SOPHOS

Security made simple.

Sophos Anti-Virus pour Linux

Guide de configuration

Version du produit : 9

Table des matières

1 À propos de ce guide....5
2 À propos de Sophos Anti-Virus pour Linux....6
2.1 Que fait Sophos Anti-Virus ?....6
2.2 Comment Sophos Anti-Virus protège votre ordinateur ?....6
2.3 Comment utiliser Sophos Anti-Virus ?....6
2.4 Comment configurer Sophos Anti-Virus ?....6
3 Contrôle sur accès....8
3.1 Vérification de l'activité du contrôle sur accès....8
3.2 Vérification du lancement automatique du contrôle sur accès au démarrage....8
3.3 Démarrage du contrôle sur accès....8
3.4 Arrêt du contrôle sur accès....9
4 Contrôle à la demande....10
4.1 Exécution des contrôles à la demande....10
4.2 Configuration de contrôles à la demande....11
5 Que se passe-t-il en cas de détection de virus ?....14
6 Nettoyage de virus....16
6.1 Informations sur le nettoyage....16
6.2 Mise en quarantaine des fichiers infectés....16
6.3 Nettoyage des fichiers infectés....17
6.4 Récupération suite aux effets secondaires des virus....18
7 Affichage du journal Sophos Anti-Virus....19
8 Mise à jour immédiate de Sophos Anti-Virus....20
9 À propos de la prise en charge des noyaux....21
9.1 À propos de la prise en charge des nouvelles versions du noyau....21
9.2 À propos de la prise en charge des noyaux personnalisés....21
10 configuration des contrôles planifiés....22
10.1 Ajout d'un contrôle planifié depuis un fichier....22
10.2 Ajout d'un contrôle planifié depuis une entrée standard....22
10.3 Exportation d'un contrôle planifié dans un fichier....23
10.4 Exportation des noms de tous les contrôles planifiés dans un fichier....23
10.5 Exportation d'un contrôle planifié dans une sortie standard....23
10.6 Exportation des noms de tous les contrôles planifiés dans une sortie standard....23
10.7 Mise à jour d'un contrôle planifié à partir d'un fichier....24
10.8 Mise à jour d'un contrôle planifié depuis une entrée standard....24

10.9 Affichage du journal d'un contrôle planifié....25
10.10 Suppression d'un contrôle planifié....25
10.11 Suppression de tous les contrôles planifiés....25
11 configuration des alertes....26
11.1 Configuration des alertes de fenêtre instantanée de bureau....26
11.2 Configuration des alertes par ligne de commande....27
11.3 Configuration des alertes par email....27
12 configuration de la journalisation....30
13 configuration de la mise à jour....31
13.1 Concepts de base....31
13.2 Commande de configuration savsetup....31
13.3 Vérification de la configuration de la mise à jour automatique d'un ordinateur....32
13.4 Configuration d'un serveur de mise à jour....32
13.5 Configuration de plusieurs clients de mise à jour pour la mise à jour 33
13.6 Configuration d'un client de mise à jour autonome pour la mise à jour....34
14 configuration de Sophos Live Protection....35
14.1 Vérification du paramètre Sophos Live Protection....35
14.2 Activation ou désactivation de Sophos Live Protection....35
15 configuration du contrôle sur accès....36
15.1 Modification de la méthode d'interception de fichiers par contrôle sur accès....36
15.2 Exclusion des fichiers et de répertoires du contrôle....36
15.3 Exclusion d'un type de système de fichiers du contrôle....38
15.4 Contrôle dans les fichiers archive....38
15.5 Nettoyage des fichiers infectés....38
16 configuration des Fichiers supplémentaires....40
16.1 À propos de la configuration des Fichiers supplémentaires....40
16.2 Utilisation de la configuration des Fichiers supplémentaires....41
16.3 Mise à jour de la configuration des Fichiers supplémentaires....44
16.4 À propos des niveaux de configuration....44
16.5 Commande de configuration savconfig....45
17 Résolution des problèmes....47
17.1 Impossible d'exécuter une commande....47
17.2 La configuration des exclusions n'a pas été appliquée....47
17.3 L'ordinateur signale « Aucune entrée de manuel pour … »....48
17.4 Espace disque insuffisant....49
17.5 Le contrôle à la demande s'exécute au ralenti....49
17.6 Le programme d'archivage sauvegarde tous les fichiers qui ont été contrôlés à la demande....50

17.7 Virus non nettoyé....50
17.8 Fragment de virus signalé....51
17.9 Accès au disque impossible....52
18 Annexe : codes de retour du contrôle à la demande....53
18.1 Codes de retour étendus....53
19 Annexe : configuration de la fonction « phone-home »....55
20 Annexe : configuration du redémarrage pour RMS....56
21 Glossaire....57
22 Support technique....59
23 Mentions légales....60

1 À propos de ce guide

Ce guide vous indique comment utiliser et configurer Sophos Anti-Virus pour Linux.

Retrouvez plus de renseignements sur l'installation ci-dessous :

Pour installer Sophos Anti-Virus et l'administrer avec Sophos Central, connectez-vous à Sophos Central, allez sur la page Téléchargements et suivez les instructions qui s'y trouvent.

Pour installer Sophos Anti-Virus et l'administrer avec Sophos Enterprise Console, reportez-vous au *Guide de démarrage deSophos Enterprise Console pour Linux et UNIX*.

Pour installer ou désinstaller la version non administrée de Sophos Anti-Virus sur les ordinateurs Linux en réseau et autonomes, reportez-vous au *Guide de démarrage de Sophos Anti-Virus pour Linux*.

Retrouvez toute la documentation Sophos sur http://www.sophos.com/fr-fr/support/documentation.aspx.

Important : les informations sur la configuration mentionnées dans ce guide s'applique également à Sophos Linux Security.

2 À propos de Sophos Anti-Virus pour Linux

2.1 Que fait Sophos Anti-Virus ?

Sophos Anti-Virus détecte et traite les virus (y compris les vers et les chevaux de Troie) sur votre ordinateur Linux. En plus de détecter tous les virus Linux, il détecte également tous les virus non Linux qui peuvent être stockés sur votre ordinateur Linux et transférés sur les ordinateurs non Linux. Il effectue cette opération en contrôlant votre ordinateur.

2.2 Comment Sophos Anti-Virus protège votre ordinateur ?

Le contrôle sur accès est la méthode principale de protection antivirus. À chaque fois que vous ouvrez, enregistrez ou copiez un fichier, Sophos Anti-Virus le contrôle et vous autorise à y accéder s'il est sain.

Sophos Anti-Virus vous permet également d'exécuter un contrôle à la demande pour bénéficier d'un niveau de protection supplémentaire. Un contrôle à la demande est un contrôle que vous lancez. Vous pouvez tout contrôler, que ce soit un fichier unique ou tout fichier de votre ordinateur sur lesquels vous avez les droits en lecture. Vous pouvez soit exécuter un contrôle manuel à la demande, soit le planifier pour qu'il s'exécute tout seul.

2.3 Comment utiliser Sophos Anti-Virus ?

Effectuez toutes les tâches avec l'interface de ligne de commande.

Veuillez ouvrir une session administrateur (root) sur l'ordinateur pour pouvoir utiliser toutes les commandes sauf **savscan**, qui est utilisée pour exécuter des contrôles à la demande.

Le présent document suppose que vous avez installé Sophos Anti-Virus dans l'emplacement par défaut : `/opt/sophos-av`. Les chemins des commandes décrites sont basés sur cet emplacement.

2.4 Comment configurer Sophos Anti-Virus ?

Les méthodes que vous utilisez pour configurer Sophos Anti-Virus dépendent de votre utilisation ou pas d'un logiciel d'administration Sophos (Sophos Enterprise Console ou Sophos Central).

Ordinateurs administrés par l'Enterprise Console ou Sophos Central

Si vos ordinateurs Linux sont administrés par Sophos Enterprise Console ou Sophos Central, configurez Sophos Anti-Virus comme suit :

- Configurez les **contrôles sur accès, les contrôles planifiés, les alertes, la journalisation et la mise à jour** de manière centralisée depuis votre console d'administration. Retrouvez plus d'informations dans l'Aide de votre console d'administration.

  Remarque : ces fonctions incluent également certains paramètres qui ne peuvent pas être définis de manière centralisée à partir de la console d'administration. Vous pouvez définir ces paramètres localement sur chaque ordinateur Linux à partir de l'interface de ligne de commande de Sophos Anti-Virus. La console d'administration les ignore.

  Remarque : si vous utilisez des serveurs Linux 64 bits administrés avec Sophos Central, reportez-vous au Guide de démarrage de Sophos Linux Security

- Configurez localement sur chaque ordinateur Linux les **contrôles à la demande** à partir de l'interface de ligne de commande de Sophos Anti-Virus.

Ordinateurs en réseau non administrés par l'Enterprise Console ou par Sophos Central

Si vous avez un réseau d'ordinateurs Linux *non* administrés par Sophos Enterprise Console ou par Sophos Central configurez Sophos Anti-Virus de la manière suivante :

- Configurez les **contrôles sur accès, les contrôles planifiés, les alertes, la journalisation et la mise à jour** de manière centralisée en modifiant un fichier de configuration à partir duquel les ordinateurs se mettent à jour. Retrouvez plus d'informations dans l'Annexe : configuration des Fichiers supplémentaires à la page 40.
- Configurez localement sur chaque ordinateur les **contrôles à la demande** à partir de l'interface de ligne de commande de Sophos Anti-Virus.

Remarque : n'utilisez pas la configuration des Fichiers supplémentaires sauf avis contraire du support technique. Autrement, vous ne pourrez plus utiliser la console d'administration Sophos. Vous ne pouvez pas utiliser la configuration de la console d'administration et la configuration des Fichiers supplémentaires simultanément.

Ordinateurs autonomes non administrés par l'Enterprise Console ou par Sophos Central

Si vous avez un ordinateur Linux autonome *non* administré par Sophos Enterprise Console ou Sophos Central, configurez toutes les fonctions de Sophos Anti-Virus à partir de l'interface de ligne de commande.

3 Contrôle sur accès

Le contrôle sur accès est la méthode principale de protection antivirus. À chaque fois que vous ouvrez, enregistrez ou copiez un fichier, Sophos Anti-Virus le contrôle et vous autorise à y accéder s'il est sain.

3.1 Vérification de l'activité du contrôle sur accès

- Pour vérifier que le contrôle sur accès est actif, saisissez :
  `/opt/sophos-av/bin/savdstatus`

3.2 Vérification du lancement automatique du contrôle sur accès au démarrage

Pour effectuer cette procédure, vous devez être connecté à l'ordinateur en tant qu'utilisateur root.

1. Vérifiez que **`savd`** démarrera automatiquement au démarrage du système :
   `chkconfig --list`

   Remarque : si cette commande ne fonctionne pas sur votre distribution Linux, utilisez l'utilitaire approprié pour afficher les services qui sont configurés pour démarrer au démarrage du système.

   Si la liste contient une entrée pour sav-protect avec 2:on, 3:on, 4:on et 5:on, le contrôle sur accès se lance automatiquement au démarrage du système.

   Sinon, saisissez :

   `/opt/sophos-av/bin/savdctl enableOnBoot savd`

2. Vérifiez que le contrôle sur accès démarrera automatiquement avec **`savd`** :
   `/opt/sophos-av/bin/savconfig query EnableOnStart`

   Si la commande renvoie `true`, le contrôle sur accès démarrera automatiquement avec **`savd`** au démarrage du système.

   Sinon, saisissez :

   `/opt/sophos-av/bin/savconfig set EnableOnStart true`

3.3 Démarrage du contrôle sur accès

Pour démarrer le contrôle sur accès, procédez de l'une des manières suivantes :

- Saisissez :
  `/opt/sophos-av/bin/savdctl enable`

- Utilisez l'outil approprié pour démarrer le service sav-protect. Par exemple, saisissez :
  `/etc/init.d/sav-protect start`

  ou

```
service sav-protect start
```

3.4 Arrêt du contrôle sur accès

Important : si vous arrêtez le contrôle sur accès, Sophos Anti-Virus ne contrôle pas la présence de virus dans les fichiers auxquels vous accédez. Votre ordinateur, ainsi que tous les autres ordinateurs qui y sont connectés, sont par conséquent en danger.

- Pour arrêter le contrôle sur accès, saisissez :
  `/opt/sophos-av/bin/savdctl disable`

4 Contrôle à la demande

Un *contrôle à la demande* est un contrôle que vous lancez. Vous pouvez tout contrôler, que ce soit un fichier unique ou tout fichier de votre ordinateur sur lesquels vous avez les droits en lecture. Vous pouvez soit exécuter un contrôle manuel à la demande, soit le planifier pour qu'il s'exécute tout seul.

Pour planifier un contrôle à la demande, utilisez la commande **`crontab`**. Retrouvez plus de renseignements dans l'article 12176 de la base de connaissances du support de Sophos.

4.1 Exécution des contrôles à la demande

La commande à saisir pour exécuter un contrôle à la demande est **`savscan`**.

4.1.1 Contrôle de l'ordinateur

- Pour contrôler l'ordinateur, saisissez :
  `savscan /`

4.1.2 Contrôle d'un répertoire ou d'un fichier particulier

- Pour effectuer le contrôle d'un répertoire ou d'un fichier particulier, utilisez le chemin menant à l'élément. Par exemple, saisissez :
  `savscan /usr/mydirectory/myfile`

  Vous pouvez saisir plus d'un répertoire ou plus d'un fichier dans la même commande.

4.1.3 Contrôle d'un système de fichiers

- Pour contrôler un système de fichiers, veuillez indiquer son nom. Par exemple, saisissez :
  `savscan /home`

  Vous pouvez saisir plus d'un système de fichiers dans la même commande.

4.1.4 Contrôle d'un secteur de démarrage

Remarque : ceci s'applique uniquement à Linux et FreeBSD.

Pour contrôler un secteur de démarrage, ouvrez une session en tant que superutilisateur. Ainsi, vous disposerez des droits suffisants pour accéder aux périphériques du disque.

Vous pouvez contrôler le secteur de démarrage d'un lecteur logique ou physique.

- Pour contrôler les secteurs de démarrage de lecteurs logiques indiqués, saisissez :
  `savscan -bs=`*`drive, drive, ...`*

  où *drive* correspond au nom d'un lecteur (par exemple `/dev/fd0` ou `/dev/hda1`.

- Pour contrôler les secteurs de démarrage de tous les lecteurs logiques, saisissez :
  `savscan -bs`

- Pour contrôler les enregistrements de démarrage maîtres de tous les lecteurs physiques fixes de l'ordinateur, saisissez :
  `savscan -mbr`

4.2 Configuration de contrôles à la demande

Dans cette section, lorsque *path* apparaît dans une commande, ceci indique le chemin à contrôler.

Pour voir une liste complète des options que vous pouvez utiliser avec le contrôle à la demande, saisissez :

`man savscan`

4.2.1 Contrôle de tous les types de fichier

Par défaut, Sophos Anti-Virus contrôle uniquement les fichiers exécutables. Pour voir une liste complète des types de fichier que Sophos Anti-Virus contrôle par défaut, saisissez **`savscan -vv`**.

- Pour contrôler tous les types de fichier et pas uniquement ceux contrôlés par défaut, utilisez l'option **-all**. Saisissez :
  `savscan` *`path`* **`-all`**

  Remarque : cette commande allonge le temps de contrôle, peut affecter les performances sur les serveurs et produire de faux rapports viraux.

4.2.2 Contrôle d'un type de fichier particulier

Par défaut, Sophos Anti-Virus contrôle uniquement les fichiers exécutables. Pour voir une liste complète des types de fichier que Sophos Anti-Virus contrôle par défaut, saisissez **`savscan -vv`**.

- Pour contrôler un type de fichier particulier, utilisez l'option **-ext** avec l'extension de fichier appropriée. Par exemple, pour contrôler les fichiers dont le nom contient l'extension `.txt`, saisissez :
  `savscan` *`path`* **`-ext=txt`**

- Pour désactiver le contrôle d'un type de fichier particulier, utilisez l'option **-next** avec l'extension de fichier appropriée.

Remarque : pour indiquer plusieurs types de fichier, séparez chaque extension de fichier par une virgule.

4.2.3 Contrôle du contenu de tous les types d'archive

Vous pouvez configurer Sophos Anti-Virus pour qu'il contrôle le contenu de tous les types d'archive. Pour voir une liste de ces types d'archive, saisissez **`savscan -vv`**.

Remarque : le moteur de détection des menaces contrôle uniquement les fichiers archivés dont la taille ne dépasse pas 8 Go (lorsqu'ils sont décompressés). En effet, il est compatible avec le format d'archive POSIX ustar qui ne prend pas en charge les fichiers de plus grande taille.

- Pour contrôler le contenu de tous les types d'archive, utilisez l'option **-archive**. Saisissez :

savscan *path* **-archive**

Les archives ‘imbriquées’ dans d'autres archives (par exemple une archive TAR dans une archive ZIP) sont contrôlées de manière récursive.

Si vous disposez de nombreuses archives complexes, le contrôle peut être plus long à s'exécuter. Pensez-y lorsque vous planifiez des contrôles sans surveillance.

4.2.4 Contrôle du contenu d'un type d'archive particulier

Vous pouvez configurer Sophos Anti-Virus pour qu'il effectue le contrôle du contenu d'un type d'archive particulier. Pour voir une liste de ces types d'archive, saisissez **savscan -vv**.

Remarque : le moteur de détection des menaces contrôle uniquement les fichiers archivés dont la taille ne dépasse pas 8 Go (lorsqu'ils sont décompressés). En effet, il est compatible avec le format d'archive POSIX ustar qui ne prend pas en charge les fichiers de plus grande taille.

- Pour contrôler le contenu d'un type d'archive particulier, utilisez l'option indiquée dans la liste. Par exemple, pour contrôler le contenu des archives TAR et ZIP, saisissez :
  savscan *path* **-tar -zip**

  Les archives « imbriquées » dans d'autres archives (par exemple une archive TAR dans une archive ZIP) sont contrôlées de manière récursive.

  Si vous disposez de nombreuses archives complexes, le contrôle peut être plus long à s'exécuter. Pensez-y lorsque vous planifiez des contrôles sans surveillance.

4.2.5 Contrôle des ordinateurs distants

Par défaut, Sophos Anti-Virus ne contrôle pas les éléments sur les ordinateurs distants (c'est-à-dire qu'il ne couvre pas les points de montage distants).

- Pour contrôler les ordinateurs distants, utilisez l'option **--no-stay-on-machine**. Saisissez :
  savscan *path* **--no-stay-on-machine**

4.2.6 Désactivation du contrôle des éléments avec des liens symboliques

Par défaut, Sophos Anti-Virus contrôle les éléments avec des liens symboliques.

- Pour désactiver le contrôle des éléments avec des liens symboliques, utilisez l'option **--no-follow-symlinks**. Saisissez :
  savscan *path* **--no-follow-symlinks**

  Pour éviter de contrôler les éléments plusieurs fois, utilisez l'option **--backtrack-protection**.

4.2.7 Contrôle du système de fichiers de démarrage uniquement

Sophos Anti-Virus peut être configuré de manière à ne pas contrôler les éléments présents au-delà du système de fichiers de démarrage (c'est-à-dire ne pas couvrir les points de montage).

- Pour contrôler le système de fichiers de démarrage uniquement, utilisez l'option **--stay-on-filesystem**. Saisissez :
  savscan *path* **--stay-on-filesystem**

4.2.8 Exclusion d'éléments du contrôle

Vous pouvez configurer Sophos Anti-Virus afin d'exclure des éléments particuliers (fichiers, répertoires ou systèmes de fichiers) à partir du contrôle en utilisant l'option **-exclude**. Sophos Anti-Virus exclut tous les éléments qui suivent l'option dans la chaîne de commande. Par exemple, pour contrôler les éléments `fred` et `harry` et pas `tom` ou `peter`, saisissez :

```
savscan fred harry -exclude tom peter
```

Vous pouvez exclure des répertoires ou des fichiers qui sont *sous* un répertoire particulier. Par exemple, pour contrôler l'intégralité du répertoire personnel de Fred et exclure le répertoire de `jeux` (ainsi que tous ses sous-répertoires et fichiers), saisissez :

```
savscan /domicile/fred -exclude /home/fred/jeux
```

Vous pouvez aussi configurer Sophos Anti-Virus pour inclure des éléments particuliers qui suivent l'option **-include**. Par exemple, pour contrôler les éléments `fred`, `harry` et `bill` et pas `tom` ou `peter`, saisissez :

```
savscan fred harry -exclude tom peter -include bill
```

4.2.9 Contrôle des types de fichier définis comme exécutables par UNIX

Par défaut, Sophos Anti-Virus ne contrôle pas les types de fichier définis comme exécutables par UNIX.

- Pour contrôler les types de fichier définis comme exécutables par UNIX, utilisez l'option **--examine-x-bit**. Saisissez :
  savscan *path* **--examine-x-bit**

  Sophos Anti-Virus continue à contrôler les fichiers dont les extensions figurent également dans sa propre liste. Pour voir une liste de ces extensions, saisissez **savscan -vv**.

5 Que se passe-t-il en cas de détection de virus ?

Quels que soient les virus détectés par le contrôle sur accès ou par le contrôle à la demande, Sophos Anti-Virus :

- Consigne l'événement dans syslog et le journal Sophos Anti-Virus (reportez-vous à la section Affichage du journal Sophos Anti-Virus à la page 19).
- Envoie une alerte à l'Enterprise Console s'il est administré par l'Enterprise Console.
- Envoie une alerte par email à root@localhost.

Par défaut, Sophos Anti-Virus affiche également des alertes selon que les virus ont été détectés par le contrôle sur accès ou par un contrôle à la demande comme décrit ci-dessous.

Contrôle sur accès

Si le contrôle sur accès détecte un virus, Sophos Anti-Virus refuse l'accès au fichier et affiche par défaut une alerte de bureau semblable à celle ci-dessous.

Si l'alerte de bureau ne peut pas être affichée, une alerte par ligne de commande est affichée.

Retrouvez plus d'informations sur le nettoyage des virus à la section Nettoyage des virus à la page 16.

Contrôle à la demande

Si un contrôle à la demande détecte un virus, Sophos Anti-Virus affiche une alerte par ligne de commande. Il signale le virus sur la ligne qui commence par >>> suivie soit de `Virus`, soit de `Fragment de virus` :

```
Utilitaire de détection virale SAVScan
Version 4.69.0 [Linux/Intel]
Version des données virales 4.69
```

```
Inclut la détection de 2871136 virus, chevaux de Troie et vers
Copyright (c) 1989-2012 Sophos Limited. Tous droits réservés.
Heure système 13:43:32, Date système 22 septembre 2012
Répertoire IDE : /opt/sophos-av/lib/sav
Utilisation du fichier IDE nyrate-d.ide
. . . . . .
Utilisation IDE du fichier injec-lz.ide
Contrôle rapide
>>> Virus 'EICAR-AV-Test' trouvé dans fichier
/usr/mydirectory/eicar.src
33 fichiers contrôlés en 2 secondes.
1 virus a été découvert.
1 fichier sur 33 a été infecté.
Veuillez envoyer les échantillons infectés à Sophos en vue d'une
analyse.
Pour obtenir des conseils, consultez www.sophos.com/fr-fr ou envoyez
 un courrier électronique à support@sophos.fr
Fin du contrôle.
```

Retrouvez plus d'informations sur le nettoyage des virus à la section Nettoyage des virus à la page 16.

6 Nettoyage de virus

6.1 Informations sur le nettoyage

Si des virus sont signalés, rendez-vous sur le site Web de Sophos pour obtenir des informations et des conseils de nettoyage de vos machines.

Pour obtenir des informations sur le nettoyage :

1. Rendez-vous sur la page des analyses de sécurité (http://www.sophos.com/fr-fr/threat-center/threat-analyses/viruses-and-spyware.aspx).
2. Recherchez l'analyse de virus en utilisant le nom indiqué par Sophos Anti-Virus.

6.2 Mise en quarantaine des fichiers infectés

Vous pouvez configurer un contrôle à la demande pour mettre les fichiers infectés en quarantaine et empêcher ainsi leur accès. Le logiciel effectue cette opération en changeant les droits de propriété et d'accès aux fichiers.

Remarque : si vous indiquez désinfection (voir section Nettoyage des fichiers infectés à la page 17) ainsi que mise en quarantaine, Sophos Anti-Virus tente de désinfecter les éléments infectés et les met en quarantaine uniquement en cas d'échec de la désinfection.

Dans cette section, lorsque *path* apparaît dans une commande, ceci indique le chemin à contrôler.

6.2.1 Définition de la mise en quarantaine

- Pour définir la mise en quarantaine, utilisez l'option **--quarantine**. Saisissez :
  `savscan` *`path`* **`--quarantine`**

6.2.2 Définition des droits de propriétés et d'accès en vigueur

Par défaut, Sophos Anti-Virus change :

- Les droits de propriété de l'utilisateur sur un fichier infecté sur ceux de l'utilisateur exécutant Sophos Anti-Virus.
- Les droits de propriété de groupe du fichier sur ceux du groupe auquel l'utilisateur appartient.
- Les droits d'accès aux fichiers sur `-r--------` (0400).

Si vous le souhaitez, vous pouvez changer les droits de propriété et d'accès de l'utilisateur ou du groupe que Sophos Anti-Virus va appliquer aux fichiers infectés. Pour cela, servez-vous des paramètres suivants :

```
uid=nnn
user=username
gid=nnn
group=group-name
mode=ppp
```

Vous ne pouvez pas définir plus d'un seul paramètre pour les droits de propriété de l'utilisateur ou pour les droits de propriété de groupe. Par exemple, vous ne pouvez pas définir un paramètre **uid** *et* **user**.

Pour chaque paramètre non défini par vos soins, c'est le paramètrage par défaut (indiqué ci-dessus) qui est utilisé.

Par exemple :

```
savscan fred --quarantine:user=virus,group=virus,mode=0400
```

change les droits de propriété de l'utilisateur d'un fichier infecté sur « virus », les droits de propriété du groupe sur « virus » et les droits d'accès au fichier sur `-r---------`. Ceci signifie que le fichier est la propriété de l'utilisateur « virus » et du groupe « virus », mais que seul l'utilisateur « virus » a accès au fichier (en lecture seulement). Aucune autre personne que l'administrateur root ne peut modifier le fichier.

Il sera peut être nécessaire d'ouvrir une session en tant qu'utilisateur spécial ou en tant que super utilisateur pour définir les droits de propriété et d'accès.

6.3 Nettoyage des fichiers infectés

Vous pouvez configurer un contrôle à la demande pour nettoyer (désinfecter ou supprimer) les fichiers infectés. Toutes les actions que Sophos Anti-Virus prend contre les fichiers infectés sont répertoriées dans le résumé des contrôle et consignées dans le journal Sophos Anti-Virus. Par défaut, le nettoyage est désactivé.

Dans cette section, lorsque *path* apparaît dans une commande, ceci indique le chemin à contrôler.

6.3.1 Désinfection d'un fichier infecté spécifique

- Pour désinfecter un fichier infecté spécifique, utilisez l'option **-di**. Saisissez :
  savscan *path* **-di**

  Sophos Anti-Virus demande confirmation avant de procéder à la désinfection.

  Remarque : la désinfection d'un document infecté ne répare pas les modifications que le virus a apportées au document. (Retrouvez plus de renseignements sur les effets secondaires des virus à la section Informations sur le nettoyage à la page 16 du site Web de Sophos).

6.3.2 Désinfection de tous les fichiers infectés sur l'ordinateur

- Pour désinfecter tous les fichiers infectés sur l'ordinateur, saisissez :
  savscan / -di

  Sophos Anti-Virus demande confirmation avant de procéder à la désinfection.

  Remarque : la désinfection d'un document infecté ne répare pas les modifications que le virus a apportées au document. (Retrouvez plus de renseignements sur les effets secondaires des virus à la section Informations sur le nettoyage à la page 16 du site Web de Sophos).

6.3.3 Suppression d'un fichier infecté spécifique

- Pour supprimer un fichier infecté spécifique, utilisez l'option **-remove**. Saisissez :
  savscan *path* **-remove**

  Sophos Anti-Virus demande confirmation avant de procéder à la suppression.

6.3.4 Suppression de tous les fichiers infectés sur l'ordinateur

- Pour supprimer tous les fichiers infectés sur l'ordinateur, saisissez :
  savscan / -remove

  Sophos Anti-Virus demande confirmation avant de procéder à la suppression.

6.3.5 Désinfection du secteur de démarrage infecté

Remarque : ceci s'applique uniquement à Linux et FreeBSD.

- Pour désinfecter un secteur de démarrage infecté, utilisez l'option de désinfection **-di** ainsi que l'option de secteur de démarrage **-bs**. Par exemple, saisissez :
  savscan -bs=/dev/fd0 -di

  où **/dev/fd0** correspond au nom du lecteur contenant le secteur de démarrage infecté.

  Sophos Anti-Virus demande confirmation avant de procéder à la désinfection.

6.4 Récupération suite aux effets secondaires des virus

Après une infection virale, la récupération dépend de la manière dont le virus a infecté l'ordinateur. Certains virus ne laissent aucun effet secondaire à traiter. D'autres peuvent avoir des effets secondaires si violents que vous serez obligé de restaurer le disque dur.

Certains virus modifient progressivement et imperceptiblement les données. Ce type de corruption est difficile à détecter. Il est donc très important de lire l'analyse de virus sur le site Web de Sophos et de procéder à une vérification soigneuse des documents suite à la désinfection.

Il est indispensable que vous disposiez de sauvegardes saines. Si vous ne disposez pas de sauvegardes, commencez à en créer afin de prévenir de futures infections.

Il est parfois possible de récupérer des données sur les disques endommagés par un virus. Sophos peut vous fournir des utilitaires pour réparer les dommages occasionnés par certains virus. Veuillez contacter le support technique Sophos pour obtenir plus de renseignements.

7 Affichage du journal Sophos Anti-Virus

Sophos Anti-Virus consigne les détails de l'activité de contrôle dans le journal Sophos Anti-Virus et dans syslog. En outre, les événements de virus/spywares et les erreurs sont consignés dans le journal Sophos Anti-Virus.

- Pour consulter le journal Sophos Anti-Virus, utilisez la commande **savlog**. Cette commande peut être utilisée avec diverses options afin de limiter le flux de sortie de certains messages et de contrôler l'affichage.

  Par exemple, pour afficher tous les messages consignés dans le journal Sophos Anti-Virus au cours des dernières 24 heures et pour afficher la date et l'heure au format UTC/ISO 8601, saisissez :

  ```
  /opt/sophos-av/bin/savlog --today --utc
  ```

- Pour voir la liste complète des options utilisables avec **savlog**, saisissez :

  ```
  man savlog
  ```

8 Mise à jour immédiate de Sophos Anti-Virus

Sophos Anti-Virus est automatiquement maintenu à jour à condition d'avoir activé la mise à jour automatique lors de l'installation. Toutefois, vous pouvez également mettre à jour Sophos Anti-Virus immédiatement sans attendre la prochaine mise à jour automatique.

- Pour mettre à jour Sophos Anti-Virus immédiatement, rendez-vous sur l'ordinateur que vous voulez mettre à jour et saisissez :
  `/opt/sophos-av/bin/savupdate`

Remarque : vous pouvez également mettre à jour les ordinateurs immédiatement depuis la Sophos Enterprise Console.

9 À propos de la prise en charge des noyaux

Remarque : cette section est seulement applicable si vous utilisez Talpa comme méthode d'interception par contrôle sur accès. Retrouvez plus d'informations à la section Modification de la méthode d'interception de fichiers par contrôle sur accès à la page 36.

9.1 À propos de la prise en charge des nouvelles versions du noyau

Lorsqu'un des éditeurs de Linux pris en charge par Sophos Anti-Virus publie une mise à jour de son noyau Linux, Sophos le prend en charge en publiant à son tour une mise à jour du module d'interface noyau Sophos (Talpa). Si vous appliquez une mise à jour de noyau Linux avant d'appliquer la mise à jour Talpa correspondante, Sophos Anti-Virus lance une compilation locale de Talpa. En cas d'échec, Sophos Anti-Virus essaie d'utiliser à la place Fanotify comme méthode d'interception. Si Fanotify est également indisponible, le contrôle sur accès est arrêté et une erreur est signalée.

Pour éviter ce problème, vous devez confirmer que la mise à jour Talpa correspondante a été publiée avant d'appliquer la mise à jour du noyau Linux. Une liste des distributions Linux prises en charge et des mises à jour est disponible dans l'article 14377 de la base de connaissances du support Sophos (http://www.sophos.com/fr-fr/support/knowledgebase/14377.aspx). Si la mise à jour Talpa requise est répertoriée, c'est qu'elle est disponible au téléchargement. Sophos Anti-Virus télécharge automatiquement la mise à jour si l'option de mise à jour automatique a été activée. Sinon, pour mettre à jour Sophos Anti-Virus immédiatement, sans attendre la mise à jour automatique suivante, saisissez :

```
/opt/sophos-av/bin/savupdate
```

Vous pouvez ensuite appliquer la mise à jour du noyau Linux.

9.2 À propos de la prise en charge des noyaux personnalisés

Si vous personnalisez vos noyaux Linux, ce manuel n'explique pas comment configurer la mise à jour pour prendre en charge cela. Retrouvez plus d'informations dans l'article 13503 de la base de connaissances du support de Sophos (http://www.sophos.com/fr-fr/support/knowledgebase/13503.aspx).

10 configuration des contrôles planifiés

Sophos Anti-Virus archive les définitions d'un ou de plusieurs contrôles planifiés.

Remarque : les noms des contrôles planifiés qui ont été ajoutés à l'aide de l'Enterprise Console sont préfixés avec « SEC: » et peuvent uniquement être mis à jour ou supprimés à l'aide de l'Enterprise Console.

10.1 Ajout d'un contrôle planifié depuis un fichier

1. Pour utiliser une définition de contrôle modèle comme point de départ, ouvrez `/opt/sophos-av/doc/namedscan.exemple.fr`.

   Pour créer une nouvelle définition de contrôle, ouvrez un nouveau fichier texte.

2. Indiquez ce que vous voulez contrôler, quand effectuer le contrôle et toutes autres options de votre choix en utilisant uniquement les paramètres répertoriés dans le modèle.

   Pour planifier le contrôle, vous devez inclure au moins un jour et une heure.

3. Enregistrez le fichier sous un emplacement de votre choix en prenant bien soin de ne pas remplacer le modèle.
4. Ajoutez le contrôle planifié à Sophos Anti-Virus à l'aide de la commande **`savconfig`** en utilisant l'opération **add** et le paramètre **NamedScans**. Indiquez le nom du contrôle et le chemin du fichier de définition du contrôle.

   Par exemple, pour ajouter le contrôle Daily archivé dans `/home/fred/DailyScan`, saisissez :

   ```
   /opt/sophos-av/bin/savconfig add NamedScans Daily
   /home/fred/DailyScan
   ```

10.2 Ajout d'un contrôle planifié depuis une entrée standard

1. Ajoutez le contrôle planifié à Sophos Anti-Virus à l'aide de la commande **`savconfig`** en utilisant l'opération **add** et le paramètre **NamedScans**. Indiquez le nom du contrôle et utilisez un tiret pour préciser que la définition doit être lue depuis une entrée standard.

   Par exemple, pour ajouter le contrôle Daily, saisissez :

   ```
   /opt/sophos-av/bin/savconfig add NamedScans Daily -
   ```

   Lorsque vous appuyez sur ENTRÉE, Sophos Anti-Virus attend que vous saisissiez la définition du contrôle planifié.

2. Indiquez ce que vous voulez contrôler, quand effectuer le contrôle et toutes autres options de votre choix en utilisant uniquement les paramètres répertoriés dans le modèle de définition de contrôle : `/opt/sophos-av/doc/namedscan.example.en`. Après avoir saisi chaque paramètre et sa valeur, appuyez sur ENTRÉE.

   Pour planifier le contrôle, vous devez inclure au moins un jour et une heure.

3. Pour terminer la définition, appuyez sur CTRL+D.

10.3 Exportation d'un contrôle planifié dans un fichier

- Pour exporter un contrôle planifié à partir de Sophos Anti-Virus dans un fichier, utilisez la commande **savconfig** en utilisant l'opération **query** et le paramètre **NamedScans**. Indiquez le nom du contrôle et le chemin du fichier dans lequel vous souhaitez exporter le contrôle.

  Par exemple, pour exporter le contrôle Daily dans le fichier `/home/fred/DailyScan`, saisissez :

  /opt/sophos-av/bin/savconfig query NamedScans Daily > /home/fred/DailyScan

10.4 Exportation des noms de tous les contrôles planifiés dans un fichier

- Pour exporter les noms de tous les contrôles planifiés (y compris ceux qui ont été créés à l'aide de l'Enterprise Console) à partir de Sophos Anti-Virus dans un fichier, utilisez la commande **savconfig** en utilisant l'opération **query** et le paramètre **NamedScans**. Indiquez le chemin du fichier dans lequel vous souhaitez exporter les noms des contrôles.

  Par exemple, pour exporter les noms de tous les contrôles planifiés dans le fichier `/home/fred/AllScans`, saisissez :

  /opt/sophos-av/bin/savconfig query NamedScans > /home/fred/AllScans

  Remarque : `SEC:FullSystemScan` est un contrôle qui est toujours défini si l'ordinateur est administré par l'Enterprise Console.

10.5 Exportation d'un contrôle planifié dans une sortie standard

- Pour exporter un contrôle planifié à partir de Sophos Anti-Virus dans une sortie standard, utilisez la commande **savconfig** en utilisant l'opération **query** et le paramètre **NamedScans**. Indiquez le nom du contrôle.

  Par exemple, pour exporter le contrôle Daily dans la sortie standard, saisissez :

  /opt/sophos-av/bin/savconfig query NamedScans Daily

10.6 Exportation des noms de tous les contrôles planifiés dans une sortie standard

- Pour exporter tous les contrôles planifiés (y compris ceux qui ont été créés à l'aide de l'Enterprise Console) depuis Sophos Anti-Virus dans une sortie standard utilisez la commande **savconfig** en utilisant l'opération **query** et le paramètre **NamedScans**.

  Par exemple, pour exporter les noms de tous les contrôles planifiés dans la sortie standard, saisissez :

  /opt/sophos-av/bin/savconfig query NamedScans

Remarque : `SEC:FullSystemScan` est un contrôle qui est toujours défini si l'ordinateur est administré par l'Enterprise Console.

10.7 Mise à jour d'un contrôle planifié à partir d'un fichier

Remarque : vous ne pouvez pas mettre à jour les contrôles planifiés qui ont été ajoutés à l'aide de l'Enterprise Console.

1. Ouvrez le fichier qui définit le contrôle planifié que vous souhaitez mettre à jour.

   Si le contrôle n'est pas déjà défini dans un fichier, vous pouvez exporter le contrôle dans un fichier comme décrit à la section Exportation d'un contrôle planifié dans un fichier à la page 23.

2. Modifiez la définition si nécessaire en utilisant uniquement les paramètres répertoriés dans le modèle de définition de contrôle : `/opt/sophos-av/doc/namedscan.example.en`. Définissez le contrôle entièrement plutôt que de préciser uniquement ce que vous désirez mettre à jour.
3. Enregistrez le fichier.
4. Procédez à la mise à jour du contrôle planifié à partir de Sophos Anti-Virus à l'aide de la commande **`savconfig`** en utilisant l'opération **update** et le paramètre **NamedScans**. Indiquez le nom du contrôle et le chemin du fichier de définition du contrôle.

   Par exemple, pour mettre à jour le contrôle Daily archivé dans `/home/fred/DailyScan`, saisissez :

   ```
   /opt/sophos-av/bin/savconfig update NamedScans Daily
   /home/fred/DailyScan
   ```

10.8 Mise à jour d'un contrôle planifié depuis une entrée standard

Remarque : vous ne pouvez pas mettre à jour les contrôles planifiés qui ont été ajoutés à l'aide de l'Enterprise Console.

1. Procédez à la mise à jour du contrôle planifié à partir de Sophos Anti-Virus à l'aide de la commande **`savconfig`** en utilisant l'opération **update** et le paramètre **NamedScans**. Indiquez le nom du contrôle et utilisez un tiret pour préciser que la définition doit être lue depuis une entrée standard.

   Par exemple, pour mettre à jour le contrôle Daily, saisissez :

   ```
   /opt/sophos-av/bin/savconfig update NamedScans Daily -
   ```

   Lorsque vous appuyez sur ENTRÉE, Sophos Anti-Virus attend que vous saisissiez la définition du contrôle planifié.

2. Indiquez ce que vous voulez contrôler, quand effectuer le contrôle et toutes autres options de votre choix en utilisant uniquement les paramètres répertoriés dans le modèle de définition de contrôle : `/opt/sophos-av/doc/namedscan.example.en`. Après avoir saisi chaque paramètre et sa valeur, appuyez sur ENTRÉE. Définissez le contrôle entièrement plutôt que de préciser uniquement ce que vous désirez mettre à jour.

   Pour planifier le contrôle, vous devez inclure au moins un jour et une heure.

3. Pour terminer la définition, appuyez sur CTRL+D.

10.9 Affichage du journal d'un contrôle planifié

- Pour afficher le journal d'un contrôle planifié, utilisez la commande **savlog** et l'option **namedscan**. Indiquez le nom du contrôle.

  Par exemple, pour afficher le journal du contrôle Daily, saisissez :

  ```
  /opt/sophos-av/bin/savlog --namedscan=Daily
  ```

10.10 Suppression d'un contrôle planifié

Remarque : vous ne pouvez pas supprimer les contrôles planifiés qui ont été ajoutés à l'aide de l'Enterprise Console.

- Pour supprimer un contrôle planifié à partir de Sophos Anti-Virus, utilisez la commande **savconfig** en utilisant l'opération **remove** et le paramètre **NamedScans**. Indiquez le nom du contrôle.

  Par exemple, pour supprimer le contrôle Daily, saisissez :

  ```
  /opt/sophos-av/bin/savconfig remove NamedScans Daily
  ```

10.11 Suppression de tous les contrôles planifiés

Remarque : vous ne pouvez pas supprimer les contrôles planifiés qui ont été ajoutés à l'aide de l'Enterprise Console.

- Pour supprimer tous les contrôles planifiés à partir de Sophos Anti-Virus, saisissez :
  ```
  /opt/sophos-av/bin/savconfig delete NamedScans
  ```

11 configuration des alertes

Remarque : si vous configurez un ordinateur autonome connecté à un réseau, cette configuration peut être remplacée si l'ordinateur télécharge une nouvelle configuration de l'Enterprise Console ou une configuration des Fichiers supplémentaires.

Vous pouvez configurer Sophos Anti-Virus afin qu'il envoie une alerte en cas de détection de virus, d'une erreur du contrôle ou de tout autre type d'erreur. Les alertes peuvent être envoyées via les méthodes suivantes :

- Fenêtres instantanées sur le bureau (contrôle sur accès uniquement)
- Ligne de commande (contrôle sur accès uniquement)
- Email (contrôle sur accès et contrôle à la demande)

Les alertes par fenêtre instantanée sur le bureau et par ligne de commande sont envoyées dans la langue de l'ordinateur qui émet l'alerte. Les alertes par email peuvent être envoyées soit en anglais, soit en japonais.

11.1 Configuration des alertes de fenêtre instantanée de bureau

11.1.1 Désactivation des alertes de fenêtre instantanée de bureau

Par défaut, les alertes de fenêtre instantanée de bureau sont activées.

- Pour désactiver les alertes instantanées de bureau, saisissez :
  `/opt/sophos-av/bin/savconfig set UIpopupNotification disabled`
- Pour désactiver à la fois les alertes instantanées de bureau et par ligne de commande, saisissez :
  `/opt/sophos-av/bin/savconfig set UINotifier disabled`

11.1.2 Personnalisation d'un message

Vous pouvez créer un message personnalisé qui sera ajouté à toutes les alertes de ligne de commande et aux alertes instantanées sur le bureau.

👉 **Pour mémoire :** le message d'alerte principal peut être affiché en différentes langues (selon les paramètres du système), toutefois, le texte personnalisé s'affiche dans la langue que vous avez utilisée pour le créer.

- Pour personnaliser un message, utilisez le paramètre **UIContactMessage**. Par exemple, saisissez :
  `/opt/sophos-av/bin/savconfig set UIContactMessage 'Contactez le service informatique'`

11.2 Configuration des alertes par ligne de commande

11.2.1 Désactivation des alertes par ligne de commande

Par défaut, les alertes par ligne de commande sont activées.

- Pour désactiver les alertes par ligne de commande, saisissez :
  `/opt/sophos-av/bin/savconfig set UIttyNotification disabled`

- Pour désactiver à la fois les alertes instantanées de bureau et par ligne de commande, saisissez :
  `/opt/sophos-av/bin/savconfig set UINotifier disabled`

11.2.2 Personnalisation d'un message

Vous pouvez créer un message personnalisé qui sera ajouté à toutes les alertes de ligne de commande et aux alertes instantanées sur le bureau.

👉 **Pour mémoire :** le message d'alerte principal peut être affiché en différentes langues (selon les paramètres du système), toutefois, le texte personnalisé s'affiche dans la langue que vous avez utilisée pour le créer.

- Pour personnaliser un message, utilisez le paramètre **UIContactMessage**. Par exemple, saisissez :
  `/opt/sophos-av/bin/savconfig set UIContactMessage 'Contactez le service informatique'`

11.3 Configuration des alertes par email

11.3.1 Désactivation des alertes par email

Par défaut, les alertes par email sont activées.

- Pour désactiver les alertes par email, saisissez :
  `/opt/sophos-av/bin/savconfig set EmailNotifier disabled`

11.3.2 Spécification du nom d'hôte ou de l'adresse IP du serveur SMTP

Par défaut, le nom d'hôte et le port du serveur SMTP sont localhost:25.

- Pour définir le nom d'hôte ou l'adresse IP du serveur SMTP, utilisez le paramètre **EmailServer**. Par exemple, saisissez :
  `/opt/sophos-av/bin/savconfig set EmailServer 171.17.31.184`

11.3.3 Spécification de la langue

Par défaut, la langue utilisée pour le message d'alerte est l'anglais.

- Pour spécifier la langue utilisée pour le message d'alerte, utilisez le paramètre **EmailLanguage**. Actuellement, les seules valeurs valides sont **`English`** (anglais) ou **`Japanese`** (japonais). Par exemple, saisissez :
  `/opt/sophos-av/bin/savconfig set EmailLanguage Japanese`

  Remarque : cette sélection de la langue s'applique uniquement au message d'alerte lui-même et pas au message personnalisé inclus dans chaque alerte par email en plus du message d'alerte.

11.3.4 Spécification des destinataires de messagerie

Par défaut, les alertes par email sont envoyées à root@localhost.

- Pour ajouter une adresse à la liste de destinataires des alertes par email, utilisez le paramètre **Email** avec l'opération **add**. Par exemple, saisissez :
  `/opt/sophos-av/bin/savconfig add Email admin@localhost`

  Remarque : vous pouvez indiquer plus d'un destinataire dans la même commande. Séparez chaque destinataire par un espace.

- Pour supprimer une adresse de la liste, utilisez le paramètre **Email** avec l'opération **remove**. Par exemple, saisissez :
  `/opt/sophos-av/bin/savconfig remove Email admin@localhost`

  Important : vous pouvez supprimer **root@localhost** avec cette commande. Pour cela, veuillez remplacer la liste complétement avec la commande suivante :
  `/opt/sophos-av/bin/savconfig set Email <adresses email>`

11.3.5 Spécification de l'adresse électronique de l'expéditeur

Par défaut, les alertes par email sont envoyées à partir de root@localhost.

- Pour spécifier une adresse électronique de l'expéditeur, utilisez le paramètre **EmailSender**. Par exemple, saisissez :
  `/opt/sophos-av/bin/savconfig set EmailSender admin@localhost`

11.3.6 Spécification de l'adresse Répondre à

- Pour spécifier une adresse électronique Répondre à, utilisez le paramètre **EmailReplyTo** . Par exemple, saisissez :
  `/opt/sophos-av/bin/savconfig set EmailReplyTo admin@localhost`

11.3.7 Action à prendre en cas de détection sur accès de virus

Par défaut, Sophos Anti-Virus envoie une alerte par email si le contrôle sur accès détecte des virus. Un message personnalisé en anglais est inclus dans chaque alerte en plus du

message d'alerte lui-même. Vous pouvez modifier le texte de ce message mais il ne sera pas traduit.

- Pour désactiver l'envoi des alertes par email si des virus sont détectés sur accès, saisissez :
  `/opt/sophos-av/bin/savconfig set SendThreatEmail disabled`

- Pour personnaliser le message, utilisez le paramètre **hreatMessage**. Par exemple, saisissez :
  `/opt/sophos-av/bin/savconfig set LogMessage 'Contactez le service informatique'`

11.3.8 Action à prendre en cas d'erreur du contrôle sur accès

Par défaut, Sophos Anti-Virus envoie une alerte par email en cas d'erreur du contrôle sur accès. Un message personnalisé en anglais est inclus dans chaque alerte en plus du message d'alerte lui-même. Vous pouvez modifier le texte de ce message mais il ne sera pas traduit.

- Pour désactiver l'envoi des alertes par email en cas d'erreur du contrôle sur accès, saisissez :

  `/opt/sophos-av/bin/savconfig set SendErrorEmail disabled`

- Pour personnaliser le message, utilisez le paramètre **ScanErrorMessage**. Par exemple, saisissez :
  `/opt/sophos-av/bin/savconfig set LogMessage 'Contactez le service informatique'`

11.3.9 Désactivation des alertes par email à la demande

Par défaut, Sophos Anti-Virus envoie uniquement un email récapitulatif du contrôle à la demande si le contrôle détecte la présence de virus.

- Pour désactiver l'envoi d'un email récapitulatif du contrôle à la demande en cas de détection de virus, saisissez :
  `/opt/sophos-av/bin/savconfig set EmailDemandSummaryIfThreat disabled`

11.3.10 Action à prendre lorsqu'un évènement est consigné dans le journal

Par défaut, Sophos Anti-Virus envoie une alerte par email lorsqu'un événement est consigné dans le journal de Sophos Anti-Virus. Un message personnalisé en anglais est inclus dans chaque alerte en plus du message d'alerte lui-même. Vous pouvez changer le texte de ce message personnalisé mais il n'est pas traduit.

- Pour personnaliser le message, utilisez le paramètre **LogMessage**. Par exemple, saisissez :
  `/opt/sophos-av/bin/savconfig set LogMessage 'Contactez le service informatique'`

12 configuration de la journalisation

Remarque : si vous configurez un ordinateur autonome connecté à un réseau, cette configuration peut être remplacée si l'ordinateur télécharge une nouvelle configuration de l'Enterprise Console ou une configuration des Fichiers supplémentaires.

Par défaut, l'activité de contrôle est consignée dans le journal de Sophos Anti-Virus : `/opt/sophos-av/log/savd.log`. Lorsque celui-ci atteint la taille de 1 Mo, il est automatiquement sauvegardé dans le même répertoire et un nouveau journal est commencé.

- Pour voir le nombre de journaux par défaut qui sont conservés, saisissez :
  `/opt/sophos-av/bin/savconfig -s query LogMaxSizeMB`

- Pour indiquer le nombre maximum de journaux qui sont conservés, utilisez le paramètre **LogMaxSizeMB**. Par exemple, pour paramétrer le nombre maximal de journaux sur 50, saisissez :
  `/opt/sophos-av/bin/savconfig set LogMaxSizeMB 50`

13 configuration de la mise à jour

Important : si vous administrez Sophos Anti-Virus avec Sophos Enterprise Console, veuillez configurer la mise à jour à l'aide de l'Enterprise Console. Retrouvez plus de renseignements sur la manière de procéder dans l'Aide de l'Enterprise Console.

13.1 Concepts de base

Serveur de mise à jour

Un *serveur de mise à jour* est un ordinateur sur lequel vous avez installé Sophos Anti-Virus pour Linux et qui sert aussi de source de mise à jour aux autres ordinateurs. Ces autres ordinateurs sont soit des serveurs de mise à jour, soit des clients de mise à jour, selon la manière dont vous déployez Sophos Anti-Virus sur le réseau.

Client de mise à jour

Un *client de mise à jour* est un ordinateur sur lequel vous avez installé Sophos Anti-Virus et qui n'a pas besoin de servir de source de mise à jour aux autres ordinateurs.

Source de mise à jour principale

La *source de mise à jour principale* est l'emplacement des mises à jour auquel accède habituellement l'ordinateur. Des codes d'accès pourraient être nécessaires.

Source de mise à jour secondaire

La *source de mise à jour secondaire* est l'emplacement des mises à jour auquel accède l'ordinateur en cas d'indisponibilité de la source de mise à jour principale. Des codes d'accès pourraient être nécessaires.

13.2 Commande de configuration savsetup

La commande **`savsetup`** vous sert à configurer la mise à jour. Utilisez-la uniquement pour les tâches spécifiques abordées dans les sous-sections suivantes.

Bien qu'elle vous permette d'accéder uniquement à certains paramètres auxquels vous pouvez accéder avec **`savconfig`**, elle est bien plus facile à utiliser. Vous êtes invité à saisir les valeurs des paramètres et vous répondez en sélectionnant ou en saisissant les valeurs. Pour exécuter **`savsetup`**, saisissez :

```
/opt/sophos-av/bin/savsetup
```

13.3 Vérification de la configuration de la mise à jour automatique d'un ordinateur

1. Sur l'ordinateur que vous voulez vérifier, saisissez :
   `/opt/sophos-av/bin/savsetup`

   `savsetup` vous demande de sélectionner ce que vous voulez faire.

2. Sélectionnez **Auto-updating configuration**.

   `savsetup` vous demande de sélectionner ce que vous voulez faire.

3. Sélectionnez **Display update configuration** pour voir la configuration actuelle.

13.4 Configuration d'un serveur de mise à jour

Vous pouvez utiliser toute installation autonome de Sophos Anti-Virus pour Linux en tant que serveur de mise à jour pour d'autres ordinateurs en réseau.

1. Sur le serveur de mise à jour, saisissez :
   `/opt/sophos-av/bin/savsetup`

   `savsetup` vous demande de sélectionner ce que vous voulez faire.

2. Sélectionnez une option et suivez les instructions pour configurer le serveur de mise à jour.

   Lorsque vous configurez les mises à jour et, surtout si vous procédez à la mise à jour à partir de Sophos, saisissez le nom d'utilisateur et le mot de passe inclus dans votre licence. Si vous procédez à la mise à jour à partir d'un serveur de mise à jour, vous pouvez indiquer soit une adresse HTTP, soit un chemin UNC, selon la manière dont vous avez paramétré le serveur de mise à jour.

3. Pour héberger les mises à jour d'autres clients Sophos Anti-Virus :

   a) Configurez le serveur de mise à jour pour télécharger les fichiers supplémentaires qui pourraient servir aux clients de mise à jour. Sur le serveur de mise à jour, saisissez :
   `/opt/sophos-av/bin/savconfig set PrimaryUpdateAllDistros true`

   b) Forcez le serveur de mise à jour à se mettre à jour afin de vous assurer que les fichiers supplémentaires ont été téléchargés. Sur le serveur de mise à jour, saisissez :
   `/opt/sophos-av/bin/savupdate --force`

   c) Copiez le répertoire de cache local (/opt/sophos-av/update/cache/) à un emplacement différent sur le système de fichiers.

   Cette opération peut être automatisée à l'aide d'un script.

   d) Mettez l'emplacement à disposition des autres ordinateurs du réseau en le publiant via HTTP, SMB, NFS ou à l'aide de toute autre méthode.

   Cet emplacement sera le répertoire d'installation centralisée (CID) à partir duquel les clients téléchargeront les mises à jour.

13.5 Configuration de plusieurs clients de mise à jour pour la mise à jour

Cette section explique comment modifier les paramètres de mise à jour dans la configuration des Fichiers supplémentaires. La configuration est alors téléchargée par les clients de mise à jour lorsqu'ils mettent à jour la fois suivante.

Cette section suppose que vous avez déjà créé la configuration des Fichiers supplémentaires. Si elle n'est pas créée, reportez-vous à l'Annexe : configuration des Fichiers supplémentaires à la page 40.

Remarque : cette section décrit la manière de configurer plusieurs clients de mise à jour à partir de la source de mise à jour *principale*. Vous pouvez utiliser la même procédure pour configurer votre source de mise à jour *secondaire* en remplaçant *Primary* par *Secondary*. Par exemple, à la place de **PrimaryUpdateSourcePath**, utilisez plutôt **SecondaryUpdateSourcePath**.

Pour configurer plusieurs clients de mise à jour pour la mise à jour :

1. Sur l'ordinateur sur lequel est stockée la configuration des Fichiers supplémentaires, paramétrez l'adresse de la source de mise à jour sur **`sophos:`**. Vous pouvez également paramétrer l'emplacement du répertoire d'installation centralisée (CID) à l'aide du paramètre **PrimaryUpdateSourcePath**.

   Pour procéder à la mise à jour à partir du CID, vous pouvez spécifier soit une adresse HTTP, soit un chemin UNC, selon la manière dont vous avez paramétré le serveur de mise à jour. Par exemple, saisissez :

   ```
   /opt/sophos-av/bin/savconfig -f offline-config-file-path -c set PrimaryUpdateSourcePath 'http://www.mywebcid.com/cid'
   ```

   Pour procéder à la mise à jour à partir de **`sophos:`**, saisissez :

   ```
   /opt/sophos-av/bin/savconfig -f offline-config-file-path -c set PrimaryUpdateSourcePath 'sophos:'
   ```

2. Si la source de mise à jour exige une authentification, définissez le nom d'utilisateur et le mot de passe respectivement à l'aide des paramètres **PrimaryUpdateUsername** et **PrimaryUpdatePassword**. Par exemple, saisissez :

   ```
   /opt/sophos-av/bin/savconfig -f offline-config-file-path -c set PrimaryUpdateUsername 'fred'
   ```

   ```
   /opt/sophos-av/bin/savconfig -f offline-config-file-path -c set PrimaryUpdatePassword 'j23rjjfwj'
   ```

3. Si vous accédez à la source de mise à jour via un proxy, définissez l'adresse, le nom d'utilisateur et le mot de passe du serveur proxy respectivement à l'aide des paramètres **PrimaryUpdateProxyAddress**, **PrimaryUpdateProxyUsername** et **PrimaryUpdateProxyPassword**. Par exemple, saisissez :

   ```
   /opt/sophos-av/bin/savconfig -f offline-config-file-path -c set PrimaryUpdateProxyAddress 'http://www-cache.xyz.com:8080'
   ```

   ```
   /opt/sophos-av/bin/savconfig -f offline-config-file-path-c set PrimaryUpdateProxyUsername 'penelope'
   ```

   ```
   /opt/sophos-av/bin/savconfig -f offline-config-file-path -c set PrimaryUpdateProxyPassword 'fj202jrjf'
   ```

4. Lorsque vous avez terminé de définir les paramètres dans le fichier de configuration hors ligne, mettez à jour le fichier de configuration en ligne à l'aide de la commande **addextra**. Utilisez la syntaxe suivante :

   /opt/sophos-av/update/addextra
   offline-config-file-pathlive-config-file-path
   --signing-key=*signing-key-file-path*
   --signing-certificate=*signing-certificate-file-path*

   Par exemple :

   /opt/sophos-av/update/addextra /opt/sophos-av/OfflineConfig.cfg /var/www/extrafiles/ --signing-key= /root/certificates/extrafiles-signing.key --signing-certificate=/root/certificates/extrafiles-signing.crt

La configuration mise à jour est désormais prête et pourra être téléchargée par les clients à leur prochaine mise à jour.

13.6 Configuration d'un client de mise à jour autonome pour la mise à jour

1. Sur l'ordinateur que vous voulez configurer, saisissez :
   /opt/sophos-av/bin/savsetup

   savsetup vous demande de sélectionner ce que vous voulez faire.

2. Sélectionnez une option et suivez les instructions pour configurer le client de mise à jour.

   Lorsque vous configurez les mises à jour et, surtout si vous procédez à la mise à jour à partir de Sophos, saisissez le nom d'utilisateur et le mot de passe inclus dans votre licence. Si vous procédez à la mise à jour à partir d'un CID, vous pouvez indiquer soit une adresse HTTP, soit un chemin UNC, selon la manière dont vous avez paramétré le serveur de mise à jour.

14 configuration de Sophos Live Protection

Remarque : si vous configurez un ordinateur autonome connecté à un réseau, cette configuration peut être remplacée si l'ordinateur télécharge une nouvelle configuration de l'Enterprise Console ou une configuration des Fichiers supplémentaires.

Sophos Live Protection détermine si un fichier suspect est une menace et, en cas de menace, prend immédiatement les mesures spécifiées dans la configuration du nettoyage de Sophos Anti-Virus.

Sophos Live Protection améliore la détection des nouveaux malwares sans aucun risque de détection indésirable. L'opération consiste à effectuer une recherche de correspondances instantanée avec les fichiers malveillants connus les plus récents. Lorsque de nouveaux programmes malveillants sont identifiés, Sophos envoie des mises à jour en quelques secondes.

Si un contrôle antivirus sur un ordinateur d'extrémité a identifié un fichier comme suspect, mais ne peut pas l'identifier davantage comme sain ou malveillant d'après les fichiers d'identités des menaces (IDE) stockés sur l'ordinateur, certaines données de ce fichier (comme sa somme de contrôle ou d'autres attributs) sont envoyées à Sophos pour une analyse approfondie.

La vérification dans le Cloud recherche instantanément un fichier suspect dans la base de données des SophosLabs. Si le fichier est identifié comme sain ou malveillant, la décision est renvoyée à l'ordinateur et l'état du fichier est automatiquement mis à jour.

14.1 Vérification du paramètre Sophos Live Protection

Sophos Live Protection est activé par défaut si vous avez installé Sophos Anti-Virus pour la première fois. Si vous avez procédé à la mise à niveau à partir d'une version précédente de Sophos Anti-Virus, il est désactivé.

- Pour vérifier le paramètre de Sophos Live Protection, saisissez :
  `/opt/sophos-av/bin/savconfig query LiveProtection`

14.2 Activation ou désactivation de Sophos Live Protection

- Pour activer Sophos Live Protection, saisissez :

  `/opt/sophos-av/bin/savconfig set LiveProtection true`

- Pour désactiver Sophos Live Protection, saisissez :

  `/opt/sophos-av/bin/savconfig set LiveProtection false`

15 configuration du contrôle sur accès

Remarque : si vous configurez un ordinateur autonome connecté à un réseau, cette configuration peut être remplacée si l'ordinateur télécharge une nouvelle configuration de l'Enterprise Console ou une configuration des Fichiers supplémentaires.

15.1 Modification de la méthode d'interception de fichiers par contrôle sur accès

Si vous procédez à la mise à niveau vers une version du noyau Linux ne prenant pas en charge Talpa, vous pouvez utiliser Fanotify comme méthode d'interception de fichiers par contrôle sur accès.

Important : l'outil Fanotify est une fonctionnalité bêta de Sophos Anti-Virus qui n'est pas encore totalement prise en charge.

- Pour utiliser Fanotify comme méthode d'interception de fichiers par contrôle sur accès, saisissez :
  `/opt/sophos-av/bin/savconfig set DisableFanotify false`

15.2 Exclusion des fichiers et de répertoires du contrôle

Vous pouvez exclure les fichiers et répertoires du contrôle de deux manières :

- En utilisant le nom de fichier ou de répertoire
- En utilisant des caractères de remplacement

Si vous souhaitez exclure des fichiers et répertoires dont les noms ne sont pas en code UTF-8, reportez-vous à la section Spécification du codage des caractères des noms de répertoires et de fichiers à la page 37.

15.2.1 Utilisation du nom de fichier ou de répertoire

Remarque : si vous configurez un ordinateur autonome connecté à un réseau, cette configuration peut être remplacée si l'ordinateur télécharge une nouvelle configuration de l'Enterprise Console ou une configuration des Fichiers supplémentaires.

- Pour exclure un fichier ou un répertoire particulier, utilisez le paramètre **ExcludeFilePaths** avec l'opération **add**. Indiquez un répertoire à l'aide d'une barre oblique finale. Par exemple, pour ajouter le fichier `/tmp/report` à la liste des fichiers et répertoires à exclure, saisissez
  `/opt/sophos-av/bin/savconfig add ExcludeFilePaths /tmp/report`

  Pour ajouter le répertoire `/tmp/report` à la liste des fichiers et répertoires à exclure, saisissez :

  `/opt/sophos-av/bin/savconfig add ExcludeFilePaths /tmp/report/`

- Pour supprimer une exclusion de la liste, utilisez le paramètre **ExcludeFilePaths** avec l'opération **remove**. Par exemple, saisissez :

  `/opt/sophos-av/bin/savconfig remove ExcludeFilePaths /tmp/report`

15.2.2 Utilisation de caractères de remplacement

Remarque : si vous configurez un ordinateur autonome connecté à un réseau, cette configuration peut être remplacée si l'ordinateur télécharge une nouvelle configuration de l'Enterprise Console ou une configuration des Fichiers supplémentaires.

- Pour exclure des fichiers et des répertoires en utilisant des caractères de remplacement, utilisez le paramètre **ExcludeFileOnGlob** avec l'opération **add**. Les caractères de remplacement valides sont *****, qui remplace une séquence quelconque de caractères et **?** qui remplace n'importe quel caractère. Par exemple, pour ajouter tous les fichiers texte du répertoire `/tmp` à la liste des fichiers et répertoires à exclure, saisissez :
  `/opt/sophos-av/bin/savconfig add ExcludeFileOnGlob '/tmp/*.txt'`

  Remarque : si vous utilisez **ExcludeFileOnGlob** pour exclure **un répertoire**, veuillez ajouter le caractère de remplacement * à la fin du chemin. Par exemple :

  `/opt/sophos-av/bin/savconfig add ExcludeFileOnGlob '/tmp/report/*'`

- Si vous ne mettez pas l'expression entre guillemets, Linux étend cette expression et transmet la liste des fichiers à Sophos Anti-Virus. Ceci est utilisé pour exclure uniquement les fichiers qui existent déjà et pour autoriser le contrôle des fichiers créés ultérieurement. Par exemple, pour ajouter juste les fichiers texte qui existent déjà dans le répertoire `/tmp` à la liste des fichiers et des répertoires à exclure, saisissez :
  `/opt/sophos-av/bin/savconfig add ExcludeFileOnGlob /tmp/*.txt`

- Pour supprimer une exclusion de la liste, utilisez le paramètre **ExcludeFileOnGlob** avec l'opération **remove**. Par exemple, saisissez :
  `/opt/sophos-av/bin/savconfig remove ExcludeFileOnGlob '/tmp/notes.txt'`

15.2.3 Spécification du codage des caractères des noms de répertoires et de fichiers

Linux vous permet d'utiliser tout codage caractères de votre choix (par exemple, UTF-8, EUC_jp) pour nommer les répertoires et fichiers. Par contre, Sophos Anti-Virus archive uniquement les exclusions en UTF-8. Par conséquent, si vous désirez exclure du contrôle des répertoires et des fichiers dont les noms utilisent des jeux de caractères non-UTF-8, spécifiez les exclusions en UTF-8 et spécifiez les jeux de caractères à l'aide du paramètre **ExclusionEncodings**. Par la suite, les noms des répertoires ou fichiers que vous excluez sont évalués dans chacun des jeux de caractères que vous avez spécifié et tous les répertoires et fichiers qui y correspondent sont exclus. Ceci s'applique aux exclusions qui ont été spécifiées à l'aide des paramètres **ExcludeFilePaths** et **ExcludeFileOnGlob**. Par défaut, UTF-8, EUC_jp et ISO-8859-1 (Latin-1) sont spécifiés.

Par exemple, si vous désirez exclure des répertoires et fichiers dont les noms sont codés en EUC_cn, spécifiez les noms des répertoires et des fichiers en utilisant le paramètre **ExcludeFilePaths** et/ou le paramètre **ExcludeFileOnGlob**. Ensuite, ajoutez EUC_cn à la liste des jeux de caractères :

`/opt/sophos-av/bin/savconfig add ExclusionEncodings EUC_cn`

Sophos Anti-Virus évalue ensuite en UTF-8, EUC_jp, ISO-8859-1 (Latin-1) et en EUC_cn tous les noms de répertoire et de fichiers spécifiés. Il exclut ensuite tous les répertoires et fichiers dont les noms correspondent.

15.3 Exclusion d'un type de système de fichiers du contrôle

Par défaut, aucun type de système de fichiers n'est exclu.

- Pour exclure un type de système de fichiers, utilisez le paramètre **ExcludeFilesystems** avec l'opération **add**. Les types de système de fichiers valides sont répertoriés dans le fichier **/proc/filesystems**. Par exemple, pour ajouter nfs à la liste des types de système de fichiers à exclure, saisissez :
  `/opt/sophos-av/bin/savconfig add ExcludeFilesystems nfs`

- Pour supprimer une exclusion de la liste, utilisez le paramètre **ExcludeFilesystems** avec l'opération **remove**. Par exemple, saisissez :
  `/opt/sophos-av/bin/savconfig remove ExcludeFilesystems nfs`

15.4 Contrôle dans les fichiers archive

Par défaut, le contrôle sur accès dans les archives est désactivé. Par contre, vous avez la possibilité d'activer l'option si vous traitez plusieurs de ces fichiers en même temps, les conséquences de la non-détection d'un virus étant élevées. Vous pouvez, par exemple, envoyer certains fichiers archives par email à un de vos contacts.

Remarque : nous vous conseillons de ne pas activer cette option, pour les raisons suivantes :

- Le contrôle dans les archives ralentit énormément le contrôle.
- Que vous activiez cette option ou non, lorsque vous ouvrez un fichier extrait d'une archive, le fichier extrait est contrôlé.

Remarque : le moteur de détection des menaces contrôle uniquement les fichiers archivés dont la taille ne dépasse pas 8 Go (lorsqu'ils sont décompressés). En effet, il est compatible avec le format d'archive POSIX ustar qui ne prend pas en charge les fichiers de plus grande taille.

- Pour *activer* le contrôle des archives, saisissez :
  `/opt/sophos-av/bin/savconfig set ScanArchives enabled`

- Pour *désactiver* le contrôle des archives, saisissez :
  `/opt/sophos-av/bin/savconfig set ScanArchives disabled`

15.5 Nettoyage des fichiers infectés

Vous pouvez configurer le contrôle sur accès pour nettoyer (désinfecter ou supprimer) les fichiers infectés. Par défaut, le nettoyage est désactivé.

Toutes les actions que Sophos Anti-Virus prend contre les fichiers infectés sont consignées dans le journal Sophos Anti-Virus.

Remarque : vous pouvez activer la désinfection et la suppression même si nous déconseillons cette pratique. Si vous le faites, Sophos Anti-Virus essaye d'abord de désinfecter le fichier. En cas d'échec de la désinfection, il le supprime.

Remarque : Sophos Anti-Virus peut désinfecter ou supprimer les fichiers lorsqu'il les contrôle « en ouverture » (c'est-à-dire lorsque les fichiers sont copiés, déplacés ou ouverts). Il ne peut pas le faire lorsqu'il les contrôle « en fermeture » (c'est-à-dire lorsque les fichiers sont enregistrés ou créés). Ceci ne pose pas problème en conditions normales d'utilisation car le

contrôle « en ouverture » ne peut pas être désactivé de manière centralisée sur les ordinateurs Linux et procédera à la désinfection ou à la suppression des fichiers au prochain accès.

15.5.1 Désinfection des fichiers et des secteurs de démarrage infectés

- Pour *activer* la désinfection sur accès des fichiers infectés et des secteurs de démarrage, saisissez :
  `/opt/sophos-av/bin/savconfig add AutomaticAction disinfect`

  Important : Sophos Anti-Virus ne demande pas confirmation avant de procéder à la désinfection.

  Remarque : la désinfection d'un document infecté ne répare pas les modifications que le virus a apportées au document. (Retrouvez plus de renseignements sur les effets secondaires des virus à la section Informations sur le nettoyage à la page 16 du site Web de Sophos).

- Pour *désactiver* la désinfection sur accès des fichiers infectés et des secteurs de démarrage, saisissez :
  `/opt/sophos-av/bin/savconfig remove AutomaticAction disinfect`

15.5.2 Suppression des fichiers infectés

Important : utilisez cette option uniquement après avoir demandé conseil auprès du support technique de Sophos. Si le fichier infecté est une boîte aux lettres électronique, il est possible que Sophos Anti-Virus la supprime dans son intégralité.

- Pour *activer* la suppression des fichiers infectés sur accès, saisissez :
  `/opt/sophos-av/bin/savconfig add AutomaticAction delete`

  Important : Sophos Anti-Virus ne demande pas confirmation avant de supprimer.

- Pour *désactiver* la suppression des fichiers infectés sur accès, saisissez :
  `/opt/sophos-av/bin/savconfig remove AutomaticAction delete`

16 configuration des Fichiers supplémentaires

Cette section vous explique comment configurer Sophos Anti-Virus à l'aide de la configuration des Fichiers supplémentaires.

16.1 À propos de la configuration des Fichiers supplémentaires

Cette section est une présentation générale de la configuration des Fichiers supplémentaires.

16.1.1 Qu'est-ce que la configuration des Fichiers supplémentaires ?

La configuration des Fichiers supplémentaires est une méthode de configuration de Sophos Anti-Virus. Elle est une alternative à la configuration à partir de Sophos Enterprise Console et ne nécessite pas l'utilisation d'un ordinateur Windows.

Utilisez uniquement cette méthode si vous ne pouvez pas utiliser l'Enterprise Console.

Remarque : vous ne pouvez pas utiliser la configuration de l'Enterprise Console et la configuration des Fichiers supplémentaires simultanément.

Vous pouvez utiliser cette méthode pour configurer toutes les fonctions de Sophos Anti-Virus à l'exception des contrôles à la demande. Reportez-vous plutôt à la section Configuration de contrôles à la demande à la page 11 à ce sujet.

16.1.2 Comment utiliser la configuration des Fichiers supplémentaires ?

Veuillez créer un fichier contenant les paramètres de configuration des Fichiers supplémentaires. Ce fichier est hors ligne afin de permettre aux autres ordinateurs d'y accéder.

Lorsque vous êtes prêt à configurer vos ordinateurs, copiez le fichier hors ligne dans un fichier de configuration en ligne à un endroit accessible par les ordinateurs d'extrémité. Veuillez configurer chaque ordinateur client pour qu'il récupère la configuration du fichier en ligne lorsque l'ordinateur en question se met à jour.

Pour reconfigurer les ordinateurs d'extrémité, procédez à la mise à jour du fichier de configuration hors ligne et copiez-le de nouveau dans le fichier de configuration en ligne.

Remarques :

- Pour vous assurer que le fichier de configuration est sécurisé, veuillez créer et utiliser les certificats de sécurité mentionnés dans les sections suivantes.
- Vous pouvez verrouiller une partie ou l'intégralité de la configuration afin qu'elle ne puisse pas être modifiée par l'utilisateur sur son ordinateur.

Les sections suivantes vous indiquent comment créer et utiliser les fichiers de la configuration des Fichiers supplémentaires.

16.2 Utilisation de la configuration des Fichiers supplémentaires

Pour utiliser les Fichiers supplémentaires, veuillez :

- Créer les certificats de sécurité sur le serveur.
- Créer la configuration des Fichiers supplémentaires.
- Installer le certificat racine sur les ordinateurs d'extrémité.
- Activer les ordinateurs d'extrémité pour qu'ils utilisent la configuration des Fichiers supplémentaires.

16.2.1 Création des certificats de sécurité sur le serveur

Veuillez créer les certificats de sécurité de la manière suivante :

Remarque : si vous utilisez OpenSSL pour générer les certificats, vous devez exécuter OpenSSL 0.9.8 ou une version supérieure.

1. Récupérez le script que vous allez utiliser pour créer les certificats. Ce script est disponible dans l'article 119602 de la base de connaissances du support Sophos.
2. Exécutez le script pour créer une série de certificats. Par exemple, saisissez :

   ```
   ./create_certificates.sh /root/certificates
   ```

   Vous pouvez indiquer un répertoire différent dans lequel seront placés les certificats. Toutefois, assurez-vous que les certificats sont à un endroit sûr.
3. Lorsque vous y êtes invité, saisissez et confirmez un mot de passe de la clé racine.
4. Lorsque vous y êtes invité, saisissez et confirmez un mot de passe de la clé de signature.
5. Assurez-vous que les certificats sont bien dans le répertoire. Saisissez :

   ```
   ls /root/certificates/
   ```

   Vous devriez voir les fichiers suivants :

   ```
   extrafiles-root-ca.crt extrafiles-root-ca.key extrafiles-signing.cnf
   extrafiles-signing.crt extrafiles-signing.key
   ```

16.2.2 Création d'une configuration des Fichiers supplémentaires

1. Sur l'ordinateur sur lequel vous voulez stocker la configuration des Fichiers supplémentaires, utilisez la commande **savconfig** pour créer le fichier de configuration hors ligne et définissez les valeurs des paramètres dans ce fichier.

   Utilisez la syntaxe suivante :

   /opt/sophos-av/bin/savconfig -f *offline-config-file-path* **-c** *operation parameter value*

   où :

   - -f *offline-config-file-path* indique le chemin du fichier de configuration hors ligne, y compris le nom du fichier. **savconfig** crée le fichier pour vous.
   - **-c** indique que vous souhaitez accéder au niveau « Corporate » (entreprise) du fichier hors ligne (retrouvez plus d'informations sur les niveaux à la section À propos des niveaux de configuration à la page 44).
   - *operation* correspond soit à **set**, **update**, **add**, **remove** ou **delete**.
   - *parameter* correspond au paramètre que vous souhaitez définir.
   - *value* correspond à la valeur sur laquelle vous souhaitez définir le paramètre.

   Par exemple, pour créer un fichier nommé `OfflineConfig.cfg` dans le répertoire `/rootconfig` et pour désactiver les alertes par email, saisissez :

   /opt/sophos-av/bin/savconfig -f /root/config/OfflineConfig.cfg -c set EmailNotifier Disabled

   Retrouvez plus d'informations sur l'utilisation de **savconfig** à la section Commande de configuration savconfig à la page 45.

2. Pour consulter les valeurs des paramètres, utilisez l'opération **query**. Vous pouvez consulter la valeur d'un paramètre individuel ou de tous les paramètres. Par exemple, pour consulter les valeurs de tous les paramètres que vous avez définis, saisissez :
   /opt/sophos-av/bin/savconfig -f /root/config/OfflineConfig.cfg -c query

3. Lorsque vous avez fini de définir les paramètres dans le fichier de configuration hors ligne, créez un partage web ou un répertoire partagé pour le stockage du fichier de configuration en ligne.
4. Créez le fichier de configuration en ligne à l'aide de la commande **addextra**. Utilisez la syntaxe suivante :

   /opt/sophos-av/update/addextra
   offline-config-file-pathlive-config-file-path
   --signing-key=*signing-key-file-path*
   --signing-certificate=*signing-certificate-file-path*

   Par exemple :

   /opt/sophos-av/update/addextra /opt/sophos-av/OfflineConfig.cfg /var/www/extrafiles/ --signing-key= /root/certificates/extrafiles-signing.key --signing-certificate=/root/certificates/extrafiles-signing.crt

16.2.3 Installation du certificat racine sur les ordinateurs d'extrémité

Veuillez installer le certificat racine sur chaque ordinateur d'extrémité.

1. Sur l'ordinateur sur lequel vous avez créé les certificats (ou sur l'ordinateur sur lequel vous les avez copiés), créez un nouveau répertoire pour le certificat racine. Saisissez :

   ```
   mkdir rootcert
   cd rootcert/
   ```

2. Copiez le certificat racine dans le nouveau répertoire. Saisissez :

   ```
   cp /root/certificates/extrafiles-root-ca.crt .
   ```

3. Copiez le nouveau répertoire dans le répertoire partagé.
4. Rendez-vous sur chaque ordinateur d'extrémité et montez le répertoire partagé.
5. Installez le certificat. Utilisez la syntaxe suivante :

   /opt/sophos-av/update/addextra_certs --install= *shared-rootcert-directory*

   Par exemple :

   ```
   /opt/sophos-av/update/addextra_certs --install= /mnt/rootcert/
   ```

16.2.4 Activation des ordinateurs d'extrémité pour utiliser la configuration des Fichiers supplémentaires

Veuillez activer les ordinateurs d'extrémité pour qu'ils téléchargent et utilisent la configuration comme indiqué ci-dessous.

1. Si votre fichier de configuration en ligne est un répertoire partagé, montez le répertoire sur chaque ordinateur client.
2. Sur chaque ordinateur d'extrémité, indiquez le chemin du fichier de configuration en ligne. Par exemple :

   ```
   /opt/sophos-av/bin/savconfig set ExtraFilesSourcePath
   http://www.exemple.fr/extrafiles
   ```

   La nouvelle configuration est désormais prête à être téléchargée par les ordinateurs clients à leur prochaine mise à jour.

3. Pour déclencher une mise à jour, saisissez :

   ```
   /opt/sophos-av/bin/savupdate
   ```

16.3 Mise à jour de la configuration des Fichiers supplémentaires

1. Sur l'ordinateur sur lequel la configuration des Fichiers supplémentaires est stockée, utilisez la commande **savconfig** pour mettre à jour le fichier de configuration hors ligne et définir les valeurs des paramètres dans ce fichier.

   Vous pouvez utiliser la même syntaxe que celle vous ayant servi à créer le fichier de configuration hors ligne.

   Par exemple, pour mettre à jour un fichier appelé `OfflineConfig.cfg` dans le répertoire `/opt/sophos-av` et pour activer les alertes par email, saisissez :

   ```
   /opt/sophos-av/bin/savconfig -f /opt/sophos-av/OfflineConfig.cfg
   -c set EmailNotifier Enabled
   ```

2. Pour consulter les valeurs des paramètres, utilisez l'opération **query**. Vous pouvez consulter la valeur d'un paramètre individuel ou de tous les paramètres. Par exemple, pour consulter les valeurs de tous les paramètres que vous avez définis, saisissez :
   ```
   /opt/sophos-av/bin/savconfig -f /opt/sophos-av/OfflineConfig.cfg
   -c query
   ```

3. Lorsque vous avez terminé de définir les paramètres dans le fichier de configuration hors ligne, mettez à jour le fichier de configuration en ligne à l'aide de la commande **addextra**. Utilisez la syntaxe suivante :

   ```
   /opt/sophos-av/update/addextra
   offline-config-file-pathlive-config-file-path
   --signing-key=signing-key-file-path
   --signing-certificate=signing-certificate-file-path
   ```

   Par exemple :

   ```
   /opt/sophos-av/update/addextra /opt/sophos-av/OfflineConfig.cfg
   /var/www/extrafiles/ --signing-key=
   /root/certificates/extrafiles-signing.key
   --signing-certificate=/root/certificates/extrafiles-signing.crt
   ```

   La configuration mise à jour est désormais prête à être téléchargée par les ordinateurs clients à leur prochaine mise à jour.

4. Pour déclencher une mise à jour, saisissez :

   ```
   /opt/sophos-av/bin/savupdate
   ```

16.4 À propos des niveaux de configuration

Chaque installation de Sophos Anti-Virus inclut un fichier de configuration local comprenant les paramètres de toutes les fonctions de Sophos Anti-Virus à l'exception des contrôles à la demande.

Chaque fichier de configuration local contient un nombre de niveaux :

- Sophos : ce niveau est toujours présent dans le fichier. Il inclut les paramètres par défaut de l'éditeur qui sont uniquement modifiés par Sophos.
- Corporate : ce niveau est présent si l'installation est configurée à l'aide de la configuration des Fichiers supplémentaires.

- User : ce niveau est présent en cas de mise en place d'une configuration locale. Il inclut des réglages s'appliquant uniquement à l'installation sur cet ordinateur.

Chaque niveau utilise les mêmes paramètres afin de pouvoir régler le même paramètre sur plusieurs niveaux. Toutefois, lorsque Sophos Anti-Virus vérifie la valeur d'un paramètre, il procède en fonction de la hiérarchie du niveau :

- Par défaut, le niveau « Corporate » est prioritaire sur le niveau « User ».
- Les niveaux « Corporate » et « User » sont prioritaires sur le niveau Sophos.

Par exemple, si un paramètre est défini au niveau « User » et au niveau « Corporate », c'est la valeur du niveau « Corporate » qui est utilisée. Néanmoins, vous pouvez déverrouiller les valeurs des paramètres individuels du niveau « Corporate » afin qu'ils puissent être remplacés.

Lorsque le fichier de configuration local est mis à jour depuis le fichier de configuration des Fichiers supplémentaires, le niveau « Corporate » du fichier local est remplacé par celui du fichier de configuration des Fichiers supplémentaires.

16.5 Commande de configuration savconfig

`savconfig` est la commande que vous utilisez pour configurer toutes les fonctions de Sophos Anti-Virus à l'exception du contrôle à la demande. Le chemin de la commande est `/opt/sophos-av/bin`. Retrouvez plus d'instructions sur l'utilisation de cette commande pour configurer des fonctions spécifiques de Sophos Anti-Virus ci-après dans le présent guide. Le reste de cette sous-section aborde la syntaxe à utiliser.

La syntaxe de **`savconfig`** est :

`savconfig [`*`option`***`] ... [`***`operation`***`] [`***`parameter`***`] [`***`value`***`] ...`**

Pour voir une liste complète des options, opérations et paramètres, saisissez :

```
man savconfig
```

16.5.1 *Option*

Vous pouvez indiquer une ou plusieurs options. Ces options sont principalement associées aux *niveaux* des fichiers de configuration locale de chaque installation. Par défaut, la commande accède au niveau « User » (utilisateur). Si vous désirez accéder au niveau « Corporate » (entreprise), par exemple, utilisez l'option **-c** ou **--corporate**.

Par défaut, les valeurs des paramètres au niveau « Corporate » sont verrouillés, afin d'être prioritaires sur les valeurs du niveau « User ». Si vous désirez autoriser que les paramètres utilisateurs soient prioritaires sur ceux de l'entreprise, utilisez l'option **--nolock**. Par exemple, pour paramétrer la valeur de **LogMaxSizeMB** et pour autoriser des valeurs prioritaires sur celle-ci, saisissez :

```
/opt/sophos-av/bin/savconfig --nolock -f corpconfig.cfg -c
LogMaxSizeMB 50
```

Si vous utilisez l'Enterprise Console, vous pouvez afficher uniquement les valeurs des paramètres de la stratégie antivirus en utilisant l'option **--consoleav**. Saisissez :

```
/opt/sophos-av/bin/savconfig --consoleav query
```

Vous pouvez afficher uniquement les valeurs de la stratégie de mise à jour de l'Enterprise Console en utilisant l'option **--consoleupdate**. Saisissez :

```
/opt/sophos-av/bin/savconfig --consoleupdate query
```

16.5.2 *Opération*

Vous pouvez indiquer une seule opération. Les opérations sont principalement associées à la manière dont vous souhaitez accéder à un paramètre. Certains paramètres peuvent uniquement avoir une seule valeur tandis que d'autres peuvent avoir une liste de valeurs. Ces opérations vous permettent d'ajouter des valeurs à une liste ou de les supprimer. Par exemple, la paramètre **Email** correspond à une *liste* de destinataires de messagerie.

Pour afficher les valeurs des paramètres, veuillez utiliser l'opération **query**. Par exemple, pour afficher la valeur du paramètre **EmailNotifier**, saisissez :

```
/opt/sophos-av/bin/savconfig query EmailNotifier
```

Si vous utilisez l'Enterprise Console, lorsque **savconfig** renvoie les valeurs des paramètres, ceux qui sont en conflit avec la stratégie définie dans l'Enterprise Console sont clairement identifiés par le terme « Conflict ».

16.5.3 *Paramètre*

Vous pouvez indiquer un seul paramètre. Pour répertorier tous les paramètres de base qui peuvent être définis, saisissez :

```
/opt/sophos-av/bin/savconfig -v
```

Certains paramètres nécessitent également la spécification de paramètres secondaires.

16.5.4 *Valeur*

Vous pouvez indiquer une ou plusieurs valeurs à affecter à un paramètre. Si une valeur contient des espaces, mettez-la entre guillemets simples.

17 Résolution des problèmes

Cette section décrit comment gérer les problèmes pouvant survenir lors de l'utilisation de Sophos Anti-Virus.

Retrouvez plus de renseignements sur les codes d'erreur de Sophos Anti-Virus concernant les contrôles à la demande à l'Annexe : codes de retour du contrôle à la demande à la page 53.

17.1 Impossible d'exécuter une commande

Symptôme

Votre ordinateur ne vous autorise pas à exécuter une commande Sophos Anti-Virus.

Cause

Vous ne disposez probablement pas des droits suffisants.

Résolution du problème

Ouvrez une session administrateur (root) sur l'ordinateur.

17.2 La configuration des exclusions n'a pas été appliquée

Symptôme

Parfois, lorsque vous configurez Sophos Anti-Virus pour inclure au contrôle sur accès des fichiers qui étaient auparavant exclus, ces fichiers demeurent exclus.

Cause

Il est possible que ce soit parce que la mémoire cache des fichiers qui ont été préalablement contrôlés inclut toujours les fichiers qui étaient préalablement exclus.

Résolution du problème

En fonction de la méthode d'interception du contrôle sur accès que vous utilisez, procédez ainsi :

- Si vous utilisez Talpa, essayez d'effacer la mémoire cache. Pour ce faire, saisissez :

  ```
  echo 'disable' > /proc/sys/talpa/intercept-filters/Cache/status
  echo 'enable' > /proc/sys/talpa/intercept-filters/Cache/status
  ```

- Si vous utilisez Fanotify, essayez de redémarrer le service installé sav-protect. Pour ce faire, saisissez :

  `/etc/init.d/sav-protect restart`

17.3 L'ordinateur signale « Aucune entrée de manuel pour ... »

Symptôme

Lorsque vous essayez de consulter une page de man de Sophos Anti-Virus, l'ordinateur affiche un message semblable à `Aucune entrée de manuel pour ...`.

Cause

La variable d'environnement MANPATH n'inclut probablement pas le chemin vers la page de man.

Résolution du problème

1. Si vous exécutez le shell sh, ksh ou bash, ouvrez `/etc/profile` pour procéder à une modification.

   Si vous exécutez le shell csh, tcsh, ouvrez `/etc/login` pour procéder à une modification.

   Remarque : si vous ne disposez pas d'un script ou d'un profil de connexion, effectuez les étapes suivantes à l'invite de commande. Procédez de cette façon à chaque fois que vous redémarrez votre ordinateur.

2. Assurez-vous que la variable d'environnement MANPATH inclut le répertoire `/usr/local/man`.

3. Si MANPATH n'inclut pas ce répertoire, ajoutez-le de la manière suivante : ne modifiez pas les paramètres existants.

   Si vous exécutez le shell sh, ksh ou bash, saisissez :

   `MANPATH=$MANPATH:/usr/local/man`

   `export MANPATH`

   Si vous exécutez le shell csh ou tcsh, saisissez :

   `setenv MANPATH` *`values`***`:/usr/local/man`**

   où *values* correspond aux paramètres existants.

4. Sauvegardez votre script ou votre profil de connexion.

17.4 Espace disque insuffisant

Symptôme

Sophos Anti-Virus n'a plus assez d'espace disque disponible lorsqu'il contrôle des fichiers archives complexes.

Causes

Ce problème pourrait être dû à l'une des raisons suivantes :

- Lorsqu'il décompresse des fichiers archives, Sophos Anti-Virus utilise le répertoire `/tmp` pour stocker les résultats de ses opérations. Si ce répertoire n'est pas assez grand, il se peut que Sophos Anti-Virus n'ait plus assez d'espace disque disponible.
- Sophos Anti-Virus a dépassé le quota fixé à l'utilisateur.

Résolution du problème

Procédez de l'une des manières suivantes :

- Augmentez la taille du répertoire `/tmp`.
- Augmentez le quota fixé à l'utilisateur.
- Modifiez le répertoire qu'utilise Sophos Anti-Virus pour stocker les résultats de ses opérations. Vous pouvez effectuer cette modification en paramétrant la variable d'environnement SAV_TMP.

17.5 Le contrôle à la demande s'exécute au ralenti

Ce problème survient pour l'une des raisons suivantes :

Symptôme

Sophos Anti-Virus prend beaucoup plus de temps pour effectuer le contrôle à la demande.

Causes

Ce problème pourrait être dû à l'une des raisons suivantes :

- Par défaut, Sophos Anti-Virus effectue un contrôle rapide des parties de fichiers susceptibles de contenir des virus. Si le contrôle est paramétré sur intégral (à l'aide de l'option **-f**), il contrôle l'intégralité du fichier.
- Par défaut, Sophos Anti-Virus contrôle uniquement les types de fichier particuliers. S'il est configuré pour vérifier *tous* les types de fichiers, la procédure dure plus longtemps.

Résolution du problème

Procédez de l'une des manières suivantes :

- Évitez d'utiliser le contrôle intégral sauf avis contraire du support technique de Sophos par exemple.
- Pour contrôler les fichiers portant des extensions spécifiques, ajoutez ces extensions à la liste des types de fichier que Sophos Anti-Virus contrôle par défaut. Retrouvez plus de renseignements à la section Contrôle d'un type de fichier particulier à la page 11.

17.6 Le programme d'archivage sauvegarde tous les fichiers qui ont été contrôlés à la demande

Symptôme

Il se peut que votre programme d'archivage sauvegarde constamment tous les fichiers que Sophos Anti-Virus a contrôlé à la demande.

Cause

Ceci peut être dû aux modifications que Sophos Anti-Virus apporte à la date de « statut modifié » des fichiers. Par défaut, Sophos Anti-Virus tente de réinitialiser le temps d'accès (**atime**) des fichiers sur le temps affiché avant le début du contrôle. Toutefois, ceci entraîne la modification de la date d'état modifié (**ctime**) de l'inode. Si votre programme d'archivage utilise le **ctime** pour décider si un fichier a changé, il sauvegarde tous les fichiers contrôlés par Sophos Anti-Virus.

Résolution du problème

Exécutez **savscan** avec l'option **--no-reset-atime**.

17.7 Virus non nettoyé

Symptômes

- Sophos Anti-Virus n'a pas essayé de nettoyer un virus.
- Sophos Anti-Virus affiche le message `Disinfection failed`.

Causes

Ce problème pourrait être dû à l'une des raisons suivantes :

- Le nettoyage automatique n'a pas été activé.
- Sophos Anti-Virus ne peut pas désinfecter ce type de virus.

- Le fichier infecté est sur un support amovible, par exemple, une disquette ou un CD-ROM, protégé en écriture.
- Le fichier infecté est sur un système de fichiers NTFS.
- Sophos Anti-Virus ne nettoie pas un fragment de virus car il n'a pas trouvé une correspondance exacte dans la base de données sur les virus.

Résolution du problème

Procédez de l'une des manières suivantes :

- Activez le nettoyage automatique.
- Si possible, autorisez l'écriture sur le support amovible.
- Favorisez le traitement des fichiers sur le système de fichiers NTFS sur un ordinateur local.

17.8 Fragment de virus signalé

Symptôme

Sophos Anti-Virus signale qu'il a détecté un fragment de virus.

Causes

Ceci indique qu'une partie du fichier correspond à une partie d'un virus. Ceci se produit pour l'une des raisons suivantes :

- De nombreux virus sont basés sur des virus existants. Par conséquent, les fragments de code classiques d'un virus connu peuvent apparaître dans des fichiers qui sont infectés par un nouveau.
- Les programmes de duplication de la majorité des virus contiennent des bogues qui provoquent une infection incorrecte des fichiers cibles. Une partie inactive du virus (il peut s'agir d'une partie conséquente), qui apparaît dans le fichier hôte, est détectée par Sophos Anti-Virus.
- Lors de l'exécution d'un contrôle intégral, Sophos Anti-Virus peut signaler qu'il y a un fragment de virus/spyware dans un fichier de base de données.

Résolution du problème

1. Procédez à la mise à jour de Sophos Anti-Virus sur l'ordinateur affecté afin qu'il dispose des données sur les virus les plus récentes.
2. Essayez de désinfecter le fichier (voir la section Désinfection d'un fichier infecté spécifique à la page 17).
3. Si des fragments de virus sont toujours signalés, veuillez prendre conseil auprès du support technique Sophos.

17.9 Accès au disque impossible

Symptôme

Vous ne parvenez pas à accéder aux fichiers sur une disque amovible.

Cause

Par défaut, Sophos Anti-Virus empêche l'accès aux disques amovibles dont les secteurs de démarrage sont infectés.

Résolution du problème

Pour autoriser l'accès (par exemple, pour copier des fichiers depuis une disquette infectée par un virus de secteur de démarrage) :

1. Saisissez :

   ```
   /opt/sophos-av/bin/savconfig set AllowIfBootSectorThreat enabled
   ```

2. Une fois que vous avez fini d'accéder au disque, saisissez :

   ```
   /opt/sophos-av/bin/savconfig set AllowIfBootSectorThreat disabled
   ```

3. Retirez le disque de l'ordinateur pour qu'il ne tente pas de réinfecter l'ordinateur au redémarrage.

18 Annexe : codes de retour du contrôle à la demande

savscan retourne un code d'erreur au shell qui indique le résultat du contrôle. Vous pouvez voir le code en saisissant une commande supplémentaire à la fin du contrôle, par exemple :

echo $?

Code de retour	Description
0	Aucune erreur n'est survenue et aucun virus n'a été détecté
1	L'utilisateur interrompt le contrôle en appuyant sur CTRL+C
2	Une erreur empêche l'exécution du contrôle de se poursuivre
3	Un virus a été détecté

18.1 Codes de retour étendus

savscan renvoie un code plus détaillé au shell si vous l'exécutez avec l'option **-eec**. Vous pouvez voir le code en saisissant une commande supplémentaire à la fin du contrôle, par exemple :

echo $?

Code de retour étendu	Description
0	Aucune erreur n'est survenue et aucun virus n'a été détecté
8	Une erreur non fatale est survenue
16	Un fichier protégé par mot de passe a été découvert (il n'a pas été contrôlé)

Code de retour étendu	Description
20	Un élément contenant un virus a été détecté et désinfecté
24	Un élément contenant un virus a été découvert et désinfecté
28	Un virus a été détecté dans la mémoire
32	La vérification de l'intégrité a échoué
36	Une erreur fatale est survenue
40	Le contrôle a été interrompu

19 Annexe : configuration de la fonction « phone-home »

Sophos Anti-Virus peut contacter Sophos pour nous envoyer des informations sur les produits et les plates-formes. Cette fonction « phone-home » nous aide à améliorer nos produits et la satisfaction de nos utilisateurs.

Lorsque vous utilisez Sophos Anti-Virus, la fonction « phone-home » est activée par défaut. Nous vous serions reconnaissant de la laisser activée. Ceci n'a aucun impact sur votre sécurité ou sur les performances de votre ordinateur :

- Vos données sont chiffrées puis envoyées vers un emplacement sécurisé dans lequel nous les conservons pendant trois mois au maximum.
- Le produit envoie uniquement environ 2 Ko de données une fois par semaine. Il établit le contact à intervalles choisis aléatoirement afin d'éviter que plusieurs ordinateurs se connectent en même temps.

Vous avez la possibilité de désactiver cette fonction à tout moment après l'installation.

Pour désactiver la fonction « phone-home », saisissez :

```
/opt/sophos-av/bin/savconfig set DisableFeedback true
```

Pour réactiver la fonction « phone-home », saisissez :

```
/opt/sophos-av/bin/savconfig set DisableFeedback false
```

20 Annexe : configuration du redémarrage pour RMS

Si RMS (Remote Management System), qui gère les communications avec le serveur, tombe en panne ou ne démarre pas correctement, un adaptateur redémarre les composants RMS, mrouter et magent.

Si vous souhaitez redémarrer RMS régulièrement, veuillez ajouter

`RestartIntervalHours=<Heures>`

à $INST/etc/sophosmgmtd.conf.

21 Glossaire

Client de mise à jour	Un ordinateur sur lequel vous avez installé Sophos Anti-Virus et qui n'a pas besoin de servir de source de mise à jour aux autres ordinateurs.
Contrôle planifié	Contrôle de l'ordinateur ou de certaines parties de ce dernier, qui s'exécute à des heures définies.
Contrôle sur accès	Votre méthode principale de protection contre les virus. À chaque fois que vous accédez (copiez, enregistrez, déplacez, ou ouvrez) un fichier, Sophos Anti-Virus contrôle le fichier et lui accorde l'accès uniquement s'il ne représente aucune menace pour votre ordinateur.
Contrôle à la demande	Contrôle que vous lancez. Vous pouvez utiliser un contrôle à la demande pour tout contrôler, que ce soit un fichier unique ou tout fichier de votre ordinateur sur lesquels vous avez les droits de lecture.
Désinfection	Désinfection signifie la suppression d'un virus dans un fichier ou un secteur de démarrage.
Extra Files (Fichiers supplémentaires)	Un emplacement utilisé pour archiver la configuration de Sophos Anti-Virus pour un réseau. Lorsque les ordinateurs se mettent à jour, ils téléchargent la configuration à partir de cet emplacement.
Répertoire d'installation centralisée (CID)	Répertoire dans lequel les logiciels et les mises à jour Sophos sont placés. Les ordinateurs en réseau se mettent à jour depuis ce répertoire.
Serveur de mise à jour	Un ordinateur sur lequel vous avez installé Sophos Anti-Virus et qui sert aussi de source de mise à jour aux autres ordinateurs. Ces autres ordinateurs sont soit des serveurs de mise à jour, soit des ordinateurs d'extrémité de mise à jour, selon la manière dont vous déployez Sophos Anti-Virus sur le réseau.
Sophos Live Protection	Fonction qui utilise la technologie dans le Cloud pour décider instantanément si un fichier suspect est une menace et prendre les mesures spécifiées dans la configuration du nettoyage de Sophos Anti-Virus.
Source de mise à jour principale	L'emplacement des mises à jour auquel accède habituellement l'ordinateur. Des codes d'accès pourraient être nécessaires.

Source de mise à jour secondaire	L'emplacement des mises à jour auquel accède l'ordinateur en cas d'indisponibilité de la source de mise à jour principale. Des codes d'accès pourraient être nécessaires.
Virus	Programme informatique qui se copie lui-même. Souvent, les virus perturbent les systèmes informatiques ou endommagent les données figurant sur ces systèmes. Un virus a besoin d'un programme hôte et n'infecte pas d'ordinateur tant qu'il n'a pas été exécuté. Certains virus se propagent via les réseaux en effectuant des copies d'eux-mêmes ou peuvent se transférer automatiquement par courriel. Le terme "virus" est aussi souvent utilisé pour désigner des virus, des vers et des chevaux de Troie.
Virus de secteur de démarrage	Un type de virus qui détruit les étapes initiales du processus de démarrage. Le virus de secteur de démarrage s'attaque soit au secteur de démarrage maître, soit au secteur de démarrage DOS.

22 Support technique

Vous bénéficiez du support technique des produits Sophos de l'une des manières suivantes :

- Rendez-vous sur le forum Sophos Community en anglais sur community.sophos.com/ et recherchez d'autres utilisateurs rencontrant le même problème que le vôtre.
- Rendez-vous sur la base de connaissances du support de Sophos sur www.sophos.com/fr-fr/support.aspx.
- Téléchargez la documentation des produits sur www.sophos.com/fr-fr/support/documentation.aspx.
- Ouvrez un incident support sur https://secure2.sophos.com/fr-fr/support/contact-support/support-query.aspx.

23 Mentions légales

ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™

correction, modification, or enhancement. A number of companies around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant. Likewise, DOC software is compliant with the new US daylight savings rule passed by Congress as "The Energy Policy Act of 2005," which established new daylight savings times (DST) rules for the United States that expand DST as of March 2007. Since DOC software obtains time/date and calendaring information from operating systems users will not be affected by the new DST rules as long as they upgrade their operating systems accordingly.

The names ACE™, TAO™, CIAO™, DAnCE™, CoSMIC™, Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. This license grants no permission to call products or services derived from this source ACE™, TAO™, CIAO™, DAnCE™, or CoSMIC™, nor does it grant permission for the name Washington University, UC Irvine, or Vanderbilt University to appear in their names.

If you have any suggestions, additions, comments, or questions, please let me know.

Douglas C. Schmidt

GNU General Public License

Certains programmes logiciels sont concédés en licence (ou en sous licence) à l'utilisateur selon les termes de la licence GNU General Public License (GPL) ou de licences pour logiciels libres similaires qui, entre autres droits, permettent à l'utilisateur de copier, modifier et redistribuer certains programs, ou parties de programmes et d'avoir accès au code source. La licence GPL exige que pour tout logiciel concédé en licence sous la licence GPL, qui est distribuée à un utilisateur sous un format binaire exécutable, le code source soit aussi mis à disposition de ces utilisateurs. Pour tout logiciel de ce type distribué avec un produit Sophos, le code source est mis à disposition en envoyant une demande à Sophos par email à savlinuxgpl@sophos.com. Une copie des termes de GPL est disponible sur www.gnu.org/copyleft/gpl.html

libmagic – file type detection

Copyright © Ian F. Darwin 1986, 1987, 1989, 1990, 1991, 1992, 1994, 1995.

Software written by Ian F. Darwin and others; maintained 1994–2004 Christos Zoulas.

This software is not subject to any export provision of the United States Department of Commerce, and may be exported to any country or planet.

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 immediately at the beginning of the file, without modification, 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.

Medusa web server

Medusa was once distributed under a 'free for non-commercial use' license, but in May of 2000 Sam Rushing changed the license to be identical to the standard Python license at the time. The standard Python license has always applied to the core components of Medusa, this change just frees up the rest of the system, including the http server, ftp server, utilities, etc. Medusa is therefore under the following license:

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 Sam Rushing not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

SAM RUSHING DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL SAM RUSHING BE LIABLE FOR 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 THIS SOFTWARE.

Sam would like to take this opportunity to thank all of the folks who supported Medusa over the years by purchasing commercial licenses.

OpenSSL Cryptography and SSL/TLS Toolkit

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL license

Copyright © 1998-2016 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 © 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 Netscape’s SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered 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 routines 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 license 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 license [including the GNU Public License.]

Protocol Buffers (libprotobuf)

Copyright 2008, Google 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:

- 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 Google Inc. 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.

Code generated by the Protocol Buffer compiler is owned by the owner of the input file used when generating it. This code is not standalone and requires a support library to be linked with it. This support library is itself covered by the above license.

pycrypto

Distribute and use freely; there are no restrictions on further dissemination and usage except those imposed by the laws of your country of residence. This software is provided "as is"

without warranty of fitness for use or suitability for any purpose, express or implied. Use at your own risk or not at all.

Incorporating the code into commercial products is permitted; you do not have to make source available or contribute your changes back (though that would be nice).

– –amk (www.amk.ca)

Python

PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2

1. This LICENSE AGREEMENT is between the Python Software Foundation (“PSF”), and the Individual or Organization (“Licensee”) accessing and otherwise using this software (“Python”) in source or binary form and its associated documentation.
2. Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, worldwide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python alone or in any derivative version, provided, however, that PSF’s License Agreement and PSF’s notice of copyright, i.e., “Copyright © 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009 Python Software Foundation; All Rights Reserved” are retained in Python alone or in any derivative version prepared by Licensee.
3. In the event Licensee prepares a derivative work that is based on or incorporates Python or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python.
4. PSF is making Python available to Licensee on an “AS IS” basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.
5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.
6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.
7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.
8. By copying, installing or otherwise using Python, Licensee agrees to be bound by the terms and conditions of this License Agreement.

TinyXML XML parser

www.sourceforge.net/projects/tinyxml

Original code by Lee Thomason (www.grinninglizard.com)

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.

zlib data compression library

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 jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

20161125

Index

A

accès aux disques 52
alertes 14, 26–27
    email 27
    fenêtre instantanée de bureau 14, 26
    ligne de commande 14, 27
alertes de fenêtre instantanée de bureau 14, 26
alertes de ligne de commande 14
alertes par email 27
alertes par ligne de commande 27
analyses des virus 16
archives 11–12
    contrôles à la demande 11–12
Aucune entrée de manuel pour ... 48

C

codage de caractères 37
codes d'erreur 53
codes de retour 53
configuration de Sophos Anti-Virus 6
contrôle sur accès 8, 36
    exclusion d'éléments 36
    Fanotify 36
contrôles à la demande 10–13, 22
    archives 11–12
    contrôles planifiés 22
    éléments avec des liens symboliques 12
    exclusion d'éléments 13
    exécutables UNIX 13
    fichiers 10
    ordinateur 10
    ordinateurs distants 12
    répertoires 10
    secteurs de démarrage 10
    systèmes de fichiers 10, 12
    types de fichier 11, 13
contrôles planifiés 22

D

désinfection 17–18
    fichiers infectés 17
    secteurs de démarrage 18
disques, accès 52

E

effets secondaires des virus 18
éléments avec des liens symboliques, contrôles à la demande 12
Enterprise Console 6
espace disque insuffisant 49
exclusion d'éléments 13, 36–37
    codage de caractères 37
    contrôle sur accès 36
exclusion d'éléments *(suite)*
    contrôles à la demande 13
exécutables UNIX, contrôles à la demande 13

F

fichiers infectés 16–18, 38
    désinfection 17
    mise en quarantaine 16
    nettoyage 17, 38
    suppression 18
fichiers, contrôles à la demande 10
fragment signalé, virus 51

I

informations sur le nettoyage 16

J

journal de Sophos Anti-Virus 30
    configuration 30
journal, Sophos Anti-Virus 30
    configuration 30

L

lenteur des contrôles à la demande 49

M

mise à jour 20–21, 31
    configuration 31
    immédiate 20
    prise en charge des nouveaux noyaux 21
    prise en charge des noyaux personnalisés 21
mise en quarantaine des fichiers infectés 16

N

nettoyage des fichiers infectés 17, 38
niveaux, dans le fichier de configuration 44
noyaux 21
    nouvelles versions 21
    personnalisé 21
noyaux personnalisés 21

O

ordinateur, contrôles à la demande 10
ordinateurs distants, contrôles à la demande 12

P

page de man introuvable 48

R

répertoires, contrôles à la demande 10

S

sauvegardes des fichiers contrôlés 50
savconfig 45
savsetup 31
secteurs de démarrage 10, 18, 52
    contrôles à la demande 10
    désinfection 18
    infecté 52
secteurs de démarrage infectés 52
Sophos Live Protection 35
suppression des fichiers infectés 18
systèmes de fichiers, contrôles à la demande 10, 12

T

types de fichier, contrôles à la demande 11, 13

V

virus 14, 16, 18, 29, 50–51
    analyses 16
    détecté 14, 29
    effets secondaires 18
    fragment signalé 51
    non nettoyé 50