



Dr.WEB

CureNet!

Manuel Administrateur



© **Doctor Web, 2018. Tous droits réservés**

Le contenu publié dans cette documentation est la propriété de la société Doctor Web et ne peut être utilisé par l'acheteur du produit qu'à des fins non commerciales. Aucune partie de cette documentation ne peut être copiée, publiée sur un lecteur réseau ou diffusée dans les médias ou ailleurs sans faire référence à la source, à moins qu'elle ne soit utilisée à des fins personnelles.

Marques déposées

Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-Desk et le logo Dr.WEB sont des marques déposées de Doctor Web en Russie et/ou dans d'autres pays. Toute autre marque ou logo ainsi que les noms de société cités ci-dessous appartiennent à leurs propriétaires.

Limitation de responsabilité

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

Dr.Web CureNet!
Version 11.0.0
Manuel Administrateur
03/08/2018

Doctor Web, Siège social en Russie

125124

Moscou, Russie

2-12A, 3e rue Yamskogo polya

Site web : <http://www.drweb.com/>

Téléphone : +7 (495) 789-45-87

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

Doctor Web

Doctor Web – éditeur russe de solutions de sécurité informatique.

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

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

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

Nous remercions tous nos clients pour leur soutien des produits Dr.Web !



Contenu


| | |
|--|-----------|
| 1. Légende | 5 |
| 2. Dr.Web CureNet! | 6 |
| 2.1. Pré-requis système | 6 |
| 2.2. Préparation des postes | 7 |
| 2.3. Configuration du contrôleur de domaine Active Directory | 11 |
| 2.4. Licence | 12 |
| 3. Lancement de Dr.Web | 14 |
| 4. Mise à jour | 15 |
| 5. Fonctions de Dr.Web | 17 |
| 5.1. Profils | 18 |
| 5.2. Sélection des postes | 20 |
| 5.3. Sélection du mode de fonctionnement | 23 |
| 5.4. Configuration supplémentaire | 24 |
| 5.4.1. Onglet Général | 25 |
| 5.4.2. Onglet Exclusions | 26 |
| 5.4.3. Onglet Actions | 28 |
| 5.4.4. Onglet Réseau | 29 |
| 5.4.5. Onglet Mise à jour | 30 |
| 5.5. Rapport sur le fonctionnement de Dr.Web | 30 |
| 5.6. Gestionnaire de Quarantaine | 33 |
| 6. Annexe A. Support technique | 37 |
| 7. Annexe B. Méthodes de Détection | 38 |
| 8. Annexe C. Masques réseau | 40 |



1. Légende

Les styles de texte ci-dessous sont utilisés dans ce manuel :

Tableau 1. Légende.

| Styles | Description |
|---|--|
|  | Remarque importante ou indication. |
| <i>Réseau antivirus</i> | Nouveau terme ou accent porté sur un terme dans des descriptions. |
| <IP-address> | Champs de remplacement des noms fonctionnels par les valeurs effectives. |
| Enregistrer | Noms des boutons de l'écran, des fenêtres, des éléments de menu et d'autres éléments de l'interface du logiciel. |
| CTRL | Noms des touches du clavier. |
| C:\Windows\ C:\Windows\ | Noms des fichiers et des répertoires, fragments du code du programme. |
| Annexe A | Liens aux autres chapitres du manuel ou liens aux ressources externes. |



2. Dr.Web CureNet!

Dr.Web est destiné à réaliser via le réseau une analyse antivirus centralisée des ordinateurs et des serveurs distants fonctionnant sous l'OS Windows. Le produit ne nécessite pas d'installation et effectue l'analyse et la désinfection des objets malveillants détectés, même si sur les ordinateurs analysés (ci-après - les postes) sont installés des logiciels antivirus d'autres éditeurs. La vitesse de diffusion de l'antivirus, la vitesse de l'analyse ainsi que la rapidité de collecte des statistiques ne dépendent pas de la bande passante de la connexion. L'analyse peut être réalisée même dans les réseaux complètement isolés d'Internet.

Dr.Web vous offre les avantages suivants :

- analyse centralisée des postes tournant sous Windows et réunis sur un réseau ;
- gestion centralisée de réactions sur la détection de menaces ;
- désinfection des objets infectés ;
- scan des archives et des conteneurs de fichiers ;
- mises à jour régulières des bases virales et des modules de programme ;
- rapidité du scan ;
- récolte des statistiques du scan antivirus ;
- sauvegarde du rapport sur les résultats du scan à distance au format CSV ou XML.

2.1. Pré-requis système

Pré-requis système pour l'ordinateur de l'administrateur

Dr.Web CureNet! peut être installé et fonctionne sur les ordinateurs possédant au minimum ces pré-requis.

Tableau 2. Pré-requis système.

| Spécification | Pré-requis |
|--------------------------|--|
| Plateforme | Processeur pleinement compatible i686 et supérieur. |
| RAM libre | Au moins 360 Mo |
| Espace sur le disque dur | Supérieur ou égal à la taille des bases virales et des modules de Dr.Web CureNet! (au moins 200 Mo). |
| Système d'exploitation | <ul style="list-style-type: none">• Window XP Professionnel avec Service Pack 2 ou supérieur ;• Microsoft Windows Server® 2003 avec Service Pack 1 ou supérieur ;• Windows Vista (édition Professionnel, Entreprise ou Intégrale) avec Service Pack 1 ou supérieur ; |



| Spécification | Pré-requis |
|---------------|--|
| | <ul style="list-style-type: none">• Microsoft Windows Server 2008 ;• Microsoft Windows 7 (édition Professionnel, Entreprise ou Intégrale) ;• Microsoft Windows Server 2008 avec Service Pack2 ;• Windows 8 et 8.1 (édition Professionnel ou Entreprise) ;• Microsoft Windows Server 2012 ;• Windows 10. |
| Autre | <p>Une connexion Internet pour les mises à jour des bases virales et des composants de Dr.Web.</p> <p>La connexion à tous les postes à scanner s'effectue via le protocole TCP/IP.</p> |

D'autres pré-requis système sont similaires à ceux du système d'exploitation correspondant.

Pré-requis système pour les postes

Les pré-requis système pour les postes sont les mêmes que pour l'ordinateur sur lequel démarre la Console d'administration, sauf le suivant :

- **Système d'exploitation** : Windows XP Professional SP2 ou supérieur, sauf les versions suivantes pour les systèmes de 64 bits : Windows Server 2003 x64 Edition et Windows XP Professional SP2 x64 Edition.
- **Autre** : une connexion Internet n'est pas requise.

2.2. Préparation des postes

Pour réaliser le scan des postes, il est nécessaire de satisfaire à toutes les conditions suivantes :

- l'option **Découverte de réseau** doit être activée sur l'ordinateur sur lequel est lancée la Console d'administration, si vous comptez rechercher les postes par ce moyen ;
- l'ordinateur distant doit être accessible via le réseau ;
- le compte sous lequel s'effectue la connexion doit être opérationnel et avoir assez de privilèges ;
- si l'ordinateur distant est protégé par un pare-feu, les paramètres avancés doivent être configurés.

Si vous utilisez le pare-feu Windows, ouvrez l'onglet **Paramètres avancés** dans ces paramètres, sélectionnez **Règles de trafic entrant** et activez les exclusions suivantes : **Service Accès réseau (NP-In)** et **Partage de fichiers et d'imprimantes (SMB-In)**. Les exclusions pour le profil du pare-feu **Private** doivent être activées. Si le poste se trouve dans le domaine, les exclusions pour le profil **Domain** doivent être activées.

Si vous utilisez d'autres pare-feux, il faut ouvrir le port 445.



- il est nécessaire d'effectuer une configuration supplémentaire (voir [Configuration supplémentaire](#)).

Avant de procéder aux opérations, assurez-vous d'avoir toutes les informations nécessaires sur les identifiants d'administrateurs sur tous les ordinateurs distants à scanner.



Toutes les étapes de préparation du système d'exploitation sur l'ordinateur distant pour l'utilisation de Dr.Web CureNet! doivent être réalisées en mode administrateur.

Configuration supplémentaire

Pour réaliser une analyse des postes distants, il est nécessaire de satisfaire simultanément aux conditions supplémentaires suivantes :

- les restrictions du système de contrôle de comptes utilisateur (UAC) doivent être désactivées, si le poste fonctionne sous l'OS Windows Vista ou supérieur. Si vous utilisez le compte administrateur intégré, la configuration de ce paramètre n'est pas requise. Passez à l'étape suivante.

Ouvrez l'éditeur de la base de registre du système d'exploitation.

1. Trouvez et sélectionnez la branche suivante
HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM.
2. Si la clé **LocalAccountTokenFilterPolicy** n'est pas présente dans la branche, créez-la :
 - a. Dans le menu **Édition**, sélectionnez la commande **Créer**, puis **Valeur DWORD**.
 - b. Entrez le nom de la clé **LocalAccountTokenFilterPolicy**.
3. Dans le menu contextuel de la clé **LocalAccountTokenFilterPolicy**, sélectionnez **Modifier**.
4. Dans le champ **Valeur**, saisissez **1**.
5. Appuyez sur **OK** et quittez l'éditeur.
6. Redémarrez la machine.
7. Reproduisez la procédure pour tous les postes à scanner.



Cette opération doit être effectuée par l'administrateur ou par un utilisateur expérimenté. Une fausse manoeuvre lors de la modification de la base de registre peut endommager le système. Les spécialistes de Microsoft recommandent de créer une copie de sauvegarde des données importantes conservées sur l'ordinateur avant de procéder à la modification de la base de registre.

- tous les services requis pour le fonctionnement du réseau doivent être installés et configurés ;



Vérification de la configuration réseau

1. Ouvrez le Panneau de configuration sur le poste.
 - lorsque vous configurez des systèmes pris en charge antérieurs à Windows Vista, sélectionnez la rubrique **Connexions réseau** (si la rubrique n'est pas affichée, cliquez sur le bouton **Basculer vers l'affichage classique**).
 - lorsque vous configurez Windows Vista, sélectionnez le mode d'affichage par catégorie. Dans la catégorie **Réseau et Internet**, sélectionnez **Afficher l'état et la gestion du réseau** → **Gestion des connexions du réseau** ;
 - lorsque vous configurez Windows 7 ou Windows Server 2008, sélectionnez le mode d'affichage par catégorie. Dans la catégorie **Réseau et Internet**, sélectionnez **Afficher l'état et la gestion du réseau** → **Modifier les paramètres de la carte**.
 - lorsque vous configurez Windows 8, Windows 10 ou Windows Server 2012, dans la catégorie **Réseau et Internet** sélectionnez **Centre de gestion du réseau et du partage** → **Modifier les paramètres de la carte**.
 - lorsque vous configurez Windows 10 dans la catégorie **Réseau et Internet**, ouvrez l'un des onglets **VPN**, **Ethernet** ou **Numérotation**, sélectionnez **Centre de gestion du réseau et du partage** → **Modifier les paramètres de la carte**.
 2. Cliquez droit sur la connexion nécessaire et sélectionnez l'élément **Propriétés**.
 3. Vérifiez que les services suivants sont installés et configurés pour la connexion sélectionnée :
 - client pour les réseaux Microsoft ;
 - service du partage de fichiers et d'imprimantes pour les réseaux Microsoft ;
 - protocole Internet en version 4 (TCP/IPv4) ou en version 6 (TCP/IPv6).
 4. Enregistrez les modifications et fermez la fenêtre de configuration.
- les paramètres de partage doivent autoriser la configuration avancée ;

Configuration du partage

1. Ouvrez le Panneau de configuration sur le poste.
 - lorsque vous configurez Windows XP ou Windows Server 2003, sélectionnez l'élément **Pare-feu Windows** (si la rubrique n'est pas présente, cliquez sur **Basculer vers l'affichage standard**) ;
 - lorsque vous configurez Windows Vista, sélectionnez le mode d'affichage par catégorie. Dans la catégorie **Réseau et Internet**, sélectionnez **Configuration du partage de fichiers** ;
 - lorsque vous configurez Windows 7 ou Windows Server 2008, sélectionnez le mode d'affichage par catégorie. Dans la catégorie **Réseau et Internet**, sélectionnez **Centre de gestion du réseau et du partage**, puis sélectionnez **Modifier les paramètres du partage** ;



- lorsque vous configurez Windows 8, Windows 10 ou Windows Server 2012, dans la catégorie **Réseau et Internet**, sélectionnez **Centre de gestion du réseau et du partage**, puis sélectionnez **Modifier les paramètres avancés du partage**.
2. Dans la fenêtre qui s'affiche, effectuez l'une des actions suivantes :
 - si vous configurez Windows XP ou Microsoft Windows Server 2003, passez à l'onglet **Exclusions** et activez le paramètre **Partage de fichiers et d'imprimantes** ;
 - si vous configurez Windows Vista, activez **Découverte du réseau** et sélectionnez **Partage de fichiers** ;
 - si vous configurez Windows 7, sélectionnez **Activer la découverte de réseau** et **Activer le partage de fichiers et d'imprimantes** ;
 - si vous configurez Microsoft Windows Server 2008, Windows 8, Windows 10 ou Microsoft Windows Server 2012, sélectionnez **Activer le partage de fichiers et d'imprimantes**.
 3. Enregistrez les modifications et fermez la fenêtre de configuration.
- pour les comptes locaux, il faut utiliser le modèle standard de partage et de sécurité.

Configuration d'un modèle de partage et de sécurité

1. Ouvrez le Panneau de configuration sur le poste.
 - lorsque vous configurez des systèmes pris en charge antérieurs à Windows Vista, sélectionnez l'élément **Outils d'administration** (si la rubrique n'est pas affichée, cliquez sur le bouton **Basculer vers l'affichage classique**) et lancez l'utilitaire **Stratégie de sécurité locale**.
 - lorsque vous configurez Windows Vista et les systèmes plus récents, sélectionnez le mode d'affichage par catégorie. Dans la catégorie **Système et sécurité**, sélectionnez le groupe **Outils d'administration** et lancez l'utilitaire **Stratégie de sécurité locale**.



Pour lancer l'utilitaire de configuration des politiques de sécurité locales, vous pouvez saisir dans le champ de recherche Windows la commande **secpol.msc**, puis cliquez sur ENTER.

2. Dans l'arborescence de la console, sélectionnez le groupe **Stratégies locales**, puis — le groupe **Paramètres de sécurité**.
3. Cliquez droit sur le paramètre **Accès réseau : modèle de partage et de sécurité pour les comptes locaux**, sélectionnez l'élément **Propriétés** et définissez la valeur **Classique — les utilisateurs locaux s'authentifient eux-mêmes**.



Par défaut, une connexion à un poste distant ne peut pas être établie si le compte utilisé contient un mot de passe vide. Pour vous connecter, spécifiez un mot de passe non vide.

4. Fermez la console.



2.3. Configuration du contrôleur de domaine Active Directory

Si l'organisation utilise le contrôleur de domaine Active Directory, il est nécessaire de configurer

- paramètres du partage de fichiers et d'imprimantes ;
- paramètres de sécurité.

Vous pouvez créer un nouvel objet de stratégie de groupe (GPO) pour appliquer ces paramètres ou modifier les paramètres d'un objet existant.

Création d'un nouvel objet de stratégie de groupe

1. Entrez **gpmmc.msc** dans le champ de la fenêtre de ligne de commande et lancez la console de gestion des stratégies de groupe **GPMC**.
2. Créez un nouvel objet de stratégie de groupe, par exemple **GPO-CureNet**. Pour ce faire, cliquez droit sur **Objets de stratégie de groupe** dans l'arborescence de la console **GPMC** de la forêt et du domaine correspondants. Cliquez sur **Créer**. Dans la fenêtre qui s'affiche, indiquez un nouveau nom de l'objet et cliquez sur **OK**.
3. Attachez l'objet créé au domaine nécessaire.
4. Cliquez droit sur l'objet créé, sélectionnez **Modifier** et corrigez les paramètres nécessaires conformément à la description ci-dessous.

Si vous avez décidé de ne pas créer un nouvel objet, mais de modifier les paramètres d'un objet existant, ouvrez la fenêtre des paramètres correspondants.

1. Sur l'ordinateur sur lequel est installé la console de gestion des stratégies de groupe GPMC cliquez sur **Démarrage** → **Outils d'administration** → **Gestion des stratégies de groupe**.
2. Si la fenêtre de contrôle de comptes s'affiche, vérifiez les données et cliquez sur **Continuer**.
3. Dans la zone de navigation trouvez le noeud **Forêt : Nom de la forêt** et développez-le, puis développez le noeud **Objets de stratégie de groupe** et cliquez droit sur le nom de l'objet pour lequel vous voulez spécifier l'autorisation.
4. Dans le menu qui s'affiche, sélectionnez **Modifier**.

Configuration de partage de fichiers et d'imprimantes

Autorisez les requêtes entrantes d'ordinateurs client pour l'accès aux fichiers. L'activation de cette exception du pare-feu ouvre les ports UDP 137 et 138 et le port TCP 445 pour les adresses IP indiquées dans cette règle.



Autorisation du partage de fichiers et d'imprimantes

1. Dans la zone de navigation de la fenêtre affichée développez les noeuds suivants : **Configuration ordinateur** → **Stratégies** → **Modèles d'administration** → **Réseau** → **Mise en réseau** → **Pare-feu Windows** → **Profil du domaine**.
2. Dans la zone de notification double-cliquez sur le paramètre **Pare-feu Windows : Autorise l'exception de partage de fichiers et d'imprimantes** et activez cette règle dans l'onglet de paramètres.
3. Dans le champ **Autoriser des messages entrants non-requis de ces adresses IP** spécifiez une plage nécessaire.
4. Cliquez sur **OK** pour enregistrer les modifications.

Configuration des paramètres de sécurité

Configurez la stratégie **Accès réseau** : modèle de partage et de sécurité pour les comptes locaux de sorte qu'au moment de connexion au réseau avec les données du compte local, le contrôle d'authenticité s'effectue conformément à ces données.

Autorisation d'accès réseau via les comptes locaux d'utilisateurs


1. Dans la zone de navigation de la fenêtre affichée développez les noeuds suivants : **Configuration Ordinateur** → **Stratégies** → **Configuration Windows** → **Paramètres de sécurité** → **Stratégies locales** → **Paramètres de sécurité**.
2. Définissez la valeur **Classique — les utilisateurs locaux s'authentifient eux-mêmes** pour la stratégie **Accès réseau : modèle de partage et de sécurité pour les comptes locaux**.

Application des modifications dans le domaine

Pour appliquer les modifications de stratégies de groupe dans le domaine, dans les deux cas (lors de la création d'un nouvel objet et lors de la modification d'un objet existant) entrez la commande **gpupdate /force**.

2.4. Licence

Acheter une licence

Pour utiliser Dr.Web, vous devez avoir une licence autorisant toutes les fonctionnalités de l'application. Vous pouvez acheter une licence sur le [site](#) de Doctor Web. Il existe deux limitations de licence: la durée de validité et le nombre de postes sélectionnés en mêmes temps pour l'analyse. Les paramètres de votre licence sont sauvegardés dans le fichier clé. Pour les consulter, cliquez sur le bouton **Aide**  et sélectionnez l'élément **A propos de**.

Le fichier clé possède l'extension .key et contient les informations suivantes :




- durée de la licence pour le produit ;
- liste des composants autorisés à utiliser ;
- période pendant laquelle la mise à jour est autorisée (délai de souscription ; peut ne pas coïncider avec le délai d'utilisation) ;
- autres restrictions (par exemple, le nombre d'ordinateurs sur lesquels vous êtes autorisé à utiliser l'antivirus).

Lors du fonctionnement de Dr.Web, le fichier clé doit se trouver dans le même dossier dans lequel vous avez extrait les fichiers du programme. S'il y a plusieurs fichiers clé, Dr.Web va sélectionner le fichier autorisant l'opération demandée. Vous pouvez consulter l'information sur l'utilisation de la licence dans le fichier de journal **CureNet.log**.

Modifier les paramètres de la licence

Si nécessaire, vous pouvez étendre le nombre autorisé de postes ou prolonger la durée de validité de la licence. Pour ce faire :

1. Lancez la Console d'administration.
2. A l'étape 1, cliquez sur **Mon Dr.Web** ou à n'importe quelle étape, cliquez sur **Aide**  et sélectionnez l'élément **Mon Dr.Web**.

Dans la fenêtre de votre navigateur par défaut, sera ouverte votre page personnelle sur le site de Dr.Web où vous pouvez non seulement modifier les paramètres de votre licence mais aussi consulter toutes les informations sur la licence et poser des questions au support technique.

3. Téléchargez une version mise à jour du package d'installation de Dr.Web qui contient votre nouveau fichier clé.

Obtention d'une période de démonstration

Si avant l'achat, vous souhaitez tester le produit, activez la période de démo. Pour ce faire, veuillez remplir un formulaire spécial sur le [site](#) officiel de la société. Dans le mode de démonstration, Dr.Web CureNet! ne supporte pas la fonction de désinfection, cependant vous pouvez tester comment les processus de scan se propagent vers les postes dans le réseau local, vérifier les postes pour les menaces informatiques et recevoir un rapport sur les virus détectés (et non neutralisés) et sur les programmes malveillant trouvés. Pour désinfecter les postes, il faut acheter une licence commerciale.



3. Lancement de Dr.Web

Dr.Web ne nécessite aucune procédure d'installation. Pour commencer à utiliser le programme et lancer le premier scan, suivez les instructions suivantes :

- Copiez sur l'ordinateur de l'administrateur le package d'installation de Dr.Web et lancez-le. Les fichiers du programme vont s'extraire dans le dossier Dr.Web puis un référentiel Dr.Web sera créé de manière automatique et la Console d'administration démarrera.
- Vérifiez que vous pouvez accéder aux postes à scanner.
- Assurez-vous que les postes sont prêts à l'analyse.

La Console d'administration démarre automatiquement après l'extraction du package d'installation Dr.Web.

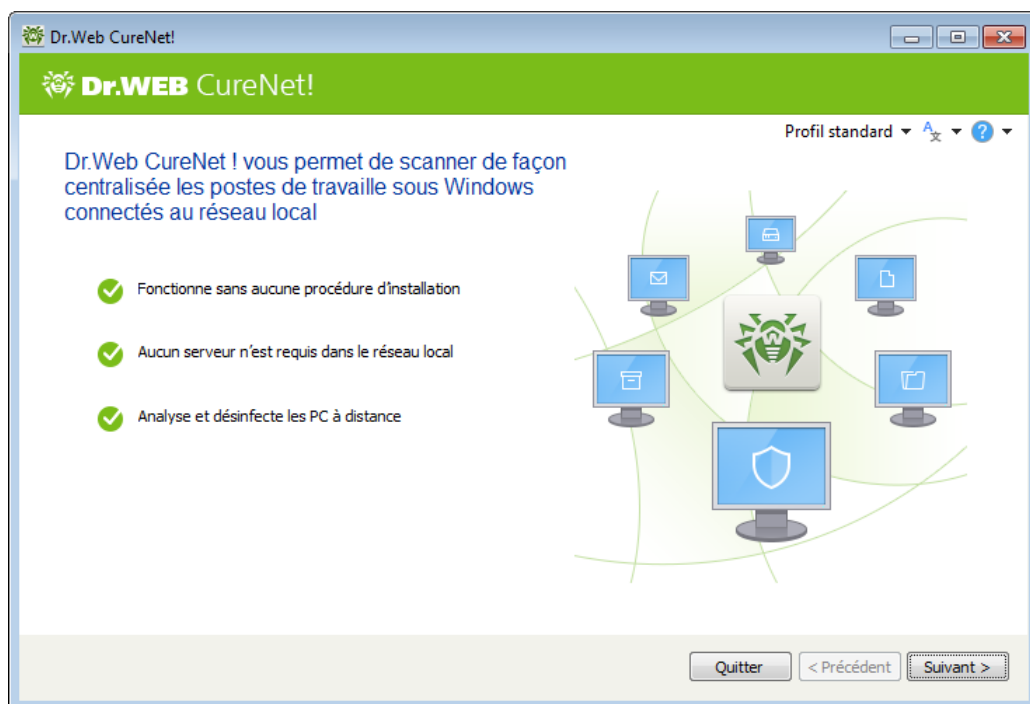


Figure 1. Console d'administration Dr.Web.



4. Mise à jour

Il est fortement recommandé d'installer toutes les mises à jour publiées par Doctor Web. Les mises à jour des bases virales permettent de détecter les virus auparavant inconnus, de bloquer leur diffusion et de désinfecter parfois les fichiers infectés qui n'étaient pas curables auparavant. Périodiquement, les algorithmes antivirus réalisés sous forme de fichiers exécutables ou de bibliothèques de programme sont améliorés. L'expérience obtenue lors de l'utilisation des antivirus Dr.Web permet de corriger les bugs détectés dans le logiciel, de mettre à jour les rubriques d'aide et la documentation.

Le logiciel Dr.Web est conçu afin de réaliser une analyse centralisée et permet ainsi d'assurer une protection maximale sans effectuer les mises à jour sur chaque ordinateur. Les bases virales Dr.Web sont téléchargées vers les postes à scanner depuis le référentiel des produits Dr.Web. Il suffit donc de mettre à jour les composants du référentiel de manière régulière afin de maintenir l'actualité des informations sur les programmes malicieux et les méthodes de neutralisation. Si les bases virales Dr.Web ne sont pas à jour pendant un certain temps, une alerte sera affichée dans la Console d'administration.



Il est interdit de créer ou de mettre à jour le référentiel de façon manuelle.

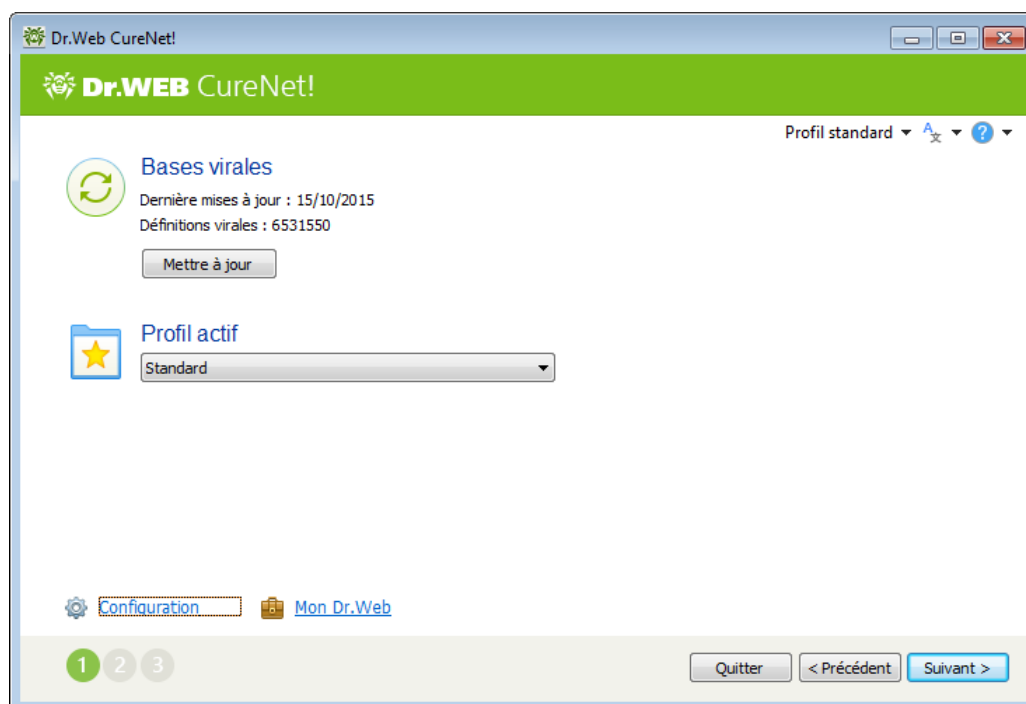


Figure 2. Mise à jour de Dr.Web.

Un accès à Internet est requis pour les mises à jour.



Mise à jour du référentiel Dr.Web CureNet!

1. Dr.Web vérifie si le fichier clé n'est pas bloqué sur le site de Doctor Web. Si le fichier clé valide est introuvable, une alerte est envoyée à l'utilisateur, la mise à jour n'est pas effectuée et les composants de logiciel peuvent être bloqués. Dans ce cas, veuillez acheter une licence ou contacter le [Support technique](#) de Doctor Web.
2. Si le fichier clé valide est trouvé, une mise à jour commence et pendant la mise à jour, Dr.Web télécharge tous les fichiers mis à jour et correspondant à la version du programme. Attendez que le processus se termine.


Console d'administration et les autres composants de programme peuvent être mis à jour automatiquement lors de la mise à jour du référentiel ou de la distribution de Dr.Web. Pendant la mise à jour du référentiel, Dr.Web vérifie la disponibilité du fichier contenant la nouvelle version de la console. Si la nouvelle version est disponible, vous serez invité à redémarrer le programme pour mettre à jour la Console d'administration. Sinon, la console sera mise à jour automatiquement pendant le lancement suivant du programme.

Notez qu'en cas d'utilisation de ce moyen de mise à jour de la Console, Dr.Web ne télécharge pas le fichier clé. Pour mettre à jour la licence dans le programme, veuillez mettre à jour la distribution via Mon Dr.Web.

Mise à jour du package d'installation de Dr.Web via la rubrique Mon Dr.Web



Le nombre de mises à jour du package d'installation du programme est illimité durant toute la période de validité de la licence.

1. Lancez la Console d'administration.
2. Dans la fenêtre de sélection de modes de l'analyse, cliquez sur **Mon Dr.Web** ou lors de n'importe quel étape, cliquez sur le bouton **Aide**  et puis sur **Mon Dr.Web**.
Votre espace personnel sera ouvert sous forme de page web sur le site de Doctor Web dans votre navigateur internet, depuis cette page vous pouvez télécharger une version renouvelée du package d'installation de Dr.Web (à condition que votre licence soit valable) ou renouveler votre licence.
3. Sauvegardez le package d'installation renouvelé de Dr.Web.
4. Lancez le package de Dr.Web pour déballer les fichiers du programme et démarrer la Console d'administration renouvelée.



5. Fonctions de Dr.Web

Le fonctionnement de Dr.Web est paramétré depuis la machine de l'administrateur avec la Console d'administration.



Il est recommandé de désactiver les mises à jour automatiques d'OS afin d'éviter d'éventuels problèmes de fonctionnement de Dr.Web.

Mise en route

1. Démarrez la Console d'administration et cliquez sur **Suivant**.
2. Dans la fenêtre qui s'affiche, vous pouvez sélectionner un [profil](#) nécessaire.
3. En cas de bases virales Dr.Web périmées, une notification correspondante sera affichée. Dans ce cas, il est fort recommandé de lancer le processus de mise à jour en cliquant sur le bouton **Mettre à jour**. Pour continuer, cliquez sur **Suivant**.
4. [Sélectionnez](#) les postes à scanner. Établissez une liste des comptes utilisés par Dr.Web pour se connecter aux postes sélectionnés. Cliquez sur **Suivant**. Une fenêtre de sélection de [mode de fonctionnement](#) va s'afficher.

Vous pouvez également [ajouter](#) de nouveaux postes plus tard : lors du scan ou lors de la gestion de la quarantaine.

Lancement et exécution de l'analyse

1. Sélectionnez le [mode d'analyse](#).
2. En cliquant sur le lien **Configuration**, vous pouvez consulter et si nécessaire modifier les paramètres de Scanner Dr.Web suivants :
 - [paramètres généraux](#) du fonctionnement des postes lors de l'analyse (notifications des utilisateurs, redémarrage des postes analysés, etc.) ;
 - analyse des [archives et des conteneurs](#) ;
 - [réaction](#) sur la détection des types particuliers de menaces ;
 - mode de [fonctionnement du réseau](#) lors de l'analyse et vérification de l'accessibilité des postes distants avant de procéder à la copie des fichiers de Dr.Web ;
 - paramètres de la [connexion réseau](#) utilisée pour la mise à jour du dépôt de Dr.Web.
3. Pour lancer l'analyse, cliquez sur **Start**.

Lors du scan vous pouvez ajouter de nouveaux postes, ainsi que suspendre, reprendre et arrêter le scan d'un poste en particulier. Pour ce faire, cliquez sur le nom du poste dans le tableau et dans le menu contextuel qui s'affiche, sélectionnez une action nécessaire.



Faites attention aux particularités suivantes de l'analyse :

- Les actions sur certains objets suspects ou infectés (par exemple, sur les clés de la base de registre, fichiers utilisés par des applications Windows) ne peuvent pas être réalisées immédiatement. En cas de détection de tels fichiers, le Scanner Dr.Web les marque comme les objets à traiter (selon l'action spécifiée) après le redémarrage de la machine et affiche un message correspondant dans le rapport. Afin de traiter correctement tels objets, vous pouvez autoriser le Scanner Dr.Web à redémarrer les OS sur les postes scannés si nécessaire ou à arrêter les postes après l'analyse de manière automatique. Dans ce cas-là, l'utilisateur du poste distant sera averti par un message de sorte qu'il a le temps d'achever son travail et de sauvegarder des informations nécessaires. Pour en savoir plus sur la configuration des actions appliquées aux objets malicieux, consultez la rubrique [Paramètres avancés](#) des actions.
- En cas de détection des virus dans le secteur boot (MBR), le Scanner Dr.Web redémarre le poste distant immédiatement après la détection du virus, dès que l'entrée correspondante est réparée (hard reset). Ce redémarrage s'effectue indépendamment du statut de la case **Redémarrer le poste**.

Le processus de scan sur les postes distants se déroule indépendamment de la Console d'administration. Pour quitter la Console d'administration, cliquez sur **Quitter**. Alors, le processus de scan des postes à distance continue mais les statistiques seront indisponibles.

Voir les résultats de recherche

La progression du processus ainsi que les résultats généraux de l'analyse sont affichés dans le [rapport](#) sur le fonctionnement de Dr.Web. Vous pouvez également sauvegarder le rapport vers un fichier au format CSV ou XML.

Vous pouvez également consulter les [informations détaillées](#) sur le scan d'un poste particulier.

Gestion de la quarantaine

1. Dans la fenêtre de sélection de [modes de fonctionnement](#), indiquez le mode **Gestionnaire de Quarantaine**.
2. Appuyez sur **Start**.
3. La fenêtre de [gestion de la quarantaine](#) va s'afficher. Dans cette fenêtre, vous pouvez consulter les informations concernant le statut de la quarantaine sur chaque poste sélectionné, récupérer les objets dans un dossier nécessaire, supprimer les objets ou les télécharger sur votre ordinateur.

5.1. Profils

Dr.Web permet de sauvegarder tous les paramètres de scan dans les fichiers de profils : la langue du programme, la liste des postes scannés, les comptes permettant d'accéder aux postes, la réaction du Scanner Dr.Web sur les menaces détectées ainsi que d'autres paramètres.

Création d'un nouveau profil

1. Lors de n'importe quel étape de l'analyse, cliquez sur le nom du profil en haut de la fenêtre (par défaut, **Profil standard**) et cliquez ensuite sur **Enregistrer**.
2. Dans la fenêtre qui s'affiche entrez le nom du nouveau profil de scan et le mot de passe pour y accéder si cela est nécessaire. Le mot de passe d'accès est requis uniquement lors de la sauvegarde des [mots de passe d'accès](#) aux postes.

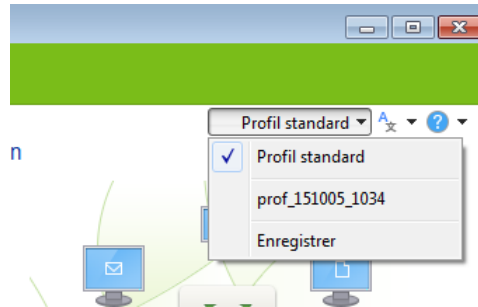


Figure 3. Profils.

3. Cliquez sur **Enregistrer**.
4. Passez aux étapes suivantes de l'analyse ou cliquez sur **Quitter**.

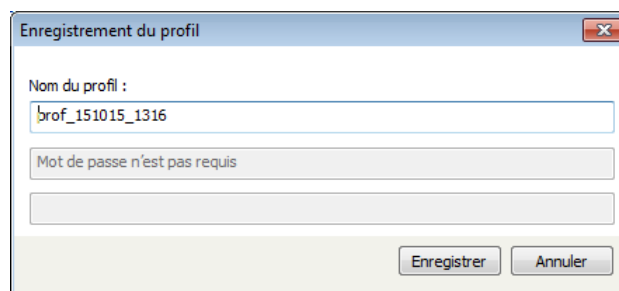


Figure 4. Enregistrement du profil.



Les modifications des paramètres ne peuvent pas être enregistrées automatiquement. Afin de sauvegarder les paramètres modifiés du profil de scan, réenregistrez le profil sous le même nom.

Se connecter au profil existant

1. Lors de n'importe quel étape de l'analyse, avant la sélection du [type d'analyse](#) cliquez sur le nom du profil en haut de la fenêtre (par défaut **Profil standard**) et sélectionnez le profil que vous souhaitez utiliser. Lors de l'étape [Mises à jour](#), vous pouvez également sélectionner un profil depuis la fenêtre Console d'administration.
2. Si nécessaire, spécifiez un mot de passe pour accéder au profil.

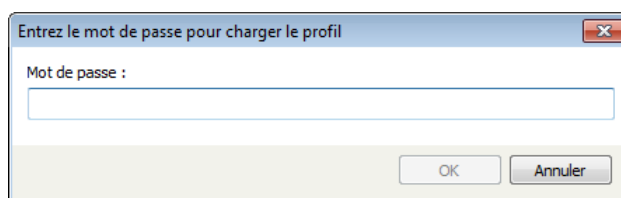


Figure 5. Chargement du profil.

3. La Console d'administration configure tous les paramètres de l'analyse conformément aux informations sauvegardées dans le profil sélectionné. Si nécessaire, vous pouvez modifier les paramètres lors des étapes correspondantes.

Suppression du profil

Il est impossible de supprimer les profils de scan avec les outils de Dr.Web. Pour supprimer un profil de scan, vous devez supprimer le fichier ayant le même nom dans le sous-dossier Profiles du répertoire Dr.Web.

5.2. Sélection des postes

A cette étape, vous pouvez sélectionner les postes à scanner ou les postes sur lesquels vous voulez gérer la quarantaine et spécifier les paramètres de connexion aux postes sélectionnés.

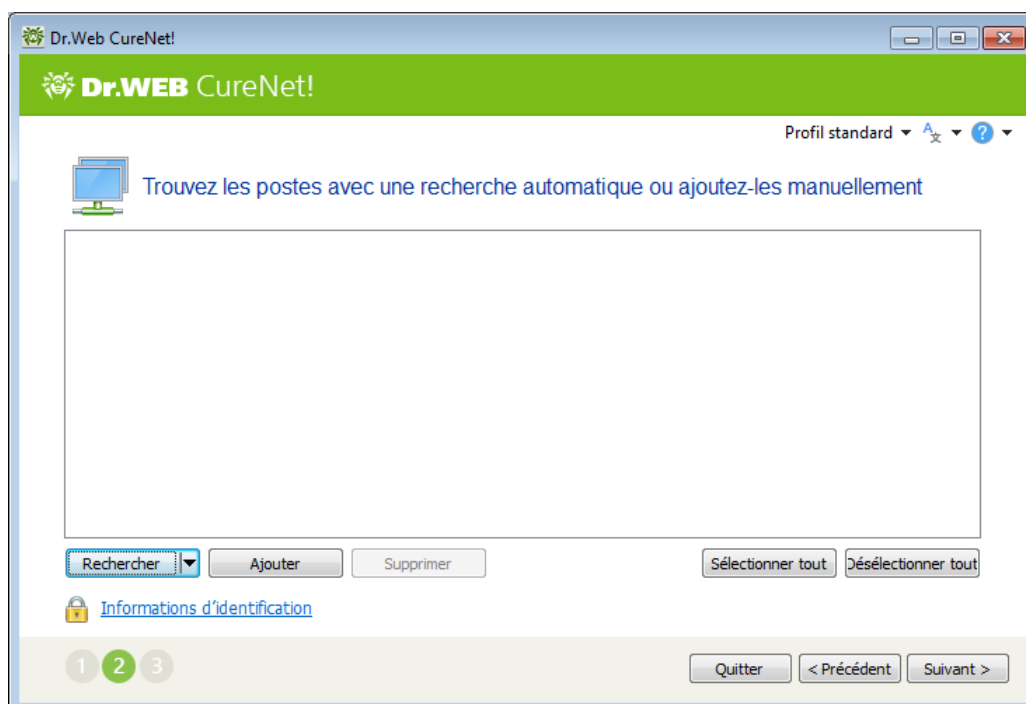


Figure 6. Sélection des postes.

Dr.Web permet d'ajouter les postes de manière manuelle ainsi que via la recherche automatique à travers tous les réseaux accessibles depuis l'ordinateur sur lequel tourne la Console d'administration.



Dr.Web détecte uniquement les réseaux et les ordinateurs visibles sous le compte sous lequel a été lancée la Console d'administration.

Recherche automatique des ordinateurs

1. Cliquez sur **Rechercher** et sélectionnez le mode de recherche nécessaire.

Si le contrôleur du domaine Active Directory est utilisé dans votre entreprise, il est recommandé de sélectionner l'option **Recherche dans Active Directory**. Dans ce cas la détection de tous les postes prend moins de temps, de plus, même les postes arrêtés seront affichés dans la liste.

Si vous sélectionnez l'option **Détection d'un réseau**, le processus de recherche de tous les ordinateurs peut prendre un certain temps. Pour arrêter la recherche, cliquez sur **Arrêter la recherche**. Tous les postes trouvés avant l'arrêt seront ajoutés dans la liste des ordinateurs. Si un ordinateur n'a pas été trouvé lors de la recherche, vous pouvez l'ajouter manuellement.

2. Sélectionnez les postes à scanner :
 - pour ajouter un poste particulier, cochez la case contre son nom ou son adresse IP dans la liste ;
 - pour scanner tous les postes listés, cliquez sur **Sélectionner tout** ;
 - pour désélectionner tous les postes et reprendre la sélection, cliquez sur **Désélectionner tout**.

Ajout manuel des ordinateurs

1. Pour ajouter un ou plusieurs postes de manière manuelle, cliquez sur le bouton **Ajouter**.
2. Dans la fenêtre **Ajout des postes**, saisissez l'une des valeurs suivantes :
 - l'adresse IP de l'ordinateur ou son nom réseau ;
 - la plage des adresses IP des ordinateurs séparées par un trait d'union («-») ou utilisez les masques (pour en savoir plus, consultez [Annexe C. Masques réseau](#)).



Lorsque vous ajoutez un poste, veuillez vous assurer que l'adresse IP spécifiée n'est pas utilisée pour les messages broadcast (n'est pas destinée à transmettre des paquets broadcast via le réseau).

3. Cliquez sur **OK**.
4. Les postes ajoutés dans la liste de manière manuelle seront sélectionnés automatiquement pour le travail postérieure. Pour exclure les postes de la liste, décochez les cases correspondantes.
5. Après la fin de sélection, rédigez une listes des comptes sous lesquels Dr.Web va se connecter aux postes spécifiés. Par défaut, la connexion s'établit sous le compte sous lequel tourne la Console d'administration. Si la connexion sous ce compte n'est pas possible, les comptes listés seront utilisés.

Suppression du poste depuis la liste

1. Sélectionnez les postes que vous voulez supprimer de la liste. Pour une sélection rapide de tous les postes, cliquez sur le nom du groupe correspondant.
2. Cliquez sur **Supprimer**.

Après la fin de sélection, rédigez une listes des comptes sous lesquels Dr.Web va se connecter aux postes spécifiés. Par défaut, la connexion s'établit sous le compte sous lequel tourne la Console d'administration. Si la connexion sous ce compte n'est pas possible, les comptes listés seront utilisés.

Configuration de la liste des comptes

1. Pour afficher la liste des comptes, lors de l'étape de création de la liste des postes, cliquez sur **Informations d'identification**La fenêtre **Comptes et mots de passe** apparaît.

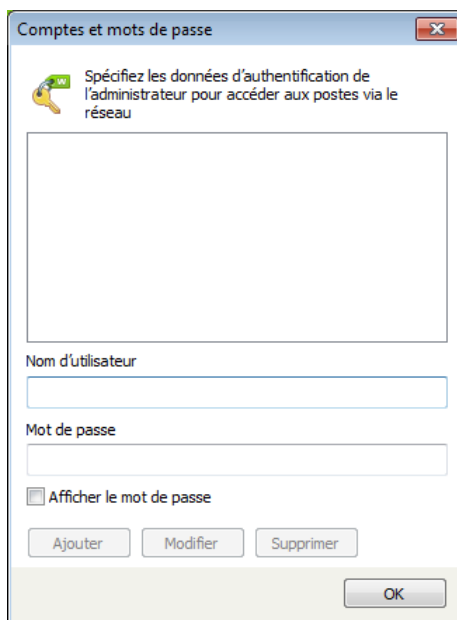


Figure 7. Gestion du compte.

2. Editez la liste. Faites attention aux particularités de l'ajout de comptes.
 - Le nom d'utilisateur doit avoir l'un des formats suivants :
 - <domaine>\<nom_d'utilisateur>, où <domaine> est le nom du domaine auquel appartient le compte spécifié ;
 - <poste>\<nom_utilisateur>, où <poste> est le nom réseau du poste ayant le compte en question.
 - Si tous les postes distants que vous souhaitez ajouter se trouvent hors des domaines ou possèdent le même compte administrateur, afin d'épargner du temps, il est recommandé de lister seulement ce compte commun et d'omettre le nom du poste. Dr.Web va essayer de se connecter automatiquement à tous les postes sous le compte en question.

Cette technique n'est applicable qu'aux réseaux correctement configurés.



3. Cliquez sur **OK**.

Ajout des postes lors du scan

1. Cliquez droit dans le tableau et, dans le menu qui s'affiche, sélectionnez **Ajouter un poste**.
2. Entrez l'adresse IP ou le nom réseau du poste.
3. Cliquez sur **OK**. Le poste correspondant aux données indiquées sera ajouté dans la liste des postes à scanner.

5.3. Sélection du mode de fonctionnement

Lors de cette étape, vous pouvez configurer le mode de fonctionnement du Scanner Dr.Web sur les postes distants ainsi que paramétrer la réaction en cas de détection des fichiers suspects ou infectés, des malwares ou des archives et des mails infectés.

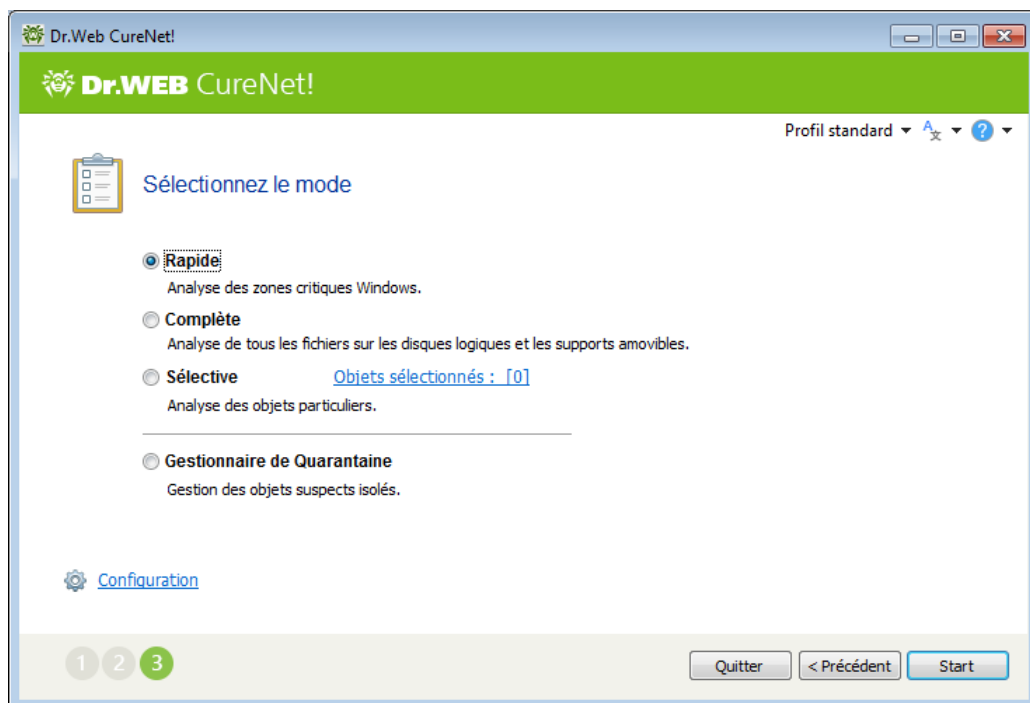


Figure 8. Sélection du mode de fonctionnement.

Modes d'analyse

Par défaut, après la copie des fichiers, Dr.Web lance sur le poste le Scanner Dr.Web qui réalise une analyse rapide (mode **Analyse rapide**).

Dans ce mode, les objets suivants sont scannés :

- mémoire vive ;
- secteurs boot de tous les disques ;
- répertoire racine du disque boot ;



- dossier système Windows ;
- dossier des Documents de l'utilisateur (« Mes documents ») ;
- répertoire système temporaire ;
- répertoire utilisateur temporaire.



Le dossier Mes Documents et le dossier avec les fichiers temporaires de l'utilisateur sont analysés pour tous les comptes sur le poste.

Dans ce mode, les fichiers archivés ne sont pas analysés.

Vous pouvez changer le mode d'analyse sélectionné par défaut pour l'un des modes suivants :

- **Analyse complète** durant laquelle seront analysés : la mémoire vive et tous les disques durs y compris les secteurs d'amorçage, la recherche des rootkits sera également effectuée.
- **Analyse sélective** durant laquelle seuls les objets sélectionnés sur les postes choisis seront analysés. Pour sélectionner des objets à scanner, cliquez sur le lien **Objets sélectionnés**. Dans la fenêtre qui s'affiche, indiquez les objets à scanner. Après être sélectionnés, ils seront ajoutés au profil lors de l'enregistrement.

Mode Gestionnaire de Quarantaine

Ce mode permet de consulter et de modifier le contenu de la Quarantaine, créée sur les postes, et de copier les fichiers isolés sur votre ordinateur pour le travail ultérieur. La Quarantaine sert à isoler les fichiers suspectés d'être malveillants. La Quarantaine stocke également des copies de sauvegarde des fichiers traités par Dr.Web.

5.4. Configuration supplémentaire

Les paramètres du programme définis par défaut sont optimaux dans la plupart des cas.

Si nécessaire, vous pouvez ajouter l'analyse des archives et des fichiers e-mail ainsi que modifier la réaction du Scanner Dr.Web en cas de détection des objets malveillants, en plus, vous pouvez configurer d'autres paramètres supplémentaires.

Paramètres avancés du scan

1. Cliquez sur **Configuration** pour accéder à la fenêtre de Configuration du Scanner Dr.Web.
2. Configurez les paramètres que vous voulez dans les onglets suivants :
 - [Général](#)
 - [Exclusions](#)
 - [Actions](#)
 - [Réseau](#)
 - [Mise à jour](#)



Cliquez sur le bouton **Appliquer** si nécessaire.

- Après la fin d'édition des paramètres, cliquez sur **OK** pour conserver les valeurs apportées ou sur **Annuler** pour les annuler.

La modification des paramètres n'est prise en compte que lors de la session courante de Dr.Web. Au redémarrage de l'utilitaire, tous les paramètres reprennent leurs valeurs initiales définies par défaut. Utilisez les [profils](#) pour conserver les paramètres.

5.4.1. Onglet Général

Cet onglet vous permet de spécifier les paramètres généraux relatifs au fonctionnement des postes distants lors de l'analyse avec Dr.Web.

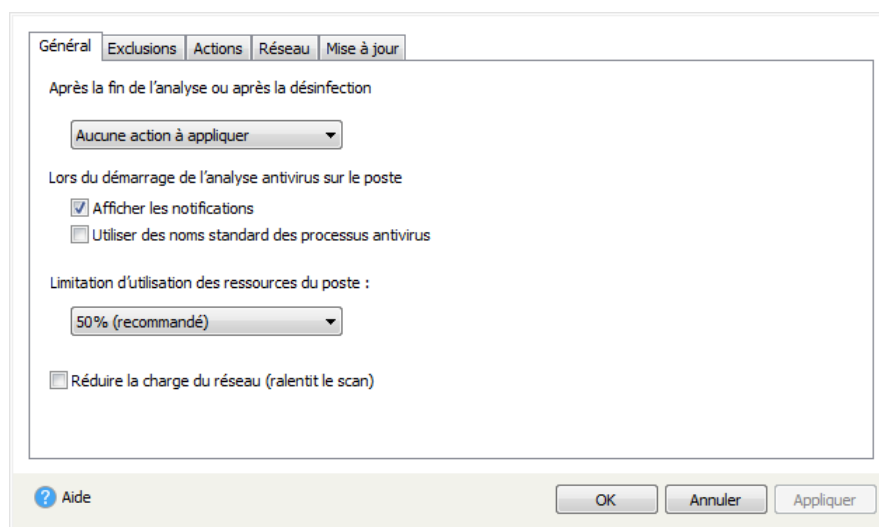


Figure 9. Configuration de Dr.Web. Onglet Général.

La désinfection de certains fichiers (par exemple, des fichiers utilisés par d'autres applications ou des paramètres de la base de registre) requiert un redémarrage de la machine. Cet onglet permet également de configurer les paramètres avancés relatifs à la désinfection de telles infections.

Les modes **Redémarrer le poste** ou **Arrêter le poste** commandent de réaliser l'action correspondante sur le poste distant de manière automatique, dans ce cas-là, l'utilisateur sera averti par une notification affichée de sorte qu'il a le temps de sauvegarder des informations nécessaires et d'achever les tâches importantes avant le redémarrage. La machine sera redémarrée une seule fois après la fin de l'analyse.

Le mode **Aucune action à appliquer** permet aux utilisateurs de continuer sans redémarrer la machine, mais dans ce cas, il peut s'avérer impossible de traiter certains fichiers infectés.



En cas de détection des virus dans le secteur boot (MBR), le Scanner Dr.Web redémarre le poste distant immédiatement après la détection du virus et dès que l'entrée correspondante est réparée (hard reset). Ce redémarrage s'effectue quel que soit le mode sélectionné.

Par défaut, Dr.Web avertit les utilisateurs du commencement de l'analyse avec les infobulles affichées dans la zone de notification Windows. Pour désactiver l'affichage des infobulles, décochez la case **Afficher les notifications**.

Par défaut lors de copie de fichiers Dr.Web vers le poste scanné, des noms sont appropriés par hasard. Si un antivirus avec un pare-feu est installé sur l'ordinateur, il se peut que l'administrateur soit obligé de spécifier les exceptions pour le pare-feu lors de chaque scan. Dans ce cas il est recommandé d'activer le mode **Utiliser des noms standard des processus antivirus** pour que les fichiers Dr.Web soient copiés vers le poste avec leurs propres noms. Dans ce cas l'administrateur sera invité à spécifier l'exception pour le pare-feu du poste scanné une seule fois.

Vous pouvez également limiter l'utilisation de ressources du poste scanné. La valeur 50% est utilisée par défaut. Pour modifier cette valeur ou supprimer la limitation, sélectionnez l'option correspondante dans la liste déroulante sous l'en-tête **Limitation d'utilisation des ressources du poste**.

En cas du réseau chargé, vous pouvez activer le paramètre **Réduire la charge du réseau (ralentit le scan)**. Dans ce mode, Dr.Web copie les fichiers de programme sur les postes à tour de rôle et augmente l'intervalle de temps à l'issue duquel le poste envoie les données à l'administrateur. Notez que ce paramètre ralentit le scan.

5.4.2. Onglet Exclusions

Dans cet onglet, vous pouvez spécifier la liste des fichiers et des dossiers à exclure de l'analyse du Scanner Dr.Web sur le poste. Vous pouvez exclure du scan les dossiers de quarantaine, les dossiers de certains programmes, les fichiers temporaires (fichiers swap), etc. Par défaut, la liste est vide.

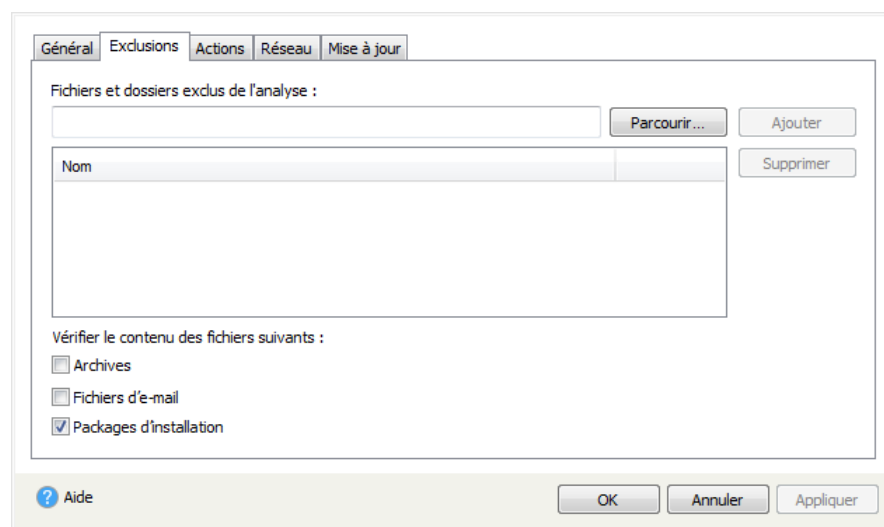


Figure 10. Configuration de Dr.Web. Onglet Exclusions.

Configuration de la liste des exclusions

1. Faites une des actions suivantes pour ajouter un dossier ou un fichier à la liste :



- pour ajouter un fichier ou un dossier existant, cliquez sur **Parcourir** et sélectionnez le fichier ou dossier dans la fenêtre standard d'ouverture de fichier. Vous pouvez entrer manuellement le chemin complet vers le fichier ou le dossier ou modifier le chemin dans le champ réservé à cet effet avant de l'ajouter à la liste ;
- pour exclure de l'analyse les fichiers et dossiers en fonction de leurs noms, entrez leur nom sans indiquer le chemin ;
- pour exclure du scan les fichiers ou les dossiers du type particulier, entrez le masque qui les détermine dans le champ d'entrée. Pour en savoir plus sur les masques

Un masque désigne la partie commune du nom de l'objet, ainsi :

- le symbole « * » remplace toute séquence (potentiellement vide) de caractères ;
- le symbole « ? » remplace n'importe quel caractère (un seul caractère) ;

Exemples :

- `rapport*.doc` : un masque qui désigne tous les documents Microsoft Word dont les noms commencent par le mot « rapport », par exemple, les fichiers `rapport-fevrier.doc`, `rapport121209.doc` etc. ;
- `*.exe` : un masque qui désigne tous les fichiers exécutable ayant l'extension EXE, par exemple, `setup.exe`, `iTunes.exe` etc. ;
- `photo????09.jpg` : un masque qui désigne tous les fichiers des images au format JPG dont le nom commence par « photo » et se termine par « 09 », dans ce cas entre ces deux fragments dans le nom de fichier, il y a quatre n'importe quels caractères, par exemple `photo121209.jpg`, `photopapa09.jpg` ou `photo----09.jpg`.

2. Cliquez sur **OK**. Le fichier ou dossier apparaît dans la liste.

Exemples de configuration des exclusions :

- `C:\folder` ou `C:\folder**` : exclut de l'analyse tous les fichiers se trouvant dans le dossier `C:\folder`. Cependant les fichiers dans les sous-dossiers seront scannés.
- `C:\folder*` : exclut de l'analyse tous les fichiers se trouvant dans le dossier `C:\folder` ainsi que dans tous les sous-dossiers à tout niveau.
- `C:\folder*.txt` : exclut de l'analyse les fichiers de type `*.txt` se trouvant dans le dossier `C:\folder`. Les fichiers `*.txt` se trouvant dans les sous-dossiers seront scannés.
- `C:\folder**.txt` : exclut de l'analyse les fichiers de type `*.txt` uniquement dans les sous-dossier de premier niveau dans le dossier `C:\folder`.
- `C:\folder***.txt` : exclut de l'analyse les fichiers de type `*.txt` dans les sous-dossiers de tout niveau dans le dossier `C:\folder`. Les fichiers `*.txt` se trouvant dans le dossier `C:\folder` seront scannés.

Si nécessaire, vous pouvez sélectionner les objets à analyser suivants :

- **Archives** : cochez cette case pour analyser les fichiers dans les archives ;
- **Fichiers d'e-mail** : cochez cette case pour analyser les fichiers dans les clients de messagerie ;



- **Packages d'installation** : cochez cette case pour analyser les fichiers de packages d'installation.

En cas de détection d'un objet infecté dans l'archive, l'action préconfigurée sera appliquée à l'archive entière et non seulement à l'objet malicieux.

L'activation de l'analyse des archives et des fichiers d'e-mail peut ralentir considérablement le processus de scan.

5.4.3. Onglet Actions



Les actions appliquées aux objets suspects ou infectés ne peuvent être réalisées que dans le mode standard (à condition que le fichier clé valide soit présent sur la machine). Dans le mode de démonstration, l'utilisateur sera seulement informé sur les menaces détectées.

Cet onglet vous permet de modifier la réaction du Scanner Dr.Web en fonction de la menace détectée ou du type de l'objet infecté.

| Catégorie | Action |
|---------------------|--|
| Infectés : | Désinfecter, déplacer en quarantaine les incurables (recommandé) |
| Suspects : | Déplacer en quarantaine (recommandé) |
| Adwares : | Déplacer en quarantaine (recommandé) |
| Dialers : | Déplacer en quarantaine (recommandé) |
| Canulars : | Déplacer en quarantaine (recommandé) |
| Riskwares : | Déplacer en quarantaine (recommandé) |
| Hacktools : | Déplacer en quarantaine (recommandé) |
| Containers : | Déplacer en quarantaine (recommandé) |
| Archives : | Déplacer en quarantaine (recommandé) |
| Fichiers d'e-mail : | Déplacer en quarantaine (recommandé) |

Figure 11. Configuration de Dr.Web. Onglet Actions.

Par défaut, en cas de détection d'un virus connu ou d'un objet suspect d'être infecté, le Scanner Dr.Web lancé par Dr.Web sur le poste réalise des actions automatiques afin de neutraliser la menace.

La réaction est spécifiée séparément pour chaque catégorie d'objets :

- **Infectés** : infectés par des virus connus et (supposés) désinfectables ;
- **Suspects** : potentiellement dangereux pour la sécurité informatique.

Vous pouvez également configurer une réaction sur les types particuliers de programmes malveillants ou sur les types particuliers de packages (archives, fichiers emails ou conteneurs de fichiers).



En cas de détection d'un objet infecté dans l'archive, une réaction spécifiée pour les archives sera appliquée. Elle sera appliquée à l'archive entière et non seulement à l'objet malicieux.

Si cela est nécessaire, vous pouvez remplacer l'action par défaut par une des réactions suivantes :

- **Désinfecter, déplacer en quarantaine les incurables (recommandé)** (applicable uniquement aux objets infectés) : commande au Scanner Dr.Web d'essayer de désinfecter l'objet infecté par un virus connu. Si le virus est incurable ou que la tentative de désinfection a échoué, le fichier sera placé en quarantaine ;
- **Déplacer en quarantaine (recommandé)** (n'est pas applicable aux secteurs boot) : commande au Scanner Dr.Web de déplacer l'objet malveillant ou suspect vers la quarantaine ;
- **Ignorer** (applicable uniquement aux programmes malveillants) : ne pas afficher les informations sur la détection du programme malveillant dans le [rapport](#) de Dr.Web ;
- **Notifier** : afficher les informations sur l'objet malveillant ou suspect dans le [rapport](#) de Dr.Web.

5.4.4. Onglet Réseau

Cet onglet vous permet de configurer les paramètres supplémentaires relatifs à l'interaction via le réseau depuis le poste distant lors de l'analyse avec le Scanner Dr.Web.

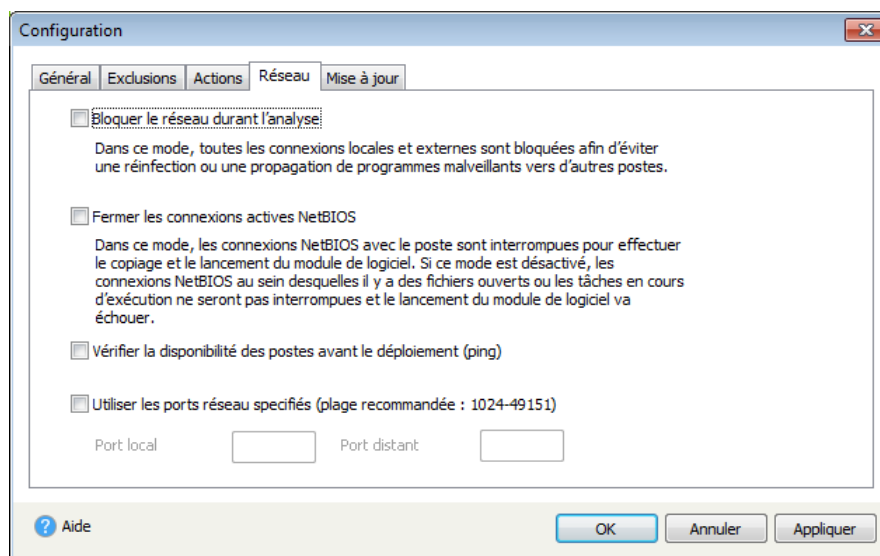


Figure 12. Configuration de Dr.Web. Onglet Réseau.

Si nécessaire, vous pouvez sélectionner les modes suivants :

- **Bloquer le réseau durant l'analyse** : sélectionnez ce mode pour bloquer l'interaction via le réseau depuis le poste distant pendant le scan afin d'éviter la diffusion de l'épidémie et la recontamination de ce poste ;
- **Fermer les connexions actives NetBIOS** : sélectionnez ce mode pour fermer avant l'analyse toutes les connexions NetBIOS y compris les connexions contenant des fichiers ouverts et des



tâches en train d'exécution (ceci est nécessaire pour copier les fichiers et lancer le Scanner Dr.Web) ;

- **Vérifier la disponibilité des postes avant le déploiement (ping)** : sélectionnez ce mode pour vérifier la disponibilité du poste via le réseau avec l'utilitaire de ping avant de procéder à la copie des fichiers ;
- **Utiliser les ports réseau spécifiés (plage recommandée : 1024-49151)** : sélectionnez ce mode pour que le Scanner Dr.Web se connecte au poste lors du scan par les ports spécifiés.

5.4.5. Onglet Mise à jour

Cet onglet vous permet de configurer les paramètres de la connexion réseau utilisée pour la mise à jour du dépôt de Dr.Web.

Si nécessaire, vous pouvez sélectionner les modes suivants :

- **Utiliser la connexion HTTPS** : cochez cette case si vous voulez télécharger les mises à jour via le protocole sécurisé ;
- **Utiliser un serveur proxy** : cochez cette case si vous voulez utiliser le serveur proxy. Spécifiez l'**Adresse** et le **Port** du serveur proxy. Si le serveur proxy spécifié requiert une authentification, saisissez les informations nécessaires dans les champs **Nom d'utilisateur** du serveur proxy et **Mot de passe**.

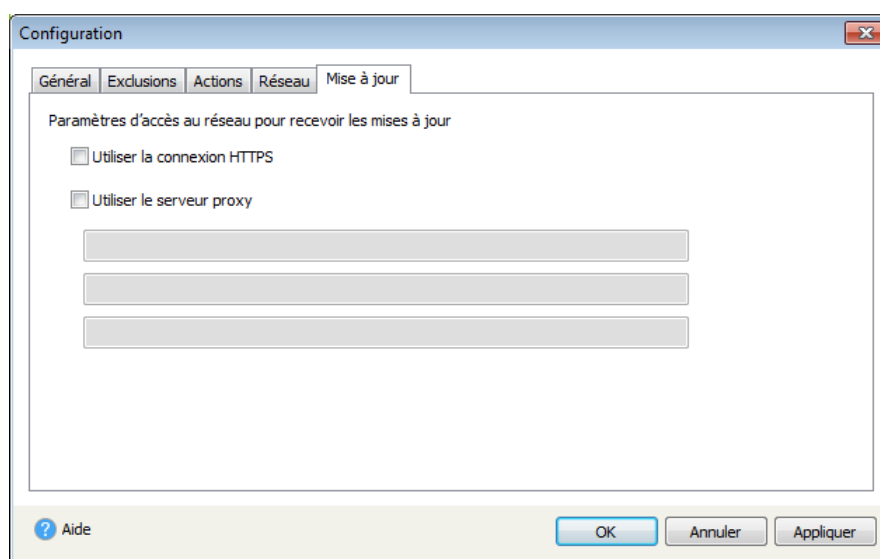


Figure 13. Configuration de Dr.Web. Onglet Mise à jour.

5.5. Rapport sur le fonctionnement de Dr.Web

La rubrique **Statistiques** affiche des informations relatives au fonctionnement du Scanner Dr.Web sur tous les postes distants. La récolte des statistiques ne dépend pas de la qualité de la connexion entre l'ordinateur sur lequel tourne la Console d'administration et les ordinateurs scannés. En cas de perte de connexion de courte durée avec le poste distant, après le début du



processus de scan, Dr.Web tente de rétablir la connexion et met à jour les statistiques de l'analyse dès que la connexion est rétablie.

La partie haute de la fenêtre affiche des informations sur le statut de l'analyse ainsi que des statistiques sommaires relatives à l'analyse sur tous les postes distants.

La sections **Postes** inclut les informations suivantes :

| Champ | Description |
|--------------------|---|
| Spécifiés | Nombre total de postes à scanner. |
| Trouvés | Nombre total de postes accessibles via le réseau. |
| Non trouvés | Nombre total de postes inaccessibles via le réseau. |
| Installés | Nombre total de postes distants auxquels la connexion a été établie et vers lesquels la copie de fichiers de Dr.Web a réussi. |
| Erreurs | Nombre de postes avec lesquels la connexion à échoué et/ou la copie de fichiers de Dr.Web n'a pas réussi non plus. |
| En cours d'analyse | Nombre total de postes en cours d'analyse. |
| Terminés | Nombre total de postes distants déjà scannés. |
| Désinfectés | Nombre total de postes complètement désinfectés sur lesquels tous les objets malicieux ont été neutralisés. |
| Redémarrés | Nombre total de postes redémarrés afin d'achever la désinfection. |

La sections **Événements** inclut les informations suivantes :

| Champ | Description |
|-------------------|---|
| Scannés | Nombre total d'objets scannés sur tous les postes distants. |
| Menaces | Nombre total de menaces virales détectées sur tous les postes distants. |
| Désinfectés | Nombre total d'objets désinfectés sur tous les postes distants. |
| Erreurs d'analyse | Nombre total d'erreurs d'analyse. |

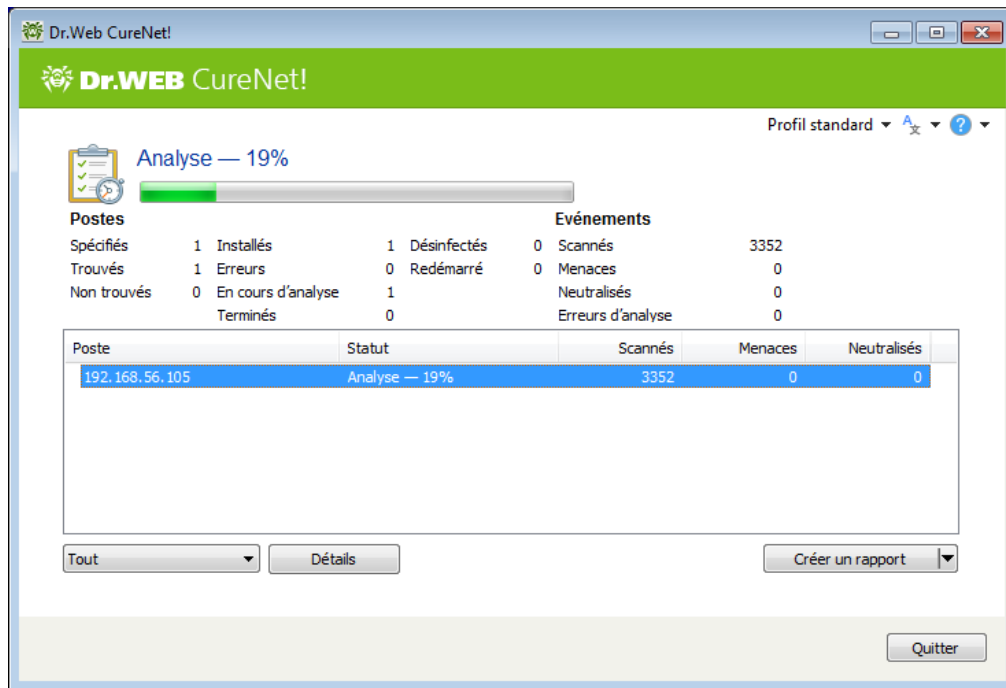


Figure 14. Rapport de Dr.Web.

La section de rapport affiche les résultats de l'analyse sur les postes distants :

| Champ | Description |
|-------------|--|
| Poste | Nom ou adresse du poste. |
| Statut | Statut de l'analyse du poste distant (installation, progression en pourcentage, message sur une erreur de scan ou sur l'inaccessibilité du poste, etc.). |
| Scannés | Nombre total d'objets scannés sur le poste distant. |
| Menaces | Nombre total de menaces détectées. |
| Désinfectés | Nombre total d'objets malveillants désinfectés (seuls les objets infectés par des virus connus et potentiellement curables peuvent être désinfectés). |

Si cela est nécessaire, utilisez un filtre pour afficher des informations spécifiques selon le statut de scan et le statut du poste distant. Vous pouvez également trier la liste en cliquant sur l'en-tête de la colonne selon laquelle vous voulez ranger les postes.



La validité du MBR (master boot record) est un critère critique de l'OS, c'est pourquoi pour supprimer les virus MBR et réparer le secteur, le Scanner Dr.Web réalise un redémarrage du système immédiatement après la détection des virus MBR et dès que les entrées du secteur MBR sont restaurées (hard reset). Dans ce cas-là, l'analyse du poste distant sera interrompue.



Le rapport de Dr.Web contient des informations sur la fin anticipée du processus de scan sur le poste infecté par rapport à la durée de l'analyse sur les autres postes ainsi que des informations sur le virus détecté dans le secteur MBR du système d'exploitation. Ces informations sont disponibles dans la fenêtre de statistiques du poste.

Pour achever l'analyse des postes infectés par des virus MBR, il faut redémarrer le scan.

Ajouter un nouveau poste à scanner

Pour ajouter un nouveau poste à scanner lors du scan déjà lancé, cliquez droit sur le champ de rapport, cliquez sur **Ajouter un poste** et entrez l'adresse IP ou le nom réseau du poste en question.

Consultation des statistiques du poste

Pour plus d'information sur les résultats de l'analyse du poste distant, effectuez l'une des actions suivantes :

- double-cliquez sur le nom ou sur l'adresse du poste dans la liste ;
- sélectionnez le poste dans la liste et cliquez sur le bouton **Détails**.

Une fenêtre affichant les statistiques du poste sera ouverte. En cas d'erreurs durant le processus de copie des fichiers de Dr.Web vers le poste ou en cas de perte de connexion lors de l'analyse, cette fenêtre affiche les notifications correspondantes.

Si des menaces ont détectées dans les archives, les fichiers email ou dans les conteneurs de fichiers, le rapport affiche les fichiers contenant les menaces détectées ainsi que les archives, les fichiers email ou les conteneurs de fichiers contenant les fichiers concernés.



Pour en savoir plus sur la configuration des actions sur les objets malveillants, consultez la rubrique [Paramètres avancés](#).

Enregistrement du rapport

Pour enregistrer le rapport, cliquez sur **Créer un rapport**, sélectionnez le format de rapport et les postes à inclure dans le rapport. Le rapport sera enregistré automatiquement dans le dossier du produit.

5.6. Gestionnaire de Quarantaine

Dr.Web permet de consulter et de modifier le contenu de la Quarantaine, créée sur les postes, et de copier les fichiers isolés sur votre ordinateur pour le travail ultérieur. La Quarantaine sert à



isoler les fichiers suspectés d'être malveillants. La Quarantaine stocke également des copies de sauvegarde des fichiers traités par Dr.Web.

Passage en mode de la quarantaine

1. [Indiquez](#) les postes sur lesquels vous voulez ouvrir le contenu de la quarantaine.
2. Dans la fenêtre de sélection de [modes de fonctionnement](#), indiquez le mode **Gestionnaire de Quarantaine**.
3. Appuyez sur **Start**.

En haut de la fenêtre, vous allez voir l'information sur le fonctionnement du Gestionnaire de quarantaine sur les postes indiqués :

| Champ | Description |
|-------------|---|
| Spécifiés | Nombre total de postes. |
| Trouvés | Nombre total de postes accessibles via le réseau. |
| Non trouvés | Nombre total de postes inaccessibles via le réseau. |
| Installés | Nombre total de postes distants auxquels la connexion a été établie et vers lesquels la copie de fichiers de Dr.Web a réussi. |
| Erreurs | Nombre de postes avec lesquels la connexion a échoué et/ou la copie de fichiers de Dr.Web n'a pas réussi non plus. |
| Lancés | Nombre total de postes sur lesquels le Gestionnaire de Quarantaine est lancé à ce moment. |
| Terminés | Nombre total de postes sur lesquels le Gestionnaire de Quarantaine a achevé son fonctionnement (par exemple, à cause de l'arrêt du poste par l'utilisateur). |

Dans cette fenêtre vous pouvez :

- modifier les informations d'identification pour la connexion au poste. Pour ce faire, sélectionnez un poste dans la liste, cliquez droit sur ce poste et sélectionnez **Modifier les informations d'identification**.
- ajouter de nouveaux postes. Pour ce faire, cliquez droit dans le tableau et sélectionnez **Ajouter un poste**. Une fenêtre va s'afficher dans laquelle il est nécessaire d'entrer l'adresse IP et le nom réseau du poste.
- filtrer les postes selon un des paramètres : avec erreurs, trouvés, non trouvés, avec la quarantaine pas vide. Pour ce faire, cliquez sur la liste déroulante sous le tableau et sélectionnez un filtre nécessaire.

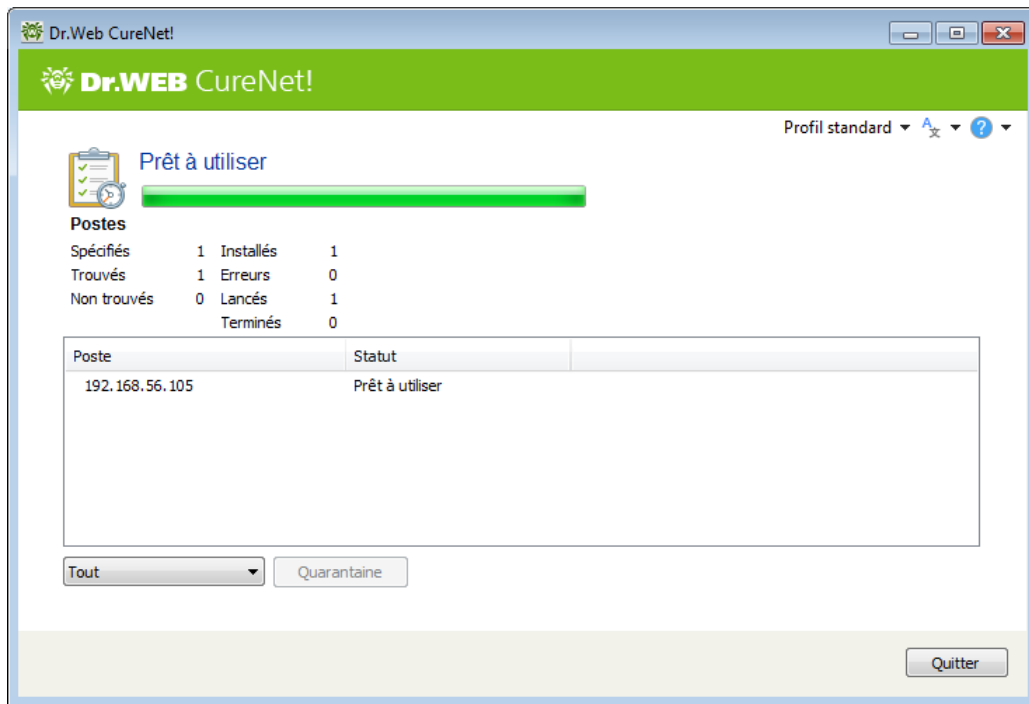


Figure 15. Gestionnaire de Quarantaine Dr.Web.

Pour consulter et modifier le contenu de la quarantaine sur un poste particulier, sélectionnez ce poste dans la liste ou dans le menu contextuel du poste et cliquez sur **Quarantaine**, ou bien cliquez sur **Quarantaine** en bas de la fenêtre.

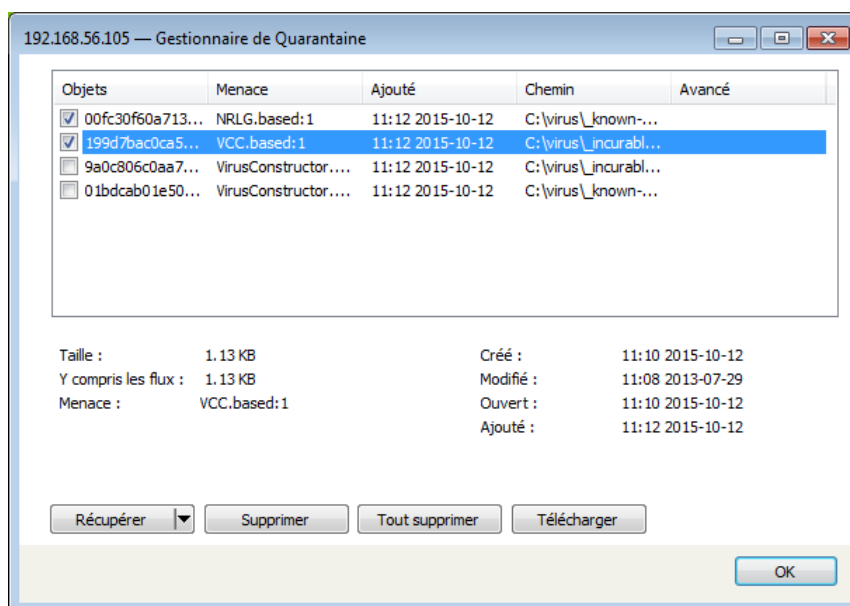


Figure 16. Consulter le contenu de la quarantaine.

Dans la fenêtre qui s'affiche, vous voyez la liste des noms des objets isolés dans la quarantaine sur ce poste ainsi qu'une brève information sur chaque objet : classification du programme malveillant déterminée par Dr.Web, date de placement de l'objet en quarantaine, chemin de l'objet avant son placement en quarantaine, etc.



Dans cette fenêtre vous pouvez :

- récupérer les objets dans leur dossier d'origine. Pour ce faire, sélectionnez les objets dans la liste et cliquez sur **Récupérer** en bas de la fenêtre.
- récupérer les objets dans le dossier spécifié. Pour ce faire, cliquez sur **Récupérer** en bas de la fenêtre et sélectionnez **Récupérer comme**.
- supprimer les objets particuliers. Pour ce faire, sélectionnez les objets dans la liste et cliquez sur **Supprimer** en bas de la fenêtre.
- supprimer tous les objets en même temps. Pour ce faire, cliquez sur **Tout supprimer** en bas de la fenêtre.
- télécharger les objets de la quarantaine sur votre ordinateur. Pour ce faire, sélectionnez dans la liste les objets nécessaires et cliquez sur **Télécharger** en bas de la fenêtre. Dans la fenêtre qui s'affiche, indiquez le dossier dans lequel les objets seront sauvegardés.



6. Annexe A. Support technique

En cas de problèmes liés à l'installation ou au fonctionnement des produits Dr.Web, avant de contacter le service de support technique, essayez de trouver une solution par les moyens suivants :

- consultez les dernières versions de descriptions et de manuels à l'adresse <https://download.drweb.com/doc/> ;
- consultez la rubrique des questions les plus fréquemment posées sur la page https://support.drweb.com/show_faq/ ;
- visiter les forums de Doctor Web à l'adresse <https://forum.drweb.com/>.

Si le problème persiste, vous pouvez utiliser l'un des moyens suivants pour contacter le support technique de Doctor Web :

- remplissez le formulaire dans la rubrique correspondante de la section <https://support.drweb.com/> ;
- appelez au numéro : 0 825 300 230.

Vous pouvez trouver les informations sur les bureaux régionaux de la société Doctor Web sur le site officiel à l'adresse <https://company.drweb.com/contacts/offices/>.



7. Annexe B. Méthodes de Détection

Toutes les solutions antivirus créées par Doctor Web utilisent un ensemble de méthodes de détection, ce qui leur permet d'effectuer des analyses en profondeur des fichiers suspects.

Méthode de détection des menaces

Analyse de signature

Cette méthode de détection est appliquée en premier. Elle est mise en oeuvre en examinant le contenu de l'objet à la recherche des signatures de menaces connues. Une *Signature* est une séquence continue et finie d'octets qui est nécessaire et suffisante pour identifier une menace. La comparaison du contenu de l'objet avec les signatures n'est pas effectuée directement, mais par leur somme de contrôle ce qui permet de réduire considérablement la taille des entrées dans les bases de données virales tout en préservant le caractère unique de la conformité et par conséquent, l'exactitude de la détection des menaces et du traitement des objets contaminés. Les entrées dans les bases de données virales Dr.Web sont rédigées de sorte que la même entrée peut détecter des classes entières ou des familles de menaces.

Origins Tracing™

Cette est une technologie unique Dr.Web permettant de détecter les nouvelles menaces ou celles modifiées et utilisant des mécanismes de contamination ou un comportement malveillant qui sont déjà connus de la base de données virale. Cette technologie intervient à la fin de l'analyse par signature et assure une protection des utilisateurs utilisant des solutions antivirus Dr.Web contre des menaces telles que Trojan.Encoder.18 (également connu sous le nom «gpcod»). En outre, l'utilisation de la technologie Origins Tracing peut réduire considérablement le nombre de faux positifs de l'analyseur heuristique. Les noms des menaces détectées à l'aide d'Origins Tracing sont complétés par `.Origin`.

Emulation de l'exécution

La méthode d'émulation d'exécution de code est utilisée pour détecter les virus polymorphes et cryptés si la recherche à l'aide des sommes de contrôle des signatures est inapplicable ou considérablement compliquée en raison de l'impossibilité de construire des signatures fiables. La méthode consiste à simuler l'exécution du code en utilisant l'*Émulateur* – un modèle du processeur et de l'environnement du programme. L'Émulateur fonctionne avec un espace mémoire protégé (*tampon d'émulation*). Dans ce cas, les instructions ne sont pas transmises à un processeur central pour exécution réelle. Si le code traité par l'émulateur est infecté, alors le résultat de son émulation est un rétablissement du code malveillant d'origine disponible pour une analyse de signature.



Analyse heuristique

Le fonctionnement de l'analyseur heuristique est fondé sur un ensemble d'*heuristiques* (hypothèses, dont la signification statistique est confirmée par l'expérience) des signes caractéristiques de logiciels malveillants et, inversement, le code exécutable sécurisé. Chaque attribut ou caractéristique du code possède un score (le nombre indiquant l'importance et la validité de cette caractéristique). Le score peut être positif si le signe indique la présence d'un comportement de code malveillant, et négatif si le signe ne correspond pas à une menace informatique. En fonction du score total du contenu du fichier, l'analyseur heuristique calcule la probabilité de la présence d'un objet malveillant inconnu. Si cette probabilité dépasse une certaine valeur de seuil, l'objet analysé est considéré comme malveillant.

L'analyseur heuristique utilise également la technologie FLY-CODE™ – un algorithme universel pour l'extraction des fichiers. Ce mécanisme permet de construire des hypothèses heuristiques sur la présence d'objets malveillants dans les objets, de logiciels compressés par des outils de compression (emballeurs), non seulement par des outils connus des développeurs des produits Dr.Web, mais également par des outils de compression nouveaux et inexplorés. Lors de la vérification des objets emballés, une technologie d'analyse de leur entropie structurelle est également utilisée, cette technologie peut détecter les menaces sur les spécificités de la localisation des fragments de leur code. Cette technologie permet avec une seule entrée de la base de données de détecter un ensemble de différents types de menaces qui sont emballées du même packer polymorphe.

Comme tout système basé sur des hypothèses, l'analyseur heuristique peut commettre des erreurs de type I ou II (omettre une menace inconnue ou faire un faux positif). Par conséquent, les objets marqués par l'analyseur heuristique comme "malveillants" reçoivent le statut «suspects».

Au cours de toute analyse, tous les composants des produits antivirus Dr.Web utilisent l'information la plus récente sur tous les programmes malveillants connus. Les signatures des menaces et les informations sur leurs caractéristiques et les comportements sont mises à jour et ajoutées à la base de données de virus immédiatement, dès que les spécialistes du laboratoire antivirus Doctor Web découvrent de nouvelles menaces, parfois jusqu'à plusieurs fois par heure. Même si un nouveau malware infiltre l'ordinateur, en évitant la protection Dr.Web, il sera détectée dans la liste des processus et neutralisée après l'obtention de nouvelles bases virales.



8. Annexe C. Masques réseau

Un masque désigne une partie commune de l'entrée binaire des adresses IP ajoutées au scan. Pour spécifier un groupe d'adresses IP avec un masque, il est nécessaire de spécifier l'adresse IP d'un des ordinateurs de groupe et le masque qui détermine les autres ordinateurs à l'aide de l'opération ET bit à bit (la conjonction bit à bit).

Par exemple, pour ajouter au scan 254 ordinateurs distants ayant les adresses de 10.30.0.1 à 10.30.0.254, vous pouvez spécifier le masque 10.30.0.0/24 :

| | |
|-------------------------------------|-------------------------------------|
| Adresse 10.30.0.1 | 00001010.00011110.00000000.00000001 |
| Masque 255.255.255.0 (24) | 11111111.11111111.11111111.00000000 |
| Hôte (minimum) 10.30.0.1 | 00001010.00011110.00000000.00000001 |
| Hôte (maximum) 10.30.0.254 | 00001010.00011110.00000000.11111110 |
| Adresse de diffusion 10.30.0.255 | 00001010.00011110.00000000.11111111 |

Hôtes dans le réseau : 254

En indiquant les ordinateurs à scanner, vous pouvez utiliser les façons suivantes de spécifier un masque :

- sous la forme décimale (système à quatre composants avec des points). Par exemple, 192.168.0.1/255.255.255.0, où 192.168.0.1 est l'adresse IP d'un des ordinateurs spécifiés, 255.255.255.0 est le masque ;
- sous la forme binaire (la soi-disant notation slash ou la notation CIDR quand le nombre de bits 1 est indiqué dans l'entrée binaire du masque). Par exemple, 192.168.0.1/24 où 192.168.0.1 est l'adresse IP d'un des ordinateurs spécifiés, 24 est l'entrée décimale du masque binaire où les premiers 24 bits ont la valeur 1, les autres – 0.

Dans les réseaux IPv4, vous pouvez utiliser les deux formes d'entrées. Dans les réseaux IPv6, on n'utilise que la notation CIDR.

