SOPHOS

Cybersecurity made simple.

Sophos for Virtual Environments

Guide de configuration pour les utilisateurs de l’Enterprise Console

Table des matières

1 À propos de ce guide

Ce guide vous indique la marche à suivre pour configurer Sophos for Virtual Environments.

Ce guide suppose que vous utilisez Sophos Enterprise Console pour administrer votre logiciel de sécurité.

Remarque
Si vous utilisez Sophos Central, veuillez plutôt consulter l'édition Sophos Central de ce guide de configuration.

2 Configuration des stratégies

Vous configurez Sophos for Virtual Environments avec les stratégies de Sophos Enterprise Console.

Lorsque vous mettez votre Sophos Security VM dans un groupe Sophos Enterprise Console, les stratégies de protection et de mise à jour des machines virtuelles clientes sont appliquées.

Nous vous conseillons d'utiliser les paramètres par défaut car ils vous garantissent le meilleur compromis entre la protection et les bonnes performances de votre système. Toutefois, vous pouvez changer les paramètres dans ces stratégies :

- Antivirus et HIPS
- Mise à jour

Les autres stratégies de Sophos Enterprise Console ne s'appliquent pas à Sophos Security VM.

Remarque
Toutes les machines virtuelles clientes protégées par Sophos Security VM utilisent les mêmes stratégies que celles de Sophos Security VM. Pour appliquer une stratégie différente à certaines machines virtuelles clientes, déplacez les sur une autre Sophos Security VM dans un autre groupe Sophos Enterprise Console. Appliquez ensuite une stratégie différente à ce groupe. Retrouvez plus d'instructions sur le déplacement de machines virtuelles clientes dans le Guide de démarrage de Sophos for Virtual Environments : édition Enterprise Console.

Retrouvez une liste de toutes les machines virtuelles clientes administrées par Sophos Security VM à la section Affichage des machines virtuelles clientes protégées (page 11).

2.1 Stratégie antivirus et HIPS

Par défaut, Sophos Security VM :

- Contrôle les fichiers lors de leur accès sur les machines virtuelles clientes.
- Bloque l'accès aux fichiers infectés.
- Nettoie automatiquement les menaces détectées.

Les paramètres de stratégie antivirus et HIPS ne s'appliquent pas tous à Sophos Security VM. Cette section décrit les options de contrôle qui s'appliquent et qui peuvent être configurées de manière centralisée.

Retrouvez plus de renseignements sur les paramètres dans l'Aide de Sophos Enterprise Console.

Contrôle sur accès

Les paramètres de contrôle sur accès sont pris en charge comme indiqué ci-dessous. La surveillance des comportements n'est pas prise en charge.

Pour ouvrir les pages des paramètres du contrôle sur accès dans Sophos Enterprise Console :

1. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**.
2. Cliquez deux fois sur la stratégie que vous désirez modifier.

3. Dans la boîte de dialogue **Stratégie antivirus et HIPS**, allez dans le panneau **Contrôle sur accès**. À côté du champ **Activer le contrôle sur accès**, cliquez sur **Configurer**.

   La boîte de dialogue d6es **Paramètres du contrôle sur accès** apparaît.

Les options de chaque onglet sont indiquées ci-dessous.

Contrôle	Compatible	Remarques
Vérifier les fichiers À la lecture/Au moment de renommer/À l'écriture	Non	Si une ou plusieurs options sont activées, Sophos Security VM contrôle les trois cas de figure. **Si les trois options sont désactivées, votre système n'est plus protégé.**
Rechercher les Adwares et PUA/Fichiers suspects	Non	
Autoriser l'accès aux lecteurs aux secteurs de démarrage infectés	Non	
Contrôler dans les fichiers archive (déconseillé)	Oui	
Contrôler la mémoire système	Non	

Extensions	Compatible	Remarques
Contrôler tous les fichiers (déconseillé)	Oui	
Contrôler uniquement les exécutables et autres fichiers vulnérables	Oui	
Extensions des types de fichiers supplémentaires à contrôler	Oui	
Contrôler les fichiers sans extension	Oui	
Exclure des types de fichiers du contrôle	Oui	

Exclusions	Compatible	Remarques
Onglet Exclusions Windows	Oui	Pour exclure un dossier, vous devez indiquer le chemin complet, notamment la lettre du lecteur ou le nom du partage réseau comme par exemple ; « C:\Outils\logs \ » ou « \\Serveur\Outils\logs\ ». Retrouvez plus de renseignements à ce sujet à la section sur la configuration de la stratégie antivirus et HIPS dans l'Aide de Sophos Enterprise Console.
Onglet Exclusions Mac	Non	
Onglet Exclusions Linux/UNIX	Non	

Nettoyage	Compatible	Remarques
Nettoyage des virus/spywares	Oui	Les actions alternatives à appliquer si l'échec du nettoyage n'a aucun effet. Sophos Security VM refuse toujours l'accès aux éléments infectés.
Nettoyage des fichiers suspects	Non	

Retrouvez plus de renseignements sur les paramètres à choisir dans l'Aide de Sophos Enterprise Console.

Contrôle planifié

Pour créer ou modifier un contrôle planifié :

- Dans la boîte de dialogue **Stratégie antivirus et HIPS**, allez dans le panneau **Contrôle planifié**.
- Cliquez sur **Ajouter** ou sur **Modifier**.

Vous pouvez également indiquer d'autres types de fichier à contrôler ou exclure des éléments du contrôle en cliquant sur **Extensions et exclusions**.

Les paramètres du contrôle planifié sont pris en charge comme indiqué ci-dessous.

Allez dans **Ajouter/Modifier > Paramètres du contrôle planifié**.

Paramètres du contrôle planifié	Compatible	Remarques
Disques durs locaux	Oui	
Disquettes et lecteurs amovibles	Oui	
Lecteurs de CD-ROM	Oui	
Planification du contrôle	Oui	Sophos Security VM Commence à contrôler à l'heure planifiée. Par défaut, le contrôle est uniquement effectué sur deux machines virtuelles clientes à la fois afin de limiter l'impact sur les performances du système.

Allez dans **Ajouter/Modifier > Paramètres du contrôle planifié > Configurer > Paramètres du contrôle et de nettoyage**

Contrôle et nettoyage	Compatible	Remarques
Onglet Contrôle		
Rechercher les Adwares et PUA/Fichiers suspects/Rootkits	Non	
Contrôler dans les fichiers archive	Oui	
Contrôler la mémoire système	Non	La mémoire du système est contrôlée par défaut. Vous ne pouvez pas configurer cette option.
Exécuter le contrôle avec une priorité inférieure	Non	
Onglet Nettoyage		
Nettoyage des virus/spywares	Oui	Sophos Security VM ne nettoie pas automatiquement les lecteurs de disquette, les lecteurs de CD-ROM ou les emplacements réseau. Les actions sur les éléments infectés n'ont aucun effet si l'opération de nettoyage n'a pas eu lieu. Sophos Security VM journalise toujours l'événement même si l'opération d'élimination n'a pas eu lieu.
Nettoyage des adwares et PUA	Non	
Nettoyage des fichiers suspects	Non	

Allez dans **Extensions et exclusions > Extensions et exclusions du contrôle planifié**.

Extensions et exclusions	Compatible	Remarques
Onglet Extensions		
Contrôler tous les fichiers (déconseillé)	Oui	
Contrôler uniquement les exécutables et autres fichiers vulnérables	Oui	
Extensions des types de fichiers supplémentaires à contrôler	Oui	
Contrôler les fichiers sans extension	Oui	
Exclure des types de fichiers du contrôle	Oui	
Onglet Exclusions		
Onglet Exclusions Windows	Oui	Pour exclure un dossier du contrôle, vous devez indiquer le chemin complet, notamment la lettre du lecteur ou le nom du partage réseau comme par exemple ; « C:\Outils\logs\ » ou « \\Serveur\Outils\logs\ ». Retrouvez plus de renseignements dans l'Aide de Sophos Enterprise Console.
Onglet Exclusions Mac	Non	
Onglet Exclusions Linux/UNIX	Non	

Sophos Live Protection

Sophos Live Protection vérifie la présence de fichiers suspects en consultant la base de données des SophosLabs recensant les malwares les plus récents.

Option	Compatible	Remarques
Activer Sophos Live Protection	Oui	
Activer Sophos Live Protection pour le contrôle à la demande	Oui	
Envoyer automatiquement des fichiers échantillons à Sophos	Non	

Protection Web

Non pris en charge.

Autorisation

L'autorisation, ainsi que la détection, des adwares et autres applications potentiellement indésirables (PUA) n'est pas prise en charge.

Messagerie

Seule la messagerie électronique est prise en charge.

2.1.1 Extensions de fichier contrôlées

Les fichiers avec les extensions suivantes sont contrôlés par défaut.

386 3gr add ani asp aspx asx bat cab chm class cmd com cpl dbx dex dll dmd doc docm	docx dot drv eml exe fas flt fon fot hlp ht? hta html i13 ifs inf ini jar jpeg jpg	Jpz js jse lnk lsp mnl mod mpd mpp mpt mso mui nws o ocx ov? pdf pdr php pif	pl pot pps ppt pptm pptx prc rtf scr sh shb shs src swf sys tif tiff vb? vlx vs?	vxd wbk wma wmf wsf xl? xlsm xlsx xsn zip zipx

Les extensions de fichier suivantes sont contrôlées par défaut si l'option **Contrôler dans les fichiers archive** est activée dans la stratégie antivirus et HIPS appliquée à la machine virtuelle de sécurité.

7z 7zip ??_ a arj bin bz2 gz hqx hxs	lha lzh rar rpm tar taz tbz tbz2 tgz uue z

Vous pouvez ajouter des extensions supplémentaires pour le contrôle ou exclure des extensions du contrôle conformément aux instructions de la section de configuration de la stratégie antivirus et HIPS dans l'Aide de Sophos Enterprise Console.

2.2 Stratégie de mise à jour

Tous les paramètres de la stratégie de mise à jour de Sophos Enterprise Console s'applique à Sophos Security VM.

Retrouvez plus de renseignements dans l’Aide de Sophos Enterprise Console sous **Mise à jour des ordinateurs > Configuration de la stratégie de mise à jour**.

3 Vérification de la protection des machines virtuelles clientes

Cette section vous indique comment vous assurer que vos machines virtuelles clientes sont protégées. Vous pouvez :

- Vérifier les paramètres de protection sur une machine virtuelle cliente.
- Tester le contrôle en temps réel sur une machine virtuelle cliente.
- Résoudre les problèmes du contrôle en temps réel.

3.1 Vérification des paramètres de protection

Pour vérifier qu'une machine virtuelle cliente est protégée ?

1. Rendez-vous sur la machine virtuelle cliente et recherchez **Sécurité et maintenance** dans le menu Démarrer. Si vous ne trouvez pas cette option, recherchez **Centre d'actions**.

   Attention
   Si aucune de ces options n'est disponible, ceci signifie que le Centre de sécurité Windows n'est pas présent sur la machine virtuelle cliente. Assurez-vous que la machine virtuelle cliente est protégée en suivant les instructions de la section Test du contrôle en temps réel (page 8).

2. Cliquez sur la flèche du menu déroulant à côté de **Sécurité**. Vous devriez voir que Sophos for Virtual Environments est activé.

   Remarque
   S'il n'est pas activé, veuillez-vous reporter à la section Résolution des problèmes du contrôle sur accès (page 9)

3.2 Test du contrôle en temps réel

Le contrôle en temps réel est la méthode principale de protection à utiliser contre les menaces. Lorsque vous ouvrez, écrivez, déplacez ou renommez un fichier, Sophos Security VM contrôle et accorde l'accès à ce fichier uniquement s'il ne représente pas une menace. Lorsque vous exécutez un programme, Sophos Security VM contrôle le fichier exécutable et tous les autres fichiers qu'il charge.

Important
Assurez-vous que Sophos Endpoint pour Windows n'est *pas* installé sur l'une des machines virtuelles clientes protégées par Sophos Security VM.

Pour vérifier qu'une machine virtuelle de sécurité effectue bien le contrôle des fichiers sur accès :

1. Rendez-vous sur eicar.org/86-0-Intended-use.html. Copiez la chaîne de caractères du test EICAR dans un nouveau fichier. Nommez le fichier avec une extension .com et enregistrez-le sur l'une des machines virtuelles clientes.
2. Essayez d'accéder au fichier à partir de la machine virtuelle cliente.
3. Dans Sophos Enterprise Console, dans la liste des ordinateurs se trouvant dans la partie inférieure droite de la fenêtre, cliquez sur l'onglet **État**.
4. Dans la liste des ordinateurs, recherchez la machine virtuelle de sécurité.
   - **Si le nettoyage automatique est activé**, cliquez deux fois sur la machine virtuelle de sécurité pour ouvrir la boîte de dialogue **Détails de l'ordinateur**. Dans la section « Historique », vous devriez voir que EICAR a été détecté et nettoyé.
   - **Si le nettoyage automatique n'est pas activé**, vous devriez voir une alerte dans la colonne **Alertes et erreurs**. Cliquez avec le bouton droit de la souris sur la machine virtuelle de sécurité. Dans la boîte de dialogue **Résoudre les alertes et les erreurs**, vous devriez voir que EICAR a été détecté et nettoyé.

Si EICAR n'a pas été détecté, veuillez-vous reporter à la section Résolution des problèmes du contrôle sur accès (page 9). Si EICAR n'a pas été éliminé, veuillez le supprimer.

3.3 Résolution des problèmes du contrôle sur accès

Si le contrôle sur accès ne fonctionne pas :

1. Assurez-vous que Sophos Security VM est dans un groupe dont la stratégie antivirus indique que le contrôle sur accès doit être activé :
   a) Dans le volet **Groupes** de l'Enterprise Console, cliquez avec le bouton droit de la souris sur le groupe dans lequel se trouve Sophos Security VM et sélectionnez **Voir/Modifier les détails de la stratégie du groupe**. Vérifiez quelle stratégie antivirus et HIPS est utilisée.
   b) Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**.
   c) Cliquez deux fois sur la stratégie utilisée par le groupe dans lequel se trouve Sophos Security VM.
   d) Dans le volet **Contrôle sur accès**, sélectionnez la case à cocher **Activer le contrôle sur accès**. Cliquez sur **OK**.
   e) Dans la liste des ordinateurs, cliquez avec le bouton droit de la souris sur la machine virtuelle de sécurité et sélectionnez **Mettre en conformité avec**. Puis, sélectionnez **Stratégie antivirus et HIPS du groupe**.
   f) Assurez-vous que Sophos Security VM est conforme à la stratégie.
2. Assurez-vous que la machine virtuelle cliente est protégée. Sur l'hôte de Sophos Security VM, consultez le fichier journal.
3. Assurez-vous que le Centre de sécurité Windows indique que la machine virtuelle cliente est protégée par Sophos for Virtual Environments.
4. Vérifiez qu'il n'y a aucun redémarrage en file d'attente requis pour appliquer les mises à jour de Microsoft. En effet, ceci pourrait empêcher l'installation de Sophos Guest VM Agent.
5. Assurez-vous qu'aucun autre produit antivirus n'est installé. Pour les plates-formes serveur sur lesquelles le centre de sécurité n'est pas présent, assurez-vous que Windows Defender n'est pas activé. En effet, vous ne pouvez pas utiliser Sophos for Virtual Environments pour protéger les machines virtuelles clientes exécutant d'autres produits antivirus.

6. Si le contrôle sur accès ne fonctionne toujours pas, veuillez contacter le support technique de Sophos.

4 Affichage des machines virtuelles clientes protégées

Vous pouvez afficher toutes les machines virtuelles clientes protégées par Sophos Security VM.

1. Naviguez jusqu'à Sophos Security VM. Veuillez impérativement utiliser l'Explorateur Windows et l'adresse IP.
2. Cliquez deux fois sur le partage **Journaux**.
3. Saisissez vos codes d'accès :
   - Le nom d'utilisateur est « Sophos ».
   - Le mot de passe est celui que vous avez créé lorsque vous avez installé Sophos Security VM.
4. Ouvrez **ProtectedGVMs.log** pour afficher les machines virtuelles clientes protégées.

   Remarque : le fichier ProtectedGVMs.log apparaît uniquement lorsque Sophos Security VM commence à protéger les machines virtuelles clientes.

5 Contrôle des machines virtuelles clientes

Sophos pour Virtual Environments contrôle les fichiers sur accès, c'est-à-dire lors de leur ouverture et de leur fermeture (si le contrôle sur accès est activé dans votre stratégie).

Sophos Security VM peut également effectuer un contrôle intégral de toutes les machines virtuelles clientes qu'elle administre. Vous avez la possibilité d'effectuer un contrôle immédiat ou planifié.

Le contrôle intégral du système détecte les menaces mais ne les élimine pas.

Remarque
Sophos Security VM ne peut pas effectuer un contrôle si elle est toujours dans le groupe **Non affectés** de Sophos Enterprise Console. Elle doit être dans un groupe auquel vous avez appliqué des stratégies.

Remarque
Sophos Security VM procède à des contrôles décalés afin que l'hyperviseur ne soit pas soumis à une trop forte charge de travail. Par défaut, le contrôle est effectué sur deux machines virtuelles clientes à la fois. Le contrôle d'un grand nombre de machines virtuelles clientes peut prendre énormément de temps.

Contrôle immédiat des machines virtuelles clientes

Pour exécuter un contrôle intégral immédiat de toutes les machines virtuelles clientes :

1. Dans Sophos Enterprise Console, recherchez Sophos Security VM dans la liste des ordinateurs.
2. Cliquez avec le bouton droit de la souris sur Sophos Security VM et sélectionnez **Contrôle intégral du système**.

Remarque
Autrement, dans le menu **Actions**, sélectionnez **Contrôle intégral du système**.

Contrôle planifié des machines virtuelles clientes

Pour exécuter un contrôle intégral planifié de toutes les machines virtuelles clientes :

1. Rendez-vous sur Sophos Enterprise Console.
2. Créez un contrôle planifié, conformément aux explications de la section sur la configuration d'une stratégie antivirus et HIPS de l'Aide de Sophos Enterprise Console.

Pour voir les détails du contrôle suite à son exécution :

Dans Sophos Enterprise Console, dans la liste des ordinateurs de la partie inférieure droite de la fenêtre, cliquez deux fois sur Sophos Security VM pour afficher la boîte de dialogue **Détails de l'ordinateur**.

6 Informations sur une menace

Pour obtenir plus de renseignements sur une menace et sur la manière de la traiter :

1. Dans Sophos Enterprise Console, dans la liste des ordinateurs de la partie inférieure droite de la fenêtre, cliquez deux fois sur Sophos Security VM pour afficher la boîte de dialogue **Détails de l'ordinateur**.
   La section **Historique** répertorie les **Éléments détectés**. Le nom de la menace est indiqué sous la colonne **Nom** et la machine virtuelle cliente affectée et le fichier apparaissent sous la colonne **Détails**.
2. Cliquez sur le nom de la menace.
   Ceci vous connecte directement au site Web de Sophos où vous pouvez lire une description de l'élément et des conseils sur les mesures à prendre.

7 Nettoyage d’une menace

La machine virtuelle de sécurité nettoie automatiquement votre ordinateur des menaces ou vous pouvez le nettoyer manuellement.

Retrouvez plus de renseignements aux sections suivantes.

7.1 Nettoyage automatique

Sophos Security VM nettoie automatiquement les ordinateurs des menaces détectées.

Remarque
Le nettoyage automatique n’est pas disponible sur CD, sur les systèmes de fichiers en lecture seule et sur les systèmes de fichiers multimédia ou distants.

Que se passe-t-il en cas de nettoyage automatique ?

Lorsqu’une menace est détectée et nettoyée automatiquement, Sophos Enterprise Console :

- Indique que la menace a été bloquée (voir la section « Historique » » de la boîte de dialogue **Détails de l’ordinateur**).
- Affiche une alerte indiquant l’identité de la menace et si elle peut être nettoyée.
- Efface l’alerte si le nettoyage a réussi et indique « Non nettoyable » si le nettoyage échoue.

Il peut parfois être nécessaire de redémarrer une machine virtuelle cliente pour terminer le nettoyage. Dans ce cas, une alerte « Redémarrage requis » s’affiche à propos de Sophos Security VM. Pour savoir à quelle machine virtuelle cliente s’applique l’alerte, cliquez deux fois sur Sophos Security VM pour ouvrir la boîte de dialogue **Détails de l’ordinateur** et recherchez la description de l’alerte sous la section **Alertes et erreurs à traiter**.

7.2 Nettoyage manuel

Vous pouvez éliminer (nettoyer) une menace manuellement.

Veuillez effacer l’alerte de Sophos Enterprise Console après avoir supprimé la menace.

7.2.1 Nettoyage de la machine virtuelle invitée

Pour procéder au nettoyage manuel, veuillez restaurer le machine virtuelle cliente. Veuillez noter que vous perdrez toutes vos données si vous procédez ainsi. Utilisez l’une des méthodes suivantes :

- Restaurez le dernier « snapshot » sain sur la machine virtuelle cliente affectée.
- Supprimez la machine virtuelle cliente affectée et créez un nouveau clone à partir de l’image du modèle.

Assurez-vous que les outils Sophos requis sont installés sur l'image du modèle. Retrouvez plus de renseignements dans le Guide de démarrage de Sophos for Virtual Environments : édition Enterprise Console.

Quelle que soit la méthode que vous utilisez, procédez ensuite au contrôle intégral de la machine virtuelle cliente afin de vérifier qu'elle n'est pas infectée.

7.2.2 Suppression d'une alerte à partir de Sophos Enterprise Console

Lorsque vous êtes sûr que la machine virtuelle cliente est propre, effacez l'alerte de Sophos Enterprise Console :

1. Dans Sophos Enterprise Console, dans la liste des ordinateurs de la partie inférieure droite de la fenêtre, cliquez avec le bouton droit de la souris sur Sophos Security VM et sélectionnez **Résoudre les alertes et les erreurs**.
2. Dans la boîte de dialogue **Résolution des alertes et des erreurs**, sur l'onglet **Alertes**, sélectionnez l'alerte et cliquez sur **Approuver**.

L'alerte n'apparaît plus dans Sophos Enterprise Console.

8 Alertes

Cette section décrit les alertes envoyées par Sophos Security VM en cas de détection et de nettoyage de menaces.

Alertes de détection d'une menace

Si Sophos Security VM détecte une menace sur l'une des machines virtuelles clientes, des alertes sont affichées dans Sophos Enterprise Console :

- Une alerte s'affiche sur le tableau de bord.
- Une icône rouge d'avertissement apparaît dans la liste des ordinateurs sur l'onglet **État** correspondant à Sophos Security VM dans la colonne **Alertes et erreurs**.

Si la menace a été nettoyée automatiquement, l'alerte de détection de la menace disparaît de Sophos Enterprise Console.

Pour savoir à quelle machine virtuelle cliente s'applique l'alerte, cliquez deux fois sur Sophos Security VM dans la liste des ordinateurs. Dans **Détails de l'ordinateur**, sous **Alertes et erreurs à traiter**, recherchez la description de l'alerte. Les informations sur la machine virtuelle cliente s'affichent suivies par le chemin de la menace au format suivant :

```
NomMachine(adresse IP)/C:\menace.exe
```

Si Sophos Security VM détecte une menace lorsqu'un utilisateur essaye d'accéder à un fichier, un message peut également apparaître sur la machine virtuelle cliente informant l'utilisateur que le fichier est inaccessible. Le message peut varier en fonction de l'application utilisée pour accéder au fichier.

Alertes après nettoyage

Si une menace a été nettoyée, l'alerte disparaît de Sophos Enterprise Console.

L'opération de nettoyage est également signalée dans Sophos Enterprise Console. Pour voir le rapport, cliquez deux fois sur Sophos Security VM dans la liste des ordinateurs pour ouvrir la boîte de dialogue **Détails de l'ordinateur** et recherchez l'**Historique**.

Si la menace a été partiellement supprimée et que la machine virtuelle cliente doit être redémarrée pour terminer l'opération de nettoyage, une alerte Redémarrage requis » s'affiche.

9 Journaux

Sur une machine virtuelle cliente, les journaux sont écrits dans le journal des événements des applications Windows. Le journal se trouve dans **Journaux des applications et des services > Sophos > SVE**.

Sur Sophos Security VM, vous pouvez collecter les journaux et les récupérer dans le répertoire des journaux partagés. Procédez de la manière suivante :

1. Ouvrez une console sur Sophos Security VM.
2. Connectez-vous :
   - Le nom d'utilisateur est « Sophos ».
   - Le mot de passe est celui que vous avez créé lorsque vous avez installé Sophos Security VM.
3. Saisissez la commande suivante :

   ```
   sudo /opt/sophox/logcollector/diagnose
   ```

   Saisissez votre mot de passe lorsque vous y êtes invité. (L'opération peut durer jusqu'à 1 minute).
4. Dans l'Explorateur Windows, vous avez désormais accès aux journaux récupérés dans `\\<Adresse-IP-SVM>\logs\logs.tgz`. Saisissez vos codes d'accès lorsque vous y êtes invité :
   - Le nom d'utilisateur est « Sophos ».
   - Le mot de passe est celui que vous avez créé lorsque vous avez installé Sophos Security VM.

Retrouvez plus de renseignements sur la journalisation dans Sophos Enterprise Console dans l'Aide de Sophos Enterprise Console.

10 Désinstallation de Sophos Security VM

Pour désinstaller Sophos Security VM, vous devez la supprimer.

Avant de commencer, assurez-vous que les machines virtuelles clientes continueront à être protégées. Rendez-vous sur Sophos Security VM et suivez les instructions de la section Affichage des machines virtuelles clientes protégées (page 11). Déplacez ensuite les machines virtuelles clientes sur une autre Sophos Security VM ayant les mêmes paramètres de stratégie.

Pour déplacer vos machines virtuelles clientes :

1. Désinstallez Sophos Guest VM Agent conformément à la section Désinstallation de Sophos Guest VM Agent (page 19).
2. Réinstallez Sophos Guest VM Agent avec la nouvelle adresse IP de Sophos Security VM. Retrouvez plus de renseignements dans le Guide de démarrage de Sophos for Virtual Environments.

Une fois vos machines virtuelles clientes déplacées, vous pouvez supprimer Sophos Security VM. Procédez de la manière suivante :

1. Allez dans votre hyperviseur.
2. Éteignez Sophos Security VM.
3. Supprimez la machine virtuelle.

11 Désinstallation de Sophos Guest VM Agent

Vous pouvez désinstaller Sophos Guest VM Agent du Panneau de configuration.

1. Sur la machine virtuelle cliente, ouvrez le **Panneau de configuration**.
2. Cliquez sur **Programmes et fonctionnalités**.
3. Sélectionnez ces fonctionnalités et cliquez sur **Désinstaller** :
    - Sophos for Virtual Environments
    - Sophos Guest VM Scanning Service
    - Sophos Virus Removal Tool.

12 Annexe : Ajout de machines virtuelles de sécurité pour la migration des machines virtuelles clientes

Vous pouvez à tout moment ajouter des machines virtuelles de sécurité qui permettront de protéger la migration des machines virtuelles clientes.

Important
Vous devez effectuer ces étapes sur la machine virtuelle de sécurité que vous voulez ajouter sur les machines virtuelles de sécurité déjà existante.

1. Avec SSH, ouvrez le fichier de configuration additional_svms.txt pour le modifier :
   /opt/sophos-svms/etc/additional_svms.txt
2. Modifiez le fichier pour ajouter ou supprimer les adresses IP des machines virtuelles de sécurité disponibles pour assurer la protection de la migration des machines virtuelles clientes.
   - Ajoutez une adresse IP par ligne sans aucun caractère de séparation. Par exemple :
     1.2.3.4
     5.6.7.8
   - Vous n'avez pas besoin d'inclure l'adresse IP de la Sophos Security VM à laquelle vous êtes actuellement connecté.
3. Enregistrez et fermez le fichier.
4. Consultez le journal SVM (/var/log/ssvm.log) pour voir si des erreurs sont survenues lors du traitement de la liste de machines virtuelles de sécurité supplémentaires.
   S'il n'y a aucune erreur, la liste mise à jour est envoyée à toutes les machines virtuelles clientes connectées afin qu'elles soient protégées à partir des nouvelles machines virtuelles de sécurité.

13 Annexe : ajout de processeurs à Sophos Security VM

Si vous avez plusieurs machines virtuelles clientes sur un hôte, assurez-vous que le processeur de Sophos Security VM est assez puissant pour contrôler les fichiers qu'elles utilisent lorsqu'elles démarrent.

Pour cela, ajoutez plusieurs processeurs à Sophos Security VM. Vous pouvez effectuer cette opération au moment de votre choix.

Remarque
Si vous ajoutez des processeurs après avoir ajouté Sophos Security VM à un groupe d'ordinateurs dans Sophos Enterprise Console, veuillez patienter jusqu'à ce que Sophos Security VM soit conforme à la stratégie de groupe.

Selon le type de charge, l'ajout de processeurs peut également permettre d'améliorer les performances générales du système.

Ajout de processeurs dans VMware ESXi

Veuillez ajouter des processeurs comme suit :

1. Éteignez Sophos Security VM.
2. Dans vSphere Client, sélectionnez votre Sophos Security VM.
3. Sélectionnez **Modifier les paramètres > Matériel > CPU.** Puis, indiquez le nombre de processeurs (CPU).

Ajout de processeurs dans Microsoft Hyper-V

Veuillez ajouter des processeurs comme suit :

1. Cliquez sur **Démarrer**, sélectionnez **Outils d'administration** et cliquez sur **Gestionnaire Hyper-V**.
2. Dans le volet des résultats, sous **Ordinateurs virtuels**, sélectionnez la machine virtuelle de sécurité.
3. Dans le volet **Action**, sous le nom de la machine virtuelle, cliquez sur **Paramètres**.
4. Cliquez sur **Processeur** et indiquez le nombre de processeurs.

14 Support technique

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

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

15 Mentions légales

Licences tierces

Les licences tierces s'appliquant à l'utilisation de ce produit sont disponibles dans le dossier suivant de la machine virtuelle de sécurité Sophos : `/usr/share/doc`.

Certains programmes logiciels sont concédés en licence (ou en sous licence) à l'utilisateur selon les termes de la licence GNU General Public License (GPL) ou de licences pour logiciels libres similaires qui, entre autres droits, permettent à l'utilisateur de copier, modifier et redistribuer certains programs, ou parties de programmes et d'avoir accès au code source. La licence GPL exige que pour tout logiciel concédé en licence sous la licence GPL, qui est distribuée à un utilisateur sous un format binaire exécutable, le code source soit aussi mis à disposition de ces utilisateurs. Pour tout logiciel de ce type distribué avec un produit Sophos, le code source est mis à disposition conformément aux instructions de l'article 124427 de la base de connaissances.