

SOPHOS

Sophos Anti-Virus pour UNIX Manuel utilisateur

Version du produit : 7

Date du document : janvier 2011



Table des matières

1	À propos de ce manuel.....	3
2	À propos de Sophos Anti-Virus pour UNIX	4
3	Contrôle à la demande.....	6
4	Que se passe-t-il en cas de détection de virus.....	10
5	Nettoyage de virus.....	11
6	Consultation du journal de Sophos Anti-Virus	14
7	Mise à jour immédiate de Sophos Anti-Virus	15
8	Annexe A : codes de retour du contrôle à la demande.....	16
9	Annexe B : à propos de la configuration à partir d'un CID.....	18
10	Annexe C : configuration des contrôles planifiés.....	23
11	Annexe D : configuration des alertes par courriel.....	27
12	Annexe E : configuration de la journalisation.....	29
13	Annexe F : configuration de la mise à jour.....	30
14	Résolution des problèmes.....	33
15	Glossaire.....	37
16	Support technique.....	39
17	Mentions légales.....	40

1 À propos de ce manuel

Ce manuel vous indique comment utiliser et configurer Sophos Anti-Virus pour UNIX.

Dans ce manuel, on suppose que vous installez et mettez à jour Sophos Anti-Virus depuis un dossier partagé créé par la Sophos Enterprise Console.

Pour *installer* Sophos Anti-Virus, consultez le *Guide de démarrage de Sophos Endpoint Security and Control pour Linux, NetWare et UNIX*.

La documentation Sophos est disponible sur www.sophos.fr/support/docs/.

2 À propos de Sophos Anti-Virus pour UNIX

2.1 Ce 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 UNIX. En plus de détecter tous les virus UNIX, il parvient aussi à détecter tous les virus non-UNIX qui peuvent être stockés sur votre ordinateur UNIX et transférés sur les ordinateurs non-UNIX. Il exécute cette opération en contrôlant votre ordinateur.

2.2 Comment Sophos Anti-Virus protège votre ordinateur

Sophos Anti-Virus vous permet d'exécuter un *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 de lecture. Vous pouvez soit exécuter manuellement un contrôle à la demande, soit le planifier pour qu'il s'exécute tout seul.

2.3 Comment utiliser Sophos Anti-Virus

Sophos Anti-Virus dispose d'une interface de ligne de commande. Celle-ci vous permet d'accéder à toutes les fonctionnalités de Sophos Anti-Virus et de procéder à toutes les configurations de votre choix.

Remarque : vous devez impérativement 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.

Dans ce manuel, on 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

Si vos ordinateurs UNIX sont administrés par la Sophos Enterprise Console, configurez Sophos Anti-Virus comme suit :

- Configurez les **contrôles planifiés, les alertes, la journalisation et la mise à jour** de manière centralisée depuis l'Enterprise Console. Pour plus d'informations, reportez-vous à l'aide de l'Enterprise Console.

Remarque : ces fonctions incluent également certains paramètres qui ne peuvent pas être définis à l'aide de l'Enterprise Console. Vous pouvez définir ces paramètres localement sur chaque ordinateur UNIX à partir de l'interface de ligne de commande de Sophos Anti-Virus. L'Enterprise Console les ignore.

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

Si vous avez un réseau d'ordinateurs UNIX *non* administrés par l'Enterprise Console, configurez Sophos Anti-Virus ainsi :

- Configurez de manière centralisée les **contrôles planifiés, les alertes, la journalisation et la mise à jour** en modifiant un fichier de configuration dans le répertoire d'installation centralisée (CID, Central Installation Directory) à partir duquel les ordinateurs se mettent à jour. Ceci s'appelle une configuration à partir d'un CID.
- Configurez les **contrôles à la demande** localement sur chaque ordinateur UNIX à partir de l'interface de ligne de commande de Sophos Anti-Virus.

Remarque : n'utilisez pas la configuration à partir d'un CID à moins que le support technique vous ait conseillé de le faire, ou si vous ne pouvez utiliser l'Enterprise Console. Vous ne pouvez pas utiliser ensemble la configuration de l'Enterprise Console et celle à partir d'un CID.

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

3 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 de lecture. Vous pouvez soit exécuter manuellement un contrôle à la demande, soit le planifier pour qu'il s'exécute tout seul.

Pour planifier un contrôle à la demande, reportez-vous à l'[Annexe C : configuration des contrôles planifiés](#) à la page 23.

3.1 Exécution des contrôles à la demande

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

3.1.1 Contrôle de l'ordinateur

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

Remarque : vous pouvez aussi utiliser la Sophos Enterprise Console pour lancer un contrôle intégral d'un ou de plusieurs ordinateurs. Pour plus de détails, reportez-vous à l'aide de l'Enterprise Console.

3.1.2 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/monrépertoire/monfichier

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

3.1.3 Contrôle d'un système de fichiers

- ❖ Pour contrôler un système de fichiers, précisez son nom. Par exemple, saisissez :
savscan /home

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

3.2 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

3.2.1 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.

3.2.2 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 de fichier 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 spécifier plusieurs types de fichier, séparez chaque extension de fichier par une virgule.

3.2.3 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**.

- ❖ 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.

3.2.4 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**.

- ❖ 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.

3.2.5 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

3.2.6 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**.

3.2.7 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

3.2.8 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 /home/fred -exclude /home/fred/games

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

3.2.9 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**.

4 Que se passe-t-il en cas de détection de virus

Si un contrôle à la demande détecte un virus, par défaut, Sophos Anti-Virus :

- Consigne l'événement dans syslog et le journal Sophos Anti-Virus (reportez-vous à la section [Consultation du journal de Sophos Anti-Virus](#) à la page 14).
- Envoie une alerte à l'Enterprise Console s'il est administré par l'Enterprise Console.
- Envoie une alerte par courriel à root@localhost.
- 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 4.50.0
[Solaris/SPARC] Version des données virales 4.50, février
2010 Inclut la détection de 1375239 virus, chevaux de Troie
et vers Copyright (c) 1989-2010 Sophos Group. All rights
reserved. Heure système 13:43:32, Date système 02 mars 2010
Répertoire IDE est : /opt/sophos-av/lib/sav Utilisation IDE
du fichier 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.fr ou envoyez un courrier électronique à
support@sophos.fr
Fin de contrôle.
```

Pour de plus amples informations sur le nettoyage des ordinateurs de tout virus, reportez-vous à la section [Nettoyage de virus](#) à la page 11.

5 Nettoyage de virus

5.1 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 (www.sophos.fr/security/analyses).
2. Recherchez l'analyse de virus en utilisant le nom indiqué par Sophos Anti-Virus.

5.2 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 optez pour la désinfection (reportez-vous à la section [Nettoyage des fichiers infectés](#) à la page 12) ainsi que pour la 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.

5.2.1 Définition de la mise en quarantaine

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

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

Par défaut, Sophos Anti-Virus modifie :

- 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=nom utilisateur
gid=nnn
```

```
group=nom-groupe  
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 une **uid** et un **utilisateur**.

Pour chaque paramètre non défini par vos soins, c'est le paramétrage 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.

5.3 Nettoyage des fichiers infectés

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

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

5.3.1 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 (reportez-vous à la section [Informations sur le nettoyage](#) à la page 11 pour savoir comment obtenir plus de détails à propos des effets secondaires des virus sur le site Web de Sophos).

5.3.2 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 (reportez-vous à la section [Informations sur le nettoyage](#) à la page 11 pour savoir comment obtenir plus de détails à propos des effets secondaires des virus sur le site Web de Sophos).

5.3.3 Suppression d'un fichier infecté spécifique

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

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

5.3.4 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.

5.4 Rétablissement suite aux effets secondaires des virus

Le rétablissement d'une infection virale 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 qu'ils nécessitent la restauration du disque dur par vos soins.

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 depuis les disques endommagés par un virus. Sophos peut vous fournir des utilitaires pour réparer les dommages occasionnés par certains virus. Contactez le support technique de Sophos pour obtenir des conseils : reportez-vous à la section [Support technique](#) à la page 39.

6 Consultation du journal de Sophos Anti-Virus

Sophos Anti-Virus consigne les détails de l'activité de contrôle dans le journal Sophos Anti-Virus et syslog. En outre, les évènements de virus et d'erreur sont consignés dans le journal de Sophos Anti-Virus.

- ❖ Pour consulter le journal de Sophos Anti-Virus, à l'invite de commande, 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 de 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

7 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. 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.

8 Annexe A : 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 et aucun virus n'ont 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

8.1 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 apparue et aucun virus n'a été détecté
8	Une erreur non fatale est apparue
16	Un fichier protégé par mot de passe a été découvert (il n'a pas été contrôlé)
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

Code de retour étendu	Description
40	Le contrôle a été interrompu

9 Annexe B : à propos de la configuration à partir d'un CID

La configuration à partir d'un répertoire d'installation centralisée ou CID (Central Installation Directory) est une alternative à la configuration depuis la Sophos Enterprise Console. Vous pouvez l'utiliser pour configurer toutes les fonctions à l'exception des contrôles à la demande. Reportez-vous plutôt à la section [Configuration de contrôles à la demande](#) à la page 6.

Remarque : n'utilisez pas la configuration à partir d'un CID à moins que le support technique vous ait conseillé de le faire, ou si vous ne pouvez utiliser l'Enterprise Console. Vous ne pouvez pas utiliser ensemble la configuration de l'Enterprise Console et celle à partir d'un CID.

La configuration depuis le CID ne nécessite pas l'utilisation d'un ordinateur Windows. Elle implique de faire des modifications dans un fichier de configuration archivé dans le CID, en définissant les valeurs des paramètres à l'aide de la commande **savconfig** (voir la section [Commande de configuration savconfig](#) à la page 21). Ainsi, les ordinateurs utiliseront cette configuration lors de leur mise à jour à partir du CID.

Vous pouvez aussi verrouiller tous les paramètres afin qu'ils ne puissent pas être modifiés sur les ordinateurs clients. De cette manière, vous pouvez déterminer la configuration de Sophos Anti-Virus sur chaque ordinateur sans craindre une quelconque modification des paramètres par l'utilisateur de cet ordinateur.

Vous disposez de deux fichiers de configuration : le fichier de configuration *en ligne* dans le CID et le fichier de configuration *hors ligne* archivé à un autre emplacement. Lorsque vous voulez modifier le fichier en ligne, modifiez d'abord le fichier hors ligne, puis remplacez le fichier en ligne par le fichier hors ligne. Cette opération est abordée dans les sections suivantes.

9.1 Création d'une configuration à partir du CID

1. Utilisez la commande **savconfig** pour définir la valeur de chaque paramètre que vous souhaitez définir dans le fichier de configuration hors ligne.

Utilisez la syntaxe suivante :

```
/opt/sophos-av/bin/savconfig -f config-file -c operation parameter value
```

où :

- **-f** indique que la paramètre doit être appliqué au fichier hors ligne.
- **config-file** correspond au chemin du fichier hors ligne qui peut se trouver dans tout autre répertoire que le CID **savconfig** crée le fichier pour vous.
- **-c** indique que vous souhaitez accéder au niveau Entreprise du fichier hors ligne (pour plus d'informations sur les niveaux, voir la section [À propos des niveaux de configuration](#) à la page 21).
- **operation** correspond soit à **set**, **update**, **add**, **remove** ou **delete**.
- **parameter** correspond au paramètre que vous souhaitez définir.
- **value** correspond à la valeur à laquelle vous souhaitez définir le paramètre.

Par exemple, pour créer un fichier nommé CIDconfig.cfg dans le répertoire ./config et pour désactiver les alertes par courriel, saisissez :

```
/opt/sophos-av/bin/savconfig -f ./config/CIDconfig.cfg -c set EmailNotifier Disabled
```

Pour plus d'informations sur l'utilisation de **savconfig**, reportez-vous à la section [Commande de configuration savconfig](#) à la page 21.

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

3. Lorsque vous avez terminé de définir les paramètres, procédez à la mise à jour de Sophos Anti-Virus :

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

4. Exécutez la commande **addcfg** avec l'option **-f** et le chemin du fichier de configuration hors ligne :

```
/opt/sophos-av/update/cache/Primary-unpacked/addcfg.sh -f config-file
```

5. Copiez le répertoire **/opt/sophos-av/update/cache/Primary-unpacked/config** dans le CID.

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

9.2 Mise à jour d'une configuration à partir du CID

1. Utilisez la commande **savconfig** pour définir la valeur de chaque paramètre que vous souhaitez définir dans le fichier de configuration hors ligne.

Utilisez la syntaxe suivante :

```
/opt/sophos-av/bin/savconfig -f config-file -c operation parameter value
```

où :

- **-f** indique que la paramètre doit être appliqué au fichier hors ligne.
- *config-file* correspond au chemin du fichier hors ligne.
- **-c** indique que vous souhaitez accéder au niveau Entreprise du fichier hors ligne (pour plus d'informations sur les niveaux, voir la section [À propos des niveaux de configuration](#) à la page 21).
- *operation* correspond soit à **set**, **update**, **add**, **remove** ou **delete**.
- *parameter* correspond au paramètre que vous souhaitez définir.
- *value* correspond à la valeur à laquelle vous souhaitez définir le paramètre.

Par exemple, pour mettre à jour un fichier nommé CIDconfig.cfg dans le répertoire ./config et pour désactiver les alertes par courriel, saisissez :

```
/opt/sophos-av/bin/savconfig -f ./config/CIDconfig.cfg -c set EmailNotifier Disabled
```

Remarque : vous devez impérativement paramétrer *tous* les paramètres que vous désirez conserver au niveau Entreprise du fichier en ligne et pas seulement ceux que vous souhaitez mettre à jour. Pour utiliser une copie du fichier de configuration en ligne actuel et du fichier hors ligne, copiez CorporateLayer.cfg dans tout autre répertoire que le CID. CorporateLayer.cfg se trouve dans le répertoire config du CID.

Pour plus d'informations sur l'utilisation de **savconfig**, reportez-vous à la section [Commande de configuration savconfig](#) à la page 21.

2. Pour consulter les valeurs des paramètres, utilisez l'opération **query** (interrogation). Vous pouvez consulter le réglage d'un paramètre individuel ou de tous les paramètres. Par exemple, pour consulter les réglages de tous les paramètres que vous avez définis, saisissez :

```
/opt/sophos-av/bin/savconfig -f ./config/CIDconfig.cfg -c query
```

3. Lorsque vous avez terminé de définir les paramètres, procédez à la mise à jour de Sophos Anti-Virus :

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

4. Exécutez la commande **addcfg** avec l'option **-f** et le chemin du fichier de configuration hors ligne :

```
/opt/sophos-av/update/cache/Primary-unpacked/addcfg.sh -f config-file
```

5. Copiez le répertoire /opt/sophos-av/update/cache/Primary-unpacked/config dans le CID.

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

9.3 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.
- **Entreprise** : ce niveau est présent si l'installation est configurée à partir du CID.
- **Utilisateur** : 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 Entreprise est prioritaire sur le niveau Utilisateur.
- Les niveaux Entreprise et Utilisateur sont prioritaires sur le niveau Sophos.

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

Lorsque le fichier de configuration local est mis à jour depuis le fichier de configuration dans le CID, le niveau Entreprise du fichier local est remplacé par celui du fichier dans le CID.

9.4 Commande de configuration savconfig

savconfig est la commande à utiliser pour configurer toutes les fonctions de Sophos Anti-Virus à l'exception du contrôle à la demande. Le chemin de cette commande est `/opt/sophos-av/bin`. L'utilisation de cette commande pour configurer des fonctions spécifiques de Sophos Anti-Virus est abordée dans la suite de ce manuel. La suite de cette sous-section aborde la syntaxe.

La syntaxe de **savconfig** est :

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

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

```
man savconfig
```

9.4.1 Options

Vous pouvez spécifier une ou plusieurs options. Ces options sont principalement associées aux *niveaux* des fichiers de configuration locale de chaque installation. Pour plus d'informations sur les niveaux, reportez-vous à la section [À propos des niveaux de configuration](#) à la page 21. Par défaut, la commande accède au niveau Utilisateur. Si vous désirez accéder au niveau Entreprise, par exemple, utilisez l'option `-c` ou `--corporate`.

Par défaut, les valeurs des paramètres au niveau Entreprise sont verrouillés, afin d'être prioritaires sur les valeurs du niveau Utilisateur. 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
```

9.4.2 Opérations

Vous pouvez spécifier une seule opération. Ces opérations dépendent principalement de la manière dont vous désirez accéder à un paramètre. Il se peut que certains paramètres n'aient qu'une seule valeur alors que d'autres ont une liste de valeurs. Les opérations vous permettent d'ajouter des valeurs à une liste ou de supprimer des valeurs d'une liste. Par exemple, le paramètre **Email** est une *liste* de destinataires de courriers électroniques.

Pour afficher les valeurs des paramètres, utilisez l'opération **query** (interrogation). 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** retourne les valeurs des paramètres, ceux qui sont en conflit avec la stratégie de l'Enterprise Console sont clairement identifiés par le mot "Conflict".

9.4.3 Paramètres

Vous pouvez spécifier 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.

9.4.4 Valeurs

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

10 Annexe C : configuration des contrôles planifiés

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

Remarque : vous pouvez également utiliser l'Enterprise Console ou la commande **crontab** pour contrôler les ordinateurs à des heures définies. Pour plus de détails, consultez l'aide de l'Enterprise Console ou l'[article 12176 de la base de connaissances du support de Sophos](#). 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. Précisez 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**. Spécifiez 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**. Spécifiez 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 ENTREE, Sophos Anti-Virus attend que vous saisissez la définition du contrôle planifié.

2. Précisez 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.exemple.en`. Après avoir saisi chaque paramètre et sa valeur, appuyez sur ENTREE.

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** avec l'opération **query** et le paramètre **NamedScans**. Indiquez le nom du contrôle et le chemin du fichier où 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**. Précisez 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 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 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 24.
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 dans Sophos Anti-Virus à l'aide de la commande **savconfig** en utilisant l'opération **update** et le paramètre **NamedScans**. Spécifiez 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**. Spécifiez 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 ENTREE, Sophos Anti-Virus attend que vous saisissez la définition du contrôle planifié.

2. Précisez 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 ENTREE. 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 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**. Précisez le nom du contrôle.

Par exemple, pour supprimer le contrôle Daily, saisissez :

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

10.10 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 Annexe D : configuration des alertes par courriel

Remarque : si vous procédez à la configuration d'un ordinateur autonome connecté à un réseau, cette configuration pourrait être remplacée si l'ordinateur télécharge une nouvelle configuration depuis la console ou depuis le CID.

Vous pouvez configurer Sophos Anti-Virus afin qu'il envoie une alerte lors de la détection de virus, d'une erreur du contrôle ou de tout autre type d'erreur. Les alertes par courriel peuvent être envoyées soit en anglais, soit en japonais.

11.1 Désactivation des alertes par courriel

Par défaut, les alertes par courriel sont activées.

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

11.2 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 Spécification de la langue

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

- ❖ Pour spécifier la langue utilisée pour le message d'alerte même, utilisez le paramètre **EmailLanguage**. Actuellement, les seules valeurs valides sont "English" ou "Japanese". 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 courriel en plus du message d'alerte.

11.4 Spécification des destinataires de messagerie

Par défaut, Sophos Anti-Virus envoie les alertes par courriel à root@localhost.

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

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

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

11.5 Désactivation des alertes par courriel à la demande

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

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

11.6 Détermination de ce qui se passe lorsqu'un événement est consigné

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

- ❖ Pour spécifier le message personnalisé, utilisez le paramètre **LogMessage**. Par exemple, saisissez :
`/opt/sophos-av/bin/savconfig set LogMessage 'Contact IT'`

12 Annexe E : configuration de la journalisation

Remarque : si vous procédez à la configuration d'un ordinateur autonome connecté à un réseau, cette configuration pourrait être remplacée si l'ordinateur télécharge une nouvelle configuration depuis la console ou depuis le CID.

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 spécifier 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 Annexe F : configuration de la mise à jour

Important : si vous administrez Sophos Anti-Virus à l'aide de la Sophos Enterprise Console, configurez la mise à jour à l'aide de l'Enterprise Console. Pour de plus amples informations sur la manière de procéder, reportez-vous à l'aide de l'Enterprise Console plutôt qu'à cette section.

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 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

savsetup est une commande qui 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, tapez :

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


savsetup vous demande de sélectionner ce que vous voulez faire.
2. Sélectionnez **Display update configuration** pour voir la configuration actuelle.

13.4 Configuration de plusieurs clients de mise à jour pour une mise à jour depuis le serveur de mise à jour

Remarque : si vous désirez modifier la configuration d'un client de mise à jour autonome, reportez-vous plutôt à la section [Configuration d'un client de mise à jour autonome pour une mise à jour depuis le serveur de mise à jour](#) à la page 32.

Sur le serveur de mise à jour, procédez à la mise à jour du fichier de configuration hors ligne, puis appliquez les modifications au fichier de configuration en ligne, afin que les clients de mise à jour puissent les télécharger à leur prochaine mise à jour. Dans la procédure ci-dessous, *config-file* représente le chemin du fichier de configuration hors ligne.

Cette section suppose que vous souhaitez configurer la source de mise à jour *principale*. Toutefois, si vous souhaitez configurer la source de mise à jour *secondaire*, utilisez plutôt les paramètres de la source de mise à jour secondaire. Par exemple, utilisez **SecondaryUpdateSourcePath** plutôt que **PrimaryUpdateSourcePath**.

Pour configurer plusieurs clients de mise à jour pour une mise à jour depuis le serveur de mise à jour :

1. Définissez l'adresse de la source de mise à jour principale sur l'emplacement du CID, à l'aide du paramètre **PrimaryUpdateSourcePath**. Vous pouvez spécifier soit une adresse HTTP ou 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 config-file -c set PrimaryUpdateSourcePath 'http://www.mywebcid.com/cid'
```
2. Si la source de mise à jour principale exige une authentification, définissez le nom utilisateur et le mot de passe respectivement à l'aide des paramètres **PrimaryUpdateUsername** et **PrimaryUpdatePassword**. Par exemple, saisissez :

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

```
/opt/sophos-av/bin/savconfig -f config-file -c set PrimaryUpdatePassword 'j23rjfwj'
```
3. Si vous accédez à la source de mise à jour principale via un proxy, définissez l'adresse, le nom 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 config-file -c set PrimaryUpdateProxyAddress 'http://www-cache.xyz.com:8080'
```

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

```
/opt/sophos-av/bin/savconfig -f config-file -c set PrimaryUpdateProxyPassword 'fj202jrjf'
```
4. Lorsque vous avez terminé de définir les paramètres, procédez à la mise à jour de Sophos Anti-Virus :

```
/opt/sophos-av/bin/savupdate
```
5. Exécutez la commande **addcfg** avec l'option **-f** et le chemin du fichier de configuration hors ligne :

```
/opt/sophos-av/update/cache/Primary-unpacked/addcfg.sh -f config-file
```

6. Copiez le répertoire `/opt/sophos-av/update/cache/Primary-unpacked/config` dans le CID.

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

13.5 Configuration d'un client de mise à jour autonome pour une mise à jour depuis le serveur de mise à jour

Remarque : si vous désirez modifier la configuration de plusieurs clients de mise à jour, reportez-vous plutôt à la section [Configuration de plusieurs clients de mise à jour pour une mise à jour depuis le serveur de mise à jour](#) à la page 31.

1. Sur l'ordinateur que vous voulez configurer, tapez :
`/opt/sophos-av/bin/savsetup`
savsetup vous demande de sélectionner ce que vous voulez faire.
2. Sélectionnez l'option afin de configurer votre propre serveur comme source de mise à jour principale (ou secondaire).
savsetup vous invite à saisir les détails de la source de mise à jour.
3. Saisissez l'adresse de la source, ainsi que le nom utilisateur et le mot de passe si nécessaire. Vous pouvez spécifier soit une adresse HTTP, soit un chemin UNC, selon la manière dont vous avez paramétré le serveur de mise à jour.
savsetup vous demande si vous avez besoin d'un proxy pour accéder au serveur de mise à jour.
4. Si vous avez besoin d'un proxy, appuyez sur Y et saisissez les détails du proxy.

14 Résolution des problèmes

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

Pour plus d'informations sur les codes d'erreur de Sophos Anti-Virus concernant les contrôles à la demande, reportez-vous à la section [Annexe A : codes de retour du contrôle à la demande](#) à la page 16.

14.1 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.

14.2 L'ordinateur signale qu'“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.

14.3 Sophos Anti-Virus n'a plus d'espace disque disponible

Symptôme

Sophos Anti-Virus n'a plus d'espace disque probablement lors du contrôle d'archives complexes.

Causes

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

- Lorsqu'il décompresse les fichiers archive, Sophos Anti-Virus utilise le répertoire /tmp pour conserver les résultats de son activité. Si ce répertoire n'est pas d'une taille suffisante, Sophos Anti-Virus peut manquer d'espace disque.
- Sophos Anti-Virus a dépassé le quota de l'utilisateur.

Résolution du problème

Procédez de l'une des manières suivantes :

- Augmentez la taille de /tmp.
- Augmentez le quota de l'utilisateur.
- Changez le répertoire que Sophos Anti-Virus utilise pour conserver les résultats de son activité. Pour cela, paramétrez la variable d'environnement SAV_TMP.

14.4 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. Pour plus d'informations, reportez-vous à la section [Contrôle d'un type de fichier particulier](#) à la page 7.

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

Symptôme

Votre programme d'archivage sauvegarde constamment tous les fichiers que Sophos Anti-Virus a contrôlés 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 de "statut 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 la commande **savscan** avec l'option **--no-reset-atime**.

14.6 Virus non nettoyé

Symptômes

- Sophos Anti-Virus n'a pas tenté de nettoyer un virus.
- Sophos Anti-Virus affiche le message **Échec de la désinfection**.

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 sur une disquette ou un CD-ROM protégé en écriture.
- Le fichier infecté est sur un système de fichiers NTFS.

- Sophos Anti-Virus n'élimine pas un fragment de virus lorsqu'il n'a pas trouvé de correspondance exacte au virus.

Résolution du problème

Procédez de l'une des manières suivantes :

- Activez le nettoyage automatique.
- Si possible, accordez les droits en écriture sur le support amovible.
- Traitez plutôt sur l'ordinateur local les fichiers se trouvant sur un système de fichiers NTFS.

14.7 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 la présence d'un fragment de virus dans un fichier de la 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 : reportez-vous à la section [Désinfection d'un fichier infecté spécifique](#) à la page 12.
3. Si des fragments de virus sont toujours signalés, veuillez contacter le support technique de Sophos pour obtenir des conseils : reportez-vous à la section [Support technique](#) à la page 39.

15 Glossaire

CID	Voir “répertoire d'installation centralisée”.
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.
Configuration à partir d'un CID	Une telle configuration implique des modifications dans un fichier de configuration archivé dans le CID, en définissant les valeurs des paramètres à l'aide de la commande savconfig . Lorsque les ordinateurs se mettent à jour depuis le CID, ils utilisent cette configuration. Cette méthode s'appelait autrefois "configuration d'entreprise".
Contrôle planifié	Contrôle de l'ordinateur ou de certaines parties de ce dernier, qui s'exécute à des heures définies.
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.
Niveau	Une des trois sections du fichier de configuration local qui contient des paramètres d'une priorité donnée. Les paramètres du niveau Entreprise remplacent ceux du niveau Utilisateur. Les paramètres du niveau Utilisateur remplacent ceux du niveau Sophos.
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	Composant qui télécharge les mises à jour depuis Sophos et met à jour une série d'emplacements de mise à jour via un réseau. Sophos Update Manager and EM Library are update servers.
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 réacheminer eux-mêmes par courriel. Le terme "virus" est aussi souvent utilisé pour désigner des virus, des vers et des chevaux de Troie.

16 Support technique

Vous pouvez obtenir du support technique pour les produits Sophos de l'une des manières suivantes :

- Rendez-vous sur le forum de la communauté SophosTalk en anglais sur <http://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 <http://www.sophos.fr/support/>.
- Téléchargez la documentation des produits sur <http://www.sophos.fr/support/docs/>.
- Envoyez un courriel à support@sophos.fr, y compris le ou les numéros de version du logiciel Sophos, le ou les systèmes d'exploitation et le ou les niveaux de correctif ainsi que le texte du ou des messages d'erreur.

17 Mentions légales

Copyright © 2008-2011 Sophos Limited. Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise, sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement ou autre sauf si vous possédez une licence valide, auquel cas vous pouvez reproduire la licence conformément à ses termes ou si vous avez le consentement préalable écrit du propriétaire du copyright.

Sophos et Sophos Anti-Virus sont des marques déposées de Sophos Limited. Tous les autres noms de produits et de sociétés mentionnés sont des marques ou des marques déposées appartenant à leurs propriétaires respectifs.

ACE™, TAO™, CIAO™, and CoSMIC™

ACE¹, TAO², CIAO³, and CoSMIC⁴ (henceforth referred to as “DOC software”) are copyrighted by Douglas C. Schmidt⁵ and his research group⁶ at Washington University⁷, University of California⁸, Irvine, and Vanderbilt University⁹, Copyright © 1993–2005, all rights reserved.

Since DOC software is open-source, free software, you are free to use, modify, copy, and distribute—perpetually and irrevocably—the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using DOC software.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not do anything to the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let us¹⁰ know so we can promote your project in the DOC software success stories¹¹.

DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies¹² 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.

Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

The ACE¹³, TAO¹⁴, CIAO¹⁵, and CoSMIC¹⁶ web sites are maintained by the DOC Group¹⁷ at the Institute for Software Integrated Systems (ISIS)¹⁸ and the Center for Distributed Object Computing of Washington University, St. Louis¹⁹ for the development of open-source software as part of the open-source software community²⁰. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge

that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters acknowledge that any such submission might become part of the copyright maintained on the overall body of code, which comprises the DOC software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source DOC software projects or their designees.

The names ACE, TAO, CIAO, 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. Further, products or services derived from this source may not be called ACE, TAO, CIAO, or CoSMIC nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

If you have any suggestions, additions, comments, or questions, please let me²¹ know.

Douglas C. Schmidt²²

References

1. <http://www.cs.wustl.edu/~schmidt/ACE.html>
2. <http://www.cs.wustl.edu/~schmidt/TAO.html>
3. <http://www.dre.vanderbilt.edu/CIAO/>
4. <http://www.dre.vanderbilt.edu/cosmic/>
5. <http://www.dre.vanderbilt.edu/~schmidt/>
6. <http://www.cs.wustl.edu/~schmidt/ACE-members.html>
7. <http://www.wustl.edu/>
8. <http://www.uci.edu/>
9. <http://www.vanderbilt.edu/>
10. mailto:doc_group@cs.wustl.edu
11. <http://www.cs.wustl.edu/~schmidt/ACE-users.html>
12. <http://www.cs.wustl.edu/~schmidt/commercial-support.html>
13. <http://www.cs.wustl.edu/~schmidt/ACE.html>
14. <http://www.cs.wustl.edu/~schmidt/TAO.html>
15. <http://www.dre.vanderbilt.edu/CIAO/>
16. <http://www.dre.vanderbilt.edu/cosmic/>
17. <http://www.dre.vanderbilt.edu/>
18. <http://www.isis.vanderbilt.edu/>
19. <http://www.cs.wustl.edu/~schmidt/doc-center.html>
20. <http://www.opensource.org/>
21. <mailto:d.schmidt@vanderbilt.edu>
22. <http://www.dre.vanderbilt.edu/~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 ce type distribué avec un produit Sophos, le code source est mis à disposition en envoyant une demande à Sophos via courriel 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.

OpenSSL cryptographic 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 © 1998–2006 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.

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 (ey@cryptsoft.com).
This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

Copyright © 1995–1998 Eric Young (ey@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (ey@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 licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

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

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 compression tools

© 1995–2002 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

If you use the zlib library in a product, we would appreciate *not* receiving lengthy legal documents to sign. The sources are provided for free but without warranty of any kind. The library has been entirely written by Jean-loup Gailly and Mark Adler; it does not include third-party code.

If you redistribute modified sources, we would appreciate that you include in the file ChangeLog history information documenting your changes.

Index

A

- alertes
 - courriel 27
 - ligne de commande 10
- alertes par courriel 27
- alertes par ligne de commande 10
- analyses des virus 11
- archives
 - contrôles à la demande 7
- Aucune entrée de manuel pour ... 33

C

- codes d'erreur 16
- codes de retour 16
- configuration à partir d'un CID 4, 18
- configuration de Sophos Anti-Virus 4, 18
- contrôle planifié 23
- contrôles à la demande 6
 - archives 7
 - contrôles planifiés 23
 - éléments avec des liens symboliques 8
 - exclusion d'éléments 8
 - exécutables UNIX 9
 - fichiers 6
 - ordinateur 6
 - ordinateurs distants 8
 - répertoires 6
 - systèmes de fichiers 6, 8
 - types de fichier 7, 9

D

- désinfection
 - fichiers infectés 12

E

- effets secondaires des virus 13
- éléments avec des liens symboliques, contrôles à la demande 8
- Enterprise Console 4
- espace disque insuffisant 34
- exclusion d'éléments
 - contrôles à la demande 8

- exécutables UNIX, contrôles à la demande 9

F

- fichiers infectés
 - désinfection 12
 - mise en quarantaine 11
 - nettoyage 12
 - suppression 13
- fichiers, contrôles à la demande 6
- fragment signalé, virus 36

I

- ILC (interface de ligne de commande) 4
- informations sur le nettoyage 11
- interface de ligne de commande (ILC) 4

J

- journal de Sophos Anti-Virus
 - affichage 14
 - configuration 29
- journal, Sophos Anti-Virus
 - affichage 14
 - configuration 29

L

- lenteur des contrôles à la demande 34

M

- mise à jour
 - configuration 30
 - immédiate 15
- mise en quarantaine des fichiers infectés 11

N

- nettoyage des fichiers infectés 12
- niveaux, dans le fichier de configuration 21

O

- ordinateur, contrôles à la demande 6
- ordinateurs distants, contrôles à la demande 8

P

page de man introuvable 33

R

répertoires, contrôles à la demande 6

S

sauvegardes des fichiers contrôlés 35

savconfig 21

savsetup 30

suppression des fichiers infectés 13

systèmes de fichiers, contrôles à la demande 6, 8

T

types de fichier, contrôles à la demande 7, 9

V

virus

analyses 11

déecté 10, 28

effets secondaires 13

fragment signalé 36

non éliminé 35