SOPHOS

Security made simple.

Sophos pour Virtual Environments

Guide de configuration : édition Enterprise Console

Version du produit : 1.0

Table des matières

1 À propos de ce guide

Ce guide vous indique la marche à suivre pour configurer Sophos pour 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'Aide de Sophos Central Admin.

2 Configuration des stratégies

Vous configurez Sophos pour Virtual Environments avec les stratégies de l'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 l'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 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 pour 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 à la 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.
- Élimine 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 l'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.

Paramètre du contrôle sur accès	S'applique à Sophos Security VM ?	Remarques
Onglet Contrôle		
Vérifier les fichiers À la lecture/Au moment de renommer/À l'écriture	Non	Si une ou plusieurs options —À la lecture/Au moment de renommer/À l'écriture—sont activées, Sophos Security VM procédera au contrôle dans les trois cas de figure. **Important :** si les trois options sont désactivées, le contrôle sur accès est désactivé et 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	.
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		

Paramètre du contrôle sur accès	S'applique à Sophos Security VM ?	Remarques
Onglet Exclusions Windows	Oui	Pour exclure un dossier du contrôle, veuillez toujours indiquer le chemin complet vers le dossier, notamment la lettre du lecteur ou le nom du partage réseau. Par exemple, « C:\Tools\logs\ » ou « \\Serveur\Tools\logs\ ». Sophos Security VM ne peut pas exclure les dossiers en se basant uniquement sur leur nom. Par exemple, « \Tools\logs\ » ne fonctionnera pas. Retrouvez plus de renseignements sur les exclusions Windows, comme par exemple la manière d'utiliser des caractères génériques dans la section sur la configuration d'une stratégie antivirus et HIPS de l'Aide de la Sophos Enterprise Console.
Onglet Exclusions Mac	Non	
Onglet Exclusions Linux/UNIX	Non	
Onglet Nettoyage		
Élimination des virus/spywares	Oui	Les actions alternatives à appliquer si l'échec de l'élimination n'a aucun effet. Sophos Security VM refuse toujours l'accès aux éléments infectés.
Élimination des fichiers suspects	Non	

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

Paramètre du contrôle planifié	S'applique à Sophos Security VM ?	Remarques
Ajouter/Modifier > Paramètres du contrôle planifié		

Paramètre du contrôle planifié	S'applique à Sophos Security VM ?	Remarques
Éléments à contrôler		
Disques durs locaux	Oui	
Disquettes et lecteurs amovibles	Oui	
Lecteurs de CD-ROM	Oui	
Planification du contrôle	Oui	Sophos Security VM commencera le contrôle à l'heure et au jour indiqués. Toutefois, il contrôlera uniquement deux machines virtuelles clientes à la fois afin de ne pas affecter les performances de votre système. Par conséquent, il se peut que le contrôle de toutes les machines virtuelles clientes soit long à effectuer.
Ajouter/Modifier > Paramètres du contrôle planifié > Configurer > Paramètres du contrôle et de nettoyage		
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 sera contrôlée par défaut. Vous ne pouvez pas configurer cette option.
Exécuter le contrôle avec une priorité inférieure	Non	
Onglet Nettoyage		
Élimination des virus/spywares	Oui	Sophos Security VM n'élimine 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 d'élimination n'a pas eu lieu. Sophos Security VM journalise toujours l'événement même si l'opération d'élimination n'a pas eu lieu.
Élimination des adwares et PUA	Non	

Paramètre du contrôle planifié	S'applique à Sophos Security VM ?	Remarques
Élimination des fichiers suspects	Non	
Extensions et exclusions > Extensions et exclusions du contrôle planifié		
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, veuillez toujours indiquer le chemin complet vers le dossier, notamment la lettre du lecteur ou le nom du partage réseau. Par exemple, « C:\Tools\logs\ » ou « \\Serveur\Tools\logs\ ». La machine virtuelle de sécurité ne peut pas exclure les dossiers en se basant uniquement sur leur nom. Par exemple, « \Tools\logs\ » ne fonctionnera pas. Retrouvez plus de renseignements sur les exclusions Windows, par exemple sur l'utilisation des caractères de remplacement dans l'Aide de l'Enterprise Console.
Onglet Exclusions Mac	Non	
Onglet Exclusions Linux/UNIX	Non	

Sophos Live Protection

Sophos Live Protection est pris en charge à l'exception de l'envoi de fichiers.

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

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	lha
7zip	lzh
??_	rar
a	rpm
arj	tar
bin	taz
bz2	tbz

gz hqx hxs	tbz2 tgz

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 l'Enterprise Console.

2.2 Stratégie de mise à jour

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

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

3 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.

4 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.

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

Note: 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 l'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**.

   Note: 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. Allez dans l'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 l'Enterprise Console.

Pour voir les détails du contrôle suite à son exécution :

Dans l'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**.

5 Recherche d'informations sur une menace

Pour rechercher plus d'informations sur une menace et sur la manière de la traiter :

1. Dans l'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** affiche une liste des **Éléments détectés**. Le nom de la menace s'affiche dans la colonne **Nom** tandis que la machine virtuelle cliente affectée et le fichier sont affichés dans la colonne **Détails**.

2. Cliquez sur le nom de la menace.

   Vous allez être directement connecté au site Web de Sophos où vous retrouverez une description et des conseils sur la marche à suivre.

6 Élimination d'une menace

6.1 Élimination automatique

Sophos Security VM élimine automatiquement les menaces détectées.

Note: l'élimination 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 d'élimination automatique ?

Lorsqu'une menace est détectée et éliminée automatiquement, l'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 qui indique l'identité de la menace et si elle peut être nettoyée.
- Efface l'alerte si l'opération d'élimination a réussi et indique « Non nettoyable » si l'opération d'élimination échoue.

Il peut parfois être nécessaire de redémarrer une machine virtuelle cliente pour terminer l'opération d'élimination. 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**.

6.2 Élimination manuelle

Vous pouvez éliminer une menace manuellement.

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

6.2.1 Nettoyage de la machine virtuelle invitée

Pour procéder à l'élimination des menaces manuellement, 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 pour 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.

6.2.2 Suppression d'une alerte à partir de l'Enterprise Console

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

1. Dans l'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 l’Enterprise Console.

7 Alertes

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

Alertes de détection d'une menace

Si Sophos Security VM détecte une menace sur l'une des machines virtuelles clientes, elle alerte l'Enterprise Console comme suit :

Dans l'Enterprise Console :

- Une alerte apparaît 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 éliminée automatiquement, l'alerte de détection de la menace disparaît de l'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 élimination

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

L'opération de nettoyage est également signalée dans l'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, mais que la machine virtuelle cliente doit être redémarrée pour terminer le nettoyage, une alerte « Redémarrage requis » apparaît.

8 Journaux

Sur une machine virtuelle cliente, les journaux sont écrits dans le journal des événements des applications Windows. Le journal se trouve dans **Applications and Services Logs** > **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 l'Aide de l'Enterprise Console.

9 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.

10 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.