TREND MICRO™

3.3

趨勢科技™

主動式雲端截毒技術伺服器

安裝和升級手冊

讓安全更具智慧

Endpoint Security

Messaging Security

Protected Cloud

Web Security

文件編號：APTM8055/171002

發行日期：2017 年 10 月

受美國專利保護，專利編號： 等待獲得專利中。

本文件介紹了產品/服務的主要功能，並/或提供作業環境的安裝說明。在安裝或使用本產品/服務前，請先閱讀此文件。

如需有關如何使用產品/服務特定功能的詳細資訊，請參閱趨勢科技線上說明中心和/或趨勢科技常見問題集。

趨勢科技十分重視文件品質的提升。如果您對於本文件或其他趨勢科技文件有任何問題、意見或建議，請與我們聯絡，電子郵件信箱為 docs@trendmicro.com。

請至下列網站並給予您對此文件的評估意見：

http://www.trendmicro.com/download/documentation/rating.asp

目錄

序言

第 1 章：規劃主動式雲端截毒技術伺服器的安裝和升級

第 2 章：安裝主動式雲端截毒技術伺服器

第 3 章：安裝後的工作

第 4 章：技術支援

序言

序言

歡迎使用《主動式雲端截毒技術伺服器™安裝和升級手冊》。本文件包含產品設定的相關資訊。

包含下列主題：

關於趨勢科技™

趨勢科技提供病毒防護、垃圾郵件防護以及內容過濾安全防護軟體與服務。趨勢科技可協助全球客戶遏止惡意程式碼傷害其電腦。

產品文件

主動式雲端截毒技術伺服器文件包含：

文件	說明
安裝和升級手冊	協助您進行安裝、升級和部署的規劃。
管理手冊	協助您設定所有產品設定。
線上說明	提供有關每個欄位以及如何透過使用者介面設定所有功能的詳細指示。
Readme 檔	包含其他文件中可能未提供的最新發表產品資訊。其中的主題包括功能的說明、安裝祕訣、已知問題和產品發行歷史記錄。

您可以在下列網址取得此文件：

http://downloadcenter.trendmicro.com/?regs=TW

讀者

主動式雲端截毒技術伺服器文件是專為 IT 管理員和系統管理員所撰寫。本文件假設讀者已具備深入的電腦網路知識。

本文件並不假設讀者具備任何病毒/惡意程式防範或垃圾郵件防範技術的知識。

文件慣例

《主動式雲端截毒技術伺服器使用者手冊》使用下列慣例。

表 1. 文件慣例

慣例	說明
全部大寫	頭字語、縮寫、特定的命令名稱和鍵盤上的按鍵
粗體	功能表和功能表命令、命令按鈕、標籤和選項
瀏覽 > 路徑	可達到特定畫面的瀏覽路徑 例如，「檔案 > 儲存」代表按一下「檔案」，然後按一下介面上的「儲存」
 注意	組態設定注意事項
 秘訣	推薦或建議
 警告!	重要的處理行動和組態設定選項

第 1 章

規劃主動式雲端截毒技術伺服器的安裝和升級

本章包含有關規劃主動式雲端截毒技術伺服器全新安裝或升級的資訊。

包含下列主題：

系統需求

下表列出系統需求：

表 1-1. 系統需求

硬體/軟體	需求
硬體	• 2.0GHz Intel™ Core2 Duo™ 64 位元處理器（支援 Intel™ 虛擬化技術™），或同等級處理器 • 2GB 的 RAM（趨勢科技建議配置 4GB） • 在虛擬機器上安裝時需要 50 GB 磁碟空間 注意 主動式雲端截毒技術伺服器會自動視情況需要，分割偵測到的磁碟空間。 注意 如果主動式雲端截毒技術伺服器偵測到可用的磁碟空間少於 1GB，「封鎖的 URL」就會停止收集資料。當管理員釋出至少 1.5GB 的可用磁碟空間時，主動式雲端截毒技術伺服器便會再次開始收集資料。 • 1024 x 768 解析度（256 色）以上的顯示器

硬體/軟體	需求
虛擬化	• Microsoft™ Windows Server™ 2008 R2 Hyper-V™ • Microsoft™ Windows Server™ 2012 Hyper-V™ • Microsoft™ Windows Server™ 2012 R2 Hyper-V™ • Microsoft™ Windows Server™ 2016 Hyper-V™ • VMware™ ESXi™ Server 6.5、6.0 Update 2、5.5 Update 3b • Citrix™ XenServer™ 7.2, 7.1, 6.5 注意 如果使用 Citrix™ XenServer，請使用「其他安裝媒體」範本建立新的虛擬機器。 注意 主動式雲端截毒技術伺服器隨附專門符合其用途、已強化且已經過效能調校的 64 位元 Linux 作業系統。
虛擬機器	• CentOS 7 64 位元或 CentOS 64 位元 • 為虛擬機器配置至少 2GB 的 RAM。趨勢科技建議您配置 4GB。 • 2.0GHz 處理器 • 至少 2 個虛擬處理器（建議使用 4 個虛擬處理器） • 50GB 磁碟空間 • 1 個網路裝置 • 網路裝置 注意 主動式雲端截毒技術伺服器核心模組將安裝 VMWare Tools 模組 vmxnet3。這代表安裝主動式雲端截毒技術伺服器後，並不需要再安裝 VMWare Tools。 如果您在安裝期間選擇 vmxnet3 NIC，可能會出現訊息「不符合最低硬體需求」，因為當時尚未安裝 vmxnet3 驅動程式。此訊息可予以忽略，安裝會正常繼續進行。

硬體/軟體	需求
Web 主控台	• Microsoft Edge™ • Microsoft™ Internet Explorer™ 11 • Mozilla™ Firefox™ 3.6.0 或更新版本 • 需要 Adobe™ Flash™ Player 8.0 或更新版本，才能檢視 Widget 中的圖表 • 1024 x 768 或更高解析度（256 色或以上） • Google Chrome™

部署規劃

下一節提供有關如何在安裝本機主動式雲端截毒技術伺服器電腦時判斷所要設定環境類型的資訊。

最佳做法

- 避免同時執行手動掃瞄和預約掃瞄。以群組方式交錯進行掃瞄。
- 避免將所有端點都設為同時執行「立即掃瞄」（例如：「更新後執行立即掃瞄」選項）。
- 請安裝多部主動式雲端截毒技術伺服器電腦，以防萬一與某個主動式雲端截毒技術伺服器的連線無法使用時，還是能夠繼續提供防護。
- 透過變更 `ptngrowth.ini` 檔案，自訂主動式雲端截毒技術伺服器以進行較慢的網路連線（約 512Kbps）。

設定 ptngrowth.ini 檔案

程序

1. 開啟 /var/tmcss/conf/ 中的 ptngrowth.ini 檔案。
2. 使用以下的建議值，修改 ptngrowth.ini 檔案：

```
[COOLDOWN]
ENABLE=1
MAX_UPDATE_CONNECTION=1
UPDATE_WAIT_SECOND=360
```

3. 儲存 ptngrowth.ini 檔案。
4. 透過在命令列介面 (CLI) 中輸入以下命令，重新啟動 lighttpd 服務：

```
systemctl restart lighttpd
```

部署指導方針

在設定本機主動式雲端截毒技術伺服器時，請考量下列事項：

- 主動式雲端截毒技術伺服器是一種 CPU-bound 應用程式。這表示增加 CPU 資源就可增加同時處理的要求數目。
- 視網路基礎結構和同時的更新要求或連線數目而定，網路頻寬可能會變成瓶頸。
- 如果主動式雲端截毒技術伺服器電腦和端點之間會有大量的同時連線，則可能需要有更多記憶體。

安裝準備工作

主動式雲端截毒技術伺服器安裝程序會格式化您現有的系統以便安裝程式。對於 VMware 或 Hyper-V 安裝，必須在安裝之前先建立虛擬機器。在決定要在網

路中使用主動式雲端截毒技術伺服器電腦的數目之後，便可開始進行安裝程序。

秘訣

請安裝多部主動式雲端截毒技術伺服器電腦，以防萬一與某個主動式雲端截毒技術伺服器的連線無法使用時，還是能夠繼續提供防護。

安裝時需要下列資訊：

- 代理伺服器資訊
- 可滿足您網路需求的虛擬機器伺服器

第 2 章

安裝主動式雲端截毒技術伺服器

本章包含有關升級和安裝主動式雲端截毒技術伺服器的資訊。

包含下列主題：

執行全新安裝

在備妥安裝需求之後，請執行安裝程式以開始安裝。

安裝主動式雲端截毒技術伺服器

本頁說明主動式雲端截毒技術伺服器的安裝程序。

注意

主動式雲端截毒技術伺服器 3.1 的使用者可透過命令列移轉工具，將預先設定的設定移轉至主動式雲端截毒技術伺服器 3.3。

如需開始移轉所需的先決條件的完整清單，請參閱移轉設定先決條件 第 A-2 頁。如需詳細資訊，請參閱從主動式雲端截毒技術伺服器 3.1 移轉設定 第 A-2 頁。

程序

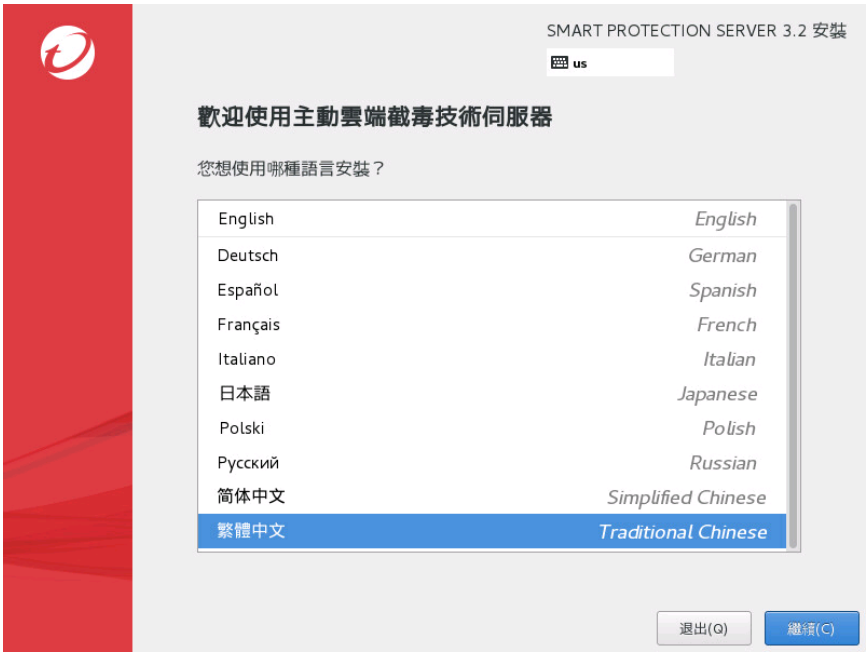
1. 在您的 VMware 或 Hyper-V 伺服器上建立虛擬機器，並指定要從主動式雲端截毒技術伺服器 ISO 映像將虛擬機器開機。

   注意

   如需詳細資訊，請參閱系統需求 第 1-2 頁中的「虛擬機器」章節。

2. 開啟虛擬機器電源。

「歡迎使用主動式雲端截毒技術伺服器」畫面隨即出現。



3. 選取此次安裝的主動式雲端截毒技術伺服器要使用的語言。
4. 按一下「繼續」。

「趨勢科技主動式雲端截毒技術伺服器授權合約」畫面隨即出現。

5. 按一下「接受」以同意條款和條件。

「安裝摘要」畫面隨即出現。

6. 按一下「日期和時間」以確認您的日期和時間設定。
   a. 若要將日期和時間設定與網路同步處理，請啟動「網路時間」。
   b. 若要自訂日期和時間，請從下拉式清單中選取您的「地區」和「城市」，或者在地圖上按一下您的地區。
   c. 按一下「完成」。
7. 按一下「網路和主機名稱」來驗證您的網路配接卡設定。

注意

如果要在安裝之後變更開機時變作用中的裝置，請登入「命令列介面」(CLI)。

如果有多個網路裝置，請針對所有裝置進行設定

---

a. 如果您的環境需要進階網路設定，請按一下「設定...」。

注意

「設定...」按鈕可讓您設定 IPv4 和 IPv6 設定。IPv4 的預設設定是「動態 IP 設定 (DHCP)」。IPv6 的預設設定是「自動發現鄰近機器」。

b. 按一下「完成」。

8. 按一下「安裝目標」以選取安裝磁碟。

a. 從「本機標準磁碟」區段中，選取虛擬磁碟。

b. 按一下「完成」。

9. 按一下「Root 密碼」以建立以下密碼：

- 「Root 密碼」：建立 root 帳號的密碼。

  root 帳號可用來存取作業系統 Shell，並具有伺服器的所有權限。此帳號包含最大權限。

- 「Admin 密碼」：建立 admin 帳號的密碼。

  admin 帳號為預設管理帳號，可用來存取主動式雲端截毒技術伺服器 Web 和 CLI 產品主控台。此帳號包含主動式雲端截毒技術伺服器應用程式的所有權限，但是不包含作業系統 Shell 的存取權。

注意

密碼長度必須最少為 6 個字元且最多為 32 個字元。如果要設計一個安全的密碼，請考慮下列作法：

- 同時包含字母和數字
- 避免在（任何語言的）字典中找得到的單字
- 故意拼錯單字
- 使用片語或組合字
- 使用大小寫字母的組合
- 使用符號

a. 按一下「完成」。

10. 按一下「開始安裝」。

警告!

如果繼續安裝，將會格式化並分割所需的磁碟空間，並且安裝作業系統和應用程式。如果硬碟上有任何必須保留的資料，請先取消安裝、備份這些資訊然後再繼續。

安裝隨即開始。在安裝完成後，系統會重新啟動。

注意

您可以在以下位置取得安裝記錄檔：

```
/root/install.log
```

11. 針對主動式雲端截毒技術伺服器 3.1 的使用者，請使用命令列移轉工具，將預先設定的設定移轉至主動式雲端截毒技術伺服器 3.3。

> **注意**
>
> 如需詳細資訊，請參閱從主動式雲端截毒技術伺服器 3.1 移轉設定 第 A-2 頁。

12. 登入主動式雲端截毒技術伺服器 Web 主控台以執行安裝後的工作（例如，設定 Proxy 設定）。如果您需要執行其他組態設定、疑難排解或維護工作，請登入主動式雲端截毒技術伺服器 CLI Shell。

> **注意**
>
> 使用 `root` 帳號以利用完整權限登入作業系統 Shell。

13. 執行安裝後的工作。

> **注意**
>
> 如需詳細資訊，請參閱安裝後的工作 第 3-1 頁。

升級

從主動式雲端截毒技術伺服器 3.2 升級至此版本的主動式雲端截毒技術伺服器。

表 2-1. 版本升級詳細資料

版本	需求
升級至主動式雲端截毒技術伺服器 3.3	• 在安裝之前，請確定符合系統需求。請參閱系統需求 第 1-2 頁。 • 主動式雲端截毒技術伺服器 3.2 • 請先清除瀏覽器的暫存 Internet 檔案，再登入 Web 主控台。

在升級過程中，會將 Web 服務關閉大約 5 分鐘。在這段時間內，端點無法將查詢傳送到主動式雲端截毒技術伺服器。趨勢科技建議在升級期間將端點重新導向到另一個主動式雲端截毒技術伺服器。如果您的網路中只安裝了一個主動式雲端截毒技術伺服器，趨勢科技建議您計劃在離峰時間進行升級。一旦與主動式雲端截毒技術伺服器的連線恢復，將立即記錄並掃瞄可疑檔案。

注意

SOCKS4 Proxy 伺服器組態設定已從主動式雲端截毒技術伺服器中移除。升級為此版本後，如果在舊版中針對 Proxy 伺服器設定已設定 SOCKS4，則必須重新設定 Proxy 伺服器設定。

升級主動式雲端截毒技術伺服器

程序

1. 登入 Web 主控台。
2. 按一下主功能表中的「更新」。

   下拉式功能表隨即出現。
3. 按一下「程式」。

   「程式」畫面隨即出現。
4. 在「上傳元件」下，按一下「瀏覽」。

   「選擇要上傳的檔案」畫面隨即出現。
5. 從「選擇要上傳的檔案」畫面中選取升級檔案。
6. 按一下「開啟」。

   「選擇要上傳的檔案」畫面隨即關閉，而檔案名稱會出現在「上傳程式套件」文字方塊。
7. 按一下「更新」。
8. 執行安裝後的工作。

請參閱安裝後的工作 第 3-1 頁

第 3 章

安裝後的工作

本章包含有關主動式雲端截毒技術伺服器安裝後工作的相關資訊。

包含下列主題：

安裝後

趨勢科技建議您執行下列安裝後工作：

- 如果您以最低系統需求來進行安裝，請使用您的 admin 帳號，從命令列介面 (CLI) 輸入下列命令，來關閉「封鎖的 Web 存取記錄檔」：

```
enable
disable adhoc-query
```

- 進行初始組態設定。請參閱初始組態設定 第 3-2 頁。
- 在其他支援雲端截毒掃瞄解決方案的趨勢科技產品上，進行主動式雲端截毒技術伺服器設定。

注意

「即時狀態」Widget 和主動式雲端截毒技術伺服器 CLI 主控台會顯示主動式雲端截毒技術伺服器的位址。

安裝主動式雲端截毒技術伺服器後，並不需要再安裝 VMWare Tools。伺服器核心模組已包含主動式雲端截毒技術伺服器所需的 VMWare Tools 模組 (vmxnet3)。

初始組態設定

安裝後請執行下列工作。

重要

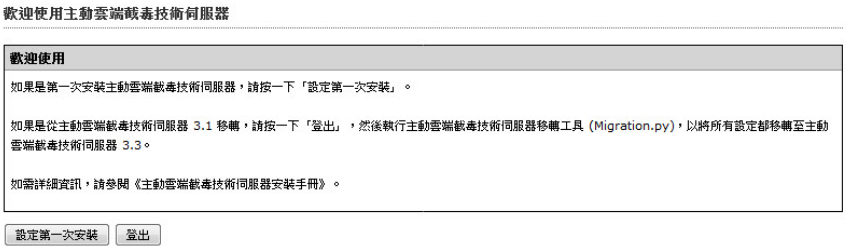
如果是從主動式雲端截毒技術伺服器 3.1 移轉，請先執行主動式雲端截毒技術伺服器移轉工具 (Migration.py) 將您所有設定移轉至主動式雲端截毒技術伺服器 3.3，然後再繼續。

如需詳細資訊，請參閱從主動式雲端截毒技術伺服器 3.1 移轉設定 第 A-2 頁。

程序

1. 登入 Web 主控台。

   「歡迎使用」畫面隨即出現。



2. 按一下「設定第一次安裝」。

   第一次安裝精靈隨即出現。

3. 選取「啟動檔案信譽評等服務」核取方塊。

4. 按「下一頁」。

   「網頁信譽評等服務」畫面隨即出現。

5. 選取「啟動網頁信譽評等服務」核取方塊。

6. （選用）過濾器優先順序設定可讓您指定 URL 查詢適用的過濾順序。

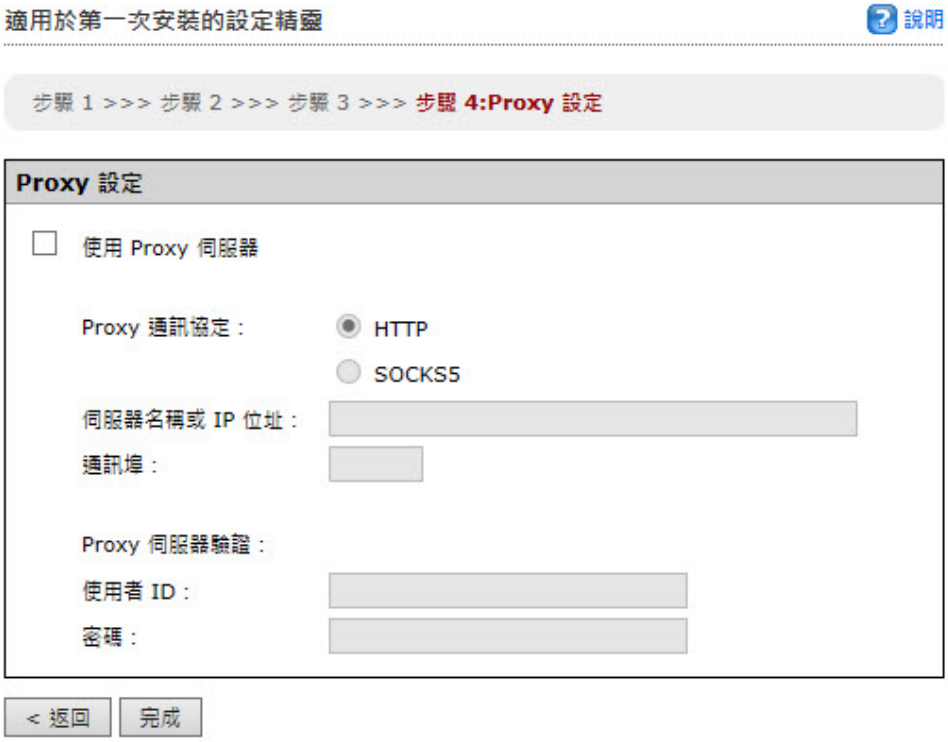
7. 按「下一頁」。

   「Smart Feedback」畫面隨即出現。

8. 選取以使用 Smart Feedback，協助趨勢科技針對新的安全威脅更快提供解決方案。

9. 按「下一頁」。

   「Proxy 設定」畫面隨即出現。



10. 如果您的網路使用 Proxy 伺服器，請指定 Proxy 伺服器設定。

11. 按一下「完成」，以完成主動式雲端截毒技術伺服器清單的初始組態設定。

    Web 主控台的「摘要」畫面隨即顯示。

> **注意**
>
> 主動式雲端截毒技術伺服器將會在初始組態設定之後，自動更新病毒碼檔案。

第 4 章

技術支援

瞭解下列主題：

疑難排解資源

聯絡技術支援之前，請考慮造訪下列趨勢科技線上資源。

使用支援入口網站

趨勢科技支援入口網站是全年無休的線上資源，包含有關常見和不常見問題的最新資訊。

程序

1. 移至 http://esupport.trendmicro.com/zh-tw/default.aspx。
2. 從可用產品中進行選取，或請點選適當的按鈕來搜尋解決方案。
3. 使用「搜尋支援」方塊搜尋可用的解決方案。
4. 如果未找到解決方案，請點選「聯絡支援」，然後選取所需的支援類型。

秘訣

若要線上提交支援案例，請造訪下列 URL：

https://esupport.trendmicro.com/zh-tw/srf/twbizmain.aspx

趨勢科技支援工程師會在 24 小時或更短時間內調查案例並對其進行回應。

安全威脅百科全書

現今的大多數惡意程式都包含混合安全威脅（合併了兩種或更多種技術），以略過電腦安全通訊協定。趨勢科技會使用建立自訂防範政策的產品來抵禦此複雜惡意程式。安全威脅百科全書提供了多種混合性安全威脅的名稱和癥狀的完整清單，包括已知惡意程式、垃圾郵件、惡意 URL 和已知弱點。

移至 http://about-threats.trendmicro.com/threatencyclopedia.aspx?language=tw&tab=malware 以瞭解更多資訊：

- 目前正在使用中或「擴散中」的惡意程式和惡意可攜式程式碼。
- 用於形成完整網頁攻擊過程的關聯安全威脅資訊頁面
- 有關目標攻擊和安全威脅的 Internet 安全威脅諮詢
- 網頁攻擊和線上趨勢資訊
- 每週惡意程式報告

聯絡趨勢科技

可以透過電話或電子郵件聯絡趨勢科技代表：

地址	趨勢科技股份有限公司 台北市敦化南路二段 198 號 8 樓
電話	(886) 2-23789666
網站	http://www.trendmicro.com
電子郵件信箱	企業授權用戶技術專線 Web mail：http://www.trend.com.tw/corpmail/

- 全球客戶服務據點：

  http://www.trendmicro.com/us/about-us/contact/index.html

- 與台灣趨勢科技聯絡：

  http://www.trendmicro.tw/tw/about-us/contact/index.html

- 趨勢科技產品文件：

  http://docs.trendmicro.com/zh-tw/home.aspx

加速支援要求

為了提高解決問題的速度，現已提供下列資訊：

- 問題模擬的步驟
- 裝置或網路資訊
- 電腦品牌、型號以及連接的任何其他硬體或裝置
- 記憶體大小和可用硬碟空間
- 作業系統和 Service Pack 版本
- 安裝的 Agent 版本
- 產品序號或啟動碼
- 安裝環境的詳細說明
- 已接收的任何錯誤訊息的確切文字

將可疑內容傳送到趨勢科技

有多個選項可供將可疑內容傳送到趨勢科技，以便進一步分析。

電子郵件信譽評等服務

查詢特定 IP 位址的信譽評等，並指定一個訊息轉移用戶端，以將其包含在全域例外清單中：

https://ers.trendmicro.com/

請參閱下列「常見問題集」項目，將訊息範例傳送給趨勢科技：

http://esupport.trendmicro.com/solution/zh-TW/1112106.aspx

檔案信譽評等服務

收集系統資訊並將可疑檔案內容提交到趨勢科技：

http://esupport.trendmicro.com/solution/zh-tw/1059565.aspx

記錄案例編號以供追蹤。

網頁信譽評等服務

查詢疑似網路釣魚網站的 URL 的安全分級和內容類型，或其他所謂「病媒」（間諜程式和惡意程式等 Internet 威脅的蓄意來源）：

http://global.sitesafety.trendmicro.com/

如果指定的分級不正確，請傳送重新分類要求到趨勢科技。

其他資源

除了解決方案和支援外，線上還提供許多其他實用資源，可讓您保持最新狀態、瞭解創新以及最新的安全趨勢。

下載專區

有時，趨勢科技可能會針對報告的已知問題發行修補程式，或是發行適用於特定產品或服務的升級。如果要瞭解是否有適用的修補程式，請移至：

http://downloadcenter.trendmicro.com/index.php?regs=tw

如果未套用修補程式（修補程式已過期），請開啟 Readme 檔以判斷其是否與您的環境相關。Readme 檔還包含安裝說明。

文件意見反應

趨勢科技始終力求改善其文件。如果您對本文件或趨勢科技的任何文件有任何疑問、意見或建議，請透過

docs@trendmicro.com 聯絡我們。

附錄 A

移轉設定

本章包含有關使用移轉工具從主動式雲端截毒技術伺服器 3.x 移轉設定的資訊。

包含下列主題：

移轉設定先決條件

主動式雲端截毒技術伺服器提供命令列移轉工具，此工具可讓您從主動式雲端截毒技術伺服器 3.1，將預先設定的設定移轉至最新版本。

重要

您只能在初始化主動式雲端截毒技術伺服器 3.3 之前移轉主動式雲端截毒技術伺服器舊版中的設定。在初始化主動式雲端截毒技術伺服器 3.3 之後，就無法再移轉設定，除非解除安裝並重新安裝伺服器。

以下是開始移轉所需的先決條件：

需求	說明
虛擬機器	• 主動式雲端截毒技術伺服器 3.3 需要虛擬機器執行個體，而且其規格至少要與欲從其中移轉設定的電腦規格相同。 • 在執行此工具之前，必須先在虛擬機器執行個體上安裝主動式雲端截毒技術伺服器 3.3 ISO。
SSH	您必須在主動式雲端截毒技術伺服器電腦（欲從其中移轉設定的電腦）上啟動 SSH。 如需詳細資訊，請參閱線上說明或管理手冊。
「可疑物件」同步處理	如果「可疑物件」同步處理已啟動，請確定新虛擬機器和「可疑物件」來源之間有正常運作的連線。

從主動式雲端截毒技術伺服器 3.1 移轉設定

主動式雲端截毒技術伺服器提供命令列移轉工具，此工具可讓您從主動式雲端截毒技術伺服器 3.1，將預先設定的設定移轉至最新版本。

重要

您只能在初始化主動式雲端截毒技術伺服器 3.3 之前移轉主動式雲端截毒技術伺服器舊版中的設定。在初始化主動式雲端截毒技術伺服器 3.3 之後，就無法再移轉設定，除非解除安裝並重新安裝伺服器。

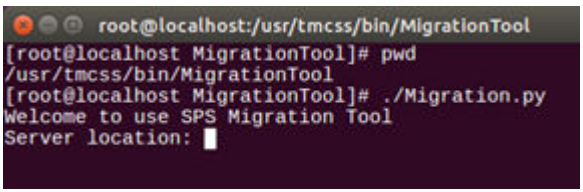
如需開始移轉所需的先決條件的完整清單，請參閱移轉設定先決條件 第 A-2 頁。

程序

1. 在主動式雲端截毒技術伺服器 3.3 虛擬機器上，使用 root 帳號認證開啟命令列。
2. 將工作目錄變更為 `/usr/tmcss/bin/MigrationTool`。
3. 使用以下命令執行移轉工具：

   ```
   #>./Migration.py
   ```

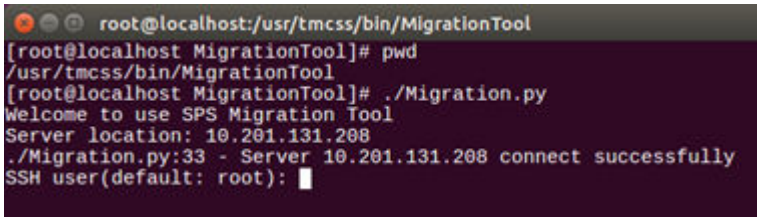
   移轉工具需要伺服器資訊。



4. 提供主動式雲端截毒技術伺服器電腦（欲從其中移轉設定的電腦）的「伺服器位置」。

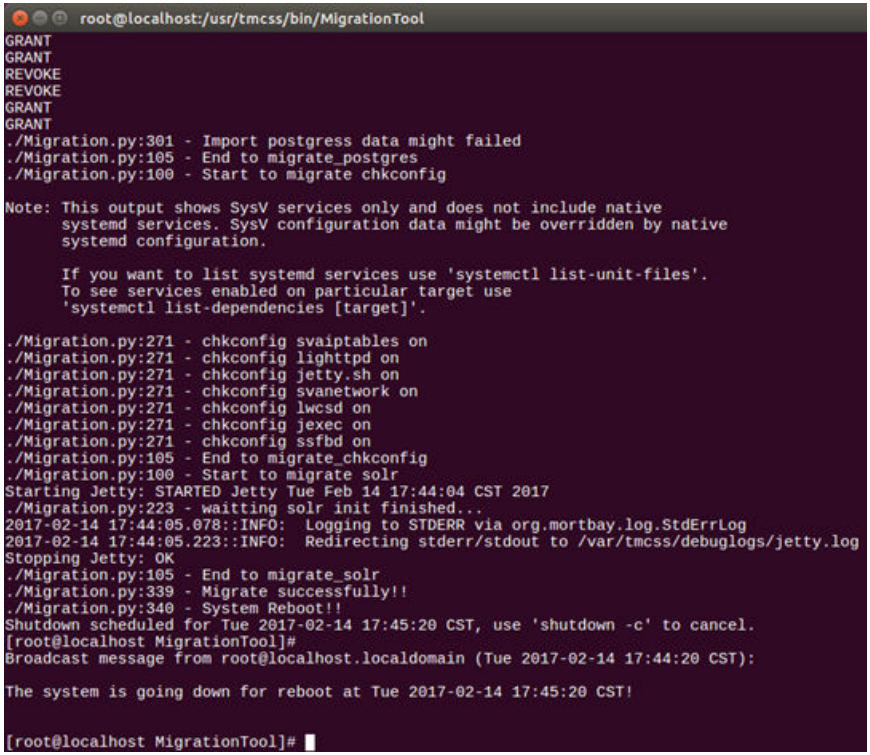
注意

「伺服器位置」支援 IP 位址或 FQDN 格式，並且會使用 SSH 連線嘗試驗證位置。



5. 若要從先前伺服器取得設定，請提供 root 帳號和密碼。

   移轉程序隨即開始。根據資料庫大小，完成移轉程序可能需要一些時間。在移轉程序成功完成後，主動式雲端截毒技術伺服器 3.3 會自動重新開機並套用已移轉的設定。



重要

如果執行移轉程序期間發生問題，主動式雲端截毒技術伺服器不會重新開機，並且會顯示錯誤訊息清單。您可以在以下位置取得移轉錯誤記錄檔：

```
/var/tmcss/debuglogs/SPSMigration.log
```

6. 使用 admin 帳號開啟主動式雲端截毒技術伺服器 3.3 主控台，然後驗證已移轉的設定。

   - 檢查檔案信譽評等服務和網頁信譽評等服務的病毒碼狀態：

     a. 移至「更新 > 病毒碼」。

     b. 請確定「檔案信譽評等」和「網頁信譽評等」均設定正確。

     c. 如果錯誤關閉了病毒碼，請按一下「立即更新」來取得最新的病毒碼。

     注意

     如果更新失敗，請檢查您是否可以存取 Internet，以及您的 Proxy 伺服器設定是否正確（「管理 > Proxy 設定」）。

   - 透過移至「主動式雲端截毒技術 > 可疑物件」，檢查「同步處理並啟動可疑物件」是否設定正確。

     注意

     如果錯誤關閉了「同步處理並啟動可疑物件」，請確認沙盒虛擬平台來源的「來源」和「API 金鑰」資訊，然後按一下「訂閱」。

   - 在主動式雲端截毒技術伺服器 Web 主控台中檢查所有其他設定。

7. 如果先前的主動式雲端截毒技術伺服器 3.1 電腦需要憑證，則您必須重新匯入憑證。

   注意

   如需詳細資訊，請參閱《主動式雲端截毒技術伺服器管理手冊》。

8. 若要在主動式雲端截毒技術伺服器 3.3 主控台上繼續使用舊版主動式雲端截毒技術伺服器的相同 IP 位址，請關閉舊版的主動式雲端截毒技術伺服器。

索引

趨勢科技股份有限公司
台北市敦化南路二段 198 號 8 樓
電話：(886) 2-23789666　傳真：(886) 2-23780993　info@trendmicro.com
www.trendmicro.com

Item Code: APTM8055/171002