SOPHOS

Cybersecurity made simple.

Sophos for Virtual Environments

Guide de configuration pour les utilisateurs de Sophos Central

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 Central pour administrer votre logiciel de sécurité.

Si vous utilisez Sophos Enterprise Console, veuillez consulter le guide de configuration pour les utilisateurs de l'Enterprise Console.

2 Configuration des stratégies

Vous configurez Sophos for Virtual Environments avec les stratégies de Sophos Central.

Vous pouvez uniquement utiliser le type de stratégie de protection contre les menaces et pouvez créer plusieurs stratégies si vous le désirez.

Par défaut, Sophos Central applique une stratégie de protection contre les menaces de base à toutes vos machines virtuelles de sécurité. Les paramètres de la stratégie sont ensuite utilisés pour les machines virtuelles clientes.

Ces paramètres offrent :

- La détection des malwares connus.
- Les vérifications Cloud pour activer la détection des malwares les plus récents recensés par Sophos.
- La détection proactive des malwares qui n'ont jamais encore été détectés.
- Le nettoyage automatique des malwares.

Retrouvez plus de renseignements dans l'Aide de Sophos Central.

Vous pouvez modifier la stratégie de base ou créez des stratégies supplémentaires que vous allez pouvoir utiliser pour appliquer différents paramètres à différentes machines virtuelles de sécurité.

Création ou modification d'une stratégie

Créez ou modifiez une stratégie de Protection contre les menaces :

1. Ouvrez Sophos Central et allez dans **Server Protection > Stratégies**.
2. Cliquez sur la stratégie **Protection contre les menaces** ou cliquez sur **Ajouter une stratégie** pour en créer une nouvelle.
3. Sur l'onglet **Serveurs**, sélectionnez les machines virtuelles de sécurité auxquelles vous souhaitez appliquer la stratégie.
4. Sur l'onglet **Paramètres**, saisissez les paramètres de votre choix.

   Retrouvez plus de renseignements sur les options que vous pouvez utiliser pour les machines virtuelles de sécurité aux sections ci-dessous.

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 ?
Utiliser Sophos Live Protection	Oui
Envoyer automatiquement les échantillons de malwares aux SophosLabs	Non

Contrôle en temps réel

Les options de **Contrôle en temps réel** sont les suivantes.

Option	Compatible ?
Activer ou Désactiver	Oui
Contrôle local ou contrôle local et à distance	Oui
À la lecture	Non
À l'écriture	Non

Contrôle en temps réel - Internet

Les options de **Contrôle en temps réel - Internet** sont les suivantes.

Option	Compatible ?
Contrôler les téléchargements en cours	Non
Bloquer l'accès aux sites Web malveillants	Non
Détecter les fichiers de réputation douteuse	Non

Correction

Les options de **Correction** sont les suivantes.

Option	Compatible ?
Nettoyage automatique des malwares	Oui

Contrôle en temps réel - Options

Les options de **Contrôle en temps réel - Options** sont les suivantes.

Option	Compatible ?
Exclure automatiquement l'activité des applications connues	Non
Détecter les comportements malveillants (HIPS)	Non

Contrôle planifié

Les options de **Contrôle planifié** sont les suivantes.

Option	Compatible ?
Activer le contrôle planifié	Oui

Protection à l’exécution (runtime)

Les options de **Protection à l’exécution (runtime)** sont les suivantes.

Option	Compatible ?
Détecter le trafic réseau vers les serveurs de commande et de contrôle	Non
Protéger les fichiers document contre les ransomwares (CryptoGuard)	Non
Activer Sophos Security Heartbeat	Non

Exclusions du contrôle

Les options d’**Exclusions du contrôle** sont les suivantes.

Option	Compatible ?
Exclusions du contrôle générales Pour modifier cette option, allez dans **Paramètres > Exclusions du contrôle générales**.	Oui
Exclusions du contrôle par stratégie (Windows et Linux)	Oui
Exclusions Heartbeat par stratégie (Windows uniquement)	Non
Exclure le serveur DNS (Windows uniquement)	Non

Messagerie de bureau

Les options de **Messagerie de bureau** sont les suivantes.

Option	Compatible ?
Activer la messagerie de bureau pour la protection contre les menaces	Non

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 5).

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 en temps réel (page 6)

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. Connectez-vous à Sophos Central.
   - **Si la fonction de nettoyage automatique est activée**, allez sur la page **Serveurs** et cliquez sur Sophos Security VM pour ouvrir la page d'informations. Sur l'onglet **Événements**, vous devriez voir qu'EICAR a été détecté et nettoyé.
   - **Si la fonction de nettoyage automatique n'est pas activée**, consultez la page **Alertes**. Vous devriez voir une alerte sur Sophos Security VM. EICAR a été détecté mais n'a pas été nettoyé.

Si EICAR n'a pas été détecté, veuillez-vous reporter à la section Résolution des problèmes du contrôle en temps réel (page 6). Si EICAR n'a pas été éliminé, veuillez le supprimer.

3.3 Résolution des problèmes du contrôle en temps réel

Si le contrôle en temps réel ne fonctionne pas :

1. Assurez-vous que le contrôle en temps réel est activé dans la stratégie Serveur appliquée à Sophos Security VM :
   a) Dans Sophos Central, allez sur la page **Serveurs** et recherchez Sophos Security VM puis cliquez dessus pour afficher les informations la concernant.
   b) Sous l'onglet **Informations**, sous **Activité**, vous pouvez voir la stratégie de protection contre les menaces qui s'applique au serveur. Cliquez sur le nom de la stratégie.
   c) Dans la stratégie, recherchez la section **Contrôle en temps réel**. Assurez-vous que le **Contrôle** est activé.
   d) 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. Retrouvez plus de renseignements à la section « Affichage des machines virtuelles clientes protégées » du Guide de configuration de Sophos for Virtual Environments.
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 VM clientes

Vous pouvez voir les informations sur toutes les machines virtuelles de sécurité comme suit :

- Affichage des VM clientes connectées (page 7). Vous pouvez effectuer cette opération dans Sophos Central.
- Affichage des machines virtuelles clientes protégées (page 7).

Les machines virtuelles clientes « Connectées » sont équipées de l'agent Sophos et peuvent se connecter à la machine virtuelle de sécurité.

Généralement, une machine virtuelle cliente connectée est également protégée. Toutefois, si l'agent vient d'être installé ou en cas de problème, le contrôle à la recherche des menaces n'a peut être pas été démarré.

4.1 Affichage des VM clientes connectées

Vous pouvez afficher toutes les machines virtuelles clientes connectées à Sophos Security VM comme indiqué ci-dessous.

1. Connectez-vous à Sophos Central.
2. Allez sur **Server Protection > Serveurs**.
3. Recherchez Sophos Security VM dans la liste et et cliquez dessus pour voir plus d'informations.
4. Sur l'onglet **Informations**, sous **État des environnements virtuels**, recherchez **Machines virtuelles connectées**. Cliquez sur le nombre affiché.

   Remarque
   Si aucune machine virtuelle cliente n'est allumée ou si vous êtes toujours en train d'installer des agents sur ces machines, vous ne verrez probablement aucune machine virtuelle cliente.

5. Une liste des noms des machines virtuelles et des adresses IP apparaît.

   Recherchez une machine virtuelles cliente particulière dans cette liste ou utilisez le filtre pour afficher les machines virtuelles clientes de bureau ou serveur.

4.2 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 Security VM contrôle toujours les fichiers sur accès, c'est-à-dire à leur ouverture et à leur fermeture.

Sophos Security VM peut également effectuer un contrôle intégral de toutes les machines virtuelles clientes. 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 procède à des contrôles décalés afin que l'hôte 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. Par conséquent, il se peut que le contrôle de toutes les machines virtuelles clientes gérées par Sophos Security VM soit long à effectuer.

Contrôle immédiat des machines virtuelles clientes

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

1. Connectez-vous à Sophos Central.
2. Allez sur la page **Serveurs**.
3. Recherchez Sophos Security VM et cliquez dessus pour ouvrir la page d'informations.
4. Dans le volet de gauche, cliquez sur **Contrôler**.

Contrôle planifié des machines virtuelles clientes

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

1. Connectez-vous à Sophos Central.
2. Allez sur la page **Serveurs**.
3. Recherchez Sophos Security VM et cliquez dessus pour voir la page d'informations.
4. Sous l'onglet **Informations** et sous **Activité**, vous pouvez voir la Stratégie de protection contre les menaces appliquée. Cliquez dessus pour la modifier.
5. Dans la stratégie, allez sous la section **Contrôle planifié**. Activez le contrôle et indiquez l'heure et le jour d'exécution du contrôle.

6 Que se passe-t-il lorsqu'une menace est détectée ?

Lorsque Sophos Security VM détecte une menace sur l'une des machines virtuelles clientes, elle :

- Bloque la menace.
- Essaye de nettoyer automatiquement les menaces détectées.
- Envoie une alerte à Sophos Central si vous devez intervenir.

Remarque
Sophos Security VM ne nettoie pas automatiquement les menaces détectées au cours d'un contrôle intégral de toutes les machines virtuelles clientes.

Ce que vous voyez dans Sophos Central

Sophos Central :

- Montre que la menace a été bloquée. Retrouvez plus de renseignements sur Sophos Security VM sur l'onglet **Événements**.
- Affiche une alerte sur la page **Alertes**. Vous pouvez voir de quelle menace il s'agit, sur quelle machine virtuelle elle se trouve et si elle peut être nettoyée.
- Efface l'alerte si le nettoyage automatique a réussi.

Si le nettoyage automatique est indisponible ou qu'il a échoué, une alerte affichée sur la page **Alertes** vous invite à procéder au nettoyage manuel.

Retrouvez plus de renseignements sur la procédure de nettoyage à la section Nettoyage d'une menace (page 11).

Ce que l'utilisateur voit sur la machine virtuelle cliente

Si Sophos Security VM détecte une menace lorsqu'un utilisateur essaye d'accéder à un fichier, un message peut 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.

7 Nettoyage d’une menace

Cette section aborde le nettoyage (élimination) manuel et automatique des menaces.

Retrouvez plus de renseignements sur les menaces et des conseils sur leur nettoyage sur la page **Alertes** de Sophos Central en recherchant l’alerte de menace et en cliquant sur le nom de la menace.

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.

Nettoyage manuel

Vous pouvez nettoyer une machine virtuelle cliente manuellement.

Pour procéder au nettoyage manuel, veuillez restaurer le machine virtuelle cliente. Vous risquez de perdre des données (retrouvez plus de renseignements à ce sujet ci-dessous).

Utilisez l’une des méthodes suivantes :

- Supprimez la machine virtuelle cliente et clonez-la de nouveau à partir de l’image du modèle (template). Vous allez perdre vos données.
- Restaurez la machine virtuelle cliente à sa précédente capture instantanée saine. Vous allez perdre toutes les données ajoutées depuis la prise de cette capture instantanée.

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.

8 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 7). 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 13).
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.

9 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.

10 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.

11 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.

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.

12 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.

13 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.