



Microsoft®

# System Center Operations Manager

## System Center 監視組件 適用於Endpoint Protection Linux

---

Microsoft Corporation

發行日期：10/26/2015

對於本文件有任何意見或建議，請寄送至 [mpgfeed@microsoft.com](mailto:mpgfeed@microsoft.com)。請在您的意見中註明管理組件指南名稱。

Operations Manager 團隊歡迎您在[管理組件目錄](http://go.microsoft.com/fwlink/?LinkID=82105) (http://go.microsoft.com/fwlink/?LinkID=82105) 中的管理組件頁面提供評論，以提供監視組件的意見。

## 內容

<b>SCEP 管理組件指南</b>	<b>3</b>
指南歷程記錄	3
4.5.10.1 版本的變更	3
支援的配置	3
先決條件	3
此管理組件中的檔案	4
快速入門	4
管理組件目的	6
視圖	7
監視器	7
如何彙總狀態	12
物件內容	13
警告	14
工作	15
<b>配置 SCEP 的管理組件</b>	<b>15</b>
最佳實務：建立自訂的管理組件	15
安全性配置	16
微調效能閾值規則	16
覆寫	16
<b>連結</b>	<b>18</b>

# SCEP 管理組件指南

這個管理組件可讓您從網路環境的 System Center 2012 Operations Manager 這個集中位置管理 System Center Endpoint Protection (SCEP)，包括工作站和伺服器。利用 Operations Manager 工作管理系統，您可以管理遠端電腦上的 SCEP、檢視警告和健全狀況狀態，並快速回應新的問題與威脅。

System Center 2012 Operations Manager 本身不針對惡意程式碼提供其他任何形式的防護。System Center 2012 Operations Manager 依據安裝 Linux 作業系統的電腦上是否有 SCEP 解決方案而定。

本指南根據 SCEP 管理組件 4.5.10.1 版所撰寫。

## 指南歷程記錄

版本	發行日期	變更
4.5.9.1	05/16/2012	本手冊原始版本。
4.5.10.1	11/06/2012	支援新的 Linux 發佈。 針對某些管理套件工具提供更完善的說明。

### 4.5.10.1 版本的變更

System Center Endpoint Protection 管理套件 4.5.10.1 版包括下列變更：

- 支援新的 Linux 發佈：
  - 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
- 附註：僅在使用 System Center 2012 Operations Manager Service Pack 1 和以上版本時支援這些新的發佈。
- 針對以下項目新增完善說明：
  - 作用中惡意軟體監視器
  - 作用中惡意軟體 (從規則) 警告

## 支援的配置

一般而言，[Operations Manager 2007 R2 支援的設定](http://go.microsoft.com/fwlink/?LinkId=90676) (http://go.microsoft.com/fwlink/?LinkId=90676) 中概述了支援的配置。

這個管理組件需要 System Center 2012 Operations Manager 2007 R2 或以上版本。下表詳列這個管理組件支援的作業系統：

作業系統名稱	x86	x64
Red Hat Enterprise Linux Server 5? 6	是	是
SUSE Linux Enterprise 10? 11	是	是
CentOS 5? 6	是	是
Debian Linux 5? 6	是	是
Ubuntu Linux 10.04? 12.04	是	是
Oracle Linux 5? 6	是	是

## 先決條件

必須符合以下需求，才能執行這個管理組件：

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

下列 SCEP 的管理組件整合於 System Center 2012 Operations Manager 2007 R2，也可從線上目錄下載。

ID	名稱	版本
Microsoft.Linux.Library	Linux 作業系統程式庫	6.1.7000.256
Microsoft.SystemCenter.InstanceGroup.Library	實例群組程式庫	6.1.7221.0
Microsoft.SystemCenter.Library	系統中心核心程式庫	6.1.7221.0
Microsoft.SystemCenter.WSManagement.Library	WS 管理程式庫	6.1.7221.0
Microsoft.SystemCenter.DataWarehouse.Library	資料倉儲程式庫	6.1.7221.0
Microsoft.Unix.Library	Unix 核心程式庫	6.1.7000.256
Microsoft.Unix.Service.Library	Unix 服務範本程式庫	6.1.7221.0
Microsoft.Windows.Library	Windows 核心程式庫	6.1.7221.0
System.Health.Library	狀態程式庫	6.1.7221.0
System.Library	系統程式庫	6.1.7221.0

**重要** 必須在配置檔案 `/etc/opt/microsoft/scep/scep.cfg` 或透過 SCEP Web 介面啟用使用 System Center 2012 Operations Manager 的 Linux SCEP 產品監視，才能正常運作。請確定上述配置檔案中的 'scom\_enabled' 參數設定為 'scom\_enabled = yes'，或在 Web 介面的 **[配置] > [全域] > [Daemon 選項] > [SCOM 啟用]** 下變更適當的設定。

## 此管理組件中的檔案

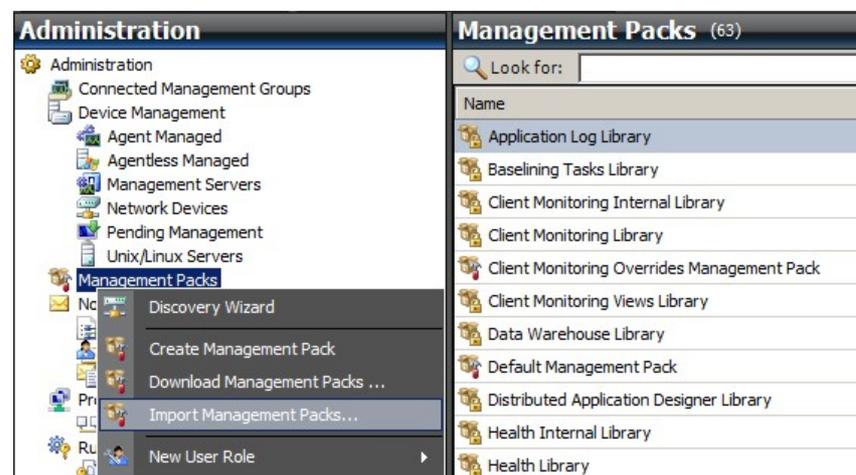
SCEP 管理組件包含以下檔案：

檔名	說明
Microsoft.SCEP.Linux.Library.mp	包含類別定義及其相互關係，同時也包含監視器類型和模組類型定義。
Microsoft.SCEP.Linux.Application.mp	實作監視和警告、工作及視圖。

## 快速入門

開始監視 SCEP 的先決條件是將管理組件匯入 Operations Manager，並識別要監視的電腦 (這個處理程序稱為「探索」)。

### 匯入管理組件

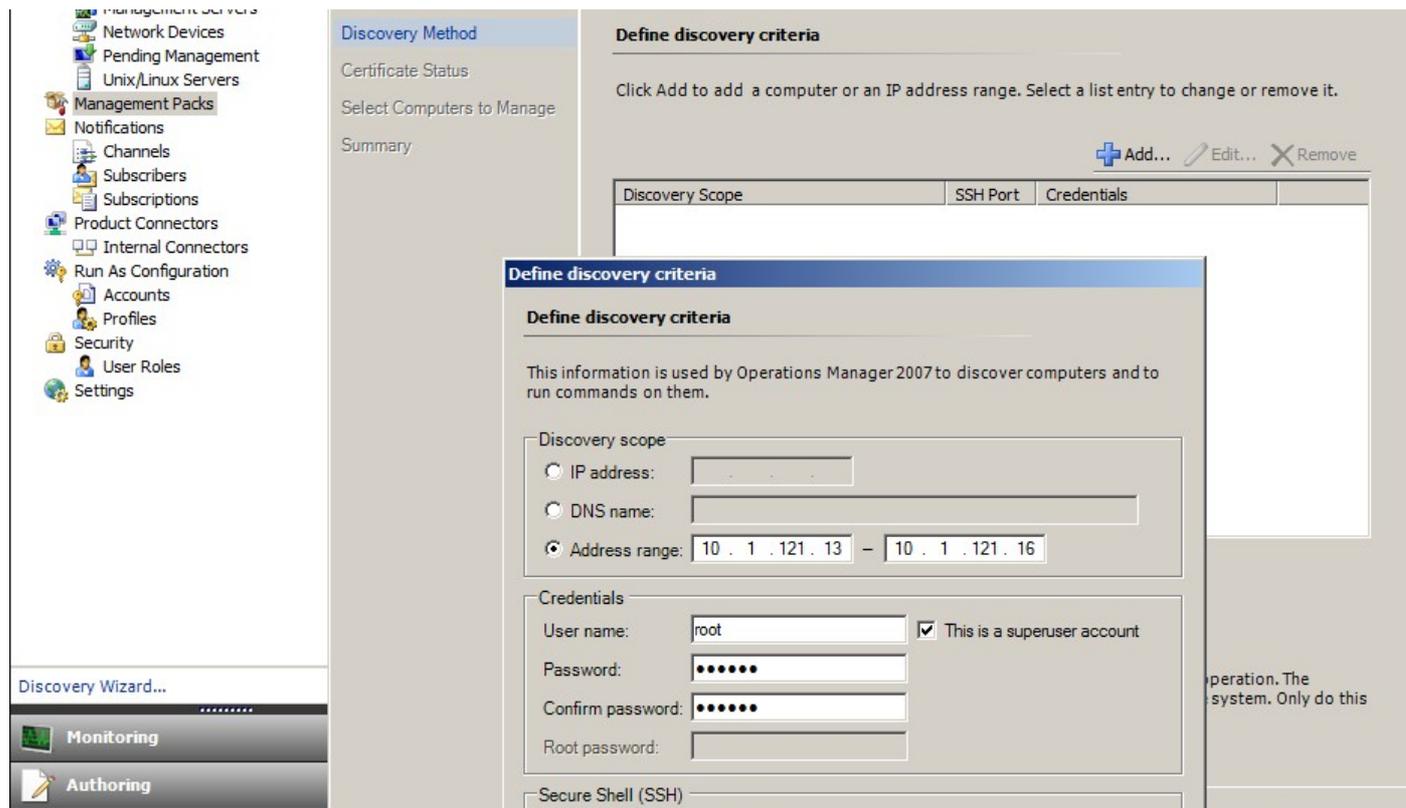


1. 按一下 [操作主控台] 視窗左窗格的 **[Administration]** 工作區。
2. 以滑鼠右鍵按一下 **[Management Packs]**，然後從內容功能表選取 **[Import Management Packs...]**。
3. 在 [管理組件] 視窗中，按一下 **[Add]** 按鈕，然後從下拉式功能表選取 **[Add from disk...]**。
4. 按一下 **[Online Catalog Connection]** 快顯視窗中的 **[Yes]**，確認讓 Operations Manager 搜尋並安裝本機磁碟沒有的相依性。
5. 務必選取兩個列出的檔案 (Microsoft.SCEP.Linux.Application.mp 及 Microsoft.SCEP.Linux.Library.mp)，然後按一下 **[Install]**。

**附註：** 如需更多匯入管理組件的指示，請參閱[如何在 Operations Manager 2007 中匯入管理組件](http://go.microsoft.com/fwlink/?LinkId=142351) (http://go.microsoft.com/fwlink/?LinkId=142351)。

## 探索

成功匯入 \*.mp 檔後，需要執行電腦探索。



1. 在 [Administration] 工作區 (位於 [操作主控台] 視窗左窗格) 中，按一下 [Discovery wizard...] 連結 (位於左窗格底端)。
2. 在 [電腦和裝置管理精靈] 中，選取 [Unix/Linux computers] 選項，然後按一下 [Next] 繼續。
3. 在 [定義探索條件] 區段中，按一下 [Add] 按鈕。
4. 設定 IP [Address range] 進行掃描，並設定電腦的 SSH [Credentials]，以便將其代理程式安裝於 System Center 2012 Operations Manager。
5. 按一下 [OK]，然後按一下 [Discover] 按鈕啟動探索處理程序，以確認範圍和憑證條件。
6. 一旦完成，將顯示清單，以供您選取系統進行監視 管理。

**附註：** 以下 [Linux 發送](#) 支援安裝 Linux 代理程式。如果無法使用探索來安裝 Linux 代理程式，請參閱以下 Microsoft 文章 [手動安裝跨平台代理程式](#) (<http://technet.microsoft.com/en-us/library/dd789016.aspx>) 中的手動安裝指示。

**附註：** 在透過 SCOM 管理的所有 Linux 電腦上，每 8 小時皆會利用 Operations Manager 安裝執行一次 Linux 伺服器探索 (也就是說，這些電腦已安裝適當的 Linux 管理組件進行系統發送)。探索將建立所有的服務模組實體：受保護的 Linux 伺服器 and 巢狀實體或未受保護的 Linux 伺服器 (可在適當的區段中找到)。「scep\_daemon」服務出現時 (已停止或執行中)，可將 SCEP 視為已完整安裝。因此，安裝管理組件時，將進行第一次探索，下一次將依據探索週期在 8 小時後進行。如果將 SCEP 產品解除安裝，個別的伺服器將自動移至 [未受保護] (無 SCEP 的伺服器)，反之亦然。

## 執行身分帳戶配置

若要建立 Unix 帳戶，請使用以下指示：

1. 在 [Administration] 工作區 (左窗格) 中，瀏覽至 [Run As Configuration] > [Accounts]。
2. 若要建立新帳戶，請開啟 [Actions] 區段 (位於 [處理方法] 窗格，也就是右窗格)，然後按一下 [Create Run As Account...]
3. 在 [一般內容] 視窗中，選取 [Basic Authentication] (位於 [Run As Account type] 下拉式功能表中)。
4. 建立帳戶之後，需要將新帳戶新增至設定檔，才會進行發送。若要這麼做，請以滑鼠右鍵按一下 [Unix Privileged Account] 設定檔 (在 [Run As Configuration] > [Profiles] 下)，選取 [Properties]，然後完成精靈以指派新建立的帳戶。



**附註：** 如需建立執行身分帳戶的詳細資訊，請參閱 System Center 2012 Operations Manager 2007 R2 線上文件庫的[設定跨平台執行身分帳戶](http://go.microsoft.com/fwlink/?LinkId=160348) (http://go.microsoft.com/fwlink/?LinkId=160348) 主題。

所有上述步驟均完成後，[Monitoring] > [System Center Endpoint Protection Linux] > [具有 SCEP 的伺服器] 下很快就會出現新探索的 Linux 伺服器 (在幾分鐘內)。

## 安裝 SCEP 的語言套件

語言套件的格式如下：

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

使用與前述**匯入管理組件**一節說明的相同步驟，來安裝語言套件。若要顯示 System Center 2012 Operations Manager 中已安裝的語言，請使用以下指示：

1. 按一下 Windows [開始] 圖示，並瀏覽至 [控制台]。
2. 在 [控制台] 中，按一下 [地區及語言選項]。
3. 在 [管理] 索引標籤中，變更非 Unicode 程式的系統地區設定。在 [位置] 索引標籤中，根據已安裝的語言套件變更目前位置。

## 管理組件目的

SCEP 的管理組件具有以下功能：

- 安全性事件及安全性狀態的即時監視和警告。
- 讓伺服器管理員能夠在伺服器遠端執行安全性相關的工作。這些工作的主要目的是修復與安全性有關的可用性問題。

## 視圖

伺服器管理員能夠使用 Operations Manager 主控台監視所有已安裝 SCEP 的電腦。以下為「System Center Endpoint Protection Linux」的視圖：

- **作用中警告** - 所有嚴重性層級的所有 SCEP 作用中警告。不包含關閉的警告。
- **儀表板** - 顯示 [具有 SCEP 的伺服器] 和 [作用中警告] 工作區。
- **具有 SCEP 的伺服器** - 顯示所有受保護的 Linux 伺服器。
- **無 SCEP 的伺服器** - 顯示所有未受保護的 Linux 伺服器。
- **工作狀態** - 列出所有已執行的工作。

使用 System Center 2012 Operations Manager 管理組件監控 SCEP 的狀態時，可立即檢視 SCEP 狀態。

按一下 Operations Manager 監視主控台中的 **[Monitoring] > [System Center Endpoint Protection Linux] > [具有 SCEP 的伺服器]** 窗格，即可隨時檢視 SCEP 元件的摘要狀態，完全不需要等候警告出現。[狀態] 欄位中的彩色圖示指示元件的狀態：

圖示	狀態	說明
	Healthy	綠色圖示指示成功，或指示有不需採取處理方法的資訊。
	Warning	黃色圖示指示錯誤或警告。
	Critical	紅色圖示指示嚴重錯誤或安全性問題，或指示無法使用服務。
	Not monitored	沒有圖示指示未收集到任何影響狀態的資料。

視圖可包含物件長清單。若要尋找特定的一個或多個物件，可使用 Operations Manager 工具列中的 [領域]、[搜尋] 和 [尋找] 按鈕。如需更多資訊，請參閱[如何在 Essentials 中使用領域、搜尋和尋找管理監視資料](http://go.microsoft.com/fwlink/?LinkId=91983) (http://go.microsoft.com/fwlink/?LinkId=91983) 主題。

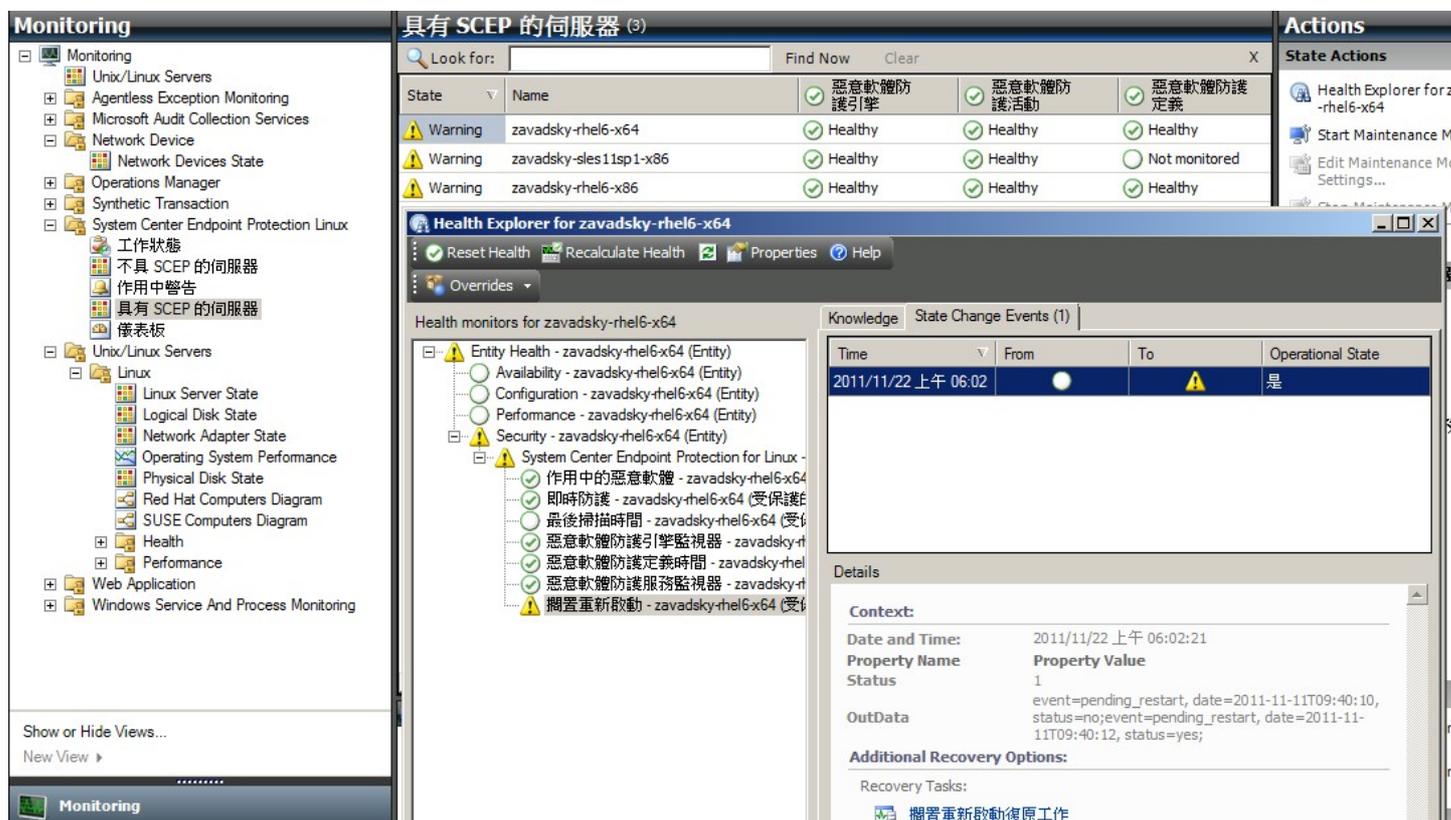
## 監視器

在 Operations Manager 2007 中，監視器可用來評估受監視的物件所可能發生的各種情況。

SCEP 總共有 17 個監視器：

- 9 個單位監視器 - 這些基本的監視元件用於監視特定的計數器、事件、指令碼和服務。
- 2 個彙總監視器 - 用於彙總，將多個監視器合併為一個監視器，然後使用該監視器設定狀態，並產生警告。
- 6 個相依性監視器 - 包含現有監視器狀態資料的參考。

**附註：** 如需更多監視器的資訊，請參閱 Operations Manager 2007 R2 說明 (在 System Center 2012 Operations Manager 中按下 F1 鍵)。



SCEP 狀態監視器有如下所述的結構和內容。

### 作用中的惡意軟體

監視器類型	單位監視器
目標	受保護的 Linux 伺服器
資料來源	監視文字防護記錄檔案： <code>/var/log/scep/eventlog_scom.dat</code>
間隔	事件驅動
警告	是。無自動解決
重設行為	經過 8 小時後，將自動返回至「狀況良好」狀態。警告將持續作用，以保留未處理的惡意軟體相關資訊。
附註	若偵測到惡意軟體且尚未將其清除，則此監視器狀態會變更為「嚴重」。此狀態在 8 小時過後會自動回復為「狀況良好」(這是因為無法精確判斷是否已清除 刪除惡意軟體)。管理員必須手動介入以考量詳細情況，並且關閉票證。
狀態	狀況良好 -沒有惡意軟體 嚴重 -作用中的惡意軟體
已啟用	真
復原工作	否

此監視器會追蹤失敗的惡意軟體清除作業。如果用戶端報告無法清除惡意軟體，則此監視器將報告「嚴重」狀態。

### 惡意軟體防護定義時間

監視器類型	單位監視器
目標	受保護的 Linux 伺服器
資料來源	用來取得監視資料的命令： <code>/opt/microsoft/scep/sbin/scep_daemon --status</code>
間隔	每 8 小時
警告	是。自動解決
狀態	狀況良好 -時間 <= 3 天 警告 -時間 > 3 且時間 <= 5 天 嚴重 -時間 > 5 天
已啟用	真

復原工作	是，手動 (無自動復原)
------	--------------

最新的定義可協助確保電腦受到保護，抵擋最新惡意軟體的威脅。

### 惡意軟體防護引擎

監視器類型	單位監視器
目標	受保護的 Linux 伺服器
資料來源	監視文字防護記錄檔案： /var/log/scep/eventlog_scom.dat
間隔	事件驅動
警告	是。自動解決
狀態	狀況良好 -已啟用 已停用 -警告
已啟用	真
復原工作	是，手動 (無自動復原)

建議您讓惡意軟體防護隨時保持啟用的狀態。

**附註：** 此監視器將追蹤與即時防護不同的病毒防護狀態。將惡意軟體防護引擎停用，則無法啟動指定掃描。

### 惡意軟體防護服務

監視器類型	單位監視器
目標	受保護的 Linux 伺服器
資料來源	處理程序的監視器狀態：scep_daemon
間隔	每 10 分鐘
警告	是。自動解決
狀態	狀況良好 -執行中 嚴重 -未執行
已啟用	真
復原工作	是，手動 (無自動復原)

當用戶端機器上的惡意軟體防護服務 (scep\_daemon) 未執行或無回應，或惡意軟體防護引擎未正常運作時，監視器會報告發生「嚴重」狀態。

### 最後掃描時間

監視器類型	單位監視器
目標	受保護的 Linux 伺服器
資料來源	用來取得監視資料的命令： /opt/microsoft/scep/sbin/scep_daemon --status
間隔	每 8 小時
警告	否
狀態	狀況良好 -時間 <= 7 警告 -時間 > 7
已啟用	真
復原工作	是，手動 (無自動復原)

此監視器將追蹤自最後電腦掃描 (無論掃描類型為何) 後所經過的時間。建議將掃描排程為每週執行一次。

### 擱置重新啟動

監視器類型	單位監視器
目標	受保護的 Linux 伺服器
資料來源	監視文字防護記錄檔案： /var/log/scep/eventlog_scom.dat
間隔	事件驅動
警告	是。自動解決

狀態	否 -狀況良好 是 -警告
已啟用	真
復原工作	是，手動 (無自動復原)

此監視器將追蹤是否需要重新啟動系統，以使配置變更生效 (一般是在啟用 停用即時保護時)。監視器將套用以下針對此狀態指定更新的呼叫：`dppt/microsoft/scep/sbin/scep_daemon --status`。

### 即時防護

監視器類型	單位監視器
目標	受保護的 Linux 伺服器
資料來源	監視文字防護記錄檔案： <code>/var/log/scep/eventlog_scom.dat</code> 監視器也將使用以下針對指定狀態更新的呼叫： <code>dppt/microsoft/scep/sbin/scep_daemon --status</code> 。
間隔	事件驅動
警告	是。自動解決
狀態	已啟用 -狀況良好 已停用 -警告
已啟用	真
復原工作	是，手動 (無自動復原)

監視即時防護的狀態。當病毒、間諜程式或其他潛在不需要軟體嘗試自行安裝於您的電腦上時，即時防護會向您發出警告。

### System Center Endpoint Protection for Linux

監視器類型	彙總監視器
目標	受保護的 Linux 伺服器
狀況	最壞
警告	否
已啟用	真
復原工作	否

此監視器是所有 SCEP 7 受保護 Linux 伺服器安全性單位監視器的狀態彙總 (最壞狀態)。如果狀態為未初始化，可能是此物件的監視尚未開始，或者此物件未定義安全性監視器。

### 惡意軟體防護引擎

監視器類型	相依性監視器
目標	惡意軟體防護引擎
警告	否
已啟用	真
復原工作	否

顯示受監視電腦的清單中受保護 Linux 伺服器 惡意軟體防護引擎單位監視器的狀態。

### 惡意軟體防護服務

監視器類型	相依性監視器
目標	惡意軟體防護引擎
警告	否
已啟用	真
復原工作	否

顯示受監視電腦的清單中受保護 Linux 伺服器 惡意軟體防護服務單位監視器的狀態。

## 惡意軟體防護定義

監視器類型	相依性監視器
目標	惡意軟體防護定義
警告	否
已啟用	真
復原工作	否

顯示受監視電腦的清單中受保護 Linux 伺服器 惡意軟體防護定義時間監視器的狀態。

## 作用中的惡意軟體

監視器類型	相依性監視器
目標	惡意軟體防護活動
警告	否
已啟用	真
復原工作	否

顯示「健全狀況總管」中針對惡意軟體防護活動的受保護 Linux 伺服器 作用中惡意軟體監視器狀態。

## 電腦 Ping

監視器類型	單位監視器
目標	惡意軟體防護活動
間隔	每 60 分鐘
警告	否
狀態	可連線 -狀況良好 無法連線 -嚴重
已啟用	假
復原工作	否

伺服器無回應時，將其狀態變更為「嚴重」。

## 惡意軟體活動

監視器類型	單位監視器
目標	惡意軟體防護活動
資料來源	監視文字防護記錄檔案： /var/log/scep/eventlog_scom.dat
間隔	事件驅動
警告	否
狀態	沒有惡意軟體 -狀況良好 已偵測到惡意軟體活動 -嚴重
已啟用	真
復原工作	否

此監視器將在惡意軟體偵測 (已清除或未處理) 之後 5 分鐘內切換至「嚴重」狀態，並且在後續 60 分鐘內維持「嚴重」。「嚴重」狀態將在每次新偵測到惡意軟體時及經過警告期間後更新。換句話說，如果在 60 分鐘內未偵測任何惡意軟體，監視器將回復「狀況良好」狀態。

## 伺服器惡意軟體爆發

監視器類型	彙總監視器
目標	惡意軟體防護活動
狀況	最佳
警告	否
已啟用	真

復原工作	否
------	---

彙總監視器：惡意軟體活動，電腦 Ping。

如果在偵測到惡意軟體 (已清除或未處理) 之後 60 分鐘內未得到伺服器的回應，會將其狀態切換至「嚴重」。如果在未得到伺服器的回應一段時間後，連線更新時立即偵測到惡意軟體，也會使得狀態變更為「嚴重」。

### 惡意軟體爆發

監視器類型	相依性監視器
目標	受保護伺服器監控程式
狀況	最壞 95%
警告	否
已啟用	真
復原工作	否

顯示「惡意軟體防護活動」/「伺服器惡意軟體爆發」監視器的狀態。

如果全部的 Linux 電腦 (受保護及未受保護) 有 5% 在過去 60 分鐘內註冊惡意軟體偵測，此監視器將變更為「嚴重」狀態。

### SCEP Linux 電腦角色狀態彙總

監視器類型	相依性監視器
目標	Linux 電腦
警告	否
已啟用	真
復原工作	否

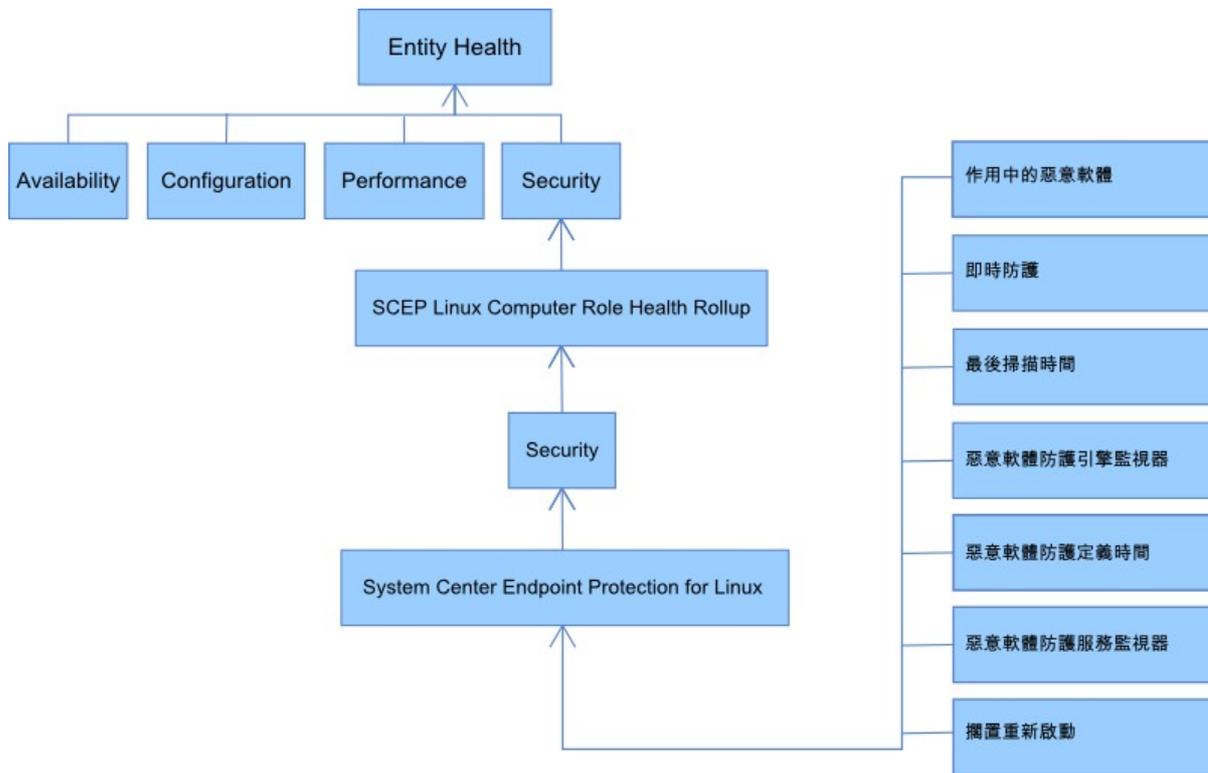
將受保護的 Linux 電腦實體狀態傳播至 Linux 電腦 安全性上層監視器。

### 如何彙總狀態

這個管理組件將 Linux 作業系統監視擴充為分層結構，每一層都是以較低一層狀況是否良好為依據。這個結構的頂層是整個實體狀態環境，而安全性環境的最底層是所有的監視器。其中一層變更狀態時，上一層也會相應變更狀態。這個動作稱為彙總狀態。

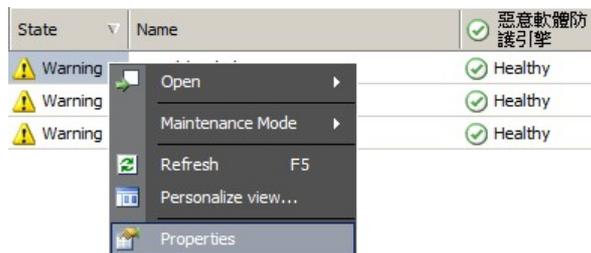
例如，如果即時防護傳回警告狀態，而其他所有元件均為狀況良好，則會透過樹狀結構將警告狀態傳輸至根層級 (實體狀態)，使該層級則取得警告狀態。

以下圖表顯示如何彙總此管理組件中的物件狀態。



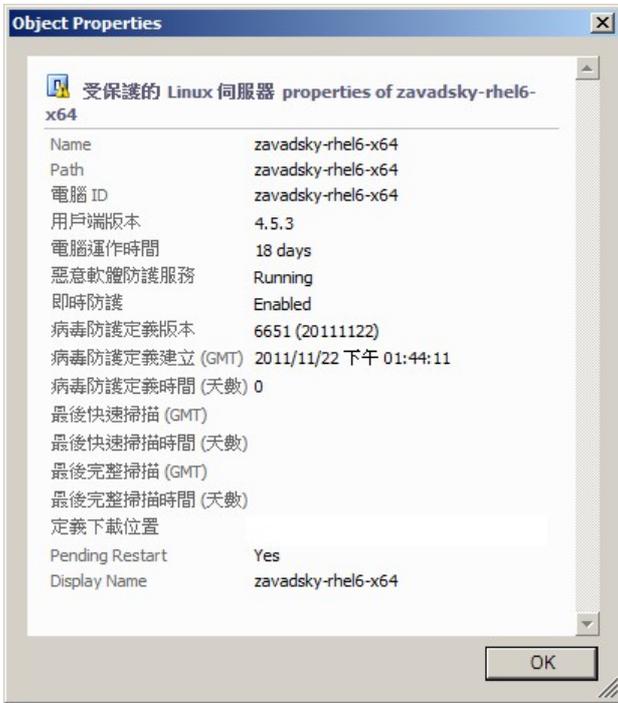
## 物件內容

若要檢視物件的內容，請以滑鼠右鍵按一下物件，並選取 [Properties]。



受保護的 Linux 伺服器物件有以下內容：

- **電腦 ID** - 伺服器識別碼、網域名稱。
- **顯示名稱** - 伺服器名稱、網域名稱。
- **用戶端版本** - 安裝的 SCEP 產品版本。
- **電腦運作時間** - 伺服器運作時間 (測量機器持續運作而未停止的時間) 並非管理組件正常運作的極重要資料，缺少這些資料可能表示管理組件發生錯誤。
- **惡意軟體防護服務** - 惡意軟體防護狀態 (執行中 未執行)。
- **即時防護** - 即時防護狀態，缺少這個狀態則表示有 SCEP 問題。
- **病毒防護定義 ...** - 病毒資料庫狀態資料 (版本、建立日期、時間)，缺少這些資料則表示 SCEP 問題。
- **最後快速 完整掃描 ...** - 上一次電腦掃描的資料。如果尚未執行掃描 (快速掃描 完整掃描)，則不會出現任何資料。
- **定義下載位置** - 更新伺服器位址 名稱。資訊將在第一次成功更新後顯示。
- **[擱置重新啟動]** - 由於新安裝或 SCEP 配置變更而需要重新啟動以套用變更的資訊。



## 警告

警告是指示以特定嚴重性預先定義的狀態已發生於所監視物件的項目。警告是依規則所定義。您可在 **[Monitoring] > [System Center Endpoint Protection Linux] > [作用中警告]** 找到 Operations Manager 主控台內的視圖，該視圖會顯示主控台使用者有權可查看的特定物件警告。

**附註：** 如果相同伺服器重複產生相同類型的警告 (例如作用中的惡意軟體)，則只會顯示第一個警告 (將忽略重複的警告)。

警告	間隔	優先順序	嚴重性	說明
重複惡意軟體感染	事件驅動	高	嚴重	在指定的時間間隔 (30 分鐘) 內，偵測到重複的惡意軟體 (出現 3 次) 情況下所產生的警告。警告包含伺服器的資料和惡意軟體的基本資訊。
已清除惡意軟體	事件驅動	低 中	資訊 -已成功清除惡意軟體 警告 -需要使用者互動，例如伺服器重新啟動	成功清除惡意軟體的警告。包含特定惡意軟體所有可用的資料。各個所偵測的惡意軟體均產生個別的事件。SCEP Linux 依據清除處理程序的效率指派優先順序和嚴重性，其中： 已清除 = 低 + 資訊 已清除但無動作 (例如重新啟動) = 中 + 警告。
作用中惡意軟體 (從監視器)	事件驅動	高	嚴重	關於未清除的惡意軟體警告。包含特定惡意軟體所有可用的資料。
作用中惡意軟體 (從規則)	事件驅動	高 中 低	嚴重 中 低 -根據惡意軟體類型	同上。用於其他監視 票務系統的連線程式。 <b>附註：</b> 此規則 (警告) 預設為停用。
System Center Endpoint Protection 惡意軟體防護服務已關閉	300 秒	中	嚴重	無法使用惡意軟體防護服務 SCEP (scep_daemon) 的警告。包含個別伺服器名稱和 SCEP 版本。
已停用惡意軟體防護	事件驅動	中	警告	停用惡意軟體防護的警告。包含個別伺服器名稱。
已停用即時防護	事件驅動	中	警告	停用即時防護的警告。包含個別伺服器名稱。

過期定義	每 8 小時	中	警告 (時間 <= 5 天 且時間 > 3 天) 嚴重 (時間 > 5 天)	超過 3 天未更新病毒資料庫的警告。 包含個別伺服器名稱和病毒資料庫的 時間。
惡意軟體爆發	事件驅動	高	嚴重	Forefront Endpoint Protection 在您 5% 以上的電腦中皆偵測到作用中的惡 意軟體。惡意軟體可能正在電腦之 間進行傳播。建議您確定所有伺服器 均使用最新的定義。如果您需要變更 可觸發此警告的作用中威脅數量，請 覆寫惡意軟體爆發監視器中的參數 (請 參閱 <a href="#">覆寫</a> 一章。)

## 工作

SCEP 的管理組件實作 13 個工作。這些工作都會立即執行。輸出將在工作執行後立即顯示，稍後也可從 [工作狀態] 視窗檢視輸出。工作執行所需的最長時間為 180 秒。無法使用覆寫。所有工作都是透過 SSH 執行的 BASH 命令。

在 [操作主控台] 視窗右窗格的 [Monitoring] > [System Center Endpoint Protection Linux] > [具有 SCEP 的伺服器] 中，可呼叫工作。

### 受保護的 Linux 伺服器 Ta... ▲

- 完整掃描
- 快速掃描
- 更新 SCEP 定義
- 重新啟動
- 重新啟動 SCEP 服務
- 停止 SCEP 服務
- 停止掃描
- 停用即時防護
- 停用病毒防護
- 啟用即時防護
- 啟動 SCEP 服務
- 啟動病毒防護
- 擷取端點設定

- **停用病毒防護** - 停用病毒防護的所有元件，停用指定掃描。
- **啟用病毒防護** - 啟用病毒防護的所有元件。
- **停用即時防護** - 停用即時防護。
- **啟用即時防護** - 啟用即時防護。
- **完整掃描** - 更新病毒資料庫並執行完整的電腦掃描。
- **快速掃描** - 更新病毒資料庫並執行快速的電腦掃描。
- **停止掃描** - 停止所有執行中的電腦掃描。
- **擷取伺服器設定** - 顯示目前的 SCEP 產品狀態，所顯示參數的清單與受保護 Linux 伺服器實體的內容相同。顯示的資料不會傳輸至受保護的 Linux 伺服器。
- **重新啟動惡意軟體防護服務** - 重新啟動 SCEP 惡意軟體防護服務 (scep\_daemon)。
- **停止惡意軟體防護服務** - 停止 SCEP 惡意軟體防護服務 (scep\_daemon)。
- **啟動惡意軟體防護服務** - 啟動 SCEP 惡意軟體防護服務 (scep\_daemon)。
- **更新惡意軟體防護定義** - 啟動病毒資料庫更新。
- **重新啟動** - 重新啟動 Linux 電腦。

## 配置 SCEP 的管理組件

### 最佳實務：建立自訂的管理組件

Operations Manager 預設將覆寫之類的設定儲存於預設管理組件中。依據最佳實務，對於您要自訂的各個密封的管理組件，您應該另行建立個別的管理組件。

建立管理組件來儲存密封的管理組件自訂的設定時，可以將新管理組件的名稱命名為將自訂的管理組件名稱，例如「SCEP 2012 自訂」。

建立新管理組件為各個密封的管理組件儲存自訂，能夠使得將測試環境的自訂匯出至生產環境的程序更加簡化。這也能夠使得刪除管理組件的程序更加簡化，因為您必須先刪除任何相依項目，才能刪除管理組件。如果所有管理組件的自訂均儲存於預設管理組件，而您需要刪除單一的管理組件，您必須先刪除預設管理組件，這也將刪除其他管理組件的自訂。

## 安全性配置

電腦必須執行 SSHD 服務，而且 SSH 連接埠 (預設值 22) 必須開啟。System Center 2012 Operations Manager 使用類型為 **Basic Authentication** 的適當 Run As Account (位於 Operations Manager 監視主控台的 [Administration] > [Run As Configuration] 窗格)，透過此連接埠連接至遠端 Linux 電腦。

執行身分設定檔名稱	附註
Unix Privileged Account	用於遠端監視 Unix 伺服器，以及在需要權限時重新啟動處理程序。

這個管理組件不使用 [Unix Action Account]。

**警告** 使用系統管理員帳戶監視電腦會有潛在安全性風險，例如密碼已遭破解。

如果您不希望使用系統管理員帳戶進行監視和管理，您可使用標準使用者帳戶，但此帳戶必須具有執行 `sudo` 命令的權限。因此，每個使用 Linux SCEP 監視的工作站中的 `/etc/sudoers` 檔案皆需要下列配置，才可將 `sudo` 提高權限授權給所選使用者帳戶。此為使用者名稱 `user1` 的配置範例：

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

user1 ALL=(root) NOPASSWD: /opt/microsoft/scx/bin/scxlogfileviewer -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
#-----
```

## 微調效能閾值規則

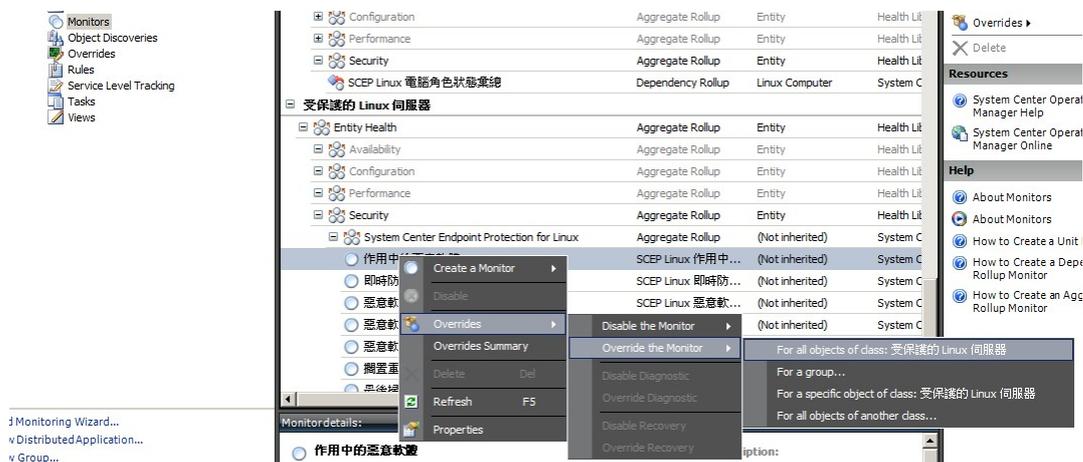
下表列出預設閾值可能需要其他微調以符合您環境的效能閾值規則。請評估這些規則，以判斷預設閾值是否適合您的環境。如果預設閾值不適合您的環境，您可覆寫閾值以調整閾值。

規則名稱	覆寫參數	預設閾值	微調限制
重複惡意軟體感染規則	重複感染計數閾值	出現 3 次	設定低於 2 的值會使規則過時。
重複惡意軟體感染規則	重複感染時間範圍	30 分鐘	不建議您設定低於指定掃描期間的值，因為時間重疊將無法產生警告。
作用中惡意軟體警告規則	已啟用	假	如果您使用其他監視 票務系統的連線程式，您可以啟用此警告。

## 覆寫

覆寫可用來調整 System Center 2012 Operations Manager 中監視物件的設定。這包含監視器、規則、物件探索，以及從匯入的管理組件取得的屬性。

若要覆寫監視器，請在 [操作主控台] 中，按一下 [Authoring] 按鈕，並展開 [Management Pack Objects] > [Monitors]。在 [監視器] 窗格中，尋找物件類型並完全展開物件類型，然後按一下監視器，並且按一下 [Overrides]。



使用 [覆寫] 視窗，建立或修改以下任何參數的覆寫：

- 作用中惡意軟體監視器回復時間 (僅與作用中惡意軟體監視器有關)
- 惡意軟體防護定義時間 (僅與惡意軟體防護定義時間監視器有關)
- 偵測間隔 (僅與最後掃描時間監視器有關)
- 警告啟用狀態
- 警告優先順序
- 警告嚴重性
- 自動解決警告
- 已啟用 - 決定啟用或停用選取的監視器。
- 產生警告
- SCEP 防護記錄檔案路徑

如果預設覆寫不適合您的環境，您可覆寫閾值以調整閾值：

覆寫參數	監視器名稱	預設值	微調附註
Ping 間隔	電腦 Ping	3600 秒	檢視受保護的 Linux 伺服器可用性的間隔。如果機器由於攻擊而停止回應，較短的期間將較快觸發「伺服器惡意軟體爆發」監視器的錯誤狀態。結果，網路、受監視的電腦及 System Center 2012 Operations Manager 伺服器的負載將增加。
惡意軟體爆發時間視窗	惡意軟體活動	3600 秒	監視器在惡意軟體活動之後返回至「狀況良好」狀態所需的間隔。「時間範圍」監視器值應該高於「電腦 Ping/Ping 間隔」，組合才能正常運作。 在「惡意軟體爆發時間範圍」間隔，如果超過所設定「惡意軟體爆發」百分比值的電腦數量 (請參閱「惡意軟體爆發」) 登錄惡意軟體活動，將產生「惡意軟體爆發」警告。  附註：這與「伺服器惡意軟體爆發」不同，因為後者不會產生警告。
作用中惡意軟體監視器回復時間	作用中的惡意軟體	28800 秒	惡意軟體偵測之後的時間間隔，經過這段時間會將惡意軟體視為已清除。
SCEP 防護記錄檔案路徑	作用中的惡意軟體	/var/log/scep/eventlog_scom.log	記錄 System Center 2012 Operations Manager 事件的檔案所在路徑。除非發生問題，否則請勿變更此參數。
惡意軟體防護定義關鍵時間	惡意軟體防護定義時間	5 天	經過這段間隔之後，將產生過期 SCEP 產品的錯誤警告。
惡意軟體防護定義狀況良好時間	惡意軟體防護定義時間	3 天	允許的惡意軟體防護時間上限，這段時間內的定義將被視為最新。這個值應該永遠小於「惡意軟體防護定義關鍵時間」值。
間隔	惡意軟體防護定義時間	28800 秒	檢查惡意軟體防護定義時間的間隔。

間隔	惡意軟體防護服務	300 秒	檢查惡意軟體防護服務可用性的間隔。
處理程序名稱	惡意軟體防護服務	scep_daemon	惡意軟體防護服務的名稱。如果監視器正常運作，請勿變更此值。
偵測間隔	最後掃描時間	28800 秒	檢查最後掃描執行的間隔。
最長掃描時間	最後掃描時間	7 天	根據 SCEP 產品設定加以設定。如果排程掃描每 7 天執行，請將此值設定為 7 天。
防護記錄檔案路徑	擱置重新啟動	/var/log/scep/eventlog_scom.log	記錄 System Center 2012 Operations Manager 事件的檔案所在路徑。除非發生問題，否則請勿變更此參數。
SCEP 防護記錄檔案路徑	即時防護	/var/log/scep/eventlog_scom.log	記錄 System Center 2012 Operations Manager 事件的檔案所在路徑。除非發生問題，否則請勿變更此參數。
百分比	惡意軟體爆發	95%	Linux 伺服器 (受保護 + 未受保護) 必須返回至「狀況良好」狀態，才能使整個受監視的群組被視為「狀況良好」的伺服器百分比。如果偵測到的惡意軟體佔總數的 5% 以上，將產生「惡意軟體爆發」。



附註：如需更多關於「覆寫」的資訊，請參閱[如何使用覆寫進行監視](http://go.microsoft.com/fwlink/?LinkID=117777) (http://go.microsoft.com/fwlink/?LinkID=117777)。

## 連結

以下連結可為您提供與這個管理套件相關聯的一般工作相關資訊：

- [管理管理組件生命週期](http://go.microsoft.com/fwlink/?LinkId=211463)
- [如何在 Operations Manager 2007 中匯入管理組件](http://go.microsoft.com/fwlink/?LinkID=142351)
- [如何使用覆寫進行監視](http://go.microsoft.com/fwlink/?LinkID=117777)
- [如何在 Operations Manager 2007 中建立執行身分帳戶](http://go.microsoft.com/fwlink/?LinkID=165410)
- [設定跨平台執行身分帳戶](http://go.microsoft.com/fwlink/?LinkId=160348)
- [如何修改現有的執行身分設定檔](http://go.microsoft.com/fwlink/?LinkID=165412)
- [如何匯出管理組件自訂](http://go.microsoft.com/fwlink/?LinkId=209940)
- [如何移除管理組件](http://go.microsoft.com/fwlink/?LinkId=209941)
- [如何在 Essentials 中使用領域、搜尋和尋找管理監視資料](http://go.microsoft.com/fwlink/?LinkId=91983)
- [使用 SCOM 2007 R2 監視 Linux](http://blogs.technet.com/b/birojtn/archive/2010/01/20/monitoring-linux-using-scom-2007-r2.aspx)
- [手動安裝跨平台代理程式](http://technet.microsoft.com/en-us/library/dd789016.aspx)
- [使用 System Center 2012 - Operations Manager 針對 UNIX 和 Linux 監視配置 sudo 提高權限](#)

(<http://social.technet.microsoft.com/wiki/contents/articles/7375.configuring-sudo-elevation-for-unix-and-linux-monitoring-with-system-center-2012-operations-manager.aspx>)

關於 Operations Manager 及監視組件的問題，請參閱 [System Center Operations Manager 社群論壇](http://go.microsoft.com/fwlink/?LinkID=179635) (<http://go.microsoft.com/fwlink/?LinkID=179635>)。

[System Center Operations Manager Unleashed 部落格](http://opsmgrunleashed.wordpress.com/) (<http://opsmgrunleashed.wordpress.com/>) 是實用的資源，其中包含特定監視組件的「範例解說」文章。

如需 Operations Manager 的詳細資訊，請參閱以下部落格：

- [Operations Manager 團隊部落格](http://blogs.technet.com/momteam/default.aspx)  
(<http://blogs.technet.com/momteam/default.aspx>)
- [Kevin Holman 的 OpsMgr 部落格](http://blogs.technet.com/kevinholman/default.aspx)  
(<http://blogs.technet.com/kevinholman/default.aspx>)
- [關於 OpsMgr 的想法](http://thoughtsonopsmgr.blogspot.com/)  
(<http://thoughtsonopsmgr.blogspot.com/>)
- [Raphael Burri 的部落格](http://rburri.wordpress.com/)  
(<http://rburri.wordpress.com/>)
- [BWren 的管理空間](http://blogs.technet.com/brianwren/default.aspx)  
(<http://blogs.technet.com/brianwren/default.aspx>)
- [System Center Operations Manager 支援團隊部落格](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))
- [System Center Operations Manager 的注意事項](http://blogs.msdn.com/mariussutara/default.aspx)  
(<http://blogs.msdn.com/mariussutara/default.aspx>)

關於疑難排解，請參閱以下的論壇討論串：

- [找不到 Microsoft.Unix.Library](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/>)