

SOPHOS

Sophos Anti-Virus pour Linux, version 7 manuel utilisateur

Date du document : mai 2010



A propos de ce manuel

Ce manuel utilisateur vous explique comment utiliser Sophos Anti-Virus pour Linux et comment configurer :

- Le contrôle des virus/spywares
- Les alertes de virus/spywares
- Le nettoyage
- La journalisation
- La mise à jour.

Ce manuel contient par ailleurs une aide à la résolution des problèmes les plus fréquents.

Si vous souhaitez installer, mettre à niveau ou désinstaller Sophos Anti-Virus sur des ordinateurs Linux en réseau ou autonomes, reportez-vous au *Guide de démarrage de Sophos Anti-Virus pour Linux, version 7*.

Si vous souhaitez installer Sophos Anti-Virus sur un réseau composé à la fois d'ordinateurs Linux et Windows, ou souhaitez administrer Sophos Anti-Virus de manière centralisée à l'aide de la Sophos Enterprise Console, reportez-vous au *Guide de démarrage avancé de Sophos Endpoint Security and Control 9*.

La documentation Sophos est disponible sur www.sophos.fr/support/docs/ et sur les CD-ROM de Sophos.

Table des matières

Conventions utilisées dans ce manuel	5
Utilisation de Sophos Anti-Virus	
1 A propos de Sophos Anti-Virus pour Linux	8
2 Exécution du contrôle sur accès	11
3 Exécution des contrôles à la demande	14
4 Que se passe-t-il lors de la découverte d'un virus/spyware ?	17
5 Nettoyage de virus/spywares	19
6 Affichage des journaux	22
Configuration de Sophos Anti-Virus	
7 Aperçu de la configuration	26
8 Configuration du contrôle sur accès	32
9 Configuration du contrôle à la demande	41
10 Configuration des alertes	51
11 Configuration du journal de Sophos Anti-Virus	59
12 Configuration de l'interface utilisateur de Sophos Anti-Virus	60
Mise à jour de Sophos Anti-Virus	
13 Mise à jour immédiate de Sophos Anti-Virus	62
14 Support technique du noyau	63
15 Configuration de la mise à jour	64
Résolution des problèmes	
16 Résolution des problèmes	70

Glossaire et index

Glossaire	76
Index	80
Support technique	82
Copyright	83

Conventions utilisées dans ce manuel

Lorsque une donnée d'entrée saisie sur la ligne de commande se poursuit sur plus d'une ligne, les lignes suivantes apparaissent en retrait, par exemple

```
/opt/sophos-av/bin/savconfig remove ExcludeFilesLike  
    /home/fred/Report.txt
```

Saisissez ce qui est reproduit sans aucun saut de ligne.

Utilisation de Sophos Anti-Virus

A propos de Sophos Anti-Virus pour Linux

Exécution du contrôle sur accès

Exécution des contrôles à la demande

Que se passe-t-il lors de la découverte d'un virus/spyware ?

Nettoyage de virus/spywares

Affichage des journaux

1 A propos de Sophos Anti-Virus pour Linux

Sophos Anti-Virus pour Linux vous permet de protéger votre réseau contre les virus/spywares.

1.1 Interfaces utilisateur

Sophos Anti-Virus dispose :

- d'une interface utilisateur par ligne de commande
- d'une interface utilisateur graphique.

La ligne de commande vous permet d'accéder à *toutes* les fonctionnalités de Sophos Anti-Virus et d'exécuter *toutes* les configurations souhaitées. La ligne de commande est la seule manière de configurer le contrôle à la demande et la mise à jour.

- ❗ Vous devez impérativement disposer des droits administrateur (root) pour pouvoir utiliser toutes les commandes Sophos Anti-Virus sauf savscan, qui est utilisée pour le contrôle à la demande.
- ❗ Dans ce manuel, il est supposé que vous avez installé Sophos Anti-Virus dans l'emplacement par défaut. Par conséquent, les chemins des commandes décrites sont basés sur cet emplacement.

L'interface utilisateur de Sophos Anti-Virus vous permet de

- vérifier l'état du contrôle sur accès
- démarrer et arrêter le contrôle sur accès
- configurer le contrôle des archives
- configurer les exclusions du contrôle
- configurer les alertes
- configurer le journal de Sophos Anti-Virus
- configurer le nettoyage.

- ❗ L'interface utilisateur peut être exécutée par l'utilisateur root (ainsi que par d'autres), en revanche, elle ne fonctionne pas avec les privilèges root. Aussi, elle ne permet pas d'accéder à tous les fichiers de l'ordinateur.

Pour utiliser l'interface utilisateur (GUI), ouvrez un explorateur. Dans le champ Adresse, saisissez

```
http://localhost:8081
```

- ❗ Si vous désirez utiliser une adresse de port http différente, configurez l'interface utilisateur en suivant les instructions du [chapitre 12](#).

L'explorateur affiche la page d'accueil de l'interface utilisateur.



Lorsque vous naviguez sur une autre page, le navigateur vous demande vos codes d'accès afin que vous puissiez utiliser l'interface utilisateur graphique pour configurer Sophos Anti-Virus.

Pour connaître votre nom utilisateur, adressez-vous à votre administrateur système ou alors, à la ligne de commande, saisissez

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

Pour connaître votre mot de passe, adressez-vous à votre administrateur système

Pour changer vos codes d'accès, reportez-vous au [chapitre 12](#).

1.2 Modes de contrôle

Sophos Anti-Virus propose deux modes de contrôle :

- sur accès
- à la demande.

Le **contrôle sur accès** intercepte les fichiers lors de leur accès et autorise uniquement l'accès à ceux ne représentant aucune menace pour votre réseau.

Le **contrôle à la demande** est un contrôle des virus/spywares sur l'ordinateur ou sur des parties de celui-ci que vous exécutez immédiatement ou que vous planifiez pour une exécution ultérieure.

1.3 Intégration avec la console d'administration

Sophos Anti-Virus est intégré à la Sophos Enterprise Console, qui fonctionne sur Windows et permet à l'administrateur réseau une administration centralisée de Sophos Anti-Virus sur les systèmes d'extrémité.

2 Exécution du contrôle sur accès

- ❓ Le **contrôle sur accès** intercepte les fichiers lors de leur accès et autorise uniquement l'accès à ceux ne représentant aucune menace pour votre réseau.

Ce chapitre vous indique comment *utiliser* le contrôle sur accès. Pour le *configurer*, reportez-vous au [chapitre 8](#).

2.1 Vérification de l'activité du contrôle sur accès

Ligne de commande

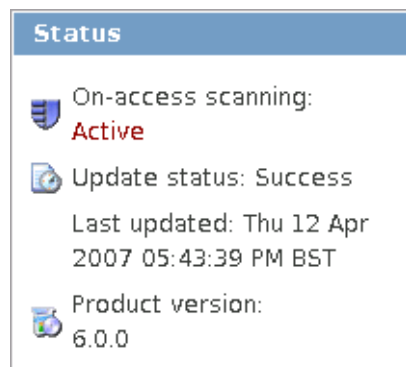
Saisissez

```
/opt/sophos-av/bin/savdstatus
```

Sophos Anti-Virus affiche l'état du contrôle sur accès.

Interface utilisateur graphique

La zone **Status** de chaque page affiche l'état du contrôle sur accès.



2.2 Vérification du lancement automatique du contrôle sur accès au démarrage du système

Ligne de commande

En supposant que vous avez les privilèges root, saisissez :

```
chkconfig --list
```

- 💡 Il se peut que cette commande ne fonctionne pas sur TurboLinux.

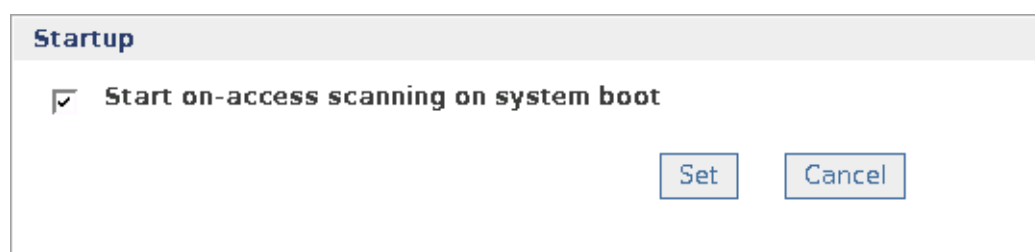
Si la liste contient une entrée pour sav-protect avec 2:on, 3:on, 4:on et 5:on, le contrôle sur accès se lance automatiquement au démarrage du système.

Sinon, pour lancer automatiquement le contrôle sur accès au démarrage du système, saisissez

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

Interface utilisateur graphique

Sur la page **Control**, dans la zone **Startup**, vérifiez si la case **Start on-access scanning on system boot** est cochée. Si elle ne l'est pas, sélectionnez-la pour exécuter automatiquement le contrôle sur accès au démarrage du système. Cliquez sur **Set** pour appliquer la modification.



2.3 Démarrage du contrôle sur accès

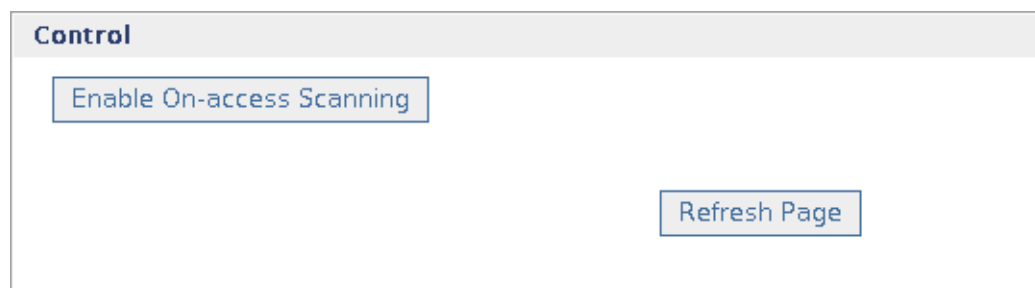
Ligne de commande

Saisissez

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

Interface utilisateur graphique

Sur la page **Control**, dans la zone **Control**, cliquez sur **Enable On-access Scanning**.



2.4 Arrêt du contrôle sur accès

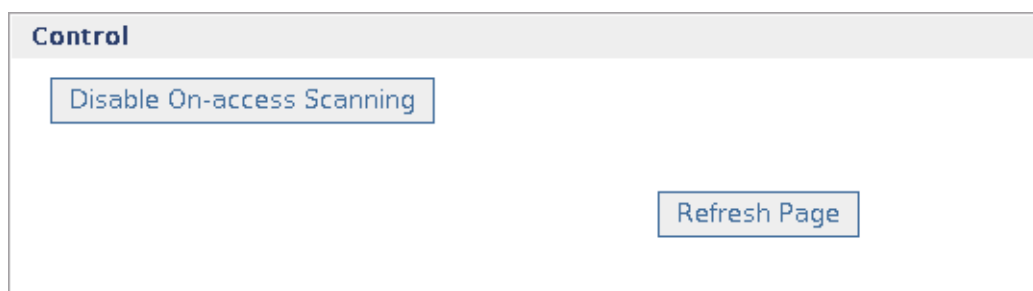
Ligne de commande

Saisissez

```
/opt/sophos-av/bin/savdctl disable
```

Interface utilisateur graphique

Sur la page **Control**, dans la zone **Control**, cliquez sur **Disable On-access Scanning**.



3 Exécution des contrôles à la demande

❓ Un **contrôle à la demande** est un contrôle des virus/spywares sur l'ordinateur ou sur des parties de celui-ci que vous exécutez immédiatement ou que vous planifiez pour une exécution ultérieure.

Par défaut, Sophos Anti-Virus contrôle les

- exécutables
- fichiers .sh et .pl
- types de fichiers pouvant être infectés par des virus macro
- fichiers HTML
- fichiers compressés avec gzip et bzip2
- sous-répertoires du répertoire spécifié
- éléments vers lesquels pointent les liens symboliques.

Pour obtenir une liste complète des types de fichier contrôlés, saisissez

```
savscan -vv
```

Pour plus d'informations sur la modification de ces paramètres, reportez-vous au [chapitre 9](#).

3.1 Contrôle de l'ordinateur

Pour contrôler l'ordinateur, saisissez

```
savscan /
```

3.2 Contrôle d'un répertoire ou d'un fichier donné

Pour effectuer le contrôle d'un répertoire ou d'un fichier donné, utilisez le chemin menant à l'élément à contrôler, par exemple

```
savscan /usr/monrépertoire/monfichier
```

3.3 Contrôle d'un système de fichiers

Pour contrôler un système de fichiers, utilisez le nom du système de fichiers, par exemple

```
savscan /home
```

Il est possible de saisir plus d'un système de fichiers à la ligne de commande.

3.4 Contrôle d'un secteur de démarrage

Vous pouvez contrôler les secteurs de démarrage des lecteurs logiques et physiques.

Pour contrôler les secteurs de démarrage, ouvrez une session en tant que superutilisateur (afin de disposer des droits d'accès suffisants aux périphériques du disque) puis utilisez une des commandes indiquées ci-dessous.

Pour contrôler les secteurs de démarrage de lecteurs logiques spécifiés, saisissez

```
savscan -bs=XXX, XXX, ...
```

où XXX correspond au nom d'un lecteur (par exemple /dev/fd0 ou /dev/hda1).

Pour contrôler les secteurs de démarrage de tous les lecteurs logiques que Sophos Anti-Virus reconnaît, saisissez

```
savscan -bs
```

Pour contrôler les enregistrements de démarrage maîtres de tous les lecteurs physiques fixes de l'ordinateur, saisissez

```
savscan -mbr
```

3.5 Planification d'un contrôle

Sophos Anti-Virus contrôle automatiquement l'ordinateur à des heures planifiées. Pour plus d'informations, reportez-vous à l'[annexe](#).

3.6 Codes d'erreur

Des codes d'erreur sont retournés par savscan en cas d'erreur ou de découverte de virus ou de spywares.

- 0 Si aucune erreur n'a été rencontrée et aucun virus/spyware découvert.
- 1 Si l'utilisateur interrompt l'exécution en pressant sur 'Control'+ 'c'.
- 2 Si une erreur empêchant la prochaine exécution d'un contrôle est découverte.
- 3 Si des virus/spywares ou des fragments de virus sont découverts.

3.6.1 Codes d'erreur avancés

Différents types de codes d'erreur sont retournés si la commande savscan est exécutée avec l'option -eec.

0 Si aucune erreur n'a été rencontrée et aucun virus/spyware découvert.

8 Si des erreurs persistantes ont eu lieu.

16 Si des fichiers protégés par mots de passe ont été découverts. (Ils ne sont pas contrôlés).

20 Si des virus/spywares ont été découverts et éliminés.

24 Si des virus/spywares ont été découverts mais pas éliminés.

28 Si des virus/spywares ont été découverts en mémoire.

32 S'il y a eu une panne du contrôle d'intégrité.

36 Si des erreurs non persistantes ont eu lieu.

40 Si l'exécution a été interrompue.

4 Que se passe-t-il lors de la découverte d'un virus/spyware ?

4.1 Si des virus/spywares sont découverts lors du contrôle sur accès

Si Sophos Anti-Virus découvre un virus ou un élément de spyware au cours du contrôle sur accès alors l'accès au fichier est refusé et une boîte de message, comme celle ci-dessous, apparaît.



Si l'affichage de la boîte de message est impossible, l'alerte est visible à la ligne de commande.

Sophos Anti-Virus consigne aussi l'évènement dans le journal Sophos Anti-Virus et envoie une alerte à l'Enterprise Console si celle-ci administre l'ordinateur.

Reportez-vous au [chapitre 5](#) pour plus d'informations sur le nettoyage des virus/spywares de vos machines.

4.2 Si des virus/spywares sont découverts lors d'un contrôle planifié

Si Sophos Anti-Virus détecte un virus ou un élément de spyware, il le signale dans la ligne qui commence par >>> suivie soit de "Virus" soit de "Fragment de virus" :

```
Utilitaire de détection virale SAVScan
Version X.XX.XX [Linux/Intel]
Version des données virales X.XX, Novembre 2009
Inclut la détection de 201433 virus, chevaux de Troie et vers
Copyright (c) 1989-2009 Sophos Group. Tous droits réservés.

Heure système 10:23:49, Date système 27 Novembre 2009

Contrôle rapide

>>> Virus 'EICAR-AV-Test' trouvé dans le fichier /usr/mydirectory/
eicar.src

33 fichiers contrôlés en 2 secondes.
1 virus découvert.
1 fichier sur 33 infecté.
Veuillez envoyer les échantillons infectés à Sophos pour analyse.
Pour plus de conseils, consultez www.sophos.fr, envoyez un courriel
à support@sophos.fr
Fin du contrôle.
```

Sophos Anti-Virus consigne aussi l'évènement dans le journal Sophos Anti-Virus.

Reportez-vous au [chapitre 5](#) pour plus d'informations sur le nettoyage des virus/spywares de vos machines.

5 Nettoyage de virus/spywares

5.1 Informations sur l'élimination des virus

Si des virus/spywares sont signalés, rendez-vous sur le site Web de Sophos pour obtenir des informations et des conseils de nettoyage de vos machines. Rendez-vous sur la page des Analyses des menaces (www.sophos.fr/security/analyses). Recherchez l'analyse de virus ou de l'élément de spyware en utilisant le nom indiqué par Sophos Anti-Virus.

5.2 Mise en quarantaine des fichiers infectés

Vous pouvez configurer Sophos Anti-Virus pour mettre les fichiers infectés en quarantaine (c'est-à-dire pour empêcher leur accès). Le logiciel effectue cette opération en changeant les droits de propriété et d'accès au fichier.

Pour définir la mise en quarantaine, saisissez

```
savscan PATH --quarantine
```

où PATH est le chemin à contrôler.

Par défaut, Sophos Anti-Virus change les droits de propriétés d'un fichier infecté sur ceux de l'utilisateur exécutant Sophos Anti-Virus ainsi qu'il change les droits d'accès sur `-r-----` (0400).

Si vous le souhaitez, il vous est possible de définir les droits de propriété et d'accès de l'utilisateur ou du groupe que Sophos appliquera aux fichiers infectés. Pour cela, servez-vous des paramètres suivants :

```
uid=NNN
user=NOMUTILISATEUR
gid=NNN
group=NOM-GROUPE
mode=PPP
```

Il n'est pas possible de définir plus d'un paramètre de chaque type, par exemple, vous ne pouvez pas saisir deux fois le même nom utilisateur ou saisir une uid et un nom 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 sophosav

et du groupe virus, mais que *seul* l'utilisateur sophosav a accès au fichier (en lecture seulement). Personne d'autre ne peut intervenir sur le fichier (sauf sur la racine ou root) de quelque manière que ce soit.

- ❗ Si vous indiquez désinfection (voir section 5.3) 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.

5.3 Paramétrage du nettoyage automatique pour le contrôle à la demande

Sophos Anti-Virus désinfecte ou supprime automatiquement les éléments infectés lorsque vous exécutez un contrôle à la demande. Toutes les actions entreprises par Sophos Anti-Virus contre les éléments infectés sont répertoriées dans le récapitulatif des contrôles et consignées dans le journal de Sophos Anti-Virus. Par défaut, le nettoyage automatique est désactivé.

La méthode que vous utilisez dépend de votre décision de nettoyer un fichier ou un secteur de démarrage.

5.3.1 Nettoyage des fichiers

Pour désinfecter un fichier spécifique, saisissez

```
savscan FILE-PATH -di
```

Autrement, pour désinfecter tous les fichiers sur l'ordinateur, saisissez

```
savscan / -di
```

Dans les deux cas, Sophos Anti-Virus vous demande confirmation avant de procéder à la désinfection.

La désinfection des documents ne corrige pas toutes les modifications causées par le virus dans le document. (reportez-vous à la [section 5.1](#) pour savoir comment obtenir plus de détails à propos des effets secondaires des virus sur le site Web de Sophos.)

Pour supprimer un fichier infecté spécifique, saisissez

```
savscan FILE-PATH -remove
```

Autrement, pour désinfecter tous les fichiers infectés sur l'ordinateur, saisissez

```
savscan / -remove
```

Dans les deux cas, Sophos Anti-Virus vous demande confirmation avant de procéder à la suppression.

5.3.2 Désinfection d'un secteur de démarrage

Pour désinfecter un secteur de démarrage, saisissez

```
savscan -bs=XXX -di
```

où XXX correspond au nom d'un lecteur.

Par exemple, pour éliminer un virus d'un lecteur de disquette, saisissez

```
savscan -bs=/dev/fd0 -di
```

5.4 Guérison des effets secondaires des virus

La guérison 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 que la guérison nécessitera 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 que vous lisiez l'analyse de virus sur le site Web de Sophos et que vous procédiez 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 dégâts occasionnés par certains virus. Contactez le [support technique](#) de Sophos pour obtenir des conseils.

6 Affichage des journaux

Sophos Anti-Virus consigne les détails de l'activité de contrôle dans le journal de Sophos Anti-Virus et dans syslog. En outre, les événements de virus/spywares et les erreurs sont consignés dans le journal Sophos Anti-Virus. Les messages du journal Sophos Anti-Virus sont traduits dans les langues prises en charge par le produit.

Ligne de commande

Utilisez la commande savlog. Cette commande peut être utilisée avec diverses options de ligne de commande 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
```

Interface utilisateur graphique

Allez sur la page **Log Viewer**.

Log Selection

Display log entries after

Display log entries before

Maximum number of log entries

Category

Time format

Local time

UTC

Log Contents

Time	Category	Event
Mon 16 Jan 2006 15:44:04 GMT	savd.daemon	Sophos Anti-Virus daemon started.
Mon 16 Jan 2006 17:41:46 GMT	savd.daemon	On-access scanning enabled.
Mon 16 Jan 2006 19:09:46 GMT	savd.daemon	On-access scanning disabled.
Tue 17 Jan 2006 13:55:27 GMT	savd.daemon	On-access scanning enabled.
Tue 17 Jan 2006 13:57:29 GMT	savd.daemon	On-access scanning enabled.

A l'aide des zones de texte et des boutons radio de la zone **Log Selection**, spécifiez les messages que vous désirez afficher. Puis, cliquez sur **View Log** pour afficher les messages dans la zone **Log Contents**.

Configuration de Sophos Anti-Virus

Aperçu de la configuration

Configuration du contrôle sur accès

Configuration du contrôle à la demande

Configuration des alertes

Configuration du journal de Sophos Anti-Virus

Configuration de l'interface utilisateur de Sophos Anti-Virus

7 Aperçu de la configuration

- ❗ Ce chapitre est applicable à toute configuration sauf à celle du contrôle à la demande abordée au [chapitre 9](#). L'utilisation de la Sophos Enterprise Console ou des commandes savconfig ou savsetup n'a aucun effet sur le contrôle à la demande.

7.1 Configuration de Sophos Anti-Virus sur un réseau depuis la console

Vous pouvez gérer la *version 7* de Sophos Anti-Virus sur les systèmes d'extrémité à l'aide de l'Enterprise Console qui fonctionne sur Windows. Elle vous permet de procéder à vos différentes configurations grâce à une interface utilisateur graphique conviviale. La procédure d'installation de la console est détaillée dans le *Guide de démarrage réseau de Sophos Endpoint Security and Control 9*, disponible sur www.sophos.fr/support/docs/ et sur les CD-ROM de Sophos.

Pour de plus amples informations sur l'utilisation de la console pour configurer Sophos Anti-Virus, reportez-vous à l'aide de la console. Par ailleurs, si vous utilisez la console, les points suivants s'appliquent concernant la configuration :

- Les paramètres ne pouvant pas être définis à l'aide de la console peuvent l'être sur chaque système d'extrémité localement à l'aide de savconfig ([section 7.4](#)). Ces paramètres sont ignorés par la console.
- La mise à jour automatique est configurée en utilisant uniquement la console : sa configuration est impossible sur le système d'extrémité.
- ❗ Sophos ne prend pas en charge l'utilisation conjointe de la configuration à partir de la console et à partir du CID, autrefois appelée configuration d'entreprise. Si vous utilisez une configuration à partir d'un CID avec la *version 5* de Sophos Anti-Virus, vous devez choisir si vous désirez continuer à utiliser cette configuration ou si vous voulez utiliser l'Enterprise Console à la place. Si vous choisissez de démarrer en utilisant l'Enterprise Console, reportez-vous à l'article 22297 de la base de connaissances du support Sophos (www.sophos.fr/support/knowledgebase/article/22297.html).

7.2 Configuration de Sophos Anti-Virus sur un réseau depuis le CID

La configuration depuis le répertoire d'installation centralisée (CID), autrefois appelée configuration d'entreprise, 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 ([section 7.4](#)). Ainsi, les systèmes d'extrémité utiliseront cette configuration lors de la mise à jour depuis le CID. Vous pouvez aussi verrouiller tous les paramètres afin qu'ils ne puissent pas être modifiés sur les systèmes d'extrémité. De cette

manière, vous pouvez déterminer la configuration de Sophos Anti-Virus sur chaque système d'extrémité sans craindre une quelconque modification des paramètres par l'utilisateur d'un système d'extrémité.

Il existe 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 utilisez un programme pour remplacer le contenu du fichier en ligne par celui du fichier hors ligne.

7.2.1 Création du fichier de configuration en ligne dans le CID

1. Créez le fichier de configuration hors ligne dans un répertoire de votre choix différent du CID. Utilisez impérativement la commande `savconfig`, et précisez
 - le nom du fichier hors ligne, y compris l'extension du nom de fichier `cfg`
 - que vous accédez au niveau *Entreprise* du fichier (pour de plus amples informations sur les niveaux, reportez-vous à la [section 7.2.3](#))
 - le réglage d'un paramètre.

Utilisez la syntaxe suivante :

```
/opt/sophos-av/bin/savconfig -f CONFIG-FILE -c VALEUR PARAMETRE
```

où `CONFIG-FILE` correspond au chemin du fichier hors ligne, `-c` indique que vous souhaitez accéder au niveau *Entreprise*, `PARAMETER` correspond au paramètre que vous souhaitez définir et `VALUE` correspond à la valeur sur laquelle vous souhaitez définir le paramètre. Par exemple, pour créer un fichier nommé `CIDconfig.cfg` et pour démarrer le contrôle sur accès au démarrage du daemon Sophos Anti-Virus, saisissez

```
/opt/sophos-av/bin/savconfig -f CIDconfig.cfg -c EnableOnStart
  Enabled
```

Voir la [section 7.4](#) pour plus d'informations sur l'utilisation de `savconfig`.

2. Si nécessaire, procédez au réglage d'autres paramètres à l'aide de la commande `savconfig`. Vous devez préciser le nom du fichier hors ligne et que vous accédez au niveau *Entreprise*, comme indiqué ci-dessus.
3. Pour afficher les réglages des paramètres, utilisez l'opération d'interrogation. Vous pouvez afficher le réglage d'un paramètre individuel ou de tous les paramètres. Par exemple, pour afficher les réglages de tous les paramètres que vous avez défini, saisissez

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

4. Lorsque vous avez terminé de régler les paramètres, exécutez l'utilitaire `addcfg` pour faire une copie de la configuration dans le CID, prête à être téléchargée par les systèmes d'extrémité à leur prochaine mise à jour. L'utilitaire se trouve dans le CID. Selon l'emplacement du CID, saisissez

```
/opt/sophos-av/update/cache/Primary/addcfg.sh -f CONFIG-FILE
```

où `CONFIG-FILE` correspond au chemin du fichier hors ligne.

7.2.2 Mise à jour du fichier de configuration en ligne dans le CID

1. Mettez à jour le fichier de configuration hors ligne. Utilisez impérativement la commande `savconfig`, et précisez
 - le nom du fichier hors ligne
 - que vous accédez au niveau *Entreprise* du fichier (pour de plus amples informations sur les niveaux, reportez-vous à la section 7.2.3)
 - le réglage d'un paramètre.

Utilisez la syntaxe suivante :

```
/opt/sophos-av/bin/savconfig -f CONFIG-FILE -c VALEUR PARAMETRE
```

où CONFIG-FILE correspond au chemin du fichier hors ligne, -c indique que vous souhaitez accéder au niveau *Entreprise*, PARAMETER correspond au paramètre que vous souhaitez définir et VALUE correspond à la valeur sur laquelle vous souhaitez définir le paramètre. Par exemple, pour mettre à jour un fichier nommé `CIDconfig.cfg` et pour démarrer le contrôle sur accès au démarrage du daemon Sophos Anti-Virus, saisissez

```
/opt/sophos-av/bin/savconfig -f CIDconfig.cfg -c EnableOnStart  
Enabled
```

Voir la [section 7.4](#) pour plus d'informations sur l'utilisation de `savconfig`.

2. Si nécessaire, procédez au réglage d'autres paramètres à l'aide de la commande `savconfig`. Vous devez préciser le nom du fichier hors ligne et que vous accédez au niveau *Entreprise*, comme indiqué ci-dessus.
3. Pour afficher les réglages des paramètres, utilisez l'opération d'interrogation. Vous pouvez afficher le réglage d'un paramètre individuel ou de tous les paramètres. Par exemple, pour afficher les réglages de tous les paramètres que vous avez défini, saisissez

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

4. Lorsque vous avez terminé de régler les paramètres, exécutez l'utilitaire `addcfg` pour faire une copie de la configuration dans le CID, prête à être téléchargée par les systèmes d'extrémité à leur prochaine mise à jour. L'utilitaire se trouve dans le CID. Selon l'emplacement du CID, saisissez

```
/opt/sophos-av/update/cache/Primary/addcfg.sh -fCONFIG-FILE
```

où CONFIG-FILE correspond au chemin du fichier hors ligne.

7.2.3 Niveaux de configuration

Chaque installation de Sophos Anti-Virus inclut un fichier de configuration local comprenant les paramètres de tous les composants de Sophos Anti-Virus.

Chaque fichier de configuration local contient un nombre de *niveaux* :

- Sophos : niveau toujours présent dans le fichier. Il inclut les réglages de l'éditeur qui sont uniquement modifiés par Sophos.
- Entreprise : niveau présent si l'installation est configurée depuis le répertoire d'installation centralisée (CID), comme le décrivent les sections [7.2.1](#) et [7.2.2](#).
- 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.

7.3 Configuration de Sophos Anti-Virus sur un ordinateur autonome

Utilisez la commande `savconfig` pour mettre en place la configuration sur un ordinateur autonome. Voir la section 7.4 pour plus d'informations sur l'utilisation de `savconfig`. Par défaut, `savconfig` applique la configuration au niveau Utilisateur du fichier de configuration local.

7.4 Commande de configuration : `savconfig`

La commande `savconfig` est celle que vous utilisez pour définir ou interroger la configuration de Sophos Anti-Virus. 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] [PARAMETRE] [VALEUR] ...
```

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

```
man savconfig
```

Veillez noter que ce qui suit n'est qu'un aperçu.

7.4.1 OPTION

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 ces niveaux, reportez-vous à la [section 7.2.3](#). Par défaut, la commande accède au niveau Utilisateur. Aussi, si vous désirez accéder au niveau Entreprise (corporate), 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. Toutefois, si vous désirez 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`. Par exemple, saisissez

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

Aussi, vous pouvez afficher uniquement les valeurs de la stratégie de mise à jour de la console en utilisant l'option `--consoleupdate`. Par exemple, saisissez

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

7.4.2 OPERATION

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. Par conséquent, les opérations vous permettent d'ajouter des valeurs à une liste ou de supprimer des valeurs d'une liste. Par exemple, le paramètre `CacheFilesystems` est une *liste* de types de systèmes de fichiers.

Pour afficher les valeurs des paramètres, utilisez l'opération d'interrogation. Par exemple, pour afficher la valeur du paramètre ExcludeFileOnGlob, saisissez

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

Si vous utilisez l'Enterprise Console, lorsque savconfig renvoie les valeurs des paramètres, ceux qui sont en conflit avec la bonne stratégie de la console sont clairement identifiés par le mot "Conflit".

7.4.3 PARAMETRE

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.

7.4.4 VALEUR

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

7.5 Commande de configuration : savsetup

L'utilitaire savsetup sert à paramétrer ou à interroger la configuration de la mise à jour et de l'interface utilisateur de Sophos Anti-Virus. Bien qu'il vous permette d'accéder seulement à certains paramètres auxquels vous pouvez accéder avec savconfig, il est plus facile à utiliser. Il vous invite à saisir les valeurs des paramètres et vous répondez simplement en sélectionnant ou en saisissant les valeurs. Pour exécuter savsetup, saisissez

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

Lorsque vous exécutez savsetup, un choix de configuration vous est proposé : mise à jour ou interface utilisateur de Sophos Anti-Virus. Saisissez le numéro correspondant à votre choix. Poursuivez en répondant aux questions qui apparaissent.

8 Configuration du contrôle sur accès

- ❗ Si vous procédez à la configuration d'un ordinateur autonome connecté à un réseau, cette configuration pourrait être rejetée si l'ordinateur télécharge une nouvelle configuration depuis la console ou depuis le CID.

8.1 Exclusion du contrôle des fichiers et répertoires

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

- en utilisant le nom du fichier ou du répertoire (section 8.1.1)
- en utilisant le type de fichier (section 8.1.2)
- en utilisant les caractères jokers (section 8.1.3)

Si vous souhaitez exclure des fichiers et répertoires dont les noms des jeux de caractères ne sont pas en UTF-8, reportez-vous à la section 8.1.4.

8.1.1 Par nom de fichier ou de répertoire

- ❗ Si vous utilisez l'Enterprise Console et que votre stratégie antivirus spécifie des exclusions en utilisant le nom du fichier ou du répertoire, toutes les exclusions paramétrées localement sur un système d'extrémité entraîneront l'affichage par la console du système d'extrémité comme n'étant pas en conformité avec la stratégie. L'utilisateur de la console peut ensuite forcer le système d'extrémité à appliquer la stratégie et ainsi rejeter l'exclusion paramétrée localement.

Ligne de commande

Pour exclure un fichier ou un répertoire spécifique, utilisez le paramètre `ExcludeFilePaths`. Par exemple, pour ajouter le fichier `/tmp/report` à la liste des fichiers et répertoires à exclure, saisissez

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

Pour supprimer une exclusion de la liste, utilisez l'opération de suppression. Par exemple, saisissez

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

Interface utilisateur graphique

Pour exclure un fichier ou un répertoire spécifique, allez sur la page **Exclusion Configuration**, dans la zone **File Scanning Exclusions**, saisissez le chemin du fichier ou du répertoire dans la zone de texte **Files or directories**

(with or without wildcards). Cliquez sur **Add New Entry** pour ajouter le chemin à la liste.

Files or directories (with or without wildcards)

Pour supprimer une exclusion de la liste, sélectionnez l'exclusion et cliquez sur **Remove Selected Entry**.

8.1.2 Par type de fichier

- ❗ Une telle spécification des exclusions entraîne un contrôle moins efficace que si les exclusions étaient spécifiées par nom de fichier ou de répertoire, par caractères joker ou expressions usuelles.

Ligne de commande

Pour exclure des fichiers du même type que le fichier spécifique, utilisez le paramètre `ExcludeFilesLike`. Par exemple, pour ajouter le type du fichier `Report.txt` à la liste des types de fichier à exclure, saisissez

```
/opt/sophos-av/bin/savconfig ExcludeFilesLike /home/fred/Report.txt
```

Pour supprimer une exclusion de la liste, utilisez l'opération de suppression. Par exemple, saisissez

```
/opt/sophos-av/bin/savconfig remove ExcludeFilesLike  
/home/fred/Report.txt
```

Pour exclure des fichiers d'un type spécifique, utilisez le paramètre `ExcludeFileType`. Le type de fichier doit impérativement être une valeur retournée par la commande de fichier. (Pour plus d'informations sur la commande du fichier, saisissez `man file`.) Par exemple, pour ajouter des fichiers texte ASCII à la liste des types de fichier à exclure, saisissez

```
/opt/sophos-av/bin/savconfig ExcludeFileType 'ASCII text'
```

Pour supprimer une exclusion de la liste, utilisez l'opération de suppression. Par exemple, saisissez

```
/opt/sophos-av/bin/savconfig remove ExcludeFileType 'ASCII text'
```

- ❗ Sophos Anti-Virus effectue des correspondances partielles des types de fichiers. Ainsi, en commençant par la gauche, il exclut tous les types de fichiers qui correspondent au type de fichiers spécifié et au nombre de caractères du type de fichiers spécifié. Par exemple, 'TIFF' exclut tous les types de fichiers TIFF, tandis que 'TIFF image data, little-endian' exclut uniquement certains types de fichiers TIFF.

Interface utilisateur graphique

Pour exclure des fichiers du même type qu'un fichier donné, sur la page **Exclusion Configuration**, dans la zone **File Scanning Exclusions**, saisissez le chemin du fichier dans la zone de texte intitulée **File type of this file**. Cliquez sur **Add New Entry** pour ajouter le type de fichiers à la liste des types de fichiers à exclure.

File types

File type of this file

File type as returned by the 'file' command

writable. regular file. no read permission
ASCII text. with no line terminators

Pour exclure les fichiers d'un type spécifique, sur la page **Exclusion Configuration**, dans la zone **File Scanning Exclusions**, saisissez le type de fichiers dans la zone de texte intitulée **File type as returned by the 'file' command**. (Pour plus d'informations sur la commande du fichier, saisissez `man file`.) Cliquez sur **Add New Entry** pour ajouter le type de fichiers à la liste.

File types

File type of this file

File type as returned by the 'file' command

writable. regular file. no read permission
ASCII text. with no line terminators

Pour supprimer une exclusion de la liste, sélectionnez l'exclusion et cliquez sur **Remove Selected Entry**.

- ❗ Sophos Anti-Virus effectue des correspondances partielles des types de fichier. Ainsi, en commençant par la gauche, il exclut tous les types de fichiers qui correspondent au type de fichiers spécifié et au nombre de caractères du type de fichiers spécifié. Par exemple, 'TIFF' exclut tous les types de fichiers TIFF, tandis que 'TIFF image data, little-endian' exclut uniquement certains types de fichiers TIFF.

8.1.3 Par caractères joker

- ❗ Si vous utilisez l'Enterprise Console et que votre stratégie antivirus spécifie des exclusions en utilisant des caractères jokers, toutes les exclusions paramétrées localement sur un système d'extrémité entraîneront l'affichage par la console du système d'extrémité comme n'étant pas en conformité avec la stratégie. L'utilisateur de la console peut ensuite forcer le système d'extrémité à appliquer la stratégie et ainsi rejeter l'exclusion paramétrée localement.

Ligne de commande

Pour exclure des fichiers et répertoires en utilisant des caractères joker, utilisez le paramètre `ExcludeFileOnGlob`. Les caractères joker 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 ExcludeFileOnGlob '/tmp/*.txt'
```

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 uniquement les fichiers texte qui existent déjà dans le répertoire `/tmp` à la liste, saisissez

```
/opt/sophos-av/bin/savconfig ExcludeFileOnGlob /tmp/*.txt
```

Pour supprimer une exclusion de la liste, utilisez l'opération de suppression. Par exemple, saisissez

```
/opt/sophos-av/bin/savconfig remove ExcludeFileOnGlob
'/tmp/notes.txt'
```

Interface utilisateur graphique

Pour exclure des fichiers ou des répertoires en utilisant les caractères joker, allez sur la page **Exclusion Configuration**, dans la zone **File Scanning**

Exclusions, saisissez le chemin des fichiers ou répertoires dans la zone de texte **Files or directories (with or without wildcards)**. Les caractères joker valides sont *, qui remplace une séquence quelconque de caractères et ?, qui remplace n'importe quel caractère. Cliquez sur **Add New Entry** pour ajouter le chemin à la liste.



Files or directories (with or without wildcards)

/tmp/*.txt Add New Entry

/usr/fred/report.rtf

Remove Selected Entry

Pour supprimer une exclusion de la liste, sélectionnez l'exclusion et cliquez sur **Remove Selected Entry**.

8.1.4 Spécification du jeu de caractères des noms de répertoires et des noms de fichiers

Linux vous permet d'utiliser tout jeu de caractères de votre choix (par exemple, UTF-8, EUC_jp) pour nommer les répertoires et fichiers. Toutefois, Sophos Anti-Virus archive uniquement les exclusions utilisant des jeux de caractères 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 chiffrés en EUC_cn, spécifiez les noms des répertoires et 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 tous les noms de répertoire et les noms de fichiers spécifiés en UTF-8, EUC_jp, ISO-8859-1 (Latin-1) et en EUC_cn. Il exclut ensuite tous les répertoires et fichiers dont les noms correspondent.

8.2 Exclusion des systèmes de fichiers du contrôle de fichiers

Ligne de commande

Pour exclure les systèmes de fichiers du contrôle de fichiers par type de système de fichiers, utilisez le paramètre `ExcludeFilesystems`. Par défaut, aucun type de système de fichiers n'est exclu. Les types de systèmes de fichiers valides sont répertoriés dans le fichier `/proc/filesystems`. Par exemple, pour ajouter `nfs` à la liste des types de systèmes de fichiers à exclure, saisissez

```
/opt/sophos-av/bin/savconfig ExcludeFilesystems nfs
```

Pour supprimer une exclusion de la liste, utilisez l'opération de suppression. Par exemple, saisissez

```
/opt/sophos-av/bin/savconfig remove ExcludeFilesystems nfs
```

Interface utilisateur graphique

Pour exclure les systèmes de fichiers du contrôle de fichiers par type de systèmes de fichiers, sur la page **Exclusion Configuration**, dans la zone **File Scanning Exclusions**, cliquez sur la flèche du menu déroulant de la boîte **Filesystem types**. Sélectionnez un des types de systèmes de fichiers dans la liste. Cliquez sur **Add New Entry** pour ajouter le type de systèmes de fichiers à la liste.



Pour supprimer une exclusion de la liste, sélectionnez l'exclusion et cliquez sur **Remove Selected Entry**.

8.3 Contrôle du contenu des archives

- ❗ Le contrôle du contenu des fichiers archive ralentit considérablement le contrôle et il est rarement nécessaire. Même si vous n'activez pas l'option, lorsque vous tentez d'accéder à un fichier extrait d'un fichier archive, le fichier extrait est contrôlé.

Ligne de commande

Pour activer le contrôle du contenu des archives, saisissez

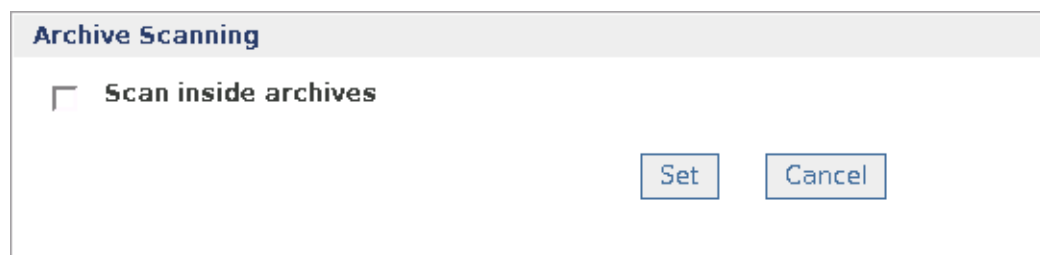
```
/opt/sophos-av/bin/savconfig set ScanArchives enabled
```

Pour désactiver le contrôle du contenu des archives, saisissez

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

Interface utilisateur graphique

Pour configurer le contrôle du contenu des archives, allez sur la page **Scanning Configuration** et dans la zone **Archive Scanning**.



Configurez le contrôle du contenu des archives comme décrit ci-dessous. Dès que vous avez terminé, cliquez sur **Set** pour appliquer les modifications. Pour annuler vos modifications depuis la dernière fois que vous avez cliqué sur **Set**, cliquez sur **Cancel**.

Pour activer le contrôle du contenu des archives, cochez la case **Scan inside archives**.

Pour désactiver le contrôle du contenu des archives, dessélectionnez la case **Scan inside archives**.

8.4 Configuration du nettoyage automatique

Sophos Anti-Virus désinfecte ou supprime automatiquement les éléments infectés lors de l'exécution du contrôle sur accès. Toutes les actions entreprises par Sophos Anti-Virus contre les éléments infectés sont consignées dans le journal de Sophos Anti-Virus. Par défaut, le nettoyage automatique est désactivé.

Ligne de commande

Pour activer la désinfection automatique des fichiers infectés et des secteurs de démarrage, saisissez

```
/opt/sophos-av/bin/savconfig AutomaticAction disinfect
```

La désinfection des documents ne corrige pas toutes les modifications causées par le virus dans le document. (Reportez-vous à la section 5.1 pour savoir comment obtenir plus de détails à propos des effets secondaires des virus sur le site Web de Sophos.)

Pour désactiver la suppression automatique, saisissez

```
/opt/sophos-av/bin/savconfig remove AutomaticAction disinfect
```

Pour activer la suppression automatique des fichiers infectés, saisissez

```
/opt/sophos-av/bin/savconfig AutomaticAction delete
```

- ❗ 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.

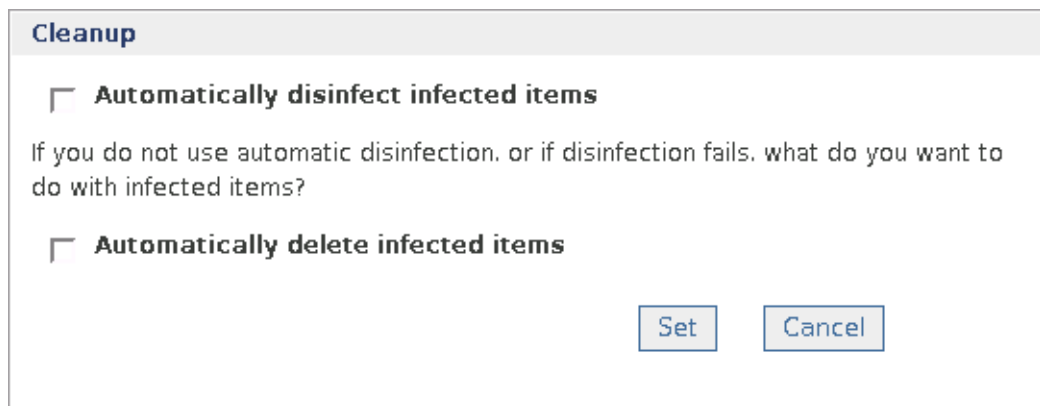
Pour désactiver la suppression automatique, saisissez

```
/opt/sophos-av/bin/savconfig remove AutomaticAction delete
```

Vous pouvez activer la suppression et la désinfection automatiques, cependant Sophos ne vous le recommande pas. Si vous faites cela, Sophos Anti-Virus essaye d'abord de *désinfecter* l'élément. Si la désinfection échoue, il le supprime.

Interface utilisateur graphique

Pour paramétrer le nettoyage automatique, allez sur la page **Scanning**, puis dans la zone **Cleanup**.



Cleanup

Automatically disinfect infected items

If you do not use automatic disinfection, or if disinfection fails, what do you want to do with infected items?

Automatically delete infected items

Set Cancel

Configurez le nettoyage comme décrit ci-dessous. Dès que vous avez terminé, cliquez sur **Set** pour appliquer les modifications. Pour annuler vos modifications depuis la dernière fois que vous avez cliqué sur **Set**, cliquez sur **Cancel**.

Pour activer la désinfection automatique des fichiers et secteurs de démarrage infectés, cochez la case **Automatically disinfect infected items**. La désinfection des documents ne corrige pas toutes les modifications

causées par le virus dans le document. (Reportez-vous à la section 5.1 pour savoir comment obtenir plus de détails à propos des effets secondaires des virus sur le site Web de Sophos.)

Pour activer la suppression automatique des fichiers infectés, cochez la case **Automatically delete infected items**.

- ❗ 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.

Vous pouvez activer la suppression et la désinfection automatiques, cependant Sophos ne vous le recommande pas. Si vous faites cela, Sophos Anti-Virus essaye d'abord de *désinfecter* l'élément. Si la désinfection échoue, il le supprime.

9 Configuration du contrôle à la demande

Dans cette section, lorsque PATH apparaît dans une commande, cela renvoie au chemin à contrôler.

9.1 Contrôle de tous les types de fichier

Par défaut, Sophos Anti-Virus contrôle uniquement les fichiers exécutables. Pour effectuer un contrôle de tous les fichiers, quel que soit leur type, saisissez

```
savscan PATH -all
```

- ❗ Cette opération est plus longue que l'opération de contrôle des exécutables uniquement et elle peut compromettre les performances des serveurs. Cette opération peut aussi générer la création de rapports viraux/spywares erronés.

9.2 Contrôle du contenu des archives

Sophos Anti-Virus peut contrôler le contenu des archives s'il est exécuté avec l'option `-archive`.

```
savscan PATH -archive
```

Les types d'archive pouvant être contrôlés incluent : ARJ, bzip2, CMZ, GZip, RAR, RPM, BZTAR, Zip.

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

Autrement, vous pouvez spécifier le contrôle de types d'archive particuliers. Par exemple, pour contrôler le contenu des archives TAR, saisissez

```
savscan PATH -tar
```

ou pour contrôler le contenu des archives TAR et Zip, saisissez

```
savscan PATH -tar -zip
```

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.

Pour obtenir une liste complète des types d'archive contrôlés, utilisez l'option `-vv`.

9.3 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 activer le contrôle sur les ordinateurs distants, saisissez

```
savscan PATH --no-stay-on-machine
```

9.4 Désactivation du contrôle des éléments avec des liens symboliques

Par défaut, Sophos Anti-Virus contrôle les éléments avec des liens symboliques. Pour désactiver ce type de contrôle, saisissez

```
savscan PATH --no-follow-symlinks
```

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

9.5 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). Saisissez

```
savscan PATH --stay-on-filesystem
```

9.6 Options de ligne de commande

Les options de ligne de commande répertoriées dans cette section vous permettent de configurer le contrôle et la désinfection. Il s'agit

- d'options qu'ont en commun Sophos Anti-Virus pour Linux et Sophos Anti-Virus pour UNIX et autres plates-formes (section 9.6.1)
- d'options qu'ont uniquement en commun Sophos Anti-Virus pour Linux et Sophos Anti-Virus pour UNIX (section 9.6.2)
- d'options spécifiques à Sophos Anti-Virus pour Linux (section 9.6.3).

9.6.1 Options de ligne de commande Sophos Anti-Virus

Pour inverser la signification d'une option de ligne de commande, ajoutez lui le préfixe 'n'. Par exemple, `-nsc` est l'inverse de `-sc`.

Pour afficher une liste de ces options à l'écran, saisissez

```
savscan -h
```

-all Contrôle tous les fichiers

Si cette option est utilisée, Sophos Anti-Virus contrôle tous les fichiers du système de fichiers plutôt que de contrôler uniquement les fichiers exécutables.

- ❗ Cette opération est plus longue que l'opération de contrôle des exécutables uniquement et elle peut compromettre les performances des serveurs. Cette opération peut aussi générer la création de rapports viraux/spywares erronés.

-archive Contrôle le contenu des archives

Si cette option est utilisée, Sophos Anti-Virus contrôle le contenu des archives. Les types d'archive contrôlés incluent : ARJ, bzip2, CMZ, GZip, RAR, RPM, TAR, Zip.

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

Autrement, vous pouvez spécifier le contrôle de types d'archive particuliers. Par exemple, pour contrôler le contenu des archives TAR, saisissez

```
savscan PATH -tar
```

ou pour contrôler le contenu des archives TAR et Zip, saisissez

```
savscan PATH -tar -zip
```

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.

Pour obtenir une liste complète des types d'archive contrôlés, utilisez l'option -vv.

-b Signal sonore lors de la détection d'un virus/spyware

Cette option ordonne à Sophos Anti-Virus d'émettre un signal sonore lors de la découverte de virus/spywares ou de fragments de virus/spywares. Elle est activée par défaut.

-c Demande de confirmation avant la désinfection ou la suppression

Cette option ordonne à Sophos Anti-Virus de demander confirmation avant la désinfection ou la suppression de fichiers. Elle est activée par défaut.

-di Désinfecte

Cette option ordonne à Sophos Anti-Virus de réaliser la désinfection automatique des fichiers de données, programmes et secteurs de démarrage. Reportez-vous à la [section 5.2](#).

-dn Affiche les noms de fichiers lorsqu'ils sont contrôlés

Cette option affiche les fichiers sur lesquels le contrôle est en cours d'exécution. Les informations affichées sont l'heure suivie de l'élément en cours de vérification.

-eec Utilise la série avancée de codes d'erreur

Cette option ordonne à Sophos Anti-Virus d'utiliser une série avancée de codes d'erreur. Pour plus de détails, reportez-vous à la [section 3.6.1](#).

-exclude Exclut des éléments du contrôle

Cette option vous permet de spécifier que tous les éléments (fichiers, répertoires ou systèmes de fichiers) qui suivent l'option sur la ligne de commande doivent être exclus du contrôle.

Suite à l'utilisation de l'option `-exclude`, vous pouvez utiliser l'option `-include` pour spécifier un contrôle des éléments qui suivent cette option sur la ligne de commande.

Par exemple :

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

contrôle les éléments fred, harry et bill, mais pas tom ou peter.

L'option `-exclude` peut être utilisée pour les fichiers ou répertoires sous un autre répertoire. Par exemple :

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

contrôle l'intégralité du répertoire domicile de Fred mais exclut le répertoire jeux du contrôle (ainsi que tous ses sous-répertoires et fichiers).

-ext= Types de fichier définis comme exécutables

Par défaut, Sophos Anti-Virus contrôle les fichiers exécutables DOS et Windows qui portent certaines extensions de fichier (exécutez `savscan` avec l'option `-vv` pour voir la liste des extensions de fichier utilisées).

Pour spécifier davantage d'extensions de fichier à contrôler par Sophos Anti-Virus, utilisez l'option `-ext=` avec une liste des extensions séparées par des virgules.

Pour exempter des extensions de fichier du contrôle, utilisez `-next`.

- 💡 Si vous désirez contrôler des fichiers définis par UNIX comme exécutables, reportez-vous à l'[option `examine-x-bit`](#) de la [section 9.6.2](#).

-f Contrôle total

Par défaut, Sophos Anti-Virus vérifie uniquement les parties de chaque fichier susceptibles de contenir des virus/spywares. Un contrôle 'total' examine le contenu complet de chaque fichier et peut être spécifié en utilisant cette option.

Le contrôle total est plus lent que le contrôle par défaut.

-h Aide

Cette option répertorie toutes les options de la ligne de commande, y compris les options spécifiques à Linux.

-idedir= Utilise un répertoire de remplacement pour les fichiers d'identités de virus/spywares (IDE)

Cette option vous permet de spécifier un répertoire de remplacement pour les IDE. Par exemple :

```
savscan PATH -idedir=/ide
```

ordonne à Sophos Anti-Virus de lire les IDE depuis le répertoire `/ide` plutôt que depuis le répertoire par défaut (généralement `/opt/sophos-av/lib/sav`).

-mime Contrôle les fichiers MIME

Cette option permet à Sophos Anti-Virus de contrôler les fichiers MIME lorsqu'il effectue un contrôle. Par défaut, le contrôle des fichiers MIME n'est **pas** activé.

-oe Contrôle des boîtes aux lettres Outlook Express

Cette option ordonne à Sophos Anti-Virus de contrôler les boîtes aux lettres Outlook Express lorsqu'il effectue un contrôle. Par défaut, le contrôle des boîtes aux lettres Outlook Express n'est **pas** activé. Vous devez aussi utiliser l'option `-mime` avec ce qualificatif.

-p= <file|device> Copie les données de sortie de l'écran sur un fichier/périphérique

Cette option ordonne à Sophos Anti-Virus de transférer toutes les informations transmises à l'écran vers un fichier ou un périphérique spécifique. Par exemple :

```
savscan PATH -p=log.txt
```

ordonne à Sophos Anti-Virus d'envoyer les informations de sortie de l'écran vers le fichier `log.txt`.

-rec Exécute un contrôle récursif

Cette option ordonne à Sophos Anti-Virus de contrôler les répertoires se trouvant en dessous de ceux spécifiés dans la ligne de commande. Elle est activée par défaut.

-remove Supprime les objets infectés

Cette option ordonne à Sophos Anti-Virus de supprimer les éléments infectés.

-s Exécute le contrôle silencieusement sans afficher les zones vérifiées

Si cette option est utilisée, Sophos Anti-Virus n'affiche pas à l'écran les fichiers qu'il contrôle. Elle est activée par défaut.

-sc Contrôle le contenu des fichiers compressés

Si cette option est utilisée, Sophos Anti-Virus recherche les virus/spywares dans les fichiers compressés en utilisant les utilitaires PKLite, LZEXE et Diet. Elle est activée par défaut.

--stop-scan Arrête le contrôle des “bombes zip”

Si cette option est utilisée, Sophos Anti-Virus arrête le contrôle des “bombes zip” lorsqu'elles sont détectées.

- ❓ Les “bombes zip” sont des fichiers malveillants conçus pour perturber le fonctionnement des scanners antivirus. Ces fichiers prennent généralement l'apparence de fichiers archive inoffensifs, qui lorsqu'ils sont extraits pour être contrôlés, nécessitent énormément de temps, d'espace disque ou de mémoire.

Par exemple :

```
savscan -all /home/fred/misc --stop-scan
```

ordonne à Sophos Anti-Virus de contrôler tous les objets (fichiers et répertoires) sous /domicile/fred/misc et d'arrêter le contrôle de toutes les “bombes zip” qui sont détectées. Lorsqu'une “bombe zip” est détectée, un message semblable à

```
Aborted checking /domicile/fred/misc/b.zip - appears  
to be a 'zip bomb'
```

est affiché.

-v Numéro de version

Si cette option est utilisée, Sophos Anti-Virus affiche le numéro de version et une liste des identités de virus/spywares (IDE) en cours d'utilisation.

-vv Informations détaillées

Si cette option est utilisée, Sophos Anti-Virus affiche le numéro de version et les listes des identités de virus/spywares (IDE) en cours d'utilisation, les extensions de fichiers contrôlés et les types d'archive contrôlés.

9.6.2 Options de la ligne de commande spécifiques à UNIX

Les options suivantes sont spécifiques à UNIX et peuvent être pourvues du préfixe 'no-' pour inverser leur signification.

Par exemple, '--no-follow-symlinks' est l'opération inverse de '--follow-symlinks'.

--args-file=[nom de fichier] Lit les arguments de la ligne de commande depuis un fichier

Sophos Anti-Virus lit les arguments de la ligne de commande depuis un fichier. Ces arguments peuvent inclure des (listes de) noms de répertoire, des noms de fichiers et des options. Par exemple :

```
savscan --args-file=scanlist
```

ordonne à Sophos Anti-Virus de lire les arguments de la ligne de commande depuis le fichier `scanlist`. Lorsque Sophos Anti-Virus atteint la fin du fichier, il poursuit la lecture des arguments depuis la ligne de commande.

Si le [nom de fichier] est '-', Sophos Anti-Virus lit les arguments depuis `stdin`. Certaines options par ligne de commande ne peuvent pas être utilisées dans le fichier : `-eec`, `-neec`, `-p=`, `-s`, `-ns`, `-dn` and `-ndn`.

--backtrack-protection Empêche le backtracking

Sophos Anti-Virus évite le contrôle des mêmes fichiers plus d'une fois ('backtracking'), problème pouvant être causé par les liens symboliques. Cette option est activée par défaut.

--examine-x-bit Contrôle tous les éléments qu'UNIX définit comme exécutables

Si cette option est utilisée, Sophos Anti-Virus contrôle tous les éléments qu'UNIX définit comme exécutables ainsi que les éléments dont les extensions de fichiers figurent dans la propre liste des exécutables de Sophos Anti-Virus (pour plus de détails sur la liste des extensions de fichier, exécutez `savscan` à l'aide de l'option `-vv`). Cette option est désactivée par défaut.

--follow-symlinks Contrôle de l'objet signalé par les liens symboliques

Sophos Anti-Virus contrôle les objets signalés par les liens symboliques. Cette option est activée par défaut.

--preserve-backtrack Sauvegarde les informations de backtracking

Sophos Anti-Virus sauvegarde les informations de backtracking pendant toute la durée de l'exécution. Cette option est activée par défaut.

--quarantine Met en quarantaine les fichiers infectés

Si cette option est utilisée, Sophos Anti-Virus met les fichiers infectés en quarantaine. Sophos Anti-Virus effectue cette opération en changeant les droits de propriété et d'accès au fichier.

Si vous avez spécifié la désinfection, Sophos Anti-Virus tente de désinfecter le fichier et met le fichier en quarantaine uniquement lorsque la désinfection échoue.

Par défaut, Sophos Anti-Virus change les droits de propriétés du fichier sur ceux d'un utilisateur exécutant Sophos Anti-Virus ainsi qu'il change les droits d'accès sur `-r-----` (0400).

Vous pouvez utiliser l'option avec des paramètres supplémentaires :

```
uid=NNN
user=NOMUTILISATEUR
gid=NNN
group=NOM-GROUPE
mode=PPP
```

Il n'est pas possible de définir plus d'un paramètre de chaque type (par exemple, vous ne pouvez pas saisir deux fois le même nom utilisateur ou saisir une uid et un nom 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 sophosav et du groupe virus, mais que *seul* l'utilisateur sophosav a accès au fichier (en lecture seulement). Personne d'autre ne peut intervenir sur le fichier (sauf sur la root) de quelque manière que ce soit.

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.

--reset-atime Réinitialiser le temps d'accès aux fichiers

Suite au contrôle d'un fichier, Sophos Anti-Virus réinitialise le temps d'accès (atime) sur le temps affiché avant le début du contrôle. Toutefois, lorsqu'un fichier est désinfecté, les temps d'accès et de modification sont mis à jour. Cette option est activée par défaut.

- ❗ Il se peut que votre archiveur sauvegarde constamment tous les fichiers qui ont été contrôlés. Ceci pourrait être dû à la réinitialisation du temps d'accès (atime) qui entraîne le changement du 'statut modifié' (ctime) de l'inode. Dans ce cas, exécutez savscan à l'aide de l'option --no-reset-atime.

--show-file-details Afficher les détails de la propriété du fichier

Si cette option est utilisée, Sophos Anti-Virus affiche les détails de la propriété et des droits d'accès au fichier lorsque les noms de fichier sont affichés ou écrits dans un journal.

--skip-special Ne pas contrôler les objets 'spéciaux'

Sophos Anti-Virus ne contrôle pas les objets spéciaux tels que /dev, /proc, /devices etc. Cette option est activée par défaut.

--stay-on-filesystem Ne pas quitter le système de fichiers de démarrage

Si cette option est utilisée, Sophos Anti-Virus contrôle uniquement le système de fichiers de démarrage, c'est-à-dire qu'il ne couvre pas les points de montage.

--stay-on-machine Ne pas quitter l'ordinateur de démarrage

Sophos Anti-Virus contrôle uniquement l'ordinateur de démarrage, c'est-à-dire qu'il ne couvre pas les points de montage distants. Cette option est activée par défaut.

9.6.3 Options de la ligne de commande spécifiques à Linux

Les options de contrôle du secteur de démarrage ci-dessous sont uniquement disponibles sur Sophos Anti-Virus pour Linux.

-bs=xxx, xxx,... Contrôle du secteur de démarrage d'un lecteur logique spécifique

Sophos Anti-Virus contrôle les secteurs de démarrage des lecteurs logiques spécifiés, où xxx correspond au nom du lecteur (par exemple /dev/fd0 ou /dev/hda1). Le lecteur de disquette est considéré comme un lecteur logique pour les besoins de cette option.

Vous pouvez utiliser cette option pour contrôler les secteurs de démarrage des disquettes qui ont été créés pour d'autres systèmes d'exploitation (par exemple Windows et DOS).

--bs Contrôle tous les secteurs de démarrage connus

Sophos Anti-Virus procède à l'extraction des informations de la table de partition depuis tous les lecteurs physiques qu'il connaît, puis contrôle les secteurs de démarrage de tous les lecteurs logiques. Le contrôle inclut aussi les secteurs de démarrage non Linux (par exemple Windows et DOS).

-cdr= Contrôle l'image boot du CD-ROM

Pour contrôler l'image boot d'un CD-ROM d'amorçage, utilisez l'option -cdr. Par exemple :

```
savscan -cdr=/dev/cdrom
```

contrôle l'image boot (s'il y en a une) du CD-ROM sur le périphérique /dev/cdrom. Si Sophos Anti-Virus trouve une image boot, il contrôle le secteur de démarrage de cette image à la recherche de virus du secteur de démarrage.

Pour rechercher des virus de programme dans tous les fichiers de l'image boot dont le type de fichiers figure dans la propre liste des exécutables de Sophos Anti-Virus, utilisez l'option -loopback. Par exemple :

```
savscan -cdr=/dev/cdrom -loopback
```

contrôle l'image boot (s'il y en a une) du CD-ROM sur le périphérique /dev/cdrom. Si Sophos Anti-Virus trouve une image boot, il contrôle le secteur de démarrage de cette image à la recherche de virus du secteur de démarrage et recherche les virus de programme dans tous les fichiers de cette image dont le type de fichier figure dans la liste des exécutables.

--mbr Contrôle des enregistrements de démarrage maître

Sophos Anti-Virus tente de contrôler les enregistrements de démarrage maîtres de tous les lecteurs physiques du système.

10 Configuration des alertes

- ❗ Si vous procédez à la configuration d'un ordinateur autonome connecté à un réseau, cette configuration pourrait être rejetée 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 découverte de virus/spywares, d'une erreur du contrôle ou de tout autre type d'erreur. Les alertes peuvent être envoyées en différentes langues et via les méthodes suivantes :

- Alerte de bureau (contrôle sur accès uniquement)
- Ligne de commande (contrôle sur accès uniquement)
- Courriel (contrôle sur accès et contrôle à la demande)

10.1 Configuration des alertes de bureau

Par défaut, les alertes de bureau sont activées. Elles sont envoyées dans la langue de l'ordinateur qui émet l'alerte.

- ❗ Les messages supplémentaires ci-dessous ne sont pas traduits.

Ligne de commande

Pour activer les alertes de bureau, réglez les paramètres UINotifier et UIpopupNotification sur "enabled". UINotifier assure le contrôle total des alertes s'ouvrant sur le bureau et de ligne de commande ; UIpopupNotification contrôle uniquement les alertes s'ouvrant sur le bureau. Par exemple, saisissez

```
/opt/sophos-av/bin/savconfig UINotifier enabled
/opt/sophos-av/bin/savconfig UIpopupNotification enabled
```

Vous pouvez spécifier quel message à envoyer en plus de l'alerte elle-même. Un message par défaut est fourni en anglais. Pour modifier ceci, utilisez le paramètre UIContactMessage. Par exemple, saisissez

```
/opt/sophos-av/bin/savconfig UIContactMessage 'Veuillez contacter
le service informatique'
```

- ❗ Les mêmes messages seront utilisés pour les alertes de bureau et par ligne de commande.

Pour désactiver les alertes de bureau, saisissez

```
/opt/sophos-av/bin/savconfig UIpopupNotification disabled
```

Pour désactiver à la fois les alertes de bureau et celles par ligne de commande, saisissez

```
/opt/sophos-av/bin/savconfig UINotifier disabled
```

Interface utilisateur graphique

Pour configurer les alertes de bureau, allez sur la page **Alerts Configuration** et dans la zone **Desktop Pop-up and Command-line**.



Desktop Pop-up and Command-line

Enable desktop pop-up alerts

Enable command-line alerts

Additional message to be displayed in command-line and desktop pop-up alerts

Please contact your IT department.

Set **Cancel**

Configurez les alertes de bureau comme décrit ci-dessous. Dès que vous avez terminé, cliquez sur **Set** pour appliquer les modifications. Pour annuler vos modifications depuis la dernière fois que vous avez cliqué sur **Set**, cliquez sur **Cancel**.

Pour activer les alertes de bureau, cochez la case **Enable desktop pop-up alerts**.

Vous pouvez spécifier quel message à envoyer en plus de l'alerte elle-même. Un message par défaut est fourni en anglais. Pour le modifier, saisissez du texte dans le champ.

- ❗ Les mêmes messages seront utilisés pour les alertes de bureau et par ligne de commande.

Pour désactiver les alertes de bureau, désélectionnez la case **Enable desktop pop-up alerts**.

10.2 Configuration des alertes par ligne de commande

Par défaut, les alertes par ligne de commande sont activées. Elles sont envoyées dans la langue de l'ordinateur qui émet l'alerte.

- ❗ Les messages supplémentaires ci-dessous ne sont pas traduits.

Ligne de commande

Pour activer les alertes par ligne de commande, réglez les paramètres `UINotifier` et `UIttyNotification` sur "enabled". `UINotifier` assure le contrôle total des alertes s'ouvrant sur le bureau et de ligne de commande,

UIttyNotification contrôle uniquement les alertes par ligne de commande. Par exemple, saisissez

```
/opt/sophos-av/bin/savconfig UINotifier enabled
/opt/sophos-av/bin/savconfig UIttyNotification enabled
```

Vous pouvez spécifier quel message à envoyer en plus de l'alerte elle-même. Un message par défaut est fourni en anglais. Pour modifier ceci, utilisez le paramètre UIContactMessage. Par exemple, saisissez

```
/opt/sophos-av/bin/savconfig UIContactMessage 'Veuillez contacter le service informatique'
```

- ❗ Les mêmes messages seront utilisés pour les alertes de bureau et par ligne de commande.

Pour désactiver les alertes par ligne de commande, saisissez

```
/opt/sophos-av/bin/savconfig UIttyNotification disabled
```

Pour désactiver à la fois les alertes de bureau et celles par ligne de commande, saisissez

```
/opt/sophos-av/bin/savconfig UINotifier disabled
```

Interface utilisateur graphique

Pour configurer les alertes par ligne de commande, allez sur la page **Alerts Configuration** et dans la zone **Desktop Pop-up and Command-line**.

Desktop Pop-up and Command-line

Enable desktop pop-up alerts

Enable command-line alerts

Additional message to be displayed in command-line and desktop pop-up alerts

Please contact your IT department.

Set Cancel

Configurez les alertes par ligne de commande comme décrit ci-dessous. Dès que vous avez terminé, cliquez sur **Set** pour appliquer les modifications. Pour annuler vos modifications depuis la dernière fois que vous avez cliqué sur **Set**, cliquez sur **Cancel**.

Pour activer les alertes par ligne de commande, cochez la case **Enable command-line alerts**.

Vous pouvez spécifier quel message à envoyer en plus de l'alerte elle-même. Un message par défaut est fourni en anglais. Pour le modifier, saisissez du texte dans le champ.

- ❗ Les mêmes messages seront utilisés pour les alertes de bureau et par ligne de commande.

Pour désactiver les alertes par ligne de commande, désélectionnez la case **Enable command-line alerts**.

10.3 Configuration des alertes par courriel

Par défaut, les alertes par courriel sont :

- activées
- envoyées lorsque des virus/spywares sont détectés, qu'il y a une erreur de contrôle ou qu'un événement est consigné dans le journal Sophos Anti-Virus
- envoyées seulement en cas d'événement fatal
- envoyées à root@localhost

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

10.3.1 Paramètres généraux

Ligne de commande

Pour activer les alertes par courriel, réglez le paramètre EmailNotifier sur "enabled":

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

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 EmailServer 171.17.31.184
```

Pour spécifier la langue des alertes par courriel, utilisez le paramètre EmailLanguage. Actuellement, les seules valeurs valides sont "en", "English" ou "Japanese". Par exemple, saisissez

```
/opt/sophos-av/bin/savconfig EmailLanguage Japanese
```

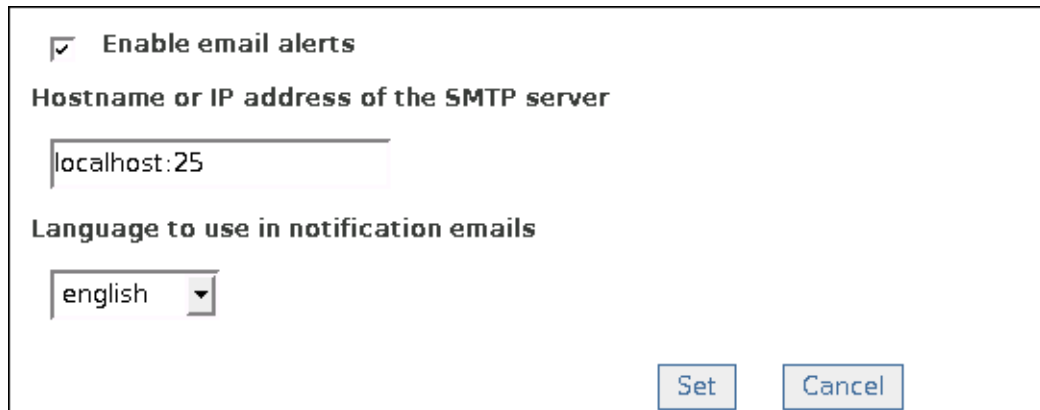
- ❗ Cette sélection s'applique uniquement à l'alerte elle-même, pas aux messages supplémentaires décrits ci-dessous.

Pour désactiver les alertes par courriel, saisissez

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

Interface utilisateur graphique

Pour configurer les alertes par courriel via l'interface utilisateur, allez sur la page **Alerts Configuration** et dans la zone **Email**.



Enable email alerts

Hostname or IP address of the SMTP server

localhost:25

Language to use in notification emails

english

Set Cancel

Pour activer les alertes par courriel, cochez la case **Enable email alerts**.

Pour définir le nom de l'hôte ou l'adresse IP du serveur SMTP, saisissez l'adresse dans la zone de texte **Hostname or IP address of the SMTP server**.

Pour spécifier la langue utilisée par les alertes par courriel, sélectionnez la langue dans la liste du menu déroulant appelée **Language to use in notification emails**.

- ⓘ Cette sélection s'applique uniquement à l'alerte elle-même, pas aux messages supplémentaires décrits ci-dessous.

Pour désactiver les alertes par courriel, dessélectionnez la case **Enable email alerts**.

Dès que vous avez terminé la configuration des alertes par courriel, cliquez sur **Set** pour appliquer les modifications. Pour annuler vos modifications depuis la dernière fois que vous avez cliqué sur **Set**, cliquez sur **Cancel**.

10.3.2 Envoi d'un courriel aux destinataires

Ligne de commande

Pour spécifier qui va recevoir les alertes par courriel, utilisez le paramètre Email. Vous pouvez spécifier un ou plusieurs destinataires. Par exemple, saisissez

```
/opt/sophos-av/bin/savconfig Email admin@localhost
```

Interface utilisateur graphique



Pour spécifier qui va recevoir les alertes par courriel, ajoutez ou supprimez les destinataires de la liste **Email recipients**.

Pour ajouter un nouveau destinataire à la liste, saisissez le texte dans le champ de l'adresse et cliquez sur **Add New Entry**.

Pour supprimer un destinataire, sélectionnez-le et cliquez sur **Remove Selected Entry**.

10.3.3 Que se passe-t-il lorsque des virus/spywares sont détectés

Ligne de commande

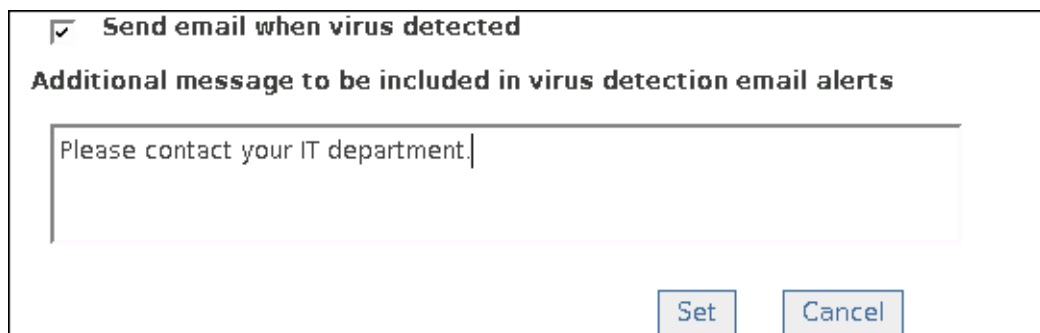
Pour activer l'envoi d'alertes par courriel lors de la détection de virus/spywares, réglez le paramètre SendThreatEmail sur "enabled":

```
/opt/sophos-av/bin/savconfig SendThreatEmail enabled
```

Vous pouvez spécifier quel message envoyer en plus de l'alerte elle-même lorsque des virus/spywares sont détectés. Un message par défaut est fourni en anglais. Pour modifier ceci, utilisez le paramètre ThreatMessage. Par exemple, saisissez

```
/opt/sophos-av/bin/savconfig ThreatMessage en 'Veuillez contacter le service informatique''
```

Interface utilisateur graphique



Pour activer l'envoi des alertes par courriel lors de la détection de virus/spywares, sélectionnez la case **Send email when virus detected**.

Vous pouvez spécifier quel message envoyer en plus de l'alerte elle-même lorsque des virus/spywares sont détectés. Un message par défaut est fourni en anglais. Pour le modifier, saisissez du texte dans le champ.

Dès que vous avez terminé la configuration des alertes par courriel, cliquez sur **Set** pour appliquer les modifications. Pour annuler vos modifications depuis la dernière fois que vous avez cliqué sur **Set**, cliquez sur **Cancel**.

10.3.4 Que se passe-t-il en cas d'une erreur de contrôle ?

Ligne de commande

Pour activer l'envoi d'alertes par courriel lors d'une erreur du contrôle, réglez le paramètre `SendErrorMessage` sur "enabled":

```
/opt/sophos-av/bin/savconfig SendErrorMessage enabled
```

Vous pouvez spécifier quel message envoyer en plus de l'alerte elle-même en cas d'erreur du contrôle. Un message par défaut est fourni en anglais. Pour modifier ceci, utilisez le paramètre `ScanErrorMessage`. Par exemple, saisissez

```
/opt/sophos-av/bin/savconfig ScanErrorMessage 'Veuillez contacter le service informatique'
```

Interface utilisateur graphique

The screenshot shows a configuration window with a checked checkbox labeled "Send email when there is a scan error". Below it is a section titled "Additional message to be included in scan error email alerts" containing a text input field with the text "Please contact your IT department." At the bottom right of the window are two buttons: "Set" and "Cancel".

Pour activer l'envoi des alertes par courriel lors d'une erreur de contrôle, cochez la case **Send email when there is a scan error**.

Vous pouvez spécifier quel message envoyer en plus de l'alerte elle-même en cas d'erreur du contrôle. Un message par défaut est fourni en anglais. Pour le modifier, saisissez du texte dans le champ.

Dès que vous avez terminé la configuration des alertes par courriel, cliquez sur **Set** pour appliquer les modifications. Pour annuler vos modifications depuis la dernière fois que vous avez cliqué sur **Set**, cliquez sur **Cancel**.

10.3.5 Que se passe-t-il lorsqu'un évènement est journalisé ?

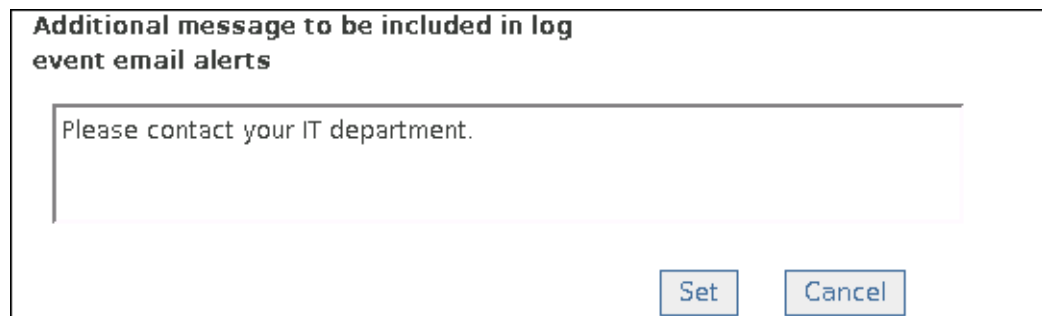
Ligne de commande

Vous pouvez spécifier quel message envoyer en plus de l'alerte elle-même lorsqu'un évènement est consigné dans le journal Sophos Anti-Virus. Un

message par défaut est fournit en anglais. Pour modifier ceci, utilisez le paramètre LogMessage. Par exemple, saisissez

```
/opt/sophos-av/bin/savconfig LogMessage 'Veuillez contacter le service informatique''
```

Interface utilisateur



The screenshot shows a dialog box titled "Additional message to be included in log event email alerts". Inside the dialog, there is a text input field containing the message "Please contact your IT department.". At the bottom right of the dialog, there are two buttons: "Set" and "Cancel".

Vous pouvez spécifier quel message envoyer par courriel lorsqu'un évènement est consigné dans le journal Sophos Anti-Virus. Un message par défaut est fournit en anglais. Pour le modifier, saisissez du texte dans le champ.

Dès que vous avez terminé la configuration des alertes par courriel, cliquez sur **Set** pour appliquer les modifications. Pour annuler vos modifications depuis la dernière fois que vous avez cliqué sur **Set**, cliquez sur **Cancel**.

11 Configuration du journal de Sophos Anti-Virus

- ❗ Si vous procédez à la configuration d'un ordinateur autonome connecté à un réseau, cette configuration pourrait être rejetée 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 Sophos Anti-Virus. Lorsque celui-ci atteint la taille de 1 Mo, il est automatiquement sauvegardé 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, saisissez

```
/opt/sophos-av/bin/savconfig LogMaxSizeMB 50
```

Le chemin du journal est `/opt/sophos-av/log/savd.log`.

12 Configuration de l'interface utilisateur de Sophos Anti-Virus

- ❗ Si vous procédez à la configuration d'un ordinateur autonome connecté à un réseau, cette configuration pourrait être rejetée si l'ordinateur télécharge une nouvelle configuration depuis la console ou depuis le CID.

Vous pouvez configurer l'interface utilisateur de Sophos Anti-Virus en utilisant

- l'utilitaire `savsetup`, ou
- la commande `savconfig`.

savsetup

1. Sur l'ordinateur, exécutez l'utilitaire `savsetup`, qui se trouve dans le sous-répertoire `bin` de l'installation :

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

2. L'utilitaire vous demande de sélectionner ce que vous voulez faire. Sélectionnez **Sophos Anti-Virus GUI configuration**.
3. L'utilitaire vous pose une série de questions à propos de l'interface utilisateur. Saisissez vos réponses pour configurer l'interface utilisateur.

savconfig

Pour définir le port http sur lequel va s'exécuter l'interface utilisateur, utilisez le paramètre `HttpPort`. (L'interface utilisateur n'est pas accessible par le biais d'un port externe.) Pour voir le port par défaut, saisissez

```
/opt/sophos-av/bin/savconfig -s query HttpPort
```

Pour changer le port, saisissez par exemple

```
/opt/sophos-av/bin/savconfig HttpPort 1880
```

Pour définir le nom utilisateur de l'interface utilisateur, utilisez le paramètre `HttpUsername`. Par exemple, saisissez

```
/opt/sophos-av/bin/savconfig HttpUsername sysadmin
```

Pour définir le mot de passe de l'interface utilisateur, utilisez le paramètre `HttpPassword`. Par exemple, saisissez

```
/opt/sophos-av/bin/savconfig HttpPassword 0jf09jf
```

Ces paramètres s'appliquent au redémarrage du programme daemon de l'interface utilisateur. Pour lancer cette opération manuellement, fermez l'interface utilisateur et à la ligne de commande, saisissez

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

Mise à jour de Sophos Anti-Virus

Mise à jour immédiate de Sophos Anti-Virus

Support technique du noyau

Configuration de la mise à jour

13 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.

Pour mettre à jour un ordinateur entre les mises à jour régulières, exécutez le script de mise à jour :

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

14 Support technique du noyau

14.1 Support technique pour les nouvelles publications 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. Si vous appliquez une mise à jour du noyau Linux *avant* d'appliquer la mise à jour correspondante du module d'interface noyau Sophos, le contrôle sur accès est désactivé et une erreur est signalée.

Pour éviter ce problème, assurez-vous que la mise à jour correspondante du module d'interface noyau Sophos 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

(www.sophos.fr/support/knowledgebase/article/14377.html). Si la la mise à jour correspondante du module d'interface noyau Sophos est répertoriée, ceci signifie qu'elle est disponible au téléchargement. Sophos Anti-Virus télécharge automatiquement la mise à jour à condition d'avoir activé la mise à jour automatique lors de l'installation. Autrement, pour mettre à jour un ordinateur entre les mises à jour régulières, exécutez le script de mise à jour :

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

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

14.2 Support technique des noyaux personnalisés

Si vous personnalisez vos noyaux Linux, ce manuel ne vous explique pas comment configurer la mise à jour pour les prendre en charge. Reportez-vous à l'article 13503 de la base de connaissances du support Sophos (www.sophos.fr/support/knowledgebase/article/13503.html).

15 Configuration de la mise à jour

- ❗ Si vous administrez Sophos Anti-Virus pour Linux à l'aide de l'Enterprise Console, utilisez celle-ci pour configurer la mise à jour. Pour de plus amples informations sur la manière de procéder, reportez-vous à l'aide de la console plutôt qu'à ce chapitre.

15.1 Principes 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 systèmes d'extrémité de mise à jour, selon la manière dont vous déployez Sophos Anti-Virus sur le réseau.

Système d'extrémité de mise à jour

Un *système d'extrémité de mise à jour* est un ordinateur sur lequel vous avez installé Sophos Anti-Virus pour Linux 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.

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

1. Sur l'ordinateur que souhaitez vérifier, exécutez l'utilitaire savsetup :

```
/opt/sophos-av/bin/savsetup
```
2. L'utilitaire vous demande de sélectionner ce que vous voulez faire. Sélectionnez **Auto-updating configuration**.
3. L'utilitaire vous demande de sélectionner ce que vous voulez faire. Sélectionnez **Display update configuration** pour voir la configuration actuelle.

15.3 Configuration du serveur de mise à jour pour une mise à jour directement depuis Sophos

1. Sur le serveur de mise à jour, exécutez l'utilitaire savsetup :

```
/opt/sophos-av/bin/savsetup
```
2. L'utilitaire vous demande de sélectionner ce que vous voulez faire. Sélectionnez **Auto-updating configuration**.
3. L'utilitaire vous demande de sélectionner ce que vous voulez faire. Sélectionnez l'option pour définir Sophos comme la source de mise à jour principale. Lorsque vous y êtes invité, saisissez le nom utilisateur et le mot de passe inclus dans votre licence.
4. L'utilitaire vous demande s'il vous faut un proxy pour accéder à Sophos. Si c'est le cas, saisissez "Y" puis saisissez les détails du proxy.

15.4 Configuration de multiples systèmes d'extrémité de mise à jour pour une mise à jour depuis le serveur de mise à jour

- ❗ Si vous désirez modifier la configuration d'un système d'extrémité de mise à jour autonome, reportez-vous plutôt à la [section 15.6](#).

Sur le serveur de mise à jour, procédez à la mise à jour du fichier de configuration hors ligne dans le CID, puis appliquez les modifications au fichier de configuration en ligne, afin que les systèmes d'extrémité 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.

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
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
PrimaryUpdateUsername 'fred'
/opt/sophos-av/bin/savconfig -f CONFIG-FILE -c
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
  PrimaryUpdateProxyAddress 'http://www-cache.xyz.com:8080'
/opt/sophos-av/bin/savconfig -f CONFIG-FILE -c
  PrimaryUpdateProxyUsername 'penelope'
/opt/sophos-av/bin/savconfig -f CONFIG-FILE -c
  PrimaryUpdateProxyPassword 'fj202jrjf'
```

4. Utilisez l'utilitaire `addcfg` pour appliquer les modifications au fichier de configuration en ligne, afin que les systèmes d'extrémité de mise à jour puissent les télécharger à leur prochaine mise à jour.

```
/opt/sophos-av/update/cache/Primary/addcfg.sh -f CONFIG-FILE
```

15.5 Configuration de multiples systèmes d'extrémité de mise à jour pour la mise à jour directement depuis Sophos en cas d'indisponibilité du serveur de mise à jour

- 🔗 Si vous désirez modifier la configuration d'un système d'extrémité de mise à jour autonome, reportez-vous plutôt à la [section 15.7](#).

Sur le serveur de mise à jour, procédez à la mise à jour du fichier de configuration hors ligne dans le CID, puis appliquez les modifications au fichier de configuration en ligne, afin que les systèmes d'extrémité 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.

1. Définissez l'adresse de la source de mise à jour secondaire sur “sophos:” à l'aide du paramètre `SecondaryUpdateSourcePath`. Par exemple, saisissez

```
/opt/sophos-av/bin/savconfig -f CONFIG-FILE -c
  SecondaryUpdateSourcePath 'sophos:'
```

2. Définissez le nom utilisateur de la source de mise à jour secondaire en utilisant celui fourni dans votre licence à l'aide du paramètre `SecondaryUpdateUsername`. Par exemple, saisissez

```
/opt/sophos-av/bin/savconfig -f CONFIG-FILE -c
  SecondaryUpdateUsername 'cust123'
```

3. Définissez le mot de passe de la source de mise à jour secondaire en utilisant celui fourni dans votre licence à l'aide du paramètre `SecondaryUpdatePassword`. Par exemple, saisissez

```
/opt/sophos-av/bin/savconfig -f CONFIG-FILE -c
  SecondaryUpdatePassword 'j23rjjfwj'
```

4. Si vous accédez à Internet via un proxy, définissez l'adresse, le nom utilisateur et le mot de passe du serveur proxy respectivement à l'aide des paramètres `SecondaryUpdateProxyAddress`, `SecondaryUpdateProxyUsername` et `SecondaryUpdateProxyPassword`. Par exemple, saisissez

```
/opt/sophos-av/bin/savconfig -f CONFIG-FILE -c
SecondaryUpdateProxyAddress 'http://www-cache.xyz.com:8080'

/opt/sophos-av/bin/savconfig -f CONFIG-FILE -c
SecondaryUpdateProxyUsername 'fred'

/opt/sophos-av/bin/savconfig -f CONFIG-FILE -c
SecondaryUpdateProxyPassword 'fj202jrjf'
```

5. Utilisez l'utilitaire `addcfg` pour appliquer les modifications au fichier de configuration en ligne, afin que les systèmes d'extrémité de mise à jour puissent les télécharger à leur prochaine mise à jour.

```
/opt/sophos-av/update/cache/Primary/addcfg.sh -f CONFIG-FILE
```

15.6 Configuration d'un système d'extrémité de mise à jour autonome pour une mise à jour depuis le serveur de mise à jour

- ❗ Si vous désirez modifier la configuration de multiples systèmes d'extrémité de mise à jour, reportez-vous plutôt à la [section 15.4](#).

Ce chapitre suppose que le serveur de mise à jour va être la source de mise à jour *principale* de cet ordinateur. Toutefois, s'il est la source de mise à jour *secondaire*, utilisez les options ou paramètres secondaires lorsqu'indiqué ci-dessous.

1. Sur l'ordinateur que souhaitez configurer, exécutez l'utilitaire `savsetup` :

```
/opt/sophos-av/bin/savsetup
```
2. L'utilitaire vous demande de sélectionner ce que vous voulez faire. Sélectionnez **Auto-updating configuration**.
3. L'utilitaire vous demande de sélectionner ce que vous voulez faire. Sélectionnez l'option afin de configurer votre propre serveur comme source de mise à jour principale (ou secondaire). Lorsque vous y êtes invité, 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 ou un chemin UNC, selon la manière dont vous avez paramétré le serveur de mise à jour.
4. L'utilitaire vous demande s'il vous faut un proxy pour accéder à Sophos. Si c'est le cas, saisissez "Y" puis saisissez les détails du proxy.

