System Center Endpoint Protection

Manuel d'installation et guide de l'utilisateur

Red Hat Enterprise Linux Server 5, 6
SUSE Linux Enterprise 10, 11
CentOS 5, 6
Debian Linux 5, 6
Ubuntu Linux 10.04, 12.04
Oracle Linux 5, 6

Microsoft

Microsoft® System Center Endpoint Protection

Table des matières

Introduction

Merci d'utiliser System Center Endpoint Protection. Le moteur d'analyse de pointe de Microsoft offre des vitesses d'analyse et de détection inégalés. Peu volumineux, c'est le choix idéal pour tout serveur sur système d'exploitation Linux.

Fonctionnalité principale

Analyse à la demande

L'analyse à la demande peut être démarrée par un utilisateur privilégié (généralement un administrateur système) par l'intermédiaire de l'interface à ligne de commande, de l'interface Web ou de l'outil de planification automatique du système d'exploitation (cron par exemple). Le terme *à la demande* fait référence aux objets du système de fichiers analysés par une demande de l'utilisateur ou du système.

Protection en temps réel

La protection en temps réel est appelée dès qu'un utilisateur et/ou un système d'exploitation essaient d'accéder aux objets du système de fichiers. Elle clarifie également l'utilisation du terme *à l'accès*, car une analyse est déclenchée par une tentative d'accès aux objets du système de fichiers.

Fonctionnalités principales du système

Algorithmes moteur avancés

Les algorithmes du moteur d'analyse antivirus Microsoft offrent le meilleur niveau de détection et les analyses les plus rapides.

Plusieurs processeurs

System Center Endpoint Protection est développé pour s'exécuter sur un ou plusieurs processeurs.

Heuristique avancée

System Center Endpoint Protection comprend une heuristique avancée pour les vers Win32, les infections par backdoor et d'autres formes de logiciel malveillant.

Fonctionnalités intégrées

Les systèmes d'archive intégrés décompressent les objets archivés sans qu'aucun programme externe soit nécessaire.

Vitesse et efficacité

Pour augmenter la vitesse et l'efficacité du système, l'architecture de System Center Endpoint Protection est basée sur le démon (programme d'exécution) en cours d'exécution vers lequel toutes les demandes d'analyse sont envoyées.

Sécurité améliorée

Tous les démons d'exécution (à l'exception de scep_dac) fonctionnent sous un compte utilisateur non privilégié afin d'améliorer la sécurité.

Configuration sélective

Le système prend en charge la configuration sélective en fonction de l'utilisateur ou du client/serveur.

Plusieurs niveaux de consignation

Vous pouvez configurer plusieurs niveaux de consignation pour obtenir des informations sur l'activité du système et les infiltrations.

Interface Web

La configuration et l'administration du logiciel sont disponibles par l'intermédiaire d'une interface Web intuitive et conviviale.

Aucune bibliothèque externe

L'installation de System Center Endpoint Protection ne nécessite aucune bibliothèque ni programme externe à l'exception de LIBC.

Notification définie par l'utilisateur

Le système peut être configuré pour informer certains utilisateurs en cas de détection d'une infiltration ou d'autres événements importants.

Configuration système minimale

Pour s'exécuter correctement, System Center Endpoint Protection n'a besoin que de 16 Mo d'espace sur le disque dur et 32 Mo de mémoire RAM. Il est compatible avec les versions 2.2.x, 2.4.x et 2.6.x du noyau du système d'exploitation Linux.

Performances et évolutivité

Qu'il s'exécute sur de petits serveurs de bureau peu puissants ou sur des serveurs de fournisseur de services Internet pouvant gérer des milliers d'utilisateurs, System Center Endpoint Protection offre les performances et l'évolutivité que vous attendez d'une solution UNIX, ainsi que la sécurité inégalée des produits de sécurité Microsoft.

Terminologie et abréviations

Dans cette section, nous allons examiner les termes et les abréviations utilisés dans ce document. Le formatage en gras est réservé aux noms des composants produit et également aux nouveaux termes et abréviations. Les termes et abréviations définis dans ce chapitre sont développés plus loin dans ce document.

SCEP

SCEP est le sigle standard du produit de sécurité développé par Microsoft pour les systèmes d'exploitation Linux. C'est également le nom du logiciel qui contient les produits.

SCEP daemon

Contrôle principal et démon d'analyse du système SCEP : *scep_daemon*.

Répertoire de base SCEP

Répertoire dans lequel sont stockés les modules chargeables SCEP contenant la base de signatures des virus. L'abréviation *@BASEDIR@* est utilisée pour les références futures à ce répertoire. La valeur *@BASEDIR@* (en fonction du système d'exploitation) est répertoriée ci-dessous :

```
Linux: /var/opt/microsoft/scep/lib
```

Répertoire de configuration SCEP

Répertoire dans lequel sont stockés tous les fichiers liés à la configuration System Center Endpoint Protection. L'abréviation *@ETCDIR@* est utilisée pour les références futures à ce répertoire. La valeur *@ETCDIR@* (en fonction du système d'exploitation) est répertoriée ci-dessous :

```
Linux: /etc/opt/microsoft/scep
```

Fichier de configuration SCEP

Fichier de configuration principal de System Center Endpoint Protection. Le chemin absolu du fichier est le suivant :

@ETCDIR@/scep.cfg

Répertoire des fichiers binaires SCEP

Répertoire dans lequel sont stockés les fichiers binaires System Center Endpoint Protection. L'abréviation *@BINDIR@* est utilisée pour les références futures à ce répertoire. La valeur *@BINDIR@* (en fonction du système d'exploitation) est répertoriée ci-dessous :

```
Linux: /opt/microsoft/scep/bin
```

Répertoire des fichiers binaires du système SCEP

Répertoire dans lequel sont stockés les fichiers binaires du système System Center Endpoint Protection. L'abréviation *@SBINDIR@* est utilisée pour les références futures à ce répertoire. La valeur *@SBINDIR@* (en fonction du système d'exploitation) est répertoriée ci-dessous :

```
Linux: /opt/microsoft/scep/sbin
```

Répertoire des fichiers d'objet SCEP

Répertoire dans lequel sont stockés les fichiers et les bibliothèques d'objet System Center Endpoint Protection. L'abréviation *@LIBDIR@* est utilisée pour les références futures à ce répertoire. La valeur *@LIBDIR@* (en fonction du système d'exploitation) est répertoriée ci-dessous :

```
Linux: /opt/microsoft/scep/lib
```

Installation

System Center Endpoint Protection est distribué sous forme de fichier binaire :

```
scep.i386.ext.bin
```

Dans le fichier binaire ci-dessus, *'ext'* est le suffixe qui dépend de la distribution du système d'exploitation Linux. Il s'agit de « deb » pour Debian, de « rpm » pour RedHat et SuSE, de « tgz » pour les autres distributions sur des systèmes d'exploitation Linux.

Pour installer ou mettre à niveau le produit, utilisez la commande suivante :

```
sh ./scep.i386.ext.bin
```

afin d'afficher le contrat de licence de l'utilisateur du produit. Lorsque vous acceptez le contrat de licence, le logiciel d'installation est placé dans le répertoire de travail en cours. Les informations concernant l'installation, la désinstallation ou la mise à niveau du logiciel s'affichent.

Après l'installation du logiciel, vous pouvez vérifier que le service SCEP principal s'exécute à l'aide de la commande suivante :

```
ps -C scep_daemon
```

Lorsque vous appuyez sur la touche ENTRÉE, le message suivant (ou un message semblable) apparaît :

```
 PID TTY TIME CMD
2226 ? 00:00:00 scep_daemon
2229 ? 00:00:00 scep_daemon
```

Deux processus de démon SCEP au moins s'exécutent en arrière-plan. Le premier PID représente le processus et le gestionnaire de threads du système. L'autre représente le processus d'analyse SCEP.

Installation d'un pack de langues

Pour installer le pack de langue souhaité pour System Center Endpoint Protection, utilisez la commande suivante :

```
sh ./scep-lang.lng.bin
```

'lng' doit être remplacé par le code de langue du fichier à importer.

Lorsque l'information *Installation completed successfully* apparaît, mettez à jour la variable système LANG et, si nécessaire, l'environnement. L'installation du pack de langue est terminée.

Chaque pack de langue se compose des éléments suivants :

- Interface Web localisée
- Résultats de console localisés des agents et commandes SCEP
- Documentation au format PDF et traduite

Présentation de l'architecture

Une fois l'application System Center Endpoint Protection installée, vous devez connaître son architecture.

Le système est composé des éléments suivants :

COMPOSANT PRINCIPAL

L'élément essentiel de System Center Endpoint Protection est le démon SCEP (scep_daemon). Le démon utilise la bibliothèque API libscep.so et les modules de chargement em00X_xx.dat SCEP qui fournissent les tâches système telles que l'analyse et la maintenance des processus des agents, la maintenance du système de soumission des exemples, la journalisation, la notification, etc. Reportez-vous à la page de manuel *scep_daemon(8)* pour obtenir des informations.

AGENTS

Les modules des agents SCEP ont pour objet d'intégrer SCEP dans l'environnement serveur Linux.

UTILITAIRES

Les modules d'utilitaire permettent de gérer le système simplement et efficacement. Ils permettent de réaliser les tâches système : gestion de la quarantaine, configuration du système et mise à jour.

CONFIGURATION

La configuration correcte de votre système de sécurité est l'élément essentiel. Ce chapitre vise à présenter tous les composants connexes. Il est également fortement recommandé de comprendre le fichier *scep.cfg*, car il contient des informations essentielles à la configuration de System Center Endpoint Protection.

Une fois le produit installé, tous ses composants de configuration sont stockés dans le répertoire de configuration SCEP. Le répertoire comprend les fichiers suivants :

@ETCDIR@/scep.cfg

Il s'agit du fichier de configuration le plus important, car il contrôle tous les aspects principaux de la fonctionnalité du produit. Le fichier scep.cfg est composé de plusieurs sections, chacune d'entre elles comportant différents paramètres. Le fichier contient une section globale et plusieurs sections d'agent ; les noms des sections sont tous entre chevrons. Les paramètres de la section globale sont utilisés pour définir les options de configuration du démon SCEP, ainsi que les valeurs par défaut de la configuration du moteur d'analyse SCEP. Les paramètres des sections d'agent permettent de définir les options de configuration des modules utilisés pour intercepter différents types de flux de données de l'ordinateur et/ou de son réseau, et de le préparer pour l'analyse. Outre les différents paramètres utilisés pour la configuration du système, des règles régissent également l'organisation du fichier. Pour obtenir des informations détaillées sur l'organisation la plus efficace de ce fichier, reportez-vous aux pages de manuel *scep.cfg(5)* et *scep_daemon(8)*, ainsi qu'aux pages de manuel correspondant aux différents agents.

@ETCDIR@/certs

Ce répertoire est utilisé pour stocker les certificats utilisés par l'interface Web SCEP pour l'authentification. Pour plus d'informations, reportez-vous à la page de manuel *scep_wwwi(8)*.

@ETCDIR@/scripts/daemon_notification_script

Si ce script est activé par le paramètre *'exec_script'* du fichier de configuration SCEP, il est exécuté si une infiltration est détectée par le système antivirus. Il envoie à l'administrateur système un message d'information sur l'événement.

Intégration avec les services du système de fichiers

Ce chapitre décrit la configuration de l'analyse à la demande et de la protection en temps réel qui offre au système de fichiers la protection la plus efficace contre les virus et les vers. La puissance de l'analyse de System Center Endpoint Protection provient de la commande de l'analyse à la demande *'scep_scan'* et de la commande de l'analyse à l'accès *'scep_dac'*. La version Linux de System Center Endpoint Protection offre une technique supplémentaire d'analyse à l'accès qui utilise le module de bibliothèque de préchargement *libscep_pac.so*. Toutes ces commandes sont décrites dans les sections suivantes.

Analyse à la demande

L'analyse à la demande peut être démarrée par un utilisateur privilégié (généralement un administrateur système) par l'intermédiaire de l'interface à ligne de commande, de l'interface Web ou de l'outil de planification automatique du système d'exploitation (cron par exemple). Le terme *à la demande* fait référence aux objets du système de fichiers analysés lors d'une demande de l'utilisateur ou du système.

L'analyseur à la demande ne nécessite aucune configuration particulière pour fonctionner. Une fois le logiciel SCEP installé, l'analyseur à la demande peut être exécuté immédiatement à l'aide de l'interface de la ligne de commande ou de l'outil Planificateur. Pour exécuter l'analyseur à la demande depuis la ligne de commande, utilisez la syntaxe suivante :

```
@SBINDIR@/scep_scan [option(s)] FILES
```

FILES correspondant à la liste des répertoires et/ou fichiers à analyser.

Plusieurs options de ligne de commande sont disponibles avec l'analyseur à la demande SCEP. Pour afficher la liste complète des options, reportez-vous à la page de manuel *scep_scan(8)*.

Protection en temps réel par Dazuko

La protection en temps réel est appelée lorsqu'un ou plusieurs utilisateurs et/ou le système d'exploitation accèdent aux objets du système de fichiers. Elle explique également le terme *à l'accès*, car une analyse est déclenchée par une tentative d'accès à un objet sélectionné du système de fichiers.

La technique de l'analyseur à l'accès SCEP utilise la technologie de module de noyau Dazuko (se prononce da-tzu-ko) et se base sur l'interception des appels du noyau. Le projet Dazuko est en Open Source, ce qui signifie que son code source est distribué gratuitement. Les utilisateurs peuvent ainsi compiler le module du noyau pour leurs propres noyaux personnalisés. Notez que le module de noyau Dazuko ne fait pas partie du produit SCEP et qu'il doit être compilé et installé dans le noyau avant l'utilisation de la commande à l'accès *scep_dac*. Avec la technique Dazuko, l'analyse à l'accès est indépendante du type de système de fichiers utilisé. Elle permet également d'analyser les objets du système de fichiers par l'intermédiaire de Network File System (NFS), de Nettalk et de Samba.

Important : avant de passer aux informations détaillées concernant la configuration et l'utilisation de l'analyse à l'accès, il convient de noter que l'analyseur a d'abord été développé et testé pour protéger les systèmes de fichiers montés en externe. S'il existe plusieurs systèmes de fichiers qui ne sont pas montés en externe, vous devrez les exclure du contrôle de l'accès aux fichiers afin d'éviter tout blocage du système. Par exemple, le répertoire *'/dev'* et tous les répertoires utilisés par SCEP doivent être exclus.

Principe

La protection en temps réel *scep_dac* (SCEP Dazuko-powered file Access Controller) est un programme résident qui permet de surveiller et de contrôler le système de fichiers. Chaque objet du système de fichiers est analysé en fonction des types d'accès personnalisables aux fichiers. La version actuelle prend en charge les types d'événement suivants :

Événements en cours

Pour activer ce type d'accès aux fichiers, définissez la valeur du paramètre *'event_mask'* à ouvrir dans la section **[fac]** du fichier scep.cfg. La partie ON_OPEN du masque d'accès Dazuko est activée.

Événements fermés

Pour activer ce type d'accès aux fichiers, définissez la valeur du paramètre *'event_mask'* à fermer dans la section **[fac]** du fichier scep.cfg. La partie ON_OPEN du masque d'accès Dazuko est activée. Les parties ON_CLOSE et ON_CLOSE_MODIFIED du masque d'accès Dazuko sont activées.

Remarque : certaines versions du noyau du système d'exploitation ne prennent pas en charge l'interception des événements ON_CLOSE. Dans ce cas, les événements fermés sont surveillés par *scep_dac*.

Événements d'exécution

Pour activer ce type d'accès aux fichiers, définissez la valeur du paramètre *'event_mask'* à exécuter dans la section **[fac]** du fichier scep.cfg. La partie ON_EXEC du masque d'accès Dazuko est activée.

La protection en temps réel garantit que tous les fichiers ouverts, fermés et exécutés sont d'abord analysés par *scep_daemon* qui y recherche des virus éventuels. En fonction des résultats de l'analyse, l'accès aux différents fichiers est refusé ou autorisé.

Installation et configuration

Le module du noyau Dazuko doit être compilé et installé dans le noyau en cours d'exécution avant l'initialisation de *scep_dac*. Pour plus d'informations sur la compilation et l'installation de Dazuko, reportez-vous à :

http://www.dazuko.org

Une fois que Dazuko est installé, consultez les sections **[global]** et **[fac]** du fichier de configuration SCEP (scep.cfg) et modifiez-les. Le bon fonctionnement de la protection en temps réel dépend de la configuration de l'option *'agent_type'* dans la section **[fac]** de ce fichier. Vous devez également définir les objets du système de fichiers (répertoires et fichiers) que la protection en temps réel doit surveiller. Pour ce faire, définissez les paramètres des options *'ctl_incl'* et *'ctl_excl'*, situées également dans la section **[fac]**. Après avoir modifié le fichier scep.cfg, vous pouvez forcer la relecture de la nouvelle configuration en rechargeant le démon SCEP.

Conseils

Pour que le module Dazuko se charge avant l'initialisation du démon *scep_dac*, effectuez les opérations suivantes :

Placez une copie du module Dazuko dans l'un des répertoires suivants réservés aux modules de noyau :

```
/lib/modules
```

ou

```
/modules
```

Utilisez les utilitaires de noyau 'depmod' et 'modprobe' (Pour le système d'exploitation BSD, reportez-vous à 'kldconfig' et à 'kldload') pour gérer les dépendances et initialiser le module Dazuko qui vient d'être ajouté.

Dans le script d'initialisation de scep_daemon '/etc/init.d/scep_daemon', insérez la ligne suivante avant l'instruction d'initialisation du démon :

```
/sbin/modprobe dazuko
```

Pour le système d'exploitation BSD, la ligne

```
/sbin/kldconfig dazuko
```

doit être insérée dans le script '/usr/local/etc/rc.d/scep_daemon.sh'.

Avertissement ! Il est extrêmement important d'exécuter ces étapes dans l'ordre exact dans lequel elles sont indiquées. Si le module de noyau ne se trouve pas dans le répertoire des modules correspondants, il ne se charge pas correctement et le système se bloque.

Protection en temps réel à l'aide de la bibliothèque de préchargement LIBC

Dans les sections précédentes, nous avons décrit l'intégration de la protection en temps réel Dazuko avec les services de système de fichiers Linux/BSD. L'utilisation de Dazuko n'est peut-être pas envisageable dans toutes les situations, notamment si les administrateurs système gèrent des systèmes essentiels dans lesquels :

- le code source et/ou les fichiers de configuration liés au noyau en cours d'exécution ne sont pas disponibles ;
- le noyau est plus monolithique que modulaire ;
- le module Dazuko ne prend pas en charge le système d'exploitation.

Dans l'un de ces cas, la technique d'analyse à l'accès basée sur la bibliothèque de préchargement LIBC doit être utilisée. Reportez-vous aux rubriques suivantes de cette section pour obtenir des informations détaillées. Veuillez noter que cette section ne concerne que les utilisateurs de système d'exploitation Linux et qu'elle contient des informations sur le fonctionnement, l'installation et la configuration de l'analyseur à l'accès à l'aide de la bibliothèque de préchargement *'libscep_pac.so'*.

Principe

La bibliothèque *libscep_pac.so* de protection en temps réel (SCEP Preload library based file Access Controller) est une bibliothèque d'objets partagés qui est activée au démarrage du système. Cette bibliothèque est utilisée pour les appels LIBC par serveurs de systèmes de fichiers tels que les serveurs FTP ou Samba. Chaque objet de système de fichier est analysé en fonction des types d'événements personnalisables d'accès aux fichiers. La version actuelle prend en charge les types d'événement suivants :

Événements en cours

Ce type d'accès aux fichiers est activé si le mot *'open'* figure dans le paramètre *'event_mask'* du fichier esest.cfg (section **[fac]**).

Événements fermés

Ce type d'accès aux fichiers est activé si le mot *'close'* figure dans le paramètre *'event_mask'* du fichier scep.cfg (section **[fac]**). Dans ce cas, toutes les fonctions de fermeture des descripteurs de fichiers et des flux FILE de la bibliothèque LIBC sont interceptées.

Événements d'exécution

Ce type d'accès aux fichiers est activé si le mot *'exec'* figure dans le paramètre *'event_mask'* du fichier scep.cfg (section **[fac]**). Dans ce cas, toutes les fonctions d'exécution de la bibliothèque LIBC sont interceptées.

Le démon SCEP analyse tous les fichiers ouverts, fermés et exécutés pour y rechercher d'éventuels virus. En fonction des résultats de ces analyses, l'accès aux fichiers est refusé ou autorisé.

Installation et configuration

Le module de bibliothèque *libscep_pac.so* est installé à l'aide d'un mécanisme standard de bibliothèques préchargées. Vous devez définir la variable d'environnement *'LD_PRELOAD'* avec le chemin absolu vers la bibliothèque *libscep_pac.so*. Pour plus d'informations, reportez-vous à la page de manuel *ld.so(8)*.

Remarque : il est important que la variable d'environnement *'LD_PRELOAD'* soit définie uniquement pour les processus du démon du serveur réseau (ftp, Samba, etc.) qui sont contrôlés par la protection en temps réel. En général, il n'est pas recommandé de précharger les appels de la bibliothèque LIBC pour tous les processus du système d'exploitation, car cela peut ralentir les performances du système et même le bloquer. Par conséquent, le fichier '/etc/ld.so.preload' ne doit pas être utilisé et la variable d'environnement 'LD_PRELOAD' ne doit pas être exportée globalement. Ces deux commandes remplaceraient tous les appels LIBC appropriés et le système se bloquerait pendant l'initialisation.

Afin de vous assurer que l'interception ne porte que sur les appels d'accès aux fichiers appropriés d'un système de fichiers, les instructions d'exécutable peuvent être ignorées à l'aide de la ligne suivante :

```
LD_PRELOAD=@LIBDIR@/libscep_pac.so COMMAND COMMAND-ARGUMENTS
```

'COMMAND COMMAND-ARGUMENTS' est l'instruction d'exécutable d'origine.

Consultez les sections **[global]** et **[fac]** du fichier de configuration SCEP (scep.cfg) et modifiez-les. Pour que l'analyse à l'accès fonctionne correctement, vous devez définir les objets du système de fichiers (répertoires et fichiers) que la bibliothèque de préchargement doit surveiller. Pour ce faire, définissez les paramètres des options *'ctl_incl'* et *'ctl_excl'*, situées également dans la section **[fac]** du fichier de configuration SCEP. Après avoir modifié le fichier scep.cfg, vous pouvez forcer la relecture de la nouvelle configuration en rechargeant le démon SCEP.

Conseils

Afin d'activer la protection en temps réel immédiatement après le démarrage du système de fichiers, la variable d'environnement *'LD_PRELOAD'* doit être définie dans le script d'initialisation du serveur de fichiers réseau approprié.

Exemple : supposons que vous souhaitez que l'analyse à l'accès surveille tous les événements d'accès au système de fichiers immédiatement après le démarrage du serveur Samba. Dans le script d'initialisation du démon Samba (/etc/init.d/smb), nous remplacerions l'instruction

```
daemon /usr/sbin/smbd $SMBDOPTIONS
```

par la ligne suivante :

```
LD_PRELOAD=@LIBDIR@/libscep_pac.so daemon /usr/sbin/smbd $SMBDOPTIONS
```

De cette manière, les objets sélectionnés du système de fichiers et contrôlés par Samba sont analysés au démarrage du système.

Mécanismes SCEP importants

Stratégie de gestion des objets

La stratégie de gestion des objets permet de filtrer les objets analysés en fonction de leur état. Cette fonctionnalité est basée sur les options de configuration suivantes :

- action_av
- action_av_infected
- action_av_notscanned
- action_av_deleted

Pour obtenir des informations détaillées sur ces options, reportez-vous à la page de manuel *scep.cfg(5)*.

Chaque objet traité est d'abord géré en fonction de la configuration de l'option *'action_av'*. Si cette option est définie sur *'accept'* (ou *'defer'*, *'discard'*, *'reject'*), l'objet est accepté (reporté, supprimé ou rejeté). Si l'option est définie sur *'scan'*, l'objet est analysé et le système recherche toute infiltration de virus. Enfin, si l'option *'av_clean_mode'* est définie sur *'yes'*, l'objet est également nettoyé. En outre, les options de configuration *'action_av_infected'*, *'action_av_notscanned'* et *'action_av_deleted'* permettent d'évaluer plus précisément la gestion des objets. Si une action *'accept'* est réalisée en résultat de ces trois options d'action, l'objet est accepté. Dans le cas contraire, l'objet est bloqué.

Configuration propre à un utilisateur

Le mécanisme de configuration propre à un utilisateur offre un degré élevé de personnalisation et de fonctionnalité. Il permet à l'administrateur système de définir des paramètres d'analyse antivirus SCEP en fonction de l'utilisateur qui accède aux objets du système de fichiers.

La page de manuel *scep.cfg(5)* contient des informations détaillées sur cette fonctionnalité. Nous allons proposer dans cette section un court exemple de configuration personnalisée en fonction de l'utilisateur.

Dans cet exemple, l'objectif est d'utiliser le module *scep_dac* pour contrôler les événements d'accès ON_OPEN et ON_EXEC pour un disque externe monté dans le répertoire /home. Le module peut être configuré dans la section **[fac]** du fichier de configuration SCEP. Voici l'exemple :

```
[fac]
agent_type = "dazuko"
event_mask = "open"
ctl_incl = "/home"
action_av = "scan"
```

Pour que vous puissiez indiquer les paramètres d'analyse propres à un utilisateur, le paramètre *'user_config'* doit indiquer le nom du fichier de configuration dans lequel sont stockées les règles d'analyse. Dans cet exemple, le fichier de configuration s'intitule *'scep_dac_spec.cfg'* et il est stocké dans le répertoire de configuration SCEP (ce répertoire est basé sur votre système d'exploitation. Reportez-vous à la page Terminologie et abréviations).

```
[fac]
agent_type = "dazuko"
event_mask = "open"
ctl_incl = "/home"
action_av = "scan"
user_config = "scep_dac_spec.cfg"
```

Une fois le paramètre de fichier *'user_config'* indiqué dans la section **[fac]**, le fichier *'scep_dac_spec.cfg'* doit être créé dans le répertoire de configuration SCEP. Enfin, vous devez ajouter les règles d'analyse souhaitées.

```
[username]
action_av = "reject"
```

Dans la partie supérieure de la section spécifique, saisissez le nom de l'utilisateur auquel ces différentes règles s'appliquent. Cette configuration permet à tous les autres utilisateurs qui essaient d'accéder au système de fichiers d'être traités normalement. En d'autres termes, tous les objets du système de fichiers auxquels les autres utilisateurs accèdent font l'objet d'une analyse visant à y détecter toute infiltration, à l'exception de l'utilisateur *'username'* dont l'accès est rejeté (bloqué).

Planificateur

Le planificateur englobe différentes opérations : exécution de tâches planifiées à un moment donné ou sur un événement spécifique, gestion et lancement de tâches avec une configuration et des propriétés prédéfinies, etc. La configuration et les propriétés des tâches peuvent influencer les date et heure du lancement. Elles diversifient également les tâches en permettant d'utiliser des profils personnalisés pendant l'exécution des tâches.

L'option *'scheduler_tasks'* est commentée par défaut, ce qui provoque l'application de la configuration du planificateur par défaut. Dans le fichier de configuration SCEP, tous les paramètres et toutes les tâches sont séparés par des points-virgules. Tous les autres points-virgules (et les barres obliques inversées) doivent être placés dans une séquence d'échappement avec une barre oblique inverse. Chaque tâche comporte 6 paramètres et la syntaxe est la suivante :

- id - numéro unique.
- name - description de la tâche.
- flags - drapeaux permettant de désactiver la tâche spécifique du planificateur.
- failstart - indique ce qui doit être fait si la tâche n'a pas pu être exécutée à la date planifiée.
- datespec - spécification de date régulière avec 6 champs (crontab correspondant à toute l'année par exemple), d'une date récurrente ou d'une option de nom d'événement.
- command - il peut s'agir d'un chemin absolu vers une commande suivi de ses arguments ou d'un nom de commande particulier avec le préfixe '@' (mise à jour antivirus par exemple : *@update*).

```
#scheduler_tasks = "id;name;flags;failstart;datespec;command;id2;name2;...";
```

Les noms d'événement suivants peuvent être utilisés à la place de l'option datespec :

- start - démarrage du démon.
- startonce - démarrage du démon, mais au moins une fois par jour.
- engine - mise à jour réussie du moteur.
- login - démarrage de la connexion à l'interface Web.
- threat - menace détectée.
- notscanned - Fichier non analysé.

Pour afficher la configuration actuelle du planificateur, utilisez l'interface Web ou exécutez la commande suivante :

```
cat @ETCDIR@/scep.cfg | grep scheduler_tasks
```

Pour obtenir la description complète du planificateur et de ses paramètres, reportez-vous à la section Planificateur de la page de manuel *scep_daemon(8)*.

Interface Web

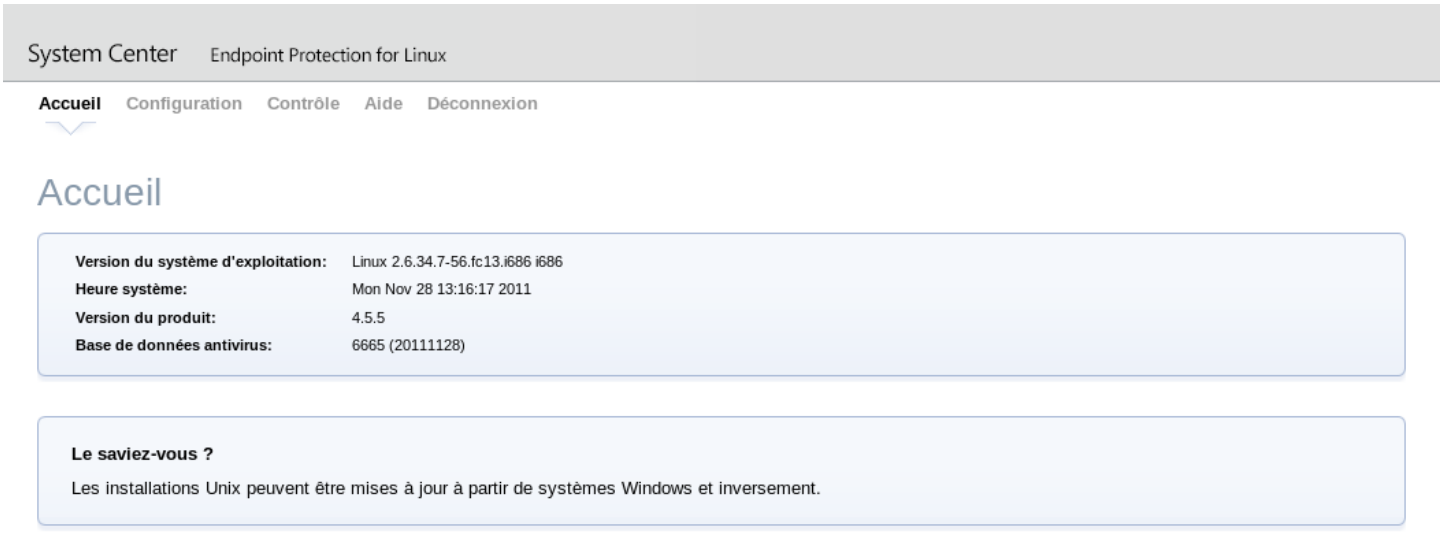
L'interface web conviviale permet de configurer et d'administrer les systèmes de sécurité SCEP. Ce module est un agent distinct et doit être activé explicitement. Pour configurer rapidement l'*interface Web*, définissez les options suivantes dans le fichier de configuration SCEP et redémarrez le démon SCEP :

```
[wwwi]
agent_enabled = yes
listen_addr = address
listen_port = port
username = name
password = pass
```

Remplacez le texte en italique par vos propres valeurs et saisissez l'adresse suivante dans votre navigateur : *'https://adresse:port'* (notez le protocole HTTPS). Connectez-vous à l'aide des informations *'username/password'*. Les instructions d'utilisation de base sont disponibles dans la page d'aide et les détails techniques concernant *scep_wwwi* sont accessibles dans la page de manuel *scep_wwwi(1)*.

L'interface Web vous permet d'accéder à distance au démon SCEP et de le déployer très facilement. Cet utilitaire puissant simplifie la lecture et l'écriture des valeurs de configuration.

Figure 6-1. System Center Endpoint Protection - Écran d'accueil.



La fenêtre de l'interface Web de System Center Endpoint Protection est divisée en deux sections principales. La fenêtre principale affiche le menu principal, ainsi que le contenu correspondant à l'option de menu sélectionnée. Cette base horizontale en haut de la fenêtre permet de parcourir les options principales suivantes :

- **Accueil** - fournit les informations de base du système et du produit Microsoft
- **Configuration** - vous pouvez modifier la configuration du système System Center Endpoint Protection
- **Contrôle** - permet d'exécuter des tâches simples et d'afficher des statistiques globales sur les objets traités par scep_daemon
- **Aide** - fournit des instructions d'utilisation détaillées pour l'interface Web de System Center Endpoint Protection
- **Déconnexion** - permet de mettre fin à la session en cours

Important : n'oubliez pas de cliquer sur le bouton **Enregistrer les modifications** après avoir effectué des modifications dans la section **Configuration** de l'interface Web pour enregistrer les nouveaux paramètres. Pour que les modifications entrent en vigueur, vous devez redémarrer le démon SCEP en cliquant sur **Appliquer les modifications** dans le volet de gauche.

Exemple de configuration de la protection en temps réel

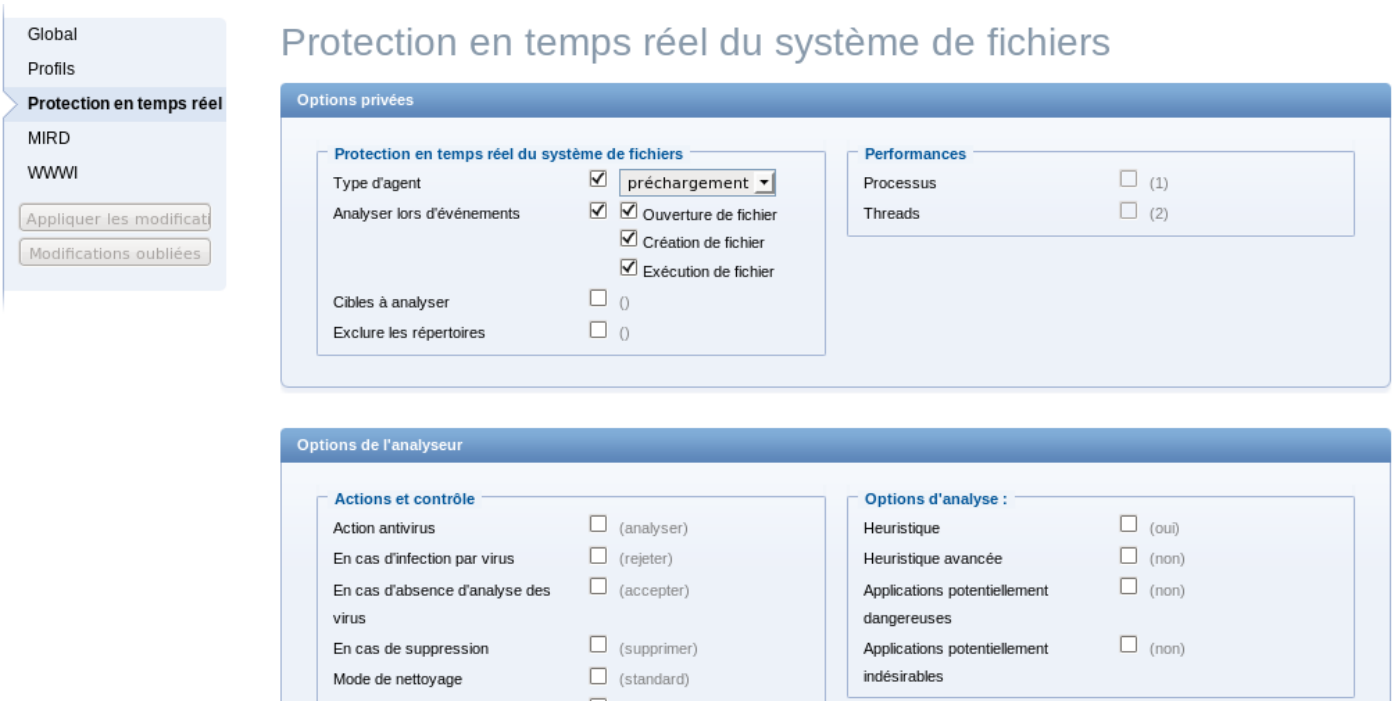
Vous pouvez configurer SCEP de deux manières. Dans notre exemple, nous allons vous indiquer comment utiliser l'une de ces méthodes pour configurer le module du contrôle d'action décrit au chapitre Protection en temps réel à l'aide de la bibliothèque de préchargement LIBC. Vous pouvez choisir l'option qui vous convient le mieux.

- Utilisation du fichier de configuration SCEP :

```
[fac]
agent_type = "preload"
event_mask = "open"
ctl_incl = "/home"
action_av_deleted = "reject"
action_av = "scan"
action_av_infected = "reject"
```

- Utilisation de l'interface Web :

Figure 6-3. SCEP - Configuration > Analyse à la demande



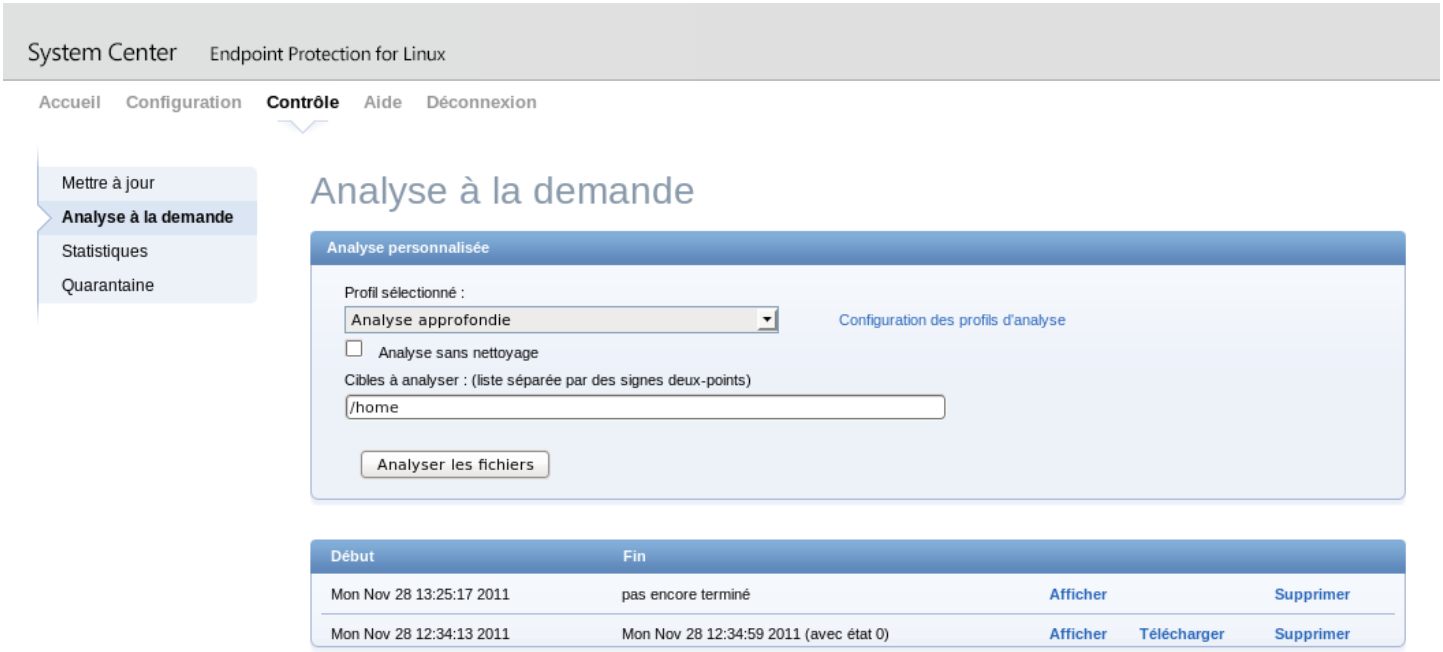
Lorsque vous modifiez les paramètres dans l'interface Web, n'oubliez pas d'enregistrer votre configuration en cliquant sur **Enregistrer les modifications**. Pour appliquer les nouvelles modifications, cliquez sur le bouton **Appliquer les modifications** dans le panneau des sections **Configuration**.

Analyse à la demande

Cette section propose un exemple d'exécution de l'analyse à la demande qui vise à détecter toute présence de virus :

- Accédez à **Contrôle > Analyse à la demande**
- Saisissez le chemin d'accès au répertoire à analyser
- Exécutez l'analyse à ligne de commande en cliquant sur le bouton **Analyser les fichiers**

Figure 6-4. SCEP - Contrôle > Analyse à la demande

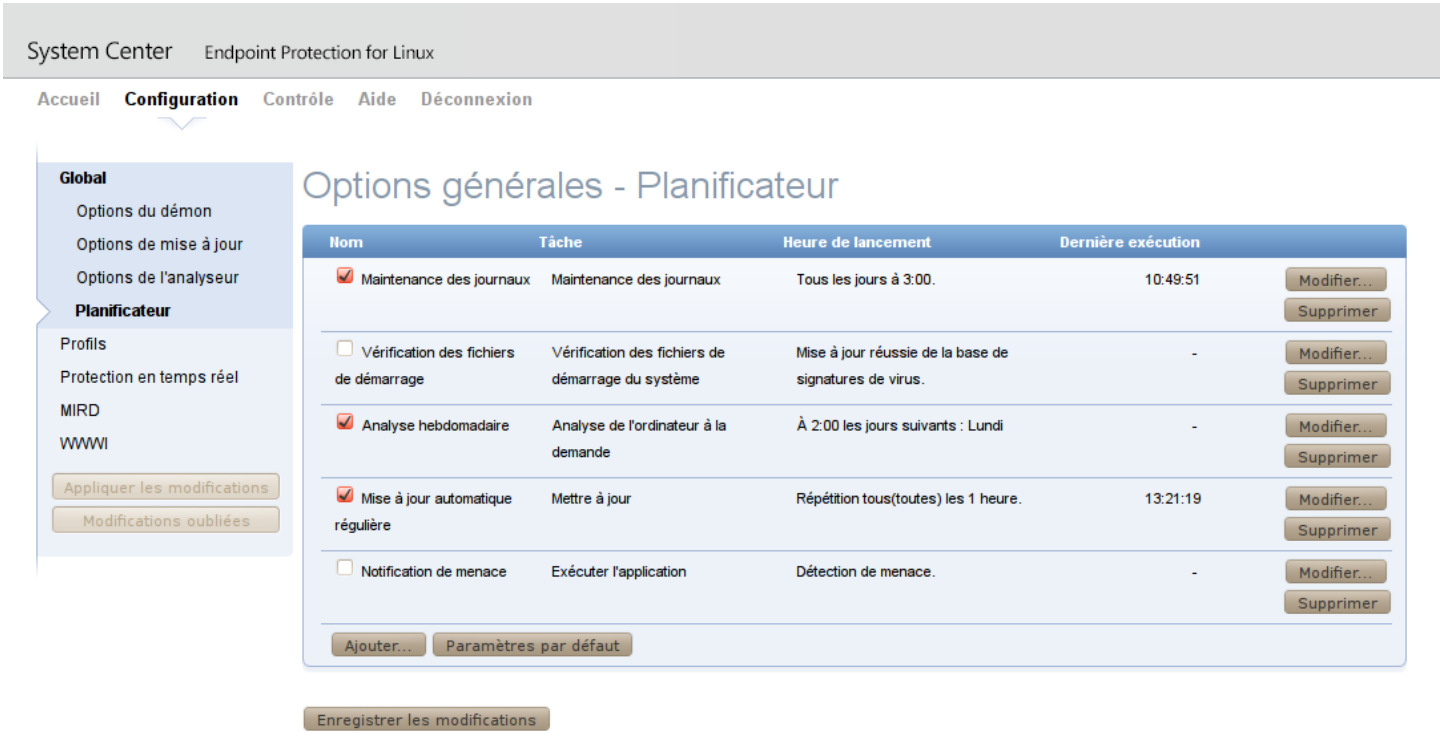


L'analyse à ligne de commande Microsoft s'exécute automatiquement en arrière-plan. Pour afficher la progression de l'analyse, cliquez sur le lien **Afficher**. Une nouvelle fenêtre de navigateur s'ouvre.

Planificateur

Vous pouvez gérer les tâches du planificateur par l'intermédiaire du fichier de configuration SCEP (reportez-vous au chapitre Planificateur) ou à l'aide de l'interface Web.

Figure 6-5. SCEP - Global > Planificateur



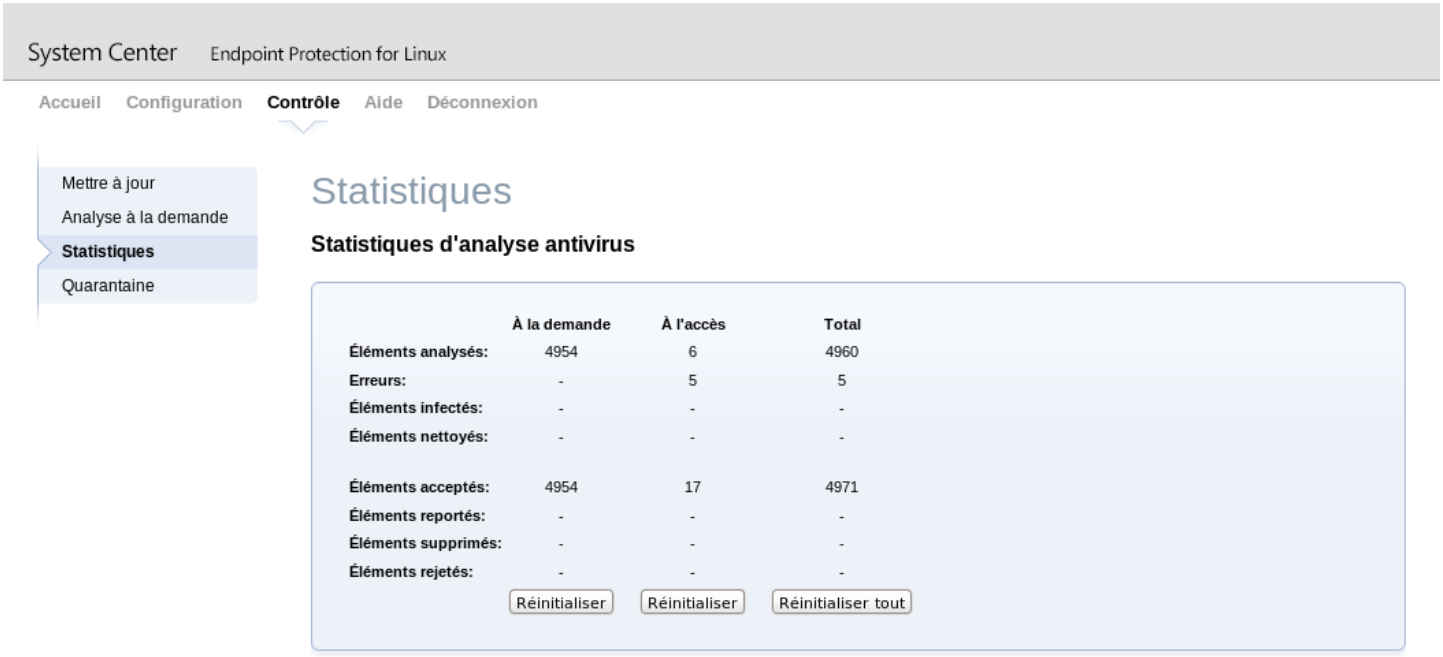
Sélectionnez ou désélectionnez la case à cocher pour activer/désactiver une tâche planifiée. Par défaut, les tâches planifiées suivantes sont affichées :

- **Maintenance des journaux** - Le programme supprime automatiquement les anciens fichiers journaux pour gagner de l'espace disque. Le planificateur commence la défragmentation des journaux. Toutes les entrées de journal vides sont supprimées pendant ce processus. De cette manière, l'utilisation des journaux est plus rapide. Cette amélioration se constate notamment si les journaux comportent un grand nombre d'entrées.
- **Vérification des fichiers de démarrage** - Analyse la mémoire et les services en cours d'exécution après la mise à jour de la base de signatures de virus.
- **Analyse hebdomadaire** - Analyse l'intégralité du système de fichiers toutes les semaines (par défaut, le lundi à 02 h 00). Cette tâche peut être personnalisée par l'utilisateur.
- **Mise à jour automatique régulière** - La mise à jour régulière de System Center Endpoint Protection est la meilleure méthode pour bénéficier du niveau maximum de sécurité sur votre ordinateur. Reportez-vous à l'utilitaire de mise à jour SCEP pour plus d'informations.
- **Notification de menace** - Par défaut, chaque menace est consignée dans le journal syslog. En outre, SCEP peut être configuré pour exécuter un script de notification externe qui informe l'administrateur système par e-mail lorsqu'une menace est détectée.

Statistiques

Vous pouvez afficher les statistiques de tous les agents SCEP actifs. Le récapitulatif **Statistiques** est actualisé toutes les 10 secondes.

Figure 6-6. SCEP - Contrôle > Statistiques



Journalisation

SCEP permet d'effectuer la journalisation par démon système par l'intermédiaire de syslog. *Syslog* est la norme en matière de consignation des messages du programme et peut être utilisé pour consigner les événements système tels que les événements de réseau et de sécurité.

Les messages font référence à un utilitaire :

```
auth, authpriv, daemon, cron, ftp, lpr, kern, mail, ..., local0, ..., local7
```

Les messages reçoivent une priorité/un niveau de la part de l'expéditeur du message :

```
Error, Warning, Summall, Summ, Partall, Part, Info, Debug
```

Cette section présente la configuration et la lecture des résultats de la journalisation de syslog. L'option *'syslog_facility'* (valeur par défaut *'daemon'*) définit l'utilitaire syslog utilisé pour la consignation. Pour modifier les paramètres syslog, modifiez le fichier de configuration SCEP ou utilisez l'interface Web. Modifiez la valeur du paramètre *'syslog_class'* pour changer de classe de journalisation. Nous vous recommandons de modifier ces paramètres uniquement si vous connaissez syslog. La configuration syslog ci-dessous est un exemple :

```
syslog_facility = "daemon"
syslog_class = "error:warning:summall"
```

Le nom et l'emplacement du fichier journal dépendent de l'installation et de la configuration de syslog (par exemple rsyslog, syslog-ng, etc.). Les fichiers de résultats syslog peuvent par exemple porter les noms standard *'syslog'*, *'daemon.log'*, etc. Pour suivre l'activité du programme syslog, exécutez l'une des commandes suivantes sur la console :

```
tail -f /var/log/syslog
tail -100 /var/log/syslog | less
cat /var/log/syslog | grep scep | less
```

Important : pour fonctionner correctement, la surveillance du produit Linux SCEP à l'aide de SCOM doit d'abord être activée dans le fichier de configuration SCEP ou par l'intermédiaire de l'interface Web SCEP. Vérifiez si le paramètre *'scom_enabled'* du fichier de configuration mentionné ci-dessus est défini sur *'scom_enabled = yes'* ou modifiez le paramètre approprié dans l'interface Web sous **Configuration** > **Global** > **Options du démon** > **SCOM activé**.

Mise à jour du système de sécurité SCEP

Utilitaire de mise à jour SCEP

Pour garantir l'efficacité de System Center Endpoint Protection, la base de signatures de virus doit être maintenue à jour. L'utilitaire *scep_update* a été développé à cette fin. Pour plus d'informations, reportez-vous à la page de manuel *scep_update(8)*. Si votre serveur accède à Internet par l'intermédiaire d'un serveur proxy HTTP, les options de configuration supplémentaires *'proxy_addr'* et *'proxy_port'* doivent être définies. Si l'accès au serveur proxy HTTP nécessite un nom d'utilisateur et un mot de passe, les options *'proxy_username'* et *'proxy_password'* doivent également être définies dans cette section. Pour lancer une mise à jour, saisissez la commande suivante :

@SBINDIR@/scep_update

Pour que l'utilisateur final bénéficie de la meilleure sécurité, l'équipe Microsoft collecte en permanence les définitions de virus du monde entier. Les nouveaux modèles sont ajoutés à la base de signatures de virus à intervalles de fréquence très courts. C'est pourquoi il est recommandé de lancer des mises à jour régulièrement. Pour indiquer la fréquence des mises à jour, vous devez configurer la tâche *'@update'* de l'option *'scheduler_tasks'* dans la section **[global]** du fichier de configuration SCEP. Vous pouvez également utiliser le planificateur pour définir la fréquence de mise à jour. Le démon SCEP doit être fonctionnel pour que la base de signatures de virus puisse être mise à jour.

Description du processus de mise à jour de SCEP

Le processus de mise à jour se compose de deux étapes : Tout d'abord, les modules de mise à jour précompilés sont téléchargés du serveur Microsoft.

La deuxième étape du processus de mise à jour consiste à compiler les modules qui sont stockés sur un miroir local et peuvent être chargés par l'analyseur System Center Endpoint Protection. En général, les modules de chargement SCEP suivants sont créés : module de chargement (em000.dat), module d'analyse (em001.dat), module de base de signatures de virus (em002.dat), module de prise en charge des archives (em003.dat), module d'heuristique avancée (em004.dat), etc. Les modules sont créés dans le répertoire suivant :

@BASEDIR@

Informez-nous

Nous espérons que ce guide vous a apporté les informations de configuration nécessaire à l'installation, à la configuration et à la maintenance de System Center Endpoint Protection. Toutefois, nous cherchons à améliorer en permanence la qualité et l'efficacité de notre documentation. Si certaines sections de ce Guide vous semblent incomplètes ou manquent de clarté, veuillez nous en informer en contactant le service client :

support.microsoft.com

Nous veillons à fournir le meilleur niveau de service afin de pouvoir vous aider si vous avez des problèmes concernant ce produit.

Annexe A. Licence PHP

The PHP License, version 3.01 Copyright (c) 1999 - 2006 The PHP Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, is permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "PHP" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact group@php.net.
4. Products derived from this software may not be called "PHP", nor may "PHP" appear in their name, without prior written permission from group@php.net. You may indicate that your software works in conjunction with PHP by saying "Foo for PHP" instead of calling it "PHP Foo" or "phpfoo"
5. The PHP Group may publish revised and/or new versions of the license from time to time. Each version will be given a distinguishing version number. Once covered code has been published under a particular version of the license, you may always continue to use it under the terms of that version. You may also choose to use such covered code under the terms of any subsequent version of the license published by the PHP Group. No one other than the PHP Group has the right to modify the terms applicable to covered code created under this License.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes PHP software, freely available from <http://www.php.net/software/>".

THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.