SOPHOS

simple + secure

Sophos Virtualization Scan Controller

操作指南

產品版本： 1.0
文件日期： 2011 年 7 月

目錄

1 關於本指南.....3

2 何謂虛擬掃描控制器？.....3

3 如何安裝虛擬掃描控制器?.....3

4 主要步驟爲何？.....4

5 安裝虛擬掃描控制器.....4

6 註冊虛擬掃描控制器.....4

7 建立配置檔.....5

8 套用配置.....9

9 開啓虛擬掃描控制器.....10

10 停止虛擬掃描控制器.....10

11 紀錄資訊.....10

12 排疑解難.....11

13 解除安裝虛擬掃描控制器.....11

14 附錄：使用分散式主控台安裝.....11

15 附錄：使用分散式主控台解除安裝.....13

16 技術支援.....13

17 法律聲明.....14

1 關於本指南

本指南描述如何安裝、使用 Sophos Enterprise Console 的虛擬掃描控制器附加元件工具。

本指南預設您已熟悉並已使用 Sophos Enterprise Console 4.0 以上。

Sophos 說明文件發佈於 http://tw.sophos.com/support/docs/。

2 何謂虛擬掃描控制器？

虛擬掃描控制器，係管理虛擬電腦排程掃描的工具。

您可使用此項工具，來確保不同電腦上的排程掃描依序進行，而非同時進行。如此能減低對您虛擬伺服器效能的影響。

此項工具：

- 可讓您使用單項配置檔管理掃描。
- 可讓您指定在下一部電腦上進行掃描前，一開始要允許在一部電腦上執行掃描多少時間。
- 依據前次掃描循環，來瞭解應許可每次掃描執行多少時間。
- 可讓您指定可對每部電腦進行掃描的頻率。

重要事項: 該項工具無法讓您指定要掃描的檔案或檔案類型。本版本產品總是以「完整掃描類型」來執行掃描。

3 如何安裝虛擬掃描控制器?

您可將虛擬掃描控制器與 Sophos Enterprise Console (SEC) 共同安裝。

要將虛擬掃描控制器安裝在哪一台電腦上，取決於您具有何種類型的 SEC 安裝。

如果您將所有的 SEC 元件安裝在單台伺服器上（「獨立」SEC)，請將虛擬掃描控制器安裝在該台伺服器上。

如果您在不同的伺服器上具有某些或所有 SEC 元件（「分散式」SEC)，請安裝以下項目：

- 在您安裝 Sophos 管理伺服器的電腦上安裝虛擬掃描控制器。
- 在您安裝 Sophos 管理資料庫的電腦上安裝虛擬掃描控制器。

本指南說明如何進行此兩種類型安裝。

4 主要步驟爲何？

如欲安裝、使用虛擬掃描控制器，請進行以下步驟：

- 安裝虛擬掃描控制器。
- 將虛擬掃描控制器註冊爲 Windows 服務 (選擇性)。
- 建立配置檔。
- 套用配置。
- 開啓虛擬掃描控制器。

此兩項策略詳述於以下章節。

5 安裝虛擬掃描控制器

重要事項: 請確保虛擬掃描控制器電腦與端點電腦上的時間一致。

本節假定您已在獨立電腦上安裝 Enterprise Console。

注意事項: 如果您有分散式安裝 (再不同的伺服器上安裝 Enterprise Console 元件)，請參閱 附錄：使用分散式主控台安裝 (第 11 頁)

如欲安裝虛擬掃描控制器：

1. 將虛擬掃描控制器檔案解壓縮至您安裝 Sophos Enterprise Console 的電腦上。
2. 開啓命令提示字元視窗，然後變更爲您解壓縮虛擬掃描控制器檔案目的地的目錄。
3. 輸入 **SavScanController install**，然後按「Enter」，開始進行安裝。

本公司建議您依照下節內容描述，將虛擬掃描控制器註冊爲 Windows 服務。

6 註冊虛擬掃描控制器

您可將虛擬掃描控制器註冊爲 Windows 服務。如果您進行此項操作，虛擬掃描控制器服務將：

- 在每次電腦啓動時，自動啓動。
- 在無需使用者登入的情況下執行。
- 自行紀錄活動。如欲瞭解登入的相關資訊，請參閱 紀錄資訊 (第 10 頁)。

如欲註冊爲 Windows 服務：

1. 前往您安裝 Sophos 管理伺服器的電腦。
   如果您在獨立電腦上進行安裝，此爲安裝 Enterprise Console 的電腦。
2. 輸入 **SavScanController register**，然後按「Enter」。
   服務將註冊爲 Sophos Scan Controller，並將配置爲以 Lcal System 執行。
3. 如果您安裝的 Enterprise Console 會防止 Local System 存取其管理主控台或資料庫，或如果您要限制服務的權限，請確保該服務能以其他使用者執行。如欲進行此項操作：
   a) 建立網域使用者帳號，來執行虛擬掃描控制器服務。請確保在網域的群組策略內具備 **登入圍服務** 權限。
   b) 如果您使用角色或子領域，請在 SEC 內編輯子領域，並爲在步驟 a 內建立的使用者帳號，提供對於整各子領域的完整權限。
   c) 將在步驟 a 內建立的使用者權限，新增至 **Sophos Console Administrators** 與 **Sophos DB Admins** 群組。
      在分散式 SEC 安裝的情況下，**Sophos Console Administrators** 群組位於您安裝 Sophos 管理伺服器的電腦上，而 **Sophos DB Admins** 群組則位於您安裝 Sophos 管理資料庫的電腦上。
   d) 請確保在步驟a內建立的使用者帳號具備對於虛擬掃描控制器檔安裝所在目錄資料夾的讀寫權限，以便寫入其日誌檔。
   e) 開啓 **控制台**，然後按兩下 **系統管理工具**。在服務的清單內，按兩下 **Sophos Scan Controller** 服務。在 **Sophos Scan Controller** 服務內容內，點選 **登入** 標籤，然後選取 **此帳號**。點選 **瀏覽**，然後選取在步驟 a 建立的使用者帳號。

7 建立配置檔

您必須在您已安裝 Sophos 管理伺服器的電腦上建立配置檔。

注意事項: 如果您在獨立電腦上進行安裝，此爲安裝 Enterprise Console 的電腦。

建立指定哪一部端點電腦應受虛擬掃描控制器控管的文字檔案。

該檔案應將電腦放置於數個清單內。一般來說，每項虛擬電腦主機皆有電腦清單。

以下爲範例配置檔的範例。以下範例定義兩項清單。此兩項清單目前使用預設設定。

```
[VM Host 1]
COMPUTERA
COMPUTERB
COMPUTERC

[VM Host 2]
COMPUTER1
COMPUTER2
COMPUTER3
...
...
COMPUTER12
```

以下內容告訴您如何：

- 使用 DNS 或 NetBIOS 名稱列出電腦。
- 指定如何執行掃描。

7.1 使用 DNS 或 NetBIOS 名稱列出電腦

當您在配置檔內輸入電腦名稱，您可使用以下這些名稱類型：

- NetBIOS 名稱。除非您另外指定，所有名稱皆可視爲 NetBIOS 名稱。
- DNS 名稱。

如果您要使用 DNS 名稱，您可另外個別指定每台電腦名稱，或者，如果您具有龐大數量的電腦，您可對檔案進行配置，使其將所有名稱是爲 DNS 檔案。

如欲指定個別 DNS 名稱，請使用以下項目：

```
[VM Host 1]
dns|computer.domain.name
```

如欲指定所有名稱皆爲 DNS 主機名稱，請將以下章節新增至配置檔開頭：

```
[defaults]
 Names=dns
```

注意事項: 如果您設定此項目，您無須使用「dns|」作爲其 DNS 主機名稱指定的電腦名稱的開頭，但您必須使用「netbios|」作爲作爲其 DNS 主機名稱指定的電腦名稱的開頭。

```
[VM Host 1]
netbios|COMPUTER
```

7.2 指定如何執行掃描

您可在配置檔內，爲每項電腦清單指定以下設定。

注意事項: 在配置檔內指定的任何時間，必須使用全球標準時間 (UTC) 24 小時時間格式。

秘訣: 您可在非工作環境內，測試虛擬掃描控制器的效能。編輯您的 Enterprise Console Anti-Virus 與 HIPS 策略，來排除資料夾，並使用 DefaultWaitHint 選項 (討論於此節內)，來減少允許的掃描時間。您可依據結果來決定最佳設定。

- **DefaultWaitHint**

  此項設定可讓您控制在下一部電腦上進行掃描前，要允許在一部電腦上執行掃描多少時間。該值以分設定。預設值爲 30 分鐘。此項設定適用於首次在電腦上執行的掃描。在首次執行掃描後，虛擬掃描控制器會使用前次掃描執行的資訊，來決定該允許多少時間進行掃描。

  範例：

```
[Group X]
DefaultWaitHint=40
COMPUTER1
COMPUTER2
COMPUTER3
```

- **MaxScanTime**

  此項設定可定義虛擬掃描控制器要讓掃描成功執行多久時間。該值以分設定。如果某項掃描耗時較久，虛擬掃描控制器便會預設該掃描已經終止，並會在其他電腦上開始進行掃描。預設值爲 180 分鐘。

  範例：

```
[Group X]
MaxScanTime=120
COMPUTER1
COMPUTER2
COMPUTER3
```

■ **MinTimeBeforeNext**

此項設定控管在清單內的每部電腦上進行掃描的頻率。此項設定的單位爲分鐘，您可藉此控管相同電腦上，兩次連續掃描之間允許的最少時間。預設值爲 1440 分鐘或 1 天。

MinTimeBeforeNext 的設定，應設爲大於清單內最長掃描時間長度的值。該設定亦須大於清單內 MaxScanTime 設定的值。

範例：

```
[Group X]
MinTimeBeforeNext=90
COMPUTER1
COMPUTER2
COMPUTER3
```

■ **MaxConcurrentScans**

此項設定可控管清單內，可同時執行掃描的電腦最大數量。預設值爲 1。

範例：

```
[Group X]
MaxConcurrentScans=3
MinTimeBeforeNext=90
ALPHA
BETA
GAMMA
```

■ **EarliestScanStart** 與 **LatestScanStart**

這些設定可控管允許掃描執行的時間。您必須使用全球標準時間 (UTC) 來設定時間。如果您要使用這些設定，您必須使用兩者。如果您僅使用一項，將無法套用設定。預設值爲允許掃描時間在每日的任何時間進行。

範例：

```
[Group X]
EarliestScanStart=04:00
LatestScanStart=23:30
```

■ **AllowedDays**

這些設定可控管一週內哪一天能執行掃描。此項值爲逗號分隔值的名稱清單。您可將以下任何值包括在清單內。

名稱	意義
Sun	星期天
Mon	星期一
Tue	星期二
Wed	星期三
Thu	星期四
Fri	星期五
Sat	星期六
WkE	週末 (與「Sat」、「Sun」相同)
WkD	非週末 (與「Mon」「Tue」「Wed」「Thu」「Fri」相同)

如果未指定此項設定，掃描可在一週的任何一天內執行。

範例：

```
[Group X]
AllowedDays=Mon,Wed,Fri
```

8 套用配置

如欲套用配置，請進行以下操作。

注意事項: 如果您之後更新配置，您必須每次重複進行此項程序。

1. 前往您安裝 Sophos 管理伺服器的電腦。
2. 開啓命令提示字元視窗，然後變更爲您具有虛擬掃描控制器檔案的目錄。
3. 輸入 **SavScanController configure <my configuration>**，此處的 <my configuration> 亦即您先前建立配置檔的名稱。然後請按「Enter」來套用配置。

   範例：SavScanController configure settings.txt

   如果您的配置檔列出未受 Enterprise Console 管理的電腦，或如果配置檔使用錯誤的句法進行配置選項。

接下來，您即可啓動虛擬掃描控制器。

9 開啓虛擬掃描控制器

在您啓動虛擬掃描控制器之前，請確保您已依 套用配置 (第 9 頁) 內的指示套用配置。

如欲開啓虛擬掃描控制器：

1. 如您已註冊爲 Windows 服務，請輸入 **SavScanController start**。否則，請輸入 **SavScanController run**

   按「Enter」開啓虛擬掃描控制器：

   注意事項: 如果您對配置進行變更，您無須停止、開啓服務，以使變更生效。

如果虛擬掃描控制器要求進行掃描，其運作方式與在 Enterprise Console 內選取對端點電腦進行「完整系統掃描」相同。用於完整系統掃描的設定，取決於套用何項防病毒與 HIPS 策略。使用的防病毒與 HIPS 設定如下：

- 許可。
- 及時掃描排除項目。
- 及時掃描副檔名。
- 所有其他的預設排程掃描選項。

10 停止虛擬掃描控制器

如欲停止虛擬掃描控制器：

1. 如您已註冊爲 Windows 服務，請輸入 **net stop SavScanController**。否則，請按 Ctrl+C。

11 紀錄資訊

在您執行虛擬掃描控制器時，會在命令提示字元視窗內通報活動。

如果您以 Windows 服務方式執行虛擬掃描控制器，會在 SavScanController.log 檔案內通報活動。紀錄檔將建立於具有 SavScanController.exe 檔的目錄內。

如果紀錄檔抵達其大小上限，該檔案便會重新命名爲 SavScanController.log.1、SavScanController.log 等。可儲存最多 4 個檔案。

12 排疑解難

您可使用診斷模式使用 SavScanController。「-d」指令行可開啓診斷紀錄資訊。該指令行可用於任何指令：

範例：

SavScanController -d register

SavScanController -d install

SavScanController start -d

13 解除安裝虛擬掃描控制器

解除安裝程序不會刪除 SEC 資料庫。解除安裝程序僅會恢復虛擬掃描控制器所進行的變更。

如果解除安裝虛擬掃描控制器，亦會解除安裝虛擬掃描控制器服務：

注意事項: 如果您只要將虛擬掃描控制器解除註冊 Windows 服務，您可使用 **SavScanController unregister** 指令。

本節假定您已在獨立電腦上安裝 Enterprise Console。

注意事項: 如果您有分散式安裝 (再不同的伺服器上安裝 Enterprise Console 元件)，請參閱 附錄：使用分散式主控台解除安裝 (第 13 頁)

如欲解除安裝虛擬掃描控制器：

1. 在您具有虛擬掃描控制器檔案的目錄資料夾，開啓命令提示字元視窗。
2. 確保虛擬掃描控制器未在您電腦上執行。
   如欲停止該項服務，如果您註冊爲 Windows 服務，請輸入 **net stop SavScanController**。否則，請按 Ctrl+C。
3. 輸入 **SavScanController uninstall**，然後按「Enter」。

14 附錄：使用分散式主控台安裝

重要事項: 請確保虛擬掃描控制器電腦與端點電腦上的時間一致。

本節假定您已安裝分散式 Enterprise Console。

注意事項: 如果您在獨立電腦上進行安裝 (所有 Enterprise Console 元件安裝在同一台伺服器上)，請參閱 安裝虛擬掃描控制器 (第 4 頁)。

安裝程序包括兩個步驟：

- 安裝服務。
- 安裝資料庫。

14.1 安裝服務

如欲安裝虛擬掃描控制器服務：

1. 在您安裝 Sophos 管理伺服器的電腦上解壓縮虛擬掃描控制器檔案。
2. 開啓命令提示字元視窗，然後變更爲您解壓縮虛擬掃描控制器檔案目的地的目錄。
3. 輸入 **SavScanController install**，然後按「Enter」。

   如此即可安裝此項服務。一項錯誤訊息會向您顯示，指示您現在需要在您安裝 Sophos 管理資料庫的電腦上，安裝虛擬掃描控制器資料庫。請記下訊息內顯示的 **資料庫伺服器** 與 **資料庫名稱**。

   錯誤：`Sophos Enterprise Console` 預設爲使用遠端資料庫。

   請參閱虛擬掃描控制器操作指南。

   您將需要以下資訊：

   資料庫伺服器：主機名稱\執行個體

   資料庫名稱：資料庫

14.2 安裝資料庫

如欲安裝虛擬掃描控制器資料庫：

1. 請前往您安裝Sophos管理資料庫的電腦，然後解壓縮虛擬掃描控制器檔案。
2. 開啓命令提示字元視窗，然後變更爲您解壓縮虛擬掃描控制器檔案目的地的目錄。
3. 輸入 **SavScanController install <Hostname>\<Instance> <Database>**。

   確保您在「*Hostname**Instance* and *Database*」輸入的值，與您在安裝 Sophos 管理伺服器的電腦上顯示的值相同 。

   按「Enter」，在資料庫建立虛擬掃描控制器需要的表格。

您現在應依照在獨立電腦上安裝Enterprise Console的相同方法，繼續設定虛擬掃描控制器。前往 註冊虛擬掃描控制器 (第 4 頁)

15 附錄：使用分散式主控台解除安裝

解除安裝程序不會刪除 SEC 資料庫。解除安裝程序僅會恢復虛擬掃描控制器所進行的變更。

如果解除安裝虛擬掃描控制器，亦會解除安裝虛擬掃描控制器服務：

注意事項: 如果您只要將虛擬掃描控制器解除註冊 Windows 服務，您可使用 **SavScanController unregister** 指令。

本節假定您已安裝分散式 Enterprise Console。

注意事項: 如果您在獨立電腦上安裝 Enterprise Console，請參閱 解除安裝虛擬掃描控制器 (第 11 頁)。

如欲解除安裝虛擬掃描控制器：

1. 在您安裝 Sophos 管理伺服器的電腦腦上，在您含有虛擬掃描控制器檔案的附錄資料夾開啓命令提示字元。
2. 確保虛擬掃描控制器未在您電腦上執行。
   如欲停止該項服務，如果您註冊爲 Windows 服務，請輸入 **net stop SavScanController**。否則，請按 Ctrl+C。
3. 輸入 **SavScanController uninstall**，然後按「Enter」。
4. 在您安裝 Sophos 管理資料夾的電腦上，開啓命令提示字元，然後輸入 **SavScanController uninstall <Hostname>\<Instance> <Database>**。
   「*Hostname**Instance*」與「*Database*」**的值必須與安裝程序使用的值相同**。

16 技術支援

您可使用以下其中一項方法，取得 Sophos 產品技術支援服務：

- 造訪 http://community.sophos.com/ 內的 SophosTalk 社群，尋找其他遭遇到相同問題的使用者。
- 造訪 http://www.sophos.com/support/ 內的技術支援知識庫。
- 下載 http://tw.sophos.com/support/docs/ 內的產品說明文件。
- 寄送電子郵件至 supporttaiwan@sophos.com，郵件內請註明您的 Sophos 軟體版本號碼、操作系統與修補層級，以及任何錯誤訊息的全文。

17 法律聲明