combiné au sel et hashé plusieurs fois. Le salage statique est désactivé par défaut, le salage dynamique est toujours utilisé.

  

  En cas de présence du salage, il est impossible de consulter et modifier le mot de passe de l'administrateur avec l'utilitaire de gestion de la base de données du Serveur Dr.Web (`drwidbsh3`).

  

  En cas d'utilisation du cluster de Serveurs Dr.Web, il faut spécifier manuellement la même valeur de salage sur tous les Serveurs Dr.Web faisant partie du cluster.

- `<location city="" country="" department="" floor="" latitude="" longitude="" organization="" province="" room="" street="" />`

  Localisation du Serveur Dr.Web.

  Description des attributs :

Attribut	Description
city	Ville
country	Pays
department	Nom du département
floor	Étage
latitude	Latitude
longitude	Longitude
organization	Nom de l'organisation
province	Nom de la région
room	Numéro de la chambre
street	Nom de la rue

- `<threads count="" />`

  Nombre de flux traitant les données issus des clients du Serveur Dr.Web (des Agents Dr.Web et de leurs installateurs, des Serveurs voisins Dr.Web, des Serveurs proxy Dr.Web). La valeur minimale est de 5. La valeur 5 est spécifiée par défaut.

  Ce paramètre influence les performances du Serveur Dr.Web. Si vous utilisez la base de données embarquée, il n'est pas recommandé de modifier la valeur par défaut. Si vous utilisez la base de données externe, une valeur supérieure peut être requise (voir la rubrique Charge sur le Serveur Dr.Web et paramètres de configuration recommandés). Si vous gérez un réseau avec un grand nombre de connexions des clients au Serveur Dr.Web, il est recommandé de consulter le support technique de la société Doctor Web avant de modifier le paramètre.

- `<newbie approve-to-group="" mode="" />`

  Mode d'accès de nouveaux postes.

  Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
approve-to-group	–	Groupe qui sera désigné par défaut comme primaire pour les nouveaux postes en mode **Approuver l'accès**	Valeur vide ce qui signifie désigner le groupe **Everyone** comme primaire.

Attribut	Valeurs autorisées	Description	Par défaut
		automatiquement (`mode='open'`).	
`mode`	• `open` : approuver l'accès automatiquement, • `closed` : toujours refuser l'accès, • `approval` : approuver l'accès manuellement.	Politique d'approbation des nouveaux postes.	–

Pour en savoir plus, voir **Manuel Administrateur**, p. Politique d'approbation des nouveaux postes.

- `<emplace-auto enabled="" />`

  Mode de création des comptes de postes manquants dans le Centre de gestion lors de l'installation des Agents Dr.Web depuis le package d'installation de groupe.

Attribut	Valeurs autorisées	Par défaut
`enabled`	• `yes` : créer automatiquement des comptes de postes manquants, • `no` : l'installation est possible seulement par le nombre de comptes déjà créés dans le groupe dont le package d'installation est lancé.	`yes`

- `<unauthorized-to-newbie enabled="" />`

  Politique des actions appliquées aux postes non approuvés. Les valeurs autorisées de l'attribut `enabled` :

  - `yes` : les postes qui n'ont pas été approuvés (par exemple, en cas d'endommagement de la base de données) seront spécifiés comme novices,
  - `no` (par défaut) : mode de fonctionnement normal.

- `<maximum-authorization-queue size="" />`

  Nombre maximum des postes dans la file d'attente de l'authentification sur le Serveur Dr.Web. Il est recommandé de ne pas modifier la valeur du paramètre sans avoir consulté le support technique de Doctor Web.

- `<reverse-resolve enabled="" />`

  Remplacer les adresses IP par les noms DNS des ordinateurs dans le fichier de journal du Serveur Dr.Web. Les valeurs autorisées de l'attribut `enabled` :

  - `yes` : afficher les noms DNS,
  - `no` (par défaut) : afficher les adresses IP.

- `<replace-netbios-names enabled="" host="" />`

  Remplacer les noms NetBIOS d'ordinateurs par les noms DNS.

Description des attributs :

Attribut	Valeurs autorisées	Description
`enabled`	• `yes` : remplacer, • `no` : ne pas remplacer. Les paramètres `<agent-host-names />` seront appliqués.	Mode de remplacement de noms NetBIOS.
`host`	• `yes` : afficher les noms DNS partiellement qualifiés (jusqu'au point dans FQDN), • `no` : afficher les noms DNS pleinement qualifiés (FQDN).	Format du nom affiché après le remplacement.

- `<agent-host-names mode="" />`

  Mode d'affichage de noms d'ordinateurs dans le réseau antivirus en cas d'appel au Serveur Dr.Web. Valeurs possibles de l'attribut `mode` :

  - `netbios` : afficher les noms NetBIOS (utilisé par défaut en cas de valeur vide de l'attribut ou en cas d'absence du paramètre entier),
  - `fqdn` : afficher les noms DNS pleinement qualifiés (FQDN),
  - `host` : afficher les noms DNS partiellement qualifiés (jusqu'au point dans FQDN).

- `<dns>`

  Paramètres DNS.

  - `<timeout value="" />`

    Délai en secondes pour autoriser les requêtes DNS directes/inverses. Laissez le champ vide pour ne pas limiter la durée d'attente pour l'autorisation.

  - `<retry value="" />`

    Nombre maximum de requêtes DNS réitérées en cas d'échec d'une requête DNS.

  - `<cache enabled="" negative-ttl="" positive-ttl="" />`

    Durée de conservation de réponses du serveur DNS dans le cache.

    Description des attributs :

Attribut	Valeurs autorisées	Description
`enabled`	• `yes` : stocker les réponses dans le cache, • `no` : ne pas stocker les réponses dans le cache.	Mode de stockage des réponses dans le cache.
`negative-ttl`	–	Durée de conservation dans le cache (TTL) des réponses négatives du serveur DNS en minutes.

Attribut	Valeurs autorisées	Description
positive-ttl	–	Durée de conservation dans le cache (TTL) des réponses positives du serveur DNS en minutes.

  - <servers>

    Liste des serveurs DNS qui remplacent la liste système par défaut. Elle contient un ou plusieurs éléments enfants <server address="" />, dans lesquels le paramètre address détermine l'adresse IP du serveur.

  - <domains>

    Liste des domaines DNS qui remplace la liste système par défaut. Elle contient un ou plusieurs éléments enfants <domain name="" />, dans lesquels le paramètre name détermine le nom de domaine.

- <cache>

  Paramètres de mise en cache.

  L'élément <cache> contient les éléments enfants suivants :

  - <interval value="" />

    Fréquence de nettoyage complet du cache en secondes.

  - <quarantine ttl="" />

    Fréquence de la suppression des fichiers en quarantaine du Serveur Dr.Web en secondes. Par défaut — 604800 (une semaine).

  - <download ttl="" />

    Fréquence de suppression de packages d'installation personnels. Par défaut — 604800 (une semaine).

  - <repository ttl="" />

    Fréquence de la suppression des fichiers en cache du référentiel du Serveur Dr.Web, en secondes.

  - <file ttl="" />

    Fréquence de nettoyage du cache de fichiers en secondes. Par défaut — 604800 (une semaine).

- <replace-station-description enabled="" />

  Activer la synchronisation des descriptions de postes entre le Serveur Dr.Web et le champ **Computer description** sur la page **System properties** du poste. Les valeurs autorisées de l'attribut enabled :

  - yes : remplacer la description sur le Serveur Dr.Web par la description du poste,
  - no (par défaut) : ignorer la description sur le poste.

- <time-discrepancy value="" />

  Décalage possible entre l'heure système du Serveur Dr.Web et celle des Agents Dr.Web en minutes. Si le décalage est supérieur à la valeur spécifiée, ceci sera indiqué dans le statut du poste

sur le Serveur Dr.Web. Par défaut, un décalage de 3 minutes est possible. La valeur 0 signifie qu'aucune vérification ne sera effectuée.

- `<encryption mode="" />`

  Mode de chiffrement du trafic. Valeurs autorisées de l'attribut `mode` :

  - `yes` : utiliser le chiffrement,
  - `no` : ne pas utiliser le chiffrement,
  - `possible` : le chiffrement est autorisé.

  Par défaut `yes`.

  Pour plus d'information, voir le **Manuel Administrateur**, p. Chiffrement et compression du trafic.

- `<compression level="" mode="" />`

  Mode de compression du trafic.

  Description des attributs :

Attribut	Valeurs autorisées	Description
`level`	Nombre entier de 1 à 9.	Niveau de compression.
`mode`	• `yes` : utiliser la compression, • `no` : ne pas utiliser la compression, • `possible` : la compression est autorisée.	Mode de compression.

  Pour plus d'information, voir le **Manuel Administrateur**, p. Chiffrement et compression du trafic.

- `<track-agent-jobs enabled="" />`

  Autoriser la surveillance et l'écriture des résultats de l'exécution des tâches sur les postes dans la base de données du Serveur Dr.Web. Les valeurs autorisées de l'attribut `enabled` : `yes` ou `no`.

- `<track-agent-status enabled="" />`

  Autoriser la surveillance de changement des statuts des postes et l'écriture des informations dans la base de données du Serveur Dr.Web. Valeurs possibles de l'attribut `enabled` : `yes` ou `no`.

- `<track-virus-bases enabled="" />`

  Autoriser la surveillance de changement des statuts (du contenu, du changement) des bases de données virales et l'écriture des informations dans la base de données du Serveur Dr.Web. Les valeurs autorisées de l'attribut `enabled` : `yes` ou `no`. Le paramètre est ignoré, si `<track-agent-status enabled="no" />`.

- `<track-agent-modules enabled="" />`

  Autoriser la surveillance de la version du module et l'écriture des informations dans la base de données du Serveur Dr.Web. Les valeurs autorisées de l'attribut `enabled` : `yes` ou `no`.

- `<track-agent-components enabled="" />`

  Autoriser la surveillance de la liste des composants installs sur les postes et l'écriture des informations dans la base de données du Serveur Dr.Web. Les valeurs autorisées de l'attribut `enabled` : `yes` ou `no`.

- `<track-agent-userlogon enabled="" />`

  Autoriser la surveillance des Sessions d'utilisateurs sur les postes et l'écriture des informations dans la base de données du Serveur Dr.Web. Les valeurs autorisées de l'attribut `enabled` : `yes` ou `no`.

- `<track-agent-environment enabled="" />`

  Autoriser la surveillance de la composition du matériel et des logiciels sur les postes et l'écriture des informations dans la base de données du Serveur Dr.Web. Les valeurs autorisées de l'attribut `enabled` : `yes` ou `no`.

- `<keep-run-information enabled="" />`

  Autoriser la surveillance des informations sur le démarrage et l'arrêt des composants sur les postes et l'écriture des informations dans la base de données du Serveur Dr.Web. Valeurs possibles de l'attribut `enabled` : `yes` ou `no`.

- `<keep-infection enabled="" />`

  Autoriser la détection des menaces sur les postes et l'écriture des informations dans la base de données du Serveur Dr.Web. Valeurs possibles de l'attribut `enabled` : `yes` ou `no`.

- `<keep-scan-errors enabled="" />`

  Autoriser la détection des erreurs de scan sur les postes et l'écriture des informations dans la base de données du Serveur Dr.Web. Les valeurs autorisées de l'attribut `enabled` : `yes` ou `no`.

- `<keep-scan-statistics enabled="" />`

  Autoriser la surveillance des statistiques de scan sur les postes et l'écriture des informations dans la base de données du Serveur Dr.Web. Les valeurs autorisées de l'attribut `enabled` : `yes` ou `no`.

- `<keep-installation enabled="" />`

  Autoriser la surveillance des informations sur les installations des Agents Dr.Web sur les postes et l'enregistrement des informations dans la base de données du Serveur Dr.Web. Valeurs possibles de l'attribut `enabled` : `yes` ou `no`.

- `<keep-blocked-devices enabled="" />`

  Autoriser la surveillance des informations sur les périphériques bloqués par le composant Office Control et l'enregistrement des informations dans la base de données du Serveur Dr.Web. Valeurs possibles de l'attribut `enabled` : `yes` ou `no`.

- `<keep-appcontrol-activity enabled="" />`

  Autoriser la surveillance de l'activité des processus sur les postes enregistrée par le Contrôle des applications (pour remplir le Répertoire d'applications) et l'enregistrement des informations dans la base de données du Serveur Dr.Web. Les valeurs autorisées de l'attribut `enabled` : `yes` ou `no`.

- `<keep-appcontrol-block enabled="" />`

  Autoriser la surveillance de blocage des processus sur les postes par le Contrôle des applications et l'enregistrement des informations dans la base de données du Serveur Dr.Web. Les valeurs autorisées de l'attribut `enabled` : `yes` ou `no`.

- `<quarantine enabled="" />`

  Autoriser la surveillance du statut de la Quarantaine sur les postes et l'écriture des informations dans la base de données du Serveur Dr.Web. Valeurs possibles de l'attribut `enabled` : `yes` ou `no`.

- `<update-bandwidth queue-size="" value="" />`

  Largeur maximale de la bande passante du trafic réseau en Ko/s pour le transfert des mises à jour entre le Serveur Dr.Web et les Agents Dr.Web.

  Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
`queue-size`	• nombre entier positif, • `unlimited`.	Nombre maximum des sessions de distribution des mises à jour lancées en même temps depuis ce Serveur Dr.Web. Si le nombre maximum est atteint, les requêtes des Agents Dr.Web sont placées dans une file d'attente. La taille de la file d'attente n'est pas limitée.	`unlimited`
`value`	• vitesse maximale en Ko/s, • `unlimited`.	Valeur maximale de la vitesse sommaire de transfert des mises à jour.	`unlimited`

- `<install-bandwidth queue-size="" value="" />`

  Largeur maximale de la bande passante du trafic réseau en Ko/s pour le transfert des données entre le Serveur Dr.Web et les Agents Dr.Web sur les postes.

  Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
`queue-size`	• nombre entier positif, • `unlimited`.	Nombre maximum des sessions d'installation de l'Agent Dr.Web lancées en même temps depuis ce Serveur Dr.Web. Si le nombre maximum est atteint, les requêtes des Agents Dr.Web sont placées dans une file d'attente. La taille de la file d'attente n'est pas limitée.	`unlimited`
`value`	• vitesse maximale en Ko/s, • `unlimited`.	Valeur maximale de la vitesse cumulée de transfert de données lors de l'installation des Agents Dr.Web.	`unlimited`

- `<geolocation enabled="" startup-sync="" />`

  Autoriser la synchronisation des emplacements géographiques de postes entre les Serveurs Dr.Web.

  Description des attributs :

Attribut	Valeurs autorisées	Description
`enabled`	• `yes` : autoriser la synchronisation, • `no` : désactiver la synchronisation.	Mode de synchronisation.

Attribut	Valeurs autorisées	Description
`startup-sync`	Nombre entier positif.	Le nombre de postes sans coordonnées géographiques, dont les informations sont demandées lors de l'établissement d'une connexion entre les Serveurs Dr.Web.

- `<audit enabled="" />`

  Autoriser la surveillance des opérations d'administrateur dans le Centre de gestion de la sécurité Dr.Web et l'écriture des informations dans la base de données du Serveur Dr.Web. Valeurs possibles de l'attribut `enabled` : `yes` ou `no`.

- `<audit-internals enabled="" />`

  Autoriser la surveillance des opérations intérieures du Serveur Dr.Web et l'écriture des informations dans la base de données du Serveur Dr.Web. Les valeurs autorisées de l'attribut `enabled` : `yes` ou `no`.

- `<audit-xml-api enabled="" />`

  Autoriser la surveillance des opérations via Web API et l'écriture des informations dans la base de données du Serveur Dr.Web. Valeurs possibles de l'attribut `enabled` : `yes` ou `no`.

- `<proxy auth-list="" enabled="" host="" password="" user="" />`

  Paramètres de connexion au Serveur Dr.Web via le serveur proxy HTTP.

  Description des attributs :

Attribut	Valeurs autorisées	Description

`auth-list`	• `none` : ne pas utiliser l'authentification,
	• `any` : toute méthode supportée,
	• `safe` : toute méthode sécurisée supportée,
	• les méthodes suivantes. S'il y en a plusieurs, les méthodes nécessaires doivent être séparées par un espace :
	  ▫ `basic`
	  ▫ `digest`
	  ▫ `digestie`
	  ▫ `ntlmwb`
	  ▫ `ntlm`
	  ▫ `negotiate`
		Type d'authentification sur le serveur proxy. Par défaut - `any`.

`enabled`	• `yes` : utiliser le serveur proxy, • `no` : ne pas utiliser le serveur proxy.	Mode de connexion au Serveur Dr.Web via le serveur proxy HTTP.

Attribut	Valeurs autorisées	Description
`host`	–	Adresse du serveur proxy.
`password`	–	Mot de passe de l'utilisateur du serveur proxy, si l'authentification sur le serveur proxy est requise.
`user`	–	Nom de l'utilisateur du serveur proxy, si l'authentification sur le serveur proxy est requise.

Lors de la création de la liste des méthodes d'authentification disponibles pour le serveur proxy, il est possible d'utiliser l'étiquette `only` (ajoutée à la fin de la liste séparée d'un espace) pour modifier l'algorithme de sélection des méthodes d'authentification.

Pour en savoir plus, consultez https://curl.se/libcurl/c/CURLOPT_HTTPAUTH.html.

- `<statistics enabled="" id="" interval="" />`

  Paramètres d'envoi des statistiques sur les événements viraux à Doctor Web, à la rubrique https://stat.drweb.com/.

  Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
`enabled`	• `yes` : envoyer les statistiques, • `no` : ne pas envoyer les statistiques.	Mode d'envoi des statistiques à Doctor Web.	–
`id`	–	MD5 de la clé de licence de l'Agent Dr.Web.	–
`interval`	Nombre entier positif.	Intervalle entre les envois des statistiques en minutes.	30

- `<cluster>`

  Paramètres du cluster des Serveurs Dr.Web pour l'échange de informations en cas de configuration du réseau antivirus multi-serveurs.

  Contient un ou plusieurs éléments enfants `<on multicast-group="" port="" interface="" />`.

  Description des attributs :

Attribut	Description
`multicast-group`	Adresse IP du groupe multicast via lequel les Serveurs Dr.Web vont échanger des informations.

Attribut	Description
port	Numéro de port de l'interface réseau à laquelle le protocole de transport sera rattaché pour la transmission des informations vers le groupe multicast.
interface	Adresse IP de l'interface réseau à laquelle le protocole de transport est lié pour transmettre les données au groupe multicast.

- `<multicast-updates enabled="" />`

  Configuration du transfert des mises à jour aux postes de travail via le protocole multicast. Les valeurs autorisées de l'attribut `enabled` : `yes` ou `no`.

  L'élément `<multicast-updates>` contient les éléments enfant et les attributs suivants :

Élément enfant	Attribut	Description	Par défaut
port <port value="" />	value	Numéro du port de l'interface réseau du Serveur Dr.Web auquel le protocole multicast de transport est lié pour transmettre des mises à jour. Ce port sera utilisé par tous les groupes multicast. Pour les mises à jour multicast, il faut spécifier n'importe quel port libre, autre que le port spécifié dans les paramètres pour le fonctionnement du protocole de transport du Serveur Dr.Web.	2197
ttl <ttl value="" />	value	Durée de vie du datagramme UDP transmis. La valeur spécifiée sera utilisée par tous les groupes multicast.	8
group <group address="" />	address	Adresse IP du groupe multicast via lequel les postes recevront des mises à jour multicast.	233.192.86.0 pour IPv4 FF0E::176 pour IPv6
on <on interface="" ttl="" />	interface	Adresse IP de l'interface réseau du Serveur Dr.Web à laquelle le protocole multicast de transport est lié pour transmettre des mises à jour.	–
	ttl	Durée de vie du datagramme UDP transmis par l'interface réseau spécifiée. Possède de priorité sur l'élément enfant commun <ttl value="" />.	8
transfer <transfer datagram-	datagram-size	Taille du datagramme UDP : taille des datagrammes UDP utilisés par le protocole multicast, en octets.	1400

Élément enfant	Attribut	Description	Par défaut
size="" assembly-timeout="" updates-interval="" chunks-interval="" resend-interval="" silence-interval="" accumulate-interval="" announce-send-times="" />		L'intervalle autorisé est 512–8192. Pour éviter la fragmentation, il est recommandé d'indiquer une valeur inférieure au MTU (Maximum Transmission Unit) du réseau utilisé.	
	assembly-timeout	Délai de transmission du fichier (ms) : durant cet intervalle de temps, le fichier de mise à jour unique est transmis, après quoi le Serveur Dr.Web commence à envoyer le fichier suivant. Tous les fichiers qui n'ont pu être transmis à l'étape de la mise à jour via le protocole multicast seront transmis lors du processus standard de mise à jour via le protocole TCP.	180000
	updates-interval	Durée des mises à jour multicast (ms) : durée du processus de mise à jour via le protocole multicast. Tous les fichiers qui n'ont pu être transmis à l'étape de la mise à jour via le protocole multicast seront transmis lors du processus standard de mise à jour via le protocole TCP.	600000
	chunks-interval	Intervalle de transmission des packages (ms) : intervalle de transmission des packages à un groupe multicast. Un intervalle faible peut provoquer des pertes significatives durant le transfert des packages et une surcharge du réseau. Il est recommandé de modifier ce paramètre.	14
	resend-interval	Intervalle entre les demandes de retransmission (ms) : avec cet intervalle, les Agents Dr.Web envoient des demandes de retransmission des paquets perdus. Le Serveur Dr.Web accumule ces requêtes puis renvoie les blocs perdus.	1000
	silence-interval	Intervalle de "Silence" sur la ligne (ms) : lorsqu'une transmission d'un fichier est terminée avant que la durée allouée ait	10000

Élément enfant	Attribut	Description	Par défaut
		expiré, si, durant l'intervalle de "silence" indiqué, aucune requête n'est envoyée par l'Agent Dr.Web pour la retransmission de packages perdus, le Serveur Dr.Web considère que tous les Agents Dr.Web ont reçu les fichiers de mise à jour et commence à envoyer le fichier suivant.	
	`accumulate-interval`	Intervalle d'accumulation des requêtes de retransmission (ms) : durant cet intervalle, le Serveur Dr.Web accumule les requêtes des Agents Dr.Web pour la retransmission des packages perdus. Les Agents Dr.Web redemandent les packages perdus. Le Serveur Dr.Web accumule ces requêtes durant un délai de temps spécifié, après quoi il envoie les blocs perdus.	2000
	`announce-send-times`	Nombre d'annonces de transfert du fichier : nombre de fois que le Serveur Dr.Web annonce le transfert du fichier au groupe multicast avant la transmission des mises a jour. En cas d'annonce, un datagramme UDP avec les métadonnées du fichier est envoyée au groupe multicast. L'augmentation du nombre d'annonces peut améliorer la sécurité de transmission mais elle peut provoquer la réduction du volume de données qui peut être transmis dans le délai imparti pour la mise à jour par le protocole multicast.	3

L'élément `<multicast-updates>` peut également contenir l'élément enfant facultatif `<acl>` qui est utilisé pour la création des listes d'accès. Cela permet de limiter la liste d'adresses TCP des postes qui pourront recevoir des mises à jour de groupes depuis ce Serveur Dr.Web par le protocole multicast. Par défaut. l'élément enfant `<acl>` n'est pas présent ce qui signifie l'absence de toute restriction.

`<acl>` au sein de`<multicast-updates>` contient les éléments enfants suivants :

- `<priority mode="" />`

  Établit la priorité des listes. Les valeurs autorisées de l'attribut `mode` : `allow` ou `deny`. En cas de la valeur `<priority mode="deny" />`, la liste `<deny >` possède une priorité plus importante que la liste `<allow>`. Les adresses qui ne sont incluses dans aucune liste ou qui sont incluses

dans les deux listes sont refusées. Seules les adresses incluses dans la liste `<allow>` et non incluses dans la liste `<deny>` sont autorisées.

- `<allow>`

  Liste des adresses TCP pour lesquelles la mise à jour via protocole multicast est disponibles. L'élément `<allow>` contient un ou plusieurs éléments enfants `<ip address="" />` qui servent à spécifier les adresses autorisées au format IPv4 ou `<ip6 address="" />` pour spécifier les adresses autorisées au format Ipv6. Dans l'attribut `address` sont spécifiées les adresses réseau au format : *<Adresse IP>*/`[`*<préfixe>*`]`.

- `<deny>`

  Liste des adresses TCP pour lesquelles la mise à jour via le protocole multicast n'est pas disponibles. L'élément `<deny>` contient un ou plusieurs éléments enfants `<ip address="" />` qui servent à spécifier les adresses bloquées au format IPv4 ou `<ip6 address="" />` pour spécifier les adresses bloquées au format Ipv6. Dans l'attribut `address` sont spécifiées les adresses réseau au format : *<Adresse IP>*/`[`*<préfixe>*`]`.

- `<database connections="" speedup="" />`

  Définition de la base de données.

  Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
`connections`	Nombre entier positif.	Nombre maximum autorisé des connexions de la base de données avec le Serveur Dr.Web. Si vous utilisez la base de données embarquée, il n'est pas recommandé de modifier la valeur par défaut. Si vous utilisez la base de données externe, une valeur supérieure peut être requise (voir la rubrique Charge sur le Serveur Dr.Web et paramètres de configuration recommandés). Si vous gérez un réseau avec un grand nombre de connexions des clients au Serveur Dr.Web, il est recommandé de consulter le support technique de la société Doctor Web avant de modifier le paramètre.	2
`speedup`	`yes | no`	Nettoyer automatiquement la base de données après son initialisation, la mise à jour et l'importation (voir le **Manuel Administrateur**, le p. Base de données).	`yes`

  L'élément `<database>` contient un des éléments enfants suivants :

L'élément <database> peut contenir un seul élément enfant déterminant la base de données concrète.

Le masque de fichier de configuration peut contenir des attributs de bases de données qui ne sont pas mentionnés dans des descriptions. Il n'est pas recommandé de modifier ces attributs sans avoir consulté le support technique de Doctor Web.

- `<sqlite dbfile="" cache="" cachesize="" readuncommitted="" precompiledcache="" synchronous="" checkintegrity="" autorepair="" mmapsize="" wal="" wal-max-pages="" wal-max-seconds="" />`

  Détermine la base de données embarquée SQLite3.

  Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
`dbfile`	–	Nom de fichier de la base de données.	`database.sqlite`
`cache`	`SHARED` | `PRIVATE`	Mode de mise en cache.	`SHARED`
`cachesize`	Nombre entier positif.	Taille de la mémoire cache de la base de données (en pages de 1.5 Ko).	2048
`readuncommitted`	`on` | `off`	Passage au niveau d'isolation de transaction READ UNCOMMITTED (lecture des données qui ont été modifiées ou supprimées mais ne sont pas enregistrées par une autre transaction).	`off`
`precompiledcache`	Nombre entier positif.	Taille du cache des opérateurs sql précompilés en octets.	1048576
`synchronous`	• `TRUE` ou `FULL` : synchrone • `FALSE` ou `NORMAL` : normal • `OFF` : asynchrone	Mode d'écriture de données.	`FULL`
`checkintegrity`	`quick` | `full` | `no`	Vérifier l'intégrité de l'image de la base de données au démarrage du Serveur Dr.Web.	`quick`
`autorepair`	`yes` | `no`	Restauration automatique de l'image corrompue de la base de	`no`

Attribut	Valeurs autorisées	Description	Par défaut
		données au démarrage du Serveur Dr.Web.	
mmapsize	Nombre entier positif.	Taille maximum (en octets) du fichier de la base de données qui peut être mappé en espace d'adresse du processus en une fois.	• pour les OS de la famille UNIX — 10485760 • sous Windows — 0
wal	yes | no	Utilisation de la journalisation préventive (Write-Ahead Logging).	yes
wal-max-pages	–	Nombre maximum de pages de modifications à atteindre pour que toutes les pages soient écrites sur le disque.	1000
wal-max-seconds	–	Délai maximum pour retarder l'écriture des pages sur le disque (en secondes).	30

- `<pgsql dbname="drwcs" host="localhost" port="5432" options="" requiressl="" user="" password="" temp_tablespaces="" default_transaction_isolation="" debugproto="yes" />`

  Détermine la base de données externe PostgreSQL.

  Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
dbname	–	Nom de fichier de la base de données.	–
host	–	Adresse du serveur PostgreSQL ou le chemin vers le socket UNIX.	–
port	–	Numéro de port du serveur PostgreSQL ou l'extension de fichier du socket UNIX.	–
options	–	Paramètres de la ligne de commande pour envoyer sur le serveur de la base de données. Pour en savoir plus, voir le chapitre 18	–

Attribut	Valeurs autorisées	Description	Par défaut
		https://www.postgresql.org/docs/9.1/libpq-connect.html	
requiressl	• 1 | 0 (via le Centre de gestion) • y | n • yes | no • on | off	N'utiliser que les connexion SSL.	• 0 • y • yes • on
user	–	Nom de l'utilisateur de la base de données.	–
password	–	Mot de passe d'utilisateur de la base de données.	–
temp_tablespaces	–	Espace de nom pour les tableaux temporaires de base de données.	–
default_transaction_isolation	• read uncommitted • read committed • repeatable read • serializable	Mode d'isolement des transactions.	read committed
debugproto	• yes | no • on | off	Enregistrer le journal de débogage du SGBD.	• yes • on

- `<oracle connectionstring="" user="" password="" client="" prefetch-rows="0" prefetch-mem="0" />`

  Détermine la base de données externe Oracle.

  Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
connectionstring	–	La ligne contenant Oracle SQL Connect URL ou les paires clé-valeur d'Oracle Net.	–
user	–	Nom d'utilisateur de la base de données.	–
password	–	Mot de passe d'utilisateur de la base de données.	–

Attribut	Valeurs autorisées	Description	Par défaut
client	–	Chemin vers le client pour l'accès à la BD Oracle (Oracle Instant Client). Le Serveur Dr.Web est fourni avec Oracle Instant Client en version 11. Si vous utilisez les serveurs Oracle en versions plus récentes, ou en cas d'erreurs liées au pilote fourni pour la BD Oracle, vous pouvez télécharger un pilote nécessaire sur le site Oracle et spécifier le chemin d'accès au pilote dans le champ en question.	–
prefetch-rows	0–65535	Nombre de lignes à prérécupérer lors de l'exécution d'une requête sur la base de données.	0 : utiliser la valeur = 1 (valeur par défaut de la base de données)
prefetch-mem	0–65535	Mémoire allouée aux lignes à prérécupérer lors de l'exécution d'une requête sur la base de données.	0 : n'est pas limité

- `<odbc dsn="drwcs" user="" pass="" limit="" transaction="DEFAULT" />`

  Détermine la connexion à la base de données externe via ODBC.

  Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
dsn	–	Nom de la source de données ODBC.	drwcs
user	–	Nom d'utilisateur de la base de données.	drwcs
pass	–	Mot de passe d'utilisateur de la base de données.	drwcs
limit	Nombre entier positif.	Se reconnecter au SGBD après le nombre indiqué de transactions.	0 : ne pas se reconnecter
transaction	• SERIALIZABLE : sérialisation • READ_UNCOMMITTED : lecture de données non validées	Mode d'isolement des transactions.	DEFAULT

Attribut	Valeurs autorisées	Description	Par défaut
	• READ_COMMITTED : lecture de données validées • REPEATABLE_READ : lecture répétée • DEFAULT : est égal à "" — dépend du SGBD.	Certains SGBD supportent uniquement READ_COMMITTED.	

- `<mysql dbname="drwcs" host="localhost" port="3306" user="" password="" ssl="no" precompiledcache="" debug="no" />`

  Détermine la base de données externe MySQL/MariaDB.

  Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
dbname	–	Nom de la base de données.	drwcs
host	Un des deux.	Adresse du serveur de la base de données en cas de connexion via TCP/IP.	localhost
		Chemin d'accès au fichier de socket UNIX en cas d'utilisation d'UDS. Si le chemin n'est pas spécifié, le Serveur Dr.Web tentera de trouver le fichier dans les répertoires standard de mysqld.	/var/run/mysqld/
port	Un des deux.	Numéro de port pour la connexion à la base de données via TCP/IP.	3306
		Nom du fichier de socket UNIX en cas d'utilisation d'UDS.	mysqld.sock
user	–	Nom d'utilisateur de la base de données.	""
password	–	Mot de passe d'utilisateur de la base de données.	""
ssl	yes | n'importe quel jeu de caractères	N'utiliser que les connexion SSL.	no
precompiledcache	Nombre entier positif.	Taille du cache des opérateurs sql précompilés en octets.	1048576

Attribut	Valeurs autorisées	Description	Par défaut
debug	• yes | no • on | off	Enregistrer le journal de débogage du SGBD.	• no • off

- **<acl>**

  Listes de contrôle d'accès. Permettent de spécifier des limitations pour les adresses réseau depuis lesquelles les Agents Dr.Web, les installateurs réseau et d'autres Serveurs Dr.Web (voisins) pourront accéder au Serveur Dr.Web spécifié.

  L'élément **<acl>** contient les éléments enfants suivants, dans lesquels sont configurées les restrictions pour les types correspondants de connexions :

  - **<install>** : liste de limitation des adresses IP depuis lesquelles les installateurs des Agents Dr.Web peuvent se connecter à ce Serveur Dr.Web.
  - **<agent>** : liste de restrictions des adresses IP depuis lesquelles les Agents Dr.Web peuvent se connecter à ce Serveur Dr.Web.
  - **<links >** : liste de restrictions des adresses IP depuis lesquelles les Serveurs voisins Dr.Web peuvent se connecter à ce Serveur Dr.Web.
  - **<discovery>** : liste de restrictions des adresses IP depuis lesquelles les requêtes de recherche broadcast sont reçues par le Service de détection du Serveur Dr.Web.

  Tous les éléments enfants ont la même structure des éléments emboîtés qui spécifient les restrictions suivantes :

  - **<priority mode="" />**

    Priorité des listes. Les valeurs autorisées de l'attribut `mode` : `allow` ou `deny`. En cas de la valeur **<priority mode="deny" />**, la liste **<deny >** possède une priorité plus importante que la liste **<allow>**. Les adresses qui ne sont incluses dans aucune liste ou qui sont incluses dans les deux listes sont refusées Seules les adresses incluses dans la liste **<allow>** et non incluses dans la liste **<deny>** sont autorisées.

  - **<allow>**

    Liste des adresses TCP depuis lesquelles l'accès est autorisé. L'élément **<allow>** contient un ou plusieurs éléments enfants **<ip address="" />** qui servent à spécifier les adresses autorisées au format IPv4 ou **<ip6 address="" />** pour spécifier les adresses autorisées au format Ipv6. Dans l'attribut `address` sont spécifiées les adresses réseau au format : *<Adresse IP>*`/[`*<préfixe>*`]`.

  - **<deny>**

    Liste des adresses TCP depuis lesquelles l'accès est interdit. L'élément **<deny>** contient un ou plusieurs éléments enfants **<ip address="" />** qui servent à spécifier les adresses interdites au format IPv4 ou **<ip6 address="" />** pour spécifier les adresses interdites au format Ipv6. Dans l'attribut `address` sont spécifiées les adresses réseau au format : *<Adresse IP>*`/[`*<préfixe>*`]`.

- **<scripts profile="" stack="" trace="" />**

  Configuration des paramètres du profilage de fonctionnement des scripts.

Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
profile	• yes, • no.	Journaliser les informations sur le profilage de l'exécution des scripts du Serveur Dr.Web. Ce paramètre est utilisé par le support technique et les développeurs. Il est recommandé de ne pas le modifier sans nécessité.	no
stack		Journaliser les informations sur l'exécution des scripts du Serveur Dr.Web depuis une pile d'appels. Ce paramètre est utilisé par le support technique et les développeurs. Il n'est pas recommandé de le modifier sans nécessité.	
trace		Journaliser les informations sur le suivi de l'exécution des scripts du Serveur Dr.Web. Ce paramètre est utilisé par le support technique et les développeurs. Il n'est pas recommandé de la modifier sans nécessité.	

- **<lua-module-path>**

  Chemins de l'interpréteur Lua.

  > L'ordre de spécification des chemin est important.

  L'élément **<lua-module-path>** contient les éléments enfants suivants :

  - **<cpath root="" />** : chemin vers le répertoire contenant les modules binaires. Valeurs autorisées de l'attribut root : home (par défaut), var, bin, lib.
  - **<path value="" />** : chemin vers le répertoire contenant les scripts. S'il n'est pas un élément enfant de l'élément **<jobs>** ou **<hooks>**, alors il concerne les deux. Les chemins spécifiés dans l'attribut value sont des chemins relatifs à ceux qui sont spécifiés dans l'attribut root de l'élément **<cpath>**.
  - **<jobs>** : chemins pour spécifier les tâches de la planification du Serveur Dr.Web.

    L'élément **<jobs>** contient un ou plusieurs éléments enfants **<path value="" />** pour spécifier le chemin vers le répertoire contenant les scripts.
  - **<hooks>** : chemins pour les procédures utilisateur du Serveur Dr.Web.

    L'élément **<hooks>** contient un ou plusieurs éléments enfants **<path value="" />** pour spécifier le chemin vers le répertoire contenant les scripts.

- **<transports>**

  Configuration des paramètres des protocoles transport utilisés par le Serveur Dr.Web pour se connecter aux clients. Contient un ou plusieurs éléments enfants **<transport discovery="" ip="" name="" multicast="" multicast-group="" port="" />**.

  Description des attributs :

Attribut	Description	Obligatoire	Valeurs autorisées	Par défaut
discovery	Détermine si le service de détection du Serveur Dr.Web sera utilisé.	non, spécifié uniquement avec l'attribut ip.	yes, no	no
ip | unix	Détermine la famille des protocoles utilisés (IP ou socket Unix) et spécifie l'adresse de l'interface.	oui	–	0.0.0.0 | –
name	Spécifie le nom du Serveur Dr.Web pour le service de détection du Serveur Dr.Web.	non	–	drwcs
multicast	Détermine si le Serveur Dr.Web fait partie du groupe multicast.	non, spécifié uniquement avec l'attribut ip.	yes, no	no
multicast-group	Spécifie l'adresse du groupe multicast auquel appartient le Serveur Dr.Web.	non, spécifié uniquement avec l'attribut ip.	–	• 231.0.0.1 • [ff18::231.0.0.1]
port	Port écouté.	non, spécifié uniquement avec l'attribut ip.	–	2193

- <**protocols**>

  Liste des protocoles désactivés. Contient un ou plusieurs éléments enfants <**protocol** enabled="" name="" />.

  Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
enabled	• yes : le protocole est activé, • yes : le protocole est désactivé.	Mode d'utilisation du protocole.	no
name	• AGENT : protocole de l'interaction du Serveur Dr.Web avec les Agents Dr.Web. • MSNAPSHV : protocole de l'interaction du Serveur Dr.Web avec le composant de vérification de l'état de santé du système Microsoft NAP Validator. • INSTALL : protocole de l'interaction du Serveur Dr.Web avec les installateurs des Agents Dr.Web.	Nom du protocole.	–

Attribut	Valeurs autorisées	Description	Par défaut
	• `CLUSTER` : protocole de l'interaction entre les Serveurs Dr.Web dans le système de cluster. • `SERVER` : protocole de l'interaction du Serveur Dr.Web avec les autres Serveurs Dr.Web.		

- **<plugins>**

  Liste des extensions désactivées. Contient un ou plusieurs éléments enfants **<plugin** enabled="" name="" />.

  Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
`enabled`	• `yes` : l'extension est activée, • `yes` : l'extension est désactivée.	Mode d'utilisation de l'extension.	`no`
`name`	• `WEBMIN` : extension pour le Centre de gestion de la sécurité Dr.Web pour la gestion du Serveur Dr.Web et du réseau antivirus via le Centre de gestion. • `FrontDoor` : extension Dr.Web Server FrontDoor qui autorise la connexion de l'utilitaire de diagnostic distant du Serveur Dr.Web.	Nom de l'extension.	–

- **<license>**

  Paramètres de l'octroi de licence.

  L'élément **<license>** contient les éléments enfants suivants :

  - **<limit-notify** min-count="" min-percent="" />

    Paramètres de la notification portant sur la limitation du nombre de licences dans la clé de licence.

    Description des attributs :

Attribut	Description	Par défaut
`min-count`	Nombre maximal des licences restantes qui déclenchera l'envoi de la notification **Limitation du nombre de licences dans la clé de licence**.	3
`min-percent`	Taux maximal des licences restantes qui déclenchera l'envoi de la notification **Limitation du nombre de licences dans la clé de licence**.	5

  - **<license-report** report-period="" active-stations-period="" />

    Paramètres du rapport sur l'utilisation des licences.

    Description des attributs :

Attribut	Description	Par défaut
report-period	Périodicité de création des rapports sur le Serveur Dr.Web portant sur les clés de licence utilisées. Si le rapport sur l'utilisation de licences est créé par le Serveur Dr.Web subordonné, ce rapport sera envoyé sur le Serveur principal Dr.Web juste après sa création. Les rapports créés sont également envoyés à chaque connexion (y compris chaque redémarrage) du Serveur Dr.Web, et en cas de modification du nombre de licences délivrées sur le Serveur principal Dr.Web.	1440
active-stations-period	Période pendant laquelle les postes actifs seront comptés pour envoyer un rapport sur l'utilisation des licences. La valeur 0 indique d'utiliser dans le rapport tous les postes quel que soit leur statut d'activité.	0

- `<exchange>`

  Paramètres de la distribution des licences entre les Serveurs Dr.Web.

  L'élément `<exchange>` contient les éléments enfants suivants :

  - `<expiration-interval value="" />`
  - `<prolong-preact value="" />`
  - `<check-interval value="" />`

  Description des éléments :

Élément	Description	Valeur de l'attribut value par défaut, min
expiration-interval	**Délai de validité des licences délivrées** : délai pour lequel les licences sont délivrées depuis la clé sur ce Serveur Dr.Web. La configuration est utilisée si ce Serveur Dr.Web délivre les licences aux Serveurs voisins Dr.Web.	1440
prolong-preact	**Période pour le renouvellement des licences obtenues** : période jusqu'à l'expiration de la licence. A commencer par cette période, ce Serveur Dr.Web démarre le renouvellement de la licence obtenue du Serveur voisin. La configuration est utilisée si le Serveur Dr.Web obtient des licences des Serveurs voisins Dr.Web.	60
check-interval	**Période de synchronisation de licences** : périodicité de synchronisation des informations sur les licences délivrées entre les Serveurs Dr.Web.	1440

- `<auth-flood count="" only-failed="" period="" />`

  Paramètres d'authentification. Si le nombre des tentatives d'authentification est dépassé, l'authentification sera impossible pendant un certain délai.
  Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
`count`	–	Nombre de tentatives d'authentification.	`5`
`only-failed`	• `yes` : prendre en compte les authentifications échouées uniquement, • `no` : prendre en compte les authentifications échouées et les authentifications réussies.	Prendre en compte les authentifications échouées uniquement.	`yes`
`period`	–	Délai pendant lequel l'authentification sera impossible.	60 secondes

- `<email from="" debug="" />`

  Paramètres d'envoi d'e-mails depuis le Centre de gestion, par exemple en tant que les notifications de l'administrateur ou lors de l'envoi de packages d'installation de postes.

  Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
`from`	–	Adresse e-mail du nom de laquelle seront envoyés les e-mails.	`drwcs@localhost`
`debug`	• `yes` : utiliser le mode de débogage, • `no` : ne pas utiliser le mode de débogage.	Utiliser le mode de débogage pour consulter le journal détaillé de la session SMTP.	`no`

  L'élément `<email>` contient les éléments enfants suivants :

  - `<smtp server="" user="" pass="" port="" start_tls="" auth_plain="" auth_login="" auth_cram_md5="" auth_digest_md5="" auth_ntlm="" conn_timeout="" />`

    Configuration des paramètres du serveur SMTP pour l'envoi d'e-mails.

    Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
`server`	–	Adresse du serveur SMTP qui sera utilisée pour envoyer des e-mails.	`127.0.0.1`
`user`	–	Nom de l'utilisateur du serveur SMTP, si le serveur SMTP exige l'authentification.	–
`pass`	–	Mot de passe de l'utilisateur du serveur SMTP, si le serveur SMTP exige l'authentification.	–
`port`	Nombre entier positif.	Port du serveur SMTP qui sera utilisé pour envoyer des e-mails.	25
`start_tls`	• `yes` : utiliser ce type d'authentification, • `no` : ne pas utiliser ce type d'authentification.	Pour l'échange chiffré de données. Dans ce cas, le passage à la connexion sécurisée s'effectue via la commande `STARTTLS`. L'utilisation du port 25 pour la connexion est prévue par défaut.	`yes`
`auth_plain`		Utiliser l'authentification *plain text* sur le serveur de messagerie.	`no`
`auth_login`		Utiliser l'authentification *LOGIN* sur le serveur de messagerie.	`no`
`auth_cram_md5`		Utiliser l'authentification *CRAM-MD5* sur le serveur de messagerie.	`no`
`auth_digest_md5`		Utiliser l'authentification *DIGEST-MD5* sur le serveur de messagerie.	`no`
`auth_ntlm`		Utiliser l'authentification *AUTH-NTLM* sur le serveur de messagerie.	`no`
`conn_timeout`	Nombre entier positif.	Délai de connexion au Serveur SMTP.	180

- `<ssl enabled="" verify_cert="" ca_certs="" />`

Configuration des paramètres du chiffrement SSL du trafic lors de l'envoi d'e-mails.

Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
`enabled`	• `yes` : utiliser SSL, • `no` : ne pas utiliser SSL.	Mode d'utilisation du chiffrement SSL.	`no`

Attribut	Valeurs autorisées	Description	Par défaut
verify_cert	• yes : vérifier le certificat SSL, • no : ne pas vérifier le certificat SSL.	Vérifier le certificat SSL du serveur de messagerie.	no
ca_certs	–	Chemin vers le certificat SSL racine du Serveur Dr.Web.	–

- `<track-epidemic enabled="" aggregation-period="" check-period="" threshold="" most-active="" />`

  Configuration des paramètres de la détection des épidémies virales dans le réseau.

  Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
enabled	yes | no	Autorise à suivre de nombreux événements d'infections des postes et à avoir la possibilité d'envoyer une notification sommaire à l'administrateur.	yes
aggregation-period	Nombre entier positif.	Délai en secondes après l'envoi de la notification portant sur une épidémie. Pendant ce délai, les notifications portant sur des infections isolées des postes ne seront pas envoyées.	300
check-period		Délai en secondes dans lequel un nombre spécifié de messages portant sur des postes infectés doit être reçu pour envoyer un rapport sommaire sur une épidémie.	3600
threshold		Nombre de messages portant sur des infections devant être reçus dans le délai indiqué afin que le Serveur Dr.Web envoie à l'administrateur une notification d'une épidémie relative à tous les cas d'infection (notification **Épidémie dans le réseau**).	100
most-active		Nombre des menaces les plus répandues à inclure dans le rapport sur les épidémies.	5

- `<track-hips-storm enabled="" aggregation-period="" check-period="" threshold="" most-active="" />`

  Configuration des paramètres de suivi des nombreux événements du composant Protection préventive.

  Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
`enabled`	`yes | no`	Autorise à suivre de nombreux événements de la Protection préventive et à avoir la possibilité d'envoyer une notification sommaire à l'administrateur.	`yes`
`aggregation-period`	Nombre entier positif.	Délai en secondes après l'envoi du rapport sommaire portant sur les événements de la Protection préventive. Pendant ce délai, les notifications portant sur des événements isolés ne seront pas envoyées.	300
`check-period`		Délai en secondes dans lequel un nombre spécifié des événements de la Protection préventive doit se produire pour envoyer un rapport sommaire.	3600
`threshold`		Nombre des événements de la Protection préventive qui doivent être reçus dans le délai indiqué afin que le Serveur Dr.Web envoie à l'administrateur un rapport sommaire sur ces événements (notification **Rapport sommaire de la Protection préventive**).	100
`most-active`		Nombre des processus les plus répandues exécutant une action suspecte à inclure dans le rapport de la Protection préventive.	5

- `<track-appctl-storm enabled="" aggregation-period="" check-period="" threshold="" most-active="" />`

  Configuration des paramètres de suivi des nombreux événements du composant Contrôle des applications.

  Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
`enabled`	`yes | no`	Autorise à suivre de nombreux événements du Contrôle des applications et à avoir la possibilité d'envoyer une notification sommaire à l'administrateur.	`yes`
`aggregation-period`	Nombre entier positif.	Délai en secondes après l'envoi du rapport sommaire portant sur les processus bloqués par le Contrôle des applications. Pendant ce délai, les notifications portant sur des blocages isolés ne seront pas envoyées.	300

Attribut	Valeurs autorisées	Description	Par défaut
check-period		Délai en secondes dans lequel un nombre spécifié de processus doit être bloqué pour envoyer un rapport sommaire.	3600
threshold		Nombre des événements des processus bloqués par le Contrôle des applications qui doivent être reçus dans le délai indiqué afin que le Serveur Dr.Web envoie à l'administrateur un rapport sommaire sur tous ces événements (notification **Un grand nombre de blocages faits par le Contrôle des applications est enregistré**).	100
most-active		Nombre des profils les plus répandus par lesquels le blocage a été fait et qu'il faut inclure dans la notifications de nombreux blocages.	5

- `<track-disconnect enabled="" aggregation-period="" check-period="" single-alert-threshold="" summary-alert-threshold="" min-session-duration="" />`

  Configuration des paramètres de suivi des nombreuses connexions interrompues avec les clients.

  Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
enabled	yes | no	Autorise à surveiller les connexions aux clients interrompues de façon anormale et d'avoir la possibilité d'envoyer les notifications correspondantes à l'administrateur.	yes
aggregation-period	Nombre entier positif.	Délai en secondes après l'envoi de la notification portant sur de nombreuses interruptions de connexions. Pendant ce délai, les notifications portant sur des interruptions isolées des connexions ne seront pas envoyées.	300
check-period		Délai en secondes dans lequel un nombre spécifié d'interruptions de connexions aux clients doit se produire pour envoyer une notification correspondante.	3600
single-alert-threshold		Nombre minimum des connexions à une adresse qui doivent être interrompues pendant le décompte pour qu'une notification d'une interruption anormale soit envoyée (notification **Arrêt d'urgence de la connexion**).	10

Attribut	Valeurs autorisées	Description	Par défaut
summary-alert-threshold		Nombre minimum des connexions qui doivent être interrompues pendant le décompte pour qu'une notification unique de nombreuses interruptions anormales soit envoyée (notification **Un grand nombre de connexions interrompues de façon anormale est enregistré**).	1000
min-session-duration		Si la durée d'une connexion au client terminée est inférieure à la durée indiquée, une notification d'interruptions isolées de connexions (notification **Arrêt d'urgence de la connexion**) sera envoyée lorsque le nombre spécifié de connexions sera atteint, quelle que soit la période de décompte. Dans ce cas, la connexion ne doit pas être interrompue plus tard par des connexions plus longues et une notification de nombreuses interruptions anormales de connexions ne doit pas être envoyée (notification **Un grand nombre de connexions interrompues de façon anormale est enregistré**).	300

- `<default-lang value="" />`

  Langue utilisée par défaut par les composants et les systèmes du Serveur Dr.Web, si les paramètres de langue n'ont pas été reçus de la base de données du Serveur Dr.Web. Notamment, elle est utilisée pour le Centre de gestion de la sécurité Dr.Web et le système de notifications de l'administrateur si la base de données a été endommagée et qu'il est impossible d'obtenir les paramètres de la langue.

- `<security-through-obscurity="" />`

  La configuration des paramètres de sécurité permettant de renforcer la sécurité grâce au masquage et à la déformation intentionnelle de certaines données.

  L'élément `<security-through-obscurity>` contient les éléments enfants suivants :

  - `<server-header enabled="" />`
  - `<lower-case-uri enabled="" />`
  - `<hacker-misleading enabled="" />`

  Description des attributs :

Attribut	Valeurs autorisées de l'attribut enabled	Description	Valeur de l'attribut enabled par défaut
server-header	yes | no	Permet de ne pas afficher la ligne de données du serveur (la version du Serveur Dr.Web, la version de	no

Attribut	Valeurs autorisées de l'attribut enabled	Description	Valeur de l'attribut enabled par défaut
		l'OS, les bibliothèques utilisées) ce qui complique la recherche de vulnérabilités connues. Correspond au paramètre **Retourner l'en-tête détaillé** dans la configuration du serveur Web.	
`lower-case-uri`	`yes | no`	Si l'option est activée, les URI sont converties en minuscules. Correspond au paramètre **Convertir URI en minuscules** dans la configuration du serveur Web.	`no`
`hacker-misleading`	`yes | no`	Une fois activé, il retourne de faux `passwd`, `hosts`, etc. en réponse à des requêtes de fichiers de type `/etc/passwd`, `/etc/hosts`, etc. (pour anticiper la présence d'une vulnérabilité de classe Path/Directory Traversal). Pour le moment il n'a pas de paramètre correspondant dans la configuration du serveur Web.	`yes`

F2. Fichier de configuration du Centre de gestion de la sécurité Dr.Web

Le fichier de configuration du Centre de gestion `webmin.conf` est disponible au format XML et il est situé dans le sous-répertoire `etc` du répertoire racine du Serveur Dr.Web.

Description des paramètres du fichier de configuration du Centre de gestion de la sécurité Dr.Web :

- `<version value="">`

  Version actuelle du Serveur Dr.Web.

- `<server-name value=""/>`

  Nom du Serveur Dr.Web.

  Spécifié au format suivant :

  Adresse IP ou nom DNS du Serveur Dr.Web`[:`*<port>*`]`

  Si l'adresse du Serveur Dr.Web n'est pas spécifiée, le nom de l'ordinateur retourné par le système d'exploitation ou l'adresse réseau du Serveur Dr.Web : nom de domaine, si disponible, sinon l'adresse IP, sont utilisés.

Si le numéro de port n'est pas indiqué, le port spécifié dans la requête est utilisé (par exemple, lors de l'accès au Serveur Dr.Web depuis le Centre de gestion ou via **Web API**). Notez que pour les requêtes depuis le Centre de gestion, c'est le port indiqué dans la ligne d'adresse lors de la connexion du Centre de gestion au Serveur Dr.Web.

- `<document-root value=""/>`

  Chemin vers le répertoire des pages web. Par défaut `value="webmin"`.

- `<ds-modules value=""/>`

  Chemin vers le répertoire des modules. Par défaut `value="ds-modules"`.

- `<threads value=""/>`

  Nombre de requêtes parallèles traitées par le serveur web. Ce paramètre affecte les performances du serveur. Il n'est pas recommandé de modifier ce paramètre sans nécessité.

- `<io-threads value=""/>`

  Nombre de flux traitant les données transmises via le réseau. Ce paramètre affecte les performances du Serveur Dr.Web. Il n'est pas recommandé de modifier ce paramètre sans nécessité.

- `<compression value="" max-size="" min-size=""/>`

  Utiliser la compression du trafic pour la transfert de données au Serveur Web via HTTP/HTTPS.

  Description des attributs :

Attribut	Description	Par défaut
`value`	Niveau de compression des données de 1 à 9, où 1 est le niveau minimum et 9 est le niveau maximum de compression.	9
`max-size`	Taille maximum des réponses HTTP qui seront compressées. Indiquez 0 pour désactiver la restriction de taille maximum de réponses HTTP à compresser.	51200 Ko
`min-size`	Taille minimum des réponses HTTP qui seront compressées. Indiquez 0 pour désactiver la restriction de taille minimum de réponses HTTP à compresser.	32 octets

- `<keep-alive timeout="" send-rate="" receive-rate=""/>`

  Maintenir la session HTTP active. Permet de configurer la connexion permanente pour les requêtes via le protocole HTTP en version 1.X.

  Description des attributs :

Attribut	Description	Par défaut
`timeout`	Timeout de la session HTTP. Lors de l'utilisation des connexions permanentes, le Serveur Dr.Web interrompt la connexion si aucune requête n'a été reçue du client depuis un délai spécifié.	15 s

Attribut	Description	Par défaut
send-rate	La vitesse minimale d'envoi de données. Si la vitesse sortante de transfert via le réseau est inférieure à la valeur spécifiée, la connexion est refusée. Saisissez 0 pour enlever cette restriction.	1024 O/s
receive-rate	La vitesse minimale de réception de données. Si la vitesse entrante de transmission via le réseau est inférieure à la valeur spécifiée, la connexion est refusée. Saisissez 0 pour enlever cette restriction.	1024 O/s

- `<buffers-size send="" receive=""/>`

  Configuration des tailles des tampons d'envoi et de la réception de données.

  Description des attributs :

Attribut	Description	Par défaut
send	Taille des tampons utilisés pour l'envoi de données. Ce paramètre affecte les performances du Serveur Dr.Web. Il n'est pas recommandé de modifier ce paramètre sans nécessité.	8192 octets
receive	Taille des tampons utilisés pour la réception de données. Ce paramètre affecte les performances du Serveur Dr.Web. Il n'est pas recommandé de modifier ce paramètre sans nécessité.	2048 octets

- `<max-request-length value=""/>`

  Taille maximale de la requête HTTP en Ko.

- `<xheaders>`

  Paramètre d'ajout d'en-têtes HTTP d'utilisateur. Il existe par défaut trois en-tête destinés à protéger contre les attaques réseau :

  - `<xheader name="X-XSS-Protection" value="1; mode=block"/>`

    L'en-tête gère le comportement du navigateur en cas de détection d'un code intégré dans la page attaquée (attaque XSS). Valeurs possibles :

Valeur	Comportement du navigateur
0	Filtre XSS désactivé.
1	Filtre XSS activé. En cas de détection d'une attaque XSS, le navigateur Web supprimera le code intégré.
1; mode=block	Filtre XSS activé. En cas de détection d'une attaque XSS, le navigateur Web ne chargera pas la page compromise. Utilisé par défaut.
1; report=<adresse-réseau>	Filtre XSS activé. En cas de détection d'une attaque XSS, le navigateur Web supprimera le code intégré et enverra le rapport à l'adresse indiquée. Supporté uniquement dans les navigateurs Web basés sur Chromium.

- `<xheader name="X-Content-Type-Options" value="nosniff"/>`

  En cas de valeur par défaut (`nosniff`), l'en-tête interdit au navigateur d'exécuter les fichiers cherchant à substituer le format MIME.

- `<xheader name="X-Frame-Options" value="SAMEORIGIN"/>`

  L'en-tête gère le comportement du navigateur Web en cas de tentative d'intégrer la page Web dans un cadre tiers (détournement de clic). Valeurs possibles :

Valeur	Comportement du navigateur
DENY	Interdit au navigateur de charger la page dans un cadre.
SAMEORIGIN	Autorise le navigateur à charger la page dans un cadre si la page et le cadre ont une source commune (domaine, port, protocole). Utilisé par défaut.
ALLOW-FROM <adresse-réseau>	Autorise le navigateur à charger la page dans un cadre à condition que la page se trouve à l'adresse indiquée.

- `<reverse-resolve enabled=""/>`

  Remplacer les adresses IP par les noms DNS des ordinateurs dans le fichier journal du Serveur Dr.Web. Les valeurs autorisées de l'attribut `enabled` : `yes` ou `no`.

- `<script-errors-to-browser enabled=""/>`

  Afficher les erreurs de script dans le navigateur (erreur 500). Ce paramètre est utilisé par le support technique et les développeurs. Il n'est pas recommandé de modifier ce paramètre sans nécessité.

- `<trace-scripts enabled=""/>`

  Activer la trace du fonctionnement des scripts. Ce paramètre est utilisé par le support technique et les développeurs. Il n'est pas recommandé de modifier ce paramètre sans nécessité. Les valeurs autorisées de l'attribut `enabled` : `yes` ou `no`.

- `<profile-scripts enabled="" stack=""/>`

  Gestion du profilage. La mesure de la performance : de la durée d'exécution des fonctions et des scripts du serveur web s'effectue. Ce paramètre est utilisé par le support technique et les développeurs. Il n'est pas recommandé de le modifier sans nécessité.

  Description des attributs :

Attribut	Valeurs autorisées	Description
enabled	• yes : activer le profilage, • no : désactiver le profilage.	Mode de profilage des scripts.
stack	• yes : enregistrer les données dans le journal, • no : ne pas enregistrer les données dans le journal.	Mode d'écriture des informations sur le profilage (paramètres des fonctions et les valeurs retournées) dans le journal du Serveur Dr.Web.

- `<abort-scripts enabled=""/>`

  Autoriser l'interruption de l'exécution de scripts, si la connexion a été interrompue par le client. Ce paramètre est utilisé par le support technique et les développeurs. Il n'est pas recommandé de modifier ce paramètre sans nécessité. Les valeurs autorisées de l'attribut `enabled` : `yes` ou `no`.

- `<search-localized-index enabled=""/>`

  Utiliser les versions localisées de pages. Si le mode est activé, le serveur va chercher une version localisée de cette page selon la priorité des langues spécifiées dans le champ `Accept-Language` de l'en-tête client. Les valeurs autorisées de l'attribut `enabled` : `yes` ou `no`.

- `<default-lang value=""/>`

  La langue des documents retournés par le serveur web si aucun en-tête `Accept-Language` n'est pas présent dans la requête HTTP. La valeur de l'attribut `value` — ISO du code de langue. Par défaut — `ru`.

- `<ssl certificate="" private-key="" keep-alive="" ciphers="" />`

  Génération du certificat SSL.

  Description des attributs :

Attribut	Description	Valeurs autorisées	Par défaut
`certificate`	Chemin vers le fichier de certificat SSL.	-	`certificate.pem`
`private-key`	Chemin vers le fichier de la clé privée SSL.	-	`private-key.pem`
`keep-alive`	Utiliser une connexion permanente pour SSL. Les anciennes versions de navigateurs peuvent ne pas fonctionner correctement avec des connexions SSL permanentes. Désactivez cette option si vous avez des problèmes avec le fonctionnement via le protocole SSL.	• `yes`, • `no`.	`yes`
`ciphers`	Liste et paramètres des chiffrements utilisés.	Pour en savoir plus, voir ici, la section "CIPHER LIST FORMAT".	`HIGH:!aNULL:!RC4:@STRENGTH`

- `<listen>`

  Configurations des paramètres pour l'écoute des connexions.

  L'élément `<listen />` contient les éléments enfants suivants :

- `<insecure>`

  Liste des interfaces qui seront écoutées pour recevoir des connexions non sécurisées via le protocole HTTPS. Le port 9080 est utilisé par défaut.

  L'élément `<insecure />` contient un ou plusieurs éléments enfants `<endpoint address="" />` qui servent à spécifier les adresses autorisées au format IPv4 ou IPv6. Dans l'attribut `address` sont spécifiées les adresses réseau au format : <*Protocole*>**:**//<*Adresse IP*>.

- `<secure>`

  Liste des interfaces qui seront écoutées pour recevoir des connexions sécurisées via le protocole HTTPS. Le port 9081 est utilisé par défaut.

  L'élément `<secure>` contient un ou plusieurs éléments enfants `<endpoint address="" />` qui servent à spécifier les adresses autorisées au format IPv4 ou IPv6. Dans l'attribut `address` sont spécifiées les adresses réseau au format : <*Protocole*>**:**//<*Adresse IP*>.

- `<access>`

  Listes de contrôle d'accès. Vous pouvez y configurer les restrictions pour les adresses réseau depuis lesquelles le Serveur Web reçoit les requêtes HTTP et HTTPS.

  L'élément `<acess />` contient les éléments enfants suivants, dans lesquels sont configurées les restrictions pour les types correspondants de connexions :

  - `<secure priority="">`

    Liste des interfaces qui seront écoutées pour recevoir des connexions sécurisées via le protocole HTTPS. Le port 9081 est utilisé par défaut.

    Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
`priority`	`allow`	Priorité d'autorisation pour HTTPS : adresses qui ne sont incluses dans aucune des listes (ou incluses dans les deux listes) sont autorisées.	`deny`
	`deny`	Priorité d'interdiction pour HTTPS : adresses qui ne sont incluses dans aucune des listes (ou incluses dans les deux listes) sont interdites.	

    L'élément `<secure>` contient un ou plusieurs éléments enfants `<allow address="" />` et `<deny address="" />`.

    Description des éléments :

Élément	Description	Valeur de l'attribut address par défaut
`allow`	Adresses depuis lesquelles l'accès via le protocole HTTPS sera autorisé pour les connexions sécurisées.	`tcp://127.0.0.1`
`deny`	Adresses depuis lesquelles l'accès via le protocole HTTPS sera interdit pour les connexions sécurisées.	-

- `<insecure priority="">`

Liste des interfaces qui seront écoutées pour recevoir des connexions non sécurisées via le protocole HTTPS. Le port 9080 est utilisé par défaut.

Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
priority	allow	Priorité d'autorisation pour HTTP : adresses qui ne sont incluses dans aucune des listes (ou incluses dans les deux listes) sont autorisées.	deny
	deny	Priorité d'interdiction pour HTTP : adresses qui ne sont incluses dans aucune des listes (ou incluses dans les deux listes) sont interdites.	

L'élément `<insecure />` contient un ou plusieurs éléments enfants `<allow address=""/>` et `<deny address=""/>`.

Description des éléments :

Élément	Description	Valeur de l'attribut address par défaut
allow	Adresses depuis lesquelles l'accès via le protocole HTTPS sera autorisé pour les connexions non sécurisées.	tcp://127.0.0.1
deny	Adresses depuis lesquelles l'accès via le protocole HTTPS sera interdit pour les connexions non sécurisées.	-

F3. Fichier de configuration download.conf

Utilisation du fichier download.conf :

1. Lors de la création et l'utilisation du système de cluster des Serveurs Dr.Web, ce fichier permet de répartir la charge entre les Serveurs Dr.Web de clusters si un grand nombre de nouveaux postes est connecté.
2. Dans le cas où un port non standard est utilisé sur le Serveur Dr.Web, ce fichier vous permet de spécifier ce port lors de la création du fichier d'installation de l'Agent Dr.Web.

Le fichier `download.conf` est utilisé lors de la création du fichier d'installation de l'Agent Dr.Web pour un nouveau poste au sein du réseau antivirus. Les paramètres de ce fichier permettent de spécifier l'adresse du Serveur Dr.Web et le port utilisés pour connecter l'installateur de l'Agent Dr.Web au Serveur Dr.Web au format suivant :

```
download = { server = '<Server_Address>'; port = <port_number> }
```

où :

- *<Server_Address>* : nom de domaine ou adresse IP du Serveur Dr.Web.

  > Il est recommandé d'utiliser le nom au format FQDN en tant qu'adresse du Serveur Dr.Web.

  Lors de la création du package d'installation de l'Agent Dr.Web, l'adresse du Serveur Dr.Web indiquée dans le fichier `download.conf` est utilisée. Si l'adresse du Serveur Dr.Web n'est pas spécifiée dans le fichier `download.conf`, la valeur du paramètre `ServerName` du fichier `webmin.conf` sera utilisée. Sinon, le nom de l'ordinateur retourné par l'OS sera pris en compte.

- *<port_number>* : le port pour connecter l'installateur de l'Agent Dr.Web au Serveur Dr.Web.

  Si le port n'est pas spécifié dans les paramètres du fichier `download.conf`, le port 2193 est utilisé par défaut (à configurer dans le Centre de gestion, dans la rubrique **Administration** → **Configuration du Serveur Dr.Web** → l'onglet **Réseau** → l'onglet **Transport**).

Par défaut, le paramètre `download` dans le fichier `download.conf` est commenté. Pour utiliser le fichier `download.conf`, il est nécessaire de décommenter ce paramètres. Pour ce faire, enlevez "`--`" au début de la ligne et spécifiez des valeurs appropriées à l'adresse et le port du Serveur Dr.Web.

F4. Fichier de configuration du Serveur proxy Dr.Web

Le fichier de configuration du Serveur proxy `drwcsd-proxy.conf` a le format XML et se trouve dans le répertoire suivant :

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

Description des paramètres du fichier de configuration du Serveur proxy Dr.Web :

- `<listen spec="">`

  L'élément racine `<drwcsd-proxy>` contient un ou plusieurs éléments obligatoires `<listen>` déterminant les paramètres de base relatifs à la réception des connexions par le Serveur proxy.

  L'élément `<listen>` contient l'attribut obligatoire `spec`, dont les attributs déterminent l'interface pour « écoute » des connexions entrantes des clients et déterminent s'il faut lancer le mode `discovery` sur cette interface.

  Attributs de l'élément `spec` :

Attribut	Obligatoire	Valeurs autorisées	Description	Par défaut
ip | unix	oui	–	Type de protocole pour recevoir les connexions entrantes. L'adresse écoutée par le Serveur proxy est spécifiée comme un paramètre.	0.0.0.0 | -
port	non	–	Numéro du port écouté par le Serveur proxy.	2193
discovery	non	yes, no	Mode d'imitation du Serveur Dr.Web. Ce mode permet aux clients de détecter le Serveur proxy en tant que Serveur Dr.Web lors de sa recherche par les requêtes broadcast.	yes
multicast	non	yes, no	Mode d'« écoute » du réseau pour la réception des requêtes broadcast par le Serveur proxy.	yes
multicast-group	non	–	Groupe multicast où se trouve le Serveur proxy.	231.0.0.1 [ff18::231.0.0.1]

En fonction du protocole, la liste des attributs non obligatoires spécifiés dans l'attribut `spec` peut varier.

Liste des propriétés non obligatoires pouvant être spécifiées (+) ou non spécifiées (–) dans l'attribut `spec` en fonction du protocole :

Protocole	Présence des propriétés			
	port	discovery	multicast	multicast-group
ip	+	+	+	+
unix	+	-	-	-

Le mode **discovery** doit être activé directement dans tous les cas même si le mode **multicast** est déjà activé.

L'algorithme de redirection en cas de présence d'une liste des Serveurs Dr.Web figure dans le **Manuel Administrateur**.

- `<compression mode="" level="">`

Si l'élément `<compression>` est subordonné (enfant) à l'élément `<listen>`, il détermine les paramètres de compression du trafic du client – Serveur Proxy.

Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
mode	yes	Compression activée.	possible
	no	Compression désactivée.	
	possible	Compression possible.	
level	nombre entier de 1 à 9	Niveau de compression. Seulement pour le trafic client : Serveur proxy	8

- `<encryption mode="">`

Si l'élément `<encryption>` est subordonné (enfant) à l'élément `<listen>`, il détermine les paramètres de chiffrement du trafic du client – Serveur Proxy.

Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
mode	yes	Chiffrement activé.	possible
	no	Chiffrement désactivé.	
	possible	Chiffrement possible.	

- `<forward to="" master="">`

Spécifie les paramètres déterminant la redirection des connexions entrantes. L'élément `<forward>` est obligatoire. Plusieurs éléments `<forward>` avec les valeurs différentes des attributs peuvent être spécifiés.

Description des attributs :

Attribut	Valeurs autorisées	Description	Obligatoire
to	L'adresse est spécifiée conformément à la spécification de l'adresse réseau : • <protocol>://<interface>:<port-number> : utiliser IPv4 et IPv6. • <protocol>://(<interface>):<port-number> : utiliser IPv4 uniquement. • <protocol>://[<interface>]:<port	Adresse du Serveur Dr.Web vers laquelle la connexion sera redirigée.	oui

Attribut	Valeurs autorisées	Description	Obligatoire
	-number> : utiliser IPv6 uniquement.		
master	• yes : le Serveur Dr.Web sera gérant sans conditions. • no : en aucun cas, le Serveur Dr.Web ne sera gérant. • possible : le Serveur Dr.Web sera gérant uniquement s'il n y a pas de Serveurs gérants sans condition (avec la valeur yes spécifiée pour l'attribut master).	L'attribut détermine s'il est possible de modifier les paramètres du Serveur proxy Dr.Web à distance via le Centre de gestion du Serveur Dr.Web indiqué dans l'attribut to. Vous pouvez designer n'importe quel nombre de Serveurs Dr.Web comme gérants (la valeur master="yes"). Dans ce cas, la connexion se fait à tous les Serveurs Dr.Web gérants dans l'ordre spécifié dans les paramètres du Serveur proxy Dr.Web jusqu'à la première obtention d'une configuration valide (non vide). Vous pouvez également ne designer aucun Serveur Dr.Web comme gérant (la valeur master="no"). Dans ce cas, la configuration des paramètres du Serveur proxy Dr.Web (y compris la désignation des Serveurs Dr.Web gérants) se fait uniquement via le fichier de configuration du Serveur proxy Dr.Web, de manière locale.	non

S'il n y a pas d'attribut master pour le Serveur Dr.Web, on considère par défaut que master="possible".

Dans le fichier de configuration créé par l'installateur lors de l'installation du Serveur proxy Dr.Web, l'attribut master n'est déterminé pour aucun Serveur Dr.Web.

- <compression mode="" level="">

  Si l'élément <compression /> est subordonné (enfant) à l'élément <forward />, il détermine les paramètres de compression du trafic Serveur Dr.Web — Serveur Proxy Dr.Web. Les attributs sont équivalents à ceux décrits ci-dessus.

- <encryption mode="">

  Si l'élément <encryption> est subordonné (enfant) à l'élément <listen>, il détermine les paramètres de chiffrement du trafic du Serveur Dr.Web – Serveur Proxy Dr.Web. Les attributs sont équivalents à ceux décrits ci-dessus.

- <update-bandwidth value="" queue-size="">

L'élément <update-bandwidth> permet de déterminer la limitation de la vitesse de transmission des mises à jour du Serveur Dr.Web aux clients et le nombre des clients qui téléchargent simultanément les mises à jour.

Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
value	• vitesse maximale en Ko/s, • unlimited	Valeur maximale de la vitesse sommaire de transfert des mises à jour.	unlimited
queue-size	• nombre entier positif, • unlimited	Nombre maximum des sessions de distribution des mises à jour lancées en même temps depuis ce Serveur Dr.Web. Si le nombre maximum est atteint, les requêtes des Agents Dr.Web sont placées dans une file d'attente. La taille de la file d'attente n'est pas limitée.	unlimited

- <bandwidth value="" time-map="">

L'élément <update-bandwidth> peut avoir un ou plusieurs éléments subordonnés (enfants) <bandwidth>. Cet élément permet de déterminer la limitation de la vitesse de transfert de données pour un délai spécifié.

Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
value	• vitesse maximale en Ko/s, • unlimited	Valeur maximale de la vitesse cumulée de transfert des données lors de la mise à jour de l'Agent Dr.Web.	unlimited
time-map	–	Masque indiquant le délai de temps, pendant lequel la limitation sera activée.	–

La valeur de l'attribut time-map est spécifiée automatiquement après l'indication du paramètre correspondant dans l'interface web du Centre de gestion (voir **Manuel Administrateur**, section Configuration distante du Serveur proxy). Il est impossible pour le moment de spécifier time-map manuellement via le fichier de configuration.

- <install-bandwidth value="" queue-size="">

L'élément <install-bandwidth> permet de déterminer la limitation de la vitesse de transfert de données lors de l'installation des Agents Dr.Web et le nombre des clients qui téléchargent simultanément les données d'installation.

Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
value	• vitesse maximale en Ko/s, • unlimited	Valeur maximale de la vitesse cumulée de transfert de données lors de l'installation des Agents Dr.Web.	unlimited

Attribut	Valeurs autorisées	Description	Par défaut
queue-size	• nombre entier positif, • unlimited	Nombre maximum des sessions d'installation de l'Agent Dr.Web lancées en même temps depuis ce Serveur Dr.Web. Si le nombre maximum est atteint, les requêtes des Agents Dr.Web sont placées dans une file d'attente. La taille de la file d'attente n'est pas limitée.	unlimited

- <bandwidth value="" time-map="">

L'élément <install-bandwidth> peut avoir un ou plusieurs éléments subordonnés (enfants) <bandwidth>. Cet élément permet de déterminer la limitation de la vitesse de transfert de données pour un délai spécifié.

Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
value	• vitesse maximale en Ko/s, • unlimited	Valeur maximale de la vitesse cumulée de transfert de données lors de l'installation de l'Agent Dr.Web.	unlimited
time-map	–	Masque indiquant le délai de temps, pendant lequel la limitation sera activée.	–

La valeur de l'attribut time-map est spécifiée automatiquement après l'indication du paramètre correspondant dans l'interface web du Centre de gestion (voir **Manuel Administrateur**, section Configuration distante du Serveur proxy). Il est impossible pour le moment de spécifier time-map manuellement via le fichier de configuration.

- <cache enabled="">

Paramètres du cache du référentiel du Serveur proxy.

Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
enabled	yes | no	Détermine si la mise en cache est activée.	yes

L'élément <cache> contient les éléments enfants suivants :

Élément	Valeurs autorisées	Description	Par défaut
<maximum-revision-queue size="">	nombre entier positif	Nombre de révisions stockées.	3
<clean-interval value="">	nombre entier positif	Intervalle entre les suppressions des anciennes révisions, en minutes.	60

Élément	Valeurs autorisées	Description	Par défaut
<unload-interval value="">	nombre entier positif	Intervalle entre les suppressions des fichiers non utilisés de la mémoire, en minutes.	10
<repo-check mode="">	idle | sync	Vérification de l'intégrité du cache au démarrage (cela peut prendre du temps) ou en tâche de fond.	idle

- <synchronize enabled="" schedule="">

Paramètres de synchronisation des référentiels du Serveur proxy et du Serveur Dr.Web.

Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
enabled	yes | no	Détermine si la synchronisation est activée.	yes
schedule	–	Planification selon laquelle les produits spécifiés seront synchronisés.	–

La valeur de l'attribut schedule est spécifiée automatiquement après l'indication du paramètre correspondant dans l'interface web du Centre de gestion (voir **Manuel Administrateur**, section Configuration distante du Serveur proxy). Il est impossible pour le moment de spécifier schedule manuellement via le fichier de configuration.

La liste des produits à synchroniser est affichée en tant que les éléments enfants de <product name=""> :

- 05-drwmeta : données de sécurité du Serveur Dr.Web,
- 10-drwbases : bases virales,
- 10-drwgatedb : bases SpIDer Gate,
- 10-drwspamdb : bases de l'Antispam,
- 10-drwupgrade : Module de mise à jour Dr.Web,
- 15-drwhashdb : hashs de menaces connus,
- 20-drwagent : Agent Dr.Web pour Windows,
- 20-drwandroid11 : bases Dr.Web pour Android,
- 20-drwcs : Serveur Dr.Web,
- 20-drwunix : Agent Dr.Web pour UNIX,
- 25-drwcsdoc : documentation,
- 40-drwproxy : Serveur proxy Dr.Web,
- 70-drwextra : produits d'entreprise Dr.Web,

- 70-drwutils : utilitaires de gestion Dr.Web,
- 80-drwnews : actualités de Doctor Web.

- `<events enabled="" schedule="">`

  Paramètres de la mise en cache des événements reçus des Agents Dr.Web.

  Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
`enabled`	`yes | no`	Détermine si la mise en cache des événements est activée. Si elle est activée, les événements seront envoyés sur le Serveur Dr.Web selon la planification. Si la mise en cache est désactivée, les événements seront envoyés sur le Serveur Dr.Web tout de suite après leur réception par le Serveur proxy.	`yes`
`schedule`	–	Panification selon laquelle les événements reçus des Agents Dr.Web seront transmis.	–

La valeur de l'attribut `schedule` est spécifiée automatiquement après l'indication du paramètre correspondant dans l'interface web du Centre de gestion (voir **Manuel Administrateur**, section Configuration distante du Serveur proxy). Il est impossible pour le moment de spécifier `schedule` manuellement via le fichier de configuration.

- `<update enabled="" schedule="">`

  Configuration de la mise à jour automatique du Serveur proxy.

  Si la mise à jour automatique et la synchronisation sont activées, les mises à jour du Serveur proxy seront téléchargées depuis le Serveur Dr.Web selon la planification de synchronisation (voir ci-dessus) et elles seront installées selon la planification de mise à jour (par défaut, sans aucune limite de temps). Si la synchronisation est désactivée, le téléchargement et l'installation se font selon la planification de la mise à jour (par défaut, sans aucune limite de temps).

  Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
`enabled`	`yes | no`	Détermine si la mise à jour automatique est activée.	`yes`
`schedule`	–	Planification selon laquelle les mises à jour seront téléchargées (si la synchronisation n'est pas spécifiée) et installées.	–

La valeur de l'attribut `schedule` est spécifiée automatiquement après l'indication du paramètre correspondant dans l'interface web du Centre de gestion (voir **Manuel Administrateur**, section Configuration distante du Serveur proxy). Il est impossible pour le moment de spécifier `schedule` manuellement via le fichier de configuration.

Par défaut, la mise à jour automatique est autorisées sans aucune limite de temps.

- `<core-dump enabled="" maximum="">`

  Mode de collecte et le nombre de dumps de mémoire en cas d'exception SEH.

  La configuration des dumps de mémoire est possible seulement sous Windows.

  Pour collecter les dumps de mémoire, l'OS doit contenir la bibliothèque `dbghelp.dll`.

  Le dump est sauvegardé dans le répertoire suivant : `%APPDATA%\Doctor Web\drwcsd-proxy\dump\`

  Description des attributs :

Attribut	Valeurs autorisées	Description	Par défaut
`enabled`	`yes | no`	Détermine si la collecte de dumps est activée.	`yes`
`maximum`	nombre entier positif	Nombre maximal de dumps. Les dumps plus anciens sont supprimés.	10

- `<dns>`

  Paramètres DNS.

  `<timeout value="">`

  Délai en secondes pour autoriser les requêtes DNS directes/inverses. Laissez le champ vide pour ne pas limiter la durée d'attente pour l'autorisation.

  `<retry value="">`

  Nombre maximum de requêtes DNS réitérées en cas d'échec d'une requête DNS.

  `<cache enabled="" negative-ttl="" positive-ttl="">`

  Durée de conservation de réponses du serveur DNS dans le cache.

  Description des attributs :

Attribut	Valeurs autorisées	Description
`enabled`	• `yes` : stocker les réponses dans le cache, • `no` : ne pas stocker les réponses dans le cache.	Mode de stockage des réponses dans le cache.

Attribut	Valeurs autorisées	Description
negative-ttl	–	Durée de conservation dans le cache (TTL) des réponses négatives du serveur DNS en minutes.
positive-ttl	–	Durée de conservation dans le cache (TTL) des réponses positives du serveur DNS en minutes.

`<servers>`

Liste des serveurs DNS qui remplacent la liste système par défaut. Elle contient un ou plusieurs éléments enfants `<server address="">`, dans lesquels le paramètre `address` détermine l'adresse IP du serveur.

`<domains>`

Liste des domaines DNS qui remplace la liste système par défaut. Elle contient un ou plusieurs éléments enfants `<domain name="">`, dans lesquels le paramètre `name` détermine le nom de domaine.

F5. Fichier de configuration du Chargeur du référentiel

Le fichier de configuration du Chargeur du référentiel `drwreploader.conf` est disponible au format XML et il est situé dans le sous-répertoire `etc` du répertoire d'installation du Serveur Dr.Web.

Pour utiliser le fichier de configuration

- Pour l'utilitaire de console, le chemin vers le fichier doit être spécifié dans la clé `--config`.
- Pour l'utilitaire graphique, le fichier doit se trouver dans le répertoire de placement de l'utilitaire même. Quand l'utilitaire graphique est lancé sans fichier de configuration, ce fichier sera créé dans le répertoire où l'utilitaire est placé et il sera utilisé lors des lancements suivants.

Description des paramètres du fichier de configuration du Chargeur du référentiel :

- `<mode value="" path="" archive="" key="">`

  Description des attributs :

Attribut	Description	Valeurs autorisées
value	Mode de téléchargement des mises à jour : • `repository` : le référentiel est téléchargé sous forme du référentiel du Serveur Dr.Web. Les fichiers téléchargés peuvent être importés via le Centre de gestion en tant que la mise à jour du référentiel du Serveur Dr.Web. • `mirror` : le référentiel est téléchargé sous forme de la zone des mises à jour du SGM. Les fichiers téléchargés peuvent être placés en miroir de mises à jour dans votre réseau local.	`repository | mirror`

Attribut	Description	Valeurs autorisées
	Ensuite, les Serveurs Dr.Web peuvent être configurés pour recevoir des mises à jours directement depuis ce miroir de mise à jour contenant la dernière version du référentiel et non pas depuis les serveurs du SGM.	
`path`	Répertoire dans lequel le référentiel sera téléchargé.	–
`archive`	Mettre automatiquement le référentiel téléchargé en archive zip. Cette option permet d'obtenir une archive du référentiel téléchargé prête à importer sur le Serveur Dr.Web à l'aide du Centre de gestion, depuis la section **Administration** → **Contenu du référentiel**.	`yes | no`
`key`	Fichier de clé de licence Dr.Web. Vous pouvez également spécifier le hash MD5 de la clé de licence que vous pouvez trouver dans le Centre de gestion, dans la section **Administration** → **Gestionnaire de licences**.	–

- `<log path="" verbosity="" rotate="">`

  Paramètres de journalisation du Chargeur du référentiel.

  Description des attributs :

Attribut	Description	Valeurs autorisées
`path`	Chemin vers le fichier journal.	–
`verbosity`	Niveau de détails du journal. Par défaut, c'est `TRACE3`.	`ALL`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `DEBUG`, `TRACE3`, `TRACE2`, `TRACE1`, `TRACE`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `CRIT`. Les valeurs `ALL` et `DEBUG3` sont des synonymes.
`rotate`	Mode de rotation du journal au format *<N><f>,<M><u>*. Équivalent à la configuration de la rotation du journal du Serveur Dr.Web. Les valeurs par défaut sont `10,10m`, ce qui enjoint de sauvegarder 10 fichiers, de 10 Mo chacun, et d'utiliser la compression.	–

- `<update url="" proto="" cdn="" update-key="" version="">`

  Paramètres généraux de téléchargement du référentiel.

  Description des attributs :

Attribut	Description	Valeurs autorisées
`url`	Répertoire se trouvant sur les serveurs SGM contenant les mises à jour des produits Dr.Web.	–
`proto`	Type de protocole pour obtenir les mises à jour depuis les Serveurs de mises à jour. Pour tous les protocoles, le téléchargement des mises à jour s'effectue conformément aux paramètres de la liste des serveurs du SGM.	`http | https | ftp | ftps | sftp | scp | file`
`cdn`	Autoriser l'utilisation de Content Delivery Network lors du chargement du référentiel.	`yes | no`
`update-key`	Chemin vers la clé publique ou le répertoire contenant la clé publique utilisée pour la vérification de la signature des mises à jour téléchargées depuis le SGM. Vous pouvez trouver les clés publiques utilisées pour la vérification de l'authenticité des mises à jour `update-key-*.upub` sur le Serveur Dr.Web, dans le répertoire `etc`.	–
`version`	Version du Serveur Dr.Web pour lequel il faut télécharger des mises à jour.	–

▫ **<servers>**

Liste des serveurs des mises à jour. Les serveurs du SGM sont listés dans l'ordre dans lequel l'utilitaire les contacte lors du téléchargement du référentiel.

Contient les éléments enfants **<server>** dans lesquels les serveurs de mises à jour sont indiqués.

▫ **<auth user="" password="">**

Identifiants de l'utilisateur utilisé pour l'authentification sur le Serveur des mises à jour, si le serveur exige l'authentification.

Description des attributs :

Attribut	Description
`user`	Nom d'utilisateur sur le serveur de mises à jour.
`password`	Mot de passe sur le serveur de mises à jour.

▫ **<proxy host="" port="" user="" password="" />**

Paramètres de connexion au SGM via le serveur proxy.

Description des attributs :

Attribut	Description
`host`	Adresse réseau du serveur proxy utilisé.

Attribut	Description
port	Numéro de port du serveur proxy utilisé. Par défaut, c'est 3128.
user	Nom de l'utilisateur du serveur proxy, si l'authentification sur le serveur proxy est requise.
password	Mot de passe sur le serveur proxy si le serveur proxy utilisé exige l'authentification.

- <ssl cert-mode="" cert-file="">

Paramètres des certificats SSL qui seront appliqués automatiquement. Ce paramètre est utilisé uniquement pour les protocoles sécurisés supportant le chiffrement.

Description des attributs :

Attribut	Description	Valeurs autorisées
cert-mode	Certificats qui seront acceptés automatiquement.	▫ any : accepter tous les certificats, ▫ valid : accepter uniquement les certificats fiables, ▫ drweb : accepter uniquement les certificats de Dr.Web, ▫ custom : accepter les certificats utilisateurs.
cert-file	Chemin vers le fichier de certificat.	–

- <ssh mode="" pubkey="" prikey="">

Type d'authentification sur le serveur de mises à jour en cas d'appel via SCP/SFTP.

Description des attributs :

Attribut	Description	Valeurs autorisées
mode	Type d'authentification.	▫ pwd : authentification avec un mot de passe. Le mot de passe est spécifié dans la balise <auth />. ▫ pubkey : auhentification par la clé publique. La clé publique est spécifiée dans l'attribut pubkey ou bien, elle est extraite de la clé privée indiquée dans prikey.
pubkey	Clé publique SSH	–
prikey	Clé privée SSH	–

- <products>

Paramètres des produits téléchargés.

- <product name="" update="">

Paramètres de chaque produit.

Description des attributs :

Attribut	Description	Valeurs autorisées
name	Nom du produit.	• 05-drwmeta : données de sécurité du Serveur Dr.Web, • 10-drwbases : bases virales, • 10-drwgatedb : bases SplDer Gate, • 10-drwspamdb : bases de l'Antispam, • 10-drwupgrade : Module de mise à jour Dr.Web, • 15-drwhashdb : hashs de menaces connus, • 20-drwagent : Agent Dr.Web pour Windows, • 20-drwandroid11 : bases Dr.Web pour Android, • 20-drwcs : Serveur Dr.Web, • 20-drwunix : Agent Dr.Web pour UNIX, • 25-drwcsdoc : documentation, • 40-drwproxy : Serveur proxy Dr.Web, • 70-drwextra : produits d'entreprise Dr.Web, • 70-drwutils : utilitaires de gestion Dr.Web, • 80-drwnews : actualités de Doctor Web.
update	Activer le déchargement de ce produit.	yes | no

- <schedule>

  Planification des mises à jour périodiques. Dans ce cas, vous n'avez pas besoin de lancer l'utilitaire manuellement, le chargement du référentiel sera effectué automatiquement conformément à la périodicité spécifiée.

  - <job period="" enabled="" min="" hour="" day="">

    Paramètres de téléchargements selon la planification.

Attribut	Description	Valeurs autorisées
period	Périodicité d'exécution des tâches de téléchargement.	• every_n_min : toutes les N minutes, • hourly : toutes les heures, • daily : tous les jours, • weekly : chaque semaine.
enabled	La tâche de téléchargement est activée.	yes | no
min	Minute d'exécution de la tâche.	nombres entiers de 0 à 59
hour	Heure d'exécution de la tâche. Cela concerne les périodes daily et weekly.	nombres entiers de 0 à 23

Attribut	Description	Valeurs autorisées
`day`	Jour d'exécution de la tâche. Cela concerne la période `weekly`.	• `mon` : lundi, • `tue` : mardi, • `wed` : mercredi, • `thu` : jeudi, • `fri` : vendredi, • `sat` : samedi, • `sun` : dimanche.

Annexe G. Paramètres de la ligne de commande relatifs aux programmes inclus dans Dr.Web Enterprise Security Suite

Les paramètres de la ligne de commande ont une priorité supérieure à celle des paramètres définis par défaut ou à celle des paramètres permanents (spécifiés dans le fichier de configuration du Serveur Dr.Web, dans la base de registre Windows etc.). Dans certains cas décrits ci-après, les paramètres spécifiés au démarrage modifient les paramètres permanents.

Lors de la description de la syntaxe des paramètres des programmes, leur partie facultative est mise entre crochets `[...]`.

Les particularités décrites ci-dessous dans l'Annexe M ne concernent pas l'installateur réseau de l'Agent Dr.Web.

Certains paramètres de la ligne de commande commencent par un trait d'union. Ces paramètres sont appelés des clés.

Beaucoup de clés peuvent être présentes sous diverses formes équivalentes. Les clés pouvant avoir une valeur logique (oui/non, interdire/autoriser) ont des variantes négatives formant des paires, par exemple la clé `-admin-rights` a la variante paire `-no-admin-rights` ayant une valeur opposée. De telles clés peuvent être spécifiées de manière explicite avec l'indication de valeur, par exemple `-admin-rights=yes` et `-admin-rights=no`.

La valeur `yes` a les synonymes suivants : `on`, `true`, `OK` La valeur `no` possède les synonymes `off`, `false`.

Si la valeur de la clé contient des espaces ou des symboles de tabulation, tout le paramètre doit être mis entre guillemets comme dans l'exemple ci-dessous :

```
"-home=c:\Program Files\DrWeb Server"
```

Les noms des clés peuvent être abrégés (il est possible d'omettre les derniers caractères) à condition que le nom abrégé ne corresponde pas à la partie abrégée d'une autre clé.

Le paramètre `elevate` peut être utilisé pour l'exécution forcée des commandes avec les droits d'administrateur dans les systèmes d'exploitation de la famille Windows. Dans ce cas le paramètre est indiqué devant tous les autres clés et paramètres, par exemple : `drwcsd elevate start`.

G1. Installateur réseau

Syntaxe de la commande de démarrage :

`drwinst.exe [<clés>]`

Clés

Les clés de la ligne de commande sont valides lors du lancement de tous les types de fichiers d'installation de l'Agent Dr.Web.

Les clés de démarrage de l'installateur réseau de l'Agent Dr.Web sont spécifiés au format : `/`<*clé*> <*paramètre*>.

Toutes les valeurs de paramètres indiquées sont séparées par un espace. Par exemple :

```
/silent yes
```

Si la valeur de la clé contient des espaces, des symboles de tabulation ou le symbole `\`, le paramètre entier doit être mis entre guillemets comme dans l'exemple ci-dessous :

```
/pubkey "C:\my folder\drwcsd-certificate.pem"
```

Clés possibles :

- `/compression` <*mode*> : mode de compression du trafic du Serveur Dr.Web. Le paramètre <*mode*> peut prendre les valeurs suivantes :
  - `yes` : utiliser la compression.
  - `no` : ne pas utiliser la compression.
  - `possible` : la compression est possible. La décision définitive est prise en fonction des paramètres du côté du Serveur Dr.Web.

  Si la clé n'est pas spécifiée, la valeur `possible` est utilisée par défaut.
- `/encryption` <*mode*> : mode de chiffrement du trafic du Serveur Dr.Web. Le paramètre <*mode*> peut prendre les valeurs suivantes :
  - `yes` : utiliser le chiffrement.
  - `no` : ne pas utiliser le chiffrement.
  - `possible` : la chiffrement est possible. La décision définitive est prise en fonction des paramètres du côté du Serveur Dr.Web.

  Si la clé n'est pas spécifiée, la valeur `possible` est utilisée par défaut.
- `/excludeFeatures` <*composants*> : liste des composants qu'il faut exclure lors de l'installation sur le poste. Si plusieurs composants sont indiqués, utilisez le caractère « `,` » pour les séparer. Les composant disponibles sont :
  - `scanner` : Scanner Dr.Web,
  - `spider-mail` : SpIDer Mail,
  - `spider-g3` : SpIDer Guard,
  - `outlook-plugin` : Dr.Web pour Microsoft Outlook,

- `firewall` : Pare-feu Dr.Web,
- `spider-gate` : SpIDer Gate,
- `parental-control` : Office Control,
- `antispam-outlook` : Antispam Dr.Web pour le composant Dr.Web pour Microsoft Outlook,
- `antispam-spidermail` : Antispam Dr.Web pour le composant SpIDer Mail.

Pour les composants indiqués directement, le statut d'installation spécifié par défaut est gardé.

- `/id` <*identificateur du poste*> : identificateur du poste sur lequel l'Agent Dr.Web est installé.

  La clé est spécifiée avec la clé `/pwd` pour l'authentification automatique sur le Serveur Dr.Web. Si les paramètres d'authentification ne sont pas spécifiés, la décision sur l'authentification est prise du coté du Serveur Dr.Web.

- `/excludeFeatures` <*composants*> : liste des composants qu'il faut installer sur le poste. Si plusieurs composants sont indiqués, utilisez le caractère « , » pour les séparer. Les composant disponibles sont :
  - `scanner` : Scanner Dr.Web,
  - `spider-mail` : SpIDer Mail,
  - `spider-g3` : SpIDer Guard,
  - `outlook-plugin` : Dr.Web pour Microsoft Outlook,
  - `firewall` : Pare-feu Dr.Web,
  - `spider-gate` : SpIDer Gate,
  - `parental-control` : Office Control,
  - `antispam-outlook` : Antispam Dr.Web pour le composant Dr.Web pour Microsoft Outlook,
  - `antispam-spidermail` : Antispam Dr.Web pour le composant SpIDer Mail.

  Pour les composants indiqués directement, le statut d'installation spécifié par défaut est gardé.

- `/installdir` <*répertoire*> : répertoire d'installation.

  Si la clé n'est pas spécifiée, l'installation s'effectue dans le répertoire "`Program Files\DrWeb`" sur le disque système.

- `/installtimeout` <*temps*> : délai maximum d'attente de réponse en cas d'installation distante, lancée depuis le Centre de gestion. Spécifié en secondes.

  Si la clé n'est pas spécifiée, la valeur 300 secondes est utilisée par défaut.

- `/instMode` <<*mode*> : mode de lancement de l'installateur. Le paramètre <*mode*> peut prendre les valeurs suivantes :
  - `change` : modifier la liste des composants installés du produit ;
  - `remove` : supprimer le produit installé ;
  - `recovery` : restaurer le produit installé si certains composants ont été endommagés.

  Si la clé n'est pas spécifiée, l'installateur détermine automatiquement le mode de lancement.

- `/lang` <*code_de_langue*> : langue de l'installateur et du produit installé. Spécifié au format ISO-639-1 pour le code de langue.

  Si la clé n'est pas spécifiée, la langue système est utilisée par défaut.

- `/pubkey` <*certificat*> : chemin complet vers le fichier de certificat du Serveur Dr.Web.

  Si le certificat n'est pas spécifié, lors du lancement de l'installation locale, l'installateur utilise par défaut le fichier de certificat `*.pem` du répertoire de lancement. Si le fichier de certificat se place dans un répertoire autre que celui de lancement de l'installateur, il faut spécifier manuellement le chemin complet vers le fichier de certificat.

  Si vous lancez le package d'installation créé dans le Centre de gestion, le certificat est inclus dans le package d'installation. Dans ce cas, il ne faut pas indiquer le fichier de certificat par les clés de la ligne de commande.

- `/pwd` <*mot de passe*> : mot de passe de l'Agent Dr.Web pour accéder au Serveur Dr.Web.

  La clé est spécifiée avec la clé `/id` pour l'authentification automatique sur le Serveur Dr.Web. Si les paramètres d'authentification ne sont pas spécifiés, la décision sur l'authentification est prise du coté du Serveur Dr.Web.

- `/regagent` <*mode*> : détermine si l'Agent Dr.Web sera enregistré dans la liste des programmes installés. Le paramètre <*mode*> peut prendre les valeurs suivantes :
  - `yes` : enregistrer l'Agent Dr.Web dans la liste des logiciels installés.
  - `no` : ne pas enregistrer l'Agent Dr.Web dans la liste des programmes installés.

  Si la clé n'est pas spécifiée, la valeur `no` est utilisée par défaut.

- `/retry` <*nombre*> : nombre de tentatives de recherche du Serveur Dr.Web par l'envoi des requêtes multicast. En cas d'absence de réponse du Serveur Dr.Web, une fois le nombre de tentatives épuisé, le Serveur est considéré comme introuvable.

  Si la clé n'est pas spécifiée, trois tentatives du Serveur Dr.Web sont effectuées par défaut.

- `/server [`<*protocole*>`/]`<*adresse_du_serveur*>`[:`<*port*>`]` : adresse du Serveur Dr.Web, de laquelle l'Agent Dr.Web sera installé et à laquelle l'Agent Dr.Web se connectera après l'installation.

  Si la clé n'est pas spécifiée, la recherche du Serveur Dr.Web s'effectue par l'envoi des requêtes multicast.

- `/silent` <*mode*> : détermine si l'installateur sera lancé en tâche de fond. Le paramètre <*mode*> peut prendre les valeurs suivantes :
  - `yes` : lancer l'installateur en tâche de fond.
  - `no` : lancer l'installateur en mode graphique.

  Si la clé n'est pas spécifiée, l'installation de l'Agent Dr.Web s'effectue par défaut en mode graphique de l'installateur (voir le **Manuel d'installation**, p. Installation de l'Agent Dr.Web avec l'installateur).

- `/timeout` <*délai*> : délai maximum d'attente de chaque réponse lors de la recherche du Serveur Dr.Web. Spécifié en secondes. La réception des messages de réponse continue jusqu'à ce que le temps d'attente ne dépasse la valeur du délai.

  Si la clé n'est pas spécifiée, la valeur 3 secondes est utilisée par défaut.

G2. Agent Dr.Web pour Windows

Syntaxe de la commande de démarrage :

```
es-service.exe [<clés>]
```

Clés

Chaque clé peut être spécifiée à l'un des formats suivants (les formats sont égaux) :

`-<clé_courte>[ <argument>]`

ou

`--<clé_longue>[=<argument>]`

Vous pouvez utiliser les clés en même temps, y compris les versions courtes et longues.

Si un argument contient des espace, il doit être placé entre guillemets. Les clés courtes peuvent prendre les valeurs sans espace, par exemple :

```
es-service -e192.168.1.1:12345
```

Toutes les clés sont exécutées indépendamment des droits autorisés pour le poste sur le Serveur Dr.Web. C'est-à-dire, même si les droits pour la modification des paramètres de l'Agent Dr.Web sont interdits sur le Serveur Dr.Web, vous pouvez modifier ces paramètres à l'aide des clés de la ligne de commande.

Clés possibles :

- Afficher l'aide :
  - `-?`
  - `--help`
- Modifier l'adresse du Serveur Dr.Web auquel se connecte l'Agent Dr.Web :
  - `-e` *<Serveur Dr.Web>*
  - `--esserver=`*<Serveur Dr.Web>*

  Pour spécifier plusieurs Serveurs Dr.Web en même temps, il faut entrer la clé de chaque adresse du Serveur Dr.Web séparée par un espace. Par exemple :

  ```
  es-service -e 192.168.1.1:12345 -e 192.168.1.2:12345 -e 10.10.1.1:1223
  ```

  ou

```
es-service --esserver=10.3.1.1:123 --esserver=10.3.1.2:123 --
esserver=10.10.1.1:123
```

- Ajouter une clé publique de chiffrement :
  - `-p <clé>`
  - `--addpubkey=<clé>`

  La clé publique indiquée comme argument est copiée dans le répertoire de l'Agent Dr.Web (par défaut, c'est le répertoire `%ProgramFiles%\DrWeb`), elle est renommée en `drwcsd.pub` (si le nom était différent) et relue par le service. Dans ce cas, le fichier de clé publique précédent (s'il a été trouvé) est renommé en `drwcsd.pub.old` et il n'est plus utilisé.

  Toutes les clés publiques utilisées auparavant (les clés transmises du Serveur Dr.Web et enregistrées dans le registre) restent et elles continuent d'être utilisées.
- Ajouter un certificat du Serveur Dr.Web :
  - `-c <certificat>`
  - `--addcert=<certificat>`

  Le fichier de certificat de Serveur Dr.Web indiqué comme argument est copié dans le répertoire de l'Agent Dr.Web (par défaut, c'est le répertoire `%ProgramFiles%\DrWeb`), il est renommée en `drwcsd-certificate.pem` (si le nom était différent) et relu par le service. Dans ce cas, le fichier de certificat précédent (s'il a été trouvé) est renommé en `drwcsd-certificate.pem.old` et il n'est plus utilisé.

  Tous les certificats utilisés auparavant (les certificats transmis du Serveur Dr.Web et enregistrés dans le registre) restent et ils continuent d'être utilisés.
- Se reconnecter au Serveur en tant que novice :
  - `-w <valeur>`
  - `--newbie=<valeur>`

  Valeurs autorisées : `once, always`. Une fois la valeur `always` spécifiée, les paramètres d'authentification de l'Agent Dr.Web seront réinitialisés à chaque lancement du service. Par consequent, l'Agent Dr.Web se connectera chaque fois au Serveur en tant que novice (pour en savoir plus, voir **Manuel Administrateur**, p. Politique d'approbation des nouveaux postes). Si la valeur `once` est spécifiée, les paramètres d'authentification de l'Agent Dr.Web sur le Serveur seront réinitialisés et l'Agent Dr.Web se connectera au Serveur en tant que novice une seule fois.
- Modifier le niveau de détail du journal de l'Agent Dr.Web :
  - `--change-loglevel= <niveau>`

  Les valeurs disponibles du niveau de détail du journal sont les suivantes : `err`, `wrn`, `inf`, `dbg`, `all`. L'exécution de cette commande demande les droits d'administrateur. La désactivation de l'autoprotection et le redémarrage manuel du service ou du système d'exploitation ne sont pas requis.

G3. Serveur Dr.Web

Il existe plusieurs variantes des commandes de démarrage du Serveur Dr.Web qui sont décrites séparément ci-dessous.

Certaines commandes nécessitent la présence dans la ligne de commande des clés obligatoires `modexec` ou `modexecdb` pour l'exécution des modules Lua et la transmission des paramètres supplémentaires, si cela est nécessaire. La commande dans ce cas se forme de manière suivante :

`drwcsd [<clés>] modexec [<nom_de_la_fonction>@]<nom_du_module> [<paramètres>]`

- *<nom_de_la_fonction>* : nom de la fonction qu'il faut exécuter dans le module Lua.
- *<nom_du_module>* : nom du module Lua exécuté.

Les commande décrites dans les paragraphes G3.1. Gestion du Serveur Dr.Web — G3.5. Copie de sauvegarde des données critiques du Serveur Dr.Web sont cross-plateforme, elles peuvent être utilisées sous Windows, ainsi que sous les OS de la famille UNIX (si le contraire n'est pas spécifié).

Si une erreur survient lors du lancement des commandes de gestion du Serveur Dr.Web, référez-vous au fichier de journal du Serveur Dr.Web pour chercher une raison possible (voir le **Manuel administrateur**, le p. Journal du Serveur Dr.Web).

G3.1. Gestion du Serveur Dr.Web

`drwcsd [<clés>]` : spécifier les paramètres du Serveur Dr.Web (les clés sont décrites en détails ci-dessous).

G3.2. Commandes standard

- `drwcsd restart` : réaliser un redémarrage complet du service du Serveur Dr.Web (la commande est exécutée comme la paire : `stop` et puis `start`).
- `drwcsd start` : démarrer le Serveur Dr.Web.
- `drwcsd stop` : effectuer un arrêt normal du Serveur Dr.Web.
- `drwcsd stat` : sortie des statistiques de fonctionnement dans le fichier de journal : heure CPU, utilisation de la mémoire etc. (sous les OS de la famille UNIX — équivalent de la commande `send_signal WINCH` ou `kill SIGWINCH`).
- `drwcsd modexec agent@verify-key` *<chemin_complet_du_fichier_de_clé>* : vérification de la correction du fichier de la clé de licence (`agent.key`).
- `drwcsd modexec enterprise@verify-key` *<nom_complet_du_fichier_de_clé>* : vérification de la correction du fichier de la clé de licence du Serveur Dr.Web (`enterprise.key`). Notez que la clé de licence du Serveur Dr.Web n'est plus utilisée depuis la version 10.
- `drwcsd verifyconfig` *<nom_complet_du_fichier_de_configuration>* : vérification de la syntaxe du fichier de configuration du Serveur Dr.Web (`drwcsd.conf`).

- `drwcsd verifycache` : vérification de la validité du contenu du cache de fichiers du Serveur Dr.Web.
- `drwcsd syncads` : synchroniser la structure du réseau : les conteneurs Active Directory qui contiennent des ordinateurs deviennent des groupes du réseau antivirus dans lesquels les postes de travail sont placés.
- `drwcsd modexec restore@repository-server-update` : restaurer la révision du Serveur Dr.Web (restaurer l'état de la révision actuelle sans sauvegarde d'une copie, la mise à jour de la base de données et des fichiers de configuration). Si cette révision est manquante dans le référentiel, la restauration est impossible.

  Cette action est enregistrée dans le journal d'audit.

- `update@repository-server-update [<revision-to>]` : mise à jour du Serveur Dr.Web. Si la révision à restaurer n'est pas indiquée, la dernière révision du serveur sera restaurée.
- `revert@repository-server-update <revision-to>` : restauration d'une révision particulière du Serveur Dr.Web.

  Les deux dernières actions sont enregistrées dans le journal d'audit.

  La mise à jour et la restauration du Serveur Dr.Web sont décrits dans la documentation d'administrateur, dans la rubrique Mise à jour du Serveur Dr.Web et restauration depuis une copie de sauvegarde.

G3.3. Commandes de gestion de la base de données

Initialisation de la base de données

Lors de l'initialisation, la base de données doit être absente ou vide.

`drwcsd [<clés>] modexecdb database-init [<clé_de_licence> [<mot_de_passe>]]` : initialisation de la base de données.

- *<clé_de_licence>* : chemin vers la clé de licence Dr.Web `agent.key`. Si la clé de licence n'est pas indiquée, il faudra l'ajouter plus tard depuis le Centre de gestion ou bien la recevoir du Serveur voisin Dr.Web par la liaison entre serveurs.
- *<mot_de_passe>* : mot de passe initial de l'administrateur du Serveur Dr.Web (le nom est **admin**). Par défaut c'est **root**.

  S'il faut sauter un ou plusieurs paramètres lors de l'écriture d'une commande, utilisez la valeur spéciale `%nil` à la place de chaque paramètre.

`%nil` peut être omis s'il n'y a pas de paramètres après.

Configuration de l'initialisation de la base de données

En cas d'utilisation de la BD interne, les paramètres d'initialisation peuvent être spécifiés depuis un fichier externe. Dans ce cas-là, la commande suivante est utilisée :

`drwcsd.exe modexecdb database-init@<response-file>`

<response-file> : fichier dans lequel sont enregistrés les paramètres d'initialisation de la BD, chacun d'eux à la ligne et dans le même ordre que les paramètres de la commande `database-init`.

Format du fichier :

```
<nom_complet_du_fichier_de_clé_de_licence>

<mot_de_passe_d'administrateur>
```

En cas d'utilisation du fichier response sous Windows, il est possible d'utiliser n'importe quels symboles dans le mot de passe administrateur.

Si la valeur `%nil` est indiquée dans la ligne, la valeur par défaut sera utilisée (comme dans `database-init`).

Mise à niveau de la version de la base de données

`drwcsd modexecdb database-upgrade [pretend] [upgrade_ver_flag]` : démarrer le Serveur Dr.Web pour mettre à jour la structure de la base de données lors de la migration vers une nouvelle version par les scripts internes.

- `pretend=false` : valeur par défaut. Indique de mettre jour la base de données. Si vous saisissez la valeur `true`, le programme vérifiera uniquement l'actualité des bases virales sans les mettre à jour physiquement.
- `upgrade_ver_flag=true` : si la valeur `true` est indiquée, lors de la mise à jour, la version de la base de données et les données sont enregistrées à chaque mise à niveau réussie vers la version suivante du schéma de la base.

Exportation de la base de données

a) `drwcsd modexecdb database-export` *<fichier>* `[ignore_tables]` : exportation de la base de données vers le fichier indiqué.

- *<chemin>* : chemin d'accès au fichier vers lequel la base de données sera exportée.

- `ignore_tables` : permet d'indiquer une ligne ou un tableau de lignes avec les noms des postes qui ne seront pas exportés.

Exemple pour Windows :

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=trace -log="C:\Program Files\DrWeb Server\var\exportdb.log"
modexecdb database-export "C:\Program Files\DrWeb Server\esbase.es"
```

Sous les OS de la famille **UNIX**, l'action s'exécute du nom de l'utilisateur `drwcs:drwcs` vers le répertoire `$DRWCS_VAR` (excepté **FreeBSD**, qui enregistre par défaut le fichier vers le répertoire depuis lequel a été lancé le script ; si le chemin est spécifié de manière explicite, le répertoire doit être disponible en écriture pour <*utilisateur*> : <*groupe*> qui ont été créés lors de l'installation, par défaut c'est `drwcs:drwcs`).

b) `drwcsd modexecdb database-export-xml` <*fichier xml*> `[ignore_tables]` : exportation de la base de données vers le fichier XML indiqué.

- <*chemin*> : chemin d'accès au fichier XML vers lequel la base de données sera exportée.
- `ignore_tables` : permet d'indiquer une ligne ou un tableau de lignes avec les noms des postes qui ne seront pas exportés.

Si vous indiquez l'extension de fichier `gz`, lors de exportation le fichier de la base de données sera placé dans une archive GZIP.

Si vous n'indiquez aucune extension ou que vous indiquez l'extension autre que `gz`, le fichier d'exportation ne sera pas archivé.

Exemple pour Windows :

- Pour exporter la base de données vers le fichier XML sans compression :

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -bin-root="C:\Program Files\DrWeb Server" -var-
root="C:\Program Files\DrWeb Server\var" -verbosity=trace -rotate=10,10m -
log="C:\Program Files\DrWeb Server\var\exportxmldb.log" modexecdb
database-export-xml database.db
```

- Pour exporter la base de données vers le fichier XML archivé :

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -bin-root="C:\Program Files\DrWeb Server" -var-
root="C:\Program Files\DrWeb Server\var" -verbosity=trace -rotate=10,10m -
log="C:\Program Files\DrWeb Server\var\exportxmldb.log" modexecdb
database-export-xml database.gz
```

Exemple pour les OS de la famille UNIX :

- Pour exporter la base de données vers le fichier XML sans compression :

```
/etc/init.d/drwcsd modexecdb database-export-xml /es/database.db
```

- Pour exporter la base de données vers le fichier XML archivé :

```
/etc/init.d/drwcsd modexecdb database-export-xml /es/database.gz
```

Importer la base de données

a) `drwcsd modexecdb database-import` <*fichier*> `[ignore_tables]` : importation de la base de données depuis le fichier spécifié (l'ancien contenu de la base de données sera effacé).

- <*chemin*> : chemin d'accès au fichier vers lequel la base de données sera exportée.
- `ignore_tables` : permet d'indiquer une ligne ou un tableau de lignes avec les noms des postes qui ne seront pas importés.

b) `drwcsd modexecdb database-import-and-upgrade` <*fichier*> `[import_only_flag] [upgrade_ver_flag] [ignore_tables]` : importation et mise à jour de la base de données obtenue lors de l'exportation depuis le Serveur Dr.Web des versions précédentes (l'ancien contenu de la base de données sera effacé).

- <*chemin*> : chemin d'accès au fichier duquel la base de données sera importée.
- `import_only_flag` : si la valeur `true` est indiquée, la mise à jour et la vérification de la base de données ne seront pas effectuées, seule l'importation sera effectuée.
- `upgrade_ver_flag` : si la valeur `true` est indiquée, lors de la mise à jour de la base, la version de la base de données et les données y sont enregistrées à chaque mise à niveau réussie vers la version suivante du schéma de la base.
- `ignore_tables` : permet d'indiquer une ligne ou un tableau de lignes avec les noms des postes qui ne seront pas importés.

Avant d'exécuter la commande `database-import-and-upgrade`, il est nécessaire de réaliser une copie de sauvegarde de la base de données.

Tous problèmes survenus lors de l'exécution de cette commande peuvent provoquer la suppression de toutes les informations de la base de données.

L'utilisation de la commande `database-import-and-upgrade` pour l'importation avec la mise à niveau de la version de la base de données est possible uniquement au sein d'un seul SGBD.

Vérification de la base de données

`drwcsd modexecdb database-verify [full=false [ignore-version=false]]` : lancer le Serveur Dr.Web pour la vérification de la base de données. Pour enregistrer les informations sur les résultats dans le fichier de journal, il faut entrer la commande avec la clé `-log`. Pour en savoir plus sur l'utilisation de cette clé, consultez le p. G3.8. Description des clés.

- `full=false` : détermine le mode d'analyse. Si la valeur par défaut (`false`) est spécifiée, l'analyse rapide sera effectuée, si la valeur `true` est spécifiée, c'est l'analyse compète qui sera effectuée.

- `ignore-version=false` : détermine s'il faut ignorer le version du schéma de la base de données lors de l'analyse. Par défaut : `false`. Si la valeur `true` est indiquée, l'analyse continuera même si la version de schéma est incorrecte.

Accélération de la base de données

`drwcsd [<clés>] modexecdb database-speedup` : exécuter les commandes `VACUUM`, `CLUSTER`, `ANALYZE` pour accélérer le fonctionnement de la base de données.

Restauration de la base de données

`drwcsd repairdb` : restaurer l'image endommagée de la base de données embarquée **SQLite3** ou des tableaux endommagés de la base de données externe **MySQL**.

La restauration de **SQLite3** peut également s'effectuer automatiquement au lancement du Serveur Dr.Web, si la case **Restaurer automatiquement l'image endommagée** a été cochée dans les paramètres de la base de données **SQLite3**, dans le Centre de gestion (voir le **Manuel administrateur**, le p. Restauration des bases de données).

Nettoyer la base de données

`drwcsd modexecdb database-clean` : nettoyer la base de données du Serveur Dr.Web par la suppression de tous les tableaux.

Changement du mot de passe de l'administrateur

`drwcsd modexecdb set-admin-password` *<nom_d'utilisateur>* *<nouveau_mot_de_passe>* : spécifier un nouveau mot de passe pour le compte d'administrateur indiqué.

G3.4. Commandes de gestion du référentiel

Avant d'exécuter les commandes `syncrepository`, `restorerepo` et `saverepo`, il faut obligatoirement arrêter le Serveur Dr.Web.

- `drwcsd syncrepository` : réaliser une synchronisation du référentiel avec le SGM Dr.Web. La commande lance le processus du Serveur Dr.Web. Une requête est envoyée au SGM et le référentiel est mis à jour en cas de disponibilité des mises à jour.
- `drwcsd rerepository` : relire le référentiel depuis le disque.
- `drwcsd updrepository` : mettre à jour le référentiel depuis le SGM Dr.Web. La commande envoie un signal au processus en cours du Serveur Dr.Web pour appeler le SGM et mettre à jour le référentiel en cas de disponibilité des mises à jour. Si le Serveur Dr.Web n'est pas lancé, le référentiel n'est pas mis à jour.

- `drwcsd [<clés>] restorerepo <nom_complet_de_l'archive>` : restaurer le référentiel du Serveur Dr.Web depuis l'archive zip créée avec la commande `saverepo`.
- `drwcsd [<clés>] saverepo <nom_complet_de_l'archive>` : sauvegarder tout le référentiel du Serveur Dr.Web dans l'archive zip spécifiée. L'archive obtenue peut être importée sur le Serveur Dr.Web avec la commande `restorerepo`.

> Les archives utilisées par les commandes `restorerepo` et `saverepo` ne sont pas compatibles avec celles utilisées pour l'exportation et l'importation du référentiel via le Centre de gestion.

G3.5. Copie de sauvegarde des données critiques du Serveur Dr.Web

La commande suivante permet de créer une copie de sauvegarde des données critiques du Serveur Dr.Web (des clés de licence, du contenu de la base de données, de la clé privée de chiffrement, de la configuration du Serveur Dr.Web et du Centre de gestion) :

`drwcsd -home=<chemin> backup [<répertoire> [<nombre>]]`

- Les données critiques du Serveur Dr.Web sont copiées dans le *<répertoire>* spécifié.
- La clé `-home` spécifie le répertoire d'installation du Serveur Dr.Web.
- Paramètre *<nombre>* : nombre de copies sauvegardées du même fichier.

Exemple pour Windows :

```
"C:\Program Files\DrWeb Server\bin\drwcsd" -home="C:\Program Files\DrWeb Server" -verbosity=all -log="C:\Program Files\DrWeb Server\var\backup.log" backup "C:\DrWeb Backup\"
```

Tous les fichiers de la copie de sauvegarde, excepté le contenu de la base de données, sont prêts à l'emploi. La copie de sauvegarde est enregistrée au format `.dz` compatible avec `gzip` ainsi qu'avec d'autres utilitaires d'archivage. Le contenu de la base de données peut être importé de la copie de sauvegarde vers la base de données opérationnelle du Serveur Dr.Web, ainsi, les données seront restaurées (voir le p. Restauration de la base de données Dr.Web Enterprise Security Suite).

Au cours de son fonctionnement, le Serveur Dr.Web enregistre régulièrement les copies de sauvegarde des informations importantes dans les répertoires suivants :

- sous **Windows** : *<disque_d'installation>* : `\DrWeb Backup`
- sous **Linux** : `/var/opt/drwcs/backup`
- sous **FreeBSD** : `/var/drwcs/backup`

Pour assurer la fonction de copie de sauvegarde, la planification du Serveur Dr.Web contient une tâche quotidienne. Si la tâche est introuvable, il est recommandé de la créer.

G3.6. Commandes disponibles uniquement sous Windows

- `drwcsd [<clés>] install[<nom_du_service>]` : installer le service du Serveur Dr.Web dans le système et assigner les clés spécifiées au lancement de ce service.

  <nom_du_service> : suffixe qui s'ajoute au nom du service par défaut. Dans ce cas, le nom complet du service est le suivant `DrWebES-<nom_du_service>`. La commande `install` crée (édite) le service avec le nom spécifié et ajoute automatiquement la clé `–service=<nom_du_service>` dans ses arguments. Les services existants ne sont pas modifiés.

- `drwcsd uninstall[<nom_du_service>]` : supprimer le service du Serveur Dr.Web depuis le système.

  <nom_du_serveur> : suffixe qui s'ajoute au nom du service par défaut. Dans ce cas, le nom complet du service est le suivant : `DrWebES-<nom_du_service>`.

- `drwcsd kill` : arrêt forcé du service du Serveur Dr.Web (si l'arrêt normal est échoué). Il n'est pas recommandé d'exécuter cette commande sans une nécessité absolue.
- `drwcsd reconfigure` : relire le fichier de configuration et redémarrer (la commande s'exécute plus vite, sans lancer un nouveau processus).
- `drwcsd silent [<options>] <commande>` : interdire l'affichage des messages du Serveur Dr.Web en cas de lancement de la commande spécifiée dans le paramètre *<commande>*. La commande est utilisée dans les fichiers de commande afin de désactiver l'interactivité du Serveur Dr.Web.

G3.7. Commandes disponibles uniquement sous les OS de la famille UNIX

- `drwcsd cacherepo` : créer ou récupérer le cache de fichiers du référentiel du Serveur Dr.Web.
- `drwcsd config` : équivalent de la commande `reconfigure` ou `kill SIGHUP` — redémarrage du Serveur Dr.Web.
- `drwcsd interactive` : démarre le Serveur Dr.Web mais ne confie pas la gestion au processus.
- `drwcsd newkey` : génération des nouvelles clés de chiffrement (`drwcsd.pri` et `drwcsd.pub`) et du certificat `drwcsd-certificate.pem`.
- `drwcsd readrepo` : relire le référentiel depuis le disque. Ceci est équivalent à la commande `rerepository`.
- `drwcsd selfcert [<nom_de_l'ordinateur>]` : génération d'un nouveau certificat SSL `(certificate.pem)` et de la clé privée RSA `(private-key.pem)`. Les paramètre spécifie le nom de l'ordinateur avec le Serveur Dr.Web installé pour lequel les fichiers seront générés. Si le paramètre n'est pas spécifié, le nom de l'ordinateur est substitué automatiquement par la fonction système.
- `drwcsd shell <nom_du_fichier>` : lancement du fichier du script. La commande lance `$SHELL` ou `/bin/sh` et lui transmet le fichier indiqué.
- `drwcsd showpath` : afficher tous les chemins du programme enregistrés dans le système.
- `drwcsd status` : afficher le statut courant du Serveur Dr.Web (en cours, arrêté).

G3.8. Description des clés

Clés cross-plateforme :

- `-activation-key=<clé_de_licence>` : clé de licence du Serveur Dr.Web. Par défaut, c'est le fichier `enterprise.key` se trouvant dans le sous-répertoire `etc` du répertoire racine.

  Notez que la clé de licence du Serveur Dr.Web n'est plus utilisée depuis la version 10. La clé `-activation-key` peut être utilisée lors de la mise à niveau du Serveur Dr.Web des versions précédentes ou lors de l'initialisation de la base de données : l'identificateur du Serveur Dr.Web sera pris dans la clé de licence indiquée.
- `-bin-root=<répertoire>` : chemin vers les fichiers exécutables. Par défaut, c'est le sous-répertoire `bin` du répertoire racine.
- `-conf=<fichier>` : nom et emplacement du fichier de configuration du Serveur Dr.Web. Par défaut, c'est le fichier `drwcsd.conf` se trouvant dans le sous-répertoire `etc` du répertoire racine.
- `-daemon` : pour les plateformes Windows : cela désigne le lancement en tant que service ; pour les plateformes UNIX : la daemonisation du processus (passer vers le répertoire racine, se déconnecter du terminal et basculer vers le mode en tâche de fond).
- `-db-verify=on` : vérifier l'intégrité de la BD au démarrage du Serveur Dr.Web. La valeur par défaut est spécifiée. Il est fortement déconseillé de lancer la clé avec une valeur opposée spécifiée de manière explicite, excepté le cas de démarrage immédiat après la vérification de la BD avec la commande `drwcsd modexecdb database-verify` (voir ci-dessus).
- `-help` : afficher la rubrique d'aide. Ceci est équivalent aux programmes décrits ci-dessus.
- `-hooks` : autoriser l'exécution par le Serveur Dr.Web des scripts d'extension utilisateur se trouvant dans le dossier suivant :
  - sous Windows : `var\extensions`
  - sous FreeBSD : `/var/drwcs/extensions`
  - sous Linux : `/var/opt/drwcs/extensions`

  se trouvant dans le répertoire d'installation du Serveur Dr.Web. Les scripts sont destinés à automatiser les opérations de l'administrateur afin de faciliter et d'accélérer l'exécution de certaines tâches. Par défaut, tous les scripts sont désactivés.
- `-home=<répertoire>` : répertoire d'installation du Serveur Dr.Web (répertoire racine). La structure de ce répertoire est décrite dans le **Manuel d'installation**, p. Installation du Serveur Dr.Web sous Windows. Par défaut c'est le répertoire courant au démarrage.
- `-log=<fichier journal>` : activer la journalisation du Serveur Dr.Web dans le fichier se trouvant dans le chemin suivant.

  A la place du nom de fichier il est possible d'utiliser le signe "moins" (pour le Serveur Dr.Web sur la plateforme UNIX), ce qui désigne la sortie du journal vers la sortie standard. Les opérations sur les plateformes UNIX sont exécutées au nom de l'utilisateur drwcs. S'il n'a pas le droit d'enregistrer le fichier de journal dans le répertoire, une erreur survient.

  Par défaut : pour les OS Windows — `drwcsd.log` dans le répertoire spécifié par la clé `-var-root`, pour les OS de la famille UNIX avec la clé `-syslog=user` (voir ci-dessous).

- `-private-key=<clé_privée>` : clé de chiffrement privée du Serveur Dr.Web. Par défaut, c'est `drwcsd.pri` dans le sous-répertoire `etc` du répertoire racine.
- `-rotate=<N><f>,<M><u>` : mode de rotation du journal de fonctionnement du Serveur Dr.Web, où :

Paramètre	Description
<*N*>	Nombre total de fichiers de journal (y compris le fichier actuel et les archives).
<*f*>	Format de sauvegarde des fichiers de journal, valeurs possibles : • z (gzip) : compresser les fichiers, utilisé par défaut, • p (plain) : ne pas compresser les fichiers.
<*M*>	Taille du fichier de journal ou période de rotation, en fonction de la valeur <*u*> ;
<*u*>	Unité de mesure, valeurs possibles : • pour paramétrer la rotation par taille de fichier de journal : ▫ k : Ko, ▫ m : Mo, ▫ g : Go. • pour paramétrer la rotation en fonction de la période : ▫ H : heures, ▫ D : jours, ▫ W : semaines.

Si la rotation par période est définie, la synchronisation s'effectue indépendamment en fonction de l'heure du lancement de la commande : la valeur H indique une synchronisation effectuée au début d'une heure, D — au début d'un jour, W — au début d'une semaine (00h00 le lundi) en fonction de la périodicité indiquée dans le paramètre <*u*>.

Éléments de référence initiaux — Janvier 01, année 01 AD, UTC+0.

Les valeurs par défaut sont `10z,10m`, ce qui signifie de sauvegarder 10 fichiers, de 10 Mo chacun, et d'utiliser la compression. Il est également possible d'utiliser le format spécialisé `none (-rotate=none)` — ce qui désigne « ne pas utiliser la rotation, écrire toujours dans le même fichier à taille illimitée ».

Dans le mode de rotation, le format suivant de noms de fichiers est utilisé : `file.<N>.log` ou `file.<N>.log.dz`, avec <*N*> — numéro d'ordre : 1, 2, etc.

Si le nom du fichier de journal (voir ci-dessus la clé `-log`) est, par exemple, `file.log`. Dans ce cas-là :

- `file.log` : fichier courant (vers lequel l'écriture est effectuée),
- `file.1.log` : fichier précédent,

  - `file.2.log` etc. : le nombre plus grand correspond à la version plus ancienne.
- `-trace` : réaliser une journalisation détaillée de l'endroit de l'erreur.
- `-var-root=<`*répertoire*`>` : chemin vers le répertoire dans lequel le Serveur Dr.Web est autorisé à écrire et qui est destiné à sauvegarder les fichiers modifiables (par exemple les journaux ainsi que les fichiers du référentiel). Par défaut c'est le sous-répertoire `var` du répertoire racine.
- `-verbosity=<`*niveau*`>` : niveau de détail du journal. Par défaut c'est `WARNING`. Les valeurs possibles sont les suivantes : `ALL`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `DEBUG`, `TRACE3`, `TRACE2`, `TRACE1`, `TRACE`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `CRIT`. Les valeurs `ALL` et `DEBUG3` sont des synonymes.

  Si nécessaire, vous pouvez spécifier les niveaux de détails particuliers pour plusieurs sources de messages en même temps au format suivant :

  `-verbosity=<`*source_du_message1*`>:<`*niveau1*`>,<`*source_du_message2*`>:<`*niveau2*`>,<`*source_du_message3*`>:<`*niveau3*`>`, etc. Dans ce cas *<niveau>* est hérité conformément au principe général, c'est-à-dire, on trouve la source parente la plus proche avec le niveau de détails spécifié. La clé au format `-verbosity=all:all` équivaut à la clé `-verbosity=all` (voir également Annexe J. Format des fichiers de journal).

  > Cette clé détermine un niveau de détail de la journalisation dans le fichier spécifié par la clé qui suit après `-log` (voir ci-dessus). Une commande peut comprendre plusieurs clés de ce type.
  >
  > ---
  >
  > Les clés `-verbosity` et `-log` sont sensibles à la position.
  >
  > En cas d'utilisation de ces deux clés à la fois, la clé `-verbosity` doit précéder la clé `-log`: la clé `-verbosity` modifie le niveau de détail des journaux se trouvant sur les chemins spécifiés après dans la ligne de commande.

Clés disponibles uniquement sous Windows :

- `-minimized` : réduire la fenêtre (uniquement en cas de démarrage en mode interactif et non pas comme service).
- `-service=<`*nom_du_service*`>` : la clé est utilisée par le processus lancé du service d'auto-identification et d'installation de l'autoprotection dans la branche de registre du service du Serveur Dr.Web. *<nom_du_serveur>* : suffixe qui s'ajoute au nom du service par défaut. Dans ce cas, le nom complet du service est le suivant : `DrWebES-<`*nom_du_service*`>`.

  La clé est utilisée par la commande `install`. L'utilisation libre n'est pas prévue.
- `-screen-size=<`*taille*`>` : (uniquement en cas de démarrage en mode interactif et non pas comme service) : taille spécifiée en lignes du journal visible dans la fenêtre du Serveur Dr.Web, par défaut c'est 1000.

Clés disponibles uniquement sous les OS de la famille UNIX :

- `-etc=<chemin>` : chemin vers le répertoire `etc` (`<var>/etc`).
- `-keep` : ne pas supprimer le contenu du répertoire temporaire après l'installation du Serveur Dr.Web.
- `-pid=<fichier>` : fichier dans lequel le Serveur Dr.Web écrit l'identificateur de son processus.
- `-syslog=<mode>` : journalisation vers le journal système. Les modes disponibles sont les suivants : `auth, cron, daemon, kern, lpr, mail, news, syslog, user, uucp, local0-local7` et en cas de certaines plateformes : `ftp, authpriv` et `console`.

> Les paramètres `-syslog` et `-log` fonctionnent en parallèle. C'est-à-dire, lorsque vous démarrez le Serveur Dr.Web avec la clé `-syslog` (par exemple, `service drwcsd start -syslog=user`), le Serveur Dr.Web démarre avec la valeur spécifiée pour la clé `-syslog` et avec la valeur par défaut de la clé `-log`.

- `-user=<utilisateur>`, `-group=<groupe>` : ne sont disponibles que sous UNIX, en cas de lancement sous le nom utilisateur **root** ; les clés enjoignent de modifier l'utilisateur ou le groupe du processus et de s'exécuter avec les privilèges de l'utilisateur/groupe spécifié.

G3.9. Variables disponibles sous les OS de la famille UNIX

Afin de faciliter la gestion du Serveur Dr.Web sous les OS de la famille UNIX, l'administrateur dispose des variables se trouvant dans le fichier de script qui est sauvegardé dans le répertoire suivant :

- Sous Linux : `/etc/init.d/drwcsd`.
- Sous FreeBSD : `/usr/local/etc/rc.d/drwcsd` (lien symbolique : `/usr/local/etc/drweb.com/software/init.d/drwcsd`).

Le Tableau H-1 affiche la correspondance entre les variables et les clés de la ligne de commande pour `drwcsd`.

Tableau H-1.

Clé	Variable	Paramètres par défaut
`-home`	DRWCS_HOME	• `/usr/local/drwcs` : sous OS FreeBSD, • `/opt/drwcs` : sous Linux.
`-var-root`	DRWCS_VAR	• `/var/drwcs` : sous FreeBSD, • `/var/opt/drwcs` : sous Linux.
`-etc`	DRWCS_ETC	`$DRWCS_VAR/etc`
`-rotate`	DRWCS_ROT	`10,10m`

Clé	Variable	Paramètres par défaut
-verbosity	DRWCS_LEV	info
-log	DRWCS_LOG	$DRWCS_VAR/log/drwcsd.log
-conf	DRWCS_CFG	$DRWCS_ETC/drwcsd.conf
-pid	DRWCS_PID	
-user	DRWCS_USER	
-group	DRWCS_GROUP	
-hooks	DRWCS_HOOKS	
-trace	DRWCS_TRACE	

Les variables DRWCS_HOOKS et DRWCS_TRACE n'ont pas de paramètres. Lors de la spécification des variables, les clés respectives sont ajoutées à l'exécution du script. Si les variables ne sont pas spécifiées, les clés ne seront pas ajoutées.

Les autres variables sont présentes dans le Tableau H-2.

Tableau H-2.

Variable	Paramètres par défaut	Description
DRWCS_ADDOPT		Clés supplémentaires de la ligne de commande qui doivent être transmises à drwcsd lors du démarrage.
DRWCS_CORE	unlimited	Taille maximum du fichier core.
DRWCS_FILES	131170	Nombre maximum de descripteurs de fichiers pouvant être ouverts par le Serveur Dr.Web.
DRWCS_BIN	$DRWCS_HOME/bin	Répertoire depuis lequel drwcsd sera lancé.
DRWCS_LIB	$DRWCS_HOME/lib	Répertoire avec les bibliothèques du Serveur Dr.Web.

Les valeurs des paramètres par défaut seront prises en compte à condition que les variables ne soient pas déterminées dans le script drwcsd.

Les variables `DRWCS_HOME`, `DRWCS_VAR`, `DRWCS_ETC`, `DRWCS_USER`, `DRWCS_GROUP`, `DRWCS_HOOKS` sont déjà déterminées dans le fichier du script `drwcsd`.

S'il existe le fichier `/var/opt/drwcs/etc/common.conf`, ce fichier sera inclus dans `drwcsd`, dans ce cas-là, certaines variables peuvent être modifiées ; cependant si elles ne sont pas exportées (avec la commande `export`), ceci n'aura pas d'impact.

Pour spécifier les variables

1. Ajoutez la définition de la variable dans le fichier du script `drwcsd`.
2. Exportez la variable avec la commande `export` (la commande est spécifiée dans le même emplacement).
3. Au lancement d'un autre processus du même script, ce processus lit les valeurs qui ont été déterminées.

G3.10. Gestion du Serveur Dr.Web sous les OS de la famille UNIX avec la commande kill

Le Serveur Dr.Web sous UNIX est géré par les signaux envoyés vers le processus du Serveur Dr.Web par l'utilitaire `kill`.

Pour obtenir une aide détaillée sur l'utilitaire `kill`, utilisez la commande `man kill`.

Signaux de l'utilitaire et actions qu'ils effectuent :

- `SIGWINCH` : sortie des statistiques vers le fichier de journal (heure CPU, utilisation de la mémoire etc.),
- `SIGUSR1` : relire le référentiel des produit depuis le disque,
- `SIGUSR2` : relire les modèles des messages depuis le disque,
- `SIGHUP` : redémarrage du Serveur Dr.Web,
- `SIGTERM` : le Serveur Dr.Web est en cours d'arrêt,
- `SIGQUIT` : le Serveur Dr.Web est en cours d'arrêt,
- `SIGINT` : le Serveur Dr.Web est en cours d'arrêt.

Les actions équivalentes pour le Serveur Dr.Web sous Windows sont effectuées avec les clés de la commande drwcsd, voir l'Annexe G3.3. Commandes de gestion de la base de données.

G4. Scanner Dr.Web pour Windows

Ce composant du logiciel installé sur le poste de travail a les paramètres de la ligne de commande décrits dans le Manuel Utilisateur **Agent Dr.Web pour Windows**. La seule différence est que lors du démarrage du Scanner effectué par l'Agent Dr.Web, les paramètres `/go /st` sont transmis au Scanner de manière automatique et obligatoire.

G5. Serveur proxy Dr.Web

Pour configurer les paramètres du Serveur proxy, lancez avec les clés correspondantes le fichier exécutable `drwcsd-proxy` qui se trouve dans le sous-répertoire `bin` du répertoire d'installation du Serveur proxy.

Syntaxe de la commande de démarrage

`drwcsd-proxy [<clés>] [<commandes> [<arguments_des_commandes>]]`

Clés possibles

Clés cross-plateforme :

- `--console=[yes/no]` : lancer le Serveur proxy en mode interactif. Dans ce cas, le journal du Serveur proxy s'affiche dans la console.

  Par défaut : `no`.
- `--etc-root=<chemin>` : chemin vers le répertoire contenant les fichiers de configuration (`drwcsd-proxy.conf`, `drwcsd.proxy.auth`, etc.).

  Par défaut : `$var/etc`
- `--home=<chemin>` : chemin vers le répertoire d'installation du Serveur proxy.

  Par défaut : `$exe-dir/`
- `--log-root=<chemin>` : chemin vers le répertoire contenant les fichiers journaux du Serveur proxy.

  Par défaut : `$var/log`
- `--pool-size=<N>` : nombre des flux pour le travail avec les clients.

  Par défaut : le nombre de noyaux de l'ordinateur sur lequel le Serveur proxy est installé (pas moins de 2).
- `-rotate=<N><f>,<M><u>` : mode de rotation du journal de fonctionnement du Serveur proxy, avec :

Paramètre	Description
<*N*>	Nombre total de fichiers de journal (y compris le fichier actuel et les archives).

Paramètre	Description
<*f*>	Format de sauvegarde des fichiers de journal, valeurs possibles : • z (gzip) : compresser les fichiers, utilisé par défaut, • p (plain) : ne pas compresser les fichiers.
<*M*>	Taille du fichier de journal ou période de rotation, en fonction de la valeur <*u*> ;
<*u*>	Unité de mesure, valeurs possibles : • pour paramétrer la rotation par taille de fichier de journal : ▫ k : Ko, ▫ m : Mo, ▫ g : Go. • pour paramétrer la rotation en fonction de la période : ▫ H : heures, ▫ D : jours, ▫ W : semaines.

Si la rotation par période est définie, la synchronisation s'effectue indépendamment en fonction de l'heure du lancement de la commande : la valeur H indique une synchronisation effectuée au début d'une heure, D — au début d'un jour, W — au début d'une semaine (00h00 le lundi) en fonction de la périodicité indiquée dans le paramètre <*u*>.

Éléments de référence initiaux — Janvier 01, année 01 AD, UTC+0.

Les valeurs par défaut sont `10,10m`, ce qui enjoint de sauvegarder 10 fichiers, de 10 Mo chacun, et d'utiliser la compression.

- `--trace=[yes/no]` : activer la journalisation détaillée des appels au Serveur proxy. Disponible uniquement si l'assemblage du Serveur Proxy supporte le suivi détaillé de la pile d'appels (en cas d'exclusion, la pile est enregistrée dans le journal).

  Par défaut : `no`.

- `--tmp-root=`<*chemin*> : chemin vers le répertoire contenant les fichiers temporaires. Utilisé lors de la mise à jour automatique du Serveur proxy.

  Par défaut : `$var/tmp`.

- `--var-root=`<*chemin*> : chemin d'accès au répertoire de travail du Serveur proxy pour la sauvegarde du cache et de la base de données.

  Par défaut :

  ▫ OS Windows : `%ALLUSERSPROFILE%\Doctor Web\drwcs`

  ▫ OS Linux : `/var/opt/drwcs`

  ▫ OS FreeBSD : `/var/drwcs`

- `--verbosity=`<*niveau_de_détails*> : niveau de détails du journal. Par défaut, `TRACE`. Les valeurs autorisées sont : `ALL`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `DEBUG`, `TRACE3`, `TRACE2`, `TRACE1`, `TRACE`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `CRIT`. Les valeurs `ALL` et `DEBUG3` sont identiques.

  Si nécessaire, vous pouvez spécifier les niveaux de détails particuliers pour plusieurs sources de messages en même temps au format suivant :
  `-verbosity=`<*source_du_message1*>`:`<*niveau1*>`,`<*source_du_message2*>`:`<*niveau2*>`,`<*source_du_message3*>`:`<*niveau3*>, etc. Dans ce cas <*niveau*> est hérité conformément au principe général, c'est-à-dire, on trouve la source parente la plus proche avec le niveau de détails spécifié. La clé au format `-verbosity=all:all` équivaut à la clé `-verbosity=all` (voir également Annexe J. Format des fichiers de journal).

  > Toutes les commandes de configuration des paramètres du Serveur Proxy peuvent être définies simultanément.

Postes tournant sous les OS de la famille UNIX :

- `--user` : spécifier l'identificateur de l'utilisateur. La clé peut être utilisée en mode standard et en mode de daemon.
- `--group` : spécifier l'identificateur du groupe. La clé peut être utilisée en mode standard et en mode de daemon.
- `--pid=`<*chemin*> : chemin vers le répertoire avec l'identificateur du processus.

  Par défaut : `/var/opt/drwcs/run/drwcsd-proxy.pid`

Commandes possibles et leurs arguments

> Si la commande n'est pas indiquée, la commande `run` est utilisée par défaut.

- `import` <*chemin*> `[`<*révision*>`]` `[`<*produits*>`]` : importer les fichiers du référentiel du Serveur Dr.Web vers le cache du Serveur proxy.
  - <*chemin*> : chemin vers le répertoire contenant le référentiel du Serveur Dr.Web. Le référentiel du Serveur Dr.Web doit être téléchargé sur l'ordinateur avec le Serveur proxy installé.
  - <*révision*> : nombre maximum des révisions à importer. Si la valeur n'est pas indiquée, toutes les révisions seront importées.
  - <*produits*> : liste des produits à importer séparés par des espaces. La liste vide est utilisée par défaut, c'est-à-dire, importer tous les produits du référentiel sauf le Serveur Dr.Web. Si la liste est spécifiée, seuls les produits listés sont importés.
- `help` : afficher un message d'aide sur les clés pour la configuration du Serveur Proxy.
- `run` : lancer le Serveur proxy en mode ordinaire.

Commandes disponibles uniquement sous Windows :

- `install` : installer le service.
- `start` : lancer le service installé.
- `stop` : arrêter le service lancé.
- `uninstall` : désinstaller le service.

Commandes disponibles uniquement sous les OS de la famille UNIX :

- `daemon` : lancer le Serveur proxy en mode de daemon (voir également Clés sous les OS de la famille UNIX).

Script de gestion du Serveur proxy et variables disponibles sous les OS de la famille UNIX

Afin de faciliter la gestion du Serveur proxy sous les OS de la famille UNIX, l'administrateur dispose des variables se trouvant dans le fichier de script `drwcsd-proxy.sh` qui est sauvegardé dans le répertoire suivant :

- **Linux** : `/etc/init.d/dwcp_proxy`
- **FreeBSD** : `/usr/local/etc/rc.d/dwcp_proxy`

Le script accepte les commandes suivantes :

- `import` <*chemin*> `[`<*révision*>`]` `[`<*produits*>`]` : importer les fichiers du référentiel du Serveur Dr.Web vers le cache du Serveur proxy (équivalent à la commande du Serveur proxy — voir ci-dessus).
- `interactive` : lancer le Serveur proxy en mode interactif. Dans ce cas, le journal du Serveur proxy s'affiche dans la console.
- `start` : lancer le Serveur proxy en mode de démon.
- `status` : vérifier si le démon est lancé.
- `stop` : arrêter le démon lancé.

Le Tableau H-3 présente la correspondance entre les variables et les clés de la ligne de commande pour `drwcsd-proxy`.

Tableau H-3.

Clé	Variable	Paramètres par défaut
`--home=`<*chemin*>	`$DRWCS_PROXY_HOME`	`$exe-dir/`
`--var-root=`<*chemin*>	`$DRWCS_PROXY_VAR`	• OS Linux : `/var/opt/drwcs` • OS FreeBSD : `/var/drwcs`

Clé	Variable	Paramètres par défaut
`--etc-root=<chemin>`	`$DRWCS_PROXY_ETC`	`$var/etc`
`--tmp-root=<chemin>`	`$DRWCS_PROXY_TMP`	`$var/tmp`
`--log-root=<chemin>`	`$DRWCS_PROXY_LOG`	`$var/log`
–	`$DRWCS_PROXY_LIB`	`$DRWCS_PROXY_HOME/lib`
–	`$DRWCS_PROXY_BIN`	`$DRWCS_PROXY_HOME/bin`
`--verbosity=<niveau_de_détails>`	`$DRWCS_PROXY_VERBOSITY`	`INFO`
`--rotate=<N><f>,<M><u>`	`$DRWCS_PROXY_ROTATE`	`10,10m`
`--pid`	`$DRWCS_PROXY_PID`	`/var/opt/drwcs/run/drwcsd-proxy.pid`
–	`$NO_DRWCS_PROXY_USER`	Si une valeur est attribuée, `$DRWCS_PROXY_USER` sera ignoré.
`--user`	`$DRWCS_PROXY_USER`	–
–	`$NO_DRWCS_PROXY_GROUP`	Si une valeur est attribuée, `$DRWCS_PROXY_GROUP` sera ignoré.
`--group`	`$DRWCS_PROXY_GROUP`	–
–	`$DRWCS_PROXY_FILES`	131170 mais pas moins de la limite actuelle.

G6. Installateur du Serveur Dr.Web sous les OS de la famille UNIX

Syntaxe de la commande de démarrage :

<nom_du_package>`.run [<`*clés*`>] [--] [<`*arguments*`>]`

où :

- `[--]` : caractère facultatif séparé qui marque la fin de la liste des clés et qui sépare la liste des clés des arguments supplémentaires.
- `[<`*arguments*`>]` : arguments supplémentaires ou scripts intégrés.

Clés pour l'obtention de l'aide ou des informations :

- `--help` : afficher l'aide sur les clés.

- `--info` : afficher les informations détaillées sur le package ; nom ; répertoire cible ; taille du package décompressé ; algorithme de compression ; date de compression ; version de `makeself` qui a été utilisé pour la compression ; commande de compression ; script qui sera lancé après la décompression ; informations sur la copie du contenu de l'archive dans un répertoire temporaire (si le contenu ne sera pas copié, rien n'est affiché) ; informations sur le répertoire cible (s'il est permanent ou il sera supprimé après le traitement du script).
- `--lsm` : afficher le contenu de l'enregistrement LSM avec les informations de base sur les package : nom, version, description, auteur, etc. Si l'enregistrement LSM n'est pas rempli, une notification correspondante va s'afficher.
- `--list` : afficher la liste des fichiers dans le package d'installation.
- `--check` : vérifier l'intégrité du package d'installation.

Clés pour le lancement du package :

- `--confirm` : afficher la demande avant de lancer le script intégré.
- `--noexec` : ne pas lancer le script intégré.
- `--keep` : ne pas supprimer le répertoire indiqué après l'exécution du script intégré.
- `--nox11` : ne pas lancer l'émulateur du terminal `xterm` à la fin de l'installation.
- `--nochown` : ne pas designer l'utilisateur qui initie l'installation comme propriétaire de fichiers extraits.
- `--log` <*chemin*> : journaliser l'installation dans le fichier dans le chemin d'accès indiqué.
- `--nolog` : ne pas journaliser les installations.
- `--target` <*répertoire*> : extraire le package d'installation dans le répertoire indiqué.
- `--tar` <*argument_1*> `[`<*argument_2*> ...`]` : obtenir l'accès au contenu du package d'installation avec la commande `tar`.

Arguments supplémentaires :

- `--help` : afficher l'aide sur les arguments supplémentaires.
- `--quiet` : lancer l'installateur en tâche de fond. Répondez par la positive à toutes les questions suivantes de l'installateur :
  - accepter le contrat de licence,
  - spécifier la copie de sauvegarde dans le répertoire par défaut,
  - continuer l'installation à condition que la distribution supplémentaire (extra) installée dans le système soit supprimée.
- `--clean` : installer le package avec les paramètres du Serveur Dr.Web par défaut sans utiliser la copie de sauvegarde pour restaurer les paramètres de l'installation précédente.
- `--preseed` <*chemin*> : chemin vers le fichier de configuration contenant les réponses préconfigurées aux questions de l'installateur lors de l'installation.

  Variables pour spécifier les réponses préconfugurées dans le fichier de configuration :

- `DEFAULT_BACKUP_DIR=<chemin>` : chemin vers le répertoire contenant la copie de sauvegarde qui sera utilisée pour restaurer les paramètres de la version précédente (n'est pas utilisée si l'installation avec les paramètres par défaut est spécifiée).
- `QUIET_INSTALL=[0|1]` : détermine l'utilisation du mode Tâche de fond de l'installateur :
  - 0 : lancer l'installateur en tâche de fond ;
  - 1 : lancer l'installateur en tâche de fond.
- `CLEAN_INSTALL=[0|1]` : détermine l'utilisation de la copie de sauvegarde lors de l'installation :
  - 0 : installation avec les paramètres par défaut sans restauration à partir d'une copie de sauvegarde ;
  - 1 : installation avec la restauration à partir d'une copie de sauvegarde placée dans le répertoire de la variable `DEFAULT_BACKUP_DIR`. Si la variable `DEFAULT_BACKUP_DIR` n'est pas spécifiée, la copie de sauvegarde de `/var/tmp/drwcs` sera utilisée.
- `ADMIN_PASSWORD=<mot de passe>` : mot de passe du compte administrateur par défaut (**admin**).
  - Si la variable `ADMIN_PASSWORD` est spécifiée dans le fichier, sa valeur sera utilisée comme mot de passe de l'administrateur. À la fin de l'installation, le message suivant s'affichera : `Password specified in the configuration file for the default administrator (admin) : <mot de passe>`
  - Si la variable `ADMIN_PASSWORD` n'est pas spécifiée dans le fichier, le mot de passe est créé automatiquement. À la fin de l'installation, le message suivant s'affichera : `Automatically generated password for the default administrator (admin) : <mot de passe>`

Si lors de l'utilisation de la clé `--preseed`, le lancement de l'installateur en tâche de fond n'est pas déterminé à l'aide de la variable `QUIET_INSTALL=0` dans le fichier de configuration, les valeurs des autres variables du fichier de configuration seront modifiées par l'utilisateur durant l'installation.

G7. Utilitaires

G7.1. Utilitaire de génération des clés numériques et des certificats

Il existe les versions suivantes de l'utilitaire de console de génération de clés numériques et de certificats :

Fichier exécutable	Localisation	Description
`drweb-sign-<OS>-<nombre de bits>`	Centre de gestion, section **Administration** → **Utilitaires**	Version indépendante de l'utilitaire. Elle peut être lancée d'un répertoire aléatoire ou sur n'importe quel ordinateur ayant le système d'exploitation correspondant.
	Répertoire du Serveur Dr.Web `webmin/utilities`	
`drwsign`	Répertoire du Serveur Dr.Web `bin`	La version de l'utilitaire dépend de la présence des bibliothèques de serveur. Elle peut être lancée uniquement du répertoire de son emplacement.

Les fonctions des versions de l'utilitaire `drweb-sign-<OS>-<nombre de bits>` et `drwsign` sont équivalentes. Vous trouverez ci-dessous la version `drwsign`, pourtant toutes les exemples concernent les deux versions.

Syntaxe de la commande de démarrage

- `drwsign check [-public-key=<clé_publique>] <fichier>`

  Vérifier la signature du fichier indiqué en utilisant la clé publique de la personne qui a signé le fichier.

Paramètre de la clé	Valeur par défaut
<clé_publique>	`drwcsd.pub`

- `drwsign extract [-private-key=<clé_privée>] [-cert=<certificat_du_Serveur_Dr.Web>] <clé_publique>`

  Extraire la clé publique du fichier de la clé privée ou du fichier de certificat et enregistrer la clé publique dans le fichier indiqué.

  Les clés `-private-key` et `-cert` s'excluent mutuellement, c'est-à-dire, une seule clé peut être spécifiée ; si les deux clés sont spécifiées, la commande se termine avec une erreur.

  Il est obligatoire de spécifier le paramètre des clés.

  Si aucune clé n'est spécifiée, `-private-key=drwcsd.pri` sera utilisé pour extraire la clé publique de la clé privée `drwcsd.pri`.

Paramètre de la clé	Valeur par défaut
<*clé_privée*>	drwcsd.pri

- `drwsign genkey [`<*clé_privée*>` [`<*clé_publique*>`]]`

  Générer une paire de clés publique-privée et les enregistrer dans les fichiers appropriés.

Paramètre de la clé	Valeur par défaut
<*clé_privée*>	drwcsd.pri
<*clé_publique*>	drwcsd.pub

> La version de l'utilitaire pour les plateformes Windows (à la différence de la version pour UNIX) ne protège pas la clé privée contre la copie.

- `drwsign gencert [-private-key=`<*clé_privée*>`] [-subj=`<*champs_du_sujet*>`] [-days=`<*durée_de_validité*>`] [`<*certificat_auto-signé*>`]`

  Générer le certificat auto-signé en utilisant la clé privée du Serveur Dr.Web et l'enregistrer dans le fichier correspondant.

Paramètre de la clé	Valeur par défaut
<*clé_privée*>	drwcsd.pri
<*champs_du_sujet*>	/CN=<*nom_de_l'hôte*>
<*durée_de_validité*>	3560
<*certificat_auto-signé*>	drwcsd-certificate.pem

- `drwsign gencsr [-private-key=`<*clé_privée*>`] [-subj=`<*champs_du_sujet*>`] [`<*requête_de_signature_de_certificat*>`]`

  Générer une requête de signature de certificat à la base de la clé privée et enregistrer cette requête dans le fichier correspondant.

  Peut être utilisé pour signer le certificat d'un autre serveur, par exemple, pour signer le certificat du Serveur proxy Dr.Web par la clé du Serveur Dr.Web.

  Pour signer une telle requête, utilisez la clé `signcsr`.

Paramètre de la clé	Valeur par défaut
<*clé_privée*>	drwcsd.pri
<*champs_du_sujet*>	/CN=<*nom_de_l'hôte*>
<*requête_de_signature_de_certificat*>	drwcsd-certificate-sign-request.pem

- `drwsign genselfsign [-show] [-subj=<champs_du_sujet>] [-days=<durée_de_validité>] [<clé_privée> [<certificat_auto-signé>]]`

  Générer le certificat RSA auto-signé et la clé privée RSA pour le serveur web et l'enregistrer dans le fichier correspondant.

  La clé `-show` affiche le contenu du certificat au format accessible en lecture.

Paramètre de la clé	Valeur par défaut
<*champs_du_sujet*>	`/CN=`<*nom_de_l'hôte*>
<*durée_de_validité*>	`3560`
<*clé_privée*>	`private-key.pem`
<*certificat_auto-signé*>	`certificate.pem`

- `drwsign hash-check [-public-key=<clé_publique>] <fichier_de_hash> <fichier_de_la_signature>`

  Vérifier la signature du nombre 256 bits au format du protocole client-serveur.

  Dans le paramètre <*fichier_de_hash*>, un fichier contenant un nombre de 256 bits à signer est spécifié. Le fichier <*fichier_de_la_signature*> contient le résultat de la signature (deux nombres de 256 bits).

Paramètre de la clé	Valeur par défaut
<*clé_publique*>	`drwcsd.pub`

- `drwsign hash-sign [-private-key=<clé_privée>] <fichier_de_hash> <fichier_de_la_signature>`

  Signer le nombre 256 bits indiqué au format du protocole client-serveur.

  Dans le paramètre <*fichier_de_hash*>, un fichier contenant un nombre de 256 bits à signer est spécifié. Le fichier <*fichier_de_la_signature*> contient le résultat de la signature (deux nombres de 256 bits).

Paramètre de la clé	Valeur par défaut
<*clé_privée*>	`drwcsd.pri`

- `drwsign help [<commande>]`

  Afficher une brève aide sur le programme ou une commande particulière au format de la ligne de commande.

- `drwsign sign [-private-key=<clé_privée>] <fichier>`

  Signer le <*fichier*> en utilisant la clé privée.

Paramètre de la clé	Valeur par défaut
<*clé_privée*>	drwcsd.pri

- `drwsign signcert [-ca-key=`<*clé_privée*>`] [-ca-cert=`<*certificat_du_Serveur_Dr.Web*>`] [-cert=`<*certificat_à_signer*>`] [-days=`<*durée_de_validité*>`] [-eku=`<*objectif*>`] [`<*certificat_signé*>`]`

  Signer le <*certificat_à_signer*> prêt par la clé privée ou le certificat du Serveur Dr.Web. Le certificat signé est enregistré dans un fichier particulier.

  Peut être utilisé pour signer le certificat du Serveur proxy Dr.Web par la clé du Serveur.

  Les valeurs suivantes de la clé `-eku` (extension Extended Key Usage) sont autorisées :

  - `drwebServerAuth` : authentification du Serveur/Serveur proxy par l'Agent Dr.Web,
  - `drwebMeshDAuth` : authentification du Serveur de scan par l'Agent virtuel.

Paramètre de la clé	Valeur par défaut
<*clé_privée*>	drwcsd.pri
<*certificat_du_Serveur_Dr.Web*>	drwcsd-ca-cerificate.pem
<*certificat_à_signer*>	drwcsd-certificate.pem
<*durée_de_validité*>	3560
<*utilisation*>	drwebServerAuth
<*certificat_signé*>	drwcsd-signed-certificate.pem

- `drwsign signcsr [-ca-key=`<*clé_privée*>`] [-ca-cert=`<*certificat_du_Serveur_Dr.Web*>`] [-csr=`<*requête_de_signature_du_certificat*>`] [-days=`<*durée_de_validité*>`] [-eku=`<*objectif*>`] [`<*certificat_signé*>`]`

  Signer par la clé privée et le certificat du Serveur Dr.Web la <*requête_de_signature_de_certificat*> générée à l'aide de la commande `gencsr`. Le certificat signé est enregistré dans un fichier particulier.

  Peut être utilisé pour signer le certificat d'un autre serveur, par exemple, pour signer le certificat du Serveur proxy Dr.Web par la clé du Serveur Dr.Web.

  Les valeurs suivantes de la clé `-eku` (extension Extended Key Usage) sont autorisées :

  - `drwebServerAuth` : authentification du Serveur/Serveur proxy par l'Agent Dr.Web,
  - `drwebMeshDAuth` : authentification du Serveur de scan par l'Agent virtuel.

Paramètre de la clé	Valeur par défaut
<*clé_privée*>	drwcsd.pri
<*certificat_du_Serveur_Dr.Web*>	drwcsd-cerificate.pem

Paramètre de la clé	Valeur par défaut
<*requête_de_signature_de_certificat*>	`drwcsd-certificate-sign-request.pem`
<*durée_de_validité*>	`3560`
<*utilisation*>	`drwebServerAuth`
<*certificat_signé*>	`drwcsd-signed-certificate.pem`

- `drwsign tlsticketkey [`<*ticket TLS*>`]`

  Générer les tickets TLS.

  Peut être utilisé dans le cluster des Serveurs Dr.Web pour les sessions TLS communes.

Paramètre de la clé	Valeur par défaut
<*ticket_TLS*>	`tickets-key.bin`

- `drwsign verify [-ss-cert] [-CAfile=`<*certificat_du_Serveur_Dr.Web*>`] [`<*certificat_à_vérifier*>`]`

  Vérifier la validité du certificat par le certificat fiable du Serveur Dr.Web.

  La clé `-ss-cert` requiert que le certificat fiable soit ignoré et seule la validité du certificat auto-signé soit vérifiée.

Paramètre de la clé	Valeur par défaut
<*certificat_du_Serveur_Dr.Web*>	`drwcsd-certificate.pem`
<*certificat_à_vérifier*>	`drwcsd-signed-certificate.pem`

- `drwsign x509dump [`<*certificat_à_imprimer*>`]`

  Imprimer le dump de tout certificat x509.

Paramètre de la clé	Valeur par défaut
<*certificat_à_imprimer*>	`drwcsd-certificate.pem`

- `drwsign version`

  Afficher les informations sur la version de l'utilitaire.

G7.2. Utilitaire d'administration de la base de données embarquée

L'utilitaire `drwidbsh3` est fourni pour la gestion de la base de données embarquée (SQLite3).

L'utilitaire se trouve dans les dossiers suivants :

- sous **Linux** : `/opt/drwcs/bin`

- sous **FreeBSD** : `/usr/local/drwcs/bin`
- pour les OS **Windows**: *<répertoire_d'installation_du_Serveur_Dr.Web>*`\bin`

  (par défaut, le répertoire d'installation du Serveur Dr.Web : `C:\Program Files\DrWeb Server`).

Syntaxe de la commande de démarrage :

`drwidbsh3` *<nom_comple_du_fichier_de_la_BD>*

Le programme fonctionne en mode dialogué et attend de la part de l'utilisateur l'entrée des commandes (les commandes commencent avec le point).

Pour avoir de l'aide sur d'autres commandes, entrez `.help`.

Pour plus d'information, consulter la documentation sur le langage SQL.

G7.3. Utilitaire du diagnostic distant pour le Serveur Dr.Web

L'utilitaire du diagnostic distant du Serveur Dr.Web permet de se connecter au Serveur Dr.Web à distance pour la gestion de base et la consultation des statistiques de fonctionnement. La version graphique de l'utilitaire est disponible uniquement sous Windows.

L'utilitaire est disponible dans les versions suivantes :

- Pour les OS Windows — la version graphique.
- Pour les OS de la famille UNIX — la version de console.

Il existe les versions suivantes de l'utilitaire du diagnostic distant du Serveur Dr.Web :

Fichier exécutable	Localisation	Description
`drweb-cntl-`*<OS>*`-`*<nombre de bits>*	Centre de gestion, section **Administration** → **Utilitaires**	Version indépendante de l'utilitaire. Elle peut être lancée d'un répertoire aléatoire ou sur n'importe quel ordinateur ayant le système d'exploitation correspondant.
	Répertoire du Serveur Dr.Web `webmin/utilities`	
`drwcntl`	Répertoire du Serveur Dr.Web `bin`	La version de l'utilitaire dépend de la présence des bibliothèques de serveur. Elle peut être lancée uniquement du répertoire de son emplacement.

Les fonctions des versions de l'utilitaire `drweb-cntl-`*<OS>*`-`*<nombre de bits>* et `drwcntl` sont équivalentes. Vous trouverez ci-dessous la version `drwcntl`, pourtant toutes les exemples concernent les deux versions.

Pour la connexion de l'utilitaire du diagnostic distant du Serveur Dr.Web, il est nécessaire d'activer l'extension Dr.Web Server FrontDoor. Pour ce faire cochez la case **Extension Dr.Web Server FrontDoor** dans l'onglet **Modules** de la rubrique **Configuration du Serveur Dr.Web**.

Pour la connexion de l'utilitaire du diagnostic distant du Serveur Dr.Web, il faut que l'administrateur qui se connecte via l'utilitaire possède le droit **Utilisation des fonctionnalités supplémentaires**. Sinon, l'accès au Serveur Dr.Web via l'utilitaire du diagnostic distant sera interdit.

Pour connecter l'utilitaire (graphique ou console) via TLS, il faut spécifier le protocole lors de l'indication de l'adresse du Serveur Dr.Web : `ssl://`<*adresse IP ou nom DNS*>.

Vous pouvez consulter la description des paramètres du Serveur Dr.Web pour la connexion de l'utilitaire du diagnostic distant du Serveur Dr.Web dans le **Manuel Administrateur**, p. Accès distant au Serveur Dr.Web.

Version console de l'utilitaire

Syntaxe de la commande de démarrage :

`drwcntl [-?|-h|--help] [+`<*fichier_de_journal*>`] [`<*serveur*>` [`<*login*>` [`<*mot_de_passe*>`]]]`

où :

- `-? -h --help` : afficher l'aide sur les commandes d'utilisation de l'utilitaire.
- <*fichier_journal*> : enregistrer toutes les actions de l'utilitaire dans le fichier journal par le chemin spécifié.
- <*serveur*> : ligne d'adresse du Serveur Dr.Web, auquel se connecte l'utilitaire au format `[(tcp|ssl)://]`<*adresse IP ou nom DNS*>`[:`<*port*>`]`.

  Pour pouvoir se connecter à un des protocoles supportés, il faut satisfaire aux conditions suivantes :

  a) Pour la connexion via `ssl`, la balise `<ssl />` doit être présente dans le fichier de configuration `frontdoor.conf`. Dans ce cas, la connexion est possible uniquement via `ssl`.

  b) Pour la connexion via `tcp`, la balise `<ssl />` doit être désactivée (commentée) dans le fichier de configuration `frontdoor.conf`. Dans ce cas, la connexion est possible uniquement via `tcp`.

  Si les paramètres de connexion ne sont pas spécifiés dans la ligne d'adresse du Serveur Dr.Web, les valeurs suivantes seront utilisées :

Paramètre	Valeur par défaut
Protocole de connexion	`tcp` ⚠ Pour la connexion via TCP, la case **Utiliser TLS** dans le Centre de gestion, dans la section **Administration** → **Accès distant au Serveur Dr.Web** doit être décochée. Cela désactive la balise `<ssl />` dans le fichier de configuration `frontdoor.conf`.
Adresse IP ou nom DNS du Serveur Dr.Web	L'utilitaire va demander entrer l'adresse du Serveur Dr.Web au format correspondant.
Port	`10101` ⚠ Du côté du Serveur Dr.Web, le port autorisé est spécifié dans la rubrique **Accès distant au Serveur Dr.Web** et sauvegardé dans le fichier de configuration `frontdoor.conf`. Au cas d'utilisation du port alternatif dans cette rubrique, il est nécessaire de spécifier clairement ce port en cas de connexion de l'utilitaire.

- <*login*> : login de l'administrateur du Serveur Dr.Web.
- <*mot_de_passe*> : mot de passe de l'administrateur pour accéder au Serveur Dr.Web.

  Si le login et le mot de passe de l'administrateur n'ont pas été spécifiés dans la ligne de connexion, l'utilitaire va demander d'entrer les identifiants correspondants.

Commandes possibles :

- `cache` <*opération*> : gestion du cache de fichiers. Pour effectuer une opération concrète, utilisez les commandes suivantes :
  - `clear` : nettoyer le cache de fichiers,
  - `list` : afficher le contenu du cache de fichiers,
  - `matched` <*expression régulière*> : afficher le contenu du cache de fichiers qui satisfait à l'expression régulière spécifiée,
  - `maxfilesize [`<*taille*>`]` : afficher/specifier la taille maximum des objets de fichiers préchargés. Lors du lancement des paramètres supplémentaires, la taille actuelle s'affiche. Pour spécifier la taille, indiquez la taille nécessaire en octets après le nom de la commande.
  - `statistics` : afficher les statistiques d'utilisation du cache de fichiers.
- `calculate` <*fonction*> : calcul de l'ordre spécifié. Pour spécifier l'ordre précis, utilisez les commandes suivantes :
  - `hash [`<*norme*>`] [`<*ligne*>`]` : calcul du hash de la chaîne donnée. Pour spécifier une norme précise, utilisez les commandes suivantes :
    - `gost` : calcul du hash de la chaîne donnée selon la norme GOST,

- `md5` : calcul du hash MD5 de la chaîne donnée,
- `sha` : calcul du hash de la chaîne donnée selon la norme SHA,
- `sha1` : calcul du hash de la chaîne donnée selon la norme SHA1,
- `sha224` : calcul du hash de la chaîne donnée selon la norme SHA224,
- `sha256` : calcul du hash de la chaîne donnée selon la norme SHA256,
- `sha384` : calcul du hash de la chaîne donnée selon la norme SHA384,
- `sha512.` : calcul du hash de la chaîne donnée selon la norme SHA512.

▫ `hmac [<`*norme*`>] [<`*ligne*`>]` : calcul du hmac de la chaîne donnée. Pour spécifier une norme précise, utilisez les commandes suivantes :

- `md5` : calcul du HMAC-MD5 pour la chaîne donnée,
- `sha256` : calcul du HMAC-SHA256 pour la chaîne donnée.

▫ `random` : génération d'un nombre aléatoire,

▫ `uuid` : génération d'un identificateur unique aléatoire.

- `clients` <*opération*> : obtention des informations et gestion des clients connectés au Serveur Dr.Web. Pour une fonction concrète, utilisez les commandes suivantes :

▫ `addresses [<`*expression régulière*`>]` : afficher les adresses réseau des postes correspondant à l'expression régulière spécifiée. Si l'expression régulière n'est pas spécifiée — afficher les adresses de tous les postes.

▫ `caddresses [<`*expression régulière*`>]` : afficher le nombre des adresses IP des postes correspondant à l'expression régulière spécifiée. Si l'expression régulière n'est pas spécifiée – afficher le nombre de tous les postes.

▫ `chosts [<`*expression régulière*`>]` : afficher le nombre des noms des postes correspondant à l'expression régulière spécifiée. Si l'expression régulière n'est pas spécifiée — afficher le nombre de tous les postes.

▫ `cids [<`*expression régulière*`>]` : afficher le nombre des identificateurs des postes correspondant à l'expression régulière spécifiée. Si l'expression régulière n'est pas spécifiée — afficher le nombre de tous les postes.

▫ `cnames [<`*expression régulière*`>]` : afficher le nombre des noms des postes correspondant à l'expression régulière spécifiée. Si l'expression régulière n'est pas spécifiée — afficher le nombre de tous les postes.

▫ `disconnect [<`*expression régulière*`>]` : interrompre la connexion avec les postes, dont les identificateurs correspondent à l'expression régulière spécifiée. Si l'expression régulière n'est pas spécifiée — interrompre la connexion avec tous les postes.

▫ `enable [<`*mode*`>]` : afficher/spécifier le mode de connexion des clients au Serveur Dr.Web. En cas de lancement sans les paramètres supplémentaires, le mode actuel est affiché. Pour spécifier le mode de lancement, utilisez les commandes suivantes :

- `on` : accepter toutes les connexions des clients.
- `off` : refuser les connexions à tous les clients.

- `hosts` *[<expression régulière>]* : afficher les noms des postes correspondant à l'expression régulière spécifiée.
- `ids` *[<expression régulière>]* : afficher les identificateurs des postes correspondant à l'expression régulière spécifiée.
- `names` *[<expression régulière>]* : afficher les noms des postes correspondant à l'expression régulière spécifiée.
- `online` <*expression régulière*> : afficher la durée de connexion des postes dont l'identificateur, le nom ou l'adresse correspondent à l'expression régulière spécifiée. La durée de connexion est compté du moment de la dernière connexion du poste au Serveur Dr.Web.
- `statistics` *[<expression régulière>]* : afficher les statistiques par le nombre de clients correspondant à l'expression régulière spécifiée.
- `traffic` *[<expression régulière>]* : afficher les données du trafic des clients connectés en ce moment, correspondant à l'expression régulière spécifiée.

- `core` : enregistrer le dump du processus du Serveur Dr.Web.
- `cpu` <*paramètre*> : afficher les statistiques d'utilisation de CPU de l'ordinateur sur lequel le Serveur Dr.Web est installé. Pour consulter un paramètre concret, utilisez les commandes suivantes :
  - `clear` : supprimer toutes les données statistiques accumulées,
  - `day` : afficher le graphique de la charge de CPU pour le jour actuel,
  - `disable` : désactiver la surveillance de la charge de CPU,
  - `enable` : activer la surveillance de la charge de CPU,
  - `hour` : afficher le graphique de la charge de CPU pour l'heure actuelle,
  - `load` : afficher le niveau moyen de la charge de CPU,
  - `minute` : afficher le graphique de la charge de CPU pour la dernière minute,
  - `rawd` : afficher les statistiques numériques de la charge de CPU pour le jour,
  - `rawh` : afficher les statistiques numériques de la charge de CPU pour la dernière heure,
  - `rawl` : afficher les statistiques numériques de la charge moyenne de CPU,
  - `rawm` : afficher les statistiques numériques de la charge de CPU pour la dernière minute,
  - `status` : afficher le statut de surveillance des statistiques de la charge de CPU.
- `debug` <*paramètre*> : configuration de débogage. Pour spécifier le paramètre concret, utilisez les commandes supplémentaires. Pour préciser la liste de commandes supplémentaires, vous pouvez afficher l'aide avec la commande : `? debug`.

  

  La commande `debug signal` est disponible uniquement pour les Serveurs Dr.Web sous les OS de la famille UNIX.

- `die` : arrêter le Serveur Dr.Web et enregistrer le dump du processus du Serveur Dr.Web.

La commande `die` est disponible uniquement pour les Serveurs Dr.Web sous les OS de la famille UNIX.

- `dwcp` <*paramètre*> : spécifier/consulter les paramètres de Dr.Web Control Protocol (inclut les journaux du Serveur Dr.Web, des Agents Dr.Web et des installateurs des Agents Dr.Web). Paramètres autorisés :
  - `compression` <*mode*> : spécifier un des modes de compression suivants :
    - `on` : compression activée,
    - `off` : compression désactivée,
    - `possible` : la compression est possible.
  - `encryption` <*mode*> : spécifier un des modes de chiffrement suivants :
    - `on` : chiffrement activé,
    - `off` : chiffrement désactivé,
    - `possible` : le chiffrement est possible.
  - `show` : afficher les paramètres actuels de Dr.Web Control Protocol.
- `io` <*paramètre*> : afficher les statistiques de la lecture/enregistrement des données par le processus du Serveur Dr.Web. Pour consulter un paramètre concret, utilisez les commandes suivantes :
  - `clear` : supprimer toutes les données statistiques accumulées,
  - `disable` : désactiver la détection des statistiques,
  - `enable` : activer la détection des statistiques,
  - `rawdr` : afficher les statistiques numérique de la lecture de données pour le jour,
  - `rawdw` : afficher les statistiques numérique de la lecture de données pour le jour,
  - `rawh` : afficher les statistiques numériques pour la dernière heure,
  - `rawm` : afficher les statistiques numériques pour la dernière minute,
  - `rday` : afficher le graphique des statistiques de la lecture de données pour le jour,
  - `rhour` : afficher le graphique des statistiques de la lecture de données pour la dernière heure,
  - `rminute` : afficher le graphique des statistiques de la lecture de données pour la dernière minute,
  - `status` : afficher le statut de surveillance des statistiques,
  - `wday` : afficher le graphique des statistiques de l'enregistrement de données pour le jour,
  - `whour` : afficher le graphique des statistiques de l'enregistrement de données pour la dernière heure,
  - `wminute` : afficher le graphique des statistiques de l'écriture de données pour la dernière minute.

- `log` <*paramètre*> : enregistrer la chaîne donnée dans le fichier journal du Serveur Dr.Web ou spécifier/consulter le niveau de détail du journal. Les actions suivantes sont effectuées en fonction des paramètres spécifiés :
  - `log` <*chaîne*> : enregistrer dans le journal du Serveur Dr.Web la chaîne donnée avec le niveau de détail `NOTICE`.
  - `log \s [`<*niveau*>`]` : spécifier/consulter le niveau de détail du journal. En cas de lancement avec la clé `\s` sans indication du niveau de détail, le niveau actuel de détail est affiché. Les valeurs autorisées du niveau de détail sont : `ALL`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `DEBUG`, `TRACE3`, `TRACE2`, `TRACE1`, `TRACE`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `CRIT`.
- `lua` <*script*> : exécuter le script LUA spécifié.
- `mallopt` <*paramètre*> : configuration de répartition de la mémoire. Pour spécifier le paramètre concret, utilisez les commandes supplémentaires. Pour préciser la liste de commandes supplémentaires, vous pouvez afficher l'aide avec la commande : `? mallopt`.

  La commande `mallopt` est disponible uniquement pour les Serveurs Dr.Web sous les OS de la famille Linux.

  Pour plus d'information sur les particularités des paramètres de cette commande, consultes la description de la fonction `mallopt()` de la bibliothèque `glibc`. Pour afficher l'aide sur cette fonction, utilisez par exemple la commande `man mallopt`.
- `memory` <*paramètre*> : afficher les statistiques d'utilisation de la mémoire de l'ordinateur sur lequel le Serveur Dr.Web est installé. Pour consulter un paramètre concret, utilisez les commandes suivantes :
  - `all` : afficher toutes les informations et les statistiques,
  - `heap` : afficher les informations sur la mémoire dynamique,
  - `malloc` : afficher les statistiques sur le placement de la mémoire,
  - `sizes` : afficher les statistiques sur la taille de la mémoire placée,
  - `system` : afficher les informations sur la mémoire systeme.

  La commande `memory` est disponible uniquement pour les Serveurs Dr.Web sous Windows, sous les OS de la famille Linux et de la famille FreeBSD. Dans ce cas, s'appliquent les limitations suivantes des paramètres supplémentaires de la commande `memory` :
  - `system` : uniquement pour les Serveurs Dr.Web sous Windows, sous les OS de la famille Linux,
  - `heap` : uniquement pour les Serveurs Dr.Web sous Windows, sous les OS de la famille Linux,
  - `malloc` : uniquement pour les Serveurs Dr.Web sous les OS de la famille Linux et de la famille FreeBSD,
  - `sizes` : uniquement pour les Serveurs Dr.Web sous les OS de la famille Linux et de la famille FreeBSD.

- `monitoring` <*mode*> : spécifier/consulter le mode de surveillance d'utilisation des ressources CPU (clé `cpu` <*paramètre*>) et d'entrée/sortie (clé `io` <*paramètre*>) par le processus du Serveur Dr.Web. Les commandes autorisées sont :
  - `disable` : désactiver la surveillance,
  - `enable` : activer la surveillance,
  - `show` : afficher le mode actuel.
- `printstat` : écrire les statistiques de fonctionnement du Serveur Dr.Web dans le journal.
- `reload` : redémarrer l'extension Dr.Web Server FrontDoor.
- `repository` <*paramètre*> : gestion du référentiel. Pur une fonction concrète, utilisez les commandes suivantes :
  - `all` : afficher la liste de tous les produits du référentiel et le nombre des fichiers par produit,
  - `clear` : effacer le contenu du cache, indépendamment de la valeur TTL des objets placés en cache,
  - `fill` : placer tous les fichiers du référentiel en cache,
  - `keep` : sauvegarder tous les fichiers du référentiel stockés en ce moment dans le cache, toujours, indépendamment de leur valeur TTL,
  - `loaded` : afficher la liste de tous les produits du référentiel et le nombre des fichiers par produits, stockés en ce moment dans le cache,
  - `reload` : recharger le référentiel depuis le disque,
  - `statistics` : afficher les statistiques d'utilisation du référentiel.
- `restart` : redémarrer le Serveur Dr.Web.
- `show` <*paramètre*> : afficher les informations sur le système sur lequel le Serveur Dr.Web est installé. Pour spécifier le paramètre concret, utilisez les commandes supplémentaires. Pour préciser la liste de commandes supplémentaires, vous pouvez afficher l'aide avec la commande : `? show`.

  

  Les limitations suivantes s'appliquent aux paramètres supplémentaires de la commande `show` :
  - `memory` : uniquement pour les Serveurs Dr.Web sous Windows, sous les OS de la famille Linux,
  - `mapping` : uniquement pour les Serveurs Dr.Web sous Windows, sous les OS de la famille Linux,
  - `limits` : uniquement pour les Serveurs Dr.Web sous les OS de la famille UNIX,
  - `processors` : uniquement pour les Serveurs Dr.Web sous les OS de la famille Linux.
- `sql` <*requête*> : exécuter la requête SQL spécifiée.
- `stop` : arrêter le Serveur Dr.Web.
- `traffic` <*paramètre*> : afficher les statistiques du trafic réseau du Serveur Dr.Web. Pour consulter un paramètre concret, utilisez les commandes suivantes :

- `all` : afficher tout le volume du trafic à compter du début du fonctionnement du Serveur Dr.Web.
- `incremental` : afficher l'accroissement du trafic depuis le dernier lancement de la commande `traffic incremental`.
- `last` : afficher le changement du trafic depuis le dernier point fixe.
- `store` : création d'un point fixe pour la clé `last`.

- `update` <*paramètre*> : obtention des informations et gestion des mises à jour. Pour une fonction concrète, utilisez les clés suivantes :
  - `active` : afficher la liste des Agents Dr.Web qui sont en train d'effectuer la mise à jour.
  - `agent [`<*mode*>`]` : afficher/spécifier le mode de mise à jour des Agents Dr.Web depuis le Serveur Dr.Web. En cas de lancement sans les paramètres supplémentaires, le mode actuel est affiché. Pour spécifier le mode de lancement, utilisez les clés suivantes :
    - `on` : activer les mises à jour des Agents Dr.Web.
    - `off` : désactiver les mises à jour des Agents Dr.Web.
  - `gus` : lancer la mise à jour du référentiel depuis le SGM indépendamment du statut de la mise à jour depuis le SGM.
  - `http [`<*mode*>`]` : afficher/spécifier le mode de mise à jour du référentiel du Serveur Dr.Web depuis le SGM. En cas de lancement sans paramètres supplémentaires, le mode actuel est affiché. Pour spécifier le mode de lancement, utilisez les clés supplémentaires suivantes :
    - `on` : activer des mises à jour du référentiel depuis le SGM.
    - `off` : désactiver des mises à jour du référentiel depuis le SGM.
  - `inactive` : afficher la liste des Agents Dr.Web qui ne sont pas en train d'effectuer la mise à jour.
  - `track [`<*mode*>`]` : afficher/spécifier le mode du suivi des mises à jour des Agents Dr.Web au Serveur. En cas de lancement sans paramètres supplémentaires, le mode actuel est affiché. Pour spécifier le mode, utilisez les commandes supplémentaires suivantes :
    - `on` : activer le suivi des mises à jour des Agents Dr.Web.
    - `off` : désactiver le suivi des mises à jour des Agents Dr.Web. Dans ce cas la clé `update active` ne va pas afficher la liste des Agents Dr.Web mis à jour.
- `version` : afficher les informations sur la version de l'utilitaire.

G7.4. Utilitaire du diagnostic distant du Serveur Dr.Web pour la gestion des scripts

L'utilitaire du diagnostic distant du Serveur Dr.Web permet de se connecter au Serveur Dr.Web à distance pour la gestion de base et la consultation des statistiques de fonctionnement. A la différence de drwcntl, l'utilitaire `drwcmd` peut être utilisé lors de la gestion de scripts.

Il existe les versions suivantes de l'utilitaire de console du diagnostic distant du Serveur Dr.Web pour la gestion des scripts :

Fichier exécutable	Localisation	Description
`drweb-cmd-<OS>-<nombre de bits>`	Centre de gestion, section **Administration** → **Utilitaires**	Version indépendante de l'utilitaire. Elle peut être lancée d'un répertoire aléatoire ou sur n'importe quel ordinateur ayant le système d'exploitation correspondant.
	Répertoire du Serveur Dr.Web `webmin/utilities`	
`drwcmd`	Répertoire du Serveur Dr.Web `bin`	La version de l'utilitaire dépend de la présence des bibliothèques de serveur. Elle peut être lancée uniquement du répertoire de son emplacement.

Les fonctions des versions de l'utilitaire `drweb-cmd-<OS>-<nombre de bits>` et `drwcmd` sont équivalentes. Vous trouverez ci-dessous la version `drwcmd`, pourtant toutes les exemples concernent les deux versions.

Pour la connexion de l'utilitaire du diagnostic distant du Serveur Dr.Web, il est nécessaire d'activer l'extension Dr.Web Server FrontDoor. Pour ce faire cochez la case **Extension Dr.Web Server FrontDoor** dans l'onglet **Modules** de la rubrique **Configuration du Serveur Dr.Web**.

Pour la connexion de l'utilitaire du diagnostic distant du Serveur Dr.Web, il faut que l'administrateur qui se connecte via l'utilitaire possède le droit **Utilisation des fonctionnalités supplémentaires**. Sinon, l'accès au Serveur Dr.Web via l'utilitaire du diagnostic distant sera interdit.

Vous pouvez consulter la description des paramètres du Serveur Dr.Web pour la connexion de l'utilitaire du diagnostic distant du Serveur Dr.Web dans le **Manuel Administrateur**, p. Accès distant au Serveur Dr.Web.

Syntaxe de la commande de démarrage :

`drwcmd [<clés>] [<fichiers>]`

Clés possibles

Le principe d'utilisation des clés par l'utilitaire `drwcmd` est soumis aux règles communes décrites dans la rubrique Annexe G. Paramètres de la ligne de commande relatifs aux programmes inclus dans Dr.Web Enterprise Security Suite.

- `--?` : afficher l'aide sur les clés.
- `--help` : afficher l'aide sur les clés.
- `--commands=<`*commandes*`>` : exécuter les commandes spécifiées (elles sont équivalentes aux commandes de l'utilitaire drwcntl). Vous pouvez spécifier plusieurs commandes en les séparant par le symbole `;`.
- `--debug=yes|no` : journaliser le fonctionnement de l'utilitaire en mode de débogage (sortie standard `stderr`). Par défaut, c'est `no`.
- `--files=yes|no` : autoriser l'exécution des commandes (elles sont équivalentes aux commandes de l'utilitaire drwcntl) depuis les fichiers spécifiés. Par défaut, c'est `yes`.

  Quand vous spécifiez des commandes dans le fichier, notez qu'une ligne doit contenir une seule commande. Les lignes vides sont ignorées. Vous pouvez utiliser le caractère `#` n tant que début du commentaire.
- `--keep=yes|no` : maintenir la connexion au Serveur Dr.Web après l'exécution de la dernière commande jusqu'à la fin du processus de l'utilitaire. Par défaut, c'est `no`.
- `--output=<`*fichier*`>` : fichier de sortie des réponses du Serveur Dr.Web. Par défaut, si le fichier n'est pas indiqué, la sortie standard `stdout` est utilisée.

  Si le nom du fichier commence par le symbole (+), le résultat de l'exécution des commandes sera ajouté à la fin du fichier. Si ce n'est pas le cas, le fichier sera réenregistré.
- `--password=<`*mot de passe*`>` : mot de passe pour l'authentification sur le Serveur Dr.Web. Il peut être déterminé dans le fichier spécifié dans la clé `--resource`.
- `--read=yes|no` : autoriser la lecture des paramètres de connexion au Serveur Dr.Web depuis le fichier de ressources. Par défaut, c'est `yes`.
- `--resource=<`*fichier*`>` : fichier de ressources contenant les paramètres de connexion au Serveur Dr.Web : l'adresse du Serveur Dr.Web et les données d'enregistrement de l'administrateur pour l'authentification sur le Serveur Dr.Web. Par défaut, c'est le fichier `.drwcmdrc` situé dans le répertoire suivant qui est utilisé :
  - Pour les OS de la famille UNIX : `$HOME`
  - Pour les OS Windows : `%LOCALAPPDATA%`

  Chaque ligne doit être composée de 3 mots séparés d'un espace : *<Serveur_Dr.Web> <utilisateur> <mot de passe>*.

  S'il faut utiliser un espace au milieu d'un mot, il est spécifié comme `%S`. S'il faut utiliser le signe pourcentage, il est spécifié comme `%P`.

  Exemple :

```
ssl://127.0.0.1 user1 password1

ssl://127.0.0.1 user2 password2

ssl://127.0.0.1 user pass%Sword
```

Si vous utilisez la clé `--resource`, il faut également indiquer la clé `--server`. La connexion se fait au Serveur Dr.Web indiqué dans la clé `--server` selon les données du fichier de ressource correspondant à l'adresse de ce Serveur Dr.Web.

- `--server=<`*Serveur_Dr.Web*`>` : adresse du Serveur Dr.Web. Par défaut, c'est `ssl://127.0.0.1`. Elle peut être déterminée dans le fichier spécifié dans la clé `--resource`.
- `--user=<`*utilisateur*`>` : nom de l'utilisateur utilisé pour l'authentification sur le Serveur Dr.Web. Il peut être déterminé dans le fichier spécifié dans la clé `--resource`.
- `--verbose=yes|no` : afficher la réponse détaillée du Serveur Dr.Web (sortie standard `stdout`). Par défaut, c'est `no`.
- `--version` : afficher les informations sur la version de l'utilitaire.

Procédure de connexion au Serveur Dr.Web :

1. Lors de la détermination des données de connexion au Serveur Dr.Web, les valeurs spécifiées dans les clés `--server`, `--user` et `--password` sont prioritaires.
2. Si la clé `--server` n'est pas spécifiée, sa valeur par défaut `ssl://127.0.0.1` est utilisée.
3. Si la clé `--user` n'est pas spécifiée, le Serveur Dr.Web nécessaire est recherché dans le fichier `.drwcmdrc` (il peut être redéfini dans la clé `--resource`) et le premier nom d'utilisateur par l'ordre alphabétique est utilisé.
4. Si la clé `--password` n'est pas spécifiée, la recherche par le Serveur Dr.Web et le nom d'utilisateur est effectuée dans le fichier `.drwcmdrc` (il peut être redéfini dans la clé `--resource`).

   

   Le nom d'utilisateur et le mot de passe seront lus dans le fichier `.drwcmdrc` (il peut être redéfini dans la clé `--resource`) si cela n'est pas interdit par la clé `--read`.

5. Si le nom d'utilisateur et le mot de passe ne sont pas spécifiés à l'aide des clés ou via le fichier de ressource, l'utilitaire demandera de saisir les identifiants via la console.

Particularités d'exécution des commandes :

- Si la valeur vide (–) est spécifiée en tant que fichiers de commandes, les commandes entrées via la console seront lues.
- Si les commandes dans la clé `--commands` et la liste de fichiers sont spécifiées en même temps, les commandes spécifiées dans la clé `--commands` sont exécutées les premières.
- Si aucun fichier ni commande n'est spécifié dans la clé `--commands`, les commandes entrées via la console sont lues.

Exemple :

Pour exécuter les commandes de la clé `--command` et, ensuite, les commandes de la console, entrez le suivant :

```
drwcmd --commands=<commandes> -- -
```

Codes de fin de fonctionnement

- 0 : exécution réussie.
- 1 : l'aide sur les clés : `--help` ou `--?` est demandée.
- 2 : erreur d'analyse de la ligne de commande : les paramètres d'authentification ne sont pas spécifiés, etc.
- 3 : erreur de création du fichier pour la sortie de la réponse du Serveur Dr.Web.
- 4 : erreur d'authentification sur le Serveur Dr.Web : nom et/ou mot de passe de l'administrateur incorrect.
- 5 : interruption d'urgence de la connexion au Serveur Dr.Web.
- 127 : erreur fatale non déterminée.

G7.5. Chargeur du référentiel Dr.Web

Vous pouvez trouver la description de la version graphique de l'utilitaire du Chargeur du référentiel dans le **Manuel Administrateur**, dans la rubrique Utilitaire graphique.

Il existe les versions suivantes de l'utilitaire de console Chargeur du référentiel Dr.Web :

Fichier exécutable	Localisation	Description
`drweb-reploader-<OS>-<nombre de bits>`	Centre de gestion, section **Administration → Utilitaires**	Version indépendante de l'utilitaire. Elle peut être lancée d'un répertoire aléatoire ou sur n'importe quel ordinateur ayant le système d'exploitation correspondant.
	Répertoire du Serveur Dr.Web `webmin/utilities`	
`drwreploader`	Répertoire du Serveur Dr.Web `bin`	La version de l'utilitaire dépend de la présence des bibliothèques de serveur. Elle peut être lancée uniquement du répertoire de son emplacement.

Les fonctions des versions de l'utilitaire `drweb-reploader-<OS>-<nombre de bits>` et `drwreploader` sont équivalentes. Vous trouverez ci-dessous la version `drwreploader`, pourtant toutes les exemples concernent les deux versions.

Pour faciliter la spécification des clés pour le lancement de l'utilitaire de console, vous pouvez utiliser le fichier de configuration du Chargeur du référentiel. Dans le fichier de configuration prédéfini, les valeurs des clés correspondent aux valeurs par défaut spécifiées ci-dessous, sauf la clé `--ssh-auth`. Dans le fichier de configuration, la valeur de cette clé est modifiée en `pubkey`.

Clés possibles

- `--archive` : archiver le référentiel. Par défaut, c'est : `no`.
- `--auth` <*argument*> : identifiants pour l'authentification sur le serveur de mises à jour au format <*utilisateur*>`[:`<*mot_de_passe*>`]`.
- `--cert-file` <*chemin*> : chemin vers le dépôt de sauvegarde des certificats racines utilisés pour l'authentification SSL.
- `--cert-mode [`<*argument*>`]` : type des certificats SSL qui seront appliqués automatiquement. Ce paramètre est utilisé uniquement pour les protocoles sécurisés supportant le chiffrement.

  <*argument*> peut prendre une des valeurs suivantes :

  - `any` : accepter tous les certificats,
  - `valid` : accepter uniquement les certificats fiables,
  - `drweb` : accepter uniquement les certificats de Dr.Web,
  - `custom` : accepter les certificats utilisateurs.

  La valeur `drweb` est utilisée par défaut.
- `--config` <*chemin*> : chemin vers le fichier de configuration du Chargeur du référentiel.
- `--cwd` <*chemin*> : chemin vers le répertoire actuel.
- `--ipc` : inclure le transfert des données sur le fonctionnement de l'utilitaire dans le flux de sortie standard. Par défaut : `no`.
- `--help` : afficher l'aide sur les clés.
- `--license-key` <*chemin*> : chemin vers le fichier clé de licence (le fichier clé ou son hash MD5 doivent être indiqués).
- `--log` <*chemin*> : chemin vers le fichier journal de téléchargement du référentiel.
- `--mode` <*mode*> : mode de téléchargement des mises à jour :
  - `repo` : le référentiel est téléchargé sous forme du référentiel du Serveur Dr.Web. Les fichiers téléchargés peuvent être importés via le Centre de gestion en tant que la mise à jour du référentiel du Serveur Dr.Web. Utilisé par défaut.
  - `mirror` : le référentiel est téléchargé sous forme de la zone des mises à jour du SGM. Les fichiers téléchargés peuvent être placés en miroir de mises à jour dans votre réseau local. Ensuite, les Serveurs Dr.Web peuvent être configurés pour recevoir des mises à jours directement depuis ce miroir de mise à jour contenant la dernière version du référentiel et non pas depuis les serveurs du SGM.
- `--only-bases` : télécharger uniquement les bases virales. Par défaut c'est `no`.

- `--path` <*argument*> : télécharger le référentiel du SGM dans le répertoire indiqué dans le paramètre <*argument*>. Lors de l'archivage avec la clé `--archive`, vous pouvez indiquer le chemin jusqu'au nom du répertoire ou nom du fichier de l'archive. Si le nom de l'archive n'est pas indiqué, le nom par défaut `repository.zip` sera utilisé.
- `--product` <*argument*> : produit mis à jour. Par défaut, le référentiel en entier est téléchargé.
- `--prohibit-cdn` : interdire l'utilisation de CDN lors de téléchargement des mises à jour. `no` par défaut, c'est-à-dire l'utilisation de CDN est autorisée.
- `--proto` <*protocole*> : protocole de téléchargement des mises à jour : `file | ftp | ftps | http | https | scp | sftp | smb | smbs`. Par défaut: `https`.
- `--proxy-auth` <*argument*> : données d'authentification sur le serveur proxy : login et mot de passe utilisateur au format suivant : <*login*>`[:`<*mot de passe*>`]`.
- `--proxy-host` <*argument*> : adresse du serveur proxy indiquée au format suivant : <*serveur*>`[:`<*port*>`]`. Port par défaut : `3128`.
- `--rotate` <*N*><*f*>`,`<*M*><*u*> : mode de rotation du journal du Chargeur du référentiel. Équivalent à la configuration de la rotation du journal du Serveur Dr.Web.

  Les valeurs par défaut sont `10,10m`, ce qui enjoint de sauvegarder 10 fichiers, de 10 Mo chacun, et d'utiliser la compression.
- `--servers` <*argument*> : adresses des serveurs du SGM. Il est recommandé de garder la valeur par défaut : `esuite.geo.drweb.com`.
- `--show-products` : afficher la liste des produits du SGM. Par défaut, c'est `no`.
- `--ssh-auth` <*type*> : type d'authentification sur le serveur de mises à jour en cas d'appel via SCP/SFTP. Une des valeurs suivantes peut être utilisée en tant que paramètre *type* :
  - `pwd` : authentification avec un mot de passe. Le mot de passe est spécifié dans la clé `--auth`.
  - `pubkey` : authentification avec une clé publique. Dans ce cas, il faut spécifier la clé privée via `--ssh-prikey` pour extraire la clé publique correspondante.
- `--ssh-prikey` <*chemin*> : chemin vers la clé privée SSH.
- `--ssh-pubkey` <*chemin*> : chemin vers la clé publique SSH.
- `--strict` : arrêter le chargement en cas d'erreur. Par défaut, c'est `no`.
- `--update-key` <*chemin*> : chemin vers la clé publique ou le répertoire contenant la clé publique utilisée pour la vérification de la signature des mises à jour téléchargées depuis le SGM. Vous pouvez trouver les clés publiques utilisées pour la vérification de l'authenticité des mises à jour `update-key-*.upub` sur le Serveur Dr.Web, dans le répertoire `etc`.
- `--update-url` <*argument*> : répertoire se trouvant sur les serveurs du SGM contenant les mises à jour des produits Dr.Web. Il est recommandé de garder la valeur par défaut : `/update`.
- `--V` : afficher les informations sur la version de l'utilitaire.
- `--verbosity` <*niveau_de_détails*> : niveau de détails du journal. Par défaut, `TRACE3`. Les valeurs autorisées sont : `ALL, DEBUG3, DEBUG2, DEBUG1, DEBUG, TRACE3, TRACE2, TRACE1, TRACE, INFO, NOTICE, WARNING, ERROR, CRIT`. Les valeurs `ALL` et `DEBUG3` sont identiques.

- `--version <version>` : version du Serveur Dr.Web qui nécessite des mises à jour au format <*version_majeure*>.<*version_mineure*>. Par exemple, pour le Serveur Dr.Web en version 13, le paramètre <*version*> prend la valeur `13.00`. L'ensemble des produits à mettre à jour peut varier en fonction de la version du Serveur Dr.Web. Vous pouvez préciser l'ensemble des produits disponibles en vérifiant la description du paramètre `<products>` du fichier de configuration du Chargeur de référentiel dans le manuel de la version en question.

Particularités de l'utilisation des clés

En cas du lancement de l'utilitaire Chargeur de référentiel, notez les règles suivantes :

Les clés doivent être obligatoirement spécifiées	A condition
`--license-key`	Toujours
`--update-key`	
`--path`	
`--cert-file`	Si les clés suivantes prennent une des valeurs : • `--cert-mode valid | drweb | custom`, • `--proto https | ftps | smbs`.
`--ssh-prikey`	Si les clés suivantes prennent une des valeurs : • `--proto sftp | scp`, • `--ssh-auth pubkey`.

Exemples d'utilisation

1. Pour créer une archive importée contenant tous les produits :

```
drwreploader.exe --path C:\Temp --archive --license-key C:\agent.key --
update-key "C:\Program Files\DrWeb Server\etc" --cert-file "C:\Program
Files\DrWeb Server\etc"
```

2. Pour créer une archive importée contenant les bases virales :

```
drwreploader.exe --path C:\Temp --archive --license-key "C:\agent.key" --
update-key "C:\Program Files\DrWeb Server\etc" --cert-file "C:\Program
Files\DrWeb Server\etc" -only-bases
```

3. Pour créer une archive importée contenant le Serveur Dr.Web seul :

```
drwreploader.exe --path C:\Temp --archive --license-key "C:\agent.key" --
update-key "C:\Program Files\DrWeb Server\etc" --cert-file "C:\Program
Files\DrWeb Server\etc" --product=20-drwcs
```

G7.6. Utilitaire d'installation à distance de l'Agent Dr.Web pour UNIX

L'utilitaire d'installation à distance de l'Agent Dr.Web pour UNIX permet d'installer à distance l'Agent Dr. Web sur les postes protégés du réseau antivirus, tournant sous l'OS de la famille UNIX. Si nécessaire, vous pouvez également installer Dr.Web pour les serveurs de fichiers UNIX à l'aide de cet utilitaire.

L'utilitaire est disponible en mode de la ligne de commande dans les versions suivantes :

Fichier exécutable	Localisation	Description
`drweb-unix-install-<OS>-<nombre de bits>`	Centre de gestion, section **Administration** → **Utilitaires**	Version indépendante de l'utilitaire. Elle peut être lancée d'un répertoire aléatoire ou sur n'importe quel ordinateur ayant le système d'exploitation correspondant. Elle est mise à jour lors de la mise à jour du référentiel ou du Serveur Dr.Web.
	Répertoire du Serveur Dr.Web `webmin/utilities`	
`drwunixinstall`	Répertoire du Serveur Dr.Web `bin`	La version de l'utilitaire dépend de la présence des bibliothèques de serveur. Elle peut être lancée uniquement du répertoire de son emplacement. Elle est mise à jour lors de la mise à jour du Serveur Dr.Web uniquement.

Les fonctions des versions de l'utilitaire `drweb-unix-install-<OS>-<nombre de bits>` et `drwunixinstall` sont équivalentes. Vous trouverez ci-dessous la version `drwunixinstall`, pourtant la syntaxe et les clés possibles concernent les deux versions.

Syntaxe de la commande de démarrage :

`drwunixinstall [<clés>] <adresse_IP_du_poste _1>[:<port_SSH>[^<nom_d'utilisateur>[^<mot_de_passe>]]] <adresse_IP_du_poste_2>[:<port_SSH>[^<nom_d'utilisateur>[^<mot de passe>]]] ...`

Clés possibles

Le principe d'utilisation des clés par l'utilitaire `drwunixinstall` est soumis aux règles communes décrites dans la rubrique Annexe G. Paramètres de la ligne de commande relatifs aux programmes inclus dans Dr.Web Enterprise Security Suite.

- `--help` : afficher l'aide sur les clés.

- `--ak` <*paramètres_d'authentification*> : spécifier les paramètres d'authentification alternative sur les postes distants avec l'utilisation des clés de chiffrement au format suivant :

  <*nom_d'utilisateur*>
  `^`<*chemin_d'accès_à_la_clé_privée_du_Serveur*>`^`<*chemin_d'accès_à_la_clé_publique_du_Serveur_Dr.Web*>`[^`<*mot_de_passe_de_la_clé_privée*>`]`

  Si, lors de la formation de la commande, vous spécifiez en même temps les paramètres d'authentification standard (la paire <*nom_d'utilisateur*>`^`<*mot_de_passe*>) et ceux d'authentification alternative par les clés de chiffrements, ce sont les paramètres avec les clés qui seront utilisés les premiers lors du lancement de l'utilitaire.

- `--ap` <*nom_d'utilisateur*>`^`<*mot_de_passe*> : utiliser le mode d'authentification interactive du clavier (keyboard-interactive) sur les postes distants.
- `--certificate` <<*chemin*> : spécifier le chemin d'accès au fichier du certificat du Serveur Dr.Web. Par défaut, c'est `webmin/install/unix/workstation/drwcsd-certificate.pem`.
- `--cpus` <*nombre*> : spécifier le nombre de coeurs de processeur utilisés lors de l'installation à distance. Par défaut : `4`.
- `--ctimeout` <*délai*> : spécifier le délai maximum d'attente de la fin du transfert des packages d'installation sur les postes distants. Il est spécifié en secondes, par défaut : `600`.
- `--debug` : créer un journal de l'utilitaire en mode de débogage. Par défaut : `no`.
- `--esuite` <*adresse_du_serveur*> : entrer l'adresse du Serveur Dr.Web depuis lequel sera effectuée l'installation à distance et auquel l'Agent Dr.Web se connectera à la fin de l'installation. Format : `[udp://]`<*adresse_IP_ou_nom_DNS*>`[:`<*port*>`]`
- `--etimeout` <*délai*> : spécifier le délai maximum d'attente de la fin de l'installation des packages sur les postes distants. Il est spécifié en secondes, par défaut : `900`.
- `--from` <*chemin*> : spécifier le chemin d'accès au répertoire contenant les packages d'installation sur le Serveur Dr.Web. Par défaut : `webmin/install/unix`.
- `--long` : créer un journal de l'utilitaire avec l'indication d'horodotages. Par défaut, c'est `no`.
- `--pwd` <*mot_de_passe*> : mot de passe pour l'authentification sur les postes distant avec la commande `su` et/ou `sudo`.
- `--remote-temp` <*chemin*> : spécifier le chemin d'accès au répertoire sur les postes distants pour le stockage temporaire de la distribution et du certificat du Serveur Dr.Web. Par défaut, c'est le répertoire spécifié dans le système qui est utilisé.
- `--server` : installer le produit Dr.Web pour les serveurs de fichiers UNIX à la place de l'Agent Dr.Web. Par défaut : `no`.
- `--simultaneously` <<*nombre*> : spécifier le nombre maximum des postes sur lesquels l'Agent Dr.Web sera installé en même temps.
- `--sshdebug` : créer un journal de fonctionnement de l'utilitaire en mode de débogage avec la description détaillée de toutes les opérations utilisant le protocole SSH. Par défaut : `no`.

- `--sshwaitdebug` : créer un journal de fonctionnement de l'utilitaire en mode de débogage avec la description détaillée de toutes les opérations utilisant le protocole SSH et . Par défaut : `no`.
- `--stimeout` <*délai*> : spécifier le délai maximum d'attente de saisie du mot de passe pour l'utilisation de la commande `su` et/ou `sudo` sur les postes distants. Il est spécifié en secondes, par défaut : `10`.
- `--su` : utiliser la commande `su` lors de l'installation pour augmenter les privilèges jusqu'au niveau de super-utilisateur sur les postes distants. Par défaut, c'est `no`.
- `--sudo` : utiliser la commande `sudo` lors de l'installation pour augmenter les privilèges jusqu'au niveau de super-utilisateur sur les postes distants. Par défaut, c'est `no`.
- `--temp` <*chemin*> : spécifier le chemin d'accès au répertoire sur le Serveur Dr.Web pour le stockage temporaire du certificat. Par défaut, c'est le répertoire spécifié dans le système qui est utilisé.
- `--timeout` <*délai*> : spécifier le délai maximum d'attente de la connexion et l'authentification sur les postes distants. Il est spécifié en secondes, par défaut c'est `30`.
- `--verbosity` <*niveau*> : spécifier le niveau de détails du journal de l'utilitaire. Par défaut, c'est `info`. Les valeurs autorisées sont `all`, `debug3`, `debug2`, `debug1`, `debug`, `trace3`, `trace2`, `trace1`, `trace`, `info`, `notice`, `warning`, `error`, `crit`. Les valeurs `all` et `debug3` sont identiques.
- `--version` : afficher les informations sur la version de l'utilitaire.

G7.7. Utilitaire d'installation à distance de l'Agent Dr.Web pour Windows

L'utilitaire d'installation à distance de l'Agent Dr.Web pour Windows permet d'installer à distance l'Agent Dr. Web sur les postes protégés du réseau antivirus, tournant sous Windows.

L'utilitaire est disponible en mode de la ligne de commande dans les versions suivantes :

Fichier exécutable	Localisation	Description
`drweb-windows-install-`<*OS*>`-`<*nombre de bits*>	Centre de gestion, section **Administration** → **Utilitaires**	Version indépendante de l'utilitaire. Elle peut être lancée d'un répertoire aléatoire ou sur n'importe quel ordinateur ayant le système d'exploitation correspondant. Elle est mise à jour lors de la mise à jour du référentiel ou du Serveur Dr.Web.
	Répertoire du Serveur Dr.Web `webmin/utilities`	
`drwwindowsinstall`	Répertoire du Serveur Dr.Web `bin`	La version de l'utilitaire dépend de la présence des bibliothèques de serveur. Elle peut être lancée uniquement du répertoire de son emplacement. Elle est mise à jour lors de la mise à jour du Serveur Dr.Web uniquement.

Les fonctions des versions de l'utilitaire `drweb-windows-install-<OS>-<nombre de bits>` et `drwwindowsinstall` sont équivalentes. Vous trouverez ci-dessous la version `drwwindowsinstall`, pourtant la syntaxe et les clés possibles concernent les deux versions.

Syntaxe de la commande de démarrage :

`drwwindowsinstall <clés>`

Clés possibles

Le principe d'utilisation des clés par l'utilitaire `drwwindowsinstall` est soumis aux règles communes décrites dans la rubrique Annexe G. Paramètres de la ligne de commande relatifs aux programmes inclus dans Dr.Web Enterprise Security Suite.

- `--help` : afficher l'aide sur les clés.
- `--console=yes|no` : afficher le journal de fonctionnement de l'utilitaire dans la console. Par défaut, c'est `no`.
- `--disable-v1=yes|no` : désactiver le protocole SMB en version 1 (SMBv1) pour la période de fonctionnement de l'utilitaire. Par défaut : `no`.
- `--distribution <<nom_du_fichier>` : spécifier manuellement le nom du fichier de l'installateur de l'Agent Dr.Web qui sera lancé sur les postes distants. Par défaut : `drwinst.exe`.
- `--install-address <adresse_IP_du_poste>` : entrer l'adresse du poste distant sur lequel l'Agent Dr.Web sera installé. Si vous spécifiez plusieurs postes en même temps, leurs adresses doivent être séparées par une virgule (« `,` ») ou un point-virgule (« `;` ») sans espaces.
- `--install-certificate <chemin>` : chemin d'accès au fichier du certificat du Serveur Dr.Web.
- `--install-clients <nombre>` : spécifier le nombre maximum des postes sur lesquels l'Agent Dr.Web sera installé en même temps. Par défaut : `8`.
- `--install-compression <mode>` : spécifier le mode de compression du trafic en cas de connexion du Serveur Dr.Web aux postes distants. `on` : la compression est activée, `off` : la compression est désactivée, `possible` : la compression est possible. La dernière valeur signifie que le mode dépend de la configuration du Serveur Dr.Web. Par défaut `possible`.
- `--install-encryption <mode>` : spécifier le mode de chiffrement du trafic en cas de connexion du Serveur Dr.Web aux postes distants. `on` : le chiffrement est activé, `off` : le chiffrement est désactivé, `possible` : le chiffrement est possible. La dernière valeur signifie que le mode dépend de la configuration du Serveur Dr.Web. Par défaut `possible`.
- `--install-language <code_de_la_langue>` : spécifier la langue de l'interface de l'Agent Dr.Web installé sous forme d'un code à deux lettres conformément à la norme ISO 639-1. Si la clé n'est pas spécifiée ou que l'Agent Dr.Web en langue spécifiée n'est pas disponible, la langue système est utilisé sur le poste distant.

- `--install-path` <*chemin*> : spécifier le chemin d'accès au répertoire d'installation de l'Agent Dr.Web sur les postes distants. Par défaut, c'est `%ProgramFiles%\DrWeb`.
- `--install-register=yes|no` : enregistrer l'Agent Dr.Web dans la liste des logiciels installés à la fin de l'installation. Par défaut, c'est `no`.
- `--install-server` <*adresse_du_Serveur*> : entrer l'adresse du Serveur Dr.Web depuis lequel sera effectuée l'installation à distance et auquel l'Agent se connectera à la fin de l'installation. Format : `[udp://]`<*adresse_IP_ou_nom_DNS*>`[:`<*port*>`]`.
- `--install-timeout` <*délai*> : spécifier le délai maximum d'attente de la fin de l'installation de l'Agent Dr.Web sur les postes distants. Il est spécifié en secondes, par défaut c'est `300`.
- `--install-user` <*nom_d'utilisateur*>`@`<*domaine*>`:`<*mot de passe*> ou <*domaine*>`\`<*nom_d'utilisateur*>`:`<mot de passe> : spécifier le nom d'utilisateur et le mot de passe pour l'authentification sur les postes distants.
- `--log` <*chemin*> : spécifier le chemin d'accès au fichier de journal de l'utilitaire. Par défaut, c'est `drwsmb.log` dans le sous-répertoire `var` du répertoire d'installation du Serveur Dr.Web.
- `--machine` <*nom*> : spécifier le nom qui sera attribué au poste distant dans le réseau antivirus Dr.Web Enterprise Security Suite à la fin de l'installation de l'Agent Dr.Web et la connexion au Serveur Dr.Web. Par défaut, c'est le nom d'ordinateur enregistré dans le système d'exploitation qui est utilisé.
- `--rotate=`<*N*><*f*>`,`<*M*><*u*> : spécifier le mode de rotation du journal de l'utilitaire. Le format est équivalent à la clé similaire qui est utilisée pour la gestion de la rotation du journal du Serveur Dr.Web. Par défaut, c'est `10,10m`.
- `--service-id` <*nom_dans_le_registre*> : spécifier le nom qui sera attribué à la rubrique du service d'installation distante de l'Agent Dr.Web dans le registre Windows. Par défaut c'est `DrWebRsvcRunner`.
- `--service-name` <*nom_affiché*> : spécifier le nom du service d'installation distante de l'Agent Dr.Web affiché dans le composant logiciel enfichable Services. Par défaut c'est `Dr.Web Remote Runner Service`.
- `--target-root` <*nom_de_répertoire*> : spécifier le nom du répertoire se trouvant dans le partage administratif sur le poste distant depuis lequel sera lancé l'installateur de l'Agent Dr.Web copié du Serveur Dr.Web. Par défaut, c'est `TEMP`.
- `--target-volume` <*nom_du_partage*> : spécifier le nom du partage administratif dans lequel se trouveront les fichiers d'installation de l'Agent Dr.Web. Par défaut, c'est `ADMIN$`.
- `--threads` <*pool*> : spécifier le nombre de flux d'entrée-sortie dans le pool. Par défaut, c'est `2`.
- `--verbosity` <*niveau*> : spécifier le niveau de détails du journal de l'utilitaire. Par défaut : `trace`. Les valeurs autorisées sont `all, debug3, debug2, debug1, debug, trace3, trace2, trace1, trace, info, notice, warning, error, crit`. Les valeurs `all` et `debug3` sont identiques.
- `--version` : afficher les informations sur la version de l'utilitaire.

Annexe H. Variables d'environnement exportées par le Serveur Dr.Web

Pour faciliter le paramétrage des processus lancés par le Serveur Dr.Web selon la planification, les données sur l'emplacement des répertoires du Serveur Dr.Web sera requise. C'est pour cette raison que le Serveur Dr.Web exporte dans l'environnement des processus lancés les variables suivantes :

- `DRWCSD_HOME` : chemin vers le répertoire racine (répertoire d'installation). La valeur de la clé est `-home` si la clé n'a pas été spécifiée au démarrage du Serveur Dr.Web, sinon c'est le répertoire courant lors du démarrage.
- `DRWCSD_BIN` : chemin vers le répertoire pour les fichiers exécutables. La valeur de la clé est `-bin-root` si la clé n'a pas été spécifiée au démarrage du Serveur Dr.Web, sinon c'est le sous-répertoire `bin` du répertoire racine.
- `DRWCSD_VAR` : chemin vers le répertoire dans lequel le Serveur Dr.Web est autorisé à écrire et qui est destiné à sauvegarder les fichiers modifiables (par exemple, les journaux et les fichiers du référentiel). La valeur de la clé est `-var-root` si la clé n'a pas été spécifiée au démarrage du Serveur Dr.Web, sinon c'est le sous-répertoire `var` du répertoire racine.

Annexe I. Utilisation des expressions régulières dans Dr.Web Enterprise Security Suite

Certains paramètres de Dr.Web Enterprise Security Suite sont spécifiés sous forme d'expressions régulières des types suivants :

- Expressions régulières du langage Lua.

  Elles sont utilisées lors de la configuration de l'appartenance automatique de postes du réseau antivirus aux groupes utilisateur.

  Pour en savoir plus sur la syntaxe des expressions régulières du langage Lua, consultez le site http://www.lua.org/manual/5.1/manual.html#5.4.1.

- Expressions régulières de la bibliothèque logicielle PCRE.

  Pour en savoir plus sur la syntaxe de la bibliothèque PCRE, consultez le site http://www.pcre.org/.

  La présente annexe ne contient qu'une description abrégée des principaux points relatifs à l'utilisation des expressions régulières de la bibliothèque PCRE.

I1. Options des expressions régulières PCRE

Les expressions régulières sont utilisées dans le fichier de configuration du Serveur Dr.Web ainsi que dans le Centre de gestion lors du paramétrage des objets à exclure de l'analyse dans la configuration du Scanner Dr.Web.

Les expressions régulières ont le format suivant :

```
qr{EXP}options
```

où `EXP` — expression même, `options` — séquence des options (ligne de caractères). `qr{}` — métacaractères littéraux. Voici un exemple de construction :

`qr{pagefile\.sys}i` : fichier swap de Windows NT

Vous trouverez ci-dessous une description des options et des expressions régulières. Pour plus d'information, visitez le lien http://www.pcre.org/pcre.txt.

- Option `'a'` correspondant à `PCRE_ANCHORED`

  Avec cette option, le motif est ancré, il est limité par la comparaison uniquement avec la première position recherchée dans la ligne de recherche (« chaîne sujet »). Il est possible d'y arriver avec des constructions respectives dans le motif.

- Option `'i'` correspondant à `PCRE_CASELESS`

  Avec cette option, les caractères du motif sont comparés aux majuscules et aux minuscules. Cette possibilité peut être modifiée dans le motif par le paramétrage de l'option `(?i)`.

- Option `'x' correspondant à PCRE_EXTENDED`

  Avec cette option, les caractères d'espacement sont ignorés, sauf lorsqu'ils sont échappés, ou à l'intérieur d'une classe de caractères. L'espace ne comprend pas le symbole `VT` (code 11). De plus,

tous les caractères entre # non échappés et en dehors d'une classe de caractères, ainsi que le caractère de nouvelle ligne sont ignorés. Cette option peut être modifiée dans le motif par le paramétrage de l'option (?x). Le paramétrage permet d'inclure les commentaires dans les masques compliqués. Il est à noter cependant que ceci n'est applicable qu'aux symboles de données. Les caractères d'espacement ne peuvent pas apparaître dans les séquences spécifiques d'un masque, par exemple à l'intérieur de la séquence (?(qui introduit une parenthèse conditionnelle.

- Option 'm' correspondant à PCRE_MULTILINE

  Par défaut, PCRE traite la chaîne sujet comme une seule ligne (même si cette chaîne contient des retours chariot). Le métacaractère "*début de ligne*" (^) ne sera valable qu'une seule fois, au début de la ligne, et le méta caractère "*fin de ligne* " ($) ne sera valable qu'à la fin de la chaîne, ou avant le retour chariot final (à moins que l'option PCRE_DOLLAR_ENDONLY ne soit activée).

  Lorsque l'option PCRE_MULTILINE est activée, les métacaractères "*début de ligne*" et "*fin de ligne*" correspondront alors aux caractères suivant et précédant immédiatement un caractère de nouvelle ligne, en plus du début et de la fin de la chaîne. Cette option peut être modifiée dans le masque par le paramétrage de l'option (?m). Si le texte ne contient pas les caractères "\n" ou que le masque ne contient pas les caractères ^ ou $, l'option PCRE_MULTILINE perd son sens.

- Option 'u' correspondant à PCRE_UNGREEDY

  Cette option inverse la tendance à la gourmandise des expressions régulières. Vous pouvez aussi inverser cette tendance au coup par coup avec un ?. De même, si cette option est activée, le ? rendra gourmand une séquence. Ceci peut également être paramétré avec l'option (?U) dans le modèle.

- Option 'd' correspondant à PCRE_DOTALL

  Avec cette option, le méta caractère point "." dans le masque est comparé avec tous les caractères, y compris le caractère de la nouvelle ligne. Si le méta caractère n'est pas présent, les caractères de la nouvelle ligne seront exclus. Cette option peut être modifiée dans le motif avec la spécification de la nouvelle option (?s). La classe négative, par exemple [^a] est toujours comparée avec le caractère de la nouvelle ligne quels que soient les paramètres de l'option.

- Option 'e' correspondant à PCRE_DOLLAR_ENDONLY

  Avec cette option, le métacaractère $ ne sera valable qu'à la fin de la chaîne sujet. Sans cette option, $ est aussi valable avant une nouvelle ligne, si cette dernière est le dernier caractère de la chaîne. L'option PCRE_DOLLAR_ENDONLY est ignorée si l'option CRE_MULTILINE est activée.

I2. Particularités des expressions régulières PCRE

L'expression régulière est un patron à comparer avec le texte de gauche à droite. La plupart des caractères contenus dans le patron se représentent eux-mêmes et s'appliquent aux caractères correspondants dans le texte.

L'avantage principal des expressions régulières consiste en la possibilité d'inclure dans le masque les variantes et les répétitions. Elles sont codées avec les métacaractères qui à leur tour ne se représentent pas eux-mêmes mais sont interprétés de manière appropriée.

Il existe deux ensembles de métacaractères : ceux qui sont utilisés entre crochets et ceux qui sont utilisés à l'extérieur. Nous allons les envisager de plus près. Les métacaractères listés ci-dessous sont utilisés hors crochets :

Symbole	Valeur
\	caractère de contrôle standard (escape) permettant plusieurs variantes d'utilisation
^	indique le début de la chaîne (ou du texte en mode multi-lignes)
$	indique la fin de la chaîne (ou du texte en mode multi-lignes)
.	correspond à n'importe quel caractère sauf le caractère de saut de ligne (par défaut)
[	début de la description d'une classe de caractères
]	fin de description d'une classe de caractères
|	début d'une branche de l'alternative
(	début du sous-masque
)	fin du sous-masque
?	étend la valeur (aussi quantificateur 0 ou 1 aussi quantificateur-minimisateur
*	0 ou plus
+	1 ou plus aussi "quantificateur possesif"
{	début du quantificateur minimum/maximum

La partie du masque se trouvant entre crochets est nommée "classe de caractères". La classe de caractère comprend les métacaractères suivants :

Symbole	Valeur
\	caractère de contrôle standard (escape)
^	négation de la classe mais uniquement dans la position au début de la classe
-	détermine la plage de caractères

Symbole	Valeur
[	classe de caractères POSIX (uniquement dans le cas où elle est suivie de la syntaxe POSIX)
]	ferme la classe de caractères

Annexe J. Format des fichiers de journal

Les fichiers de journal du Serveur Dr.Web (voir le **Manuel Administrateur**, p. Journal du Serveur Dr.Web) et de l'Agent Dr.Web sont au format texte, chaque ligne est comprise comme un message séparé.

La ligne de message a le format suivant :

<année><mois><date>.<heure><minute><seconde>.<centièmes_de_seconde>
<type_de_message> [*<id_du-processus>*] *<nom_du_flux>* [*<source_du_message>*] *<message>*

où :

- *<année><mois><date>.<heure><minute><seconde>.<centièmes_de_seconde>* est la date précise de l'écriture du message dans le fichier de journal.
- *<type_de_message>* : niveau de journal :
  - **ftl** (fatal error — erreur fatale) : messages sur des erreurs critiques relatives au fonctionnement ;
  - **err** (error — erreur) : messages sur des erreurs de fonctionnement ;
  - **wrn** (warning — avertissement) : avertissements sur des erreurs ;
  - **ntc** (notice — note) : messages d'information importants ;
  - **inf** (info — information) : messages d'information ;
  - **tr0..3** (trace0..3 – traçage) : traçage des actions réalisées de divers niveaux de détail (**Traçage3** : niveau de détail maximum) ;
  - **db0..3** (debug0..3 — débogage) : message de débogage de divers niveau de détail (**Débogage3** : niveau maximum de détail).

  

  Les messages de niveau de journal **tr0..3** (traçage) et de **db0..3** (débogage) sont écrits seulement pour les développeurs de Dr.Web Enterprise Security Suite.

- [*<id_du_processus>*] : identificateur numérique unique du processus durant lequel le flux écrivant le message dans le fichier de journal a été exécuté. Sous certains OS [*<id_du-processus>*] peut être représenté sous la forme [*<id_du_processus> <id_du_flux>*].
- *<nom_du_flux>* : désignation symbolique du flux au sein duquel l'écriture du message vers le fichier de journal a été effectuée.
- [*<source_du_message>*] : désignation du système initiateur de l'écriture du message vers le fichier de journal. La source n'est pas toujours présente.
- *<message>* : message texte décrivant les actions conformément au niveau du journal. Il peut comprendre une description formelle ainsi que les valeurs des variables importantes pour le cas courant.

Exemple :

1. `20081023.171700.74 inf [001316] mth:12 [Sch] Job "Purge unsent IS events" said OK`

   où :

   - `20081023` : <*année*><*mois*><*jour*>,
   - `171700` : <*heure*><*minute*><*seconde*>,
   - `74` : <*centième_de_seconde*>,
   - `inf` — <*type_de_message*> : message d'information,
   - `[001316]` — [<*id_du_processus*>],
   - `mth:12` — <*nom_du_flux*>,
   - `[Sch]` — [<*source_du_message*>] — planificateur,
   - `Job "Purge unsent IS events" said OK` : message sur l'exécution correcte de la tâche **Suppression des événements non envoyés**.

2. `20081028.135755.61 inf [001556] srv:0 tcp/10.3.0.55:3575/025D4F80:2: new connection at tcp/10.3.0.75:2193`

   où :

   - `20081028` : <*année*><*mois*><*jour*>,
   - `135755` : <*heure*><*minute*><*seconde*>,
   - `61` : <*centième_de_seconde*>,
   - `inf` — <*type_de_message*> : message d'information,
   - `[001556]` — [<*id_du_processus*>],
   - `srv:0` — <*nom_du_flux*>,
   - `tcp/10.3.0.55:3575/025D4F80:2: new connection at tcp/10.3.0.75:2193` : message d'installation d'une nouvelle connexion via le socket spécifié.

Annexe K. Intégration de Web API avec Dr.Web Enterprise Security Suite

Pour en savoir plus sur **Web API**, consultez le manuel **Web API pour Dr.Web Enterprise Security Suite**.

Application

L'intégration de **Web API** avec Dr.Web Enterprise Security Suite offre les fonctions permettant de réaliser des opérations avec les comptes et d'automatiser le processus d'administration des utilisateurs du service. Vous pouvez utiliser ce processus, par exemple, lors de la création des pages dynamiques destinées à recevoir des requêtes utilisateur à fournir à l'utilisateur le fichier d'installation.

Authentification

L'interaction avec le Serveur Dr.Web est effectuée via le protocole HTTP(S). **Web API** reçoit des requêtes REST et retourne XML. Pour accéder à Web API, l'authentification Basic HTTP est utilisée (conformément à la norme RFC 2617). Si la norme RFC 2617 n'est pas respectée, le serveur HTTP(S) ne demandera pas les données d'authentification du client (le login et le mot de passe de l'administrateur de Dr.Web Enterprise Security Suite) pour réussir l'authentification.

Annexe L. Licences

Dans cette rubrique vous pouvez consulter la liste des bibliothèques extérieures qui sont utilisées par le logiciel Dr.Web Enterprise Security Suite, ainsi que les informations concernant leurs licences et les adresses des projets de développement.

Bibliothèque extérieure	Licence	URL du projet
asio	https://www.boost.org/LICENSE_1_0.txt*	https://think-async.com/Asio/
Base58	https://github.com/leafo/lua-base58/blob/master/LICENSE	https://github.com/leafo/lua-base58
boost	https://www.boost.org/LICENSE_1_0.txt*	https://www.boost.org/
brotli	MIT License**	https://github.com/google/brotli
bsdiff	Custom	http://www.daemonology.net/bsdiff/
c-ares	https://c-ares.org/license.html*	https://c-ares.org/
cairo	Mozilla Public License** GNU Lesser General Public License**	https://www.cairographics.org/
CodeMirror	MIT License**	https://codemirror.net/
curl	https://curl.se/docs/copyright.html*	https://curl.se/libcurl/
fontconfig	Custom	https://www.freedesktop.org/wiki/Software/fontconfig/
freetype	GNU General Public License** FreeType Project License (BSD like)	https://freetype.org/
GCC runtime libraries	GNU General Public License** with exception*	https://gcc.gnu.org/
HTMLayout	Custom	https://terrainformatica.com/a-homepage-section/htmlayout/
ICU	https://www.unicode.org/copyright.html#License*	https://icu.unicode.org/home
jemalloc	https://github.com/jemalloc/jemalloc/blob/dev/COPYING*	https://github.com/jemalloc/jemalloc

Bibliothèque extérieure	Licence	URL du projet
jQuery	MIT License** GNU General Public License**	https://jquery.com/
JSON	https://github.com/nlohmann/json/blob/develop/LICENSE.MIT	https://github.com/nlohmann/json
JSON4Lua	MIT License**	https://github.com/craigmj/json4lua
Leaflet	BSD License https://github.com/Leaflet/Leaflet/blob/main/LICENSE*	https://leafletjs.com
libipeg turbo	https://github.com/libjpeg-turbo/libjpeg-turbo/blob/main/LICENSE.md	https://libjpeg-turbo.org/
libpng	http://libpng.org/pub/png/src/libpng-LICENSE.txt*	http://libpng.org/pub/png/libpng.html
libradius	Juniper Networks, Inc.*	https://www.freebsd.org
libssh2	3-Clause BSD License https://github.com/libssh2/libssh2/blob/master/COPYING*	https://libssh2.org/
libxml2	MIT License**	https://gitlab.gnome.org/GNOME/libxml2/-/wikis/home
Linenoise NG	BSD license*	https://github.com/arangodb/linenoise-ng
lua	MIT License**	https://www.lua.org/
lua-xmlreader	MIT License**	https://asbradbury.org/projects/lua-xmlreader/
lzma	Public Domain	https://www.7-zip.org/sdk.html
ncurses	MIT License**	https://invisible-island.net/ncurses/announce.html
Net-snmp	http://www.net-snmp.org/about/license.html*	http://www.net-snmp.org/
nghttp2	MIT License**	https://nghttp2.org/

Bibliothèque extérieure	Licence	URL du projet
Noto Sans CJK	https://scripts.sil.org/cms/scripts/render_download.php?format=file&media_id=OFL_plaintext&filename=OFL.txt*	https://fonts.google.com/noto/use
OpenLDAP	https://www.openldap.org/software/release/license.html*	https://www.openldap.org
OpenSSL	https://www.openssl.org/source/license.html*	https://www.openssl.org/
Oracle Instant Client	https://www.oracle.com/downloads/licenses/instant-client-lic.html*	https://www.oracle.com
ParaType Free Font	https://www.paratype.ru/eula*	https://www.paratype.ru
pcre	http://www.pcre.org/licence.txt*	http://www.pcre.org/
pixman	MIT License**	http://pixman.org/
Prototype JavaScript framework	MIT License**	http://prototypejs.org/assets/2009/8/31/prototype.js
quirc	https://github.com/dlbeer/quirc/blob/master/LICENSE	https://github.com/dlbeer/quirc/
QR Code generator	https://github.com/nayuki/QR-Code-generator	https://www.nayuki.io/page/qr-code-generator-library
script.aculo.us scriptaculous.js	https://madrobby.github.io/scriptaculous/license/*	http://script.aculo.us/
slt	MIT License**	https://code.google.com/archive/p/slt
SQLite	Public Domain https://www.sqlite.org/copyright.html	https://www.sqlite.org/index.html
wtl	Common Public License** Microsoft Public License**	https://sourceforge.net/projects/wtl/
zlib	https://www.zlib.net/zlib_license.html*	https://www.zlib.net/

* : les textes des licences sont disponibles ci-dessous.

** : vous pouvez trouver les textes des licences de base aux adresses suivantes :

Licence	Adresse
Common Public License	https://opensource.org/license/cpl1-0-txt/
GNU General Public License	https://www.gnu.org/licenses/gpl-3.0.html
GNU Lesser General Public License	https://www.gnu.org/licenses/lgpl-3.0.html
Microsoft Public License	https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff649456(v=pandp.10)
MIT License	https://opensource.org/license/mit/
Mozilla Public License	https://www.mozilla.org/en-US/MPL/2.0/
3-Clause BSD License	https://opensource.org/license/bsd-3-clause/

L1. Base58

```
The MIT License (MIT)


Copyright (c) 2015 leaf


Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:


The above copyright notice and this permission notice shall be included in all
copies or substantial portions of the Software.


THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
```

```
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE

AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER

LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,

OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE

SOFTWARE.
```

L2. Boost

```
Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of
the software and accompanying documentation covered by this license (the "Software") to use,
reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative
works of the Software, and to permit third-parties to whom the Software is furnished to do so,
all subject to the following:

The copyright notices in the Software and this entire statement, including the above license
grant, this restriction and the following disclaimer, must be included in all copies of the
Software, in whole or in part, and all derivative works of the Software, unless such copies or
derivative works are solely in the form of machine-executable object code generated by a source
language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING
BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE
AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE
SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE,
ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
SOFTWARE.
```

L3. C-ares

```
Copyright (c) 2007 - 2018, Daniel Stenberg with many contributors, see AUTHORS file.

Copyright 1998 by the Massachusetts Institute of Technology.

Permission to use, copy, modify, and distribute this software and its documentation for any
purpose and without fee is hereby granted, provided that the above copyright notice appear in
all copies and that both that copyright notice and this permission notice appear in supporting
documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to
distribution of the software without specific, written prior permission. M.I.T. makes no
representations about the suitability of this software for any purpose. It is provided "as is"
without express or implied warranty.
```

L4. Curl

```
Copyright (c) 1996 - 2013, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.
```

```
Permission to use, copy, modify, and distribute this software for any purpose with or without
fee is hereby granted, provided that the above copyright notice and this permission notice
appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING
BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE
LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR
OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS
IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in
advertising or otherwise to promote the sale, use or other dealings in this Software without
prior written authorization of the copyright holder.
```

L5. GCC runtime libraries—exception

```
GCC is Copyright (C) 1986, 1987, 1988, 1989, 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997,
1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008 Free Software Foundation, Inc.

GCC is free software; you can redistribute it and/or modify it under the terms of the GNU
General Public License as published by the Free Software Foundation; either version 3, or (at
your option) any later version.

GCC is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even
the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the GNU
General Public License for more details.

Files that have exception clauses are licensed under the terms of the GNU General Public
License; either version 3, or (at your option) any later version.

The following runtime libraries are licensed under the terms of the GNU General Public License
(v3 or later) with version 3.1 of the GCC Runtime Library Exception (included in this file):

 - libgcc (libgcc/, gcc/libgcc2.[ch], gcc/unwind*, gcc/gthr*, gcc/coretypes.h, gcc/crtstuff.c,
gcc/defaults.h, gcc/dwarf2.h, gcc/emults.c, gcc/gbl-ctors.h, gcc/gcov-io.h, gcc/libgcov.c,
gcc/tsystem.h, gcc/typeclass.h).

 - libdecnumber

 - libgomp

 - libssp

 - libstdc++-v3

 - libobjc

 - libmudflap

 - libgfortran

 - The libgnat-4.4 Ada support library and libgnatvsn library.

 - Various config files in gcc/config/ used in runtime libraries.

GCC RUNTIME LIBRARY EXCEPTION

Version 3.1, 31 March 2009

Copyright (C) 2009 Free Software Foundation, Inc. <http://fsf.org/>
```

```
Everyone is permitted to copy and distribute verbatim copies of this license document, but
changing it is not allowed.

This GCC Runtime Library Exception ("Exception") is an additional permission under section 7 of
the GNU General Public License, version 3 ("GPLv3"). It applies to a given file (the "Runtime
Library") that bears a notice placed by the copyright holder of the file stating that the file
is governed by GPLv3 along with this Exception.

When you use GCC to compile a program, GCC may combine portions of certain GCC header files and
runtime libraries with the compiled program. The purpose of this Exception is to allow
compilation of non-GPL (including proprietary) programs to use, in this way, the header files
and runtime libraries covered by this Exception.

0. Definitions.

A file is an "Independent Module" if it either requires the Runtime Library for execution after
a Compilation Process, or makes use of an interface provided by the Runtime Library, but is not
otherwise based on the Runtime Library.

"GCC" means a version of the GNU Compiler Collection, with or without modifications, governed by
version 3 (or a specified later version) of the GNU General Public License (GPL) with the option
of using any subsequent versions published by the FSF.

"GPL-compatible Software" is software whose conditions of propagation, modification and use
would permit combination with GCC in accord with the license of GCC.

"Target Code" refers to output from any compiler for a real or virtual target processor
architecture, in executable form or suitable for input to an assembler, loader, linker and/or
execution phase. Notwithstanding that, Target Code does not include data in any format that is
used as a compiler intermediate representation, or used for producing a compiler intermediate
representation.

The "Compilation Process" transforms code entirely represented in non-intermediate languages
designed for human-written code, and/or in Java Virtual Machine byte code, into Target Code.
Thus, for example, use of source code generators and preprocessors need not be considered part
of the Compilation Process, since the Compilation Process can be understood as starting with the
output of the generators or preprocessors.

A Compilation Process is "Eligible" if it is done using GCC, alone or with other GPL-compatible
software, or if it is done without using any work based on GCC. For example, using non-GPL-
compatible Software to optimize any GCC intermediate representations would not qualify as an
Eligible Compilation Process.

1. Grant of Additional Permission.

You have permission to propagate a work of Target Code formed by combining the Runtime Library
with Independent Modules, even if such propagation would otherwise violate the terms of GPLv3,
provided that all Target Code was generated by Eligible Compilation Processes. You may then
convey such a combination under terms of your choice, consistent with the licensing of the
Independent Modules.

2. No Weakening of GCC Copyleft.

The availability of this Exception does not imply any general presumption that third-party
software is unaffected by the copyleft requirements of the license of GCC.
```

L6. ICU

```
Copyright © 1991-2018 Unicode, Inc. All rights reserved.

Distributed under the Terms of Use in http://www.unicode.org/copyright.html.
```

```
Permission is hereby granted, free of charge, to any person obtaining a copy of the Unicode data
files and any associated documentation (the "Data Files") or Unicode software and any associated
documentation (the "Software") to deal in the Data Files or Software without restriction,
including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or
sell copies of the Data Files or Software, and to permit persons to whom the Data Files or
Software are furnished to do so, provided that either (a) this copyright and permission notice
appear with all copies of the Data Files or Software, or (b) this copyright and permission
notice appear in associated Documentation.

THE DATA FILES AND SOFTWARE ARE PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT
HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR
CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS,
WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN
CONNECTION WITH THE USE OR PERFORMANCE OF THE DATA FILES OR SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in
advertising or otherwise to promote the sale, use or other dealings in these Data Files or
Software without prior written authorization of the copyright holder.
```

L7. Jemalloc

```
Unless otherwise specified, files in the jemalloc source distribution are subject to the
following license:

--------------------------------------------------------------------------------

Copyright (C) 2002-2018 Jason Evans <jasone@canonware.com>.

All rights reserved.

Copyright (C) 2007-2012 Mozilla Foundation.  All rights reserved.

Copyright (C) 2009-2018 Facebook, Inc.  All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted
provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice(s), this list of
conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice(s), this list of
conditions and the following disclaimer in the documentation and/or other materials provided
with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER(S) ``AS IS'' AND ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS
FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER(S) BE LIABLE FOR
ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

--------------------------------------------------------------------------------
```

L8. JSON

```
MIT License



Copyright (c) 2013-2022 Niels Lohmann



Permission is hereby granted, free of charge, to any person obtaining a copy

of this software and associated documentation files (the "Software"), to deal

in the Software without restriction, including without limitation the rights

to use, copy, modify, merge, publish, distribute, sublicense, and/or sell

copies of the Software, and to permit persons to whom the Software is

furnished to do so, subject to the following conditions:



The above copyright notice and this permission notice shall be included in all

copies or substantial portions of the Software.



THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR

IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,

FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE

AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER

LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,

OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE

SOFTWARE.
```

L9. Leaflet

```
Copyright (c) 2010-2018, Vladimir Agafonkin

Copyright (c) 2010-2011, CloudMade

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted
provided that the following conditions are met:

   1. Redistributions of source code must retain the above copyright notice, this list of
conditions and the following disclaimer.
```

```
   2. Redistributions in binary form must reproduce the above copyright notice, this list of
conditions and the following disclaimer in the documentation and/or other materials provided
with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND
FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.
```

L10. libjpeg turbo

```
libjpeg-turbo note:  This file has been modified by The libjpeg-turbo Project
to include only information relevant to libjpeg-turbo, to wordsmith certain
sections, and to remove impolitic language that existed in the libjpeg v8
README.  It is included only for reference.  Please see README.md for
information specific to libjpeg-turbo.



The Independent JPEG Group's JPEG software
==========================================


This distribution contains a release of the Independent JPEG Group's free
JPEG
software.  You are welcome to redistribute this software and to use it for
any
purpose, subject to the conditions under LEGAL ISSUES, below.


This software is the work of Tom Lane, Guido Vollbeding, Philip Gladstone,
Bill Allombert, Jim Boucher, Lee Crocker, Bob Friesenhahn, Ben Jackson,
Julian Minguillon, Luis Ortiz, George Phillips, Davide Rossi, Ge' Weijers,
and other members of the Independent JPEG Group.
```

```
IJG is not affiliated with the ISO/IEC JTC1/SC29/WG1 standards committee
(also known as JPEG, together with ITU-T SG16).



DOCUMENTATION ROADMAP
=====================

This file contains the following sections:

OVERVIEW            General description of JPEG and the IJG software.
LEGAL ISSUES        Copyright, lack of warranty, terms of distribution.
REFERENCES          Where to learn more about JPEG.
ARCHIVE LOCATIONS   Where to find newer versions of this software.
FILE FORMAT WARS    Software *not* to get.
TO DO               Plans for future IJG releases.

Other documentation files in the distribution are:

User documentation:
  usage.txt         Usage instructions for cjpeg, djpeg, jpegtran,
                    rdjpgcom, and wrjpgcom.
  *.1               Unix-style man pages for programs (same info as
usage.txt).
  wizard.txt        Advanced usage instructions for JPEG wizards only.
  change.log        Version-to-version change highlights.
Programmer and internal documentation:
  libjpeg.txt       How to use the JPEG library in your own programs.
  example.txt       Sample code for calling the JPEG library.
  structure.txt     Overview of the JPEG library's internal structure.
```

```
  coderules.txt     Coding style rules --- please read if you contribute
code.


Please read at least usage.txt.  Some information can also be found in the
JPEG

FAQ (Frequently Asked Questions) article.  See ARCHIVE LOCATIONS below to
find

out where to obtain the FAQ article.


If you want to understand how the JPEG code works, we suggest reading one or

more of the REFERENCES, then looking at the documentation files (in roughly

the order listed) before diving into the code.




OVERVIEW

========


This package contains C software to implement JPEG image encoding, decoding,

and transcoding.  JPEG (pronounced "jay-peg") is a standardized compression

method for full-color and grayscale images.  JPEG's strong suit is
compressing

photographic images or other types of images that have smooth color and

brightness transitions between neighboring pixels.  Images with sharp lines
or

other abrupt features may not compress well with JPEG, and a higher JPEG

quality may have to be used to avoid visible compression artifacts with such

images.


JPEG is lossy, meaning that the output pixels are not necessarily identical
to

the input pixels.  However, on photographic content and other "smooth"
images,
```

very good compression ratios can be obtained with no visible compression artifacts, and extremely high compression ratios are possible if you are willing to sacrifice image quality (by reducing the "quality" setting in the compressor.)

This software implements JPEG baseline, extended-sequential, and progressive compression processes. Provision is made for supporting all variants of these
processes, although some uncommon parameter settings aren't implemented yet. We have made no provision for supporting the hierarchical or lossless processes defined in the standard.

We provide a set of library routines for reading and writing JPEG image files,
plus two sample applications "cjpeg" and "djpeg", which use the library to perform conversion between JPEG and some other popular image file formats. The library is intended to be reused in other applications.

In order to support file conversion and viewing software, we have included considerable functionality beyond the bare JPEG coding/decoding capability; for example, the color quantization modules are not strictly part of JPEG decoding, but they are essential for output to colormapped file formats or colormapped displays. These extra functions can be compiled out of the library if not required for a particular application.

We have also included "jpegtran", a utility for lossless transcoding between different JPEG processes, and "rdjpgcom" and "wrjpgcom", two simple applications for inserting and extracting textual comments in JFIF files.

```
The emphasis in designing this software has been on achieving portability and
flexibility, while also making it fast enough to be useful.  In particular,
the software is not intended to be read as a tutorial on JPEG.  (See the
REFERENCES section for introductory material.)  Rather, it is intended to
be reliable, portable, industrial-strength code.  We do not claim to have
achieved that goal in every aspect of the software, but we strive for it.

We welcome the use of this software as a component of commercial products.
No royalty is required, but we do ask for an acknowledgement in product
documentation, as described under LEGAL ISSUES.



LEGAL ISSUES
============

In plain English:

1. We don't promise that this software works.  (But if you find any bugs,
   please let us know!)
2. You can use this software for whatever you want.  You don't have to pay
us.
3. You may not pretend that you wrote this software.  If you use it in a
   program, you must acknowledge somewhere in your documentation that
   you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied,
with respect to this software, its quality, accuracy, merchantability, or
```

```
fitness for a particular purpose.  This software is provided "AS IS", and
you,

its user, assume the entire risk as to its quality and accuracy.


This software is copyright (C) 1991-2020, Thomas G. Lane, Guido Vollbeding.

All Rights Reserved except as specified below.


Permission is hereby granted to use, copy, modify, and distribute this

software (or portions thereof) for any purpose, without fee, subject to these

conditions:

(1) If any part of the source code for this software is distributed, then
this

README file must be included, with this copyright and no-warranty notice

unaltered; and any additions, deletions, or changes to the original files

must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying

documentation must state that "this software is based in part on the work of

the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts

full responsibility for any undesirable consequences; the authors accept

NO LIABILITY for damages of any kind.


These conditions apply to any software derived from or based on the IJG code,

not just to the unmodified library.  If you use our work, you ought to

acknowledge us.


Permission is NOT granted for the use of any IJG author's name or company
name

in advertising or publicity relating to this software or products derived
from
```

it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

REFERENCES
==========

We recommend reading one or more of these references before trying to understand the innards of the JPEG software.

The best short technical introduction to the JPEG compression algorithm is
        Wallace, Gregory K. "The JPEG Still Picture Compression Standard",
        Communications of the ACM, April 1991 (vol. 34 no. 4), pp. 30-44.
(Adjacent articles in that issue discuss MPEG motion picture compression, applications of JPEG, and related topics.) If you don't have the CACM issue handy, a PDF file containing a revised version of Wallace's article is available at http://www.ijg.org/files/Wallace.JPEG.pdf. The file (actually a preprint for an article that appeared in IEEE Trans. Consumer Electronics) omits the sample images that appeared in CACM, but it includes corrections and some added material. Note: the Wallace article is copyright ACM and IEEE,
and it may not be used for commercial purposes.

A somewhat less technical, more leisurely introduction to JPEG can be found in

"The Data Compression Book" by Mark Nelson and Jean-loup Gailly, published by M&T Books (New York), 2nd ed. 1996, ISBN 1-55851-434-1. This book provides good explanations and example C code for a multitude of compression methods including JPEG. It is an excellent source if you are comfortable reading C code but don't know much about data compression in general. The book's JPEG sample code is far from industrial-strength, but when you are ready to look at a full implementation, you've got one here...

The best currently available description of JPEG is the textbook "JPEG Still Image Data Compression Standard" by William B. Pennebaker and Joan L. Mitchell, published by Van Nostrand Reinhold, 1993, ISBN 0-442-01272-1. Price US$59.95, 638 pp. The book includes the complete text of the ISO JPEG standards (DIS 10918-1 and draft DIS 10918-2).

The original JPEG standard is divided into two parts, Part 1 being the actual specification, while Part 2 covers compliance testing methods. Part 1 is titled "Digital Compression and Coding of Continuous-tone Still Images, Part 1: Requirements and guidelines" and has document numbers ISO/IEC IS 10918-1, ITU-T T.81. Part 2 is titled "Digital Compression and Coding of Continuous-tone Still Images, Part 2: Compliance testing" and has document numbers ISO/IEC IS 10918-2, ITU-T T.83.

The JPEG standard does not specify all details of an interchangeable file format. For the omitted details, we follow the "JFIF" conventions, revision 1.02. JFIF version 1 has been adopted as ISO/IEC 10918-5 (05/2013) and Recommendation ITU-T T.871 (05/2011): Information technology - Digital compression and coding of continuous-tone still images: JPEG File Interchange Format (JFIF). It is available as a free download in PDF file format from

https://www.iso.org/standard/54989.html and http://www.itu.int/rec/T-REC-T.871.

A PDF file of the older JFIF 1.02 specification is available at

http://www.w3.org/Graphics/JPEG/jfif3.pdf.

The TIFF 6.0 file format specification can be obtained from

http://mirrors.ctan.org/graphics/tiff/TIFF6.ps.gz. The JPEG incorporation

scheme found in the TIFF 6.0 spec of 3-June-92 has a number of serious

problems. IJG does not recommend use of the TIFF 6.0 design (TIFF Compression

tag 6). Instead, we recommend the JPEG design proposed by TIFF Technical Note

#2 (Compression tag 7). Copies of this Note can be obtained from

http://www.ijg.org/files/. It is expected that the next revision

of the TIFF spec will replace the 6.0 JPEG design with the Note's design.

Although IJG's own code does not support TIFF/JPEG, the free libtiff library

uses our library to implement TIFF/JPEG per the Note.

ARCHIVE LOCATIONS

==========

The "official" archive site for this software is www.ijg.org.

The most recent released version can always be found there in

directory "files".

The JPEG FAQ (Frequently Asked Questions) article is a source of some

general information about JPEG. It is available at

http://www.faqs.org/faqs/jpeg-faq.

```
FILE FORMAT COMPATIBILITY

=========================

This software implements ITU T.81 | ISO/IEC 10918 with some extensions from
ITU T.871 | ISO/IEC 10918-5 (JPEG File Interchange Format-- see REFERENCES).
Informally, the term "JPEG image" or "JPEG file" most often refers to JFIF or
a subset thereof, but there are other formats containing the name "JPEG" that
are incompatible with the DCT-based JPEG standard or with JFIF (for instance,
JPEG 2000 and JPEG XR).  This software therefore does not support these
formats.  Indeed, one of the original reasons for developing this free
software
was to help force convergence on a common, interoperable format standard for
JPEG files.

JFIF is a minimal or "low end" representation.  TIFF/JPEG (TIFF revision 6.0
as
modified by TIFF Technical Note #2) can be used for "high end" applications
that need to record a lot of additional data about an image.



TO DO

=====

Please send bug reports, offers of help, etc. to jpeg-info@jpegclub.org.
```

```
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:



Redistributions of source code must retain the above copyright notice, this
list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice,
this list of conditions and the following disclaimer in the documentation
and/or other materials provided with the distribution.

Neither the name of the libjpeg-turbo Project nor the names of its
contributors may be used to endorse or promote products derived from this
software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS",
AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.
```

```
Copyright (c) <year> <copyright holders>



This software is provided 'as-is', without any express or implied warranty.
In no event will the authors be held liable for any damages arising from the
use of this software.



Permission is granted to anyone to use this software for any purpose,
including commercial applications, and to alter it and redistribute it
freely, subject to the following restrictions:



1. The origin of this software must not be misrepresented; you must not claim
that you wrote the original software. If you use this software in a product,
an acknowledgment in the product documentation would be appreciated but is
not required.



2. Altered source versions must be plainly marked as such, and must not be
misrepresented as being the original software.
```

```
3. This notice may not be removed or altered from any source distribution.
```

L11. Libpng

```
If you modify libpng you may insert additional notices immediately following this sentence.

This code is released under the libpng license.

libpng versions 1.0.7, July 1, 2000 through 1.6.32, August 24, 2017 are Copyright (c) 2000-2002,
2004, 2006-2017 Glenn Randers-Pehrson, are derived from libpng-1.0.6, and are distributed
according to the same disclaimer and license as libpng-1.0.6 with the following individuals
added to the list of Contributing Authors:

   Simon-Pierre Cadieux

   Eric S. Raymond

   Mans Rullgard

   Cosmin Truta

   Gilles Vollant

   James Yu

   Mandar Sahastrabuddhe

   Google Inc.

   Vadim Barkov

and with the following additions to the disclaimer:

There is no warranty against interference with your enjoyment of the library or against
infringement.  There is no warranty that our efforts or the library will fulfill any of your
particular purposes or needs.  This library is provided with all faults, and the entire risk of
satisfactory quality, performance, accuracy, and effort is with the user.

Some files in the "contrib" directory and some configure-generated files that are distributed
with libpng have other copyright owners and are released under other open source licenses.

libpng versions 0.97, January 1998, through 1.0.6, March 20, 2000, are Copyright (c) 1998-2000
Glenn Randers-Pehrson, are derived from libpng-0.96, and are distributed according to the same
disclaimer and license as libpng-0.96, with the following individuals added to the list of
Contributing Authors:

   Tom Lane

   Glenn Randers-Pehrson

   Willem van Schaik

libpng versions 0.89, June 1996, through 0.96, May 1997, are Copyright (c) 1996-1997 Andreas
Dilger, are derived from libpng-0.88, and are distributed according to the same disclaimer and
license as libpng-0.88, with the following individuals added to the list of Contributing
Authors:

   John Bowler

   Kevin Bracey
```

```
   Sam Bushell

   Magnus Holmgren

   Greg Roelofs

   Tom Tanner

Some files in the "scripts" directory have other copyright owners but are released under this
license.

libpng versions 0.5, May 1995, through 0.88, January 1996, are Copyright (c) 1995-1996 Guy Eric
Schalnat, Group 42, Inc.

For the purposes of this copyright and license, "Contributing Authors" is defined as the
following set of individuals:

   Andreas Dilger

   Dave Martindale

   Guy Eric Schalnat

   Paul Schmidt

   Tim Wegner

The PNG Reference Library is supplied "AS IS".  The Contributing Authors and Group 42, Inc.
disclaim all warranties, expressed or implied, including, without limitation, the warranties of
merchantability and of fitness for any purpose.  The Contributing Authors and Group 42, Inc.
assume no liability for direct, indirect, incidental, special, exemplary, or consequential
damages, which may result from the use of the PNG Reference Library, even if advised of the
possibility of such damage.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions
hereof, for any purpose, without fee, subject to the following restrictions:

  1. The origin of this source code must not be misrepresented.

  2. Altered versions must be plainly marked as such and must not be misrepresented as being the
original source.

  3. This Copyright notice may not be removed or altered from any source or altered source
distribution.

The Contributing Authors and Group 42, Inc. specifically permit, without fee, and encourage the
use of this source code as a component to supporting the PNG file format in commercial products.
 If you use this source code in a product, acknowledgment is not required but would be
appreciated.



Glenn Randers-Pehrson

glennrp at users.sourceforge.net

April 1, 2017
```

L12. Libradius

```
 Copyright 1998 Juniper Networks, Inc.
```

```
 All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted
provided that the following conditions are met:

 1. Redistributions of source code must retain the above copyright notice, this list of
conditions and the following disclaimer.

 2. Redistributions in binary form must reproduce the above copyright notice, this list of
conditions and the following disclaimer in the documentation and/or other materials provided
with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS
FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING,
BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

$FreeBSD: src/lib/libradius/radlib_private.h,v 1.6.30.3 2012/04/21 18:30:48 melifaro Exp $
```

L13. Libssh2

```
Copyright (c) 2004-2007 Sara Golemon <sarag@libssh2.org>

Copyright (c) 2005,2006 Mikhail Gusarov <dottedmag@dottedmag.net>

Copyright (c) 2006-2007 The Written Word, Inc.

Copyright (c) 2007 Eli Fant <elifantu@mail.ru>

Copyright (c) 2009-2014 Daniel Stenberg

Copyright (C) 2008, 2009 Simon Josefsson

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted
provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions
and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of
conditions and the following disclaimer in the documentation and/or other materials provided
with the distribution.

Neither the name of the copyright holder nor the names of any other contributors may be used to
endorse or promote products derived from this software without specific prior written
permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND
FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.
```

L14. Linenoise NG

linenoise

```
Copyright (c) 2010, Salvatore Sanfilippo <antirez at gmail dot com>

Copyright (c) 2010, Pieter Noordhuis <pcnoordhuis at gmail dot com>

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted
provided that the following conditions are met:

  * Redistributions of source code must retain the above copyright notice, this list of
conditions and the following disclaimer.

  * Redistributions in binary form must reproduce the above copyright notice, this list of
conditions and the following disclaimer in the documentation and/or other materials provided
with the distribution.

  * Neither the name of Redis nor the names of its contributors may be used to endorse or
promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND
FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.
```

wcwidth

```
Markus Kuhn -- 2007-05-26 (Unicode 5.0)

Permission to use, copy, modify, and distribute this software for any purpose and without fee is
hereby granted. The author disclaims all warranties with regard to this software.
```

ConvertUTF

```
Copyright 2001-2004 Unicode, Inc.

 Disclaimer

 This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any
particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to
determine applicability of information provided. If this file has been purchased on magnetic or
optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective
media within 90 days of receipt.

 Limitations on Rights to Redistribute This Code

 Unicode, Inc. hereby grants the right to freely use the information supplied in this file in
the creation of products supporting the Unicode Standard, and to make copies of this file in any
form for internal or external distribution as long as this notice remains attached.
```

L15. Net-snmp

```
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ''AS IS'' AND ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND
FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.
```

L16. Noto Sans CJK

```
Copyright (c) <dates>, <Copyright Holder> (<URL|email>), with Reserved Font Name <Reserved Font
Name>.

Copyright (c) <dates>, <additional Copyright Holder> (<URL|email>), with Reserved Font Name
<additional Reserved Font Name>.

Copyright (c) <dates>, <additional Copyright Holder> (<URL|email>).

This Font Software is licensed under the SIL Open Font License, Version 1.1.

This license is copied below, and is also available with a FAQ at:

http://scripts.sil.org/OFL

-----------------------------------------------------------

SIL OPEN FONT LICENSE Version 1.1 - 26 February 2007

-----------------------------------------------------------

PREAMBLE

The goals of the Open Font License (OFL) are to stimulate worldwide development of collaborative
font projects, to support the font creation efforts of academic and linguistic communities, and
to provide a free and open framework in which fonts may be shared and improved in partnership
with others.

The OFL allows the licensed fonts to be used, studied, modified and redistributed freely as long
as they are not sold by themselves. The fonts, including any derivative works, can be bundled,
embedded, redistributed and/or sold with any software provided that any reserved names are not
used by derivative works. The fonts and derivatives, however, cannot be released under any other
type of license. The requirement for fonts to remain under this license does not apply to any
document created using the fonts or their derivatives.

DEFINITIONS

"Font Software" refers to the set of files released by the Copyright Holder(s) under this
license and clearly marked as such. This may include source files, build scripts and
documentation.

"Reserved Font Name" refers to any names specified as such after the copyright statement(s).

"Original Version" refers to the collection of Font Software components as distributed by the
Copyright Holder(s).

"Modified Version" refers to any derivative made by adding to, deleting, or substituting -- in
part or in whole -- any of the components of the Original Version, by changing formats or by
porting the Font Software to a new environment.
```

```
"Author" refers to any designer, engineer, programmer, technical writer or other person who
contributed to the Font Software.

PERMISSION & CONDITIONS

Permission is hereby granted, free of charge, to any person obtaining a copy of the Font
Software, to use, study, copy, merge, embed, modify, redistribute, and sell modified and
unmodified copies of the Font Software, subject to the following conditions:

1) Neither the Font Software nor any of its individual components, in Original or Modified
Versions, may be sold by itself.

2) Original or Modified Versions of the Font Software may be bundled, redistributed and/or sold
with any software, provided that each copy contains the above copyright notice and this license.
These can be included either as stand-alone text files, human-readable headers or in the
appropriate machine-readable metadata fields within text or binary files as long as those fields
can be easily viewed by the user.

3) No Modified Version of the Font Software may use the Reserved Font Name(s) unless explicit
written permission is granted by the corresponding Copyright Holder. This restriction only
applies to the primary font name as presented to the users.

4) The name(s) of the Copyright Holder(s) or the Author(s) of the Font Software shall not be
used to promote, endorse or advertise any Modified Version, except to acknowledge the
contribution(s) of the Copyright Holder(s) and the Author(s) or with their explicit written
permission.

5) The Font Software, modified or unmodified, in part or in whole, must be distributed entirely
under this license, and must not be distributed under any other license. The requirement for
fonts to remain under this license does not apply to any document created using the Font
Software.

TERMINATION

This license becomes null and void if any of the above conditions are not met.

DISCLAIMER

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED,
INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE
AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL THE
COPYRIGHT HOLDER BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL,
SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT
OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER
DEALINGS IN THE FONT SOFTWARE.
```

L17. OpenLDAP

```
The OpenLDAP Public License

  Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with or
without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,

2. Redistributions in binary form must reproduce applicable copyright statements and notices,
this list of conditions, and the following disclaimer in the documentation and/or other
materials provided with the distribution, and

3. Redistributions must contain a verbatim copy of this document.
```

```
The OpenLDAP Foundation may revise this license from time to time. Each revision is
distinguished by a version number. You may use this Software under terms of this license
revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS ``AS IS'' AND ANY
EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE
OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING,
BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
OF THIS SOFTWARE, EVEN IF ADVISED OF THE  POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to
promote the sale, use or other dealing in this Software without specific, written prior
permission.  Title to copyright in this Software shall at all times remain with copyright
holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA.  All Rights
Reserved.  Permission to copy and distribute verbatim copies of this document is granted.
```

L18. OpenSSL

```
Copyright (c) 1998-2018 The OpenSSL Project.  All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted
provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of
conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of
conditions and the following disclaimer in the documentation and/or other materials provided
with the distribution.

3. All advertising materials mentioning features or use of this software must display the
following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.
(http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote
products derived from this software without prior written permission. For written permission,
please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in
their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit
(http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS
FOR A PARTICULAR PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
```

```
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

=====================================================================

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).  This
product includes software written by Tim Hudson (tjh@cryptsoft.com).

 Original SSLeay License

 -----------------------

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions
are aheared to.  The following conditions apply to all code found in this distribution, be it
the RC4, RSA, lhash, DES, etc., code; not just the SSL code.  The SSL documentation included
with this distribution is covered by the same copyright terms except that the holder is Tim
Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be
removed.

If this package is used in a product, Eric Young should be given attribution as the author of
the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or
textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted
provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and
the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of
conditions and the following disclaimer in the documentation and/or other materials provided
with the distribution.

3. All advertising materials mentioning features or use of this software must display the
following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

   The word 'cryptographic' can be left out if the rouines from the library being used are not
cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory
(application code) you must include an acknowledgement:

   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR
ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
```

```
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this
code cannot be changed.  i.e. this code cannot simply be copied and put under another
distribution licence [including the GNU Public Licence.]
```

L19. Oracle Instant Client

```
Export Controls on the Programs

Selecting the "Accept License Agreement" button is a confirmation of your agreement that you
comply, now and during the trial term, with each of the following statements:

-You are not a citizen, national, or resident of, and are not under control of, the government
of Cuba, Iran, Sudan, Libya, North Korea, Syria, nor any country to which the United States has
prohibited export.

-You will not download or otherwise export or re-export the Programs, directly or indirectly, to
the above mentioned countries nor to citizens, nationals or residents of those countries.

-You are not listed on the United States Department of Treasury lists of Specially Designated
Nationals, Specially Designated Terrorists, and Specially Designated Narcotic Traffickers, nor
are you listed on the United States Department of Commerce Table of Denial Orders.

You will not download or otherwise export or re-export the Programs, directly or indirectly, to
persons on the above mentioned lists.

You will not use the Programs for, and will not allow the Programs to be used for, any purposes
prohibited by United States law, including, without limitation, for the development, design,
manufacture or production of nuclear, chemical or biological weapons of mass destruction.

EXPORT RESTRICTIONS

You agree that U.S. export control laws and other applicable export and import laws govern your
use of the programs, including technical data; additional information can be found on Oracle®'s
Global Trade Compliance web site (http://www.oracle.com/products/export).

You agree that neither the programs nor any direct product thereof will be exported, directly,
or indirectly, in violation of these laws, or will be used for any purpose prohibited by these
laws including, without limitation, nuclear, chemical, or biological weapons proliferation.

Oracle Employees: Under no circumstances are Oracle Employees authorized to download software
for the purpose of distributing it to customers. Oracle products are available to employees for
internal use or demonstration purposes only. In keeping with Oracle's trade compliance
obligations under U.S. and applicable multilateral law, failure to comply with this policy could
result in disciplinary action up to and including termination.

Note: You are bound by the Oracle Technology Network ("OTN") License Agreement terms. The OTN
License Agreement terms also apply to all updates you receive under your Technology Track
subscription.

The OTN License Agreement terms below supercede any shrinkwrap license on the OTN Technology
Track software CDs and previous OTN License terms (including the Oracle Program License as
modified by the OTN Program Use Certificate).

Oracle Technology Network Development and Distribution License Agreement for Instant Client

"We," "us," and "our" refers to Oracle America, Inc. "You" and "your" refers to the individual
or entity that wishes to use the Programs from Oracle under this Agreement. "Programs" refers to
the Software Products referenced below that you wish to download and use and Program
documentation. "License" refers to your right to use the Programs and Program documentation
under the terms of this Agreement. The substantive and procedural laws of California govern this
```

Agreement. You and Oracle agree to submit to the exclusive jurisdiction of, and venue in, the courts of San Francisco, San Mateo, or Santa Clara counties in California in any dispute arising out of or relating to this Agreement.

We are willing to license the Programs to you only upon the condition that you accept all of the terms contained in this Agreement. Read the terms carefully and select the "Accept" button at the bottom of the page to confirm your acceptance. If you are not willing to be bound by these terms, select the "Do Not Accept" button and the registration process will not continue.

Software Product

- Instant Client

License Rights

License.

We grant you a non-exclusive right and license to use the Programs solely for your business purposes and development and testing purposes, subject to the terms of this Agreement. You may allow third parties to use the Programs, subject to the terms of this Agreement, provided such third party use is for your business operations only.

Distribution License

We grant you a non-exclusive right and license to distribute the Programs, provided that you do not charge your end users for use of the Programs. Your distribution of such Programs shall at a minimum include the following terms in an executed license agreement between you and the end user that: (1) restrict the use of the Programs to the business operations of the end user; (2) prohibit (a) the end user from assigning, giving, or transferring the Programs or an interest in them to another individual or entity (and if your end user grants a security interest in the Programs, the secured party has no right to use or transfer the Programs); (b) make the Programs available in any manner to any third party for use in the third party's business operations (unless such access is expressly permitted for the specific program license or materials from the services you have acquired); and (c) title to the Programs from passing to the end user or any other party; (3) prohibit the reverse engineering (unless required by law for interoperability), disassembly or decompilation of the Programs and prohibit duplication of the Programs except for a sufficient number of copies of each Program for the end user's licensed use and one copy of each Program media; (4) disclaim, to the extent permitted by applicable law, our liability for any damages, whether direct, indirect, incidental, or consequential, arising from the use of the Programs; (5) require the end user at the termination of the Agreement, to discontinue use and destroy or return to you all copies of the Programs and documentation; (6) prohibit publication of any results of benchmark tests run on the Programs; (7) require the end user to comply fully with all relevant export laws and regulations of the United States and other applicable export and import laws to assure that neither the Programs, nor any direct product thereof, are exported, directly or indirectly, in violation of applicable laws; (8) do not require us to perform any obligations or incur any liability not previously agreed to between you and us; (9) permit you to audit your end user's use of the Programs or to assign your right to audit the end user's use of the Programs to us; (10) designate us as a third party beneficiary of the end user license agreement; (11) include terms consistent with those contained in the sections of this Agreement entitled "Disclaimer of Warranties and Exclusive Remedies," "No Technical Support," "End of Agreement," "Relationship Between the Parties," and "Open Source"; and (11) exclude the application of the Uniform Computer Information Transactions Act.

You may allow your end users to permit third parties to use the Programs on such end user's behalf for the purposes set forth in the end user license agreement, subject to the terms of such agreement. You shall be financially responsible for all claims and damages to us caused by your failure to include the required contractual terms set forth above in each end user license agreement between you and an end user. We are a third party beneficiary of any end user license agreement between you and the end user, but do not assume any of your obligations thereunder, and you agree that you will not enter into any end user license agreement that excludes us as a third party beneficiary and will inform your end users of our rights.

If you want to use the Programs for any purpose other than as expressly permitted under this Agreement you must contact us to obtain the appropriate license. We may audit your use of the Programs. Program documentation is either shipped with the Programs, or documentation may be accessed online at http://www.oracle.com/technetwork/indexes/documentation/index.html.

You agree to: (a) defend and indemnify us against all claims and damages caused by your distribution of the Programs in breach of this Agreement and/or failure to include the required contractual provisions in your end user agreement as stated above; (b) keep executed end user agreements and records of end user information including name, address, date of distribution and identity of Programs distributed; (c) allow us to inspect your end user agreements and records upon request; and, (d) enforce the terms of your end user agreements so as to effect a timely cure of any end user breach, and to notify us of any breach of the terms.

Ownership and Restrictions

We retain all ownership and intellectual property rights in the Programs. You may make a sufficient number of copies of the Programs for the licensed use and one copy of the Programs for backup purposes.

You may not:

-use the Programs for any purpose other than as provided above;

-charge your end users for use of the Programs;

-remove or modify any Program markings or any notice of our proprietary rights;

-assign this agreement or give the Programs, Program access or an interest in the Programs to any individual or entity except as provided under this agreement;

-cause or permit reverse engineering (unless required by law for interoperability), disassembly or decompilation of the Programs;

-disclose results of any Program benchmark tests without our prior consent.

Export

You agree that U.S. export control laws and other applicable export and import laws govern your use of the Programs, including technical data; additional information can be found on Oracle's Global Trade Compliance web site located at http://www.oracle.com/products/export/index.html. You agree that neither the Programs nor any direct product thereof will be exported, directly, or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation.

Disclaimer of Warranty and Exclusive Remedies

THE PROGRAMS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. WE FURTHER DISCLAIM ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT.

IN NO EVENT SHALL WE BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR DATA USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR ENTIRE LIABILITY FOR DAMAGES HEREUNDER SHALL IN NO EVENT EXCEED ONE THOUSAND DOLLARS (U.S. $1,000).

No Technical Support

Our technical support organization will not provide technical support, phone support, or updates to you or end users for the Programs licensed under this agreement.

Restricted Rights

If you distribute a license to the United States government, the Programs, including documentation, shall be considered commercial computer software and you will place a legend, in addition to applicable copyright notices, on the documentation, and on the media label, substantially similar to the following:

NOTICE OF RESTRICTED RIGHTS

"Programs delivered subject to the DOD FAR Supplement are 'commercial computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement. Otherwise, programs delivered subject to the Federal Acquisition Regulations are 'restricted computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065."

End of Agreement

You may terminate this Agreement by destroying all copies of the Programs. We have the right to terminate your right to use the Programs if you fail to comply with any of the terms of this Agreement, in which case you shall destroy all copies of the Programs.

Relationship Between the Parties

The relationship between you and us is that of licensee/licensor. Neither party will represent that it has any authority to assume or create any obligation, express or implied, on behalf of the other party, nor to represent the other party as agent, employee, franchisee, or in any other capacity. Nothing in this Agreement shall be construed to limit either party's right to independently develop or distribute software that is functionally similar to the other party's products, so long as proprietary information of the other party is not included in such software.

Open Source

"Open Source" software - software available without charge for use, modification and distribution - is often licensed under terms that require the user to make the user's modifications to the Open Source software or any software that the user 'combines' with the Open Source software freely available in source code form. If you use Open Source software in conjunction with the Programs, you must ensure that your use does not: (i) create, or purport to create, obligations of us with respect to the Oracle Programs; or (ii) grant, or purport to grant, to any third party any rights to or immunities under our intellectual property or proprietary rights in the Oracle Programs. For example, you may not develop a software program using an Oracle Program and an Open Source program where such use results in a program file(s) that contains code from both the Oracle Program and the Open Source program (including without limitation libraries) if the Open Source program is licensed under a license that requires any "modifications" be made freely available. You also may not combine the Oracle Program with programs licensed under the GNU General Public License ("GPL") in any manner that could cause, or could be interpreted or asserted to cause, the Oracle Program or any modifications thereto to become subject to the terms of the GPL.

Entire Agreement

You agree that this Agreement is the complete agreement for the Programs and licenses, and this Agreement supersedes all prior or contemporaneous Agreements or representations. If any term of this Agreement is found to be invalid or unenforceable, the remaining provisions will remain effective.

Last updated: 01/24/08

L20. ParaType Free Font

LICENSING AGREEMENT

for the fonts with Original Name: PT Sans, PT Serif, PT Mono

Version 1.3 - January 20, 2012

GRANT OF LICENSE

ParaType Ltd grants you the right to use, copy, modify the fonts and distribute modified and unmodified copies of the fonts by any means, including placing on Web servers for free

```
downloading, embedding in documents and Web pages, bundling with commercial and non commercial
products, if it does not conflict with the conditions listed below:

- You may bundle the fonts with commercial software, but you may not sell the fonts by
themselves. They are free.

- You may distribute the fonts in modified or unmodified versions only together with this
Licensing Agreement and with above copyright notice. You have no right to modify the text of
Licensing Agreement. It can be placed in a separate text file or inserted into the font file,
but it must be easily viewed by users.

- You may not distribute modified version of the font under the Original name or a combination
of Original name with any other words without explicit written permission from ParaType.

TERMINATION & TERRITORY

This license has no limits on time and territory, but it becomes null and void if any of the
above conditions are not met.

DISCLAIMER

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED,
INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE
AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL PARATYPE
BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT,
INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE,
ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE
FONT SOFTWARE.

ParaType Ltd
```

L21. PCRE

```
PCRE2 is a library of functions to support regular expressions whose syntax and semantics are as
close as possible to those of the Perl 5 language.

Release 10 of PCRE2 is distributed under the terms of the "BSD" licence, as specified below,
with one exemption for certain binary redistributions. The documentation for PCRE2, supplied in
the "doc" directory, is distributed under the same terms as the software itself. The data in the
testdata directory is not copyrighted and is in the public domain.

The basic library functions are written in C and are freestanding. Also included in the
distribution is a just-in-time compiler that can be used to optimize pattern matching. This is
an optional feature that can be omitted when the library is built.

THE BASIC LIBRARY FUNCTIONS

---------------------------

Written by:       Philip Hazel

Email local part: ph10

Email domain:     cam.ac.uk

University of Cambridge Computing Service,

Cambridge, England.

Copyright (c) 1997-2018 University of Cambridge

All rights reserved.
```

```
PCRE2 JUST-IN-TIME COMPILATION SUPPORT

------------------------------------

Written by:       Zoltan Herczeg

Email local part: hzmester

Email domain:     freemail.hu

Copyright(c) 2010-2018 Zoltan Herczeg

All rights reserved.

STACK-LESS JUST-IN-TIME COMPILER

--------------------------------

Written by:       Zoltan Herczeg

Email local part: hzmester

Email domain:     freemail.hu

Copyright(c) 2009-2018 Zoltan Herczeg

All rights reserved.

THE "BSD" LICENCE

-----------------

Redistribution and use in source and binary forms, with or without

modification, are permitted provided that the following conditions are met:

 * Redistributions of source code must retain the above copyright notices, this list of
conditions and the following disclaimer.

 * Redistributions in binary form must reproduce the above copyright notices, this list of
conditions and the following disclaimer in the documentation and/or other materials provided
with the distribution.

  * Neither the name of the University of Cambridge nor the names of any contributors may be
used to endorse or promote products derived from this      software without specific prior
written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND
FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

EXEMPTION FOR BINARY LIBRARY-LIKE PACKAGES

------------------------------------------

The second condition in the BSD licence (covering binary redistributions) does not apply all the
way down a chain of software. If binary package A includes PCRE2, it must respect the condition,
```

```
but if package B is software that includes package A, the condition is not imposed on package B
unless it uses PCRE2 independently.
```

L22. QR Code Gnerator

```
Copyright © 2022 Project Nayuki. (MIT License)

https://www.nayuki.io/page/qr-code-generator-library



Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:



The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.



The Software is provided "as is", without warranty of any kind, express or
implied, including but not limited to the warranties of merchantability,
fitness for a particular purpose and noninfringement. In no event shall the
authors or copyright holders be liable for any claim, damages or other
liability, whether in an action of contract, tort or otherwise, arising from,
out of or in connection with the Software or the use or other dealings in the
Software.
```

L23. quirc

```
quirc -- QR-code recognition library

Copyright (C) 2010-2012 Daniel Beer <dlbeer@gmail.com>



ISC License

===========



Permission to use, copy, modify, and/or distribute this software for

any purpose with or without fee is hereby granted, provided that the
```

```
above copyright notice and this permission notice appear in all

copies.


THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL

WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED

WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE

AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL

DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR

PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER

TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR

PERFORMANCE OF THIS SOFTWARE.
```

L24. Script.aculo.us

```
Copyright © 2005-2008 Thomas Fuchs (http://script.aculo.us, http://mir.aculo.us)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software
and associated documentation files (the "Software"), to deal in the Software without
restriction, including without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the
Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or
substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING
BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM,
DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
```

L25. Zlib

```
zlib.h -- interface of the 'zlib' general purpose compression library

  version 1.2.11, January 15th, 2017

  Copyright (C) 1995-2017 Jean-loup Gailly and Mark Adler

  This software is provided 'as-is', without any express or implied warranty.  In no event will
the authors be held liable for any damages arising from the use of this software.

  Permission is granted to anyone to use this software for any purpose, including commercial
applications, and to alter it and redistribute it freely, subject to the following restrictions:
```

```
  1. The origin of this software must not be misrepresented; you must not claim that you wrote
the original software. If you use this software in a product, an acknowledgment in the product
documentation would be appreciated but is not required.

  2. Altered source versions must be plainly marked as such, and must not be misrepresented as
being the original software.

  3. This notice may not be removed or altered from any source distribution.

  Jean-loup Gailly        Mark Adler

  jloup@gzip.org          madler@alumni.caltech.edu
```

Annexe M. Procédures utilisateur

Cette rubrique contient la description des catégories suivantes des procédures utilisateur :

Procédure	Description
Administrateurs	gestion de l'authentification des administrateurs
Groupe	gestion des groupes
Accès	gestion de l'accès
Autre	divers
Novices	gestion des nouveaux postes
Liaisons	gestion des liaisons entre les Serveurs voisins Dr.Web
Serveur	gestion du Serveur Dr.Web
Connexions	gestion des connexions avec les clients
Postes	gestion des postes
Ldap	transformation des noms utilisateur

M1. Administrateurs

Administrateur authentifié

Appelé en cas d'authentification réussie de l'administrateur dans le Centre de gestion de la sécurité.

Base de données	Paramètres	Valeur retournée
disponible	• `login` : login de l'administrateur, • `address` : adresse réseau depuis laquelle l'administrateur s'est authentifié, • `subsys` : sous-système du Serveur Dr.Web (voir le fichier `adm-subsys.ds`), • `id` : ID de l'administrateur, • `authorizer` : nom du module d'authentification (base de données, LDAP, AD), • `language` : code de la langue du compte d'administrateur, • `date_format` : format de la date du compte d'administrateur	ignoré

Texte de la procédure :

```
--[[
Called:
  when Administrator authorize successfully

Database:
  available

Parameters:
  login              Administrator`s login name
  address            Administrator`s network address
  subsys             Server subsystem (see adm-subsys.ds)
  id                 Administrator`s ID
  authorizer         Authorizer name (database, LDAP, AD)
  language           Administrator`s language code
  date_format        Administrator`s date format

Returned value:
  ignored

]]

local args = ... -- args.login, args.address, args.subsys, args.error, args.id,
args.authorizer,
                 -- args.language, args.date_format
```

L'administrateur est authentifié via Microsoft Active Directory Service

Appelé en cas d'authentification réussie de l'administrateur via Microsoft Active Directory (MSAD).

Base de données	Paramètres	Valeur retournée
disponible	• `login` : login de l'administrateur, • `address` : adresse réseau depuis laquelle l'administrateur s'est authentifié, • `is_secure` : l'administrateur utilise une connexion sécurisée HTTPS (`true` | `false`), • `name` : nom LDAP de l'administrateur, • `DN` : LDAP DN de l'administrateur, • `SID` : identificateur de sécurité Windows (SID) de l'administrateur, • `GUID` : identificateur global unique (GUID) de l'administrateur, • `primary_group` : nom du groupe primaire de l'administrateur, • `primary_group_DN` : LDAP DN du groupe primaire de l'administrateur, • `primary_group_SID` : identificateur de sécurité (SID) du groupe primaire de l'administrateur, • `primary_group_GUID` : identificateur global unique (GUID) du groupe primaire de l'administrateur, • `groups` : tableau contenant les noms du groupe de l'administrateur (inclus dans l'attribut MSAD), • `groups_DN` : tableau contenant les noms DN du groupe de l'administrateur (dans le même ordre que les groupes), • `groups_SID` : tableau contenant les identificateurs de sécurité (SID) du groupe de l'administrateur (dans le même ordre que les groupes), • `groups_GUID` : tableau contenant les identificateur globaux uniques (GUID) du groupe de l'administrateur (dans le même ordre que les groupes)	• `nil` : ne rien faire, • `string` : empty ne rien faire, • `not-empty` : spécifier en tant que groupe d'administrateur le groupe avec ID correspondant à cette ligne

Texte de la procédure :

```
--[[
Called:
  when the external administrator was authorized successfully using Microsoft Active
Directory Service

Database:
  available
```

```
Parameters:
  login              Administrator's login name
  address            Administrator's network address
  is_secure          Is true if administrator uses HTTPS connection
  name               Administrator's LDAP name
  DN                 Administrator's LDAP distinguished name
  SID                Administrator's Windows security identifier
  GUID               Administrator's GUID
  primary_group      Administrator's primary group name
  primary_group_DN   Administrator's primary group LDAP distinguished name
  primary_group_SID  Administrator's primary group SID
  primary_group_GUID Administrator's primary group GUID
  groups             Table containg Administrator's group names (memberOf MSAD
attribute)
  groups_DN          Table containg Administrator's group distinguished names (in the
same order as groups)
  groups_SID         Table containg Administrator's group SIDs (in the same order as
groups)
  groups_GUID        Table containg Administrator's group GUIDs (in the same order as
groups)

Returned value:
             nil        do nothing
  string     empty      do nothing
             not-empty  set administrator group to this string (group ID)

]]

local args = ... -- args.is_secure, args.login, args.address,
                 -- args.name, args.DN, args.SID, args.GUID,
                 -- args.primary_group, args.primary_group_DN, args.primary_group_SID,
args.primary_group_GUID,
                 -- args.groups, args.groups_DN, args.groups_SID, args.groups_GUID
```

Administrateur non authentifié

Appelé en cas d'erreur d'authentification de l'administrateur dans le Centre de gestion de la sécurité.

Base de données	Paramètres	Valeur retournée
disponible	• `login` : login de l'administrateur, • `address` : adresse réseau de l'administrateur, • `subsys` : sous-système du Serveur Dr.Web (voir le fichier adm-subsys.ds), • `error` : code d'erreur (voir le fichier auth-error.ds)	ignoré

Texte de la procédure :

```
--[[
Called:
  when Administrator authorization failed

Database:
  available

Parameters:
  login               Administrator`s login name
  address             Administrator`s network address
  subsys              Server subsystem (see adm-subsys.ds)
  error               Error code (see auth-error.ds)

Returned value:
  ignored

]]

local args = ... -- args.login, args.address, args.subsys, args.error
```

M2. Groupe

Un groupe est créé

Appelé après la création d'un nouveau groupe.

Base de données	Paramètres	Valeur retournée
disponible à moins que la procédure ne soit lancée par la fonction `drwcs.new_group()`	• `login` : login de l'administrateur, • `id` : ID du groupe, • `name` : nom du groupe, • `pid` : ID du groupe parent	ignoré

Texte de la procédure :

```
--[[
Called:
  when new group created

Database:
  available

Parameters:
  login       administrator`s login name
  id          group ID
  name        group name
  pid         parent group ID

Returned value:
  ignored

]]

local args = ... -- args.login, args.id, args.name, args.pid
```

Le groupe a été supprimé

Appelé après la suppression du groupe.

Base de données	Paramètres	Valeur retournée
disponible	• `login` : login de l'administrateur, • `id` : ID du groupe, • `name` : nom du groupe	ignoré

Texte de la procédure :

```
--[[
Called:
  when group deleted

Database:
  available

Parameters:
  login      administrator`s login name
  id         group ID
  name       group name

Returned value:
  ignored

]]

local args = ... -- args.login, args.id, args.name
```

Les propriétés du groupe sont modifiées

Appelé après la modification des propriétés du groupe.

Base de données	Paramètres	Valeur retournée
disponible	• `login` : login de l'administrateur, • `id` : ID du groupe, • `name` : nom du groupe, • `descr` : description du groupe, • `pid` : ID du groupe parent	ignoré

Texte de la procédure :

```
--[[
Called:
  when group properties changed

Database:
  available

Parameters:
  login      administrator`s login name
  id         group ID
  name       group name
  descr      group description
  pid        parent group ID

Returned value:
  ignored

]]

local args = ... -- args.login, args.id, args.name, args.descr, args.pid
```

M3. Accès

L'accès est bloqué

Appelé en cas d'accès bloqué selon les paramètres ACL ou selon le résultat de l'exécution de la procédure `access_check`.

Base de données	Paramètres	Valeur retournée
disponible	• `id` : ID temporaire du client (pour les novices/Serveurs Dr.Web), • `address` : adresse réseau du client, • `station` : nom NetBIOS du client. N'est pas spécifié pour les Serveurs Dr.Web et n'est pas remplacé par le nom DNS, • `type` : « station », « installer », « newbie », « server », « proxy », • `description` : description du poste	ignoré

Texte de la procédure :

```
--[[
Called:
  when access denied according ACLs settings or result
  of 'access_check' procedure

Database:
  available

Parameters:
  id              station (temporary for newbie/server) ID
  address         station network address
  station         station name (undefined for servers)
                  this is NetBIOS station name (not replaced by DNS one)
  type            one of 'station' | 'installer' | 'newbie' | 'server' | 'proxy'
  description     station description

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.type, args.description

-- no return => `nil' value
```

Vérification d'accès

Appelé avant la vérification d'accès selon ACL (Acces Control List - listes de contrôle d'accès).

Base de données	Paramètres	Valeur retournée
disponible	• `id` : ID temporaire du client (pour les novices/Serveurs Dr.Web), • `address` : adresse réseau du client, • `station` : nom NetBIOS du client. N'est pas spécifié pour les Serveurs Dr.Web et n'est pas remplacé par le nom DNS, • `type` : « station », « installer », « newbie », « server », « proxy »	• `nil` : vérifier les adresses avec les ACL spécifiées, • `boolean` : ne pas vérifier les adresses avec ACL, dans tous les cas : ▫ `true` : autoriser l'accès, ▫ `false` : interdire l'accès

Texte de la procédure

```
--[[
Called:
  before check access against appropriate ACL

Database:
  available

Parameters:
  id              station ID (temporary for newbie/server)
  address         station network address
  station         station name (undefined for servers)
                  this is NetBIOS station name (not replaced by DNS one)
  type            one of 'station | installer | newbie | server | proxy'

Returned value:
              nil         check address against configured ACLs
  boolean     true        allow access, do not check agains ACLs
              false       reject access, do not check agains ACLs

Procedure from next set will be called if returned nothing.
]]

local args = ... -- args.id, args.address, args.station, args.type

-- no return => `nil' value
```

M4. Autre

Mise à jour automatique de la clé de licence

Appelé à l'expiration de la clé de licence.

Base de données	Paramètres	Valeur retournée

disponible	• `event` : type de l'événement:
	  ▫ `expire` : la clé de licence va expirer, la mise à jour automatique n'est pas disponible
	  ▫ `diff` : une nouvelle clé de licence est téléchargée mais le contenu des composants soumis à la licence de la clé actuelle est différent de celui de la nouvelle clé. La clé de licence doit être remplacée manuellement
	  ▫ `renew` : la clé de licence a été mise à jour automatiquement
	• `old_key` : contenu de l'ancienne clé de licence
	• `new_key` : contenu de la nouvelle clé de licence. Disponible si le type d'événement est `diff` ou `renew`
		ignoré

Texte de la procédure :

```
--[[
Called:
  when license key expire or have been renewed

Database:
  available

Parameters:
  event       event type: "expire" - license key expires or have done it
                          "diff"   - received new key, but components differs from
current one
                          "renew"  - current key have been renewed, old one was
deleted

  old_key     content of old license key
  new_key     content of renew license key, available at event type "diff" or "renew"

Returned value:
  ignored

]]

local args = ... -- args.event, args.old_key, args.new_key
```

Une épidémie est détectée

Appelé en cas de détection de l'épidémie sur le réseau.

Base de données	Paramètres	Valeur retournée
disponible	• `virus` : la menace la plus répandue, • `total` : nombre total de menaces détectées	ignoré

Texte de la procédure :

```
--[[
Called:
  when virus epidemic has been detected by the server

Database:
  available

Parameters:
  total             total count of viruses
  virus             most frequently detected virus name

Returned value:
  ignored

]]

local args = ... -- args.total, args.virus
```

Rapport du Contrôle des applications

Appelé lors de la réception du rapport du Contrôle des applications depuis le poste.

Base de données	Paramètres	Valeur retournée
disponible	• `id` : ID du poste, • `address` : adresse réseau du poste, • `station` : nom du poste, • `time` : heure de l'événement (heure du poste), • `sid` : SID du poste, • `user` : l'utilisateur qui a lancé un processus ayant une activité suspecte, • `type` : type de l'événement, • `action` : action appliquée, • `policy_type` : type de la politique qui a fonctionné, • `policy_mask` : masque de la politique qui a fonctionné,	ignoré

Base de données	Paramètres	Valeur retournée
	• `test_mode` : l'événement s'est produit en mode test, • `profile_id` : UUID du profil par lequel le blocage a été fait, • `profile_name` : nom du profil par lequel le blocage a été fait, • `rule_id` : UUID de la règle par laquelle le blocage a été fait (si existe), • `rule_name` : nom de la règle par laquelle le blocage a été fait (si existe), • `process_path` : chemin d'accès au processus bloqué, • `process_file_sha256` : SHA-256 du ficher de processus, • `process_file_version` : version du fichier de processus, • `process_file_description` : description du fichier de processus, • `process_file_origname` : nom d'origine du fichier de processus, • `process_file_prodname` : nom du produit du fichier de processus, • `process_file_prodver` : version du produit du fichier de processus, • `process_file_company` : nom de l'entreprise du fichier de processus, • `process_cert_thumbprint` : empreinte du certificat (SHA-1) avec lequel le processus est signé (si existe), • `process_cert_serial` : numéro de série du certificat avec lequel le processus est signé (si existe) • `process_cert_issuer` : éditeur du certificat avec lequel le processus est signé (si existe), • `process_cert_subject` : sujet du certificat avec lequel le processus est signé (si existe), • `process_cert_timestamp` : heure de délivrance du certificat avec lequel le processus est signé (si existe), • `process_cert_not_before` : heure de la mise en place du certificat avec lequel le processus est signé (si existe), • `process_cert_not_after` : heure d'expiration du certificat avec lequel le processus est signé (si existe),	

Base de données	Paramètres	Valeur retournée
	• `process_hashdb` : bulletin contenant le hash du fichier de processus, • `object_path` : chemin ver le script bloqué ou valeur vide, • `object_file_sha256` : SHA-256 du ficher de script (si existe), • `object_file_version` : version du fichier de script (si existe), • `object_file_description` : description du fichier de script (si existe), • `object_file_origname` : nom d'origine du ficher de script (si existe), • `object_file_prodname` : nom du produit du ficher de script (si existe), • `object_file_prodver` : version du produit du fichier de script (si existe), • `object_file_company` : nom d'entreprise du ficher de script (si existe), • `object_cert_thumbprint` : empreinte du certificat (SHA-1) avec lequel le script est signé (si existe), • `object_cert_serial` : numéro de série du certificat avec lequel le script est signé (si existe), • `object_cert_issuer` : éditeur du certificat avec lequel le script est signé (s'il existe) • `object_cert_subject` : sujet du certificat avec lequel le script est signé (si existe), • `object_cert_timestamp` : heure de délivrance du certificat avec lequel le script est signé (si existe), • `object_cert_not_before` : heure de la mise en place du certificat avec lequel le script est signé (si existe), • `object_cert_not_after` : heure d'expiration du certificat avec lequel le script est signé (si existe), • `object_hashdb` : bulletin contenant le hash du fichier de script	

Texte de la procédure :

```
--[[
Called:
  when application control event received from Agent
```

```
Database:
  available

Parameters:
  id                  station ID
  address             station address
  station             station name
  time                station time
  sid                 SID of user initiated activity
  user                name of user initiated activity
  type                event type
  action              applied action
  policy_type         matched policy type
  policy_mask         matched policy mask
  test_mode           event occured in test mode
  profile_id          profile UUID used for activity blocking
  profile_name        profile name used for activity blocking
  rule_id             rule UUID used for activity blocking (if exist)
  rule_name           rule name used for activity blocking (if exist)

  process_path                path to affected process file
  process_file_sha256         process file SHA-256
  process_file_version        process file version
  process_file_description    process file description
  process_file_origname       process file original name
  process_file_prodname       process file product name
  process_file_prodver        process file product version
  process_file_company        process file company name
  process_cert_thumbprint     process file signing certificate thumbprint (SHA-1) (if
exist)
  process_cert_serial         process file signing certificate serial number (if exist)
  process_cert_issuer         process file signing certificate issuer (if exist)
  process_cert_subject        process file signing certificate subject (if exist)
  process_cert_timestamp      process file signing certificate sign issuance timestamp
(if exist)
  process_cert_not_before     process file signing certificate NotBefore timestamp (if
exist)
  process_cert_not_after      process file signing certificate NotAfter timestamp (if
exist)
  process_hashdb              hash database containing process file

  object_path                 path to affected object file (script, etc) or empty
  object_file_sha256          object file SHA-256 (if exist)
  object_file_version         object file version (if exist)
  object_file_description     object file description (if exist)
  object_file_origname        object file original name (if exist)
  object_file_prodname        object file product name (if exist)
  object_file_prodver         object file product version (if exist)
  object_file_company         object file company name (if exist)
  object_cert_thumbprint      object file signing certificate thumbprint (SHA-1) (if
exist)
  object_cert_serial          object file signing certificate serial number (if exist)
  object_cert_issuer          object file signing certificate issuer (if exist)
  object_cert_subject         object file signing certificate subject (if exist)
  object_cert_timestamp       object file signing certificate sign issuance timestamp
(if exist)
  object_cert_not_before      object file signing certificate NotBefore timestamp (if
exist)
  object_cert_not_after       object file signing certificate NotAfter timestamp (if
exist)
  object_hashdb               hash database containing object file

Returned value:
  ignored

]]
```

```
local args = ...
```

Rapport du Contrôle des applications du Serveur voisin

Appelé lors de la réception par le poste du rapport du Contrôle des applications depuis le Serveur Dr.Web voisin.

Base de données	Paramètres	Valeur retournée
disponible	• `neighborid` : ID du Serveur Dr.Web voisin depuis lequel l'événement est reçu, • `neighborname` : nom du Serveur Dr.Web voisin, • `originatorid` : ID du Serveur Dr.Web source de l'événement, • `originatorname` : nom du Serveur Dr.Web source de l'événement, • `stationid` : ID du poste, • `stationname` : nom du poste, • `eventid` : ID de l'événement, • `event_time` : l'heure de l'apparition de l'événement sur le poste, • `sid` : SID du poste, • `user` : l'utilisateur qui a lancé un processus ayant une activité suspecte, • `type` : type de l'événement, • `action` : action appliquée, • `policy_type` : type de la politique qui a fonctionné, • `policy_mask` : masque de la politique qui a fonctionné, • `test_mode` : l'événement s'est produit en mode test, • `profile_id` : UUID du profil par lequel le blocage a été fait, • `profile_name` : nom du profil par lequel le blocage a été fait, • `rule_id` : UUID de la règle par laquelle le blocage a été fait (si existe), • `rule_name` : nom de la règle par laquelle le blocage a été fait (si existe), • `process_path` : chemin d'accès au processus bloqué,	ignoré

Base de données	Paramètres	Valeur retournée
	• `process_file_sha256` : SHA-256 du ficher de processus, • `process_file_version` : version du fichier de processus, • `process_file_description` : description du fichier de processus, • `process_file_orignаme` : nom d'origine du fichier de processus, • `process_file_prodname` : nom du produit du fichier de processus, • `process_file_prodver` : version du produit du fichier de processus, • `process_file_company` : nom de l'entreprise du fichier de processus, • `process_cert_thumbprint` : empreinte du certificat (SHA-1) avec lequel le processus est signé (si existe), • `process_cert_serial` : numéro de série du certificat avec lequel le processus est signé (si existe), • `process_cert_issuer` : éditeur du certificat avec lequel le processus est signé (si existe), • `process_cert_subject` : sujet du certificat avec lequel le processus est signé (si existe), • `process_cert_timestamp` : heure de délivrance du certificat avec lequel le processus est signé (si existe), • `process_cert_not_before` : heure de la mise en place du certificat avec lequel le processus est signé (si existe), • `process_cert_not_after` : heure d'expiration du certificat avec lequel le processus est signé (si existe), • `process_hashdb` : bulletin contenant le hash du fichier de processus, • `object_path` : chemin ver le script bloqué ou valeur vide, • `object_file_sha256` : SHA-256 du ficher de script (si existe), • `object_file_version` : version du fichier de script (si existe), • `object_file_description` : description du fichier de script (si existe),	

Base de données	Paramètres	Valeur retournée
	• `object_file_origname` : nom d'origine du ficher de script (si existe), • `object_file_prodname` : nom du produit du ficher de script (si existe), • `object_file_prodver` : version du produit du fichier de script (si existe), • `object_file_company` : nom d'entreprise du ficher de script (si existe), • `object_cert_thumbprint` : empreinte du certificat (SHA-1) avec lequel le script est signé (si existe), • `object_cert_serial` : numéro de série du certificat avec lequel le script est signé (si existe), • `object_cert_issuer` : éditeur du certificat avec lequel le script est signé (s'il existe) • `object_cert_subject` : sujet du certificat avec lequel le script est signé (si existe), • `object_cert_timestamp` : heure de délivrance du certificat avec lequel le script est signé (si existe), • `object_cert_not_before` : heure de la mise en place du certificat avec lequel le script est signé (si existe), • `object_cert_not_after` : heure d'expiration du certificat avec lequel le script est signé (si existe), • `object_hashdb` : bulletin contenant le hash du fichier de script	

Texte de la procédure :

```
--[[
Called:
  when application control event received from neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  event_time          station time
  recv_time           server originator time
  sid                 SID of user initiated activity
  user                name of user initiated activity
```

```
  type                event type
  action              applied action
  policy_type         matched policy type
  policy_mask         matched policy mask
  test_mode           event occured in test mode
  profile_id          profile UUID used for activity blocking
  profile_name        profile name used for activity blocking
  rule_id             rule UUID used for activity blocking (if exist)
  rule_name           rule name used for activity blocking (if exist)

  process_path                path to affected process file
  process_file_sha256         process file SHA-256
  process_file_version        process file version
  process_file_description    process file description
  process_file_origname       process file original name
  process_file_prodname       process file product name
  process_file_prodver        process file product version
  process_file_company        process file company name
  process_cert_thumbprint     process file signing certificate thumbprint (SHA-1) (if
exist)
  process_cert_serial         process file signing certificate serial number (if exist)
  process_cert_issuer         process file signing certificate issuer (if exist)
  process_cert_subject        process file signing certificate subject (if exist)
  process_cert_timestamp      process file signing certificate sign issuance timestamp
(if exist)
  process_cert_not_before     process file signing certificate NotBefore timestamp (if
exist)
  process_cert_not_after      process file signing certificate NotAfter timestamp (if
exist)
  process_hashdb              hash database containing process file

  object_path                 path to affected object file (script, etc) or empty
  object_file_sha256          object file SHA-256 (if exist)
  object_file_version         object file version (if exist)
  object_file_description     object file description (if exist)
  object_file_origname        object file original name (if exist)
  object_file_prodname        object file product name (if exist)
  object_file_prodver         object file product version (if exist)
  object_file_company         object file company name (if exist)
  object_cert_thumbprint      object file signing certificate thumbprint (SHA-1) (if
exist)
  object_cert_serial          object file signing certificate serial number (if exist)
  object_cert_issuer          object file signing certificate issuer (if exist)
  object_cert_subject         object file signing certificate subject (if exist)
  object_cert_timestamp       object file signing certificate sign issuance timestamp
(if exist)
  object_cert_not_before      object file signing certificate NotBefore timestamp (if
exist)
  object_cert_not_after       object file signing certificate NotAfter timestamp (if
exist)
  object_hashdb               hash database containing object file

Returned value:
  ignored

]]

local args = ...
```

Le Serveur proxy Dr.Web est créé

Appelé à la fin de la création du Serveur proxy Dr.Web.

Base de données	Paramètres	Valeur retournée
disponible	• `login` : login de l'administrateur, • `id` : ID du Serveur proxy Dr.Web, • `name` : nom du Serveur proxy Dr.Web, • `state` : statut de la fin de l'opération: ▫ `0` :créé avec succès, ▫ `1` : erreur lors de l'exécution de l'opération (erreur de la base de données), ▫ `2` : le délai d'attente de l'opération s'est écoulé (la base de données est surchargée), ▫ `4` : Le Serveur proxy Dr.Web existe déjà	ignoré

Texte de la procédure :

```
--[[
Called:
  when proxy create completed

Database:
  available

Parameters:
  login         administrator`s login name
  id            proxy ID
  name          proxy name
  state         operation completion state:
                  0  created successfully
                  1  operation failed (database error)
                  2  operation timed out (database overloaded)
                  4  already exists

Returned value:
  ignored

]]

local args = ... -- args.login, args.id, args.name, args.state
```

Le Serveur proxy Dr.Web est supprimé

Appelé lors de la suppression du Serveur proxy Dr.Web.

Base de données	Paramètres	Valeur retournée
disponible	• `login` : login de l'administrateur, • `id` : ID du Serveur proxy Dr.Web, • `name` : nom du Serveur proxy Dr.Web,	ignoré

Texte de la procédure :

```
--[[
Called:
  when proxy deleted

Database:
  available

Parameters:
  login     administrator`s login name
  id        proxy id
  name      proxy name

Returned value:
  ignored

]]

local args = ... -- args.login, args.id, args.name
```

M5. Novices

Le novice est enregistré

Après que l'accès est fourni à un novice mais avant que les informations appropriées sont enregistrées dans la base de données.

Base de données	Paramètres	Valeur retournée
disponible	• `id` : ID du poste temporaire/permanent • `address` : adresse réseau du poste, • `station` : nom du poste, • `existing` : confirmer pour le poste existant	ignoré

Texte de la procédure :

```
--[[
Database:
  available

Called:
  when newbie access granted but before information stored in database

Parameters:
  id              station temporary/permanent ID
  address         station network address
  station         station name
  existing        approved using existing station

Returned value:
  ignored
```

```
]]

local args = ... -- args.id, args.address, args.station
```

Le novice se connecte au Serveur Dr.Web

Appelé lorsqu'un novice se connecte au Serveur Dr.Web.

Base de données	Paramètres	Valeur retournée
disponible	• `id` : ID du poste temporaire, • `address` : adresse réseau du poste, • `station` : nom du poste, • `description` : description du poste (uniquement pour les clients sous Windows), • `ldapdn` : LDAP DN du poste (uniquement pour les clients sous Windows), • `sid` : SID du poste, • `mac` : adresse MAC du poste,	• `nil` : utiliser les paramètres par défaut comme dans le cas de fonctionnement standard du Serveur Dr.Web, • `boolean` : action du Serveur Dr.Web : ▫ `true` : demander l'approbation manuelle (similaire à `Newbie approval`), ▫ `false` : interdire l'accès (similaire à `Newbie closed`), • `string` : groupe primaire lors de l'approbation: ▫ `empty` : approuver, spécifier le groupe `Everyone` comme primaire (similaire à `Newbie open`), ▫ `not-empty` : approuver l'accès et spécifier comme primaire le groupe dont l'ID correspond à

Base de données	Paramètres	Valeur retournée
		la ligne donnée. Attention ! L'existence de cette ID sera vérifiée et, si l'ID n'existe pas, le groupe `Everyone` sera spécifié comme primaire, • `vector` : approuver par défaut, contient les commandes suivantes et les arguments non obligatoires: ▫ `pgroup` : spécifier le groupe primaire, ensuite vient l'ID de groupe, ▫ `rate` : spécifier le groupe de tarif, ensuite vient l'ID de groupe de tarif, ▫ `id` : spécifier l'ID du poste, ensuite vient l'ID du poste ▫ approve : demander l'approbation manuelle au lieu de l'approbation automatique, ▫ `into` : approuver dans le poste existant, ensuite vient l'ID du poste existant

Texte de la procédure :

```
--[[
Called:
  when newbie connected

Database:
  available

Parameters:
  id              station temporary ID
  address         station network address
  station         station name
  description     station description (Windows client only)
  ldapdn          station LDAP DN (Windows client only)
  sid             station computer SID
  mac             station computer MAC

Returned value:
              nil         default, standard server operation according settings
  boolean     true        request approval (like 'Newbie approval' does)
              false       reject access (like 'Newbie closed' does)
  string      empty       accept, set primary group to 'Everyone'
                            (like 'Newbie open' does)
              not-empty   accept, set primary group to this string (ID) (substring after
space treated as rate group id)
                          Attention! Existence of This ID will be checked and
                          if it does not exist it will be replaced by `Everyone'
  vector                  accept by default, must contain commands and optional
arguments:
                          "pgroup"  - set primary group, must be followed by group id
                          "rate"    - set rate group, must be followed by rate group id
                          "id"      - set station id, must be followed by station id
                          "approve" - request approval instead of accepting
                          "into"    - accept into existing station, must be followed by
existing station id


Procedure from next set will be called if returned nothing.
]]

local args = ... -- args.id, args.address, args.station

-- place my station (named ADMINISTRATOR) into `Everyone' group ignoring newbie policy
and newbie's preference
if string.upper( args.station ) == 'ADMINISTRATOR' then
  return ''
end

-- set new UUID for any station with this id and request for manual approve, useful
for cloned stations
if args.id == '01234567-89ab-cdef-0123-456789abcdef' then
  return { "id", dwcore.get_uuid(), "approve" }
end

-- no return => `nil' value => according server settings
```

Le novice est approuvé

Appelé si l'accès est fourni à un novice et que son authentification est réussie et un poste est créé dans la base de données.

Base de données	Paramètres	Valeur retournée
disponible	• `id` : ID du poste temporaire, • `address` : adresse réseau du poste, • `station` : nom du poste, • `compsid` : SID du poste, • `compmac` : adresse MAC du poste, • `description` : description du poste	ignoré

Texte de la procédure :

```
--[[
Called:
  when newbie access granted, authorization is successfull
  and station created in database

Database:
  available

Parameters:
  id              station temporary ID
  address         station network address
  station         station name
  compsid         station UID (SID on Windows)
  compmac         station MAC address
  description     station description

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.compsid, args.compmac,
args.description
```

M6. Liaisons

Arrêt d'un composant sur le poste du Serveur Dr.Web voisin

Appelé lorsque l'événement `component completed` est reçu du Serveur Dr.Web voisin.

Base de données	Paramètres	Valeur retournée
disponible	• `neighborid` : ID du Serveur Dr.Web voisin depuis lequel l'événement est reçu, • `neighborname` : nom du Serveur Dr.Web voisin, • `originatorid` : ID du Serveur Dr.Web source de l'événement,	ignoré

Base de données	Paramètres	Valeur retournée
	• `originatorname` : nom du Serveur Dr.Web source de l'événement, • `stationid` : ID du poste, • `stationname` : nom du poste, • `eventid` : ID de l'événement, • `component` : numéro du composant, • `pid` : ID du processus, • `infections` : menaces détectées, • `errors` : erreurs d'accès détectées, • `exitcode` : code de fin du composant, • `time` : heure de la fin (heure du poste)	

Texte de la procédure :

```
--[[
Called:
  when "component completed" event recived from neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  component           component number
  pid                 process ID
  infections          infections found
  errors              access errors detected
  exitcode            component exit code
  time                end time (station time)

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname,
                 -- args.originatorid, args.originatorname,
                 -- args.eventid, args.stationid,
                 -- args.stationname, args.time
                 -- args.component, args.pid, args.infections
                 -- args.errors, args.exitcode
```

Lancement d'un composant sur le poste du Serveur voisin Dr.Web

Appelé lorsque l'événement `component started` est reçu du Serveur voisin Dr.Web.

Base de données	Paramètres	Valeur retournée
disponible	• `neighborid` : ID du Serveur Dr.Web voisin depuis lequel l'événement est reçu, • `neighborname` : nom du Serveur Dr.Web voisin, • `originatorid` : ID du Serveur Dr.Web source de l'événement, • `originatorname` : nom du Serveur Dr.Web source de l'événement, • `stationid` : ID du poste, • `stationname` : nom du poste, • `eventid` : ID de l'événement, • `component` : numéro du composant, • `pid` : ID du processus, • `engine` : version du moteur de recherche, • `records` : total d'entrées virales, • `user` : nom de l'utilisateur et groupe du propriétaire du processus, • `time` : heure du début (heure du poste)	ignoré

Texte de la procédure :

```
--[[
Called:
  when "component started" event recived from neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  component           component number
  pid                 process ID
  engine              virus-finding engine version
  records             virus records number
  user                user name and group (process owner)
  time                start time (station time)

Returned value:
  ignored

]]
```

```
local args = ... -- args.neighborid, args.neighborname,
                 -- args.originatorid, args.originatorname,
                 -- args.eventid, args.stationid,
                 -- args.stationname,
                 -- args.component, args.pid, args.engine
                 -- args.records, args.user, args.time
```

Les coordonnées du Serveur Dr.Web voisin ou du poste du Serveur Dr.Web voisin sont changées

Appelé lorsque l'événement `geolocation` est reçu du Serveur voisin Dr.Web.

Base de données	Paramètres	Valeur retournée
disponible	• `neighborid` : ID du Serveur Dr.Web voisin depuis lequel l'événement est reçu, • `neighborname` : nom du Serveur Dr.Web voisin, • `originatorid` : ID du Serveur Dr.Web source de l'événement, • `originatorname` : nom du Serveur Dr.Web source de l'événement, • `stationid` : ID du poste, • `stationname` : nom du poste, • `latitude` : latitude au format DD.DDDDDD, • `longitude` : longitude au format DD.DDDDDD	ignoré

Texte de la procédure :

```
--[[
Called:
  when "geolocation" event received from neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  latitude            latitude in DD.DDDDDD format
  longitude           longitude in DD.DDDDDD format

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname,
```

```
                -- args.originatorid, args.originatorname,
                -- args.eventid, args.stationid,
                -- args.stationname,
                -- args.latidue,args.longitude
                -- ...
```

Le matériel et les logiciels du serveur voisin sont modifiés

Appelé lorsque l'événement `environment changed` est reçu du Serveur voisin Dr.Web.

Base de données	Paramètres	Valeur retournée
disponible	• `neighborid` : ID du Serveur Dr.Web voisin depuis lequel l'événement est reçu, • `neighborname` : nom du Serveur Dr.Web voisin, • `originatorid` : ID du Serveur Dr.Web source de l'événement, • `originatorname` : nom du Serveur Dr.Web source de l'événement, • `stationid` : ID du poste, • `stationname` : nom du poste, • `eventid` : ID de l'événement, • `group_name` : nom du groupe primaire du poste, • `category` : catégorie de l'objet d'environnement	ignoré

Texte de la procédure :

```
--[[
Called:
  when "environment changed" event recived from neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  group_name          station primary group name
  category            environment category

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname,
                 -- args.originatorid, args.originatorname,
```

```
                -- args.eventid, args.stationid,args.stationname,
                -- args.group_name, args.category
```

Une menace est détectée sur le poste du Serveur Dr.Web voisin

Appelé lorsque l'événement `virus detected` est reçu du Serveur voisin Dr.Web.

Base de données	Paramètres	Valeur retournée
disponible	• `neighborid` : ID du Serveur Dr.Web voisin depuis lequel l'événement est reçu, • `neighborname` : nom du Serveur Dr.Web voisin, • `originatorid` : ID du Serveur Dr.Web source de l'événement, • `originatorname` : nom du Serveur Dr.Web source de l'événement, • `stationid` : ID du poste, • `stationname` : nom du poste, • `eventid` : ID de l'événement, • `component` : numéro du composant, • `pid` : ID du processus, • `time` : heure de l'événement (heure du poste), • `user` : nom de l'utilisateur et groupe du propriétaire du processus, • `object` : chemin d'accès au fichier dans le système de fichiers, • `owner` : nom d'utilisateur et groupe du propriétaire de l'objet, • `action` : code d'action, • `objecttype` : type d'objet: ▫ `-1` inconnu ▫ `0` fichier ▫ `1` :secteur d'amorçage, ▫ `2` bloc de mémoire ou processus ▫ `3` activité virale • `infectiontype` : type de menace (voir Dr.Web API), • `sha1` : hash SHA-1 de l'objet trouvé, • `sha256` : hash SHA-256 de l'objet détecté, • `hashdb` : bulletin contenant le hash	ignoré

Texte de la procédure :

```
--[[
Called:
  when "" event recived from neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  component           component number
  pid                 process ID
  time                event time (station time)
  user                user name and group (process owner)
  object              filesystem object path
  owner               object owner (user name and group)
  action              action code (see Dr.Web API; only errors bit set)
  objecttype          object type
                        -1    unknown
                         0    file
                         1    boot sector
                         2    memory block / process
                         3    virus like activity
  infectiontype       infection type (see Dr.Web API)
  sha1                object SHA-1 hash
  sha256              object SHA-256 hash
  hashdb              hash database containing object

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname,
                 -- args.originatorid, args.originatorname,
                 -- args.eventid, args.stationid,
                 -- args.stationname,
                 -- args.component, args.pid, args.time, args.user,
                 -- args.object, args.owner,
                 -- args.action, args.objecttype, args.infectiontype,
                 -- args.sha1, args.sha256, args.hashdb
```

Rapport de la Protection préventive du Serveur voisin

Appelé lors de la réception du rapport de la Protection préventive pour le poste depuis le Serveur voisin Dr.Web.

Base de données	Paramètres	Valeur retournée
disponible	• `neighborid` : ID du Serveur Dr.Web voisin depuis lequel l'événement est reçu,	ignoré

Base de données	Paramètres	Valeur retournée
	• `neighborname` : nom du Serveur Dr.Web voisin, • `originatorid` : ID du Serveur Dr.Web source de l'événement, • `originatorname` : nom du Serveur Dr.Web source de l'événement, • `stationid` : ID du poste, • `stationname` : nom du poste, • `eventid` : ID de l'événement, • `pid` : ID du processus, • `path` : chemin d'accès au fichier exécutable du processus ayant une activité suspecte • `target_path` : chemin d'accès à l'objet protégé auquel une tentative d'accès a été faite, • `hips_type` : type de l'objet protégé (valeur numérique), • `shell_guard_type` : raison de blocage du code non autorisé (valeur numérique), • `denied` : l'accès a été interdit (true | false), • `is_user_action` : l'action a été demandée auprès de l'utilisateur (`true` | `false`), • `event_count` : nombre d'événements interdits automatiquement (uniquement si la valeur `false` est spécifiée pour `is_user_action`), • `event_user` : l'utilisateur qui a lancé un processus ayant une activité suspecte • `action_user` : l'utilisateur qui a spécifié la réaction à l'activité suspecte du processus (seulement si la valeur `true` est spécifiée pour `is_user_action`), • `event_time` : l'heure de l'apparition de l'événement sur le poste, • `recv_time` : délai de réception du rapport par le Serveur Dr.Web voisin • `sha1` : hash SHA-1 de l'objet trouvé, • `sha256` : hash SHA-256 de l'objet détecté, • `hashdb` : bulletin contenant le hash	

Texte de la procédure :

```
--[[
```

```
Called:
  when HIPS event received from neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  pid                 numeric,process id
  path                process file path
  target_path         affected resource path
  hips_type           numeric, HIPS type
  shell_guard_type    numeric, Shell Guard event type
  denied              boolean, access was denied
  is_user_action      boolean, user was asked
  event_count         event number (for accumulation period - if is_user_action is
false)
  event_user          user which initiated the suspicious activity
  action_user         user which allowed or denied the activity (non-empty only if
is_user_action is true)
  event_time          station time
  recv_time           server originator time
  sha1                process file SHA-1 hash
  sha256              process file SHA-256 hash
  hashdb              hash database containing process file

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname, args.originatorid,
args.originatorname,
                 -- args.stationid, args.stationname, args.eventid
                 -- args.pid, args.path, args.target_path, args.hips_type,
args.shell_guard_type,
                 -- args.denied, args.is_user_action, args.event_count,
args.event_user, args.action_user
                 -- args.event_time, args.recv_time, args.sha1, args.sha256,
args.hashdb
```

Erreur d'authentification sur le Serveur Dr.Web voisin

Appelé après le refus de connexion au Serveur voisin Dr.Web à cause d'une erreur d'authentification.

Base de données	Paramètres	Valeur retournée
disponible	• `id` : ID du Serveur Dr.Web, • `address` : adresse du Serveur Dr.Web, • `name` : nom du Serveur Dr.Web • `reason` : cause de l'échec	ignoré

Texte de la procédure :

```
--[[
Called:
  just after server connection rejected due (authorization) error

Database:
  available

Parameters:
  id          server ID
  address     server address
  name        server name
  reason      failure reason

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.name, args.reason
```

Erreur de scan sur le poste du Serveur Dr.Web voisin

Appelé lorsque l'événement `scan error` est reçu du Serveur voisin Dr.Web

Base de données	Paramètres	Valeur retournée
disponible	• `neighborid` : ID du Serveur Dr.Web voisin depuis lequel l'événement est reçu, • `neighborname` : nom du Serveur Dr.Web voisin, • `originatorid` : ID du Serveur Dr.Web source de l'événement, • `originatorname` : nom du Serveur Dr.Web source de l'événement, • `stationid` : ID du poste, • `stationname` : nom du poste, • `eventid` : ID de l'événement, • `component` : numéro du composant, • `pid` : ID du processus, • `time` : heure de l'événement (heure du poste), • `user` : nom de l'utilisateur et groupe du propriétaire du processus, • `object` : chemin d'accès au fichier dans le système de fichiers, • `owner` : nom d'utilisateur et groupe du propriétaire de l'objet,	ignoré

Base de données	Paramètres	Valeur retournée
	• `action` : code d'action, • `sha1` : hash SHA-1 de l'objet trouvé, • `sha256` : hash SHA-256 de l'objet détecté, • `hashdb` : bulletin contenant le hash	

Texte de la procédure :

```
--[[
Called:
  when "" event recived from neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  component           component number
  pid                 process ID
  time                event time (station time)
  user                user name and group (process owner)
  object              filesystem object path
  owner               object owner (user name and group)
  action              action code (error bit(s) set)
  sha1                object SHA-1 hash
  sha256              object SHA-256 hash
  hashdb              hash database containing object

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname,
                 -- args.originatorid, args.originatorname,
                 -- args.eventid, args.stationid,
                 -- args.stationname,
                 -- args.component, args.pid, args.time, args.user,
                 -- args.object, args.owner, args.action,
                 -- args.sha1, args.sha256, args.hashdb
```

Le Serveur Dr.Web voisin est connecté

Appelé lors de la connexion au Serveur voisin Dr.Web.

Base de données	Paramètres	Valeur retournée
disponible	• `id` : ID du Serveur Dr.Web, • `address` : adresse du Serveur Dr.Web, • `name` : nom du Serveur Dr.Web	ignoré

Texte de la procédure :

```
--[[
Called:
  when server connected

Database:
  available

Parameters:
  id          server ID
  address     server address
  name        server name

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.name
```

Statut du poste du Serveur Dr.Web voisin

Appelé lorsque le Serveur Dr.Web voisin communique le statut du poste y compris le statut des composants et des bases virales ainsi que certaines politiques locales (l'envoi des événements, la réception des mises à jour et des tâches)

Base de données	Paramètres	Valeur retournée
disponible	• `neighborid` : ID du Serveur Dr.Web voisin depuis lequel l'événement est reçu, • `neighborname` : nom du Serveur Dr.Web voisin, • `originatorid` : ID du Serveur Dr.Web source de l'événement, • `originatorname` : nom du Serveur Dr.Web source de l'événement, • `stationid` : ID du poste, • `stationname` : nom du poste, • `eventid` : ID de l'événement, • `count` : nombre de codes de statut différents	ignoré

Base de données	Paramètres	Valeur retournée
	• state_0 : valeur du statut, • number_0 : nombre de postes dans state_0	

Texte de la procédure :

```
--[[
Called:
  when "" event recived from neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  count               number of different status code
  state_0             state value
  number_0            number of the stations in 'state_0'

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname,
                 -- args.originatorid, args.originatorname,
                 -- args.eventid, args.stationid,
                 -- args.stationname,
                 -- args.count,
                 -- args.state_0, args.number_0
                 -- args.state_1, args.number_1
                 -- ...
```

Le poste du Serveur Dr.Web voisin a été supprimé

Appelé lors de la suppression du poste sur le Serveur voisin Dr.Web

Base de données	Paramètres	Valeur retournée
disponible	• neighborid : ID du Serveur Dr.Web voisin depuis lequel l'événement est reçu, • neighborname : nom du Serveur Dr.Web voisin, • originatorid : ID du Serveur Dr.Web source de l'événement,	ignoré

Base de données	Paramètres	Valeur retournée
	• originatorname : nom du Serveur Dr.Web source de l'événement, • stationid : ID du poste, • stationname : nom du poste	

Texte de la procédure :

```
--[[
Called:
  when station was deleted on neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname,
                 -- args.originatorid, args.originatorname,
                 -- args.eventid, args.stationid,
                 -- args.stationname
                 -- ...
```

Statistiques de scan du poste du Serveur Dr.Web voisin

Appelé lorsque l'événement scan statistics est reçu du Serveur voisin Dr.Web.

Base de données	Paramètres	Valeur retournée
disponible	• neighborid : ID du Serveur Dr.Web voisin depuis lequel l'événement est reçu, • neighborname : nom du Serveur Dr.Web voisin, • originatorid : ID du Serveur Dr.Web source de l'événement, • originatorname : nom du Serveur Dr.Web source de l'événement, • stationid : ID du poste,	ignoré

Base de données	Paramètres	Valeur retournée
	• `stationname` : nom du poste, • `eventid` : ID de l'événement, • `component` : numéro du composant, • `pid` : ID du processus, • `user` : nom de l'utilisateur et groupe du propriétaire du processus, • `time` : heure de l'événement (heure du poste), • `size` : taille sommaire de tous les objets scannés, • `elapsedtime` : temps écoulé, • `scanned` : nombre d'objets scannés, • `infected` : nombre d'objets contaminés par un virus connu, • `modifications` : nombre d'objets contaminés par une modification de virus, • `suspicious` : nombre de fichiers suspects, • `cured` : nombre de fichiers désinfectés, • `deleted` : nombre de fichiers supprimés, • `renamed` : nombre de fichiers renommés, • `moved` : nombre des fichiers déplacés en quarantaine, • `locked` : nombre de fichiers bloqués (uniquement par SpIDer Guard), • `errors` : nombre des fichiers non scannés à cause d'une erreur d'accès	

Texte de la procédure :

```
--[[
Called:
  when "scan statistics" event received from neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  component           number of component
  pid                 process ID
  user                user name and group (process owner)
```

```
  time                event time (station time)
  size                summary size of all scanned objects
  elapsedtime         elapsed time
  scanned             number of scanned objects
  infected            number of objects infected by known virus
  modifications       number of objects infected by virus modification
  suspicious          number of suspicious objects
  cured               number of cured files
  deleted             number of deleted files
  renamed             number of renamed files
  moved               number of quarantined files
  locked              number of locked files (SpIDer Guard only)
  errors              number of not scanned files (due access error)

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname,
                 -- args.originatorid, args.originatorname,
                 -- args.eventid, args.stationid,
                 -- args.stationname,
                 -- args.component, args.pid, args.time, args.user,
                 -- args.scanned, args.infected, args.modifications,
                 -- args.suspicious, args.cured, args.deleted, args.renamed,
                 -- args.moved, args.locked, args.errors, args.size, args.elapsedtime
```

Installation de l'Agent depuis le Serveur voisin Dr.Web

Appelé lorsque l'événement `installation` est reçu du Serveur voisin Dr.Web.

Base de données	Paramètres	Valeur retournée

disponible	• `neighborid` : ID du Serveur Dr.Web voisin depuis lequel l'événement est reçu,
	• `neighborname` : nom du Serveur Dr.Web voisin,
	• `originatorid` : ID du Serveur Dr.Web source de l'événement,
	• `originatorname` : nom du Serveur Dr.Web source de l'événement,
	• `stationid` : ID du poste,
	• `stationname` : nom du poste,
	• `eventid` : ID de l'événement,
	• `event` : type de l'événement:
	  ▫ `0` : installation en cours,
	  ▫ `1` : l'installation est terminée avec succès,
	  ▫ `2` : refusé,
	  ▫ `3` :délai expiré,
	  ▫ `4` : échoué,
		ignoré

Base de données	Paramètres	Valeur retournée
	▫ `5` : inaccompli • `message` : message d'erreur (ou message vide si aucune erreur n'est survenue), • `address` : adresse du poste, • `begtime` : heure du début, • `endtime` : heure de la fin	

Texte de la procédure :

```
--[[
Called:
  when "installation" event recived from neighbor server

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  event               event type:
                        0   installation begin
                        1   successully completed
                        2   rejected
                        3   timed out
                        4   failed
                        5   incomplete
  message             error message (or empty if there is no error)
  address             station address
  begtime             begin time
  endtime             end time

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname,
                 -- args.originatorid, args.originatorname,
                 -- args.eventid, args.stationid,
                 -- args.stationname,
                 -- args.event, args.message, args.address
                 -- args.begtime, args.endtime
```

M7. Serveur

Le fichier binaire du Serveur Dr.Web a été téléchargé

Appelé après le chargement du fichier binaire de Serveur Dr.Web pour réaliser certaines fonctions de service (le Serveur Dr.Web ne servira pas les clients).

Base de données	Paramètres	Valeur retournée
indisponible	non	ignoré

Texte de la procédure :

```
--[[
Called:
  when server binary file loaded for execute some service function
  (the server will not serve clients)

Database:
  NOT available

Parameters:
  none

Returned value:
  ignored

]]
```

La vérification de la BD est terminée

Appelé après la fin de la vérification de la base de données.

Base de données	Paramètres	Valeur retournée
indisponible	• `state` : statut de la fin : ▫ `true` : réussi, ▫ `false` : échoué,	ignoré

Texte de la procédure :

```
--[[
Called:
  when database verification completed

Database:
  NOT available

Parameters:
  state     true   success
```

```
                    failed

Returned value:
  ignored

]]

local args = ... -- args.state
```

La limitation de licence est atteinte (la connexion n'est pas établie)

Appelé lorsqu'il est impossible d'établir une connexion au client à cause des limitations de licence. Après la fermeture de la connexion, `bad_connection.ds` est appelé.

Base de données	Paramètres	Valeur retournée
disponible	• `reason` : cause de l'erreur de connexion : ▫ `connection` : aucune licence disponible, ▫ `database` : erreur de création d'un nouveau poste dans la BD car il n'y a plus de licences disponibles	ignoré

Texte de la procédure :

```
--[[
Called:
  when new client connection cannot be established due license limitation

Database:
  available

Parameters:
  reason     "connection"   no free license
             "database"     cannot create new station in database due
                            no free license

Returned value:
  ignored

]]

local args = ... -- args.reason
```

Certaines fonctions du Serveur Dr.Web s'arrêtent

Appelé après que le Serveur Dr.Web achevé l'exécution de certaines fonctions du service (le Serveur Dr.Web n'a pas servi les clients).

Base de données	Paramètres	Valeur retournée
indisponible	non	ignoré

Texte de la procédure :

```
--[[
Called:
  when server completed execute some service function
  (the server did not serve clients)

Database:
  NOT available

Parameters:
  none

Returned value:
  ignored

]]
```

Le téléchargement du pilote de la BD est terminé

Appelé après la fin du chargement du pilote de la base de données.

Base de données	Paramètres	Valeur retournée

indisponible	• `state` : statut de la fin :
	  ▫ `true` : téléchargé avec succès,
	  ▫ `false` : erreur de téléchargement,
	• `driver` : nom du pilote de la base de données,
	• `library` : chemin d'accès complet à la bibliothèque du pilote de la base de données,
	• `message` : message d'erreur en cas de statut `false`
		ignoré

Texte de la procédure :

```
--[[
Called:
  when database driver load process completed

Database:
  NOT available
```

```
Parameters:
  state     true     successful load
            false    load failed
  driver             database driver name
  library            full path to database driver library
  message            error message text when state is 'false'

Returned value:
  ignored

]]

local args = ... -- args.state, args.driver, args.library, args.message
```

La tâche sur le Serveur Dr.Web est exécutée

Appelé après l'exécution de la tâche sur le Serveur Dr.Web.

Base de données	Paramètres	Valeur retournée

disponible	• `id` : ID du Serveur Dr.Web,
	• `done` : statut de la fin :
	  ▫ `true` : exécuté avec succès,
	  ▫ `false` : échec d'exécution,
	• `time` : heure de la fin de la tâche,
	• `name` : nom de la tâche,
	• `error` : message du journal d'exécution de tâches
		ignoré

Texte de la procédure :

```
--[[
Called:
  when job executed on the server

Database:
  available

Parameters:
  id                server ID
  done      true    executed successfully
            false   execution failed
  time              job completion time
  name              job name
  error             error or other message

Returned value:
  ignored

]]

local args = ... -- args.id, args.done, args.name, args.time, args.error
```

Le module de protocole a été déchargé

Appelé lors du déchargement du module de protocole.

Base de données	Paramètres	Valeur retournée
indisponible	• `name` : nom interne du protocole, • `path` : chemin d'accès au fichier du module de protocole	ignoré

Texte de la procédure :

```
--[[
Called:
  when protocol module unloaded

Database:
  NOT available

Parameters:
  name                    protocol name
  path                    path to protocol module file

Returned value:
  ignored

]]

local args = ... -- args.path
```

Le module de protocole est téléchargé

Appelé après le chargement du module de protocole.

Base de données	Paramètres	Valeur retournée
indéfini	• `path` : chemin d'accès au fichier du module de protocole, • `name` : nom interne du protocole, • `desc` : description du module de protocole, • `state` : statut: ▫ `loaded` : le module de protocole est chargé avec succès,	ignoré

Base de données	Paramètres	Valeur retournée
	▫ `disabled` : le module de protocole est désactivé dans le fichier `drwcsd.conf`, • `error` : texte du message d'erreur en cas de statut `invalid`	

Texte de la procédure :

```
--[[
Called:
  when protocol module loaded

Parameters:
  path                    path to protocol module file
  name                    internal protocol name
  desc                    protocol module description string
  state      "loaded"     protocol module loaded successfully
             "disabled"   protocol module is disabled in drwcsd.conf
             "invalid"    invalid protocol module format
  error                   error message if state is "invalid"

Returned value:
  ignored

]]

local args = ... -- args.state, args.path, args.name
```

L'extension est déchargée

Appelé lors du déchargement du module de l'extension.

Base de données	Paramètres	Valeur retournée
indisponible	• `name` : nom de l'extension, • `path` : chemin d'accès au fichier de l'extension	ignoré

Texte de la procédure :

```
--[[
Called:
  when plugin module unloaded

Database:
  NOT available

Parameters:
  name                    plugin name
```

```
  path                    path to plugin file

Returned value:
  ignored

]]

local args = ... -- args.name, yargs.path
```

L'extension est téléchargée

Appelé après le chargement du module de l'extension.

Base de données	Paramètres	Valeur retournée
indisponible	• `path` : chemin d'accès au fichier de l'extension, • `name` : nom interne de l'extension, • `desc` : description de l'extension, • `state` : statut: ▫ `loaded` : l'extension est chargée avec succès ▫ `disabled` : l'utilisation de l'extension est désactivée dans le fichier `drwcsd.conf`, ▫ `invalid` : format incorrect de l'extension, • `error` : texte du message d'erreur en cas de statut `invalid`	ignoré

Texte de la procédure :

```
--[[
Called:
  when plugin module loaded

Database:
  NOT available

Parameters:
  path                    path to plugin file
  name                    internal plugin name
  desc                    plugin description string
  state       "loaded"    plugin loaded successfully
              "disabled"  plugin is disabled in drwcsd.conf
              "invalid"   invalid plugin format
  error                   error message if state is "invalid"
```

```
Returned value:
  ignored

]]


local args = ... -- args.state, args.path, args.name, args.error
```

Copie de sauvegarde

Appelé après la fin de la copie de sauvegarde de fichiers mais avant la suppression des fichiers sauvegardés précédemment.

Base de données	Paramètres	Valeur retournée
disponible	• `state` : statut de la fin : ▫ `true` : réussi, ▫ `false` : échoué,	ignoré

Texte de la procédure :

```
--[[
Called:
  when backup completed but before deleting previous backup files

Database:
  available

Parameters:
  state  true  successful
         false failed

Returned value:
  ignored

]]

local args = ... -- args.state
```

Le Serveur Dr.Web s'arrête

Appelé lorsque le Serveur Dr.Web achève de servir les clients.

Base de données	Paramètres	Valeur retournée
indisponible	non	ignoré

Texte de la procédure :

```
--[[
```

```
Called:
  when server completed serve clients

Database:
  NOT available

Parameters:
  none

Returned value:
  ignored

]]
```

Le Serveur Dr.Web est lancé et prêt

Appelé lorsque le Serveur Dr.Web démarre et qu'il est prêt à servir les clients.

Base de données	Paramètres	Valeur retournée
indisponible	non	ignoré

Texte de la procédure :

```
--[[
Called:
  when server started and going to serve clients

Database:
  NOT available

Parameters:
  none

Returned value:
  ignored

]]
```

M8. Connexions

La limitation de licence est atteinte (connexion refusée)

Appelé en cas de connexion refusée conformément aux limitations du contrat de licence ignoré.

Base de données	Paramètres	Valeur retournée
disponible	• `id` : ID du poste, • `address` : adresse réseau du poste,	ignoré

Base de données	Paramètres	Valeur retournée
	• `station` : nom NetBIOS du poste. Ce nom ne peut pas être remplacé par le nom DNS, • `type` : type `station`	

Texte de la procédure :

```
--[[
Called:
  when connection denied according license limitation

Database:
  available

Parameters:
  id              station ID
  address         station network address
  station         station name
                  this is NetBIOS station name (not replaced by DNS one)
  type            one of 'station'

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.type

-- no return => `nil' value
```

Erreur de connexion

Appelé s'il est impossible d'établir une connexion avec le nouveau client.
Causes possibles : pas de licences disponibles (dans ce cas, en premier lieu est appelé `license_error.ds`), pas de connexion avec la BD, une erreur de la BD, un excès de postes attendant une approbation, le serveur ou la BD est surchargé.

Base de données	Paramètres	Valeur retournée

disponible si la cause est `no license` et potentiellement disponible si la cause est `overload` (durant cette période, il n'est pas recommandé d'utiliser la BD)	• `address` : adresse du client,
	• `reason` : cause de l'erreur de connexion :
	  ▫ `no database` : la connexion à la base de données n'a pas été établie,
	  ▫ `overload` : la base de données est surchargée,
	  ▫ `no license` : aucune licence disponible pour accepter la connexion
		ignoré

Texte de la procédure :

```
--[[
Called:
  when new client connection cannot be established

Database:
  available if reason is "no license" and potentialy available if
  reason is "overload" (but it is not recommended to use DB that time)

Parameters:
  address                  client address
  reason   "no database"   no established database connection
           "overload"      database is overloaded
           "no license"    no free license to accept connection

Returned value:
  ignored

]]

local args = ... -- args.address, args.reason
```

Un PONG a été reçu du client

Appelé lors de la réception d'un PONG du client.

Base de données	Paramètres	Valeur retournée
disponible	• `id` : ID du client, • `address` : adresse réseau du client, • `station` : nom du client (pour l'Agent, le Serveur, l'Installateur), • `time` : temps aller-retour (round-trip) du paquet	ignoré

Texte de la procédure :

```
--[[
Called:
  when 'PONG' received from client

Database:
  available

Parameters:
  id         client ID
  address    network address
  station    station name (for Agent, Server, Installer)
  time       packet round-trip time in milliseconds

Returned value:
  ignored

]]
```

```
local args = ... -- args.id, args.address, args.station,
                 -- args.time
```

La connexion au client est interrompue

Appelé après l'interruption de la connexion au client.

Base de données	Paramètres	Valeur retournée
disponible	• `id` : ID du client, • `address` : adresse réseau du client, • `type` : `unknown`, `station`, `console`, `server`, `installer`, `newbie` • `station` : nom du poste (seulement pour l'Agent), • `bytesin` : octets reçus sans compression, • `bytesout` : octets envoyés sans compression, • `totalbytesin` : octets compressés reçus, • `totalbytesout` : octets compressés envoyés, • `reason` : cause de la déconnexion	ignoré

Texte de la procédure :

```
--[[
Called:
  when client disconnected

Database:
  available

Parameters:
  id              client ID
  address         network address
  type            client type: "unknown", "station", "proxy",
                               "server", "installer", "newbie"
  station         station name (only for Agent)
  bytesin         bytes received
  bytesout        bytes sent
  totalbytesin    compressed bytes received
  totalbytesout   compressed bytes sent
  reason          disconnect reason

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.type, args.station
                 -- args.bytesin, args.bytesout
                 -- args.totalbytesin, args.totalbytesout
                 -- args.reason
```

M9. Postes

L'Agent est désinstallé

Appelé après la fin de la suppression de l'Agent.

Base de données	Paramètres	Valeur retournée

disponible	• `login` : login de l'administrateur,
	• `state` : statut de la fin :
	  ▫ `true` : réussi,
	  ▫ `false` : échoué,
	• `id` : ID du poste,
	• `address` : adresse du poste,
	• `station` : nom du poste,
	• `message` : vide si le statut est `true`, dans la cas contraire, contient un message d'erreur
		ignoré

Texte de la procédure :

```
--[[
Called:
  when deinstallation of Agent completed

Database:
  available

Parameters:
  login           login name of administrator
  state           true    success
                  false   failed
  id                      station ID
  address                 station address
  station                 station name
  message                 empty if state is 'true' or contains error message

Returned value:
  ignored

]]

local args = ... -- args.login, args.state, args.id
                 -- args.address, args.station, args.message
```

Arrêt d'un composant sur le poste

Appelé lorsque l'événement `component completed` est reçu de l'Agent.

Base de données	Paramètres	Valeur retournée
disponible	• `id` : ID du poste, • `address` : adresse du poste, • `station` : nom du poste, • `component` : numéro du composant, • `pid` : ID du processus, • `infections` : menaces détectées, • `errors` : erreurs d'accès détectées, • `exitcode` : code de fin du composant,	ignoré

Texte de la procédure :

```
--[[
Called:
  when "component completed" event received from Agent

Database:
  available

Parameters:
  id          station ID
  address     station address
  station     station name
  component   component number
  pid         process ID
  infections  infections found
  errors      access errors detected
  exitcode    component exit code

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.component,
                 -- args.pid, args.exitcode, args.infections, args.errors
```

La tâche est exécutée

Appelé lorsque l'événement `job executed` est reçu de l'Agent.

Base de données	Paramètres	Valeur retournée
disponible	• `id` : ID du poste, • `address` : adresse du poste,	ignoré

Base de données	Paramètres	Valeur retournée

	• `station` : nom du poste,
	• `done` : statut d'exécution :
	  ▫ `true` : exécuté avec succès,
	  ▫ `false` : échec d'exécution,
	• `time` : heure de la fin de la tâche,
	• `name` : nom de la tâche,
	• `error` : message d'erreur ou de statut	

Texte de la procédure :

```
--[[
Called:
  when "job executed" event received from Agent

Database:
  available

Parameters:
  id                station ID
  address           station address
  station           station name
  done      true    executed successfully
            false   execution failed
  time              job completion time
  name              job name
  job               job ID (empty for Agent prior version 11 (protocol 3.1+))
  error             error or other message

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.done,
                 -- args.name, args.job, args.time, args.error
```

Lancement d'un composant sur le poste

Appelé lorsque l'événement `component started` est reçu de l'Agent.

Base de données	Paramètres	Valeur retournée
disponible	• `id` : ID du poste, • `address` : adresse du poste, • `station` : nom du poste,	ignoré

Base de données	Paramètres	Valeur retournée
	• `component` : numéro du composant, • `pid` : ID du processus, • `engine` : version du moteur de recherche, • `records` : total d'entrées virales, • `user` : nom de l'utilisateur et groupe du propriétaire du processus, • `time` : heure du début (heure du poste)	

Texte de la procédure :

```
--[[
Called:
  when "component started" event received from Agent

Database:
  available

Parameters:
  id          station ID
  address     station address
  station     station name
  component   component number
  pid         process ID
  engine      virus-finding engine version
  records     virus records number
  user        user name and group (process owner)
  time        start time (station time)

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.component,
                 -- args.pid, args.records, args.user, args.time, args.engine
```

La position géographique du poste est changée

Appelé en cas de modification de l'emplacement géographique du poste.

Base de données	Paramètres	Valeur retournée
disponible	• `id` : ID du poste, • `address` : adresse du poste,	ignoré

Base de données	Paramètres	Valeur retournée
	• `station` : nom du poste, • `latitude` : latitude du poste au format DD.DDDDDD, • `longitude` : longitude du poste au format DD.DDDDDD	

Texte de la procédure :

```
--[[
Called:
  when agent geolocation changed

Database:
  available

Parameters:
  id          station ID
  address     station address
  station     station name
  latitude    station latitude in DD.DDDDDD format
  longitude   station longitude in DD.DDDDDD format

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.name, args.latitude, args.longitude
```

Un redémarrage du poste est requis

Appelé après la réception du message `reboot required` du poste par le Serveur Dr.Web.

Base de données	Paramètres	Valeur retournée
disponible	• `id` : ID du poste, • `address` : adresse réseau du poste, • `station` : nom NetBIOS du poste. Ce nom ne peut pas être remplacé par le nom DNS, • `product` : ID du produit • `description` : description du produit, • `from_revision` : numéro de la révision actuelle,	ignoré

Base de données	Paramètres	Valeur retournée
	• `to_revision` : numéro de la nouvelle révision, • `from_revision_date` : date de la révision actuelle, • `to_revision_date` : date de la nouvelle révision	

Texte de la procédure :

```
--[[
Called:
  after server received 'reboot required' station message.

Database:
  available

Parameters:
  id                  station ID
  address             station network address
  station             station name (this is NetBIOS station name not replaced by DNS
one)
  product             product ID
  description         product description
  from_revision       current revision number
  to_revision         new revision number
  from_revision_date  current revision date
  to_revision_date    new revision date

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.product,
args.description, args.from_revision, args.to_revision, args.from_revision_date,
args.to_revision_date
```

Une menace a été détectée sur le poste

Appelé lorsque l'événement `virus detected` est reçu de l'Agent.

Base de données	Paramètres	Valeur retournée
disponible	• `id` : ID du poste, • `address` : adresse du poste, • `station` : nom du poste, • `component` : numéro du composant, • `pid` : ID du processus,	ignoré

Base de données	Paramètres	Valeur retournée

	• `time` : heure de l'événement (heure du poste),
	• `user` : nom de l'utilisateur et groupe du propriétaire du processus,
	• `object` : chemin d'accès au fichier dans le système de fichiers,
	• `owner` : nom d'utilisateur et groupe du propriétaire de l'objet,
	• `virus` : nom du virus,
	• `action` : code d'action,
	• `objecttype` : type d'objet:
	  ▫ `-1` inconnu,
	  ▫ `0` fichier,
	  ▫ `1` :secteur d'amorçage,
	  ▫ `2` :bloc de mémoire ou processus,
	  ▫ `3` :activité virale
	• `infectiontype` : type de menace (voir Dr.Web API),
	• `compsid` : SID du poste,
	• `compmac` : adresse MAC du poste,
	• `description` : description du poste,
	• `compdn` : LDAP DN du poste (uniquement pour les clients sous Windows),
	• `sha1` : hash SHA-1 de l'objet trouvé,
	• `sha256` : hash SHA-256 de l'objet détecté,
	• `hashdb` : bulletin contenant le hash	

Texte de la procédure :

```
--[[
```

```
Called:
  when "virus detected" event received from Agent

Database:
  available

Parameters:
  id                station ID
  address           station address
  station           station name
  component         component number
  pid               process ID
  time              event time (station time)
  user              user name and group (process owner)
  object            filesystem object path
  owner             object owner (user name and group)
  virus             virus name
  action            action code (see Dr.Web API; only errors bit set)
  objecttype        object type
                      -1    unknown
                       0    file
                       1    boot sector
                       2    memory block / process
                       3    virus like activity
  infectiontype     infection type (see Dr.Web API)
  compsid           computer sid
  compmac           computer MAC
  description       computer description
  compdn            computer LDAP DN
  sha1              object SHA-1 hash
  sha256            object SHA-256 hash
  hashdb            hash database containing object

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.component,
                 -- args.pid, args.time, args.user, args.object, args.owner,
                 -- args.virus, args.action, args.objecttype, args.infectiontype
                 -- args.compsid, args.compmac, args.description, args.compdn
                 -- args.sha1, args.sha256, args.hashdb
```

Rapport de la Protection préventive

Appelé lors de la réception du rapport de la Protection préventive depuis le poste.

Base de données	Paramètres	Valeur retournée
disponible	• `id` : ID du poste, • `address` : adresse du poste, • `station` : nom du poste, • `time` : l'heure de l'apparition de l'événement sur le poste, • `pid` : ID du processus, • `path` : chemin d'accès au fichier exécutable du	ignoré

Base de données	Paramètres	Valeur retournée
	processus ayant une activité suspecte • `target_path` : chemin d'accès à l'objet protégé auquel une tentative d'accès a été faite, • `hips_type` : type de l'objet protégé (valeur numérique), • `shell_guard_type` : raison de blocage du code non autorisé (valeur numérique), • `denied` : l'accès a été interdit (true | false), • `is_user_action` : l'action a été demandée auprès de l'utilisateur (`true` | `false`), • `event_count` : nombre d'événements interdits automatiquement (uniquement si la valeur `false` est spécifiée pour `is_user_action`), • `event_user` : l'utilisateur qui a lancé un processus ayant une activité suspecte • `action_user` : l'utilisateur qui a spécifié la réaction pour l'activité suspecte du processus (uniquement si la valeur `true` est spécifiée pour `is_user_action`), • `sha1` : hash SHA-1 de l'objet trouvé, • `sha256` : hash SHA-256 de l'objet détecté, • `hashdb` : bulletin contenant le hash	

Texte de la procédure :

```
--[[
Called:
  when HIPS event received from Agent
```

```
Database:
  available

Parameters:
  id                  station ID
  address             station address
  station             station name
  time                station time
  pid                 numeric,process id
  path                process file path
  target_path         affected resource path
  hips_type           numeric, HIPS type
  shell_guard_type    numeric, Shell Guard event type
  denied              boolean, access was denied
  is_user_action      boolean, user was asked
  event_count         event number (for accumulation period - if is_user_action is
false)
  event_user          user which initiated the suspicious activity
  action_user         user which allowed or denied the activity (non-empty only if
is_user_action is true)
  sha1                process file SHA-1 hash
  sha256              process file SHA-256 hash
  hashdb              hash database containing process file

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.time,
                 -- args.pid, args.path, args.target_path, args.hips_type,
args.shell_guard_type,
                 -- args.denied, args.is_user_action, args.event_count,
args.event_user, args.action_user
                 -- args.sha1, args.sha256, args.hashdb
```

Erreur d'authentification du poste

Appelé après le refus de connexion à l'Agent à cause d'une erreur d'autorisation.

Base de données	Paramètres	Valeur retournée
disponible	• `id` : ID du poste, • `address` : adresse du poste, • `station` : nom du poste, • `reason` : cause de l'échec, • `type` : l'un des `station`, `installer`, `proxy`, • `compsid` : SID du poste, • `compmac` : adresse MAC du poste, • `description` : description du poste	ignoré

Texte de la procédure :

```
--[[
Called:
  just after Agent connection rejected due authorization error

Database:
  available

Parameters:
  id          station ID
  address     station address
  station     station name
  reason      failure reason
  type        one of 'station' | 'installer' | 'proxy'
  compsid     station UID (SID on Windows)
  compmac     station MAC address
  description station description

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.reason, args.type,
args.compsid, args.compmac, args.description
```

Erreur de date/heure sur le poste

Appelé en cas de détection de la date/l'heure invalide sur le poste.

Base de données	Paramètres	Valeur retournée
disponible	• `id` : ID du poste, • `address` : adresse du poste, • `station` : nom du poste, • `now` : heure du Serveur Dr.Web (en millisecondes), • `time` : heure du poste (en millisecondes), • `valid_delta` : décalage horaire acceptable (en millisecondes)	ignoré

Texte de la procédure :

```
--[[
Called:
  when invalid station time/date detected

Database:
  available
```

```
Parameters:
  id              station ID
  address         station address
  station         station name
  now             server time (in milliseconds)
  time            station time (in milliseconds)
  valid_delta     valid time delta (in milliseconds)

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station
                 -- args.now, args.date, args.valid_delta
```

Erreur de mise à jour du poste

Appelé après le message `update failed` reçu par le Serveur Dr.Web depuis le poste.

Base de données	Paramètres	Valeur retournée
disponible	• `id` : ID du poste, • `address` : adresse réseau du poste, • `station` : nom NetBIOS du poste. Ce nom ne peut pas être remplacé par le nom DNS, • `product` : ID du produit • `description` : description du produit, • `from_revision` : numéro de la révision actuelle, • `to_revision` : numéro de la nouvelle révision, • `from_revision_date` : date de la révision actuelle, • `to_revision_date` : date de la nouvelle révision	ignoré

Texte de la procédure :

```
--[[
Called:
  after server received 'update failed' station message.

Database:
  available

Parameters:
```

```
  id                  station ID
  address             station network address
  station             station name (this is NetBIOS station name not replaced by DNS
one)
  product             product ID
  description         product description
  from_revision       current revision number
  to_revision         new revision number
  from_revision_date  current revision date
  to_revision_date    new revision date

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.product,
args.description, args.from_revision, args.to_revision, args.from_revision_date,
args.to_revision_date
```

Erreur de scan sur le poste

Appelé lorsque l'événement `scan error` est reçu de l'Agent.

Base de données	Paramètres	Valeur retournée
disponible	• `id` : ID du poste, • `address` : adresse du poste, • `station` : nom du poste, • `component` : numéro du composant, • `pid` : ID du processus, • `time` : heure de l'événement (heure du poste), • `user` : nom de l'utilisateur et groupe du propriétaire du processus, • `object` : chemin d'accès au fichier dans le système de fichiers, • `owner` : nom d'utilisateur et groupe du propriétaire de l'objet, • `action` : code d'action, • `compsid` : SID du poste, • `compmac` : adresse MAC du poste, • `description` : description du poste,	ignoré

Base de données	Paramètres	Valeur retournée
	• `ldapdn` : LDAP DN du poste (uniquement pour les clients sous Windows), • `sha1` : hash SHA-1 de l'objet trouvé, • `sha256` : hash SHA-256 de l'objet détecté, • `hashdb` : bulletin contenant le hash	

Texte de la procédure :

```
--[[
Called:
  when "scan error" event received from Agent

Database:
  available

Parameters:
  id                station ID
  address           station address
  station           station name
  component         component number
  pid               process ID
  time              event time (station time)
  user              user name and group (process owner)
  object            filesystem object path
  owner             object owner (user name and group)
  action            action code (error bit(s) set)
  compsid           computer SID
  compmac           computer MAC
  description       computer description
  ldapdn            computer LDAP DN
  sha1              object SHA-1 hash
  sha256            object SHA-256 hash
  hashdb            hash database containing object

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.component,
                 -- args.pid, args.time, args.user, args.object, args.owner,
                 -- args.action, args.compsid, args.compmac, args.description,
args.ldapdn
                 -- args.sha1, args.sha256, args.hashdb
```

Une liste des composants est reçue

Appelé lorsque l'Agent communique une liste des composants installés.

Base de données	Paramètres	Valeur retournée
disponible	• `id` : ID du poste, • `address` : adresse du poste, • `station` : nom du poste, • `count` : nombre de composants annoncés, • `component_0` : nom du composant, • `time_0` : heure d'installation, • `from_0` : source d'installation (l'adresse du Serveur Dr.Web, MSI etc.), • `path_0` : chemin d'installation	ignoré

Texte de la procédure :

```
--[[
Called:
  when Agent reported installed components

Database:
  available

Parameters:
  id                  station ID
  address             station address
  station             station name
  count               number of components reported
  component_0         component name
  time_0              installation time
  from_0              installation source (server address, MSI, etc)
  path_0              installation path

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.count
                 -- args.component_0, args.time_0, args.from_0, args.path_0
                 -- args.component_1, args.time_1, args.from_1, args.path_1
                 -- ...
```

Des informations sur les bases virales sont reçues

Appelé lorsque l'Agent envoie des informations sur les bases virales.

Base de données	Paramètres	Valeur retournée
disponible	• `id` : ID du poste,	ignoré

Base de données	Paramètres	Valeur retournée
	• `address` : adresse du poste, • `station` : nom du poste, • `count` : nombre de bases virales, • `name_0` : nom du fichier de la base virale, • `md5_0` : MD5 du fichier de la base virale, • `version_0` : version de la base virale, • `issued_0` : date et heure de la sortie de la base virale • `records_0` : nombre d'entrées dans la base virale, • `type_0` : type de la base virale	

Texte de la procédure :

```
--[[
Called:
  when Agent sent virus bases information

Database:
  available

Parameters:
  id          station ID
  address     station address
  station     station name
  count       number of found virus bases
  name_0      virus base file name
  md5_0       virus base file MD5
  version_0   virus base version
  issued_0    virus base issue date and time
  records_0   number of records
  type_0      virus base type

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.count,
                 -- args.name_0, args.md5_0, args.version_0,
                 -- args.issued_0, args.records_0, args.type_0,
                 -- args.name_1, args.md5_1, args.version_1,
                 -- args.issued_1, args.records_1, args.type_1,
                 -- ...
```

Statut du poste

Appelé lorsque l'Agent communique le statut des composants, des bases virales et de certaines politiques locales (l'envoi d'événements, la réception de mises à jour et de tâches)

Base de données	Paramètres	Valeur retournée
disponible	• `events` : message sur des événements: ▫ `true` : l'Agent envoie des informations sur les événements, ▫ `false` : l'Agent n'envoie pas d'informations sur les événements, • `jobs` : acceptation de tâches (selon la planification et scans à distance) : ▫ `true` : l'Agent accepte des tâches, ▫ `false` : l'Agent n'accepte pas de tâches, • `updates` : réception de mises à jour: ▫ `true` : l'Agent reçoit des mises à jour, ▫ `false` : l'Agent ne reçoit pas de mises à jour	ignoré

Texte de la procédure :

```
--[[
Called:
  when Agent report its local policy

Database:
  available

Parameters:
  events    true     Agent send events
            false    Agent do not send events
  jobs      true     Agent accept jobs (schedule & remote scan)
            false    Agent do not accept jobs
  updates   true     Agent accept updates
            false    Agent do not accept updates


Returned value:
  ignored

]]

local args = ... -- args.events, args.jobs, args.updates
```

Le poste est en cours d'authentification

Appelé lorsque le poste tente de s'authentifier (l'ID et le mot de passe sont déjà vérifiés, valides et connus).

Base de données	Paramètres	Valeur retournée

disponible	• `id` : ID du poste,
	• `connected` : vérification de la disponibilité des postes ayant le même ID et déjà connectés au Serveur Dr.Web :
	  ▫ `true` : un autre poste ayant le même ID est déjà connecté au Serveur Dr.Web,
	  ▫ `false` : pas d'autres postes connectés ayant le même ID,
	• `current_address` : adresse réseau du poste connecté ayant le même ID (non vide, uniquement si `connected` prend la valeur `true`),
	• `current_name` : nom du poste connecté ayant le même ID,
	• `last_address` : adresse réseau du poste ayant le même ID lors de sa dernière connexion,
	• `last_time` : heure de la dernière connexion du poste ayant le même ID,
	• `last_server` : Serveur Dr.Web du poste ayant le même ID lors de sa dernière connexion,
	• `new_name` : nom du poste qui se connecte,
	• `new_address` : adresse réseau du poste qui se connecte
		• `string` : résultat de la requête pour la connexion du poste
		• `nil` : comportement du Serveur Dr.Web par défaut
		• `deny` : refuser l'authentification au poste
		• `force` : autoriser l'authentification même si un autre poste ayant le même ID s'est déjà connecté (déconnecter le poste connecté)
		• `newbie` : remettre le poste dans le statut novice

Texte de la procédure :

```
--[[
Called:
  when station tries to authorize (id and password already checked, valid and known)

Database:
  available

Parameters:
  id                      station ID
  connected       true    station with same ID already connected to server
                  false   no any station with same ID connected
  current_address         already connected station network address (not empty only if
'connected' is true)
  current_name            last connected station name
  last_address            last disconnected station network address
  last_time               last disconnected station seen time
  last_server             last connected station server
  new_name                now connecting station name
  new_address             now connecting station network address

Returned value:
          nil             default server behavior
  string  'deny'          deny authorization for station
          'force'         allow authorization even if other station with same ID
already connected (by disconnecting it)
          'newbie'        reset station to newbie

Procedure from next set will be called if returned nothing.
]]

local args = ... -- args.id, args.connected, args.current_address, args.current_name,
args.last_address,
                 -- args.last_time, args.last_server, args.new_name, args.new_address

-- no return => `nil' value
```

Le poste est connecté

Appelé en cas de connexion réussi de l'Agent.

Base de données	Paramètres	Valeur retournée
disponible	• `id` : ID du poste, • `address` : adresse du poste, • `station` : nom du poste, • `os` : OS du poste, • `platform` : plateforme du poste, • `compsid` : SID du poste, • `compmac` : adresse MAC du poste,	ignoré

Base de données	Paramètres	Valeur retournée
	• `description` : description du poste	

Texte de la procédure :

```
--[[
Called:
  when Agent connected successfully

Database:
  available

Parameters:
  id          station ID
  address     station address
  station     station name
  os          station os
  platform    station platform
  compsid     station UID (Security ID on Windows)
  compmac     station MAC address
  description station description

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.name, args.os, args.platform,
args.compsid, args.compmac, args.description
```

Un poste est créé

Appelé à la fin de la création du poste.

Base de données	Paramètres	Valeur retournée
disponible	• `login` : login de l'administrateur, • `id` : ID du poste, • `name` : nom du poste, • `state` : statut de la fin : ▫ `0` :créé avec succès ▫ `1` : erreur lors de l'exécution de l'opération (erreur de la base de données), ▫ `2` : le délai d'attente de l'opération s'est écoulé (la	ignoré

Base de données	Paramètres	Valeur retournée
	base de données est surchargée), ▫ 3 : aucune licence disponible, ▫ 4 : le poste existe déjà	

Texte de la procédure :

```
--[[
Called:
  when station create completed

Database:
  available

Parameters:
  login         administrator`s login name
  id            station ID
  name          station name
  state         operation completion state:
                  0  created successfully
                  1  operation failed (database error)
                  2  operation timed out (database overloaded)
                  3  no free license
                  4  already exists

Returned value:
  ignored

]]

local args = ... -- args.login, args.id, args.name, args.state
```

Le poste est supprimé

Appelé lors de la suppression du poste.

Base de données	Paramètres	Valeur retournée
disponible	• login : login de l'administrateur, • id : ID du poste	ignoré

Texte de la procédure :

```
--[[
Called:
  when station deleted

Database:
  available
```

```
Parameters:
  login     administrator`s login name
  id        station id

Returned value:
  ignored

]]

local args = ... -- args.login, args.id
```

Statistiques de scan du poste

Appelé lorsque l'événement `scan statistics` est reçu de l'Agent.

Base de données	Paramètres	Valeur retournée
disponible	• `id` : ID du poste, • `address` : adresse du poste, • `station` : nom du poste, • `component` : numéro du composant, • `pid` : ID du processus, • `user` : nom de l'utilisateur et groupe du propriétaire du processus, • `time` : heure de l'événement (heure du poste), • `size` : taille sommaire de tous les objets scannés, • `elapsedtime` : temps écoulé, • `scanned` : nombre d'objets scannés, • `infected` : nombre d'objets contaminés par un virus connu, • `modifications` : nombre d'objets contaminés par une modification de virus, • `suspicious` : nombre de fichiers suspects, • `cured` : nombre de fichiers désinfectés, • `deleted` : nombre de fichiers supprimés,	ignoré

Base de données	Paramètres	Valeur retournée
	• `renamed` : nombre de fichiers renommés, • `moved` : nombre des fichiers déplacés en quarantaine, • `locked` : nombre de fichiers bloqués (uniquement par SpIDer Guard), • `errors` : nombre des fichiers non scannés à cause d'une erreur d'accès	

Texte de la procédure :

```
--[[
Called:
  when "scan statistics" event received from Agent

Database:
  available

Parameters:
  id                station ID
  address           station address
  station           station name
  component         number of component
  pid               process ID
  user              user name and group (process owner)
  time              event time (station time)
  size              summary size of all scanned objects
  elapsedtime       elapsed time
  scanned           number of scanned objects
  infected          number of objects infected by known virus
  modifications     number of objects infected by virus modification
  suspicious        number of suspicious objects
  cured             number of cured files
  deleted           number of deleted files
  renamed           number of renamed files
  moved             number of quarantined files
  locked            number of locked files (SpIDer Guard only)
  errors            number of not scanned files (due access error)

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.component,
                 -- args.pid, args.time, args.user, args.scanned,
                 -- args.infected, args.modifications, args.suspicious,
                 -- args.cured, args.deleted, args.renamed, args.moved,
                 -- args.locked, args.errors, args.size, args.elapsedtime
```

Installation de l'Agent

Appelé après la réception de l'événement `installation`.

Base de données	Paramètres	Valeur retournée

disponible	• `id` : ID de l'installation (attention : ce n'est pas l'ID du poste),
	• `address` : adresse du poste,
	• `station` : nom du poste,
	• `event` : type de l'événement:
	  ▫ `0` : début de l'installation,
	  ▫ `1` : terminée avec succès,
	  ▫ `2` : refusé,
	  ▫ `3` :délai expiré,
	  ▫ `4` : échoué,
	  ▫ `5` : inaccompli
	• `message` : message d'erreur (ou message vide si aucune erreur n'est survenue),
	• `sessionid` : ID de la session d'installation
		ignoré

Texte de la procédure :

```
--[[
Called:
  when "installation" event occured

Database:
  available

Parameters:
  id                installation ID (not station!)
  address           station address
  station           station name
  event             event type:
                      0   installation begin
                      1   successully completed
                      2   rejected
                      3   timed out
                      4   failed
                      5   incomplete
  message           error message (or empty if there is no error)
  sessionid         installation session ID

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station
                 -- args.event, args.message, args.sessionid
```

L'appareil est bloqué

Appelé en cas de blocage de l'appareil sur le poste.

Base de données	Paramètres	Valeur retournée
disponible	• `id` : ID du poste, • `address` : adresse du poste, • `name` : nom du poste, • `user` : nom d'utilisateur, • `instance_id` : identificateur de l'appareil, • `friendly_name` : nom convivial de l'appareil, • `description` : description de l'appareil, • `guid` : GUID de l'appareil, • `class` : classe de l'appareil (nom du groupe parent)	ignoré

Texte de la procédure :

```
--[[
Called:
  when device on station blocked

Database:
  available

Parameters:
  id              station ID
  address         station address
  station         station name
  user            user name
  instance_id     device instance id
  friendly_name   device friendly name
  description     device description
  guid            device guid
  class           device group class guid
  blocktime       time when station was blocked
  blockrcvtime    time when server received alert

Returned value:
  ignored

]]

local args = ... -- args.id args.address args.station args.user args.instance_id
                 -- args.friendly_name args.description args.guid args.class
                 -- args.station_time args.args.recv_time
```

M10. LDAP

Transformation des noms utilisateur en LDAP DN

Appelé lors de la transformation des noms d'utilisateurs en LDAP DN.

Base de données	Paramètres	Valeur retournée
disponible	• `user` : nom d'utilisateur	• `nil` : utilisateur inconnu • `string` : informations sur l'utilisateur: ▫ `empty` : utilisateur inconnu ▫ `non-empty` : DN de l'utilisateur

Texte de la procédure

```
--[[

Called:
  when AuthLDAP module translates user name to DN

Database:
  available

Parameters:
  user           username

Returned value:
              nil         unknown user
  string      empty       unknown user
              non-empty   DN of user

Procedure from next set will be called if returned nothing.
]]

local args = ... -- args.user

-- example code:
-- if args.user == 'super-admin' then return 'CN=super,DC=example,DC=com' end

-- no return => `nil' value
```

Chapitre 3 : Questions fréquentes

Déplacement du Serveur Dr.Web vers un autre ordinateur (sous Windows)

En cas de déplacement du Serveur Dr.Web sur un autre ordinateur, prenez en compte les paramètres des protocoles de transport et, si nécessaire, apportez des modifications correspondantes à la rubrique **Administration** → **Configuration du Serveur Dr.Web**, dans l'onglet **Transport**.

La procédure de démarrage et d'arrêt du Serveur Dr.Web est décrite dans le **Manuel Administrateur**, p. Démarrage et arrêt du Serveur Dr.Web.

Pour déplacer le Serveur Dr.Web (en cas d'installation d'une version équivalente du Serveur Dr.Web) sous Windows

1. Arrêtez le service du Serveur Dr.Web.
2. Depuis la ligne de commande, lancez le fichier `drwcsd.exe` accompagné de la clé `modexecdb database-export` afin d'exporter le contenu de la base de données vers un fichier. La ligne de commande complète pour l'exportation sous Windows est approximativement la suivante :

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" -verbosity=trace -log="C:\Program Files\DrWeb Server\var\exportdb.log" modexecdb database-export <nom_complet_du_fichier>
   ```

3. Sauvegardez le contenu du répertoire `C:\Program Files\DrWeb Server\etc`.
4. Supprimez le Serveur Dr.Web.
5. Installez un nouveau Serveur Dr.Web (vide et avec une nouvelle base) sur un ordinateur choisi. Arrêtez le service du Serveur Dr.Web avec les outils de gestion des services de Windows ou depuis le Centre de gestion.
6. Copiez le contenu du répertoire `etc` sauvegardé précédemment dans le répertoire `C:\Program Files\DrWeb Server\etc`.
7. Lancez depuis la ligne de commande le fichier `drwcsd.exe` accompagné de la clé `modexecdb database-import` pour importer le contenu de la base de données depuis le fichier. La ligne de commande complète pour l'importation sous Windows est approximativement la suivante :

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" -verbosity=trace -log="C:\Program Files\DrWeb Server\var\importdb.log" modexecdb database-import <nom_complet_du_fichier>
   ```

8. Lancez le service du Serveur Dr.Web.

En cas d'utilisation de la base de données intégrée, il est possible de ne pas effectuer les procédures d'exportation/importation de la BD, il suffit de sauvegarder le fichier de la base intégrée `database.sqlite` et de remplacer ensuite le nouveau fichier de la BD sur le Serveur Dr.Web installé par le fichier sauvegardé précédemment depuis le Serveur Dr.Web antérieur.

Pour déplacer le Serveur Dr.Web (en cas d'installation d'une autre version du Serveur Dr.Web) sous Windows

1. Arrêtez le service du Serveur Dr.Web.
2. Sauvegardez la base de données avec les outils du Serveur SQL (en cas d'utilisation de la BD intégrée, sauvegardez tout simplement le fichier `database.sqlite`).
3. Sauvegardez le contenu du répertoire `C:\Program Files\DrWeb Server\etc`.
4. Supprimez le Serveur Dr.Web.
5. Installez un nouveau Serveur Dr.Web (vide et avec une nouvelle base) sur un ordinateur choisi. Arrêtez le service du Serveur Dr.Web avec les outils de gestion des services de Windows ou depuis le Centre de gestion.
6. Copiez le contenu du répertoire `etc` sauvegardé précédemment dans le répertoire `C:\Program Files\DrWeb Server\etc`.
7. Restaurez la base de données sur le nouveau Serveur Dr.Web, dans le fichier de configuration `drwcsd.conf`, spécifiez le chemin vers la base de données.
8. Depuis la ligne de commande lancez le fichier `drwcsd.exe` accompagné de la clé `modexecdb database-upgrade` pour mettre à jour la base de données. La ligne de commande complète pour l'importation sous Windows est approximativement la suivante :

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -verbosity=all -log="C:\Program Files\DrWeb Server\var\upgradedb.log" modexecdb database-upgrade
```

9. Lancez le service du Serveur Dr.Web.

En cas de changement d'adresse IP ou en cas de déplacement du Serveur Dr.Web :

Pour la connexion des Agents Dr.Web pour lesquels l'adresse du nouveau Serveur Dr.Web est spécifié via le Centre de gestion et non dans les paramètres de l'Agent Dr.Web sur le poste, laissez les deux Serveurs Dr.Web activés jusqu'à la fin de la procédure.

Il est recommandé d'utiliser le nom du serveur au format FQDN en tant qu'adresse du Serveur Dr.Web.

1. Réalisez un déplacement du Serveur Dr.Web conformément à la procédure décrite ci-dessus.

2. Pour tous les Agents Dr.Web servis par l'ancien Serveur Dr.Web, spécifiez l'adresse du nouveau Serveur Dr.Web conformément à la procédure correspondante de la rubrique Connexion de l'Agent Dr.Web à un autre Serveur Dr.Web.

   Pour la connexion des Agents Dr.Web pour lesquels l'adresse du nouveau Serveur Dr.Web est spécifié via le Centre de gestion et non dans les paramètres de l'Agent Dr.Web sur le poste, les paramètres de l'Agent Dr.Web sur les deux Serveurs Dr.Web doivent contenir l'adresse du nouveau Serveur Dr.Web.
3. Attendez que tous les Agents Dr.Web passent sur le nouveau Serveur Dr.Web. Ensuite, l'ancien Serveur Dr.Web peut être supprimé.

Déplacement du Serveur Dr.Web vers un autre ordinateur (sous Linux)

En cas de déplacement du Serveur Dr.Web sur un autre ordinateur, prenez en compte les paramètres des protocoles de transport et, si nécessaire, apportez des modifications correspondantes à la rubrique **Administration** → **Configuration du Serveur Dr.Web**, dans l'onglet **Transport**.

La procédure de démarrage et d'arrêt du Serveur Dr.Web est décrite dans le **Manuel Administrateur**, p. Démarrage et arrêt du Serveur Dr.Web.

Pour déplacer le Serveur Dr.Web (en cas d'installation d'une version équivalente du Serveur Dr.Web) sous Linux

1. Installez un nouveau Serveur (vide et avec une nouvelle base) sur l'ordinateur choisi conformément aux instructions décrites dans le **Manuel d'installation**, le p.Installation du Serveur Dr.Web pour les OS de la famille UNIX.

   

   Si vous planifiez déplacer l'ancien Serveur Dr.Web avec la sauvegarde de l'adresse IP, assignez une adresse IP temporaire au nouveau Serveur pour que les postes puissent interagir avec l'ancien Serveur Dr.Web lors du déplacement.

2. Ajoutez la clé de votre licence valide `Agent.key` dans le **Gestionnaire de licences** pour le nouveau Serveur Dr.Web et distribuez-la au groupe **Everyone**.
3. Dans l'interface Web du nouveau Serveur, accédez a la section **Statut du référentiel** et assurez-vous que le répertoire est mis à jour correctement.
4. Ouvrez la section **Administration** → **Serveur Dr.Web** et assurez-vous que cette section affiche la date qui correspond à la date de la révision actuelle du Serveur Dr.Web dans la section **Statut du référentiel**. Si la date ne correspond pas ou qu'il y a un messages informant sur les mises à jour disponibles, cliquez sur le bouton **Voir la liste des versions** et effectuez une mise à niveau du Serveur Dr.Web vers la version actuelle.
5. Arrêtez le nouveau Serveur Dr.Web via l'interface Web ou via la console avec la commande :

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

6. Sur le nouveau Serveur Dr.Web remplacez le fichier `/var/opt/drwcs/etc/drwcsd.conf` par le fichier équivalent de l'ancien Serveur Dr.Web.

En cas de migration vers un autre OS il faut vérifier le contenu du fichier `drwcsd.conf` pour la présence de chemins win. S'il y en a, il faut les corriger manuellement avent le déplacement.

Attention, les chemins pour FreeBSD sont différents :

- `/var/opt/drwcs/ -> /var/drwcs/`
- `/opt/drwcs/ -> /usr/local/drwcs/`

7. Supprimez le fichier de certificat `drwcsd-certificate.pem` du répertoire `/opt/drwcs/webmin/install/windows` sur le nouveau Serveur Dr.Web.

```
# rm /opt/drwcs/webmin/install/windows/drwcsd-certificate.pem
```

8. Supprimez le fichier de la clé privée `drwcsd.pri` et la deuxième copie du certificat `drwcsd-certificate.pem` du répertoire `/var/opt/drwcs/etc/` sur le nouveau Serveur Dr.Web.
9. Supprimez le fichier de la base de données du répertoire `/var/opt/drwcs/` sur le nouveau Serveur Dr.Web.
10. Si Windows est installé sur l'ancien Serveur Dr.Web, copiez la clé privée `drwcsd.pri` et le certificat `drwcsd-certificate.pem` du répertoire `%programfiles%\DrWeb Server\etc` de l'ancien Serveur vers le répertoire `/var/opt/drwcs/etc/` sur le nouveau Serveur Dr.Web. Si Linux est installé sur l'ancien Serveur Dr.Web, copiez ces fichiers dans le répertoire `var/opt/drwcs/etc/` sur l'ancien Serveur et collez-les dans le même répertoire sur le nouveau Serveur.
11. Arrêtez l'ancien Serveur Dr.Web via l'interface Web (**Démarrer** → **Tous les programmes** → **Dr.Web Server** → **Contrôle du serveur**) ou via la console (si un OS de la famille Linux est installé) :

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

12. Vérifiez la base de données sur l'ancien Serveur Dr.Web avec la commande :
    - pour le Serveur Dr.Web en version antérieure à la version 13 :

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

    - pour le Serveur Dr.Web en version 13 :

```
# /etc/init.d/drwcsd modexecdb database-verify
```

    Si lors de l'exécution de cette commande un message d'erreur s'affiche dans le fichier `drwscd.log`, contactez le support technique.
13. Sauvegardez la base de données avec les outils du serveur SQL (en cas d'utilisation de la BD embarquée, sauvegardez tout simplement le fichier `database.sqlite`). Copiez le fichier de la base de données du répertoire `%programfiles%\DrWeb Server\var` de l'ancien Serveur Dr.Web (du répertoire `/var/opt/drwcs/` si un OS de la famille Linux est installé) vers le répertoire `/var/opt/drwcs/` du nouveau Serveur Dr.Web.
14. Démarrez l'ancien Serveur Dr.Web pour qu'il continue à maintenir les agents via l'interface Web ou via la console avec la commande :

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

15. Sur le nouveau Serveur Dr.Web, désignez l'utilisateur `drwcs` comme le propriétaire du répertoire `/var/opt/drwcs/database.sqlite`, ainsi que comme le propriétaire des fichiers `/var/opt/drwcs/etc/drwcsd.pri` et `/var/opt/drwcs/etc/drwcsd-certificate.pem` :

```
# chown -R drwcs /var/opt/drwcs/database.sqlite

# chown drwcs /var/opt/drwcs/etc/drwcsd.pri

# chown drwcs /var/opt/drwcs/etc/drwcsd-certificate.pem
```

16. Copiez le certificat `drwcsd-certificate.pem` vers le répertoire `/opt/drwcs/webmin/install/windows`

```
# cp /var/opt/drwcs/etc/drwcsd?
certificate.pem /opt/drwcs/webmin/install/windows
```

17. Lancez le nouveau Serveur Dr.Web :

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

18. Accédez à l'interface Web du nouveau Serveur Dr.Web avec le même login et le mot de passe que sur l'ancien Serveur Dr.Web. Assurez-vous que tous les Agents Dr.Web s'affichent correctement dans la liste du réseau antivirus.
19. Accédez à la section **Administration** → **Statut du référentiel** et assurez-vous que le référentiel sur le nouveau Serveur Dr.Web est mis à jour sans erreurs. Si dans le tableau contenant la liste des produits il y a des messages d'erreurs dans la ligne Statut du référentiel, contactez le support technique. Joignez le fichier `drwscd.log` à la demande. Il ne faut pas effectuer des actions quelconques des instructions avant la réception de la réponse à la demande.
20. Accédez à la section **Administration** → **Planificateur de tâches du Serveur Dr.Web** et sélectionnez la tâche **Backup sensitive data** (Sauvegarde des données critiques). Cliquez sur l'icône  ; dans la fenêtre d'édition de la tâche, sélectionnez l'onglet **Action**. Assurez-vous que le champ **Chemin** ne contient pas le chemin d'accès au répertoire sur l'ancien Serveur Dr.Web. Videz le champ et laissez-le vide (dans ce cas le répertoire par défaut `/var/opt/drwcs/backup` sera utilisé pour la sauvegarde des copies) ou saisissez le chemin d'accès à un répertoire sur le nouveau Serveur Dr.Web.
21. Accédez à la section **Réseau antivirus** → **Everyone** → **Paramètres de connexion** sur le nouveau serveur et indiquez l'adresse du nouveau Serveur dans le champ **Serveur Dr.Web**.

S'il faut sauvegarder l'ancienne adresse IP pour le nouveau Serveur Dr.Web (voir le p.1), arrêtez l'ancien Serveur Dr.Web et assignez au nouveau Serveur Dr.Web son adresse IP. Redémarrez le nouveau Serveur Dr.Web pour appliquer les modifications des paramètres système.

Pour connecter un poste au nouveau Serveur Dr.Web

1. Accédez à l'interface Web de l'ancien Serveur Dr.Web et sélectionnez le poste ou le groupe qu'il faut reconnecter.
2. Accédez à la section **Paramètres de connexion** et indiquez l'adresse du nouveau Serveur Dr.Web pour les objets sélectionnés. Assurez-vous que tous les postes se sont déconnectés se l'ancien Serveur et se sont connectés au nouveau Serveur.

Connexion de l'Agent Dr.Web à un autre Serveur Dr.Web

L'Agent Dr.Web peut se connecter à un autre Serveur Dr.Web de deux façons :

1. Via le Centre de Gestion.

   La configuration distante sans accès au poste est possible si le poste est toujours connecté à l'ancien Serveur Dr.Web. Dans ce cas, l'accès aux Centres de gestion de l'ancien et du nouveau Serveurs Dr.Web est requis.
2. Directement sur le poste.

   Pour exécuter les actions directement sur le poste il faut posséder les droits d'administrateur de ce poste et les droits de modification des paramètres de l'Agent Dr.Web, spécifiés sur le Serveur Dr.Web. Si vous ne possédez pas ces droits, la connexion à un autre Serveur Dr.Web est possible uniquement après la suppression de l'Agent installé et l'installation d'un nouvel Agent Dr.Web avec les paramètres du nouveau Serveur Dr.Web. Si vous ne possédez pas les droits de suppression de l'Agent Dr.Web en mode local, utilisez l'utilitaire Dr.Web Remover pour supprimer l'Agent Dr.Web du poste ou supprimez l'Agent Dr.Web via le Centre de gestion.

Connexion de l'Agent Dr.Web à un autre Serveur Dr.Web

La connexion de l'Agent Dr.Web à un autre Serveur Dr.Web peut être requise si les agents sont connectés au Serveur Dr.Web dont l'adresse a été modifiée ou que le Serveur Dr.Web a été réinstallé sans utilisation du certificat du serveur précédent.

L'Agent Dr.Web peut se connecter à un autre Serveur Dr.Web de deux façons :

1. Via le Centre de Gestion.

   La configuration distante sans accès au poste est possible si le poste est toujours connecté à l'ancien Serveur Dr.Web. Dans ce cas, l'accès aux Centres de gestion de l'ancien et du nouveau Serveurs Dr.Web est requis.
2. Directement sur le poste.

   Pour exécuter des actions directement sur le poste il faut posséder les droits d'administrateur de ce poste et, en cas de leur modification via l'interface de l'agent, il faut également avoir les droits de modification des paramètres de l'Agent Dr.Web, spécifiés sur le Serveur. Si vous ne possédez pas ces droits, la connexion à un autre Serveur est possible uniquement après la suppression de l'Agent installé du Centre de gestion et l'installation d'un nouvel Agent avec les paramètres du nouveau Serveur.

Vous pouvez modifier certains paramètres de connexion depuis la ligne de commande au nom de l'administrateur du poste :

- OS Windows :
  ```
  "%ProgramFiles%\DrWeb\es-service.exe" --
  esserver=<adresse_du_serveur> --
  addcert=<chemin_d'accès_au_certificat>
  ```
- OS UNIX :
  ```
  drweb-ctl esdisconnect && drweb-ctl esconnect
  <adresse_du_serveur> --Certificate <chemin_d'accès_au_certificat>
  ```

  `<adresse_du_serveur>` : si l'adresse du Serveur a changé.

  `<chemin_d'accès_au_certificat>` : si le serveur a été réinstallé sans utilisation du certificat du serveur précédent.

Le certificat du serveur est disponible dans la section **Administration > Clés de chiffrement** du Centre de gestion.

Pour connecter l'Agent Dr.Web à un autre Serveur Dr.Web à l'aide du Centre de gestion

1. Sur le nouveau Serveur Dr.Web, autorisez les postes ayant les paramètres d'authentification incorrects à requérir de nouveaux paramètres d'authentification en tant que novices. Pour ce faire, dans le Centre de gestion, sélectionnez l'élément **Administration** du menu principal → l'élément **Configuration du Serveur Dr.Web** du menu de gestion → l'onglet **Général** :
   a) Cochez la case **Spécifier les non approuvés comme novices**, si elle est décochée.
   b) Si l'option **Toujours refuser l'accès** est sélectionnée dans la liste déroulante **Mode d'enregistrement des novices** changez-la en **Confirmer l'accès manuellement** ou **Approuver l'accès automatiquement**.
   c) Cliquez sur **Enregistrer** pour appliquer les modifications et redémarrez le Serveur Dr.Web.

   Si la politique du réseau de l'entreprise n'autorise pas la modification des paramètres de l'étape 1, il faut spécifier directement sur le poste les paramètres d'authentification du poste correspondant au compte créé avant dans le Centre de gestion.

2. Sur l'ancien Serveur Dr.Web auquel l'Agent Dr.Web est connecté, spécifiez les paramètres du nouveau Serveur Dr.Web. Pour cela, dans le Centre de gestion, sélectionnez dans le menu principal l'élément **Réseau antivirus** → dans la liste hiérarchique du réseau, sélectionnez le poste nécessaire (ou le groupe des postes pour connecter tous les postes de ce groupe) → dans le menu de gestion, sélectionnez l'élément **Paramètres de connexion** :
   a) Si le certificat du nouveau Serveur Dr.Web ne correspond pas au certificat de l'ancien Serveur Dr.Web, spécifiez le chemin d'accès au certificat du nouveau Serveur Dr.Web dans le champ **Certificat**.
   b) Dans le champ **Serveur**, spécifiez l'adresse du nouveau Serveur Dr.Web.

Il est recommandé d'utiliser le nom du serveur au format FQDN en tant qu'adresse du Serveur Dr.Web.

c) Cliquez sur **Enregistrer**.

Pour connecter l'Agent Dr.Web à un autre Serveur Dr.Web directement sur le poste

1. Dans les paramètres de l'Agent Dr.Web, spécifiez les paramètres du nouveau Serveur Dr.Web. Pour cela, dans le menu contextuel de l'icône Agent Dr.Web, ouvrez le **Centre de gestion** → cliquez sur le cadenas  , s'il n'est pas encore ouvert, pour avoir l'accès aux paramètres avancés → bouton  pour accéder aux paramètres → élément **Serveur** → bouton **Modifier les paramètres** :
   a) Si le certificat du nouveau Serveur Dr.Web ne correspond pas au certificat de l'ancien Serveur Dr.Web, spécifiez le chemin d'accès au certificat du nouveau Serveur Dr.Web en cliquant sur le bouton**Liste de certificats**.
   b) En cliquant sur le bouton **Ajouter**, spécifiez les paramètres correspondants du nouveau Serveur Dr.Web.
2. Basculer le poste vers le statut novice (réinitialisez les paramètres d'authentification sur le Serveur Dr.Web). Pour ce faire, dans la section des paramètres de connexions de l'étape 1, cliquez sur les boutons suivants : le bouton **Paramètres de connexion du poste** → le bouton **Réinitialiser les paramètres et se connecter en tant que novice** → le bouton **Réinitialiser les paramètres**.

Si vous connaissez ID et le mot de passe pour la connexion au nouveau Serveur Dr.Web, vous pouvez les entrer dans les champs **ID du poste** et **Mot de passe**. Dans ce cas, il n'est pas nécessaire de basculer le poste vers le statut novice.

Charge sur le Serveur Dr.Web et paramètres de configuration recommandés

Si vous utilisez une base de données externe dans les réseaux antivirus de grande taille, il est possible qu'il vous faudra modifier les valeurs des paramètres suivants pour assurer le fonctionnement du Serveur Dr.Web :

- **Administration → Configuration du Serveur Dr.Web → Base de données → Nombre de connexions** (paramètre `database connections=""` dans le fichier de configuration du Serveur Dr.Web) : nombre maximum des connexions du Serveur Dr.Web à la base de données.
- **Administration → Configuration du Serveur Dr.Web → Général → Nombre de requêtes parallèles des clients** (paramètre `threads count=""` dans le fichier de configuration du Serveur Dr.Web) : nombre de requêtes pour le traitement des données issues des clients : Agents Dr.Web, installateurs des Agents, Serveurs voisins Dr.Web, Serveurs proxy Dr.Web.

Ces paramètres affectent les performances du Serveur Dr.Web. Ne modifiez pas leurs valeurs s'il n'est pas nécessaire. Pour déterminer la nécessite de leur modification, referez-vous au tableau des rapports entre les dimensions du réseau antivirus, les capacités matérielles du Serveur Du Serveur et les valeurs optimales des paramètres :

Nombre de connexion des clients au Serveur Dr.Web	Nombre de coeurs du processus du Serveur Dr.Web	Nombre de connexions à la base de données (database connections)	Nombre de requêtes parallèles des clients (threads count)
jusqu'à 500	2	2 (valeur par défaut)	5 (valeur par défaut)
500–1500	3–5	3–5	6–10
plus de 1500	5–8	5–8	10–14

La valeur du paramètre **Nombre de requêtes parallèles des clients** (`threads count`) ne doit pas dépasser le double du nombre des coeurs de processeur sur l'ordinateur exécutant les fonctions du Serveur Dr.Web.

Si vous utilisez la base de données embarquée, il n'est pas recommandé de modifier les valeurs par défaut.

Si vous gérez un réseau avec un grand nombre de connexions et que vous souhaitez de modifier les valeurs des paramètres indiqués, il est recommandé de consulter le service de support technique de la société Doctor Web.

Changement du type de la BD Dr.Web Enterprise Security Suite

Sous Windows

> La procédure de démarrage et d'arrêt du Serveur Dr.Web est décrite dans le **Manuel Administrateur**, p. Démarrage et arrêt du Serveur Dr.Web.

1. Arrêtez le service du Serveur Dr.Web.
2. Depuis la ligne de commande, lancez le fichier `drwcsd.exe` accompagné de la clé `modexecdb database-export` afin d'exporter le contenu de la base de données vers un fichier. La ligne de commande complète pour l'exportation sous Windows est approximativement la suivante :

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
   Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
   verbosity=trace -log="C:\Program Files\DrWeb Server\var\exportdb.log"
   modexecdb database-export D:\esbase.es
   ```

   Cet exemple sous-entend que le Serveur Dr.Web est installé dans le répertoire `C:\Program Files\DrWeb Server` et que la base sera exportée vers le fichier `esbase.es` se trouvant dans la racine du disque `D`.

   Si le chemin vers le fichier comporte des espaces et/ou des caractères nationaux (ou le nom du fichier inclut des espaces et/ou des caractères nationaux), il est nécessaire de mettre le chemin avec entre guillemets :

   ```
   "D:\<nom long>\esbase.es"
   ```

3. Lancez le service du Serveur Dr.Web, connectez-y le Centre de gestion et reconfigurez ensuite le Serveur Dr.Web de sorte qu'il utilise une autre BD. Refusez le redémarrage du Serveur Dr.Web.
4. Arrêtez le service du Serveur Dr.Web.
5. Placez le fichier de la base de données dans un répertoire temporaire jusqu'à ce que vous vous assuriez que le changement du type de la BD est effectué avec succès.
6. Lancez depuis la ligne de commande le fichier `drwcsd.exe` accompagné de la clé `modexecdb database-init` pour initialiser la nouvelle base de données. La ligne de commande relative à l'initialisation de la base de données de la version du Serveur Dr.Web sous Windows est la suivante :

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
   Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
   verbosity=all -log="C:\Program Files\DrWeb Server\var\initdb.log"
   modexecdb database-init
   ```

   Il est sous-entendu que le Serveur Dr.Web est installé dans le répertoire `"C:\Program Files\DrWeb Server"`.

7. Lancez depuis la ligne de commande le fichier `drwcsd.exe` accompagné de la clé `modexecdb database-import` pour importer le contenu de la base de données depuis le fichier. La ligne de commande complète pour l'importation sous Windows est approximativement la suivante :

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=trace -log="C:\Program Files\DrWeb Server\var\importdb.log"
modexecdb database-import D:\esbase.es
```

8. Lancez le service du Serveur Dr.Web.

Sous OS de la famille UNIX

1. Arrêtez le service de Serveur Dr.Web avec le script :
   - sous **Linux** :

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

   - sous **FreeBSD** :

```
/usr/local/etc/rc.d/drwcsd stop
```

   ou depuis le Centre de gestion.
2. Lancez le Serveur Dr.Web accompagné de la clé `modexecdb database-export` pour exporter le contenu de la base vers le fichier. La ligne de commande depuis le répertoire d'installation du Serveur Dr.Web est la suivante :
   - sous **Linux** :

```
/etc/init.d/drwcsd modexecdb database-export /var/opt/drwcs/esbase.es
```

   - sous **FreeBSD** :

```
/usr/local/etc/rc.d/drwcsd modexecdb database-export /var/drwcs/esbase.es
```

   Ceci sous-entend que l'exportation de la base se fait vers le fichier `esbase.es` se trouvant dans le répertoire d'utilisateur.
3. Lancez le service de Serveur Dr.Web avec le script :
   - sous **Linux** :

```
/etc/init.d/drwcsd start
```

   - sous **FreeBSD** :

```
/usr/local/etc/rc.d/drwcsd start
```

   connectez-y le Centre de gestion et reconfigurez le Serveur Dr.Web de sorte qu'il utilise une autre BD : dans le menu **Administration** → l'élément **Configuration du Serveur Dr.Web** → l'onglet **Base de données**.

Vous pouvez également reconfigurer le Serveur Dr.Web pour utiliser une autre BD en éditant directement le fichier de configuration du Serveur Dr.Web `drwcsd.conf`. Pour ce faire, commentez/supprimez l'entrée sur la BD actuelle et écrivez une nouvelle BD (pour en savoir plus, voirF1. Fichier de configuration du Serveur Dr.Web).

Refusez le redémarrage du Serveur Dr.Web.

4. Arrêtez le Serveur Dr.Web (voir l'étape **1**).
5. Placez le fichier de la base de données dans un répertoire temporaire jusqu'à ce que vous vous assuriez que le changement du type de la BD est effectué avec succès.
6. Lancez le fichier `drwcsd` accompagné de la clé `modexecdb database-init` pour initialiser une nouvelle base de données. La ligne d'initialisation est la suivante :
   - sous **Linux** :

```
/etc/init.d/drwcsd modexecdb database-init
```

   - sous **FreeBSD** :

```
/usr/local/etc/rc.d/drwcsd modexecdb database-init
```

7. Lancez le fichier `drwcsd` accompagné de la clé `modexecdb database-import` pour importer le contenu de la base de données depuis le fichier. La ligne de commande relative à l'importation est la suivante :
   - sous **Linux** :

```
/etc/init.d/drwcsd modexecdb database-import /var/opt/drwcs/esbase.es
```

   - sous **FreeBSD** :

```
/usr/local/etc/rc.d/drwcsd modexecdb database-import /var/drwcs/esbase.es
```

8. Lancez le Serveur Dr.Web (voir l'étape **3**).

Si vous avez besoin de spécifier des paramètres lors du lancement du script de Serveur Dr.Web (par exemple pour spécifier le répertoire d'installation du Serveur Dr.Web, pour modifier le niveau de détail du journal etc.), vous pouvez modifier les valeurs correspondantes dans le script de lancement :

- sous **FreeBSD** :

```
/usr/local/etc/rc.d/drwcsd
```

- sous **Linux** :

```
/etc/init.d/drwcsd
```

Restauration de la base de données Dr.Web Enterprise Security Suite

Au cours de son fonctionnement, le Serveur Dr.Web enregistre régulièrement les copies de sauvegarde des informations importantes (des clés de licence, du contenu de la base de données, de la clé privée de chiffrement, de la configuration du Serveur Dr.Web et du Centre de gestion).

Les copies de sauvegarde sont enregistrées dans les répertoires suivants :

- sous **Windows** : <*disque_d'installation*>**:** `\DrWeb Backup`
- sous **Linux** : `/var/opt/drwcs/backup`
- sous **FreeBSD** : `/var/drwcs/backup`

Pour assurer la fonction de copie de sauvegarde, la planification du Serveur Dr.Web contient une tâche quotidienne. Si la tâche est introuvable, il est recommandé de la créer.

Tous les fichiers de la copie de sauvegarde, excepté le contenu de la base de données, sont prêts à l'emploi. La copie de sauvegarde est enregistrée au format `.dz` compatible avec `gzip` ainsi qu'avec d'autres utilitaires d'archivage. Le contenu de la base de données peut être importé depuis la copie de sauvegarde vers une base de données opérationnelle du Serveur Dr.Web à l'aide de la commande `modexecdb database-import` , ainsi, les données seront récupérées.

Pour restaurer la base de données, vous pouvez utiliser la copie de sauvegarde créée manuellement par l'administrateur dans la section **Administration** → **Gestion de la base de données** → **Exportation** du Centre de gestion (uniquement pour le mode **Exporter toute la base de données**).

La base de données ne peut être restaurée que depuis la copie de sauvegarde créée avec le Serveur Dr.Web dans la même version majeure que celle du Serveur Dr.Web sur lequel la restauration est effectuée.

Exemple :

- Vous pouvez restaurer la BD depuis la copie de sauvegarde, créée à l'aide du Serveur Dr.Web en version 13, seulement en utilisant le Serveur Dr.Web en version 13.
- Vous ne pouvez pas restaurer la BD depuis la copie de sauvegarde, créée à l'aide du Serveur Dr.Web en version 10 en utilisant le Serveur Dr.Web en version 13.

Si lors de la mise à niveau du Serveur Dr.Web vers la version 13 depuis les versions antérieures la BD a été endommagée, procédez comme suit :

1. Supprimez le Serveur Dr.Web en version 13. Dans ce cas, les copies de sauvegarde des fichiers utilisés par le Serveur Dr.Web seront sauvegardées automatiquement.
2. Installez le Serveur Dr.Web en version qui a été installée avant la mise à jour et avec laquelle la copie de sauvegarde a été créée.

Dans ce cas, suite à la procédure de mise à jour standard, il faut utiliser tous les fichiers sauvegardés du Serveur Dr.Web sauf le fichier de la base de données.

Créez une nouvelle base de données lors de l'installation du Serveur Dr.Web.

3. Restaurez la base de données depuis la copie de sauvegarde conformément aux règles générales (voir ci-dessous).
4. Dans les paramètres du Serveur Dr.Web, désactivez les protocols de l'Agent Dr.Web, du Serveur Dr.Web et de l'Installateur Réseau. Pour ce faire, sélectionnez l'élément **Administration** du menu principal du Centre de gestion. Ensuite, dans la fenêtre qui s'affiche, sélectionnez l'élément du menu de gestion **Configuration du Serveur Dr.Web**, passez dans l'onglet **Modules** et décochez les cases correspondantes.
5. Effectuez la mise à niveau du Serveur Dr.Web vers la version 13 conformément aux règles générales (voir le **Manuel Administrateur**, p. Chapitre 11 : Mise à jour des composants de Dr.Web Enterprise Security Suite lors du fonctionnement du produit).
6. Activez les protocoles de l'Agent Dr.Web, du Serveur Dr.Web et de l'Installateur réseau désactivés à l'étape 4.

Restauration de la BD sous Windows

La procédure de démarrage et d'arrêt du Serveur Dr.Web est décrite dans le **Manuel Administrateur**, p. Démarrage et arrêt du Serveur Dr.Web.

Pour restaurer la BD depuis une copie de sauvegarde

1. Arrêtez le service du Serveur Dr.Web, s'il est lancé.
2. Importez le contenu de la base de données depuis le fichier correspondant de la copie de sauvegarde. La ligne d'importation est la suivante :

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=trace -log="C:\Program Files\DrWeb Server\var\importdb.log"
modexecdb database-import "<chemin_d'accès_au_fichier_de_sauvegarde>\database.gz"
```

Cette commande doit être mise en une seule ligne. Cet exemple sous-entend que le Serveur Dr.Web est installé dans le répertoire `C:\Program Files\DrWeb Server`.

3. Lancez le service du Serveur Dr.Web.

Pour restaurer la BD depuis une copie de sauvegarde en cas de changement de version du Serveur Dr.Web (au sein de la version majeure) ou en cas d'endommagement de la version actuelle de la BD

1. Arrêtez le service du Serveur Dr.Web, s'il est lancé.
2. Initialisez la nouvelle base de données.
   - Lors de l'utilisation d'une BD intégrée :

a) Déplacez le fichier de la base de données `database.sqlite` dans un répertoire temporaire jusqu'à ce que vous vous assuriez que la restauration de la BD a été effectuée avec succès.

b) La ligne d'initialisation de la base de données relative à la version du Serveur Dr.Web opérant sous Windows est la suivante :

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=all -log="C:\Program Files\DrWeb Server\var\initdb.log"
modexecdb database-init
```

Cette commande doit être mise en une seule ligne (voir aussi le format de la commande `drwcsd` accompagnée de la clé `modexecdb database-init` dans l'Annexe G3.3. Commandes de gestion de la base de données). L'exemple sous-entend que le Serveur Dr.Web est installé dans le répertoire `C:\Program Files\DrWeb Server`.

c) Après l'exécution de cette commande, le nouveau fichier `database.sqlite` doit apparaitre dans le sous-répertoire `var` du répertoire d'installation du Serveur Dr.Web.

- Lors de l'utilisation d'une BD externe :

a) exportez le fichier de la base de données dans un répertoire temporaire jusqu'à ce que vous vous assuriez que la restauration de la BD a été effectuée avec succès.

b) effectuez le nettoyage de la BD avec la commande `modexecdb database-clean` (voir l'Annexe G3.3. Commandes de gestion de la base de données).

3. Importez le contenu de la base de données depuis le fichier correspondant de la copie de sauvegarde. La ligne d'importation est la suivante :

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=trace -log="C:\Program Files\DrWeb Server\var\importdb.log"
modexecdb database-import "<chemin_d'accès_au_fichier_de_sauvegarde>\database.gz"
```

Cette commande doit être mise en une seule ligne. Cet exemple sous-entend que le Serveur Dr.Web est installé dans le répertoire `C:\Program Files\DrWeb Server`.

4. Lancez le service du Serveur Dr.Web.

Restauration de la BD sous UNIX

1. Arrêtez le Serveur Dr.Web (s'il est lancé) :

- sous **Linux** :

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

- sous **FreeBSD** :

```
/usr/local/etc/rc.d/drwcsd stop
```

2. Déplacez le fichier de la base de données dans un répertoire temporaire jusqu'à ce que vous vous assuriez que la restauration de la BD a été effectuée avec succès. Le fichier de la base de

données `database.sqlite` se trouve dans le dossier suivant du répertoire d'installation du Serveur Dr.Web :

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

Lorsque vous utilisez une base de données externe, nettoyez-la préalablement avec la commande `modexecdb database-clean` (voir l'Annexe G3.3. Commandes de gestion de la base de données).

3. Initialisez la base de données du Serveur Dr.Web. Pour ce faire, exécutez la commande suivante :
   - sous **Linux** :

```
/etc/init.d/drwcsd modexecdb database-init
```

   - sous **FreeBSD** :

```
/usr/local/etc/rc.d/drwcsd modexecdb database-init
```

4. Après l'exécution de cette commande, le nouveau fichier `database.sqlite` doit apparaitre dans le dossier `var` du répertoire d'installation du Serveur Dr.Web.
5. Importez le contenu de la base de données depuis le fichier correspondant de la copie de sauvegarde. La ligne d'importation est la suivante :
   - sous **Linux** :

```
/etc/init.d/drwcsd modexecdb database-import
"<chemin_d'accès_au_fichier_backup>/database.gz"
```

   - sous **FreeBSD** :

```
/usr/local/etc/rc.d/drwcsd modexecdb database-import
"<chemin_d'accès_au_fichier_backup>/database.gz"
```

6. Démarrez le Serveur Dr.Web.
   - sous **Linux** :

```
/etc/init.d/drwcsd start
```

   - sous **FreeBSD** :

```
/usr/local/etc/rc.d/drwcsd start
```

Si vous avez besoin de spécifier des paramètres lors du lancement du script de Serveur Dr.Web (par exemple, spécifier le répertoire d'installation du Serveur Dr.Web, etc.), vous pouvez modifier les valeurs correspondantes dans le script de lancement :

- sous FreeBSD : `/usr/local/etc/rc.d/drwcsd` ;

- sous Linux : `/etc/init.d/drwcsd`.

S'il est nécessaire de modifier le niveau de détail du journal du Serveur Dr.Web, utilisez le fichier `local.conf` :

- sous Linux : `/var/opt/drwcs/etc/local.conf` ;
- sous FreeBSD : `/var/drwcs/etc/local.conf`.

S'il y a des Agents Dr.Web installés après la création de la dernière copie de sauvegarde, ils ne pourront pas se connecter au Serveur Dr.Web après la restauration de la base de données depuis la copie de sauvegarde. Vous pouvez basculer à distance ces postes en mode de novices. Dans la section **Administration** → **Configuration du Serveur Dr.Web**, dans l'onglet **Général**, cochez la case **Spécifier les non autorisés comme novices**. Dans la liste déroulante **Mode d'enregistrement de novices**, sélectionnez l'option **Autoriser l'accès automatiquement**. Cliquez sur le bouton **Enregistrer** et redémarrez le Serveur Dr.Web.

Après la connexion réussie de tous les postes au nouveau Serveur Dr.Web, modifiez ces paramètres du Serveur Dr.Web conformément à la politique de votre société.

Après avoir restauré la base de données, il est recommandé de se connecter au Serveur Dr.Web via le Centre de gestion, d'ouvrir la section **Administration** → **Planificateur de tâches du Serveur Dr.Web** et de vérifier si la tâche **Copie de sauvegarde des données critiques du Serveur** est présente. S'il n'y a pas de telle tâche, il est recommandé de la créer.

Mise à jour des Agents sur les serveurs LAN

Lors des mises à jour des Agents Dr.Web installés sur les serveurs LAN, il vaut mieux éviter la surcharge des postes ainsi que d'éventuels arrêts du logiciel réseau tournant sur ces postes.

Afin d'assurer la stabilité du fonctionnement des postes nécessaires à l'utilisation du LAN, le mode suivant de mise à jour des Agents Dr.Web et du logiciel antivirus est recommandé :

1. Modifiez les tâches standard de mise à jour de tous les composants dans la planification du Serveur Dr.Web de sorte que seules les bases virales soient mises à jour.
2. Créez une nouvelle tâche de mise à jour de tous les composants à l'heure où cela n'aura aucun impact sur le fonctionnement des serveurs LAN.

   Pour en savoir plus sur la création et l'édition des tâches dans la planification du Serveur Dr.Web, consultez le **Manuel Administrateur**, p. Configuration de la planification du Serveur Dr.Web.

Il n'est pas recommandé d'installer les composants SpIDer Gate, SpIDer Mail et le Pare-feu Dr.Web sur les serveurs exécutant des fonctions réseau importantes (contrôleurs de domaine, serveurs de distribution des licences etc.) afin d'éviter d'éventuels conflits entre les services réseau et les composants intérieurs de l'antivirus Dr.Web.

Utilisation de DFS lors de l'installation de l'Agent via Active Directory

Lors de l'installation de l'Agent Dr.Web via Active Directory, il est possible d'utiliser le service du Système de fichiers distribué (Distributed File System).

Cela peut être utile notamment en cas de plusieurs contrôleurs de domaine présents dans le LAN.

Pour installer l'Agent Dr.Web dans un réseau avec plusieurs contrôleurs de domaine

1. Créer sur chaque contrôleur de domaine un répertoire de sorte que les répertoires reçoivent les mêmes noms.
2. Avec DFS fusionnez les répertoires créés en un répertoire racine.
3. Installez le package `*.msi` dans le répertoire cible en mode administrateur (voir **Manuel d'installation**, p. Installation de l'Agent Dr.Web avec le service Active Directory).
4. Utilisez ce répertoire cible lors de la spécification de package dans l'éditeur des objets de la politique de groupes.

   Utilisez le nom réseau au format suivant : \\<*domain*>\<*folder*>

   avec : <*domain*> — nom du domaine, <*folder*> — nom du répertoire cible.

Restauration du réseau antivirus après une panne du Serveur Dr.Web

En cas de panne fatale du Serveur Dr.Web, il est recommandé d'utiliser les procédures indiquées pour restaurer l'état opérationnel du système antivirus sans réinstaller les Agents Dr.Web sur les postes.

Il est implicite que le nouveau Serveur Dr.Web sera installe sur l'ordinateur ayant la même adresse IP et le même nom DNS.

Restauration en cas de disponibilité d'une copie de sauvegarde du Serveur Dr.Web

Au cours de son fonctionnement, le Serveur Dr.Web enregistre régulièrement les copies de sauvegarde des informations importantes (des clés de licence, du contenu de la base de données, de la clé privée de chiffrement, de la configuration du Serveur Dr.Web et du Centre de gestion).

Les copies de sauvegarde sont enregistrées dans les répertoires suivants :

- sous **Windows** : <*disque_d'installation*>**:** `\DrWeb Backup`
- sous **Linux** : `/var/opt/drwcs/backup`
- sous **FreeBSD** : `/var/drwcs/backup`

Pour assurer la fonction de copie de sauvegarde, la planification du Serveur Dr.Web contient une tâche quotidienne. Si la tâche est introuvable, il est recommandé de la créer.

Tous les fichiers de la copie de sauvegarde, excepté le contenu de la base de données, sont prêts à l'emploi. La copie de sauvegarde est enregistrée au format `.gz` compatible avec `gzip` ainsi qu'avec d'autres utilitaires d'archivage. Le contenu de la base de données peut être importé depuis la copie de sauvegarde vers la base de données opérationnelle du Serveur Dr.Web à l'aide de la commande `modexecdb database-import-and-upgrade`, ainsi, les données seront récupérées.

Pour restaurer la base de données, vous pouvez utiliser la copie de sauvegarde créée manuellement par l'administrateur dans la section **Administration** → **Gestion de la base de données** → **Exportation** du Centre de gestion (uniquement pour le mode **Exporter toute la base de données**).

Il est également recommandé de sauvegarder sur un autre ordinateur les copies de sauvegarde et les autres fichiers importants. Vous pourrez ainsi éviter le risque de perdre des données en cas d'endommagement de l'ordinateur sur lequel est installé Serveur Dr.Web, dans ce cas-là, ceci vous permet de récupérer les données et de rétablir le fonctionnement du Serveur Dr.Web. En cas de perte des clés de licence, vous pouvez les redemander comme décrit dans le paragraphe **Manuel Administrateur**, p. Licence.

Pour restaurer le Serveur Dr.Web après une panne si une copie de sauvegarde des données du Serveur Dr.Web est disponible

1. Sélectionnez l'ordinateur sur lequel le nouveau Serveur Dr.Web sera installé. Isolez cet ordinateur des Agents Dr.Web en cours de fonctionnement : déconnectez l'ordinateur du réseau sur lequel les Agents Dr.Web sont installés ou modifiez temporairement son adresse IP ou faites-le à votre façon.
2. Installez un nouveau Serveur Dr.Web.
3. Dans la section **Administration** → **Gestionnaire de licences**, ajoutez une clé de licence de l'installation précédente du Serveur Dr.Web et diffusez-la sur les groupes correspondants, notamment sur le groupe **Everyone**. Cette étape est obligatoire si la clé de licence n'a pas été spécifiée lors de l'installation du Serveur Dr.Web.
4. Mettez à jour le référentiel du Serveur Dr.Web installé depuis le SGM :
   a) Ouvrez la section du Centre de gestion **Administration** → **Statut du référentiel**.
   b) Cliquez sur **Vérifier les mises à jour** pour voir si des mises à jour sont disponibles sur les serveurs SGM et pour les télécharger.
5. Si de nouvelles versions du logiciel du Serveur Dr.Web sont disponibles, effectuez la mise à niveau vers la dernière version :
   a) Ouvrez la section du Centre de gestion **Administration** → **Serveur Dr.Web**.
   b) Pour ouvrir la liste des versions du Serveur Dr.Web, cliquez sur la version actuelle du Serveur Dr.Web ou cliquez sur le bouton **Liste des versions**. La rubrique **Mises à jour du Serveur Dr.Web** va s'afficher contenant la liste des mises à jour disponibles et des copies de sauvegarde du Serveur Dr.Web.
   c) Pour mettre à niveau le Serveur Dr.Web, cochez la case contre la dernière version dans la liste **Toutes les versions**. Cliquez sur **Appliquer**.
   d) Attendez la fin de la mise à niveau du Serveur Dr.Web.
6. Arrêter le Serveur Dr.Web.
7. Remplacez les données critiques du Serveur Dr.Web par les données obtenues de la copie de sauvegarde :

Système d'exploitation	Fichiers de configuration
Windows	`etc` dans le répertoire d'installation du Serveur Dr.Web
Linux	`/var/opt/drwcs/etc`
FreeBSD	`/var/drwcs/etc`

8. Configure la base de données.
   a) Base de données externe :

      Aucune action pour connecter la base de données au Serveur Dr.Web n'est requise (à condition que le fichier de configuration du Serveur Dr.Web soit enregistré).

Si la version du Serveur Dr.Web installée depuis les dernières mises à jour est plus récente que celle du Serveur perdu Dr.Web, mettez à jour la base de données externe avec la commande `modexecdb database-upgrade` :

- sous Windows :

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -verbosity=all -log="C:\Program Files\DrWeb Server\var\upgradedb.log" modexecdb database-upgrade
```

- sous Linux :

```
/etc/init.d/drwcsd modexecdb database-upgrade
```

- sous FreeBSD :

```
/usr/local/etc/rc.d/drwcsd modexecdb database-upgrade
```

b) Copie de sauvegarde de la base de données externe ou embarquée :

Lorsque vous utilisez une base de données externe, nettoyez-la préalablement avec la commande `modexecdb database-clean` (voir l'Annexe G3.3. Commandes de gestion de la base de données).

Importez la base de données depuis le fichier correspondant de la copie de sauvegarde avec la mise à niveau du format de la base de données vers la version du Serveur Dr.Web installé avec la commande `modexecdb database-import-and-upgrade` :

- sous Windows :

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -verbosity=trace -log="C:\Program Files\DrWeb Server\var\importupgradedb.log" modexecdb database-import-and-upgrade "<chemin_d'accès_au_fichier_de_sauvegarde>\database.gz"
```

- sous Linux :

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log modexecdb database-import-and-upgrade "<chemin_d'accès_au_fichier_backup>/database.gz"
```

- sous FreeBSD :

```
/usr/local/etc/rc.d/drwcsd modexecdb database-import-and-upgrade "<chemin_d'accès_au_fichier_backup>/database.gz"
```

Tous les fichiers remplaçants du Serveur Dr.Web doivent avoir les mêmes droits système que les droits attribués lors de l'installation précédente (perdue) du Serveur Dr.Web.

Sous les OS de la famille UNIX : `rw` pour `drwcs:drwcs`.

9. Démarrez le Serveur Dr.Web.

10. Assurez-vous de l'intégrité et de l'actualité des données obtenues de la copie de sauvegarde de la base de données : les paramètres des Agents Dr.Web, l'état de l'arborescence du réseau antivirus, etc.
11. Restaurez l'accessibilité du Serveur Dr.Web pour les Agents Dr.Web en fonction du mode d'isolation du Serveur Dr.Web sélectionné à l'étape 1.

> S'il y a des Agents Dr.Web installés après la création de la dernière copie de sauvegarde, ils ne pourront pas se connecter au Serveur Dr.Web après la restauration de la base de données depuis la copie de sauvegarde. Vous pouvez basculer à distance ces postes en mode de novices. Dans la section **Administration** → **Configuration du Serveur Dr.Web**, dans l'onglet **Général**, cochez la case **Spécifier les non autorisés comme novices**. Dans la liste déroulante **Mode d'enregistrement de novices**, sélectionnez l'option **Autoriser l'accès automatiquement**. Cliquez sur le bouton **Enregistrer** et redémarrez le Serveur Dr.Web.
>
> Après la connexion réussie de tous les postes au nouveau Serveur Dr.Web, modifiez ces paramètres du Serveur Dr.Web conformément à la politique de votre société.

Restauration en cas d'absence de copies de sauvegarde du Serveur Dr.Web

Pour restaurer le Serveur après une panne s'il n y a aucune copie de sauvegarde

1. Sélectionnez l'ordinateur sur lequel le nouveau Serveur Dr.Web sera installé. Vous pouvez restaurer la connexion au serveur sur le même ordinateur (avec la même adresse) ou sur un autre ordinateur (en changeant l'adresse de connexion au Serveur Dr.Web dans les paramètres des Agents Dr.Web).
   Pour pouvoir effectuer la configuration initiale du Serveur Dr.Web et du réseau antivirus, avant de connecter les Agents Dr.Web, isolez cet ordinateur des Agents Dr.Web qui fonctionnent : lors de l'installation, changez le port par défaut 2193 (ensuite vous pourrez revenir au port par défaut). Après la première configuration, vérifiez la connexion au Serveur Dr.Web sur l'exemple d'un ou de deux Agents Dr.Web.
   Il est possible de restaurer le Serveur sur le même ordinateur (avec la même adresse) ou sur un autre ordinateur en changeant l'adresse de connexion au serveur Dr.Web dans les paramètres des Agents Dr.Web.
2. Installez un nouveau Serveur Dr.Web.
3. Dans la section **Administration** → **Gestionnaire de licences**, ajoutez une clé de licence de l'installation précédente du Serveur Dr.Web et diffusez-la sur les groupes correspondants, notamment sur le groupe **Everyone**. Cette étape est obligatoire si la clé de licence n'a pas été spécifiée lors de l'installation du Serveur Dr.Web.
4. Mettez à jour le référentiel du Serveur Dr.Web installé depuis le SGM :
   a) Ouvrez la section du Centre de gestion **Administration** → **Statut du référentiel**.

b) Cliquez sur **Vérifier les mises à jour** pour voir si des mises à jour sont disponibles sur les serveurs SGM et pour les télécharger.

5. Si de nouvelles versions du logiciel du Serveur Dr.Web sont disponibles, effectuez la mise à niveau vers la dernière version :
   a) Ouvrez la section du Centre de gestion **Administration** → **Serveur Dr.Web**.
   b) Pour ouvrir la liste des versions du Serveur Dr.Web, cliquez sur la version actuelle du Serveur Dr.Web ou cliquez sur le bouton **Liste des versions**. La rubrique **Mises à jour du Serveur Dr.Web** va s'afficher contenant la liste des mises à jour disponibles et des copies de sauvegarde du Serveur Dr.Web.
   c) Pour mettre à niveau le Serveur Dr.Web, cochez la case contre la dernière version dans la liste **Toutes les versions** et cliquez sur **Enregistrer**.
   d) Attendez la fin de la mise à niveau du Serveur Dr.Web.
6. Modifiez les paramètres de connexion de postes dans la configuration du Serveur Dr.Web :
   a) Ouvrez la section **Administration** → **Configuration du Serveur Dr.Web**.
   b) Dans l'onglet **Général**, Cochez la case **Spécifier les non approuvés comme novices**.
   c) Dans l'onglet **Général**, dans la liste déroulante **Mode d'enregistrement de novices**, sélectionnez l'option **Autoriser l'accès automatiquement**.
   d) Cliquez sur le bouton **Enregistrer** et redémarrez le Serveur Dr.Web.
7. Dans la section **Réseau antivirus** du Centre de gestion, créez les groupes utilisateurs dans l'arborescence du réseau antivirus par analogie à la version précédente. Si nécessaire, créez les règles automatiques d'appartenance pour les postes inclus dans des groupes utilisateurs.
8. Si nécessaire, spécifiez les paramètres des Agents Dr.Web et les paramètres du Serveur Dr.Web (excepté les paramètres de l'étape 6) par analogie à la version précédente.
9. Si nécessaire, modifie les parametres du référentiel, y compris les paramètres de la section **Administration** → **Configuration détaillée du référentiel**.
10. Restaurez l'accessibilité du Serveur Dr.Web pour les Agents Dr.Web en fonction du mode d'isolation du Serveur Dr.Web sélectionné à l'étape 1.
11. Remplacez le certificat sur tous les postes de réseau qui doivent se connecter au nouveau Serveur Dr.Web. Vous pouvez télécharger le certificat dans la section **Administration** → **Clés de chiffrement**.
    - Si l'autoprotection est activée, copiez sur le poste la certificat créé lors de l'installation du nouveau Serveur Dr.Web et exécutez la commande suivante :

      ```
      %ProgramFiles%\DrWeb\es-service.exe -p <clé>
      ```

      ou

      ```
      %ProgramFiles%\DrWeb\es-service.exe --addcert=<clé>
      ```

      En tant que *<clé>* spécifiez le chemin d'accès au certificat de serveur copié.

      La certificat, par conséquent, sera copié dans le répertoire d'installation de l'Agent Dr.Web. Par défaut c'est le répertoire `%ProgramFiles%\DrWeb` (pour en savoir plus, voir l'Annexe G2. Agent Dr.Web pour Windows).

- Si l'autoprotection est désactivée sur le poste, vous pouvez utiliser le certificat créé lors de l'installation du nouveau Serveur Dr.Web et le placer dans le répertoire indiqué ci-dessus.

12. Si vous avez restauré la connexion au Serveur Dr.Web sur un autre ordinateur, changez l'adresse de connexion au serveur dans les paramètres des Agents Dr.Web.

Il est recommandé d'utiliser le nom du serveur au format FQDN en tant qu'adresse du Serveur Dr.Web.

13. Après la connexion réussie de tous les postes au nouveau Serveur Dr.Web, modifiez les paramètres du Serveur Dr.Web spécifiés à l'étape 6 conformément à la politique de votre société.

Restauration du noeud du cluster des Serveurs Dr.Web

Si un des Serveurs Web du cluster ne marche pas pour une raison quelconque, les Agents Dr.Web ayant perdu la connexion, se connecteront à un autre noeud du cluster. En cas d'échec fatal du Serveur Dr.Web, il faut le restaurer (installer le Serveur Dr.Web et l'ajouter du nouveau au cluster).

Installation du Serveur Dr.Web pour son futur ajout dans le cluster

Pour pouvoir fonctionner avec une seule base de données, tous les Serveurs Dr.Web doivent avoir la même version.

Vous pouvez utiliser la copie de sauvegarde du Serveur Dr.Web tombé en panne s'il en a une. Cela va faciliter la procédure de restauration du noeud du cluster. La copie de sauvegarde contient les paramètres du référentiel, les fichiers de configuration, les clés de chiffrement, les certificats, la copie de sauvegarde de la base de données interne.

Quand vous installez un Serveur Dr.Web à la place d'un noeud du cluster tombé en panne, suivez les instructions ci-dessous.

Installation du Serveur sous les OS de la famille UNIX

Suivez les instructions du **Manuel d'installation**, la rubrique Installation du Serveur Dr.Web pour les OS de la famille UNIX. Vous pouvez installer un nouveau Serveur Dr.Web ou utiliser une copie de sauvegarde d'un Serveur Dr.Web faisant partie du cluster mais tombé en panne.

Les copies de sauvegarde sont stockées dans les répertoires suivants :

- pour le Serveur Dr.Web sous OS Linux : `/var/opt/drwcs/backup`,
- pour le Serveur Dr.Web sous OS FreeBSD : `/var/drwcs/backup`,

Le Serveur Dr.Web installé d'une copie de sauvegarde utilisera la base de données commune que les noeuds du cluster appellent.

En cas d'installation sans copie de sauvegarde, le Serveur Dr.Web utilisera la base de données embarquée. Une fois l'installation terminée, il faudra connecter le Serveur Dr.Web à la base de données commune utilisée par le cluster.

Installation du Serveur Dr.Web sous Windows

Vous pouvez installer un nouveau Serveur Dr.Web ou utiliser une copie de sauvegarde d'un Serveur Dr.Web faisant partie du cluster mais tombé en panne. Par défaut les copies de sauvegarde sont stockées dans le répertoire <*disque_d'installation*>`:\DrWeb Backup`.

Suivez les instructions du **Manuel d'installation**, de la rubrique Installation du Serveur Dr.Web pour Windows en faisant attention aux points suivants :

- L'installation avec la connexion à la base de données externe n'est pas recommandée car cela peut provoquer la perte des données stockées dans la base lors de la connexion du Serveur Dr.Web au cluster.
- En cas d'installation depuis une copie de sauvegarde, indiquez les paramètres de configuration suivants :
  - **Pilote de la base de données** : sélectionnez l'option **SQLite (base de données embarquée)**. Il n'est pas recommandé de laisser la base de données externe car cela peut provoquer la perte de données lors de la connexion du Serveur Dr.Web au cluster. Il faut connecter la base de données externe utilisée dans le cluster après la fin de l'installation du Serveur Dr.Web.
  - **Configuration du réseau** : indiquez les valeurs pertinentes des champs **Interface** et **Port**. Si la case **Activer le service de détection du Serveur Dr.Web** est décochée, cochez-la pour que le Serveur Dr.Web puisse échanger les informations avec les autres noeuds du cluster à l'aide du groupe multicast. Indiquez ci-dessous les paramètres du groupe multicast utilisé par les Serveurs Dr.Web dans le cluster.

  Les valeurs des autres paramètres peuvent être spécifiées conformément à la section **Installation du Serveur Dr.Web sous Windows**.
- Lors de l'installation d'un nouveau Serveur Dr.Web, indiquez les paramètres de configuration suivants :
  - **Configuration du Serveur Dr.Web** : indiquez les chemins d'accès au fichier de configuration `drwcsd.conf` et à la clé de chiffrement privée utilises par le Serveur Dr.Web tombe en panne, s'ils sont présents. Sinon laissez les champs vides pour créer de nouvelles clés de chiffrement, un certificat et un fichier de configuration avec les paramètres par défaut. Il faudra modifier les valeurs de ces paramètres après l'installation du Serveur Dr.Web.
  - **Pilote de la base de données** : sélectionnez l'option **SQLite (base de données embarquée)**. Il faut connecter la base de données externe utilisée dans le cluster après la fin de l'installation du Serveur Dr.Web.
  - **Configuration du réseau** : indiquez les valeurs pertinentes des champs **Interface** et **Port**. Cochez la case **Activer le service de détection du Serveur Dr.Web** pour que le Serveur Dr.Web puisse échanger les informations avec les autres noeuds du cluster à l'aide du groupe multicast. Indiquez ci-dessous les paramètres du groupe multicast utilisé par les Serveurs Dr.Web dans le cluster.

Les valeurs des autres paramètres peuvent être spécifiées conformément à la section **Installation du Serveur Dr.Web sous Windows**.

Ajout du Serveur Dr.Web au cluster

Pour connecter le Serveur Dr.Web installé au cluster, suivez les instructions mentionnées dans le **Manuel Administrateur**, la rubrique Cluster des Serveurs Dr.Web.

Gestion du niveau de journalisation du Serveur Dr.Web sous Windows

Vous pouvez modifier le niveau de détails du journal du Serveur Dr.Web sous Windows par l'un des moyens suivants :

- A l'aide de la section **Configuration du Serveur Dr.Web → Journal** dans le Centre de gestion.

  Ce moyen est préférable. Dans la section **Journal**, vous pouvez spécifier n'importe quel niveau de détails du journal du Serveur Dr.Web ainsi que ses autres paramètres.

  Pour en savoir plus, consultez le **Manuel Administrateur**, la rubrique Configuration du Serveur Dr.Web → Journal.

- A l'aide de la commande de console :

  ```
  drwcsd [<clés>] install
  ```

  Vous pouvez spécifier n'importe quel niveau de détails du journal du Serveur Dr.Web avec la clé `--verbosity`.

  Pour plus d'informations sur les clés de ligne de commande pour gérer le Serveur Dr.Web, consultez la section G3.8. Description des clés.

  Exemple d'une commande pour spécifier le niveau de détails de journalisation **Trace** :

  ```
  drwcsd --daemon "--home=C:\Program Files\DrWeb Server" "--bin-root=C:
  \Program Files\DrWeb Server" "--var-root=C:\Program Files\DrWeb Server\var"
  --verbosity=trace --log="C:\Program Files\DrWeb Server\var\install.log" --
  rotate=10,50m install
  ```

  Les autres clés sont obligatoires, notamment si les chemins standard de l'installation du Serveur Dr.Web et de ses répertoires ont été redéfinies.

  Après la modification du niveau de journalisation, il faut redémarrer le Serveur Dr.Web :

  ```
  drwcsd restart
  ```

- A l'aide des commandes se trouvant dans le menu principal de Windows **Démarrer**.

  Dans ce cas, uniquement deux niveaux de détails de journal sont disponibles **Détaillé** ou **Standard** :

a) **Logiciels** → **Dr.Web Server** → **Journal détaillé**
ou
Logiciels → **Dr.Web Server** → **Journal par défaut**

b) **Logiciels** → **Dr.Web Server** → **Redémarrer**.

Localisation automatique d'un poste tournant sous l'OS Android

Dr.Web Enterprise Security Suite permet de fournir automatiquement à l'administrateur les informations de la localisation des appareils mobiles protégés tournant sous Android.

Pour déterminer la localisation de l'appareil mobile :

1. Configurez le transfert des données de localisation de l'appareil mobile sur le Serveur Dr.Web :
   a) Dans la Centre de gestion de sécurité Dr.Web, dans la section **Réseau antivirus**, dans l'arborescence du réseau, sélectionnez un poste ou un groupe de postes tournant sous Android.
   b) Sélectionnez l'élément **Dr.Web pour Android** dans le menu de gestion.
   c) Dans l'onglet **Général**, cochez la case **Suivre la localisation**. Dans la liste déroulante **Périodicité de transfert des coordonnées**, sélectionnez une valeur selon laquelle les données de localisation de l'appareil seront actualisées.
   d) Enregistrez les modifications apportées.
2. La localisation est déterminée automatiquement par l'un des moyens suivants :
   - Si les fournisseurs de localisation (GPS, réseaux mobiles) sont activés sur l'appareil ou qu'il y a un signal stable, la localisation se fait par des outils de l'appareil mobile.
   - Si les fournisseurs de localisation (GPS, réseaux mobiles) sont desactivés sur l'appareil ou qu'il n'y a pas de signal stable, Dr.Web Enterprise Security Suite donne la possibilité d'utiliser la technologie Yandex.Locator pour localiser l'appareil par les coordonnées des antennes-relais de téléphonie mobile (GSM, 3D, LTE) et de WiFi ID.
     Pour configurer la technologie Yandex.Locator, il faut activer et configurer l'**Extension Yandex.Locator** :
     a) Obtenez une clé API sur le site de Yandex par le lien suivant : https://yandex.ru/dev/locator/keys/.
     b) Cochez la case **Extension Yandex.Locator** dans le Centre de gestion de sécurité, dans la section **Administration** → **Configuration du Serveur Dr.Web** → **Modules**.
     c) Dans le champ **Clé API**, entrez la clé obtenue à l'étape a).
     d) Enregistrez les modifications apportées et redémarrez le Serveur Dr.Web.

L'utilisation de WiFi ID est possible uniquement pour les appareils mobiles tournant sous Android 5.1 ou une version antérieure.

3. Pour consulter la localisation d'un poste dans le Centre de gestion de la sécurité Dr.Web :
   a) Dans la section **Réseau antivirus**, dans l'arborescence du réseau, sélectionnez un poste pour lequel vous avez spécifié les paramètres à l'étape 1.
   b) Dans les propriétés du poste, dans la section **Localisation**, les cordonnées géographiques reçues de l'appareil mobile seront automatiquement indiquées.
   c) Cliquez sur **Afficher sur la carte** pour voir la localisation géographique de l'appareil mobile sur OpenStreetMap selon les coordonnées reçues.

Critères de l'analyse fonctionnelle

Les critères de l'analyse fonctionnelle permettent de construire la protection maximale, c'est pourquoi il est nécessaire de les spécifier lors de la configuration de l'analyse fonctionnelle.

La section **Critères de l'analyse fonctionnelle** contient les catégories que vous pouvez utiliser pour la protection du profil. La sélection des catégories dépend du niveau de sécurité nécessaire et des particularités du système. Valeur par défaut de tous les paramètres : **Désactivé**.

Catégories de critères de l'analyse fonctionnelle

Lancement d'applications

Active le contrôle des processus lancés pour la liste des applications de confiance.

- *Bloquer le lancement des applications signées par des certificats connus dans Doctor Web comme des certificats pour les adwares.*
  Bloque le lancement des applications pouvant diffuser de la publicité.
- *Bloquer le chargement des applications signées par des certificats connus dans Doctor Web comme gris.*
  Bloque le lancement des applications signées par des certificats « gris ». Ce type de certificats est souvent utilisé pour signer des applications non sécurisées.
- *Bloquer le lancement des applications signées par des certificats connus dans Doctor Web comme des certificats pour les hacktools.*
  Bloque le lancement des applications signées par les certificats qui sont utilisés pour le piratage de logiciels. Il est recommandé d'utiliser ce critère.
- *Bloquer le lancement des applications signées par des certificats falsifiés/corrompus.*
  Bloque le lancement des applications malveillantes signées par des certificats invalides (corrompus ou joints au fichier binaire pour empêcher la détermination de la menace - par exemple, par les certificats du logiciel licite). Cela peut également être utile en cas de tentatives de modifier le fichier licite ou infecter par un virus. Il est recommandé d'utiliser ce critère.
- *Bloquer le lancement des applications signées par des certificats connus dans Doctor Web comme des certificats pour les programmes malveillants.*
  Bloque le lancement des applications signées par des certificats compromis. Il est recommandé d'utiliser ce critère.
- *Bloquer le lancement des applications signées par des certificats annulés.*
  Bloque le lancement des applications signées par des certificats volés ou compromis. Il est recommandé d'utiliser ce critère car cela permet de prévenir le lancement des applications malveillantes.
- *Bloquer le lancement des applications signées par des certificats auto-signés.*
  Bloque des logiciels contrefaits qui peuvent être malveillants. Les programmes malveillants peuvent ajouter à ses fichiers binaires une signature falsifiée avec un nom connu (par

exemple, Microsoft) et/ou ajouter un certificat racine dans le système pour que ce fichier soit affiché et traité par l'OS comme celui signé d'une manière légale.

- *Bloquer le lancement des applications non signées.*
  Bloque le lancement des applications malveillantes ou non fiables dont la source n'est pas connue.
- *Bloquer le lancement des utilitaires de Sysinternals.*
  Protège le système contre la compromission via les utilitaires Sysinternals.

Si la case **Autoriser le lancement des applications système et des applications de Microsoft** est cochée dans l'onglet **Autorisations**, les utilitaires Sysinternals seront lancés même si le lancement est bloqué.

- *Bloquer le lancement des applications depuis les flux alternatifs NTFS (ADS).*
  Les applications des flux alternatifs NTFS (ADS) sont souvent malveillantes c'est pourquoi l'utilisation de ce critère est obligatoire.
- *Bloquer le lancement des applications depuis le réseau et les ressources partagées.*
  Le lancement des applications depuis le réseau et les ressources partagées est un scénario inhabituel et peut compromettre la sécurité du système. Il est recommandé d'utiliser ce critère.
- *Bloquer le lancement des applications depuis les supports amovibles.*
  Le lancement des applications depuis les supports amovibles est un scénario inhabituel et peut compromettre la sécurité du système. Il est recommandé d'utiliser ce critère.
- *Bloquer le lancement des applications depuis les répertoires temporaires.*
  Bloque le lancement des applications depuis les répertoires temporaires
- *Bloquer le lancement des applications Windows/Microsoft Store (uniquement sous Windows 8 ou une version supérieure).*
  Bloque le lancement des applications téléchargées depuis Windows/Microsoft Store.
- *Bloquer le lancement des applications avec une extension double/inhabituelle.*
  Bloque le lancement des applications suspectes avec une extension inhabituelle (par exemple, `*.jpg.exe`).
- *Bloquer le lancement des shells Bash et des applications WSL (uniquement sous Windows 10 ou une version supérieure).*
  Bloque le lancement des shells Bash et des applications WSL.

Exclusions du blocage ci-dessus :

- *Autoriser le lancement des applications système et des applications de Microsoft.*
- *Autoriser le lancement des applications connus ou celles de confiance Doctor Web.*
  Si activé, le fonctionnement des applications signées par le certificat fiable est autorisé.

Si cette option est activée, le fonctionnement des applications signées par le certificat fiable est autorisé. Cette fonction permet de ne pas créer trop de règles en se basant sur les données déjà analysées par Dr.Web. La fiabilité dans ce cas est basée sur la cryptographie, une large base qui est constamment mise à jour.

Téléchargement et exécution des modules

Active le contrôle des modules téléchargés. Les critères peuvent fonctionner en deux modes :

- *Contrôler le chargement et l'exécution de tous les modules*. L'option globale qui inclut le contrôle de modules pour les applications de confiance. Ce mode nécessite des ressources considérables c'est pourquoi il est recommandé de l'utiliser uniquement si vous avez besoin d'un contrôle élevé.
- *Contrôler le chargement et l'exécution des modules dans les applications hôtes*.
  Ce mode nécessite moins de ressources. Il contrôle le fonctionnement des modules uniquement dans les processus qui sont utilisés pour compromettre le système ou pour insérer un programme malveillant sous forme d'un fichier système ou d'un fichier fiable. Si vous n'avez pas besoin de contrôle élevé, utilisez ce mode. Dans ce mode vous pouvez :

- *Bloquer le chargement et l'exécution des modules signés par des certificats connus dans Doctor Web comme des certificats pour les adwares*.
  Bloque le lancement des modules pouvant diffuser de la publicité.
- *Bloquer le chargement et l'exécution des modules signés par des certificats connus dans Doctor Web comme gris*.
  Bloque le lancement des modules signés par des certificats « gris ». Ce type de certificats est souvent utilisé pour signer des applications non sécurisées.
- *Bloquer le chargement et l'exécution des modules signés par des certificats connus dans Doctor Web comme des certificats pour les hacktools*.
  Bloque le lancement des modules signés par les certificats qui sont utilisés pour le piratage de logiciels. Il est recommandé d'utiliser ce critère.
- *Bloquer le chargement et l'exécution des modules signés par des certificats falsifiés/corrompus*.
  Bloque le lancement des modules malveillants signés par des certificats invalides (corrompus ou joints au fichier binaire pour empêcher la détermination de la menace - par exemple, par les certificats du logiciel licite). Cela peut également être utile en cas de tentatives de modifier le fichier licite ou infecter par un virus. Il est recommandé d'utiliser ce critère.
- *Bloquer le chargement et l'exécution des modules signés par des certificats connus dans Doctor Web comme des certificats pour les programmes malveillants*.
  Bloque le lancement des modules signés par des certificats compromis. Il est recommandé d'utiliser ce critère.
- *Bloquer le chargement et l'exécution des modules signés par des certificats annulés*.
  Bloque le lancement des modules signés par des certificats volés ou compromis. Il est recommandé d'utiliser ce critère car cela permet de prévenir le lancement des applications qui peuvent être malveillantes.
- *Bloquer le chargement et l'exécution des modules signés par des certificats auto-signés*.
  Bloque des logiciels contrefaits qui peuvent être malveillants. Les programmes malveillants peuvent ajouter à ses fichiers binaires une signature falsifiée avec un nom connu (par exemple, Microsoft) et/ou ajouter un certificat racine dans le système pour que ce fichier soit affiché et traité par l'OS comme celui signé d'une manière légale.

- *Bloquer le chargement et l'exécution des modules non signés*.
  Bloque le lancement des modules malveillants ou non fiables dont la source n'est pas connue.
- *Bloquer le chargement et l'exécution des modules depuis des flux alternatifs NTFS (ADS)*.
  Les modules des flux alternatifs NTFS (ADS) sont souvent malveillantes c'est pourquoi l'utilisation de ce critère est obligatoire.
- *Bloquer le chargement et l'exécution des modules du réseau et des ressources partagées*.
  Le lancement des modules depuis le réseau et les ressources partagées est un scénario inhabituel et peut compromettre la sécurité du système. Il est recommandé d'utiliser ce critère.
- *Bloquer le chargement et l'exécution des modules depuis des supports amovibles*.
  Le lancement des modules depuis les supports amovibles est un scénario inhabituel et peut compromettre la sécurité du système. Il est recommandé d'utiliser ce critère.
- *Bloquer le chargement et l'exécution des modules des répertoires temporaires*.
  Bloque le lancement des modules depuis les répertoires temporaires.
- *Bloquer le chargement et l'exécution des modules avec une extension double/inhabituelle*.
  Bloque le lancement des modules suspects avec une extension inhabituelle (par exemple, *.jpg.exe).

Exclusions du blocage ci-dessus :

- *Autoriser le chargement et l'exécution des modules système et des modules de Microsoft*.
- *Autoriser le chargement et l'exécution des modules connus et des modules de confiance de Doctor Web*.
  Si activé, le fonctionnement des modules signés par le certificat fiable est autorisé.

Lancement des interpréteurs de script

Active le contrôle des scénarios de script lancés pour la liste des applications de confiance.

- *Bloquer le lancement des scripts CMD/BAT*.
  Bloque le lancement des fichiers avec les extensions `cmd` et `bat`.
- *Bloquer le lancement des scripts HTA*.
  Bloque le lancement des scripts HTA. Ces scripts peuvent traiter des scripts malveillants et télécharger des fichiers exécutables qui peuvent nuire au système.
- *Bloquer le lancement de VBScript/JavaScript*.
  Bloque le lancement des applications écrites en langages de script VBScript et JavaScript. Ces applications peuvent traiter des scripts malveillants et télécharger des fichiers exécutables qui peuvent nuire au système.
- *Bloquer le lancement des scripts PowerShell*.
  Bloque le lancement des scripts écrits en langage de script PowerShell. Ces scripts peuvent traiter des scripts malveillants et télécharger des fichiers exécutables qui peuvent nuire au système.

- *Bloquer le lancement des scripts REG.*
  Bloque le lancement des scripts de registre (fichiers avec l'extension `reg`). Ces fichiers peuvent être utilisés pour ajouter ou modifier les valeurs dans le registre.
- *Bloquer le lancement des scripts depuis les flux alternatifs NTFS (ADS).*
  Les applications des flux alternatifs NTFS (ADS) sont souvent malveillantes c'est pourquoi l'utilisation de ce critère est obligatoire.
- *Bloquer le lancement des scripts depuis le réseau et les ressources partagées.*
  Le lancement des modules depuis le réseau et les ressources partagées est un scénario inhabituel et peut compromettre la sécurité du système. Il est recommandé d'utiliser ce critère.
- *Bloquer le lancement des scripts depuis les supports amovibles.*
  Le lancement des scripts depuis les supports amovibles est un scénario inhabituel et peut compromettre la sécurité du système. Il est recommandé d'utiliser ce critère.
- *Bloquer le lancement des scripts depuis les répertoires temporaires.*
  Bloque le lancement des scripts depuis les répertoires temporaires.

Exclusions du blocage ci-dessus :

- *Autoriser le lancement des scripts système et des scripts de Microsoft.*
- *Autoriser le lancement des scripts connus ou des scripts de confiance de Doctor Web.*
  Si activé, le lancement des scripts signés par le certificat fiable est autorisé.

Téléchargement de pilotes,

Active le contrôle des pilotes téléchargés pour la liste des applications de confiance.

- *Bloquer le chargement des pilotes signés par des certificats connus dans Doctor Web comme des certificats pour les adwares.*
  Bloque le lancement des pilotes pouvant diffuser de la publicité.
- *Bloquer le chargement des pilotes signés par des certificats connus dans Doctor Web comme gris.*
  Bloque le lancement des pilotes signés par des certificats « gris ». Ce type de certificats est souvent utilisé pour signer des applications non sécurisées.
- *Bloquer le chargement des pilotes signés par des certificats connus dans Doctor Web comme des certificats pour les hacktools.*
  Bloque le lancement des pilotes signés par les certificats qui sont utilisés pour le piratage de logiciels. Il est recommandé d'utiliser ce critère.
- *Bloquer le chargement des pilotes signés par des certificats falsifiés/corrompus.*
  Bloque le lancement des pilotes malveillants signés par des certificats invalides (corrompus ou joints au fichier binaire pour empêcher la détermination de la menace - par exemple, par les certificats du logiciel licite). Cela peut également être utile en cas de tentatives de modifier le fichier licite ou infecter par un virus. Il est recommandé d'utiliser ce critère.
- *Bloquer le chargement des pilotes signés par des certificats connus dans Doctor Web comme des certificats pour les programmes malveillants.*

Bloque le lancement des pilotes signés par des certificats compromis. Il est recommandé d'utiliser ce critère.

- *Bloquer le chargement des pilotes signés par des certificats annulés.*
  Bloque le lancement des pilotes signés par des certificats volés ou compromis. Il est recommandé d'utiliser ce critère car cela permet de prévenir le lancement des applications malveillantes.
- *Bloquer le chargement des pilotes signés par des certificats auto-signés.*
  Bloque des logiciels contrefaits qui peuvent être malveillants. Les programmes malveillants peuvent ajouter à ses fichiers binaires une signature falsifiée avec un nom connu (par exemple, Microsoft) et/ou ajouter un certificat racine dans le système pour que ce fichier soit affiché et traité par l'OS comme celui signé d'une manière légale.
- *Bloquer le téléchargement des pilotes non signés.*
  Bloque le lancement des pilotes malveillants ou non fiables dont la source n'est pas connue.
- *Bloqueruer le chargement des pilotes de flux alternatifs NTFS (ADS).*
  Les applications des flux alternatifs NTFS (ADS) sont souvent malveillantes c'est pourquoi l'utilisation de ce critère est obligatoire.
- *Bloquer le chargement des pilotes du réseau et des ressources partagées.*
  Le chargement des pilotes depuis le réseau et les ressources partagées est un scénario inhabituel et peut compromettre la sécurité du système. Il est recommandé d'utiliser ce critère.
- *Bloquer le chargement des pilotes depuis des supports amovibles.*
  Le chargement des pilotes depuis les supports amovibles est un scénario inhabituel et peut compromettre la sécurité du système. Il est recommandé d'utiliser ce critère.
- *Bloquer le chargement des pilotes depuis les répertoires temporaires.*
  Bloque le lancement des pilotes depuis les répertoires temporaires
- *Bloquer le téléchargement des versions de pilotes vulnérables d'un logiciel populaire.*
  Bloque le téléchargement des versions non sécurisées de pilotes d'un logiciel populaire. Les pilotes d'un logiciel licite, par exemple VirtualBox, Asus, etc. peuvent être utilisés pour accéder au système via RDP. Une fois cette option activée, les versions non sécurisées de ces pilotes seront bloqués lors du téléchargement.

L'interdiction de télécharger des versions de pilotes vulnérables d'un logiciel populaire ne peut pas être annulée par les exclusions.

- Bloquer le lancement des pilotes avec un extension double/inhabituelle.
  Bloque le lancement des pilotes suspects avec une extension inhabituelle (par exemple, *.jpg.exe).

Exclusions du blocage ci-dessus :

- *Autoriser le chargement des pilotes système et des pilotes de Microsoft.*
- *Autoriser le chargement des pilotes connus et des pilotes de confiance de Doctor Web.*
  Si activé, le chargement des pilotes signés par un certificat fiable est autorisé.

Installation des paquets MSI

Active le contrôle des packages MSI lancés pour la liste des applications de confiance.

- *Bloquer l'installation des packages signés par des certificats connus dans Doctor Web comme des certificats pour les adwares.*
  Bloque le lancement des packages pouvant diffuser de la publicité.
- *Bloquer l'installation des packages signés par des certificats connus dans Doctor Web comme gris.*
  Bloque le lancement des packages signés par des certificats « gris ». Ce type de certificats est souvent utilisé pour signer des applications non sécurisées.
- *Bloquer l'installation des packages signés par des certificats connus dans Doctor Web comme des certificats pour les hacktools.*
  Bloque le lancement des packages signés par les certificats qui sont utilisés pour le piratage de logiciels. Il est recommandé d'utiliser ce critère.
- *Bloquer l'installation des packages signés par des certificats falsifiés/corrompus.*
  Bloque le lancement des packages malveillants signés par des certificats invalides (corrompus ou joints au fichier binaire pour empêcher la détermination de la menace - par exemple, par les certificats du logiciel licite). Cela peut également être utile en cas de tentatives de modifier le fichier licite ou infecter par un virus. Il est recommandé d'utiliser ce critère.
- *Bloquer l'installation des packages signés par des certificats connus dans Doctor Web comme des certificats pour les programmes malveillants.*
  Bloque le lancement des packages signés par des certificats compromis. Il est recommandé d'utiliser ce critère.
- *Bloquer l'installation des packages signés par des certificats annulés.*
  Bloque le lancement des packages signés par des certificats volés ou compromis. Il est recommandé d'utiliser ce critère car cela permet de prévenir le lancement des applications qui peuvent être malveillantes.
- *Bloquer l'installation des packages signés par des certificats auto-signés.*
  Bloque des logiciels contrefaits qui peuvent être malveillants. Les programmes malveillants peuvent ajouter à ses fichiers binaires une signature falsifiée avec un nom connu (par exemple, Microsoft) et/ou ajouter un certificat racine dans le système pour que ce fichier soit affiché et traité par l'OS comme celui signé d'une manière légale.
- *Bloquer l'installation des packages non-signés.*
  Bloque le lancement des packages malveillants ou non fiables dont la source n'est pas connue.
- *Bloquer le lancement des packages depuis les flux alternatifs NTFS (ADS).*
  Les applications des flux alternatifs NTFS (ADS) sont souvent malveillantes c'est pourquoi l'utilisation de ce critère est obligatoire.
- *Bloquer le lancement des packages depuis le réseau et les ressources partagées.*
  L'installation des packages depuis le réseau et les ressources partagées est un scénario inhabituel et peut compromettre la sécurité du système. Il est recommandé d'utiliser ce critère.

- *Bloquer l'installation des packages depuis les supports amovibles.*
  L'installation des packages depuis les supports amovibles est un scénario inhabituel et peut compromettre la sécurité du système. Il est recommandé d'utiliser ce critère.
- *Bloquer le lancement des packages depuis les répertoires temporaires.*
  Bloque le lancement des packages depuis les répertoires temporaires.

Exclusions du blocage ci-dessus :

- *Autoriser l'installation des paquets système et des paquets de Microsoft.*
- *Autoriser l'installation des paquets connus et des paquets de confiance de Doctor Web.*
  Si activé, l'installation des packages signés par le certificat fiable est autorisée.

Intégrité de fichiers exécutables

Active le contrôle d'intégrité des fichiers exécutables. Les critères **Intégrité de fichiers exécutables** sont utilisés uniquement dans des systèmes fonctionnant en mode d'exécution approuvée. Dans tels systèmes, tous les processus sont contrôlés par l'administrateur (par exemple, les distributeurs automatiques et d'autres systèmes). L'utilisation des critères **Intégrité de fichiers exécutables** dans d'autres systèmes peut entraîner des conséquences imprévisibles, jusqu'à la panne du poste.

- *Bloquer la création de nouveaux fichiers exécutables.*
  Bloque les tentatives de création des nouveaux fichiers exécutables sur le disque.
- *Bloquer la modification de fichiers exécutables.*
  Bloque les tentatives de modification des fichiers exécutables sur le disque.

Exclusions du blocage ci-dessus :

- *Autoriser la création et la modification des fichiers exécutables par les applications système signées ou les applications de Microsoft.*
- *Autoriser la création et la modification des fichiers exécutables par les applications signées connues ou les applications de confiance de Doctor Web.*
  Si activé, l'installation des packages signés par le certificat fiable est autorisée.

Les critères **Intégrité de fichiers exécutables** ne peuvent pas être annulés par les règles d'autorisation et les règles de blocage.

Exemples de l'accès à la base de données du Serveur Dr.Web

Ensuite, vous pouvez trouver les exemples de requêtes SQL à la base de données PostgreSQL. Les requêtes aux autres bases de données peuvent avoir certaines différences résultant des particularités de la base de données et de son utilisation.

Le langage SQL ne permet pas de respecter la hiérarchie de groupes et de postes dans des requêtes.

Pour accéder directement à la base de données

1. Ouvrez le Centre de gestion de votre Serveur Dr.Web.
2. Allez dans la section **Administration** → **Console SQL**.
3. Entrez la requête SQL nécessaire. Les exemples des requêtes sont listés ci-après.
4. Cliquez sur **Effectuer**.

Exemples de requêtes SQL

1. Trouver les postes sur lesquels la version serveur de Windows est installée et les bases virales sont plus anciennes que 2019.07.04-00:00:00 UTC (12.0).

```
SELECT
  stations.name Station,
  groups_list.name OS,
  station_products.crev Bases
FROM
  stations
  INNER JOIN groups_list ON groups_list.platform =(
    CAST(stations.lastos AS INTEGER) & ~15728640
  )
  AND (
    (
      CAST(stations.lastos AS INTEGER) & 2130706560
    ) = 33554560
  )
  INNER JOIN station_products ON station_products.id = stations.id
  AND station_products.product = '10-drwbases'
  AND station_products.crev < 12020190704000000;
```

2. Trouver les postes ayant des entrées avec le taux d'importance **Haute** ou **Maximale** dans la section **Réseau antivirus** → **Statistiques** → **Statut**.

```
SELECT
  stations.name Station
FROM
  stations
WHERE
  id IN (
    SELECT
      DISTINCT id
    FROM
      station_status
    WHERE
      severity >= 1342177280
  );
```

3. Recevoir la correspondance des statuts et du nombre de postes ayant ces statuts.

```
SELECT
  code Code,
  COUNT(code) Num
FROM
  (
    SELECT
      DISTINCT id,
      code
    FROM
      station_status
```

```
  ) AS t
GROUP BY
  Code
ORDER BY
  Code;
```

4. Recevoir 10 menaces les plus répandues détectées du 2019.06.01 au 2019.07.01 sur les postes faisant partie du groupe avec l'identificateur '373a9afb-9c9a-4d4d-b9b1-de817b96bcc5' ou dans un de ses sous-groupes.

```
SELECT
  cat_virus.str Threat,
  COUNT(cat_virus.str) Num
FROM
  station_infection
  INNER JOIN cat_virus ON cat_virus.id = station_infection.virus
WHERE
  station_infection.infectiontime BETWEEN 20190601000000000
  AND 20190701000000000
  AND station_infection.id IN (
    SELECT
      sid
    FROM
      station_groups
    WHERE
      gid = '373a9afb-9c9a-4d4d-b9b1-de817b96bcc5'
      OR gid IN (
        SELECT
          child
        FROM
          group_children
        WHERE
          id = '373a9afb-9c9a-4d4d-b9b1-de817b96bcc5'
      )
  )
GROUP BY
  cat_virus.str
ORDER BY
  Num DESC
LIMIT
  10;
```

5. Recevoir 10 postes les plus infectés.

```
SELECT
  Station,
  Grp,
  Num
FROM
  (
    SELECT
      stations.id,
      groups_list.id,
      stations.name Station,
      groups_list.name Grp,
      COUNT(stations.id) Num
    FROM
      station_infection
      INNER JOIN stations ON station_infection.id = stations.id
      INNER JOIN groups_list ON groups_list.id = stations.gid
    GROUP BY
      stations.id,
      groups_list.id,
      stations.name,
      groups_list.name
    ORDER BY
```

```
      Num DESC
    LIMIT
      10
  ) AS t;
```

6. Supprimer l'appartenance de tous les postes des groupes utilisateurs qui ne sont pas primaires pour ces postes.

```
DELETE FROM
  station_groups;
INSERT INTO station_groups(sid, gid)
SELECT
  stations.id,
  groups_list.id
FROM
  stations
  INNER JOIN groups_list ON stations.gid = groups_list.id
  AND groups_list.type NOT IN(1, 4);
```

7. Trouver les objets du réseau antivirus dans lesquels le domaine indiqué est présent dans la liste blanche du composant SpIDer Gate, dans les paramètres personnalisés.

```
SELECT
  stations.name Station
FROM
  station_cfg
  INNER JOIN stations ON stations.id = station_cfg.id
WHERE
  station_cfg.component = 38
  AND station_cfg.name = 'WhiteVirUrlList'
  AND station_cfg.value = 'domain.tld';
SELECT
  groups_list.name Grp
FROM
  group_cfg
  INNER JOIN groups_list ON groups_list.id = group_cfg.id
WHERE
  group_cfg.component = 38
  AND group_cfg.name = 'WhiteVirUrlList'
  AND group_cfg.value = 'domain.tld';
SELECT
  policy_list.name Policy
FROM
  policy_cfg
  INNER JOIN policy_list ON policy_list.id = policy_cfg.id
WHERE
  policy_cfg.component = 38
  AND policy_cfg.name = 'WhiteVirUrlList'
  AND policy_cfg.value = 'domain.tld';
```

8. Recevoir du Contrôle des événements les événements d'entrée échouée des Administrateurs dans le Centre de gestion avec les codes des erreurs d'authentification.

```
SELECT
  admin_activity.login Login,
  admin_activity.address Address,
  activity_data.value ErrorCode,
  admin_activity.createtime EventTimestamp
FROM
  admin_activity
  INNER JOIN activity_data ON admin_activity.record = activity_data.record
WHERE
  admin_activity.oper = 10100
  AND admin_activity.status != 1
  AND activity_data.item = 'Error';
```

9. Trouver les postes sous Windows sur lesquels les corrections de sécurité nécessaires ne sont pas installées.

```
SELECT
  stations.name Station
FROM
  stations
WHERE
  id NOT IN (
    SELECT
      station_env_kb.id
    FROM
      station_env_kb
      INNER JOIN stations ON stations.id = station_env_kb.id
    WHERE
      (
        CAST(stations.lastos AS INTEGER) & 2130706432
      )= 33554432
      AND station_env_kb.name IN (
        SELECT
          id
        FROM
          env_strings
        WHERE
          str IN(
            'KB4012212', 'KB4012213', 'KB4012214',
            'KB4012215', 'KB4012216', 'KB4012217',
            'KB4012598'
          )
      )
  );
```

Chapitre 4 : Dépannage

Diagnostic des problèmes de l'installation distante

Principe de l'installation :

1. Le Serveur Dr.Web se connecte à la ressource `ADMIN$` sur la machine distante `\\<machine_distante>\ADMIN$\Temp` et copie dans le répertoire `\\<machine_distante>\ADMIN$\Temp` son installateur réseau `drwinst.exe` se trouvant dans le répertoire `webmin\install\windows` du répertoire d'installation du Serveur Dr.Web et le certificat SSL `drwcsd-certificate.pem` se trouvant dans le répertoire `etc` du répertoire d'installation du Serveur Dr.Web.
2. Le Serveur Dr.Web lance le fichier `drwinst.exe` sur la machine distante avec les clés de la ligne de commande, correspondant aux paramètres dans le Centre de gestion.

Pour réussir l'installation, il est nécessaire que les conditions suivantes soient satisfaites sur le Serveur Dr.Web depuis lequel se fait l'installation :

1. La ressource `ADMIN$\Temp` doit être accessible sur la machine distante.

   L'accessibilité de la ressource peut être vérifiée de la manière suivante :

   Dans la ligne d'adresse de l'application `Windows Explorer`, entrez :

   `\\<machine_distante>\ADMIN$\Temp`

   Alors vous devez être invités à entrez le nom d'utilisateur et le mot de passe pour accéder à cette ressource. Veuillez entrer les identifiants qui ont été spécifiées à la page d'installation.

   La ressource `\ADMIN$\Temp` peut être inaccessible pour des raisons listées ci-dessous :

   a) le compte n'a pas de droits d'administrateur ;

   b) la machine est déconnectée ou le pare-feu bloque l'accès au port 445 ;

   c) l'accès à la ressource `\ADMIN$\Temp` peut être restreinte sous Windows Vista ou supérieur s'ils ne font pas partie du domaine ;

   d) le titulaire du répertoire n'est pas présent ou l'utilisateur ou le groupe ne possèdent pas assez de droits.
2. L'accès au fichier `drwinst.exe` et à la clé de chiffrement publique `*.pub` doit être ouvert.

Le Centre de gestion affiche les informations exhaustives (étape et code d'erreur) pouvant aider à diagnostiquer la cause de l'erreur.

Liste des erreurs de l'installation distante de l'Agent Dr.Web

Étape	Erreur	Cause
Connexion au poste <*host*> via SMB	Adresse incorrecte du poste <*host*>	L'adresse IP spécifiée pour l'installation de l'Agent Dr.Web n'est pas une adresse IPv4/IPv6 correcte, ou bien, il est impossible de convertir le nom DNS en une adresse : ce nom DNS n'existe pas ou le Serveur de noms n'est pas correctement configuré.
	Erreur de connexion au poste <*host*> via SMB	Impossible de se connecter au poste via SMB. Causes possibles : • le service du serveur est désactivé sur le poste ; • le port TCP 445 sur la machine distante est indisponible, les causes possibles sont les suivantes : ▫ la machine est déconnectée ; ▫ le pare-feu bloque le port indiqué ; ▫ l'OS installé sur la machine distante n'est pas Windows ; • aucun modèle d'accès partagé et de sécurité pour les comptes locaux n'est configuré ; • serveur d'authentification indisponible (contrôleur de domaine) ; • utilisateur inconnu ou mot de passe invalide.
	Droits insuffisants pour ouvrir la ressource partagée <*share*> sur le poste <*host*>	La ressource `ADMIN$` n'existe pas sur la machine distante ou les droits sont insuffisant pour l'ouvrir.
Envoi des fichiers sur le poste <*host*>	Impossible de trouver le chemin <*path*> dans la ressource partagée <*share*> sur le poste <*host*>	Le répertoire `ADMIN$/TEMP` est introuvable.
	Impossible de créer le répertoire temporaire <*path*> dans la ressource partagée <*share*> sur le poste <*host*>	Impossible de créer le répertoire temporaire dans `ADMIN$/TEMP`, par exemple, les droits sont insuffisants pour écrire.

Étape	Erreur	Cause
	Impossible de supprimer le répertoire temporaire <*path*> dans la ressource partagée <*share*> sur le poste <*host*>	Impossible de supprimer le répertoire dans `ADMIN$/TEMP` après la fin de la procédure. Par exemple, le service n'a pas été terminé, ou bien quelqu'un a ouvert un fichier dans ce répertoire.
	Impossible d'ouvrir le fichier <*path*> en lecture sur le Serveur Dr.Web Impossible de lire le fichier <*path*> en lecture sur le Serveur Dr.Web	Le fichier d'installateur est introuvable sur le Serveur Dr.Web ou les droits invalides sont spécifiés pour le fichier d'installateur.
	Impossible d'ouvrir le fichier <*path*> en écriture dans la ressource partagée <*share*> sur le poste <*host*> Impossible d'écrire le fichier <*path*> dans la ressource partagée <*share*> sur le poste <*host*>	Droits insuffisants pour lire/écrire les fichiers correspondants ou dans les répertoires correspondants.
Création du service sur le poste <*host*>	Erreur de connexion au service de serveur (srvsvc RPC) sur le poste <*host*>	La gestion des services distants n'est pas disponible.
	Erreur de connexion au SCM sur le poste <*host*> Impossible de créer le service sur le poste <*host*> Impossible de lancer le service sur le poste <*host*> Impossible d'arrêter le service sur le poste <*host*> Impossible de supprimer le service sur le poste <*host*>	Droits insuffisants pour gérer les services.
Exécution du service sur le poste <*host*>	Impossible d'obtenir le statut du service sur le poste <*host*>	Erreur possible de SCM.
	L'installation sur le poste *{host}* est interrompue après le délai spécifié	L'installateur n'a pas réussi à installer l'Agent Dr.Web pendant le délai indiqué. Causes possibles : canal lent entre le poste

Étape	Erreur	Cause
		et le Serveur Dr.Web, temps insuffisant pour télécharger les données nécessaires.
	Impossible d'obtenir le chemin local vers la ressource partagée <*share*> sur le poste <*host*>	Impossible de déterminer le chemin sur le poste vers la ressource `ADMIN$`.
	Le service s'est arrêté avec une erreur sur le poste <*host*>. Statut d'arrêt <*state*>. Code d'erreur : <*rc*>.	Erreurs de l'installateur de l'Agent Dr.Web.

Résolution de l'erreur du service BFE lors de l'installation de l'Agent Dr.Web pour Windows

Le fonctionnement de certains composants de l'Antivirus Dr.Web pour Windows demande que le service du module de filtrage de base (BFE) soit lancé. Si ce service est introuvable ou endommagé, l'installation de l'Agent Dr.Web pour Windows sera impossible. La corruption ou l'absence du service BFE peut indiquer la présence de menaces sur le poste.

Si la tentative d'installation de l'Agent Dr.Web pour Windows se termine avec une erreur du service BFE, exécutez les actions suivantes :

1. Scannez le système du poste avec l'utilitaire CureNet! de Doctor Web.

   Vous pouvez demander la version de démo (diagnostic sans fonction de désinfection) de l'utilitaire ici : https://download.drweb.com/curenet/.

   Vous pouvez consulter les conditions d'utilisation et le prix de la version complète de l'utilitaire ici : https://estore.drweb.com/utilities/.
2. Lancez ou redémarrez manuellement le service BFE. Si vous n'arrivez pas à lancer le service BFE ou que ce service n'est pas présent dans la liste, contactez le service technique de Microsoft.
3. Lancez l'installateur de l'Agent Dr.Web pour Windows et effectuez l'installation conformément à la procédure standard décrite dans le **Manuel d'installation**.

   Si le problème persiste, veuillez contacter le service de support technique de Doctor Web.

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 :

1. Consultez les dernières versions des descriptions et des manuels à l'adresse https://download.drweb.com/doc/.
2. Lisez la rubrique de questions fréquentes à l'adresse https://support.drweb.com/show_faq/.
3. 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 :

1. Remplissez le formulaire de question dans la section correspondante de la rubrique https://support.drweb.com/.
2. Appelez le numéro de l'assistance technique française 0 825 300 230 ou le numéro de l'assistance internationale +7 (495) 789 45 86. Les utilisateurs en Russie peuvent nous contacter en appelant le numéro vert 8 800 333 7932.

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/.

Référence