System Center 監視パック (Linux用Endpoint Protection用)

Microsoft Corporation

発刊日: 10/26/2015

本書に関するご意見またはご質問は、mpgfeed@microsoft.comまでお送りください。その際、管理パックガイドの書名もお知らせください。

管理パックに関するご意見またはご質問を気軽にお寄せいただくために、Management Pack Catalog (http://go.microsoft.com/fwlink/?LinkID=82105) (英語版) の中のMonitoring Packのページに、Operations Manager担当者による確認事項が記載されています。

目次

SCEP管理パックガイド

この管理パックを使用すると、System Center Endpoint Protection (SCEP)を、ワークステーションおよびサーバを含むネットワーク環境にあるSystem Center 2012 Operations Managerから、1箇所で集中管理できます。Operations Managerタスク管理システムを使用すると、リモートコンピュータ上のSCEPを管理し、警告状態および状況を表示して、新たな問題および脅威に対して速やかに対応できます。

System Center 2012 Operations Managerそのものには、悪意のあるコードに対する他のどんな形式の保護機能もありません。System Center 2012 Operations Managerでは、Linuxオペレーティングシステムがインストールされたコンピュータ上にSCEPソリューションが存在することが前提となります。

本ガイドは、SCEP用のバージョン4.5.10.1の管理パックをもとに作成されています。

ガイド履歴

バージョン	リリース日	変更
4.5.9.1	05/16/2012	このガイドの最初のリリース。
4.5.10.1	11/06/2012	新しいLinuxディストリビューションをサポート。 一部の管理パックツールについての説明を改善。

バージョン4.5.10.1における変更

バージョン4.5.10.1のSystem Center Endpoint Protection管理パックには、以下の変更があります。

- サポート対象の新しいLinuxディストリビューション:
  - 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

  注意: これらの新しいディストリビューションは、System Center 2012 Operations Manager Service Pack 1以上を使用した場合にのみサポートされます。
- 以下についての説明の改善:
  - アクティブなマルウェア監視
  - アクティブなマルフェア(ルールから)の警告

サポートされている設定

一般的に、サポートされている設定は、Operations Manager 2007 R2 でサポートされている構成(http://technet.microsoft.com/ja-jp/library/bb309428.aspx)に概略されています。

本管理パックには、System Center 2012 Operations Manager 2007 R2以降が必要です。以下の表は、本管理パックでサポートされているオペレーティングシステムの詳細を示しています。

OS名	x86	x64
Red Hat Enterprise Linux Server 5? 6	はい	はい
SUSE Linux Enterprise 10? 11	はい	はい
CentOS 5? 6	はい	はい
Debian Linux 5? 6	はい	はい
Ubuntu Linux 10.04? 12.04	はい	はい
Oracle Linux 5? 6	はい	はい

前提条件

この管理パックを実行するには、以下の前提条件を満たす必要があります。

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

以下に一覧で示されているSCEPの管理パックは、System Center 2012 Operations Manager 2007 R2に統合されているか、あるいはオンラインカタログからダウンロードできます。

ID	ファイル名	バージョン
Microsoft.Linux.Library	Linuxオペレーティングシステムライブラリ	6.1.7000.256
Microsoft.SystemCenter.InstanceGroup.Library	インスタンスグループライブラリ	6.1.7221.0
Microsoft.SystemCenter.Library	システムセンターコアライブラリ	6.1.7221.0
Microsoft.SystemCenter.WSManagement.Library	WS管理ライブラリ	6.1.7221.0
Microsoft.SystemCenter.DataWarehouse.Library	データウェアハウスライブラリ	6.1.7221.0
Microsoft.Unix.Library	Unixコアライブラリ	6.1.7000.256
Microsoft.Unix.Service.Library	Unixサービステンプレートライブラリ	6.1.7221.0
Microsoft.Windows.Library	Windowsコアライブラリ	6.1.7221.0
System.Health.Library	状況ライブラリ	6.1.7221.0
System.Library	システムライブラリ	6.1.7221.0

重要: System Center 2012 Operations Managerを使用したLinux SCEP製品の監視が正しく機能するには、まず構成ファイル*/etc/opt/microsoft/scep/scep.cfg*またはSCEP Webインターフェイスを介して有効化する必要があります。上述の設定ファイル中の'scom_enabled'パラメータが、*'scom_enabled = yes'*と設定されていることを確認するか、または[**設定**] > [**グローバル**] > [**デーモンオプション**] > [**SCOMは有効です**]の下のWebインターフェイスの該当する設定を変更します。

この管理パック内のファイル

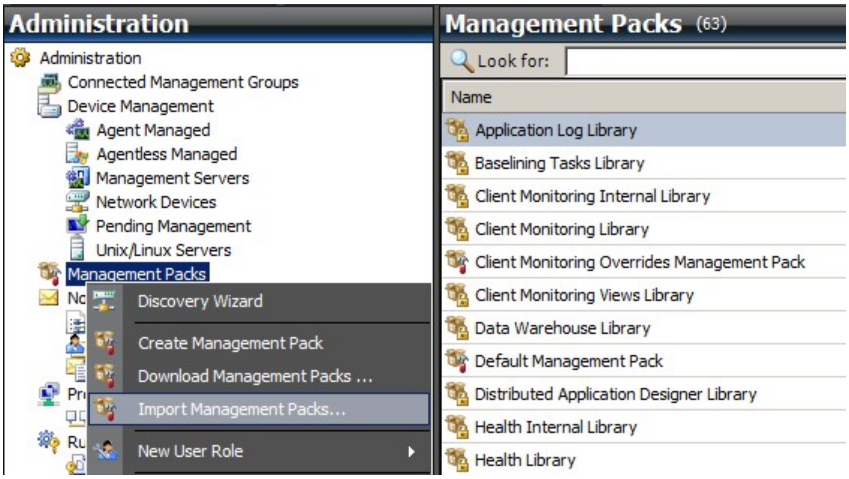
SCEPの管理パックには、以下のファイルが収められています。

ファイル名	説明
Microsoft.SCEP.Linux.Library.mp	クラス定義とその相互の関係、さらに監視機能タイプおよびモジュールタイプの定義が入っています。
Microsoft.SCEP.Linux.Application.mp	監視と警告、タスクとビューを実装します。

クイックスタート

SCEPの監視を開始するための前提条件には、Operations Managerへの管理パックのインポートと、監視対象のコンピュータの識別(「探索」と呼ばれるプロセス)があります。

管理パックのインポート

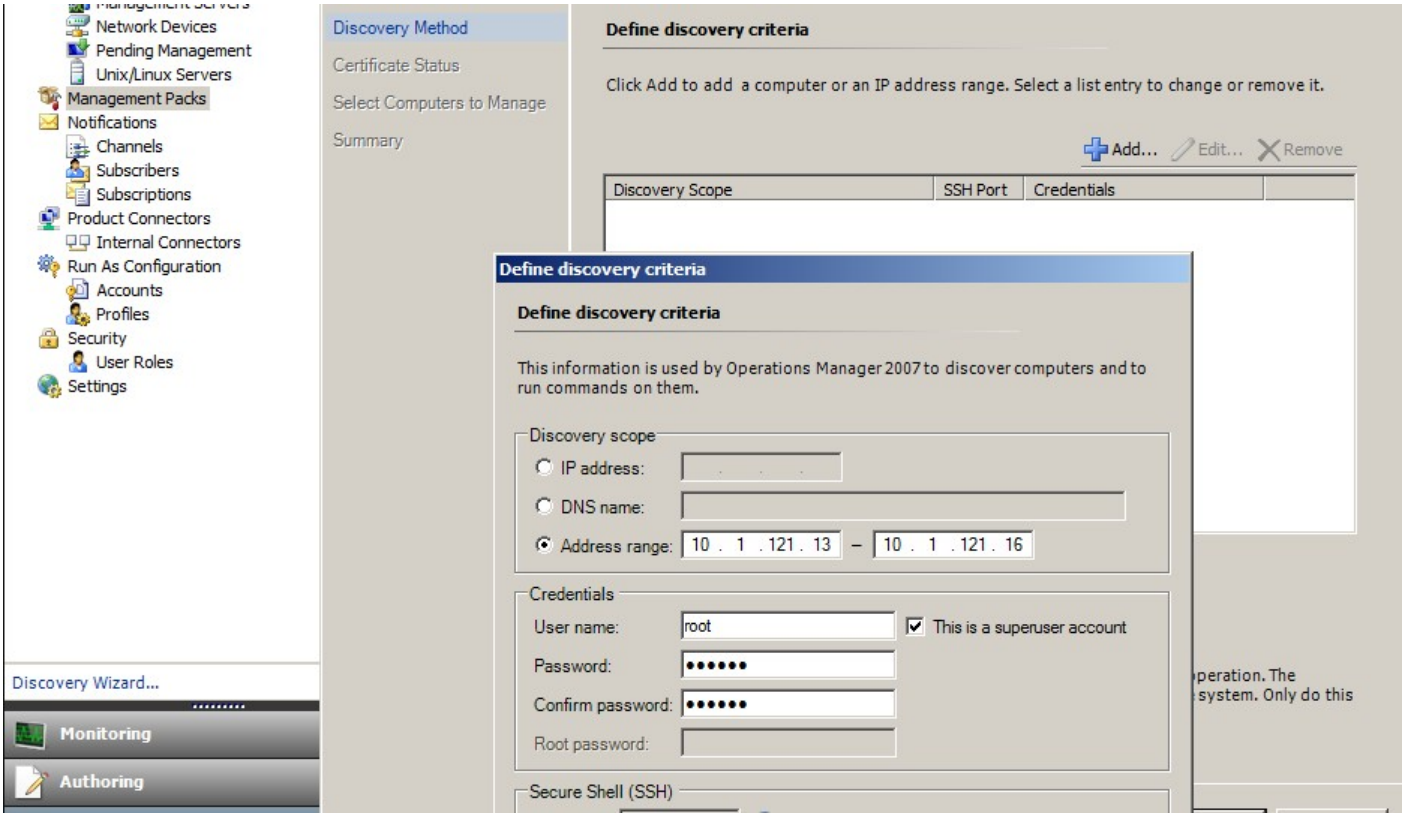


1. [操作コンソール]ウィンドウの左ペインにある[**Administration**]ワークスペースをクリックします。
2. [**Management Packs**]を右クリックし、コンテキストメニューから[**Import Management Packs...**]を選択します。
3. [管理パック]ウィンドウで、[**Add**]ボタンをクリックし、ドロップダウンメニューから[**Add from disk...**]を選択します。
4. ローカルディスク上にない依存関係をOperations Managerで探索してインストールすることを確認します。確認するには、[**Online Catalog Connection**]ポップアップウィンドウで[**Yes**]をクリックします。
5. 一覧表示されている両方のファイル(Microsoft.SCEP.Linux.Application.mpとMicrosoft.SCEP.Linux.Library.mp)を必ず選択し、[**Install**]をクリックします。

注意: 管理パックのインポートに関する詳細は、Operations Manager 2007 で管理パックをインポートする方法 (http://technet.microsoft.com/ja-jp/library/cc974494.aspx) を参照してください。

探索

*.mpファイルのインポートが正常に完了したら、コンピュータの探索を実行する必要があります。



1. [操作コンソール]ウィンドウの左ペインにある[**Administration**]ワークスペースで[**Discovery wizard...**]リンク(左ペインの下)をクリックします。
2. コンピューターとデバイスの管理ウィザードで、[**Unix/Linux computers**]オプションを選択し、[**Next**]をクリックして継続します。
3. [探索条件の定義]セクションで、[**Add**]ボタンをクリックします。
4. 検査する[IP**Address range**]とSystem Center 2012 Operations Managerがエージェントをインストールする先のコンピューターに該当する[SSH **Credentials**]を設定します。
5. 範囲と資格情報の条件を確認します。確認するには、[**OK**]をクリックし、[**Discover**]ボタンをクリックして、探索プロセスを開始します。
6. 完了するとリストが表示され、監視 管理の対象となるシステムを選択できます。

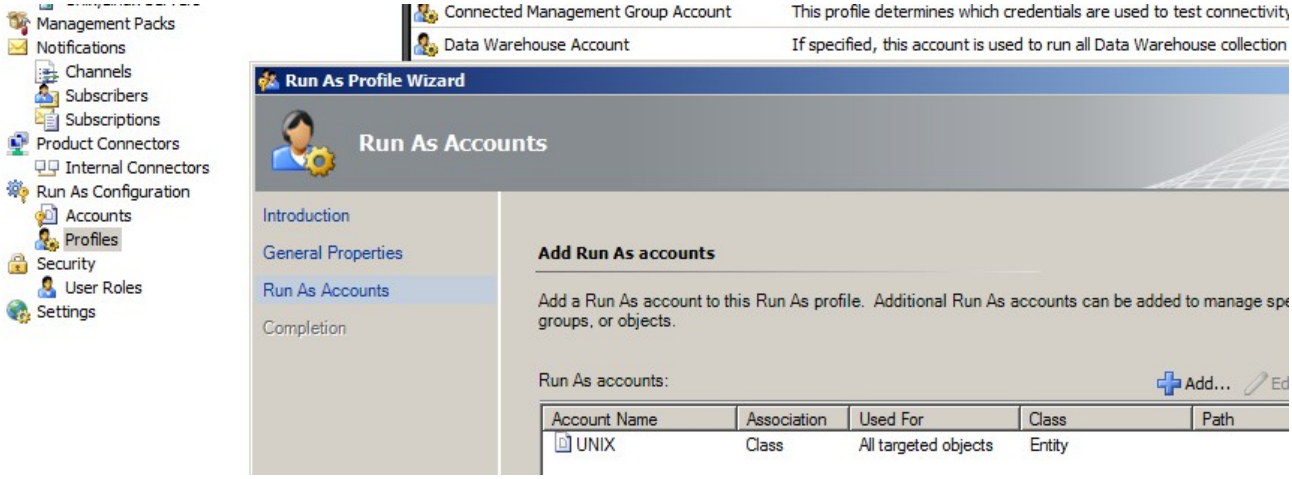
注意: Linuxエージェントのインストールは、次のLinuxディストリビューションでサポートされています。[探索]を使用してLinuxエージェントをインストールできない場合、以下のMicrosoft記事クロス プラットフォーム エージェントの手動インストール(http://technet.microsoft.com/ja-jp/library/dd789016.aspx)を参照してください。

注意: SCEPをインストールしたLinuxサーバの探索は、Operations Managerを介して管理される(つまり、システムディストリビューション用の該当するLinux管理パックがインストールされている)すべてのLinuxコンピュータ上で8時間間隔で自動的に実行されます。その探索によって、次のすべてのサポートモジュールエンティティが作成されます。保護対象Linuxサーバおよびネストされたエンティティまたは保護されていないLinuxサーバ(該当セクションを参照)。scep_daemonサービス(停止中または稼働中のどちらであっても)が存在する場合に、SCEPは完全にインストールされているとみなすことができます。このように、最初の探索は管理パックのインストール時に行われますが、その次は、探索サイクルに従って8時間後に実行されます。SCEPパックをアンインストールすると、それぞれのサーバーは自動的に保護対象外(SCEPを備えていないサーバー)に移行し。この逆の移行もあります。

実行アカウント設定

Unixアカウントを作成するには、以下の指示に従ってください。

1. [**Administration**]ワークスペース(左ペイン)で[**Run As Configuration**] > [**Accounts**]に移動します。
2. 新規アカウントを作成するには、[**Actions**[**アクション**]ペイン(右ペイン)にあるセクションを開き、[**Create Run As Account...**]をクリックします。
3. [全般プロパティ]ウィンドウで、[**Run As Account type**]ドロップダウンメニューから[**Basic Authentication**]を選択します。
4. アカウントの作成が完了したら、配布を実行するためにその新しいアカウントをプロファイルに追加する必要があります。そのためには、[**Run As Configuration**] > [**Profiles**]の下の[**Unix Privileged Account**]プロファイルを右クリックして[**Properties**]を選択し、ウィザードを完了して新たに作成したアカウントを割り当てます。



注意: 実行アカウントの作成の詳細は、System Center 2012 Operations Manager 2007 R2オンラインライブラリーの中のアカウントとしてのクロス プラットフォーム 実行の構成 (http://technet.microsoft.com/ja-jp/library/dd788981.aspx) を参照してください。

上述の手順をすべて完了した後、新たに検出したLinuxサーバーは間もなく[**Monitoring**] > [**System Center Endpoint Protection Linux**] > [**SCEPを備えたサーバ**]の下で使用可能になります。

SCEPの言語パックのインストール

言語パックのフォーマットは次のとおりです。
Microsoft.SCEP.Linux.Application.LNG.mpおよびMicrosoft.SCEP.Linux.Library.LNG.mp

言語パックをインストール際には、上述の「**管理パックのインポート**」セクションの説明と同じステップに従います。
System Center 2012 Operations Managerにインストールされた言語を表示するには、以下の指示に従います。

1. Windowsの[**スタート**]アイコンをクリックし、[**コントロールパネル**]に移動します。
2. コントロールパネルで、[**地域と言語のオプション**]をクリックします。
3. [**管理**]タブで、Unicode対応でないプログラムのシステムロケールに変更します。[**ロケーション**]タブで、インストールされた言語パックに対応する現在のロケーションに変更します。

管理パックの目的

SCEPの管理パックには次のような機能があります。

- セキュリティに関する出来事およびセキュリティ上の健常状態についてのリアルタイムの監視および警告。
- サーバ管理者が、自分のサーバ上でセキュリティ関連タスクをリモートから実行できるようにします。これらのタスクの主な目標は、セキュリティに関連した可用性問題を修正することにあります。

ビュー

サーバ管理者は、Operations Managerコンソールを使用して、SCEPがインストールされたすべてのコンピュータを監視できます。System Center Endpoint Protection Linuxでは、以下のビューを利用できます。

- [**アクティブな警告**] - すべての重大度レベルのすべてのSCEPのアクティブな警告。閉じられた警告は含まれません。
- [**ダッシュボード**] - [SCEPを備えたサーバ]タブと[アクティブな警告]ワークスペースの両方を表示します。
- [**SCEPを備えたサーバ**] - 保護されているLinuxサーバーをすべて表示します。
- [**SCEPを備えていないサーバ**] - 保護されていないLinuxサーバをすべて表示します。
- **タスクの状態** - 実行済みのすべてのタスクを一覧で表示します。

System Center 2012 Operations Manager管理パックでSCEPの状態を監視すると、SCEP状況のビューをすぐに表示できます。

警告が表示されるまで待つまでもなく、SCEPコンポーネントの状態の概要はいつでも表示できます。表示させるには、Operations Manager監視コンソールの[**Monitoring**] > [**System Center Endpoint Protection Linux**] > [**SCEPを備えたサーバ**]ペインをクリックします。コンポーネントの状態は、次のように、色分けされたアイコンで[状態]フィールドに表示されます。

アイコン	状態	説明
	Healthy	緑色のアイコンは成功を示します。または、アクションを必要としない情報があることを示します。
	Warning	黄色のアイコンは、エラーまたは警告を示します。
	Critical	赤色のアイコンは、重大なエラーまたはセキュリティ上の問題を示すか、またはサービスが稼働していないことを示します。
	Not monitored	アイコンがない場合は、状態に影響を与えるデータは収集されていないことを示します。

ビューに表示されるオブジェクトが長いリストになることがあります。特定のオブジェクトまたはオブジェクトのグループを見つけだすには、Operations Managerツールバーの[スコープ]、[検索]、および[検索]ボタンを使用します。詳細は、Essentials でスコープおよび検索を使用してデータの監視を管理する方法 (http://technet.microsoft.com/ja-jp/library/bb437275.aspx)トピックを参照してください。

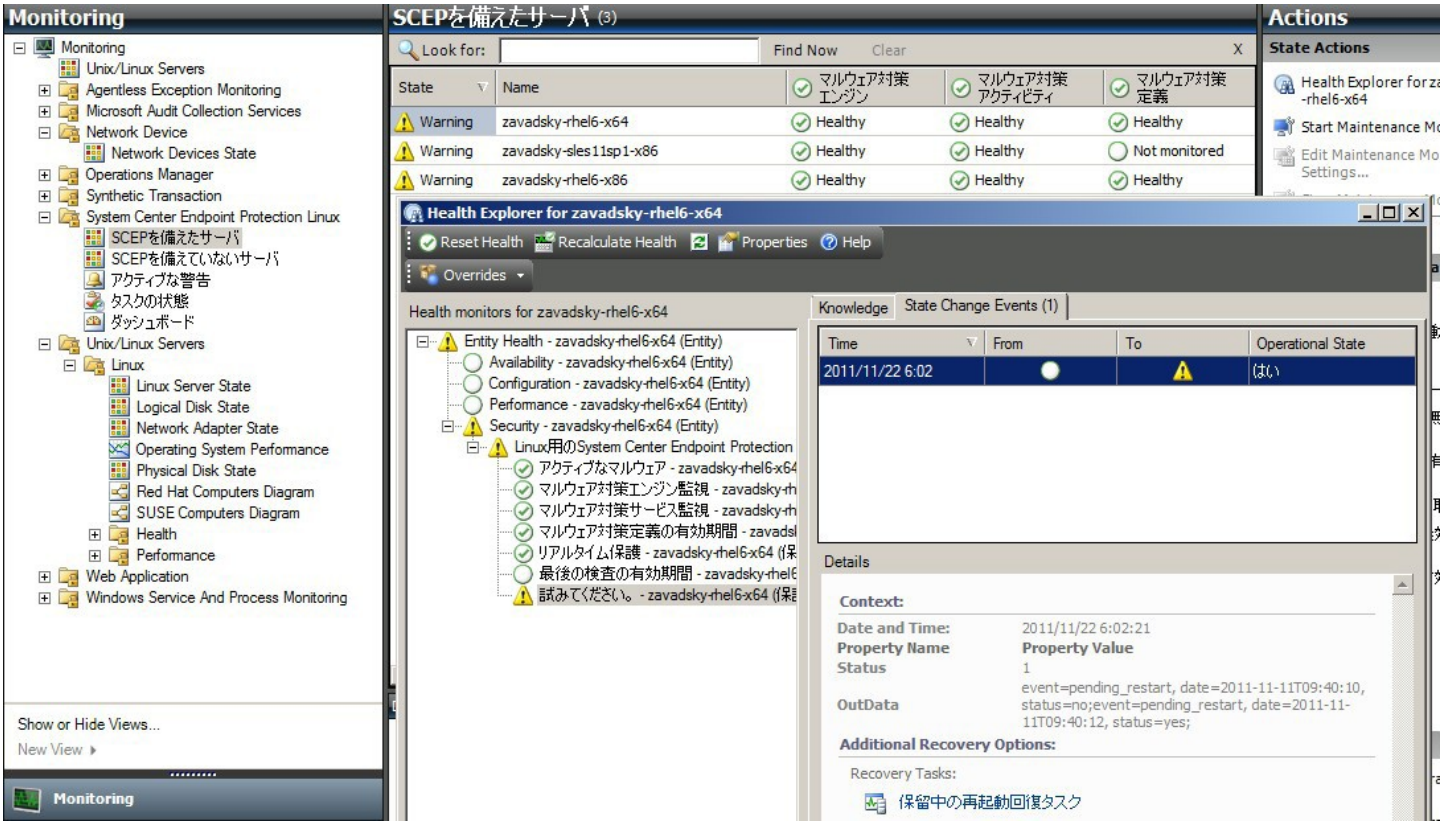
監視機能

Operations Manager 2007では監視機能を使用して、監視対象オブジェクトで発生する可能性のある多様な条件を評価できます。

SCEPで使用できる監視機能は以下の17個です。

- 9つのユニット監視機能 -基本監視コンポーネントです。個々のカウンター、イベント、スクリプト、およびサービスの監視に使用されます。
- 2つの集約監視機能 -集約ロールアップによって複数の監視機能を1つの監視機能にまとめ、その後その監視機能を使用して状況を設定して警告を生成するのに使用されます。
- 6つの依存関係監視機能 - 既存の監視機能の状態データを格納している参照機能。

注意: 監視機能の詳細は、Operations Manager 2007 R2のヘルプを参照してください(System Center 2012 Operations ManagerでF1キーを押します)。



SCEPの状況監視機能の構造と特性について、以下に説明します。

アクティブなマルウェア

監視機能タイプ	ユニット監視機能
対象	保護対象Linuxサーバ
データソース	テキストログファイル(/var/log/scep/eventlog_scom.dat)を監視します。
間隔	イベントにより起動
警告	あり。自動解決なし
リセット動作	8時間が経過した後、自動的に健全状態に戻ります。未対処のマルウェアに関する情報の保持のため、警告はアクティブのままになります
メモ	この監視機能は、マルウェアが見つかり、駆除できなかった場合に、状態を[重大]に変更します。状態は8時間後に[健常]に戻ります(マルウェアが駆除または削除されたかどうかを正確に判断することは不可能だからです)。状況を検討し、チケットを手動で閉じるには、管理者が関与する必要があります。
状態	健全 -マルウェアなし 重大 -マルウェアがアクティブ
有効	オン
回復タスク	なし

この監視では、失敗したマルウェアのクリーンアップ操作が追跡されます。マルウェアの駆除に失敗したことをクライアントが報告すると、この監視機能は重大状態を報告します。

マルウェア対策定義の有効期間

監視機能タイプ	ユニット監視機能
対象	保護対象Linuxサーバ
データソース	監視データを取得する際に使用されるコマンド： /opt/microsoft/scep/sbin/scep_daemon --状態
間隔	8時間ごと
警告	あり。自動解決

状態	健常 -期間が3日以下の場合 警告 -期間が3日を超え、かつ5日以下 重大 -期間が5日を超える場合
有効	オン
回復タスク	あり。手動(自動回復なし)

コンピューターを最新のマルウェアの脅威から保護するには、最新の定義を使用する必要があります。

マルウェア対策エンジン

監視機能タイプ	ユニット監視機能
対象	保護対象Linuxサーバ
データソース	テキストログファイル(/var/log/scep/eventlog_scom.dat
間隔	イベントにより起動
警告	あり。自動解決
状態	健常 -有効 無効 -警告
有効	オン
回復タスク	あり。手動(自動回復なし)

マルウェア対策保護を常時有効にしておくことをお勧めします。
注意: この監視機能は、ウイルス対策保護の状態を追跡します。これはリアルタイム保護と同じではありません。マルウェア対策エンジンが無効になっていると、オンデマンド検査を開始できません。

マルウェア対策サービス

監視機能タイプ	ユニット監視機能
対象	保護対象Linuxサーバ
データソース	プロセスscep_daemonの状態を監視します。
間隔	10分おき
警告	あり。自動解決
状態	健常 -稼動中 重大 -稼動していない
有効	オン
回復タスク	あり。手動(自動回復なし)

クライアントマシンでマルウェア対策サービス(scep_daemon)が実行されていない場合や無応答の場合、あるいはマルウェア対策エンジンが正常に稼動していない場合、監視機能は重大状態を報告します。

最後の検査の有効期間

監視機能タイプ	ユニット監視機能
対象	保護対象Linuxサーバ
データソース	監視データを取得する際に使用されるコマンド： /opt/microsoft/scep/sbin/scep_daemon --状態
間隔	8時間ごと
警告	なし
状態	健常 -期間が7日以下の場合 警告 -期間が7日を超える場合
有効	オン
回復タスク	あり。手動(自動回復なし)

この監視機能は、最後のコンピュータの検査（検査タイプには関係なく)からの経過時間を追跡します。毎週検査を実行するようスケジュールすることをお勧めします。

保留中の再起動

監視機能タイプ	ユニット監視機能
対象	保護対象Linuxサーバ
データソース	テキストログファイル(/var/log/scep/eventlog_scom.dat
間隔	イベントにより起動
警告	あり。自動解決
状態	なし -健常 あり -警告
有効	オン
回復タスク	あり。手動(自動回復なし)

この監視機能は、設定の変更を有効化するためにシステムの再起動が必要かどうかを追跡します(通常はリアルタイム保護の有効化 無効化のとき)。監視機能では、この状態のオンデマンドアップデートに対し、以下の呼び出しを適用します:/opt/microsoft/scep/sbin/scep_daemon --状態。

リアルタイム保護

監視機能タイプ	ユニット監視機能
対象	保護対象Linuxサーバ
データソース	テキストログファイル(/var/log/scep/eventlog_scom.dat この監視機能では、状態のオンデマンドアップデートに以下の呼び出しも使用できます: /opt/microsoft/scep/sbin/scep_daemon --状態。
間隔	イベントにより起動
警告	あり。自動解決
状態	有効 -健常 無効 -警告
有効	オン
回復タスク	あり。手動(自動回復なし)

リアルタイム保護の状態を監視します。リアルタイム保護は、ウイルス、スパイウェア、または潜在的に不要な他のソフトウェアが、お使いのコンピューターにインストールされようとしたときに警告を生成します。

Linux用のSystem Center Endpoint Protection

監視機能タイプ	集約監視機能
対象	保護対象Linuxサーバ
状態	最悪の状況をロールアップ
警告	なし
有効	オン
回復タスク	なし

この監視機能は、すべてのSCEP 7保護対象サーバセセキュリティユニット監視機能の状況ロールアップ(最悪の状況をロールアップ)です。状態が未初期化である場合、このオブジェクトに対して監視機能がまだ開始していないか、またはこのオブジェクトに対して定義されたセキュリティ監視機能がありません。

マルウェア対策エンジン

監視機能タイプ	依存関係監視機能
対象	マルウェア対策エンジン
警告	なし
有効	オン
回復タスク	なし

保護対象Linuxサーバ /マルウェア対策エンジンユニット監視機能の状態を、監視対象コンピュータのリストに表示します。

マルウェア対策サービス

監視機能タイプ	依存関係監視機能
対象	マルウェア対策エンジン
警告	なし
有効	オン
回復タスク	なし

保護対象Linuxサーバー /マルウェア対策サービスユニット監視機能の状態を、監視対象コンピューターのリストに表示します。

マルウェア対策定義

監視機能タイプ	依存関係監視機能
対象	マルウェア対策定義
警告	なし
有効	オン
回復タスク	なし

保護対象Linuxサーバー /マルウェア対策定義有効期間監視機能の状態を、監視対象コンピューターのリストに表示します。

アクティブなマルウェア

監視機能タイプ	依存関係監視機能
対象	マルウェア対策アクティビティ
警告	なし
有効	オン
回復タスク	なし

保護対象Linuxサーバ /アクティブマルウェア監視機能の状態を、マルウェア対策アクティビティのHealth Explorerに表示します。

マシンのPing

監視機能タイプ	ユニット監視機能
対象	マルウェア対策アクティビティ
間隔	60分おき
警告	なし
状態	到達可能 -健常 未達 -重大
有効	オフ
回復タスク	なし

サーバから応答がない場合は、状態を重大に変更します。

マルウェアのアクティビティ

監視機能タイプ	ユニット監視機能
対象	マルウェア対策アクティビティ
データソース	テキストログファイル(/var/log/scep/eventlog_scom.dat
間隔	イベントにより起動
警告	なし
状態	マルウェアなし -健常 マルウェアのアクティビティ検出 -重大
有効	オン
回復タスク	なし

この監視機能は、マルウェアの検出(駆除済みまたは未処理のどちらでも)から5分以内に重大状態に切り替わり、その後60分間重大状態を維持します。重大の状態は、その後検出があるたびに更新され、それとともに警告期間の長さも更新されます。つまり、システム上でマルウェアが60分間検出されない場合、監視機能は健全状態に戻ります。

サーバマルウェアの大規模感染

監視機能タイプ	集約監視機能
対象	マルウェア対策アクティビティ
状態	最良
警告	なし
有効	オン
回復タスク	なし

集約監視機能:マルウェアアクティビティ、マシンのPing
マルウェアの検出(駆除済みまたは未処理のどちらであっても)から60分以内にサーバから応答がない場合、状態を重大に変更します。サーバが無応答である期間の後、接続の更新の直後にマルウェアが検出された場合も、状態が重大に変更されることがあります。

マルウェアの大規模感染

監視機能タイプ	依存関係監視機能
対象	保護対象サーバウォッチャ
状態	95%の最悪
警告	なし
有効	オン
回復タスク	なし

マルウェア対策アクティビティ /サーバマルウェアの大規模感染監視機能の状態を表示します。
過去60分以内にマルウェアが検出されたLinuxコンピュータが、すべてのLinuxコンピュータ(保護対象であってもなくても)の5%を越えた場合、この監視機能の状態は重大に変わります。

SCEP Linuxコンピューターロール状況ロールアップ

監視機能タイプ	依存関係監視機能
対象	Linuxコンピュータ
警告	なし
有効	オン
回復タスク	なし

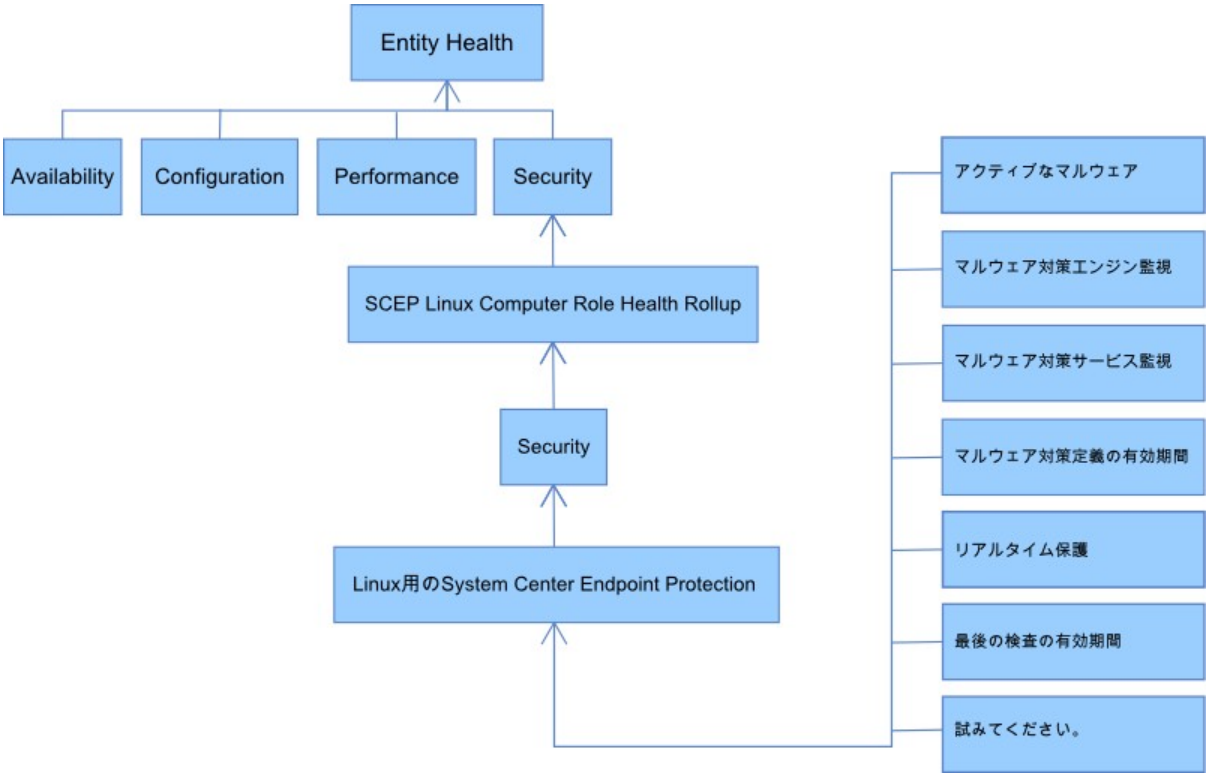
保護対象Linuxコンピュータエンティティの状態をLinuxコンピュータ セキュリティ親監視機能に伝搬します。

状況のロールアップの方法

本管理パックは、Linuxオペレーティングシステムの監視機構を層化構造に拡張します。そこでは各層は、下位の層に依存して健常性を保ちます。この構造の最上部には全エンティティ状況環境があり、セキュリティ環境の最低レベルにはすべての監視機構があります。層の1つの状態が変わると、それにあわせて、その上位の層の状態も変わります。このアクションを状況のロールアップと呼びます。

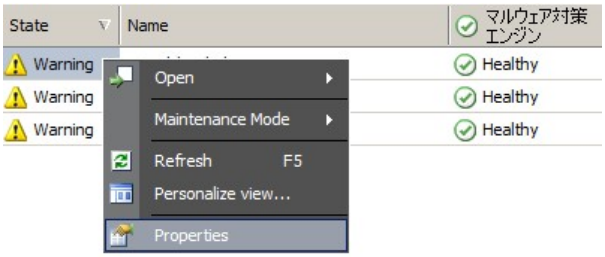
たとえば、リアルタイム保護が警告状態を返した場合に、他のコンポーネントはすべて健常であっても、警告状態はツリー構造を介してルート(エンティティ状況)に送られ、そこでも警告状態を受け取ることになります。

以下の図は、管理パックにおいてオブジェクトの状況がどのようにロールアップするかを示しています。



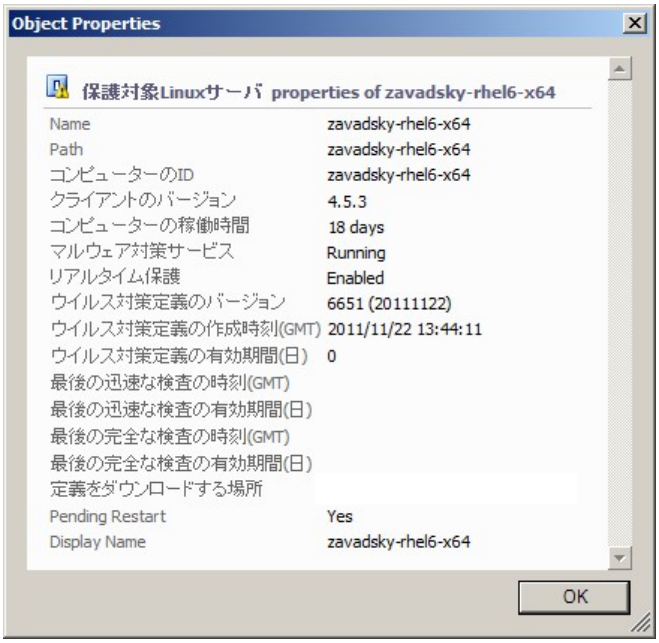
オブジェクトのプロパティ

オブジェクトのプロパティを表示するには、そのオブジェクトを右クリックして**Properties**を選択します。



保護対象Linuxサーバオブジェクトには以下のプロパティがあります。

- [**コンピューターのID**] - サーバーID、ドメイン名。
- [**表示名**]- サーバー名、ドメイン名。
- [**クライアントのバージョン**] - インストールされているSCEP製品のバージョン。
- [**コンピューターの稼働時間**] - サーバーの稼働時間(マシンがダウンタイムなしに稼働していた期間の測定値)は、管理パックが正しく稼働するために不可欠なデータであるため、これがないと管理パックにエラーが示される場合があります。
- [**マルウェア対策サービス**] - マルウェア対策保護の状態(実行中 実行されていない)
- [**リアルタイム保護**] - リアルタイム保護の状態。保護がないとSCEP問題として示されます。
- **ウイルス対策定義 ...**- ウイルスデータベース状態データ(バージョン、作成日、経過期間)。このデータがないと、SCEP問題として示されます。
- **最後の迅速な検査の時刻 最後の完全な検査の時刻 ...**- 最後のコンピューターの検査に関するデータ。検査(迅速な検査 完全な検査)がまだ実行されていない場合、データは表示されません。
- **定義をダウンロードする場所** - アップデートサーバーのアドレス 名前。この情報は、アップデートが最初に正常完了した後で表示されます。
- **保留中の再起動** - SCEPの新規インストールまたはその設定の変更が行われたため、変更を適用するために再起動する必要があるかどうかに関する情報。



警告

警告は、特定の重大度(深刻さ)を持つ事前定義の状態が、監視対象のオブジェクトで起きたことを示します。警告は、ルールによって定義されます。Operations Managerコンソールのビューを使用するには、[**Monitoring**] > [**System Center Endpoint Protection Linux**] > [**アクティブな警告**]を選択します。このビューには、特定のオブジェクトに関してコンソールユーザーが表示権限を持つ警告が表示されます。

注意: 同一のサーバで同一タイプの警告がくり返し生成された場合(たとえばアクティブなマルウェア)場合、最初の1つのみが表示されます(重複する警告は無視されます)。

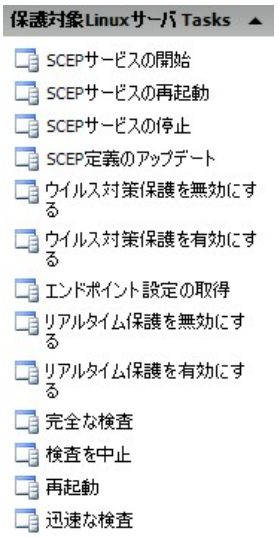
警告	間隔	優先順位	重大度	説明
繰り返しマルウェア感染	イベントにより起動	高	重大	警告は、所定の時間間隔(30分)内にマルウェアがくり返し(3回)検出された場合に生成されます。警告には、サーバに関するデータと、マルウェアに関する基本情報が含まれます。
駆除されたマルウェア	イベントにより起動	低 中	情報 -マルウェアは正常に駆除されました 警告 -サーバの再起動などのユーザーの操作が必要	正常に駆除されたマルウェアに関する警告。特定のマルウェアに関する利用可能なすべてのデータが示されます。検出された各マルウェアごとに、個別のイベントが生成されます。SCEP Linuxは、次のように、駆除プロセスの効率性に基づいて優先順位と重大度を割り当てます。 駆除済み＝低＋情報 駆除済みだがアクション(再起動など)が必要＝中＋警告
アクティブなマルウェア(監視から)	イベントにより起動	高	重大	駆除されなかったマルウェアに関する警告。特定のマルウェアに関する利用可能なすべてのデータが示されます。
アクティブなマルウェア(ルールから)	イベントにより起動	高 中 低	重大 中 低 -マルウェアのタイプをベースとして	同上。他の監視 チケットシステムへの接続に使用されます。 **注意:** このルール(警告)は、既定では無効化されています。

System Center Endpoint Protectionマルウェア対策サービスがダウンしています	300秒	中	重大	マルウェア対策サービスSCEP (scep_daemon)を使用できないことに関する警告。個々のサーバ名とSCEPバージョンも含まれます。
マルウェア対策保護は無効	イベントにより起動	中	警告	マルウェア対策保護が無効であることに関する警告。個々のサーバ名も含まれます。
リアルタイム保護は無効	イベントにより起動	中	警告	リアルタイム保護が無効であることに関する警告。個々のサーバ名も含まれます。
定義が最新ではない	8時間ごと	中	警告(期間が5日以下および期間が3日を越える場合) 重大(期間が5日を超える場合)	3日以上更新されていないウイルス定義データベースに関する警告。個々のサーバ名とウイルス定義データベースの経過時間も含まれます。
マルウェアの大規模感染	イベントにより起動	高	重大	Forefront Endpoint Protectionにより、5%を越えるコンピュータ上でアクティブなマルウェアが検出されました。コンピュータでマルウェアが増殖している可能性があります。すべてのサーバで最新の定義が使用されていることを確認するようお勧めします。この警告の原因となるアクティブな脅威の数を変更する必要がある場合、マルウェア大規模感染監視機能のパラメーターを指定変更してください(「上書き」の章を参照)。

タスク

SCEP用の管理パックは、13個のタスクを実装します。それらのタスクはただちに実行されます。出力は、タスクの実行直後に表示されますが、後で[タスクの状態]ウィンドウに表示することもできます。タスクの実行に要する最大時間は180秒です。上書きは使用できません。すべてのタスクは、SSHを介してBASHコマンドによって実行されます。

タスクは、[操作コンソール]ウィンドウの右ペインの[**Monitoring**] > [**System Center Endpoint Protection Linux**] > [**SCEPを備えたサーバ**]の下で起動できます。



- [**ウイルス対策保護の無効化**] - ウイルス対策保護のすべてのコンポーネントを無効にし、オンデマンド検査を無効にします。
- [**ウイルス対策保護を有効化する**] - ウイルス対策保護のすべてのコンポーネントを有効にします。
- [**リアルタイム保護の無効化**] - リアルタイム保護を無効にします。
- [**リアルタイム保護の有効化**] - リアルタイム保護を有効にします。
- [**完全な検査**] - ウイルス定義データベースをアップデートし、完全なコンピューターの検査を実行します。
- [**迅速な検査**] - ウイルス定義データベースをアップデートし、迅速なコンピューターの検査を実行します。
- [**検査を中止**] - 実行中のすべてのコンピュータの検査を停止します。
- [**サーバ設定の取得**] - SCEP製品の現在の状態を表示します。表示されたパラメーターのリストは、保護対象Linuxサーバーエンティティのプロパティと同じです。表示されたデータは、保護対象Linuxサーバには転送されません。
- [**マルウェア対策サービスの再起動**] - SCEPマルウェア対策サービス(scep_daemon)を再起動します。
- [**マルウェア対策サービスの停止**] - SCEPマルウェア対策サービス(scep_daemon)を停止します。
- [**マルウェア対策サービスの開始**] - SCEPマルウェア対策サービス(scep_daemon)を開始します。
- [**マルウェア対策定義のアップデート**]- ウイルス定義データベースのアップデートを開始します。
- **再起動** - Linuxコンピュータを再起動します。

SCEP用の管理パックの設定

ベストプラクティス:カスタマイズ用の管理パックの作成

既定ではOperations Managerは、上書きなどのすべてのカスタマイズを既定の管理パックに保存します。その代わりに、ベストプラクティスとしては、カスタマイズする各シールド管理パックごとに、別の管理パックを作成します。

シールド管理パック用にカスタマイズした設定を保管する目的で管理パックを作成する場合、「SCEP 2012 Customizations」のように、カスタマイズの元の管理パックの名前に基づいて新規の管理パックに名前を付けると便利です。

各シールド管理パックのカスタマイズを保管するための新規管理パックを作成すると、テスト環境から実働環境にカスタマイズをエクスポートするのが簡単になります。また、管理パックを削除するのも簡単になります。管理パックを削除する前に、すべての依存関係を削除する必要があるからです。すべての管理パックのカスタマイズを既定の管理パックに保存しておけば、管理パックを1つだけ削除する必要が生じたときには、まず既定の管理パックを削除する必要があります。そうすると、他の管理パックに加えられたカスタマイズも削除されます。

セキュリティの設定

コンピュータがSSHDサービスを実行し、SSHポート(既定値は22)が開いている必要があります。System Center 2012 Operations Managerはこのポートを通して、**Basic Authentication**タイプで適切なRun As Account(Operations Manager管理コンソールの**Administration** > **Run As Configuration**ペイン)を使用してリモートのLinuxコンピューターに接続します。

実行プロファイル名	メモ
Unix Privileged Account	Unixサーバーをリモートから監視するのに使用されるとともに、特権を必要とするプロセスの再起動にも使用されます。

この管理パックは、Unix Action Accountを使用しません。

警告: コンピューターの監視でrootアカウントを使用すると、パスワードが破られた場合などの潜在的セキュリティリスクとなります。

rootアカウントを使用して監視や管理をしない場合、標準ユーザーのアカウントを使用できますが、このアカウントには、*sudo*コマンドを実行する権限が必要です。そのため、選択したユーザーアカウントのsudo昇格を許可するために、Linux SCEPの監視対象の各ワークステーションにある/etc/sudoersファイルに以下のような設定が必要です。以下は、user1というユーザー名の設定例です。

```
#--------------------------------------------------------------------------------
# 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
#--------------------------------------------------------------------------------
```

パフォーマンスしきい値ルールのチューニング

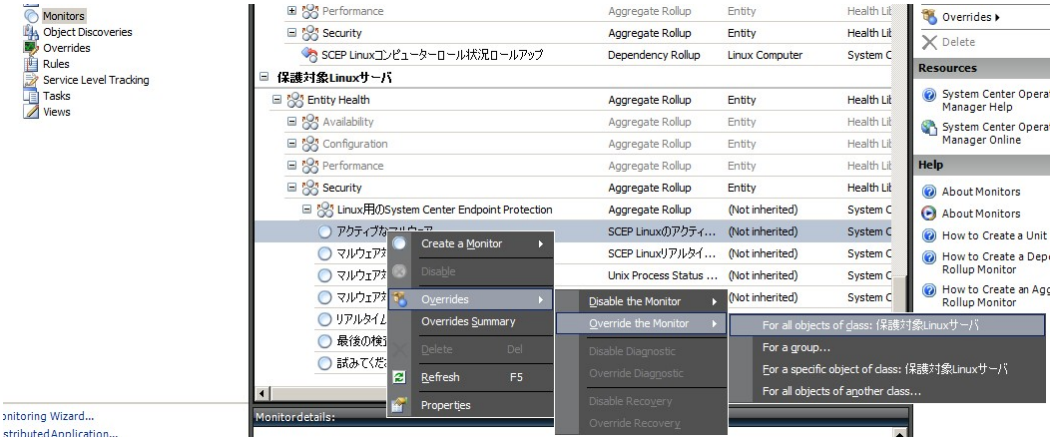
以下の表は、環境にあわせてさらに既定のしきい値のチューニングが必要になる可能性のあるパフォーマンスしきい値ルールを一覧で示しています。これらのルールを評価して、既定のしきい値が自分の環境に適しているかどうかを判別します。既定のしきい値が適切ではない環境の場合、しきい値に上書きを適用して調整できます。

ルール名	上書きパラメータ	既定のしきい値	チューニングの制約事項
繰り返しマルウェア感染ルール	繰り返し感染カウントのしきい値	3回の発生回数	値を2より小さく設定すると、ルールが廃棄されます。
繰り返しマルウェア感染ルール	繰り返し感染時間ウィンドウ	30分	オンデマンド検査の持続時間より小さい値を設定することは推奨されません。オーバーラップにより、警告の生成が妨げられることがあるからです。
アクティブなマルウェアの警告ルール	有効	オフ	他の監視 *ポケットシステムへのコネクタを使用する場合は、この警告を有効化できます。

上書き

上書きを使用して、System Center 2012 Operations Manager内の監視オブジェクトの設定を調整できます。それには、インポートした管理パックにあった監視、ルール、オブジェクト探索、および属性も含まれます。

監視機能を上書きするには、操作コンソールで[**Authoring**]ボタンをクリックし、[**Management Pack Objects**] > [**Monitors**]を展開します。[監視機能]ペインで、オブジェクトタイプを見つけて完全に展開してから、監視機能をクリックし、次に[**Overrides**]をクリックします。



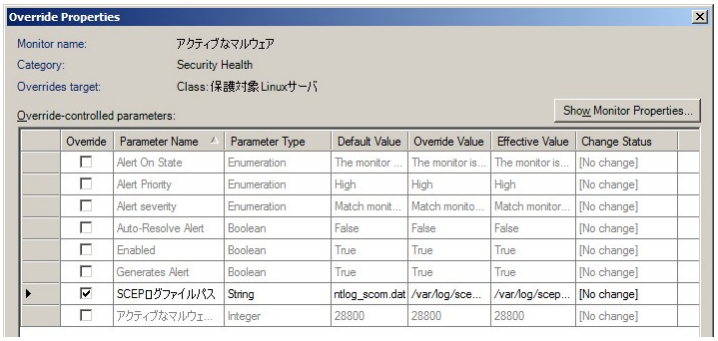
以下のパラメータの上書きの作成または変更を行うには、[上書き]ウィンドウを使用します。

- [**アクティブなマルウェア監視のフォールバック時間**](アクティブなマルウェア監視にのみ関連します)
- [**マルウェア対策定義の有効期間**](マルウェア対策定義の有効期間の監視にのみ関連します)
- [**検出間隔**](最後の検査の有効期間の監視にのみ関連します)
- **警告オン状態**
- **警告優先順位**
- **警告の重大度**
- **自動解決警告**
- [**有効**] - 選択した監視機能が有効または無効のどちらであるかを判別します。
- **警告の生成**
- **SCEPログファイルパス**

既定の上書きが適切ではない環境の場合、しきい値に上書きを適用して調整できます。

上書きパラメータ	監視機能名	既定値	チューニングメモ
Ping間隔	マシンのPing	3600秒	保護対象Linuxサーバの可用性をチェックする間隔。間隔を短くすると、攻撃を受けたためにマシンが応答を停止した場合に、サーバマルウェアの大規模感染監視機能がより早くエラー状態になります。その結果、ネットワーク、監視対象のコンピュータ、およびSystem Center 2012 Operations Managerサーバに対する負荷が増大します。
マルウェアの大規模感染時間ウィンドウ	マルウェアのアクティビティ	3600秒	マルウェアアクティビティ後に監視機能が健常状態に戻るのに要する期間。時間ウィンドウ監視値がマシンPing/Ping間隔よりも高くないと、この組み合わせは正常に機能しません。 マルウェア大規模感染時間ウィンドウの間隔中に、設定されているマルウェアの大規模感染のパーセンテージ値(「マルウェアの大規模感染」を参照)を超える数のコンピュータがマルウェアアクティビティを登録すると、マルウェアの大規模感染警告が生成されます。 注意:これは、サーバマルウェアの大規模感染とは異なります。サーバマルウェアの大規模感染では警句は生成されません。
アクティブなマルウェア監視のフォールバック時間	アクティブなマルウェア	28800秒	マルウェア検出以降の時間間隔。その時点以後は、マルウェアは駆除済みとみなされます。
SCEPログファイルパス	アクティブなマルウェア	/var/log/scep/eventlog_scom.log	System Center 2012 Operations Managerイベントの記録先のファイルへのパス。問題が起きない限り、このパラメーターは変更しないでください。
マルウェア対策定義の重大状態の有効期間	マルウェア対策定義の有効期間	5日間	この期間が過ぎると、SCEP製品が期限切れであることを知らせるエラー警告が生成されます。
マルウェア対策定義の正常状態の有効期間	マルウェア対策定義の有効期間	3日間	マルウェア対策定義の最大許容有効期間。その期間中は、定義を最新とみなすことができます。この値は、マルウェア対策定義の重大状態の有効期間の値より常に小さくなければなりません。
間隔	マルウェア対策定義の有効期間	28800秒	マルウェア対策定義の有効期間をチェックする間隔。
間隔	マルウェア対策サービス	300秒	マルウェア対策サービスの可用性をチェックする間隔。

プロセス名	マルウェア対策サービス	scep_daemon	マルウェア対策サービスの名前。監視機能が使用中の場合、この値を変更しないでください。
検出間隔	最後の検査の有効期間	28800秒	最後の検査の実行をチェックする間隔。
最長検査有効期間	最後の検査の有効期間	7日間	SCEP製品の設定に従って設定します。検査が7日おきにスケジュールされていれば、この値も7日に設定します。
ログファイルパス	保留中の再起動	/var/log/scep/eventlog_scom.log	System Center 2012 Operations Managerイベントの記録先のファイルへのパス。問題が起きない限り、このパラメーターは変更しないでください。
SCEPログファイルパス	リアルタイム保護	/var/log/scep/eventlog_scom.log	System Center 2012 Operations Managerイベントの記録先のファイルへのパス。問題が起きない限り、このパラメータは変更しないでください。
パーセント	マルウェアの大規模感染	95%	監視対象のグループ全体が健常とみなされるために、Linuxサーバ(保護対象であってもなくても)のうちの何パーセントのサーバが健常の状態を戻す必要があるか。総数のうちの5%以上でマルウェアが検出された場合、マルウェアの大規模感染が生成されます。



注意: 上書きの詳細は、上書きを使用して監視する方法 (http://go.microsoft.com/fwlink/?LinkID=117777) を参照してください。

リンク

以下のリンクは、本管理パックに関連した共通タスクに関する情報を表示します。

- 管理パック ライフ サイクルの管理
  (http://technet.microsoft.com/ja-jp/library/cc974486.aspx)
- Operations Manager 2007 で管理パックをインポートする方法
  (http://technet.microsoft.com/ja-jp/library/cc974494.aspx)
- 上書きを使用して監視する方法
  (http://technet.microsoft.com/ja-jp/library/bb309719.aspx)
- Operations Manager 2007 で実行アカウントを作成する方法
  (http://technet.microsoft.com/ja-jp/library/bb309445.aspx)
- アカウントとしてのクロス プラットフォーム 実行の構成
  (http://technet.microsoft.com/ja-jp/library/dd788981.aspx)
- 既存の実行アカウントを変更する方法
  (http://technet.microsoft.com/ja-jp/library/dd891202.aspx)
- 管理パックのカスタマイズをエクスポートする方法
  (http://technet.microsoft.com/ja-jp/library/cc974487.aspx)
- 管理パックを削除する方法
  (http://technet.microsoft.com/ja-jp/library/cc974489.aspx)
- Essentials でスコープおよび検索を使用してデータの監視を管理する方法
  (http://technet.microsoft.com/ja-jp/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 (英語版))
- クロス プラットフォーム エージェントの手動インストール
  (http://technet.microsoft.com/ja-jp/library/dd789016.aspx)
- Configuring sudo Elevation for UNIX and Linux Monitoring with System Center 2012 - Operations Manager (System Center 2012 - Operations Managerを使用したUNIX/Linux監視のsudo昇格の設定)
  (http://social.technet.microsoft.com/wiki/contents/articles/7375.configuring-sudo-elevation-for-unix-and-linux-monitoring-with-system-center-2012-operations-manager.aspx)(英語版)

Operations Managerおよび監視パックの詳細は、System Center Operations Manager フォーラム (http://social.technet.microsoft.com/Forums/ja-jp/category/systemcenteroperationsmanager) を参照してください。
個々の監視パックの「用例」の記事が載っているSystem Center Operations Manager Unleashed blog (http://opsmgrunleashed.wordpress.com/) (英語版) が役に立ちます。

Operations Managerに関する追加情報は、以下のブログを参照してください。

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

トラブルシューティングの詳細は、以下のフォーラムのスレッドを参照してください。

- Microsoft.Unix.Library is missing

(http://social.technet.microsoft.com/Forums/ja-jp/operationsmanagermgmtpacks/thread/8469d0ff-54d6-4cb4-9909-49ab62126b74/)