Guide du client Symantec™ Endpoint Protection 14.3 RU3 pour Linux - French - France

September 2021

Table of Contents

Protection des périphériques Linux avec Symantec Endpoint Protection

A propos de l'agent Symantec pour Linux

L'agent Symantec pour Linux protège vos périphériques Linux contre les menaces, risques et vulnérabilités de malware. Il garantit la sécurisation proactive de vos périphériques Linux contre les malwares connus comme inconnus.

Les fonctions de protection contre les malwares sont assurées par la fonctionnalité **Antimalware** (AMD) qui protège vos périphériques Linux contre les logiciels malveillants, tels que les virus, les spywares, les ransomwares, etc., et par la fonctionnalité **Auto-Protect** (AP) qui détecte les menaces malveillantes lorsqu'une application est lancée.

Symantec recommande d'activer Auto-Protect pour assurer la protection en temps réel. Tout malware détecté est immédiatement mis en quarantaine. Si vous désactivez Auto-Protect, vous pouvez tout de même exécuter une analyse à la demande afin de détecter les malwares.

Démarrage sur l'agent Linux

Configuration système requise pour l'agent Symantec pour Linux

Cette section indique la configuration système requise pour la version la plus actuelle du produit.

Pour la configuration requise pour les versions antérieures de Symantec Endpoint Protection, ou pour la version la plus récente de la configuration requise, consultez la page web suivante :

Notes de mise à jour, nouveaux correctifs et configuration système requise pour toutes les versions d'Endpoint Protection

Table 1: Configuration système requise pour l'agent Symantec pour Linux

Composant	Configuration requise
Matériel	• Intel Pentium 4 (2 GHz) ou supérieur • 500 Mo de RAM libre (4 Go de RAM recommandés) • 2 Go d'espace disque disponible si les répertoires `/var`, `/opt` et `/tmp` partagent le même système de fichiers/volume • 500 Mo d'espace disque disponible dans chaque répertoire `/var`, `/opt` et `/tmp` s'ils se trouvent sur des volumes différents
Systèmes d'exploitation	• Amazon Linux 2 • CentOS 6, 7, 8 • Debian 9, 10 • Oracle Enterprise Linux 6, 7, 8 • Red Hat Enterprise Linux 6, 7, 8 • SuSE Linux Enterprise Server 12.x, 15.x • Ubuntu 14.04 LTS, 16.04 LTS, 18.04 LTS, 20.04 LTS Pour obtenir la liste des noyaux de système d'exploitation pris en charge, reportez-vous à la section Noyaux Linux pris en charge pour Symantec Endpoint Protection.

Composant	Configuration requise
Autres spécifications d'environnement	• Glibc Les systèmes d'exploitation exécutant une version de glibc antérieure à 2.6 ne sont pas pris en charge. • net-tools ou iproute2 Symantec Endpoint Protection utilise l'un de ces deux outils, selon ce qui est déjà installé sur l'ordinateur. • OpenSSL 1.0.2 k-FIPS ou version ultérieure

Installation de l'agent Symantec pour Linux ou du client Symantec Endpoint Protection pour Linux

(Versions 14.3 RU1 et ultérieures)

Vous installez l'agent Symantec pour Linux directement sur un périphérique Linux. Vous ne pouvez pas déployer le client Linux à distance depuis instance de Symantec Endpoint Protection Manager.

Pour installer l'agent Symantec pour Linux, créez un package d'installation dans instance de Symantec Endpoint Protection Manager, transférez-le vers une unité Linux, puis exécutez le programme d'installation. Le programme d'installation configure le nouvel agent et l'enregistre avec instance de Symantec Endpoint Protection Manager.

> **NOTE**
> L'agent Symantec pour Linux 14.3 RU1 et versions ultérieures ne peut pas s'exécuter en tant que client non géré.Toutes les tâches de gestion doivent donc être effectuées dans instance de Symantec Endpoint Protection Manager ou dans la console cloud.

Pour la version 14.3 RU1 et versions ultérieures : pour installer l'agent Symantec pour Linux

1. Dans instance de Symantec Endpoint Protection Manager, créez et téléchargez le package d'installation.
2. Placez le package sur un partage réseau, un périphérique USB ou tout autre mécanisme de partage.
   Configurez un référentiel local si les appareils sur lesquels vous souhaitez installer l'agent Linux se trouvent dans un réseau isolé ou ne disposent pas d'un accès à Internet.Voir :
   Création d'un référentiel local
3. Suivez l'une des procédures ci-dessous pour installer l'agent Linux :

Si vous avez transféré le package vers l'appareil Linux	1. Accédez à l'emplacement du dossier et exécutez la commande suivante pour que le fichier **LinuxInstaller** devienne exécutable :
	`chmod u+x LinuxInstaller`
	2. Exécutez la commande suivante pour installer l'agent :
	`./LinuxInstaller`

Si vous avez configuré un référentiel local	1. Exécutez la commande suivante :
	`./LinuxInstaller – --local-repo <URL_répertoire_LOCAL>`
	Par exemple :
	`./LinuxInstaller – --local-repo https://votre_domaine.com/sep_linux_agent/14_3RU3`

   Vous devez exécuter la commande en tant qu'utilisateur racine.
   Pour afficher la liste des options d'installation, exécutez la commande `./LinuxInstaller-h`.
4. Pour vérifier l'installation, accédez à `/usr/lib/symantec` et exécutez `./status.sh` pour confirmer que les modules sont chargés et que les démons sont en cours d'exécution :

```
./status.sh
Version de l'agent Symantec pour Linux : 14.3.450.1000
Vérification du statut de l'agent Symantec pour Linux (SEPM).
```

```
Statut du démon :
cafagent en cours d'exécution
sisamdagent en cours d'exécution
sisidsagent en cours d'exécution
sisipsagent en cours d'exécution
Statut du module :
sisevt chargé
sisap chargé
```

Notez que l'`état de communication` est uniquement disponible pour les clients gérés dans le cloud.

Pour la version 14.3 MP1 et versions antérieures

Vous installez un client Symantec Endpoint Protection géré ou autonome directement sur un ordinateur Linux. Vous ne pouvez pas déployer le client Linux à distance depuis instance de Symantec Endpoint Protection Manager. Les étapes d'installation sont semblables, qu'il s'agisse d'un client autonome ou géré.

Le seul moyen d'installer un client géré est par l'utilisation d'un package d'installation créé avec instance de Symantec Endpoint Protection Manager. Vous pouvez convertir un client autonome en client géré à tout moment en important les paramètres de communication client-serveur sur le client Linux.

Si le noyau de système d'exploitation Linux est incompatible avec le module précompilé de noyau Auto-Protect, le programme d'installation essaye de compiler un module de noyau Auto-Protect compatible. Le processus de compilation se lance automatiquement si nécessaire. Cependant, il est possible que le programme d'installation ne soit pas en mesure de compiler un module de noyau Auto-Protect compatible. Dans ce cas, Auto-Protect est installé mais désactivé. Pour plus d'informations, consultez l'article :

Supported Linux kernels for Symantec Endpoint Protection

> **NOTE**
>
> Vous devez disposer des privilèges de superutilisateur pour installer le client Symantec Endpoint Protection sur un ordinateur Linux. La procédure utilise `sudo` pour démontrer cette escalade de privilège.

Pour la version 14.3 MP1 et version antérieures : pour installer le client Symantec Endpoint Protection pour Linux

1. Copiez le package d'installation créé sur l'ordinateur Linux. Le package est un fichier.zip.
2. Sur l'ordinateur Linux, ouvrez une fenêtre d'application.
3. Accédez au répertoire d'installation avec la commande suivante :

   ```
   cd /directory/
   ```

   Où directory est le nom du répertoire dans lequel vous avez copié le fichier .zip.
4. Extrayez le contenu du fichier .zip vers un répertoire appelé `tmp` à l'aide de la commande suivante :

   ```
   unzip "InstallPackage" -d sepfiles
   ```

   Où `InstallPackage` est le nom complet du fichier .zip et `sepfiles` représente un dossier cible dans lequel le processus d'extraction place les fichiers d'installation.

   Si le dossier cible n'existe pas, le processus d'extraction le crée.
5. Accédez au répertoire `sepfiles` avec la commande suivante :

   ```
   cd sepfiles
   ```
6. Pour définir correctement les autorisations d'exécution de fichiers sur `install.sh`, utilisez la commande suivante :

   ```
   chmod u+x install.sh
   ```

7. Utilisez le script intégré pour installer Symantec Endpoint Protection avec la commande suivante :

   ```
   sudo ./install.sh -i
   ```

   Entrez votre mot de passe s'il vous est demandé.

   Ce script lance l'installation des composants de Symantec Endpoint Protection. Le répertoire d'installation par défaut est le suivant :

   ```
   /opt/Symantec/symantec_antivirus
   ```

   Le répertoire de travail par défaut pour LiveUpdate est le suivant :

   ```
   /opt/Symantec/LiveUpdate/tmp
   ```

   L'installation se termine quand l'invite de commande revient. Vous n'avez pas besoin de redémarrer l'ordinateur pour terminer l'installation.

Pour la version 14.3 MP1 et versions antérieures

Pour vérifier l'installation du client, cliquez avec le bouton gauche ou droit sur le bouclier jaune de Symantec Endpoint Protection, puis sur **Ouvrir Symantec Endpoint Protection**. L'emplacement du bouclier jaune varie selon la version Linux. L'interface utilisateur client affiche des informations sur la version du programme, les définitions de virus, l'état de la connexion serveur et la gestion.

Autres informations

- Compilation automatique pour le client Symantec Endpoint Protection pour Linux
- A propos de l'interface utilisateur graphique du client pour Linux
- Importation des paramètres de communication serveur-client dans le client Linux
- Préparation de l'installation client
- Installation de Symantec Endpoint Protection 14.x pour les distributions basées sur RedHat

Démarrage sur l'agent Linux

L'administrateur instance de Symantec Endpoint Protection Manager peut vous avoir autorisé à définir les paramètres du client sur l'agent Linux.

Table 2: Etapes de démarrage sur l'agent Linux (pour les versions 14.3 RU1 et ultérieures)

Etape	Tâche	Description
Etape 1	Installez l'agent Symantec pour Linux.	L'administrateur vous fournit le package d'installation d'un client géré ou vous envoie un lien de téléchargement de ce package par email.Voir : Installation de l'agent Symantec pour Linux ou du client Symantec Endpoint Protection pour Linux
Etape 2	Vérifiez que l'agent Linux communique avec instance de Symantec Endpoint Protection Manager ou avec la console cloud.	Pour confirmer la connexion à instance de Symantec Endpoint Protection Manager ou à la console cloud, vous pouvez exécuter la commande suivante : `/usr/lib/symantec/status.sh`
Etape 3	Vérifiez que la protection automatique est en cours d'exécution.	Pour vérifier l'état de la protection automatique, exécutez la commande suivante : `cat /proc/sisap/status`
Etape 4	Vérifiez que les définitions sont à jour.	Les définitions LiveUpdate sont disponibles dans l'emplacement suivant : `/opt/Symantec/sdcssagent/AMD/sef/definitions/`

Table 3: Etapes de démarrage sur le client Linux (version 14.3 MP1 et antérieures)

Etape	Tâche	Description
Etape 1	Installez le client pour Linux.	L'administrateur instance de Symantec Endpoint Protection Manager vous fournit le package d'installation d'un client géré ou vous envoie un lien de téléchargement de ce package par email. Vous pouvez également désinstaller un client non géré qui ne communique pas avec instance de Symantec Endpoint Protection Manager. L'utilisateur de l'ordinateur principal est chargé d'administrer l'ordinateur client ainsi que de mettre à jour le logiciel et les définitions. Vous pouvez convertir un client non géré en client géré. Voir : Installation de l'agent Symantec pour Linux ou du client Symantec Endpoint Protection pour Linux
Etape 2	Vérifiez que le client pour Linux communique avec instance de Symantec Endpoint Protection Manager.	Double-cliquez sur le bouclier Symantec Endpoint Protection. Si le client communique avec instance de Symantec Endpoint Protection Manager, les informations sur le serveur s'affichent sous **Gestion**, en regard de **Serveur**. Si l'état **Hors ligne** s'affiche, contactez l'administrateur instance de Symantec Endpoint Protection Manager. Si l'état **Gestion automatique** s'affiche, cela signifie que le client n'est pas géré. L'icône en forme de bouclier indique également l'état de la gestion et de la communication.
Etape 3	Vérifiez qu'Auto-Protect est en cours d'exécution.	Double-cliquez sur le bouclier Symantec Endpoint Protection. L'état d'Auto-Protect s'affiche sous **Etat**, en regard de **Auto-Protect**. Vous pouvez également consulter l'état d'Auto-Protect à l'aide de l'interface de ligne de commande : `sav info -a`
Etape 4	Vérifiez que les définitions sont à jour.	LiveUpdate est lancé automatiquement une fois l'installation terminée. Vous pouvez vérifier que les définitions sont à jour en double-cliquant sur le bouclier Symantec Endpoint Protection. La date des définitions s'affiche sous **Définitions**. Par défaut, LiveUpdate pour le client pour Linux s'exécute toutes les quatre heures. Si les définitions sont obsolètes, vous pouvez cliquer sur **LiveUpdate** pour l'exécuter manuellement. Vous pouvez également utiliser l'interface de ligne de commande pour exécuter LiveUpdate : `sav liveupdate -u`
Etape 5	Exécutez une analyse.	Par défaut, le client Linux géré analyse l'ensemble des fichiers et dossiers tous les jours à 12 h 30. Toutefois, vous pouvez lancer une analyse manuelle à l'aide de l'interface de ligne de commande : sav manualscan -s pathname **Note:** La commande de lancement d'une analyse manuelle requiert des privilèges de superutilisateur.

Autres informations

Symantec Endpoint Protection for Linux Frequently Asked Questions (Foire aux questions concernant Symantec Endpoint Protection pour Linux)

Mise à niveau de l'agent Symantec pour Linux

(Versions 14.3 RU1 et ultérieures)

À partir de la version 14.3 RU1, le programme d'installation du client Linux détecte et désinstalle le client Linux hérité (antérieur à la version 14.3 RU1), puis effectue une nouvelle installation. Les anciennes configurations ne seront pas conservées.

Pour mettre à niveau l'agent Symantec pour Linux

1. Dans instance de Symantec Endpoint Protection Manager, créez et téléchargez le package d'installation.
   Exportation de packages d'installation client
2. Copiez le package téléchargé sur l'appareil Linux.
3. Accédez à l'emplacement du dossier et exécutez la commande suivante pour que le fichier **LinuxInstaller** devienne exécutable :

   ```
   chmod u+x LinuxInstaller
   ```
4. Exécutez la commande suivante pour désinstaller l'agent Symantec pour Linux existant et le réinstaller :

   ```
   ./LinuxInstaller
   ```

   Exécutez la commande en tant qu'utilisateur racine.
5. Pour vérifier l'installation, accédez à `/usr/lib/symantec` et exécutez le script `./status.sh` pour confirmer que les modules sont chargés et que les démons sont en cours d'exécution :

   ```
   ./status.sh
   Version de l'agent Symantec pour Linux : 14.3.450.1000
   Vérification de l'état de l'agent Symantec pour Linux (SEPM).
   Statut du démon :
   cafagent en cours d'exécution
   sisamdagent en cours d'exécution
   sisidsagent en cours d'exécution
   sisipsagent en cours d'exécution
   Statut du module :
   sisevt chargé
   sisap chargé
   ```

Mise à jour des modules de noyau pour l'agent Symantec pour Linux

L'agent Symantec pour Linux est le même client, que vous le gériez depuis Symantec Endpoint Protection Manager ou depuis la console cloud.

(Versions 14.3 RU1 et ultérieures)

Lorsqu'une nouvelle mise à jour du noyau Linux est publiée, l'agent Symantec pour Linux pour cette plate-forme doit être mis à jour pour prendre en charge le nouveau noyau. Pour améliorer l'efficacité du processus, les modules de noyau de l'agent Linux peuvent désormais être mis à jour à l'aide du référentiel Linux.

> **NOTE**
> Assurez-vous que les agents peuvent se connecter au serveur de référentiel Symantec (https://linux-repo.us.securitycloud.symantec.com/) pour télécharger les mises à jour du module de noyau.

A chaque fois exécution sur un système RHEL, Amazon Linux, Oracle Linux ou CentOS, la commande `yum update` vérifie également si des nouveaux packages d'agent sont disponibles. Si une mise à jour est disponible, le dernier module de noyau est téléchargé et l'agent est mis à jour automatiquement. Une fois le module de noyau mis à jour, vous devez redémarrer l'instance pour que la mise à jour prenne effet.

Vous pouvez également mettre à jour le module de noyau de l'agent en exécutant la commande suivante dans l'instance. Ouvrez une fenêtre de terminal avec des privilèges racines, accédez au dossier `/usr/lib/symantec/` et exécutez la commande suivante :

```
/usr/lib/symantec/installagent.sh --update-kmod
```

Pour mettre à jour des modules de noyau sur des systèmes Ubuntu

1. Pour actualiser et mettre à jour la base de données de packages locale, saisissez les commandes suivantes :

```
sudo apt-get clean
sudo apt-get update
```

2. Pour mettre à niveau vers le module de noyau le plus récent, saisissez les commandes suivantes :
   `/usr/lib/symantec/installagent.sh --update-kmod`
   Des privilèges de superutiliseur sont requis pour cette opération.

Pour mettre à jour des modules de noyau dans un environnement restreint sans connexion Internet

1. Méthode 1 : transférez manuellement le dernier package KMOD vers un système ne disposant pas d'une connexion à Internet, rattachez le package KMOD au programme d'exécution de Linux, puis exécutez le programme d'exécution de Linux.
   1. Sur un système doté d'une connexion à Internet, téléchargez le package KMOD.
      `./LinuxInstaller -d`
   2. Copiez le package KMOD et collez-le manuellement dans l'agent que vous voulez mettre à niveau.
   3. Répertoriez les packages rattachés.
      `./LinuxInstaller -l`
   4. Rattachez le nouveau package KMOD au programme d'installation Linux.
      `tar czf - [nom_package_KMOD] >> LinuxInstaller`
   5. Assurez-vous que le nouveau package KMOD est inclus dans la liste des packages rattachés.
      `./LinuxInstaller -l`
   6. Exécutez le programme d'installation afin de mettre à jour les modules de noyau.
      `./LinuxInstaller -- --update-kmod`
2. Méthode 2 : définissez un référentiel local et modifiez ses paramètres de sorte que l'agent utilise le référentiel local et non le référentiel Symantec par défaut.
   1. Définissez le référentiel local qui héberge les packages KMOD.
      Pour plus d'informations sur la création d'un référentiel local, reportez-vous à la documentation correspondant à la distribution linux que vous utilisez.
   2. Sur l'ordinateur client, exécutez la commande suivante pour qu'il utilise le référentiel local :
      `./LinuxInstaller --local-repo <URL_référentiel_local>`
      Exemple d'URL : `--local-repo 'http://<adresse_IP_ou_nom_hôte_référentiel>:<port_facultatif>/sep_linux'`
   3. Pour mettre à jour le KMOD, exécutez :
      `./LinuxInstaller -- --update-kmod`

Si vous mettez à jour les modules de noyau du système d'exploitation, vous devez également mettre à jour la mise à jour de module de noyau correspondante pour le client Symantec Endpoint Protection. En effet, sans les modules de noyau compatibles, le client Symantec Endpoint Protection risque de ne pas fonctionner correctement et certaines fonctions risquent d'être désactivées.

Autres informations

Création et installation d'un package d'installation de l'agent Symantec Linux

Gestion du client Linux à l'aide de l'outil de ligne de commande (sav)

L'outil de ligne de commande du client Linux permet de contrôler le client Linux et de vérifier qu'il s'exécute correctement.

Pour gérer le client Linux à l'aide de l'outil de ligne de commande, voir :

(Pour les versions 14.3 RU2 et ultérieures)

L'outil de ligne de commande du client Linux permet de contrôler le client Linux et de vérifier qu'il s'exécute correctement.

Pour gérer le client Linux à l'aide de l'outil de ligne de commande

1. Sur un ordinateur client Linux, accédez à l'emplacement suivant :
   `/opt/Symantec/sdcssagent/AMD/tools`
2. Exécutez la commande sav comme suit :
   `./sav [options] commande`

Table 4: Options pour sav

Option	Description	S'applique à
`-q`	Silencieux	A partir de la version 14.3 RU2
`-h`	Affiche les options et les commandes disponibles pour sav.	A partir de la version 14.3 RU2

Table 5: Commandes pour sav

Option	Description	S'applique à
`autoprotect - e`	Active Auto-Protect. Pour vérifier l'état d'Auto-Protect, exécutez la commande suivante : `[root@localhost tools]# cat /proc/sisap/status | grep -i MODE` L'une des réponses suivantes est alors envoyée : • `mode=ENA` (en cas d'activation) • `mode=DIS` (en cas de désactivation)	A partir de la version 14.3 RU2
`autoprotect -d`	Désactive Auto-Protect.	A partir de la version 14.3 RU2
`info -d`	Affiche la version et la date des définitions de virus et de risque de sécurité utilisées sur le périphérique.	À compter de la version 14.3 RU3
`info -e`	Affiche la version du moteur d'analyse utilisé sur le périphérique.	À compter de la version 14.3 RU3
`info -p`	Affiche la version de l'agent Symantec utilisé sur le périphérique.	À compter de la version 14.3 RU3
`info -a`	Affiche l'état du module Auto-Protect utilisé sur le périphérique.	À compter de la version 14.3 RU3
`liveupdate -u`	Exécute LiveUpdate immédiatement.	À compter de la version 14.3 RU3
`manage -i <fichier>`	Importe le fichier *sylink.xml* à l'emplacement spécifié.	A partir de la version 14.3 RU2

Option	Description	S'applique à
`manualscan -s <file list>`	Démarre une analyse manuelle. <file list> indique la liste des fichiers et répertoires à analyser. Pour spécifier cette liste, entrez les divers fichiers et répertoires en les séparant par un saut de ligne et en terminant par un signal de fin de fichier, tel que CTRL-D. Si vous spécifiez un répertoire, tous ses sous-répertoires sont eux aussi analysés. Les caractères génériques sont pris en charge. Par défaut, un nombre maximum de 100 éléments peuvent être ajoutés à une analyse manuelle lancée à partir de l'interface de ligne de commande. Vous pouvez utiliser **symcfg** pour modifier la valeur DWORD de VirusProtect6MaxInput afin d'augmenter cette limite. Pour supprimer entièrement la limite, définissez la valeur de VirusProtect6MaxInput sur 0. Si vous saisissez un trait d'union (-) au lieu d'une liste de fichiers et de répertoires, la liste des noms de chemin d'accès est lue à partir de l'entrée standard. Vous pouvez utiliser des commandes qui établissent une liste de fichiers ou de noms de chemin d'accès séparés par un retour à la ligne.L'envoi d'une liste d'éléments très longue à cette commande peut nuire aux performances. Symantec recommande de limiter les listes à un maximum de quelques milliers d'éléments.	À compter de la version 14.3 RU3
`manualscan -t`	Arrête une analyse manuelle en cours.	À compter de la version 14.3 RU3

Autres informations

Résolution des problèmes liés à l'agent Symantec pour Linux

Résolution des problèmes liés à l'agent Symantec pour Linux

Le tableau ci-dessous présente les ressources de dépannage des problèmes liés à l'agent Symantec pour Linux (à partir de la version 14.3 RU1).

Table 6: ressources pour la résolution des problèmes liés à l'agent Symantec pour Linux

Action	Description
Vérification de l'état de l'agent	Pour vérifier la version et l'état de connexion de l'agent et confirmer le chargement des modules ainsi que l'exécution des démons, ouvrez `/usr/lib/symantec` et exécutez la commande suivante : `./status.sh`
Vérification des versions des packages d'agent	Ouvrez `/usr/lib/symantec` et exécutez la commande suivante : `./version.sh`

Affichage des journaux	Les journaux de l'agent Symantec pour Linux sont disponibles aux emplacements suivants :
	• Journal AMD : fournit des informations relatives à l'analyse.
	`/var/log/sdcsslog/amdlog`
	• Journal CAF : fournit des informations relatives aux activités de l'agent, telles que la communication avec le serveur, l'inscription, les commandes, les événements, etc.
	`/var/log/sdcss-caflog/`
	• Journal d'agent : fournit des informations relatives aux activités de l'agent.
	`/var/log/sdcsslog/SISIDSEvents*.csv`
	• Journal CVE : fournit des informations relatives à la communication entre instance de Symantec Endpoint Protection Manager et l'agent.
	`/var/log/sdcss-caflog/cve.log`

Action	Description
Collecte des journaux dans un fichier .zip	Vous pouvez utiliser le script `GetAgentInfo` pour collecter tous les fichiers journaux dans un fichier .zip que vous pouvez envoyer au support client. 1. Connectez-vous au système Agent Symantec pour Linux. 2. Accédez à `/opt/Symantec/sdcssagent/IPS/tools/`. 3. Ouvrez `./getagentinfo.sh` en tant qu'utilisateur racine. 4. Un fichier .zip sera créé dans le répertoire `/tmp/`. Le nom du fichier apparaîtra comme suit : `20201208_184935_0001_CU_mihsan-rhel8.zip`. `-out <répertoire>` vous permet de modifier l'emplacement et le nom du fichier .zip généré.
Modification du niveau de journalisation CVE	Par défaut, le niveau de journalisation CVE est défini sur `infos`. Vous pouvez définir le niveau de journalisation sur `debug` dans le fichier `/opt/Symantec/cafagent/bin/log4j.properties`. Après avoir modifié le fichier, vous devez redémarrer le service `cafagent`.

Modification du niveau de journalisation AMD	Par défaut, le niveau de journalisation AMD est défini sur `infos`.
	Vous pouvez remplacer le niveau de journalisation `trace` par `avertissement` ou `erreur` dans le fichier `/opt/Symantec/sdcssagent/AMD/system/AntiMalware.ini`.
	Note: Avant de modifier le fichier AntiMalware.ini, arrêtez l'agent sisamdagent :
	`service sisamdagent stop`
	Note: Après avoir modifié le fichier, redémarrez le service :
	`service sisamdagent start`

Désinstallation de l'agent Symantec pour Linux ou du client Symantec Endpoint Protection pour Linux

Vous pouvez désinstaller le client Symantec Endpoint Protection pour Linux avec le script fourni à l'installation.

> **NOTE**
>
> Vous devez disposer des privilèges de superutilisateur pour désinstaller le client Symantec Endpoint Protection sur un ordinateur Linux. La procédure utilise `sudo` pour démontrer cette escalade de privilège.

Pour la version 14.3 RU1 et versions ultérieures : pour désinstaller l'agent Symantec pour Linux

1. Sur l'ordinateur Linux, ouvrez une fenêtre d'application.
2. Accédez au répertoire suivant :
   `/usr/lib/symantec/`
3. Pour désinstaller l'agent Symantec pour Linux, exécutez le script intégré suivant :
   `./uninstall.sh`
4. Lorsque la désinstallation est terminée et que l'invite de redémarrage s'affiche, redémarrez l'ordinateur.
   Notez que le script `uninstall.sh` supprimera tous les composants de l'agent Symantec pour Linux (`sdcss-caf`, `sdcss-sepagent` et `sdcss-kmod`).

```
[root@localhost symantec]# ./uninstall.sh
Exécution de ./uninstall.sh (PWD /usr/lib/symantec ; version 2.2.4.41)
Désinstallation de l'agent Symantec pour Linux (SEPM) ...
Suppression des packages sdcss-caf sdcss-sepagent sdcss-kmod sdcss-scripts
L'agent Symantec pour Linux (SEPM) a été désinstallé.
Le redémarrage est requis pour terminer la désinstallation.
Redémarrez votre ordinateur dès que possible.
```

Pour la version 14.3 MP1 et version antérieures : pour désinstaller le client Symantec Endpoint Protection pour Linux

1. Sur l'ordinateur Linux, ouvrez une fenêtre d'application.
2. Accédez au dossier d'installation de Symantec Endpoint Protection à l'aide de la commande suivante :

   ```
   cd /opt/Symantec/symantec_antivirus
   ```

   Le chemin d'accès correspond au chemin d'installation par défaut.
3. Utilisez le script intégré pour désinstaller Symantec Endpoint Protection avec la commande suivante :

   ```
   sudo ./uninstall.sh
   ```

   Entrez votre mot de passe s'il vous est demandé.

   Ce script lance la désinstallation des composants de Symantec Endpoint Protection.
4. A l'invite, saisissez `Y`, puis appuyez sur **Entrée**.

   La désinstallation se termine quand l'invite de commande revient.

   NOTE

   Sur certains systèmes d'exploitation, si le contenu du dossier `/opt` est uniquement constitué des fichiers du client Symantec Endpoint Protection, le script de désinstallation supprime également `/opt`. Pour recréer ce dossier, entrez la commande suivante : `sudo mkdir /opt`

Pour procéder à la désinstallation à l'aide d'un gestionnaire de package ou de logiciel, consultez la documentation spécifique de votre produit Linux.


Symantec
A Division of Broadcom