整合式管理模組 I
使用手冊

整合式管理模組 I
使用手冊

第七版（**2013** 年 **5** 月）

目錄

表

第 1 章 簡介

整合式管理模組 (IMM) 會將服務處理器功能、Super I/O、視訊控制器和遠端顯示功能合併在伺服器主機板上的單一晶片中。IMM 會取代 IBM® System x 伺服器中的基板管理控制器 (BMC) 和 Remote Supervisor Adapter II。

在 IBM 伺服器中使用 IMM 之前，基板管理控制器 (BMC) 和基本輸入/輸出系統 (BIOS) 是標準系統管理硬體和韌體。System x 伺服器使用 BMC 服務處理器來管理系統管理軟體與平台硬體之間的介面。Remote Supervisor Adapter II 和 Remote Supervisor Adapter II Slimline 是用於頻外伺服器管理的選用控制器。

重要事項：雖然 IMM 在部分 IBM BladeCenter 產品和 IBM 刀鋒伺服器中是標準配置，但 BladeCenter 進階管理模組仍保留用於 BladeCenter 和刀鋒伺服器的系統管理功能和鍵盤/視訊/滑鼠 (KVM) 多工的主要管理模組。與「IMM Web 介面」及「指令行介面」相關的內容，不適用於 IBM BladeCenter 及刀鋒伺服器。想要在刀鋒伺服器上配置 IMM 設定的使用者，應在刀鋒伺服器上使用 Advanced Settings Utility (ASU) 來執行這些動作。

IMM 提供了對 BMC 和 Remote Supervisor Adapter II 的合併功能的數項改進：

- 可選擇專用或共用乙太網路連線。專用乙太網路連線不可用於刀鋒伺服器或部分 System x 伺服器。

  註：您的伺服器可能未提供專用的系統管理網路埠。如果您的硬體沒有專用的網路埠，*shared* 設定是唯一可用的 IMM 設定。
- 一個用於「智慧型平台管理介面 (IPMI)」和服務處理器介面的 IP 位址。此特性不適用於刀鋒伺服器。
- Embedded Dynamic System Analysis (DSA)。
- 可以從本機或遠端更新其他實體，而不需要重新啓動伺服器來起始更新處理程序。
- 使用 Advanced Settings Utility (ASU) 進行遠端配置。此特性不適用於刀鋒伺服器。
- 可在頻內或頻外存取 IMM 的應用程式和工具的功能。刀鋒伺服器僅支援頻內 IMM 連線。
- 加強的遠端顯示功能。此特性不適用於刀鋒伺服器。

IBM System x® Server Firmware 是 IBM 的 Unified Extensible Firmware Interface (UEFI) 的實作。它取代 System x 伺服器和 IBM 刀鋒伺服器中的 BIOS。BIOS 是控制基本硬體作業（如與軟式磁碟機、硬碟和鍵盤的互動）的標準韌體程式碼。IBM System x Server Firmware 提供了數項 BIOS 沒有的特性，包括 UEFI 2.1 相符性、iSCSI 相容性、Active Energy Manager 技術及加強的可靠性和服務功能。Setup Utility 提供了伺服器資訊、伺服器設定、自訂作業相容性，並建立了開機裝置順序。

注意事項：

- 在本文件中，IBM System x Server Firmware 通常稱爲伺服器韌體，有時稱爲 UEFI。
- IBM System x Server Firmware 與非 UEFI 作業系統完全相容。
- 如需使用 IBM System x Server Firmware 的相關資訊，請參閱伺服器隨附的文件。

本文件說明如何使用 IBM 伺服器中 IMM 的功能。IMM 會與 IBM System x Server Firmware 搭配運作，以提供 System x 和 BladeCenter 伺服器的系統管理功能。

本文件不包含錯誤或訊息的說明。伺服器隨附的《*問題判斷與服務手冊*》中對 IMM 錯誤和訊息進行了說明。若要在「IBM® 支援中心入口網站」上尋找本文件或 IBM 白皮書 *Transitioning to UEFI and IMM* 的最新版本，請完成下列步驟。

註：第一次存取 IBM Support Portal 時，您必須選擇適用於您的伺服器的產品種類、系列產品和型號。下次存取 IBM Support Portal 時，您最初選取的產品會由網站預載，且僅顯示適用於您的產品的鏈結。若要變更或新增至您的產品清單，請按一下**管理我的產品清單**鏈結。

IBM 網站會定期進行變更。尋找韌體和文件的程序可能與本文件的說明略有不同。

1. 請造訪 http://www.ibm.com/support/entry/portal。
2. 在**選擇產品**下，選取**瀏覽產品**，然後展開**硬體**。
3. 視您的伺服器類型而定，按一下 **Systems** > **System x** 或 **Systems** > **BladeCenter**，然後勾選適用於您的伺服器的方框。
4. 在**選擇作業** 下，按一下**文件**。
5. 在**查看結果** 下，按一下**檢視頁面**。
6. 在「文件」方框中，按一下**更多結果**。
7. 在「種類」方框中，選取**整合式管理模組 (IMM)**勾選框。畫面上會出現 IMM 和 UEFI 文件的鏈結。

如果韌體更新項目已可供使用，您可以從 IBM 網站下載它們。IMM 可能具有文件中未說明的特性，因此可能會不定期更新該文件來併入那些特性的相關資訊，或者，也可能透過技術更新項目的形式提供 IMM 文件中未包含的其他資訊。

若要查看韌體更新項目，請完成下列步驟。

註：第一次存取 IBM Support Portal 時，您必須選擇適用於您的伺服器的產品種類、系列產品和型號。下次存取 IBM Support Portal 時，您最初選取的產品會由網站預載，且僅顯示適用於您的產品的鏈結。若要變更或新增至您的產品清單，請按一下**管理我的產品清單**鏈結。

IBM 網站會定期進行變更。尋找韌體和文件的程序可能與本文件的說明略有不同。

1. 請造訪 http://www.ibm.com/support/entry/portal。
2. 在**選擇產品**下，選取**瀏覽產品**，然後展開**硬體**。
3. 視您的伺服器類型而定，按一下 **Systems** > **System x** 或 **Systems** > **BladeCenter**，然後勾選適用於您的伺服器的方框。
4. 在**選擇作業**下，按一下**下載**。
5. 在**查看結果** 下，按一下**檢視頁面**。
6. 在「Flash 與警示」方框中，按一下適用的下載的鏈結，或按一下**更多結果**以查看其他鏈結。

IMM 特性

IMM 提供了下列功能：

- 全天候遠端存取和管理您的伺服器
- 獨立於受管理伺服器狀態的遠端管理
- 遠端控制硬體和作業系統
- 使用標準 Web 瀏覽器進行 Web 型管理

IMM 提供了兩種類型的 IMM 功能：IMM Standard 特性和 IMM Premium 特性。如需伺服器中 IMM 硬體類型的相關資訊，請參閱伺服器隨附的文件。

IMM Standard 特性

註：下列部分特性不適用於刀鋒伺服器。

- 重要伺服器設定的存取權
- 伺服器重要產品資料 (VPD) 的存取權
- 進階 Predictive Failure Analysis (PFA) 支援
- 自動通知和警示
- 持續的性能監視和控制
- 可選擇專用或共用乙太網路連線（如果適用的話）。

  註：您的伺服器可能未提供專用的系統管理網路埠。
- 網域名稱系統 (DNS) 伺服器支援
- 動態主機配置通訊協定 (DHCP) 支援
- 電子郵件警示
- Embedded Dynamic System Analysis (DSA)
- 加強的使用者權限層級
- 用於 IMM 頻內通訊的 LAN over USB
- 可以進行時間戳記、儲存在 IMM 上，以及可以附加至電子郵件警示的事件日誌
- 業界標準的介面和通訊協定
- OS 監視器
- 透過 Advanced Settings Utility (ASU) 進行遠端配置
- 遠端韌體更新
- 遠端電源控制
- 無縫的遠端加速圖形
- 安全的 Web 伺服器使用者介面
- Serial over LAN
- 伺服器主控台重新導向
- 簡易網路管理通訊協定 (SNMP) 支援
- 使用「輕量型目錄存取通訊協定 (LDAP)」伺服器的安全連線進行使用者鑑別

IMM Premium 特性

註：下列部分特性不適用於刀鋒伺服器。

- 重要伺服器設定的存取權
- 伺服器重要產品資料 (VPD) 的存取權
- 進階 Predictive Failure Analysis (PFA) 支援
- 自動通知和警示
- 持續的性能監視和控制
- 可選擇專用或共用乙太網路連線（如果適用的話）。

  註：您的伺服器可能未提供專用的系統管理網路埠。
- 網域名稱系統 (DNS) 伺服器支援
- 動態主機配置通訊協定 (DHCP) 支援
- 電子郵件警示
- Embedded Dynamic System Analysis (DSA)
- 加強的使用者權限層級
- 用於 IMM 頻內通訊的 LAN over USB
- 可以進行時間戳記、儲存在 IMM 上，以及可以附加至電子郵件警示的事件日誌
- 業界標準的介面和通訊協定
- OS 監視器
- 透過 Advanced Settings Utility (ASU) 進行遠端配置
- 遠端韌體更新
- 遠端電源控制
- 無縫的遠端加速圖形
- 安全的 Web 伺服器使用者介面
- Serial over LAN
- 伺服器主控台重新導向
- 簡易網路管理通訊協定 (SNMP) 支援
- 使用「輕量型目錄存取通訊協定 (LDAP)」伺服器的安全連線進行使用者鑑別
- 遠端顯示，包括遠端控制伺服器
- Web 介面中的作業系統失敗畫面擷取和顯示
- 遠端磁碟，可連接軟式磁碟機、CD/DVD 光碟機、USB 快閃記憶體隨身碟或伺服器的磁碟映像檔

註：下列 Remote Supervisor Adapter II 的特性不在 IMM 中：
- 顯示伺服器 MAC 位址
- 多個 NTP 伺服器項目

從 IMM Standard 升級至 IMM Premium

如果您的伺服器具有 IMM Standard 功能，您可以購買虛擬媒體鎖並安裝在您的伺服器主機板上，從而升級至 IMM Premium。不需要新的韌體。

若要訂購虛擬媒體鎖，請造訪 http://www.ibm.com/systems/x/newgeneration。

註：如需安裝虛擬媒體鎖的相關資訊，請參閱伺服器隨附的文件。

如果您需要訂單方面的協助，請撥打零售商零件頁上所列出的免付費電話，或是聯絡您當地的 IBM 業務代表取得協助。

將 IMM 與 System x 伺服器中的其他系統管理硬體比較

下表將 IMM 特性與 System x 伺服器中的 BMC 和 Remote Supervisor Adapter II 特性比較。

註：與 BMC 相似，IMM 使用標準 IPMI 規格。

表 1. IMM 特性與 System x 伺服器中結合的 BMC 和 Remote Supervisor Adapter II 特性的比較

說明	BMC 與 Remote Supervisor Adapter II	IMM
網路連線	BMC 使用與伺服器和不同於 Remote Supervisor Adapter II IP 位址的 IP 位址的網路連線。 Remote Supervisor Adapter II 使用專用的系統管理網路連線和不同於 BMC IP 位址的 IP 位址。	IMM 透過相同的網路連線提供 BMC 和 Remote Supervisor Adapter II 功能。一個 IP 位址用於這兩種功能。如果您的伺服器具有專用的系統管理網路埠，您可以選擇專用的或共用的網路連線。 **註**：您的伺服器可能未提供專用的系統管理網路埠。如果您的硬體沒有專用的網路埠，*shared* 設定是唯一可用的 IMM 設定。
更新功能	每一個伺服器都需要 BMC 和 Remote Supervisor Adapter II 的唯一更新項目。 可以在頻內更新 BIOS 和診斷工具。	一個 IMM 韌體映像檔可以用於所有適用的伺服器。 在頻內和頻外都可以更新 IMM 韌體、System x 伺服器韌體和「動態系統分析 (DSA)」韌體。 IMM 可以從本機或遠端更新本身、伺服器韌體及 DSA 韌體，而無需重新啓動伺服器來起始更新處理程序。
配置功能	僅在頻內提供具有 ASU 的配置變更。系統需要 BMC、Remote Supervisor Adapter II 及 BIOS 的個別配置。	ASU 可以在頻內或頻外執行，且可以配置 IMM 和伺服器韌體。使用 ASU，您也可以修改開機順序、iSCSI 和 VPD（機型、序號、UUID 和資產 ID）。 伺服器韌體配置設定由 IMM 保留。因此，您可以在伺服器關閉或作業系統正在執行時，進行伺服器韌體配置變更，且這些變更會在下次啓動伺服器時生效。 您可以透過下列 IMM 使用者介面，在頻內或頻外配置 IMM 配置設定： • Web 介面 • 指令行介面 • IBM Systems Director 介面 • SNMP

表 1. IMM 特性與 System x 伺服器中結合的 BMC 和 Remote Supervisor Adapter II 特性的比較 (繼續)

說明	BMC 與 Remote Supervisor Adapter II	IMM
作業系統畫面擷取	在作業系統發生故障時，Remote Supervisor Adapter II 會執行畫面擷取。畫面擷取的顯示需要 Java Applet。	此特性僅用於 IMM Premium。如需從 IMM Standard 升級至 IMM Premium 的相關資訊，請參閱第 4 頁的『從 IMM Standard 升級至 IMM Premium』。 Web 瀏覽器直接顯示畫面擷取，而無需 Java Applet。
錯誤記載	BMC 提供了 BMC 系統事件日誌（IPMI 事件日誌）。 Remote Supervisor Adapter II 提供了文字型日誌，其中包括 BMC 報告的事件說明。此日誌還包含 Remote Supervisor Adapter II 本身偵測到的任何資訊或事件。	IMM 具有兩個事件日誌： 1. IPMI 介面提供了系統事件日誌。 2. 其他 IMM 介面提供了機箱事件日誌。機箱事件日誌顯示使用「分散式管理工作小組」規格 DSP0244 和 DSP8007 產生的文字訊息。 **註**：如需特定事件或訊息的說明，請參閱伺服器隨附的*《問題判斷與服務手冊》*。
監視	具有 Remote Supervisor Adapter II 的 BMC 具有下列監視功能： • 監視伺服器和電池電壓、伺服器溫度、風扇、電源供應器以及處理器和 DIMM 狀態 • 風扇速度控制 • Predictive Failure Analysis (PFA) 支援 • 系統診斷 LED 控制（電源、硬碟、活動、警示、活動訊號） • 自動伺服器重新啓動 (ASR) • 自動 BIOS 回復 (ABR)	IMM 提供了與 BMC 和 Remote Supervisor Adapter II 相同的監視功能。在 RAID 配置中使用時，IMM 支援展開的硬碟狀態，包括磁碟機 PFA。

表 1. IMM 特性與 System x 伺服器中結合的 BMC 和 Remote Supervisor Adapter II 特性的比較 (繼續)

說明	BMC 與 Remote Supervisor Adapter II	IMM
遠端顯示	具有 Remote Supervisor Adapter II 的 BMC 具有下列遠端顯示功能： • 透過 LAN 的圖形主控台重新導向 • 遠端虛擬磁片和 CD-ROM • PCI 視訊、鍵盤和滑鼠的高速遠端重新導向 • 支援最高 1024 x 768（頻率爲 70 Hz）的視訊解析度 • 資料加密	此特性僅用於 IMM Premium。如需從 IMM Standard 升級至 IMM Premium 的相關資訊，請參閱第 4 頁的『從 IMM Standard 升級至 IMM Premium』。 除了 Remote Supervisor Adapter II 遠端顯示特性，IMM 還具有下列功能。 **註**：IMM 需要 Java Runtime Environment 1.5 版或更新版本，或者 ActiveX（如果 Windows 中使用了 Internet Explorer）。 • 支援最高 1280 x 1024（頻率爲 75 Hz）的視訊解析度 • USB 2.0 支援虛擬鍵盤、滑鼠和大量儲存裝置 • 15 位元色彩深度 • 可選擇絕對或相對滑鼠模式 • USB 快閃記憶體隨身碟支援 • Remote Control 視窗上的伺服器電腦和重設項 • Remote Control 視窗上的視訊可以儲存在檔案中 IMM 提供了兩個個別用戶端視窗。一個用於視訊與鍵盤和滑鼠互動，另一個用於虛擬媒體。 IMM Web 介面具有可調整色彩深度以減少低頻寬狀況下傳輸的資料的功能表項目。Remote Supervisor Adapter II 介面具有頻寬調節器。
安全	Remote Supervisor Adapter II 具有進階安全特性，包括 Secure Sockets Layer (SSL) 和加密。	IMM 具有與 Remote Supervisor Adapter II 相同的安全特性。

表 1. IMM 特性與 System x 伺服器中結合的 BMC 和 Remote Supervisor Adapter II 特性的比較 (繼續)

說明	BMC 與 Remote Supervisor Adapter II	IMM
序列重新導向	IPMI Serial over LAN (SOL) 功能是 BMC 的標準功能。 Remote Supervisor Adapter II 可讓您將伺服器序列資料重新導向至 Telnet 或 SSH 階段作業。 **註**：部分伺服器未提供此特性。	COM1 埠用於 System x 伺服器上的 SOL。COM1 僅可透過 IPMI 介面進行配置。 COM2 埠用於透過 Telnet 或 SSH 的序列重新導向。COM2 可透過所有 IMM 介面（除 IPMI 介面之外）進行配置。COM2 埠用於刀鋒伺服器上的 SOL。 這兩種 COM 埠配置僅限於 8 個資料位元、空值同位檢查、1 個停止位元，以及 9600、19200、38400、57600、115200 或 230400 的傳輸速率選擇。 在刀鋒伺服器上，COM2 埠是無外部存取權的內部 COM 埠。IPMI 序列埠不能在刀鋒伺服器上共用。 在機架裝載式和直立式伺服器上，IMM COM2 埠是無外部存取權的內部 COM 埠。
SNMP	SNMP 支援僅限於 SNMPv1。	IMM 支援 SNMPv1 和 SNMPv3。

具有 BladeCenter 進階管理模組的 IMM

BladeCenter 進階管理模組是 IBM BladeCenter 和 IBM 刀鋒伺服器的標準系統管理介面。雖然 IMM 現在包含在部分 IBM BladeCenter 和 IBM 刀鋒伺服器中，但進階管理模組仍保留用於 BladeCenter 和刀鋒伺服器的系統管理功能和鍵盤、視訊及滑鼠 (KVM) 多工的管理模組。BladeCenter 未提供 IMM 的外部網路介面。

刀鋒伺服器沒有 IMM 的外部網路存取權。進階管理模組必須用於刀鋒伺服器的遠端管理。IMM 取代過去刀鋒伺服器產品中 BMC 及「並行鍵盤、視訊和滑鼠 (cKVM)」選項卡的功能。

Web 瀏覽器和作業系統需求

IMM Web 介面需要 Java™ 外掛程式 1.5 版或更新版本（用於遠端顯示特性）和下列其中一個 Web 瀏覽器：

- 具有最新版 Service Pack 的 Microsoft Internet Explorer 6.0、7.0 或 8.0 版。不支援 8.0 之後的版本。
- Mozilla Firefox 1.5 版或更新版本

下列伺服器作業系統具有 USB 支援（遠端顯示特性需要）：

- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008
- Microsoft Windows Server 2003
- Red Hat Enterprise Linux 4.0 版和 5.0 版
- SUSE Linux 10.0 版

- Novell NetWare 6.5

註：IMM Web 介面不支援雙位元組字元集 (DBCS) 語言。

本書使用的注意事項

文件使用了下列注意事項：

- **附註**：這些注意事項提供重要的提示、指引或建議。
- **重要事項**：這些注意事項提供的資訊或建議，有助於排除疑難或有問題的狀況。
- **注意**：這些注意事項指出可能對程式、裝置或資料造成的損壞。此注意事項出現在可能造成損壞的指示或狀況前面。

第 2 章 開啓和使用 IMM Web 介面

IMM 將服務處理器功能、視訊控制器及遠端顯示功能（安裝選用虛擬媒體金鑰時）結合在單一晶片中。若要使用 IMM Web 介面從遠端存取 IMM，您必須先登入。本章說明您可以從 IMM Web 介面執行的登入程序和動作。

存取 IMM Web 介面

IMM 支援靜態和「動態主機配置通訊協定 (DHCP)」IPv4 定址。指派給 IMM 的預設靜態 IPv4 位址爲 192.168.70.125。IMM 最初配置爲嘗試從 DHCP 伺服器取得位址，如果無法取得，則使用靜態 IPv4 位址。

IMM 也支援 IPv6，但依預設，IMM 沒有固定的靜態 IPv6 IP 位址。對於 IPv6 環境中 IMM 的起始存取權，您可以使用 IPv4 IP 位址或 IPv6 鏈結本端位址。IMM 會產生唯一的鏈結本端 IPv6 位址，該位址顯示在「網路介面」頁面上的 IMM Web 介面中。鏈結本端 IPv6 位址具有與下列範例相同的格式。

```
fe80::21a:64ff:fee6:4d5
```

存取 IMM 時，下列 IPv6 狀況設爲預設值：

- 啓用自動 IPv6 位址配置。
- 停用 IPv6 靜態 IP 位址配置。
- 啓用 DHCPv6。
- 啓用無狀態自動配置。

IMM 可讓您選擇專用的系統管理網路連線（如果適用的話），或與伺服器共用的連線。機架裝載式和直立式伺服器的預設連線是使用專用的系統管理網路接頭。

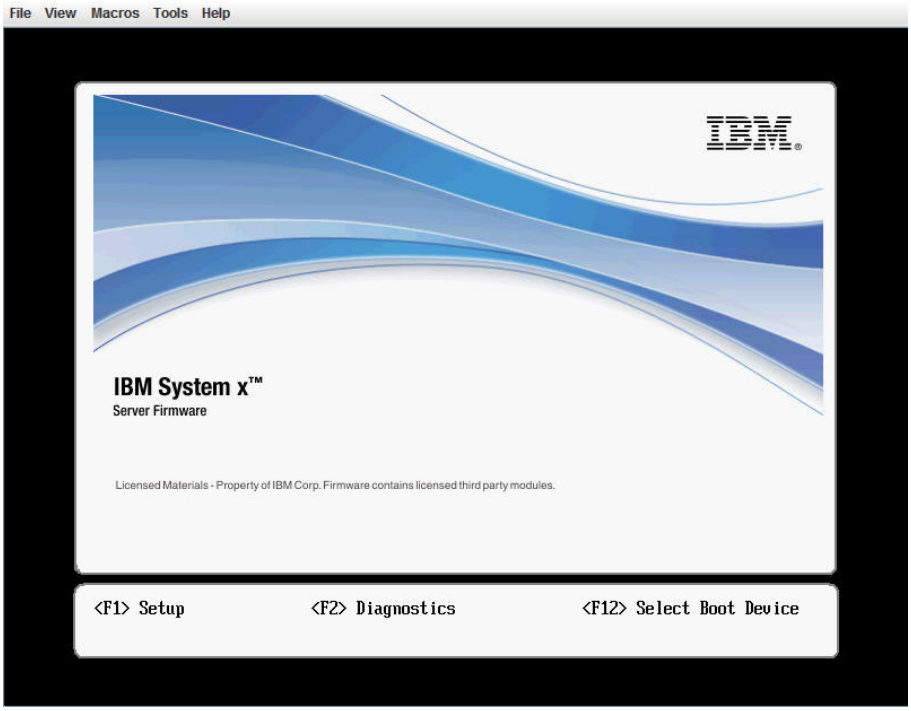
註：您的伺服器可能未提供專用的系統管理網路埠。如果您的硬體沒有專用的網路埠，*shared* 設定是唯一可用的 IMM 設定。

透過 IBM System x Server Firmware Setup Utility 設定 IMM 網路連線

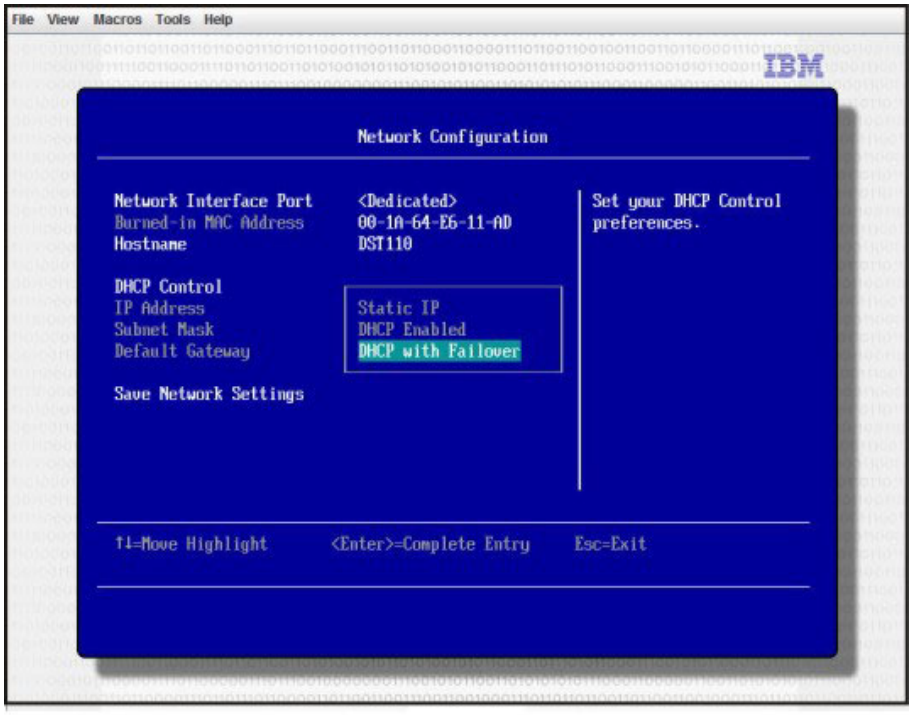
啓動伺服器後，您可以使用 Setup Utility 來選取 IMM 網路連線。必須將具有 IMM 硬體的伺服器連接至「動態主機配置通訊協定 (DHCP)」伺服器，或者必須將伺服器網路配置爲使用 IMM 靜態 IP 位址。若要透過 Setup Utility 設定 IMM 網路連線，請完成下列步驟：

1. 開啓伺服器。畫面上會顯示 IBM System x Server Firmware 歡迎使用畫面。

註：在伺服器接通 AC 電源大約 2 分鐘後，電源控制按鈕就會變成作用中狀態。



2. 顯示 <F1> Setup 提示時，請按 F1 鍵。如果您已設定開機密碼和管理者密碼，您必須輸入管理者密碼，才能存取完整的 Setup Utility 功能表。
3. 從 Setup Utility 主功能表，選取 **System Settings**。
4. 在下一個畫面上，選取 **Integrated Management Module**。
5. 在下一個畫面上，選取 **Network Configuration**。
6. 強調顯示 **DHCP Control**。**DHCP Control** 欄位中有三個 IMM 網路連線選項：
   - Static IP
   - DHCP Enabled
   - DHCP with Failover（預設值）



7. 選取其中一個網路連線選項。
8. 如果您選擇使用靜態 IP 位址，則必須指定 IP 位址、子網路遮罩及預設閘道。
9. 您也可以使用 Setup Utility 來選取專用網路連線（如果您的伺服器具有專用網路埠），或選取共用 IMM 網路連線。

   注意事項：

   - 專用系統管理網路埠在您的伺服器上可能無法使用。如果您的硬體沒有專用網路埠，則 *shared* 設定是唯一可用的 IMM 設定。在 **Network Configuration** 畫面上，於 **Network Interface Port** 欄位中選取 **Dedicated**（如果適用的話）或 **Shared**。
   - 若要尋找您伺服器上 IMM 所使用的乙太網路接頭的位置，請參閱伺服器隨附的文件。
10. 選取 **Save Network Settings**。
11. 結束 Setup Utility。

注意事項：

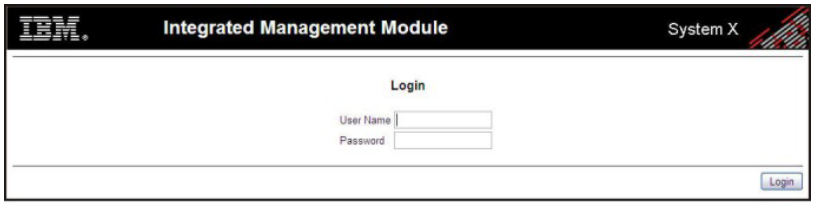
- 您必須等待大約 1 分鐘的時間以便變更生效，之後伺服器韌體方能再次運作。
- 您也可以透過 IMM Web 介面配置 IMM 網路連線。如需相關資訊，請參閱第 33 頁的『配置網路介面』。

登入 IMM

重要事項：IMM 最初設定的使用者名稱和密碼分別爲 USERID 和 PASSW0RD（當中所含的是數字 0，不是字母 O）。此預設使用者設定具有 Supervisor 存取權。請在起始配置期間變更此預設密碼，以獲得加強安全性。

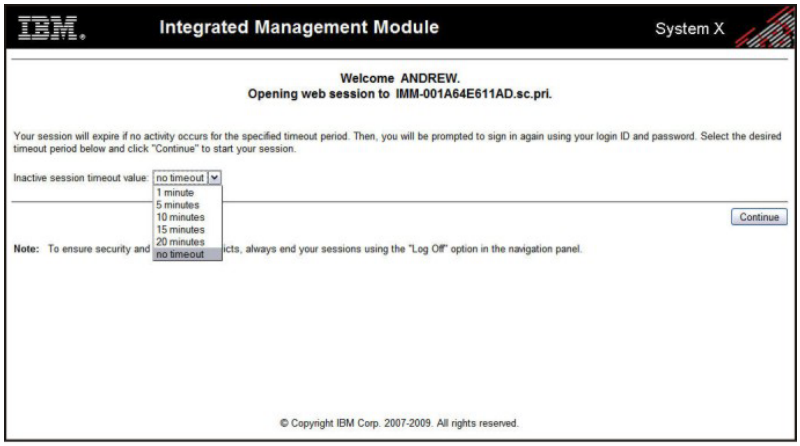
若要透過 IMM Web 介面存取 IMM，請完成下列步驟：

1. 開啓 Web 瀏覽器。在網址或 URL 欄位中，鍵入您要連接之 IMM 伺服器的 IP 位址或主機名稱。

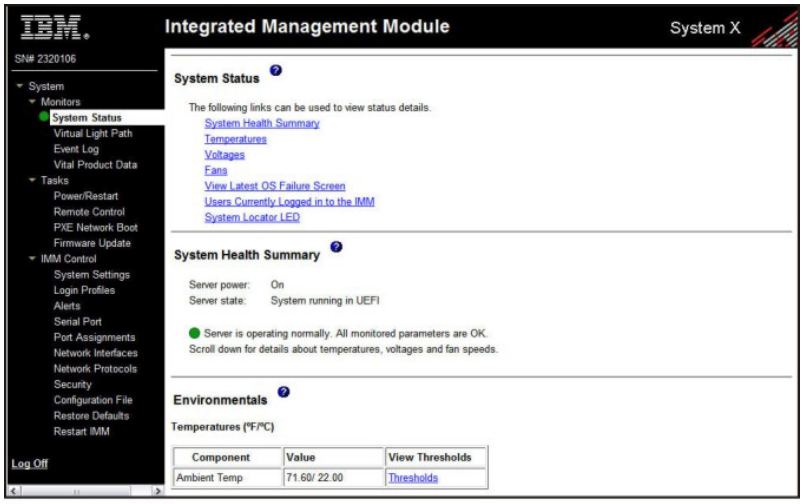


2. 在 IMM Login 視窗中鍵入您的使用者名稱和密碼。如果您是第一次使用 IMM，可以從系統管理者處取得使用者名稱和密碼。所有的登入嘗試都會記載在事件日誌中。視系統管理者配置使用者 ID 的方式而定，您可能需要輸入新密碼。
3. 在 Welcome 網頁上，從所提供欄位的下拉清單中選取逾時值。如果瀏覽器處於非作用中狀態的時間達到您指定的分鐘數，IMM 便會將您登出 Web 介面。

   註：視系統管理者配置廣域登入設定的方式而定，逾時值可能爲固定值。



4. 按一下 **Continue**，以啓動階段作業。瀏覽器會開啓 System Status 頁面，該頁面可讓您快速檢視伺服器狀態和伺服器性能狀態摘要。



如需可從 IMM Web 介面左側導覽窗格中的鏈結執行的動作的說明，請參閱『IMM 動作說明』。然後，移至第 17 頁的第 3 章, 『配置 IMM』。

IMM 動作說明

表 2 列出在登入 IMM 時可用的動作。

表 2. IMM 動作

鏈結	操作	說明
System Status	檢視伺服器的系統性能狀態，檢視作業系統失敗畫面擷取，以及檢視登入 IMM 的使用者	您可以在 System Health 頁面上監視伺服器電源和系統性能狀態，以及伺服器的溫度、電壓和風扇狀態。您也可以檢視前次作業系統失敗畫面擷取的影像，及登入 IMM 的使用者。
虛擬光徑	檢視伺服器光徑上每個 LED 的名稱、色彩和狀態	Virtual Light Path 頁面顯示伺服器上 LED 的現行狀態。
Event Log	檢視遠端伺服器的事件日誌	Event Log 頁面包含目前儲存在機箱事件日誌中的項目。日誌包含 BMC 報告的事件的文字說明，以及所有遠端存取嘗試和配置變更的相關資訊。日誌中的所有事件都使用 IMM 日期和時間設定進行時間戳記。部分事件也會產生警示（如果這些事件配置爲在 Alerts 頁面上執行此作業）。您可以排序和過濾事件日誌中的事件。
Vital Product Data	檢視伺服器重要產品資料 (VPD)	IMM 會收集伺服器資訊、伺服器韌體資訊和伺服器元件 VPD。Vital Product Data 頁面中提供了此資料。
Power/Restart	遠端開啓或重新啓動伺服器	IMM 使用開啓電源、關閉電源和重新啓動動作，來提供對您的伺服器進行完全遠端電源控制。此外，會擷取和顯示電源開啓和重新啓動統計資料，以顯示伺服器硬體可用性。
Remote Control	重新導向伺服器視訊主控台，並使用您的電腦磁碟機或磁碟映像檔作爲伺服器上的硬碟	從 Remote Control 頁面，您可以啓動 Remote Control 特性。使用 Remote Control，您可以從電腦檢視伺服器主控台，且您可以將其中一個電腦磁碟機（如 CD-ROM 光碟機或軟式磁碟機）裝載在伺服器上。您可以使用滑鼠和鍵盤，來與伺服器互動及控制伺服器。裝載磁碟後，您可以使用它來重新伺服器，及更新伺服器上的韌體。裝載的磁碟顯示爲連接至伺服器的 USB 隨身碟。
PXE Network Boot	變更下次重新啓動的主伺服器啓動（開機）順序，以嘗試「開機前執行環境 (PXE)」/「動態主機配置通訊協定 (DHCP)」網路啓動	如果已正確定義伺服器韌體和 PXE Boot Agent Utility，從 PXE Network Boot 頁面，您可以變更下次重新啓動的主伺服器啓動（開機）順序，以嘗試 PXE/DHCP 網路啓動。僅當主機不在 Privileged Access Protection (PAP) 下時，才會變更主機啓動順序。在下次重新啓動之後，PXE Network Boot 頁面上的勾選框將會清除。
Firmware Update	更新 IMM 上的韌體	使用 Firmware Update 頁面上的選項來更新 IMM 韌體、伺服器韌體和 DSA 韌體。
System Settings	檢視和變更 IMM 伺服器設定	您可以從 System Settings 頁面，配置伺服器位置和一般資訊，如 IMM 的名稱、伺服器逾時設定，以及 IMM 的聯絡資訊。
	設定 IMM 時鐘	您可以設定用於對事件日誌中的項目進行時間戳記的 IMM 時鐘。
	啓用或停用 USB 頻內介面	您可以啓用或停用 USB 頻內（或 LAN over USB）介面。
Login Profiles	配置 IMM 登入設定檔和廣域登入設定檔	您可以定義最多 12 個可存取 IMM 的登入設定檔。您也可以定義可套用至所有登入設定檔的廣域登入設定，包括啓用「輕量型目錄存取通訊協定 (LDAP)」伺服器鑑別及自訂帳戶安全層次。

表 2. IMM 動作 (繼續)

鏈結	操作	說明
Alerts	配置遠端警示和遠端警示接收者	您可以將 IMM 配置爲產生和轉遞不同事件的警示。在 Alerts 頁面上，您可以配置受監視的警示和被通知的接收者。
	配置「簡易網路管理通訊協定 (SNMP)」事件	您可以設定傳送 SNMP 設陷的事件種類。
	配置警示設定	您可以建立可套用至所有遠端警示接收者的廣域設定，如警示重試次數和重試之間的延遲。
Serial Port	配置 IMM 序列埠設定	從 Serial Port 頁面，您可以配置序列重新導向功能使用的序列埠傳輸速率。您也可以配置用於在序列重新導向與指令行介面 (CLI) 模式之間切換的按鍵順序。
Port assignments	變更 IMM 通訊協定的埠號	從 Port Assignments 頁面，您可以檢視和變更指派給 IMM 通訊協定的埠號（例如，HTTP、HTTPS、Telnet 和 SNMP）。
Network Interfaces	配置 IMM 的網路介面	從 Network Interfaces 頁面，您可以配置 IMM 上的乙太網路連線的網路存取權設定。
Network Protocols	配置 IMM 的網路通訊協定	您可以從 Network Protocols 頁面，配置 IMM 使用的「簡易網路管理通訊協定 (SNMP)」、「網域名稱系統 (DNS)」和「簡易郵件傳送通訊協定 (SMTP)」設定。您也可以配置 LDAP 參數。
Security	配置 Secure Sockets Layer (SSL)	您可以啓用或停用 SSL，及管理使用的 SSL 憑證。您也可以啓用或停用 SSL 連線是否用於連接至 LDAP 伺服器。
	啓用 Secure Shell (SSH) 存取權	您可以啓用 IMM 的 SSH 存取權。
Configuration File	備份和還原 IMM 配置	您可以從 Configuration File 頁面，備份、修改和還原 IMM 的配置，及檢視配置摘要。
Restore Default Settings	還原 IMM 預設值	**警告：** 按一下 **Restore Defaults** 時，您對 IMM 所做的所有修改都會遺失。 您可以將 IMM 的配置重設爲原廠預設值。
Restart IMM	重新啓動 IMM	您可以重新啓動 IMM。
Scalable Partitioning	將伺服器配置爲可調式複合體中的分割區。	如果在可調式複合體中配置伺服器，IMM 可讓您在複合體中控制系統。如果可調式伺服器發生問題，IMM 會報告錯誤。
Service Advisor	將可用事件碼轉遞給 IBM 支援中心	啓用時，Service Advisor 容許 IMM 將可用事件碼轉遞給 IBM 支援中心以進一步疑難排解。 **註：**請參閱您的伺服器的文件，以查看您的伺服器是否支援此特性。
Log off	登出 IMM	您可以登出與 IMM 的連線。

您可以按一下 **View Configuration Summary** 鏈結（位於大部分頁面的右上角），以快速檢視 IMM 的配置。

第 3 章 配置 IMM

使用導覽窗格中 **IMM Control** 下的鏈結來配置 IMM。

從 System Settings 頁面，您可以：
- 設定伺服器資訊
- 設定伺服器逾時
- 設定 IMM 日期和時間
- 啓用或停用 USB 介面上的指令

從 Login Profiles 頁面，您可以：
- 設定登入設定檔以控制 IMM 的存取權
- 配置廣域登入設定，如登入嘗試不成功後的鎖定期間
- 配置帳戶安全層次

從 Alerts 頁面，您可以：
- 配置遠端警示接收者
- 設定遠端警示嘗試次數
- 選取警示之間的延遲
- 選取傳送的警示，及轉遞這些警示的方式

從 Serial Port 頁面，您可以：
- 爲序列重新導向配置序列埠 2 (COM2) 的傳輸速率
- 指定用於在序列重新導向與指令行介面 (CLI) 之間切換的按鍵順序

從 Port Assignments 頁面，您可以變更 IMM 服務的埠號。

從 Network Interfaces 頁面，您可以設定 IMM 的乙太網路連線。

從 Network Protocols 頁面，您可以配置：
- SNMP 設定
- DNS 設定
- Telnet 通訊協定
- SMTP 設定
- LDAP 設定
- Service Location Protocol

從 Security 頁面，您可以安裝和配置 Secure Sockets Layer (SSL) 設定。

從 Configuration File 頁面，您可以備份、修改和還原 IMM 的配置。

從 Restore Defaults 頁面，您可以將 IMM 配置重設爲原廠預設值。

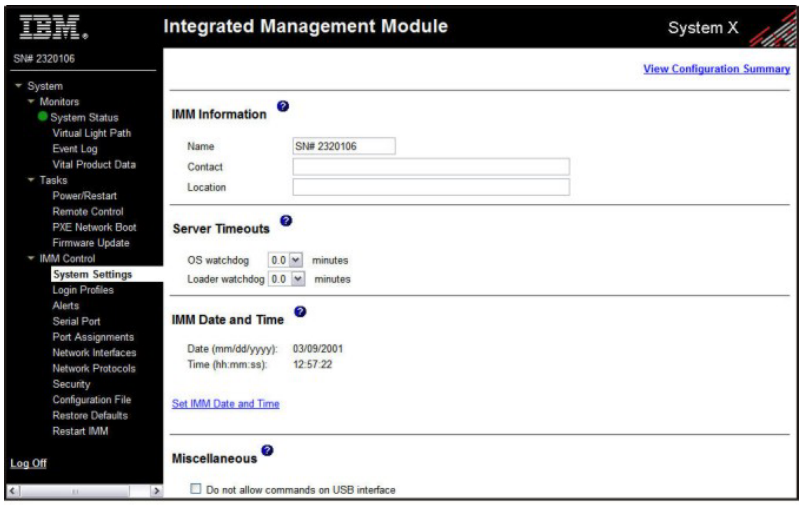
從 Restart IMM 頁面，您可以重新啓動 IMM。

設定系統資訊

若要設定 IMM 系統資訊，請完成下列步驟：

1. 登入您要在其中設定系統資訊的 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **System Settings**。畫面上會顯示類似下圖的頁面。

   註：System Settings 頁面中的可用欄位由存取的遠端伺服器決定。



3. 在 **IMM Information** 區域的 **Name** 欄位中，鍵入 IMM 的名稱。使用 **Name** 欄位來指定此伺服器中 IMM 的名稱。該名稱會包含在電子郵件和 SNMP 警示通知中，以識別警示的來源。

   註：您的 IMM 名稱（**Name** 欄位中的名稱）和 IMM 的 IP 主機名稱（Network Interfaces 頁面 **Hostname** 欄位中的名稱）不會自動共用相同的名稱，因爲 **Name** 欄位限制在 16 個字元。而 **Hostname** 欄位最多可以包含 63 個字元。爲盡量減少混淆，請將 **Name** 欄位設定爲 IP 主機名稱的非完整部分。非完整 IP 主機名稱最多由完整 IP 主機名稱第一個句點之前的部分組成。例如，對於完整 IP 主機名稱 imm1.us.company.com，非完整 IP 主機名稱爲 imm1。如需主機名稱的相關資訊，請參閱第 33 頁的『配置網路介面』。
4. 在 **Contact** 欄位中，鍵入聯絡資訊。例如，您可以指定在此伺服器發生問題時要聯絡的人員的姓名和電話號碼。在此欄位中，您最多可以鍵入 47 個字元。
5. 在 **Location** 欄位中，鍵入伺服器的位置。在此欄位中包含足夠的詳細資料可快速找到伺服器，以便進行維護或用於其他用途。在此欄位中，您最多可以鍵入 47 個字元。
6. 捲動到頁面底端，然後按一下 **Save**。

設定伺服器逾時

註：伺服器逾時需要啓用頻內 USB 介面（或 LAN over USB），才能容許指令執行。如需爲 USB 介面啓用或停用指令的相關資訊，請參閱第 21 頁的『停用 USB 頻內介面』。如需有關安裝必要裝置驅動程式的資訊，請參閱第 114 頁的『安裝裝置驅動程式』。

若要設定伺服器逾時值，請完成下列步驟：

1. 登入您要在其中設定伺服器逾時的 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **System Settings**，並向下捲動到 **Server Timeouts** 區域。

   您可以設定 IMM 自動回應下列事件：

   - 作業系統停機
   - 無法載入作業系統
3. 啓用與您要 IMM 自動回應的事件相對應的伺服器逾時。

   OS 監視器

   使用 **OS watchdog** 欄位可指定 IMM 檢查作業系統所間隔的分鐘數。如果作業系統無法回應其中一次檢查，IMM 便會產生 OS 逾時警示並重新啓動伺服器。重新啓動伺服器之後，在作業系統關閉並關機後再開啓伺服器之前，OS 監視器會一直處於停用狀態。

   若要設定 OS 監視器值，請從功能表中選取時間間隔。若要關閉此監視器，請從功能表中選取 **0.0**。若要擷取作業系統失敗畫面，您必須啓用 **OS watchdog** 欄位中的監視器。

   載入器監視器

   使用 **Loader watchdog** 欄位可指定 IMM 在完成 POST 和啓動作業系統之間所等待的分鐘數。如果超出此間隔，IMM 便會產生載入器逾時警示並自動重新啓動伺服器。重新啓動伺服器之後，在關閉作業系統並關機後再開啓伺服器（或者啓動作業系統並成功載入軟體）之前，載入器逾時會自動停用。

   若要設定載入器逾時值，請選取 IMM 等待作業系統啓動完成的時間限制。若要關閉此監視器，請從功能表中選取 **0.0**。

   關閉電源延遲

   使用 **Power off delay** 欄位，可指定 IMM 在關閉伺服器電源（如果作業系統本身未關閉電源的話）之前等待作業系統關閉的分鐘數。如果您設定關閉電源延遲，則可確保在關閉伺服器電源之前，作業系統有足夠的時間來依序關閉。若要確定您伺服器的關閉電源延遲，請關閉伺服器並觀察它關閉所花費的時間量。增加該值的時間緩沖，並將產生的數值做爲您的關閉電源延遲設定。

   若要設定關閉電源延遲值，請從功能表中選取所需的時間值。值 X'0' 表示作業系統（而非 IMM）關閉伺服器電源。
4. 捲動到頁面底端，然後按一下 **Save**。

設定 IMM 日期和時間

IMM 使用自己的即時時鐘，爲事件日誌中記載的所有事件貼上時間戳記。

註：IMM 日期和時間設定僅會影響 IMM 時鐘，不會影響伺服器時鐘。IMM 即時時鐘和伺服器時鐘是分開、獨立的時鐘，可以設定爲不同的時間。若要同步化 IMM 時鐘與伺服器時鐘，請移至頁面的 **Network Time Protocol** 區域，將 NTP 伺服器主機名稱或 IP 位址設定爲用於設定伺服器時鐘的相同伺服器主機名稱或 IP 位址。如需相關資訊，請參閱第 20 頁的『同步化網路中的時鐘』。

透過電子郵件和 SNMP 所傳送的警示，會使用即時時鐘設定爲警示貼上時間戳記。時鐘設定支援格林威治標準時間 (GMT) 偏移和日光節約時間 (DST)，以便從遠端管理跨不同時區系統的管理者在操作上更爲便利。您可以從遠端存取事件日誌，即使伺服器已關閉或已停用亦可存取。

若要驗證 IMM 的日期和時間設定，請完成下列步驟：

1. 登入您要在其中設定 IMM 日期和時間值的 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **System Settings** 並捲動到 **IMM Date and Time** 區域，該區域顯示產生網頁的日期和時間。
3. 若要置換日期和時間設定，以及啓用日光節約時間 (DST) 和格林威治標準時間 (GMT) 偏移，請按一下 **Set IMM Dateand Time**。畫面上會顯示類似下圖的頁面。

4. 在 **Date** 欄位中，鍵入現行月份、日期及年份的數字。
5. 在 **Time** 欄位中，於適用的輸入欄位中鍵入對應於現行小時、分鐘及秒的數字。以 24 小時制表示時，小時 (hh) 必須是介於 00 - 23 之間的數字。分鐘 (mm) 和秒 (ss) 必須是介於 00 - 59 之間的數字。
6. 在 **GMT offset** 欄位中，選取指定偏移的數字，該偏移採用小時格式、基於格林威治標準時間 (GMT) 且對應於伺服器所在時區。
7. 選取或清除 **Automatically adjust for daylight saving changes** 勾選框，以指定當當地時間在標準時間和日光節約時間之間進行變更時，IMM 時鐘是否自動調整。
8. 按一下 **Save**。

同步化網路中的時鐘

「網路時間通訊協定 (NTP)」提供了同步化整個電腦網路中時鐘的方法，這使得任何 NTP 用戶端都能從 NTP 伺服器取得正確時間。

IMM NTP 特性提供了一種方法，可將 IMM 即時時鐘與 NTP 伺服器所提供的時間同步化。您可以指定要使用的 NTP 伺服器、指定 IMM 的同步化頻率、啓用或停用 NTP 特性，以及要求立即同步化時間。

NTP 特性不提供透過 NTP Version 3 和 NTP Version 4 中的加密演算法所提供的進階安全和鑑別。IMM NTP 特性僅提供不含鑑別功能的「簡易網路時間通訊協定 (SNTP)」。

若要設定 IMM NTP 特性設定，請完成下列步驟：

1. 登入您要在其上同步化網路中時鐘的 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **System Settings**，並向下捲動到 **IMM Date and Time** 區域。

3. 按一下 **Set IMM Date and Time**。畫面上會顯示類似下圖的頁面。

4. 在 **Network Time Protocol (NTP)** 下，您可以選取下列設定：

   NTP auto-synchronization service
   使用此選項可啓用或停用 IMM 時鐘與 NTP 伺服器自動同步化。

   NTP server host name or IP address
   使用此欄位可指定要用於時鐘同步化的 NTP 伺服器的名稱。

   NTP update frequency
   使用此欄位可指定同步化要求之間的估計間隔（分鐘）。請輸入 3 - 1440 分鐘之間的值。

   Synchronize Clock Now
   按一下此按鈕可要求立即同步化，而非等到間隔時間才進行。

5. 按一下 **Save**。

停用 USB 頻內介面

重要事項：如果您停用 USB 頻內介面，則無法使用 Linux 或 Windows 快閃記憶體公用程式來執行 IMM 韌體、伺服器韌體及 DSA 韌體的頻內更新。如果 USB 頻內介面已停用，則請使用 IMM Web 介面上的 Firmware Update 選項來更新韌體。如需相關資訊，請參閱第 109 頁的『更新韌體』。

如果您停用 USB 頻內介面，也請停用監視器逾時，防止伺服器非預期地重新啓動。如需相關資訊，請參閱第 18 頁的『設定伺服器逾時』。

USB 頻內介面或 LAN over USB 用於與 IMM 的頻內通訊。若要防止在伺服器上執行的任何應用程式要求 IMM 執行作業，您必須停用 USB 頻內介面。如需 LAN over USB 的相關資訊，請參閱第 113 頁的第 6 章, 『LAN over USB』。

若要停用 USB 頻內介面，請完成下列步驟：

1. 登入想要在其上停用 USB 裝置驅動程式介面的 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **System Settings**，並向下捲動到 **Miscellaneous** 區域。畫面上會顯示類似下圖的頁面。

3. 若要停用 USB 頻內介面，請從 **Allow commands on the USB interface** 清單中選取 **Disabled**。 選取此選項並不會影響 USB 遠端顯示狀態功能（例如，鍵盤、滑鼠和大量儲存裝置）。當您停用 USB 頻內介面時，頻內系統管理應用程式（例如「進階設定公用程式 (ASU)」和韌體更新項目套件公用程式）可能會無法運作。

   註：如果已安裝 IPMI 裝置驅動程式，則 ASU 可以與停用的 USB 頻內介面搭配運作。
   如果您嘗試在停用頻內介面時使用系統管理應用程式，則它們可能會無法運作。
4. 按一下 **Save**。

若要在其停用後啓用 USB 裝置驅動程式介面，請清除 **Do not allow commands on USB interface** 勾選框並按一下 **Save**。

註：

1. USB 頻內介面也稱爲 ″LAN over USB″，第 113 頁的第 6 章, 『LAN over USB』中有詳細說明。
2. 嘗試部分 Linux 發行套件的網路安裝時，如果 IMM USB 頻內介面已啓用，則安裝可能會失敗。如需相關資訊，請參閱 http://rhn.redhat.com/errata/RHBA-2009-0127.html。
3. 如果您要執行的網路安裝不包含前述附註 2 中所述 Red Hat 網站上的更新，則必須在執行安裝前停用 USB 頻內介面，並在安裝完成後將其啓用。
4. 如需 LAN over USB 介面配置的相關資訊，請參閱第 114 頁的『手動配置 LAN over USB 介面』。

建立登入設定檔

使用 Login Profiles 表格可檢視、配置或變更個別登入設定檔。使用 Login ID 直欄中的鏈結可配置個別登入設定檔。您最多可以定義 12 個唯一設定檔。Login ID 直欄中的每個鏈結都使用關聯設定檔的已配置登入 ID 標示。

一些 IPMI 使用者 ID 會共用某些登入設定檔，進而提供一組可使用所有 IMM 使用者介面（包括 IPMI）的本端使用者帳戶（使用者名稱/密碼）。下列清單中說明了與這些共用登入設定檔相關的規則：

- IPMI 使用者 ID 1 一律爲空值使用者。
- IPMI 使用者 ID 2 對映至登入 ID 1，IPMI 使用者 ID 3 對映至登入 ID 2，依此類推。
- 對於 IPMI 使用者 ID 2 和登入 ID 1，IMM 預設使用者設定爲 USERID 和 PASSW0RD（當中所含的是數字 0，不是字母 O）。

例如，如果是透過 IPMI 指令新增使用者，則也可以透過 Web、Telnet、SSH 及其他介面鑑別該使用者資訊。相反地，如果是在 Web 或其他介面上新增使用者，則該使用者資訊可供啓動 IPMI 階段作業使用。

因爲使用者帳戶共用 IPMI ，所以會強制某些限制，以在使用這些帳戶的介面之間提供共同基礎。下列清單說明 IMM 和 IPMI 登入設定檔限制：

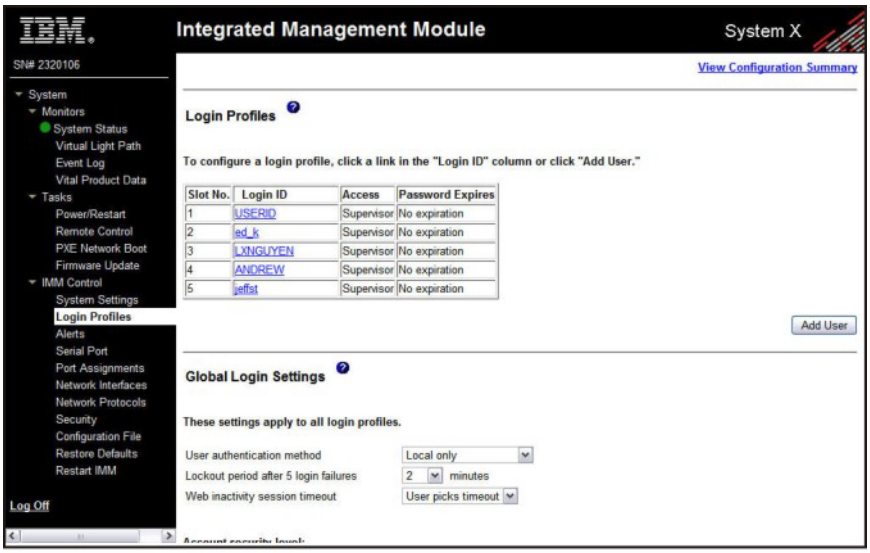
- IPMI 最多容許 64 個使用者 ID。IMM IPMI 實作僅容許 12 個使用者帳戶。
- IPMI 容許匿名登入（空值使用者名稱和空值密碼），但 IMM 不容許。
- IPMI 容許多個使用者 ID 具有相同的使用者名稱，但 IMM 不容許。

- IPMI 要求將使用者名稱由現行名稱變更爲相同現行名稱時會傳回 `invalid parameter` 完成碼，因爲要求的使用者名稱已在使用中。
- 對於 IMM，IPMI 密碼長度上限爲 16 個位元組。
- 下列字詞受限制且不能用作本端 IMM 使用者名稱：
  - immroot
  - nobody
  - ldap
  - lighttpd
  - sshd
  - daemon
  - immftp

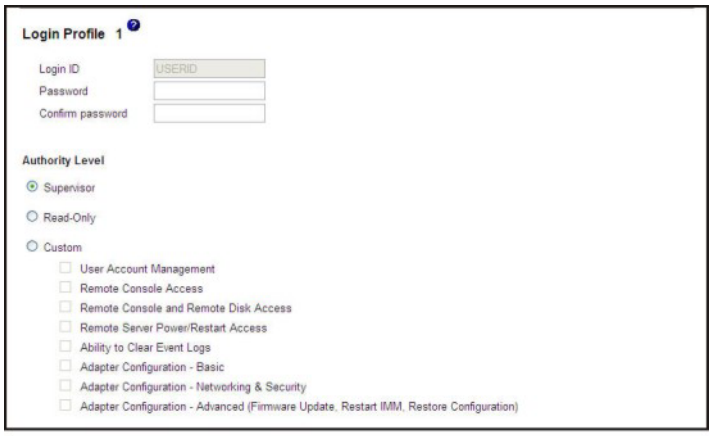
若要配置登入設定檔，請完成下列步驟：

1. 登入您要在其中建立登入設定檔的 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **Login Profiles**。

   註：如果您尚未配置設定檔，則它不會出現在 Login Profiles 表格中。
   Login Profiles 頁面顯示每個登入 ID、登入存取層次及密碼有效期限資訊，如下圖所示。



   重要事項：依預設，IMM 使用一個登入設定檔配置，該設定檔使用登入使用者 ID `USERID` 和密碼 `PASSWORD`（當中所含的是數字 0，不是字母 O）來啓用遠端存取。爲了避免潛在的暴露安全性問題，請在 IMM 的起始設定期間變更此預設登入設定檔。
3. 按一下 **Add User**。個別設定檔頁面與下圖所示頁面類似。



4. 在 **Login ID** 欄位中，鍵入設定檔的名稱。在 **Login ID** 欄位中，您最多可以鍵入 16 個字元。有效字元包括爲大寫字母和小寫字母、數字、句點及底線。

   註：此登入 ID 用於授與對 IMM 的遠端存取權。

5. 在 **Password** 欄位中，指派登入 ID 的密碼。密碼必須至少包含五個字元，並且其中一個字元必須爲非字母字元。接受空值密碼或空密碼。

   註：此密碼與登入 ID 一起使用，以授與對 IMM 的遠端存取權。

6. 在 **Confirm password** 欄位中，再次鍵入密碼。
7. 在 **Authority Level** 區域中，請選取下列其中一個選項以設定此登入 ID 的存取權：

   Supervisor

   使用者無任何限制。

   Read Only

   使用者僅具有唯讀存取權，無法執行諸如檔案傳送之類動作、電源和重新啓動動作或遠端顯示功能。

   Custom

   如果您選取 Custom 選項，則必須選取下列一個以上的自訂權限層級：

   - **User Account Management**：使用者可以新增、修改或刪除使用者，以及變更 Login Profiles 頁面中的廣域登入設定。
   - **Remote Console Access**：使用者可以存取遠端主控台。
   - **Remote Console and Virtual Media Access**：使用者可以存取遠端主控台和虛擬媒體特性。
   - **Remote Server Power/Restart Access**：使用者可以存取遠端伺服器的電源開啓和重新啓動功能。Power/Restart 頁面中提供這些功能。
   - **清除事件日誌的能力**：使用者可以清除事件日誌。每個人都可以查看事件日誌，但需要具有此特定權限才能清除日誌。
   - **Adapter Configuration - Basic**：使用者可以修改 System Settings 和 Alerts 頁面中的配置參數。
   - **Adapter Configuration - Networking & Security**：使用者可以修改 Security、Network Protocols、Network Interface、Port Assignments 及 Serial Port 頁面中的配置參數。

- **Adapter Configuration - Advanced**：使用者在配置 IMM 時沒有任何限制。此外，據說使用者還具有對 IMM 的管理存取權，這意味著使用者也可以執行下列進階功能：韌體更新、PXE 網路開機、還原 IMM 原廠預設值、從配置檔修改和還原 IMM 配置，以及重新啓動和重設 IMM。

當使用者設定 IMM 登入 ID 的權限層級時，會根據下列優先順序來設定產生的對應 IPMI 使用者 ID 的 IPMI 專用權層次：

- 如果使用者將 IMM 登入 ID 權限層級設定爲 Supervisor，則 IPMI 專用權層次會設定爲 Administrator。
- 如果使用者將 IMM 登入 ID 權限層級設定爲 Read Only，則 IPMI 專用權層次會設定爲 User。
- 如果使用者將 IMM 登入 ID 權限層級設定爲具有下列任一存取權類型，則 IPMI 專用權層次會設定爲 Administrator：
  - User Account Management Access
  - Remote Console Access
  - Remote Console and Remote Disk Access
  - Adapter Configuration - Networking & Security
  - Adapter Configuration - Advanced
- 如果使用者將 IMM 登入 ID 權限層級設定爲具有 Remote Server Power/Restart Access 或 Ability to Clear Event Logs 存取權類型，則 IPMI 專用權層次會設定爲 Operator。
- 如果使用者將 IMM 登入 ID 權限層級設定爲具有 Adapter Configuration (Basic) 存取權類型，則 IPMI 專用權層次會設定爲 User。

註：若要將登入設定檔恢復爲原廠預設值，請按一下 **Clear Login Profiles**。

8. 在 **Configure SNMPv3 User** 區域中，如果使用者應使用 SNMPv3 通訊協定來存取 IMM，則請選取該勾選框。按一下該勾選框後，畫面上會出現類似下圖的頁面區域。

使用下列欄位來設定使用者設定檔的 SNMPv3 設定：

Authentication Protocol

使用此欄位可將 **HMAC-MD5** 或 **HMAC-SHA** 指定爲鑑別通訊協定。SNMPv3 安全模式使用雜湊演算法來進行鑑別。將使用 Linux 帳戶的密碼來進行鑑別。如果您選擇 **None**，則不會使用鑑別通訊協定。

Privacy Protocol

可以使用加密來保護 SNMP 用戶端與代理程式之間的資料傳送。支援的方法爲 **DES** 和 **AES**。僅當鑑別通訊協定設定爲 HMAC-MD5 或 HMAC-SHA 時，保密通訊協定才有效。

Privacy Password

使用此欄位可指定加密密碼。

Confirm Privacy Password

使用此欄位可確認加密密碼。

Access Type

使用此欄位可將 **Get** 或 **Set** 指定爲存取類型。存取類型爲 Get 的 SNMPv3 使用者只能執行查詢作業。存取類型爲 Set 的 SNMPv3 使用者不僅可以執行查詢作業，而且可以修改設定（例如，設定使用者的密碼）。

Hostname/IP address for traps

使用此欄位可指定使用者的設陷目的地。這可以是 IP 位址或主機名稱。SNMP 代理程式使用設陷來通知管理工作站發生的事件（例如，當處理器溫度超過限制時）。

9. 按一下 **Save**，以儲存您的登入 ID 設定。

刪除登入設定檔

若要刪除登入設定檔，請完成下列步驟：

1. 登入您要爲其建立登入設定檔的 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **Login Profiles**。Login Profiles 頁面顯示每個登入 ID、登入存取層次及密碼有效期限資訊。
3. 按一下您要刪除的登入設定檔。畫面上會顯示該使用者的 Login Profile 頁面。
4. 按一下 **Clear Login Profile**。

配置廣域登入設定

完成下列步驟，以設定適用於 IMM 的所有登入設定檔的狀況：

1. 登入您要設定廣域登入設定的 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **Login Profiles**。
3. 向下捲動至 **Global Login Settings** 區域。畫面上會顯示與下圖類似的頁面。

4. 在 **User authentication method** 欄位中，指定鑑別嘗試登入的使用者的方式。選取下列其中一種鑑別方法：
   - **Local only**：透過搜尋 IMM 本端的表格來鑑別使用者。如果使用者 ID 和密碼不相符，會拒絕存取。會爲順利鑑別的使用者指派第 22 頁的『建立登入設定檔』中配置的權限層級。
   - **LDAP only**：IMM 嘗試使用 LDAP 伺服器鑑別使用者。永不使用此鑑別方法搜尋 IMM 上的本端使用者表格。
   - **Local first, then LDAP**：先嘗試本端鑑別。如果本端鑑別失敗，會嘗試 LDAP 鑑別。
   - **LDAP first, then Local**：先嘗試 LDAP 鑑別。如果 LDAP 鑑別失敗，會嘗試本端鑑別。

     註：

     a. 僅本端管理的帳戶與 IPMI 介面共用，因爲 IPMI 不支援 LDAP 鑑別。

     b. 即使 **User authentication method** 欄位設定爲 **LDAP only**，使用者也可以使用本端管理的帳戶登入 IPMI 介面。
5. 如果偵測到連續超過五次遠端登入失敗，請在 **Lockout period after 5 login failures** 欄位中，指定 IMM 禁止遠端登入嘗試的時間（分鐘）。鎖定一位使用者不會造成其他使用者無法登入。
6. 在 **Web inactivity session timeout** 欄位中，指定 IMM 在中斷連接非作用中 Web 階段作業之前等待的時間（分鐘）。選取 **No timeout** 以停用此特性。如果使用者將在登入程序期間選取逾時期間，請選取 **User picks timeout**。
7. （選用）在 **Account security level** 區域中，選取密碼安全層次。**Legacy security settings** 和 **High security settings** 可設定如需求清單所示的預設值。
8. 若要自訂安全設定，請選取 **Custom security settings** 以檢視和變更帳戶安全管理配置。

   User login password required

   使用此欄位可指示是否容許無密碼的登入 ID。

   Number of previous passwords that cannot be used

   使用此欄位可指示無法重複使用的先前密碼數目。最多可以比較五個先前的密碼。選取 **0** 可容許重複使用先前的所有密碼。

Maximum Password Age

使用此欄位可指示容許的密碼有效期限上限，之後必須變更密碼。支援的值爲 0-365 天。選取 **0** 可停用密碼有效期限檢查。

9. 按一下 **Save**。

配置遠端警示設定

您可以從導覽窗格上的 **Alerts** 鏈結，配置遠端警示接收者、警示嘗試次數、可觸發遠端警示的發生事件，以及本端警示。

配置遠端警示接收者之後，當從 Monitored Alerts 群組中選取的任何事件發生時，IMM 會將警示傳送給該接收者。警示包含事件本質、事件的時間和日期，以及產生警示的系統名稱之相關資訊。

註：如果 **SNMP Agent** 或 **SNMP Traps** 欄位未設定爲 **Enabled**，則不會傳送 SNMP 設陷。如需這些欄位的相關資訊，請參閱第 38 頁的『配置 SNMP』。

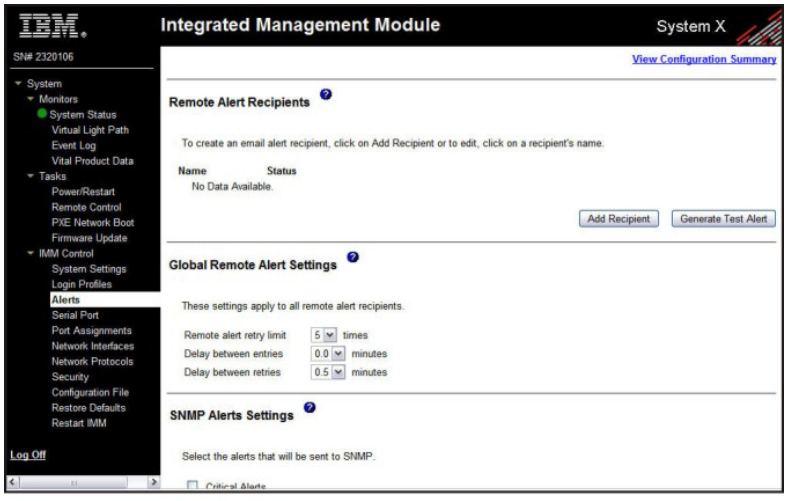
配置遠端警示接收者

您可以定義最多 12 個唯一的遠端警示接收者。警示接收者的每一個鏈結都標有接收者名稱和警示狀態。

註：如果您未配置警示接收者設定檔，則設定檔不會出現在遠端警示接收者清單中。

若要配置遠端警示接收者，請完成下列步驟：

1. 登入您要配置遠端警示設定的 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **Alerts**。畫面上會顯示 Remote Alert Recipients 頁面。如果已設定接收者，您可以查看每一個接收者的通知方法和警示狀態。



3. 按一下其中一個遠端警示接收者鏈結，或按一下 **Add Recipient**。類似下圖的個別接收者視窗即會開啓。

4. 在 **Status** 欄位中，按一下 **Enabled** 以啓動遠端警示接收者。
5. 在 **Name** 欄位中，鍵入接收者或其他 ID 的名稱。您鍵入的名稱顯示爲 Alerts 頁面上接收者的鏈結。
6. 在 **E-mail address** 欄位中，輸入警示接收者的電子郵件位址。
7. 使用此勾選框來併入具有電子郵件警示的事件日誌。
8. 在 **Monitored Alerts** 欄位中，選取傳送至警示接收者的警示類型。遠端警示按下列嚴重性層次分類：

   嚴重警示

   針對表示伺服器元件不再能發揮作用的事件，產生嚴重警示。

   警告警示

   針對可能會發展爲嚴重層次的事件，產生警告警示。

   系統警示

   針對會導致系統錯誤的事件，或會導致配置變更的事件，產生系統警示。

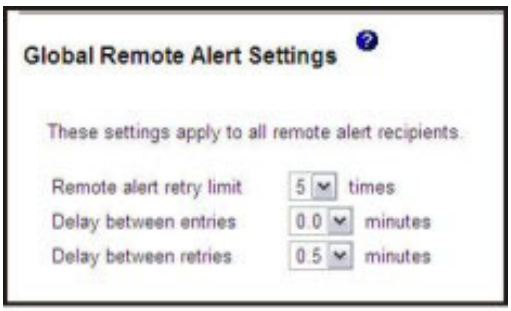
   所有警示都會儲存在事件日誌中，並會傳送至所有配置的遠端警示接收者。
9. 按一下 **Save**。

配置廣域遠端警示設定

廣域遠端警示設定僅適用於轉遞的警示。

請完成下列步驟，以設定 IMM 嘗試傳送警示的次數：

1. 登入您要在其上設定遠端警示嘗試的 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **Alerts**，然後向下捲動至 **Global Remote Alert Settings** 區域。



使用這些設定來定義遠端警示嘗試次數，及各嘗試之間的持續時間。此設定適用於所有配置的遠端警示接收者。

Remote alert retry limit

使用 **Remote alert retry limit** 欄位，可指定 IMM 嘗試將警示傳送至接收者的額外次數。IMM 不會傳送多個警示；僅在 IMM 嘗試傳送起始警示的情況下發生失敗時，才會進行額外的警示嘗試。

註：此警示設定不適用於 SNMP 警示。

Delay between entries

使用 **Delay between entries** 欄位，可指定 IMM 在將警示傳送至清單中的下一個接收者之前等待的時間間隔（分鐘）。

Delay between retries

使用 **Delay between retries** 欄位，可指定 IMM 在傳送警示至接收者的各次嘗試之間等待的時間間隔（分鐘）。

3. 捲動至頁面的底端，然後按一下 **Save**。

配置 SNMP 警示設定

SNMP 代理程式透過 SNMP 設陷通知 IMM 關於事件。您可以配置 SNMP 以根據事件類型過濾事件。可用於過濾的事件種類爲「嚴重」、「警告」和「系統」。SNMP 警示設定對於所有 SNMP 設陷都是廣域設定。

註：

1. IMM 提供了兩個與 SNMP 應用程式搭配使用的「管理資訊庫 (MIB)」檔案。MIB 檔案包含在 IMM 韌體更新項目套件中。
2. IMM 支援 SNMPv1 和 SNMPv3 標準。

請完成下列步驟，以選取傳送至 SNMP 的警示類型：

1. 登入您要在其上設定遠端警示嘗試的 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **Alerts**，然後向下捲動至 **SNMP Alerts Settings** 區域。
3. 選取警示的類型。遠端警示按下列嚴重性層次分類：
   - 嚴重
   - 警告
   - 系統
4. 捲動至頁面的底端，然後按一下 **Save**。

配置序列埠設定

IMM 提供了兩個用於序列重新導向的序列埠。

System x 伺服器上的序列埠 1 (COM1) 用於 IPMI Serial over LAN (SOL)。COM1 僅可透過 IPMI 介面進行配置。

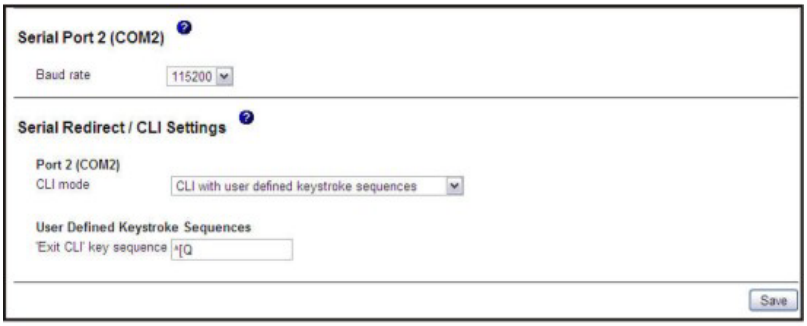
在刀鋒伺服器上，序列埠 2 (COM2) 用於 SOL。在 System x 伺服器上，COM2 用於透過 Telnet 或 SSH 的序列重新導向。COM2 無法透過 IPMI 介面進行配置。在機架裝載式和直立式伺服器上，COM2 是無外部存取權的內部 COM 埠。

這兩個序列埠使用 8 個資料位元、空值同位檢查和 1 個停止位元。提供了 9600、19200、38400、57600、115200 和 230400 的傳輸速率選擇。

您可以爲 IMM 中的 COM2 埠配置序列重新導向和指令行介面。

若要配置序列資料傳送速率和重新導向，請完成下列步驟：

1. 登入您要配置序列埠的 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **Serial Port**。畫面上會顯示類似下圖的頁面。



3. 在 **Baud rate** 欄位中，選取與要用於序列重新導向的伺服器 COM 埠的速率相符的資料傳送速率。使用 **Baud rate** 欄位來指定您的序列埠連線的資料傳送速率。若要設定傳輸速率，請選取對應於您的序列埠連線的資料傳送速率（每秒位元數）。
4. 在 **Serial Redirect/CLI Settings** 區域的 **CLI mode** 欄位中，選取 **CLI with EMS compatible keystroke sequences**（如果您要使用「Microsoft Windows Server 2003 緊急管理服務 (EMS)」相容按鍵順序來結束序列重新導向作業，或選取 **CLI with user defined keystroke sequences**（如果您要使用自己的按鍵順序）。

   註：如果選取 **CLI with user defined keystroke sequences**，您必須定義按鍵順序。

   序列重新導向啓動之後，它會繼續，直到使用者鍵入結束按鍵順序。鍵入結束按鍵順序時，序列重新導向會停止，使用者會返回 Telnet 或 SSH 階段作業中的指令模式。使用此欄位來指定結束按鍵順序。
5. 按一下 **Save**。

配置 serial-to-Telnet 或 SSH 重新導向

serial-to-Telnet 或 SSH 重新導向可讓系統管理者將 IMM 用作序列終端機伺服器。在啓用序列重新導向時，您可以從 Telnet 或 SSH 連線存取伺服器序列埠。

注意事項：

1. IMM 容許最多兩個開啓的 Telnet 階段作業。Telnet 階段作業可以獨立地存取序列埠，以便多個使用者可以同時檢視重新導向的序列埠。
2. 指令行介面 **console 1** 指令用於透過 COM 埠啓動序列重新導向階段作業。

階段作業範例

```
telnet 192.168.70.125 (Press Enter.)
Connecting to 192.168.70.125...
username: USERID (Press Enter.)
password: ******** (Press Enter.)
system> console 1 (Press Enter.)
```

來自 COM2 的所有資料流量都會立即遞送至 Telnet 階段作業。來自 Telnet 或 SSH 階段作業的所有資料流量都會遞送至 COM2。

```
ESC Q
```

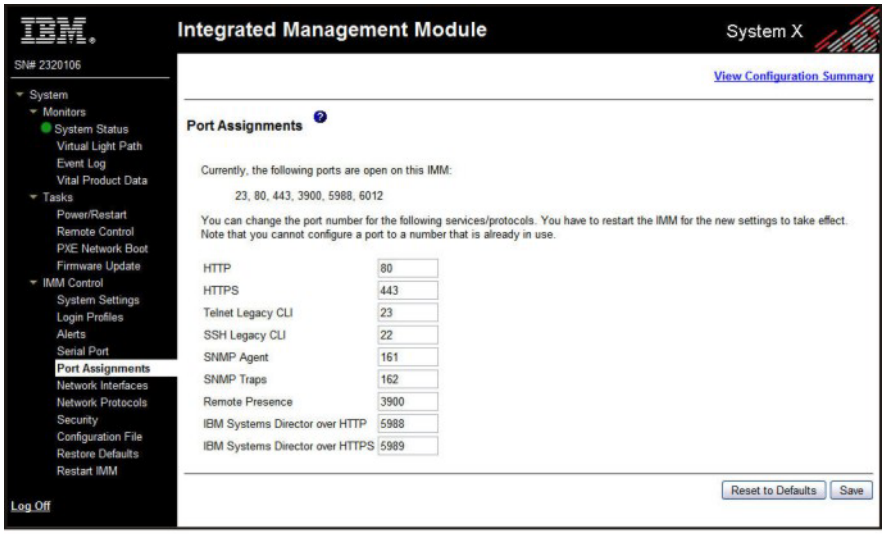
鍵入結束按鍵順序，以返回指令行介面。在此範例中，按 Esc 鍵，然後鍵入 q。

```
Back to LegacyCLI console....
```

配置埠指派

若要變更 IMM 服務的埠號，請完成下列步驟：

1. 登入您要配置埠指派的 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **Port Assignments**。畫面上會顯示與下圖類似的頁面。



3. 使用下列資訊爲欄位指派值：

   HTTP 這是 IMM 的 HTTP 伺服器的埠號。預設埠號是 80。其他有效值在 1-65535 範圍內。如果變更此埠號，您必須在網址結尾加上此埠號，前面有冒號。例如，如果 HTTP 埠變更爲 8500，請鍵入 `http://hostname:8500/` 以開啓 IMM Web 介面。請注意，您必須在 IP 位址和埠號前面鍵入字首 `http://`。

   HTTPS
   這是用於 Web 介面 HTTPS (SSL) 資料流量的埠號。預設值是 443。其他有效值在 1-65535 範圍內。

   Telnet Legacy CLI
   這是透過 Telnet 服務登入的 Legacy CLI 的埠號。預設值是 23。其他有效值在 1-65535 範圍內。

SSH Legacy CLI
這是針對透過 SSH 登入的 Legacy CLI 配置的埠號。預設值是 22。

SNMP Agent
這是在 IMM 上執行的 SNMP 代理程式的埠號。預設值是 161。其他有效值在 1-65535 範圍內。

SNMP Traps
這是用於 SNMP 設陷的埠號。預設值是 162。其他有效值在 1-65535 範圍內。

Remote Presence
這是用於檢視伺服器主控台並與伺服器主控台互動的 Remote Control 特性的埠號。機架裝載式和直立式伺服器的預設值是 3900。

註：BladeCenter 上的「並行鍵盤、視訊和滑鼠 (cKVM)」特性要求埠號爲 2068。請勿在刀鋒伺服器上變更此埠號。

IBM Systems Director over HTTP
這是 IBM Systems Director 用於與伺服器主控台互動的埠號。預設值是 5988。

IBM Systems Director over HTTPS
這是 IBM Systems Director 用於透過 SSL 與伺服器主控台互動的埠號。預設值是 5989。

下列埠號將保留，且只能用於對應的服務。

表 3. 保留的埠號

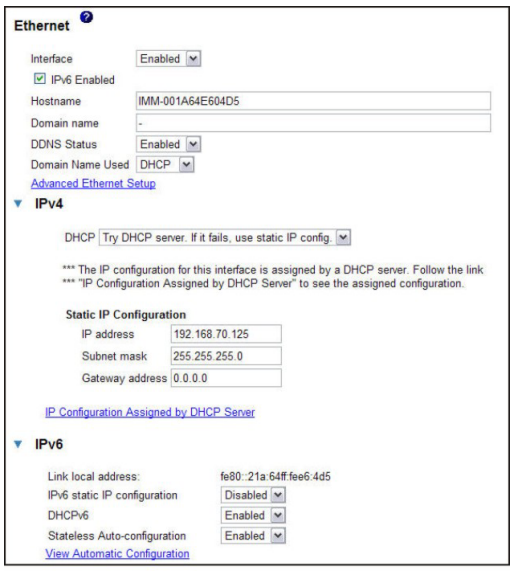
埠號	服務對象
427	SLP
7070 至 7077	分割區管理

4. 按一下 **Save**。

配置網路介面

在 Network Interfaces 頁面上，您可以透過配置 IMM 的乙太網路連線來設定 IMM 的存取權。若要配置 IMM 的乙太網路設定，請根據需要在 Network Interfaces 頁面的 Ethernet、IPv4 或 IPv6 區域中修改設定。接下來的章節說明了每一個區域中的設定。

註：下列影像中的值是範例。您的設定將會不同。



若要查看所有現行配置設定的摘要，請按一下 Network Interfaces 頁面上的 **View Configuration Summary**。在 Network Interfaces 頁面上配置設定之前，檢閱接下來的章節中的資訊。

註：您也可以透過 Setup Utility 配置 IMM 網路連線。如需相關資訊，請參閱第 11 頁的『透過 IBM System x Server Firmware Setup Utility 設定 IMM 網路連線』。

配置乙太網路設定

您可以在 Network Interfaces 頁面的 Ethernet 區域中修改下列設定。

Interface

使用此欄位可啓用或停用此網路介面。若要容許透過此網路介面進行網路連線，請選取 **Enabled**。

IPv6 Enabled

使用此勾選框啓用或停用 IMM 上的 IPv6 支援。

註：如果清除 **IPv6 Enabled** 勾選框，畫面上會顯示 **Hide all IPv6 configuration fields when IPv6 is disabled** 勾選框。如果選取新的勾選框，Web 介面上會隱藏 Network Interfaces 頁面上的 IPv6 區域。

Hostname

使用此欄位可定義 IMM 子系統的唯一主機名稱。您可以在此欄位中鍵入最多 63 個字元。主機名稱只能由英數字元、連字號和底線組成。

註：依預設，主機名稱爲 IMM-，後接燒錄的 MAC 位址。

Domain name

使用此欄位可定義 DNS 網域名稱。

DDNS Status

使用此欄位可啓用或停用「動態 DNS (DDNS)」。DDNS 可讓 IMM 即時通知

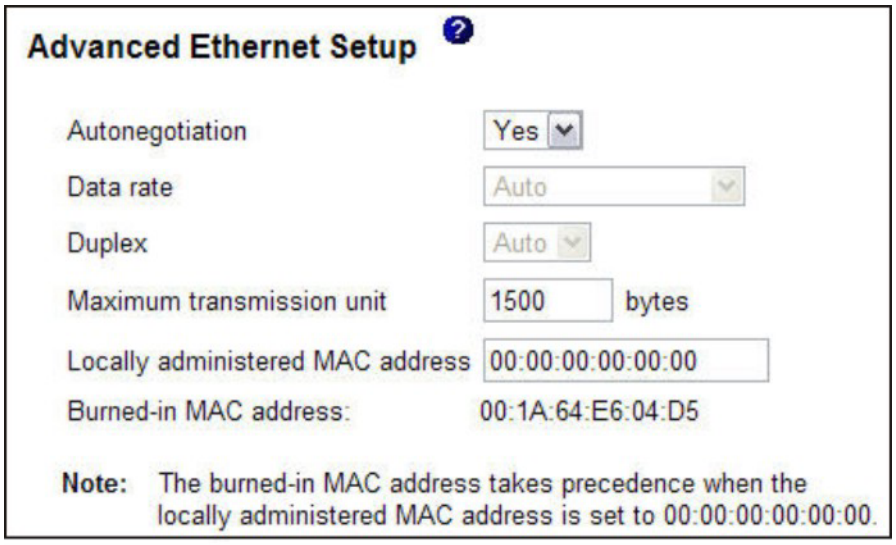
DNS 伺服器變更所配置主機名稱、位址或 DNS 中儲存的其他資訊的作用中 DNS 配置。啓用 DDNS 時，IMM 會通知 DNS 伺服器從 DHCP 伺服器或透過自我配置收到的 IP 位址。

Domain Name Used

使用此欄位可選取在啓用 DDNS 時，DHCP 或手動指派的網域名稱是否傳送至 DNS。此值將設定爲 DHCP 或 Manual。

Advanced Interface Setup

按一下此鏈結可開啓 Advanced Interface Setup 頁面，此頁面看起來像下列影像。



從此頁面，您可以檢視和變更介面的其他設定。下表說明 Advanced Ethernet Setup 頁面上的設定。

表 4. Advanced Ethernet Setup 頁面上的設定

設定	功能
Autonegotiate	使用此設定可選擇 Data rate 和 Duplex 網路設定是否可配置。如果 Autonegotiate 設定爲 **Yes**，則 Data rate 和 Duplex 設定都設定爲 **Auto**，且不可配置。如果 Autonegotiate 設定爲 **No**，則使用者可以配置 Data rate 和 Duplex 設定。
Data rate	使用此欄位可指定透過 LAN 連線每秒傳送的資料量。若要設定資料傳送速率，請選取對應於您的網路功能的資料傳送速率，以百萬位元 (Mb) 爲單位。若要自動偵測資料傳送速率，請選取 **Auto**。
Duplex	使用此欄位來指定網路中使用的通訊通道的類型。若要設定雙工模式，請選取 **Full** 或 **Half**。Full 雙工容許同時以雙向傳送資料。Half 雙工通道容許以某個方向或另一個方向傳送資料，但不能同時以兩個方向傳送。若要自動偵測雙面列印類型，請選取 **Auto**。

表 4. Advanced Ethernet Setup 頁面上的設定 (繼續)

設定	功能
Maximum transmission unit (MTU)	使用此欄位可指定您的網路介面的封包大小上限（以位元組爲單位）。若要設定 MTU 值，請在文字欄位中輸入所需的數字。對於乙太網路，有效的 MTU 範圍爲 68-1,500。
Locally administered MAC address	使用此欄位可指定此 IMM 子系統的實際位址。如果已指定值，本端管理的位址會置換燒錄的 MAC 位址。本端管理的位址必須是介於 000000000000 - FFFFFFFFFFFF 之間的十六進位值。此值的格式必須是 *XX:XX:XX:XX:XX:XX*，其中 *X* 是介於 0-9 和 A-F 之間的數值。 IMM 不容許使用多重播送位址。多重播送位址將第一個位元組集的最小有效位元設定爲 1。因此，第一個位元組必須是偶數。
Burned-in MAC address	燒錄的 MAC 位址是製造商指派給 IMM 的唯一實際位址。

配置 IPv4 設定

您可以在 Network Interfaces 頁面的 IPv4 區域中修改下列設定。

DHCP 使用此欄位可指定是否要透過網路上的「動態主機配置通訊協定 (DHCP)」伺服器設定 IMM 子系統的乙太網路埠 TCP/IP 設定。若要使用 DHCP 配置，請選取 **Enabled - Obtain IP config. from DHCP server**。若要手動配置 TCP/IP 設定，請選取 **Disabled - Use static IP configuration**。如果您要嘗試 DHCP 伺服器，然後在無法存取 DHCP 伺服器時回復爲靜態 IP 配置，請選取 **Try DHCP server. If it fails, use static IP config**。

如果 IP 配置由 DHCP 伺服器指派，請按一下鏈結 **IP Configuration Assigned by DHCP server** 以檢視配置詳細資料。

註：

1. 如果您選取 **Enabled - Obtain IP config. from DHCP server** 選項，則您的網路上必須具有可存取的、作用中和已配置的 DHCP 伺服器。
2. DHCP 伺服器指派的配置將置換任何靜態 IP 設定。
3. 並非所有 IMM 都支援 **Try DHCP server. If it fails, use static IP config.** 選項。

Static IP Configuration

下列欄位包含此介面的靜態 IP 配置。這些設定將僅在停用 DHCP 時使用。如果已啓用 DHCP，DHCP 伺服器指派的動態 IP 配置將置換這些靜態設定。

- **IP address**：使用此欄位可定義透過此網路介面存取的 IMM 子系統的 IP 位址。若要設定 IP 位址，請在文字框中鍵入位址。IP 位址必須包含四個整數 (0-255)，由句點區隔且無空格。

  註：此欄位的預設值爲 `192.168.70.125`。

- **Subnet mask**：使用此欄位可定義 IMM 子系統將使用的子網路遮罩。若要設定子網路遮罩，請在文字框中鍵入位元遮罩。子網路遮罩必須包含四個整數 (0-255)，由句點區隔且無空格。位元必須以最左側位元開始連續地設定。例如，0.255.0.0 不是有效的子網路遮罩。此欄位不能設定爲 0.0.0.0 或 255.255.255.255。

  註：此欄位的預設值爲 255.255.255.0。

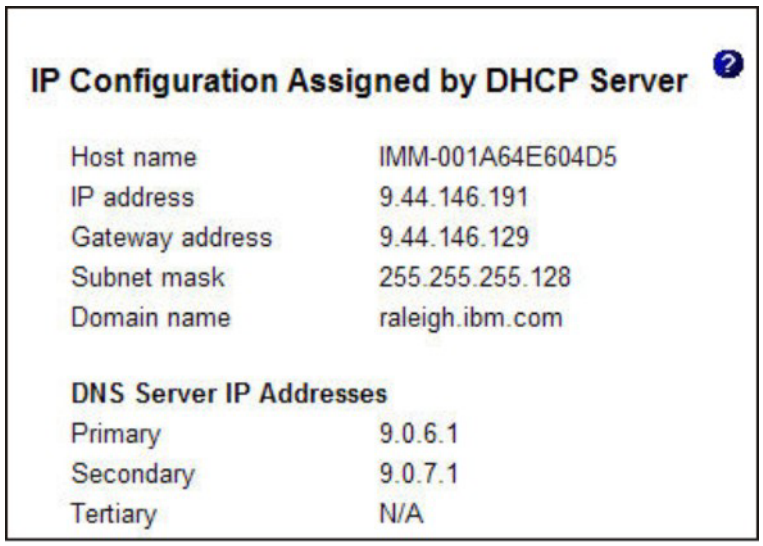
- **Gateway address**：使用此欄位可識別預設閘道的 IP 位址。若要設定閘道位址，請在文字框中鍵入位址。閘道位址必須包含四個整數 (0-255)，由句點區隔，且無空格或連續句點。

  註：此欄位的預設值爲 0.0.0.0。

IP Configuration Assigned by DHCP Server

按一下此鏈結可檢視 DHCP 伺服器指派的 IP 配置。畫面上會顯示類似下列影像的 IP Configuration Assigned by DHCP Server 頁面。

註：僅在啓用 DHCP 時，才能使用此選項。



配置 IPv6 設定

您可以在 Network Interfaces 頁面的 IPv6 區域中修改下列設定。

註：必須啓用此章節中所述的至少一個 IPv6 配置選項（IPv6 Static Configuration、DHCPv6 或 Stateless Auto-configuration）。

Link local address

鏈結本端位址是指派給 IMM 的 IPv6 位址。鏈結本端位址的格式類似下列範例：

```
fe80::21a:64ff:fee6:4d5
```

IPv6 Static Configuration

使用此欄位可啓用或停用 IPv6 的靜態配置設定。選取 **IPv6 Static Configuration** 勾選框時，下列選項可用：

- **IP address**：使用此欄位可定義透過此網路介面存取的 IMM 的 IPv6 位址。若要設定 IP 位址，請在文字框中鍵入 IPv6 位址。此欄位中的值必須是有效的 IPv6 位址。

  註：此欄位的預設值爲 0::0。
- **Address prefix length (1 - 128)**：使用此欄位可設定靜態 IPv6 位址的字首長度。
- **Default route**：使用此欄位可設定您的預設路由的 IPv6 位址。若要設定預設路由，請在對應方框中鍵入 IPv6 位址。此欄位中的值必須是有效的 IPv6 位址。

  註：此欄位的預設值爲 0::0。

  .

DHCPv6

使用此欄位可啓用或停用 IMM 上的 DHCPv6 指派的配置。

Stateless Auto-configuration

使用此欄位可啓用或停用 IMM 上的無狀態自動配置。

View Automatic Configuration (link)

若要檢視 DHCP 伺服器指派的 IPv6 配置，請按一下此鏈結。畫面上會顯示 IPv6 Automatic Configuration 頁面。

配置網路通訊協定

在 Network Protocols 頁面上，您可以執行下列功能：

- 配置簡易網路管理通訊協定 (SNMP)
- 配置網域名稱系統 (DNS)
- 配置 Telnet 通訊協定
- 配置簡易郵件傳送通訊協定 (SMTP)
- 配置輕量型目錄存取通訊協定 (LDAP)
- 配置 Service Location Protocol (SLP)

變更網路通訊協定設定需要重新啓動 IMM，才能使變更生效。如果您要變更多個通訊協定，您可以等到所有通訊協定變更都已執行且已儲存，然後再重新啓動 IMM。

配置 SNMP

您可以使用 SNMP 代理程式來收集資訊和控制伺服器。IMM 也可以配置爲將 SNMP 警示傳送至已配置的主機名稱或 IP 位址。

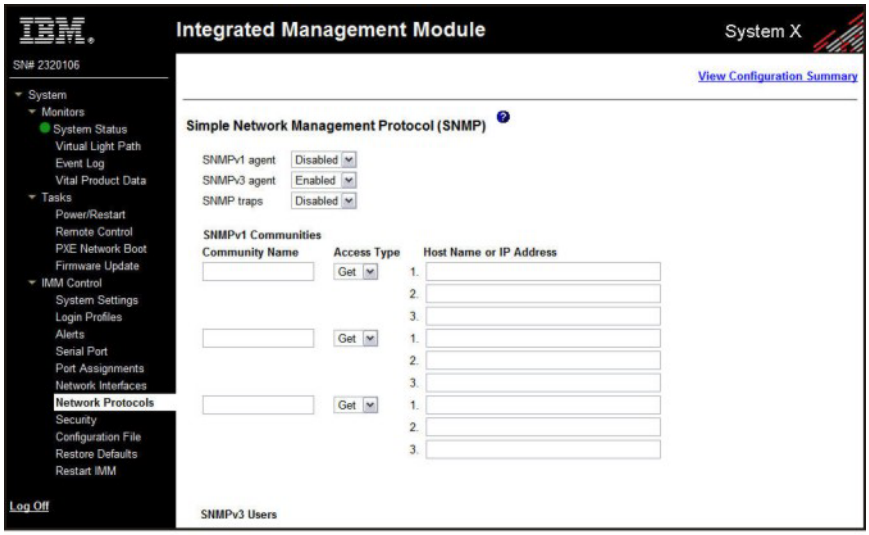
註：

1. IMM 提供了兩個與 SNMP 應用程式搭配使用的「管理資訊庫 (MIB)」檔案。MIB 檔案包含在 IMM 韌體更新項目套件中。
2. IMM 支援 SNMPv1 和 SNMPv3 標準。

若要配置 SNMP，請完成下列步驟：

1. 登入您要配置 SNMP 的 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。

2. 在導覽窗格中，按一下 **Network Protocols**。畫面上會顯示與下圖類似的頁面。



3. 在 **SNMPv1 agent** 或 **SNMPv3 agent** 欄位中選取 **Enabled**。

   註： 如果已啓用 SNMPv3 代理程式，您必須針對作用中登入設定檔配置 SNMPv3 設定，以使 SNMPv3 管理程式與 SNMPv3 代理程式之間的互動正常工作。您可以在 Login Profiles 頁面上個別登入設定檔設定的底端，配置這些設定（如需相關資訊，請參閱第 22 頁的『建立登入設定檔』）。按一下要配置的登入設定檔的鏈結，捲動至頁面的底端，然後按一下 **Configure SNMPv3 User** 勾選框。

4. 選取 **SNMP traps** 欄位中的 **Enabled**，以將警示轉遞至您的網路上的 SNMP 社群。若要啓用 SNMP 代理程式，必須符合下列準則：
   - 必須在 System Settings 頁面上指定系統聯絡人。如需 System Settings 頁面設定的相關資訊，請參閱第 18 頁的『設定系統資訊』。
   - 必須在 System Settings 頁面上指定系統位置。
   - 必須指定至少一個社群名稱。
   - 必須爲該社群指定至少一個有效的 IP 位址或主機名稱（如果已啓用 DNS）。

   註：通知方法是 SNMP 的警示接收者無法接收警示，除非 **SNMPv1 agent** 或 **SNMPv3 agent** 和 **SNMP traps** 欄位設定爲 **Enabled**。

5. 設定社群，以定義 SNMP 代理程式與 SNMP 管理程式之間的管理關係。您必須定義至少一個社群。每一個社群定義由下列參數組成：
   - 社群名稱
   - 存取類型
   - IP 位址

   如果其中任一參數不正確，則無法授與 SNMP 管理存取權。

   註：如果錯誤訊息視窗開啓，請對錯誤視窗中列出的欄位進行必要的調整。然後，捲動至頁面的底端，並按一下 **Save** 以儲存已更正的資訊。您必須配置至少一個社群，才能啓用此 SNMP 代理程式。

6. 在 **Community Name** 欄位中，輸入名稱或鑑別字串以指定社群。

7. 在 **Access Type** 欄位中，選取存取類型。選取 **Trap** 以容許社群中的所有主機接收設陷；選取 **Get** 以容許社群中的所有主機接收設陷和查詢 MIB 物件；選取 **Set** 以容許社群中的所有主機接收設陷、查詢和設定 MIB 物件。
8. 在對應的 **Host Name or IP Address** 欄位中，輸入每一個社群管理程式的主機名稱或 IP 位址。
9. 捲動至頁面的底端，然後按一下 **Save**。
10. 在導覽窗格中，按一下 **Restart IMM** 以啓動變更。

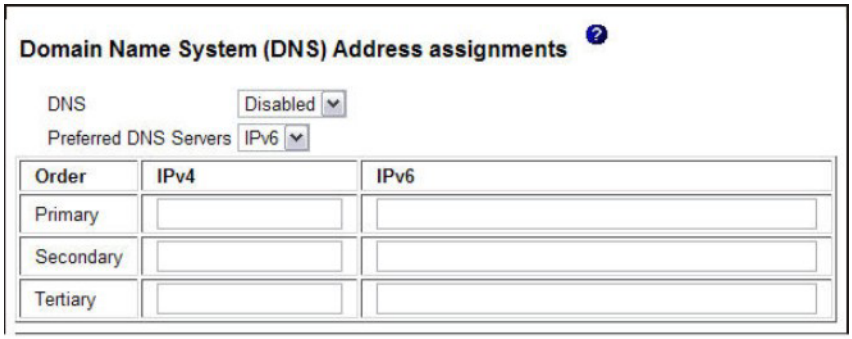
配置 DNS

您可以配置「網域名稱系統 (DNS)」設定，以指定是否應按主機名稱至 IP 位址解析的搜尋順序包括其他 DNS 伺服器位址。DNS 查閱一律處於啓用狀態，其他 DNS 位址則在啓用 DHCP 功能時可能由 DHCP 伺服器自動指派。

若要啓用其他 DNS 位址，其中至少一個位址必須是零以外的值。其他 DNS 伺服器將新增至搜尋清單的頂端，因此在由 DHCP 伺服器自動指派的 DNS 伺服器上進行主機名稱查閱之前，先在其他 DNS 伺服器上執行主機名稱查閱。

若要配置 DNS，請完成下列步驟：

1. 登入您要配置 DNS 的 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **Network Protocols**，然後向下捲動至此頁面的 **Domain Name System (DNS) Address assignments** 區域。畫面上會顯示類似下圖的頁面區段。



3. 如果您的網路上提供了 DNS 伺服器，請在 **DNS** 欄位中選取 **Enabled**。**DNS** 欄位指定您是否使用網路上的 DNS 伺服器，來將主機名稱轉換爲 IP 位址。
4. 如果您具有 IPv4 和 IPv6 DNS 伺服器位址，請在 **Preferred DNS Servers** 清單中選取 **IPv4** 或 **IPv6**，以指定偏好的伺服器位址。
5. 如果您已啓用 DNS，請使用 Primary、Secondary 和 Tertiary 文字欄位，來指定您的網路上最多六個 DNS 伺服器的 IP 位址。若要設定三個 IPv4 或三個 IPv6 DNS 伺服器位址，請在適用的文字欄位中鍵入位址。請確定 IPv4 或 IPv6 位址的格式有效。
6. 捲動至頁面的底端，然後按一下 **Save**。
7. 在導覽窗格中，按一下 **Restart IMM** 以啓動變更。

配置 Telnet

若要配置 Telnet，請完成下列步驟：

1. 登入您要配置 Telnet 的 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **Network Protocols**，然後向下捲動至此頁面的 **Telnet Protocol** 區域。您可以設定並行 Telnet 使用者的數目上限，或者您可以停用 Telnet 存取權。
3. 捲動至頁面的底端，然後按一下 **Save**。
4. 在導覽窗格中，按一下 **Restart IMM** 以啓動變更。

配置 SMTP

若要指定「簡易郵件傳送通訊協定 (SMTP)」伺服器的 IP 位址或主機名稱，請完成下列步驟。

1. 登入您要配置 SMTP 的 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **Network Protocols**，然後向下捲動至此頁面的 **SMTP** 區域。
3. 在 **SMTP Server Host Name or IP address** 欄位中，鍵入 SMTP 伺服器的主機名稱。使用此欄位指定 IP 位址，或 SMTP 伺服器的主機名稱（如果已啓用或配置 DNS）。
4. 捲動至頁面的底端，然後按一下 **Save**。
5. 在導覽窗格中，按一下 **Restart IMM** 以啓動變更。

配置 LDAP

使用「輕量型目錄存取通訊協定 (LDAP)」伺服器，IMM 可以透過查詢或搜尋 LDAP 伺服器上的 LDAP 目錄（而非查看本端使用者資料庫）來鑑別使用者。然後，IMM 可以透過中央 LDAP 伺服器從遠端鑑別任何使用者存取。這需要 IMM 上的 LDAP 用戶端支援。您也可以根據 LDAP 伺服器上找到的資訊，指派權限層級。

您還可以使用 LDAP 將使用者和 IMM 指派給群組，並執行除一般使用者（密碼檢查）鑑別之外的群組鑑別。例如，IMM 可以與一個以上群組相關聯，且僅在使用者屬於至少一個與 IMM 相關聯的群組時，使用者才傳遞群組鑑別。

本章節提供了配置下列兩個 LDAP 伺服器的相關資訊：

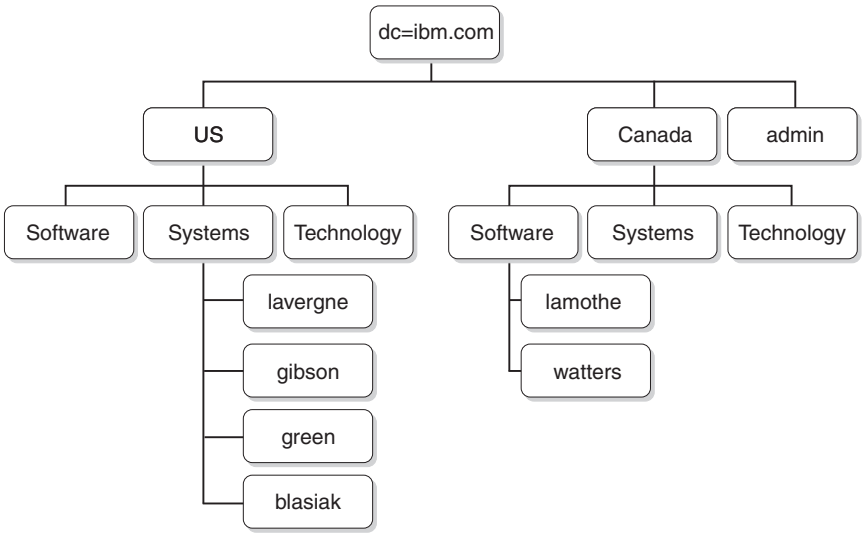
- Novell eDirectory 8.7.1 版
- Microsoft Windows Server 2003 Active Directory

使用者綱目範例

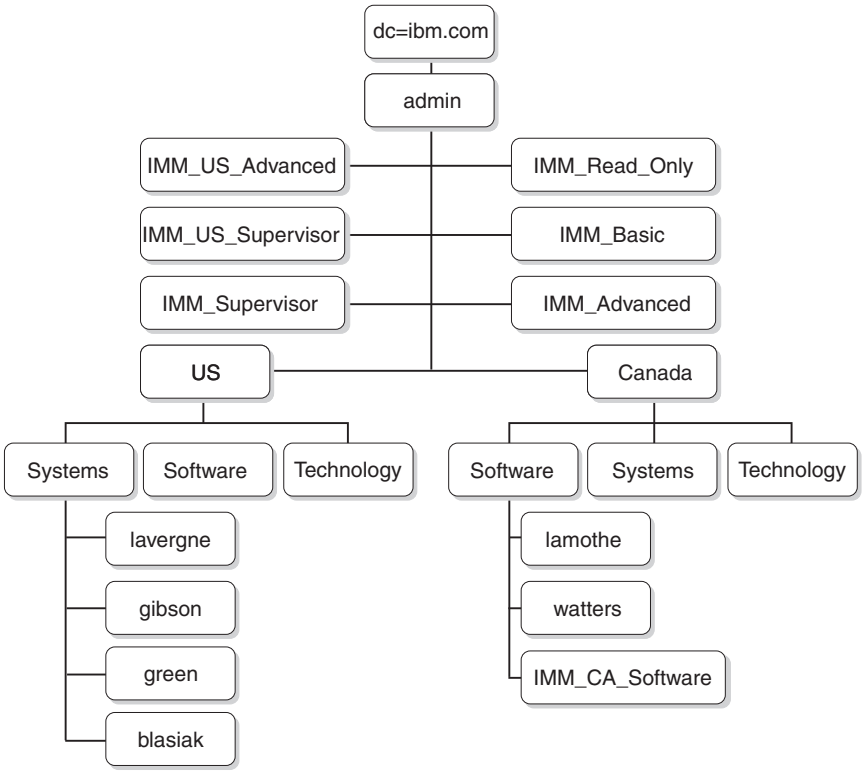
本節將說明簡式使用者綱目範例。在整個文件中，皆會使用此綱目範例來說明 LDAP 用戶端和 LDAP 伺服器上的配置。

此使用者綱目範例以稱爲 ibm.com 的網域元件爲根。換言之，此樹狀結構中的每個物件皆具有等於 dc=ibm,dc=com 的根識別名稱。現在，假設此樹狀結構所代表的公司，想要根據使用者的國家/地區和組織對使用者和使用者群組進行分類。階層爲根 → 國家/地區 → 組織 → 人員。

下圖顯示本文件中所用綱目的簡化視圖。請注意根正下方使用者帳戶 (userid=admin) 的用法。此爲管理者。



下圖顯示如何新增使用者群組。圖中定義了六個使用者群組，並已將其新增至第一層，同時還將另一個使用者群組新增至國家/地區爲 Canada 的 Software 組織。



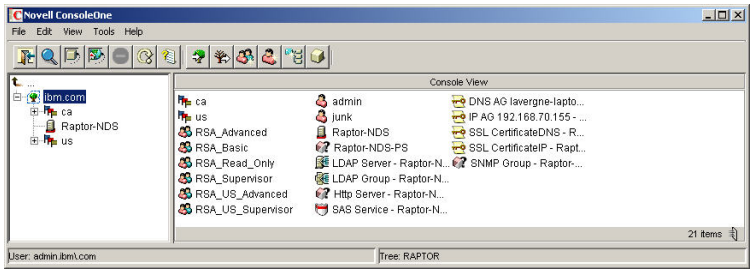
第 43 頁的表 5 中的使用者和相關聯使用者群組，可用來完成此綱目。

表 5. 使用者至群組對映

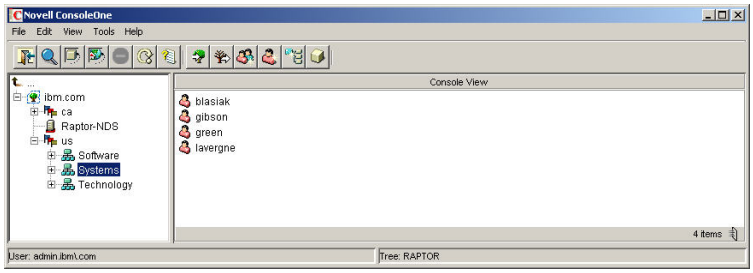
使用者識別名稱	群組成員資格
cn=lavergne、o=Systems、c=us、dc=ibm.com	cn=IMM_Supervisor、dc=ibm.com cn=IMM_US_Supervisor、dc=ibm.com
cn=blasiak、o=Systems、c=us、dc=ibm.com	cn=IMM_US_Advanced、dc=ibm.com
cn=gibson、o=Systems、c=us、dc=ibm.com	cn=IMM_Basic、dc=ibm.com
cn=green、o=Systems、c=us、dc=ibm.com	cn=IMM_Read_Only、dc=ibm.com
cn=watters、o=Systems、c=ca、dc=ibm.com	cn=IMM_CA_Software、o=Software、 c=ca、dc=ibm.com
cn=lamothe、o=Systems、c=ca、dc=ibm.com	cn=IMM_CA_Software、o=Software、 c=ca、dc=ibm.com

Novell eDirectory 網目視圖

使用 Novell ConsoleOne 工具，將第 41 頁的『使用者網目範例』中所述的網目擷取至 Novell eDirectory。下圖顯示透過 ConsoleOne 工具所看到的網目最上層視圖。



下圖擷取 o=Systems、c=us、dc=ibm.com 下的使用者。



群組成員資格

Novell eDirectory 使用稱爲 **GroupMembership** 的屬性，來識別使用者屬於其成員的群組。User 物件類別專門使用此屬性。在查詢使用者屬於其成員的群組時，LDAP 用戶端會在它向 LDAP 伺服器發出的搜尋要求中使用 **memberOf** 的預設值。

您可以使用下列其中一種方法來配置 LDAP 用戶端以查詢成員資格：

- 在 LDAP 用戶端上，配置 **Group Search Attribute** 欄位中的 **GroupMembership** 值。
- 在 Novell eDirectory LDAP 伺服器上，建立 **GroupMembership** 與 **memberOf** 之間的屬性對映。

完成下列步驟以在 LDAP 用戶端上配置預設屬性：

1. 在 IMM Web 介面的左導覽窗格中，按一下 **Network Protocols**。
2. 捲動到 **LDAP Search Attributes** 區域。
3. 在 **Group Search Attribute** 欄位中，鍵入所需的預設屬性。

如果 **Group Search Attribute** 欄位爲空白，則會預設爲 **memberOf**，且您必須配置 Novell eDirectory 伺服器以將 **GroupMembership** 屬性對映至 **memberOf**。完成下列步驟，配置 Novell eDirectory 伺服器以將 **GroupMembership** 屬性對映至 **memberOf**。

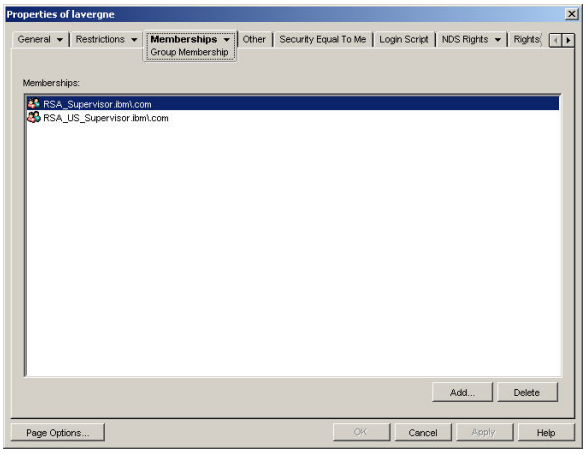
1. 使用 ConsoleOne 工具，用滑鼠右鍵按一下 **LDAP Group** 圖示，然後按一下 **Properties**。Properties of LDAP Group 視窗即會開啓。
2. 按一下 **Attribute Mappings** 標籤。
3. 按一下 **Add**，然後建立 **Group Membership** 與 **memberOf** 之間的對映。
4. 按一下 **OK**。顯示 LDAP 群組內容的頁面即會開啓。

將使用者新增至使用者群組

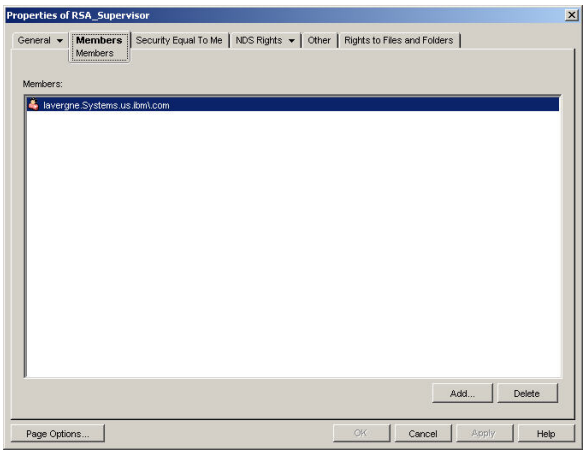
您可以透過將群組新增至使用者的設定檔，或將使用者新增至群組的設定檔，來將使用者新增至適當的使用者群組。最終結果是相同的。

例如，在前一個使用者綱目範例中，使用者 lavergne 是 IMM_US_Supervisor 和 IMM_Supervisor 的成員。透過使用 Novell ConsoleOne 等瀏覽器工具，您可以驗證綱目（按兩下 **user lavergne**，然後選取 **Memberships** 標籤）。

類似下圖的頁面即會開啓。



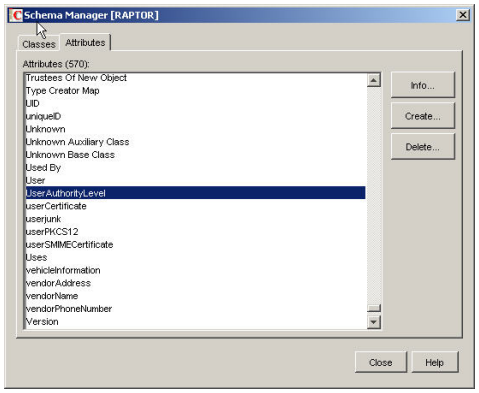
同樣，如果顯示 IMM_Supervisor 群組的內容，且您選取 **Members** 標籤，類似下圖的頁面即會開啓。



權限層級

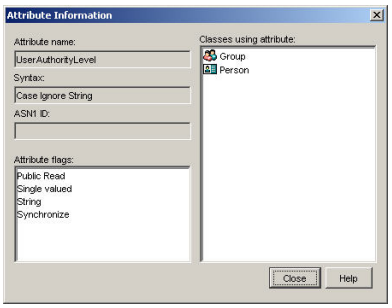
若要使用權限層級特性，請使用 ConsoleOne 在 Novell eDirectory 中建立標示爲 `UserAuthorityLevel` 的新屬性。此新屬性將用於支援權限層級。

1. 在 Novell ConsoleOne 工具中，按一下 **Tools** > **Schema Manager**。
2. 按一下 **Attributes** 標籤，然後按一下 **Create**。
3. 將屬性標示爲 **UserAuthorityLevel**。將 **ASN1 ID** 保留空白，或諮詢您的 LDAP 管理者以確定要使用的值。按一下 **Next**。
4. 將語法設定爲 **Case Ignore String**。按一下 **Next**。
5. 適當設定旗標。請諮詢您的 LDAP 管理者以確定是否正確設定這些旗標。按一下 **Public Read** 勾選框；然後按一下 **Next**。
6. 請按一下**完成**。類似下圖的頁面即會開啓。



7. 回到 Schema Manager 視窗，然後按一下 **Classes** 標籤。
8. 按一下 **Person** 類別，然後按一下 **Add**。請注意，您可以改用 User 物件類別。
9. 向下捲動到 **UserAuthorityLevel** 屬性，選取該屬性，然後將其新增至此類別的屬性。按一下 **OK**。
10. 按一下 **Group** 類別，然後按一下 **Add**。
11. 向下捲動到 **UserAuthorityLevel** 屬性，選取該屬性，然後將其新增至此類別的屬性。按一下 **OK**。
12. 若要驗證是否已將屬性順利新增至類別，請在 Schema Manager 視窗中選取 **Attributes** 類別。

13. 捲動到 **UserAuthorityLevel** 屬性；然後按一下 **Info**。類似下圖的頁面即會開啓。



設定權限層級

本節說明如何解譯和使用 UserAuthorityLevel 屬性。指派給 UserAuthorityLevel 屬性的值，將決定在成功鑑別之後指派給使用者的權限（或權限層級）。

UserAuthorityLevel 屬性會被讀取爲位元字串，或 0 和 1。這些位元將從左至右編號。第一個位元是位元位置 0。第二個位元是位元位置 1，依此類推。

下表提供每個位元位置的說明。

表 6. 權限位元

位元位置	功能	說明
0	一律拒絕	如果設定此位元，使用者將一律鑑別失敗。此功能可用於封鎖特定使用者或與特定群組相關聯的使用者。
1	Supervisor 存取權	如果設定此位元，則會將管理者專用權授與使用者。使用者具有對每個功能的讀寫權。如果您設定此位元，則無需個別地設定其他位元。
2	Read Only 存取權	如果設定此位元，使用者將具有唯讀存取權，且無法執行任何維護程序（例如重新啓動、遠端動作或韌體更新）。使用儲存、清除或還原功能將無法進行任何修改。位元位置 2 與所有其他位元互斥，且位元位置 2 具有最低的優先順序。如果設定任何其他位元，則會忽略此位元。
3	網路功能與安全性	如果設定此位元，使用者可以修改 Security、Network Protocols、Network Interface、Port Assignments 及 Serial Port 畫面中的配置。
4	使用者帳戶管理	如果設定此位元，使用者可以新增、修改或刪除使用者，以及變更 Login Profiles 畫面中的 Global Login Settings。
5	遠端主控台存取	如果設定此位元，使用者可以存取遠端伺服器主控台，以及修改 Serial Port 畫面中的配置。

表 6. 權限位元 (繼續)

位元位置	功能	說明
6	遠端主控台及遠端磁碟存取	如果設定此位元，使用者可以存取遠端伺服器主控台，以及遠端伺服器的遠端磁碟功能。使用者也可以修改 Serial Port 畫面中的配置。
7	端伺服器電源/重新啓動存取	如果設定此位元，使用者可以存取遠端伺服器的開啓電源、重新啓動及伺服器逾時功能。
8	基本配接器配置	如果設定此位元，使用者可以修改 System Settings 和 Alerts 畫面中的配置參數（Contact、Location 及 Server Timeout 參數除外）。
9	清除事件日誌的能力	如果設定此位元，使用者可以清除事件日誌。 **註**：所有使用者都可以檢視事件日誌；但是，使用者需要具有此層次的權限才能清除日誌。
10	進階配接器配置	如果設定此位元，使用者在配置配接卡時沒有任何限制，並且具有對 IMM 的管理存取權。使用者可以執行下列進階功能：韌體升級、PXE 網路開機、還原配接卡原廠預設值、從配置檔修改和還原配接卡配置，以及重新啓動/重設配接卡。這不包括 Server Power/Restart Control 和逾時功能。
11	保留	此位元位置保留給將來使用（目前會忽略）。

注意事項：

- 如果沒有使用任何位元，則會將使用者的預設值設定爲 Read Only。
- 直接從使用者記錄擷取的登入權限將享有優先順序。如果使用者記錄在 **Login Permission Attribute** 欄位中沒有包含名稱，則會嘗試從使用者所屬且符合群組過濾器的群組中擷取權限。在此情況下，將爲使用者指派所有群組的所有位元之內含 OR。
- 如果爲任何群組設定「一律拒絕」（位元位置 0）位元，將拒絕使用者存取。「一律拒絕」位元優先於所有其他位元。
- 如果使用者能夠修改基本、網路或安全相關的配接卡配置參數，您應該考量賦予使用者重新啓動 IMM 的能力（位元位置 10）。如果沒有此能力，使用者或許能夠變更參數；但是，此參數不會生效。

下表包含範例及其說明：

表 7. UserLevelAuthority 屬性範例和說明

UserLevelAuthority 屬性範例	說明
IBMRBSPermissions=010000000000	Supervisor 存取權（設定位元位置 1）
IBMRBSPermissions=001000000000	Read-Only 存取權（設定位元位置 2）
IBMRBSPermissions=100000000000	無存取權（設定位元位置 0）
IBMRBSPermissions=000011111100	除進階配接器配置以外的所有權限

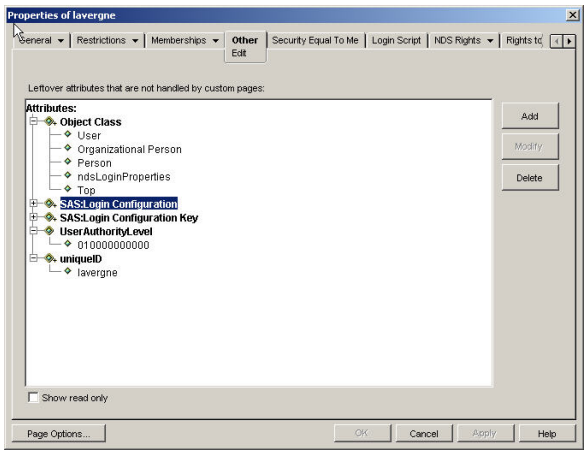
表 7. UserLevelAuthority 屬性範例和說明 (繼續)

UserLevelAuthority 屬性範例	說明
IBMRBSPermissions=000011011110	除虛擬媒體存取權以外的所有權限

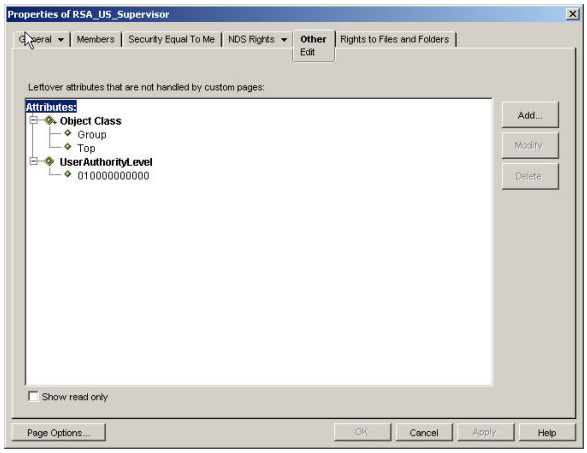
完成下列步驟即可將 UserAuthorityLevel 屬性新增至使用者 *lavergne*，以及每個使用者群組：

1. 用滑鼠右鍵按一下使用者 **lavergne**，然後按一下 **Properties**。
2. 按一下 **Other** 標籤。按一下 **Add**。
3. 向下捲動到 **UserAuthorityAttribute**，然後按一下 **OK**。
4. 填寫您需要的屬性值。例如，如果您要指派 Supervisor 存取權，請將屬性設定爲 **IBMRBSPermissions=010000000000**。按一下 **OK**。
5. 針對每個使用者群組重複步驟 1 至 4，然後適當設定 **UserAuthorityLevel**。

下圖顯示使用者 *lavergne* 的內容。



下圖顯示 IMM_US_Supervisor 的內容。



下表顯示指派給使用者網目範例中每個使用者群組的 **UserAuthorityLevel**。

表 8. 將 UserAuthorityLevel 指派給使用者群組

使用者群組	UserAuthorityLevel	轉換
IMM_Basic	IBMRBSPermissions=000100000000	網路功能與安全性
IMM_CA_Software	IBMRBSPermissions=000101111010	網路功能與安全性 遠端主控台和虛擬媒體存取，遠端伺服器電源和重新啓動存取 基本配接器配置 進階配接器配置
IMM_Advanced	IBMRBSPermissions=000110111100	網路功能與安全性 遠端主控台和虛擬媒體存取，遠端伺服器電源和重新啓動存取 基本配接器配置 進階配接器配置 清除事件日誌的能力
IMM_Supervisor	IBMRBSPermissions=010000000000	Supervisor 存取權
IMM_Read_Only	IBMRBSPermissions=001000000000	Read-only 存取權
IMM_US_Advanced	IBMRBSPermissions=000110111100	網路功能與安全性 使用者帳戶管理 遠端主控台和虛擬媒體存取，遠端伺服器電源和重新啓動存取 基本配接器配置 清除事件日誌的能力
IMM_US_Supervisor	IBMRBSPermissions=010000000000	Supervisor 存取權

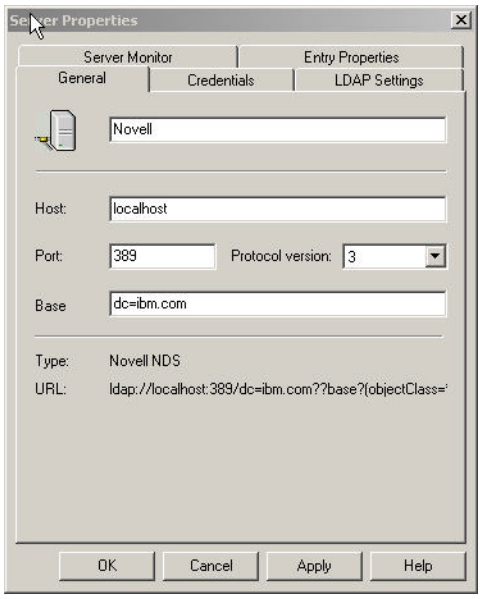
瀏覽 LDAP 伺服器

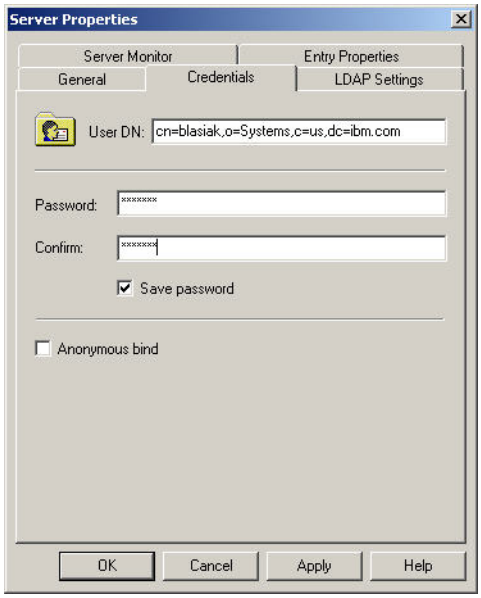
嘗試從 IMM 上的 LDAP 用戶端連接至 LDAP 伺服器之前，請使用所選協力廠商 LDAP 瀏覽器連接至 LDAP 伺服器。例如，從 http://www.ldapbrowser.com 上可取得目錄瀏覽工具。

在嘗試使用 IMM LDAP 用戶端之前使用 LDAP 瀏覽器具有下列優點：

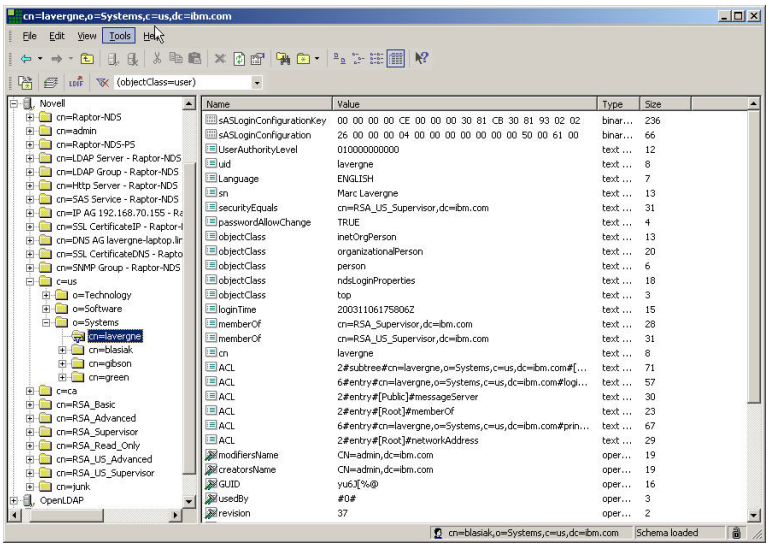
- 可使用各種認證連結至伺服器。這將顯示是否正確設定 LDAP 伺服器上的使用者帳戶。如果您可以使用瀏覽器連結至伺服器，但無法使用 IMM LDAP 用戶端連結至伺服器，則表示未正確配置 LDAP 用戶端。如果您使用瀏覽器無法進行連結，則使用 IMM 上的 LDAP 用戶端也將無法進行連結。
- 順利連結至伺服器之後，即可導覽 LDAP 伺服器資料庫並快速發出搜尋查詢。這將確認是否針對各種物件的存取權，按您所需方式來配置 LDAP 伺服器。例如，您可能會發現自己無法檢視特定屬性，或可能看不到預期在特定搜尋要求中看到的所有物件。這表示未正確配置指派給物件的權限（例如，哪個是公開可見或隱藏的物件）。請聯絡 LDAP 伺服器管理者以更正此問題。請務必注意，您用於連結的認證會決定您在伺服器中擁有的專用權。
- 驗證所有使用者的群組成員資格。驗證指派給使用者和使用者群組的 **UserAuthorityLevel** 屬性。

下圖顯示對使用第 41 頁的『使用者綱目範例』配置的 Novell eDirectory 伺服器，所做的各種查詢和搜尋結果。在此案例中，使用的是 Softerra LDAP 瀏覽器工具。起始連結至伺服器時使用的是圖中所示的內容和認證。

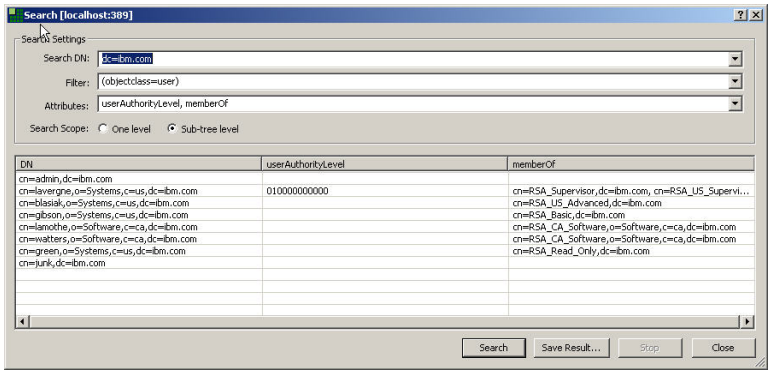




起始連結成功之後，將會顯示 Novell eDirectory 上綱目的下列視圖。



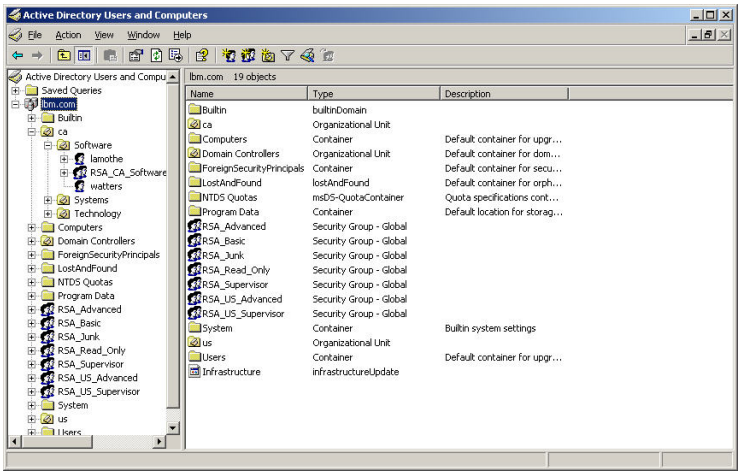
下圖顯示透過擷取 **userAuthorityLevel** 和 **memberOf** 屬性的要求，對所有使用者進行的查詢。



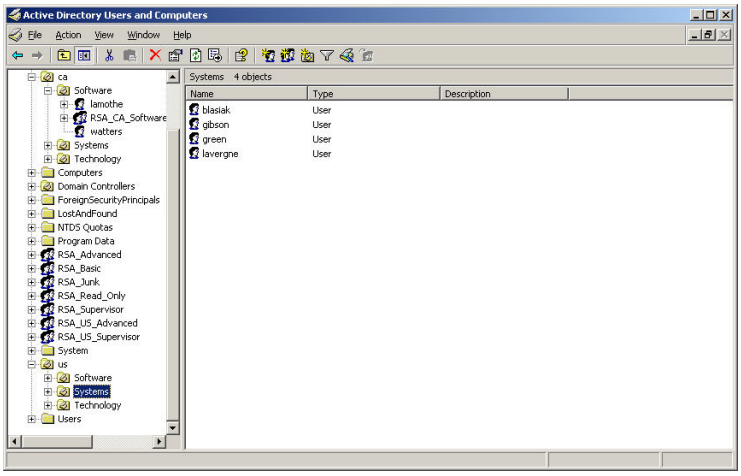
Microsoft Windows Server 2003 Active Directory 綱目視圖

本節說明與在 Microsoft Windows Server 2003 Active Directory 上，擷取第 41 頁的『使用者綱目範例』中資訊相關的部分配置方面。

下圖顯示透過「Active Directory 使用者和電腦」管理工具所看到的綱目最上層視圖。



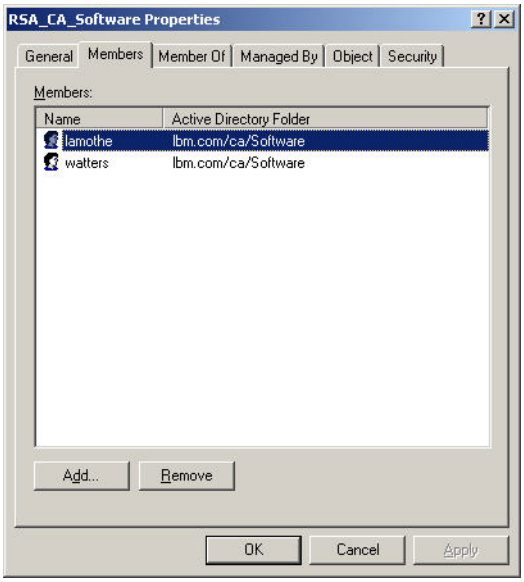
下圖顯示 ou=Systems、ou=us、dc=ibm、dc=com 下的使用者。



將使用者新增至使用者群組

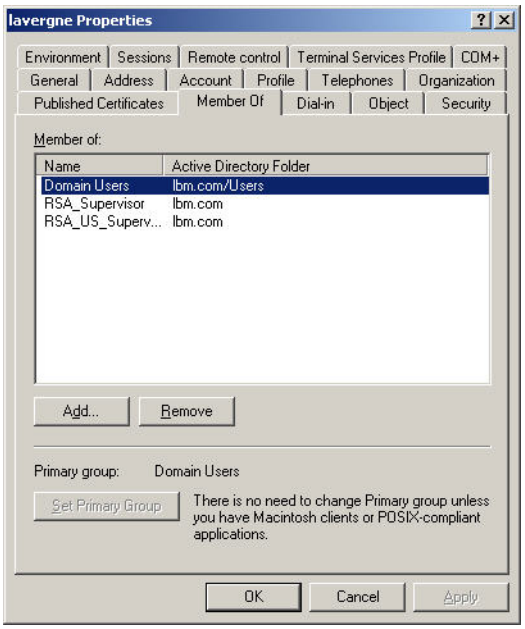
在 Active Directory 中，您可以將群組新增至特定使用者，或將使用者新增至特定群組。用滑鼠右鍵按一下使用者或使用者群組物件，然後按一下**內容**。

如果您選取某個使用者群組，然後按一下 **Members** 標籤，類似下圖中的頁面即會開啓。



若要在使用者群組中新增或刪除使用者，請按一下**新增**或**移除**。

如果您選取某個使用者，然後按一下**成員屬於**標籤，類似下圖中的頁面即會開啓。

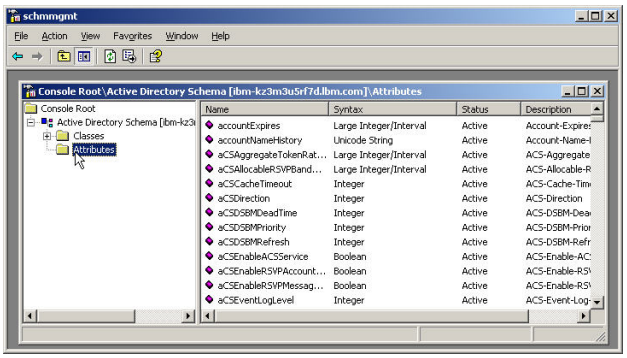


若要在使用者群組中新增或刪除使用者，請按一下**新增**或**移除**。

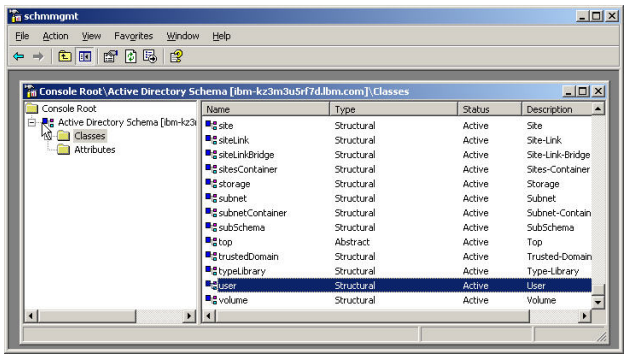
權限層級

第 45 頁的『權限層級』一節說明如何使用 Novell eDirectory 伺服器建立新屬性來支援權限層級概念，以及如何將這些權限層級指派給從 IMM 向 LDAP 伺服器進行鑑別的使用者。建立的屬性稱爲 **UserAuthorityLevel**。在此章節中，您將在 Active Directory 中建立此屬性。

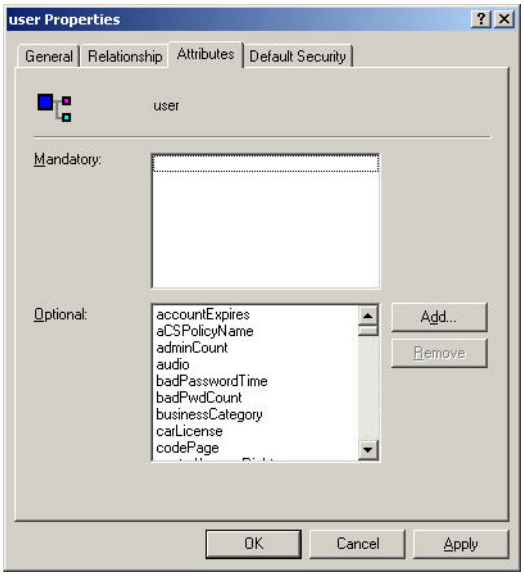
1. 安裝「Active Directory 架構嵌入式管理單元」工具。如需相關資訊，請參閱 Active Directory 隨附的文件。
2. 啓動「Active Directory 架構」。
3. 按一下**動作 > 建立屬性**。完成下列欄位：
   a. 將「一般名稱」設定爲 **UserAuthorityLevel**
   b. 將「語法」設定爲**不區分大小寫字串**
   c. 將「最小值」和「最大值」設定爲 **12**
4. 聯絡系統管理者以指派新的 X.500 OID。如果您不想定義新的 X.500 OID，請使用現有屬性，而不要爲權限層級建立新屬性。



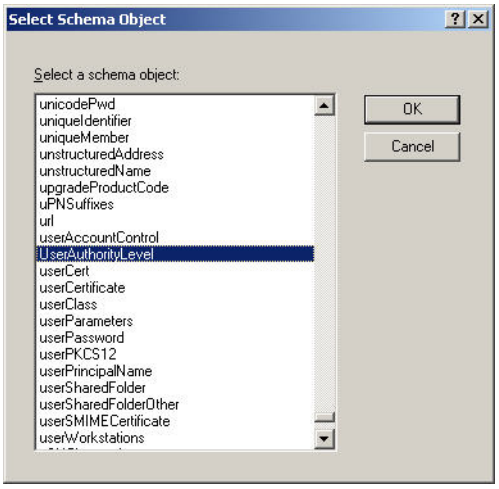
5. 儲存屬性之後，請選取**類別**資料夾。



6. 按兩下 **User** 類別。「使用者內容」視窗即會開啓。

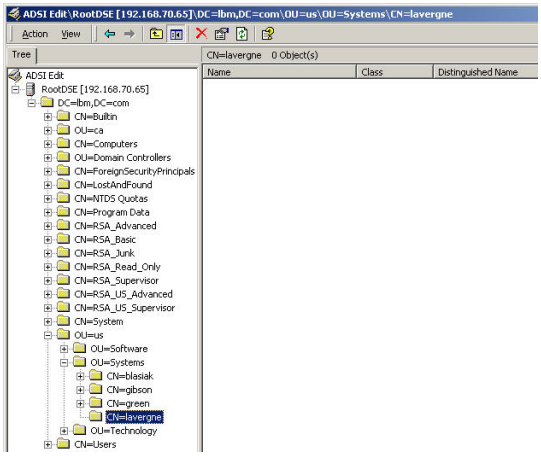


7. 選取**屬性**標籤，然後按一下**新增**。「選取架構物件」視窗即會開啓。

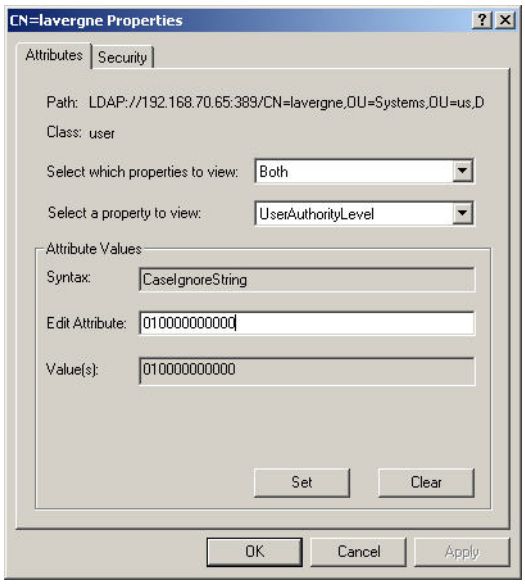


8. 向下捲動到 **UserAuthorityLevel**，然後按一下**確定**。此屬性即會出現在使用者物件類別的選用屬性清單中。
9. 針對 Group 類別，重複步驟 6 至步驟 8。如此即允許將 **UserAuthorityLevel** 屬性指派給使用者或使用者群組。只有這兩個物件類別才需要使用此新屬性。

10. 將 **UserAuthorityLevel** 屬性指派給適當的使用者和使用者群組。若要符合在 Novell eDirectory 伺服器下定義的綱目，請使用與第 46 頁的『設定權限層級』中相同的值。您可以使用「ADSI 編輯」工具來執行此作業。Microsoft 的「ADSI 編輯」支援工具是一個 Microsoft Management Console (MMC) 嵌入式管理單元，用於檢視目錄中的所有物件（包括綱目和配置資訊）、修改物件，以及設定物件的存取控制清單。
11. 對於本範例，假設您要將 **UserAuthorityLevel** 屬性新增至使用者 lavergne。請使用「ADSI 編輯」執行此作業。您必須提供適當的認證以連接至 Active Directory；否則，您可能沒有適當的使用者專用權來修改伺服器上的物件。下圖顯示在連接至伺服器之後透過 ADSI 所看到的綱目。



12. 用滑鼠右鍵按一下 **lavergne**，然後按一下**內容**。類似下圖的視窗即會開啓。



13. 在**選取要檢視的內容**欄位中，選取 **UserAuthorityLevel**。
14. 在**編輯屬性**欄位中，鍵入將會轉換爲 Supervisor 存取權的 IBMRBSPermissions=010000000000。按一下**設定**。
15. 按一下**確定**。
16. 您可以執行與針對要修改之使用者群組物件相同的步驟，以將此屬性新增至使用者群組。

檢查 Active Directory 配置

嘗試將 LDAP 用戶端連接至 Active Directory（以鑑別使用者）之前，請使用 LDAP 瀏覽器來瀏覽 Active Directory 綱目。至少，請發出下表中所列的查詢，以檢查權限層級和群組成員資格。

表 9. 檢查權限層級和群組成員資格

搜尋識別名稱	過濾器	屬性
DC=ibm、DC=com	(objectclass=user)	memberOf、userAuthorityLevel
DC=ibm、DC=com	(objectclass=group)	member、userAuthorityLevel

配置 LDAP 用戶端

您可以配置 LDAP 以鑑別管理模組使用者。IMM 支援本端和遠端使用者鑑別。本端鑑別會使用在 Login Profiles 頁面中提供的資訊來鑑別使用者。使用 LDAP 伺服器時，管理模組可透過查詢或搜尋遠端 LDAP 伺服器上的 LDAP 目錄（而非檢查其本端使用者資料庫）來鑑別使用者。

使用任何類型的遠端鑑別時，您皆可選擇在本端或根據 LDAP 伺服器中儲存的用於遠端鑑別的資訊，將權限授與已順利鑑別的每個使用者。授與使用者的權限將指定每個使用者在登入 IMM 時可以執行的動作。在下列主題中將說明遠端鑑別方法：

- 使用本端授權的 Active Directory 鑑別
- Active Directory 角色型鑑別和授權
- 舊式 LDAP 鑑別和授權

使用本端授權的 Active Directory 鑑別

您可以使用 Active Directory 鑑別，透過本端使用者授權來設定使用者的遠端 LDAP 鑑別。

註：使用本端授權的 Active Directory 鑑別僅適用於在 Active Directory 環境中使用的伺服器。

將 Active Directory 鑑別與本端授權搭配使用時，Active Directory 伺服器僅用於透過驗證使用者認證來鑑別使用者。在 Active Directory 伺服器中沒有爲給定使用者儲存的授權資訊；必須使用授權資訊來配置 IMM 儲存的群組設定檔。透過從 Active Directory 伺服器擷取使用者的成員資格資訊，可以取得用於配置群組設定檔的授權資訊。此成員資格資訊會提供使用者所屬的群組清單（支援巢狀群組）。然後，將在 Active Directory 伺服器中指定的群組，與在 IMM 中本端配置的群組名稱進行比較。對於使用者是其成員的每個群組，皆會從該群組爲使用者指派權限。對於在 IMM 中本端配置的每個群組名稱，皆有爲該群組配置的對應授權設定檔。

IMM 最多支援 16 個本端配置的群組名稱。每個群組名稱的長度限制爲 63 個字元。必須將下列其中一個屬性配置爲群組名稱，以符合從 Active Directory 伺服器擷取的群組成員資格資訊：

- 識別名稱 (DN)
- ″cn″ 屬性
- ″name″ 屬性
- ″sAMAccountName″ 屬性

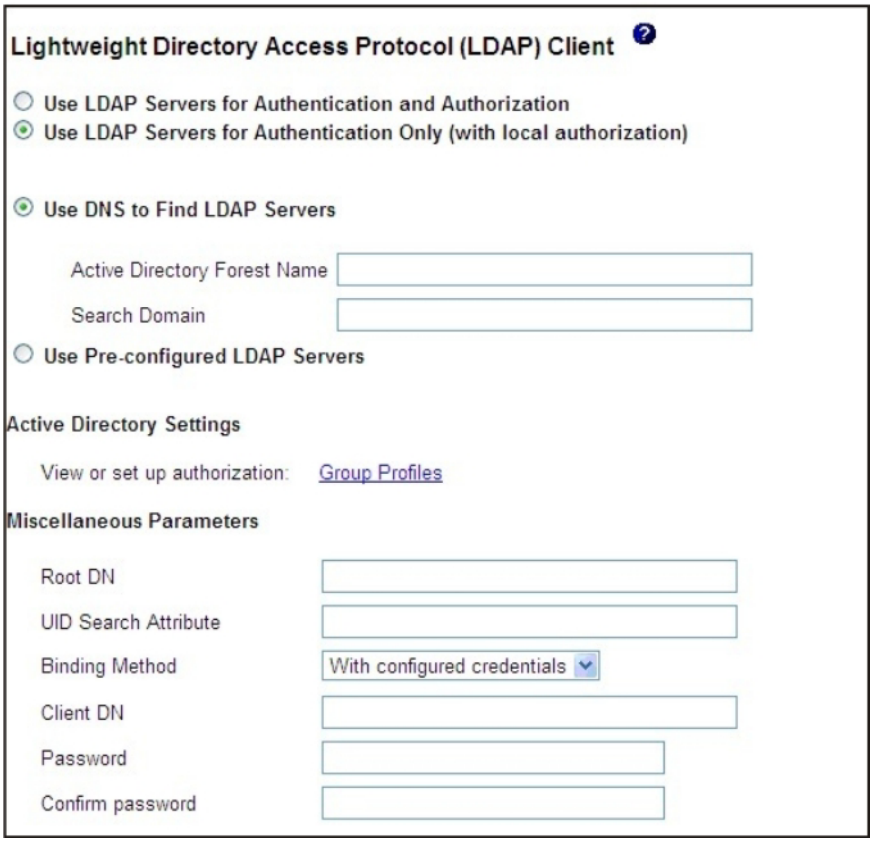
若要爲 IMM 配置使用本端授權的 Active Directory 鑑別，請完成下列步驟：

1. 在導覽窗格中，按一下 **Network Protocols**。
2. 向下捲動到 **Lightweight Directory Access Protocol (LDAP) Client** 區段。
3. 選取 **Use LDAP Servers for Authentication Only (with local authorization)**。
4. 選取下列其中一個選項以手動配置或動態探索網域控制站：
   - 選取 **Use DNS to find LDAP Servers** 以根據 DNS SVR 記錄來動態探索網域控制站。
   - 選取 **Use Pre-Configured LDAP Servers**（預設選項）以手動配置網域控制站。
5. 如果您是使用 DNS 動態探索網域控制站，請配置下列設定；然後，繼續執行步驟 第 58 頁的 7。

   註：如果要使用 DNS 動態探索網域控制站，您必須指定網域控制站的完整網域名稱。

   - Search Domain
     - 在 **Search Domain** 欄位中輸入網域控制站的網域名稱。
   - Active Directory Forest Name
     - 此選用欄位用於探索廣域型錄。屬於跨網域中通用群組的使用者需要廣域型錄。在跨網域群組成員資格不適用的環境中，可將此欄位保留空白。

   下圖顯示使用 DNS 動態探索網域控制站時的 LDAP 用戶端視窗。



6. 如果要手動配置網域控制站和廣域型錄，請使用 **Use Pre-Configured LDAP Servers**（預設）選項；然後，配置 **LDAP Server Host Name or IP Address** 和 **Port** 欄位。

   使用一個 IP 位址或完整主機名稱最多可以配置四個網域控制站。廣域型錄伺服器使用埠號 3268 或 3269 來識別。使用任何其他埠號均表示正在配置網域控制站。

7. 如果您是使用群組授權設定檔，請按一下 Active Directory Settings 區段中的 **Group Profiles**，以檢視或配置它們（如需相關資訊，請參閱第 59 頁的『Active Directory 使用者的群組設定檔』）。
8. 回到 Network Protocols 頁面。按一下 Group Profiles for Active Directory Users 頁面中的 **LDAP Client section of the Network Protocols page** 鏈結；然後捲動到 **Lightweight Directory Access Protocol (LDAP) Client** 區段。
9. 配置 IMM 的細項參數。如需參數的相關資訊，請參閱下表。

表 10. 細項參數

欄位	說明	選項
Root DN	IMM 使用 DN 格式的 **Root DN** 欄位作爲目錄樹的根項目。此 DN 將用作所有搜尋的基本物件。範例可能類似於 `dc=mycompany,dc=com`。	

表 10. 細項參數 (繼續)

欄位	說明	選項
Binding Method	**Binding Method** 欄位用於與網域控制站伺服器的起始連結，請選取一個選項。	• With configured credentials： 輸入用於起始連結的用戶端 DN 和密碼。如果此連結失敗，鑑別程序也會失敗。如果此連結成功，搜尋作業將嘗試尋找符合在 **Client DN** 欄位中所輸入用戶端 DN 的使用者記錄。搜尋作業通常會尋找符合在登入程序期間所提供使用者 ID 的共同屬性。這些屬性包括 displayName、sAMAccountName 及 userPrincipalName。如果已配置 **UID search attribute** 欄位，則搜尋中也會包括此屬性。 如果搜尋成功，則會嘗試第二個連結，此時會使用在登入程序期間提供的使用者 DN（從搜尋中擷取）和密碼。如果第二次連結嘗試成功，鑑別部分也會成功，且會擷取使用者的群組成員資格資訊，並將該資訊與在 IMM 中本端配置的群組進行比對。符合的群組將會定義指派給使用者的授權權限。 • With login credentials： 使用在登入程序期間提供的認證與網域控制站伺服器進行起始連結。如果此連結失敗，鑑別程序也會失敗。如果此連結成功，搜尋作業將嘗試尋找使用者記錄。一旦找到使用者記錄，即會擷取使用者的群組成員資格資訊，並將該資訊與在 IMM 中本端配置的群組進行比對。符合的群組將會定義指派給使用者的授權權限。 • Anonymously： 不使用 DN 或密碼來與網域控制站伺服器進行起始連結。建議不要選取此選項，因爲大部分伺服器都配置爲禁止對特定使用者記錄的搜尋要求。

Active Directory 使用者的群組設定檔

配置群組設定檔以爲使用者群組提供本端授權規格。每個群組設定檔均包括以「權限層級（角色）」表示的授權，且與登入設定檔中的授權完全相同。若要配置群組設定檔，使用者必須具有使用者帳戶管理授權。若要將使用者與群組設定檔相關聯，則需要 LDAP 鑑別伺服器。

群組設定檔清單

按一下 **IMM Control** > **Login Profiles**，即可存取群組設定檔清單。將會顯示每個群組設定檔（與登入設定檔相同）的群組 ID 和角色摘要。從此清單中，可新增群組，並可選取要編輯或刪除的現有群組。

下圖顯示 Group Profiles for Active Directory Users 視窗。

若要編輯群組設定檔，請按一下 **Edit**。即會開啓該群組的 Group Profile 頁面。若要刪除群組設定檔，請按一下 **Delete**。您需要確認是否刪除群組設定檔。若要新增群組設定檔，請按一下 **Add a group** 鏈結。即會開啓 Group Profile 頁面，讓您輸入新群組設定檔的資訊。最多可新增 16 個群組設定檔。群組設定檔名稱不必是唯一的。

下表說明 Group Profile 頁面中的欄位。

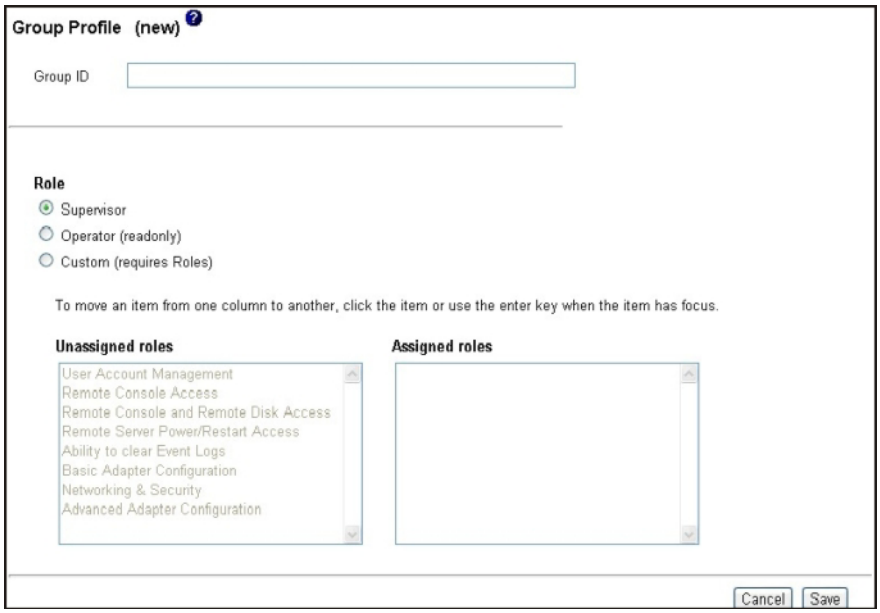
表 11. 群組設定檔資訊

欄位	選項	說明
Group ID		此欄位用於指定群組設定檔的群組 ID。您最多可以輸入 63 個字元。群組 ID 必須與其在 LDAP 伺服器中的對應項目相同。群組名稱的範例爲 IMM Admin Group 和 IMM/Robert。
Role		選取與此登入 ID 相關聯的角色（權限層級），並將其移至 **Assigned roles** 方框。按 Enter 鍵或點擊滑鼠可將所選項目從一個方框移至其他方框。
	Supervisor	除指派的範圍以外，使用者無任何限制。
	Operator	使用者只有唯讀存取權，無法執行任何變更，例如儲存、修改及清除。這還包括影響狀態的作業，例如重新啓動 IMM、還原預設值及升級韌體。
Role	Custom	視指派給使用者的自訂權限層級而定，使用者可能有或沒有任何限制。如果您選取 Custom 選項，則必須選取下列一個以上的自訂權限層級： • 網路功能與安全性 – 使用者可以修改 Security、Network Protocols、Network Interface、Port Assignments 及 Serial Port 畫面中的配置。 • 使用者帳戶管理 – 使用者可以新增、修改或刪除使用者，以及變更 Login Profiles 畫面中的 Global Login Settings。 • 遠端主控台存取 – 使用者可以存取遠端伺服器主控台。 • 遠端主控台及遠端磁碟存取 – 使用者可以存取遠端伺服器主控台，及遠端伺服器的遠端磁碟功能。

表 11. 群組設定檔資訊 (繼續)

欄位	選項	說明
		• 端伺服器電源/重新啓動存取 – 使用者可以存取遠端伺服器的開啓電源、重新啓動及伺服器逾時功能。 • 基本配接器配置 – 使用者可以修改 System Settings 和 Alerts 畫面中的配置參數（Contact、Location 及 Server Timeouts 除外）。 • 清除事件日誌的能力 – 使用者可以清除事件日誌。 **註**：每個人都可以檢視事件日誌；但需要具有此權限才能清除日誌。 • 進階配接器配置 – 使用者在配置配接卡時沒有任何限制，並且具有對 IMM 的管理存取權。使用者可以執行下列進階功能：韌體升級、「開機前執行環境 (PXE)」網路開機、還原配接卡原廠預設值、從配置檔修改和還原配接卡配置，以及重新啓動/重設配接卡。 **註**：此權限層級不包括 Server Power/Restart Control 和逾時功能。
註：爲了避免使用者沒有讀寫權的狀況，必須將第一個登入設定檔設定爲至少能夠修改登入設定檔。必須將 Supervisor 存取權或 User Account Management 存取權授與使用者。這可保證至少有一個使用者可以執行動作、變更配置，以及將亦可執行動作或變更配置的使用者新增至登入設定檔。		

下圖顯示 Group Profile 視窗。



Active Directory 角色型鑑別和授權

您可以使用 Active Directory 設定使用者的遠端 LDAP 鑑別和授權。

注意事項：

- Active Directory 角色型鑑別和授權僅適用於在 Active Directory 環境中使用的伺服器。
- Active Directory 角色型鑑別和授權需要「加強角色型安全嵌入式管理單元」工具。

Active Directory 角色型鑑別和授權使用在 Active Directory 伺服器中儲存的配置資訊來鑑別使用者，然後將權限與使用者相關聯。在啓用 Active Directory 角色型鑑別和授權之前，請使用「加強角色型安全嵌入式管理單元」工具，將配置資訊儲存在將權限與使用者相關聯的 Active Directory 伺服器上。此工具可在任何 Microsoft Windows 用戶端上執行，並可從 http://www.ibm.com/systems/support/ 下載。

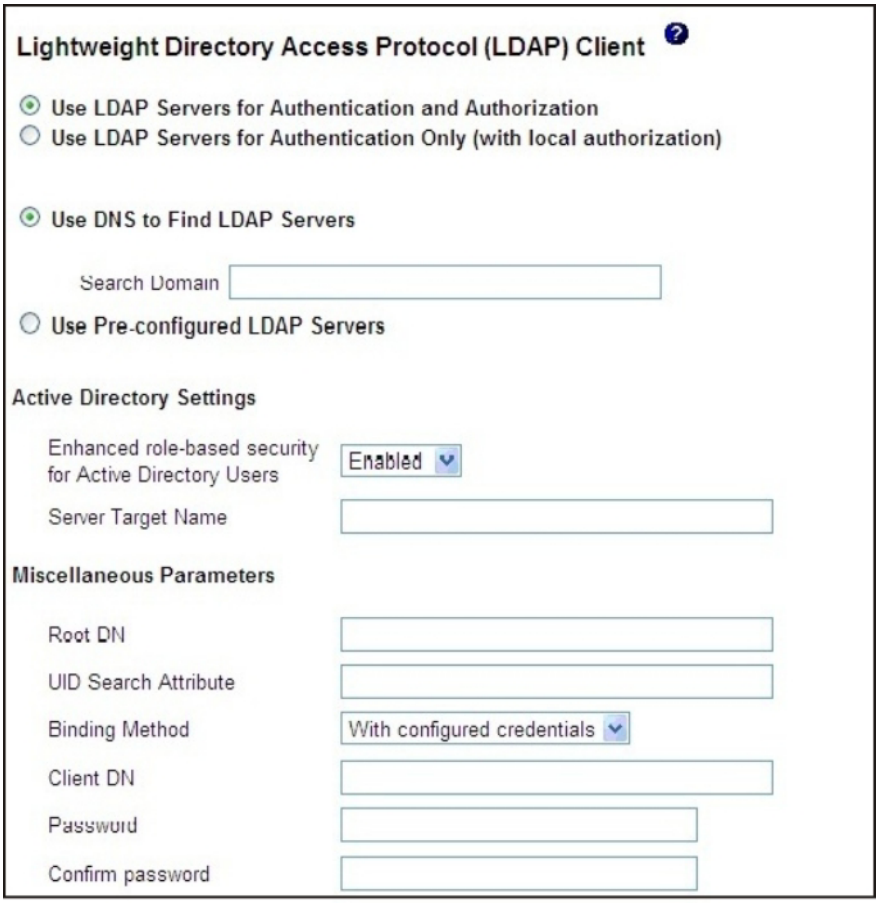
「加強角色型安全嵌入式管理單元」工具可讓您在 Active Directory 伺服器上配置角色，並將 IMM、使用者及群組與這些角色相關聯。如需相關資訊和指示，請參閱「加強角色型安全嵌入式管理單元」工具的文件。角色可識別指派給使用者和群組的權限，並可識別它所附加至的指令目標，例如 IMM 或刀鋒伺服器。在啓用 Active Directory 角色型鑑別和授權之前，應該在 Active Directory 伺服器上配置角色。

在 **Server Target Name** 欄位中配置的選用名稱可識別特定的 IMM，並可透過「角色型安全嵌入式管理單元」工具與 Active Directory 伺服器中的一個以上角色相關聯。透過建立受管理目標、提供目標特定名稱，以及將目標與適當的角色相關聯，即可達成此目的。如果已配置「伺服器目標名稱」，則此名稱可以定義使用者的特定角色，以及屬於相同角色成員的 IMM 目標。當使用者登入 IMM 並透過 Active Directory 進行鑑別時，將會從目錄中擷取此使用者的角色。指派給使用者的權限擷取自適當的角色，這些角色擁有作爲成員且名稱符合該 IMM 的目標，或擁有符合任何 IMM 的目標。您可以爲 IMM 提供唯一名稱，多個 IMM 亦可共用相同目標名稱。將多個 IMM 指派給相同目標名稱，並將其組合在一起，然後將其指派給相同角色。

若要爲 IMM 配置 Active Directory 角色型鑑別和授權，請完成下列步驟：

1. 在導覽窗格中，按一下 **Network Protocols**。
2. 向下捲動到 **Lightweight Directory Access Protocol (LDAP) Client** 區段。
3. 選取 **Use LDAP Servers for Authentication and Authorization**。
4. 爲 **Enhanced role-based security for Active Directory Users** 欄位選取 **Enabled**。
5. 選取下列其中一個選項以動態探索或手動配置網域控制站：
   - 選取 **Use DNS to find LDAP Servers** 以根據 DNS SVR 記錄來動態探索網域控制站。
   - 選取 **Use Pre-Configured LDAP Servers**（預設選項）以手動配置網域控制站。
6. 如果您是使用 DNS 動態探索網域控制站，請配置網域控制站的網域名稱；然後，繼續執行步驟 第 64 頁的 8。您必須指定網域控制站的完整網域名稱。在 **Search Domain** 欄位中輸入網域控制站的網域名稱。

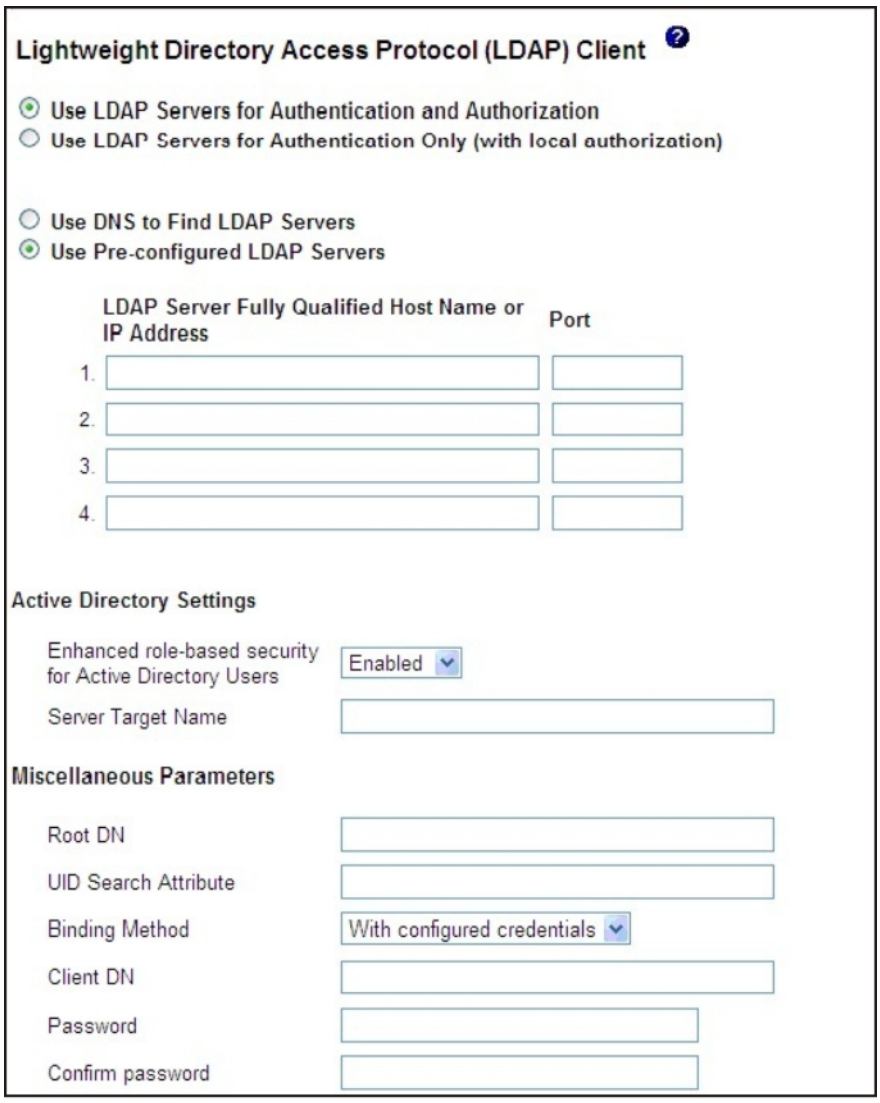
下列視窗顯示使用 DNS 動態探索網域控制站時的 LDAP 用戶端視窗。



7. 如果您是手動配置網域控制站，請配置 **LDAP Server Host Name or IP Address** 和 **Port** 欄位。

   註：使用一個 IP 位址或完整主機名稱最多可以配置四個網域控制站。

下圖顯示手動配置網域控制站時的 LDAP 用戶端視窗。



8. 從 **Enhanced role-based security for Active Directory Users** 功能表中選取 **Enabled**，以配置 Active Directory Settings。
9. 配置細項參數。如需參數的相關資訊，請參閱下表。

表 12. 細項參數

欄位	說明	選項
Root DN	IMM 使用 DN 格式的 **Root DN** 欄位作爲目錄樹的根項目。此 DN 將用作所有搜尋的基本物件。範例可能類似於 `dc=mycompany,dc=com`。	

表 12. 細項參數 (繼續)

欄位	說明	選項
Binding Method	**Binding Method** 欄位用於與網域控制站伺服器的起始連結，請選取一個選項。	• Anonymously： 不使用 DN 或密碼來與網域控制站伺服器進行起始連結。建議不要選取此選項，因爲大部分伺服器都配置爲禁止對特定使用者記錄的搜尋要求。 • With configured credentials： 輸入用於起始連結的用戶端 DN 和密碼。 • With login credentials： 使用在登入程序期間提供的認證與網域控制站伺服器進行起始連結。使用 DN、部分 DN、完整網域名稱，或透過符合在 IMM 中所配置 **UID Search Attribute** 欄位的使用者 ID，皆可提供使用者 ID。 如果認證類似於部分 DN（例如 `cn=joe`），在嘗試建立符合該使用者記錄的 DN 時，即會將此部分 DN 作爲已配置根 DN 的字首。如果此連結嘗試失敗，則會將字首 `cn=` 新增至登入認證，然後將此字串結果新增至已配置根 DN，以進行最終的連結嘗試。

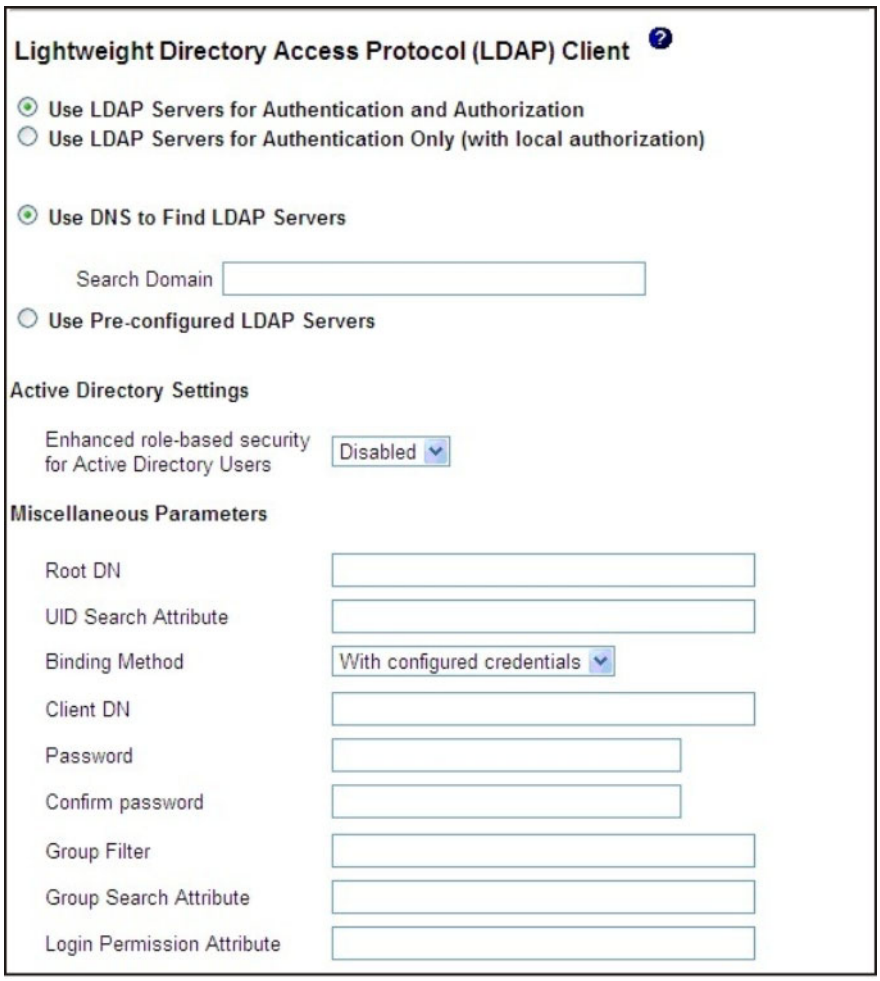
舊式 LDAP 鑑別和授權

舊式 LDAP 鑑別和授權是與 IMM 搭配使用的原始模型。舊式 LDAP 鑑別和授權支援 Active Directory、Novell eDirectory、OpenLDAP 環境，並且會根據 LDAP 伺服器中儲存的配置資訊，將權限與使用者相關聯。舊式 LDAP 鑑別和授權可用於透過 LDAP 伺服器，對使用者進行鑑別和授權。如果在 IMM 中停用 Enhanced Role-based Security for Active Directory Users，則容許您爲 IMM 配置 LDAP 搜尋屬性。

若要爲 IMM 配置舊式 LDAP 鑑別和授權，請完成下列步驟：

1. 在導覽窗格中，按一下 **Network Protocols**。
2. 向下捲動到 **Lightweight Directory Access Protocol (LDAP) Client** 區段。
3. 選取 **Use LDAP Servers for Authentication and Authorization**。
4. 爲 **Enhanced role-based security for Active Directory Users** 欄位選取 **Disabled**。
5. 選取下列其中一個選項以動態探索或手動配置用於鑑別的 LDAP 伺服器：
   - 選取 **Use DNS to find LDAP Servers** 以根據 DNS SVR 記錄來動態探索 LDAP 伺服器。
   - 選取 **Use Pre-Configured LDAP Servers**（預設選項）以手動配置 LDAP 伺服器。
6. 如果您是使用 DNS 動態探索 LDAP 伺服器，請配置 LDAP 伺服器的網域名稱；然後，繼續執行步驟 第 67 頁的 8。您必須指定 LDAP 伺服器的完整網域名稱。在 **Search Domain** 欄位中輸入 LDAP 伺服器的網域名稱

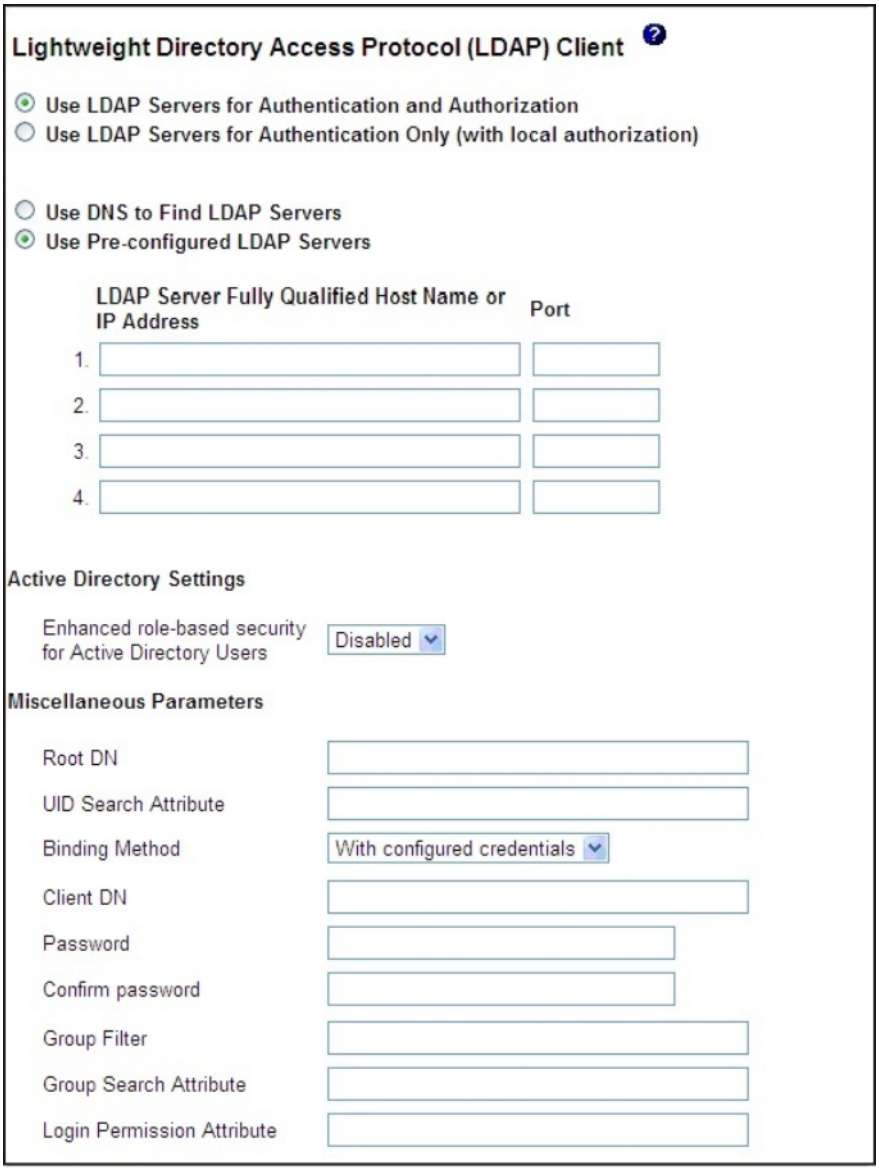
下列視窗顯示使用 DNS 動態探索 LDAP 伺服器時的 LDAP 用戶端視窗。



7. 如果您是手動配置 LDAP 伺服器，請配置 **LDAP Server Host Name or IP Address** 和 **Port** 欄位；然後，繼續執行步驟 第 67 頁的 8。

   註：使用一個 IP 位址或完整主機名稱最多可以配置四個 LDAP 伺服器。

下列視窗顯示手動配置 LDAP 伺服器時的 LDAP 用戶端視窗。



8. 從 **Enhanced role-based security for Active Directory Users** 功能表中選取 **Disabled**，以配置 Active Directory Settings。
9. 配置細項參數。如需必要參數欄位的說明，請參閱下列清單。
   - IMM 使用 DN 格式的 **Root DN** 欄位作爲目錄樹的根項目。此 DN 將用作所有搜尋的基本物件。範例可能類似於 `dc=mycompany,dc=com`。
   - **Binding Method** 欄位用於與網域控制站伺服器的起始連結，請使用下列其中一個連結選項：
     – Anonymously：

       不使用 DN 或密碼來與網域控制站伺服器進行起始連結。建議不要選取此選項，因爲大部分伺服器都配置爲禁止對特定使用者記錄的搜尋要求。

     – With configured credentials：

       輸入用於起始連結的用戶端 DN 和密碼。

– With login credentials：

使用在登入程序期間提供的認證進行連結。使用 DN、部分 DN、完整網域名稱，或透過符合在 IMM 中所配置 **UID Search Attribute** 欄位中之資訊的使用者 ID，皆可提供使用者 ID。如果認證類似於部分 DN（例如 cn=joe），在嘗試建立符合該使用者記錄的 DN 時，即會將此部分 DN 作爲已配置根 DN 的字首。如果此連結嘗試失敗，則會將字首 cn= 新增至登入認證，然後將此字串結果新增至已配置根 DN，以進行最終的連結嘗試。

- **Group Filter** 欄位用於群組鑑別。它可指定 IMM 所屬的群組。如果將群組過濾器保留空白，群組鑑別即會自動成功。如果已啓用群組鑑別，在進行使用者鑑別之後即會進行群組鑑別。系統會嘗試將 Group Filter 中的至少一個群組與使用者所屬的群組進行比對。如果沒有相符項，使用者鑑別即會失敗，且會拒絕使用者存取。如果有至少一個相符項，群組鑑別即會通過。比較會區分大小寫。

  停用群組鑑別時，使用者自己的記錄必須包含權限屬性；否則，將會拒絕存取。對於符合過濾器的每個群組，皆會將與該群組相關聯的權限指派給使用者。透過擷取 **Login Permission Attribute** 資訊，即可找到與群組相關聯的權限。

  過濾器限制爲 511 個字元，且由一個以上的群組名稱組成。必須使用冒號 (:) 字元來指定多個群組名稱。前導空格和尾端空格將會忽略，所有其他空格皆會視爲群組名稱的一部分。您可以將群組名稱指定爲完整 DN，或僅使用 *cn* 部分來指定群組名稱。例如，您可以使用實際 DN 或 adminGroup，來指定 DN 等於 cn=adminGroup,dc=mycompany,dc=com 的群組。

  註：先前使用的星號 (*) 符號不再視爲萬用字元符號。萬用字元概念由於安全原因而移除。

- 搜尋演算法會使用 **Group Search Attribute** 欄位，來搜尋特定使用者的群組成員資格資訊。如果已配置群組過濾器名稱，則必須從 LDAP 伺服器擷取使用者所屬的群組清單。需要此清單才能執行群組鑑別。若要擷取此清單，傳送至 LDAP 伺服器的搜尋過濾器必須指定與群組相關聯的屬性名稱。**Group Search Attribute** 欄位可指定屬性名稱。

  在 Active Directory 或 Novell eDirectory 環境中，**Group Search Attribute** 欄位可指定用於識別使用者所屬群組的屬性名稱。在 Active Directory 中使用的是 **memberOf** 屬性，在 Novell eDirectory 中使用的則是 **groupMembership** 屬性。在 OpenLDAP 伺服器環境中，通常會將使用者指派給 objectClass 爲 PosixGroup 的群組。在此環境定義中，Group Search Attribute 參數可指定用於識別特定 PosixGroup 成員的屬性名稱；此屬性名稱通常爲 **memberUid**。如果將 **Group Search Attribute** 欄位保留空白，過濾器中的屬性名稱將預設爲 **memberOf**。

- **Login Permission Attribute** 欄位可指定與使用者登入權限相關聯的屬性名稱。當使用者使用 LDAP 伺服器順利進行鑑別時，必須擷取該使用者的登入權限。

  註：此 **Login Permission Attribute** 欄位不得爲空白；否則，將無法擷取該使用者的權限。如果沒有已驗證的權限，登入嘗試將會失敗。

  使用關鍵字字串 IBMRBSPermissions=，可搜尋 LDAP 伺服器傳回的屬性值。此關鍵字後面必須緊接位元字串（最多 12 個連續的 0 或 1）。每個位元皆代表特定的功能集。這些位元將根據其位置進行編號。最左側的位元是位元位置 0，最右

側的位元是位元位置 11。特定位置的值 1 將啓用該特定功能。值 0 將停用該功能。字串 IBMRBSPermissions=010000000000 爲範例。

IBMRBSPermissions= 關鍵字可置於 **Login Permission Attribute** 欄位中的任何位置。這將容許 LDAP 管理者重複使用現有屬性；因此，可防止延伸 LDAP 綱目並容許將屬性用於其原始用途。使用者現在可以在此欄位的開頭、結尾或任何位置新增此關鍵字字串。所用的屬性將容許自由格式的字串。

下表提供每個位元位置的說明。

表 13. 權限位元

位元位置	功能	說明
0	一律拒絕	如果設定此位元，使用者將一律鑑別失敗。此功能可用於封鎖特定使用者或與特定群組相關聯的使用者。
1	Supervisor 存取權	如果設定此位元，則會將管理者專用權授與使用者。使用者具有對每個功能的讀寫權。如果您設定此位元，則無需個別地設定其他位元。
2	Read Only 存取權	如果設定此位元，使用者將具有唯讀存取權，且無法執行任何維護程序（例如重新啓動、遠端動作或韌體更新）。使用儲存、清除或還原功能將無法進行任何修改。位元位置 2 與所有其他位元互斥，且位元位置 2 具有最低的優先順序。如果設定任何其他位元，則會忽略此位元。
3	網路功能與安全性	如果設定此位元，使用者可以修改 Security、Network Protocols、Network Interface、Port Assignments 及 Serial Port 畫面中的配置。
4	使用者帳戶管理	如果設定此位元，使用者可以新增、修改或刪除使用者，以及變更 Login Profiles 畫面中的 Global Login Settings。
5	遠端主控台存取	如果設定此位元，使用者可以存取遠端伺服器主控台，以及修改 Serial Port 畫面中的配置。
6	遠端主控台及遠端磁碟存取	如果設定此位元，使用者可以存取遠端伺服器主控台，以及遠端伺服器的遠端磁碟功能。使用者也可以修改 Serial Port 畫面中的配置。
7	遠端伺服器電源/重新啓動存取	如果設定此位元，使用者可以存取遠端伺服器的開啓電源、重新啓動及伺服器逾時功能。
8	基本配接器配置	如果設定此位元，使用者可以修改 System Settings 和 Alerts 畫面中的配置參數（Contact、Location 及 Server Timeout 參數除外）。

表 13. 權限位元 (繼續)

位元位置	功能	說明
9	清除事件日誌的能力	如果設定此位元，使用者可以清除事件日誌。 **註**：所有使用者都可以檢視事件日誌；但是，使用者需要具有此層次的權限才能清除日誌。
10	進階配接器配置	如果設定此位元，使用者在配置配接卡時沒有任何限制，並且具有對 IMM 的管理存取權。使用者可以執行下列進階功能：韌體升級、PXE 網路開機、還原配接卡原廠預設值、從配置檔修改和還原配接卡配置，以及重新啓動/重設配接卡。這不包括 Server Power/Restart Control 和逾時功能。
11	保留	此位元位置保留給將來使用（目前會忽略）。

注意事項：

- 如果沒有使用任何位元，則會將使用者的預設值設定爲 Read Only。
- 直接從使用者記錄擷取的登入權限將享有優先順序。如果使用者記錄在 **Login Permission Attribute** 欄位中沒有包含名稱，則會嘗試從使用者所屬且符合群組過濾器的群組中擷取權限。在此情況下，將爲使用者指派所有群組的所有位元之內含 OR。
- 如果爲任何群組設定「一律拒絕」（位元位置 0）位元，將拒絕使用者存取。「一律拒絕」位元優先於所有其他位元。
- 如果使用者能夠修改基本、網路或安全相關的配接卡配置參數，您應該考量賦予使用者重新啓動 IMM 的能力（位元位置 10）。如果沒有此能力，使用者或許能夠變更參數；但是，此參數不會生效。

配置安全

您可以使用本節中的一般程序，爲機密資料加密、IMM Web 伺服器、IMM 與 IBM Systems Director 之間的連線、IMM 與 LDAP 伺服器之間的連線，以及加密法管理，配置安全保護。如果您不熟悉使用 SSL 憑證，請閱讀第 72 頁的『SSL 憑證』中的資訊。

若要爲 IMM 配置安全保護，請執行下列作業：

1. 配置機密資料加密：
   a. 在導覽窗格中，按一下 **Security**。捲動至 **Enable Data Encryption** 區段，並選取 **Enable** 以啓用資料加密。若要停用資料加密，請選取 **Disable**。
2. 配置安全 Web 伺服器：
   a. 在導覽窗格中，按一下 **Security**。捲動至 **HTTPS Server Configuration for Web Server** 區段，並選取 **Disable** 以停用 SSL 伺服器。
   b. 若要產生或匯入憑證，請在導覽窗格中按一下 **Security** 並捲動至 **HTTPS Server Certificate Management** 區段。如需管理憑證的相關資訊，請參閱第 73 頁的『SSL 伺服器憑證管理』。

c. 若要啓用 SSL 伺服器，請在導覽窗格中按一下 **Security** 並捲動至 **HTTPS Server Configuration for Web Server** 區段。如需啓用 SSL 的相關資訊，請參閱第 76 頁的『爲安全 Web 伺服器或 IBM Systems Director over HTTPS 啓用 SSL』。

3. 配置 IBM Systems Director 連線：
   a. 若要停用 **Systems Director over HTTPS** 設定，請在導覽窗格中按一下 **Security** 並捲動至 **IBM Systems Director over HTTPS Server Configuration** 區段。
   b. 若要產生或匯入憑證，請在導覽窗格中按一下 **Security** 並捲動至 **IBM Systems Director over HTTPS Server Certificate Management** 區段。如需相關資訊，請參閱第 73 頁的『SSL 伺服器憑證管理』。
   c. 若要啓用 SSL 伺服器，請在導覽窗格中按一下 **Security** 並捲動至 **IBM Systems Director over HTTPS Server Configuration** 區段。如需啓用 SSL 的相關資訊，請參閱第 76 頁的『爲安全 Web 伺服器或 IBM Systems Director over HTTPS 啓用 SSL』。
4. 配置 LDAP 連線的 SSL 安全保護：
   a. 若要停用 SSL 用戶端，請在導覽窗格中按一下 **Security** 並捲動至 **SSL Client Configuration for LDAP Client** 區段。
   b. 若要產生或匯入憑證，請在導覽窗格中按一下 **Security** 並捲動至 **SSL Client Certificate Management** 區段。如需相關資訊，請參閱第 73 頁的『SSL 伺服器憑證管理』。
   c. 若要匯入一個以上的信任憑證，請在導覽窗格中按一下 **Security** 並捲動至 **SSL Client Trusted Certificae Management** 區段。如需相關資訊，請參閱 SSL 用戶端信任憑證管理。
   d. 若要啓用 SSL 用戶端，請在導覽窗格中按一下 **Security** 並捲動至 **SSL Client Configuration for LDAP Client** 區段。如需相關資訊，請參閱第 76 頁的『爲安全 Web 伺服器或 IBM Systems Director over HTTPS 啓用 SSL』。
5. 配置加密法管理：
   a. 在導覽窗格中，按一下 **Security** 並捲動至 **Cryptography Management** 區段。選取 **Basic Compatible Mode**。
   b. 在導覽窗格中，按一下 **Security** 並捲動至 **Cryptography Management** 區段。選取 **High Security Mode**。
6. 重新啓動 IMM 讓 SSL 伺服器配置的變更生效。如需相關資訊，請參閱第 82 頁的『重新啓動 IMM』。

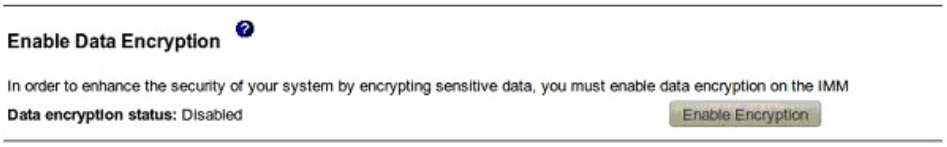
註：對資料加密及 SSL 用戶端配置的變更會立即生效，不需要重新啓動 IMM。

啓用資料加密

依預設，機密資料會在未加密的狀態下儲存，以和舊版保持相容。若要加強系統安全，您必須在 IMM 上啓用資料加密。

若要啓用資料加密，請完成下列程序：

1. 在導覽窗格中，按一下 **Security**。



2. 按一下 **Enable Encryption** 以啓用資料加密。

   註：

   - 如果您需要將 IMM 韌體 1.42 版降到不提供資料加密的舊版，必須在降級之前先停用資料加密。如果未在降級前停用資料加密，將會遺失帳戶資訊。
   - 如果您日後需要停用資料加密，請選取 **Disable Encryption** 停用資料加密。

保護 Web 伺服器、IBM Systems Director 及安全 LDAP 的安全

Secure Sockets Layer (SSL) 是一種提供通訊保密的安全通訊協定。SSL 可讓用戶端伺服器應用程式能以防止竊聽、竄改和僞造訊息的方式進行通訊。

您可以將 IMM 配置爲針對下列兩種連線類型使用 SSL 支援：安全伺服器 (HTTPS) 與安全 LDAP 連線 (LDAPS)。視連線類型之不同，IMM會充當 SSL 用戶端或 SSL 伺服器的角色。

下表顯示 IMM 在安全 Web 伺服器連線和安全 LDAP 連線中的角色。

表 14. IMM SSL 連線支援

連線類型	SSL 用戶端	SSL 伺服器
安全 Web 伺服器 (HTTPS)	Web 瀏覽器（例如：Microsoft Internet Explorer）	IMM Web 伺服器
安全的 IBM Systems Director 連線	IBM Systems Director	IMM Systems Director 伺服器
安全的 LDAP 連線 (LDAPS)	IMM LDAP 用戶端	LDAP 伺服器

您可以從 Security 頁面中檢視或變更 SSL 設定，包括啓用或停用 SSL，以及爲 SSL 管理所需的憑證。

SSL 憑證

您可以將 SSL 與自簽憑證或與協力廠商憑證管理中心簽章的憑證搭配使用。

自簽憑證是使用 SSL 最簡單的方法，但它會造成安全風險。當您使用自簽方法時，SSL 用戶端無法在第一次嘗試進行用戶端與伺服器連線時，驗證 SSL 伺服器的身分。第三方有可能假冒伺服器並截取在 IMM 與 Web 瀏覽器間流動的資料。如果自簽憑證在瀏覽器與 IMM 起始連線時匯入至瀏覽器的憑證儲存庫，則該瀏覽器所有之後的通訊將可安全進行（假設起始連線未受攻擊損害）。

如需更完整的安全，請使用憑證管理中心簽章的憑證。若要取得已簽章的憑證，請使用 SSL Certificate Management 頁面來產生憑證簽章要求。您必須將憑證簽章要求傳送至憑證管理中心，並進行必要步驟以取得憑證。收到憑證後，憑證會透過 **Import a Signed Certificate** 鏈結匯入 IMM，接著您便可以啓用 SSL。

憑證管理中心的功能是驗證 IMM 的身分。憑證包含憑證管理中心和 IMM 的數位簽章。如果知名的憑證管理中心發出憑證，或憑證管理中心的憑證已匯入 Web 伺服器，則瀏覽器可以驗證憑證，並明確識別 IMM Web 伺服器。

IMM 需要安全 Web 伺服器的憑證和安全 LDAP 用戶端的憑證。此外，安全 LDAP 用戶端也需要一個以上信任憑證。安全 LDAP 用戶端使用信任憑證，來明確識別 LDAP 伺服器。信任憑證是簽署 LDAP 伺服器憑證的憑證管理中心的憑證。如果 LDAP 伺服器使用自簽憑證，則信任憑證可以是 LDAP 伺服器本身的憑證。如果在配置中使用了多個 LDAP 伺服器，則必須匯入其他信任憑證。

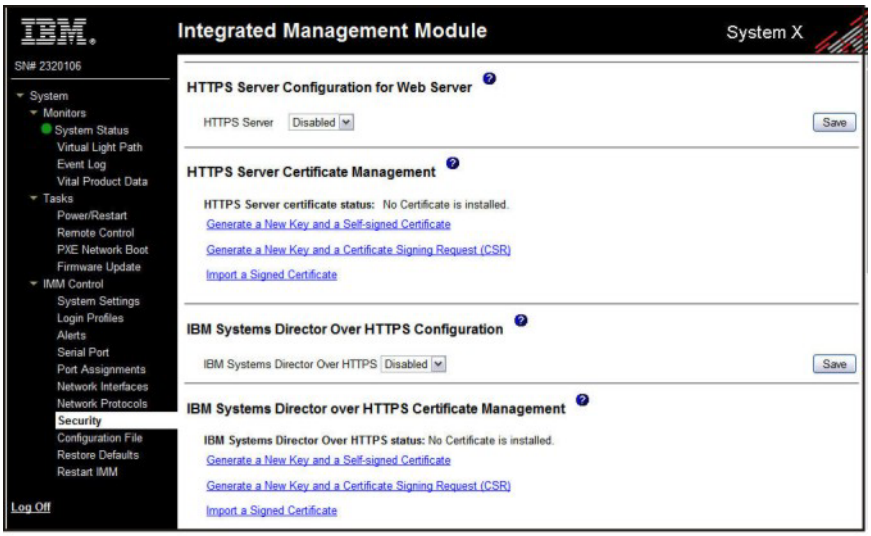
SSL 伺服器憑證管理

在啓用 SSL 之前，SSL 伺服器需要安裝有效的憑證和對應的私密加密金鑰。下列兩種方法可用於產生私密金鑰和必要憑證：使用自簽憑證，和使用憑證管理中心簽章的憑證。如果您要爲 SSL 伺服器使用自簽憑證，請參閱『產生自簽憑證』以取得相關資訊。如需爲 SSL 伺服器使用憑證管理中心簽章之憑證的相關資訊，請參閱第 74 頁的『產生憑證簽章要求』。

產生自簽憑證

若要產生新私密加密金鑰和自簽憑證，請完成下列步驟：

1. 按一下位於導覽窗格中的 **Security**，隨即會顯示以下頁面。

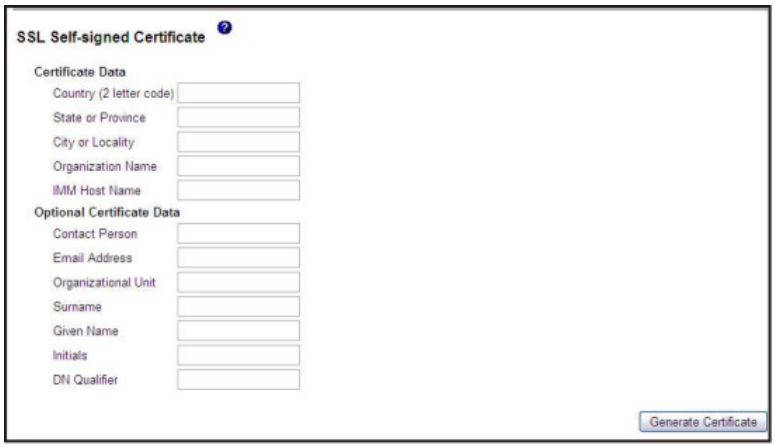


2. 在 **SSL Server Configuration for Web Server** 區域或 **IBM Systems Director Over HTTPS Configuration** 區域中，確定設定爲 **Disabled**。如果尚未停用，請選取 **Disabled**，然後按一下 **Save**。

   註：

   a. 必須重新啓動 IMM，選取的值（**Enabled** 或 **Disabled**）才會生效。
   b. 有效的 SSL 憑證必須到位才能啓用 SSL。
   c. 若要使用 SSL，您必須將用戶端 Web 瀏覽器配置爲使用 SSL3 或 TLS。不能使用僅具有 SSL2 支援的舊版出口級瀏覽器。

3. 在 **SSL Server Certificate Management** 區域中，選取 **Generate a New Key and a Self-signed Certificate**。畫面上會顯示類似下圖的頁面。

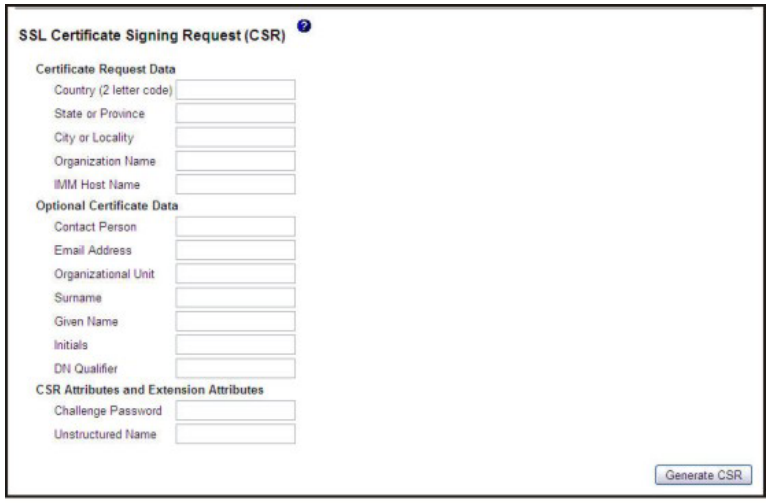


4. 在必要欄位和適用於配置的任何選用欄位中鍵入資訊。如需欄位的說明，請參閱「必要憑證資料」。74. 輸入完資訊之後，請按一下 **Generate Certificate**。即會產生新的加密金鑰和憑證。此程序可能需要幾分鐘的時間。您會看到自簽憑證是否已安裝的確認訊息。

產生憑證簽章要求

若要產生新的私密加密金鑰和憑證簽章要求，請完成下列步驟：

1. 在導覽窗格中，按一下 **Security**。
2. 在 **SSL Server Configuration for Web Server** 區域中，確定已停用 SSL 伺服器。如果尚未停用，請於 **SSL Server** 欄位中選取 **Disabled**，然後按一下 **Save**。
3. 在 **SSL Server Certificate Management** 區域中，選取 **Generate a New Key and a Certificate-Signing Request**。畫面上會顯示類似下圖的頁面。



4. 在必要欄位和適用於配置的任何選用欄位中鍵入資訊。這些欄位與用於自簽憑證的欄位相同，同時還具有一些額外的欄位。

   如需每個一般欄位的說明，請閱讀下節中的資訊。

Required certificate data 下列使用者輸入欄位，是用於產生自簽憑證或憑證簽章要求的必要欄位：

Country

使用此欄位可指出 IMM 實際所在的國家/地區。此欄位必須包含 2 個字元的國碼。

State or Province

使用此欄位可指出 IMM 實際所在的州/省（縣/市）。此欄位最多可以包含 30 個字元。

City or Locality

使用此欄位可指出 IMM 實際所在的城市或地區。此欄位最多可以包含 50 個字元。

Organization Name

使用此欄位可指出擁有 IMM 的公司或組織。使用此欄位產生憑證簽章要求時，發出憑證管理中心可以驗證要求憑證的組織，在法律上是否有資格要求給定公司或組織名稱的所有權。此欄位最多可以包含 60 個字元。

IMM Host Name

使用此欄位可指出目前出現在瀏覽器網址列中的 IMM 主機名稱。

請確定您在此欄位中鍵入的值，與 Web 瀏覽器所識別的主機名稱完全相符。瀏覽器會將已解析網址中的主機名稱，與憑證中出現的名稱進行比較。爲了防止瀏覽器發出憑證警告，在此欄位中使用的值，必須符合瀏覽器用於連接至 IMM 的主機名稱。例如，如果網址列中的位址是 http://mm11.xyz.com/private/main.ssi，則用於 IMM Host Name 欄位的值必須是 mm11.xyz.com。如果網址是 http://mm11/private/main.ssi，則使用的值必須是 mm11。如果網址是 http://192.168.70.2/private/main.ssi，則使用的值必須是 192.168.70.2。

此憑證屬性通常稱爲通用名稱。

此欄位最多可以包含 60 個字元。

Contact Person

使用此欄位可指出負責 IMM 的聯絡人名稱。此欄位最多可以包含 60 個字元。

Email Address

使用此欄位可指出負責 IMM 的聯絡人電子郵件位址。此欄位最多可以包含 60 個字元。

Optional certificate data 下列使用者輸入欄位，是用於產生自簽憑證或憑證簽章要求的選用欄位：

Organizational Unit

使用此欄位可指出擁有 IMM 的公司或組織內的單位。此欄位最多可以包含 60 個字元。

Surname

使用此欄位可指出其他資訊，例如負責 IMM 的人員暱稱。此欄位最多可以包含 60 個字元。

Given Name

使用此欄位可指出其他資訊，例如負責 IMM 的人員名字。此欄位最多可以包含 60 個字元。

Initials

使用此欄位可指出其他資訊，例如負責 IMM 的人員名字縮寫。此欄位最多可以包含 20 個字元。

DN Qualifier

使用此欄位可指出其他資訊，例如 IMM 的識別名稱限定元。此欄位最多可以包含 60 個字元。

Certificate-Signing request attributes 除非您選取的憑證管理中心需要，否則下列欄位爲選用欄位：

Challenge Password

使用此欄位可將密碼指派給憑證簽章要求。此欄位最多可以包含 30 個字元。

Unstructured Name

使用此欄位可指出其他資訊，例如指派給 IMM 的非結構化名稱。此欄位最多可以包含 60 個字元。

5. 鍵入完資訊之後，按一下 **Generate CSR**。即會產生新的加密金鑰和憑證。此程序可能需要幾分鐘的時間。
6. 按一下 **Download CSR**，然後按一下 **Save** 以將檔案儲存至工作站。建立憑證簽章要求時產生的檔案爲 DER 格式。如果憑證管理中心預期的資料爲其他格式（如 PEM），您可以使用 OpenSSL (http://www.openssl.org) 等工具來轉換該檔案。如果憑證管理中心要求您將憑證簽章要求檔案的內容複製到 Web 瀏覽器視窗，則通常預期的是 PEM 格式。

   使用 OpenSSL 將憑證簽章要求從 DER 轉換成 PEM 格式的指令類似於下列範例：

   ```
   openssl req -in csr.der -inform DER -out csr.pem -outform PEM
   ```

7. 將憑證簽章要求傳送至憑證管理中心。在憑證管理中心傳回已簽章的憑證時，您可能要將該憑證轉換成 DER 格式。（如果您是以電子郵件或網頁中的文字形式收到該憑證，則它可能是 PEM 格式。）您可以使用憑證管理中心提供的工具，或使用 OpenSSL (http://www.openssl.org) 等工具來變更格式。將憑證從 PEM 轉換成 DER 格式的指令類似於下列範例：

   ```
   openssl x509 -in cert.pem -inform PEM -out cert.der -outform DER
   ```

   在憑證管理中心傳回已簽章的憑證之後，請移至步驟 8。
8. 在導覽窗格中，按一下 **Security**。捲動到 **SSL Server Certificate Management** 區域或 **IBM Systems Director Over HTTPS Certificate Management** 區域。
9. 按一下 **Import a Signed Certificate**。
10. 按一下 **Browse**。
11. 按一下要匯入的憑證檔，然後按一下 **Open**。 **Browse** 按鈕旁邊的欄位中會顯示檔名（包括完整路徑）。
12. 按一下 **Import Server Certificate** 以開始此程序。將檔案傳送至 IMM 上的儲存體時，畫面上會顯示進度指示器。繼續顯示此頁面，直到傳送完成爲止。

為安全 Web 伺服器或 IBM Systems Director over HTTPS 啓用 SSL

請完成下列步驟，以啓用安全 Web 伺服器。

註：若要啓用 SSL，必須安裝有效的 SSL 憑證。

1. 在導覽窗格中，按一下 **Security**。顯示的頁面會顯示安裝的有效 SSL 伺服器憑證。如果 SSL 伺服器憑證狀態未顯示安裝的有效 SSL 憑證，則請移至第 73 頁的『SSL 伺服器憑證管理』。
2. 捲動到 **SSL Server Configuration for web Server** 區域或 **IBM Systems Director Over HTTPS Configuration** 區域，於 **SSL Client** 欄位中選取 **Enabled**，然後按一下 **Save**。選取的值會在 IMM 下次重新啓動時生效。

SSL 用戶端憑證管理

在啓用 SSL 之前，SSL 用戶端需要安裝有效的憑證和對應的私密加密金鑰。下列兩種方法可用於產生私密金鑰和必要憑證：使用自簽憑證，或使用憑證管理中心簽章的憑證。

爲 SSL 用戶端與爲 SSL 伺服器產生私密加密金鑰和憑證的程序是相同的，除您使用 Security 網頁的 **SSL Client Certificate Management** 區域而不是 **SSL Server Certificate Management** 區域之外。如果您要針對 SSL 用戶端使用自簽憑證，請參閱第 73 頁的『產生自簽憑證』。如果您要爲 SSL 用戶端使用憑證管理中心所簽章的憑證，請參閱第 74 頁的『產生憑證簽章要求』以取得相關資訊。

SSL 用戶端信任憑證管理

安全 SSL 用戶端（LDAP 用戶端）使用信任憑證來明確識別 LDAP 伺服器。信任憑證可以是簽署 LDAP 伺服器憑證的憑證管理中心的憑證，也可以是 LDAP 伺服器的實際憑證。在啓用 SSL 用戶端之前，必須至少將一個憑證匯入 IMM。您最多可以匯入三個信任憑證。

若要匯入信任憑證，請完成下列步驟：

1. 在導覽窗格中，選取 **Security**。
2. 在 **SSL Client Configuration for LDAP Client** 區域中，確定已停用 SSL 用戶端。如果尚未停用，請於 **SSL Client** 欄位中選取 **Disabled**，然後按一下 **Save**。
3. 捲動到 **SSL Client Trusted Certificate Management** 區域。
4. 按一下其中一個 **Trusted CA Certificate 1** 欄位旁邊的 **Import**。
5. 按一下 **Browse**。
6. 選取您想要的憑證檔，然後按一下 **Open**。 **Browse** 按鈕旁邊的方框中會顯示檔名（包括完整路徑）。
7. 若要開始匯入程序，請按一下 **Import Certificate**。將檔案傳送至 IMM 上的儲存體時，畫面上會顯示進度指示器。繼續顯示此頁面，直到傳送完成爲止。

   Remove 按鈕現在即可供 Trusted CA Certificate 1 選項使用。如果您想要移除信任憑證，請按一下對應的 **Remove** 按鈕。

   您可以使用 Trusted CA Certificate 2 和 Trusted CA Certificate 3 的 **Import** 按鈕，匯入其他信任憑證。

為 LDAP 用戶端啓用 SSL

使用 Security 頁面上的 **SSL Client Configuration for LDAP Client** 區域，可爲 LDAP 用戶端啓用或停用 SSL。若要啓用 SSL，必須先安裝有效的 SSL 用戶端憑證和至少一個信任憑證。

若要爲客戶端啓用 SSL，請完成下列步驟：

1. 在導覽窗格中，按一下 **Security**。

   Security 頁面會顯示已安裝的 SSL 用戶端憑證和 Trusted CA Certificate 1。

2. 在 SSL Client Configuration for LDAP Client 頁面上，於 **SSL Client** 欄位中選取 **Enabled**。

   註：

   a. 選取的值（Enabled 或 Disabled）會立即生效。

   b. 有效的 SSL 憑證必須到位才能啓用 SSL。

   c. 您的 LDAP 伺服器必須支援要與 LDAP 用戶端所使用 SSL 實作相容的 SSL3 或 TLS。

3. 按一下 **Save**。選取的值會立即生效。

加密法管理

使用 Security 頁面上的 **Cryptography Management** 區域，可爲 IMM 中的 SSL 伺服器配置密碼組合的強度，包括 HTTPS 伺服器及 IBM System Director over HTTPS。

加密法管理模式具有不同的安全強度。預設模式爲「基本相容」模式，且與舊版韌體、瀏覽器，以及其他沒有實作更嚴密之安全保護需求的網路用戶端相容。「高安全性」模式會限制 IMM 使用長度不得小於 128 個位元的 SSL 對稱金鑰。

若要配置模式，請完成下列步驟：

1. 在導覽窗格中，按一下 **Security**。
2. 找到 **Cryptography Management** 區域，並選取 **Basic Compatible Mode** 或 **High Security Mode**。
3. 按一下 **Save**，選取的模式會在 IMM 重新啓動之後生效。

配置 Secure Shell 伺服器

Secure Shell (SSH) 特性可讓您安全地存取 IMM 的指令行介面和序列（文字主控台）重新導向特性。

透過交換使用者 ID 和密碼來鑑別 Secure Shell 使用者。在建立加密通道之後，傳送密碼和使用者 ID。使用者 ID 和密碼配對可以是 12 個本端儲存的使用者 ID 和密碼之一，它們也可以儲存在 LDAP 伺服器上。不支援公開金鑰鑑別。

產生 Secure Shell 伺服器金鑰

Secure Shell 伺服器金鑰用於向用戶端鑑別 Secure Shell 伺服器的身分。建立新 Secure Shell 私密金鑰之前，必須先停用 Secure Shell。啓用 Secure Shell 伺服器之前，必須先建立伺服器金鑰。

當您要求新伺服器金鑰時，會同時建立 Rivest, Shamir, and Adelman 金鑰和 DSA 金鑰，以容許從 SSH 第 2 版用戶端存取 IMM。爲安全起見，在配置儲存和還原作業期間不會備份 Secure Shell 伺服器私密金鑰。

若要建立新 Secure Shell 伺服器金鑰，請完成下列步驟：

1. 在導覽窗格中，按一下 **Security**。

2. 捲動到 **Secure Shell (SSH) Server** 區域，確定 Secure Shell 伺服器已停用。如果尚未停用，請於 **SSH Server** 欄位中選取 **Disabled**，然後按一下 **Save**。
3. 捲動到 **SSH Server Key Management** 區域。
4. 按一下 **Generate SSH Server Private Key**。此時會開啓進度視窗。等待作業完成。

啓用 Secure Shell 伺服器

在 Security 頁面中，您可以啓用或停用 Secure Shell 伺服器。所做的選取只能在重新啓動 IMM 後生效。畫面上顯示的值（Enabled 或 Disabled)）不僅是最後選取的值，同時也是 IMM 重新啓動後使用的值。

註：僅當已安裝有效的 Secure Shell 伺服器私密金鑰時，您才能啓用 Secure Shell 伺服器。

若要啓用 Secure Shell 伺服器，請完成下列步驟：

1. 在導覽窗格中，按一下 **Security**。
2. 捲動到 **Secure Shell (SSH) Server** 區域。
3. 在 **SSH Server** 欄位中按一下 **Enabled**。
4. 在導覽窗格中，按一下 **Restart IMM** 以重新啓動 IMM。

使用 Secure Shell 伺服器

如果您要使用 Red Hat Linux 7.3 版隨附的 Secure Shell 用戶端，將 Secure Shell 階段作業啓動至網址爲 192.168.70.132 的 IMM，請鍵入類似下列範例的指令：

```
ssh -x -l userid 192.168.70.132
```

其中，-x 指示無 X Window 系統轉遞，-l 指示階段作業應使用使用者 ID *userid*。

還原和修改 IMM 配置

您可以完整還原儲存的配置，也可以先修改儲存的配置中的索引鍵欄位，然後再將配置還原到您的 IMM。透過在還原配置檔之前先對其進行修改，您可以使用類似配置設定多個 IMM。您可以快速指定需要唯一值（例如名稱和 IP 位址）的參數，而不必輸入一般且共用的資訊。

若要還原或修改現行配置，請完成下列步驟：

1. 登入您要在其中還原配置的 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **Configuration File**。
3. 在 **Restore IMM Configuration** 區域中，按一下 **Browse**。
4. 按一下想要的配置檔，然後按一下 **Open**。 **Browse** 旁邊的方框中會出現該檔案（包括完整路徑）。
5. 如果您不想對配置檔進行變更，請按一下 **Restore**。即會開啓顯示 IMM 配置資訊的新視窗。確定這就是您要還原的配置。如果不是正確配置，則請按一下 **Cancel**。

   如果您想要在還原配置前對配置檔進行變更，請按一下 **Modify and Restore** 以開啓可編輯的配置摘要視窗。最初僅顯示容許變更的欄位。若要在此視圖和完整

配置摘要視圖之間進行變更，請按一下視窗頂端或底端的 **Toggle View** 按鈕。若要修改欄位的內容，請按一下對應文字框並輸入資料。

註：當您按一下 **Restore** 或 **Modify and Restore** 時，如果發生以下情況則可能會開啓警示視窗：您嘗試要還原的配置檔是使用其他類型的服務處理器建立的，或者建立該配置檔使用的服務處理器類型相同但韌體版本較舊（進而導致功能較少）。此警示訊息包含完成還原後必須配置的系統管理功能清單。部分功能需要在多個視窗上進行配置。

6. 若要繼續將此檔案還原到 IMM，請按一下 **Restore Configuration**。更新 IMM 上的韌體時，畫面上會顯示進度指示器。會開啓確認視窗以確認更新是否成功。

   註：還原作業不會還原 Security 頁面上的安全設定。若要修改安全設定，請參閱第 72 頁的『保護 Web 伺服器、IBM Systems Director 及安全 LDAP 的安全』。

7. 收到還原程序完成的確認後，請在導覽窗格中按一下 **Restart IMM**；然後按一下 **Restart**。
8. 按一下 **OK** 以確認您想要重新啓動 IMM。
9. 按一下 **OK** 以關閉現行瀏覽器視窗。
10. 若要再次登入 IMM，請啓動瀏覽器，並遵循一般登入程序進行。

使用配置檔

選取導覽窗格中的 **Configuration File** 可備份和還原 IMM 配置。

重要事項：備份作業不會儲存 Security 頁面設定，並且無法透過還原作業來還原這些設定。

備份現行配置

您可以下載現行 IMM 配置的副本至正在執行 IMM Web 介面的用戶端電腦。如果您的 IMM 配置意外變更或損壞，使用此備份副本可還原您的 IMM 配置。使用它作爲您可以修改的基礎，以使用類似的配置來配置多個 IMM。

根據此程序儲存的配置資訊不包括 System x® 伺服器韌體配置設定，或與非 IMPI 使用者介面不共用的任何 IPMI 設定。

若要備份現行配置，請完成下列步驟：

1. 登入您要備份現行配置的 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **Configuration File**。
3. 在 **Backup IMM Configuration** 區域中，按一下 **view the current configuration summary**。
4. 驗證設定，然後按一下 **Close**。
5. 若要備份此配置，請按一下 **Backup**。
6. 鍵入備份的名稱，選取將儲存檔案的位置，然後按一下 **Save**。

   在 Mozilla Firefox 中，按一下 **Save File**，然後按一下 **OK**。

   在 Microsoft Internet Explorer 中，按一下 **Save this file to disk**，然後按一下 **OK**。

還原和修改 IMM 配置

您可以完整還原儲存的配置，也可以先修改儲存的配置中的索引鍵欄位，然後再將配置還原到您的 IMM。透過在還原配置檔之前先對其進行修改，您可以使用類似配置設定多個 IMM。您可以快速指定需要唯一值（例如名稱和 IP 位址）的參數，而不必輸入一般且共用的資訊。

若要還原或修改現行配置，請完成下列步驟：

1. 登入您要在其中還原配置的 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **Configuration File**。
3. 在 **Restore IMM Configuration** 區域中，按一下 **Browse**。
4. 按一下想要的配置檔，然後按一下 **Open**。 **Browse** 旁邊的方框中會出現該檔案（包括完整路徑）。
5. 如果您不想對配置檔進行變更，請按一下 **Restore**。即會開啓顯示 IMM 配置資訊的新視窗。確定這就是您要還原的配置。如果不是正確配置，則請按一下 **Cancel**。

   如果您想要在還原配置前對配置檔進行變更，請按一下 **Modify and Restore** 以開啓可編輯的配置摘要視窗。最初僅顯示容許變更的欄位。若要在此視圖和完整配置摘要視圖之間進行變更，請按一下視窗頂端或底端的 **Toggle View** 按鈕。若要修改欄位的內容，請按一下對應文字框並輸入資料。

   註：當您按一下 **Restore** 或 **Modify and Restore** 時，如果發生以下情況則可能會開啓警示視窗：您嘗試要還原的配置檔是使用其他類型的服務處理器建立的，或者建立該配置檔使用的服務處理器類型相同但韌體版本較舊（進而導致功能較少）。此警示訊息包含完成還原後必須配置的系統管理功能清單。部分功能需要在多個視窗上進行配置。
6. 若要繼續將此檔案還原到 IMM，請按一下 **Restore Configuration**。更新 IMM 上的韌體時，畫面上會顯示進度指示器。會開啓確認視窗以確認更新是否成功。

   註：還原作業不會還原 Security 頁面上的安全設定。若要修改安全設定，請參閱第 72 頁的『保護 Web 伺服器、IBM Systems Director 及安全 LDAP 的安全』。
7. 收到還原程序完成的確認後，請在導覽窗格中按一下 **Restart IMM**；然後按一下 **Restart**。
8. 按一下 **OK** 以確認您想要重新啓動 IMM。
9. 按一下 **OK** 以關閉現行瀏覽器視窗。
10. 若要再次登入 IMM，請啓動瀏覽器，並遵循一般登入程序進行。

還原預設值

如果您具有 Supervisor 存取權，則可使用 **Restore Defaults** 鏈結還原 IMM 的預設配置。

警告： 當您按一下 **Restore Defaults** 時，您將會遺失對 IMM 所做的所有修改。

若要還原 IMM 預設值，請完成下列步驟：

1. 登入 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **Restore Defaults** 以還原 IMM 的預設值。如果這是本端伺服器，則 TCP/IP 連線會中斷，您必須重新配置網路介面才能恢復連線功能。
3. 再次登入以使用 IMM Web 介面。
4. 重新配置網路介面，以恢復連線功能。如需網路介面的相關資訊，請參閱第 33 頁的『配置網路介面』。

重新啓動 IMM

使用 **Restart IMM** 鏈結可重新啓動 IMM。僅當您具有 Supervisor 存取權時才能執行此功能。任何乙太網路連線都會暫時中斷。您必須再次登入才能使用 IMM Web 介面。

若要重新啓動 IMM，請完成下列步驟：

1. 登入 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **Restart IMM** 以重新啓動 IMM。您的 TCP/IP 或數據機連線會中斷。
3. 再次登入以使用 IMM Web 介面。

可調式分割區

IMM 可讓您在可調式複合體中配置和控制系統。

IMM 可讓您在可調式複合體中配置和控制系統。如果伺服器發生錯誤，IMM 會將事件碼傳回至事件日誌（請參閱第 91 頁的『檢視事件日誌』）。

1. 登入您要還原配置的 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **Scalable Partitioning**，然後按一下 **Manage Partitions**。

Service Advisor 特性

Service Advisor 特性可偵測及收集系統硬體錯誤事件，並自動將資料轉遞給「IBM 支援中心」以進行問題判斷。Service Advisor 特性還可以收集系統錯誤相關資訊，並將該資料轉遞給「IBM 支援中心」。請參閱您伺服器的文件，以了解伺服器是否支援此特性。下列主題中包含設定、測試及維護 Service Advisor 的相關指示。

- 配置 Service Advisor
- 使用 Service Advisor

配置 Service Advisor

若要配置 Service Advisor，請完成下列步驟。

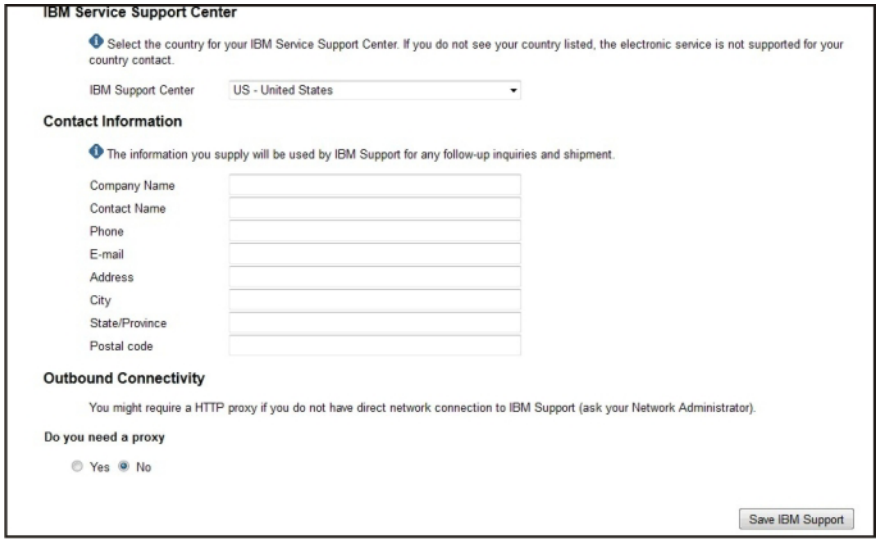
1. 登入您要在其中啓動 Service Advisor 的 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **Service Advisor**。
3. 如果這是您第一次使用此選項或 IMM 重設爲預設值，您必須閱讀並接受授權合約。

a. 按一下 **View Terms and Conditions** 以檢視 Service Advisor 合約。

b. 按一下 Terms and Conditions 頁面上的 **I accept the agreement**，以啓動 Service Advisor。

4. 按一下 **Service Advisor Settings** 標籤。

畫面上會顯示類似下圖的頁面。



5. 輸入伺服器管理者的聯絡資訊。如需 **Contact Information** 欄位的說明，請參閱下表。

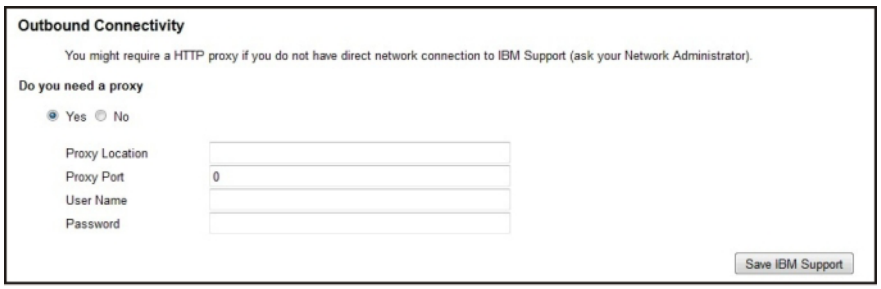
表 15. 聯絡資訊

欄位	說明
IBM Service Support Center	在此欄位中指定「IBM 服務支援中心」的國碼。這是一個雙字元 ISO 國碼，且僅適用於具有「IBM 服務支援中心」存取權的情況。
Company Name	在此欄位中指定聯絡人的組織或公司名稱。此欄位可以包含 1 到 30 個字元。
Contact Name	在此欄位中指定聯絡人的組織或公司名稱。此欄位可以包含 1 到 30 個字元。
Phone	在此欄位中指定聯絡人的電話號碼。此欄位可以包含 5 到 30 個字元。
Email	在此欄位中指定聯絡人的電子郵件位址。此欄位長度上限爲 30 個字元。
Address	在此欄位中指定 IMM 實際所在的地址。此欄位可以包含 1 到 30 個字元。
City	在此欄位中指定 IMM 實際所在的城市或地區。
State/Province	在此欄位中指定 IMM 實際所在的州/省（縣/市）。此欄位可以包含 2 到 3 個字元。
Postal Code	在此欄位中指定此伺服器所在位置的郵遞區號。此欄位可以包含 1 到 9 個字元（僅英數字元有效）。

6. 如果 IMM 沒有與「IBM 支援中心」的直接網路連線，請建立 HTTP Proxy。請完成下列步驟，以配置出埠連線功能資訊。

a. 在 **Do you need a proxy** 欄位中，按一下 **Yes**。請參閱上一張圖。

畫面上會顯示類似下圖的頁面。

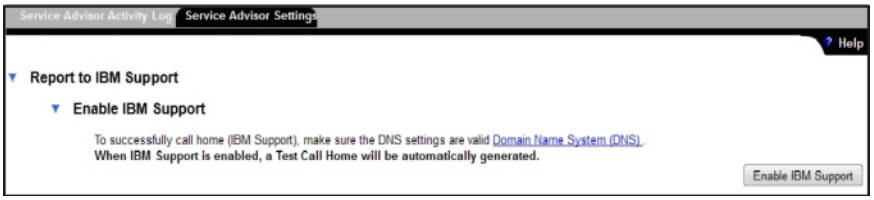


b. 輸入 **Proxy Location**、**Proxy Port**、**User Name** 及 **Password**。

7. 按一下 **Save IBM Support** 以儲存您的變更。
8. 按一下 **Enable IBM Support**（位置靠近頁面頂端），以在產生可服務的事件碼後，Service Advisor 能夠聯絡「IBM 支援中心」。

   註：啓用「IBM 支援中心」後，便會向「IBM 支援中心」網站傳送測試碼。
9. 按一下 **Service Advisor Activity Log** 標籤，以檢視測試碼的狀態。

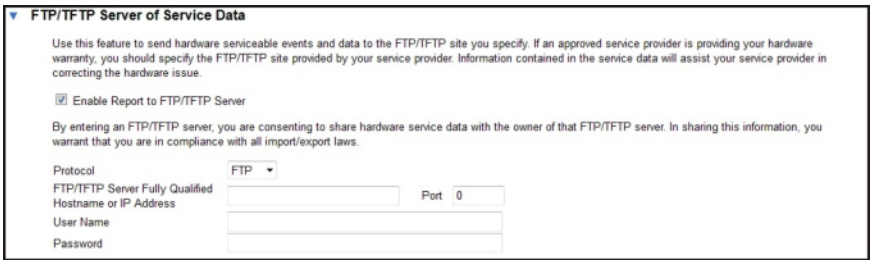
   畫面上會顯示類似下圖的頁面。



10. 如果您想要容許其他服務提供者接收事件碼，然後再聯絡「IBM 支援中心」，則請按一下 **Enable Report to FTP/TFTP Server**。

    注意：輸入 FTP/TFTP 伺服器，即表示您同意與該 FTP/TFTP 伺服器的擁有者共用硬體服務資料。共用此資訊時，您須保證服從所有進口/出口法規。

    畫面上會顯示類似下圖的頁面。



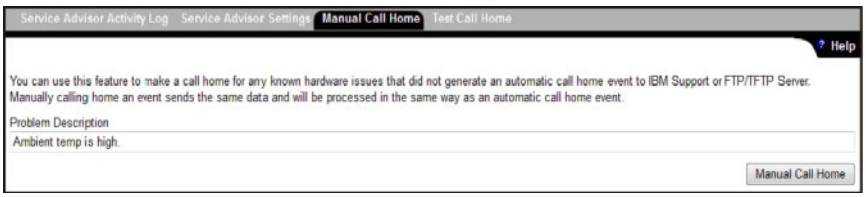
使用 Service Advisor

設定 Service Advisor 之後，您可以檢視活動日誌或產生測試訊息。

請完成下列步驟，以爲您的伺服器建立硬體問題報告：

1. 登入您要在其中使用 Service Advisor 的 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **Service Advisor**。
3. 按一下 **Manual Call Home** 標籤。

畫面上會顯示類似下圖的頁面。

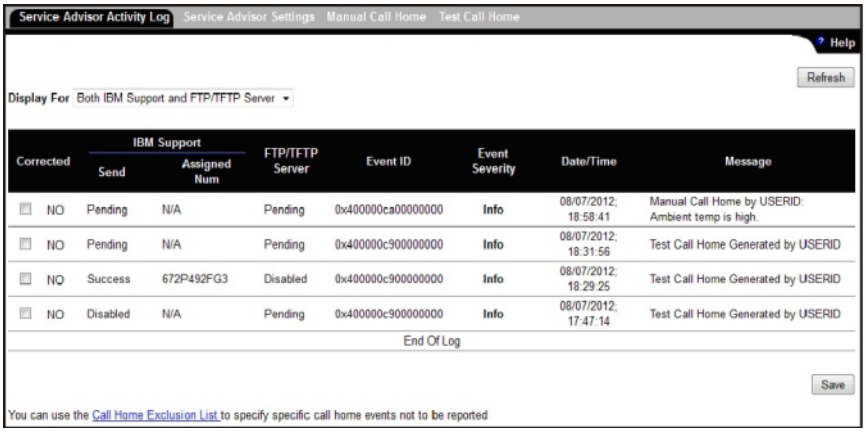


4. 完成下列步驟，以手動 Call Home 事件。
   a. 在 **Problem Description** 欄位中輸入問題說明。
   b. 按一下 **Manual Call Home** 按鈕。
5. 若要產生測試訊息，請按一下 **Test Call Home** 標籤；然後選取 **Test Call Home** 按鈕。

   注意事項：

   - Test Call Home 功能表會使用現行設定，來驗證 IMM 和 IBM 或 FTP/TFTP 之間的通訊路徑。（Test Call Home?）
   - 如果測試失敗，則會驗證網路設定。
   - 若要報告至「IBM 支援中心」，Service Advisor 需要 IMM 上正確設定 DNS 伺服器位址。
   - 如果呼叫成功，則會指派 Assigned Service Number 或問題單號碼。在「IBM 支援中心」上開啓的問題單將被識別爲測試問題單。「IBM 支援中心」不需要對測試問題單執行任何動作，並且會結束呼叫。
6. 按一下 **Service Advisor Activity Log** 標籤，以檢視活動日誌的狀態。

   畫面上會顯示類似下圖的頁面。



   注意事項：

   - 活動日誌會顯示最後五個 Call Home 事件，包括 Test Call Home 和 Manual Call Home 事件。
   - **Send** 欄位中的結果可以是下列其中一項：

     Success

     IBM 或 FTP/TFTP 成功收到呼叫。**Assigned Service Number** 欄位包含問題單號碼。

Pending

Call Home 事件正在進行中。

Failed Call Home 事件失敗。在 Call Home 事件失敗的情況下，請聯絡「IBM 支援中心」以報告硬體服務事件。不會重試失敗的 Call Home 事件。

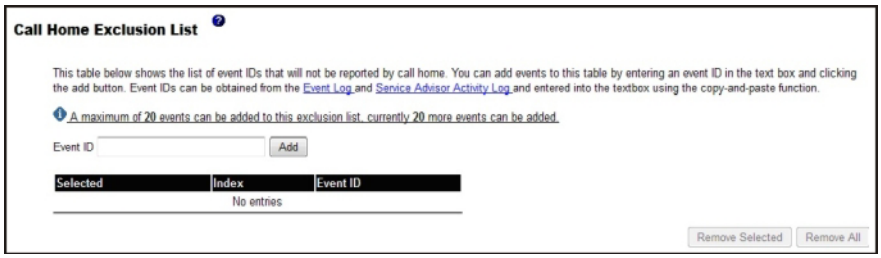
7. 解決事件後，請按一下該事件所對應的 **Corrected** 勾選框，以方便尋找未解決的事件。

   註：如果未選取事件所對應的 **Corrected** 勾選框，則下次出現相同事件時，若距第一次出現該事件的時間不超過五天，則不會進行 *Call Home*。

8. 按一下 **Refresh** 以顯示最新資訊。

   註：與「IBM 支援中心」通訊時，可以使用 **Assigned Service Number** 來參照 Call Home 事件。

9. 若要從傳送給「IBM 支援中心」的報告中移除指定事件，請執行下列步驟：
   a. 按一下 **Call Home Exclusion List** 鏈結。畫面上會顯示類似下圖的頁面。



   b. 在 **Event ID** 欄位中輸入十六進位的事件 ID。
   c. 按一下 **Add**。

登出

若要登出 IMM 或其他遠端伺服器，請按一下導覽窗格中的 **Log Off**。

第 4 章 監視伺服器狀態

使用導覽窗格的 **Monitors** 標題下的鏈結，來檢視您正在存取的伺服器狀態。

從 System Status 頁面，您可以：

- 監視伺服器的電源狀態，並檢視作業系統的狀態
- 檢視伺服器溫度讀數、電壓臨界值和風扇速度
- 檢視最新伺服器作業系統失敗畫面擷取
- 檢視登入 IMM 的使用者清單

從 Virtual Light Path 頁面，您可以檢視伺服器上亮起的任何 LED 的名稱、色彩和狀態。

從 Event Log 頁面，您可以：

- 檢視 IMM 的事件日誌中記錄的特定事件
- 檢視事件的嚴重性

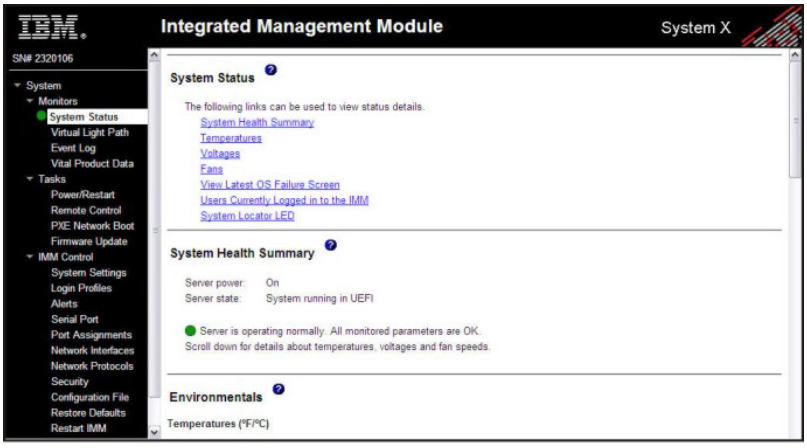
從 Vital Product Data (VPD) 頁面，您可以檢視重要產品資料。

檢視系統狀態

在 System Status 頁面上，您可以監視伺服器的溫度讀數、電壓臨界值及風扇狀態。您還可以檢視最新的作業系統失敗畫面、登入 IMM 的使用者及系統定位器 LED。

若要檢視伺服器的系統性能狀態和環境資訊，請完成下列步驟：

1. 登入 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **System Status** 以檢視動態產生的伺服器整體性能的更新。畫面上會顯示類似下圖的頁面。



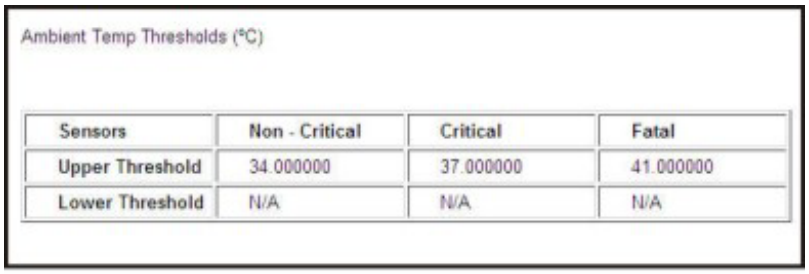
伺服器的狀態會決定 System Health Summary 頁面頂端所顯示的訊息。畫面上會顯示下列其中一種症狀：

- 實心綠色圓圈和片語 Server is operating normally
- 含有 X 的紅色圓圈或者含有驚嘆號的黃色三角形，以及片語 One or more monitored parameters are abnormal

如果受監視的參數在正常範圍以外運作，System Health Summary 頁面上便會顯示特定的異常參數清單。

3. 捲動到該頁面 **Environmentals** 區段中的 **Temperature** 區域，該頁面中包含溫度、電壓及風扇速度資訊。

IMM 會追蹤系統元件（例如微處理器、主機板及硬碟背板）的現行溫度讀數和臨界值層次。按一下溫度讀數，即會開啓新視窗。



Temperature Thresholds 頁面顯示 IMM 所反應的溫度層次。溫度臨界值是在遠端伺服器上預設的，且無法變更。

報告的溫度是根據下列臨界值範圍測量的：

非嚴重 當溫度達到指定值時，便會向配置的遠端警示接收者傳送溫度警示。您必須選取 Alerts 頁面 **SNMP Alerts Settings** 區域中的 **Warning Alerts** 勾選框，或者 Remote Alert Recipient 頁面上的 **Warning Alerts** 勾選框，才能傳送警示。

如需選取警示選項的相關資訊，請參閱第 30 頁的『配置 SNMP 警示設定』或第 28 頁的『配置遠端警示接收者』。

嚴重 當溫度達到的指定值高於警告值（非強迫關機臨界值）時，便會向配置的遠端警示接收者傳送第二個溫度警示，並且伺服器會透過依序關閉作業系統開始關閉程序。之後伺服器便會自行關閉。您必須選取 Alerts 頁面 **SNMP Alerts Settings** 區域中的 **Critical Alerts** 勾選框，或者 Remote Alert Recipient 頁面上的 **Critical Alerts** 勾選框，才能傳送警示。

如需選取警示選項的相關資訊，請參閱第 30 頁的『配置 SNMP 警示設定』或第 28 頁的『配置遠端警示接收者』。

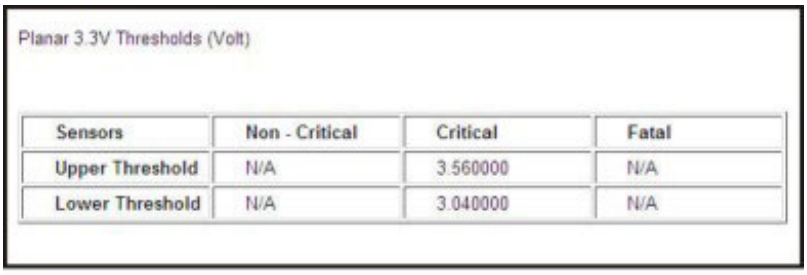
危險 當溫度達到的指定值高於非強迫關機值（硬關機臨界值）時，伺服器會立即關閉並向配置的遠端警示接收者傳送警示。您必須選取 Alerts 頁面 **SNMP Alerts Settings** 區域中的 **Critical Alerts** 勾選框，或者 Remote Alert Recipient 頁面上的 **Critical Alerts** 勾選框，才能傳送警示。

如需選取警示選項的相關資訊，請參閱第 30 頁的『配置 SNMP 警示設定』或第 28 頁的『配置遠端警示接收者』。

IMM 會在達到臨界值時產生非嚴重或嚴重事件，並起始關閉動作（如果需要的話）。

4. 捲動到 **Voltages** 區域。如果任何受監視的電源電壓落於其指定作業範圍之外，IMM 將傳送警示。

   如果您按一下電壓讀數，即會開啓新視窗。



   Voltage Thresholds 頁面顯示 IMM 所反應的電壓範圍。電壓臨界值是在遠端伺服器上預設的，且無法變更。

   IMM Web 介面會顯示主機板和電壓調節器模組 (VRM) 的電壓讀數。系統會設定採取下列動作的電壓範圍：

   非嚴重 當電壓低於或超出指定的電壓範圍時，便會向配置的遠端警示接收者傳送電壓警示。您必須選取 Alerts 頁面 **SNMP Alerts Settings** 區域中的 **Warning Alerts** 勾選框，才能傳送警示。

   如需選取警示選項的相關資訊，請參閱第 30 頁的『配置 SNMP 警示設定』。

   嚴重 當電壓低於或超出指定的電壓範圍時，便會向配置的遠端警示接收者傳送電壓警示，並且伺服器會透過依序關閉作業系統開始關閉程序。之後伺服器便會自行關閉。您必須選取 Alerts 頁面 **SNMP Alerts Settings** 區域中的 **Critical Alerts** 勾選框，才能傳送警示。

   如需選取警示選項的相關資訊，請參閱第 30 頁的『配置 SNMP 警示設定』。

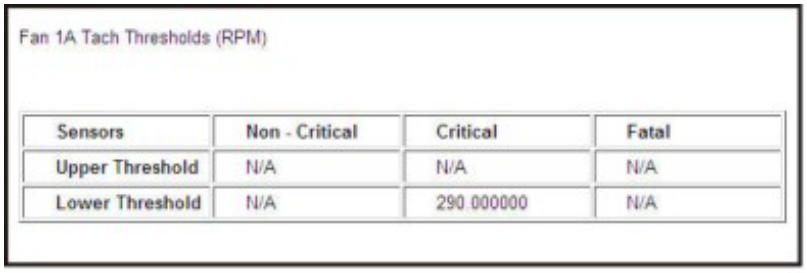
   危險 當電壓低於或超出指定的電壓範圍時，伺服器會立即關閉並向配置的遠端警示接收者傳送警示。您必須選取 Alerts 頁面 **SNMP Alerts Settings** 區域中的 **Critical Alerts** 勾選框，才能傳送警示。

   註：硬關機警示僅會在尚未傳送非強迫關機警示時傳送。

   如需選取警示選項的相關資訊，請參閱第 30 頁的『配置 SNMP 警示設定』。

   IMM 會在達到臨界值時產生非嚴重或嚴重事件，並產生任何關閉動作（如果需要的話）。
   非嚴重 如果 IMM 指示尚未達到此臨界值，則會產生警告事件。
   嚴重 如果 IMM 指示已達到此臨界值，則會產生嚴重事件。

5. 向下捲動到 **Fan Speeds (% of max)** 區域。IMM Web 介面會顯示伺服器風扇的運轉速度（以風扇速度上限的百分比表示）。如果您按一下風扇讀數，即會開啓新視窗。


Fan 1A Tach Thresholds (RPM)

Sensors	Non - Critical	Critical	Fatal
Upper Threshold	N/A	N/A	N/A
Lower Threshold	N/A	290.000000	N/A

如果風扇速度低於不可接受層次或風扇停止運轉，則您會收到風扇警示。您必須選取 Alerts 頁面 **SNMP Alerts Settings** 區域中的 **Critical Alerts** 勾選框，才能傳送警示。

如需選取警示選項的相關資訊，請參閱第 30 頁的『配置 SNMP 警示設定』。

6. 向下捲動到 **View Latest OS Failure Screen** 區域。按一下 **View OS Failure Screen**，以存取作業系統失敗畫面（在伺服器停止運作後擷取）的影像。

註：

僅 IMM Premium 提供作業系統失敗畫面擷取特性。如需從 IMM Standard 升級至 IMM Premium 的相關資訊，請參閱第 4 頁的『從 IMM Standard 升級至 IMM Premium』。

如果發生導致作業系統停止運作的事件，便會觸發作業系統監視器，從而導致 IMM 擷取作業系統失敗畫面並加以儲存。IMM 僅會儲存最新的錯誤事件資訊，在發生新錯誤事件時便會改寫較舊的作業系統失敗畫面資料。

若要遠端存取伺服器作業系統失敗畫面影像，請完成下列步驟：

a. 登入 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
b. 在導覽窗格中，按一下 **System Health**，然後向下捲動到 **View Latest OS Failure Screen** 區域。
c. 按一下 **View OS Failure Screen**。畫面上即會顯示作業系統失敗畫面影像。

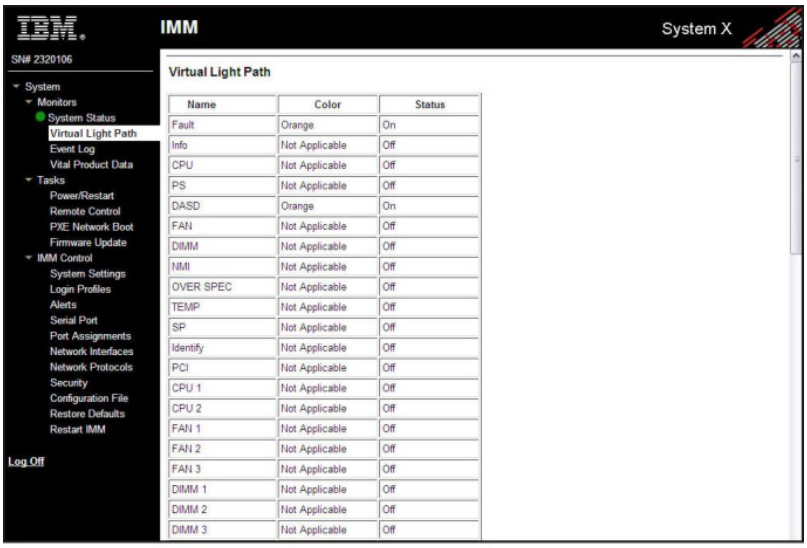
7. 向下捲動到 **Users Currently Logged in** 區域。 IMM Web 介面會顯示已登入 IMM 的每位使用者的登入 ID 和存取方法。
8. 向下捲動到 **System Locator LED** 區域。 IMM Web 介面會顯示系統定位器 LED 的狀態。它還會提供用於變更 LED 狀態的按鈕。如需此區域中所顯示圖形的意義，請參閱線上說明。

檢視虛擬光徑

「虛擬光徑」畫面顯示伺服器上亮起的任何 LED 的名稱、色彩和狀態。

若要存取和檢視虛擬光徑，請完成下列步驟：

1. 登入 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **Virtual Light Path** 以檢視伺服器上事件的最新歷程。畫面上會顯示類似下圖的頁面。



3. 向下捲動以檢視虛擬光徑的完整內容。

   註： 如果伺服器上未亮起 LED，Virtual Light Path 表格的 Color 直欄會指示 LED Color 爲 Not Applicable。

檢視事件日誌

註：如需特定事件或訊息的說明，請參閱伺服器文件。
錯誤碼和訊息會顯示在下列類型的事件日誌中：

- **系統事件日誌：**這種日誌包含 POST 和系統管理岔斷 (SMI) 事件，以及由內嵌於 IMM 的 BMC 產生的所有事件。您可以透過 Setup Utility 以及透過 Dynamic System Analysis (DSA) 程式來檢視系統事件日誌（作爲 IPMI 事件日誌）。

  系統事件日誌的大小有限制。當日誌已滿時，新的項目將不會改寫現有的項目；因此，您必須透過 Setup Utility 定期儲存然後再清除系統事件日誌。在進行疑難排解時，您可能必須儲存然後再清除系統事件日誌，讓最近的事件可供進行分析。

  訊息會列示在畫面左側，而關於選定訊息的詳細資料則顯示在畫面的右側。若要從某個項目移至下一個項目，請使用上移鍵 (↑) 和下移鍵 (↓)。

  事件發生時，系統事件日誌會指出主張事件。當事件不再發生時，日誌會指出非斷定事件。

  部分的 IMM 感應器會在達到其設定點時記載斷定事件。而當設定點狀況不再存在時，會記載對應的非斷定事件。不過，並不是所有的事件都是斷定類型的事件。
- **整合式管理模組 (IMM) 事件日誌：**這種日誌包含所有 IMMP、POST 和系統管理岔斷 (SMI) 事件的已過濾子集。您可以透過 IMM Web 介面和 DSA 程式來檢視 IMM 事件日誌（作爲 ASM 事件日誌）。

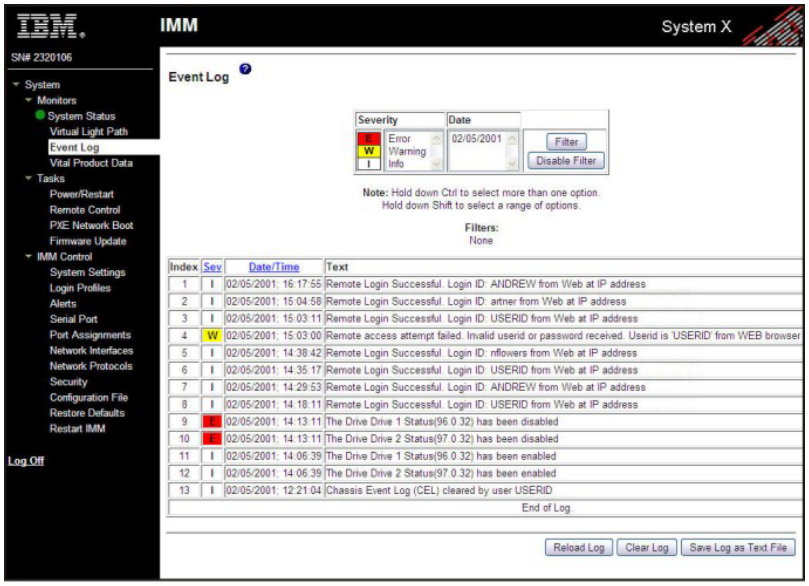
- **DSA 日誌**：該日誌是由 DSA 程式所產生，並且由系統事件日誌（作爲 IPMI 事件日誌）、IMM 機箱事件日誌（作爲 ASM 事件日誌）和作業系統事件日誌合併而成，並按照時間先後順序排列。您可以透過 DSA 程式檢視 DSA 日誌。
- **機箱事件日誌**：IMM 會產生 IPMI 斷定和非斷定事件的文字訊息，並在機箱事件日誌中建立這些事件的項目。透過「分散式管理工作小組 (DMTF)」規格 DSP0244 和 DSP8007 針對這些事件產生文字。此日誌還包含除 IPMI 感應器斷定和非斷定事件之外的事件的項目，例如，機箱事件日誌包含在使用者變更網路設定或在使用者登入 Web 介面時的項目。您可以從 IMM Web 介面檢視此日誌。

透過 Web 介面檢視系統事件日誌

註：系統事件日誌的容量有限制。達到該限制時，便會依先進先出順序刪除較早的事件。

若要存取和檢視事件日誌，請完成下列步驟：

1. 登入 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **Event Log** 以檢視伺服器上事件的最新歷程。畫面上會顯示類似下圖的頁面。



3. 向下捲動以檢視事件日誌的完整內容。事件具有下列嚴重性層次：

   資訊　此嚴重性層次指派給您應予以注意的事件。

   警告　此嚴重性層次指派給可能會影響伺服器效能的事件。

   錯誤　此嚴重性層次指派給需要立即引起注意的事件。

   IMM Web 介面會透過在嚴重性直欄中以黃色背景的字母 W 來識別警告事件，以紅色背景的字母 E 來識別錯誤事件。
4. 按一下 **Save Log as Text File** 可將事件日誌的內容儲存爲文字檔。按一下 **Reload Log** 可重新整理事件日誌的顯示畫面。按一下 **Clear Log** 可刪除事件日誌的內容。

透過 Setup Utility 檢視事件日誌

如需使用 Setup Utility 的完整資訊，請參閱伺服器隨附的文件。

如果要檢視 POST 事件日誌或系統事件日誌，請完成下列步驟：

1. 開啓伺服器。

   註：在伺服器接通 AC 電源大約 2 分鐘後，電源控制按鈕就會變成作用中狀態。

2. 顯示 <F1> Setup 提示時，請按 F1 鍵。如果您同時設定了開機密碼和管理者密碼，則必須輸入管理者密碼才能檢視事件日誌。
3. 選取 **System Event Logs**，使用下列其中一個程序：
   - 如果要檢視 POST 事件日誌，請選取 **POST Event Viewer**。
   - 如果要檢視系統事件日誌，請選取 **System Event Log**。

檢視事件日誌而不重新啓動伺服器

如果伺服器沒有當機，則有一些方法可供您無需重新啓動伺服器就可檢視一或多個事件日誌。

如果已安裝 Portable 或 Dynamic System Analysis (DSA)，可以用它來檢視系統事件日誌（當成 IPMI 事件日誌）、IMM 事件日誌（當成 ASM 事件日誌）、作業系統事件日誌或合併的 DSA 日誌。您也可以使用 DSA Preboot 來檢視這些日誌，不過您必須重新啓動伺服器才能使用 DSA Preboot。若要安裝 Portable DSA、Installable DSA 或 DSA Preboot，或是要下載 DSA Preboot CD 映像檔，請造訪 http://www.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=SERV-DSA&brandind=5000008，或完成下列步驟：

註：IBM 網站會定期進行變更。實際的程序可能與本文件的說明略有不同。

1. 請造訪 http://www.ibm.com/systems/support/。
2. 在 **Product support** 下，按一下 **System x**。
3. 在 **Popular links** 下，按一下 **Software and device drivers**。
4. 在 **Related downloads** 下，按一下 **Dynamic System Analysis (DSA)** 以顯示可下載的 DSA 檔案矩陣。

如果伺服器中有安裝 IPMItool，可以用它來檢視系統事件日誌。最新版的 Linux 作業系統隨附 IPMItool 的現行版本。如需 IPMItool 的相關資訊，請造訪 http://sourceforge.net/。

註：IBM 網站會定期進行變更。實際的程序可能與本文件的說明略有不同。

1. 請造訪 http://publib.boulder.ibm.com/infocenter/toolsctr/v1r0/index.jsp。
2. 在導覽窗格中，按一下 **IBM System x and BladeCenter Tools Center**。
3. 依序展開 **Tools reference**、**Configuration tools**、**IPMI tools**，然後按一下 **IPMItool**。

如需 IPMI 的概觀，請造訪 http://publib.boulder.ibm.com/infocenter/systems/index.jsp?topic=/liaai/ipmi/liaaiipmi.htm，或完成下列步驟：

1. 造訪 http://publib.boulder.ibm.com/infocenter/systems/index.jsp。
2. 在導覽窗格中，按一下 **IBM Systems Information Center**。

3. 依序展開 **Operating systems**、**Linux information**、**Blueprints for Linux on IBM systems**，然後按一下 **Using Intelligent Platform Management Interface (IPMI) on IBM Linux platforms**。

您可以透過 IMM Web 介面中的 **Event Log** 鏈結來檢視 IMM 事件日誌。

下表說明一些可用來檢視事件日誌的方法，視伺服器的狀況而定。一般而言，前兩種狀況並不需要重新啓動伺服器。

表 16. 檢視事件日誌的方法

狀況	操作
伺服器未當機並已連接至網路。	請使用下列任一方法： • 執行 Portable 或 Installable DSA 以檢視事件日誌，或者建立可傳送至 IBM 服務與支援的輸出檔。 • 鍵入 IMM 的 IP 位址，並移至 Event Log 頁面。 • 使用 IPMItool 檢視系統事件日誌。
伺服器未當機且未連接至網路。	在本端使用 IPMItool 檢視系統事件日誌。
伺服器已當機。	• 如果已安裝 DSA Preboot，請重新啓動伺服器並按 F2 鍵，以啓動 DSA Preboot 和檢視事件日誌。 • 如果尚未安裝 DSA Preboot，請插入 DSA Preboot CD 並重新啓動伺服器，以啓動 DSA Preboot 和檢視事件日誌。 • 此外，您可以重新啓動伺服器，然後按 F1 鍵啓動 Setup Utility，以及檢視 POST 事件日誌或系統事件日誌。如需相關資訊，請參閱第 93 頁的『透過 Setup Utility 檢視事件日誌』。

檢視重要產品資料

伺服器啓動時，IMM 會收集伺服器資訊、伺服器韌體資訊及伺服器元件重要產品資料 (VPD)，並將該資訊儲存在永久記憶體中。您可以隨時從幾乎任何電腦存取該資訊。Vital Product Data 頁面包含 IMM 所監視的遠端受管理伺服器的主要資訊。

若要檢視伺服器元件重要產品資料，請完成下列步驟：

1. 登入 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **Vital Product Data** 以檢視伺服器上軟硬體元件的狀態。
3. 向下捲動以檢視下列 VPD 讀數：

   機器層次 VPD

   此區域顯示伺服器的重要產品資料。對於檢視 VPD，機器層次 VPD 包含通用唯一 ID (UUID)。

註：機器層次 VPD、元件層次 VPD 及元件活動日誌僅在開啓伺服器後提供資訊。

表 17. 機器層次重要產品資料

欄位	功能
Machine type and model	識別 IMM 所監視伺服器的類型和型號。
Serial number	識別 IMM 所監視伺服器的序號。
UUID	識別 IMM 所監視伺服器的通用唯一 ID (UUID)（一個 32 位數的十六進位數）。

元件層次 VPD

此區域顯示遠端受管理伺服器的元件的重要產品資料。

表 18. 元件層次重要產品資料

欄位	功能
FRU name	識別每個元件的現場可更換組件 (FRU)。
Serial number	識別每個元件的序號。
Mfg ID	識別每個元件的製造商 ID。

元件活動日誌

在此區域中，您可以檢視元件活動的記錄。

表 19. 元件活動日誌

欄位	功能
FRU name	識別元件的現場可更換組件 (FRU) 名稱。
Serial number	識別元件的序號。
Mfg ID	識別元件的製造商。
Action	識別針對每個元件所採取的動作。
Timestamp	識別元件動作的日期和時間。日期以 *mm/dd/yy* 格式顯示。時間以 *hh:mm:ss* 格式顯示。

IMM VPD

在此區域中，您可以檢視遠端受管理伺服器的 IMM 韌體、System x 伺服器韌體及 Dynamic System Analysis 韌體 VPD。

表 20. IMM、UEFI 及 DSA 韌體重要產品資料

欄位	功能
Firmware type	指示韌體碼的類型。
Version string	指示韌體碼的版本。
Release date	指示韌體的發行時間。

第 5 章 執行 IMM 作業

使用導覽窗格中 **Tasks** 標題下的功能，來直接控制 IMM 和您的伺服器的動作。您可以執行的作業視安裝 IMM 所在的伺服器而定。

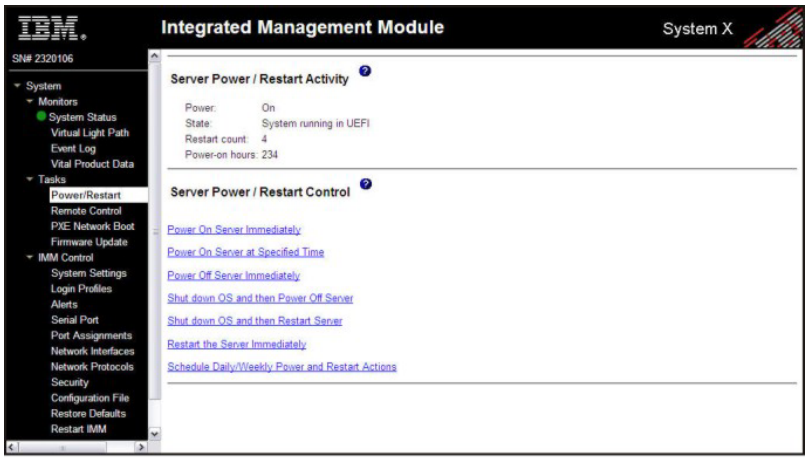
您可以執行下列作業：

- 檢視伺服器電源和重新啓動活動
- 遠端控制伺服器的電源狀態
- 遠端存取伺服器主控台
- 遠端將磁碟或磁碟映像檔連接至伺服器
- 更新 IMM 韌體

註：部分特性僅適用於執行受支援 Microsoft Windows 作業系統的伺服器。

檢視伺服器電源和重新啓動活動

Server Power/Restart Activity 區域顯示產生網頁時的伺服器的電源狀態。



Power 此欄位顯示產生現行網頁時的伺服器的電源狀態。

State 此欄位顯示產生現行網頁時的伺服器的狀態。狀態可能如下：

- 系統電源關閉/狀態不明
- 系統開啓/正在啓動 UEFI
- 系統在 UEFI 已停止（偵測到錯誤）
- 系統在 UEFI 執行中
- 啓動作業系統或作業系統不受支援（如果作業系統未配置爲支援 IMM 的頻內介面，則可能在作業系統中）
- 作業系統已啓動

Restart count

此欄位顯示伺服器已重新啓動的次數。

註：每次 IMM 子系統清除爲原廠預設值時，計數器重設爲零。

Power-on hours
此欄位顯示伺服器已開啓的總小時數。

控制伺服器的電源狀態

IMM 透過電源開啓、電源關閉和重新啓動動作，提供對伺服器的完整電源控制。此外，還會擷取和顯示電源開啓和重新啓動統計資料，以顯示伺服器硬體可用性。若要執行 **Server Power/Restart Control** 區域中的動作，您必須具有 IMM 的 Supervisor 存取權。

若要執行伺服器電源和重新啓動動作，請完成下列步驟。

註：請僅在發生緊急情況或者您在異地且伺服器沒有回應時，選取下列選項。

1. 登入 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **Power/Restart**。向下捲動到 **Server Power/Restart Control** 區域。
3. 按下列其中一個選項：

Power on server immediately
開啓伺服器並啓動作業系統。

Power on server at specified time
在指定時間開啓伺服器，並啓動作業系統。

Power off server immediately
關閉伺服器而不關閉作業系統。

Shut down OS and then power off server
關閉作業系統後關閉伺服器。

註：嘗試執行 ″Shut down OS and then power off server″ 要求時，如果作業系統處於螢幕保護程式或鎖定模式，則 IMM 可能無法起始以正常方式關機。IMM 會在電源關閉延遲間隔到期後執行硬重設或關機，而 OS 可能仍處於啓動且執行中狀態。

Shut down OS and then restart server
重新啓動作業系統。

註：嘗試執行 ″Shut down OS and then restart server″ 要求時，如果作業系統處於螢幕保護程式或鎖定模式，則 IMM 可能無法起始以正常方式關機。IMM 會在電源關閉延遲間隔到期後執行硬重設或關機，而 OS 可能仍處於啓動且執行中狀態。

Restart the server immediately
立即關閉並開啓伺服器，而不先關閉作業系統。

Schedule daily/weekly power and restart actions
在指定的每日或每週時間關閉作業系統、關閉伺服器（包含或不包含重新啓動伺服器），以及在指定的每日或每週時間開啓伺服器。

選取這些選項的任何一項都會顯示確認訊息，如果是意外選取的選項，您可以取消作業。

遠端顯示

註：

1. IMM 遠端顯示功能僅在 IMM Premium 中可用。如需從 IMM Standard 升級至 IMM Premium 的相關資訊，請參閱第 4 頁的『從 IMM Standard 升級至 IMM Premium』。
2. Remote Control 特性僅透過 IMM Web 介面提供。您必須使用具有 Supervisor 存取權的使用者 ID 登入 IMM，才能使用任何 Remote Control 特性。

您可以使用 IMM Web 介面中的遠端顯示功能或 Remote Control 特性，才能檢視伺服器主控台及與伺服器主控台互動。您也可以爲伺服器指派 CD 或 DVD 光碟機、軟式磁碟機、USB 快閃記憶體隨身碟，或您的電腦上的磁碟映像檔。

Remote Control 特性提供下列功能：

- 無論伺服器狀態爲何，都能以最高達 1280 x 1024（頻率爲 75 Hz）的圖形解析度，從遠端檢視視訊
- 從遠端用戶端使用鍵盤和滑鼠，以遠端方式存取伺服器
- 對映遠端用戶端上的 CD 或 DVD 光碟機、軟式磁碟機及 USB 快閃記憶體隨身碟，以及將 ISO 和磁片映像檔對映爲可供伺服器使用的虛擬磁碟機
- 將磁片映像檔上傳至 IMM 記憶體，並將它對映至伺服器作爲虛擬磁碟機

更新 IMM 韌體和 Java 或 ActiveX Applet

重要事項：IMM 使用 Java Applet 或 ActiveX Applet，來執行遠端顯示功能。將 IMM 更新至最新韌體層次時，也會將 Java Applet 和 ActiveX Applet 更新至最新層次。依預設，Java 會快取（在本端儲存）先前使用的 Applet。對 IMM 韌體進行快閃更新後，伺服器使用的 Java Applet 可能不是最新層次。

若要更正此問題，請完成下列步驟：

1. 按一下**開始 → 設定 → 控制台**。
2. 按兩下 **Java Plug-in 1.5**。Java Plug-in Control Panel 視窗即會開啓。
3. 按一下 **Cache** 標籤。
4. 選擇下列其中一個選項：
   - 清除 **Enable Caching** 勾選框可使 Java 快取永遠停用。
   - 按一下 **Clear Caching**。如果您選擇此選項，則必須在每次 IMM 韌體更新後按一下 **Clear Caching**。

如需更新 IMM 韌體的相關資訊，請參閱第 109 頁的『更新韌體』。

啓用遠端顯示功能

註：IMM 遠端顯示功能僅在 IMM Premium 中可用。如需從 IMM Standard 升級至 IMM Premium 的相關資訊，請參閱第 4 頁的『從 IMM Standard 升級至 IMM Premium』。

如果要啓用遠端顯示特性，請完成下列步驟：

1. 拔掉電源線以切斷伺服器電源。
2. 將虛擬媒體金鑰安裝至主機板上的專用插槽。
3. 重新接通伺服器電源。

   註：在伺服器接通 AC 電源大約 2 分鐘後，電源控制按鈕就會變成作用中狀態。
4. 開啓伺服器。

遠端控制

IMM 的 Remote Control 特性由下列兩個個別視窗中的兩個 Java 應用程式組成：

Video Viewer

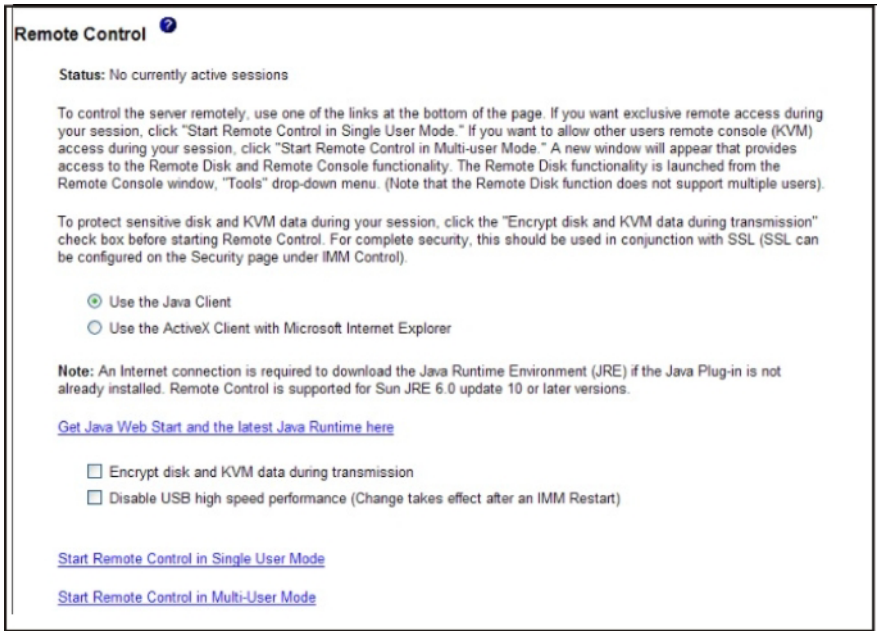
Video Viewer 使用遠端主控台來進行遠端系統管理。遠端主控台是伺服器的互動式圖形使用者介面 (GUI) 顯示，可在您的電腦上進行檢視。您在顯示器上看到的畫面與伺服器主控台上的畫面完全相同，並且您具有主控台鍵盤和滑鼠的控制權。

Virtual Media Session

Virtual Media Session 視窗會列出用戶端上的所有磁碟機，可將該用戶端對映爲遠端磁碟機。它可讓您將 ISO 和磁片映像檔對映爲虛擬磁碟機。每個對映磁碟機都可以標示爲唯讀。CD/DVD 光碟機和 ISO 映像檔一律爲唯讀。

若要遠端存取伺服器主控台，請完成下列步驟：

1. 登入 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **Remote Control**。畫面上會顯示類似下圖的頁面。



3. 選擇下列其中一個選項：
   - 按一下 **Use the Java Client**，可使用 Java Applet 來執行遠端顯示。

- 按一下 **Use the ActiveX Client with Microsoft Internet Explorer**，可使用 Windows 作業系統中的 Internet Explorer，並且您想要使用 ActiveX Applet 來執行遠端顯示功能。

  註：IMM 韌體 1.28 版提供 32 位元「ActiveX 遠端顯示用戶端」。IMM 韌體 1.30 版提供 64 位元「ActiveX 用戶端」。

4. 若要遠端控制伺服器，請使用 Remote Control 頁面底端的其中一個鏈結。如果想要在階段作業期間獨占遠端存取權，請按一下 **Start Remote Control in Single User Mode**。如果想要在階段作業期間容許其他使用者擁有遠端主控台 (KVM) 存取權，則請按一下 **Start Remote Control in Multi-user Mode**。即會開啓新視窗，供存取 Remote Disk 和 Remote Console 功能。

   如果在開啓 Remote Control 視窗之前已選取 **Encrypt disk and KVM data during transmission** 勾選框，則會使用 ADES 加密對磁碟資料進行加密。

完成使用 Remote Control 特性之後，請關閉 Video Viewer 視窗和 Virtual Media Session 視窗。

注意事項：

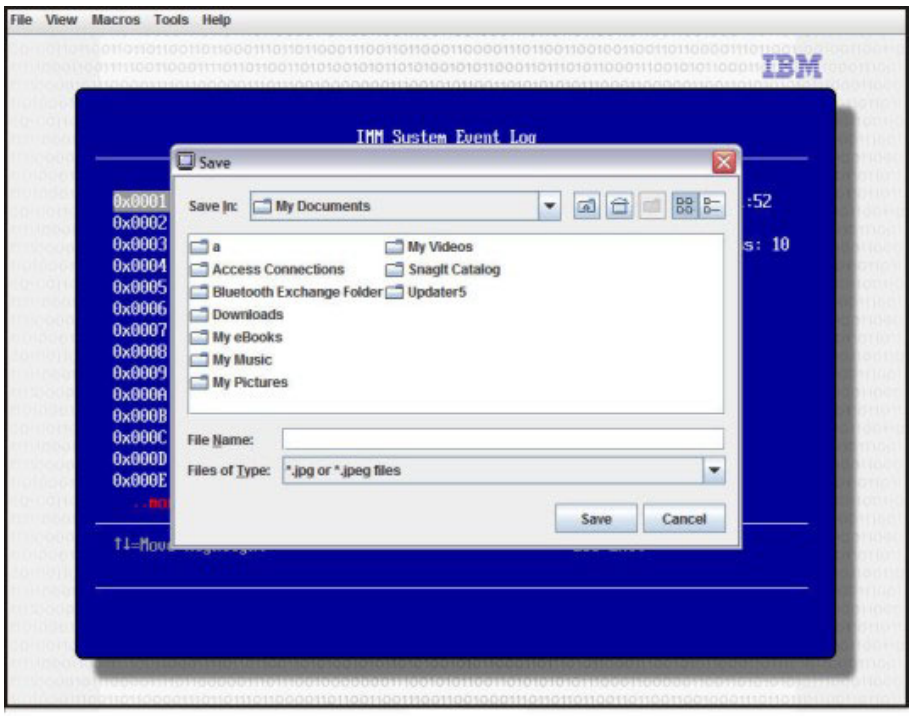
1. 如果目前已對映遠端磁碟，則請勿關閉 Virtual Media Session 視窗。如需關閉和取消對映遠端磁碟的相關指示，請參閱第 107 頁的『遠端磁碟』。
2. 如果在使用 Remote Control 時遇到滑鼠或鍵盤方面的問題，請參閱說明（可從 Web 介面的 Remote Control 頁面中取得）。
3. 如果您使用遠端主控台在 Setup Utility 程式中變更 IMM 的設定，伺服器可能會重新啓動 IMM。您將會遺失遠端主控台和登入階段作業。在短暫延遲之後，您可以再次登入 IMM、再次啓動遠端主控台，並結束 Setup Utility 程式。

遠端控制畫面擷取

Video Viewer 視窗中的畫面擷取特性，可擷取伺服器的視訊顯示內容。若要擷取並儲存畫面影像，請完成下列步驟：

1. 在 Video Viewer 視窗中，按一下 **File**。
2. 從功能表中選取 **Capture to File**。
3. 出現提示時，命名影像檔並將其儲存至本端用戶端上您選擇的位置。

註：畫面擷取影像會儲存爲 JPG 或 JPEG 檔案類型。



遠端控制 Video Viewer 檢視模式

若要變更 Video Viewer 視窗的視圖，請按一下 **View**。下列功能表選項可供使用：

Refresh

Video Viewer 使用伺服器中的視訊資料重新顯示視訊顯示畫面。

Full Screen

Video Viewer 使用視訊顯示畫面填滿用戶端桌面。僅當 Video Viewer 不在全螢幕模式時，才能使用此選項。

Windowed

Video Viewer 從全螢幕模式切換爲一般視窗模式。僅當 Video Viewer 在全螢幕模式時，才能使用此選項。

Fit Video Viewer 將大小調整爲完全顯示目標桌面，而沒有額外邊框或捲軸。這要求用戶端桌面足夠大，才能顯示此調整大小的視窗。

遠端控制視訊色彩模式

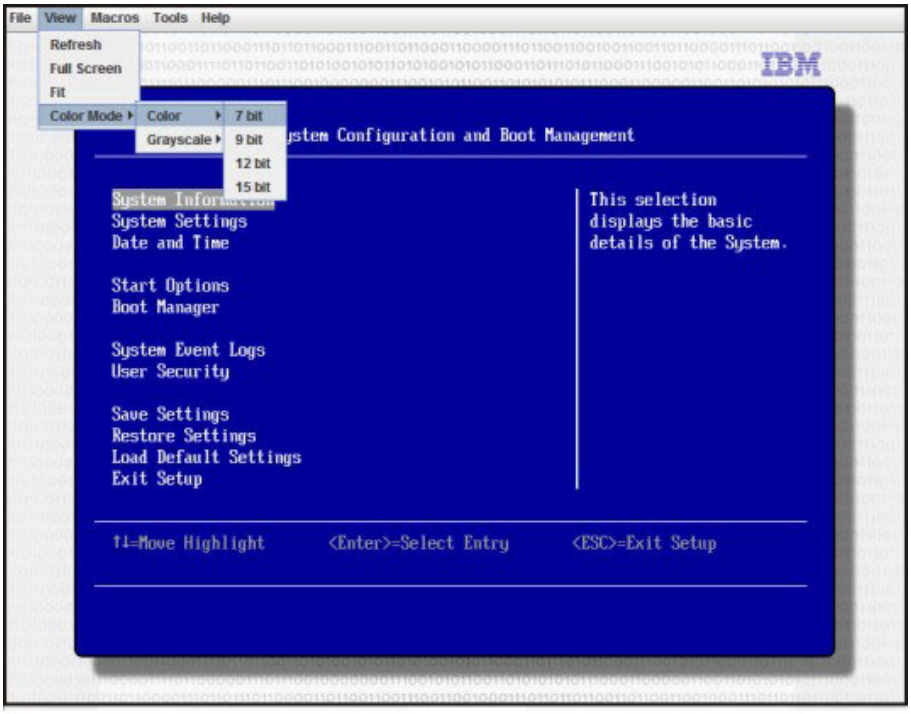
如果與遠端伺服器連線的頻寬受限，則您可以減少 Video Viewer 的頻寬需求，方法是調整 Video Viewer 視窗中的色彩設定。

註：IMM 具有可調整色彩深度的功能表項目，以減少在低頻寬狀況下傳輸的資料，而非使用 Remote Supervisor Adapter II 介面中的頻寬調節器。

若要變更視訊色彩模式，請完成下列步驟：

1. 在 Video Viewer 視窗中，按一下 **View**。
2. 將滑鼠指標移到功能表中的 **Color Mode** 上時，會顯示兩個色彩模式選項：

- Color：7、9、12 及 15-bit
- Grayscale：16、32、64、128 shades

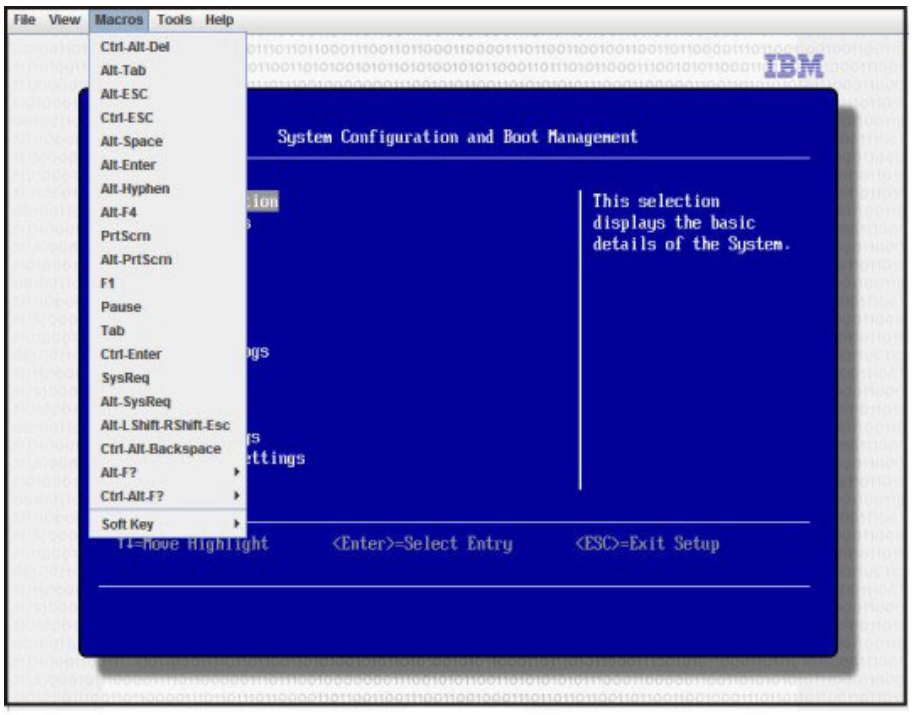


3. 選取色彩或灰階設定。

遠端控制鍵盤支援

您所使用的用戶端伺服器上的作業系統會設陷捕捉某些組合鍵，例如 Microsoft Windows 中的 Ctrl+Alt+Del，而非將它們傳輸至伺服器。其他按鍵（例如 F1）可能會導致同時在電腦和伺服器上執行動作。若要使用影響遠端伺服器（而非本端用戶端）的組合鍵，請完成下列步驟：

1. 在 Video Viewer 視窗中，按一下 **Macros**。
2. 從功能表中選取預先定義的其中一個組合鍵，或者選取 **Soft Key** 以選擇或新增使用者定義的組合鍵。



使用 Video Viewer **Macros** 功能表項目可建立或編輯自訂按鈕，使用這些按鈕可將按鍵傳送至伺服器。

若要建立和編輯自訂按鈕，請完成下列步驟：

1. 在 Video Viewer 視窗中，按一下 **Macros**。
2. 依序選取 **Soft Key** 和 **Add**。即會開啓一個新視窗。
3. 按一下 **New** 以新增組合鍵，或者選取組合鍵並按一下 **Delete** 以移除現有組合鍵。
4. 如果您要新增組合，請在蹦現視窗中鍵入您想要定義的組合鍵，然後按一下 **OK**。
5. 完成定義或移除組合鍵後按一下 **OK**。

國際鍵盤支援

Video Viewer 使用平台專用的本機字碼來截取按鍵事件，以直接存取實際按鍵資訊。用戶端會偵測實際按鍵事件，並將它們傳遞至伺服器。伺服器會偵測用戶端所經歷的相同實體按鍵，並支援所有標準鍵盤佈置，唯一限制是目標和用戶端須使用相同的鍵盤佈置。如果遠端使用者的鍵盤佈置與伺服器不同，該使用者可以在遠端存取伺服器時切換伺服器佈置，並在之後重新切回。

鍵盤透通模式

鍵盤透通特性可停用對用戶端上大部分特殊組合鍵的處理，以便它們能夠直接傳遞至伺服器。這提供了使用巨集的替代方案。

部分作業系統會將某些按鍵定義爲不受應用程式控制，以便透通機制行爲的運作獨立於伺服器。例如，在 Linux X 階段作業中，Ctrl+Alt+F2 按鍵組合可用於切換至虛擬主控台 2。由於沒有截取此按鍵順序的機制，因此用戶端無法將這些按鍵直接傳遞至目標。在此情況下的唯一選項是使用針對此目的定義的鍵盤巨集。

若要啓用或停用鍵盤透通模式，請完成下列步驟：

1. 在 Video Viewer 視窗中，按一下 **Tools**。
2. 從功能表中選取 **Session Options**。
3. 當畫面上顯示 Session Options 視窗時，按一下 **General** 標籤。
4. 選取 **Pass all keystrokes to target** 勾選框，以啓用或停用該特性。
5. 按一下 **OK** 以儲存選擇。

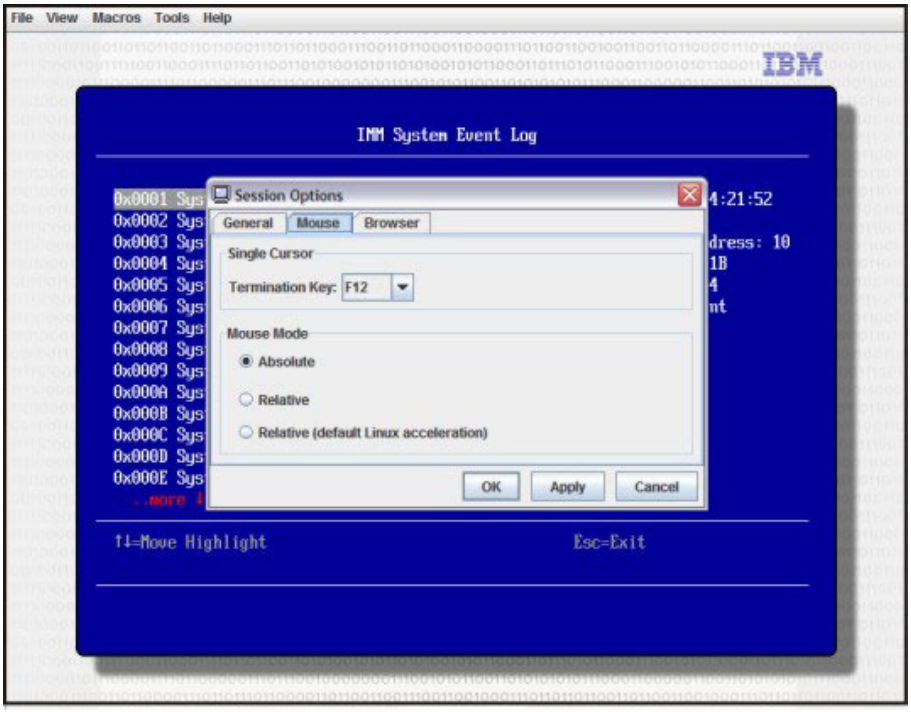
遠端控制滑鼠支援

Video Viewer 視窗提供了用於滑鼠控制的數個選項，包括絕對滑鼠控制、相對滑鼠控制和單一游標模式。

絕對和相對滑鼠控制

若要存取用於控制滑鼠的絕對和相對選項，請完成下列步驟：

1. 在 Remote Control 視窗中，按一下 **Tools**。
2. 從功能表選取 **Session Options**。
3. 在顯示 Session Options 視窗時，按一下 **Mouse** 標籤。



4. 選取下列其中一個滑鼠模式：

Absolute

用戶端會將滑鼠位置訊息傳送至一律與檢視區域的原點（左上方）相對的伺服器。

Relative

用戶端傳送滑鼠位置作爲距先前位置的偏移。

Relative (default Linux acceleration)
用戶端將套用加速因素，以在 Linux 目標上更好地對齊滑鼠。已選取加速設定，來最大化與 Linux 發行套件的相容性。

單游標模式

部分作業系統無法對齊本端和遠端游標，這會導致本端和遠端滑鼠游標之間出現偏移。單游標模式可在滑鼠位於 Video Viewer 視窗內時，隱藏本端用戶端游標。啓動單游標模式後，您只能看到遠端游標。

若要啓用單游標模式，請完成下列步驟：

1. 在 Video Viewer 視窗中，按一下 **Tools**。
2. 選取 **Single Cursor**。

當 Video Viewer 處於單游標模式時，您無法使用滑鼠切換至其他視窗或者按 KVM 用戶端視窗以外的地方，因爲沒有本端游標。若要停用單游標模式，請按定義的終止鍵。若要檢視定義的終止鍵，或變更終止鍵，請按一下 **Tools > Session Options > Mouse**。

遠端電源控制

您可以從 Video Viewer 視窗傳送伺服器電源和重新啓動指令，而不需回到 Web 瀏覽器。若要使用 Video Viewer 來控制伺服器電源，請完成下列步驟：

1. 在 Video Viewer 視窗中，按一下 **Tools**。
2. 將滑鼠指標移到功能表中的 **Power** 上時，會顯示下列選項：

   On 開啓伺服器電源。

   Off 關閉伺服器電源。

   Reboot
   重新啓動伺服器。

   Cycle 關閉再開啓伺服器電源。

檢視效能統計資料

若要檢視 Video Viewer 效能統計資料，請完成下列步驟：

1. 在 Video Viewer 視窗中，按一下 **Tools**。
2. 按一下 **Stats**。畫面上會顯示下列資訊：

   Frame Rate
   用戶端每秒解碼的訊框數目的執行平均值。

   Bandwidth
   用戶端每秒接收的 KB 總數的執行平均值。

   Compression
   因視訊壓縮而縮減的頻寬的執行平均值。此值通常會顯示爲 100.0%。該值會四捨五入到千分之一。

   Packet Rate
   每秒接收的視訊封包數目的執行平均值。

啓動遠端桌面通訊協定

如果已安裝 Windows 型「遠端桌面通訊協定 (RDP)」用戶端，您可以使用 RDP 用戶端（而不是 KVM 用戶端）進行切換。遠端伺服器必須配置爲接收 RDP 連線。

遠端磁碟

從 Virtual Media Session 視窗，您可以爲伺服器指派您的電腦上的 CD 或 DVD 光碟機、軟式磁碟機或 USB 快閃記憶體隨身碟，或者，您可以爲伺服器指定您的電腦上要使用的映像檔。您可以將硬碟用於各種功能，如重新啓動（啓動）伺服器、更新程式碼、在伺服器上安裝新軟體，以及在伺服器上安裝或更新作業系統。您可以使用 Remote Control 特性來存取遠端磁碟。硬碟和磁碟映像檔在伺服器上顯示爲 USB 隨身碟。

注意事項：

1. 下列伺服器作業系統具有 USB 支援（遠端磁碟特性需要）：
   - Microsoft Windows Server 2008
   - Microsoft Windows Server 2003
   - Red Hat Linux 4.0 版和 5.0 版
   - SUSE Linux 10.0 版
   - Novell NetWare 6.5
2. 用戶端伺服器需要 Java 1.5 外掛程式或更新版本。
3. 用戶端伺服器必須具有 Intel Pentium III 微處理器或更新版本（以 700 MHz 或更快頻率作業），或等同產品。

存取遠端控制

若要開始遠端控制階段作業和存取遠端磁碟，請完成下列步驟：

1. 登入 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **Remote Control**。
3. 在 Remote Control 頁面上，按一下其中一個 **Start Remote Control** 選項：
   - 如果想要在階段作業期間獨占遠端存取權，請按一下 **Start Remote Control in Single User Mode**。
   - 如果想要在階段作業期間容許其他使用者具有遠端主控台 (KVM) 存取權，請按一下 **Start Remote Control in Multi-user Mode**。

   Video Viewer 視窗即會開啓。
4. 若要開啓 Virtual Media Session 視窗，請在 Video Viewer 視窗中，按一下 **Tools > Launch Virtual Media**。

註：如果在開啓 Remote Control 視窗之前已選取 **Encrypt disk and KVM data during transmission** 勾選框，則會使用 ADES 加密對磁碟資料進行加密。

Virtual Media Session 視窗與 Video Viewer 視窗不同。Virtual Media Session 視窗會列出用戶端上的所有磁碟機，可將該用戶端對映爲遠端磁碟機。Virtual Media Session 視窗也可讓您將 ISO 和磁片映像檔對映爲虛擬磁碟機。每一個對映磁碟機可以標示爲唯讀。CD 和 DVD 光碟機及 ISO 映像檔一律爲唯讀。

使用 IMM 韌體 1.03 版或更新版本對映和取消對映磁碟機

若要對映磁碟機，請選取您要對映的磁碟機旁邊的 **Select** 勾選框。

註：對映 CD 或 DVD 光碟機之前，其中必須含有媒體。如果光碟機是空的，則會提示您將 CD 或 DVD 插入光碟機中。

按一下 **Mount Selected** 按鈕，以裝載和對映選取的磁碟機。

如果您按一下 **Add Image**，則可以將磁片映像檔和 ISO 映像檔新增至可用磁碟機清單。Virtual Media Session 視窗中列出磁片或 ISO 映像檔後，就可以像其他磁碟機一樣進行對映。

若要取消對映磁碟機，請按一下 **Unmount All** 按鈕。取消對映磁碟機之前，您必須確認想要取消對映磁碟機。

註：確認您要取消對映磁碟機後，便會取消裝載所有磁碟機。您無法個別取消裝載磁碟機。

您可以選取磁片映像檔，並將磁片映像儲存在 IMM 記憶體中。如此可使磁碟保持裝載在伺服器上，以便您稍後存取磁碟，即使在 IMM Web 介面階段作業結束後也可以存取。最多只能將一個磁碟機映像儲存在 IMM 卡上。磁碟機或映像內容大小不得大於 1.44 MB。若要上傳磁片映像檔，請完成下列步驟：

1. 按一下 **RDOC**。
2. 新視窗開啓後，按一下 **Upload**。
3. 按一下 **Browse** 以選取您要使用的映像檔。
4. 在 **Name** 欄位中輸入映像的名稱，然後按一下 **OK** 以上傳檔案。

   註：若要從記憶體中卸載映像檔，請在 RDOC Setup 視窗選取名稱，然後按一下 **Delete**。

使用 IMM 韌體 1.02 版或更舊版本對映和取消對映磁碟機

若要對映磁碟機，請選取您要對映的磁碟機旁邊的 **Mapped** 勾選框。

註：對映 CD 或 DVD 光碟機之前，其中必須含有媒體。如果光碟機是空的，則會提示您將 CD 或 DVD 插入光碟機中。

如果您按一下 **Add Image**，則可以將磁片映像檔和 ISO 映像檔新增至可用磁碟機清單。Virtual Media Session 視窗中列出磁片或 ISO 映像檔後，就可以像其他磁碟機一樣進行對映。

若要取消對映磁碟機，清除該磁碟機對應的 **Mapped** 勾選框即可。取消對映磁碟機之前，您必須確認想要取消對映該磁碟機。

您可以選取磁片映像檔，並將磁片映像儲存在 IMM 記憶體中。如此可使磁碟保持裝載在伺服器上，以便您稍後存取磁碟，即使在 IMM Web 介面階段作業結束後也可以存取。最多只能將一個磁碟機映像儲存在 IMM 卡上。磁碟機或映像內容大小不得大於 1.44 MB。若要上傳磁片映像檔，請完成下列步驟：

1. 按一下 **RDOC**。
2. 新視窗開啓後，按一下 **Upload**。
3. 按一下 **Browse** 以選取您要使用的映像檔。
4. 在 **Name** 欄位中輸入映像的名稱，然後按一下 **OK** 以上傳檔案。

註：若要從記憶體中卸載映像檔，請在 RDOC Setup 視窗選取名稱，然後按一下 **Delete**。

結束 Remote Control

完成使用 Remote Control 特性之後，請關閉 Video Viewer 視窗和 Virtual Media Session 視窗。

設定 PXE 網路開機

若要設定您的伺服器在伺服器下次重新啓動時嘗試「開機前執行環境 (PXE)」網路開機，請完成下列步驟：

1. 登入 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
2. 在導覽窗格中，按一下 **PXE Network Boot**。
3. 選取 **Attempt PXE network boot at next server restart** 勾選框。
4. 按一下 **Save**。

更新韌體

使用導覽窗格中的 Firmware Update 選項，可更新 IMM 韌體、System x 伺服器韌體及 Dynamic System Analysis (DSA) 韌體。

若要更新韌體，請完成下列步驟。

註：IBM 網站會定期進行變更。實際的程序可能與本文件的說明略有不同。

1. 下載其中已安裝 IMM 的伺服器所適用的最新韌體更新：
   a. 請造訪 http://www.ibm.com/systems/support/。
   b. 在 **Product support** 下，按一下 **System x** 或 **BladeCenter**。
   c. 在 **Popular links** 下，按一下 **Software and device drivers**。
   d. 按一下您伺服器的適用鏈結，以顯示可下載檔案矩陣。
   e. 捲動到 IMM、伺服器韌體或 DSA 區域，選取韌體更新的鏈結，並儲存更新檔案。
2. 登入 IMM。如需相關資訊，請參閱第 11 頁的第 2 章, 『開啓和使用 IMM Web 介面』。
3. 在導覽窗格中，按一下 **Firmware Update**。
4. 按一下 **Browse**。
5. 導覽至您要更新的更新套件。

   註：
   a. 當伺服器處於關閉狀態或伺服器正在啓動時，無法更新 System x 伺服器韌體。
   b. 若要確定要使用的韌體檔案類型，請參閱更新套件 Readme 檔。在大部分情況下，IMM 可以使用 EXE 或 BIN 檔案來執行更新。
6. 按一下 **Open**。**Browse** 旁邊的方框中便會顯示該檔案（包括完整路徑）。
7. 若要開始更新程序，請按一下 **Update**。將檔案傳送至 IMM 上的暫時儲存體時會開啓進度指示器。檔案傳送完成後，即會開啓確認視窗。

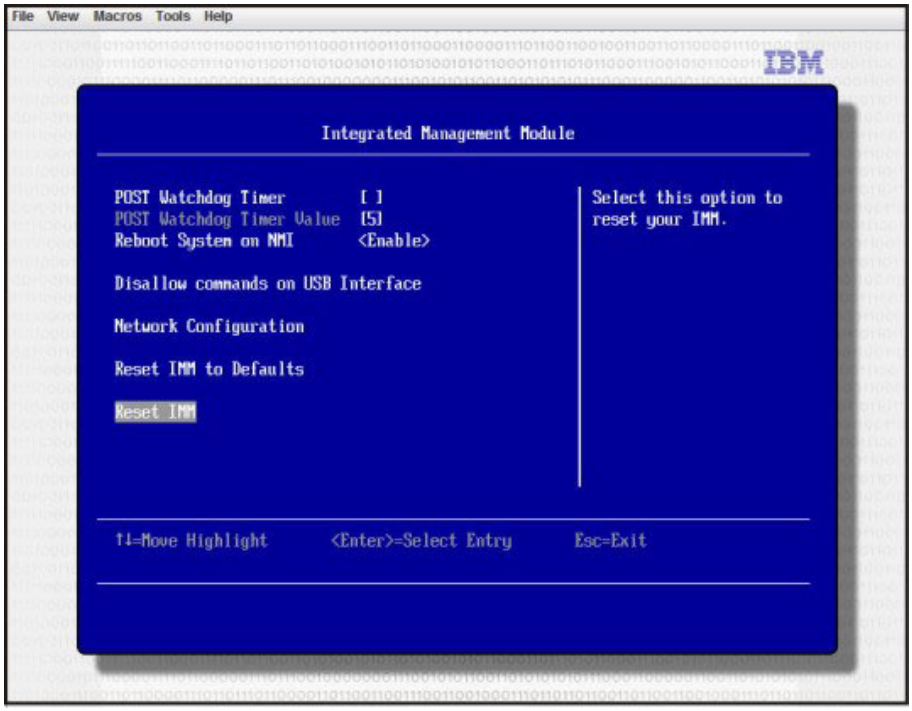
8. 檢查 Confirm Firmware Update 視窗中所顯示的檔案是否就是要更新的檔案。如果不是，請按一下 **Cancel**。
9. 若要完成更新程序，請按一下 **Continue**。更新韌體時會開啓進度指示器。會開啓確認視窗以確認更新是否成功。
10. 如果您是更新 IMM 韌體，請按一下導覽窗格中的 **Restart IMM**，然後按一下 **Restart**。System x 伺服器韌體和 DSA 更新則不需要重新啓動 IMM。這些更新會在伺服器下次啓動後生效。
11. 按一下 **OK** 以確認您想要重新啓動 IMM。
12. 按一下 **OK** 以關閉現行瀏覽器視窗。
13. 在 IMM 重新啓動後，再次登入 IMM 以存取 Web 介面。

使用 Setup Utility 重設 IMM

若要透過 Setup Utility 重設 IMM，請完成下列步驟：

1. 開啓伺服器。

   註：在伺服器接通 AC 電源大約 2 分鐘後，電源控制按鈕就會變成作用中狀態。
2. 當顯示 F1 Setup 提示時，請按 F1 鍵。如果您已設定開機密碼和管理者密碼，您必須輸入管理者密碼，才能存取完整的 Setup Utility 功能表。
3. 從 Setup Utility 主功能表，選取 **System Settings**。
4. 在下一個畫面上，選取 **Integrated Management Module**。
5. 選取 **Reset IMM**。



註：在您重設 IMM 之後，畫現上會立即顯示以下確認訊息：

```
IMM reset command has been sent successfully!! Press ENTER to continue.
```

IMM 重設程序尚未完成。您必須等待大約 4 分鐘的時間以便 IMM 進行重設，之後 IMM 方能再次運作。如果嘗試在伺服器正在重設時存取伺服器韌體資訊，則欄位中會顯示 Unknown，並顯示說明 Error retrieving information from IMM。

管理具有 IMM 和 IBM System x Server Firmware 的工具及公用程式

本章節說明 IMM 和 IBM System x Server Firmware 支援的工具及公用程式。您用於在頻內管理 IMM 的 IBM 工具不需要您安裝裝置驅動程式。然而，如果您選擇在頻內使用某些工具（例如 IPMItool），則必須安裝 OpenIPMI 驅動程式。

IBM 網站提供了用於 IBM 系統管理工具及公用程式的更新項目和下載項目。若要檢查工具和公用程式的更新項目，請完成下列步驟。

註：IBM 網站會定期進行變更。尋找韌體和文件的程序可能與本文件的說明略有不同。

1. 請造訪 http://www.ibm.com/systems/support/。
2. 在 **Product support** 下，按一下 **System x**。
3. 在 **Popular links** 下，按一下 **Utilities**。

使用 IPMItool

IPMItool 提供各種工具，您可以用來管理及配置 IPMI 系統。您可以使用 IPMItool 頻內或頻外來管理和配置 IMM。

如需 IPMItool 的相關資訊，或若要下載 IPMItool，請造訪 http://sourceforge.net/。

使用 OSA System Management Bridge

OSA System Management Bridge (SMBridge) 是一種工具，可用於從遠端管理伺服器。您可以使用該工具，利用 IPMI 1.5 及 Serial over LAN (SOL) 通訊協定來管理伺服器。

如需 SMBridge 的相關資訊，請造訪 http://www-947.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-62198&brandind=5000008，或完成下列步驟：

1. 請造訪 http://www.ibm.com/systems/support/。
2. 按一下 **System x**。
3. 在 **Support & downloads** 下，按一下 **Search**。
4. 在搜尋欄位中鍵入 smbridge，然後按一下 **Search**。
5. 從結果清單中，按一下 **SMBridge Tool Help - Servers** 鏈結。

使用 IBM Advanced Settings Utility

需要 IBM Advanced Settings Utility (ASU) 3.0.0 或更新版本才能管理 IMM。ASU 是一種工具，可用於從多個作業系統平台上的指令行介面中修改韌體設定。它還可讓您發出選取的 IMM 設定指令。您可以使用 ASU 頻內或頻外來管理和配置 IMM。

註：如果已停用 USB 頻內介面 (LAN over USB)，則 ASU 需要安裝 IPMI 裝置驅動程式。

如需 ASU 的相關資訊，請參閱 http://www-947.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-55021&brandind=5000008，或完成下列步驟：

1. 請造訪 http://www.ibm.com/systems/support/。

2. 按一下 **System x**，從 **Product family** 功能表中選取您的伺服器，然後按一下 **Go**。
3. 從 **Refine results** 功能表中選取 **Advanced Settings Utility**，然後按一下 **Go**。
4. 按一下最新版本 ASU 的鏈結。

使用 IBM 快閃記憶體公用程式

快閃記憶體公用程式可讓您更新硬體及伺服器韌體，因此不需要從實體磁片或其他媒體中，手動安裝新的韌體或韌體更新項目。您可以將 IBM 快閃記憶體公用程式用於 IMM、伺服器韌體及 DSA（頻內或頻外）。若要尋找快閃記憶體公用程式，請完成下列步驟：

1. 請造訪 http://www.ibm.com/systems/support/。
2. 在 **Product support** 下，按一下 **System x**。
3. 在搜尋欄位中鍵入 `flash utility`，然後按一下 **Search**。
4. 按一下適用之快閃記憶體公用程式的鏈結。

用於管理 IMM 的其他方法

您可以使用下列使用者介面來管理和配置 IMM：

- IMM Web 介面
- SNMPv1
- SNMPv3
- Telnet CLI
- SSH CLI

第 6 章 LAN over USB

與 BMC 和 Remote Supervisor Adapter II 不同，IMM 不需要 IPMI 裝置驅動程式或 USB 常駐程式，就能進行頻內 IMM 通訊。而是 LAN over USB 介面會啓用與 IMM 的頻內通訊；主機板上的 IMM 硬體會呈現從 IMM 到作業系統的內部乙太網路 NIC。

註：在 IMM Web 介面中，LAN over USB 也稱爲「USB 頻內介面」。

LAN over USB 介面的 IMM IP 位址設定爲靜態位址 169.254.95.118，而子網路遮罩爲 255.255.0.0。唯一例外是多節點系統（例如，x3850 X5 或 x3950 X5）的次要節點中的 IMM，其中 LAN over USB 介面的 IMM 端 IP 位址爲 169.254.96.118。

LAN over USB 介面的潛在衝突

在某些情況下，IMM LAN over USB 介面會與特定網路配置和（或）應用程式發生衝突。例如，Open MPI 會嘗試使用伺服器上的所有可用網路介面。Open MPI 偵測到 IMM LAN over USB 介面，並嘗試使用它與叢集環境中的其他系統進行通訊。LAN over USB 介面是內部介面，因此這個介面不適用於與叢集中的其他系統進行外部通訊。

解決 IMM LAN over USB 介面的衝突

有幾種動作可以解決網路配置和應用程式的 LAN over USB 衝突：

- 如果是與 Open MPI 的衝突，請配置應用程式，使其不要嘗試使用此介面。
- 關閉介面（在 Linux 下執行 `ifdown`）。
- 移除裝置驅動程式（在 Linux 下執行 `rmmod`）。
- 透過下列其中一種方法，停用 IMM 上的 USB 頻內介面。

  重要事項：如果您停用 USB 頻內介面，則無法使用 Linux 或 Windows 快閃記憶體公用程式來執行 IMM 韌體的頻內更新。如果 USB 頻內介面已停用，則請使用 IMM Web 介面上的 Firmware Update 選項來更新韌體。如需相關資訊，請參閱第 109 頁的『更新韌體』。

  如果您停用 USB 頻內介面，也請停用監視器逾時，防止伺服器非預期地重新啓動。如需停用監視器的相關資訊，請參閱第 18 頁的『設定伺服器逾時』。

  – 若要從 IMM Web 介面停用 LAN over USB 介面，請參閱第 21 頁的『停用 USB 頻內介面』。
  – 若要從進階管理模組 Web 介面停用 LAN over USB 介面，請完成下列步驟：
    1. 登入進階管理模組 Web 介面。
    2. 在導覽窗格中，按一下 **Blade Tasks** 標題下的 **Blade Configuration**。
    3. 在 Blade Configuration 網頁上，向下捲動到服務處理器 LAN over USB 介面。此區段會列出機箱中可以啓用和停用 LAN over USB 介面的所有刀鋒伺服器。
    4. 選取您要啓用或停用之刀鋒伺服器旁邊的勾選框。
    5. 按一下 **Disable** 即可停用所選取刀鋒伺服器上的 LAN over USB 介面。

手動配置 LAN over USB 介面

爲讓 IMM 使用 LAN over USB 介面，如果自動設定失敗，或您偏好手動設定 LAN over USB，您可能需要完成其他配置作業。韌體更新項目套件或 Advanced Settings Utility (ASU) 會嘗試自動執行設定。如需不同作業系統上 LAN over USB 配置的相關資訊，請參閱 IBM 網站上的 IBM 白皮書 *Transitioning to UEFI and IMM*。

安裝裝置驅動程式

爲讓 IMM 使用 LAN over USB 介面，您可能需要安裝作業系統驅動程式。如果自動設定失敗或您偏好手動設定 LAN over USB，則請使用下列其中一個程序。如需不同作業系統上 LAN over USB 配置的相關資訊，請參閱 IBM 網站上的 IBM 白皮書 *Transitioning to UEFI and IMM*。

安裝 Windows IPMI 裝置驅動程式

Microsoft Windows Server 2003 R2 作業系統預設不會安裝 Microsoft IPMI 裝置驅動程式。若要安裝 Microsoft IPMI 裝置驅動程式，請完成下列步驟：

1. 從 Windows 桌面，按一下**開始 > 控制台 > 新增或移除程式**。
2. 按一下**新增/移除 Windows 元件**。
3. 從元件清單中，選取 **Management and Monitoring Tools**，然後按一下**詳細資料**。
4. 選取**硬體管理**。
5. 按**下一步**。隨即開啓安裝精靈，並引導您完成安裝。

   註：可能需要 Windows 安裝 CD。

安裝 LAN over USB Windows 裝置驅動程式

安裝 Windows 時，「裝置管理員」中會顯示不明的 RNDIS 裝置。您必須安裝用於識別此裝置的 Windows INF 檔案，Windows 作業系統需要此檔案才能偵測和使用 LAN over USB 功能。所有 Windows 版本的 IMM、UEFI 和 DSA 更新套件都會包括簽署的 INF 版本。此檔案只需要安裝一次。若要安裝 Windows INF 檔案，請完成下列步驟：

1. 取得 Windows 版本的 IMM、伺服器韌體或 DSA 更新套件（如需相關資訊，請參閱第 109 頁的『更新韌體』）。
2. 從韌體更新項目套件解壓縮 `ibm_rndis_server_os.inf` 和 `device.cat` 檔案，並將它們複製至 `\WINDOWS\inf` 子目錄。
3. **對於 Windows 2003**：用滑鼠右鍵按一下 `ibm_rndis_server_os.inf` 檔案，並選取**安裝**以安裝該檔案。這樣會在 `\WINDOWS\inf` 中產生同名的 PNF 檔案。 **對於 Windows 2008**：依序移至**電腦管理**和**裝置管理員**，並找到 RNDIS Device。請選取**內容 > 驅動程式 > 重新安裝驅動程式**。將伺服器指向 `\Windows\inf` 目錄（可在其中找到 `ibm_rndis_server_os.inf` 檔案），並安裝裝置。
4. 依序移至**電腦管理**和**裝置管理員**，用滑鼠右鍵按一下**網路介面卡**，然後選取**硬體變更掃描**。畫面上會出現一則訊息，確認已找到並安裝乙太網路裝置。「新增硬體精靈」會自動啓動。
5. 向您提示 `Windows 是否可以連線到 Windows Update 尋找軟體?` 時，按一下**不，現在不要**。請按**下一步**繼續。

6. 向您提示您要精靈執行什麼工作? 時，按一下**從清單或特定位置安裝 (進階)**。請按**下一步**繼續。
7. 向您提示請選擇您的搜尋和安裝選項時，按一下**不要搜尋，我將選擇要安裝的驅動程式**。請按**下一步**繼續。
8. 向您提示選取硬體類型並按 [下一步] 時，按一下**網路介面卡**。請按**下一步**繼續。
9. 向您提示完成尋找新增硬體精靈時，按一下**完成**。

   註：畫面上會出現新的區域連線，而且可能會指出這個連線有限制或沒有連線功能。請略過此訊息。
10. 回到「裝置管理員」。確認**網路介面卡**下方出現 **IBM USB Remote NDIS Network Device**。
11. 開啓命令提示字元，並鍵入 `ipconfig`，然後按 Enter 鍵。畫面上會顯示 IBM USB RNDIS 的區域連線，而其 IP 位址位於 169.254.*xxx.xxx* 範圍內，且子網路遮罩設爲 255.255.0.0。

安裝 LAN over USB Linux 裝置驅動程式

現行 Linux 版本（例如 RHEL5 Update 2 和 SLES10 Service Pack 2）預設支援 LAN over USB 介面。在安裝這些作業系統期間，會偵測並顯示此介面。當您配置裝置時，請使用靜態 IP 位址 169.254.95.130，而其子網路遮罩爲 255.255.0.0。

註：舊的 Linux 發行套件可能會偵測不到 LAN over USB 介面，可能需要手動配置。如需在特定 Linux 發行套件上配置 LAN over USB 的相關資訊，請參閱 IBM 網站上的 IBM 白皮書 *Transitioning to UEFI and IMM*。

IMM LAN over USB 介面需要載入 `usbnet` 和 `cdc_ether` 裝置驅動程式。如果尚未安裝這些裝置驅動程式，請使用 modprobe 指令來進行安裝。安裝這些裝置驅動程式後，IMM USB 網路介面會在作業系統中顯示爲網路裝置。若要探索作業系統已指派給 IMM USB 網路介面的名稱，請鍵入：

```
dmesg | grep -i cdc ether
```

使用 ifconfig 指令將該介面配置成使用 169.254.*xxx.xxx* 範圍內的 IP 位址。例如：

```
ifconfig IMM_device_name 169.254.1.102 netmask 255.255.0.0
```

每次啓動作業系統時，都會將此介面配置成使用 169.254.*xxx.xxx* 範圍內的 IP 位址。

第 7 章 指令行介面

使用 IMM 指令行介面 (CLI) 可存取 IMM，而無需使用 Web 介面。它提供 Web 介面提供的管理功能的子集。

您可以透過 Telnet 或 SSH 階段作業存取 CLI。您必須先由 IMM 進行鑑別，然後才能發出任何 CLI 指令。

管理具有 IPMI 的 IMM

IMM 隨附使用者 ID 2，最初設定的使用者名稱和密碼分別爲 USERID 和 PASSW0RD（當中所含的是數字 0，不是字母 O）。此使用者具有 Supervisor 存取權。

重要事項：請在起始配置期間變更此預設密碼，以獲得加強安全性。

此外，IMM 還提供下列 IPMI 遠端伺服器管理功能：

指令行介面

指令行介面透過 IPMI 2.0 通訊協定，提供對伺服器管理功能的直接存取。您可以使用 SMBridge 或 IPMItool 發出指令，以控制伺服器電源、檢視伺服器資訊及識別伺服器。您也可以使用 SMBridge 將一個以上的指令儲存爲文字檔，並以 Script 形式執行該檔案。如需 IPMItool 的相關資訊，請參閱第 111 頁的『使用 IPMItool』。如需 SMBridge 的相關資訊，請參閱第 111 頁的『使用 OSA System Management Bridge』。

Serial over LAN

若要從遠端位置管理伺服器，請使用 SMBridge 或 IPMItool 來建立 Serial over LAN (SOL) 連線。如需 IPMItool 的相關資訊，請參閱第 111 頁的『使用 IPMItool』。如需 SMBridge 的相關資訊，請參閱第 111 頁的『使用 OSA System Management Bridge』。

存取指令行

若要存取指令行，請將 Telnet 或 SSH 階段作業啓動至 IMM IP 位址（如需相關資訊，請參閱第 31 頁的『配置 serial-to-Telnet 或 SSH 重新導向』）。

登入指令行階段作業

若要登入指令行，請完成下列步驟：

1. 與 IMM 建立連線。
2. 在使用者名稱提示處鍵入使用者 ID。
3. 在密碼提示處，鍵入您登入 IMM 所使用的密碼。

   您即已登入指令行。指令行提示爲 `system>`。指令行階段作業會繼續進行，直到您在指令行中鍵入 `exit` 爲止。隨後您將被登出，並結束階段作業。

指令語法

在使用指令之前，請先閱讀下列準則：

- 每一個指令具有下列格式：

  ```
  command [arguments] [-options]
  ```

- 指令語法區分大小寫。
- 指令名稱都是小寫。
- 所有引數都必須緊接在指令後面。選項緊接在引數後面。
- 每一個選項前面一律有連字號 (-)。選項可以是短選項（單一字母）或長選項（多個字母）。
- 如果選項具有引數，則引數是必要的，例如：

  ```
  ifconfig eth0 -i 192.168.70.34 -g 192.168.70.29 -s 255.255.255.0
  ```

  其中 **ifconfig** 是指令，eth0 是引數，-i、-g 和 -s 是選項。在此範例中，這三個選項都具有引數。
- 方括弧（[ ]）指示引數或選項是可選的。方括弧（[ ]）不是您鍵入的指令的一部分。

特性和限制

CLI 具有下列特性和限制：

- 容許使用不同的存取方法（Telnet 或 SSH）進行多個並行 CLI 階段作業。在大部分情況下，兩個 Telnet 指令行階段作業隨時可以處於作用中狀態。

  註：Telnet 階段作業數目是可配置的；有效值爲 0、1 及 2。值 0 表示停用 Telnet 介面。
- 每行容許一個指令（160 個字元限制，包括空格）。
- 執行時間較長的指令沒有接續字元。唯一的編輯功能是倒退鍵，可消除您剛鍵入的字元。
- 可以使用上移鍵和下移鍵來瀏覽最後八個指令。**history** 指令顯示最後八個指令的清單，然後您可以將其用作執行指令的快速鍵，如在下列範例：

  ```
  system> history
   0 ifconfig eth0
   1 readlog
   2 readlog
   3 readlog
   4 history
  system> !0
  -state enabled
  -c dthens
  -i 192.168.70.125
  -g 0.0.0.0
  -s 255.255.255.0
  -n IMMA00096B9E003A
  -r auto
  -d auto
  -m 1500
  -b 00:09:6B:9E:00:3A
  -l 00:00:00:00:00:00
  system>
  ```

- 在指令行介面中，輸出緩衝區限制爲 2 KB。沒有緩衝。個別指令的輸出不能超出 2048 個字元。此限制不適用於序列重新導向模式（在序列重新導向期間緩衝資料）。

- 在完成執行指令之後，畫面上會顯示指令的輸出。這會導致指令無法報告即時執行狀態。例如，在 **flashing** 指令的詳細模式中，不會即時顯示閃動進度。它會在指令完成執行之後顯示。
- 簡式文字訊息用於表示指令執行狀態，如在下列範例中：

```
system> power on
ok
system> power state
Power: On
State: System power off/State unknown
system>
```

- 指令語法區分大小寫。
- 選項及其引數之間必須至少具有一個空格。例如， `ifconfig eth0 -i192.168.70.133` 是不正確的語法。正確的語法是 `ifconfig eth0 -i 192.168.70.133`。
- 所有指令都具有 `-h`、`-help` 和 `?` 選項，這些選項提供了語法說明。下列所有範例都提供相同的結果：

```
system> power -h
system> power -help
system> power ?
```

- 接下來的章節所述的部分指令可能無法使用。若要查看支援的指令清單，請使用 help 或 ? 選項，如下列範例所示：

```
system> help
system> ?
```

公用程式指令

公用程式指令如下：

- exit
- help
- history

exit 指令

使用 **exit** 指令可登出並結束指令行介面階段作業。

help 指令

使用 **help** 指令可顯示包含每個指令簡要說明的所有指令清單。您也可以在命令提示字元中鍵入 `?`。

history 指令

使用 **history** 指令可顯示已發出的最後八個指令的索引歷程清單。然後即可將這些索引用作捷徑（前面帶有 !），以從此歷程清單重新發出這些指令。

範例：

```
system> history
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
system> ifconfig eth0
-state enabled
```

```
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n IMMA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system>
```

監視指令

監視指令如下：

- clearlog
- fans
- readlog
- syshealth
- temps
- volts
- vpd

clearlog 指令

使用 **clearlog** 指令可清除 IMM 的事件日誌。您必須具有清除事件日誌的權限才能使用此指令。

fans 指令

使用 **fans** 指令可顯示每個伺服器風扇的速度。

範例：

```
system> fans
fan1 75%
fan2 80%
fan3 90%
system>
```

readlog 指令

使用 **readlog** 指令可顯示 IMM 事件日誌項目（每次五個）。這些項目將按從最新到最舊的順序顯示。

readlog 會在其第一次執行時顯示事件日誌中的前五個項目（從最新項目開始），後續每次呼叫時則會顯示下五個項目。

readlog -f 會重設計數器並顯示事件日誌中的前 5 個項目（從最新項目開始）。

語法：

```
readlog [options]
options:
-f
```

範例：

```
system> readlog -f
1 I SERVPROC 12/18/03 10:18:58 Remote Login Successful.
Login ID:''USERID' CLI authenticated from 192.168.70.231 (Telnet).'
2 I SERVPROC 12/18/03 10:12:22 Remote Login successful.
Login ID: ''USERID' from web browser at IP@=192.168.70.231'
3 E SERVPROC 12/18/03 10:10:37 Failure reading I2C device.
4 E SERVPROC 12/18/03 10:10:37 Environmental monitor not responding.
5 E SERVPROC 12/18/03 10:10:37 Failure reading I2C device.
system> readlog
6 E SERVPROC 12/18/03 10:09:31 Fan 2 Fault. Multiple fan failures
7 E SERVPROC 12/18/03 10:09:31 Fan 1 Fault. Single fan failure
8 I SERVPROC 12/18/03 10:09:25 Ethernet[0] Link Established at 100Mb, Full Duplex.
9 I SERVPROC 12/18/03 10:09:24 Ethernet[0] configured to do Auto Speed/Auto Duplex.
10 I SERVPROC 12/18/03 10:09:24 Ethernet[0] MAC Address currently
being used: 0x00-09-6B-CA-0C-80
system>
```

syshealth 指令

使用 **syshealth** 指令可顯示伺服器性能的摘要。將會顯示電源狀態、系統狀態、重新啓動計數及 IMM 軟體狀態。

範例：

```
system> syshealth
Power On
State System on/starting UEFI
Restarts 71
system>
```

temps 指令

使用 **temps** 指令可顯示所有溫度和溫度臨界值。這組溫度與 Web 介面中顯示的相同。

範例：

```
system> temps
Temperatures are displayed in degrees Fahrenheit/Celsius
        WR      W       T     SS     HS
---------------------------------------
CPU1   65/18  72/22  80/27  85/29  90/32
CPU2   58/14  72/22  80/27  85/29  9/320
DASD1  66/19  73/23  82/28  88/31  9/332
Amb    59/15  70/21  83/28  90/32  9/355
system>
```

注意事項：

1. 此輸出具有下列直欄標題：
   - WR：警告重設
   - W：警告
   - T：溫度（現行值）
   - SS：非強迫關機
   - HS：強迫關機
2. 所有溫度值均以華氏度/攝氏度爲單位。

volts 指令

使用 **volts** 指令可顯示所有電壓和電壓臨界值。這組電壓與 Web 介面中顯示的相同。

範例：

```
system> volts
      HSL   SSL   WL    WRL   V     WRH   WH   SSH    HSH
-------------------------------------------------------------
5v    5.02  4.00  4.15  4.50  4.60  5.25  5.50  5.75  6.00
3.3v  3.35  2.80  2.95  3.05  3.10  3.50  3.65  3.70  3.85
12v   12.25 11.10 11.30 11.50 11.85 12.15 12.25 12.40 12.65
-5v   -5.10 -5.85 -5.65 -5.40 -5.20 -4.85 -4.65 -4.40 -4.20
-3.3v -3.35 -4.10 -3.95 -3.65 -3.50 -3.10 -2.95 -2.80 -2.70
VRM1                        3.45
VRM2                        5.45
system>
```

註：此輸出具有下列直欄標題：

HSL：強迫關機（低）

SSL：非強迫關機（低）

WL：警告（低）

WRL：警告重設（低）

V：電壓（現行值）

WRH：警告重設（高）

WH：警告（高）

SSH：非強迫關機（高）

HSH：強迫關機（高）

vpd 指令

使用 **vpd** 指令可顯示系統 (sys)、IMM、伺服器韌體 (bios) 及 Dynamic System Analysis Preboot (dsa) 的重要產品資料。此資訊與 Web 介面中顯示的相同。

語法：

```
vpd sys
vpd IMM
vpd biosvpd dsa
```

範例：

```
system> vpd dsa
Type     Version      ReleaseDate
----     -------      -----------
dsa      D6YT19AUS    02/27/2009
system>
```

伺服器電源和重新啓動控制指令

伺服器電源和重新啓動指令如下：

- power
- reset

power 指令

使用 **power** 指令可控制伺服器電源。若要發出 **power** 指令，您必須具有電源和重新啓動存取權。

power on 用於開啓伺服器電源。

power off 用於關閉伺服器電源。**-s** 選項用於在關閉伺服器之前關閉作業系統。

power state 用於顯示伺服器電源狀態（on 或 off）和伺服器的現行狀態。

power cycle 用於在關閉伺服器電源後關閉電源。**-s** 選項用於在關閉伺服器之前關閉作業系統。

語法：

```
power on
power off [-s]
power state
power cycle [-s]
```

reset 指令

使用 **reset** 指令可重新啓動伺服器。若要使用此指令，您必須具有電源和重新啓動存取權。 **-s** 選項用於在重新啓動伺服器之前關閉作業系統。

語法：

```
reset [option]
option:
-s
```

序列重新導向指令

具有一個序列重新導向指令：主控台。

console 指令

使用 **console** 指令可啓動 IMM 指定序列埠的序列重新導向主控台階段作業。

語法：

```
console 1
```

配置指令

配置指令如下：

- dhcpinfo
- dns
- gprofile
- ifconfig
- ldap
- ntp
- passwordcfg
- portcfg
- slp
- srcfg
- ssl
- tcpcmdmode
- timeouts
- usbeth

- users

dhcpinfo 指令

使用 **dhcpinfo** 指令可檢視 DHCP 伺服器爲 eth0（如果此介面是由 DHCP 伺服器自動配置）指派的 IP 配置。您可以使用 **ifconfig** 指令來啓用或停用 DHCP。

語法：

```
dhcpinfo eth0
```

範例：

```
system> dhcpinfo eth0

-server : 192.168.70.29
-n     : IMMA-00096B9E003A
-i     : 192.168.70.202
-g     : 192.168.70.29
-s     : 255.255.255.0
-d     : linux-sp.raleigh.ibm.com
-dns1   : 192.168.70.29
-dns2   : 0.0.0.0
-dns3   : 0.0.0.0
-i6    : 0::0
-d6    : *
-dns61  : 0::0
-dns62  : 0::0
-dns63  : 0::0
system>
```

下表說明此範例的輸出。

選項	說明
-server	指派配置的 DHCP 伺服器
-n	指派的主機名稱
-i	指派的 IPv4 位址
-g	指派的閘道位址
-s	指派的子網路遮罩
-d	指派的網域名稱
-dns1	主要 IPv4 DNS 伺服器 IP 位址
-dns2	次要 IPv4 DNS IP 位址
-dns3	第三層 IPv4 DNS 伺服器 IP 位址
-i6	IPv6 位址
-d6	IPv6 網域名稱
-dns61	主要 IPv6 DNS 伺服器 IP 位址
-dns62	次要 IPv6 DNS IP 位址
-dns63	第三層 IPv6 DNS 伺服器 IP 位址

dns 指令

使用 **dns** 指令可檢視 IMM 的 DNS 配置。

語法：

```
dns
```

註：下列範例顯示已啓用 DNS 的 IMM 配置。

範例：

```
system> dns
-state  : enabled
-i1     : 192.168.70.202
-i2     : 192.168.70.208
-i3     : 192.168.70.212
-i61    : fe80::21a:64ff:fee6:4d5
-i62    : fe80::21a:64ff:fee6:4d6
-i63    : fe80::21a:64ff:fee6:4d7
-ddns   : enabled
-dnsrc  : dhcp
-p     : ipv6

system>
```

下表說明此範例的輸出。

選項	說明
-state	DNS 的狀態（enabled 或 disabled）
-i1	主要 IPv4 DNS 伺服器 IP 位址
-i2	次要 IPv4 DNS IP 位址
-i3	第三層 IPv4 DNS 伺服器 IP 位址
-i61	主要 IPv6 DNS 伺服器 IP 位址
-i62	次要 IPv6 DNS IP 位址
-i63	第三層 IPv6 DNS 伺服器 IP 位址
-ddns	DDNS 的狀態（enabled 或 disabled）
-dnsrc	偏好的 DDNS 網域名稱（dhcp 或 manual）
-p	偏好的 DNS 伺服器（ipv4 或 ipv6）

gprofile 指令

使用 **gprofile** 指令可顯示和配置 IMM 的群組設定檔。

下表顯示各選項的引數。

選項	說明	值
-clear	刪除群組	Enabled、disabled
-n	群組名稱	*group_name* 的最多 63 個字元的字串。*group_name* 必須是唯一的。
-a	角色型安全（權限）層次	Supervisor、operator、rbs <role list>: nsluam|rca|rcrda|rpr|bac|cel|aac 角色清單值是使用以垂直線區隔的值清單來指定。
-h	顯示指令用法和選項	

語法：

```
gprofile [1 - 16] [options]
options:
-clear state
-n  group_name
-a  security level:
    -ns network and security
    -uam user account management
    -rca remote console access
    -rcrda remote console and remote disk access
    -rpr remote server power/restart access
    -bac basic adapter configuration
    -ce ability to clear event logs
    -aac advanced adapter configuration
-h
```

ifconfig 指令

使用 **ifconfig** 指令可配置乙太網路介面。鍵入 `ifconfig eth0` 可顯示現行乙太網路介面配置。若要變更乙太網路介面配置，請依次鍵入選項和值。若要變更介面配置，您必須至少具有 Adapter Networking and Security Configuration 權限。

下表顯示各選項的引數。

選項	說明	值
-state	介面狀態	disabled、enabled
-c	配置方法	dhcp、static、dthens（dthens 對應於 Web 介面上的 **try dhcp server, if it fails use static config** 選項）
-i	靜態 IP 位址	有效格式的位址
-g	閘道位址	有效格式的位址
-s	子網路遮罩	有效格式的位址
-n	主機名稱	最多 63 個字元的字串。字串可以包括字母、數字、句點、底線及連字號。
-dn	網域名稱	有效格式的網域名稱
-ipv6	IPv6 狀態	disabled、enabled
-lla	鏈結本端位址 **註**：僅在啓用 IPv6 時才會出現鏈結本端位址。	鏈結本端位址由 IMM 決定。此值是唯讀且不可配置。
-ipv6static	靜態 IPv6 狀態	disabled、enabled
-i6	靜態 IP 位址	乙太網路通道 0 的 IPv6 格式靜態 IP 位址
-p6	位址字首長度	介於 1 與 128 之間的數字
-g6	閘道或預設路由	乙太網路通道 0 的 IPv6 格式閘道或預設路由 IP 位址
-dhcp6	DHCPv6 狀態	disabled、enabled
-sa6	IPv6 Stateless 自動配置狀態	disabled、enabled
-address_table	自動產生的 IPv6 位址及其字首長度表格 **註**：僅在啓用 IPv6 和 Stateless 自動配置時，此選項才可見。	此值是唯讀且不可配置

選項	說明	值
-auto	決定是否可配置資料傳送速率和雙工網路設定的自動協調設定	true、false
-r	資料傳送速率	10、100、auto
-d	雙工模式	full、half、auto
-m	MTU	介於 60 與 1500 之間的數字
-l	LAA	MAC 位址格式。不容許多重播送位址（第一個位元組必須爲偶數）。

語法：

```
ifconfig eth0 [options]
options:
-state interface_state
-c config_method
-i static_ip_address
-g gateway_address
-s subnet_mask
-n hostname
-r data_rate
-d duplex_mode
-m max_transmission_unit
-l locally_administered_MAC
```

範例：

```
system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n IMMA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system> ifconfig eth0 -c static -i 192.168.70.133
These configuration changes will become active after the next reset of the IMM.
system>
```

註：ifconfig 顯示畫面中的 **-b** 選項用於燒錄 MAC 位址。燒錄 MAC 位址是唯讀且不可配置。

ldap 指令

使用 **ldap** 指令可顯示和配置 LDAP 通訊協定配置參數。

下表顯示各選項的引數。

選項	說明	值
-aom	僅限鑑別模式	Enabled、disabled
-a	使用者鑑別方法	僅限本端、僅限 LDAP、先本端後 LDAP、先 LDAP 後本端

選項	說明	值
-b	連結方法	使用匿名連結、使用用戶端 DN 和密碼連結以及使用登入認證連結
-c	用戶端識別名稱	*client_dn* 的最多 63 個字元的字串
-fn	樹系名稱	Active Directory 環境，*forest_name* 的最多 127 個字元的字串
-d	搜尋網域	*search_domain* 的最多 31 個字元的字串
-f	群組過濾器	*group_filter* 的最多 63 個字元的字串
-g	群組搜尋屬性	*group_search_attr* 的最多 63 個字元的字串
-l	登入權限屬性	*string* 的最多 63 個字元的字串
-p	用戶端密碼	*client_pw* 的最多 15 個字元的字串
-pc	確認用戶端密碼	*confirm_pw* 的最多 15 個字元的字串 指令用法：ldap -p *client_pw* -pc *confirm_pw* 變更用戶端密碼時需要此選項。它會比較 *confirm_pw* 引數與 *client_pw* 引數，如果它們不相符，此指令將會失敗。
-r	根項目識別名稱 (DN)	*root_dn* 的最多 63 個字元的字串
-rbs	Active Directory 使用者的加強角色型安全	Enabled、disabled
s1ip	伺服器 1 的主機名稱/IP 位址	*host name/ip_addr* 的最多 63 個字元的字串或是 IP 位址
s2ip	伺服器 2 的主機名稱/IP 位址	*host name/ip_addr* 的最多 63 個字元的字串或是 IP 位址
s3ip	伺服器 3 的主機名稱/IP 位址	*host name/ip_addr* 的最多 63 個字元的字串或是 IP 位址
-s4ip	伺服器 4 的主機名稱/IP 位址	*host name/ip_addr* 的最多 63 個字元的字串或是 IP 位址
s1pn	伺服器 1 的埠號	*port_number* 的最多 5 位數的數字埠號。
s2pn	伺服器 2 的埠號	*port_number* 的最多 5 位數的數字埠號。
s3pn	伺服器 3 的埠號	*port_number* 的最多 5 位數的數字埠號
s4pn	伺服器 4 的埠號	*port_number* 的最多 5 位數的數字埠號
-t	伺服器目標名稱	啓用 -rbs 選項時，此欄位將指定可透過「角色型安全嵌入式管理單元」與 Active Directory 伺服器中一個以上角色相關聯的目標名稱。
-u	UID 搜尋屬性	*search_attrib* 的最多 23 個字元的字串
-v	透過 DNS 取得 LDAP 伺服器位址	Off、on
-h	顯示指令用法和選項	

語法：

```
ldap [options]
options:
   -aom enabled|disabled|
   -a loc|ldap|locId|ldloc
   -b anon|client|login
```

```
-c client_dn
-d search_domain
-fn forest_name
-f group_filter
-g group_search_attr
-l string
-p client_pw
-pc confirm_pw
-r root_dn
-rbs enabled|disabled
-s1ip host name/ip_addr
-s2ip host name/ip_addr
-s3ip host name/ip_addr
-s4ip host name/ip_addr
-s1pn port_number
-s2pn port_number
-s3pn port_number
-s4pn port_number
-t name
-u search_attrib
-v off|on
-h
```

ntp 指令

使用 **ntp** 指令可顯示和配置「網路時間通訊協定 (NTP)」。

下表顯示各選項的引數。

選項	說明	值
-en	啓用或停用「網路時間通訊協定」	Enabled、disabled
-i	「網路時間通訊協定」伺服器的名稱或 IP 位址	用於時鐘同步化的 NTP 伺服器名稱。
-f	IMM 時鐘與「網路時間通訊協定」伺服器同步化的頻率（分鐘）	3 - 1440 分鐘
-synch	要求與「網路時間通訊協定」伺服器立即同步化	沒有任何值與此參數搭配使用。

語法：

```
ntp [options]
options:
-en state
-i  hostname
-f  frequency
-synch
```

範例：

```
system> ntp
-en: disabled
-f: 3 minutes
-i: not set
```

passwordcfg 指令

使用 **passwordcfg** 指令可顯示和配置密碼參數。

選項	說明
-legacy	將帳戶安全設定爲預先定義的舊式預設值集
-high	將帳戶安全設定爲預先定義的高預設值集
-exp	密碼經歷時間上限（0 - 365 天）。若無有效期限，請設定爲 0。
-cnt	前一個密碼不得重複使用的次數 (0 - 5)
-nul	容許沒有密碼的帳戶 (yes | no)
-h	顯示指令用法和選項

語法：

```
passwordcfg [options]
options: {-high}|{-legacy}|{-exp|-cnt|-nul}
-legacy
-high
-exp:
-cnt:
-nul:
-h
```

範例：

```
system> passwordcfg
Security Level: Legacy
system> passwordcfg -exp 365
ok
system> passwordcfg -nul yes
ok
system> passwordcfg -cnt 5
ok
system> passwordcfg
Security Level: Customize
-exp: 365
-cnt: 5
-nul: allowed
```

portcfg 指令

使用 **portcfg** 指令可配置序列埠。若要變更序列埠配置，請依次鍵入選項和值。若要變更序列埠配置，您必須至少具有 Adapter Networking and Security Configuration 權限。

下列參數設定於硬體中且無法變更：

- 8 個資料位元
- 無同位檢查
- 1 個停止位元

下表顯示各選項的引數。

選項	說明	值
-b	傳輸速率	9600、19200、38400、57600、115200、230400

選項	說明	值
-climode	CLI 模式	none、cliems、cliuser • none：停用指令行介面 • cliems：使用 EMS 相容按鍵順序來啓用指令行介面 • cliuser：利用使用者定義的按鍵順序來啓用指令行介面

語法：

```
portcfg [options]
portcfg [options]
options:
-b baud_rate
-climode cli_mode
-cliauth cli_auth
```

範例：

```
system> portcfg
-b       : 115200
-climode : 2 (CLI with user defined keystroke sequences) system>
system>
```

portcontrol 指令

使用 **portcontrol** 指令可配置 IMM 服務的埠狀態。若要變更埠狀態，請依次鍵入選項和值。若要變更埠的控制狀態，您必須至少具有 Adapter Networking and Security Configuration 的權限。

下表顯示各選項的引數。

選項	說明	值
-ipmi	IPMI 埠	on、off

語法：

```
portcontrol [options]
options:
-ipmi status
```

範例：

```
system> portcontrol
-ipmi: on
```

srcfg 指令

使用 **srcfg** 指令可配置序列重新導向。鍵入 srcfg 可顯示現行配置。若要變更序列重新導向配置，請依次鍵入選項和值。若要變更序列重新導向配置，您必須至少具有 Adapter Networking and Security Configuration 權限。

下表顯示 -exitcliseq 選項的引數。

選項	說明	值
-exitcliseq	結束指令行介面按鍵順序	用於結束 CLI 的使用者定義的按鍵順序。如需詳細資料，請參閱此表格中 -entercliseq 選項的值。

語法：

```
srcfg [options]
options:
-exitcliseq exitcli_keyseq
```

範例：

```
system> srcfg
-exitcliseq ^[Q
system>
```

ssl 指令

使用 **ssl** 指令可顯示和配置 Secure Sockets Layer (SSL) 參數。

註： 必須先安裝用戶端憑證，然後才能啓用 SSL 用戶端。

選項	說明
-ce	啓用或停用 SSL 用戶端
-se	啓用或停用 SSL 伺服器
-h	列出用法和選項

語法：

```
ssl [options]
options:
-ce on | off
-se on | off
-h
```

參數：下列參數會呈現在 **ssl** 指令的選項狀態顯示畫面中，並且是僅來自指令行介面的輸出：

Server secure transport enable
此狀態顯示是唯讀且無法直接設定。

Server Web/CMD key status
此狀態顯示是唯讀且無法直接設定。可能的指令行輸出值如下：

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

SSL server CSR key status
此狀態顯示是唯讀且無法直接設定。可能的指令行輸出值如下：

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

SSL client LDAP key status

此狀態顯示是唯讀且無法直接設定。可能的指令行輸出值如下：

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

SSL client CSR key status

此狀態顯示是唯讀且無法直接設定。可能的指令行輸出值如下：

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

timeouts 指令

使用 **timeouts** 指令可顯示或變更逾時值。若要顯示逾時，請鍵入 timeouts。若要變更逾時值，請依次鍵入選項和值。若要變更逾時值，您必須至少具有 Adapter Configuration 權限。

下表顯示逾時值的引數。這些值符合 Web 介面上伺服器逾時的分度標下拉選項。

選項	逾時	單位	值
-o	作業系統逾時	分鐘	disabled、2.5、3、3.5、4
-l	載入器逾時	分鐘	d i s - abled、0.5、1、1.5、2、2.5、3、3.5、4、4.5、5、7.5、10、15、20、30、60、120

語法：

```
timeouts [options]
options:
-o OS_watchdog_option
-l loader_watchdog_option
```

範例：

```
system> timeouts
-o disabled
-l 3.5
system> timeouts -o 2.5
ok
system> timeouts
-o 2.5
-l 3.5
```

usbeth 指令

使用 **usbeth** 指令可啓用或停用頻內 LAN over USB 介面。如需啓用或停用此介面的相關資訊，請參閱第 21 頁的『停用 USB 頻內介面』。

語法：

```
usbeth [options]
options:
-en <enabled|disabled>
```

範例：

```
system>usbeth
-en : disabled
system>usbeth -en enabled
ok
system>usbeth
-en : disabled
```

users 指令

使用 **users** 指令可存取所有使用者帳戶及其權限層級，並可建立新的使用者帳戶和修改現有帳戶。

請閱讀有關 **users** 指令的下列準則：

- 使用者數目必須在 1（含）至 12（含）之間。
- 使用者名稱必須少於 16 個字元，且只能包含數字、字母、句點及底線。
- 密碼長度必須大於 5 個字元且小於 16 個字元，並且必須至少包含一個英文字母字元和一個非英文字母字元。
- 權限層級可以是下列其中一個層級：
  - super (supervisor)
  - ro (read only)
  - 下列值的任意組合（以 | 區隔）：

    am (User account management access)

    rca (Remote console access)

    rcvma (Remote console and virtual media access)

    pr (Remote server power/restart access)

    cel (Ability to clear event logs)

    bc (Adapter configuration [basic])

    nsc (Adapter configuration [network and security])

    ac (Adapter configuration [advanced])

語法：

```
users [options]
options:
-user number
-n username
-p password
-a authority level
```

範例：

```
system> users
1. USERID Read/Write
Password Expires: no expiration
2. manu Read Only
Password Expires: no expiration
3. eliflippen Read Only
```

```
Password Expires: no expiration
4.  <not used>
5. jacobyackenovic custom:cel|ac
Password Expires: no expiration
system> users -7 -n sptest -p PASSW0RD -a custom:am|rca|cel|nsc|ac
ok
system> users
1. USERID  Read/Write
Password Expires: no expiration
2. test    Read/Write
Password Expires: no expiration
3. test2   Read/Write
Password Expires: no expiration
4. <not used>
5. jacobyackenovic custom:cel|ac
Password Expires: no expiration
6. <not used>
7. sptest  custom:am|rca|cel|nsc|ac
Password Expires: no expiration
8. <not used>
9. <not used>
10. <not used>
11. <not used>
12. <not used>
system>
```

IMM 控制指令

IMM 控制指令如下：

- clearcfg
- clock
- identify
- resetsp
- update

clearcfg 指令

使用 **clearcfg** 指令可將 IMM 配置設定爲其原廠預設值。您必須至少具有進階配接器配置權限才能發出此指令。清除 IMM 配置之後，將會重新啓動 IMM。

clock 指令

使用 **clock** 指令可根據 IMM 時鐘和 GMT 偏移來顯示現行日期和時間。您可以設定日期、時間、GMT 偏移及日光節約時間設定。

請注意下列資訊：

- 若 GMT 偏移爲 +2 或 +10，則需要特殊日光節約時間設定。
- 若爲 +2，則日光節約時間選項如下：off、ee (Eastern Europe)、gtb (Great Britain)、egt (Egypt)、fle (finland)。
- 若爲 +10，則日光節約時間設定如下：off、ea (Eastern Australia)、tas (Tasmania)、vlad (Vladivostok)。
- 年份必須在 2000（含）至 2089（含）之間。
- 月份、日期、小時、分鐘及秒鐘可以是單位數值（例如 9:50:25 而非 09:50:25）。
- 若爲正偏移，則 GMT 偏移格式可以是 +2:00、+2 或 2；若爲負偏移，則其格式可以是 -5:00 或 -5。

語法：

```
clock [options]
options:
-d mm/dd/yyyy
-t hh:mm:ss
-g gmt offset
-dst on/off/special case
```

範例：

```
system> clock
12/12/2003 13:15:23 GMT-5:00 dst on
system> clock -d 12/31/2004
ok
system> clock
12/31/2004 13:15:30 GMT-5:00 dst on
```

identify 指令

使用 **identify** 指令可讓機箱識別 LED 亮起或熄滅，或讓其閃爍。在 -s 爲 on 時，可使用 -d 選項以讓 LED 僅在使用 -d 參數指定的秒數內亮起。在此秒數過去之後，LED 會熄滅。

語法：

```
identify [options]
options:
-s on/off/blink
-d seconds
```

範例：

```
system> identify
-s off
system> identify -s on -d 30
ok
system>
```

resetsp 指令

使用 **resetsp** 指令可重新啓動 IMM。您必須至少具有進階配接器配置權限才能發出此指令。

update 指令

使用 **update** 指令可更新 IMM 中的韌體。若要使用此指令，您必須至少具有進階配接器配置權限。韌體檔案（由 *filename* 指定）首先會從 TFTP 伺服器（由其 IP 位址指定）傳送至 IMM，然後再進行更新。 **-v** 選項可指定詳細模式。

註：請確定 TFTP 伺服器正在將要從中下載檔案的伺服器上執行。

選項	說明
-i	TFTP 伺服器 IP 位址
-l	檔名（待更新）
-v	詳細模式

語法：

```
update -i TFTP_server_IP_address -l filename
```

範例：在詳細模式中，會以完成百分比即時顯示更新進度。

```
system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Firmware update is in progress. Please wait..
Downloading image - 66%

system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Firmware update is in progress. Please wait..
Image Downloaded.

system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Firmware update is in progress. Please wait..
Image Downloaded.
Flashing image - 45%

system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Firmware update is in progress. Please wait..
Image Downloaded.
Flash operation completed.
system>
```

如果不是在詳細模式中進行更新，則會以連續的 # 字元顯示進度。

```
system>update -i 192.168.70.200 -l dsa_d6yt28a_68608_2.upd
Firmware update is in progress. Please wait..
Downloading image: ##################################################
Flashing image: ##################################################
Flash operation completed.
```

Service Advisor 指令

Service Advisor 指令如下：

- autoftp
- chconfig
- chlog
- chmanual
- events
- sdemail

autoftp 指令

使用 **autoftp** 指令可顯示和配置 Service Advisor 的 FTP/TFTP 伺服器設定。

註：使用此指令之前，必須接受 Service Advisor 條款。

下表顯示各選項的引數。

選項	說明	值
-m	自動化問題報告模式	*ftp*、*tftp*、*disabled*
-i	用於自動化問題報告的 ftp/tftp 伺服器 IP 位址或主機名稱	IP 位址或主機名稱
-p	ftp/tftp 傳輸埠	*port_number* 的介於 1 與 65535 之間的數字
-u	引號定界的用於問題報告的 ftp 使用者名稱	*user_name* 的最多 63 個字元的字串

選項	說明	值
-pw	引號定界的用於問題報告的 ftp 密碼	*password* 的最多 63 個字元的字串
註：對於 *ftp* 值，必須設定所有選項（-i、-p、-u 及 -pw 欄位）。對於 *tftp* 值，僅 -i 和 -p 爲必要選項。		

語法：

```
autoftp [options]
options:
-m ftp|tftp|disable
-i host name|ip_addr
-p port_number
-u user_name
-pw password
```

chconfig 指令

使用 **chconfig** 指令可顯示和配置 IMM 的 Service Advisor 設定。

下表顯示各選項的引數。

選項	說明	值
-li	檢視或接受 Service Advisor 條款。設定其他選項之前，必須透過此選項接受 Service Advisor 條款。	view、accept
-sa	Service Advisor 的「IBM 支援中心」狀態	enabled、disabled
-sc	「IBM 服務支援中心」的國碼	兩個字元的 ISO 國碼
-ca	引號定界的機器位置所處地址	*address* 的最多 30 個字元的字串
-cci	引號定界的機器位置所處城市	*city* 的最多 30 個字元的字串
-ce	*userid@hostname* 格式的聯絡人電子郵件位址	*email_addr* 的最多 30 個字元的字串
-cn	引號定界的聯絡人名稱	*contact_name* 的最多 30 個字元的字串
-co	引號定界的聯絡人所屬組織/公司名稱	*company_name* 的最多 30 個字元的字串
-cph	引號定界的聯絡人電話號碼	*phone_number* 的介於 5 與 30 個字元之間的字串
-cs	機器位置所處州/省	*state/provice* 的介於 2 與 3 個字元之間的字串
-cz	引號定界的機器位置所處郵遞區號	*postal_code* 的最多 9 個字元的字串
-loc	HTTP Proxy 的完整主機名稱或 IP 位址	*host_name/ip_addr* 的最多 63 個字元的字串或是 IP 位址
-po	HTTP Proxy 埠	*port_number* 的介於 1 與 65535 之間的數字埠號
-ps	HTTP Proxy 狀態	enabled、disabled
-pw	引號定界的 HTTP Proxy 密碼	*password* 的最多 15 個字元的字串

選項	說明	值
-u	引號定界的 HTTP Proxy 使用者名稱	*user_name* 的最多 30 個字元的字串
1. 設定其他選項之前，必須透過 -li 選項接受 Service Advisor 條款。 2. 需要設定所有 Contact Information 欄位以及 IBM Service Support Center 欄位，然後才能啓用 Service Advisor 的「IBM 支援中心」。如果需要 Proxy，則還必須設定 HTTP Proxy 欄位。		

語法：

```
chconfig [options]
options:
-li view|accept
-sa service advisor state
-sc country_code
-ca address
-cci city
-ce email_addr
-cn contact_name
-co company_name
-cph phone_number
-cs state/provice
-cz postal_code
-loc host_name/ip_addr
-po port_number
-ps status
-pw password
-u user_name
```

chlog 指令

使用 **chlog** 指令可顯示系統或使用者產生的最後五個 Call Home 事件。最新的 Call Home 項目會最先列出。

下表顯示各選項的引數。

註：使用此指令之前，必須接受 Service Advisor 條款。

選項	說明	值
-event_index	使用 Activity Log 中的 Index 指定 Call Home 項目	介於 1 與 5 之間的數字
-ack	認可/未認可，已更正 Call Home 事件	yes、no
-s	僅顯示「IBM 支援中心」的結果	
-f	僅顯示 FTP/TFTP 伺服器的結果	

語法：

```
chlog [options]
options:
-event_index
-ack yes|no
-s
-f
```

chmanual 指令

使用 **chmanual** 指令可產生 Manual Call Home 事件或 Test Call Home 事件。

註：使用此指令之前，必須接受 Service Advisor 條款。

下表顯示各選項的引數。

選項	說明	值
-test	產生 Test Call Home 事件	
-desc	引號定界的問題說明	*description* 的最多 100 個字元的字串

語法：

```
chmanual [options]
options:
-test
-desc description
```

events 指令

使用 **events** 指令可檢視和編輯排除事件。

註：使用此指令之前，必須接受 Service Advisor 條款。

下表顯示各選項的引數。

選項	說明	值
-che	檢視和編輯排除事件	
-add	將 Call Home 事件新增至 Call Home 排除清單	`0xhhhhhhhhhhhhhhhh` 格式的 *event_id*
-rm	從 Call Home 排除清單移除 Call Home 事件	`0xhhhhhhhhhhhhhhhh` 格式的 *event_id*|*all* 或 all

語法：

```
events [options]
options: -che {-add}|{-rm}
-add event_id
-rm event_id|all
```

sdemail 指令

使用 **sdemail** 指令可配置指定收件者的電子郵件服務資訊。

下表顯示各選項的引數。

選項	說明	值
-subj	引號定界的電子郵件主旨	*email_subject* 的最多 119 個字元的字串
-to	收件者的電子郵件位址。此選項可由以逗點區隔的多個位址組成。	*email_addrs* 的最多 119 個字元的字串

語法：

```
sdemail [options]
options:
-subj email_subject
-to email_addrs
```

附錄 A. 取得說明和技術協助

如果您需要說明、服務或技術協助，或者只想瞭解 IBM 產品的相關資訊，您可以從 IBM 取得各式各樣的協助。

使用本資訊可取得 IBM 與 IBM 產品的其他相關資訊、判定在 IBM 系統或選用裝置發生問題時應採取的動作，以及判定在必要時應向誰致電請求服務。

撥打電話前

撥打電話前，請確定您已採取下列步驟來嘗試自行解決問題。

當您認爲需要 IBM 對您的 IBM 產品執行保固服務時，如果您在撥打電話前準備妥當，則 IBM 服務中心維修技術人員將能夠更有效率地協助您。

- 檢查所有的纜線，確定纜線都已連接。
- 檢查電源開關，確定系統及任何選用裝置的電源都已經開啓。
- 檢查適用於您 IBM 產品的更新軟體、韌體及作業系統裝置驅動程式。 IBM 保固條款規定，您作爲 IBM 產品的擁有者，有責任維護並更新產品的所有軟體及韌體（除非此項工作涵蓋於其他維護合約中）。如果軟體升級中具有已記載的問題解決方案，IBM 服務技術人員將會要求您升級軟體及韌體。
- 如果您已在環境中安裝新的硬體或軟體，請檢查 http://www.ibm.com/systems/info/x86servers/serverproven/compat/us，以確定 IBM 產品支援此軟硬體。
- 請造訪 http://www.ibm.com/supportportal，檢查是否有資訊可協助您解決問題。
- 收集下列資訊以提供給「IBM 支援中心」。此資料將會協助「IBM 支援中心」快速提供問題的解決方案，確保您能獲得所約定的服務層次。
  - 軟硬體維護合約號碼（如果適用的話）
  - 機型號碼（IBM 4 位數機器 ID）
  - 型號
  - 序號
  - 現行系統 UEFI 及韌體層次
  - 其他相關資訊，例如錯誤訊息及日誌
- 請造訪 http://www.ibm.com/support/entry/portal/Open_service_request，以提交「電子服務要求」。提交「電子服務要求」所開始的程序，是藉由快速、有效率地向「IBM 支援中心」提供相關資訊，以便服務人員能判定問題並找出解決方案。您一完成並提交「電子服務要求」之後，IBM 服務中心技術人員即可開始處理您的解決方案。

按照 IBM 在線上說明或 IBM 產品隨附的文件中提供的疑難排解程序進行操作，無需外界協助您就可以解決許多問題。IBM 系統隨附的文件也會說明您可執行的診斷測試。大部分的系統、作業系統和程式都附有文件，其中包含疑難排解程序以及錯誤訊息和錯誤碼的說明。如果您懷疑是軟體問題，請參閱作業系統或程式的文件。

使用文件

您的 IBM 系統以及預先安裝軟體（如果有的話）或選用裝置的相關資訊都可以在產品隨附的文件中找到。該文件的形式包含印刷文件、線上文件、Readme 檔和說明檔。

請參閱系統文件中的疑難排解資訊，以取得使用診斷程式的指示。疑難排解資訊或診斷程式可能會告訴您，您還需要其他或已更新的裝置驅動程式或其他軟體。IBM 在「全球資訊網 (WWW)」上提供許多網頁，您可以從中取得最新的技術資訊，並可下載裝置驅動程式和更新項目。若要存取這些頁面，請造訪 http://www.ibm.com/supportportal。

從全球資訊網取得說明和資訊

在「全球資訊網」可取得 IBM 產品和支援的最新相關資訊。

在「全球資訊網」上，提供了 IBM 系統、選用裝置、服務及支援的最新相關資訊，網址爲 http://www.ibm.com/supportportal。IBM System x 資訊位於 http://www.ibm.com/systems/x。IBM BladeCenter 資訊位於 http://www.ibm.com/systems/bladecenter。IBM IntelliStation 資訊位於 http://www.ibm.com/systems/intellistation。

如何將 DSA 資料傳送至 IBM

使用「IBM 加強型客戶資料儲存庫」可將診斷資料傳送給 IBM。

在將診斷資料傳送至 IBM 之前，請先閱讀 http://www.ibm.com/de/support/ecurep/terms.html 上的使用條款。

您可以使用以下任何一種方法將診斷資料傳送至 IBM：

- **標準上傳**：http://www.ibm.com/de/support/ecurep/send_http.html
- **標準上傳（含系統序號）**：http://www.ecurep.ibm.com/app/upload_hw
- **安全上傳**：http://www.ibm.com/de/support/ecurep/send_http.html#secure
- **安全上傳（含系統序號）**：https://www.ecurep.ibm.com/app/upload_hw

建立個人化的支援網頁

您可以透過識別您感興趣的 IBM 產品，來建立個人化的支援網頁。

若要建立個人化的支援網頁，請造訪 http://www.ibm.com/support/mynotifications。您可從這個個人化頁面中，訂閱關於新技術文件的每週電子郵件通知、搜尋資訊與下載，以及存取各項管理服務。

軟體服務和支援

透過「IBM 技術支援專線」，您可以使用付費電話來取得 IBM 產品在用法、配置及軟體問題等方面的協助。

如需您所在國家或地區「技術支援專線」支援的產品相關資訊，請參閱 http://www.ibm.com/services/supline/products。

如需「技術支援專線」和其他 IBM 服務中心的相關資訊，請參閱 http://www.ibm.com/services，或參閱 http://www.ibm.com/planetwide，以取得支援電話號碼。在美國和加拿大，請撥 1-800-IBM-SERV (1-800-426-7378)。

硬體服務和支援

您可以透過 IBM 轉銷商或「IBM 服務中心」來取得硬體服務。

若要尋找 IBM 授權提供保固服務的轉銷商，請造訪 http://www.ibm.com/partnerworld 並按一下 **Business Partner Locator**。如需 IBM 支援電話號碼，請參閱 http://www.ibm.com/planetwide。在美國和加拿大，請撥 1-800-IBM-SERV (1-800-426-7378)。

在美國和加拿大地區，提供 24 小時全年無休的硬體服務與支援。若是在英國地區，則是星期一到星期五的 9 a.m. 到 6 p.m. 提供這些服務。

台灣 IBM 公司產品服務中心

使用此資訊，可聯絡「台灣 IBM 產品服務中心」。

台灣 IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路 7 號 3 樓
電話：0800-016-888

台灣 IBM 公司產品服務中心聯絡資訊：

台灣 IBM 公司
松仁路 7 號 3 樓
台北市，台灣
電話號碼：0800-016-888

附錄 B. 注意事項

本資訊係針對 IBM 在美國所提供之產品與服務所開發。

在其他國家或地區中，IBM 不見得有提供本文件所提及的各項產品、服務或特性。請洽詢當地的 IBM 業務代表，以取得當地目前提供的產品和服務之相關資訊。本文件在提及 IBM 的產品、程式或服務時，不表示或暗示只能使用 IBM 的產品、程式或服務。只要未侵犯 IBM 智慧財產權，任何功能相當的產品、程式或服務皆可取代 IBM 的產品、程式或服務。不過，任何非 IBM 之產品、程式或服務，使用者必須自行負責作業之評估和驗證責任。

對於本文件所說明之主題內容，IBM 可能擁有其專利或正在進行專利申請。提供本文件不代表提供這些專利的授權。您可以書面提出授權查詢，來函請寄到：

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

International Business Machines Corporation 只依「現況」提供本出版品，不提供任何明示或默示之保證，其中包括且不限於不違反規定、適售性或特定目的之適用性的隱含保證。有些地區在某些交易上並不接受明示或默示保證的排除，因此，這項聲明對 貴客戶不見得適用。

本資訊中可能會有技術上或排版印刷上的訛誤。因此，IBM 會定期修訂；並將修訂後的內容納入新版中。IBM 可能會隨時改進及/或變更本出版品所提及的產品及/或程式，而不另行通知。

本資訊中任何對非 IBM 網站的敘述僅供參考，IBM 對該等網站並不提供保證。這些網站所提供的資料不是本 IBM 產品的一部份，如果要使用這些網站的資料，您必須自行承擔風險。

IBM 得以各種 IBM 認爲適當的方式使用或散布貴客戶提供的任何資訊，而無需對貴客戶負責。

商標

IBM、IBM 標誌和 ibm.com 是 International Business Machines Corp. 的商標，已在全球許多國家/地區或司法管轄區註冊。其他產品及服務名稱可能是 IBM 或其他公司的商標。

現行 IBM 商標清單可於網頁上取得，網址爲 http://www.ibm.com/legal/us/en/copytrade.shtml。

Adobe 及 PostScript 是 Adobe Systems Incorporated 在美國及/或其他國家的註冊商標或商標。

Cell Broadband Engine 是 Sony Computer Entertainment, Inc. 在美國及 (或) 其他國家的商標，而且依其授權使用。

Intel、Intel Xeon、Itanium 及 Pentium 是 Intel Corporation 或其分公司在美國及其他國家的商標或註冊商標。

Java 和所有以 Java 爲基礎的商標及標誌是 Oracle 及（或）其子公司的商標或註冊商標。

Linux 是 Linus Torvalds 在美國及 (或) 其他國家的註冊商標。

Microsoft、Windows 及 Windows NT 是 Microsoft Corporation 在美國及 (或) 其他國家的商標。

UNIX 是 The Open Group 在美國及其他國家的註冊商標。

重要注意事項

處理器速度表示微處理器的內部時鐘速度；其他因素也會影響應用程式效能。

CD 或 DVD 光碟機速度是變動的讀取速度。實際速度會有所不同，且通常小於可能達到的最大速度。

當提到處理器儲存體、實際和虛擬儲存體或通道容體時，KB 代表 1024 位元組，MB 代表 1,048,576 位元組，而 GB 代表 1,073,741,824 位元組。

在提到硬碟容量或通訊磁區時，MB 代表 1,000,000 位元組，而 GB 代表 1,000,000,000 位元組。使用者可存取的總容量不一定，視作業環境而定。

內部硬碟的最大容量，是指使用 IBM 所提供的現存最大容量硬碟，來替換任何標準硬碟，並移入所有硬碟機槽時的容量。

如果要達到最大的記憶體，則必須以選用的記憶體模組來更換標準記憶體。

每個固態記憶體單元都有該單元可以承受的固有且有限的寫入週期數。因此，固態硬碟有寫入週期數上限的限制，其以「寫入的位元數總數」(TBW) 表示。超過此限制的裝置可能無法回應系統產生的指令，或可能無法被寫入。如更換超過其程式/清除週期保證數上限（在裝置的「官方出版規格書」中有記載）的裝置，IBM 概不負責。

IBM 對於非 IBM 產品以及 ServerProven® 服務，並不負責保固，亦不發表聲明，包括但不限於適售性或符合特定效用之默示保證。該等產品僅由第三人提供及保固。

IBM 對於非 IBM 產品不負有責任或保固。若有任何非 IBM 產品之支援，則由第三人提供，而非由 IBM 提供。

部分軟體可能與其零售版（若有的話）不同，且可能不含使用手冊或完整的程式功能。

微粒污染

注意：空氣中的微粒（包括金屬薄片或微粒）及單獨起作用或結合其他環境因素（例如：濕度或溫度）而起作用的反應性氣體，可能會給裝置帶來本文件中所述的危險。

過量的微粒層次或有害氣體濃度所帶來的風險，包括可讓裝置故障或完全停止運作的損害。這項規格設定了微粒與氣體的限制，主要爲避免這類的傷害。這些限制不能視爲或是用來作爲明確的限制，因爲還有許多其他的因素，如溫度或空氣的溼氣內容，都可能會影響到微粒或是環境的腐蝕性與氣體的傳播。如果沒有本文件中所設定之特定的限制，您必須實作能維護符合人類健康與安全之微粒與氣體層次的方案。如果 IBM 判定您環境中的微粒或氣體已經對裝置造成損害，IBM 可能會提供修復或更換裝置，或是適當地修復一些組件，以減輕這類的環境污染。這類修復的作業屬於客戶的責任。

表 21. 微粒與氣體的限制

污染	限制
微粒	• 室內空氣必須持續按照 ASHRAE Standard 52.2[1]，以 40% 的大氣粉塵污點效率 (MERV 9) 來進行過濾。 • 進入資料中心的空氣必須利用符合 MIL-STD-282 的高效微粒空氣 (HEPA) 過濾器來過濾，有效性要達 99.97% 或以上。 • 微粒污染的潮解性相對溼度，必須大於 60%[2]。 • 室內不可以有傳導性污染物，如鋅晶須。
氣體	• 銅：類別 G1，根據 ANSI/ISA 71.04-1985[3] • 銀：30 天內腐蝕率小於 300 Å

[1] ASHRAE 52.2-2008 - *測試用於有效移除微粒大小的一般空氣清靜通風裝置的方法*。亞特蘭大：美國供熱、冷凍和空調工程師協會

[2] 微粒污染的潮解性相對溼度，是灰塵吸收足夠的水分而變成潮溼，並且可傳導離子的相對溼度。

[3] ANSI/ISA-71.04-1985。*程序測量及控制系統的環境條件：空中傳播的污染物*。Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

文件格式

本產品的發佈使用 Adobe 可攜式文件格式 (PDF)，而且應該符合可存取性標準。若您在使用 PDF 檔案時遇到問題，並且想要索取 Web 型格式或可存取的 PDF 文件出版品，請將郵件寄至下列地址：

Information Development
IBM Corporation
205/A015
3039 E. Cornwallis Road
P.O. Box 12195
Research Triangle Park, North Carolina 27709-2195
U.S.A.

在這份要求中，請務必包含出版品的產品編號及標題。

當您傳送資訊至 IBM 時，IBM 得以各種 IBM 認爲適當的方式使用或散布 貴客戶提供的任何資訊，而無需對 貴客戶負責。

電信法規聲明

本產品可能未在貴國通過認證，無法透過任何方式連線至公用電信網路的介面。根據法律規定，需要進一步憑證，才能進行連線。如有任何問題，請聯絡 IBM 業務代表或轉銷商。

電子輻射注意事項

將顯示器連接至此設備時，您必須使用指定的顯示器纜線，以及隨顯示器一同提供的任何干擾抑制裝置。

美國聯邦通訊委員會 (FCC) 聲明

附註：本裝置已經過測試，根據 FCC 規則第 15 條，確定已符合 A 級數位裝置的限制。These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. 操作受到下列兩個條件的限制：(1) 此裝置不會造成有害干擾，(2) 此裝置必須接受任何接收到的干擾，包括會造成不想要之操作的干擾在內。

加拿大工業部 A 級輻射符合聲明

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

澳洲與紐西蘭 A 級聲明

警告： 此爲 A 級產品。In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

歐盟 EMC 法令相符性聲明

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a nonrecommended modification of the product, including the fitting of non-IBM option cards.

警告： This is an EN 55022 Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Responsible manufacturer:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504 914-499-1900

European Community contact:

IBM Deutschland GmbH
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Germany
Telephone: +49 7032 15 2941
Email: lugi@de.ibm.com

德國 A 級聲明

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/ eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden: **Warnung:** Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen.

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG). Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:

International Business Machines Corp.
New Orchard Road Armonk, New York 10504
914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland GmbH
Technical Regulations, Abteilung M372
IBM-Allee 1, 71139 Ehningen, Germany
Telephone: +49 7032 15 2941
Email: lugi@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

日本 VCCI A 級聲明

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI). If this equipment is used in a domestic environment, radio interference may occur, in which case the user may be required to take corrective actions.

韓國通訊委員會 (KCC) 聲明

이 기기는 업무용(A급)으로 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

This is electromagnetic wave compatibility equipment for business (Type A). Sellers and users need to pay attention to it. This is for any areas other than home.

俄羅斯電磁干擾 (EMI) A 級聲明

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать радиопомехи, для снижения которых необходимы дополнительные меры

中華人民共和國 A 級電子放射聲明

中华人民共和国“A类”警告声明

声 明

此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

台灣甲類標準聲明

警告使用者:
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

索引

索引順序以中文字，英文字，及特殊符號之次序排列。

〔一劃〕

〔二劃〕

〔三劃〕

〔四劃〕

〔五劃〕

〔六劃〕

〔七劃〕

〔八劃〕

〔九劃〕

〔十劃〕

〔十一劃〕

〔十二劃〕

〔十三劃〕

〔十四劃〕

〔十五劃〕

〔十六劃〕

〔十七劃〕

〔十八劃〕

〔十九劃〕

〔二十劃〕

〔二十二劃〕

A

B

D

F

I

J

L

M

N

O

P

R

S

T

U

V

W

產品編號： 00FH269

Printed in Taiwan

(1P) P/N: 00FH269