SOPHOS

Security made simple.

Sophos pour Virtual Environments

Guide de démarrage : édition Sophos Central

Version du produit : 1.0

Table des matières

1 À propos de ce guide....3
2 À propos de Sophos pour Virtual Environments....4
3 Étapes principales de l'installation....7
4 Vérification de la configuration système requise....8
4.1 Configuration requise pour VMware....8
4.2 Conditions requises pour Microsoft Hyper-V....9
4.3 Configuration requise pour la machine virtuelle cliente....9
4.4 Conditions requises pour le réseau....10
4.5 Configuration requise pour l’administration Sophos....11
5 Désinstallation d'autres produits antivirus....12
6 Installation de Sophos Security VM....13
6.1 Comment vérifier que vous avez les mots de passe adéquats ?....13
6.2 Vérification de la synchronisation des systèmes....13
6.3 Vérification de la configuration requise pour le programme d’installation....13
6.4 Téléchargement du programme d'installation de Sophos Security VM....14
6.5 Installation de Sophos Security VM....14
6.6 Vérification de l’installation de Sophos Security VM....16
7 Installation de Sophos Guest VM Agent....17
8 Vérification de la protection des machines virtuelles clientes....18
8.1 Vérification des paramètres de protection....18
8.2 Test du contrôle en temps réel....18
8.3 Résolution des problèmes du contrôle en temps réel....19
9 Affichage des machines virtuelles clientes protégées....20
10 Contrôle des machines virtuelles clientes....21
11 Que se passe-t-il lorsqu'une menace est détectée ?....22
12 Élimination d'une menace....23
13 Maintenance de la machine virtuelle de sécurité....24
14 Désinstallation de Sophos Security VM....25
15 Désinstallation de Sophos Guest VM Agent....26
16 Migration vers Sophos pour Virtual Environments....27
17 Annexe : ajout de processeurs à Sophos Security VM....29
18 Support technique....30
19 Mentions légales....31

1 À propos de ce guide

Ce guide vous explique comment :

- Utiliser Sophos pour Virtual Environments afin d'assurer la protection centrale contre les menaces des machines virtuelles (VM) sous un environnement VMware ESXi ou Microsoft Hyper-V.
- Utiliser Sophos Central pour administrer Sophos pour Virtual Environments.

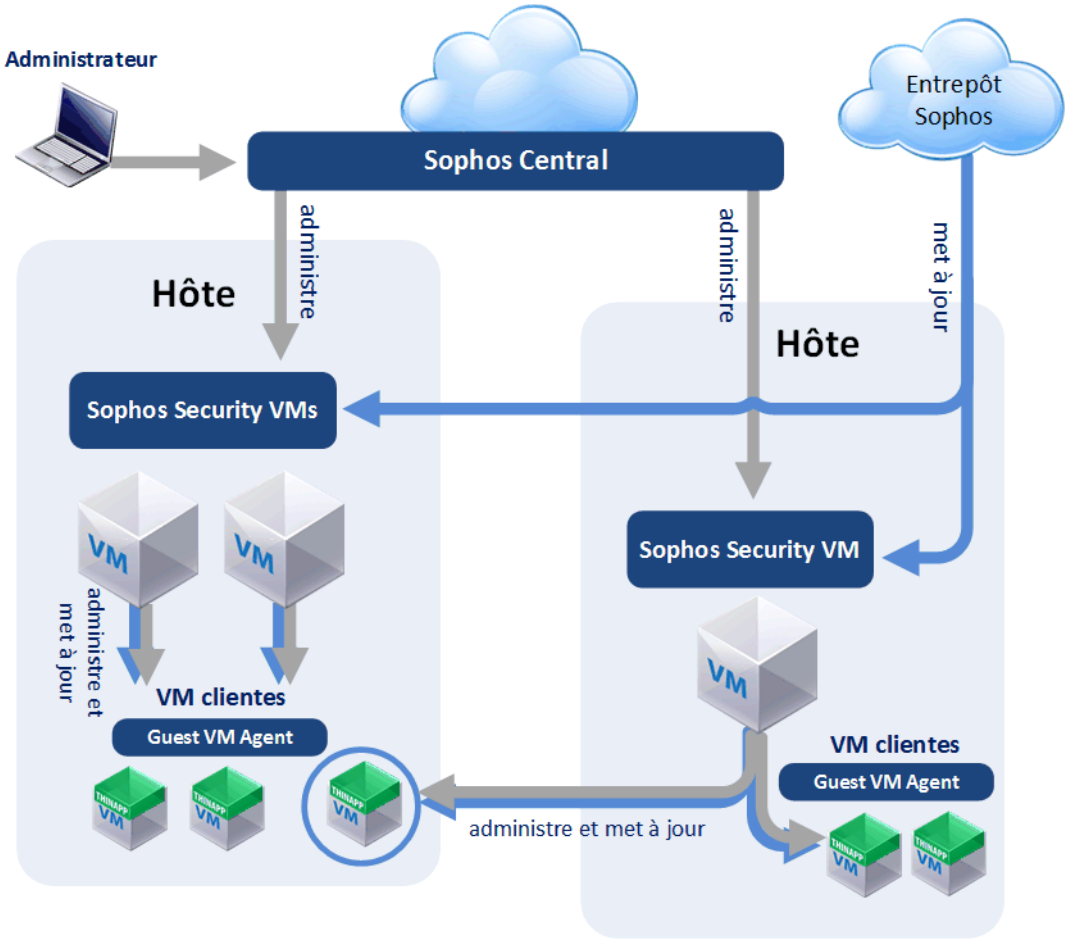
Retrouvez plus de renseignements sur la migration vers Sophos pour Virtual Environments à la section Migration vers Sophos pour Virtual Environments à la page 27.

Si vous voulez utiliser Sophos Enterprise Console plutôt que Sophos Central, veuillez consulter le *Guide de démarrage de Sophos pour Virtual Environments : édition Enterprise Console*.

2 À propos de Sophos pour Virtual Environments

Sophos pour Virtual Environments est un système de sécurité qui protège les machines virtuelles (VM). Son fonctionnement est le suivant :

- Vous installez une ou plusieurs **Sophos Security VM** sur chaque hôte. Sophos Security VM peut ensuite détecter et bloquer les menaces sur les machines virtuelles clientes.
- Veuillez installer **Sophos Guest VM Agent** sur chaque machine virtuelle cliente.
- Vous utilisez **Sophos Central** pour gérer Sophos Security VM.



Environnements compatibles avec Sophos ?

Sophos pour Virtual Environments protège les machines virtuelles sur les environnements VMware ESXi ou Microsoft Hyper-V.

Protection des machines virtuelles clientes compatibles

Sophos Security VM protège les machines virtuelles clientes sous systèmes d'exploitation Windows. Retrouvez plus de renseignements à la section Configuration requise pour la machine virtuelle cliente à la page 9.

Remarque : Sophos Security VM protège les machines virtuelles clientes se trouvant sur un hôte différent.

Fonctionnement du contrôle ?

Lorsqu'une machine virtuelle cliente essaye d'accéder à un fichier :

- Sophos Guest VM Agent en cours d'exécution sur la machine virtuelle informe Sophos Security VM.
- Sophos Security VM contrôle le fichier.
- Si Sophos Security VM détecte une menace, l'accès au fichier est bloqué et Sophos Security VM envoie une alerte à Sophos Central.

Sophos Security VM peut également effectuer un contrôle intégral de toutes les machines virtuelles clientes. Ce contrôle peut être exécuté immédiatement ou programmé.

Le contrôle des fichiers utilise la mise en mémoire cache intelligente pour conserver les résultats des contrôles précédents. Ceci permet d'améliorer les performances générales lorsque plusieurs machines virtuelles clientes sont utilisées ou lorsque le même fichier est accédé à plusieurs reprises.

Gestion de Sophos Security VM

Sophos Central affiche l'état de Sophos Security VM, notamment son état de mise à jour et si elle a détecté des menaces.

Sophos Central vous permet également de configurer le contrôle à l'aide d'une stratégie.

Traitement des menaces

Sophos Security VM permet d'éliminer automatiquement les menaces. Retrouvez plus de renseignements à la section Élimination d'une menace à la page 23.

Mise à jour de Sophos Security VM

Sophos Security VM reçoit, récupère et installe les mises à jour automatiquement depuis Sophos.

Mise à jour de Sophos Guest VM Agent

Sophos Guest VM Agent est mis à jour automatiquement.

L'agent ne contrôle pas les fichiers et n'a donc pas besoin d'utiliser les plus récentes identités de menaces. En revanche, il reçoit les mises à jour lorsque nous apportons des améliorations à notre produit.

Sophos Security VM reçoit les mises à jour produit de Sophos et les déploie sur les machines virtuelles clientes.

Les mises à jour sont échelonnées afin de réduire la charge sur Sophos Security VM et sur l’hôte de l’hyperviseur sous-jacent.

3 Étapes principales de l'installation

L'installation s'effectue via les étapes principales décrites dans les sections qui suivent :

- Vérification de la configuration système requise.
- Désinstallation d'autres produits antivirus.
- Installation de Sophos Security VM.
- Installation de Sophos Guest VM Agent sur les machines virtuelles clientes.
- Vérification de la protection des machines virtuelles clientes.

4 Vérification de la configuration système requise

Cette section aborde les différentes configurations système requises et la manière de vérifier si vous les respectez.

Elle vous indique également quelles informations (détails de l'ordinateur) vous devez avoir à disposition lorsque vous installez Sophos Security VM.

Elle aborde les conditions requises pour les environnements VMware EXSi et Microsoft Hyper-V.

4.1 Configuration requise pour VMware

Cette section vous indique les logiciels à utiliser dans un environnement VMware.

4.1.1 Hôte VMware ESXi

Sur chaque hôte qui va exécuter Sophos Security VM, veuillez installer :

- La version 5.5, 6.0 ou 6.5 de l'hôte VMware ESXi.

Remarque : nous vous conseillons de configurer l'hôte afin de récupérer les mises à jour à partir de VMware.

Configuration matérielle requise

L'hôte VMware ESXi doit fournir les ressources suivantes à Sophos Security VM :

- 2 CPU.
- 20 Go d'espace disque.
- 4 Go de RAM.

Remarques

N'appliquez en aucun cas de limites de ressources processeur (CPU) sur Sophos Security VM.

Par défaut, les 2 CPU sont alloués. Si vous devez protéger plusieurs machines virtuelles clientes, vous pouvez configurer d'autres CPU après avoir installé la machine virtuelle de sécurité. Ce guide vous indique la marche à suivre.

Sophos Security VM met de la mémoire en réserve. La haute disponibilité et les systèmes d'équilibrage de charge font des choix automatiques selon les réserves de mémoire disponibles pour les machines virtuelles dans votre environnement VMware. Veuillez ne pas supprimer la réserve de mémoire de Sophos Security VM.

4.1.2 VMware vCenter et vSphere

Vous devez disposer des logiciels vCenter et vSphere suivants.

Logiciel	Version	Remarques
vCenter	Version 5.5 ou 6.5. La version 6.5 est requise pour administrer la version 6.0 de l'hôte ESXi mais peut également administrer des versions plus anciennes d'ESXi.	Vous allez également avoir besoin de : L'adresse réseau. Un compte d'administrateur.
vSphere Client	Version 5.5 ou 6.5.	

4.1.3 Outils VMware

Ces composants ne sont pas nécessaires pour utiliser Sophos pour Virtual Environments. Toutefois, nous vous conseillons de les utiliser car ils améliorent les performances réseau.

4.2 Conditions requises pour Microsoft Hyper-V

Cette section vous indique les logiciels à utiliser dans un environnement Microsoft Hyper-V.

Le système Microsoft Hyper-V utilisé doit être l'un des suivants :

- Hyper-V dans Windows Server 2012 (base, complète)
- Hyper-V dans Windows Server 2012 R2 (base, complète)

Composants d'intégration de Microsoft Hyper-V

Les composants d'intégration de Microsoft Hyper-V seront installés automatiquement si la mise à jour de Windows est activée et fonctionne. Sans ces outils, les performances de votre machine virtuelle risquent d'être amoindries.

Instructions d'utilisation de l'antivirus pour Microsoft Hyper-V

Microsoft publie des instructions sur la manière de sécuriser efficacement votre serveur Hyper-V. Retrouvez plus de renseignements dans l'article 3105657 de la base de connaissances de Microsoft.

4.3 Configuration requise pour la machine virtuelle cliente

Les machines virtuelles clientes doivent exécuter l'un des systèmes d'exploitation suivants :

Système d'exploitation	Service packs	Commentaires
Windows 10 (32 et 64 bits). L'article 125679 de la base de connaissances		Conteneurs Windows et Hyper-V non pris en charge.

Système d'exploitation	Service packs	Commentaires
répertorie toutes les versions compatibles.		
Windows 8.1 (32 et 64 bits)	---	
Windows 7 (32 et 64 bits)	SP1+	
Windows Server 2016 (64 bits)		Conteneurs Windows et Hyper-V non pris en charge.
Windows Server 2012 R2 (64 bits)	---	
Windows Server 2012 (64 bits)	---	
Windows Server 2008 R2 (64 bits)	---	
Windows Server 2008 (64 bits)	---	

4.4 Conditions requises pour le réseau

Les conditions requises pour l'infrastructure sont :

- Sophos Security VM et les machines virtuelles clientes doivent partager la même connexion au réseau. Idéalement, il doit s'agir d'un réseau local (LAN) à haut débit sans aucune limite de trafic réseau.
- Le trafic réseau entre Sophos Security VM et les machines virtuelles clientes ne doit pas être bloqué par les pare-feu ou par les contrôleurs d'accès au réseau.

4.4.1 Conditions requises pour les réseaux NAT

Si vous utilisez des machines virtuelles clientes sur un réseau NAT (traduction d'adresses réseau), vous pouvez les protéger avec Sophos Security VM sur ou en dehors de ce réseau.

Pendant l'installation, veuillez configurer Sophos Security VM comme suit :

- Une adresse IP principale en dehors du réseau NAT (cette adresse doit pouvoir communiquer avec la console d'administration
- Une adresse IP secondaire sur le réseau NAT.

4.4.2 Sous-réseaux

Vous pouvez configurer Sophos Security VM avec un nombre maximal de cinq adresses IP. Chaque adresse IP doit se trouver sur un sous-réseau différent.

4.5 Configuration requise pour l'administration Sophos

Avant de pouvoir protéger et administrer vos machines virtuelles, vous devez avoir :

- Un compte Sophos Central.

5 Désinstallation d'autres produits antivirus

Veuillez désinstaller tous les produits antivirus (**produits Sophos inclus**) déjà présents sur vos machines virtuelles clientes.

Veuillez désactiver Windows Defender sur les plates-formes serveur sur lesquelles le centre de sécurité n’est pas présent. Nous vous conseillons d’utiliser une stratégie de groupe pour effectuer cette action.

Vous ne pouvez pas utiliser Sophos pour Virtual Environments pour protéger les machines virtuelles clientes exécutant d'autres produits antivirus. Si vous essayez ceci, les performances du système seront amoindries ou le système risque de se bloquer et la machine virtuelle cliente ne répondra plus.

Cette limite s'applique également aux machines virtuelles équipées de produits passerelle ou serveur de Sophos et qui intègrent ou nécessitent l'utilisation de composants antivirus.

Retrouvez plus de renseignements dans l'article 125679 de la base de connaissances.

6 Installation de Sophos Security VM

Vous pouvez installer une ou plusieurs Sophos Security VM sur chaque hôte sur lequel vous souhaitez protéger les machines virtuelles clientes.

Avant de commencer, assurez-vous que l'hôte satisfait aux conditions requises par le système. Nous vous conseillons également de configurer l'hôte afin de récupérer les mises à jour à partir de VMware.

L'installation se fait par les étapes décrites dans les sections qui suivent :

- Vérification de la possession des mots de passe adéquats.
- Vérification de la synchronisation des systèmes.
- Téléchargement du programme d'installation.
- Installation de Sophos Security VM.
- Vérification de l'installation de Sophos Security VM

6.1 Comment vérifier que vous avez les mots de passe adéquats ?

Lorsque vous exécutez le programme d'installation de Sophos Security VM, veuillez saisir certains mots de passe. Veuillez-vous assurer que vous avez les mots de passe pour les comptes suivants :

- Le compte Sophos Central.
- Le compte d'administrateur vCenter si vous êtes dans un environnement VMware.

6.2 Vérification de la synchronisation des systèmes

Assurez-vous que l'heure est synchronisée sur l'hôte sur lequel vous installez Sophos Security VM et sur les machines virtuelles clientes.

Vous pouvez utiliser la synchronisation NTP (Network Time Protocol) pour chaque hôte.

Avertissement : si l'heure n'est pas synchronisée, vous pouvez installer Sophos Security VM mais vous ne pourrez pas l'administrer à partir de Sophos Central.

6.3 Vérification de la configuration requise pour le programme d'installation

Assurez-vous que l'ordinateur et le compte d'utilisateur que vous allez utiliser répondent aux conditions requises.

- Le programme d'installation doit se trouver sur un ordinateur ayant accès à votre VMware vCenter ou au serveur Microsoft Hyper-V sur le réseau.
- L'installation de Sophos Security VM doit être effectuée sur le réseau local. Le programme d'installation n'est actuellement pas être utilisé avec un proxy.

- Le programme d'installation ne peut pas être utilisé sur un ordinateur Windows XP ou Windows Server 2003.
- Si vous utilisez Microsoft Hyper-V, veuillez exécuter le programme d'installation en tant qu'utilisateur avec les droits de suffisants pour créer et contrôler les machines virtuelles sur le serveur Hyper-V. Il peut s'agir d'un compte d'utilisateur local sur le serveur Hyper-V ou d'un domaine d'utilisateur.

L'ordinateur sur lequel vous conservez le programme d'installation est uniquement utilisé pour procéder à l'installation. Il n'est pas utilisé pour l'administration ou la protection de votre Sophos Security VM ou des machines virtuelles clientes après l'installation.

6.4 Téléchargement du programme d'installation de Sophos Security VM

Téléchargez le programme d'installation à partir de Sophos Central (si vous ne l'avez pas déjà fait).

Les étapes suivantes supposent que vous avez un compte Sophos Central.

Remarques :

- Vous pouvez télécharger le programme d'installation sur tout ordinateur de votre choix et le copier par la suite sur l'ordinateur sur lequel vous allez l'utiliser.
- Les consignes d'installation évoquées dans les prochaines sections vous indiquent sur quel(s) ordinateur(s) utiliser le programme d'installation.

Pour télécharger le programme d'installation :

1. Connectez-vous à Sophos Central.
2. Allez sur la page **Protection des appareils**.
3. Sous **Protection de l'environnement virtuel**, cliquez sur le lient pour télécharger le programme d'installation correspondant à votre environnement (Hyper-V ou ESXi).

Après avoir installé Sophos Security VM, vous pourrez récupérer Sophos Guest VM Agent à partir d'un partage public sur Sophos Security VM.

6.5 Installation de Sophos Security VM

Pour installer Sophos Security VM, vous allez avoir besoin du programme d'installation de Sophos Security VM. Si vous ne l'avez pas encore téléchargé, retrouvez plus de renseignements sur la marche à suivre à la section Téléchargement du programme d'installation de Sophos Security VM à la page 14.

Assurez-vous que l'ordinateur et le compte d'utilisateur que vous allez utiliser répondent aux conditions requises à la page 13.

Certaines étapes de l'installation s'appliquent uniquement à VMware ESXi ou à Microsoft Hyper-V. Ceci sera indiquée au début de l'étape.

1. Cliquez deux fois sur le programme d'installation.

   Un assistant se lance pour vous guider tout au long de la procédure d'installation.

2. Acceptez le contrat de licence.
3. Sur la page de bienvenue, cliquez sur **Install** pour extraire les fichiers d'installation dans un dossier sur votre ordinateur.

4. Assurez-vous que toutes les conditions préalables à l'installation sont remplies dans **Prerequisites for installation**.
5. **Uniquement dans un environnement VMware ESXi :**

   Dans le champ **VMware vCenter credentials**, saisissez vos codes d'accès et un nom pour Sophos Security VM.

   Remarque : saisissez le même nom d'utilisateur de l'administrateur que vous avez utilisé pour vous connecter à vCenter à l'aide du client vSphere. En d'autres termes, saisissez ce nom avec ou sans préfixe de domaine, le cas échéant et en respectant la casse majuscule/minuscule.

6. Dans **ESXi host** ou **Hyper-V host name**, indiquez l'hôte sur lequel vous voulez installer Sophos Security VM.
7. Dans **Management console**, sélectionnez **Use Sophos Central**.
8. Saisissez les informations de votre compte dans **Sophos Central account details** :

   a) Saisissez l'adresse email et le mot de passe que vous allez utiliser pour vous connecter à Sophos Central.

   b) Saisissez les informations du serveur proxy utilisé pour vous connecter à Sophos Central (si applicable).

9. Dans **Password for access**, créez un mot de passe d'accès à votre Sophos Security VM.

   Vous allez avoir besoin de ce mot de passe pour voir les machines virtuelles clientes protégées. Vous allez également en avoir besoin si vous souhaitez que le support technique de Sophos vous aide à résoudre à distance tout problème que vous pourriez rencontrer à l'installation. Il l'utilisera pour récupérer des journaux que vous pourrez vérifier avant de les envoyer à Sophos si nécessaire.

10. Dans **Timezone**, sélectionnez le fuseau horaire que Sophos Security VM va utiliser pour planifier les contrôles.
11. **Uniquement dans un environnement VMware ESXi :**

    Dans **Datastore for the Security VM**, sélectionnez le type de banque de données sur laquelle vous souhaitez installer Sophos Security VM.

    Remarque : Sophos Security VM Protège les machines virtuelles clientes même si leurs modèles sont stockées dans différentes banques de données.

12. Dans **IP settings for the Sophos Security VM**, saisissez les paramètres IP de tous les réseaux sur lesquels vous souhaitez protéger les machines virtuelles clientes. Une Sophos Security VM peut protéger des machines virtuelles sur plusieurs réseaux.

    a) Dans **Select virtual LAN** (ESXi) ou **Select vSwitch** (Hyper-V), sélectionnez ceux qui sont disponibles.

    b) Saisissez l'adresse IPv4 statique dans **Static IPv4 address**. Seules des adresses statiques peuvent être utilisées.

    c) Saisissez le masque de sous-réseau dans **Subnet mask**.

    d) Saisissez le suffixe du domaine dans **Domain suffix**.

    e) Sélectionnez **Make Primary** s'il s'agit du réseau qui doit avoir accès à la console d'administration de Sophos. Vous pouvez uniquement utiliser un réseau principal.

    Vous pouvez utiliser le bouton « + » au-dessus des champs pour ajouter un autre réseau. Le bouton « - » supprime un réseau. Les boutons « < » et « > » vous permettent de vous déplacer entre les paramètres des différents réseaux.

13. Dans **Gateway and DNS server details for the primary network card**, saisissez les informations qui permettront à Sophos Security VM de communiquer avec la console d'administration et de télécharger les mises à jour.

    Remarque : vous pouvez saisir un ou deux (facultatif) serveurs DNS.

14. **Uniquement dans un environnement Microsoft Hyper-V :**

    Dans **Disk image location**, indiquez l'emplacement de l'image du disque de Sophos Security VM. Il peut s'agir d'un partage réseau ou d'un dossier local sur l'hôte.

15. Sur la page **Summary of installation**, vous pouvez voir les informations complètes sur l'installation. Cliquez sur **Install**.
16. Sur la page **Finished**, vous pouvez voir si l'installation de la machine virtuelle de sécurité a réussi. En cas d'échec, consultez le journal pour obtenir plus de renseignements.

    Conseil : vous pouvez cliquer sur **Start Over** pour lancer une autre installation ou réessayer en cas d'échec de l'installation.

17. La page **What to do next** vous indique comment configurer Sophos Security VM et protéger les machines virtuelles clientes.

Suivez les instructions de la section suivante pour vérifier que vous voyez bien Sophos Security VM dans Sophos Central.

Avertissement : ne « suspendez » pas Sophos Security VM. Si vous le faites, les communications avec le logiciel d'administration ne pourront pas reprendre ultérieurement.

6.6 Vérification de l'installation de Sophos Security VM

Cette section vous indique comment vérifier si Sophos Security VM est installée et dispose des ressources nécessaires.

Vérifiez si Sophos Security VM est visible

Lorsque la machine virtuelle de sécurité est installée, allez dans Sophos Central.

Vous pouvez voir les machines virtuelles de sécurité sur la page **Serveurs** dans Sophos Central. Recherchez « Sophos Security VM » dans la colonne « Nom / Syst. d'expl. ».

Pour voir uniquement Sophos Security VM, sélectionnez **Serveurs virtuels** dans la liste de filtrage.

Vérifiez s'il est nécessaire de configurer les ressources

Généralement, il n'est pas nécessaire de configurer les ressources pour Sophos Security VM. Remarque :

- **Si vous avez un grand nombre de machines virtuelles clientes** sur un seul hôte, assurez-vous que le processeur de Sophos Security VM est assez puissant pour effectuer le contrôle. Retrouvez plus de renseignements à la section Annexe : ajout de processeurs à Sophos Security VM à la page 29.
- **Le programme d'installation réserve de la mémoire pour Sophos Security VM.** Dans un environnement VMware, la haute disponibilité et les systèmes d'équilibrage de charge font des choix automatiques selon les réserves de mémoire disponibles pour les machines virtuelles. Ces choix peuvent être différents après l'installation de Sophos Security VM. Veuillez ne pas supprimer la réserve de mémoire de Sophos Security VM.

7 Installation de Sophos Guest VM Agent

Sophos Guest VM Agent doit être exécuté sur chaque machine virtuelle cliente que vous voulez protéger.

Vérifiez sur quels systèmes d'exploitation vous pouvez installer Sophos Guest VM Agent. Retrouvez plus de renseignements à la section Configuration requise pour la machine virtuelle cliente à la page 9.

1. Sur la machine virtuelle cliente, naviguez jusqu'à l'hôte sur lequel Sophos Security VM est installée. Veuillez utiliser l'adresse IP.
2. Dans le partage **Public**, recherchez le programme d'installation **SVE-Guest-Installer.exe**
3. Cliquez deux fois sur le programme d'installation pour l'exécuter ou transférez le programme d'installation sur la machine virtuelle cliente pour l'exécuter. Suivez les instructions à l'écran. Vous pouvez également :
   - Utiliser la ligne de commandes. Vous pouvez choisir de procéder à l'installation avec (interface d'utilisation limitée) ou sans (aucune interface d'utilisation) barre de progression de l'installation. Les commandes sont sensibles aux majuscules. Saisissez soit :

     Interface d'utilisation limitée : `SVE-Guest-Installer.exe SVMIPAddress=<Adresse IP de SVM> /install /passive`

     Aucune interface d'utilisation : `SVE-Guest-Installer.exe SVMIPAddress=<Adresse IP de SVM> /install /quiet`
   - Utiliser le déploiement d'une Stratégie de groupe. Retrouvez plus de renseignements dans l'article de Microsoft : http://support.microsoft.com/kb/816102

Nous vous conseillons de prendre un « snapshot » de la machine virtuelle cliente suite à l'installation de l'agent. De cette manière, vous pourrez toujours restaurer la machine virtuelle cliente en cas de besoin.

8 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 sur accès sur une machine virtuelle cliente.
- Résoudre les problèmes du contrôle sur accès.

8.1 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 à la page 18.

2. Cliquez sur la flèche du menu déroulant à côté de **Sécurité**. Vous devriez voir que Sophos pour 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 à la page 19

8.2 Test du contrôle en temps réel

Le contrôle en temps réel est la méthode principale de protection que vous devez 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 d'élimination automatique est activée**, allez sur la page **Serveurs** et cliquez sur Sophos Security VM pour ouvrir la page d'informations. Sous l'onglet **Événements**, vous devriez voir que EICAR a été détecté et éliminé.
   - **Si la fonction d'élimination 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 éliminé.

Si EICAR n'a pas été détecté, veuillez-vous reporter à la section Résolution des problèmes du contrôle en temps réel à la page 19. Si EICAR n'a pas été éliminé, veuillez le supprimer.

8.3 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 conformément aux instructions de la section Affichage des machines virtuelles clientes protégées à la page 20.
3. Assurez-vous que le Centre de sécurité Windows indique que la machine virtuelle cliente est protégée par Sophos pour 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 pour Virtual Environments pour protéger les machines virtuelles clientes exécutant d'autres produits antivirus.
6. Si le contrôle sur accès fonctionne toujours, veuillez contacter le support technique Sophos.

9 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.

10 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.

11 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 d'éliminer automatiquement les menaces détectées.
- Envoie une alerte à Sophos Central si vous devez prendre une quelconque action.

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. Consultez l'onglet **Événements** de la page d'informations de Sophos Security VM.
- 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 éliminée.
- Efface l'alerte si l'opération d'élimination automatique a réussi.

Si l'élimination automatique est indisponible ou qu'elle a échoué, une alerte affichée sur la page **Alertes** vous invite à l'éliminer manuellement.

Retrouvez plus de renseignements sur la procédure d'élimination à la section Élimination d'une menace à la page 23.

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.

12 Élimination d'une menace

Cette section aborde l'élimination manuelle et automatique des menaces.

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

Élimination automatique

Sophos Security VM élimine automatiquement les menaces détectées.

Remarque : 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.

Élimination manuelle

Vous pouvez éliminer les menaces d'une machine virtuelle cliente manuellement.

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 :

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

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.

13 Maintenance de la machine virtuelle de sécurité

Cette section vous donne des conseils sur les tâches postérieures à l'installation et de maintenance à effectuer.

- **Veuillez allumer Sophos Security VM manuellement à chaque fois que l'hôte est sorti du mode de maintenance ou du mode veille.** Veuillez procéder de la sorte avant d'allumer les machines virtuelles clientes afin qu'elles soient protégées immédiatement.
- **Ne « suspendez » pas la machine virtuelle de sécurité.** Si vous le faites, les communications avec le logiciel d’administration ne pourront pas reprendre ultérieurement.
- **Vérifiez que Sophos Security VM reçoit bien les mises à jour de sécurité de Sophos.** Vous pouvez faire ceci en vérifiant l’état de la mise à jour dans Sophos Central.
- **Sauvegardes.** Nous vous conseillons d’exclure Sophos Security VM des tâches de sauvegarde régulières afin de ne pas affecter les performances. Si Sophos Security VM doit être récupérée en raison d’échecs de l’infrastructure, nous vous conseillons de redéployer Sophos Security VM.

14 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 à la page 20. 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 à la page 26.
2. Réinstallez Sophos Guest VM Agent avec la nouvelle adresse IP de Sophos Security VM conformément à la section Installation de Sophos Guest VM Agent à la page 17.

Une fois les 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.

15 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 les fonctionnalités et cliquez sur **Désinstaller** :
   - Sophos for Virtual Environments
   - Sophos Guest VM Scanning Service
   - Sophos Virus Removal Tool.

16 Migration vers Sophos pour Virtual Environments

À partir de quels produits puis-je procéder à la migration ?

Vous pouvez procéder à la migration vers Sophos pour Virtual Environments à partir des produits suivants.

- Sophos Anti-Virus pour vShield dans un environnement VMWare ESXi.
- Sophos Anti-Virus exécuté localement sur chaque machine virtuelle cliente dans un environnement VMware ESXi ou Microsoft Hyper-V.
- Produits antivirus d'autres éditeurs dans un environnement VMware ESXi ou Microsoft Hyper-V.

Remarque : Sophos pour Virtual Environments protège les machines virtuelles clientes sur un hôte VMware ESXi même lorsqu'il est exécuté dans un environnement NSX. Toutefois, Sophos pour Virtual Environments ne s'intègre pas au gestionnaire NSX. N'installez pas de logiciel antivirus sur NSX sous peine d'affecter les performances et d'entraîner des arrêts de fonctionnement.

Remarque : Sophos pour Virtual Environments utilise Security VM pour assurer le contrôle centralisé des menaces. Dès que vous l'avez installé, les machines virtuelles clientes n'ont plus besoin des mises à jour des données sur les menaces.

Quelle est la procédure de migration ?

Suivez les étapes ci-dessous. Retrouvez plus de renseignements sur chacune de ces étapes dans le présent guide.

Remarque : si vous procédez à la migration à partir d'un logiciel antivirus tiers, sachez que :

- Sophos pour Virtual Environments a besoin d'une connexion réseau entre Security VM et les machines virtuelles clientes.
- Sophos pour Virtual Environments est compatible avec les technologies d'équilibrage de charge des machines virtuelles comme vMotion et la migration Live. Toutefois, vous bénéficierez de performances optimales si la connexion haut débit entre Security VM et les machines virtuelles clientes est maintenue.

Pour procéder à la migration :

1. Installez Sophos Security VM.

   Remarque : la nouvelle Security VM peut être installée sur le même hôte qu'une Security VM existante exécutant Sophos Anti-Virus pour vShield.

2. Rendez-vous sur la console d'administration et assurez-vous que Sophos Security VM se met à jour correctement.
3. Arrêtez l'ancienne Sophos Security VM ou désinstallez votre ancien logiciel antivirus.

Attention : vos machines virtuelles clientes ne seront plus protégées. Veuillez donc assurer leur sécurité.

4. Installez le nouveau Sophos Guest VM Agent très peu volumineux.
5. Vérifiez, conformément aux instructions du présent guide, que toutes les machines virtuelles clientes sont à présent protégées.

17 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** > **Les 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.

18 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.

19 Mentions légales

Copyright © 2017 Sophos Limited. Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise, sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement ou autre sauf si vous possédez une licence valide, auquel cas vous pouvez reproduire la documentation conformément aux termes de cette licence ou si vous avez le consentement préalable écrit du propriétaire du copyright.

Sophos, Sophos Anti-Virus et SafeGuard sont des marques déposées de Sophos Limited, Sophos Group et de Utimaco Safeware AG, partout où ceci est applicable. Tous les autres noms de produits et d'entreprises mentionnés dans ce document sont des marques ou des marques déposées de leurs propriétaires respectifs.

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.