



Microsoft®  
**System Center**  
**Operations Manager**

## **System Center Monitoring Pack für Endpoint Protection für Linux**

---

Microsoft Corporation

Veröffentlicht: 10/26/2015

Feedback und Vorschläge zu diesem Dokument können Sie an diese Adresse senden:  
[mpgfeed@microsoft.com](mailto:mpgfeed@microsoft.com). Erwähnen Sie dabei bitte den Titel des Management Pack-Handbuchs.

Sie können dem Operations Manager-Team Ihre Meinung auch mit einem Meinungsbericht auf der Seite des Management Packs im [Management Pack-Katalog](http://go.microsoft.com/fwlink/?LinkID=82105) (<http://go.microsoft.com/fwlink/?LinkID=82105>) mitteilen.

## Inhalt

|   |          |
|---|----------|
| <b>Handbuch zum SCEP Management Pack</b>      | <b>3</b> |
| Änderungsprotokoll                            | 3        |
| Änderungen in Version 4.5.10.1                | 3        |
| Unterstützte Konfigurationen                  | 3        |
| Voraussetzungen                               | 3        |
| Dateien in diesem Management Pack             | 4        |
| Erste Schritte                                | 4        |
| Zweck des Management Packs                    | 6        |
| Ansichten                                     | 6        |
| Monitore                                      | 7        |
| Integritätsstatus-Rollup                      | 11       |
| Objekteigenschaften                           | 12       |
| Warnungen                                     | 13       |
| Tasks   | 14       |
| Konfiguration des Management Packs für SCEP   | 15       |
| Best Practice: Management Pack für            | 15       |
| Sicherheitskonfigurationen erstellen          | 15       |
| Optimierung der Leistungsschwellenwert-Regeln | 16       |
| Außerkräftsetzungen                           | 16       |
| Links   | 18       |

# Handbuch zum SCEP Management Pack

Mit diesem Management Pack können Sie System Center Endpoint Protection (SCEP) über System Center 2012 Operations Manager in einer Netzwerkumgebung für mehrere Workstations und Serverrechner zentral verwalten. Mit dem Taskverwaltungssystem von Operations Manager können Sie SCEP auf Remotecomputern verwalten, Warnungen und Integritätsstatusinformationen anzeigen sowie schnell auf neue Probleme und Bedrohungen reagieren.

System Center 2012 Operations Manager bietet selbst keinen Schutz gegen Schadcode und benötigt daher eine SCEP-Lösung auf den verwalteten Linux-Computern.

Dieses Handbuch basiert auf Version 4.5.10.1 des Management Packs für SCEP.

## Änderungsprotokoll

| Version  | VÖ-Datum   | Änderungen   |
|----------|------------|--|
| 4.5.9.1  | 16.05.2012 | Erste Fassung dieses Handbuchs   |
| 4.5.10.1 | 06.11.2012 | Unterstützung für weitere Linux-Distributionen<br>Bessere Beschreibung einiger Management Pack-Tools |

## Änderungen in Version 4.5.10.1

Version 4.5.10.1 des Management Packs für System Center Endpoint Protection umfasst die folgenden Änderungen:

- Unterstützung für weitere Linux-Distributionen:
  - 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**Hinweis:** Diese neuen Distributionen werden nur bei der Verwendung von System Center 2012 Operations Manager Service Pack 1 oder höher unterstützt.
- Bessere Beschreibung der folgenden Elemente:
  - Monitor „Aktive Malware“
  - Warnung „Aktive Malware (von Regel)“

## Unterstützte Konfigurationen

Die grundsätzlich unterstützten Konfigurationen sind im Artikel [Unterstützte Konfigurationen in Operations Manager 2007 R2](http://go.microsoft.com/fwlink/?LinkId=90676) (<http://go.microsoft.com/fwlink/?LinkId=90676>) beschrieben.

Für dieses Management Pack ist System Center 2012 Operations Manager 2007 R2 oder höher erforderlich. Die unterstützten Betriebssysteme für dieses Management Pack sind in der folgenden Tabelle aufgeführt:

| Betriebssystem                       | x86 | x64 |
|--------------------------------------|-----|-----|
| Red Hat Enterprise Linux Server 5, 6 | Ja  | Ja  |
| SUSE Linux Enterprise 10, 11         | Ja  | Ja  |
| CentOS 5, 6                          | Ja  | Ja  |
| Debian Linux 5, 6                    | Ja  | Ja  |
| Ubuntu Linux 10.04, 12.04            | Ja  | Ja  |
| Oracle Linux 5, 6                    | Ja  | Ja  |

## Voraussetzungen

Für die Ausführung dieses Management Packs müssen die folgenden Voraussetzungen gegeben sein:

- [System Center Operations Manager 2007 R2 Kumulatives Update 5](http://support.microsoft.com/kb/2449679) (<http://support.microsoft.com/kb/2449679>)

Die unten aufgeführten Management Packs für SCEP sind entweder Bestandteil von System Center 2012 Operations Manager 2007 R2 oder können aus dem Online-Katalog heruntergeladen werden.

| ID | Name | Version |
|----|------|---------|
|----|------|---------|

|  |                                    |              |
|--|------------------------------------|--------------|
| Microsoft.Linux.Library                      | Linux-Betriebssystembibliothek     | 6.1.7000.256 |
| Microsoft.SystemCenter.InstanceGroup.Library | Instanzengruppenbibliothek         | 6.1.7221.0   |
| Microsoft.SystemCenter.Library               | System Center-Kernbibliothek       | 6.1.7221.0   |
| Microsoft.SystemCenter.WSManagement.Library  | WS-Verwaltungsbibliothek           | 6.1.7221.0   |
| Microsoft.SystemCenter.DataWarehouse.Library | Data Warehouse-Bibliothek          | 6.1.7221.0   |
| Microsoft.Unix.Library                       | Unix-Kernbibliothek                | 6.1.7000.256 |
| Microsoft.Unix.Service.Library               | Bibliothek der Unix-Dienstvorlagen | 6.1.7221.0   |
| Microsoft.Windows.Library                    | Windows-Kernbibliothek             | 6.1.7221.0   |
| System.Health.Library                        | Zustandsbibliothek                 | 6.1.7221.0   |
| System.Library                               | Systembibliothek                   | 6.1.7221.0   |

**Wichtig:** Damit die Überwachung von SCEP für Linux durch System Center 2012 Operations Manager korrekt ausgeführt wird, muss sie erst in der Konfigurationsdatei `/etc/opt/microsoft/scep/scep.cfg` oder über die SCEP-Weboberfläche aktiviert werden. Stellen Sie sicher, dass der in dieser Datei enthaltene Parameter 'scom\_enabled' auf 'scom\_enabled = yes' eingestellt ist. Alternativ können Sie die entsprechende Einstellung in der Web-Oberfläche unter **Konfiguration > Global > Daemon-Einstellungen > SCOM aktiviert** vornehmen.

## Dateien in diesem Management Pack

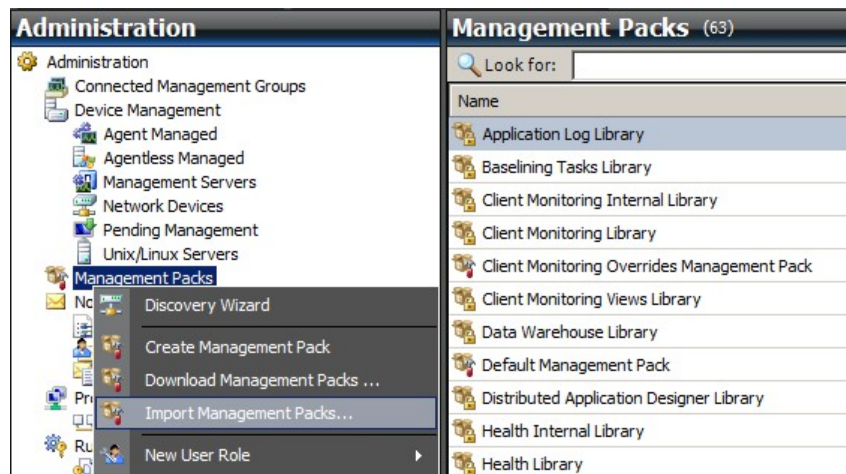
Das Management Pack für SCEP enthält folgende Dateien:

| Dateiname                           | Beschreibung   |
|-------------------------------------|--|
| Microsoft.SCEP.Linux.Library.mp     | Enthält Klassendefinitionen und Klassenbeziehungen sowie Monitortypen und Modultypen-Definitionen. |
| Microsoft.SCEP.Linux.Application.mp | Implementiert die Funktionen für Überwachung, Warnung, Tasks und Ansichten.                        |

## Erste Schritte

Zur Überwachung von SCEP müssen zunächst die Management Packs in Operations Manager importiert und anschließend die zu überwachenden Computer ermittelt werden.

### Importieren der Management Packs

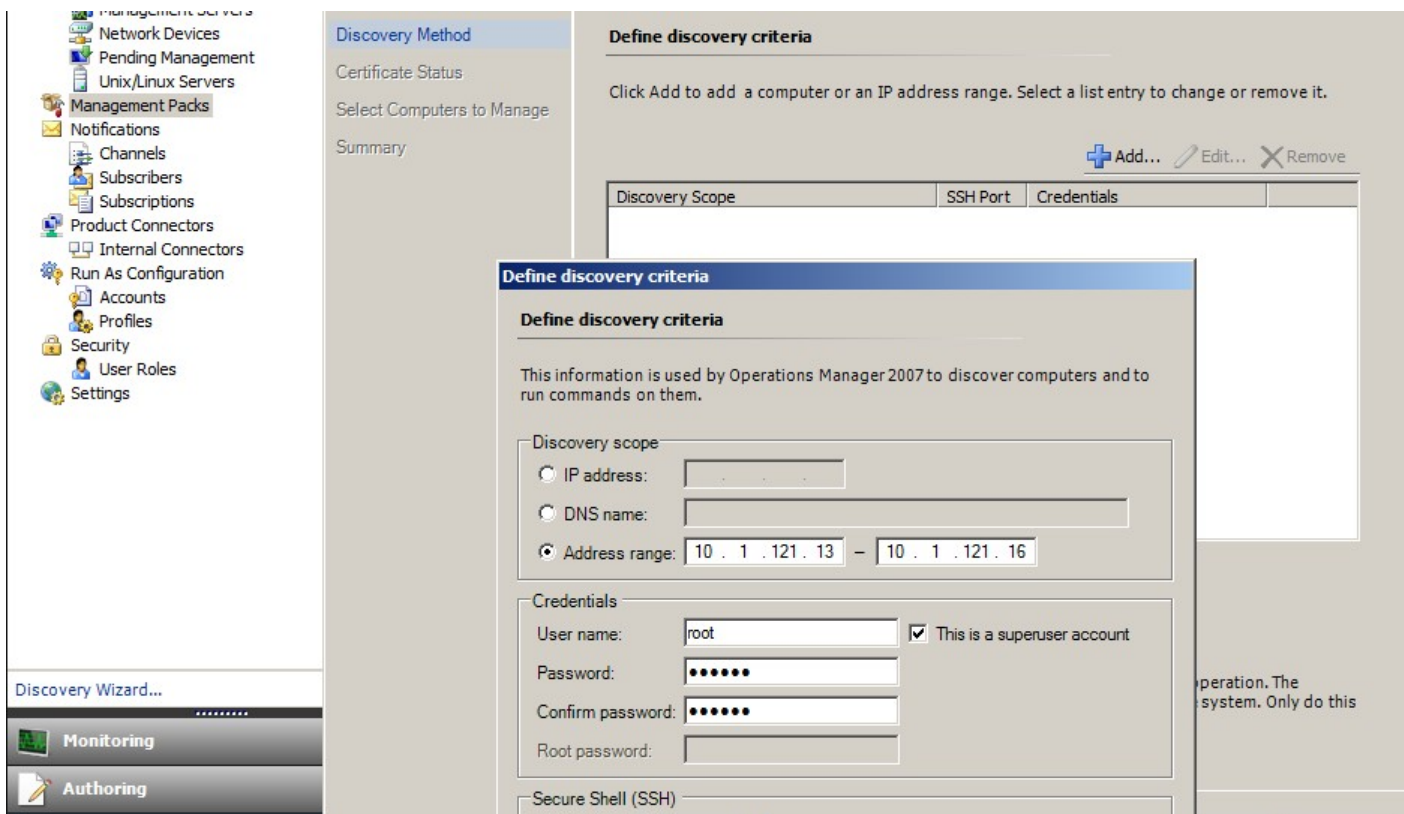


1. Klicken Sie auf den Arbeitsbereich **Administration** im linken Teilfenster der Betriebskonsole.
2. Klicken Sie mit der rechten Maustaste auf **Management Packs** und wählen Sie **Import Management Packs...** aus dem Kontextmenü.
3. Klicken Sie im Fenster „Management Packs“ auf **Add** und wählen Sie **Add from disk...** aus dem Dropdown-Menü.
4. Bestätigen Sie, dass Operations Manager auch Abhängigkeiten suchen und installieren soll, die nicht auf dem lokalen Datenträger vorhanden sind, indem Sie auf **Yes** im Fenster **Online Catalog Connection** klicken.
5. Wählen Sie die beiden aufgeführten Dateien (Microsoft.SCEP.Linux.Application.mp, Microsoft.SCEP.Linux.Library.mp) aus und klicken Sie auf **Install**.

**Hinweis:** Eine ausführliche Anleitung zum Importieren von Management Packs finden Sie im Artikel [Importieren eines Management Packs in Operations Manager 2007](http://go.microsoft.com/fwlink/?LinkId=142351) (<http://go.microsoft.com/fwlink/?LinkId=142351>).

### Ermittlung

Nach dem Importieren der MP-Dateien müssen Sie die zu überwachenden Computer ermitteln.



1. Klicken Sie im Arbeitsbereich **Administration** im linken Teilfenster der Betriebskonsole auf die Verknüpfung **Discovery wizard...** (unten links).
2. Wählen Sie im Assistenten für Computer- und Geräteverwaltung die Option **Unix/Linux computers** und klicken Sie auf **Next**, um fortzufahren.
3. Klicken Sie im Abschnitt „Define discovery criteria“ auf **Add**.
4. Legen Sie unter **Address range** einen IP-Adressbereich für die Prüfung sowie unter **Credentials** die Anmeldedaten für den SSH-Zugriff auf die Computer fest, auf denen der System Center 2012 Operations Manager-Agent installiert werden soll.
5. Bestätigen Sie den Ermittlungsumfang und die Anmeldedaten, indem Sie auf **OK** klicken. Klicken Sie dann auf **Discover**, um die Ermittlung zu starten.
6. Nach Abschluss des Vorgangs wird eine Liste angezeigt, aus der Sie die gewünschten Systeme für die Überwachung/Verwaltung auswählen können.

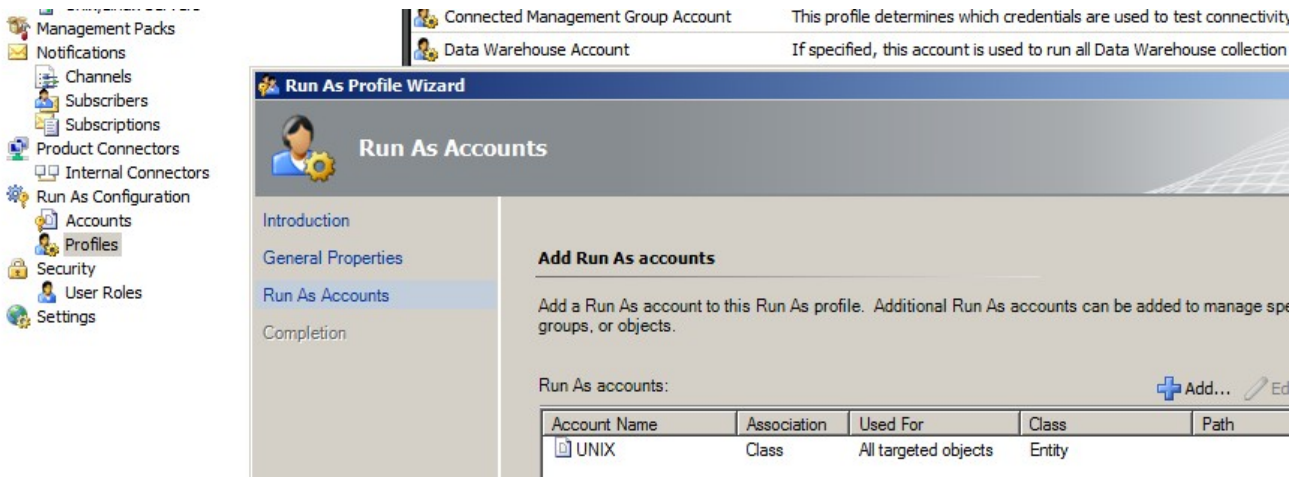
**Hinweis:** Unter welchen Linux-Distributionen die Installation eines Linux-Agents unterstützt wird, können Sie [hier nachlesen](#). Falls der Linux-Agent nicht auf dem Wege der Ermittlung installiert werden kann, finden Sie eine Anleitung zur manuellen Installation im Microsoft-Artikel [Manuelles Installieren plattformübergreifender Agents](http://technet.microsoft.com/en-us/library/dd789016.aspx) (<http://technet.microsoft.com/en-us/library/dd789016.aspx>).

**Hinweis:** Die Ermittlung der Linux-Server mit einer SCEP-Installation wird automatisch alle 8 Stunden für alle Linux-Computer durchgeführt, die über Operations Manager verwaltet werden (d. h. für die das zur jeweiligen Distribution passende Linux-Management Pack installiert ist). Bei der Ermittlung werden alle Dienstmodul-Entitäten erstellt, also „Geschützter Linux-Server“ und die untergeordneten Entitäten bzw. „Nicht geschützter Linux-Server“ (zu finden in den jeweiligen Abschnitten). Eine SCEP-Installation gilt als vorhanden, wenn der Dienst „scep\_daemon“ vorhanden ist (unabhängig davon, ob er ausgeführt wird). Die erste Ermittlung wird daher bei der Installation eines Management Packs ausgeführt, die nächste 8 Stunden später im jeweiligen Ermittlungszyklus. Bei der Deinstallation eines SCEP-Produkts wird der betreffende Server automatisch in die Gruppe „Nicht geschützt“ (Server ohne SCEP) verschoben bzw. analog umgekehrt.

## Konfiguration ausführender Konten

Um ein Unix-Konto zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie im Arbeitsbereich **Administration** im linken Teilfenster den Punkt **Run As Configuration > Accounts**.
2. Um ein neues Konto zu erstellen, öffnen Sie den Bereich **Actions** im Teilfenster **Actions** rechts und klicken auf **Create Run As Account**.
3. Wählen Sie im Fenster „General Properties“ die Option **Basic Authentication** aus dem Dropdown-Menü **Run As Account type**.
4. Nachdem Sie das Konto erstellt haben, müssen Sie es zur Verteilung noch einem Profil hinzufügen. Hierzu klicken Sie unter **Run As Configuration > Profiles** mit der rechten Maustaste auf das Profil **Unix Privileged Account**, wählen **Properties** und weisen über den Assistenten das neu erstellte Konto zu.



**Hinweis:** Weitere Informationen zum Erstellen eines ausführenden Kontos finden Sie im Artikel [Konfigurieren eines plattformübergreifenden ausführenden Kontos](http://go.microsoft.com/fwlink/?LinkId=160348) (<http://go.microsoft.com/fwlink/?LinkId=160348>) in der System Center 2012 Operations Manager 2007 R2-Onlinebibliothek.

Nach Abschluss dieser Schritte sind die neu ermittelten Linux-Server nach wenigen Minuten unter **Monitoring > System Center Endpoint Protection Linux > Server mit SCEP** verfügbar.

## Installieren eines Sprachpakets für SCEP

Die Dateinamen von Sprachpaketen haben das folgende Format:

Microsoft.SCEP.Linux.Application.LNG.mp und Microsoft.SCEP.Linux.Library.LNG.mp

Zur Installation eines Sprachpakets verwenden Sie ebenfalls die bereits im Abschnitt **Importieren der Management Packs** beschriebenen Schritte. Zum Anzeigen der installierten Sprache in System Center 2012 Operations Manager gehen Sie wie folgt vor:

1. Klicken Sie in der Windows-Taskleiste auf **Start** und dann **Systemsteuerung**.
2. Klicken Sie in der Systemsteuerung auf **Regions- und Sprachoptionen**.
3. Ändern Sie auf der Registerkarte **Verwaltung** die „Sprache für Unicode-inkompatible Programme“. Ändern Sie auf der Registerkarte **Standort** den aktuellen Standort passend zum installierten Sprachpaket.

## Zweck des Management Packs

Das Management Pack für SCEP hat folgende Funktionen:

- Echtzeit-Überwachung und Warnungen in Bezug auf sicherheitskritische Ereignisse und den Sicherheits-Integritätsstatus
- Remoteausführung von Tasks auf Servern, um sicherheitsrelevante Verfügbarkeitsprobleme zu beheben

## Ansichten





Über die Operations Manager-Konsole kann der Serveradministrator alle Computer überwachen, auf denen SCEP installiert ist. Für „System Center Endpoint Protection Linux“ sind die folgenden Ansichten verfügbar:

- **Aktive Warnungen** - Alle aktiven SCEP-Warnungen aller Schweregrade. Bereits abgeschlossene Warnungen sind nicht enthalten.
- **Dashboard** - Schließt die Arbeitsbereiche „Server mit SCEP“ und „Aktive Warnungen“ ein.
- **Server mit SCEP** - Zeigt alle geschützten Linux-Server an.
- **Server ohne SCEP** - Zeigt alle nicht geschützten Linux-Server an.
- **Task-Status** - Zeigt alle ausgeführten Tasks an.

Durch die Überwachung von SCEP mit diesem Management Pack für System Center 2012 Operations Manager können Sie sich schnell einen Überblick über den SCEP-Integritätsstatus verschaffen.



Sie müssen nicht warten, bis eine Warnung erzeugt wird, sondern können sich jederzeit den Gesamtstatus der SCEP-Komponenten anzeigen lassen. Hierzu klicken Sie einfach in der Operations Manager-Überwachungskonsole auf **Monitoring > System Center Endpoint Protection Linux > Server mit SCEP**. Der Status der einzelnen Komponenten wird dann im Feld „Status“ mit farbigen Symbolen angezeigt:

| Symbol   | Status        | Beschreibung   |
|--|---------------|--|
|  | Healthy       | Ein grünes Symbol steht für erfolgreich abgeschlossene Vorgänge oder zeigt an, dass Informationen vorhanden sind, jedoch kein Eingriff erforderlich ist. |
|  | Warning       | Ein gelbes Symbol steht für einen Fehler oder eine Warnung.  |
|  | Critical      | Ein rotes Symbol bedeutet, dass ein kritischer Fehler bzw. ein Sicherheitsproblem vorliegt oder dass ein Dienst nicht verfügbar ist.                     |
|  | Not monitored | Wenn kein Symbol angezeigt wird, wurden keine Daten zum Status erfasst.  |

Ansichten können sehr viele Objekte umfassen. Um schnell die gewünschten Objekte zu finden, können Sie die Schaltflächen „Bereich“, „Suchen“ und „Finden“ in der Symbolleiste von Operations Manager verwenden. Nähere Informationen finden Sie im Artikel [Verwalten der Datenüberwachung mit Bereichen, Suchen und Finden](http://go.microsoft.com/fwlink/?LinkId=91983) (<http://go.microsoft.com/fwlink/?LinkId=91983>).

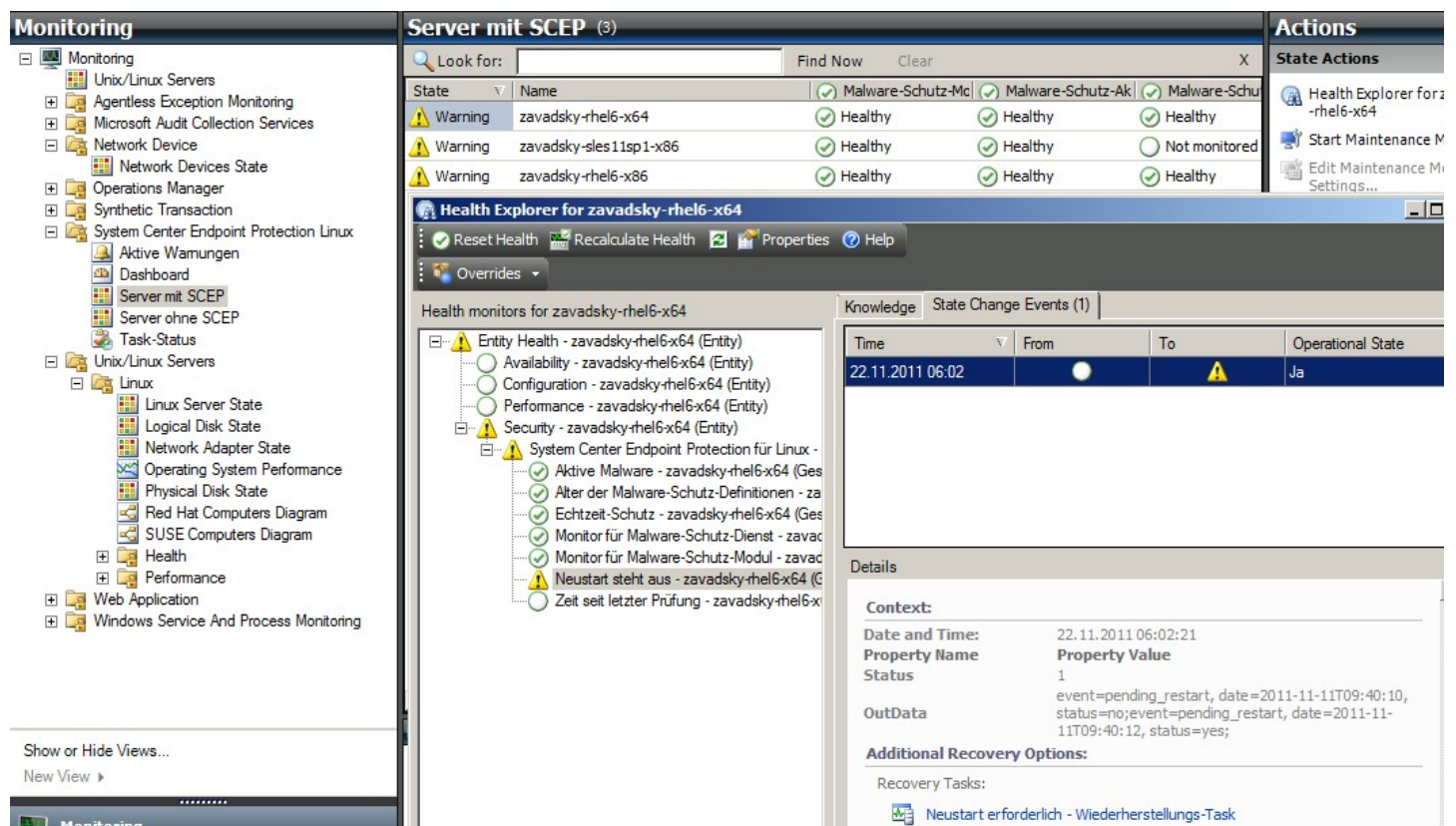
## Monitore

In Operations Manager 2007 wird der Zustand von überwachten Objekten mithilfe von Monitoren bewertet.

Für SCEP gibt es insgesamt 17 Monitore:

- 9 Einheitenmonitore - Diese Monitore der ersten Schicht überwachen bestimmte Zähler, Ereignisse, Skripte und Dienste.
- 2 Aggregatmonitore - Mit diesen Monitoren werden die Daten mehrerer Monitore zusammengefasst, daraus der Integritätsstatus ermittelt und ggf. Warnungen erzeugt.
- 6 Abhängigkeitsmonitore - Diese Monitore verweisen auf die Statusdaten anderer Monitore.

**Hinweis:** Weitere Informationen zu Monitoren finden Sie in der Hilfe zu Operations Manager 2007 R2 (F1-Taste in System Center 2012 Operations Manager drücken).



The screenshot shows the Microsoft Operations Manager console. The left pane displays the monitoring hierarchy, including 'System Center Endpoint Protection Linux' and 'Server mit SCEP'. The main pane shows a table of health monitors for the server 'zavadsky-rhel6-x64'. The table has columns for State, Name, and three specific monitors: Malware-Schutz-Mcl, Malware-Schutz-Ak, and Malware-Schutz-Modul. The 'Health Explorer' window is open, showing a warning event for 'Neustart steht aus' with a status of 'Ja'.

Nachfolgend werden Aufbau und Eigenschaften der SCEP-Integritätsmonitore aufgeführt.

### Aktive Malware

|             |  |
|-------------|--|
| Monitortyp  | Einheitenmonitor   |
| Objekt      | Geschützter Linux-Server                                 |
| Datenquelle | Überwacht Log-Textdatei: /var/log/scep/eventlog_scom.dat |
| Intervall   | Ereignisgesteuert  |

|                        |   |
|------------------------|---|
| Monitortyp             | Einheitenmonitor  |
| Warnung                | Ja. Keine automatische Auflösung  |
| Rücksetzverhalten      | Automatische Rückkehr in den Status „Fehlerfrei“ nach 8 Stunden. Die Warnung bleibt aktiv, damit Informationen zu der noch vorhandenen Malware erhalten bleiben.  |
| Anmerkungen            | Dieser Monitor wechselt in den Status „Kritisch“, wenn Malware gefunden, aber nicht entfernt wurde. Nach 8 Stunden kehrt er automatisch in den Status „Fehlerfrei“ zurück, da nicht hundertprozentig sicher festgestellt werden kann, ob die Malware entfernt wurde oder nicht. Der Administrator muss den Vorfall daher überprüfen und das Ticket manuell schließen. |
| Status                 | Fehlerfrei - Keine Malware<br>Kritisch - Aktive Malware   |
| Aktiviert              | Wahr  |
| Wiederherstellungstask | Nein  |

Mit diesem Monitor werden fehlgeschlagene Malware-Säuberungsvorgänge überwacht. Der Monitor meldet den Status „Kritisch“, wenn vom Client gemeldet wird, dass die Malware nicht entfernt werden konnte.

#### Alter der Malware-Schutz-Definitionen

|                        |   |
|------------------------|---|
| Monitortyp             | Einheitenmonitor  |
| Objekt                 | Geschützter Linux-Server  |
| Datenquelle            | Befehl zum Abruf der Überwachungsdaten: /opt/microsoft/scep/sbin/scep_daemon --status                   |
| Intervall              | Alle 8 Stunden  |
| Warnung                | Ja. Automatische Auflösung  |
| Status                 | Fehlerfrei - jünger als 3 Tage<br>Warnung - Alter zwischen 3 und 5 Tagen<br>Kritisch - älter als 5 Tage |
| Aktiviert              | Wahr  |
| Wiederherstellungstask | Ja, manuell (keine automatische Wiederherstellung)  |

Aktuelle Definitionen tragen dazu bei, dass der Computer vor neuen Malware-Bedrohungen geschützt bleibt.

#### Malware-Schutz-Modul

|                        |  |
|------------------------|--|
| Monitortyp             | Einheitenmonitor   |
| Objekt                 | Geschützter Linux-Server                                 |
| Datenquelle            | Überwacht Log-Textdatei: /var/log/scep/eventlog_scom.dat |
| Intervall              | Ereignisgesteuert  |
| Warnung                | Ja. Automatische Auflösung                               |
| Status                 | Fehlerfrei - Aktiviert<br>Deaktiviert - Warnung          |
| Aktiviert              | Wahr   |
| Wiederherstellungstask | Ja, manuell (keine automatische Wiederherstellung)       |

Der Malware-Schutz sollte ständig aktiviert sein.

**Hinweis:** Dieser Monitor überwacht den Virenschutz-Status (nicht zu verwechseln mit dem Echtzeit-Schutz). Wenn das Malware-Schutz-Modul deaktiviert ist, kann keine On-Demand-Prüfung gestartet werden.

#### Malware-Schutz-Dienst

|                        |  |
|------------------------|--|
| Monitortyp             | Einheitenmonitor   |
| Objekt                 | Geschützter Linux-Server   |
| Datenquelle            | Überwacht den Status des Prozesses scep_daemon                   |
| Intervall              | Alle 10 Minuten  |
| Warnung                | Ja. Automatische Auflösung                                       |
| Status                 | Fehlerfrei - Wird ausgeführt<br>Kritisch - Wird nicht ausgeführt |
| Aktiviert              | Wahr   |
| Wiederherstellungstask | Ja, manuell (keine automatische Wiederherstellung)               |

Der Monitor meldet den Status „Kritisch“, wenn der Malware-Schutz-Dienst (scep\_daemon) auf dem Clientrechner nicht ausgeführt wird bzw. nicht antwortet oder wenn das Malware-Schutz-Modul nicht korrekt funktioniert.

#### Zeit seit letzter Prüfung

|            |                  |
|------------|------------------|
| Monitortyp | Einheitenmonitor |
|------------|------------------|



|                        |   |
|------------------------|---|
| Objekt                 | Geschützter Linux-Server  |
| Datenquelle            | Befehl zum Abruf der Überwachungsdaten: /opt/microsoft/scep/sbin/scep_daemon --status |
| Intervall              | Alle 8 Stunden  |
| Warnung                | Nein  |
| Status                 | Fehlerfrei - jünger als 7 Tage<br>Warnung - älter als 7 Tage                          |
| Aktiviert              | Wahr  |
| Wiederherstellungstask | Ja, manuell (keine automatische Wiederherstellung)                                    |

Mit diesem Monitor wird der Zeitpunkt der letzten Computerprüfung überwacht, unabhängig vom Typ der Prüfung. Es wird empfohlen, jede Woche eine Prüfung durchzuführen.

#### Neustart steht aus

|                        |  |
|------------------------|--|
| Monitortyp             | Einheitenmonitor   |
| Objekt                 | Geschützter Linux-Server                                 |
| Datenquelle            | Überwacht Log-Textdatei: /var/log/scep/eventlog_scom.dat |
| Intervall              | Ereignisgesteuert  |
| Warnung                | Ja. Automatische Auflösung                               |
| Status                 | Nein - Fehlerfrei<br>Ja - Warnung                        |
| Aktiviert              | Wahr   |
| Wiederherstellungstask | Ja, manuell (keine automatische Wiederherstellung)       |

Mit diesem Monitor wird überwacht, ob ein Neustart des Systems erforderlich ist, um Änderungen an der Konfiguration abzuschließen, z. B. beim Aktivieren/Deaktivieren des Echtzeit-Schutzes. Für die manuelle Aktualisierung des Status führt der Monitor folgenden Aufruf aus: /opt/microsoft/scep/sbin/scep\_daemon --status.

#### Echtzeit-Schutz

|                        |   |
|------------------------|---|
| Monitortyp             | Einheitenmonitor  |
| Objekt                 | Geschützter Linux-Server  |
| Datenquelle            | Überwacht Log-Textdatei: /var/log/scep/eventlog_scom.dat<br>Für die manuelle Status-Aktualisierung kann der Monitor auch folgenden Aufruf ausführen: /opt/microsoft/scep/sbin/scep_daemon --status. |
| Intervall              | Ereignisgesteuert   |
| Warnung                | Ja. Automatische Auflösung  |
| Status                 | Aktiviert - Fehlerfrei<br>Deaktiviert - Warnung   |
| Aktiviert              | Wahr  |
| Wiederherstellungstask | Ja, manuell (keine automatische Wiederherstellung)  |

Mit diesem Monitor wird der Status des Echtzeit-Schutzes überwacht. Der Echtzeit-Schutz warnt Sie, wenn Viren, Spyware oder sonstige eventuell unerwünschte Anwendungen versuchen, sich auf Ihrem Computer zu installieren.

#### System Center Endpoint Protection für Linux

|                        |                          |
|------------------------|--------------------------|
| Monitortyp             | Aggregatmonitor          |
| Objekt                 | Geschützter Linux-Server |
| Bedingung              | Schlechtester Status     |
| Warnung                | Nein                     |
| Aktiviert              | Wahr                     |
| Wiederherstellungstask | Nein                     |

Dieser Monitor stellt den Integritätsstatus-Rollup (d. h. den schlechtesten Status) aller SCEP 7-Einheitenmonitore für geschützte Linux-Server dar. Wenn der Status nicht initialisiert ist, wurde entweder die Überwachung für dieses Objekt noch nicht begonnen, oder es sind keine Sicherheitsmonitore für dieses Objekt definiert.

#### Malware-Schutz-Modul

|                        |                      |
|------------------------|----------------------|
| Monitortyp             | Abhängigkeitsmonitor |
| Objekt                 | Malware-Schutz-Modul |
| Warnung                | Nein                 |
| Aktiviert              | Wahr                 |
| Wiederherstellungstask | Nein                 |

Mit diesem Monitor wird der Status des Einheitenmonitors „Geschützter Linux-Server/Malware-Schutz-Modul“ in der Liste der überwachten Computer angezeigt.

#### Malware-Schutz-Dienst

|                        |                      |
|------------------------|----------------------|
| Monitortyp             | Abhängigkeitsmonitor |
| Objekt                 | Malware-Schutz-Modul |
| Warnung                | Nein                 |
| Aktiviert              | Wahr                 |
| Wiederherstellungstask | Nein                 |

Mit diesem Monitor wird der Status des Einheitenmonitors „Geschützter Linux-Server/Malware-Schutz-Dienst“ in der Liste der überwachten Computer angezeigt.

#### Malware-Schutz-Definitionen

|                        |                             |
|------------------------|-----------------------------|
| Monitortyp             | Abhängigkeitsmonitor        |
| Objekt                 | Malware-Schutz-Definitionen |
| Warnung                | Nein                        |
| Aktiviert              | Wahr                        |
| Wiederherstellungstask | Nein                        |

Mit diesem Monitor wird der Status des Einheitenmonitors „Geschützter Linux-Server/Alter der Malware-Schutz-Definitionen“ in der Liste der überwachten Computer angezeigt.

#### Aktive Malware

|                        |                          |
|------------------------|--------------------------|
| Monitortyp             | Abhängigkeitsmonitor     |
| Objekt                 | Malware-Schutz-Aktivität |
| Warnung                | Nein                     |
| Aktiviert              | Wahr                     |
| Wiederherstellungstask | Nein                     |

Mit diesem Monitor wird der Status des Einheitenmonitors „Geschützter Linux-Server/Aktive Malware“ im Integritäts-Explorer für Malware-Schutz-Aktivität angezeigt.

#### Ping an Geräte

|                        |  |
|------------------------|--|
| Monitortyp             | Einheitenmonitor                                       |
| Objekt                 | Malware-Schutz-Aktivität                               |
| Intervall              | Alle 60 Minuten  |
| Warnung                | Nein   |
| Status                 | Erreichbar - Fehlerfrei<br>Nicht erreichbar - Kritisch |
| Aktiviert              | Falsch   |
| Wiederherstellungstask | Nein   |

Bei nicht antwortendem Server wird der Status in „Kritisch“ geändert.

#### Malware-Aktivität

|                        |  |
|------------------------|--|
| Monitortyp             | Einheitenmonitor   |
| Objekt                 | Malware-Schutz-Aktivität   |
| Datenquelle            | Überwacht Log-Textdatei: /var/log/scep/eventlog_scom.dat           |
| Intervall              | Ereignisgesteuert  |
| Warnung                | Nein   |
| Status                 | Keine Malware - Fehlerfrei<br>Malware-Aktivität erkannt - Kritisch |
| Aktiviert              | Wahr   |
| Wiederherstellungstask | Nein   |

Mit diesem Monitor wird 5 Minuten nach der Erkennung von entfernter oder nicht entfernter Malware der Status „Kritisch“ ausgelöst. Der kritische Status bleibt 60 Minuten lang aktiv. Bei jeder neuen Erkennung wird erneut der Status „Kritisch“ ausgelöst und damit die abgelaufene Warnzeit zurückgesetzt. Der Monitor kehrt also erst zum Status „Fehlerfrei“ zurück, wenn innerhalb von 60 Minuten keine Malware erkannt wurde.

### Malware-Ausbruch auf Server

|                        |                          |
|------------------------|--------------------------|
| Monitortyp             | Aggregatmonitor          |
| Objekt                 | Malware-Schutz-Aktivität |
| Bedingung              | Bester Status            |
| Warnung                | Nein                     |
| Aktiviert              | Wahr                     |
| Wiederherstellungstask | Nein                     |

Zusammenfassung der Monitore: Malware-Aktivität, Ping an Geräte

Dieser Monitor ändert seinen Status in „Kritisch“, wenn der Server nicht innerhalb von 60 Minuten nach der Erkennung von entfernter bzw. nicht entfernter Malware antwortet. Diese Statusänderung kann auch ausgelöst werden, wenn der Server längere Zeit nicht geantwortet hat und kurz nach der Verbindungswiederherstellung Malware erkannt wird.

### Malware-Ausbruch

|                        |                               |
|------------------------|-------------------------------|
| Monitortyp             | Abhängigkeitsmonitor          |
| Objekt                 | Watcher für geschützte Server |
| Bedingung              | Schlechtester Status von 95 % |
| Warnung                | Nein                          |
| Aktiviert              | Wahr                          |
| Wiederherstellungstask | Nein                          |

Mit diesem Monitor wird der Status des Monitors „Malware-Schutz-Aktivität/Malware-Ausbruch auf Server“ angezeigt.

Wenn in den letzten 60 Minuten auf mehr als 5 % aller geschützten und ungeschützten Linux-Computer Malware erkannt wurde, wechselt der Monitor in den Status „Kritisch“.

### SCEP Linux-Computerrollen – Integritätsstatus-Rollup

|                        |                      |
|------------------------|----------------------|
| Monitortyp             | Abhängigkeitsmonitor |
| Objekt                 | Linux-Computer       |
| Warnung                | Nein                 |
| Aktiviert              | Wahr                 |
| Wiederherstellungstask | Nein                 |

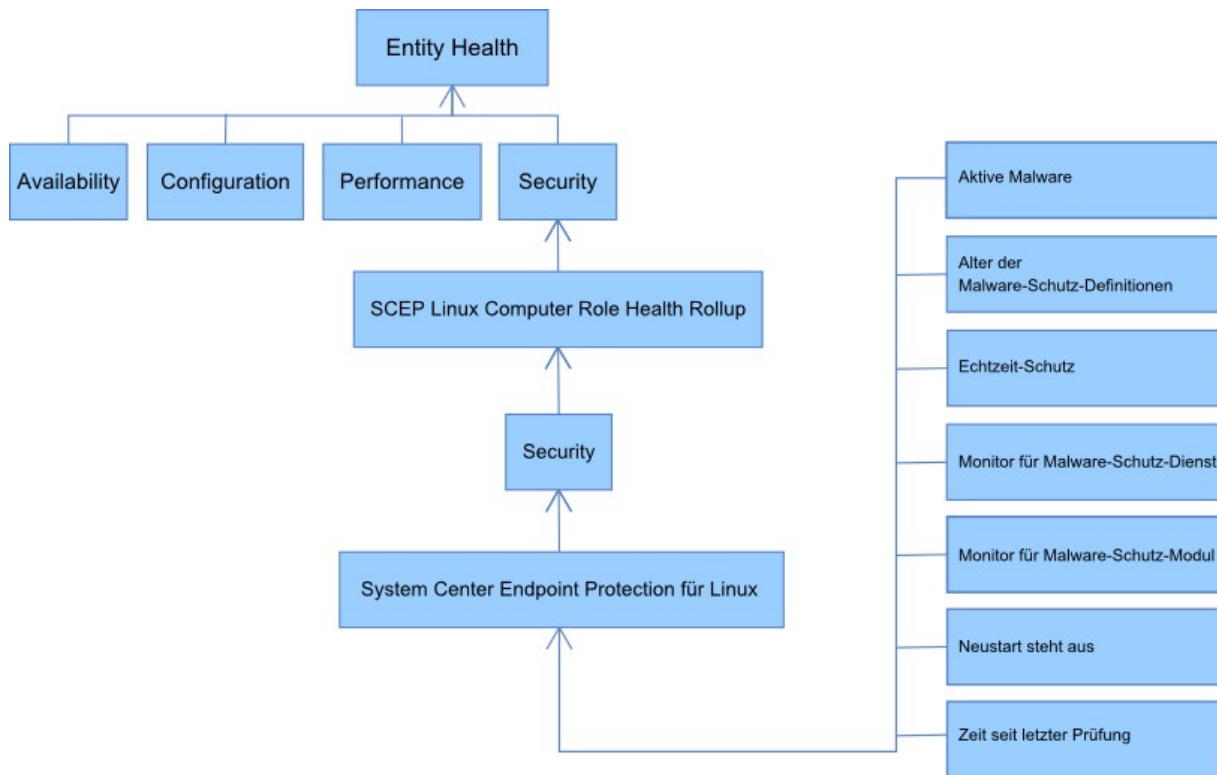
Überträgt den Status von „Geschützter Linux-Computer“ auf den übergeordneten Linux-Computer-/Sicherheitsmonitor.

### Integritätsstatus-Rollup

Dieses Management Pack ermöglicht eine erweiterte Überwachung von Linux-Betriebssystemen auf der Grundlage eines Mehrschichtenmodells. In diesem Modell bestimmt der Integritätszustand der niedrigeren Schicht den der jeweils übergeordneten Schicht. An der Spitze steht dabei die Umgebung „Entitätszustand“; die Monitore bilden dagegen die unterste Sicherheitsschicht. Ändert sich der Zustand einer Schicht, wird diese Änderung an die darüberliegende Schicht weitergegeben. Dieser Vorgang wird als „Rollup des Integritätsstatus“ bezeichnet.

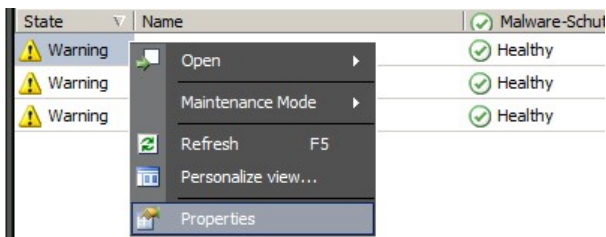
Beispiel: Wenn der Echtzeit-Schutz eine Warnung zurückgibt, während alle anderen Komponenten keine Probleme zeigen, erhält über die Baumstruktur auch die oberste Schicht („Entitätszustand“) den Warnstatus.

Das unten stehende Diagramm zeigt die Funktionsweise des Integritätsstatus-Rollups in diesem Management Pack.



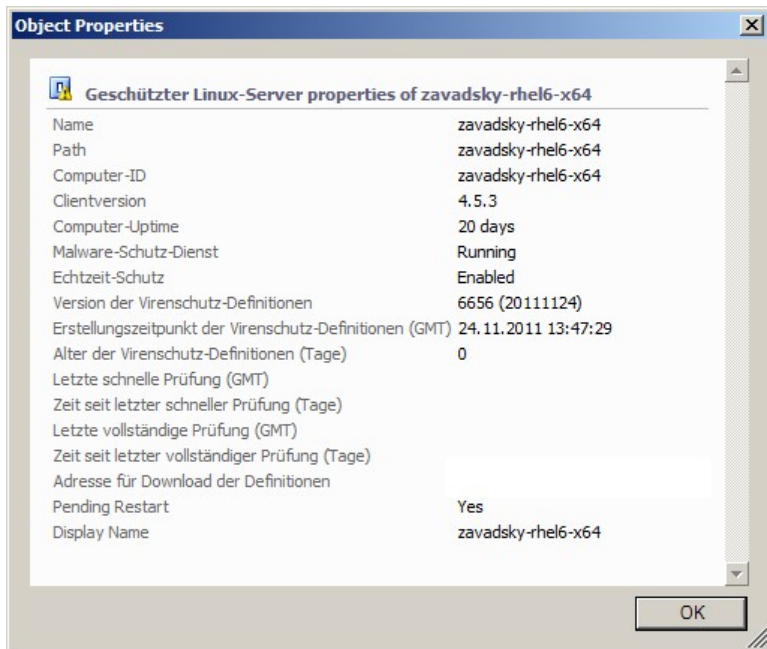
## Objekteigenschaften

Um die Eigenschaften eines Objekts anzuzeigen, klicken Sie mit der rechten Maustaste auf das Objekt und wählen Sie **Properties** aus.



Das Objekt „Geschützter Linux-Server“ hat die folgenden Eigenschaften:

- **Computer-ID** - Serverkennung, Domainname
- **Anzeigename** - Servername, Domainname
- **Clientversion** - installierte SCEP-Version
- **Computer-Uptime** - Serverbetriebszeit (Zeit seit dem letzten Geräteausfall). Diese Angabe ist nicht unbedingt essentiell für die korrekte Ausführung des Management Packs; ein Fehlen deutet jedoch eventuell auf einen Fehler im Management Pack hin.
- **Malware-Schutz-Dienst** - Status des Malware-Schutzes (wird ausgeführt/nicht ausgeführt)
- **Echtzeit-Schutz** - Status des Echtzeit-Schutzes; ein Fehlen deutet auf Probleme mit SCEP hin
- **Virenschutz-Definitionen...** - Statusdaten zur Signaturdatenbank (Version, Erstellungsdatum, Alter); ein Fehlen deutet auf Probleme mit SCEP hin
- **Letzte schnelle/vollständige Prüfung...** - Daten zur zuletzt ausgeführten Computerprüfung. Wenn bisher noch keine Prüfung der betreffenden Art (schnell bzw. vollständig) stattgefunden hat, werden keine Daten angezeigt.
- **Adresse für Download der Definitionen** - Adresse/Name des Update-Servers. Hier wird erst nach dem ersten erfolgreichen Update etwas angezeigt.
- **Neustart steht aus** - Zeigt an, ob ein Neustart erforderlich ist, um Neuinstallationen oder Änderungen an der SCEP-Konfiguration abzuschließen.



## Warnungen

Mit einer Warnung wird angezeigt, dass in einem überwachten Objekt eine vordefinierte Situation mit einem bestimmten Schweregrad eingetreten ist. Warnungen werden durch Regeln definiert. In der Operations Manager-Konsole sind unter **Monitoring > System Center Endpoint Protection Linux > Aktive Warnungen** die objektspezifischen Warnungen angezeigt, für die der Konsolenbenutzer Leserechte hat.

**Hinweis:** Wenn für denselben Server mehrmals Warnungen desselben Typs (z. B. „Aktive Malware“) erzeugt werden, wird nur die erste angezeigt; die übrigen werden ignoriert.

| Warnung   | Intervall         | Priorität               | Schweregrad  | Beschreibung   |
|---|-------------------|-------------------------|--|--|
| Wiederholte Malware-Infektion   | Ereignisgesteuert | Hoch                    | Kritisch   | Warnung bei wiederholter Erkennung von Malware innerhalb eines festgelegten Zeitraums (standardmäßig dreimal in 30 Minuten). Enthält Daten zum Server und allgemeine Informationen über die Malware.   |
| Malware entfernt  | Ereignisgesteuert | Niedrig<br>Mittel       | Information - Malware entfernt<br>Warnung - Eingreifen des Benutzers erforderlich, z. B. Server-Neustart | Warnung zu erfolgreich entfernter Malware. Enthält alle verfügbaren Informationen über die jeweilige Malware. Jede erkannte Malware löst ein separates Ereignis aus. Je nachdem, wie der Säuberungsprozess verlaufen ist, weist SCEP Linux dem Ereignis eine Priorität und einen Schweregrad zu. Dabei gilt:<br>Entfernt = Niedrig + Information<br>Entfernt, aber Aktion erforderlich (z. B. Neustart) = Mittel + Warnung |
| Aktive Malware (von Monitor)  | Ereignisgesteuert | Hoch                    | Kritisch   | Warnung, dass die Malware nicht entfernt wurde. Enthält alle verfügbaren Informationen über die jeweilige Malware.   |
| Aktive Malware (von Regel)  | Ereignisgesteuert | Hoch/mittel/<br>niedrig | Kritisch/mittel/niedrig je nach Art der Malware  | Siehe oben. Verwendet für Connectors zu anderen Überwachungs-/Ticketing-Systemen.<br><b>Hinweis:</b> Diese Regel (Warnung) ist standardmäßig deaktiviert.  |
| Malware-Schutz-Dienst von System Center Endpoint Protection ausgefallen | 300 Sekunden      | Mittel                  | Kritisch   | Warnung, dass der Malware-Schutz-Dienst von SCEP (scep_daemon) nicht verfügbar ist. Enthält den Namen des betroffenen Servers und die Version von SCEP.  |

|                             |                   |        |  |  |
|-----------------------------|-------------------|--------|--|--|
| Malware-Schutz deaktiviert  | Ereignisgesteuert | Mittel | Warnung  | Warnung, dass der Malware-Schutz deaktiviert ist. Enthält den Namen des betroffenen Servers.   |
| Echtzeit-Schutz deaktiviert | Ereignisgesteuert | Mittel | Warnung  | Warnung, dass der Echtzeit-Schutz deaktiviert ist. Enthält den Namen des betroffenen Servers.  |
| Definitionen veraltet       | Alle 8 Stunden    | Mittel | Warnung (Alter <= 5 Tage<br>UND Alter > 3 Tage)<br>Kritisch (Alter > 5 Tage) | Warnung, wenn die Signaturdatenbank seit mehr als 3 Tagen nicht aktualisiert wurde. Enthält den Namen des betroffenen Servers und die Version der Signaturdatenbank.   |
| Malware-Ausbruch            | Ereignisgesteuert | Hoch   | Kritisch   | Von Forefront Endpoint Protection wurde aktive Malware auf mehr als 5 % Ihrer Computer erkannt.<br>Möglicherweise breitet sich derzeit Malware auf Ihren Computern aus. Alle Server sollten auf die neuesten Definitionen aktualisiert werden. Falls Sie die Anzahl der aktiven Bedrohungen ändern möchten, bei der diese Warnung ausgelöst wird, setzen Sie den Parameter des Monitors „Malware-Ausbruch“ außer Kraft (siehe Kapitel <a href="#">Außerkräftsetzungen</a> ). |

## Tasks

Im Management Pack für SCEP stehen 13 verschiedene Tasks zur Verfügung. Diese Tasks werden sofort ausgeführt. Ihre Ausgabe wird direkt nach der Ausführung angezeigt oder kann später über das Fenster „Task-Status“ eingesehen werden. Als Zeitbeschränkung für die Ausführung sind 180 Sekunden festgelegt. Eine Außerkräftsetzung ist nicht möglich. Bei allen Tasks handelt es sich um Bash-Befehle, die über SSH ausgeführt werden.

Die Tasks können im rechten Teilfenster der Betriebskonsole unter **Monitoring > System Center Endpoint Protection Linux > Server mit SCEP** aufgerufen werden.

### Geschützter Linux-Server... ▲

-  Computer neu starten
-  Echtzeit-Schutz aktivieren
-  Echtzeit-Schutz deaktivieren
-  Endpunkteinstellungen abrufen
-  Prüfung abbrechen
-  SCEP-Definitionen aktualisieren
-  SCEP-Dienst beenden
-  SCEP-Dienst neu starten
-  SCEP-Dienst starten
-  Schnelle Prüfung
-  Virenschutz aktivieren
-  Virenschutz deaktivieren
-  Vollständige Prüfung

- **Virenschutz deaktivieren** - Deaktiviert alle Virenschutz-Komponenten einschließlich der On-Demand-Prüfung.
- **Virenschutz aktivieren** - Aktiviert alle Virenschutz-Komponenten.
- **Echtzeit-Schutz deaktivieren** - Deaktiviert den Echtzeit-Schutz.
- **Echtzeit-Schutz aktivieren** - Aktiviert den Echtzeit-Schutz.
- **Vollständige Prüfung** - Aktualisiert die Signaturdatenbank und startet eine vollständige Prüfung des Computers.
- **Schnelle Prüfung** - Aktualisiert die Signaturdatenbank und startet eine schnelle Prüfung des Computers.
- **Prüfung abbrechen** - Beendet alle laufenden Prüfungen.
- **Servereinstellungen abrufen** - Zeigt den aktuellen SCEP-Produktstatus an. Die Liste der angezeigten Parameter ist identisch mit den Eigenschaften der Entität „Geschützter Linux-Server“. Die angezeigten Daten werden nicht in „Geschützter Linux-Server“ übernommen.
- **Malware-Schutz-Dienst neu starten** - Startet den Malware-Schutz-Dienst von SCEP (scep\_daemon) neu.
- **Malware-Schutz-Dienst beenden** - Beendet den Malware-Schutz-Dienst von SCEP (scep\_daemon).
- **Malware-Schutz-Dienst starten** - Startet den Malware-Schutz-Dienst von SCEP (scep\_daemon).
- **Malware-Schutz-Definitionen aktualisieren** - Startet ein Update der Signaturdatenbank.
- **Computer neu starten** - Startet den Linux-Computer neu.

## Konfiguration des Management Packs für SCEP

### Best Practice: Management Pack für benutzerdefinierte Anpassungen erstellen

Standardmäßig speichert Operations Manager Anpassungen wie z. B. Außerkraftsetzungen im Standard-Management Pack. Es hat sich allerdings bewährt, stattdessen für jedes versiegelte Management Pack, das Sie anpassen möchten, ein neues Management Pack zu erstellen.

Bei der Erstellung eines Management Packs, in dem angepasste Einstellungen eines versiegelten Management Packs gespeichert werden sollen, ist es hilfreich, den Namen des ursprünglichen Management Packs teilweise zu übernehmen, z. B. nach dem Muster „SCEP 2012 Anpassungen“.

Indem Sie für Anpassungen an einem versiegelten Management Pack ein neues Management Pack erstellen, erleichtern Sie sich den Export dieser Anpassungen aus einer Test-Umgebung in eine Produktionsumgebung. Darüber hinaus erleichtert dieses Vorgehen auch das Löschen eines Management Packs, da davor zunächst alle Abhängigkeiten gelöscht werden müssen. Wenn nun die Anpassungen für alle Management Packs im Standard-Management Pack gespeichert sind, Sie aber nur ein einziges Pack löschen möchten, müssen Sie zuerst das Standard-Management Pack löschen, womit auch die Anpassungen für die anderen Packs verloren gehen.

### Sicherheitskonfiguration

Auf dem Computer muss der SSHD-Dienst ausgeführt werden, und der SSH-Port (standardmäßig 22) muss geöffnet sein. Über diesen Port baut System Center 2012 Operations Manager unter Verwendung der im ausführenden Konto (Run As Account, Typ **Basic Authentication**) unter **Administration > Run As Configuration** in der Operations Manager-Betriebskonsole hinterlegten Anmeldedaten die Verbindung zu den Linux-Remotecomputern auf.

| Name des ausführenden Profils | Anmerkungen  |
|-------------------------------|--|
| Unix Privileged Account       | Dient zur Remoteüberwachung des Unix-Servers sowie zum Neustarten von Prozessen, für die erhöhte Rechte erforderlich sind. |

Das Unix-Aktionskonto (Unix Action Account) wird von diesem Management Pack nicht verwendet.

**Warnung:** Die Überwachung von Computern über das root-Konto stellt ein Sicherheitsrisiko dar, wenn beispielsweise das Passwort dieses Kontos in falsche Hände gerät.

Wenn Sie das root-Konto nicht zur Überwachung und Verwaltung nutzen möchten, können Sie stattdessen auch ein Standardbenutzerkonto verwenden, das dann jedoch über die nötigen Rechte zum Ausführen von *sudo*-Befehlen verfügen muss. Hierzu muss auf jedem Rechner, der mit SCEP Linux überwacht werden soll, die folgende Konfiguration in der Datei */etc/sudoers* vorhanden sein. Die gezeigte Konfiguration ist ein Beispiel für den Benutzernamen 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
#-----

```

## Optimierung der Leistungsschwellenwert-Regeln

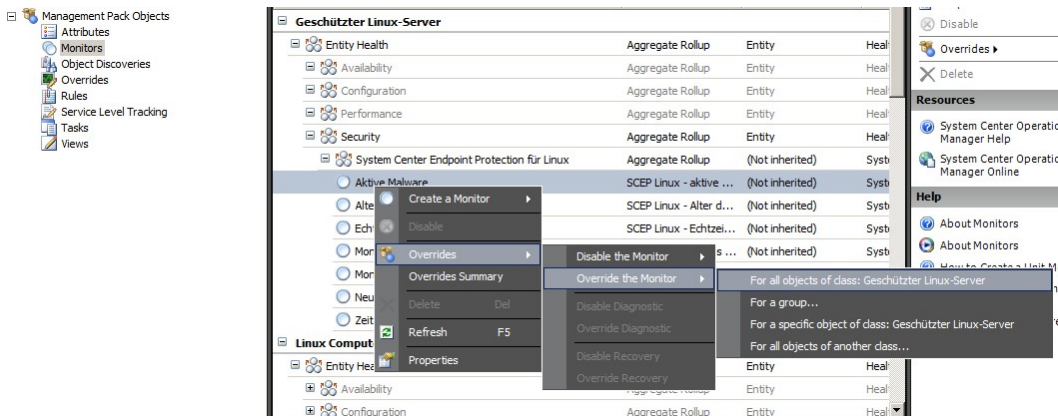
In der folgenden Tabelle sind Leistungsschwellenwert-Regeln aufgeführt, deren Standardschwellenwerte eventuell für Ihre Umgebung optimiert werden müssen. Überprüfen Sie diese Regeln darauf, ob die Standardschwellenwerte für Ihre Umgebung angemessen sind. Wenn nicht, können Sie sie mithilfe einer Außerkräftsetzung anpassen.

| Regelname                               | Parameter der Außerkräftsetzung                   | Standardschwellenwert | Einschränkungen   |
|---|---|-----------------------|---|
| Regel für wiederholte Malware-Infektion | Grenzwert für Anzahl der wiederholten Infektionen | 3 Fälle               | Bei einem Wert unter 2 wird die Regel sinnlos.  |
| Regel für wiederholte Malware-Infektion | Zeitfenster für wiederholte Infektionen           | 30 Minuten            | Der Wert sollte mindestens so hoch eingestellt werden wie die Dauer einer On-Demand-Prüfung, da sonst aufgrund von Überschneidungen eventuell keine Warnung erzeugt wird. |
| Regel für Warnung bei aktiver Malware   | Aktiviert   | Falsch                | Diese Warnung können Sie aktivieren, wenn Sie Connectors zu anderen Überwachungs- und Ticketing-Systemen verwenden.   |

## Außerkräftsetzungen

In System Center 2012 Operations Manager können die Einstellungen zu einem Überwachungsobjekt mithilfe von Außerkräftsetzungen angepasst werden. Diese betreffen Monitore, Regeln, Objektermittlungen und Attribute importierter Management Packs.

Zum Außerkräftsetzen einer Monitor-Einstellung klicken Sie in der Betriebskonsole auf **Authoring** und erweitern Sie **Management Pack Objects > Monitors**. Suchen Sie den jeweiligen Objekttyp im Bereich „Monitors“ und erweitern Sie ihn vollständig. Klicken Sie dann auf einen Monitor und auf **Overrides**.



Im Fenster „Außerkräftsetzungen“ können Sie Außerkräftsetzungen für folgende Parameter erstellen bzw. ändern:

- **Monitor für aktive Malware - Status-Rückkehrzeit** (nur für den Monitor „Aktive Malware“)
- **Alter der Malware-Schutz-Definitionen** (nur für den Monitor „Alter der Malware-Schutz-Definitionen“)
- **Erkennungsintervall** (nur für den Monitor „Zeit seit letzter Prüfung“)
- **Warnung bei Status**
- **Warnungspriorität**
- **Warnungsschweregrad**
- **Warnung automatische Auflösung**
- **Aktiviert** - Legt fest, ob der ausgewählte Monitor aktiviert oder deaktiviert ist.
- **Generiert Warnungen**
- **Pfad für SCEP-Logdateien**

Wenn eine Standard-Außerkräftsetzung in der ausgewählten Umgebung nicht passt, können Sie die Schwellenwerte anhand einer Außerkräftsetzung anpassen:

| Parameter der Außerkräftsetzung                                   | Monitorname                           | Standardwert                    | Hinweise zur Feineinstellung   |
|---|---------------------------------------|---------------------------------|--|
| Ping-Intervall  | Ping an Geräte                        | 3.600 Sekunden                  | Zeitabstand zur Prüfung der Verfügbarkeit des geschützten Linux-Servers. Je kürzer der Zeitraum, desto eher wird der Status „Fehler“ im Monitor „Malware-Ausbruch auf Server“ ausgelöst, wenn das Gerät angegriffen wird und nicht mehr antwortet. Dementsprechend erhöht sich auch die Netzwerklast sowie die des überwachten Computers und des System Center 2012 Operations Manager-Servers.  |
| Zeitfenster für Malware-Ausbruch                                  | Malware-Aktivität                     | 3.600 Sekunden                  | Zeitraum, nach dem der Monitor nach Malware-Aktivitäten in den Status „Fehlerfrei“ zurückkehrt. Der Zeitfenster-Wert muss größer sein als der Zeitraum „Ping an Geräte/Ping-Intervall“, damit die Kombination korrekt funktioniert.<br>Falls während der unter „Zeitfenster für Malware-Ausbruch“ festgelegten Zeitspanne für einen größeren Anteil (%) an Computern Malware-Aktivitäten registriert werden, als für einen „Malware-Ausbruch“ festgelegt sind (siehe „Malware-Ausbruch“), wird eine „Malware-Ausbruch“-Warnung generiert.<br><br>Hinweis: „Malware-Ausbruch auf Server“ unterscheidet sich dahingehend, dass dieser Monitor keine Warnung generiert. |
| Monitor für aktive Malware - Status-Rückkehrzeit                  | Aktive Malware                        | 28.800 Sekunden                 | Zeitraum seit Malware-Erkennung, nach dessen Ablauf die Malware als entfernt gilt.   |
| Pfad für SCEP-Logdateien  | Aktive Malware                        | /var/log/scep/eventlog_scom.log | Pfad zu der Datei, in der System Center 2012 Operations Manager-Ereignisse protokolliert werden. Ändern Sie diesen Parameter nur bei Problemen.  |
| Alter der Malware-Schutz-Definitionen für Status „Kritisch“       | Alter der Malware-Schutz-Definitionen | 5 Tage                          | Nach Ablauf des Zeitraums wird eine Fehlerwarnung über eine veraltete SCEP-Version generiert.  |
| Alter der Malware-Schutz-Definitionen für Status „Keine Probleme“ | Alter der Malware-Schutz-Definitionen | 3 Tage                          | Höchstalter der Malware-Schutz-Definitionen, bis zu dem sie als aktuell gelten. Dieser Wert sollte immer unter dem Alter der Malware-Schutz-Definitionen für den Status „Kritisch“ liegen.   |
| Intervall   | Alter der Malware-Schutz-Definitionen | 28.800 Sekunden                 | Zeitabstand für die Prüfung des Alters der Malware-Schutz-Definitionen.  |
| Intervall   | Malware-Schutz-Dienst                 | 300 Sekunden                    | Zeitabstand für die Verfügbarkeitsprüfung für den Malware-Schutz-Dienst.   |
| Prozessname   | Malware-Schutz-Dienst                 | scep_daemon                     | Name des Malware-Schutz-Dienstes. Ändern Sie diesen Wert nicht, wenn der Monitor in Betrieb ist.   |
| Erkennungsintervall   | Zeit seit letzter Prüfung             | 28.800 Sekunden                 | Zeitabstand, in dem die Zeit seit der letzten Prüfung abgefragt wird.  |
| Maximale Zeit seit letzter Prüfung                                | Zeit seit letzter Prüfung             | 7 Tage                          | Muss passend zu den SCEP-Produkteinstellungen eingestellt werden. Wenn alle 7 Tage geprüft wird, müssen hier 7 Tage festgelegt sein.   |
| Pfad für Logdateien   | Neustart steht aus                    | /var/log/scep/eventlog_scom.log | Pfad zu der Datei, in der System Center 2012 Operations Manager-Ereignisse protokolliert werden. Ändern Sie diesen Parameter nur bei Problemen.  |
| Pfad für SCEP-Logdateien  | Echtzeit-Schutz                       | /var/log/scep/eventlog_scom.log | Pfad zu der Datei, in der System Center 2012 Operations Manager-Ereignisse protokolliert werden. Ändern Sie diesen Parameter nur bei Problemen.  |
| Prozent   | Malware-Ausbruch                      | 95%                             | Prozentanteil geschützter und ungeschützter Linux-Server, deren Status zu „Fehlerfrei“ zurückkehren muss, bevor die gesamte überwachte Gruppe diesen Status erhält. Wenn bei mehr als 5 % aller Server Malware erkannt wird, wird eine „Malware-Ausbruch“-Warnung generiert.   |

| Override                            | Parameter Name               | Parameter Type | Default Value   | Override Value    | Effective Value   | Change Status |
|-------------------------------------|------------------------------|----------------|-----------------|-------------------|-------------------|---------------|
| <input type="checkbox"/>            | Alert On State               | Enumeration    | The monitor ... | The monitor is... | The monitor is... | [No change]   |
| <input type="checkbox"/>            | Alert Priority               | Enumeration    | High            | High              | High              | [No change]   |
| <input type="checkbox"/>            | Alert severity               | Enumeration    | Match monit...  | Match monito...   | Match monitor...  | [No change]   |
| <input type="checkbox"/>            | Auto-Resolve Alert           | Boolean        | False           | False             | False             | [No change]   |
| <input type="checkbox"/>            | Enabled                      | Boolean        | True            | True              | True              | [No change]   |
| <input type="checkbox"/>            | Generates Alert              | Boolean        | True            | True              | True              | [No change]   |
| <input type="checkbox"/>            | Monitor für aktive Malwar... | Integer        | 28800           | 28800             | 28800             | [No change]   |
| <input checked="" type="checkbox"/> | Pfad für SCEP-Logdateien     | String         | /var/log/sc...  | entlog_scom.dat   | /var/log/scep...  | [Added]       |

**Hinweis:** Weitere Informationen zu Außerkräftsetzungen finden Sie im Artikel [Überwachen mithilfe von Außerkräftsetzungen](http://go.microsoft.com/fwlink/?LinkID=117777) (<http://go.microsoft.com/fwlink/?LinkID=117777>).

## Links

Unter den folgenden Links finden Sie Informationen zu Standardaufgaben bei der Arbeit mit diesem Management Pack:

- [Verwalten des Management Pack-Lebenszyklus](http://go.microsoft.com/fwlink/?LinkID=211463) (<http://go.microsoft.com/fwlink/?LinkID=211463>)
- [Importieren eines Management Packs in Operations Manager 2007](http://go.microsoft.com/fwlink/?LinkID=142351) (<http://go.microsoft.com/fwlink/?LinkID=142351>)
- [Überwachen mithilfe von Außerkräftsetzungen](http://go.microsoft.com/fwlink/?LinkID=117777) (<http://go.microsoft.com/fwlink/?LinkID=117777>)
- [Erstellen eines ausführenden Kontos in Operations Manager 2007](http://go.microsoft.com/fwlink/?LinkID=165410) (<http://go.microsoft.com/fwlink/?LinkID=165410>)
- [Konfigurieren eines plattformübergreifenden ausführenden Kontos](http://go.microsoft.com/fwlink/?LinkID=160348) (<http://go.microsoft.com/fwlink/?LinkID=160348>)
- [Ändern eines ausführenden Profils](http://go.microsoft.com/fwlink/?LinkID=165412) (<http://go.microsoft.com/fwlink/?LinkID=165412>)
- [Exportieren von Management Pack-Anpassungen](http://go.microsoft.com/fwlink/?LinkID=209940) (<http://go.microsoft.com/fwlink/?LinkID=209940>)
- [Entfernen eines Management Packs](http://go.microsoft.com/fwlink/?LinkID=209941) (<http://go.microsoft.com/fwlink/?LinkID=209941>)
- [Verwalten der Datenüberwachung mit Bereichen, Suchen und Finden](http://go.microsoft.com/fwlink/?LinkID=91983) (<http://go.microsoft.com/fwlink/?LinkID=91983>)
- [Linux-Überwachung mit SCOM 2007 R2 \(englisch\)](http://blogs.technet.com/b/birojitrn/archive/2010/01/20/monitoring-linux-using-scom-2007-r2.aspx) (<http://blogs.technet.com/b/birojitrn/archive/2010/01/20/monitoring-linux-using-scom-2007-r2.aspx>)
- [Manuelles Installieren plattformübergreifender Agents](http://technet.microsoft.com/de-de/library/dd789016.aspx) (<http://technet.microsoft.com/de-de/library/dd789016.aspx>)
- [In System Center Operations Manager 2012 mithilfe von sudo erhöhte Rechte für die Überwachung von Unix- und Linux-Rechnern konfigurieren \(englisch\)](http://social.technet.microsoft.com/wiki/contents/articles/7375.configuring-sudo-elevation-for-unix-and-linux-monitoring-with-system-center-2012-operations-manager.aspx) (<http://social.technet.microsoft.com/wiki/contents/articles/7375.configuring-sudo-elevation-for-unix-and-linux-monitoring-with-system-center-2012-operations-manager.aspx>)

Weitere Informationen zu Operations Manager und Überwachungspaketen finden Sie im [Forum der System Center Operations Manager-Community](http://go.microsoft.com/fwlink/?LinkID=179635) (<http://go.microsoft.com/fwlink/?LinkID=179635>).

Ebenfalls hilfreich ist das Blog [System Center Operations Manager Unleashed](http://opsmgrunleashed.wordpress.com/) (<http://opsmgrunleashed.wordpress.com/>); es enthält Beiträge mit Beispielen für bestimmte Überwachungspakete.

Auch in diesen englischsprachigen Blogs finden Sie Informationen zu Operations Manager:

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

Hilfe bei der Fehlerbehebung finden Sie in diesen Forenthemen:

- [Microsoft.Unix.Library fehlt](http://social.technet.microsoft.com/Forums/en-US/operationsmanagemgmtpacks/thread/8469d0ff-54d6-4cb4-9909-49ab62126b74/)  
(<http://social.technet.microsoft.com/Forums/en-US/operationsmanagemgmtpacks/thread/8469d0ff-54d6-4cb4-9909-49ab62126b74/>)