IBM® Technical Support Appliance 配置輔助程式手冊

2.7.0.0 版

2020 年 8 月

目錄

簡介

IBM Technical Support Appliance (TSA) 是一個易用工具，可讓您從「IBM 支援中心」合約獲得更多價值。TSA 會探索您 IT 基礎架構內重要的資訊技術元素及其關係，並且安全地將資料傳輸給「IBM 支援中心」進行分析。此資料讓「IBM 支援中心」得以洞察您資料中心中伺服器與網路元件之間的複雜關係。

本文件的用意在於提供資訊和指引，以有助於安裝、規劃及配置 TSA。

探索前的網路注意事項

配置 TSA 以進行起始探索作業和傳輸作業之前，請確定已解決下列項目。會假設 TSA 已安裝、Web 介面可存取，且 TSA 已更新成最新層次，若非如此，請參閱《Technical Support Appliance 設置手冊》（本文件後續稱為「設置手冊」）。

TSA 探索前的網路注意事項	
網路功能	
	請開放從 TSA 至 IBM 的防火牆存取權。請參閱設置手冊中的**連接至 IBM 支援中心時的配置需求**一節。
	如果使用 SSL Proxy 來連接回 IBM，請確定已在 TSA 中配置它。請參閱設置手冊中的**設定 IBM Connectivity** 一節。 - 不支援 SSL 檢驗。如果在 Proxy 上採用 SSL 檢驗，請在進行這些流程時停用它。
	如果在 TSA 和目標裝置之間存在任何防火牆，請確定必要的埠是開啟的。如需相關資訊，請參閱第 33 頁「防火牆注意事項」一節。

說明

下列鏈結會將您直接指向 Technical Support Appliance 資訊網站。這裡有開始使用 IBM Technical Support Appliance 所需的一切資訊。您可以從 ibm.com 業務中心存取安裝手冊和安全文件、檢視範例報告，以及下載 Technical Support Appliance 安裝程式碼。

進一步瞭解 Technical Support Appliance：https://ibm.biz/TSAdemo

概觀

TSA 可以探索您的 IT 基礎架構的相關資訊，包括：已部署的作業系統元件、韌體元件、實體伺服器、網路裝置、虛擬 LAN 等。如果要將所收集資訊的廣度和深度最佳化，則需要在 TSA 內執行配置作業，以識別探索裝置。

TSA 會嘗試將對客戶網路環境的衝擊降至最低。因此，探索程序採用反覆和測量方法，這可能造成完整探索需耗時 72 小時。如果要監視探索作業的狀態，可檢視**摘要**畫面中的**作業摘要**區段。

在探索程序過程中，TSA 最初會在不使用認證的情況下，嘗試偵測所定義範圍內的裝置。這會使用到 Nmap，透過低侵害性的 IP 掃描、堆疊指紋和埠對映，來探索及釐清裝置。一般而言，此活動應不足以發動侵入偵測系統 (IDS)，但如果本端設定較為嚴格，就可能會。

若要讓 TSA 收集您 IT 基礎架構的相關資訊，請提供：

- 範圍
- 存取認證

定義範圍集

範圍集是個別範圍的邏輯分組。範圍使用 IP 位址，來告知 TSA 要從何處開始探索環境。範圍集由一或多個範圍組成。範圍項目有三種類型：

- 子網路 - 以 IP 位址和子網路遮罩來定義。子網路限制只能是類別 C 子網路。
- IP 範圍 - 包含起始和結尾之間的所有 IP 位址。
- IP 位址 / 主機 - 個別的 IP 位址或主機名稱。

> 主機名稱會在輸入期間（而非探索期間）解析。如需詳細資料，請參閱第 5 頁「建立範圍時的考量因素」一節。

必要時，可指定主機、範圍或子網路定義，來定義範圍的範圍排除項。產生的 IP 位址將不會視為範圍的一部分，且不會掃描。

TSA 支援三種範圍集：

1. **一般範圍集**：容許您探索個別 IT 網路元素。該範圍集包含的一個以上的範圍可使用 IP 位址、IP 位址範圍或者網路或子網路來識別這些網路元素的位置。
2. **HMC 動態範圍集**：容許您指定一個以上 IBM POWER Systems HMC 的 IP 位址以及相關聯的認證。此外，HMC 管理的所有 LPAR 的相關資訊也可以加以收集，而無需識別 LPAR 的 IP 位址。動態範圍集會使用您提供的認證資訊來順利存取這些 LPAR。

3. **VMware 動態範圍集**：容許您指定一個以上 VMware vCenter Server 或 ESXi 實例的 IP 位址以及相關聯的認證。此外，VMware 管理的所有虛擬機器的相關資訊也可以加以收集，而無需識別虛擬機器的 IP 位址。動態範圍集會使用您提供的認證資訊來順利存取這些虛擬機器。

對於 HMC 以及 VMware vCenter Server / ESXi，建議使用動態範圍集。動態範圍集要求在 TSA 中進行較少的配置，而為個別 LPAR/虛擬機器建立和管理探索範圍需要較多的配置。此外，如果在環境中隨時間新增和刪除 LPAR 或虛擬機器，則動態範圍集可以處理這項工作，而不需要修改任何範圍集。

如需獲取相關詳細指示以瞭解如何在 TSA 上定義探索範圍，請參閱設置手冊中的**設置探索範圍**一節。

建立範圍時的考量因素

雖然在設置範圍方面，並未定義任何標準，但有些實用的考量可以省時省力：

- 實用時，使用動態範圍集來定義 HMC 及其管理的 LPAR 或者 VMware vCenter Server / ESXi 及其管理的虛擬機器的探索。使用動態範圍集時，無需給 LPAR 或虛擬機器定義範圍。
- 請使用「IP 範圍」或「子網路」範圍，來探索多部裝置，而非使用個別的 IP 位址或主機名稱。這會限制範圍定義的數量，管理上更為輕鬆。
- 如果使用子網路範圍定義，每一個範圍集請只包含一個。請確定子網路範圍定義是解析成「類別 C」網路（256 個 IP 位址）或以內。
- 請使用**匯入範圍集**特性，以根據輸入文字檔中的指定名稱和 IP 位址清單，來建立新的範圍集。如需相關資訊，請參閱設置手冊中的**探索範圍 → 匯入一般範圍集**一節。
- TSA 目前只會儲存 IP 位址。也就是說，主機名稱是在輸入期間（而非探索期間）解析。對於範圍定義，最佳作法會建議您使用「IP 位址」或「IP 範圍」，而非主機名稱。
- 範圍集中的 IP 位址越多，探索時間越久。如果要將探索時間減至最少，請將範圍設置成僅以您想探索的元素為目標。

使用「一般範圍集」時，請將範圍集解析成的 IP 位址累計數目（在展開任何範圍或子網路範圍定義之後），限制在 400 個以內。以單一範圍集來說，在探索程序期間，如果要掃描的 IP 位址超過 400 個，可能會遇到效能、伺服器或網路問題。

- TSA 不會阻止將 IP 位址定義在多個範圍集中。一般而言，應避免這樣的作法，因為這會在不收集任何其他資訊的情況下，增加探索時間。
- 將範圍分組成範圍集，而這些範圍集構成裝置的邏輯分組：
  - 將相同的裝置類型分組在一個範圍集內。例如，為 IBM FlashSystem 儲存體子系統建立一個範圍集。

- 將位於相同地理位置的裝置分組在一起。
- 根據商業應用程式或服務來分組裝置。

探索認證

除了少數例外，探索程序需要某種存取層次，以獲得全面瞭解環境所需的詳細資訊。

一般而言，應在探索裝置上建立服務帳戶，以供 TSA 使用。請參閱下列各節，以瞭解每一種平台類型所需的特定存取權。如果要簡化這些服務帳戶的管理，請針對給定系列產品的所有裝置，使用同一使用者名稱。

在維護 TSA 用來連接裝置的服務帳戶時，可利用下列其中一種策略，來簡化這項維護作業：

- 建立含有未過期密碼的服務帳戶
- 將 SSH 金鑰用於支援使用 SSH 金鑰的裝置系列產品

有關如何定義應用裝置上的存取認證，如需詳細指示，請參閱設置手冊中的**設置探索認證**一節。

設定探索認證時的考量因素

應用裝置會依認證在存取清單中的出現順序，嘗試使用認證。如果要加快探索速度，請確定這些認證的順序最符合您的環境。部分考量如下：

- 在適當情況下，將認證侷限在特定的範圍集內。這會限制不必要的登入嘗試次數，並改良探索效能。
- SSH 金鑰可用於下列的裝置探索：
  - AIX
  - Cisco
  - Linux
  - HMC
  - IBM i
  - IVM
  - Sun SPARC (Solaris)
  - SVC / V7000
  - VIOS
  - Fortinet
  - HP-UX
  - IBM FlashSystem
  - F5 Big IP
  - Check Point

一份 SSH 金鑰認證只能鏈結至一個範圍集。

- 最佳作法是建立個別的服務帳戶供 TSA 專用，並具備必要的最低權限層級。

入門

本節涵蓋有關配置 TSA 時的最佳作法和建議。

TSA 的起始設置和配置

逐一瀏覽設置手冊下列各節中指定的指示：

- 安裝 Technical Support Appliance
- 登入 Technical Support Appliance
- 接受授權合約
- 使用設定精靈來設定 Technical Support Appliance

準備探索

建議採取反覆程序，藉以一開始先配置一小部分的網路進行探索，再於每一次的反覆程序中新增更多的區段，直到涵蓋所有想要的網路為止。

> 最佳作法是在您對範圍及/或認證進行大幅的新增/修改之後，就儲存您的 TSA 配置的備份。如需相關資訊，請參閱 IBM Technical Support Appliance 設定手冊中的「備份及還原」一節。

探索步驟

請針對每一次的探索反覆程序，執行下列步驟：

1. 準備裝置以進行探索。如需任何必要的裝置和認證配置需求，請參閱第 9 頁「裝置探索配置」一節。
2. 對於「HMC 動態範圍集」，請執行下列步驟：
   a. 在 **HMC 動態範圍集**頁面上新增 HMC 的 IP 位址。
   b. 在 **HMC 動態範圍集**頁面上新增 HMC 的認證。
   c. 選取您想要探索的 LPAR 類型。為每個類型提供認證。

      > 您可以選取 LPAR 類型來探索何時建立了動態範圍集，也可以透過編輯動態範圍集在後續疊代中新增 LPAR 類型。

   d. （選用項目）使用 **HMC 動態範圍集**頁面上的測試功能來驗證認證是否已正確定義，以及是否可用於建立連到 HMC 或其 LPAR 的連線。
3. 對於「VMWare 動態範圍集」，請執行下列步驟：
   a. 新增 VMware vCenter Server 的 IP 位址。
   b. 新增不受 VMware vCenter Server 管理的任何 VMware ESXi 主機的 IP 位址。

c. 在 **VMware 動態範圍集**頁面上新增 VMware vCenter Server 和 ESXi 實例的認證。

d. 選取您想要探索的虛擬機器類型。為每個類型提供認證。

> 您可以選取虛擬機器類型來探索何時建立了動態範圍集，也可以透過編輯動態範圍集在後續疊代中新增虛擬機器類型。

e. （選用項目）使用 **VMware 動態範圍集**頁面上的測試功能來驗證認證是否已正確定義，以及是否可用於建立連到 VMware vCenter Server 和 ESXi 實例及其虛擬機器的連線。

4. 對於「一般探索範圍」，請執行下列步驟：

   a. 在適當的範圍集 / 範圍中，新增想要的 IP 位址。如果 TSA 實例與探索裝置之間存在防火牆，請確定已在防火牆中開啟適當的埠，才能讓探索順利進行。如需取得哪些埠必須可供各平台類型存取的相關資訊，請參閱第 33 頁「防火牆注意事項」一節。

   b. 建立必要的認證。請使用**新增探索認證**畫面上的「測試」功能，驗證認證是否已正確定義，以及是否可用於建立連到目標裝置的連線。

5. 執行完整探索，以掃描在這次反覆程序中所新增的 IP 位址。

6. 執行傳輸，將資料上傳給 IBM。

裝置探索配置

除了提供認證，可能需符合特定的探索裝置配置先決條件，TSA 才能有效地探索及收集有用的元件資訊。本節可讓您識別您環境中將需要特定配置的探索裝置。建議您建立具備最起碼之必要權限的服務帳戶，此外，也請參閱「防火牆注意事項」一節，取得埠和通訊協定資訊。

- 對於已同時開啟 SSH 和 Telnet 埠的裝置，TSA 會先嘗試使用 SSH 進行連線（基於安全原因）。如果此 SSH 連線失敗，TSA 會接著嘗試經由 Telnet 進行連線。

作業系統和主機

平台
IBM Power Systems • 硬體管理主控台 (HMC) • Integrated Virtualization Manager (IVM) • Virtual I/O Server (VIOS) 分割區 • AIX • Linux on Power
IBM i
UNIX 系統 • Solaris • Solaris（透過 iLOM） • Linux • HP-UX
VMware vCenter Server 和 VMware ESXi
Windows
ATM 裝置

管理模組

- Flex System Manager (FSM)
- 機箱管理模組 (CMM)
- 進階管理模組 (AMM)
- HP ProLiant 刀鋒伺服器（透過 HP OnBoard Administrator）
- 整合管理模組（IMM 和 IMM2）
- HP Integrity 和 HP9000 伺服器（透過 iLO）

請按一下上方的每一個鏈結，以取得詳細資訊。

IBM Power Systems

對於 IBM Power Systems，如果其中的 LPAR 配置是由 HMC 或 IVM 管理，請使用「HMC 動態範圍集」。使用「HMC 動態範圍集」時，您將為 HMC 建立範圍定義，並提供相關聯的 HMC 和 LPAR 認證，但不需要為每一個受管理的 LPAR 建立範圍。當探索 HMC 時，TSA 會判斷當時存在哪些 LPAR，並自動掃描每一個 LPAR。

對於 IBM Power Systems，如果其中的 LPAR 配置大致是靜態的，「HMC 動態範圍集」的替代方法是依下列順序，反覆新增實體的範圍和認證：

1. **HMC 或 IVM 實例**：HMC 會針對它所管理的所有 Power Systems 以及其中所包含的邏輯分割區，傳回相關的高階資訊。IVM 會針對它所管理的單一系統，傳回類似資訊。
2. **VIOS 分割區**：這會針對這些分割區所擁有的實體配接卡和資源，傳回相關資訊。
3. **個別的分割區**：在某些情況下，非 VIOS 分割區擁有實體配接卡。

硬體管理主控台 (HMC)

如果要探索 HMC 實例，請完成下列步驟：

準備環境：

- 若要讓 TSA 透過 HMC 來收集相關的 LPAR 管理資訊，HMC 必須能夠利用 RMC 工具與 LPAR 通訊。請確定 HMC 和 LPAR 已配置成容許進行這項通訊。如需適用於 Linux 的 RMC 工具的相關資訊，請參閱 https://www14.software.ibm.com/webapp/set2/sas/f/lopdiags/yum.html
- 若要啟用安全資料收集，必須在 HMC 上啟用遠端指令執行。如需相關資訊，請參閱「啟用和停用 HMC 遠端指令」，其位址如下：https://www.ibm.com/support/knowledgecenter/POWER7/p7ha1/enablinganddisablinghmcremotecommands.htm

存取清單的認證：

- 對於「HMC 動態範圍集」- HMC 服務帳戶的使用者名稱 / 密碼或使用者名稱 / SSH 金鑰鑑別。
- 對於「一般探索範圍集」- 電腦系統：HMC 服務帳戶的使用者名稱 / 密碼或使用者名稱 / SSH 金鑰鑑別。
- HMC 使用者必須具備下列角色：
  - 資源角色：AllSystemResources
  - 作業角色（以使用指令行作業的 **hmcoperator** 為基礎）：
    - 受管理系統（lshwres、lssyscfg）
    - 邏輯分割區（lshwres、lssyscfg、viosvrcmd）
    - HMC 配置 (lshmc)
- 必要時，可以使用具備 **hmcviewer** 權限的使用者（服務帳戶），不過，這會導致局部的資料收集。

> 當以 **hmcviewer** 權限來執行時，無法取得 VIOS 分割區所擁有之配接卡的相關資訊。如果要取得此資訊，請確定服務帳戶最起碼具備 **hmcoperator** 權限。如果不可能如此，請新增範圍和認證，以便除了 HMC 之外，直接探索 VIOS 分割區。

Integrated Virtualization Manager (IVM)

如果要探索 IVM 實例，請完成下列步驟：

存取清單的認證：

- 電腦系統：IVM 服務帳戶的使用者名稱 / 密碼或使用者名稱 / SSH 金鑰鑑別。
- 服務帳戶必須具備「僅檢視」許可權。

Virtual I/O Server (VIOS) 分割區

如果要探索 VIOS 實例，請完成下列步驟：

存取清單的認證：

- 對於「HMC 動態範圍集」- VIOS 分割區服務帳戶的使用者名稱 / 密碼或使用者名稱 / SSH 金鑰鑑別。
- 對於「一般探索範圍集」- 電腦系統：VIOS 分割區服務帳戶的使用者名稱 / 密碼或使用者名稱 / SSH 金鑰鑑別。
- 服務帳戶必須是管理者帳戶（例如 **padmin**）。
- 服務帳戶必須具有使用者屬性 **rlogin=true**。您可以使用 SMIT 或編輯 **/etc/security/user** 檔，來設定這個屬性。
- **/etc/ssh/sshd_config** 檔中的參數 **PermitUserEnvironment** 必須設為 **yes**。

AIX

如果要探索 AIX 實例，請完成下列步驟：

準備環境：

- 請確定已安裝 bos.perf.tools 和 openSSH/openSSL 套件。
- 停用服務帳戶的無效登入嘗試失敗。

存取清單的認證：

- 對於「HMC 動態範圍集」- AIX 分割區服務帳戶的使用者名稱 / 密碼或使用者名稱 / SSH 金鑰鑑別。
- 對於「一般探索範圍集」- 電腦系統：AIX 服務帳戶的使用者名稱 / 密碼或使用者名稱 / SSH 金鑰鑑別。
- 服務帳戶可以是 root 或具備 sudo 權限的帳戶。
- 服務帳戶必須具有使用者屬性 **rlogin=true**。您可以使用 SMIT 或編輯 **/etc/security/user** 檔，來設定這個屬性。
- 若要讓非 root 服務帳戶能夠在 AIX 上使用 sudo 權限，請執行下列動作：
  - 安裝 sudo RPM (sudo-1.6.9p15-2noldap) 和 ssh 檔案集（AIX 實例上的 openssh.base.server、openssh.base.client）。
  - 在目標 AIX 實例上，建立一個可供 TSA 用來存取系統的非 root 使用者 ID。
  - 修改每一個 AIX 實例上的 **/etc/sudoers**，以容許 TSA 使用 sudo 權限來執行指定的指令。

    # Cmnd alias specification
    Cmnd_Alias TSA_CMDS = /usr/bin/lparstat, /usr/sbin/no, /usr/sbin/nfso, /usr/bin/lslicense, /usr/sbin/vmo, /usr/sbin/ioo, /usr/sbin/lvmo, /usr/sbin/schedo, /usr/bin/sysdumpdev, /usr/sbin/smtctl, /usr/sbin/emgr, /usr/bin/sissasraidmgr, /usr/sbin/lswpar, /usr/sbin/cpuextintr_ctl, /usr/sbin/lsnim, /usr/sbin/raso, /usr/sbin/bosdebug, /usr/sbin/chedition, /usr/esa/bin/esacli, /usr/sbin/bootinfo, /usr/bin/mpio_get_config, /usr/bin/cat /etc/objrepos/CuData,
    /usr/bin/cat /etc/objrepos/CuData.vc, /usr/bin/cat /var/adm/ras/bootlog, /usr/bin/cat /etc/lpp/diagnostics/data/diagrpt*.dat, /usr/bin/tapeutil, /usr/lpp/OV/bin/opcagt, /usr/DynamicLinkManager/bin/dlnkmgr view, /usr/sbin/powermt version, /usr/sbin/powermt display, /usr/bin/pcmpath query, /usr/sbin/datapath query

    # User privilege specification
    <User Name> ALL = NOPASSWD: TSA_CMDS

    <User Name> 是 TSA 收集 AIX 資訊時使用的非 root 服務帳戶。這個 <User Name> 是每一個 AIX 實例上的使用者。必須以上述規格來更新每一個 AIX 實例上的 **/etc/sudoers** 檔。

    或者

    除了如上修改 **/etc/sudoers**，也可以使用下列使用者專用權規格：
    <User Name> ALL = NOPASSWD: ALL

> <User Name> 是 TSA 收集 AIX 資訊時使用的非 root 服務帳戶。這項使用者規格容許服務帳戶在任何 AIX 指令上使用 sudo 權限。

Linux on Power

如果要探索 Linux on Power 實例，請完成下列步驟：

準備環境：

- 停用服務帳戶的無效登入嘗試失敗

存取清單的認證：

- 對於「HMC 動態範圍集」- Linux 分割區服務帳戶的使用者名稱 / 密碼或使用者名稱 / SSH 金鑰鑑別。
- 對於「一般探索範圍集」- 電腦系統：Linux 服務帳戶的使用者名稱 / 密碼或使用者名稱 / SSH 金鑰鑑別。
- 若要讓非 root 服務帳戶能夠在 Linux 上使用 sudo 權限，請執行下列動作：
  - 在實際的目標 Linux 實例上，建立一個可供 TSA 用來存取系統的非 root 使用者 ID。
  - 修改每一個 Linux 實例上的 **/etc/sudoers**，以容許 TSA 使用 sudo 權限來執行指定的指令。

```
# Cmnd alias specification
Cmnd_Alias TSA_CMDS = /usr/sbin/lsvpd, /sbin/lsvpd, /usr/sbin/lscfg,
/sbin/lscfg, /usr/sbin/lsmcode, /sbin/lsmcode, /usr/sbin/lvmdiskscan,
/sbin/lvmdiskscan, /usr/sbin/dmidecode, /usr/bin/mtlib, /usr/bin/tapeutil,
/usr/bin/crontab, /sbin/fdisk, /bin/ls -alR /boot/*, /bin/cat /proc/irq/*, /bin/cat
/proc/net/vlan/config, /bin/cat /proc/ppc64/rtas/*, /bin/cat
/proc/sys/kernel/cap-bound, /bin/cat /proc/sys/kernel/random/entropy_avail

# User privilege specification
<User Name> ALL = NOPASSWD: TSA_CMDS
```

> <User Name> 是 TSA 收集 Linux 資訊時使用的非 root 服務帳戶。這個 <User Name> 是每一個 Linux 實例上的使用者。必須以上述規格來更新每一個 Linux 實例上的 **/etc/sudoers** 檔。

或者

除了如上修改 **/etc/sudoers**，也可以使用下列使用者專用權規格：

```
<User Name> ALL = NOPASSWD: ALL
```

> <User Name> 是 TSA 收集 Linux 資訊時使用的非 root 服務帳戶。這項使用者規格容許服務帳戶在任何 Linux 指令上使用 sudo 權限。

- 如果您將 IBM Proweb for AIX 入口網站用作 IBM 支援產品與服務的一部分，建議您使用「HMC 動態範圍集」來配置 TSA。替代方法是配置 TSA 以探索 Power Systems 上的 HMC 和邏輯分割區（包括 VIOS）。
- 透過使用「HMC 動態範圍集」進行掃描，取得可透過 ProWeb 進行擷取和分析的每個 LPAR 的較詳細 OS 配置資訊。

> 如需瞭解如何為 HMC 環境新增範圍和認證的相關資訊，請參閱 IBM Technical Support Appliance 設置手冊中的「**HMC 動態範圍**」一節。

- 掃描各種 Power Systems 實體，為報告所收集的資料層次如下：
  - 如果只掃描 HMC，您會取得 Identified 標籤、HMC Topology、Power Systems Firmware 、 IBM i Recommendations 、 Linux Recommendations、HMC/VIOS/AIX 和 Contract 等標籤的所有必要資訊，以及一些「配接卡」資訊。
  - 如果直接掃描 VIOS 分割區，您會取得配接卡韌體和所連接的儲存體的其他資訊。
  - 透過直接掃描 LPAR，您將取得 LPAR 的相關資訊，包括 OS 詳細資料和特定軟體的實例（例如 PowerHA、GPFS 和 PowerSC）。

IBM i

IBM i 實例是使用 SSH 連線來探索。如果 IBM i 實例未安裝及配置 SSH，請完成下列步驟：

準備環境：

若為 IBM i 7.2，請確定已安裝及配置下列產品/選項：

- IBM Portable Utilities for i (5733-SC1)
- Qshell（5770-SS1，選項 30）
- Portable App Solutions Environment（5770-SS1，選項 33）
- IBM Developer Kit for Java (5770-JV1)

若為 IBM i 7.3，請確定已安裝及配置下列產品/選項：

- IBM Portable Utilities for i (5733-SC1)
- Qshell（5770-SS1，選項 30）
- Portable App Solutions Environment（5770-SS1，選項 33）
- IBM Developer Kit for Java（5770-JV1，選項 16）
- Java SE 8 32 位元

若為 IBM i 7.4，請確定已安裝及配置下列產品/選項：

- IBM Portable Utilities for i (5733-SC1)
- Qshell（5770-SS1，選項 30）
- Portable App Solutions Environment（5770-SS1，選項 33）

- IBM Developer Kit for Java（5770-JV1，選項 16）
- Java SE 8 32 位元

如果要啟動 SSH 常駐程式，請執行下列指令：
SBMJOB CMD (CALL PGM (QP2SHELL) PARM('/QOpenSys/usr/sbin/sshd'))

如果要在 IBM i 上啟動 SSHD 服務，請執行下列指令：
STRTCPSVR SERVER(*SSHD)

如需如何在 IBM i 上配置 SSH 的其他相關資訊，請參閱下列紅皮書中的第 21 到 23 章：- http://www.redbooks.ibm.com/redpapers/pdfs/redp4163.pdf

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼。
- 服務帳戶可以具有任何使用者類別（包括 ***USER**），不過，需要具備額外的物件權限需求，才能收集 PTF 資訊（使用 **DSPPTF** 指令來完成）。
- **DSPPTF** 隨附了下列的物件權限限制：
  - 指令隨附了 ***EXCLUDE** 公用權限
  - **QPGMR**、**QSYSOPR**、**QSRV** 和 **QSRVBAS** 使用者設定檔隨附了專用權限來使用這個指令
  - 一如既往，**QSECOFR** 使用者設定檔或者是使用者類別為 ***SECOFR** 的任何使用者設定檔，可以執行這個指令
- 物件類型是 ***CMD** 的 **QSYS/DSPPTF** 物件可以編輯其權限，以容許其他任何使用者執行這個指令。
- 如果為 TSA 建立了新的服務帳戶，則建議如下：
  - 請建立一個使用者類別為 ***USER** 的使用者設定檔
  - 請使用 **GRTOBJAUT** 指令，以容許這個使用者設定檔執行 **DSPPTF** 指令；物件是 **QSYS/DSPPTF**，其物件類型是 ***CMD**。

UNIX 系統

Solaris

如果要探索 Solaris 裝置，請完成下列步驟：

準備環境：

- 在 Solaris 系統上，請確定已安裝 SUNWscpu（程式碼相容性）套件。
- 在某些 Solaris 系統上，需要安裝及配置 SNEEP，以取得序號。

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼或使用者名稱 / SSH 金鑰鑑別。
- 服務帳戶可以是非 root。

Solaris（透過 Oracle iLOM）

如果要透過 Oracle iLOM 來探索 Solaris 裝置，請完成下列步驟：

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼。
- 服務帳戶可以具備**操作員**或**管理者**專用權。

Linux

如果 Linux 實例是在 IBM Power System 上執行，請參閱第 13 頁 Linux on Power 一節的 IBM Power Systems 下取得相關指示。

如果要探索 Linux on x86 裝置，請完成下列步驟：

準備環境：

- 請確定已安裝 pciutils 套件。其中所包含的 lspci 指令用來收集配接卡和外部儲存體裝置連線的相關資訊。

存取清單的認證：

- 對於「VMware 動態範圍集」- Linux 虛擬機器服務帳戶的使用者名稱 / 密碼或使用者名稱 / SSH 金鑰鑑別。
- 對於「一般探索範圍集」- 電腦系統：Linux 服務帳戶的使用者名稱 / 密碼或使用者名稱 / SSH 金鑰鑑別。
- 設定 /bin/sh，以作為這個帳戶的 Shell。
- 若為 Linux (x86)，服務帳戶可以是 root 或具備 sudo 權限的帳戶。
- 如果要使用非 root 服務帳戶進行探索，請在 Linux 系統上的 **/etc/sudoers** 檔案中新增下列：

  # Cmnd alias specification
  Cmnd_Alias TSA_CMDS = /usr/sbin/dmidecode

  # User privilege specification
  <User Name> ALL = NOPASSWD: TSA_CMDS

  > <User Name> 是 TSA 收集 Linux 資訊時使用的非 root 服務帳戶。這個 <User Name> 是每一個 Linux 實例上的使用者。必須以上述規格來更新每一個 Linux 實例上的 **/etc/sudoers** 檔。

  或者

  除了如上修改 **/etc/sudoers**，也可以使用下列使用者專用權規格：
  <User Name> ALL = NOPASSWD: ALL

  > <User Name> 是 TSA 收集 Linux 資訊時使用的非 root 服務帳戶。這項使用者規格容許服務帳戶在任何 Linux 指令上使用 sudo 權限。

HP-UX

如果要探索 HP-UX 裝置，請完成下列步驟：

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼或使用者名稱 / SSH 金鑰鑑別。
- 若要讓非 root 服務帳戶能夠在 HP-UX 上使用 sudo 權限，請執行下列動作：
  - 修改每一個 HP-UX 實例上的 **/usr/local/etc/sudoers**，以容許 TSA 使用 sudo 權限來執行指定的指令。

```
# Cmnd alias specification
Cmnd_Alias TSA_CMDS =/usr/sbin/diskinfo,/opt/hpvm/bin/hpvmstatus

# User privilege specification
<User Name> ALL=(ALL) NOPASSWD:TSA_CMDS
```

 <User Name> 是 TSA 收集 HP-UX 資訊時使用的非 root 服務帳戶。

VMware vCenter Server 和 VMware ESXi

對於 VMware 環境，請使用「VMware 動態範圍集」。使用「VMware 動態範圍集」時，您將為 VMware vCenter Server / ESXi 建立範圍定義，並提供相關聯的 VMware 和虛擬機器認證，但不需要為每一個受管理的虛擬機器建立範圍。當探索 VMware vCenter Server / ESXi 時，TSA 會判斷當時存在哪些虛擬機器，並自動掃描每一個虛擬機器。

對於 VMware 環境，如果其中的虛擬機器配置大致是靜態的，「VMware 動態範圍集」的替代方法是依下列順序，反覆新增實體的範圍和認證：

1. **「vCenter 伺服器」實例**：這會針對它們所管理的 ESXi 主機，以及其中所包含的「虛擬機器」訪客，傳回相關的高階資訊。
2. **ESXi 主機**：新增不受 vCenter Server 管理的 ESXi 主機。
3. **個別的「虛擬機器」訪客**：這容許收集作業系統的相關詳細資訊。

為 VMware 環境配置 TSA 時，建議執行下列動作：

1. 可行時，配置 TSA 以探索 VMware vCenter Server。如果探索 VMware vCenter Server，則會自動導致 TSA 收集 vCenter Server 管理的所有 VMware ESXi 主機的相關資訊。不需要 ESXi 主機的相關配置資訊。
2. 只有在 ESXi 主機不受 VMware vCenter Server 管理時，才配置 TSA 以探索 VMware ESXi 主機。
3. 將 VMware Tools 安裝在 ESXi 主機上代管的每個虛擬機器中。如果 VMware Tools 未安裝，則部分庫存資料（例如 IP 位址或安裝的作業系統）將無法存取。

4. 配置每個 VMware ESXi 主機，以啟動 CIM 介面。CIM 介面容許 TSA 收集 ESXi 主機內配接器的詳細資訊。如需 CIM 提供者的相關資訊，請參閱第 44 頁「附錄 C」。

如果要探索 vCenter 伺服器實例，以及它們所管理之 ESXi 伺服器的資訊，請完成下列步驟：

準備環境

- 將 VMware Tools 安裝在 ESXi 主機上代管的每個虛擬機器中。
- 配置每個 VMware ESXi 主機，以啟動 CIM 介面。
- CIM 埠 (5989) 必須可從 TSA 進行存取（未被防火牆封鎖，等等）才能進行完整探索。

存取清單的認證

- 對於「VMware 動態範圍集」- VMware vCenter Server 服務帳戶的使用者名稱 / 密碼。
- 對於「一般探索範圍集」- 電腦系統：VMware vCenter Server 服務帳戶的使用者名稱 / 密碼。
- 服務帳戶必須具備**管理者**角色許可權，或至少具備自訂「唯讀」角色的許可權，外加擁有下列的專用權：
  - 廣域 → 授權
  - 廣域 → 設定
  - 主機 → CIM
  - 主機 → 配置 → 變更設定
  - 主機 → CIM→ CIM 互動

如果要直接探索 ESXi 裝置，請完成下列步驟：

準備環境

- 將 VMware Tools 安裝在 ESXi 主機上代管的每個虛擬機器中。
- 配置每個 VMware ESXi 主機，以啟動 CIM 介面。

存取清單的認證

- 對於「VMware 動態範圍集」- VMware ESXi 服務帳戶的使用者名稱 / 密碼。
- 對於「一般探索範圍集」- 電腦系統：VMware ESXi 服務帳戶的使用者名稱 / 密碼。
- 服務帳戶必須具備**管理者**角色許可權。

Windows

TSA 支援採用下列方法來探索 Windows 實例：

- WINRM
- SMB1

> 建議採用「Windows（透過 WINRM）」，因為這是更安全的介面。

Windows（透過 WINRM）

如果要透過 WINRM 來探索 Windows，請完成下列步驟：

準備環境：

準備環境最常用的方式是使用安裝在目標 Windows 伺服器上之憑證管理中心所產生的伺服器憑證。憑證必須符合下列條件：

- 來自憑證管理中心的主要憑證與中繼憑證存在於「受信任的主要憑證管理中心」憑證中。
- 伺服器憑證已安裝在「個人」憑證中。
- 伺服器憑證必須顯示它是簽發至伺服器的完整主機名稱。
- 伺服器憑證必須包含此伺服器的私密金鑰。

下列指令是配置 WINRM，以進行遠端 HTTPS 連線：
winrm quickconfig -transport:https

這個指令會執行下列動作：

- 啟用 WINRM（如果目前不在作用中）
- 修改 WINRM 服務，使 WINRM 在重新啟動時自動啟動
- 配置 WINRM HTTPS 接聽器
- 修改「Windows 防火牆」規則，以接受遠端 HTTPS 連線

指令會產生下列輸出。請輸入 **y**，確認這些變更。

```
WinRM 服務已經在這部機器上執行。
WinRM 未設定成容許遠端存取這部機器以進行管理。
必須進行下列變更：

在 HTTPS://* 上建立 WinRM 接聽器以接受對這部機器上任何 IP 的 WS-Man 要求。
為服務配置 CertificateThumbprint 設定以用於 CredSSP 鑑別。
配置 LocalAccountTokenFilterPolicy 以授予本端使用者遠端管理權限。

進行下列變更 [y/n]？ y

WinRM 已更新進行遠端管理。

已在 HTTPS://* 上建立 WinRM 接聽器以接受對這部機器上任何 IP 的 WS-Man 要求。
已配置服務所需的設定。
已配置 LocalAccountTokenFilterPolicy 以授予本端使用者遠端管理權限。
```

最後，若要容許經由 HTTPS 來進行使用者 ID / 密碼鑑別，請執行下列指令：
winrm set winrm/config/service/auth @{Basic="true"}

替代作法是使用自簽憑證。如需這項配置的指示，請參閱第 44 頁附錄 D：使用 WINRM 的 Windows。

存取清單的認證：

- 對於「VMware 動態範圍集」：服務帳戶的使用者名稱 / 密碼。
- 對於「一般探索範圍集」：電腦系統 (Windows)：服務帳戶的使用者名稱 / 密碼。
- 服務帳戶必須是下列其中一個群組的成員：
  - 管理者
  - WinRMRemoteWMIUsers__

如果要將使用者新增至 WinRMRemoteWMIUsers__ 群組，請使用下列指令：
net localgroup WinRMRemoteWMIUsers__ [user_id] /add

Windows（透過 SMB1）

如果要探索 Windows 裝置，請完成下列步驟：

準備環境：

- 請確定目標裝置上已啟用 Windows Scripting Host (WSH) 或 Windows Management Instrumentation (WMI) 服務和 VBScript。
- 請確定埠 445 未被防火牆或 IP 安全原則封鎖，因為 TSA 需要使用經由 TCP/IP 的「伺服器訊息區塊 (SMBv1)」通訊協定。
- 如果要套用安全原則，請移至**開始 → 控制台 → 系統管理工具**，然後根據您的原則是儲存在本端還是 Active Directory 中，來選擇下列導覽：
  - 儲存在本端的原則：**系統管理工具 → 本機安全性原則 → IP 安全原則**（位置：本機電腦）
  - 儲存在 Active Directory 中的原則：**系統管理工具 → 預設網域安全性設定 → IP 安全性原則**（位置：Active Directory）或**系統管理工具 → 預設網域控制器安全性設定 → IP 安全性原則**（位置：Active Directory）
- TSA 對隱藏的遠端管理磁碟共用項需具備存取權，以便存取系統 %TEMP% 和其他目錄。此外，也需具備「交互處理通訊」共用項 (IPC$) 的存取權，這樣 TSA 才能存取遠端登錄。請確定「交互處理通訊」共用項的「伺服器」服務已啟動。如果要啟動「伺服器」服務，請移至 → **控制台 → 系統管理工具 → 服務 → 伺服器**。
- 請確定「遠端登錄服務」處於作用中。這是必要的，如此 TSA 才能與 Windows 裝置之間建立階段作業。

存取清單的認證：

Windows 2012 R2 版及更新版本：

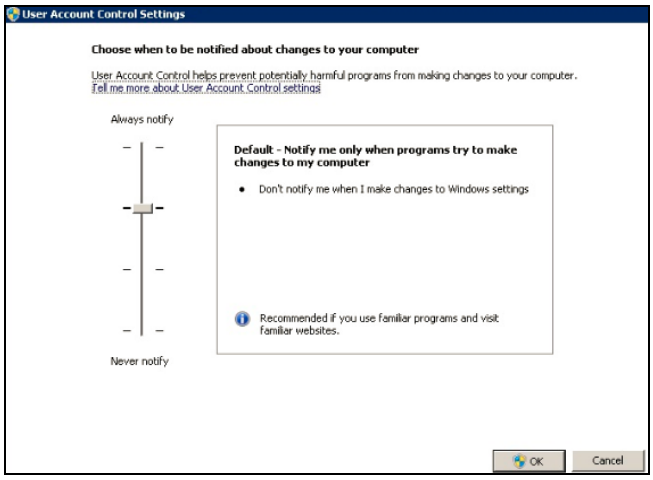
- 對於「VMware 動態範圍集」- 基本「管理者」帳戶 / 密碼。這個帳戶將會運作，而不考慮「使用者帳戶控制 (UAC)」設定。
- 對於「一般探索範圍集」- 電腦系統 (Windows)：基本「管理者」帳戶 / 密碼。這個帳戶將會運作，而不考慮「使用者帳戶控制 (UAC)」設定。

如果符合特定條件，有可能使用基本「管理者」帳戶以外的帳戶。帳戶必須是一個本端或網域管理者帳戶，且「使用者帳戶控制 (UAC)」設定必須符合特定需求。請參照下表，瞭解支援的「帳戶類型與 UAC 設定」組合。請參照 Microsoft Windows 說明文件，取得有關 UAC 的其他詳細資料。

	「使用者帳戶控制」設定			
	一律通知	**只在程式嘗試變更我的電腦時才通知我（預設值）**	**只在程式嘗試變更我的電腦時才通知我（不要將桌面變暗）**	**不要通知**
基本管理者	**是**	**是**	**是**	**是**
「網域管理者群組」中的使用者	**否**	**是**	**是**	**是**
「本端管理者群組」中的使用者	**否**	**是**	**是**	**是**
非管理者帳戶（網域或本端）	**否**	**否**	**否**	**否**

如果要存取「UAC 設定」，請按一下**開始**，然後按一下**控制台**。在搜尋框中輸入 **uac**，然後按一下**變更使用者帳戶控制設定**。

下列是預設值：



ATM 裝置

可以探索 ATM 裝置中的特定型號。如果要探索 ATM 裝置（包括其元件的相關基本資訊），請完成下列步驟：

準備環境：

- Wincor Nixdorf 型號 - 請遵循 Windows（透過 SMB）的指示。

管理模組

對於 IBM Flex Systems，最好的作法是依下列順序，反覆新增實體的範圍和認證：

1. **Flex System Manager (FSM)：**這會針對 Flex System Manager 和其管理的機箱，連同其相關聯的計算節點，傳回相關的高階資訊。

   > 如果不存在 FSM，建議在 Flex 系統上掃描 CMM 和任何管理 POWER 計算節點的 HMC。

2. **機箱管理模組 (CMM)：**對於不受 FSM 管理的機箱，請指向每一個 CMM，以擷取每一個機箱和其相關聯節點的相關高階資訊。
3. **計算節點：**這會傳回作業系統的相關詳細資訊。

Flex System Manager (FSM) 裝置

如果要探索 FSM 裝置，請完成下列步驟：

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼。
- 服務帳戶必須具備 **SMAdmin** 權限。

機箱管理模組 (CMM) 裝置

如果要探索 CMM 裝置，請完成下列步驟：

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼。
- 服務帳戶必須至少具備**操作員**權限。

進階管理模組 (AMM) 裝置

如果要探索 AMM 裝置，請完成下列步驟：

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼。
- 服務帳戶必須至少具備**操作員**權限。

HP Proliant 刀鋒伺服器（透過 HP OnBoard Administrator）

對於 Hewlett Packard (HP) ProLiant 伺服器，最好的作法是針對 HP OnBoard Administrator (HP OBA) 的實體，新增範圍和認證。HP OBA 會針對 HP OnBoard Administrator、它所管理的機箱，以及附帶在機箱中的計算節點，傳回相關的高階資訊。

如果要透過 HP OnBoard Administrator (OBA) 來探索 HP Proliant 刀鋒伺服器，請完成下列步驟：

準備環境：

- HP OBA 必須處於作用中模式。

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼。
- 服務帳戶在 HP OnBoard Administrator 上必須具備 **OA 管理者**、**OA 操作員**或 **OA 使用者權限**。建議具備 **OA 使用者權限**角色。

> TSA 只會從處於作用中狀態的 HP OnBoard Administrator 收集資訊。不會從處於待命狀態的 HP OnBoard Administrator 收集任何資訊。

「整合管理模組 (IMM)」和「整合管理模組 II (IMM2)」裝置

如果要探索 IMM 和 IMM2 裝置，請完成下列步驟：

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼。
- 服務帳戶可以具備任何有效的權限。

HP Integrity 和 HP9000 伺服器（透過 iLO）

iLO 是 HP Integrity 和 HP9000 伺服器內一個獨立的處理器卡片，可提供伺服器的基本硬體資訊。只要一插上伺服器，iLO 就會立即起作用，即使伺服器本身尚未開啟電源也一樣。

如果要透過 iLO 來探索 HP Integrity 和 HP9000 伺服器的庫存資訊（摘要層次），請完成下列步驟：

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼。
- 服務帳戶可以使用任何有效的權限層級。建議具備**使用者**權限。

網路裝置

本節針對下列類型的網路裝置，提供詳細資訊：

平台
BNT 交換器
Brocade 交換器
Check Point
Cisco 交換器
F5 Big-IP (TMOS)
Fortinet (FortiOS)
IBM b 型儲存區域網路 (SAN) 交換器
Juniper 交換器
Palo Alto Networks (PAN-OS)
QLogic 交換器
請按一下上方的每一個鏈結，以取得詳細資訊。

BNT 交換器

如果要探索 BNT 交換器，請完成下列步驟：

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼。
- 服務帳戶必須具備 **admin** 權限。

Brocade

如果要探索 Brocade 裝置，請完成下列步驟：

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼。

- 已停用「虛擬光纖」模式：服務帳戶可以使用任何有效的權限。建議具備**使用者**權限。
- 已啟用「虛擬光纖」模式：服務帳戶在 Fabric OS 上需具備**管理者**權限。

Check Point

如果要探索 Check Point 系統，請完成下列步驟：

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼或使用者名稱 / SSH 金鑰鑑別。
- 服務帳戶必須具備管理者權限 (**adminRole**)。
- 服務帳戶必須具備 SSH 存取權，才能執行 CLI 指令。

Cisco

如果要探索 Cisco 裝置，您可以使用下列的電腦系統認證或 SNMP 認證：

存取清單的認證：

- 電腦系統或其他（Cisco 裝置）或其他 (Cisco Works)：服務帳戶的使用者名稱 / 密碼或使用者名稱 / SSH 金鑰。
- 服務帳戶需要具備**網路管理者**角色專用權。
- SNMP：請輸入社群字串（若為 SNMPv1 和 SNMPv2）。
- SNMP (SNMPv3)：
  - 輸入：
    - 使用者名稱
    - 密碼
    - 專用密碼（選用）
  - 請選取鑑別通訊協定：無、MD5、SHA

> 對於具備範圍中所有網路裝置之唯讀權的 TSA，務必提供單一社群字串給該 TSA。

F5 Big-IP (TMOS)

如果要探索正在執行 TMOS 的 F5 Big-IP 系統，請完成下列步驟：

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼或使用者名稱 / SSH 金鑰鑑別。
- 服務帳戶必須具備 F5 管理者權限。
- 服務帳戶必須具備 SSH 存取權，才能執行 TMSH CLI 指令。

Fortinet (FortiOS)

如果要探索正在執行 FortiOS 的 Fortinet 裝置，請完成下列步驟：

準備環境

- 請確定系統主控台已配置成顯示整個指令輸出：
  config system console

```
set output standard
end
```

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼或使用者名稱 / SSH 金鑰鑑別。
- 服務帳戶必須至少具備「唯讀」許可權。

IBM b 型儲存區域網路 (SAN) 交換器

如果要探索 IBM b 類型 SAN 裝置，請完成下列步驟：

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼。
- 已停用「虛擬光纖」模式：服務帳戶可以使用任何有效的權限。建議具備**使用者**權限。
- 已啟用「虛擬光纖」模式：服務帳戶在 Fabric OS 上需具備**管理者**權限。

Juniper

如果要探索 Juniper 裝置，請完成下列步驟：

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼
- 服務帳戶必須具備管理者權限。

> **附註**：如果要探索記憶體大小資訊，則裝置上必須安裝 Junos® 12.1 版或更新版本。

Palo Alto Networks (PAN-OS)

如果要探索正在執行 PAN-OS 的 Palo Alto Networks 系統，請完成下列步驟：

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼。
- 服務帳戶必須具備「超級使用者」或「超級使用者（唯讀）」
- 服務帳戶必須具備 REST API 存取權（埠 443）。

QLogic 交換器

如果要探索 QLogic 交換器，請完成下列步驟：

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼。
- 服務帳戶必須具備管理者權限。

儲存裝置

本節針對下列類型的「儲存體」和「磁帶機」裝置，提供詳細資訊：

平台

平台
EMC 公司儲存體
HP StorageWorks P2000 模組化智慧型陣列
IBM DS3xxx、DS4xxx 或 DS5xxx
IBM DS6xxx 或 DS8xxx
IBM FlashSystem V9000
IBM ProtecTier
IBM SVC 或 V7000/V3700
IBM TS3100 磁帶庫
IBM TS3200 磁帶庫
IBM TS3310 磁帶庫
IBM TS3494、TS3953 磁帶庫
IBM TS3500、TS3584 磁帶庫
IBM TS4500 磁帶庫
IBM TS7700 磁帶庫
IBM V7000 Unified
IBM XIV
nSeries 或 NetApp
請按一下上方的每一個鏈結，以取得詳細資訊。

EMC 公司儲存體

EMC CLARiiON / VNX / VMAX

如果要探索 EMC CLARiiON / VNX / VMAX 裝置，請完成下列步驟：

準備環境：

- 請確定 EMC SMI-S Provider 產品實例已安裝在 Windows 或 Linux 系統上。依預設，TSA 會遵循 EMC SMI-S 建議，使用 SLP 來探索提供者的位置。如果您的網路安全原則會封鎖 SLP 網路資料流量，可將 TSA 配置成直接存取 SMI-S Provider，而不使用 SLP。
- 如果您的網路安全不接受 SLP 網路資料流量，請使用**探索設定 → 連線設定**頁面，來提供有關 EMC SMI-S Provider 使用哪些埠來接聽查詢要求的資訊。
- 請確定範圍集中至少已定義 SMI-S Provider 正在採用的其中一個 IP 位址。TSA 會連接至 SMI-S Provider，以擷取它所管理之 EMC 裝置的相關資訊。不需將個別 EMC 裝置的 IP 位址放在範圍集中。TSA 會嘗試使用 HTTPS（若有的話）來連接至 SMI-S Provider，否則，會使用 HTTP。

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼。
- 服務帳戶可以使用任何有效的角色。建議具備**監視者**角色。

只需將 SMI-S Provider 的認證輸入到 TSA 中。不需輸入 EMC 裝置的任何認證。

EMC Data Domain

如果要探索 EMC Data Domain 裝置，請完成下列步驟：

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼。
- 服務帳戶可具備最起碼的必要權限。

HP StorageWorks P2000 模組化智慧型陣列

如果要探索 HP Storage 系統，請完成下列步驟：

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼。
- 服務帳戶可具備最起碼的必要權限。

IBM DS3xxx、DS4xxx 或 DS5xxx 儲存體

如果要探索 IBM DS3xxx、DS4xxx 或 DS5xxx 裝置，請完成下列步驟：

準備環境：

- 請確定儲存體管理程式容許使用遠端 **smcli** 指令。

存取清單的認證：

- 對於非安全的儲存裝置，則不需要認證。
- 對於安全儲存裝置，請完成下列步驟：
  - 電腦系統：服務帳戶的使用者名稱 / 密碼。

- 服務帳戶可以具備**管理者**或**監視者**角色。建議具備**監視者**角色。

IBM DS6xxx / DS8xxx 儲存體

如果要探索 IBM DS6xxx / DS8xxx 裝置，請完成下列步驟：

準備環境：

- 請確定儲存體管理程式容許使用遠端 **dscli** 指令。

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼。
- 服務帳戶必須具備**監視者**角色。

IBM FlashSystem V9000

如果要探索 IBM FlashSystem，請完成下列步驟：

準備環境：

- 若為舊型號，MCP（管理控制埠）必須處於作用中狀態，才能順利探索系統。
  - 如果要檢查系統是否處於作用中狀態，請執行下列指令：system status。
  - 有兩個 IP 位址，如果其中一個 IP 停止運作，系統會進入被動狀態。若要讓另一個乙太網路埠變成作用中，請執行下列指令 - sync activate。
  - 探索到的系統必須是管理 IP 位址及/或配置節點。

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼或使用者名稱 / SSH 金鑰鑑別。
- 服務帳戶可以使用任何有效的角色。建議具備**監視者**角色。

IBM ProtecTIER

如果要探索 ProtecTIER 裝置，請完成下列步驟：

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼。
- 服務帳戶必須具備管理者專用權。

IBM SVC、V7000/V3700 儲存體

如果要探索 SVC 和 V7000/V3700 裝置，請完成下列步驟：

存取清單的認證：

- 電腦系統：使用者名稱 / 密碼或使用者名稱 / 鑑別用的 SSH 金鑰。
- 服務帳戶可以使用任何有效的角色。建議具備**監視者**角色。

IBM TS3100 磁帶庫

如果要探索「TS3100 磁帶庫」裝置，請完成下列步驟：

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼。
- 服務帳戶必須具備管理者權限。

IBM TS3200 磁帶庫

如果要探索「TS3200 磁帶庫」裝置，請完成下列步驟：

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼。
- 服務帳戶必須具備管理者權限。

IBM TS3310 磁帶庫

如果要探索「TS3310 磁帶庫」裝置，請完成下列步驟：

準備環境：

- Web 服務一律配置成安全模式。

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼。
- 服務帳戶必須具備管理者權限。

IBM TS3494、TS3953 磁帶庫

如果要探索「TS3494、TS3953 磁帶庫」裝置，請完成下列步驟：

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼。
- 服務帳戶可具備最起碼的必要權限。

IBM TS3500、TS3584 磁帶庫

需要符合下列先決條件：

- 「TS3500 磁帶庫」的韌體層次必須是 8xxx（或更高）。
- 必須已安裝及啟用 Advanced Library Management System (ALMS)。


同時支援 SSL 和非 SSL 連線。

如果要探索「TS35xx 磁帶庫」裝置，請完成下列步驟：

準備環境：

- 可以將 TS3500 Web 介面配置成**無密碼保護**或**密碼保護**
  - 如果啟動了**密碼保護**，請依照下面**存取清單的認證**中的說明建立認證。

- 如果停用了**密碼保護**，則不需要任何認證。

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼。
- 服務帳戶必須具備管理者權限。

IBM TS4500 磁帶庫

需要符合下列先決條件：

- 「TS4500 磁帶庫」的韌體層次必須是 1.4.1.2 或更高（最高可達 1.7.0.0）。
- 必須已安裝及啟用 Advanced Library Management System (ALMS)。

同時支援 SSL 和非 SSL 連線。

如果要探索「TS4500 磁帶庫」裝置，請完成下列步驟：

準備環境：

- TS4500 Web 介面只能配置成**密碼保護**。

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼。
- 服務帳戶必須對映至**服務**角色。

IBM TS7700 磁帶庫

如果要探索「TS7700 磁帶庫」裝置，請完成下列步驟：

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼。
- 服務帳戶只需要**唯讀**權限。

IBM V7000 Unified 儲存體

如果要探索 V7000 Unified 裝置，請完成下列步驟：

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼。
- 服務帳戶可以使用任何有效的角色。建議具備**監視者**角色。

IBM XIV 儲存體

如果要探索 XIV 裝置，請完成下列步驟：

準備環境：

- 請確定儲存體管理程式容許使用遠端 **xcli** 指令。

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼。
- 服務帳戶必須具備**唯讀**使用者角色。

- 請注意，XIV 系統在「產生警示之前的無效登入嘗試次數」臨界值方面，可能偏低。如果您使用的認證集頗大，可能會超出此限制，因而會報告不必要的問題。請嘗試將 XIV 裝置分組成單一範圍集，並將其服務帳戶認證侷限在該範圍集內。

nSeries 或 NetApp 儲存體

如果要探索 nSeries 或 NetApp 裝置，請完成下列步驟：

準備環境：

- 如果系統配置了 Data ONTAP CLI、RLM CLI 和 SP CLI，則支援資料收集。不過，不支援 BMC CLI。
- **telnet.distinct.enable** 選項必須開啟。

存取清單的認證：

- 電腦系統：服務帳戶的使用者名稱 / 密碼。
- 服務帳戶可具備最起碼的必要權限。

防火牆注意事項

應用裝置與探索裝置之間的防火牆可能阻礙探索的完成與成功。

假設需要穿越防火牆，視使用者想要探索的裝置類型而定，可能得在防火牆中開啟埠。一般而言，埠 22 (SSH) 和 161 (SNMP) 應該開啟，且隨後接著下表中的一些適當埠（視支援的裝置而定）。

探索端點	**埠**	**介面 / 通訊協定**
多數	161	SNMP
儲存裝置		
DS6000 / DS8000	1750 (HTTP) 或 1751 (HTTPS)	DSCLI
DS3000 / DS4000 / DS5000	2463	SMCLI
XIV	7778	XCLI
nSeries 或 NetApp	22 / 23	SSH 或 Telnet
SVC 或 V7000/V3700	22	SSH
V7000 Unified	22	SSH
IBM TS3500	443 / 80	HTTPS 或 HTTP
IBM TS4500	443 / 80	HTTPS 或 HTTP
IBM TS7700	443 / 80	HTTPS 或 HTTP
IBM TS3100 / TS3200 / TS3310	80	HTTP
IBM TS3494、TS3953	23	Telnet
IBM ProtecTier	22	SSH
HP Storage	22 / 23	SSH 或 Telnet
IBM Flash System V9000	22	SSH

探索端點	埠	介面 / 通訊協定
EMC 公司儲存體 - CLARiion/VNX/VMAX	427 -（預設值）當容許 SLP 探索時，如果 SLP 探索已停用，則不會使用此埠。 HTTPS / HTTP 埠由 EMC SMI-S Provider 所配置；預設值是 5989 / 5988	SLP、HTTPS / HTTP
	您可以啟用或停用 SLP 探索選項，以透過 EMC SMI-S Provider 來探索 EMC 儲存裝置。	
EMC 公司儲存體 – EMC Data Domain	22	SSH*
作業系統和主機		
FSM	22 / 23	SSH 或 Telnet
CMM	22 / 23	SSH 或 Telnet
AMM	22 / 23	SSH 或 Telnet
HP Proliant 刀鋒伺服器（透過 HP OnBoard Administrator）	22 / 23	SSH 或 Telnet
IMM 和 IMM2	22 / 23	SSH 或 Telnet
適用於 HP Integrity 和 HP 9000 伺服器的 HP iLO	22 / 23	SSH* 或 Telnet
網路裝置		
Brocade	161 / 22 / 23	SNMP、SSH、Telnet
IBM b 型儲存區域網路 (SAN) 交換器	22 / 23	SSH、Telnet
Cisco	161 / 22 / 23	SNMP、SSH、Telnet

探索端點	埠	介面 / 通訊協定
BNT	22 / 23	SSH 或 Telnet
Juniper	22 / 23	SSH 或 Telnet
QLogic	22 / 23	SSH* 或 Telnet
Fortinet (FortiOS)	22 / 23	SSH 或 Telnet
Palo Alto Networks (PAN-OS)	443	HTTPS
F5 Big-IP (TMOS)	22 / 23	SSH 或 Telnet
Check Point	22 / 23	SSH 或 Telnet
作業系統 / 伺服器平台		
HMC	22	SSH
VIOS	22	SSH
AIX	22	SSH
Linux	22	SSH
Windows	445	SMBv1
VMware vCenter	443	HTTPS
VMware ESXi	443、5989	HTTPS
IVM	22 / 23	SSH 或 Telnet
IBM i	22	SSH
SUN	22	SSH

- 對於標示了 SSH* 的裝置，TSA 只支援 SSH 第 1 版。

探索作業問題

大部分的探索作業問題都是因存取權或授權問題所致。

最常見的存取權問題是因防火牆封鎖了對裝置上必要埠的存取權所造成。需要開啟和可呼叫到的埠，會因裝置類型而異。請參閱第 33 頁「防火牆注意事項」一節，以判斷哪些埠適用。

最常見的授權問題包括：

- **未定義任何認證**。請確定裝置的認證已定義在 TSA 中，且裝置上已建立適當的服務帳戶。
- **認證的使用者名稱或密碼不正確**。建立或編輯認證時使用**測試**功能來驗證認證是否有效。
- **認證密碼已過期**。
- **認證在裝置上缺乏必要的權限**。如果要判斷目標裝置的認證需求，請參閱第 9 頁裝置探索配置一節。
- **使用有效的認證類型**。對於 Windows 裝置，請建立「電腦系統 (Windows)」認證，而不是「電腦系統」認證。

- 請檢查**鑑別狀態**頁面（**工具 → 鑑別狀態**），查看是否有任何服務帳戶含有到期密碼或是已停止運作。

後續注意事項

當想要的網路部分已定義在 TSA 中，並已順利掃描之後，可依想要的排程，讓 TSA 維持執行定期的探索和傳輸。

以下是一些預期要有的後續活動：

- 定期與您的 IBM 業務代表一起檢閱 TSA 產生的報告。
- 定期透過 TSA 使用者介面執行備份，以儲存 TSA 配置副本。

這項作業不會儲存 TSA 所收集的資料。只會儲存配置資訊。

- 定期檢查**鑑別狀態**頁面（**工具 → 鑑別狀態**），以查看是否有任何服務帳戶認證含有到期密碼或是已停止運作。
- 當裝置上的服務帳戶密碼已更新時，請務必同時更新 TSA 中的密碼，以便讓 TSA 中的認證定義與目標裝置上的認證維持同步。
- 在安全原則允許的情況下，請考量在設置服務帳戶時，使其具有不會到期的密碼或使用 SSH 金鑰。如此就不必定期在 TSA 使用者介面中以及在裝置上，更新密碼。

疑難排解

用於 AMM 探索的作用中階段作業

AMM 裝置有一項設定，會限制同時作用中的階段作業數目（上限為 20）。如果這項設定不夠高到足以容許 TSA 建立階段作業，就無法探索 AMM 裝置。

如果要變更 AMM 裝置的作用中階段作業限制，請遵循下列步驟：

1. 在 Web 瀏覽器中鍵入 AMM 裝置的 IP 位址，以登入 AMM Web 介面。
2. 移至 **MM 控制 → 登入設定檔**。
3. 按一下 TSA 用來探索裝置的登入 ID。
4. 增加**同時作用中的階段作業數目上限**設定值。
5. 按一下頁面右下方的**儲存**。

附錄 A：術語與定義

假設讀者已深入瞭解「網際網路通訊協定 (IP)」網路和通訊協定。

術語	定義
探索裝置	是指可讓 TSA 探索之已部署的 IT 基礎架構元件。一般的裝置包括：伺服器、電腦系統（例如：IBM、Dell 和 HP）、「儲存體」元素，以及「網路」元素（例如：交換器、橋接器、路由器）。

附錄 B：雜項

使用者介面下載功能

在某些情況下，當使用 Web 瀏覽器時，「下載所有日誌」（從**活動日誌**頁面）、檔案下載（從**探索歷程**頁面），或是說明文件下載（從**說明文件**頁面）不會順利完成。如果要解決這個問題，請依照《IBM Technical Support Appliance 設置手冊》中的記載，嘗試切換至另一個支援的 Web 瀏覽器。如果無法選擇這樣做，請嘗試將您瀏覽器的內容設為其預設值。

附錄 C：VMware ESXi 的 CIM 提供者

CIM 提供者是一組 VMware ESXi 外掛程式，可收集 VMware ESXi 執行所在之伺服器相關的其他硬體和韌體資訊。TSA 與 VMware vCenter 兩者都能充分運用這項額外資訊。

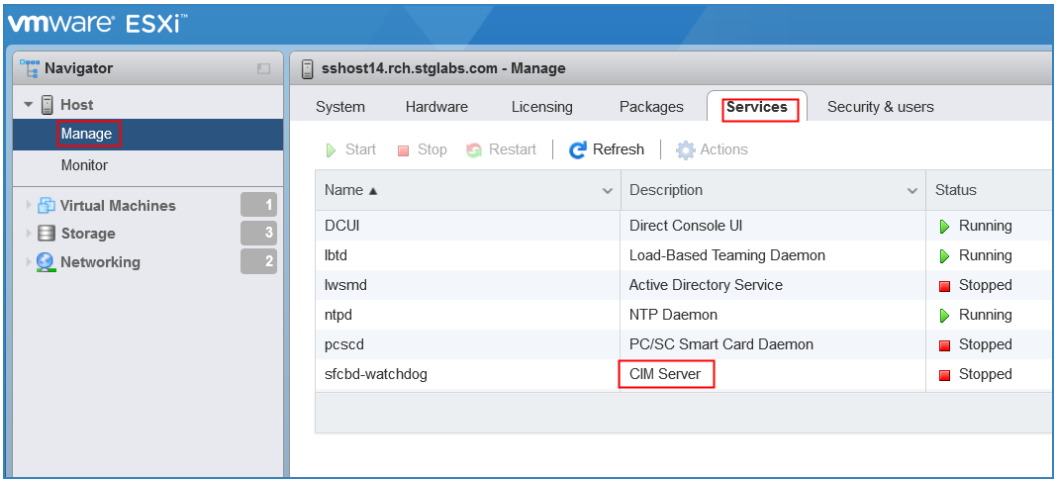
CIM 提供者外掛程式由伺服器和元件製造商所開發。為了確保 CIM 提供者外掛程式包含在 ESXi 中，請使用含有 CIM 提供者外掛程式的自訂安裝映像檔。如果現有的 VMware ESXi 實例未安裝 CIM 提供者，請從服務和元件製造商取得必要的外掛程式，並安裝至 ESXi。VMware 會提供一份清單，其中列出製造商所提供的各種外掛程式。

如需相關資訊，請參閱 https://www.vmware.com/resources/compatibility/pdf/vi_cim_guide.pdf。

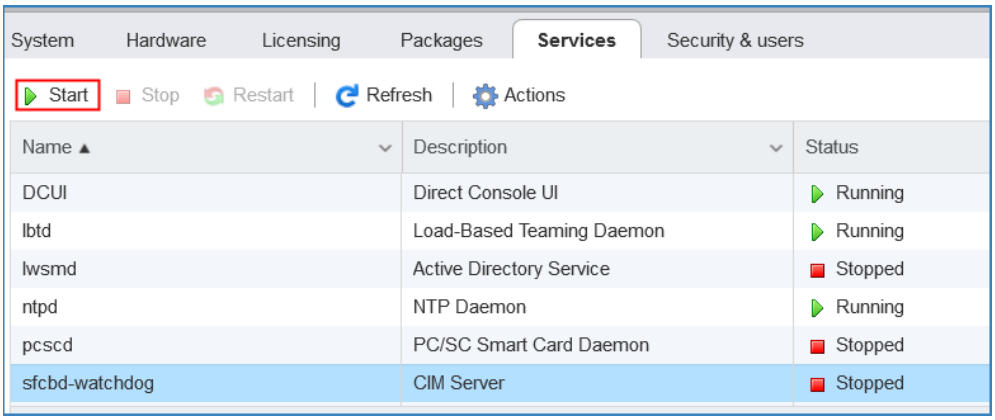
如果要判斷 CIM 提供者是否處於作用中，以及開啟 CIM 提供者（如果不在作用中），請逐一執行下列步驟。

在 VMware vSphere Web Client 上

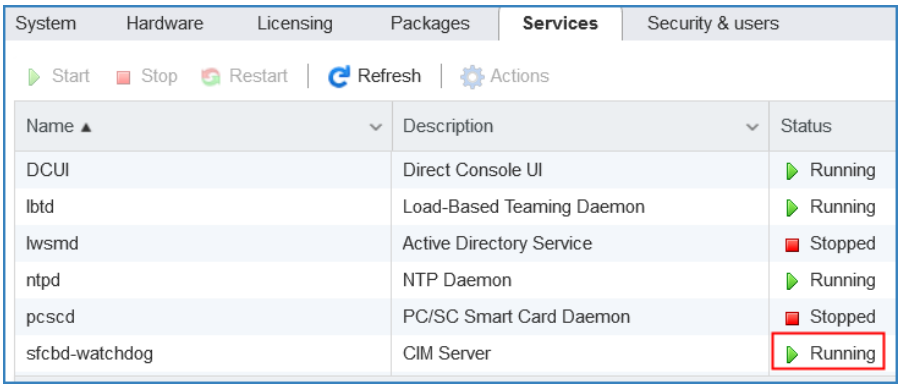
- 登入 VMware vSphere Web Client。
- 按一下左導覽視窗中的**主機 → 管理**，並在右窗格中選取**服務**標籤。
- 會顯示一組服務，其中包括 **CIM 伺服器**。



- 如果 **CIM 伺服器**處於**已停止**狀態，請選取它，並按一下**啟動**。

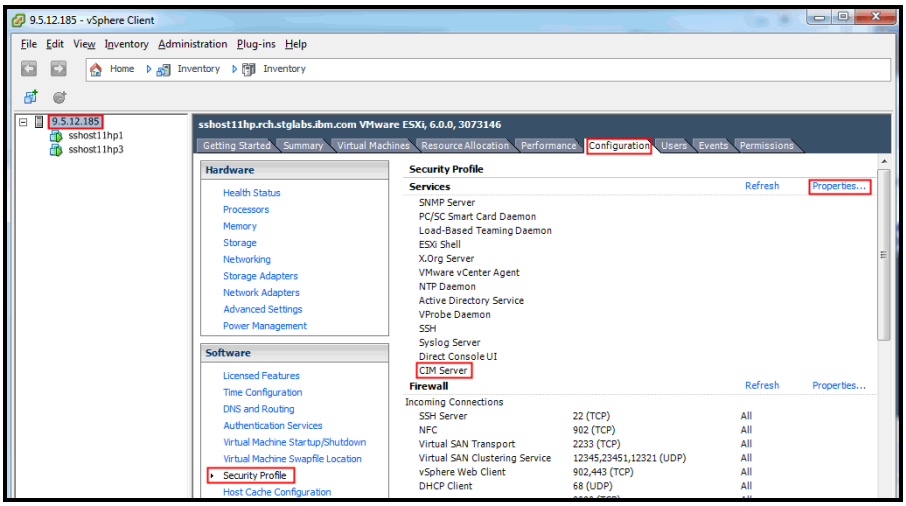


- 「CIM 伺服器」服務會啟動，且狀態會是**執行中**。

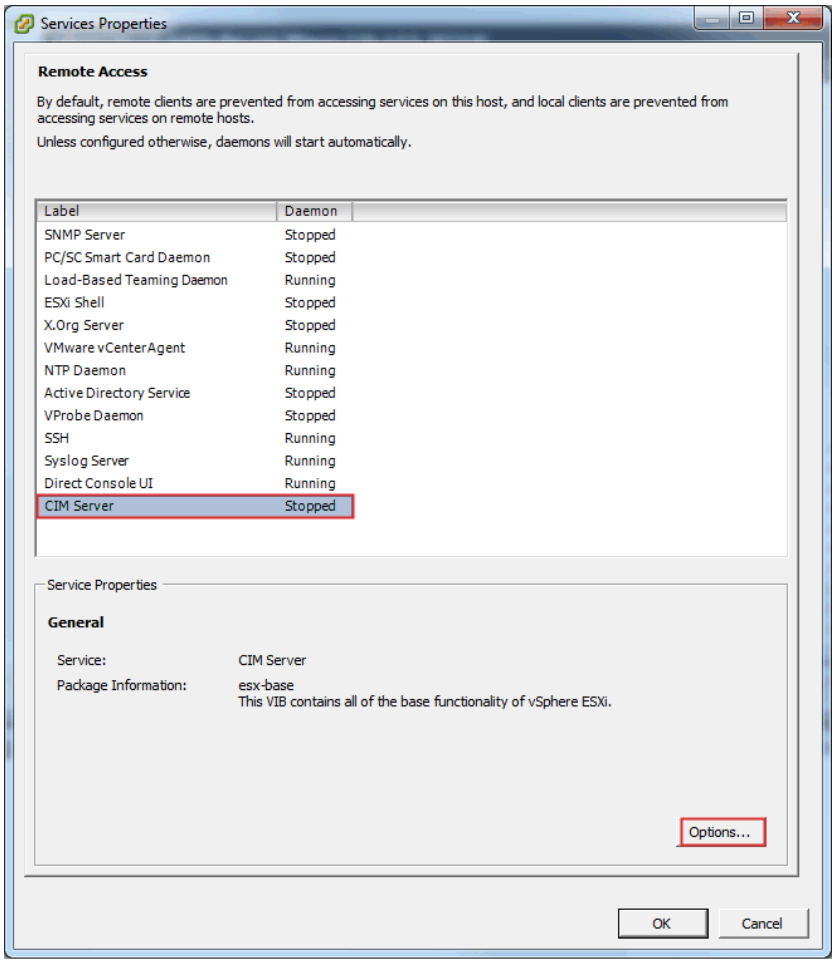


在 VMware vSphere Client 上

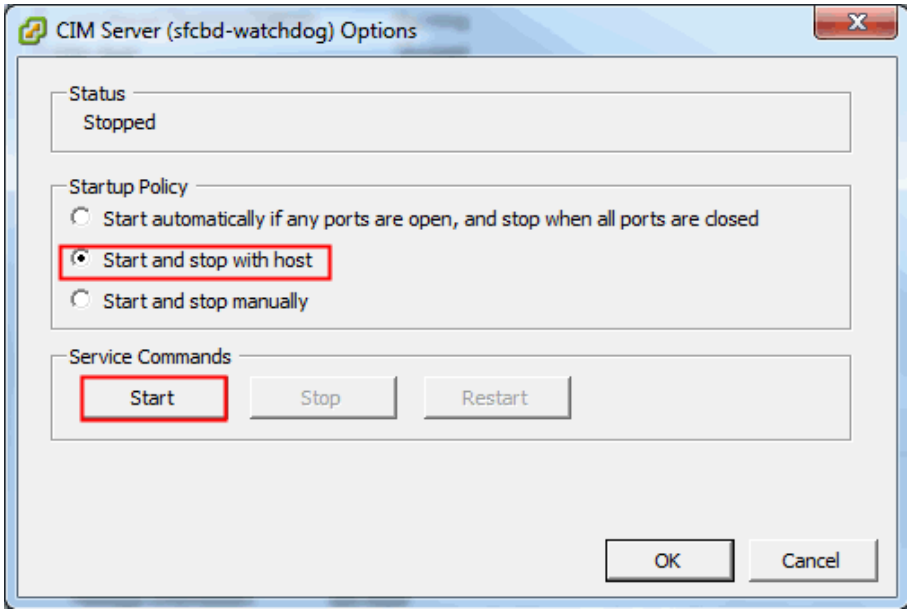
- 啟動 VMware vSphere Client。
- 按一下左導覽視窗中的 ESXi 伺服器 IP，並在右窗格中選取**配置**標籤。
- 從右窗格的**軟體**選擇功能表中，選取**安全設定檔**。在**服務**區段中，會顯示一組服務，其中包括 **CIM 伺服器**。



- 選取**服務**區段中的**內容...**項目。



- 如果 **CIM 伺服器**處於**已停止**狀態，請選取它，並按一下**選項...**。系統會顯示下列視窗。



- 選取**啟動原則（隨主機啟動及停止**選項），並按一下**啟動**以啟動「CIM 伺服器」。

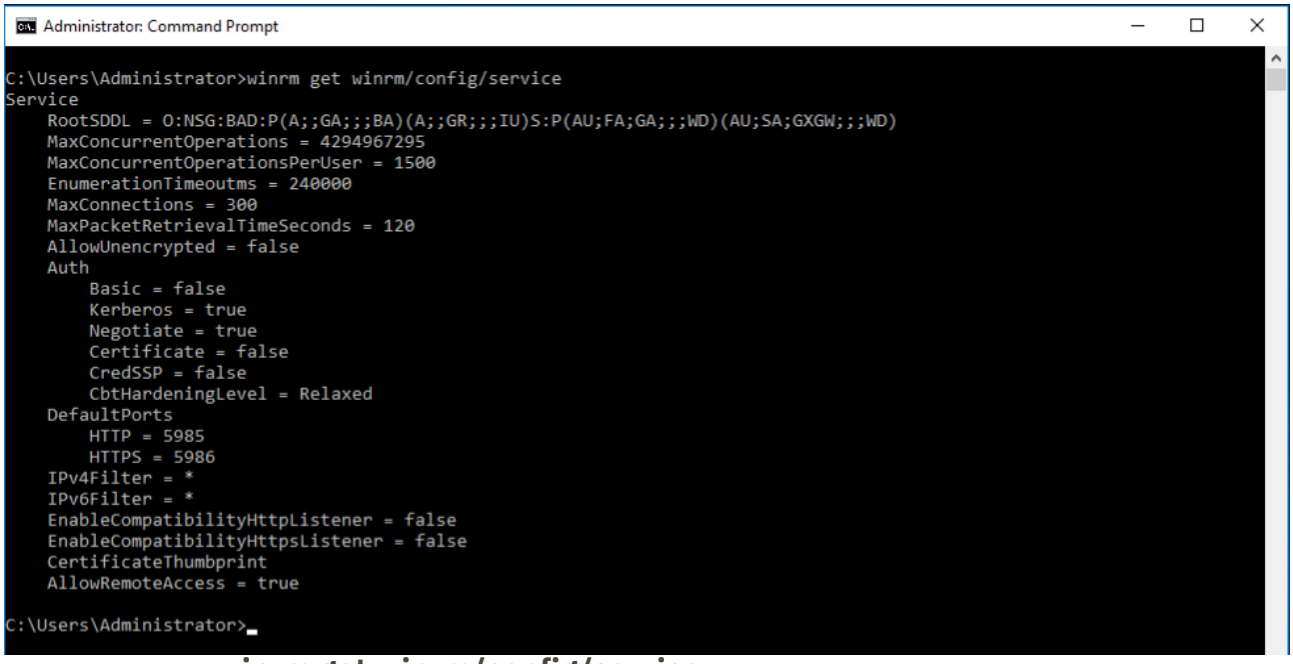
附錄 D：使用 WINRM 的 Windows

若為 Windows 2012 和 2016 Server，WINRM 服務會自動啟動。不過，依預設，不會啟用遠端管理。這裡簡要概述需執行哪些動作，以啟用 WINRM 來容許使用自簽憑證來進行遠端連線：

- 啟用 WINRM 以接受利用使用者 ID / 密碼進行鑑別的 HTTPS 連線
- 使自簽憑證與已啟用之 WINRM 的 HTTPS 接聽器產生關聯
- 修改 Windows 防火牆，以容許透過埠 5986（預設 WINRM HTTPS 埠）進行入埠連線

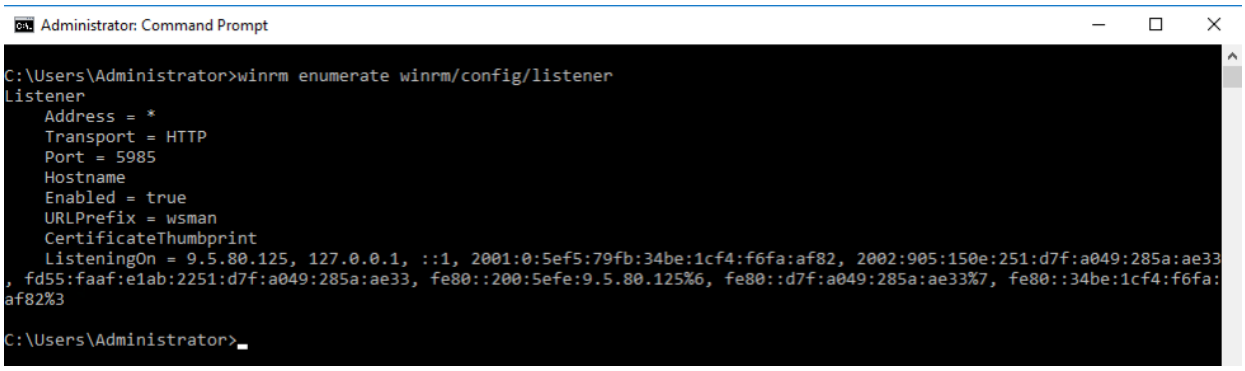
下列指令是準備 WINRM 以容許經由 HTTPS 進行遠端連線：

- 使用下列指令，判斷 WINRM 服務的現行狀態：



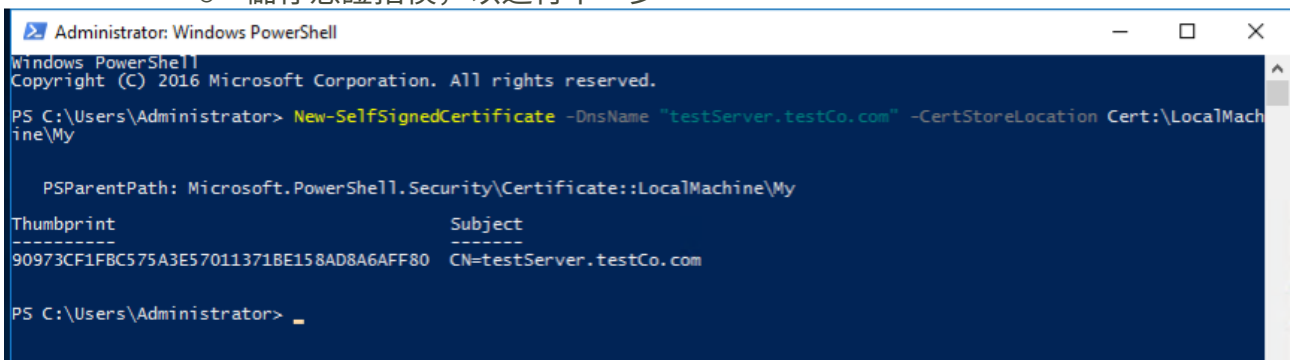
winrm get winrm/config/service

- **AllowUnencrypted** 的值必須是 *false*。若為 *true*，請使用下列指令來變更為 *false*：
  winrm set winrm/config/service @{AllowUnencrypted="false"}
- **Basic** 的值必須是 *true*。若為 *false*，請使用下列指令來變更為 *true*：
  winrm set winrm/config/service/auth @{Basic="true"}
- 使用此指令判斷 WINRM 是否具有 HTTPS 接聽器：
  winrm enumerate winrm/config/listener



- 在上述指令範例中，只存在 HTTP 接聽器，因此需要配置 HTTPS 接聽器。如果 HTTPS 接聽器未配置而要啟用的話，請執行下列動作：
  - 使用 PowerShell，建立自簽憑證：
    New-SelfSignedCertificate -DnsName "myHost@myBusiness.com" -CertStoreLocation Cert:\LocalMachine\My

    將上述範例中的 DnsName **(myHost@myBusiness.com)** 取代為 Windows 伺服器的 Windows 完整網域名稱。
  - 儲存憑證指模，以進行下一步



- 建立 HTTPS 接聽器：
  winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="myHost@myBusiness.com"; CertificateThumbprint="[COPIED_CERTIFICATE_THUMBPRINT]"}
- 檢查確定 HTTPS 現在已配置：
  winrm enumerate winrm/config/listener
- 修改 Windows 防火牆，以容許指向 WINRM 的入埠遠端連線：
  - 移至**控制面板 → 系統與安全 → Windows 防火牆**
  - 按一下**進階設定。**系統會顯示**具有進階安全性的 Windows 防火牆**視窗。
  - 按一下**輸入規則**。
  - 選取**動作**功能表，並按一下**新增規則**。會顯示**新增輸入規則精靈。**
  - 選取**連接埠**，並按**下一步。**
  - 選取 **TCP → 特定本機連接埠**，並指定 5986。按**下一步。**
  - 選取**允許連線**選項，並按**下一步。**
  - 選取**網域、專用、公用**勾選框（如果尚未勾選）並按**下一步。**

- 為新規則命名，例如 Windows Remote Management (HTTPS-In)，並按一下**完成**。

注意事項

IBM Corporation
Marketing Communications
Systems and Technology Group
Route 100
Somers, New York 10589
美國出版
2020 年 8 月。

本文件係針對 IBM 在美國所提供之產品和/或服務所開發。在其他國家，IBM 不見得有提供本文件所提及之各項產品、功能或服務。

本資訊如有變動，恕不另行通知。請洽詢當地的 IBM 業務人員，以取得當地提供的產品、功能和服務之相關資訊。

一切關於 IBM 未來方針或目的之聲明，隨時可能變更或撤銷，不必另行通知，且僅代表目標與主旨。

IBM、IBM 標誌、POWER、System I、System p、i5/OS 是 International Business Machines Corporation 在美國及/或其他國家或地區的商標或註冊商標。IBM 所擁有的美國商標的完整清單可在此處取得：http://www.ibm.com/legal/copytrade.shtml。

其他公司、產品及服務名稱，可能是第三者的商標或服務標誌。

IBM 硬體產品，係以全新組件或新舊組件混用製成。但均適用 IBM 的保固條款。

此設備受限於 FCC 規則。在最終交付給買方之前，設備將遵守適當的 FCC 規則。

本文件所提及之非 IBM 產品資訊，係取自這些產品的供應商。

有關非 IBM 產品的性能問題，應直接洽詢供應商。

IBM 在網際網路上的首頁位於：http://www.ibm.com。

IBM System p 在網際網路上的首頁位於：http://www.ibm.com/systems/p。

IBM System I 在網際網路上的首頁位於：http://www.ibm.com/systems/i。

PSW03007-TWZH-00