System Center Endpoint Protection

安裝手冊與使用手冊

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

Microsoft

Microsoft® System Center Endpoint Protection

內容

說明

感謝您使用 System Center Endpoint Protection。Microsoft 尖端的掃描引擎可達到絕佳的掃描速度及偵測率，而且佔用的使用量相當小，因此是任何 Linux OS 伺服器的理想選擇。

主要功能

指定掃描器

有權限的使用者 (通常是系統管理員) 可透過命令列介面、Web 介面或作業系統的自動排程工具 (例如 cron) 啟動指定掃描器。*指定*一詞是指使用者或系統指定掃描檔案系統物件。

即時防護

使用者及 *或*系統嘗試存取檔案系統物件時，將呼叫即時防護。這也可釐清*常駐*一詞的使用，因為掃描是由存取檔案系統物件的嘗試所觸發。

系統主要功能

進階引擎演算法

Microsoft 防毒掃描引擎演算法提供最高的偵測率及最快的掃描時間。

多重處理

System Center Endpoint Protection 能夠在單一和多重處理器裝置上運作。

進階探索法

System Center Endpoint Protection 包含 Win32 蠕蟲、後門程式感染及其他形式惡意程式獨特的進階探索法。

內建功能

內建解壓縮軟體能夠將壓縮的物件解壓縮，完全不需要任何外部程式。

速度與效率

為提升系統的速度與效率，System Center Endpoint Protection 的架構採用執行中 Daemon (常駐程式)，所有掃描要求皆傳送到此。

增強的安全性

所有執行 Daemon (except scep_dac) 都是在無權限的使用者帳戶下執行，使安全性更為增強。

選擇性配置

系統支援依據使用者或用戶端 *伺*服器的選擇性配置。

多重記錄層級

多重記錄層級經過配置即可取得系統活動及入侵的資訊。

Web 介面

配置及管理均透過方便使用的直覺化 Web 介面進行。

不需要外部程式庫

除了 LIBC 之外，System Center Endpoint Protection 安裝不需要外部程式庫或程式。

使用者指定的通知

可配置系統在偵測到入侵或其他重要事件時通知特定使用者。

低系統需求

System Center Endpoint Protection 僅需要 16MB 的硬碟空間和 32MB 的 RAM，即可有效運作。它可在 2.2.x、2.4.x 及 2.6.x Linux OS 核心版本下平順運作。

效能及延展性

從低耗電量的小型辦公室伺服器到擁有數千位使用者的企業級 ISP 伺服器，System Center Endpoint Protection 均能夠發揮 UNIX 型解決方案應有的效能及延展性，並達到 Microsoft 安全性產品絕佳的安全性。

術語及縮寫

本小節將檢視本文件中使用的術語及縮寫。請注意，粗體字型保留用於產品元件名稱，並且保留用於新定義的術語及縮寫。本文件稍後將解說本章定義的術語及縮寫。

SCEP

SCEP 是 Microsoft 針對 Linux 作業系統開發的安全產品標準的縮寫。這也是包含該產品的軟體套件名稱。

SCEP daemon

主要 SCEP 系統控制及掃描 Daemon： *scep_daemon*.

SCEP 基礎目錄

包含病毒資料庫的 SCEP 可載入模組儲存目錄。後續參照此目錄時將使用縮寫 *@BASEDIR@*。*@BASEDIR@* 值 (依據作業系統) 如下所列：

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

SCEP 配置目錄

所有與 System Center Endpoint Protection 配置相關的檔案儲存目錄。後續參照此目錄時將使用縮寫 *@ETCDIR@*。*@ETCDIR@* 值 (依據作業系統) 如下所列：

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

SCEP 配置檔案

主要System Center Endpoint Protection 配置檔案。檔案的絕對路徑如下：

@ETCDIR@/scep.cfg

SCEP 二進位檔案目錄

相關 System Center Endpoint Protection 二進位檔案的儲存目錄。後續參照此目錄時將使用縮寫 *@BINDIR@*。*@BINDIR@* 值 (依據作業系統) 如下所列：

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

SCEP 系統二進位檔案目錄

相關 System Center Endpoint Protection 系統二進位檔案的儲存目錄。後續參照此目錄時將使用縮寫 *@SBINDIR@*。*@SBINDIR@* 值 (依據作業系統) 如下所列：

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

SCEP 物件檔案目錄

相關 System Center Endpoint Protection 物件檔案及程式庫的儲存目錄。後續參照此目錄時將使用縮寫 *@LIBDIR@*。*@LIBDIR@* 值 (依據作業系統) 如下所列：

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

安裝

System Center Endpoint Protection 是以二進位檔案的形式散佈：

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

在以上所示的二進位檔案中，*'ext'* 是 Linux OS 散佈的從屬字尾，例如 'deb' 表示 Debian，'rpm' 表示 RedHat 和 SuSE，'tgz' 表示其他 Linux OS 散佈。

若要安裝或升級產品，請使用下列命令：

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

顯示產品的使用者授權接受合約。一旦確認該接受合約，安裝套件便會放置在目前的工作目錄中，並且在畫面顯示套件安裝、解除安裝或升級的相關資訊。

一旦安裝套件，即可使用下列命令驗證主要 SCEP 服務是否執行：

```
ps -C scep_daemon
```

按下 ENTER 之後，應該會看見下列 (或類似) 的訊息：

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

背景至少有兩個 SCEP Daemon 處理程序正在執行。第一個 PID 表示系統的處理程序及執行緒管理員。另一個表示 SCEP 掃描處理程序。

安裝語言套件

為了安裝必要的 System Center Endpoint Protection 語言套件，請使用下列命令：

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

其中 *'lng'* 必須以您要匯入之檔案的語言代碼來取代。

顯示 *[Installation completed successfully]* 通知後，請依照指示更新 LANG 系統變數，並視需要更新環境。這樣即完成語言套件安裝。

每個語言套件都包含下列各項：

- 當地語系化的 Web 介面
- SCEP 代理程式及命令的當地語系化主控台輸出
- 當地語系化的 PDF 文件

架構概要

一旦成功安裝 System Center Endpoint Protection，您應可逐漸熟悉其架構。

系統由以下部分組成：

核心

System Center Endpoint Protection 的核心是 SCEP Daemon (scep_daemon)。該 Daemon 使用 SCEP API 程式庫 libscep.so 及 SCEP 載入模組 em00X_xx.dat 提供基礎系統工作，例如掃描、維護代理程式 Daemon 處理程序、範例提交系統維護、記錄、通知等。如需詳細資訊，請參閱 *scep_daemon(8)* 手冊頁面。

代理程式

SCEP 代理程式模組的目的是將 SCEP 與 Linux 伺服器環境相互整合。

公用程式

工作程式模組提供簡單而有效的系統管理。這些模組負責的系統工作包括隔離區管理、系統設定和更新。

配置

適當的配置是安全系統最重要的層面，本章後續將專門解說所有相關的元件。另外強烈建議徹底瞭解 *scep.cfg* 檔，因為這個檔案包含對於 System Center Endpoint Protection 配置相當重要的資訊。

成功安裝產品之後，產品所有的配置元件將儲存於 SCEP 配置目錄中。該目錄包含以下檔案：

@ETCDIR@/scep.cfg

這是最重要的配置檔案，因為它控制產品功能所有的主要層面。scep.cfg 檔包含數個區段，各個區段均包含不同的參數。該檔案包含一個全域的區段和多個「代理程式」區段，其中所有的區段名稱均以方括弧括住。全域區段中的參數用於定義 SCEP Daemon 的配置選項，以及 SCEP 掃描引擎配置的預設值。代理程式區段中的參數用於定義模組的配置選項，這些模組用於擷取電腦和 *或*其鄰近電腦的各種資料流類型，以便進行掃描。請注意，除了用於系統配置的各種參數之外，另外也有管理檔案組織的規則。如需更多與最有效組織此檔案的方法有關的詳細資訊，請參閱 *scep.cfg(5)* 和 *scep_daemon(8)* 手冊頁面，以及相關代理程式的手冊頁面。

@ETCDIR@/certs

此目錄用於儲存 SCEP Web 介面進行驗證所用的憑證。如需詳細資訊，請參閱 *scep_wwwi(8)* 手冊頁面。

@ETCDIR@/scripts/daemon_notification_script

如果由 SCEP 配置檔案參數 *'exec_script'* 啟用，此指令碼將在防毒系統偵測到入侵時執行，以將事件的電子郵件通知傳送給系統管理員。

檔案系統服務的整合

本章說明有效防範病毒及蠕蟲檔案系統感染的指定和即時防護配置。透過指定掃描器命令 *'scep_scan'* 及常駐掃描器命令 *'scep_dac'* 即可使用 System Center Endpoint Protection 的掃描功能。Linux 版本的 System Center Endpoint Protection 提供額外的常駐掃描器技術，能夠使用預載程式庫模組 *libscep_pac.so*。以下小節將說明所有這些命令。

指定掃描器

有權限的使用者 (通常是系統管理員) 可透過命令列介面、Web 介面或作業系統的自動排程工具 (例如 cron) 啟動指定掃描器。*指定*一詞是指使用者或系統指定掃描檔案系統物件。

指定掃描器不需要特殊的配置即可執行。適當安裝 SCEP 套件之後，即可使用命令列介面或排程器工具立即執行指定掃描器。若要從命令列執行指定掃描器，請使用下列語法：

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

其中 FILES 是將掃描的目錄和 *或*檔案清單。

使用 SCEP 指定掃描器有多個命令列選項可供使用。若要查看選項的完整清單，請參閱 *scep_scan(8)* 手冊頁面。

Dazuko 提供的即時保護

：
使用者存取及 *或*系統存取檔案系統物件時，將呼叫即時防護。這也說明*常駐*一詞的意義；掃描器是由存取所選檔案系統物件的任何嘗試所觸發。

SCEP 常駐掃描器使用的技術由 Dazuko (da-tzu-ko) 核心模組提供，這是以核心呼叫的攔截為基礎。Dazuko 專案是開放原始碼專案，這表示來源程式碼可供自由散佈。這能夠讓使用者編譯本身自訂核心的核心模組。請注意，Dazuko 核心模組不屬於任何 SCEP *產品*的一部份，因此必須在使用常駐命令 *scep_dac* 之前，必須先編譯並安裝於核心。Dazuko 技術能夠使得任何使用的檔案系統類型都能夠進行常駐掃描。這也適合透過 Network File System (NFS)、Nettalk 及 Samba 掃描檔案系統物件。

重要 雖然我們針對常駐掃描器配置及使用提供詳細的資訊，不過必須注意，掃描器是主要針對保護外部裝載的檔案系統所開發和測試。如果有多個檔案系統並非外部裝載，則需要將這些檔案系統排除在檔案存取控制之外，以避免系統懸置。例如，*'/dev'* 目錄以及 SCEP 使用的任何目錄便是一般需要排除的目錄。

作業原則

即時防護 *scep_dac* (SCEP Dazuko-powered file Access Controller) 是持續監測和控制檔案系統的常駐程式。各個檔案系統物件均依據可自訂的檔案存取事件類型掃描。目前的版本支援下列事件類型：

開啟事件

若要啟動此檔案存取類型，請在 scep.cfg 檔的 **[fac]** 區段中，將 *'event_mask'* 參數的值設定為開啟。這將啟用 Dazuko 存取遮罩的 ON_OPEN 位元。

關閉事件

若要啟動此檔案存取類型，請在 scep.cfg 檔的 **[fac]** 區段中，將 *'event_mask'* 參數的值設定為關閉。這將啟用 Dazuko 存取遮罩的 ON_OPEN 位元。這將啟用 Dazuko 存取遮罩的 ON_CLOSE 及 ON_CLOSE_MODIFIED 位元。

附註： 某些作業系統核心版本不支援 ON_CLOSE 事件的攔截。在這些情況下，*scep_dac* 將不會監測關閉事件。

執行事件

若要啟動此檔案存取類型，請在 scep.cfg 檔的 **[fac]** 區段中，將 *'event_mask'* 參數的值設定為執行。這將啟用 Dazuko 存取遮罩的 ON_EXEC 位元。

即時防護可確保 *scep_daemon* 掃描所有已開啟、已關閉和已執行的檔案是否有病毒。是否拒絕或允許存取特定檔案端視掃描結果而定。

安裝及配置

Dazuko 核心模組必須先在執行核心中編譯及安裝，才能初始化 *scep_dac*。如需如何編譯和安裝 Dazuko 的詳細資訊，請參閱：

http://www.dazuko.org

一旦安裝 Dazuko，請檢視並編輯 SCEP 配置檔案 (scep.cfg) 中的 **[global]** 及 **[fac]** 區段。請注意，若要讓即時防護功能正確運作，則必須在此檔案的 **[fac]** 區段中配置 *['agent_type']* 選項。另外，您必須定義將由即時防護監視的檔案系統物件 (亦即目錄和檔案)。只要定義同樣位於 **[fac]** 區段內的 *'ctl_incl'* 及 *'ctl_excl'* 選項參數即可完成。變更 scep.cfg 檔之後，重新載入 SCEP Daemon 即可強制重新讀取新建立的配置。

提示

!

若要確保在 *scep_dac* Daemon 初始化之前載入 Dazuko 模組，請按照以下步驟進行：

將 Dazuko 模組放在下列為核心模組保留的目錄中：

```
/lib/modules
```

或

```
/modules
```

使用核心公用程式 'depmod' 及 'modprobe' (若為 BSD OS，則使用 'kldconfig' 及 'kldload') 處理相依性，並成功初始化新增的 Dazuko 模組。

在 scep_daemon 初始化指令碼 '/etc/init.d/scep_daemon' 中，將以下一行插入於 Daemon 初始化陳述式之前：

```
/sbin/modprobe dazuko
```

若為 BSD OS，該行

```
/sbin/kldconfig dazuko
```

必須插入於 '/usr/local/etc/rc.d/scep_daemon.sh' 指令碼中。

警告 這些步驟必須按照確切的指定順序進行。如果核心模組不在核心模組目錄中，將無法正確載入，這將導致系統懸置。

使用預載 LIBC 程式庫的即時防護

先前小節已說明 Dazuko 提供的即時保護與 Linux/BSD 檔案系統服務兩者的整合。可能並非所有情況下都能夠使用 Dazuko，包括維護以下重大的系統：

- 沒有與執行核心相關的來源程式碼及 *或*配置檔案、
- 核心為整合型而非模組式、
- Dazuko 模組不支援指定的作業系統。

在上述任何情況下，都應該使用以預載 LIBC 程式庫為依據的常駐掃描技術。如需更多資訊，請參閱本節中以下的主題。請注意，本節僅與 Linux OS 使用者有關，其中包含使用預載程式庫 *'libscep_pac.so'* 的常駐掃描器相關的操作、安裝及配置等資訊。

作業原則

即時防護 *libscep_pac.so* (SCEP Preload library based file Access Controller) 是系統啟動時啟動的共用物件程式庫。此程式庫用於系統伺服器的 LIBC 呼叫，例如 FTP 伺服器、Samba 伺服器等。各個檔案系統物件均依據可自訂的檔案存取事件類型掃描。目前的版本支援下列事件類型：

開啟事件

如果 *'open'* 這個字出現在 esest.cfg 檔的 *'event_mask'* 參數 (**[fac]** 區段) 中，將啟動此檔案存取類型。

關閉事件

如果 *'close'* 這個字出現在 scep.cfg 檔的 *'event_mask'* 參數 (**[fac]** 區段) 中，將啟動此檔案存取類型。在此情況下，將攔截 LIBC 所有的檔案描述元和 FILE 串流關閉函數。

執行事件

如果 *'exec'* 這個字出現在 scep.cfg 的 *'event_mask'* 參數 (**[fac]** 區段) 中，將啟動此檔案存取類型。在此情況下，將攔截 LIBC 所有的 exec 函數。

SCEP Daemon 可掃描所有已開啟、已關閉和已執行的檔案是否有病毒。是否拒絕或允許存取特定檔案端視這類掃描結果而定。

安裝及配置

使用預載程式庫的標準安裝機制，即可安裝 *libscep_pac.so* 程式庫模組。您需要以 *libscep_pac.so* 程式庫的絕對路徑定義環境變數 *'LD_PRELOAD'*。如需更多詳細資訊，請參閱 *ld.so(8)* 手冊頁面。

附註： 必須僅針對將受即時防護控制的網路伺服器 Daemon 處理程序 (ftp、Samba 等) 定義 *'LD_PRELOAD'* 環境變數。一般而言，不建議預載所有作業系統處理程序的 LIBC 呼叫，因為這會造成系統效能嚴重緩慢，甚至造成系統懸置。在此情況下，不應使用 '/etc/ld.so.preload' 檔案，也不應全域匯出 'LD_PRELOAD' 環境變數。這兩者將複寫所有相關的 LIBC 呼叫，而導致系統在初始化期間懸置。

若要確保僅攔截指定的檔案系統內相關的檔案存取呼叫，可使用以下一行覆寫可執行的陳述式。

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

其中 'COMMAND COMMAND-ARGUMENTS' 是原始可執行的陳述式。

請檢視並編輯 SCEP 配置檔案 (scep.cfg) 中的 **[global]** 及 **[fac]** 區段。為了使常駐掃描器正常運作，您必須定義需要受預載程式庫控制的檔案系統物件 (亦即目錄和檔案)。只要定義 SCEP 配置檔案 **[fac]** 區段內的 *'ctl_incl'* 及 *'ctl_excl'* 選項參數即可完成。變更 scep.cfg 檔之後，重新載入 SCEP Daemon 即可強制重新讀取新建立的配置。

提示

為了在檔案系統啟動之後立即啟動即時防護，必須在適當的網路檔案伺服器初始化指令碼中定義 *'LD_PRELOAD'* 環境變數。

範例 假設我們想要在啟動 Samba 伺服器後立即使用常駐掃描器監視所有的檔案系統存取事件。在 Samba Daemon 初始化指令碼 (/etc/init.d/smb) 中，將陳述式

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

取代為以下一行：

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

藉於此方式，將在系統啟動時掃描由 Samba 控制的所選檔案系統物件。

重要的 SCEP 機制

處理物件原則

「處理物件原則」機制可根據物件的狀態過濾已掃描的物件。此功能係以下列配置選項為基礎：

- action_av
- action_av_infected
- action_av_notscanned
- action_av_deleted

如需這些選項的更多詳細資訊，請參閱 *scep.cfg(5)* 手冊頁面。

首先會根據 *'action_av'* 選項處理各個已處理的物件。如果此選項是設定為 *'accept'* (或 *'defer'*？ *'discard'*？ *'reject'*)，將接受 (或延遲、放棄、拒絕) 物件。如果選項式設定為 *'scan'*，將掃描物件是否遭受病毒入侵，如果 *'av_clean_mode'* 選項是設定為 *'yes'*，也將清除物件。此外，將考量配置選項 *'action_av_infected'*？ *'action_av_notscanned'* 及 *'action_av_deleted'*，以進一步評估物件處置。如果已將 *'accept'* 動作視為這三個動作選項的結果，將接受物件，否則將封鎖物件。

使用者特定配置

使用者特定配置機制的用途是提供更高層次的自訂與功能。這允許系統管理員依據存取檔案系統物件的使用者定義 SCEP 防毒掃描器參數。

在 *scep.cfg(5)* 手冊頁面可找到此功能的詳細說明。本小節將提供使用者特定配置的簡短範例。

此範例的目的是使用 *scep_dac* 模組針對 /home 目錄下裝載的外接式磁碟控制 ON_OPEN 及 ON_EXEC 存取事件。在 SCEP 配置檔案的 **[fac]** 區段中可設定該模組。請參閱以下項目：

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

若要指定個別使用者的掃描指定，*'user_config'* 參數必須指定將儲存個別掃描規則的特別配置檔案名稱。在這裡顯示的範例中，特別的配置檔案稱為 *'scep_dac_spec.cfg'*，並且位於 SCEP 配置目錄內 (此目錄以您的作業系統為依據)。請參閱術語及縮寫頁面)。

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

一旦在 **[fac]** 區段中指定 *'user_config'* 檔案參數，則必須在 SCEP 配置目錄中建立 *'scep_dac_spec.cfg'* 檔案。最後，新增所需的掃描規則。

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

在特別區段的頂端，輸入將套用個別規則的使用者名稱。此配置將允許正常處理嘗試存取檔案系統的其他所有使用者，也就是將掃描其他使用者存取的所有檔案系統物件是否遭入侵，但不包括將拒絕 (封鎖) 存取的使用者*「使用者名稱」*。

排程器

排程器的功能包括在指定時間或特定事件執行排程工作、使用預先定義的配置與屬性管理及啟動工作等。工作配置及屬性可用來影響啟動的日期及時間，也可以用來在工作執行時使用自訂設定檔來擴大工作的應用。

'scheduler_tasks' 選項預設為有註解，這會套用預設的排程器配置。在 SCEP 配置檔案中，所有參數及工作均以分號分隔。其他任何分號 (以及反斜線) 必須加上反斜線逸出。各個工作都有 6 個參數，語法如下：

- id - 唯一編號。
- name - 工作說明。
- flag - 可在此設定停用指定排程器工作的特殊旗標。
- failstart - 指示如何處理無法在排程日期執行工作的情況。
- datespec - 有 6 (如 crontab 全年排程) 個欄位的一般日期規格、循環日期或事件名稱選項。
- command - 可為命令的絕對路徑，後面加上標示 @' 前置詞的引數或特殊命令名稱 (例如防毒更新： *@update*).

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

下列事件名稱可用於取代 datespec 選項：

- start - Daemon 啟動。
- startonce - Daemon 啟動，但是一天最多一次。
- engine - 成功引擎更新。
- login - Web 介面登入啟動。
- threat - 偵測到威脅。
- notscanned - 無已掃描的檔案。

若要顯示目前的排程器配置，請使用 Web 介面或執行下列命令：

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

如需排程器及其參數的完整說明，請參閱 *scep_daemon(8)* 手冊頁面的排程器一節。

Web 介面

Web 介面可方便進行 SCEP 安全系統的配置及管理。此模組是個別的代理程式，必須另行啟用。若要快速配置 *Web 介面*，請在 SCEP 配置檔案中設定下列選項，並重新啟動 SCEP Daemon：

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

將斜體的文字更換為您自己的值，並且將瀏覽器導向至 *'https://位址:連接埠'* (請注意是 https)。以*「使用者名稱/密碼」*登入。在說明頁面可找到基本使用指示，在 *scep_wwwi(1)* 手冊頁面可找到 *scep_wwwi* 的說明頁面及技術詳細資料。

Web 介面可讓您遠端存取 SCEP Daemon 並輕鬆部署。這個強大的公用程式可用來讀取和寫入配置值。

圖 6-1. System Center Endpoint Protection - 首頁畫面。

System Center Endpoint Protection 的 Web 介面視窗分為兩個主要區段。顯示所選功能表選項及主要功能表內容的主要視窗。頂端的水平列可讓您瀏覽以下的主要選項：

- **首頁** - 提供基本的系統及 Microsoft 產品資訊
- **配置** - 您可以在這裡變更 System Center Endpoint Protection 系統配置
- **控制項** - 讓您執行簡單的工作，並檢視 scep_daemon 處理的物件的相關 全域統計
- **Help** - 提供 System Center Endpoint Protection Web 介面的詳細使用指示
- **登出** - 用來結束目前的工作階段

重要： 在 Web 介面的 **[配置]** 區段中進行任何變更之後，務必按一下 **[儲存變更]** 按鈕，以儲存新設定。若要套用設定，需要按一下左窗格的 **[套用變更]**，重新啟動 SCEP Daemon。

即時防護配置範例

有兩種方法可以配置 SCEP。我們的範例將示範如何按照使用預載 LIBC 程式庫的即時防護一章所述，使用這些方法設定「存取控制器」模組。您可以選擇最適合您的選項。

- 使用 SCEP 配置檔案：

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

- 使用 Web 介面：

圖 6-3. SCEP - [配置] > [常駐掃描器]。

在 Web 介面中變更設定時，務必按一下 **[儲存變更]** 儲存配置。若要套用新變更，請按一下 **[配置]** 區段面板中的 **[套用變更]** 按鈕。

指定掃描器

本小節提供如何執行指定掃描器掃描病毒的範例：

- 瀏覽至 **[控制項] > [指定掃描]**
- 輸入要掃描的目錄路徑
- 按一下 **[掃描檔案]** 按鈕，執行命令列掃描器

圖 6-4. SCEP - [控制項] > [指定掃描器]。

Microsoft 命令列掃描器將在背景自動執行。若要檢視掃描進度，請按一下 **[檢視]** 連結。新的瀏覽器視窗隨即開啟。

排程器

您可以透過 SCEP 配置檔案 (請參閱排程器一章) 或使用 Web 介面管理排程器工作。

圖 6-5. SCEP - [全域] > [排程器]。

按一下該核取方塊即可啟用 /停用排程的工作。依預設，將顯示下列已排程的工作：

- **防護記錄維護** - 程式會自動刪除較舊的防護記錄以節省硬碟空間。排程器將開始重組防護記錄。所有空白的防護記錄將在此處理程序中移除。這將提升處理防護記錄的速度。如果防護記錄包含許多項目，則可更明顯察覺提升效果。
- **啟動檔案檢查** - 成功更新病毒資料庫後，掃描記憶體及執行中的服務。
- **每週掃描** - 每星期掃描整個檔案系統一次 (預設時間為星期一上午 2:00)。使用者能自訂此項工作。
- **定期自動更新** - 定期更新 System Center Endpoint Protection 是維持電腦最高等級安全性的最佳方法。如需更多資訊，請參閱 SCEP 更新公用程式。
- **威脅通知** - 各個威脅預設將記錄於系統日誌。此外，SCEP 可配置為執行外部 (通知) 指令碼，透過電子郵件將威脅偵測通知系統管理員。

統計

您可以在這裡檢視所有作用中 SCEP 代理程式的統計。**[統計]** 摘要每 10 秒重新整理一次。

圖 6-6. SCEP - [控制] > [統計]。

記錄

：

SCEP 透過 syslog 提供系統 Daemon 記錄。*Syslog* 是標準的記錄程式訊息，可用來記錄網路及安全事件之類的系統事件。

訊息指的是某個設備：

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

訊息由訊息的寄件者指派優先順序 層級：

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

本小節說明如何配置和讀取系統日誌的記錄輸出。*'syslog_facility'* 選項 (預設值 *'daemon*) 定義用於記錄的系統日誌設備。若要修改系統日誌設定，請編輯 SCEP 配置檔案，或使用 Web 介面。修改 *'syslog_class'* 參數的值即可變更記錄等級。建議只有在熟悉系統日誌的前提下修改這些設定。系統日誌配置的範例如下所示：

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

防護記錄檔案的名稱及位置端視系統日誌安裝及配置而定 (例如 rsyslog、syslog-ng 等)。例如，syslog 輸出檔案的標準檔案名稱可為 *'syslog*? *'daemon.log'* 等。若要追蹤系統日誌活動，請從主控台執行下列任一個命令：

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

重要 必須先在 SCEP 配置檔案或透過 SCEP Web 介面啟用使用 System Center Operations Manager 監視 Linux SCEP 產品，監視動作才能正常運作。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。

SCEP 安全性系統更新

SCEP 更新公用程式

為維持 System Center Endpoint Protection 的效率，病毒資料庫必須保持最新狀態。*scep_update* 公用程式專用此目的而開發。如需詳情，請參閱 *scep_update(8)* 手冊頁面。伺服器透過 HTTP Proxy 存取網路時，必須定義其他的配置選項 *'proxy_addr*? *'proxy_port'*。如果存取 HTTP Proxy 需要使用者名稱及密碼，也必須在此區段中定義 *'proxy_username'* 及 *'proxy_password'* 選項。若要開始更新，請輸入下列命令：

@SBINDIR@/scep_update

為提供使用者最高的安全性，Microsoft 團隊持續收集來自全世界的病毒定義，在極短的時間內將新模式加入病毒資料庫中。因此，建議務必定期進行更新。若要指定更新的頻率，需要在 SCEP 配置檔案 **[global]** 區段的 *'scheduler_tasks'* 選項中配置 *'@update'* 工作。您也可以使用排程器設定更新頻率。SCEP Daemon 必須啟動並執行，才能成功更新病毒資料庫。

SCEP 更新程序說明

更新程序分為兩個階段：首先，從 Microsoft 伺服器下載預先編輯的更新模組。

更新程序的第二個階段是編譯可由 System Center Endpoint Protection 掃描器從儲存在本機映像中的模組所載入的模組。一般而言，將建立以下的 SCEP 載入模組：載入器模組 (em000.dat)、掃描器模組 (em001.dat)、病毒資料庫模組 (em002.dat)、壓縮檔支援模組 (em003.dat)、進階探索法模組 (em004.dat) 等。程式將在以下目錄中建立模組：

@BASEDIR@

告訴我們

我們希望本手冊能夠讓您充分瞭解 System Center Endpoint Protection 安裝、配置及維護的需求。不過，我們的目標是持續提升我們文件的品質及效率。如果您認為本手冊的任何小節不明確或不完整，請連絡客戶關懷讓我們知道：

support.microsoft.com

我們致力於提供最高層級的支援，並期盼在您遭遇關於本產品的任何問題時協助您。

附錄 A. PHP 授權

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

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

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

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