System Center Pack de surveillance pour Endpoint Protection pour Linux

Microsoft Corporation

Publication : 10/26/2015

Envoyer vos commentaires ou suggestions concernant ce document à mpgfeed@microsoft.com. Veuillez mentionner le nom du guide du Management Pack dans vos commentaires.

L'équipe Operations Manager vous encourage à faire part de vos commentaires sur le pack de surveillance en rédigeant une critique sur la page du Management Pack dans le Management Pack Catalog (http://go.microsoft.com/fwlink/?LinkID=82105).

Sommaire

Guide du Management Pack SCEP

Ce Management Pack permet de gérer System Center Endpoint Protection (SCEP) à partir de System Center 2012 Operations Manager dans un environnement de réseau, y compris les postes de travail et serveurs, à partir d'un emplacement central. Grâce au système d'administration des tâches Operations Manager, vous pouvez gérer SCEP sur des ordinateurs distants, consulter les alertes et les états d'intégrité, et réagir rapidement aux nouveaux problèmes et menaces.

System Center 2012 Operations Manager lui-même ne procure aucune autre forme de protection contre les codes malveillants. System Center 2012 Operations Manager requiert la présence d'une solution SCEP sur des ordinateurs tournant sous le système d'exploitation Linux.

Ce guide a été rédigé sur la base de la version 4.5.10.1 du Management Pack pour SCEP.

Historique du guide

Version	Date de sortie	Modifications
4.5.9.1	16/05/2012	Version originale de ce guide.
4.5.10.1	06/11/2012	Nouvelles distributions Linux prises en charge. Meilleure description de certains outils Management Pack.

Modifications dans la version 4.5.10.1

La version 4.5.10.1 du Management Pack pour System Center Endpoint Protection comprend les modifications suivantes :

- Nouvelles distributions Linux prises en charge :
  - Red Hat Enterprise Linux Server 5
  - SUSE Linux Enterprise 10
  - CentOS 5, 6
  - Debian Linux 5, 6
  - Ubuntu Linux 10.04, 12.04
  - Oracle Linux 5, 6

  Remarque : ces nouvelles distributions ne sont prises en charge qu'avec System Center 2012 Operations Manager Service Pack 1 et les versions ultérieures.
- Ajout d'une meilleure description pour :
  - Surveillance de logiciel malveillant actif
  - Alerte de logiciel malveillant actif (depuis la règle)

Configurations prises en charge

En général, les configurations prises en charge sont reprises dans Configurations prises en charge par Operations Manager 2007 R2 (http://technet.microsoft.com/fr-fr/library/bb309428.aspx).

Ce Management Pack requiert System Center 2012 Operations Manager 2007 R2 ou une version ultérieure. Le tableau suivant répertorie les systèmes d'exploitation pris en charge pour ce Management Pack :

Nom du système d'exploitation	x86	x64
Red Hat Enterprise Linux Server 5, 6	Oui	Oui
SUSE Linux Enterprise 10, 11	Oui	Oui
CentOS 5, 6	Oui	Oui
Debian Linux 5, 6	Oui	Oui
Ubuntu Linux 10.04, 12.04	Oui	Oui
Oracle Linux 5, 6	Oui	Oui

Configuration requise

La configuration suivante est requise pour exécuter ce Management Pack :

- System Center Operations Manager 2007 R2 Cumulative Update 5 (http://support.microsoft.com/kb/2449679)

Les Management Packs pour SCEP répertoriés ci-dessous sont soit intégrés à System Center 2012 Operations Manager 2007 R2 soit disponibles en téléchargement depuis le catalogue en ligne.

ID	Nom	Version

Microsoft.Linux.Library	Linux Operating System Library	6.1.7000.256
Microsoft.SystemCenter.InstanceGroup.Library	Instance Group Library	6.1.7221.0
Microsoft.SystemCenter.Library	System Center Core Library	6.1.7221.0
Microsoft.SystemCenter.WSManagement.Library	WS-Management Library	6.1.7221.0
Microsoft.SystemCenter.DataWarehouse.Library	Data Warehouse Library	6.1.7221.0
Microsoft.Unix.Library	Unix Core Library	6.1.7000.256
Microsoft.Unix.Service.Library	Unix Service Template Library	6.1.7221.0
Microsoft.Windows.Library	Windows Core Library	6.1.7221.0
System.Health.Library	Health Library	6.1.7221.0
System.Library	System Library	6.1.7221.0

Important : La surveillance du produit Linux SCEP en utilisant System Center 2012 Operations Manager doit d'abord être activée dans le fichier de configuration */etc/opt/microsoft/scep/scep.cfg* ou via l'interface Web SCEP pour fonctionner correctement. 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**.

Fichiers de ce Management Pack

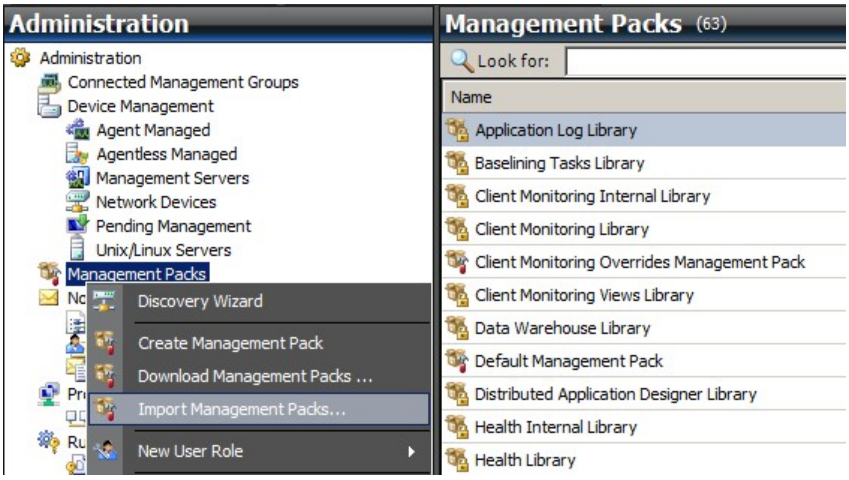
Le Management Pack pour SCEP comprend les fichiers suivants :

Nom de fichier	Description
Microsoft.SCEP.Linux.Library.mp	Contient des définitions de classes et leurs relations mutuelles ainsi que des définitions de types de module et de types de moniteur.
Microsoft.SCEP.Linux.Application.mp	Déploie la surveillance et les alertes, les tâches et les vues.

Démarrage rapide

Pour démarrer la surveillance de SCEP, vous devez importer des Management Packs dans Operations Manager et identifier les ordinateurs à surveiller (processus appelé « détection »).

Importation des Management Packs

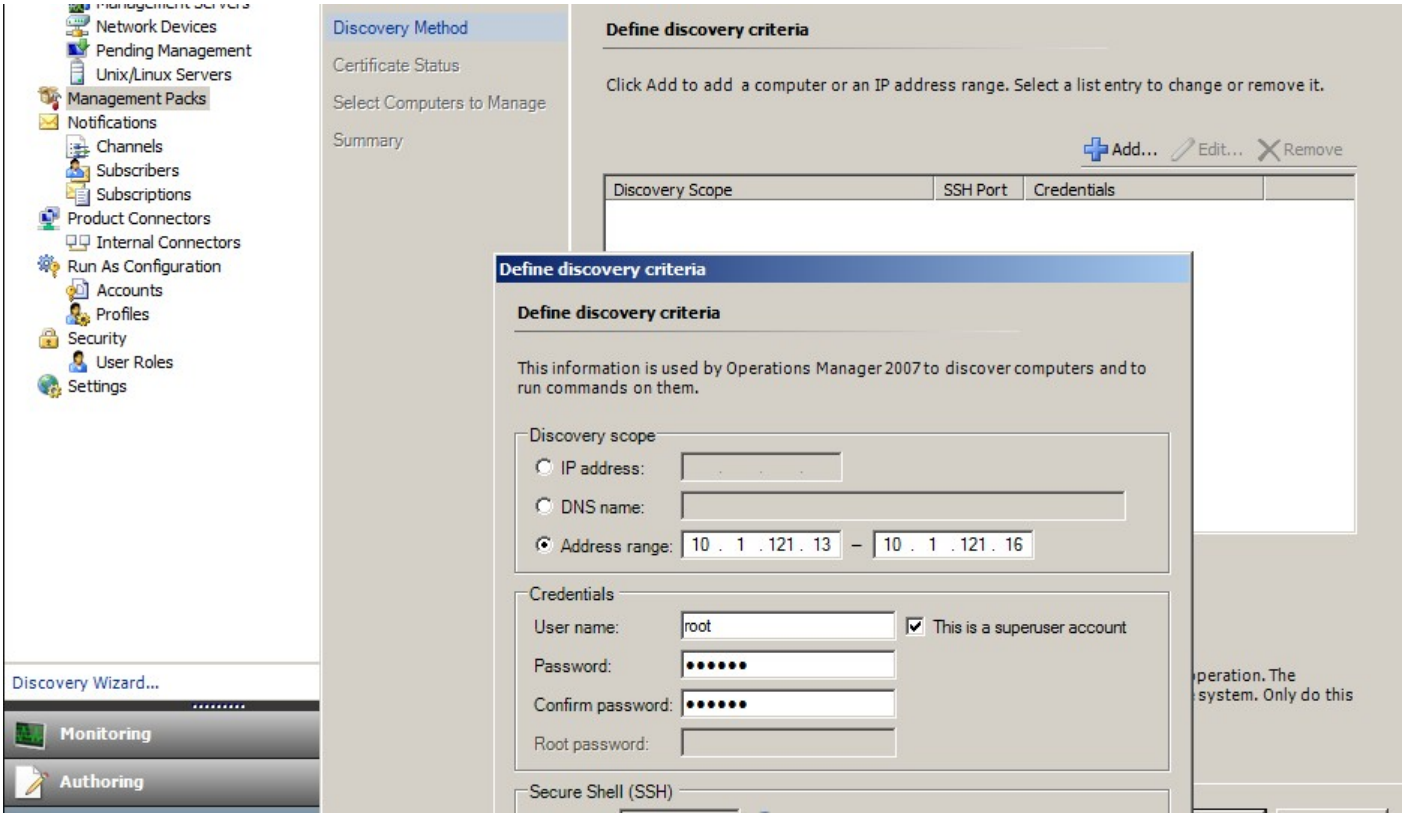


1. Cliquez sur l'espace de travail **Administration** dans le volet gauche de la fenêtre Console des opérations.
2. Cliquez avec le bouton droit sur **Management Packs** et sélectionnez **Import Management Packs...** dans le menu contextuel.
3. Dans la fenêtre des Management Packs, cliquez sur le bouton **Add** et sélectionnez **Add from disk...** dans le menu contextuel.
4. Confirmez que vous souhaitez que Operations Manager cherche les dépendances et ne les installe pas non plus sur le disque local en cliquant sur **Yes** dans la fenêtre contextuelle **Online Catalog Connection**.
5. Veillez à sélectionner les deux fichiers répertoriés (Microsoft.SCEP.Linux.Application.mp et Microsoft.SCEP.Linux.Library.mp) et cliquez sur **Install**.

Remarque : pour plus d'instructions sur l'importation d'un Management Pack, consultez Procédure d'importation d'un pack d'administration dans Operations Manager 2007 (http://go.microsoft.com/fwlink/?LinkId=142351).

Détection

Une fois les fichiers *.mp importés, vous devez exécuter une découverte des ordinateurs.



1. Dans l'espace de travail **Administration** (dans le volet gauche de la fenêtre Console des opérations), cliquez sur le lien **Discovery wizard...** (en bas du volet de gauche).
2. Dans l'Assistant Gestion des ordinateurs et des périphériques, sélectionnez l'option **Unix/Linux computers** et cliquez sur **Next** pour continuer.
3. Dans la boîte de dialogue de définition des critères de détection, cliquez sur le bouton **Add**.
4. Définissez une plage d'adresses (**Address range**) IP à analyser et les informations d'identification (**Credentials**) SSH applicables aux ordinateurs sur lesquels System Center 2012 Operations Manager installe son agent.
5. Confirmez l'étendue et les critères des informations d'identification en cliquant sur **OK**, puis sur le bouton **Discover** pour lancer la procédure de détection.
6. Une fois l'opération terminée, une liste va s'afficher, permettant de sélectionner les systèmes à surveiller/administrer.

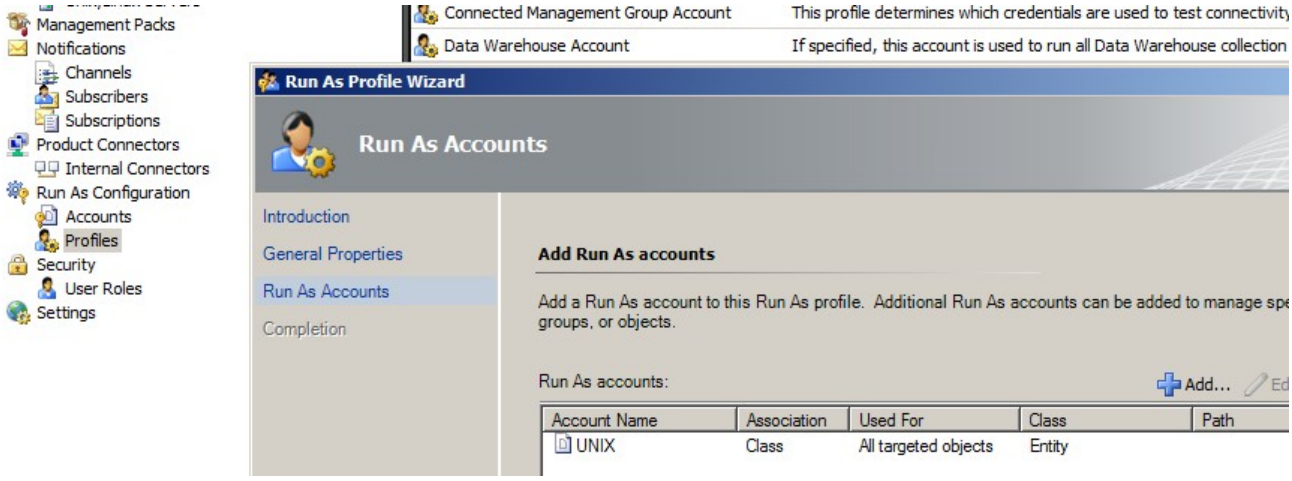
Remarque : l'installation d'un agent Linux est prise en charge par ces distributions de Linux. Si l'agent Linux ne peut pas être installé en utilisant la détection, consultez les instruction d'installation manuelle dans l'article Microsoft suivant : Installation manuelle d'agents interplateforme (http://technet.microsoft.com/fr-fr/library/dd789016.aspx).

Remarque : la détection des serveurs Linux avec une installation SCEP s'exécute automatiquement à intervalles de huit heures sur tous les ordinateurs Linux administrés via Operations Manager (autrement dit, le Management Pack Linux adéquat est installé pour leur distribution système). La détection crée toutes les entités de module de service : serveur Linux protégé et entités imbriquées ou serveur Linux non protégé (que l'on peut trouver dans les sections adéquates). SCEP peut être considéré comme complètement installé lorsque le service « scep_daemon » est présent (arrêté ou en cours d'exécution). La première détection a donc lieu lors de l'installation d'un Management Pack, tandis que la suivante sera effectuée dans huit heures, en fonction du cycle de détection. Si un produit SCEP est désinstallé, le serveur correspondant prendra automatiquement l'état Non protégé (serveurs sans SCEP) et inversement.

Configuration des comptes d'identification

Pour créer un compte Unix, suivez la procédure suivante :

1. Dans l'espace de travail **Administration** (volet gauche), accédez à **Run As Configuration** > **Accounts**.
2. Pour créer un nouveau compte, ouvrez la section **Actions** du volet **Actions** (volet droit) et cliquez sur **Create Run As Account...**
3. Dans la fenêtre des propriétés générales, sélectionnez **Basic Authentication** dans le menu déroulant **Run As Account type**.
4. Après avoir créé un compte, vous devez l'ajouter à un profil pour que la distribution s'exécute. Pour ce faire, cliquez avec le bouton droit sur le profil **Unix Privileged Account** sous **Run As Configuration** > **Profiles**, select **Properties** et complétez l'assistant pour attribuer le nouveau compte.



Remarque : pour plus d'informations sur la création d'un compte d'identification, consultez le sujet Configuration d'un compte d'identification interplateforme (http://technet.microsoft.com/fr-fr/library/dd788981.aspx) de la bibliothèque en ligne System Center 2012 Operations Manager 2007 R2.

Une fois toutes ces étapes exécutées, les nouveaux serveurs Linux détectés sont disponibles (après quelques minutes) sous **Monitoring** > **System Center Endpoint Protection pour Linux** > **Serveurs avec SCEP**.

Installation d'un pack de langues pour SCEP

Le pack de langue a le format suivant :
Microsoft.SCEP.Linux.Application.LNG.mp et Microsoft.SCEP.Linux.Library.LNG.mp

Pour l'installation du pack de langue, suivez les étapes de la section **Importation des Management Packs** ci-dessus. Pour afficher la langue installée dans System Center 2012 Operations Manager, suivez cette procédure :

1. Cliquez sur le bouton **Démarrer** de Windows et accédez au **Panneau de configuration**.
2. Dans le Panneau de configuration, cliquez sur **Options régionales et linguistiques**.
3. Changez la langue du système pour les programmes non-Unicode dans l'onglet **Administration**. Dans l'onglet **Emplacement**, changez l'emplacement en fonction du pack de langue installé.

Objectif du Management Pack

Le Management Pack pour SCEP intègre les fonctionnalités suivantes :

- Surveillance en temps réel et alertes pour les incidents de sécurité et l'état d'intégrité en matière de sécurité.
- Permettre aux administrateurs de serveurs d'exécuter à distance des tâches relatives à la sécurité sur leurs serveurs. Le principal objectif de ces tâches est de résoudre les problèmes de disponibilité liés à la sécurité.

Vues

L'administrateur de serveurs peut surveiller tous les ordinateurs sur lesquels est installé SCEP en utilisant la console Operations Manager. « System Center Endpoint Protection pour Linux » propose les vues suivantes :

- **Alertes actives** - Toutes les alertes actives SCEP de tous les niveaux de gravité. Les alertes fermées ne sont pas incluses.
- **Tableau de bord** - Affiche à la fois les espaces de travail Serveurs avec SCEP et Alertes actives.
- **Serveurs avec SCEP** - Affiche tous les serveurs Linux protégés.
- **Serveurs sans SCEP** - Affiche tous les serveurs Linux non protégés.
- **État de la tâche** - Répertorie toutes les tâches exécutées.

Lorsque vous surveillez l'état de SCEP avec ce Management Pack System Center 2012 Operations Manager, vous pouvez avoir une vue instantanée de l'intégrité de SCEP.

Plutôt que d'attendre qu'une alerte soit déclenchée, vous pouvez afficher le résumé de l'état des composants SCEP à tout moment en cliquant sur le volet **Monitoring** > **System Center Endpoint Protection pour Linux** > **Serveurs avec SCEP** de la console de surveillance Operations Manager. L'état d'un composant est représenté par des icônes colorées dans la zone État :

Icône	État	Description
	Healthy	Une icône verte indique une réussite ou la disponibilité d'informations ne requérant pas d'intervention.
	Warning	Une icône jaune indique une erreur ou un avertissement.
	Critical	Une icône rouge indique une erreur critique, un problème de sécurité ou l'indisponibilité d'un service.
	Not monitored	L'absence d'indication signifie qu'aucune donnée ayant un impact sur l'état n'a été recueillie.

Une vue peut contenir une très longue liste d'objets. Pour trouver un objet spécifique ou un groupe d'objets, vous pouvez utiliser les boutons Étendue, Rechercher et Trouver dans la barre d'outils Operations Manager. Pour plus d'informations, consultez le sujet Procédure de gestion des données d'analyse à l'aide des options Étendue, Rechercher et Trouver (http://technet.microsoft.com/fr-fr/library/bb437275.aspx).

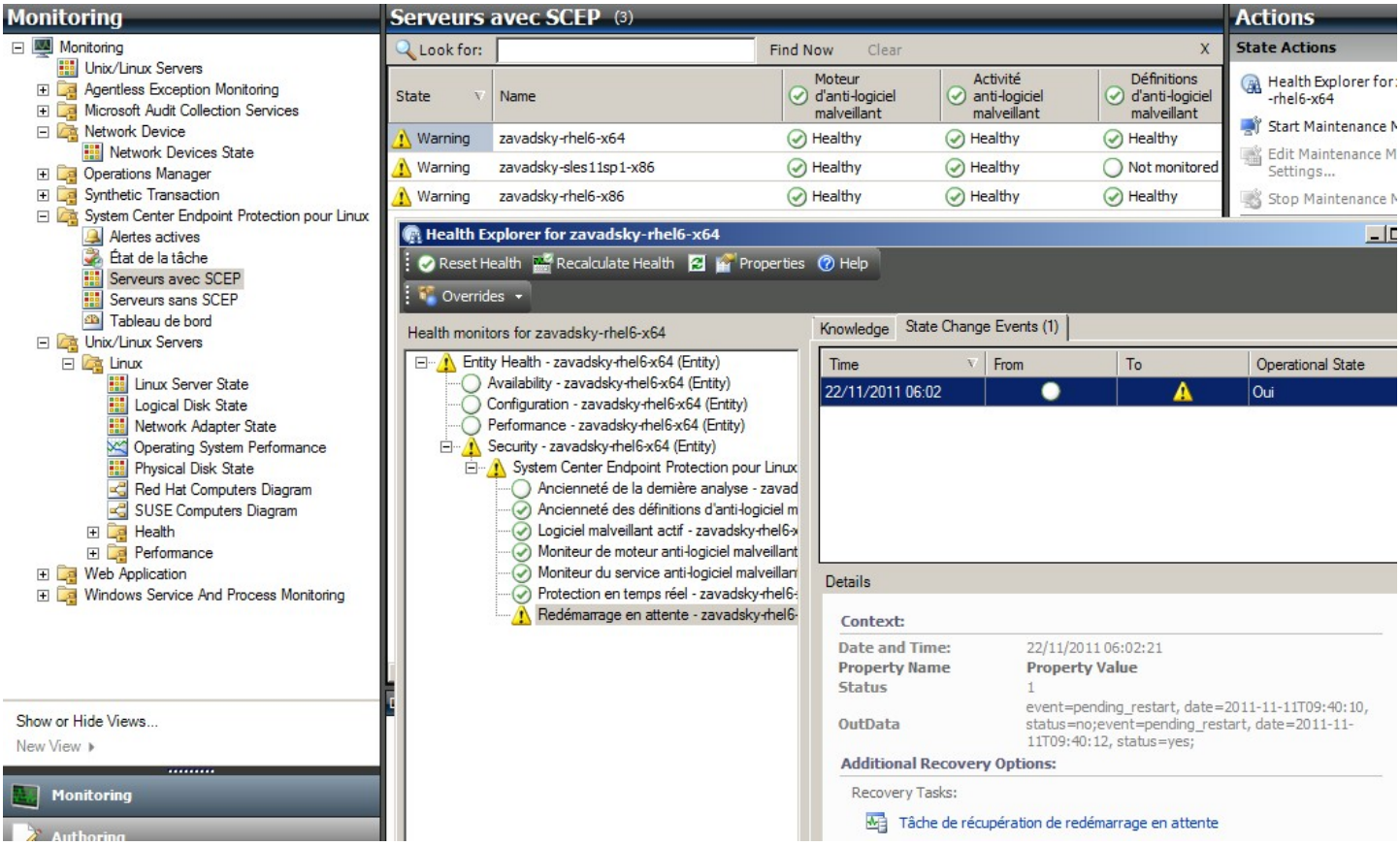
Moniteurs

Dans Operations Manager 2007, les moniteurs permettent d'évaluer les divers états pouvant affecter les objets surveillés.

Un total de 17 moniteurs sont disponibles pour SCEP :

- 9 moniteurs d'unité - Les composants de surveillance de base sont utilisés pour surveiller des compteurs, événements, scripts et services spécifiques.
- 2 moniteurs d'agrégat – Utilisés pour un cumul d'agrégats afin de regrouper plusieurs moniteurs en un seul, puis utiliser ce dernier pour définir l'état d'intégrité et générer une alerte.
- 6 moniteurs de dépendance - Références contenant les données d'état des moniteurs existants.

Remarque : pour plus d'informations sur les moniteurs, consultez l'aide d'Operations Manager 2007 R2 (appuyez sur la touche F1 dans System Center 2012 Operations Manager).



Les moniteurs d'intégrité de SCEP ont la structure et les propriétés décrites ci-dessous.

Logiciel malveillant actif

Type de moniteur	Moniteur d'unité
Cible	Serveur Linux protégé

Type de moniteur	Moniteur d'unité
Source de données	Surveille le fichier journal au format texte : /var/log/scep/eventlog_scom.dat
Intervalle	Basé sur événements
Alerte	Oui. Pas de résolution automatique
Comportement de réinitialisation	Retour automatique à l'état intègre après une période de huit heures. L'alerte reste active afin de conserver les informations sur le logiciel malveillant non traité.
Remarques	Ce moniteur passe à l'état critique si un logiciel malveillant a été détecté et n'a pas été nettoyé. L'état redevient automatiquement intègre après 8 heures (en effet, il n'est pas possible de déterminer avec précision si le logiciel malveillant a été nettoyé/supprimé ou pas). L'administrateur doit intervenir pour prendre en compte les circonstances et clôturer le ticket manuellement.
État	Intègre - Aucun logiciel malveillant Critique - Logiciel malveillant actif
Activé	Vrai
Tâche de récupération	Non

Ce moniteur effectue le suivi des opérations de nettoyage des logiciels malveillants qui n'ont pas abouti. Il signale un état critique si le client signale qu'il n'est pas parvenu à nettoyer le logiciel malveillant.

Ancienneté des définitions d'anti-logiciel malveillant

Type de moniteur	Moniteur d'unité
Cible	Serveur Linux protégé
Source de données	Commande utilisée pour obtenir les données d'analyse : /opt/microsoft/scep/sbin/scep_daemon --status
Intervalle	Toutes les 8 heures
Alerte	Oui. Résolution automatique
État	Intègre - ancienneté <= 3 jours Avertissement - ancienneté > 3 ET <= 5 jours Critique - ancienneté > 5 jours
Activé	Vrai
Tâche de récupération	Oui, manuellement (pas de récupération automatique)

Les définitions à jour garantissent que l'ordinateur est protégé des dernières menaces de logiciels malveillants.

Moteur d'anti-logiciel malveillant

Type de moniteur	Moniteur d'unité
Cible	Serveur Linux protégé
Source de données	Surveille le fichier journal au format texte : /var/log/scep/eventlog_scom.dat
Intervalle	Basé sur événements
Alerte	Oui. Résolution automatique
État	Intègre - Activé Désactivé - Avertissement
Activé	Vrai
Tâche de récupération	Oui, manuellement (pas de récupération automatique)

Il est recommandé d'activer en permanence la protection anti-logiciel malveillant.
Remarque : ce moniteur surveille l'état de la protection antivirus, qui ne correspond pas à une protection en temps réel. Lorsque le moteur d'anti-logiciel malveillant est désactivé, l'analyse à la demande ne peut pas être lancée.

Service anti-logiciel malveillant

Type de moniteur	Moniteur d'unité
Cible	Serveur Linux protégé
Source de données	Surveille l'état du processus : scep_daemon
Intervalle	Toutes les 10 minutes
Alerte	Oui. Résolution automatique
État	Intègre - En cours d'exécution Critique - Pas en cours d'exécution
Activé	Vrai
Tâche de récupération	Oui, manuellement (pas de récupération automatique)

Le moniteur signale un état critique lorsque le service anti-logiciel malveillant (scep_daemon) sur la machine client n'est pas en

cours d'exécution ou ne réagit pas, ou lorsque le moteur anti-logiciel malveillant ne fonctionne pas correctement.

Ancienneté de la dernière analyse

Type de moniteur	Moniteur d'unité
Cible	Serveur Linux protégé
Source de données	Commande utilisée pour obtenir les données d'analyse : /opt/microsoft/scep/sbin/scep_daemon --status
Intervalle	Toutes les 8 heures
Alerte	Non
État	Intègre - ancienneté <= 7 Avertissement - ancienneté > 7
Activé	Vrai
Tâche de récupération	Oui, manuellement (pas de récupération automatique)

Ce moniteur surveille la durée écoulée depuis la dernière analyse de l'ordinateur (quel que soit le type d'analyse). Nous recommandons de planifier une analyse hebdomadaire.

Redémarrage en attente

Type de moniteur	Moniteur d'unité
Cible	Serveur Linux protégé
Source de données	Surveille le fichier journal au format texte : /var/log/scep/eventlog_scom.dat
Intervalle	Basé sur événements
Alerte	Oui. Résolution automatique
État	Non - Intègre Oui - Avertissement
Activé	Vrai
Tâche de récupération	Oui, manuellement (pas de récupération automatique)

Ce moniteur évalue la nécessité de redémarrer le système pour l'application de modifications de configuration (généralement lors de l'activation/la désactivation de la protection en temps réel). Le moniteur applique la demande suivante pour une mise à jour sur demande de cet état : /opt/microsoft/scep/sbin/scep_daemon --status.

Protection en temps réel

Type de moniteur	Moniteur d'unité
Cible	Serveur Linux protégé
Source de données	Surveille le fichier journal au format texte : /var/log/scep/eventlog_scom.dat Le moniteur peut aussi utiliser l'appel suivant pour une mise à jour d'état sur demande : /opt/microsoft/scep/sbin/scep_daemon --status.
Intervalle	Basé sur événements
Alerte	Oui. Résolution automatique
État	Activé - Intègre Désactivé - Avertissement
Activé	Vrai
Tâche de récupération	Oui, manuellement (pas de récupération automatique)

Surveille l'état de la protection en temps réel. La protection en temps réel vous alerte lorsque des virus, des logiciels espions ou d'autres logiciels potentiellement dangereux essaient de s'installer sur votre ordinateur.

System Center Endpoint Protection pour Linux

Type de moniteur	Moniteur d'agrégat
Cible	Serveur Linux protégé
Condition	Le pire de
Alerte	Non
Activé	Vrai
Tâche de récupération	Non

Ce moniteur est le système de remontée des informations sur l'intégrité (pire état) de tous les moniteurs d'unité de sécurité de serveur Linux protégé avec SCEP 7. Si l'état n'est pas initialisé, la surveillance n'a pas commencé pour cet objet ou aucun moniteur de sécurité n'est défini pour cet objet.

Moteur d'anti-logiciel malveillant

Type de moniteur	Moniteur de dépendance
Cible	Moteur d'anti-logiciel malveillant
Alerte	Non
Activé	Vrai
Tâche de récupération	Non

Affiche l'état du moniteur d'unité Serveur Linux protégé/Moteur d'anti-logiciel malveillant dans la liste des ordinateurs surveillés.

Service anti-logiciel malveillant

Type de moniteur	Moniteur de dépendance
Cible	Moteur d'anti-logiciel malveillant
Alerte	Non
Activé	Vrai
Tâche de récupération	Non

Affiche l'état du moniteur d'unité Serveur Linux protégé/Service anti-logiciel malveillant dans la liste des ordinateurs surveillés.

Définitions d'anti-logiciel malveillant

Type de moniteur	Moniteur de dépendance
Cible	Définitions d'anti-logiciel malveillant
Alerte	Non
Activé	Vrai
Tâche de récupération	Non

Affiche l'état du moniteur d'unité Serveur Linux protégé/Ancienneté des définitions d'anti-logiciel malveillant dans la liste des ordinateurs surveillés.

Logiciel malveillant actif

Type de moniteur	Moniteur de dépendance
Cible	Activité anti-logiciel malveillant
Alerte	Non
Activé	Vrai
Tâche de récupération	Non

Affiche l'état du moniteur Serveur Linux protégé/Logiciel malveillant actif dans l'explorateur d'intégrité pour l'activité anti-logiciel malveillant.

Commande Ping pour la machine

Type de moniteur	Moniteur d'unité
Cible	Activité anti-logiciel malveillant
Intervalle	Toutes les 60 minutes
Alerte	Non
État	Accessible - Intègre Inaccessible - Critique
Activé	Faux
Tâche de récupération	Non

Passe sur l'état critique en cas d'absence de réponse du serveur.

Activité de logiciel malveillant

Type de moniteur	Moniteur d'unité
Cible	Activité anti-logiciel malveillant
Source de données	Surveille le fichier journal au format texte : /var/log/scep/eventlog_scom.dat
Intervalle	Basé sur événements
Alerte	Non
État	Aucun logiciel malveillant - Intègre Activité de logiciel malveillant détectée - Critique
Activé	Vrai

Tâche de récupération	Non

Ce moniteur bascule sur l'état critique dans les cinq minutes qui suivent le détection d'un logiciel malveillant (nettoyé ou non traité) et reste sur critique pendant les 60 prochaines minutes. L'état critique est renouvelé à chaque nouvelle détection positive et la période d'alerte est aussi prolongée. Autrement dit, si aucun logiciel malveillant n'est détecté sur le système pendant une période de 60 minutes, le moniteur revient sur l'état intègre.

Déclenchement de logiciel malveillant de serveur

Type de moniteur	Moniteur d'agrégat
Cible	Activité anti-logiciel malveillant
Condition	Le meilleur de
Alerte	Non
Activé	Vrai
Tâche de récupération	Non

Moniteurs agrégés : Activité de logiciel malveillant, Commande Ping pour la machine.
Passe sur l'état critique si le serveur ne réagit pas dans les 60 minutes qui suivent une détection de logiciel malveillant (nettoyé ou non traité). Le passage au statut critique peut également être déclenché si, après une période sans réaction du serveur, un logiciel malveillant est détecté peu après un renouvellement de connexion.

Déclenchement de logiciel malveillant

Type de moniteur	Moniteur de dépendance
Cible	Observateur des serveurs protégés
Condition	Le pire de 95%
Alerte	Non
Activé	Vrai
Tâche de récupération	Non

Affiche l'état du moniteur Activité anti-logiciel malveillant/Déclenchement de logiciel malveillant de serveur.
Si plus de 5% de tous les ordinateurs Linux (protégés et non protégés) enregistrent une détection de logiciel malveillant dans les 60 dernières minutes, ce moniteur passe à l'état critique.

Remonter les informations sur l'intégrité du rôle des ordinateurs Linux SCEP

Type de moniteur	Moniteur de dépendance
Cible	Ordinateur Linux
Alerte	Non
Activé	Vrai
Tâche de récupération	Non

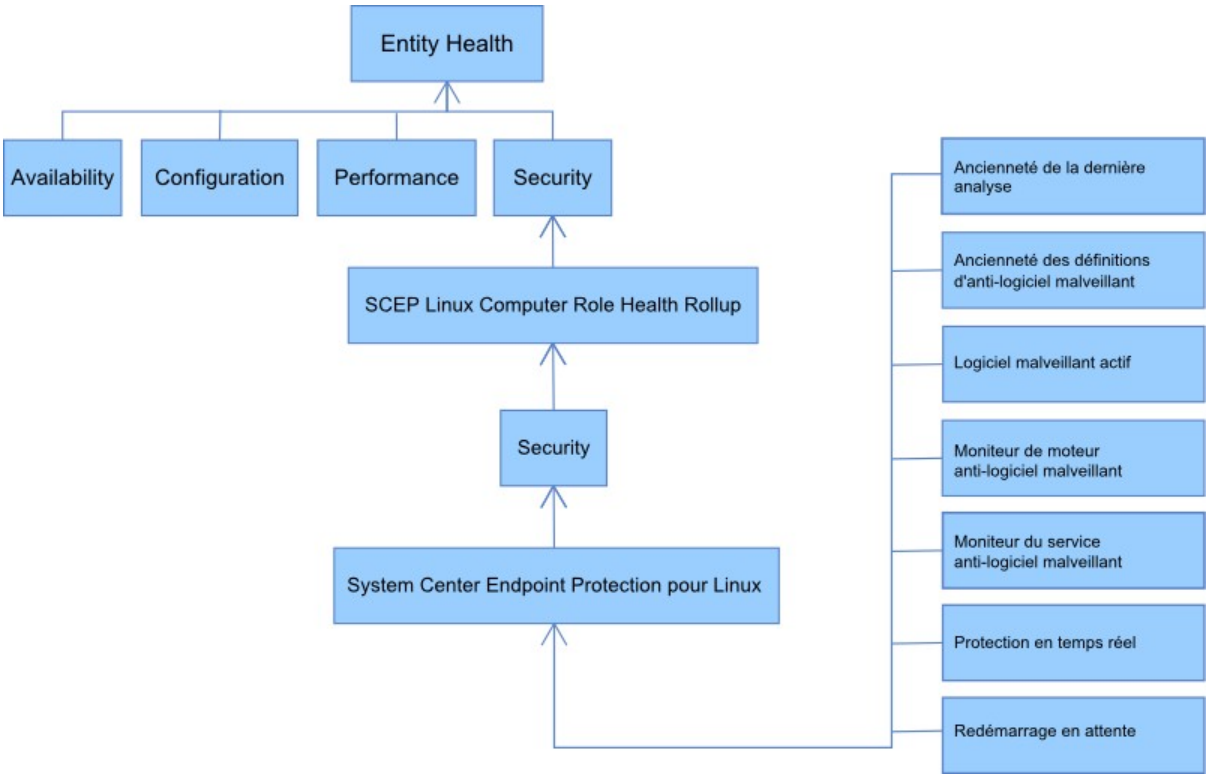
Propage l'état d'entité de l'ordinateur Linux protégé au moniteur Ordinateur Linux/Sécurité parent.

Remontée des informations sur l'intégrité

Ce Management Pack développe la surveillance du système d'exploitation Linux par couches, chaque couche dépendant de la couche inférieure pour être intègre. Le sommet de cette structure par couches constitue l'ensemble de l'environnement d'intégrité d'entité et le niveau le plus bas des environnements de sécurité représente tous les moniteurs. Lorsque une couche change d'état, la couche supérieure change d'état pour y correspondre. Cette action s'appelle la remontée des informations sur l'intégrité.

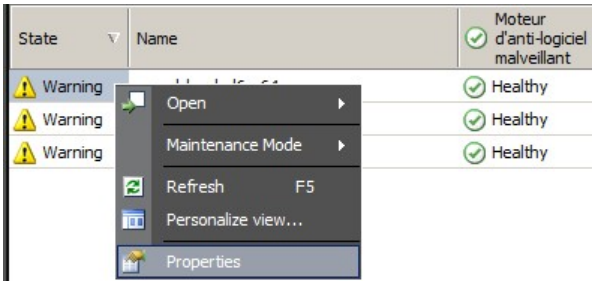
Par exemple, si la protection en temps réel revient à l'état d'avertissement et que tous les autres composants sont intègres, l'état d'avertissement sera transféré via l'arborescence à la racine (intégrité d'entité), qui acquerra également l'état d'avertissement.

Le diagramme suivant illustre la remontée des états d'intégrité des objets dans le Management Pack.



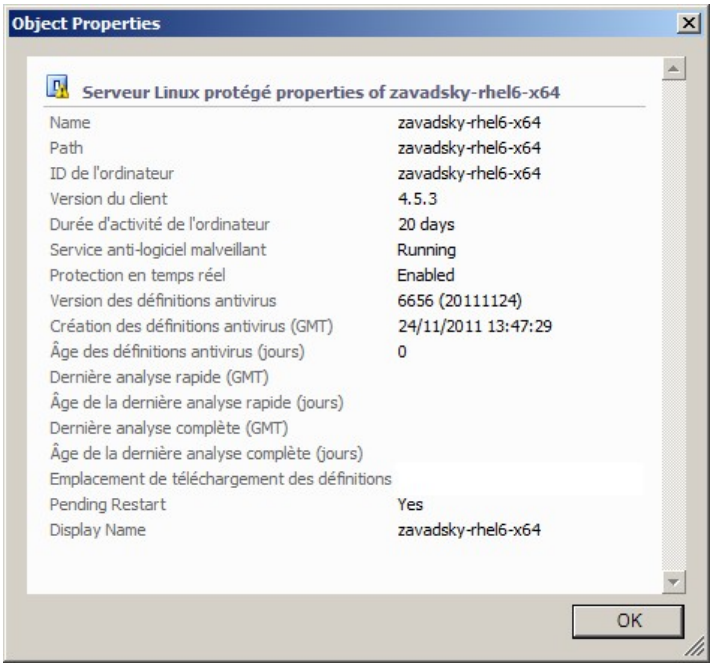
Propriétés des objets

Pour afficher les propriétés d'un objet, cliquez avec le bouton droit sur l'objet et sélectionnez **Properties**.



L'objet de serveur Linux protégé a les propriétés suivantes :

- **ID de l'ordinateur** - Identifiant du serveur, nom de domaine.
- **Nom d'affichage** - Nom du serveur, nom de domaine.
- **Version du client** - Version du produit SCEP installé.
- **Durée d'activité de l'ordinateur** - La durée d'activité du serveur (mesure la durée d'activité d'une machine sans temps d'arrêt) n'est pas essentielle au fonctionnement du Management Pack, mais son absence peut indiquer une erreur dans le Management Pack.
- **Service anti-logiciel malveillant** - État de la protection anti-logiciel malveillant (active/inactive).
- **Protection en temps réel**- État de la protection en temps réel ; son inactivité indique des problèmes avec SCEP.
- **Définitions antivirus...** - Données de l'état de la base de données des virus (version, date de création, ancienneté) ; l'absence de données indique des problèmes avec SCEP.
- **Dernière analyse rapide/complète...** - Données sur la dernière analyse de l'ordinateur. Si l'analyse (rapide/complète) n'a pas encore été exécutée, aucune donnée n'est disponible.
- **Emplacement de téléchargement des définitions** - Mise à jour de l'adresse/du nom de serveur. Les informations s'affichent lorsque la mise à jour a été effectuée.
- **Redémarrage en attente**- Informations sur la nécessité de redémarrer pour appliquer les modifications, en raison d'une nouvelle installation ou de modifications de la configuration de SCEP.



Alertes

L'alerte est un élément indiquant qu'une situation prédéfinie d'une certaine gravité s'est présentée pour un objet surveillé. Les alertes sont définies par des règles. Une vue est disponible dans la console Operations Manager, sous **Monitoring** > **System Center Endpoint Protection pour Linux** > **Alertes actives**. Elle affiche les alertes que l'utilisateur de la console a le droit de voir pour un objet spécifique.

Remarque : si plusieurs alertes du même type sont sans cesse générées (par ex. logiciel malveillant actif) depuis le même serveur, seule la première est affichée (les alertes redondantes sont ignorées).

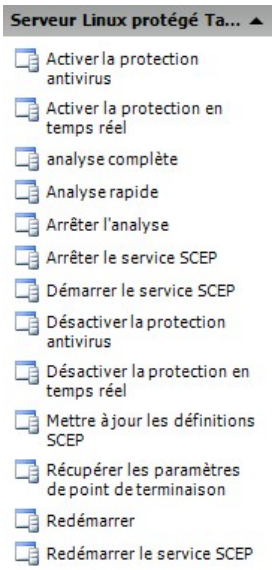
Alerte	Intervalle	Priorité	Gravité	Description
Infections répétées de logiciels malveillants	Basé sur événements	Élevée	Critique	L'alerte est générée lorsque des détections de logiciel malveillant se répètent (3 occurrences) sur un intervalle de temps donné (30 minutes). L'alerte contient des données sur le serveur ainsi que des informations de base sur le logiciel malveillant.
Logiciel malveillant nettoyé	Basé sur événements	Faible Moyenne	Information - Nettoyage du logiciel malveillant réussie Avertissement - Intervention de l'utilisateur requise, par ex. redémarrage du serveur	Alertes signalant le nettoyage réussi d'un logiciel malveillant. Contient toutes les informations disponibles sur ce logiciel malveillant spécifique. Chaque logiciel malveillant détecté génère un événement individuel. Linux SCEP attribue un niveau de priorité et de gravité en fonction de l'efficacité du processus de nettoyage : Nettoyé = Faible + Information Nettoyé, mais action (par ex. redémarrage) requise = Moyenne + Avertissement
Logiciel malveillant actif (depuis le moniteur)	Basé sur événements	Élevée	Critique	Alertes signalant un logiciel malveillant qui n'a pas été nettoyé. Contient toutes les informations disponibles sur ce logiciel malveillant spécifique.
Logiciel malveillant actif (depuis la règle)	Basé sur événements	Élevé//Moyen/ Faible	Critique/Moyen/Faible - en fonction d'un type de logiciel malveillant	Même que précédemment. Utilisé pour les connecteurs vers d'autres systèmes de surveillance/génération de ticket. **Remarque :** Cette règle (alerte) est désactivée par défaut.

Le service de protection anti-logiciel malveillant de System Center Endpoint Protection est arrêté	300 secondes	Moyenne	Critique	Alertes signalant l'indisponibilité du service anti-logiciel malveillant SCEP (scep_daemon). Comprend le nom de serveur correspondant et la version de SCEP.
Protection anti-logiciel malveillant désactivée	Basé sur événements	Moyenne	Avertissement	Alertes signalant la désactivation de la protection anti-logiciel malveillant. Comprend le nom de serveur correspondant.
Protection en temps réel désactivée	Basé sur événements	Moyenne	Avertissement	Alertes signalant la désactivation de la protection en temps réel. Comprend le nom de serveur correspondant.
Définitions obsolètes	Toutes les 8 heures	Moyenne	Avertissement (ancienneté <= 5 jours) ET ancienneté > 3 jours) Critique (ancienneté > 5 jours)	Alertes signalant que la base des signatures de virus n'a pas été mise à jour depuis plus de trois jours. Comprend le nom de serveur correspondant et l'ancienneté de la base des signatures de virus.
Déclenchement de logiciel malveillant	Basé sur événements	Élevée	Critique	Forefront Endpoint Protection a détecté un logiciel malveillant actif sur plus de 5% de vos ordinateurs. Il est possible qu'un logiciel malveillant se propage sur vos ordinateurs. Il est recommandé de vérifier si tous les serveurs utilisent les dernières définitions. Pour modifier le nombre de menaces actives qui déclenchent cette alerte, remplacez le paramètre du moniteur Déclenchement de logiciel malveillant (reportez-vous au chapitre Remplacements).

Tâches

Le Management Pack pour SCEP déploie 13 tâches. L'exécution de ces tâches est immédiate. Les résultats s'affichent directement après l'exécution de la tâche ou ils peuvent être consultés ultérieurement depuis la fenêtre d'état des tâches. L'exécution de la tâche prend au maximum 180 secondes. Le remplacement n'est pas disponible. Toutes les tâches sont des commandes BASH exécutées via SSH.

Les tâches peuvent être appelées sous **Monitoring** > **System Center Endpoint Protection pour Linux** > **Serveurs avec SCEP** dans le volet droit de la fenêtre Console des opérations.



- **Désactiver la protection antivirus** - Désactive tous les composants de la protection antivirus, désactive l'analyse à la demande.
- **Activer la protection antivirus** - Active tous les composants de la protection antivirus.
- **Désactiver la protection en temps réel** - Désactive la protection en temps réel.
- **Activer la protection en temps réel** - Active la protection en temps réel.
- **Analyse complète** - Met à jour la base des signatures de virus et exécute une analyse complète de l'ordinateur.
- **Analyse rapide** - Met à jour la base des signatures de virus et exécute une analyse rapide de l'ordinateur.
- **Arrêter l'analyse** - Arrête toutes les analyses d'ordinateur en cours d'exécution.
- **Récupérer les paramètres serveur** - Affiche l'état du produit SCEP actuel ; la liste des paramètres affichés est identique aux propriétés de l'entité Serveur Linux protégé. Les données affichées ne sont pas transférées vers le serveur Linux protégé.
- **Redémarrer le service anti-logiciel malveillant** - Redémarre le service anti-logiciel malveillant SCEP (scep_daemon).
- **Arrêter le service anti-logiciel malveillant** - Arrête le service anti-logiciel malveillant SCEP (scep_daemon).
- **Démarrer le service anti-logiciel malveillant** - Démarre le service anti-logiciel malveillant SCEP (scep_daemon).
- **Mettre à jour les définitions d'anti-logiciel malveillant** - Démarre la mise à jour de la base des signatures de virus.
- **Redémarrer** - Redémarre l'ordinateur Linux.

Configuration du Management Pack pour SCEP

Meilleure pratique : création d'un Management Pack pour les personnalisations

Par défaut, Operations Manager enregistre toutes les personnalisations telles que les remplacements dans le Management Pack par défaut. Nous vous recommandons plutôt de créer un Management Pack séparé pour chaque Management Pack verrouillé que vous souhaitez personnaliser.

Lorsque vous créez un Management Pack dans le but d'y placer des paramètres de Management Pack verrouillé personnalisés, il est utile de baser le nom du nouveau Management Pack sur celui du Management Pack qui est personnalisé, par exemple « Personnalisations SCEP 2012 ».

Créer un nouveau Management Pack pour chaque Management Pack verrouillé facilite l'exportation des personnalisations d'un environnement de test vers un environnement de production. Il est alors également plus facile de supprimer un Management Pack, car vous devez supprimer toutes les dépendances avant de pouvoir supprimer un Management Pack. Lorsque les personnalisations de tous les Management Packs sont enregistrées dans le Management Pack par défaut et qu'il vous faut supprimer un seul Management Pack, vous devez d'abord supprimer le Management Pack par défaut, ce qui supprime aussi les personnalisations des autres Management Packs.

Configuration de la sécurité

L'ordinateur doit exécuter le service SSHD et le port SSH (valeur par défaut = 22) doit être ouvert. System Center 2012 Operations Manager se connecte à distance aux ordinateurs Linux par l'intermédiaire du port en utilisant l'option Run As Account adéquate (dans le volet **Administration** > **Run As Configuration** de la console de surveillance Operations Manager) avec le type **Basic Authentication**.

Nom du profil d'identification	Remarques
Unix Privileged Account	Utilisé pour surveiller le serveur Unix à distance, ainsi que pour redémarrer les processus lorsque des privilèges sont requis.

Ce Management Pack n'utilise pas l'option Unix Action Account.

Avertissement : la surveillance des ordinateurs à l'aide du compte racine présente un risque de sécurité, par exemple si le mot de passe n'est plus confidentiel.

Si vous ne souhaitez pas utiliser le compte racine pour la surveillance et la gestion, vous pouvez utiliser un compte utilisateur standard. Ce compte doit néanmoins disposer de certains droits pour exécuter les commandes *sudo*. Par conséquent, pour que le compte utilisateur sélectionné soit autorisé à exécuter les commandes sudo par élévation des privilèges, le fichier /etc/sudoers doit avoir la configuration suivante sur chaque poste de travail SCEP Linux surveillé. Voici un exemple de configuration pour le nom d'utilisateur user1 :

```
#--------------------------------------------------------------------------------
# User configuration for SCEP monitoring - for a user with the name: user1

user1  ALL=(root)    NOPASSWD:     /opt/microsoft/scx/bin/scxlogfilereader -p
user1  ALL=(root)    NOPASSWD:     /bin/sh -c /sbin/reboot
user1  ALL=(root)    NOPASSWD:     /bin/sh -c CONSOLETYPE=serial /etc/init.d/scep restart
user1  ALL=(root)    NOPASSWD:     /bin/sh -c CONSOLETYPE=serial /etc/init.d/scep start
user1  ALL=(root)    NOPASSWD:     /bin/sh -c CONSOLETYPE=serial /etc/init.d/scep stop
user1  ALL=(root)    NOPASSWD:     /bin/sh -c export LANG=C;if \[ -e /opt/microsoft/scep/sbin/
scep_daemon \] ; then echo scep_daemon installed; else echo scep_daemon unprotected; fi; kill -0
`cat /var/run/scep_daemon.pid 2>/dev/null` 2>/dev/null; if \[ $\? -eq 0 \] ; then echo scep_daemon
running; else echo scep_daemon stop;fi ; /opt/microsoft/scep/sbin/scep_daemon --status; uptime
user1  ALL=(root)    NOPASSWD:     /bin/sh -c /opt/microsoft/scep/sbin/scep_daemon *
```

```
user1  ALL=(root)    NOPASSWD:     /bin/sh -c /opt/microsoft/scep/lib/scep_sci --scom *
user1  ALL=(root)    NOPASSWD:     /bin/sh -c pkill scep_sci
user1  ALL=(root)    NOPASSWD:     /bin/sh -c export LANG=C; kill -0 `cat /var/run/scep_daemon.pid 2>/
dev/null` 2>/dev/null; if \[ $? -eq 0 \] ; then echo scep_daemon running; else echo scep_daemon
stop;fi ; /opt/microsoft/scep/sbin/scep_daemon --status; uptime

# End user configuration for SCEP monitoring
#--------------------------------------------------------------------------------
```

Réglage des règles des seuils de performance

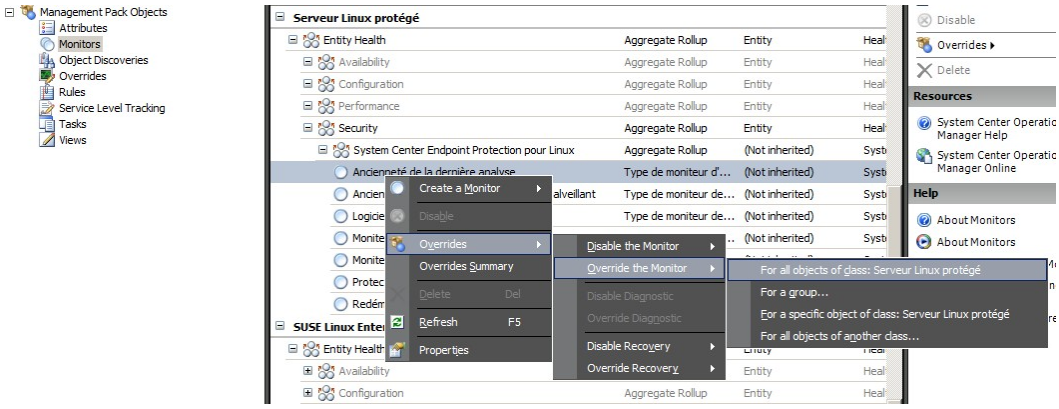
Le tableau suivant répertorie les règles des seuils de performance ayant des seuils par défaut pouvant nécessiter un réglage supplémentaire pour s'adapter votre environnement. Évaluez si les seuils par défaut de ces règles sont adaptés à votre environnement. Si ce n'est pas le cas, vous devriez les ajuster en y appliquant un remplacement.

Nom de la règle	Paramètre de remplacement	Seuil par défaut	Limitations du réglage
Règle des infections répétées de logiciels malveillants	Seuil du nombre d'infections répétées	3 occurrences	La définition d'une valeur inférieure à 2 rend la règle obsolète.
Règle des infections répétées de logiciels malveillants	Fenêtre horaire des infections répétées	30 minutes	Il est déconseillé de définir une valeur inférieure à la durée d'une analyse sur demande, car un chevauchement pourrait empêcher la génération d'une alerte.
Règle d'alerte de logiciel malveillant actif	Activé	Faux	Si vous utilisez des connecteurs vers d'autres systèmes de surveillance/ génération de ticket, vous pouvez activer cette alerte.

Remplacements

Les remplacements permettent de régler les paramètres d'un objet de surveillance dans System Center 2012 Operations Manager. Ils englobent les moniteurs, les règles, les découvertes d'objet et les attributs provenant de Management Packs importés.

Pour remplacer un moniteur, dans la Console des opérations, cliquez sur le bouton **Authoring** et développez **Management Pack Objects** > **Monitors**. Dans le volet des moniteurs, cherchez et développez complètement un type d'objet, puis cliquez sur un moniteur et sur **Overrides**.



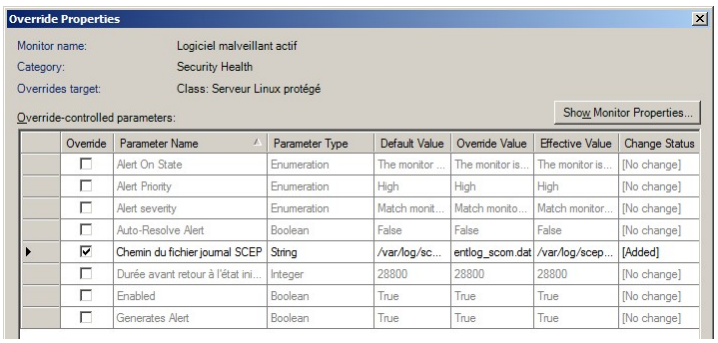
Utilisez la fenêtre des remplacements pour créer ou modifier un remplacement pour l'occurrence de l'un des paramètres suivants :

- **Durée avant retour à l'état initial du moniteur de logiciel malveillant actif** (lié uniquement au moniteur de logiciel malveillant actif)
- **Ancienneté des définitions d'anti-logiciel malveillant** (lié uniquement au moniteur d'ancienneté des définitions d'anti-logiciel malveillant)
- **Intervalle de détection** (lié uniquement au moniteur Ancienneté de la dernière analyse)
- **Alerte sur état**
- **Priorité d'alerte**
- **Gravité d'alerte**
- **Résolution automatique d'alerte**
- **Activée** - Détermine si le moniteur sélectionné est activé ou désactivé.
- **Génère une alerte**
- **Chemin du fichier journal SCEP**

Si un remplacement par défaut n'est pas adapté à votre environnement, vous devriez ajuster les seuils en y appliquant un remplacement :

Paramètre de remplacement	Nom du moniteur	Valeur par défaut	Remarques sur le réglage
Intervalle de Ping	Commande Ping pour la machine	3 600 secondes	Intervalle de vérification de la disponibilité du serveur Linux protégé. Une durée plus courte déclenche plus rapidement un état d'erreur sur le moniteur Déclenchement de logiciel malveillant de serveur, au cas où la machine ne réagirait plus en raison d'une attaque. Par conséquent, la charge augmente sur le réseau, l'ordinateur surveillé et le serveur System Center 2012 Operations Manager.
Fenêtre horaire de déclenchement de logiciel malveillant	Activité de logiciel malveillant	3 600 secondes	Intervalle requis avant que le moniteur ne revienne à l'état intègre après l'activité d'un logiciel malveillant. La valeur du moniteur Fenêtre horaire doit être supérieure à la commande ping pour la machine/à l'intervalle de ping pour que la combinaison fonctionne correctement. Dans l'intervalle de la fenêtre horaire de déclenchement de logiciel malveillant, si un pourcentage d'ordinateurs dépassant la valeur de déclenchement de logiciel malveillant définie (cf. Déclenchement de logiciel malveillant) enregistre une activité de logiciel malveillant, une alerte de déclenchement de logiciel malveillant est générée. Remarque : ceci est différent du déclenchement de logiciel malveillant de serveur, qui ne génère pas une alerte.
Durée avant retour à l'état initial du moniteur de logiciel malveillant actif	Logiciel malveillant actif	28 800 secondes	Intervalle de temps depuis la détection de logiciel malveillant et au terme duquel le logiciel malveillant est considéré comme nettoyé.
Chemin du fichier journal SCEP	Logiciel malveillant actif	/var/log/scep/ eventlog_scom.log	Chemin d'accès vers le fichier où les événements System Center 2012 Operations Manager sont enregistrés. Ne modifiez pas ce paramètre, sauf en cas de problème.
Âge critique des définitions d'anti-logiciel malveillant	Ancienneté des définitions d'anti-logiciel malveillant	5 jours	Après cet intervalle, une alerte d'erreur signalant un produit SCEP obsolète est générée.
Ancienneté de l'intégrité des définitions d'anti-logiciel malveillant	Ancienneté des définitions d'anti-logiciel malveillant	3 jours	Ancienneté maximale admise pour les définitions d'anti-logiciel malveillant, jusqu'où on peut les considérer à jour. Cette valeur doit toujours être inférieure à la valeur Âge critique des définitions d'anti-logiciel malveillant.
Intervalle	Ancienneté des définitions d'anti-logiciel malveillant	28 800 secondes	Intervalle de vérification de l'ancienneté des définitions d'anti-logiciel malveillant.
Intervalle	Service anti-logiciel malveillant	300 secondes	Intervalle de vérification de la disponibilité du service anti-logiciel malveillant.
Nom du processus	Service anti-logiciel malveillant	scep_daemon	Nom du service anti-logiciel malveillant. Ne modifiez pas cette valeur si le moniteur est opérationnel.
Intervalle de détection	Ancienneté de la dernière analyse	28 800 secondes	Intervalle de vérification de l'exécution de la dernière analyse.
Âge d'analyse maximum	Ancienneté de la dernière analyse	7 jours	À définir en fonction des paramètres du produit SCEP. Si une analyse est planifiée tous les 7 jours, définissez cette valeur sur 7 jours.
Chemin du fichier journal	Redémarrage en attente	/var/log/scep/ eventlog_scom.log	Chemin d'accès vers le fichier où les événements System Center 2012 Operations Manager sont enregistrés. Ne modifiez pas ce paramètre, sauf en cas de problème.
Chemin du fichier journal SCEP	Protection en temps réel	/var/log/scep/ eventlog_scom.log	Chemin d'accès vers le fichier où les événements System Center 2012 Operations Manager sont enregistrés. Ne modifiez pas ce paramètre, sauf en cas de problème.

Pourcentage	Déclenchement de logiciel malveillant	95 %	Pourcentage des serveurs Linux (protégés + non protégés) qui doivent revenir à l'état intègre pour que l'ensemble du groupe surveillé soit considéré comme intègre. Si des logiciels malveillants sont détectés sur au moins 5 % du total, un déclenchement de logiciel malveillant est généré.



Remarque : Pour plus d'informations sur les remplacements, consultez l'article Procédure d'analyse à l'aide de remplacements (http://technet.microsoft.com/fr-fr/library/bb309719.aspx).

Liens

Les liens suivants renvoient à des informations sur les tâches courantes associées à ce Management Pack :

- Administration du cycle de vie des packs d'administration (http://technet.microsoft.com/fr-fr/library/cc974486.aspx)
- Procédure d'importation d'un pack d'administration dans Operations Manager 2007 (http://technet.microsoft.com/fr-fr/library/cc974494.aspx)
- Procédure d'analyse à l'aide de remplacements (http://technet.microsoft.com/fr-fr/library/bb309719.aspx)
- Procédure de création d'un compte d'identification dans Operations Manager 2007 (http://technet.microsoft.com/fr-fr/library/bb309445.aspx)
- Configuration d'un compte d'identification interplateforme (http://technet.microsoft.com/fr-fr/library/dd788981.aspx)
- Procédure de modification d'un profil d'identification existant (http://technet.microsoft.com/fr-fr/library/dd891202.aspx)
- Procédure d'exportation des personnalisations de packs d'administration (http://technet.microsoft.com/fr-fr/library/cc974487.aspx)
- Procédure de suppression d'un pack d'administration (http://technet.microsoft.com/fr-fr/library/cc974489.aspx)
- Procédure de gestion des données d'analyse à l'aide des options Étendue, Rechercher et Trouver dans Essentials (http://technet.microsoft.com/fr-fr/library/bb437275.aspx)
- Monitoring Linux Using SCOM 2007 R2 (http://blogs.technet.com/b/birojitn/archive/2010/01/20/monitoring-linux-using-scom-2007-r2.aspx)
- Installation manuelle d'agents interplateforme (http://technet.microsoft.com/fr-fr/library/dd789016.aspx)
- Configuration de l'élévation des privilèges sudo pour la surveillance UNIX et Linux avec System Center 2012 - Operations Manager (http://social.technet.microsoft.com/wiki/contents/articles/7375.configuring-sudo-elevation-for-unix-and-linux-monitoring-with-system-center-2012-operations-manager.aspx)

Pour des questions sur Operations Manager et les packs de surveillance, consultez le forum communautaire System Center Operations Manager (http://social.technet.microsoft.com/Forums/fr-fr/category/systemcenteroperationsmanager).
Le blog System Center Operations Manager Unleashed (http://opsmgrunleashed.wordpress.com/) peut être utile : il contient des articles illustrant des packs de surveillance spécifiques.

Pour plus d'informations sur Operations Manager, consultez les blogs suivants :

- Operations Manager Team Blog
  (http://blogs.technet.com/momteam/default.aspx)
- Kevin Holman's OpsMgr Blog
  (http://blogs.technet.com/kevinholman/default.aspx)
- Thoughts on OpsMgr
  (http://thoughtsonopsmgr.blogspot.com/)
- Raphael Burri's blog
  (http://rburri.wordpress.com/)
- BWren's Management Space
  (http://blogs.technet.com/brianwren/default.aspx)
- The System Center Operations Manager Support Team Blog
  (http://blogs.technet.com/operationsmgr/)
- Ops Mgr ++
  (http://blogs.msdn.com/boris_yanushpolsky/default.aspx)
- Notes on System Center Operations Manager
  (http://blogs.msdn.com/mariussutara/default.aspx)

Pour un dépannage, consultez les fils de discussion du forum suivant :

- Microsoft.Unix.Library is missing
  (http://social.technet.microsoft.com/Forums/en-US/operationsmanagermgmtpacks/thread/8469d0ff-54d6-4cb4-9909-49ab62126b74/)