Lenovo

XClarity Controller，搭載 Intel Xeon SP（第 1 代、第 2 代）
使用手冊

附註：使用本資訊之前，請先閱讀第 185 頁附錄 B 「聲明」中的一般資訊。

第 15 版 (2021 年 5 月)

目錄

第 1 章　簡介

Lenovo XClarity Controller (XCC) 是新一代的管理控制器，可取代 Lenovo ThinkSystem 伺服器的基板管理控制器 (BMC)。

這是新一代 Integrated Management Module II (IMM2) 服務處理器，將服務處理器功能、超級 I/O、視訊控制器和遠端顯示功能整合在伺服器主機板上的單一晶片中。所提供的功能如下：

- 可選擇用於系統管理的專用或共用乙太網路連線
- 支援 HTML5
- 支援透過 XClarity 行動版存取
- XClarity Provisioning Manager
- 使用 XClarity Essentials 或 XClarity Controller CLI 遠端配置。
- 應用程式和工具能夠在本端或遠端存取 XClarity Controller。
- 加強的遠端顯示功能。
- REST API（Redfish 綱目）支援其他 Web 相關服務和軟體應用程式。

  附註：XClarity Controller 目前支援 Redfish 可調式平台管理 API 規格 1.0.2 和綱目 2016.2

附註：

- 在 XClarity Controller Web 介面中，BMC 用來代表 XCC。
- 部分 ThinkSystem 伺服器可能無法使用專用系統管理網路埠；這些伺服器只能透過與伺服器作業系統共用的網路埠，才能存取 XClarity Controller。
- 對於 Flex 伺服器，Chassis Management Module (CMM) 是系統管理功能的主要管理模組。使用 CMM 的網路埠，才能存取 XClarity Controller。

本文件說明如何使用 ThinkSystem 伺服器上的 XClarity Controller 功能。XClarity Controller 搭配使用 XClarity Provisioning Manager 和 UEFI，可為 ThinkSystem 伺服器提供系統管理功能。

若要查看韌體更新項目，請完成下列步驟。

附註：第一次存取 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 Support Portal 時，網站會預先載入您最初選取的產品，而且僅顯示適用於您產品的鏈結。若要在您的產品清單中變更或新增內容，請按一下**管理我的產品清單**鏈結。網站將定期進行變更。尋找韌體和文件的程序可能與本文件的說明略有不同。

1. 前往 http://datacentersupport.lenovo.com。
2. 在 **Support（支援）**下，選取 **Data Center（資料中心）**。
3. 內容載入後，選取 **Servers（伺服器）**。
4. 在 **Select Series（選取系列）**下，先選取特定伺服器硬體系列，然後在 **Select SubSeries（選取子系列）**下，選取特定伺服器產品子系列，最後在 **Select Machine Type（選取機型）**下選取特定機型。

XClarity Controller 標準、進階和企業版功能

使用 XClarity Controller，提供標準版、進階版和企業版的 XClarity Controller 功能。如需您的伺服器所安裝的 XClarity Controller 版本的相關資訊，請參閱伺服器的文件。所有版本都提供下列功能：

- 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

附註：部分功能可能不適用於 Flex System 伺服器。

XClarity Controller 標準版的功能清單如下：

XClarity Controller 標準版功能

XClarity Controller 標準版的功能清單如下：

業界標準管理介面

- IPMI 2.0 介面
- Redfish
- CIM-XML
- DCMI 1.5
- SNMPv3
- SNMPv1（僅設陷）需要至少 v2.10 或 v2.12 的 XCC 韌體更新，具體取決於伺服器類型。如需詳細資料，請參閱 XCC 韌體更新變更檔。

其他管理介面

- Web
- 舊式 CLI
- 前方面板 USB - 透過行動裝置的虛擬操作面板

電源/重設控制

- 開啟電源
- 強迫關機/正常關機
- 排定的電源控制
- 系統重設
- 開機順序控制

事件日誌

- IPMI SEL
- 使用者可讀取日誌
- 審核日誌

環境監視

- 無代理程式監視
- 感應器監視
- 風扇控制
- LED 控制
- 晶片組錯誤（Caterr、IERR、等...）
- 系統性能狀態指示
- I/O 配接卡適用的 OOB 效能監視
- 顯示及匯出庫存

RAS

- 虛擬 NMI
- 自動回復韌體
- 備份韌體自動升級
- POST 監視器
- 作業系統載入器監視器
- 藍色畫面擷取（OS 失敗）
- 嵌入式診斷工具

網路配置

- IPv4
- IPv6
- IP 位址、子網路遮罩、閘道
- IP 位址指派模式
- 主機名稱
- 可程式化 MAC 位址
- 雙 MAC 選項（如果伺服器硬體支援的話）
- 網路埠重新指派
- VLAN 標記

網路通訊協定

- DHCP
- DNS
- DDNS
- HTTP/HTTPS
- SNMPv3
- SNMPv1（僅設陷）
- SSL
- SSH
- SMTP
- LDAP 用戶端
- NTP
- SLP
- SSDP

警示

- PET 設陷
- CIM 指示
- SNMP 設陷
- 電子郵件
- Redfish 事件

序列重新導向

- IPMI SOL
- 序列埠配置

安全性

- XClarity Controller 可信賴測量之核根 (CRTM)
- 數位方式簽署的韌體更新
- 角色型存取控制 (RBAC)
- 本端使用者帳戶
- LDAP/AD 使用者帳戶
- 韌體安全回復
- 機箱侵入偵測（僅可在部分伺服器型號上使用）
- XCC 遠端 UEFI TPM 物理現場授權生效
- 審核配置變更和伺服器動作的日誌
- 公開金鑰 (PK) 鑑別
- 系統退役/重新規劃

遠端顯示

- 卡上的遠端磁碟 (RDOC)：透過 CIFS、NFS、HTTP、HTTPS、FTP、SFTP 和 LOCAL，對遠端 ISO/IMG 檔案執行虛擬媒體裝載

電源管理

- 即時電源計量表

授權管理

- 啟動金鑰驗證及儲存庫

部署與配置

- 遠端配置
- 使用內嵌式 XClarity Provisioning Manager 的部署與配置工具和驅動程式套件
- 配置備份及還原

韌體更新

- 無代理程式更新
- 遠端更新

XClarity Controller 進階版功能

XClarity Controller 進階版的功能清單如下：

所有 XClarity Controller 標準版功能，再加上：

警示

- Syslog

遠端顯示

- 遠端 KVM

序列重新導向

- 透過 SSH 的序列重新導向

安全性

- Security Key Lifecycle Manager (SKLM)
- IP 位址封鎖

電源管理

- 即時電源圖形
- 歷程電源計數器
- 溫度圖形

部署與配置

- 使用內嵌式 XClarity Provisioning Manager 搭配 XClarity Controller 遠端 KVM 功能進行遠端 OS 部署

XClarity Controller 企業版功能

XClarity Controller 企業版的功能清單如下：

所有 XClarity Controller 標準版和進階版功能，再加上：

RAS

- 開機擷取

遠端顯示

- 品質/頻寬控制
- 虛擬主控台協同作業（六個使用者）
- 虛擬主控台聊天
- 虛擬媒體
  - 透過遠端主控台裝載遠端 ISO/IMG 檔案
  - 從網路裝載檔案：- 從檔案伺服器（HTTPS、CIFS、NFS）將 ISO 或 IMG 映像檔裝載至主機成為 DVD 光碟機或 USB 隨身碟

電源管理

- 功率上限
- OOB 效能監視 - 系統效能計量

部署與配置

- 使用 Lenovo XClarity Administrator 進行遠端部署。使用 Lenovo XClarity Administrator 進行作業系統部署時，請參閱 https://pubs.lenovo.com/lxca/supported_operating_system_images 以取得支援的作業系統的詳細資料。

升級 XClarity Controller

如果您的伺服器隨附標準或進階版本的 XClarity Controller 韌體功能，您可以升級伺服器中的 XClarity Controller 功能。如需可用升級版本和訂購方式的相關資訊，請參閱第 79 頁第 8 章 「授權管理」。

Web 瀏覽器和作業系統需求

使用本主題中的資訊可檢視您的伺服器所支援的瀏覽器、密碼組合和作業系統清單。

XClarity Controller Web 介面需要下列其中一款 Web 瀏覽器：

- Chrome 48.0 或更高版本（對於遠端主控台，則需要 55.0 或更高版本）
- Firefox ESR 38.6.0 或更高版本
- Microsoft Edge
- Safari 9.0.2 或更高版本（iOS 7 或更新版本以及 OS X）

附註：行動裝置作業系統上的瀏覽器不支援遠端主控台功能。

上述所列出的瀏覽器符合 XClarity Controller 韌體目前所支援的項目。XClarity Controller 韌體可能會定期加強，以包括對其他瀏覽器的支援。

視 XClarity Controller 中的韌體版本而定，Web 瀏覽器支援可能會因本章節中所列的瀏覽器而異。若要查看 XClarity Controller 中目前所用韌體的受支援瀏覽器清單，請從 XClarity Controller 登入頁面中按一下**支援的瀏覽器**功能表清單。

為了增加安全性，在使用 HTTPS 時目前僅支援高強度密碼。在使用 HTTPS 時，您的用戶端作業系統及瀏覽器組合必須支援下列其中一個密碼組合：

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-ECDSA-AES256-SHA
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES128-SHA
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256

網際網路瀏覽器的快取會儲存您所造訪網頁的相關資訊，以便日後更快地載入這些網頁。對 XClarity Controller 韌體進行快閃更新後，您的瀏覽器可能會繼續使用其快取資訊，而非從 XClarity Controller 擷取資訊。建議您在更新 XClarity Controller 韌體之後清除瀏覽器快取，以確保正確顯示 XClarity Controller 所提供的網頁。

多國語言支援

使用本主題中的資訊以檢視 XClarity Controller 所支援的語言清單。

依預設，XClarity Controller Web 介面所選用的語言為英文。該介面可顯示多國語言。這些多國語言如下：

- 法文
- 德文
- 義大利文
- 日文

- 韓文
- 葡萄牙文（巴西）
- 俄文
- 簡體中文
- 西班牙文（國際）
- 繁體中文

若要選擇您所喜好的語言，請按一下目前選取語言旁邊的箭頭。則會出現下拉功能表，可讓您選擇喜好的語言。

XClarity Controller 韌體產生的文字字串會以瀏覽器指定的語言顯示。如果瀏覽器指定的語言不是上述其中一種翻譯語言，則會以英文顯示文字。此外，由 XClarity Controller 韌體顯示、但不是由 XClarity Controller 產生的任何文字字串（例如，由 UEFI、PCIe 配接卡等產生的訊息），都會以英文顯示。

目前不支援英文以外的語言特定文字輸入，例如**侵害訊息**。僅支援以英文輸入的文字。

MIB 簡介

使用本主題中的資訊來存取管理資訊庫。

SNMP MIB 可從 https://support.lenovo.com/ 下載（在入口網站上依機型搜尋）。其中包含下列四個 MIB。

- **SMI MIB** 描述 Lenovo Data Center Group 的管理資訊的結構。
- **產品 MIB** 描述 Lenovo 產品的物件 ID。
- **XCC MIB** 提供 Lenovo XClarity Controller 的庫存和監視資訊。
- **XCC 警示 MIB** 為 Lenovo XClarity Controller 偵測到的警示條件定義設陷。

附註：四個 MIB 的匯入順序為 **SMI MIB** → **產品 MIB** → **XCC MIB** → **XCC 警示 MIB**。

本文件所使用的注意事項

使用此資訊可瞭解本文件所使用的注意事項。

本文件所使用的注意事項如下：

- **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：**這些注意事項表示可能損壞程式、裝置或資料。此警示注意事項出現在可能造成損壞的指示或狀況前面。

第 2 章　開啟並使用 XClarity Controller Web 介面

本主題說明您可以從 XClarity Controller Web 介面執行的登入程序和動作。

XClarity Controller 將服務處理器功能、視訊控制器及遠端顯示功能組合在單一晶片中。您必須先登入，才能使用 XClarity Controller Web 介面遠端存取 XClarity Controller。本章說明您可以從 XClarity Controller Web 介面執行的登入程序和動作。

存取 XClarity Controller Web 介面

本主題的資訊說明如何存取 XClarity Controller Web 介面。

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

XClarity Controller 也支援 IPv6，但預設為沒有固定的靜態 IPv6 IP 位址。若要在 IPv6 環境中起始存取 XClarity Controller，您可以使用 IPv4 IP 位址或 IPv6 鏈結本端位址。XClarity Controller 會使用 IEEE 802 MAC 位址產生唯一的鏈結本端 IPv6 位址，方法是如 RFC4291 所述，在 48 位元 MAC 的中間，以 0xFF 和 0xFE 的十六進位值插入兩個八位元組，然後將 MAC 位址的第一個八位元組中右邊第 2 個位元翻轉。例如，假設 MAC 位址為 08-94-ef-2f-28-af，則鏈結本端位址如下：

```
fe80::0a94:efff:fe2f:28af
```

存取 XClarity Controller 時，下列 IPv6 狀況設為預設值：

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

XClarity Controller 可讓您選擇使用 **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。

大部分伺服器提供使用獨立 1Gbit 網路介面控制器的專用系統管理網路連線。不過，部分系統可能使用網路控制器側頻介面 (NCSI)，為多埠網路介面控制器的某個網路埠提供專用系統管理網路連線。在此情況下，專用系統管理網路連線的上限速度為側頻介面的 10/100。如需系統上管理埠實作的資訊和所有限制，請參閱系統文件。

附註：可能無法在您的伺服器上使用**專用**系統管理網路埠。如果您的硬體沒有**專用**網路埠，則**共用**設定是 XClarity Controller 唯一可用的設定。

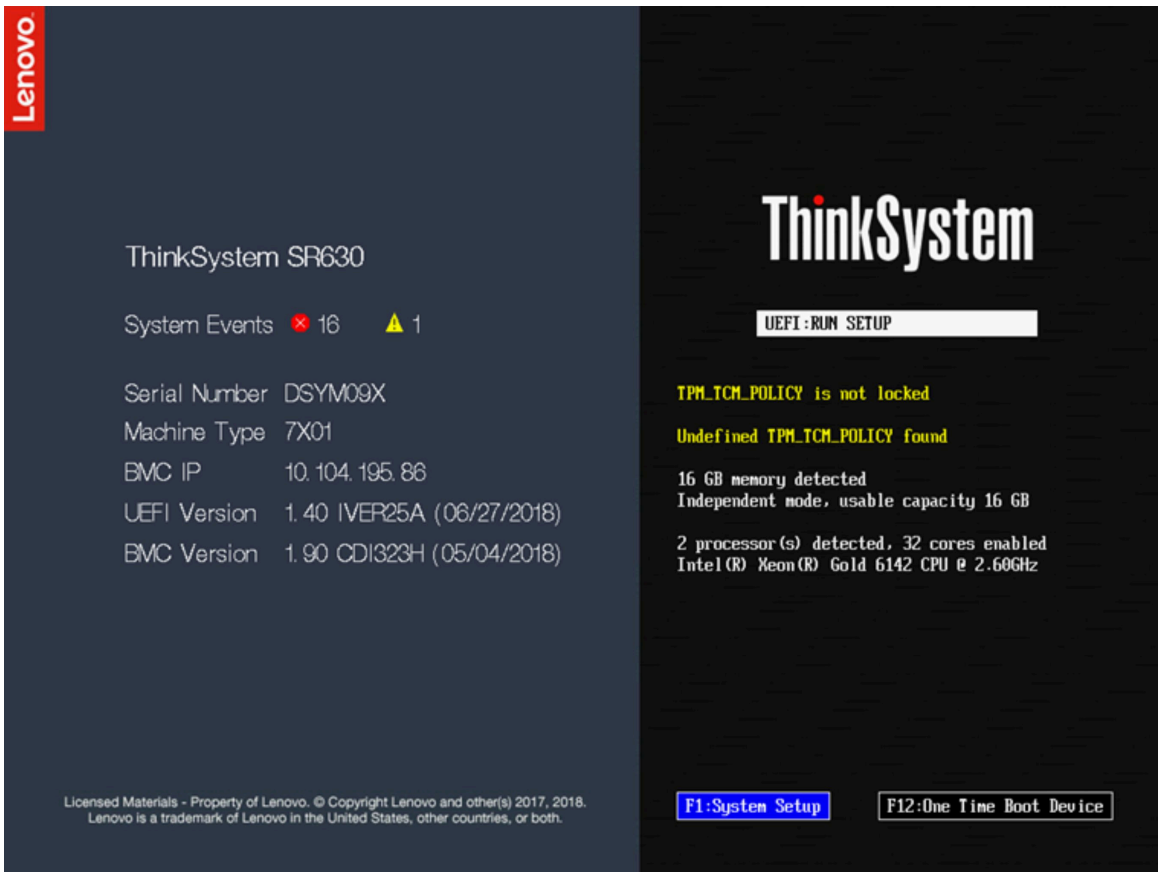
透過 XClarity Provisioning Manager 設定 XClarity Controller 網路連線

使用本主題中的資訊可透過 XClarity Provisioning Manager 設定 XClarity Controller 網路連線。

啟動伺服器後，您可以使用 XClarity Provisioning Manager 來配置 XClarity Controller 網路連線。必須將具有 XClarity Controller 的伺服器連接至 DHCP 伺服器，或者必須將伺服器網路配置為使用 XClarity Controller 靜態 IP 位址。若要透過 Setup Utility 設定 XClarity Controller 網路連線，請完成下列步驟：

步驟 1. 開啟伺服器。會顯示 ThinkSystem 歡迎使用畫面。

> **附註：**伺服器連接至 AC 電源之後，可能需要 40 秒才能讓電源控制按鈕變成作用中。



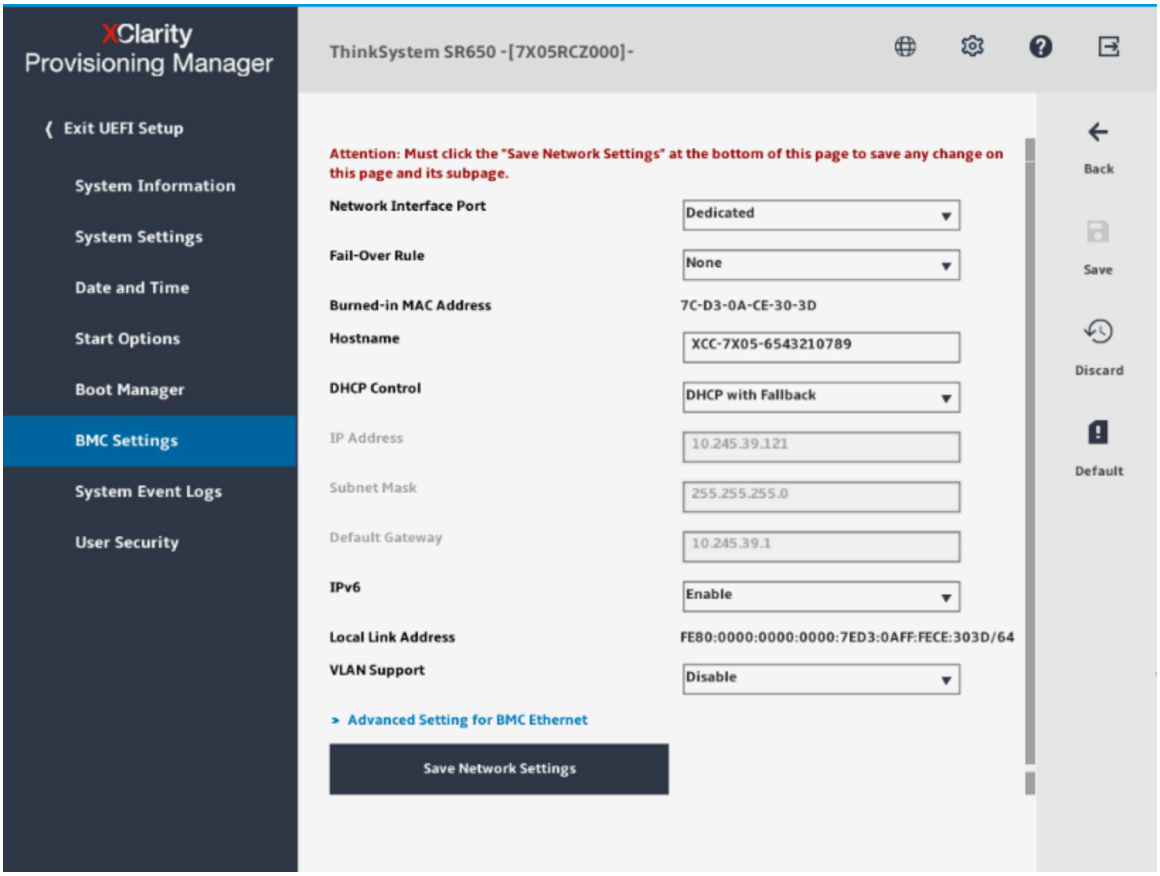
步驟 2. 當顯示 `<F1> System Setup` 提示時，請按 F1 鍵。如果您已設定開機密碼和管理者密碼，則必須輸入管理者密碼，才能存取 XClarity Provisioning Manager。

步驟 3. 從 XClarity Provisioning Manager 主功能表中，選取 **UEFI Setup**。

步驟 4. 在下一個畫面上，選取 **BMC Settings**，然後按一下 **Network Settings**。

步驟 5. **DHCP Control** 欄位中有三個 XClarity Controller 網路連線選項：

- 靜態 IP
- 已啟用 DHCP
- 具有備援的 DHCP



步驟 6. 選取其中一個網路連線選項。

步驟 7. 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。

步驟 8. 您也可以使用 Lenovo XClarity Controller Manager 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 XClarity Controller 網路連線。

附註：

- 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**共用**設定是唯一可用的 XClarity Controller 設定。在 **Network Configuration** 畫面中，選取 **Network Interface Port** 欄位中的 **Dedicated**（如果適用的話）或 **Shared**。
- 若要尋找您伺服器上 XClarity Controller 所使用的乙太網路接頭位置，請參閱伺服器隨附的文件。

步驟 9. 按一下**儲存**。

步驟 10. 從 XClarity Provisioning Manager 結束。

附註：

- 您必須先等待大約 1 分鐘的時間讓變更生效，然後伺服器韌體才能再次運作。
- 您也可以透過 XClarity Controller Web 介面或指令行介面 (CLI)，來配置 XClarity Controller 網路連線。在 XClarity Controller Web 介面中，只要按一下左側導覽面板上的 **BMC 配置**，然後選取**網路**，即可配置網路連線。在 XClarity Controller CLI 中，使用數個指令（視您安裝的配置而定）配置網路連線。

登入 XClarity Controller

使用本主題的資訊可透過 XClarity Controller Web 介面存取 XClarity Controller。

重要事項：XClarity Controller 初始設定的使用者名稱及密碼分別為 USERID 和 PASSWORD（其中所含的是數字 0，不是字母 O）。此預設使用者設定具有監督者存取權。請在起始配置期間變更此使用者名稱和密碼，以加強安全性。進行變更後，無法再次將 PASSWORD 設定為登入密碼。

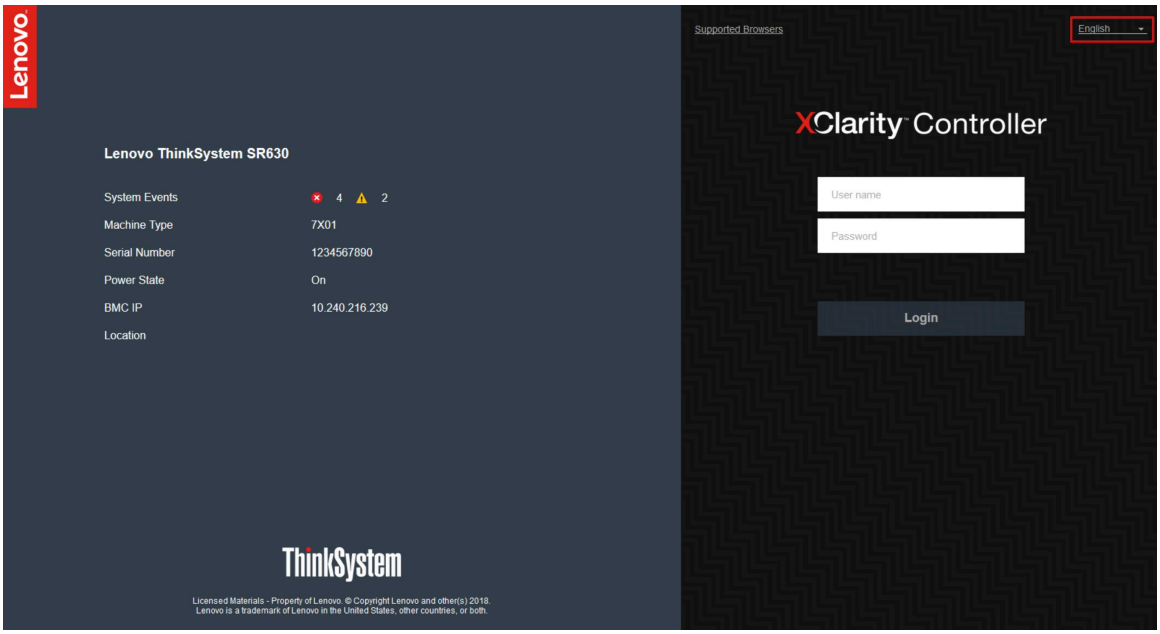
附註：在 Flex System 中，XClarity Controller 使用者帳戶由 Flex System Chassis Management Module (CMM) 管理，而且可能與上述「USERID/PASSW0RD」組合不同。

若要透過 XClarity Controller Web 介面存取 XClarity Controller，請完成下列步驟：

步驟 1. 開啟 Web 瀏覽器。在網址或 URL 欄位中，輸入要連線的 XClarity Controller IP 位址或主機名稱。

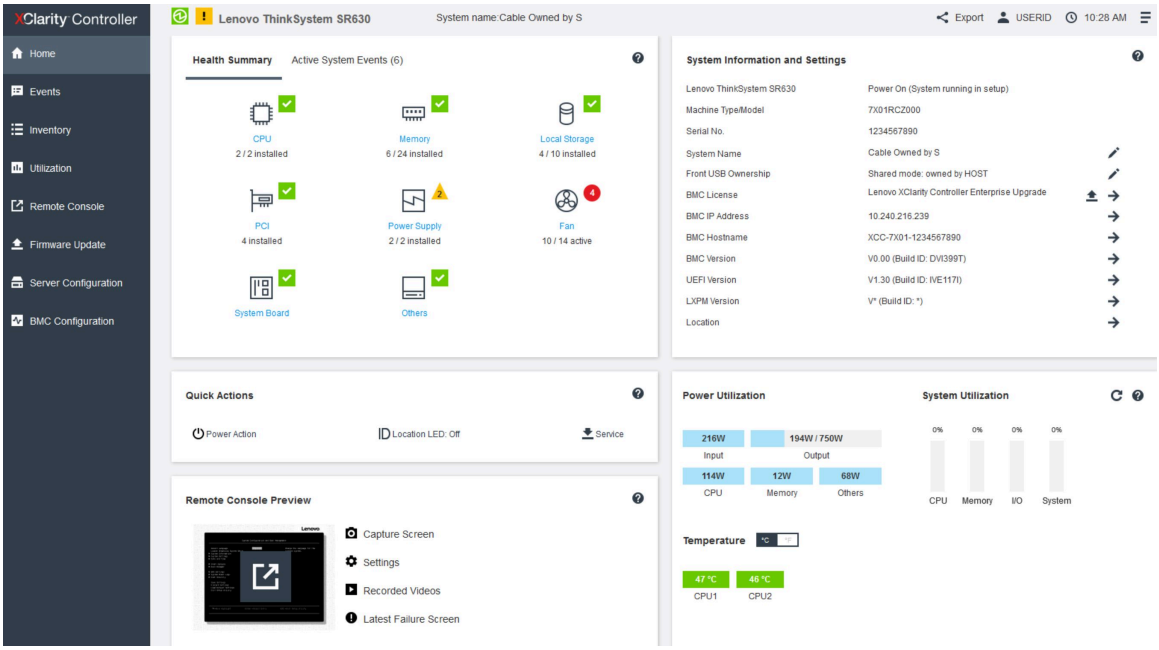
步驟 2. 在語言下拉清單中選取所需的語言。

下圖顯示「登入」視窗。



步驟 3. 在 XClarity Controller 登入視窗中，輸入使用者名稱及密碼。如果您是第一次使用 XClarity Controller，您可以向系統管理者取得使用者名稱及密碼。所有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，登入後您可能需要輸入新密碼。

步驟 4. 按一下**登入**以啟動階段作業。瀏覽器會開啟 XClarity Controller 首頁，如下圖所示。首頁顯示 XClarity Controller 管理的系統相關資訊，以及指出目前系統中存在多少嚴重錯誤 1 和多少警告 1 的圖示。



首頁基本上分為兩個部分。第一個部分是左側的導覽面板，其主題可讓您執行下列動作：

- 監視伺服器狀態
- 配置伺服器
- 配置 XClarity Controller 或 BMC
- 更新韌體

第二個部分是導覽面板右側所呈現的圖形資訊。模組化格式可供您快速檢視伺服器狀態和部分可執行的快速動作。

XClarity Controller Web 介面功能的說明

下表說明左側導覽面板中的 XClarity Controller 功能。

附註：瀏覽 Web 介面時，您也可以按一下問號圖示，以取得線上說明。

表格 1. XClarity Controller 功能

三個直欄的表格內容包括您可以從 XClarity Controller Web 介面執行的動作說明。

標籤	選項	說明
首頁	性能摘要/作用中系統事件	顯示系統中主要硬體元件的目前狀態。
	系統資訊和設定	提供常見系統資訊的摘要。
	快速動作	提供快速鏈結來控制伺服器電源和位置 LED，以及要下載服務資料的按鈕。
	電源使用率/系統使用率/溫度	提供目前電源使用率、系統使用率和整體伺服器溫度的快速概觀。
	遠端主控台預覽	在作業系統等級控制伺服器。您可以從您的電腦檢視及操作伺服器主控台。XClarity Controller 首頁的遠端主控台區段會顯示附有啟動按鈕的畫面影像。右側工具列包含下列的快速動作： • 擷取畫面

表格 1. XClarity Controller 功能（繼續）

標籤	選項	說明
		• 設定 • 錄製的視訊 • 上次失敗畫面
事件	事件日誌	提供所有硬體和管理事件的歷程清單。
	審核日誌	提供使用者動作的歷程記錄，例如登入至 Lenovo XClarity Controller、建立新使用者和變更使用者密碼。您可以使用審核日誌來追蹤及記錄 IT 系統中的鑑別和控制。
	維護歷程	顯示所有韌體更新、配置及硬體更換歷程。
	警示接收者	管理系統事件通知的接收者。它可讓您配置每一位接收者，以及管理適用於所有事件接收者的設定。您也可以產生測試事件，以驗證通知配置設定。
庫存		顯示系統中的所有元件，以及元件狀態和主要資訊。您可以按一下要顯示其他資訊的裝置。 **附註：**如需解決方案電源狀態的其他詳細資料，請參閱 SMM2 Web 介面。
使用率		以圖形或表格格式顯示伺服器及其元件的環境/元件溫度、電源使用率、電壓層次、系統子系統使用率以及風扇速度資訊。
儲存體	詳細資料	顯示儲存裝置的實體結構和儲存體配置。
	設定 RAID	檢視或修改目前的 RAID 配置，包括虛擬磁碟和實體儲存裝置的資訊。
遠端主控台		可讓您存取遠端主控台功能。您可以使用虛擬媒體功能裝載位於系統上、或透過 BMC 使用 CIFS、NFS、HTTPS 或 SFTP 可存取的網路位置上的 ISO 檔或 IMG 檔。裝載的磁碟顯示為連接至伺服器的 USB 隨身碟。
韌體更新		• 顯示韌體版本。 • 更新 XClarity Controller 韌體及伺服器韌體。
伺服器配置	配接卡	顯示已安裝的網路配接卡資訊，以及可透過 XClarity Controller 配置的設定值。
	開機選項	• 選取下次伺服器重新啟動期間的單次開機裝置。 • 變更開機模式和開機順序設定值。
	電源原則	• 在電源供應器的故障事件期間配置電源備援。 • 配置電源上限原則。 • 配置電源還原原則。 **附註：**如需解決方案電源狀態的其他詳細資料，請參閱 SMM2 Web 介面。
	伺服器內容	• 監視伺服器的各種內容、狀態狀況及設定。 • 管理伺服器啟動逾時，以偵測伺服器當機並從當機狀況中回復。 • 建立侵害訊息。侵害訊息是您可以為使用者建立的訊息，讓他們在登入 XClarity Controller 時看到。

表格 1. XClarity Controller 功能（繼續）

標籤	選項	說明
BMC 配置	備份和還原	將 XClarity Controller 的配置重設為原廠預設值，備份現行配置或是從檔案還原配置。
	授權	管理選配 XClarity Controller 功能的啟動金鑰。
	網路	配置 XClarity Controller 的網路內容、狀態和設定值。
	安全性	配置 XClarity Controller 的安全屬性、狀態和設定值。
	使用者/LDAP	• 配置 XClarity Controller 登入設定檔和廣域登入設定。 • 請檢視目前登入 XClarity Controller 的使用者帳戶。 • LDAP 標籤可配置用於一部以上 LDAP 伺服器的使用者鑑別。它也可讓您啟用或停用 LDAP 安全性，以及管理其憑證。

第 3 章　配置 XClarity Controller

使用本章的資訊，可瞭解 XClarity Controller 可用的配置選項。

配置 XClarity Controller 時，可用的重要選項如下：

- 備份和還原
- 授權
- 網路
- 安全性
- 使用者/LDAP

配置使用者帳戶/LDAP

使用本主題中的資訊，以瞭解如何管理使用者帳戶。

按一下 **BMC 配置**下的**使用者/LDAP**，以建立、修改及檢視使用者帳戶，以及配置 LDAP 設定。

本端使用者標籤會顯示在 XClarity Controller 中配置的使用者帳戶，以及目前有哪些使用者帳戶登入 XClarity Controller。

LDAP 標籤會顯示用來存取保留在 LDAP 伺服器上之使用者帳戶的 LDAP 配置。

使用者鑑別方法

使用本主題中的資訊，以瞭解 XClarity Controller 可用來鑑別登入嘗試的模式。

按一下**允許登入來源**，以選取用來鑑別使用者登入嘗試的方式。您可以選取下列其中一種鑑別方法：

- **僅限本端：**藉由搜尋 XClarity Controller 中配置的本端使用者帳戶來鑑別使用者。如果沒有相符的使用者 ID 和密碼，會拒絕存取。
- **僅限 LDAP：**XClarity Controller 會嘗試使用保存在 LDAP 伺服器上的認證來鑑別使用者。**不會**使用此鑑別方法來搜尋 XClarity Controller 中的本端使用者帳戶。
- **先本端後 LDAP：**先嘗試本端鑑別。如果本端鑑別失敗，則會嘗試 LDAP 鑑別。
- **先 LDAP 後本端使用者：**先嘗試 LDAP 鑑別。如果 LDAP 鑑別失敗，則會嘗試本端鑑別。

附註：

- 只有本端管理的帳戶會與 IPMI 和 SNMP 介面共用。這些介面不支援 LDAP 鑑別。
- 當**允許登入來源**欄位設定為**僅限 LDAP** 時，IPMI 和 SNMP 使用者可以使用本端管理的帳戶登入。

建立新的使用者帳戶

使用本主題中的資訊來建立新的本端使用者。

建立使用者

按一下**建立**，以建立新的使用者帳戶。

請完成下列欄位：**使用者名稱**、**密碼**、**確認密碼**和**權限層級**。如需權限層級的進一步詳細資訊，請參閱下一節。

使用者權限層級

可供使用的使用者權限層級如下：

監督者

監督者使用者權限層級無任何限制。

唯讀

唯讀使用者權限層級具有唯讀存取權，無法執行檔案傳送之類的動作、電源和重新啟動動作，或是遠端顯示功能。

自訂

自訂使用者權限層級可設定容許使用者執行的動作，讓使用者權限具有更高度自訂化的設定檔。

選取下列其中一個或多個自訂使用者權限層級：

配接器配置 – 網路功能與安全性

使用者可以修改「安全」、「網路」和「序列埠」頁面中的配置參數。

使用者帳戶管理

使用者可以新增、修改或刪除使用者，以及變更廣域登入設定。

遠端主控台存取權

使用者可以存取遠端主控台。

遠端主控台和遠端磁碟存取權

使用者可以存取遠端主控台及虛擬媒體特性。

遠端伺服器電源/重新啟動

使用者可以對伺服器執行電源開啟和重新啟動功能。

配接器配置 – 基本

使用者可以修改「伺服器內容」和「事件」頁面中的配置參數。

清除事件日誌的能力

使用者可以清除事件日誌。任何人都可以檢視事件日誌；但是清除日誌需要此權限層級。

配接器配置 – 進階（韌體更新、重新啟動 BMC、還原配置）

使用者在配置 XClarity Controller 時沒有任何限制。此外，使用者具有對 XClarity Controller 的管理存取權。管理存取權包括下列進階功能：韌體更新、PXE 網路開機、還原 XClarity Controller 原廠預設值、從配置檔修改和還原 XClarity Controller 設定，以及重新啟動和重設 XClarity Controller。

當使用者設定 XClarity Controller 登入 ID 的權限層級時，會根據下列優先順序，設定對應 IPMI 使用者 ID 的 IPMI 專用權層級。

- 如果使用者將 XClarity Controller 登入 ID 權限層級設為**監督者**，IPMI 專用權層級會設為「管理者」。
- 如果使用者將 XClarity Controller 登入 ID 權限層級設為**唯讀**，IPMI 專用權層級會設為「使用者」。
- 如果使用者將 XClarity Controller 登入 ID 權限層級設為下列任何存取權類型，IPMI 專用權層級會設為「管理者」：
  - 使用者帳戶管理存取
  - 遠端主控台存取權
  - 遠端主控台和遠端磁碟存取權
  - 配接器配置 - 網路功能與安全性
  - 配接器配置 - 進階
- 如果使用者將 XClarity Controller 登入 ID 權限層級設為**遠端伺服器電源/重新啟動存取**或**清除事件日誌的能力**，IPMI 專用權層級會設為「操作員」。

- 如果使用者將 XClarity Controller 登入 ID 權限層級設為**配接器配置 - 基本**，IPMI 專用權層級會設為「使用者」。

SNMPv3 設定

如果要為使用者啟用 SNMPv3 存取權，請選取 **SNMPv3 設定**旁邊的勾選框。下列使用者存取權選項說明：

存取類型
僅支援 **GET** 作業。XClarity Controller 不支援 SNMPv3 **SET** 作業。SNMP3 只能執行查詢作業。

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

鑑別通訊協定
僅支援 **HMAC-SHA** 做為鑑別通訊協定。SNMPv3 安全模式會使用此演算法來進行鑑別。

保密通訊協定
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。支援的方法為 **CBC-DES** 和 **AES**。

附註：即使 SNMPv3 使用者使用包含重複字串的密碼，仍將允許其存取 XClarity Controller。以下兩個範例供您參考。

- 如果密碼設定為「**11111111**」（包含八個 1 的八位數），而使用者在輸入密碼時意外超過八個 1，該使用者仍然可以存取 XClarity Controller。例如，如果輸入的密碼為「**1111111111**」（包含十個 1 的十位數），仍將授與存取權。重複字串將視為具有相同的金鑰。
- 如果密碼設定為「**bertbert**」，而使用者意外將密碼輸入成「**bertbertbert**」，該使用者仍然可以存取 XClarity Controller。這兩個密碼視為具有相同的金鑰。

如需進一步的詳細資料，請參閱 RFC 3414 網際網路標準文件 (https://tools.ietf.org/html/rfc3414) 的第 72 頁。

SSH 金鑰

XClarity Controller 支援「SSH 公開金鑰鑑別」（RSA 金鑰類型）。如果要新增 SSH 金鑰至本端使用者帳戶，請選取 **SSH 金鑰**旁邊的勾選框。提供下列兩種選項：

選取金鑰檔
選取要從伺服器匯入 XClarity Controller 中的 SSH 金鑰檔。

在文字欄位中輸入金鑰
將 SSH 金鑰的資料貼上或輸入文字欄位中。

附註：

- 部分 Lenovo 工具在伺服器作業系統上執行時，可能會建立暫時的使用者帳戶，用於存取 XClarity Controller。此暫時帳戶是無法檢視的，且不會佔用 12 個本端使用者帳戶的位置。此帳戶是使用隨機的使用者名稱（例如「20luN4SB」）和密碼來建立。此帳戶只能用於存取內部 Ethernet over USB 介面上的 XClarity Controller，且僅適用於 CIM-XML 和 SFTP 介面。此暫時帳戶的建立和移除，以及工具使用這些認證執行的任何動作都會記錄在審核日誌中。
- 對於 SNMPv3 引擎 ID，XClarity Controller 使用十六進位字串表示該 ID。此十六進位字串是從預設 XClarity Controller 主機名稱轉換而來。請參閱以下範例：

  主機名稱「XCC-7X06-S4AHJ300」先轉換成 ASCII 格式：88 67 67 45 55 88 48 54 45 83 52 65 72 74 51 48 48

  然後使用 ASCII 格式生成十六進位字串（忽略中間的空格）：58 43 43 2d 37 58 30 36 2d 53 34 41 48 4a 33 30 30

刪除使用者帳戶

使用本主題中的資訊來移除本端使用者帳戶。

如果要刪除本端使用者帳戶，請按一下您希望移除的帳戶的那一列上的垃圾桶圖示。如果您獲得授權，您可以移除自己的帳戶或其他使用者的帳戶（即使他們目前已登入），除非這是剩下唯一具有「使用者帳戶管理」權限的帳戶。刪除使用者帳戶時已在進行中的階段作業將不會自動終止。

使用雜湊密碼進行鑑別

使用本主題中的資訊，以瞭解如何使用雜湊密碼進行鑑別。

除了使用密碼和 LDAP/AD 使用者帳戶，XClarity Controller 也支援使用協力廠商雜湊密碼進行鑑別。特殊密碼使用單向雜湊 (SHA256) 格式，而且受 XClarity Controller Web、OneCLI 和 CLI 介面支援。不過請注意，XCC SNMP、IPMI 和 CIM 介面的鑑別都不支援協力廠商雜湊密碼。只有 OneCLI 工具和 XCC CLI 介面可以建立採用雜湊密碼的新帳戶，或執行雜湊密碼更新。如果啟用了讀取雜湊密碼的功能，XClarity Controller 也允許 OneCLI 工具和 XClarity Controller CLI 介面擷取雜湊密碼。

透過 XClarity Controller Web 設定雜湊密碼

按一下 **BMC 配置**下的**安全性**，然後捲動至 **Security Password Manager** 區段以啟用或停用協力廠商密碼功能。如果啟用，便會採用協力廠商雜湊密碼進行登入鑑別。也可以啟用或停用從 XClarity Controller 擷取協力廠商雜湊密碼。

附註：依預設，**協力廠商密碼**和**允許擷取協力廠商密碼**功能都已停用。

若要檢查使用者密碼是**原生**還是**協力廠商密碼**，請按一下 **BMC 配置**下的**使用者/LDAP** 以取得詳細資料。相關資訊位於**進階屬性**欄下方。

附註：

- 如果密碼是協力廠商密碼，則使用者無法加以變更，而且**密碼**和**確認密碼**欄位都已變成灰色。
- 如果協力廠商密碼已過期，則使用者登入程序期間將顯示警告訊息。

透過 OneCLI 功能設定雜湊密碼

- 啟用功能

  ```
  $ sudo OneCli config set IMM.ThirdPartyPassword Enabled
  ```

- 建立雜湊密碼（無 Salt）。以下顯示使用密碼 **password123** 登入 XClarity Controller 的範例。

  ```
  $ pwhash = `echo -n password123 | openssl dgst -sha256 | awk '{print $NF}'`
  $ echo $pwhash 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
  $ sudo OneCli config set IMM.Loginid.2 admin
  $ sudo OneCli config set IMM.SHA256Password.2 $pwhash
  $ sudo OneCli config set IMM.SHA256PasswordSalt.2 ""
  ```

- 建立採用雜湊密碼的使用者（含 Salt）。以下顯示使用密碼 **password123** 登入 XClarity Controller 的範例。Salt=abc。

  ```
  $ pwhash = `echo -n password123abc | openssl dgst -sha256 | awk '{print $NF}'`
  $ echo $pwhash 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
  $ sudo OneCli config set IMM.Loginid.3 Admin
  $ sudo OneCli config set IMM.SHA256Password.3 $pwhash
  $ sudo OneCli config set IMM.SHA256PasswordSalt.3 'abc'
  ```

- 擷取雜湊密碼和 salt。

```
$ sudo OneCli config set IMM.ThirdPartyPasswordReadable Enabled
$ sudo OneCli config show IMM.SHA256Password.3
$ sudo OneCli config show IMM.SHA256PasswordSalt.3
```

- 刪除雜湊密碼和 salt。

```
$ sudo OneCli config set IMM.SHA256Password.3 ""
$ sudo OneCli config set IMM.SHA256PasswordSalt.3 ""
```

- 為現有帳戶設定雜湊密碼。

```
$ sudo OneCli config set IMM.Loginid.2 admin
$ sudo OneCli config set IMM.Password.2 Passw0rd123abc
$ sudo OneCli config set IMM.SHA256Password.2 $pwhash
$ sudo OneCli config set IMM.SHA256PasswordSalt.2 ""
```

附註：雜湊密碼一旦設定，將立即生效。原始標準密碼將不再有效。在此範例中，除非刪除雜湊密碼，否則無法再次使用原始標準密碼 **Passw0rd123abc**。

透過 CLI 功能設定雜湊密碼

- 啟用功能

```
> hashpw -sw enabled
```

- 建立雜湊密碼（無 Salt）。以下顯示使用密碼 **password123** 登入 XClarity Controller 的範例。

```
$ pwhash = `echo -n password123 | openssl dgst -sha256 | awk '{print $NF}'`
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
> users -2 -n admin -shp 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a
super
```

- 建立採用雜湊密碼的使用者（含 Salt）。以下顯示使用密碼 **password123** 登入 XClarity Controller 的範例。Salt=abc。

```
$ pwhash = `echo -n password123abc | openssl dgst -sha256 | awk '{print $NF}'`
$ echo $pwhash 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
> users -3 -n Admin -shp 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
-ssalt 'abc' -a super
```

- 擷取雜湊密碼和 salt。

```
> hashpw -re enabled
> users -3 -ghp -gsalt
```

- 刪除雜湊密碼和 salt。

```
> users -3 -shp "" -ssalt ""
```

- 為現有帳戶設定雜湊密碼。

```
> users -2 -n admin -p Passw0rd123abc -shp 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd6
2a11ef721d1542d8 -a super
```

附註：雜湊密碼一旦設定，將立即生效。原始標準密碼將不再有效。在此範例中，除非刪除雜湊密碼，否則無法再次使用原始標準密碼 **Passw0rd123abc**。

設定雜湊密碼後，請記得不要使用此密碼登入 XClarity Controller。登入時，您將需要使用純文字密碼。在以下範例中，純文字密碼是「password123」。

```
$ pwhash = ‘echo –n password123 | openssl dgst –sha256 | awk '{print $NF}''
```

```
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

> users -2 -n admin -shp 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a super
```

配置廣域登入設定

使用本主題中的資訊，可配置套用在所有使用者的登入及密碼原則設定。

Web 閒置階段作業逾時

使用本主題中的資訊來設定 Web 閒置階段作業逾時選項。

在 **Web 閒置階段作業逾時**欄位中，您可以指定 Web 階段作業在處於非作用狀態多久（以分鐘為單位）之後，XClarity Controller 會與其中斷連接。最長等待時間是 1,440 分鐘。如果設定為 0，則 Web 階段作業永不到期。

XClarity Controller 韌體最多可支援六個同步 Web 階段作業。若要釋出階段作業供其他使用者使用，建議您在完成時登出 Web 階段作業，而不要依賴閒置逾時自動關閉您的階段作業。

附註：如果您在會自動重新整理的 XClarity Controller 網頁上將瀏覽器保留為開啟狀態，您的 Web 階段作業不會因為閒置而自動關閉。

帳戶安全原則設定

使用此資訊來瞭解及設定伺服器的帳戶安全原則。

附註：在 Flex System 中，帳戶安全原則設定由 Flex System Chassis Management Module (CMM) 管理，且無法透過 XCC 修改。使用 CMM 配置帳戶安全原則時，請注意下列事項：

- 與 XCC 不同，CMM 沒有**密碼有效警告期間（天）**設定。如果在 CMM 中將**密碼有效期間**配置為超過 5 天，XCC 會將密碼有效警告期間設定為 5 天。相反地，如果設定不到 5 天，密碼有效警告期間將與**密碼有效期間**中輸入的值相同。
- 對於**登入失敗次數上限（次）**設定，CMM 中設定的範圍為 0-100 次。不過，XCC 中定義的範圍為 0-10 次。因此，當使用者在 CMM 中選取了超過 10 次的值，XCC 仍然會將登入失敗次數上限設定為 10 次。
- 對於**最短密碼變更間隔（小時）**設定，CMM 中設定的範圍為 0-1440 小時。不過，XCC 中定義的範圍為 0-240 小時。因此，當使用者在 CMM 中選取了超過 240 小時的值，XCC 仍然會將最短密碼變更間隔設定為 240 小時。

下列資訊是安全設定的欄位說明。

強制在第一次存取時變更密碼

使用預設密碼設定新使用者之後，選取此勾選框會強制使用者在第一次登入時變更其密碼。此欄位的預設值為已啟用勾選框。

強制下次登入時必須變更預設帳戶密碼

提供了製造選項，以在第一次成功登入之後重設預設 USERID Profile。啟用此勾選框時，必須先變更預設密碼，然後才能使用帳戶。新密碼必須遵循所有作用中密碼強制執行規則。此欄位的預設值為已啟用勾選框。

需要複式密碼

此選項框預設為勾選，複式密碼必須遵循下列規則：

- 僅包含以下字元（不允許空格字元）：A-Z、a-z、0-9、~`!@#$%^&*()-+={}[]|:;"'<>,?/._
- 必須至少包含一個字母
- 必須至少包含一個數字
- 必須至少包含下列組合的其中兩種：

— 至少一個大寫字母。

— 至少一個小寫字母。

— 至少一個特殊字元。

- 不允許其他字元（尤其是空格或空白字元）
- 密碼中同一字元不能連續使用兩次以上（例如「aaa」）。
- 密碼不能與使用者名稱完全相同、僅僅重複使用者名稱一或多次，或是使用者名稱的相反字元順序。
- 密碼長度必須最少 8 個字元，最多 32 個字元

如果未勾選選項框，則密碼長度下限所指定的數字可設為 0-32 個字元。如果密碼長度下限設為 0，則帳戶密碼可為空白。

密碼有效期間（天）
此欄位包含在必須變更密碼之前允許的密碼有效期限上限。支援的值為 0 至 30 天。此欄位的預設值為 14 天。

密碼有效警告期間（天）
此欄位包含密碼到期之前警告使用者的天數。如果其設定為 0，則不會傳送警告。支援的值為 0 至 30 天。此欄位的預設值為 14 天。

密碼長度下限
此欄位包含密碼的基本長度。此欄位支援 8 至 32 個字元。此欄位的預設值為 10。

密碼重複使用週期下限
此欄位包含無法重複使用先前密碼的數目。最多可以比對前十個密碼。選取 0 可容許重複使用所有先前的密碼。支援的值為 0 至 10。此欄位的預設值為 5。

最短密碼變更間隔（小時）
此欄位包含使用者必須等待的密碼變更間隔時間。支援的值為 0 至 240 小時。此欄位的預設值為 1 小時。

登入失敗次數上限（次）
此欄位包含在使用者鎖定一段時間之前，容許的失敗登入嘗試次數。支援的值為 0 至 10。此欄位的預設值為 5 次登入失敗。

已達登入失敗數目上限後的鎖定期間（分鐘）
此欄位指定在達到登入失敗次數上限後，XClarity Controller 子系統會停用嘗試遠端登入的時間（以分鐘為單位）。支援的值為 0 至 2,880 分鐘。此欄位的預設值為 60 分鐘。

配置 LDAP

使用本主題中的資訊來檢視或變更 XClarity Controller LDAP 設定。

LDAP 支援包含：

- 支援 LDAP 通訊協定第 3 版 (RFC-2251)
- 支援標準 LDAP 用戶端 API (RFC-1823)
- 支援標準 LDAP 搜尋過濾器語法 (RFC-2254)
- 支援適用於傳輸層安全的輕量型目錄存取通訊協定 (v3) 擴充 (RFC-2830)

LDAP 實作支援下列 LDAP 伺服器：

- Microsoft Active Directory（Windows 2003、Windows 2008、Windows 2012、Windows 2016、Windows 2019）
- Microsoft Active Directory 應用程式模式 (Windows 2003 Server)
- Microsoft 輕量型目錄服務（Windows 2008、Windows 2012）

- Novell eDirectory Server 8.7、8.8 和 9.4 版
- OpenLDAP Server 2.1、2.2、2.3 和 2.4

按一下 **LDAP** 標籤可檢視或修改 XClarity Controller LDAP 設定。

XClarity Controller 可以透過中央 LDAP 伺服器，還有儲存在 XClarity Controller 本身內的本端使用者帳戶遠端鑑別使用者的存取權。可以使用 IBMRBSPermissions 字串為每個使用者帳戶指定權限。您還可以使用 LDAP 伺服器將使用者指派給群組，並執行除了一般使用者（密碼檢查）鑑別之外的群組鑑別。例如，XClarity Controller 可以與一個以上的群組相關聯，唯有當使用者屬於至少一個與 XClarity Controller 相關聯的群組時，使用者才能通過群組鑑別。

如果要配置 LDAP 伺服器，請完成下列步驟：

1. 在 **LDAP 伺服器資訊**下，項目清單中提供下列選項：
   - **使用 LDAP 伺服器只進行鑑別（使用本端授權）**：此選項會指示 XClarity Controller 僅使用認證來鑑別 LDAP 伺服器，以及擷取群組成員資格資訊。您可以在「Active Directory 設定」區段中配置群組名稱和權限。
   - **使用 LDAP 伺服器進行鑑別和授權**：此選項會指示 XClarity Controller 使用認證來鑑別 LDAP 伺服器，以及識別使用者權限。

   附註：您可以手動配置或透過 DNS SRV 記錄動態探索要用於鑑別的 LDAP 伺服器。
   - **使用預先配置的伺服器**：您可以透過輸入各伺服器的 IP 位址或主機名稱（如果已啟用 DNS），來配置最多四個 LDAP 伺服器。每一個伺服器的埠號是選用的。如果此欄位保留空白，不安全的 LDAP 連線會使用預設值 389。對於安全的連線，預設埠值為 636。您必須至少配置一個 LDAP 伺服器。
   - **使用 DNS 尋找伺服器**：您可以選擇動態探索 LDAP 伺服器。會使用 RFC2782 中所述的機制（DNS RR 適用於指定服務位置）來找出 LDAP 伺服器。這稱為 DNS SRV。您必須指定完整網域名稱 (FQDN) 以做為 DNS SRV 要求中的網域名稱。
     - **AD 樹系**：在具有跨網域中通用群組的環境中，必須配置樹系名稱（網域集）以便探索所需的廣域型錄（GC）。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。
     - **AD 網域**：您必須指定完整網域名稱 (FQDN) 以做為 DNS SRV 要求中的網域名稱。

   如果您要啟用安全 LDAP，請按一下**啟用安全 LDAP** 勾選框。若要支援安全 LDAP，必須備妥有效的 SSL 憑證，且必須將至少一個 SSL 用戶端授信憑證匯入 XClarity Controller。LDAP 伺服器必須支援傳輸層安全 (TLS) 1.2 版本，以使其與 XClarity Controller 安全 LDAP 用戶端相容。如需憑證處理的相關資訊，請參閱第 34 頁 「SSL 憑證處理」。
2. 請填寫**其他參數**下的資訊。參數說明如下。

   連結方法

   您必須先傳送連結要求，才能搜尋或查詢 LDAP 伺服器。此欄位控制對 LDAP 伺服器執行此起始連結的方式。下列連結方法可供使用：
   - **無需認證**

     使用此方法可在沒有識別名稱 (DN) 或密碼的情況下進行連結。強烈建議不要選取此方法，因為大部分伺服器都配置為禁止對特定使用者記錄執行搜尋要求。
   - **使用配置的認證**

     使用此方法可使用配置的用戶端 DN 和密碼進行連結。
   - **使用登入認證**

     使用此方法可使用在登入程序期間提供的認證進行連結。透過 DN、部分 DN、完整網域名稱，或透過符合在 XClarity Controller 所配置 UID 搜尋屬性的使用者 ID，皆可提供使用者 ID。如果提供的認證類似於部分 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 做為已配置根 DN 的字首。如果此連結嘗試失敗，最終的嘗試是將字首 cn= 新增至登入認證，然後將此結果字串新增至已配置根 DN 前方。

若起始連結成功，便會執行搜尋，以在 LDAP 伺服器上尋找屬於所登入使用者的項目。必要的話，會再次嘗試進行連結，此時會使用從使用者的 LDAP 記錄擷取的 DN 和在登入程序期間輸入的密碼。如果第二次嘗試連結失敗，則會拒絕使用者存取。第二次連結僅在使用**無需認證**或**使用配置的認證**連結方法時執行。

根識別名稱 (DN)

這是 LDAP 伺服器上目錄樹根項目的識別名稱 (DN)（例如，dn=mycompany,dc=com）。此 DN 用做所有搜尋要求的基本物件。

UID 搜尋屬性

連結方法設定為**無需認證**或**使用配置的認證**時，LDAP 伺服器的起始連結後接搜尋要求，以擷取使用者的相關特定資訊，包括使用者的 DN、登入權限及群組成員資格。此搜尋要求必須指定代表該伺服器上使用者 ID 的屬性名稱。此屬性名稱是在此欄位中配置。在 Active Directory 伺服器上，屬性名稱通常為 **sAMAccountName**。在 Novell eDirectory 和 OpenLDAP 伺服器上，屬性名稱為 **uid**。如果此欄位保留空白，預設值為 **uid**。

群組過濾器

群組過濾器欄位用於群組鑑別。在順利驗證使用者的認證之後，會嘗試進行群組鑑別。如果群組鑑別失敗，則會拒絕使用者的登入嘗試。配置群組過濾器後，它會用於指定 XClarity Controller 所屬的群組。這表示使用者必須屬於至少其中一個所配置的群組，群組鑑別才會成功。如果**群組過濾器**欄位保留空白，群組鑑別會自動成功。如果配置了群組過濾器，系統會嘗試將清單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，群組鑑別會成功。
此比對會區分大小寫。過濾器限制為 511 個字元，且可以由一個以上的群組名稱組成。必須使用冒號 (:) 字元來分隔多個群組名稱。將會忽略前導和尾端空格，但其他任何空格都會視為群組名稱的一部分。

附註：不再將萬用字元 (*) 視為萬用字元。已停用萬用字元概念，以避免暴露安全性問題。您可以將群組名稱指定為完整 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 為 cn=adminGroup, dc=mycompany, dc=com 的群組。

僅在 Active Directory 環境中支援巢狀群組成員資格。例如，如果某位使用者是 GroupA 和 GroupB 的成員，且 GroupA 也是 GroupC 的成員，則該使用者也可以說是 GroupC 的成員。如果已搜尋 128 個群組，巢狀搜尋便會停止。會先搜尋某個層次中的群組，然後再搜尋較低層次中的群組。不偵測迴圈。

群組搜尋屬性

在 Active Directory 或 Novell eDirectory 環境中，**群組搜尋屬性**欄位可指定用於識別使用者所屬群組的屬性名稱。在 Active Directory 環境中，屬性名稱為 **memberOf**。在 eDirectory 環境中，屬性名稱為 **groupMembership**。在 OpenLDAP 伺服器環境中，通常會將使用者指派給其 objectClass 等於 PosixGroup 的群組。在該環境定義中，此欄位指定用於識別特定 PosixGroup 成員的屬性名稱。此屬性名稱為 **memberUid**。如果此欄位保留空白，則過濾器中的屬性名稱預設為 **memberOf**。

登入權限屬性

透過 LDAP 伺服器順利鑑別使用者時，必須擷取使用者的登入權限。若要擷取登入權限，傳送至伺服器的搜尋過濾器必須指定與登入權限相關聯的屬性名稱。**登入權限屬性**欄位可指定該屬性名稱。如果此欄位保留空白，將為使用者指派預設的唯讀權限（假設使用者已通過使用者和群組鑑別）。
LDAP 伺服器傳回的屬性值會搜尋關鍵字字串 IBMRBSPermissions=。此關鍵字字串後面必須緊接輸入為 12 個連續的 0 或 1 的位元字串。每一個位元都代表一組功能。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。位元位置的值 1 將啟用與該位元位置相關聯的功能。在位元位置的值 0 則停用與該位元位置相關聯的功能。
字串 IBMRBSPermissions=010000000000 是有效的範例。使用 IBMRBSPermissions= 關鍵字可讓它置於此欄位中的任何位置。這可讓 LDAP 管理者重複使用現有屬性；因此，可防止延伸 LDAP 綱目。這也可讓屬性用於其原始用途。您可以在此欄位中的任何位置新增關鍵字字串。您使用的屬性容許自由格式的字串。順利擷取屬性時，會根據下表中的資訊解譯 LDAP 伺服器傳回的值。

表格 2. 權限位元

此三欄表格提供位元位置的說明。

位元位置	功能	說明
0	一律拒絕	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	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	使用者具有唯讀存取權，且無法執行任何維護程序（例如，重新啟動、遠端動作或韌體更新），或進行修改（例如，儲存、清除或還原功能）。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。如果設定了任何其他位元，則會忽略此位元。
3	網路功能與安全性	使用者可以修改安全性、網路通訊協定、網路介面、埠指派及序列埠配置。
4	使用者帳戶管理	使用者可以新增、修改或刪除使用者，以及變更登入設定檔視窗中的「廣域登入設定」。
5	遠端主控台存取權	使用者可以存取遠端伺服器主控台。
6	遠端主控台和遠端磁碟存取權	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。
7	遠端伺服器電源/重新啟動存取權	使用者可以存取遠端伺服器的電源開啟和重新啟動功能。
8	基本配接器配置	使用者可以修改「系統設定」和「警示」視窗中的配置參數。
9	清除事件日誌的能力	使用者可以清除事件日誌。 **附註：**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事件日誌。
10	進階配接器配置	使用者在配置 XClarity Controller 時沒有任何限制。此外，使用者具有對 XClarity Controller 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 XClarity Controller 原廠預設值、從配置檔修改和還原配接卡配置，以及重新啟動/重設 XClarity Controller。
11	保留	此位元位置保留以供日後使用。如果未設定任何位元，則使用者具有唯讀權限。直接從使用者記錄擷取的登入權限將享有優先順序。 如果登入權限屬性不在使用者的記錄中，則會嘗試從使用者所屬的群組擷取權限。此作業是在群組鑑別階段中執行。將為使用者指派對所有群組的所有位元進行 OR（含）運算的結果。 僅在所有其他位元設定為零時，設定「唯讀存取權」位元（位置 2）。如果為任何群組設定「一律拒絕」位元（位置 0），將拒絕使用者存取。「一律拒絕」位元（位置 0）一律優先於所有其他位元。

如果不設定這些位元，則會將使用者的預設值設定為**唯讀**。

請注意，直接從使用者記錄擷取的登入權限將享有優先順序。如果使用者在其記錄中沒有登入權限屬性，則會嘗試從使用者所屬且符合群組過濾器（如果已配置）的群組中擷取權限。在此情況下，將為使用者指派所有群組的所有位元之內含 OR。同樣地，僅當所有其他位元為零時，才會設定**唯讀存取權**位元。此外請注意，如果為任何群組設定**一律拒絕**位元，將拒絕使用者存取。**一律拒絕**位元一律優先於其他所有位元。

附註：若您允許使用者修改基本、網路和/或安全相關的配接卡配置參數，您應該考量賦予這位使用者重新啟動 XClarity Controller 的能力（位元位置 10）。否則，如果沒有此能力，使用者或許能夠變更參數（例如，配接卡的 IP 位址），但參數無法生效。

3. 選擇是否要在 **Active Directory 設定**下**為 Active Directory 使用者啟用以角色為基礎的安全性加強**（如果已使用**使用 LDAP 伺服器進行鑑別和授權**模式），或配置**本端授權的群組**（如果已使用**使用 LDAP 伺服器僅進行鑑別（使用本端授權）**模式）。

   - **為 Active Directory 使用者啟用以角色為基礎的安全性加強**

     若啟用「以角色為基礎的安全性加強」設定，則必須配置自由格式的伺服器名稱，以做為此特定 XClarity Controller 的目標名稱。透過「角色型安全 (RBS) 嵌入式管理單元」，便可將目標名稱與 Active Directory 伺服器中一個以上的角色相關聯。透過建立受管理目標、提供特定名稱，然後將目標與適當的角色相關聯，即可達成此目的。如果已在此欄位中配置名稱，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 XClarity Controller（目標）。當使用者登入 XClarity Controller 並透過 Active Directory 進行鑑別時，將會從目錄中擷取使用者所屬的角色。指派給使用者的權限擷取自適當的角色，這些角色也擁有做為成員且目標符合這裡所配置的伺服器名稱，或擁有符合任何 XClarity Controller 的目標。多個 XClarity Controller 可共用相同的目標名稱。這可用於將多個 XClarity Controller 組合在一起，並使用單一管理目標將相同角色指派給這些 XClarity Controller。相反地，每個 XClarity Controller 可獲給定一個唯一名稱。

   - **本端授權的群組**

     配置群組名稱以為使用者群組提供本端授權規格。可以為每個群組名稱指派與上表中所述相同的權限（角色）。LDAP 伺服器會將使用者與群組名稱相關聯。使用者登入時，會獲指派與使用者所屬群組相關聯的權限。按一下「+」圖示可配置更多群組，按一下「x」圖示可刪除群組。

配置網路通訊協定

使用本主題中的資訊來檢視或建立 XClarity Controller 的網路設定。

配置乙太網路設定

使用本主題中的資訊，可檢視或變更 XClarity Controller 透過乙太網路連線進行通訊的方式。

XClarity Controller 使用兩個網路控制器。一個網路控制器是連接至專用管理埠，而另一個網路控制器則連接至共用埠。每個網路控制器都已獲指派其本身的燒錄 MAC 位址。如果使用 DHCP 將 IP 位址指派給 XClarity Controller，當使用者切換網路埠時，或發生從專用網路埠到共用網路埠的失效接手時，DHCP 伺服器可能會將不同的 IP 位址指派給 XClarity Controller。建議使用者在使用 DHCP 時，應使用主機名稱來存取 XClarity Controller，而不要依賴 IP 位址。即使 XClarity Controller 網路埠未變更，DHCP 伺服器仍然可能在 DHCP 租賃過期時，或在 XClarity Controller 重新開機時，將不同的 IP 位址指派給 XClarity Controller。如果使用者需要使用不變的 IP 位址來存取 XClarity Controller，則應針對靜態 IP 位址 (而非 DHCP) 進行 XClarity Controller 配置。

按一下 **BMC 配置**下的**網路**，以修改 XClarity Controller 乙太網路設定。

配置 XClarity Controller 主機名稱

預設 XClarity Controller 主機名稱是由字串「XCC -」後接伺服器機型和伺服器序號組合產生（例如「XCC-7X03-1234567890」）。您可以變更 XClarity Controller 主機名稱（在此欄位輸入最多 63 個字元）。主機名稱不能包含句點 (.)，而且僅能使用字母、數字、連字號和底線字元。

乙太網路埠

此設定控制管理控制器所用乙太網路埠的啟用，包括共用和專用埠。

啟用後，則不會為所有乙太網路埠指派任何 IPv4 或 IPv6 位址，並阻止對任何乙太網路配置進行任何進一步的變更。

附註：此設定不會影響伺服器前面的 USB LAN 介面或 USB 管理埠。這些介面具有自己的專用啟用設定。

配置 IPv4 網路設定

若要使用 IPv4 乙太網路連線，請完成下列步驟：

1. 啟用 **IPv4** 選項。

   附註：停用乙太網路介面會阻止從外部網路存取 XClarity Controller。
2. 在**方法**欄位中選取下列其中一個選項：
   - **從 DHCP 取得 IP**：XClarity Controller 會從 DHCP 伺服器取得其 IPv4 位址。
   - **使用靜態 IP 位址**：XClarity Controller 會以使用者指定的值作為其 IPv4 位址。
   - **先 DHCP 後靜態 IP 位址**：XClarity Controller 會嘗試從 DHCP 伺服器取得其 IPv4 位址，但如果嘗試失敗，XClarity Controller 會以使用者指定的值作為其 IPv4 位址。
3. 在**靜態位址**欄位中，輸入您要指派給 XClarity Controller 的 IP 位址。

   附註：IP 位址必須包含 0 至 255 的四個整數，無空格且由句點區隔。如果將此方法設定為**從 DHCP 取得 IP**，則無法配置此欄位。
4. 在**網路遮罩**欄位中，輸入 XClarity Controller 使用的子網路遮罩。

   附註：子網路遮罩必須包含 0 至 255 的四個整數，無空格或連續的句點，且由句點區隔。預設值為 255.255.255.0。如果將此方法設定為**從 DHCP 取得 IP**，則無法配置此欄位。
5. 在**預設閘道**欄位中，輸入您的網路閘道路由器。

   附註：閘道位址必須包含 0 至 255 的四個整數，無空格或連續的句點，且由句點區隔。如果將此方法設定為**從 DHCP 取得 IP**，則無法配置此欄位。

配置進階乙太網路設定

按一下**進階乙太網路**標籤，以設定其他乙太網路設定值。

附註：在 Flex System 中，VLAN 設定由 Flex System CMM 管理，且無法在 XClarity Controller 中修改。

如果要啟用虛擬 LAN (VLAN) 標記，請選取**啟用 VLAN** 勾選框。在啟用 VLAN 及配置 VLAN ID 時，XClarity Controller 僅接受具有指定 VLAN ID 的封包。VLAN ID 可以使用 1 與 4094 之間的數值配置。

從 **MAC 選項**清單中，選擇下列其中一個選項：

- 使用燒錄 MAC 位址

  燒錄 MAC 位址選項是製造商指派給此 XClarity Controller 的唯一實際位址。此位址是唯讀欄位。
- 使用自訂 MAC 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 `00000000000` 至 `FFFFFFFFFFFF` 的十六進位值。此值的格式必須是 **xx:xx:xx:xx:xx:xx**，其中 **x**是數字 0 到 9 或「a」到「f」的十六進位值。XClarity Controller 不支援使用多重播送位址。多重播送位址的第一個位元組是奇數（最小有效位元設定為 1）；因此，第一個位元組必須是偶數。

在**最大傳輸單位**欄位中，指定您網路介面的封包最大傳輸單位（以位元組為單位）。最大傳輸單位範圍從 60 到 1500。此欄位的預設值為 1500。

若要使用 IPv6 乙太網路連線，請完成下列步驟：

配置 IPv6 網路設定

1. 啟用 **IPv6** 選項。
2. 您可以使用下列其中一種指派方法，將 IPv6 位址指派給介面：
   - 使用無狀態位址自動配置
   - 使用具狀態位址配置 (DHCPv6)
   - 使用靜態指派的 IP 位址

附註：選擇**使用靜態指派的 IP 位址**時，系統會要求您輸入下列資訊：

— IPv6 位址

— 字首長度

— 閘道

配置 DNS

使用本主題中的資訊來檢視或變更 XClarity Controller 網域名稱系統 (DNS) 設定。

附註：在 Flex System 中，無法修改 XClarity Controller 中的 DNS 設定。DNS 設定由 CMM 管理。

按一下 **BMC 配置**下的**網路**，以檢視或修改 XClarity Controller DNS 設定。

如果您按一下**使用其他 DNS 位址伺服器**勾選框，請指定您的網路上最多三個「網域名稱系統」伺服器的 IP 位址。每個 IP 位址必須包含 0 到 255 的整數，以句點區隔。這些 DNS 伺服器位址將新增至搜尋清單的頂端，因此在 DHCP 伺服器自動指派位址之前，會先在這些伺服器上執行主機名稱查閱。

配置 DDNS

使用本主題中的資訊、可啟用或停用 XClarity Controller 上的「動態網域名稱系統 (DDNS) 通訊協定」。

按一下 **BMC 配置**下的**網路**，以檢視或修改 XClarity Controller DDNS 設定。

按一下**啟用 DDNS** 勾選框，以啟用 DDNS。啟用 DDNS 時，XClarity Controller 會通知網域名稱伺服器即時變更，包括 XClarity Controller 配置主機名稱的作用中網域名稱伺服器配置、位址或儲存在網域名稱伺服器中的其他資訊。

從項目清單中選擇選項，以決定您要選取 XClarity Controller 網域名稱的方式。

- **使用自訂網域名稱**：您可以指定 XClarity Controller 所屬的網域名稱。
- **使用取自 DHCP 伺服器的網域名稱**：由 DHCP 伺服器指定 XClarity Controller 所屬的網域名稱。

配置 Ethernet over USB

使用本主題中的資訊來控制 Ethernet over USB 介面，以用於伺服器與 XClarity Controller 之間的頻內通訊。

按一下 **BMC 配置**下的**網路**，以檢視或修改 XClarity Controller Ethernet over USB 設定。

Ethernet over USB 可用來對 XClarity Controller 進行頻內通訊。按一下此勾選框，以啟用或停用 Ethernet over USB 介面。

重要事項：如果您停用 Ethernet over USB，則無法使用 Linux 或 Windows 快閃記憶體公用程式來執行 XClarity Controller 韌體或伺服器韌體的頻內更新。

選取 XClarity Controller 用來指派位址給 Ethernet over USB 介面端點的方法。

- **為 Ethernet over USB 使用 IPv6 鏈結本端位址**： 此方法使用以 MAC 位址為基礎的 IPv6 位址，而這些位址已配置給 Ethernet over USB 介面端點。一般而言，IPv6 鏈結本端位址是使用 MAC 位址 (RFC 4862) 來產生的，但是 Windows 2008 和較新的 2016 年作業系統不支援在介面的主機端使用靜態鏈結本端 IPv6 位址。而預設的 Windows 行為會在執行時，重新產生隨機鏈結本端位址。如果將 XClarity Controller Ethernet over USB 介面配置為使用 IPv6 鏈結本端位址模式，則使用此介面的各種功能將無法運作，因為 XClarity Controller 不知道 Windows 已將什麼位址指派給介面。如果伺服器是執行 Windows，請使用其他 Ethernet over USB 位址配置方法，或是使用下列指令來停用預設的 Windows 行為：**netsh interface ipv6 set global randomizeidentifiers=disabled**

- **為 Ethernet over USB 使用 IPv4 鏈結本端位址**： 會將 169.254.0.0/16 範圍內的 IP 位址指派給 XClarity Controller 和網路的伺服器端。
- **為 Ethernet over USB 配置 IPv4 設定**： 此方法會指定已指派給 XClarity Controller 和 Ethernet over USB 介面伺服器端的 IP 位址和網路遮罩。

附註：

1. 作業系統 IP 配置設定不用於設定 Ethernet Over USB 介面的作業系統 IP 位址，但用於通知 BMC，指出 Ethernet over USB 的作業系統 IP 位址已變更。
2. 配置 Ethernet over USB 的三個 IP 設定之前，您需要在本端作業系統中手動配置 Ethernet over USB 介面的作業系統 IP 位址。

若要控制外部乙太網路埠號與 Ethernet over USB 埠號的對映，您可以按一下**啟用外部乙太網路至 Ethernet over USB 埠轉遞**勾選框，並完成您希望從管理網路介面轉遞至伺服器的埠對映資訊。

配置 SNMP

使用本主題中的資訊來配置 SNMP 代理程式。

請完成下列步驟，以配置 XClarity Controller SNMP 警示設定。

1. 按一下 **BMC 配置**下的**網路**。
2. 勾選對應的勾選框，以啟用 **SNMPv1 設陷**、**SNMPv2 設陷**和/或 **SNMPv3 設陷**。
3. 如果啟用 **SNMPv1 設陷**或 **SNMPv2 設陷**，請完成下列欄位：
   a. 在**社群名稱**欄位中，輸入社群名稱；名稱不可以空白。
   b. 在**主機**欄位中，輸入主機位址。
4. 如果啟用 **SNMPv3 設陷**，請完成下列欄位：
   a. 在**引擎 ID**欄位中，輸入引擎 ID。引擎 ID 不可以空白。
   b. 在**設陷接收器埠**欄位中，輸入埠號。預設埠號為 162。
5. 如果啟用「SNMP 設陷」，請選取下列您要接收警示的事件類型：
   - **嚴重**
   - **注意**
   - **系統**

   附註：按一下每個主要種類，以進一步選取您要接收警示的子種類事件類型。

啟用或停用 IPMI 網路存取

使用本主題中的資訊，以控制對 XClarity Controller 的 IPMI 網路存取。

按一下 **BMC 配置**下的**網路**，以檢視或修改 XClarity Controller IPMI 設定。請完成下列欄位，以檢視或修改 IPMI 設定：

IPMI over LAN 存取
按一下開關，以啟用或停用對 XClarity Controller 的 IPMI 網路存取。

重要事項：

- 如果您沒有透過 IPMI 通訊協定的網路使用存取 XClarity Controller 的任何工具或應用程式，強烈建議您停用 IPMI 網路存取，以提升安全性。
- 依預設會停用對 XClarity Controller 的 IPMI over LAN 存取。

使用 IPMI 指令配置網路設定

使用本主題中的資訊，利用 IPMI 指令來配置網路設定。

由於每個 BMC 網路設定都是使用不同的 IPMI 要求配置的，而且沒有特定順序，因此 BMC 在重新啟動以套用擱置的網路變更之前，無法完整檢視所有的網路設定。變更網路設定的要求在提出之時可能會成功，但稍後有額外變更的要求時，就會被視為無效。重新啟動 BMC 時，如果擱置的網路設定不相容，將不會套用新設定。重新啟動 BMC 之後，您應該嘗試使用新設定存取 BMC，以確保其套用如您預期。

服務啟用和埠指派

使用本主題中的資訊來檢視或變更 XClarity Controller 上部分服務所使用的埠號。

按一下 **BMC 配置**下的**網路**，以檢視或修改 XClarity Controller 埠指派。請完成下列欄位，以檢視或修改埠指派：

Web
埠號是 80。使用者無法配置此欄位。

Web over HTTPS
在此欄位中指定 Web Over HTTPS 的埠號。預設值是 443。

REST over HTTPS
埠號將會自動變更為 Web over HTTPS 欄位中指定的埠號。此欄位不是使用者可配置的。

CIM over HTTP
在此欄位中指定 CIM over HTTP 的埠號。預設值是 5989。

附註：依預設會停用 CIM。

遠端顯示
在此欄位中指定「遠端顯示」的埠號。預設值是 3900。

IPMI over LAN
埠號是 623。使用者無法配置此欄位。

附註：依預設會停用 IPMI。

SFTP
在此欄位中指定用於 SSH 檔案傳送通訊協定 (SFTP) 的埠號。埠號是 115。使用者無法配置此欄位。

附註：若要執行 OneCLI 頻內更新，IMM.SFTPPortControl=open 是必要條件。

SLP
在此欄位中指定用於 SLP 的埠號。埠號是 427。使用者無法配置此欄位。

附註：XClarity Controller 回報的服務類型有兩種：

- 服務：management-hardware.Lenovo:lenovo-xclarity-controller
- 服務：wbem

SSDP
埠號是 1900。使用者無法配置此欄位。

SSH
在此欄位中指定要透過 SSH 通訊協定來存取指令行介面而配置的埠號。預設值是 22。

SNMP 代理程式
在此欄位中指定在 XClarity Controller 上執行之 SNMP 代理程式的埠號。預設值是 161。有效的埠號值為 1 至 65535。

SNMP 設陷
在此欄位中指定用於 SNMP 設陷的埠號。預設值是 162。有效的埠號值為 1 至 65535。

配置存取限制

使用本主題中的資訊，來檢視或變更阻止從 IP 位址或 MAC 位址存取 XClarity Controller 的設定。

按一下 **BMC 配置**下的**網路**，以檢視或修改 XClarity Controller 存取控制設定。

封鎖清單和時間限制

這些選項可讓您封鎖特定 IP/Mac 位址一段時間。

- **封鎖的 IP 位址清單**
  - 您最多可以輸入三個 IPv4 位址（或範圍）和三個 IPv6 位址（或範圍）並以逗點分隔，以指定不允許存取 XClarity Controller 的 IP 位址。請參閱下列 IPv4 範例：
  - 單一 IPv4 位址範例：192.168.1.1
  - 超網 IPv4 位址範例：192.168.1.0/24
  - IPv4 範圍範例：192.168.1.1—192.168.1.5
- **封鎖的 MAC 位址清單**
  - 您最多可以輸入三個 MAC 位址並以逗點分隔，以指定不允許存取 XClarity Controller 的 MAC 位址。例如：11:22:33:44:55:66。
- **限制存取（單次）**
  - 您可以排程無法存取 XClarity Controller 的單次時間間隔。對於您所指定的時間間隔：
  - 開始日期與時間必須晚於目前的 XCC 時間。
  - 結束日期與時間必須晚於開始日期與時間。
- **限制存取（每日）**
  - 您可以排程一個或多個無法存取 XClarity Controller 的每日時間間隔。對於您所指定的每個時間間隔：
  - 結束日期與時間必須晚於開始日期與時間。

外部觸發的封鎖清單

這些選項可在用戶端從特定 IP 位址（IPv4 和 IPv6）嘗試使用不同的錯誤使用者名稱或密碼登入 XClarity Controller 時，讓您設定自動封鎖這些位址。

自動封鎖將動態判斷何時從特定 IP 位址發生過多的登入失敗，並封鎖該位址存取 XClarity Controller 一段預定時間。

- **來自特定 IP 的登入失敗數目上限**
  - 次數上限表示在使用者被鎖定之前，允許來自特定 IP 位址的使用者使用不正確密碼的登入失敗數目。
  - 如果設定為 0，則 IP 位址將永遠不會由於登入失敗而被鎖定。
  - 從該 IP 位址成功登入後，特定 IP 位址的失敗登入計數器將重設為零。
- **封鎖 IP 的鎖定期間**
  - 使用者可以嘗試從鎖定的 IP 位址重新登入之前，必須經過的最短時間（分鐘）。
  - 如果設定為 0，則被鎖定 IP 位址的存取權將保持鎖定，直到管理者明確解除鎖定為止。
- **封鎖清單**

— 表格「封鎖清單」顯示所有鎖定的 IP 位址。您可以從封鎖清單中解除鎖定一個或全部 IP 位址。

配置前方面板 USB 埠至管理

使用本主題中的資訊來配置 XClarity Controller 前方面板 USB 埠至管理。

在部分伺服器上，可切換前方面板 USB 埠，以連接至伺服器或 XClarity Controller。連接至 XClarity Controller 主要用於執行 Lenovo XClarity 行動版應用程式的行動裝置。當連接行動裝置和伺服器前方面板之間的 USB 纜線時，則會在執行行動版應用程式的裝置上和 XClarity Controller 之間建立 Ethernet over USB 連線。

按一下 **BMC 配置**下的**網路**，以檢視或修改 XClarity Controller 前方面板 USB 埠至管理的設定。

以下有四種設定類型可供您選擇：

僅限主機模式
前方面板 USB 埠一律只能連接至伺服器。

僅限 BMC 模式
前方面板 USB 埠一律只能連接至 XClarity Controller。

共用模式：BMC 所擁有
伺服器和 XClarity Controller 共用前方面板 USB 埠，不過該埠已切換至 XClarity Controller。

共用模式：主機所擁有
伺服器和 XClarity Controller 共用前方面板 USB 埠，不過該埠已切換至主機。

如需行動版應用程式的相關資訊，請參閱下列網站：

https://pubs.lenovo.com/lxca/lxca_usemobileapp.html

附註：

- 如果前方面板 USB 埠配置為「共用模式」，則沒有電源時，該埠會連接至 XClarity Controller；若是有電源時，該埠會連接至伺服器。有電源時，可以在伺服器和 XClarity Controller 之間自由切換控制前方面板 USB 埠。在共用模式中，按住前方面板識別按鈕（若是計算節點，可能是 USB 管理按鈕）3 秒鐘以上，也可以在主機和 XClarity Controller 之間自由切換該埠。
- 在共用模式下配置而且 USB 埠目前連接至伺服器時，XClarity Controller 可支援將前方面板 USB 埠切換回 XClarity Controller 的要求。執行此要求時，前方面板 USB 埠會維持與 XClarity Controller 的連線，直到閒置逾時指定期間內沒有與 XClarity Controller 的任何 USB 活動為止。

配置安全設定

使用本主題中的資訊來配置安全性通訊協定。

附註：預設最小的 TLS 版本設定為 TLS 1.2，但如果您的瀏覽器或管理應用程式有需要，您可以配置 XClarity Controller 來使用其他 TLS 版本。如需相關資訊，請參閱第 136 頁 「tls 指令」。

按一下 **BMC 配置**下的**安全性**，以存取及配置 XClarity Controller 的安全性內容、狀態和設定。

SSL 概觀

本主題是 SSL 安全通訊協定的概觀。

SSL 是提供通訊隱私的安全通訊協定。SSL 可讓主從式應用程式以防止竊聽、竄改和偽造訊息的方式來進行通訊。您可以配置 XClarity Controller，以針對不同類型的連線（例如安全 Web 伺服器 (HTTPS)、安全 LDAP 連線 (LDAPS)、CIM over HTTPS 和 SSH 伺服器）來使用 SSL 支援，以及管理 SSL 所需的憑證。

SSL 憑證處理

本主題提供可與 SSL 安全通訊協定搭配使用之憑證的管理相關資訊。

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。使用自簽憑證是使用 SSL 最簡單的方法；但它會造成一些安全風險。會導致風險是因為在用戶端與伺服器之間第一次嘗試連線時，SSL 用戶端無法驗證 SSL 伺服器的身分。例如，第三方可能會假冒 XClarity Controller Web 伺服器，並截取在真正 XClarity Controller Web 伺服器與使用者 Web 瀏覽器之間傳輸的資料。如果在瀏覽器與 XClarity Controller 之間起始連線時，自簽憑證匯入瀏覽器的憑證庫中，則該瀏覽器未來的所有通訊都會是安全的（假設起始連線未受攻擊損害）。

如需更完整的安全保護，您可以使用憑證管理中心 (CA) 已簽章的憑證。若要取得已簽章的憑證，您需要選取**產生憑證簽章要求 (CSR)**。選取**下載憑證簽章要求 (CSR)**，並將「憑證簽章要求 (CSR)」傳送至 CA，以取得已簽章的憑證。收到已簽章的憑證後，選取**匯入已經簽章的憑證**，以將其匯入 XClarity Controller 中。

CA 的功能是要驗證 XClarity Controller 的身分。憑證包含 CA 和 XClarity Controller 的數位簽章。如果知名的 CA 發出憑證，或 CA 的憑證已匯入 Web 瀏覽器，瀏覽器就可以驗證憑證，並明確識別 XClarity Controller Web 伺服器。

XClarity Controller 需要憑證來與 HTTPS 伺服器、CIM over HTTPS 和安全 LDAP 用戶端搭配使用。此外，安全 LDAP 用戶端也需要匯入一個或多個授信憑證。安全 LDAP 用戶端會使用授信憑證，以明確識別 LDAP 伺服器。授信憑證是簽署 LDAP 伺服器憑證的 CA 的憑證。如果 LDAP 伺服器使用自簽憑證，則授信憑證可以是 LDAP 伺服器本身的憑證。如果配置中使用多個 LDAP 伺服器，則必須匯入額外的授信憑證。

SSL 憑證管理

本主題提供使用 SSL 安全通訊協定來進行憑證管理時，可選取之部分動作的相關資訊。

按一下 **BMC 配置**下的**安全性**，以配置 SSL 憑證管理。

管理 XClarity Controller 憑證時，會顯示下列動作：

下載已經簽章的憑證
使用此鏈結可下載目前安裝的憑證副本。憑證可下載成 PEM 或 DER 格式。您可以使用 OpenSSL (www.openssl.org) 之類的協力廠商工具來檢視憑證內容。使用 OpenSSL 來檢視憑證內容的指令行範例如下所示：

```
openssl x509 -in cert.der -inform DER -text
```

下載憑證簽章要求 (CSR)
使用此鏈結可下載憑證簽章要求副本。CSR 可下載成 PEM 或 DER 格式。

產生已經簽章的憑證
產生自簽憑證。作業完成之後，即可使用新憑證來啟用 SSL。

附註：執行**產生已經簽章的憑證**動作時，會開啟「產生 HTTPS 的自簽憑證」視窗。系統會提示您完成必要和選用欄位。您**必須** 完成必要欄位。輸入資訊後，按一下**產生**，以完成作業。

產生憑證簽章要求 (CSR)
產生憑證簽章要求 (CSR)。作業完成之後，可以下載 CSR 檔案，並傳送至憑證管理中心 (CA) 以供簽章。

附註：執行**產生憑證簽章要求 (CSR)** 動作時，會開啟「產生 HTTPS 的憑證簽章要求」視窗。系統會提示您完成必要和選用欄位。您**必須** 完成必要欄位。輸入資訊後，按一下**產生**，以完成作業。

匯入已經簽章的憑證

使用此動作可匯入已經簽章的憑證。若要取得已經簽章的憑證，必須先產生憑證簽章要求 (CSR)，並傳送至憑證管理中心 (CA)。

配置 Secure Shell 伺服器

使用本主題中的資訊，以瞭解及啟用 SSH 安全通訊協定。

按一下 **BMC 配置**下的**網路**，以配置 Secure Shell 伺服器。

若要使用 SSH 通訊協定，必須先產生金鑰，以啟用 SSH 伺服器。

附註：

- 不需要任何憑證管理，即可使用此選項。
- XClarity Controller 一開始就會建立 SSH 伺服器金鑰。如果希望產生新的 SSH 伺服器金鑰，請按一下 **BMC 配置**下的**網路**；然後，按一下**重新產生金鑰**。
- 完成此動作之後，您必須重新啟動 XClarity Controller，以使變更生效。

IPMI over Keyboard Controller Style (KCS) 存取

使用本主題中的資訊來控制對 XClarity Controller 的 IPMI over Keyboard Controller Style (KCS) 存取。

XClarity Controller 透過不需要驗證的 KCS 通道來提供 IPMI 介面。

按一下 **BMC 配置**下的**安全性**，以啟用或停用 IPMI over KCS 存取。

附註：變更設定之後，您必須重新啟動 XClarity Controller，以使變更生效。

重要事項：如果您沒有在伺服器上執行會透過 IPMI 通訊協定存取 XClarity Controller 的任何工具或應用程式，強烈建議您停用 IPMI KCS 存取，以提升安全性。XClarity Essentials 會對 XClarity Controller 使用 IPMI over KCS 介面。如果您已停用 IPMI over KCS 介面，在伺服器上執行 XClarity Essentials 之前，請先將其啟用。執行完成之後，再停用此介面。

防止系統韌體降低層級

使用本主題中的資訊來防止系統韌體變更為較舊的韌體版本。

此特性可讓您決定要讓系統韌體回復至較舊的韌體版本。

按一下 **BMC 配置**下的**網路**，以防止系統韌體降低層級

若要啟用或停用此特性，請按一下 **BMC 配置**下的**網路**。所做的任何變更都會立即生效，XClarity Controller 不需要重新啟動。

物理現場授權生效

使用本主題中的資訊，從 XClarity Controller 網頁使物理現場授權生效或失效，而不需要實際在伺服器上操作。

只有透過 UEFI 啟用**物理現場授權原則**，才能使用此功能。在啟用後，您可以按一下 **BMC 配置**下的**安全性**，以存取物理現場授權功能。

配置安全金鑰管理 (SKM)

使用本主題中的資訊來建立和管理安全金鑰。

此功能使用集中式金鑰管理伺服器提供用於解鎖儲存硬體的金鑰，進而存取儲存在 ThinkSystem 伺服器 SED 中的資料。金鑰管理伺服器包括 SKLM - IBM SED 金鑰管理伺服器，以及 KMIP - Thales/Gemalto SED 金鑰管理伺服器（KeySecure 和 CipherTrust）。

XClarity Controller 使用網路從金鑰管理伺服器擷取金鑰；因此，XClarity Controller 必須能夠存取金鑰管理伺服器。XClarity Controller 在金鑰管理伺服器與提出要求的 ThinkSystem 伺服器之間提供通訊通道。XClarity Controller 韌體會嘗試與所配置的每部金鑰管理伺服器連接，成功建立連線之後即停止嘗試。

如果符合下列條件，XClarity Controller 就會與金鑰管理伺服器建立通訊：

- XClarity Controller 中已配置一個或多個金鑰管理伺服器主機名稱/IP 位址。
- XClarity Controller 中已安裝用來與金鑰管理伺服器通訊的兩個憑證（用戶端和伺服器）。

附註：為裝置配置至少兩個（主要和次要）具有相同通訊協定的金鑰管理伺服器。如果主要金鑰管理伺服器未回應來自 XClarity Controller 的連線嘗試，則會起始與其他金鑰管理伺服器的連線嘗試，直到成功建立連線為止。

必須在 XClarity Controller 與金鑰管理伺服器之間建立傳輸層安全 (TLS) 連線。XClarity Controller 會比較由金鑰管理伺服器提交的伺服器憑證，與先前匯入 XClarity Controller 信任儲存庫中的金鑰管理伺服器憑證，以鑑別金鑰管理伺服器。金鑰管理伺服器會鑑別與其通訊的每個 XClarity Controller，並檢查以確認 XClarity Controller 有權存取金鑰管理伺服器。此鑑別是藉由比較 XClarity Controller 提交的用戶端憑證與儲存在金鑰管理伺服器上的受信任憑證來達成。

至少會連接一部金鑰管理伺服器，而裝置群組會被視為選用性。需要匯入金鑰管理伺服器憑證，並需要指定用戶端憑證。預設會使用 HTTPS 憑證。如果您要將其更換，可以建立新的憑證。

附註：若要連接 KMIP 伺服器（KeySecure 和 CipherTrust），必須產生憑證簽章要求 (CSR)，且其一般名稱必須與 KMIP 伺服器中定義的使用者名稱相符合，然後為 CSR 匯入由 KMIP 伺服器所信任的憑證管理中心 (CA) 簽章的憑證。

配置金鑰管理伺服器

使用本主題中的資訊為金鑰管理伺服器建立主機名稱或 IP 位址以及相關聯的埠資訊。

金鑰管理伺服器配置區段包含下列欄位：

主機名稱或 IP 位址
在此欄位中輸入金鑰管理伺服器的主機名稱（如果已啟用並配置 DNS）或 IP 位址。最多可以新增 4 部伺服器。

埠
在此欄位中輸入金鑰管理伺服器的埠號。如果此欄位保留空白，則會使用預設值 5696。有效的埠號值為 1 至 65535。

配置裝置群組

使用本主題中的資訊配置 SKLM 伺服器中使用的裝置群組。

在 SKLM 伺服器中，裝置群組可讓使用者以群組方式，管理多部伺服器上的自我加密型硬碟 (SED) 金鑰。具有相同名稱的裝置群組也必須建立在 SKLM 伺服器上。

「裝置群組」區段中包含下列欄位：

裝置群組
裝置群組可讓使用者以群組方式，管理多部伺服器上的 SED 金鑰。具有相同名稱的裝置群組也必須建立在 SKLM 伺服器上。此欄位的預設值為 IBM_SYSTEM_X_SED。

建立憑證管理

本主題提供用戶端和伺服器憑證管理的相關資訊。

用戶端和伺服器憑證可用來驗證 SKLM 伺服器與位於 ThinkSystem 伺服器中的 XClarity Controller 之間的通訊。本節討論用戶端和伺服器憑證管理。

用戶端憑證管理

本主題提供用戶端憑證管理的相關資訊。

用戶端憑證分類如下：

- XClarity Controller 自行指派憑證。
- 從 XClarity Controller 憑證簽章要求 (CSR) 產生並由第三方 CA 簽章（外部）的憑證。

與 SKLM 伺服器進行通訊時，需要用戶端憑證。用戶端憑證包含 CA 和 XClarity Controller 的數位簽章。

附註：

- 在韌體更新之間會保留憑證。
- 如果未建立用來與 SKLM 伺服器通訊的用戶端憑證，則會使用 XClarity Controller HTTPS 伺服器憑證。
- CA 的功能是要驗證 XClarity Controller 的身分。

如果要建立用戶端憑證，請按一下加號圖示 ( )，並選取下列其中一個項目：

- 產生新金鑰和自簽憑證
- 產生新金鑰和憑證簽章要求 (CSR)

產生新金鑰和自簽憑證動作項目會產生新的加密金鑰和自簽憑證。在「產生新金鑰和自簽憑證」視窗中，於必要欄位以及適用於您的配置的任何選用欄位中（請參閱下表），輸入或選取資訊。按一下**確定**，以產生加密金鑰和憑證。在產生自簽憑證時，會顯示進度視窗。順利安裝憑證之後，會顯示確認視窗。

附註：新的加密金鑰和憑證會取代任何現有的金鑰和憑證。

表格 3. 產生新金鑰和自簽憑證

包含兩個直欄的表格，標頭中記載「產生新金鑰和自簽憑證」動作的必要和選用欄位。最後一列橫跨兩個直欄。

欄位	說明
國家/地區[1]	從清單項目中選取 BMC 實際所在的國家/地區。
州/省（縣/市）[1]	輸入 BMC 實際所在的州/省（縣/市）。
鄉鎮/市區[1]	輸入 BMC 實際所在的鄉鎮/市區。
組織名稱[1]	輸入擁有 BMC 的公司或組織名稱。
BMC 主機名稱[1]	輸入出現在網址列中的 BMC 主機名稱。
聯絡人	輸入負責 BMC 的聯絡人名稱。
電子郵件位址	輸入負責 BMC 的聯絡人電子郵件位址。
組織單位	輸入公司中擁有 BMC 的單位。
姓氏	輸入負責 BMC 的聯絡人姓氏。此欄位最多可以包含 60 個字元。
名字	輸入負責 BMC 的聯絡人名字。此欄位最多可以包含 60 個字元。
姓名縮寫	輸入負責 BMC 的聯絡人姓名縮寫。此欄位最多可以包含 20 個字元。

表格 3. 產生新金鑰和自簽憑證（繼續）

欄位	說明
DN 限定元	輸入 BMC 的識別名稱限定元。此欄位最多可以包含 60 個字元。
1. 這是必要欄位。	

產生用戶端憑證之後，您可以選取**下載憑證**動作項目，將憑證下載至 XClarity Controller 上的儲存體。

產生新金鑰和憑證簽章要求 (CSR) 動作項目會產生新的加密金鑰和 CSR。在「產生新金鑰和憑證簽章要求」視窗中，於必要欄位以及適用於您的配置的任何選用欄位中（請參閱下表），輸入或選取資訊。按一下**確定**，以產生新的加密金鑰和 CSR。

在產生 CSR 時，會顯示進度視窗，而順利完成後，會顯示確認視窗。產生 CSR 之後，您必須將 CSR 傳送至 CA，以進行數位簽章。選取**下載憑證簽章要求 (CSR)** 動作項目，並按一下**確定**，以將 CSR 儲存至您的伺服器。然後您就可以將 CSR 提交給 CA 進行簽章。

表格 4. 產生新金鑰和憑證簽章要求

包含兩個直欄的表格，標頭中記載「產生新金鑰和憑證簽章要求」動作的必要和選用欄位。最後一列橫跨兩個直欄。

欄位	說明
國家/地區[1]	從清單項目中選取 BMC 實際所在的國家/地區。
州/省（縣/市）[1]	輸入 BMC 實際所在的州/省（縣/市）。
鄉鎮/市區[1]	輸入 BMC 實際所在的鄉鎮/市區。
組織名稱[1]	輸入擁有 BMC 的公司或組織名稱。
BMC 主機名稱[1]	輸入出現在網址列中的 BMC 主機名稱。
聯絡人	輸入負責 BMC 的聯絡人名稱。
電子郵件位址	輸入負責 BMC 的聯絡人電子郵件位址。
組織單位	輸入公司中擁有 BMC 的單位。
姓氏	輸入負責 BMC 的聯絡人姓氏。此欄位最多可以包含 60 個字元。
名字	輸入負責 BMC 的聯絡人名字。此欄位最多可以包含 60 個字元。
姓名縮寫	輸入負責 BMC 的聯絡人姓名縮寫。此欄位最多可以包含 20 個字元。
DN 限定元	輸入 BMC 的識別名稱限定元。此欄位最多可以包含 60 個字元。
盤查密碼	輸入 CSR 的密碼。此欄位最多可以包含 30 個字元。
未結構化的名稱	輸入其他資訊，例如指派給 BMC 的非結構化名稱。此欄位最多可以包含 60 個字元。
1. 這是必要欄位。	

CA 會透過使用者的憑證處理工具（例如 **OpenSSL** 或 **Certutil** 指令行工具），以數位方式簽署 CSR。透過使用者的憑證處理工具來簽署的所有用戶端憑證，都有相同的**基本**憑證。這個**基本**憑證也必須匯入 SKLM 伺服器中，以便 SKLM 伺服器接受使用者以數位方式簽署的所有伺服器。

CA 簽署憑證之後，您必須將其匯入 BMC 中。請選取**匯入已經簽章的憑證**動作項目，並選取要上傳為用戶端憑證的檔案，然後按一下**確定**。在上傳 CA 簽署的憑證時，會顯示進度視窗。如果上傳程序成功，會顯示「憑證上傳」視窗。如果上傳程序不成功，則會顯示「憑證上傳錯誤」視窗。

附註：

- 為了增加安全性，請使用由 CA 以數位方式簽署的憑證。
- 匯入 XClarity Controller 中的憑證必須對應於先前產生的 CSR。

CA 簽署的憑證匯入 BMC 中之後，請選取**下載憑證**動作項目。當您選取此動作項目時，就會從 XClarity Controller 下載 CA 簽署的憑證，以儲存在您的系統上。

伺服器憑證管理

本主題提供伺服器憑證管理的相關資訊。

伺服器憑證產生於 SKLM 伺服器中，必須匯入 XClarity Controller 中，安全硬碟存取功能才能運作。若要將用來鑑別 SKLM 伺服器的憑證匯入 BMC，請從「硬碟存取」頁面的「伺服器憑證狀態」區段按一下**匯入憑證**。在檔案傳送至 XClarity Controller 上的儲存體時，會顯示進度指示器。

在伺服器憑證順利傳送至 XClarity Controller 之後，「伺服器憑證狀態」區域會顯示下列內容：`A server certificate is installed`。

如果您想要移除授信憑證，請按一下對應的**移除**按鈕。

延伸審核日誌

使用本主題中的資訊來控制延伸審核日誌。

此功能可讓您決定是否將來自 LAN 和 KCS 通道的 IPMI 設定指令的日誌項目（原始資料）包含到審核日誌中。

請按一下 XCC Web 上「**BMC 配置**」下的「**安全性**」，以啟用/停用延伸審核日誌。

附註：如果 IPMI 設定指令來自 LAN 通道，則使用者名稱和來源 IP 位址將包含在日誌訊息中。且會排除所有具有敏感安全性資訊（例如密碼）的 IPMI 指令。

加密法設定

使用本主題中的資訊，以瞭解不同的加密法設定。

高安全性模式

- 僅支援現代和強式密碼。
- 符合 NIST 標準。
- 符合 PFS（完全前向保密）標準。

相容模式

- 支援廣泛的密碼組合以實現最大的相容性。
- 不符合 PFS 和 NIST 標準。

NIST 相容模式

- 支援廣泛的密碼組合以實現最大的相容性。
- 符合 NIST 標準。
- 符合 PFS 標準。

TLS 版本支援

- TLS 1.0 和以上版本
- TLS 1.1 和以上版本
- TLS 1.2 和以上版本
- TLS 1.3

TLS 加密法設定是為了限制對 BMC 服務支援的TLS 密碼組合。

請參閱下表以瞭解不同設定所支援的 TLS 密碼組合

安全性模式	TLS 版本	TLS 密碼組合
高安全性模式	TLS 1.3 和以下版本	• TLS_AES_256_GCM_SHA384
高安全性模式	TLS 1.2 和以下版本	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
NIST 相容模式	TLS 1.3 和以下版本	• TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256
NIST 相容模式	TLS 1.2 和以下版本	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256
相容模式	TLS 1.3 和以下版本	• TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256

安全性模式	TLS 版本	TLS 密碼組合
相容模式	TLS 1.2 和以下版本	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256
相容模式	TLS 1.1 和以下版本	• TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256

備份和還原 BMC 配置

本主題中的資訊說明如何還原或修改 BMC 配置。

選取 **BMC 配置**下的**備份及還原**，以執行下列動作：

- 檢視管理控制器配置摘要
- 備份或還原管理控制器配置
- 檢視備份或還原狀態
- 將管理控制器配置重設為原廠預設值
- 存取管理控制器起始設定精靈

備份 BMC 配置

本主題中的資訊說明如何備份 BMC 配置。

選取在 **BMC 配置**下的**備份及還原**。最上方是**備份 BMC 配置**區段。

如果之前已完成備份，則您可在**上次備份**欄位看到詳細資料。

若要備份現行的 BMC 配置，請遵循下列步驟：

1. 指定 BMC 備份檔的密碼。
2. 請選擇您要加密整個檔案或僅加密機密資料。
3. 按一下**開始備份**即可開始備份程序。在備份程序中，您不得執行任何還原/重設動作。
4. 完成程序後，會出現可讓您下載及儲存檔案的按鈕。

附註：當使用者設定新的 XClarity Controller 使用者/密碼並執行配置備份時，其中也會包含預設帳戶/密碼 (USERID/PASSWORD)。隨後從備份刪除預設帳戶/密碼將導致系統顯示一則訊息，通知使用者在還原 XClarity Controller 帳戶/密碼時發生錯誤。使用者可以忽略此訊息。

還原 BMC 配置

本主題中的資訊說明如何還原 BMC 配置。

選取在 **BMC 配置**下的**備份及還原**。**備份 BMC 配置**下方是**從配置檔還原 BMC** 區段。

若要將 BMC 還原為先前儲存的配置，請遵循下列步驟：

1. 瀏覽並選取備份檔，然後在提示時輸入密碼。
2. 按一下**檢視內容**來檢視詳細資料，以驗證檔案。
3. 驗證內容之後，按一下**開始還原**。

將 BMC 重設為原廠預設值

本主題中的資訊說明如何將 BMC 重設為原廠預設值。

選取在 **BMC 配置**下的**備份及還原**。**從配置檔還原 BMC** 下方是**將 BMC 重設為原廠預設值**區段。

若要將 BMC 重設為原廠預設，請遵循下列步驟：

1. 按一下**開始將 BMC 重設為原廠預設值**。

   附註：

   - 只有具備監督者使用者權限層級的使用者，才能執行此動作。
   - 乙太網路連線暫時中斷。重設作業完成之後，您必須重新登入 XClarity Controller Web 介面。
   - 一旦您按下**開始將 BMC 重設為原廠預設值**，所有先前的配置變更都會遺失。如果您想要在還原 BMC 配置時啟用 LDAP，就必須先匯入授信安全憑證，然後再進行還原。
   - 處理程序完成之後，XClarity Controller 會重新啟動。如果這是本端伺服器，TCP/IP 連線將會中斷，而您可能需要重新配置網路介面來還原連線功能。
   - 將 BMC 重設為原廠預設值不會影響 UEFI 設定。

重新啟動 XClarity Controller

本主題的資訊說明如何重新啟動 XClarity Controller。

如需有關如何重新啟動 XClarity Controller 的詳細資訊，請參閱第 53 頁 「電源動作」

第 4 章　監視伺服器狀態

使用本主題中的資訊，可瞭解如何檢視和監視您所存取的伺服器資訊。

在登入 XClarity Controller 後，則會顯示系統狀態頁面。在此頁面中，您可以檢視伺服器硬體狀態、事件日誌和審核日誌、系統狀態、維護歷程及警示接收者。

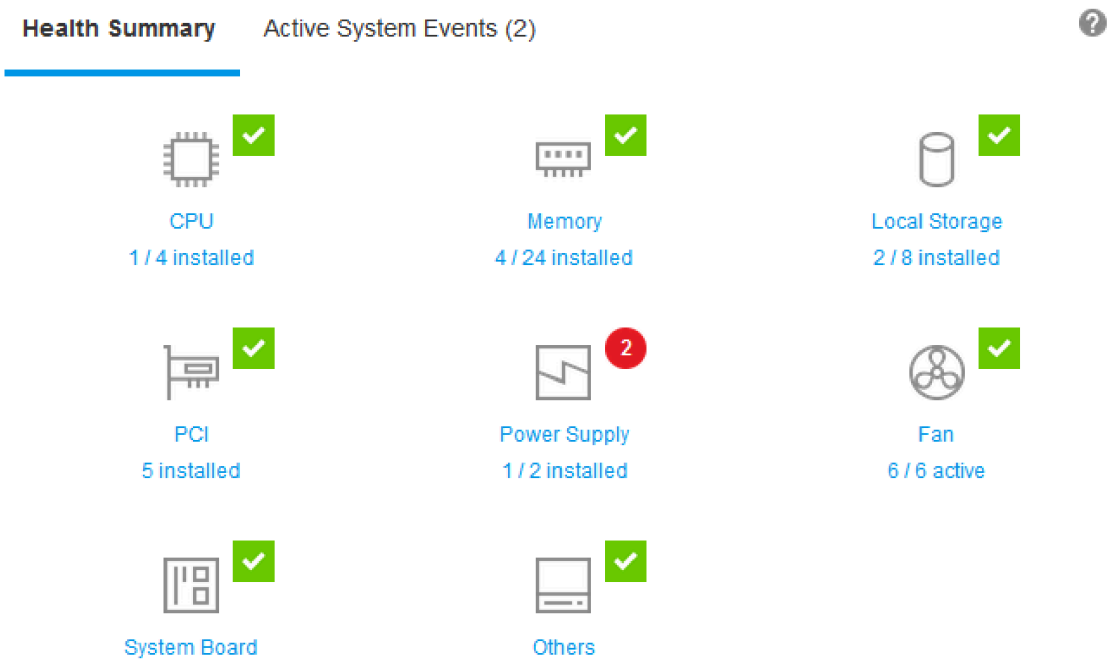
檢視性能摘要/作用中系統事件

使用本主題中的資訊，來瞭解如何檢視性能摘要/作用中系統事件。

當您存取 XClarity Controller 首頁時，預設會顯示**性能摘要**。將會以圖形表示法來顯示已安裝的硬體元件數目及其各自的性能狀態。所監視的硬體元件包括下列各項：

- 處理器 (CPU)
- 記憶體
- 本端儲存體
- PCI 配接卡
- 電源供應器
- 風扇
- 主機板
- 其他

附註：在具有簡易抽換背板配置的系統上，**本端儲存體**可能會顯示「無法使用」。



如果有任何硬體元件運作不正常，將會以嚴重或警告圖示來標示。嚴重狀況會以紅色圓形圖示表示，而警告狀況會以黃色三角形圖示表示。若將滑鼠指標停留在嚴重或警告符號上，將會顯示該元件的目前作用中事件，最多三個。

如果要檢視其他事件，請按一下**作用中系統事件**標籤。視窗將會出現，顯示系統中目前作用中的事件。按一下**檢視所有事件日誌**以檢視整個事件歷程。

如果硬體元件標示綠色勾號，表示運作正常，且沒有任何作用中事件。

硬體元件下方的文字會指出已安裝的元件數目。如果按一下該文字，您將會被導向**庫存**頁面。

檢視系統資訊

本主題說明如何取得共用伺服器資訊的摘要。

位於首頁左側的**系統資訊和設定**窗格會提供共用伺服器資訊的摘要，包括下列資訊：

- 機器名稱、電源和作業系統狀態
- 機型/型號
- 序號
- 系統名稱
- 正面 USB 所有權
- BMC 授權
- BMC IP 位址
- BMC 主機名稱
- UEFI 版本
- BMC 版本
- LXPM 版本
- 位置

伺服器可能處於下表中列出的其中一種系統狀態。

表格 5. 系統狀態說明

兩欄表格，標頭記載伺服器的系統狀態。

狀態	說明
系統電源關閉/狀態不明	伺服器的電源已關閉。
系統開啟/正在啟動 UEFI	伺服器的電源已開啟；但是，UEFI 未執行。
系統在 UEFI 執行中	伺服器的電源已開啟，且 UEFI 正在執行中。
系統在 UEFI 已停止	伺服器的電源已開啟；UEFI 偵測到問題，且已停止執行。

表格 5. 系統狀態說明（繼續）

狀態	說明
正在啟動作業系統或處於不支援的作業系統中	伺服器可能由於下列其中一種原因，而處於此狀態： • 作業系統載入器已啟動，但作業系統未執行 • BMC Ethernet over USB 介面已停用。 • 作業系統未載入支援 Ethernet over USB 介面的驅動程式。
作業系統已開機	伺服器作業系統正在執行。
暫停至 RAM	伺服器已處於待命或休眠狀態。
在記憶體測試中執行的系統	伺服器的電源已開啟，且正在執行記憶體診斷工具。
系統在設定執行中	伺服器電源已開啟，而且系統已開機至 UEFI F1 設定功能表或 LXPM 功能表。
系統正在 LXPM 維護模式中執行	伺服器電源已開啟，而且系統已開機至 LXPM 維護模式，在此模式下，使用者無法瀏覽 LXPM 功能表。

如果您要變更系統名稱，請按一下鉛筆圖示。輸入您想要使用的系統名稱，然後按一下綠色勾號。

如果您想要變更正面 USB 所有權，請按一下鉛筆圖示，然後從下拉功能表中選取您想要的**正面 USB 所有權**模式。然後按一下綠色勾號。

如果伺服器具有 XClarity Controller 企業版授權以外的授權，您可以購買授權升級來啟用增強的特性。在取得升級授權之後，若要安裝升級授權，請按一下向上箭頭圖示。

如果要新增、刪除或匯出授權，請按一下向右箭頭圖示。

如果要變更 BMC IP 位址、BMC 主機名稱、UEFI 版本、BMC 版本和位置項目的相關設定，請按一下向右箭頭。

- 若為 IP 位址和主機名稱，您將會被導向**網路**下的**乙太網路配置**區段。
- 若為 UEFI 和 BMC 版本項目，您將會被導向**韌體更新**頁面。
- 若為位置項目，您將會被導向**伺服器配置**頁面上的**伺服器內容**區段。

檢視系統使用率

只要按一下左窗格中**使用率**，就會提供共用伺服器使用率資訊的摘要。

系統使用率是一項以處理器、記憶體和 I/O 子系統之即時使用率為基準的複合計量。這些使用率資料全都來自於 ME (Node Manager) 端，包括下列資訊：

- **CPU 使用率**
  - 彙總 C 狀態駐留
  - 測量 C0 時間，以使用的百分比和最大 C0 駐留百分比顯示（每秒）。
- **記憶體使用率**
  - 所有記憶體通道的彙總讀取/寫入磁區。
  - 測量頻寬，以使用的百分比和可用的最大記憶體頻寬百分比來計算（每秒）。
- **I/O 使用率**
  - PCIe* 匯流排中根連接埠的彙總讀取/寫入磁區。
  - 測量頻寬，以使用的百分比和可用的最大 I/O 頻寬百分比來計算（每秒）。

檢視事件日誌

事件日誌提供所有硬體和管理事件的歷程清單。

選取在**事件**中的**事件日誌**標籤，可顯示**事件日誌**頁面。日誌中的所有事件皆已使用 XClarity Controller 日期和時間設定加上時間戳記。部分事件在發生時也會產生警示（如果它們在**警示接收者**中配置為執行此作業）。您可以排序和過濾事件日誌中的事件。

以下是可在**事件日誌**頁面中執行的動作說明。

- **自訂表格**：請選取此動作項目，以選擇要在表格中顯示的資訊類型。當有一個以上的事件具有相同的時間戳記時，可顯示序號以協助判斷事件順序。

  附註：內部 BMC 程序會使用部分序號，因此按序號排序事件時，序號中可能有間隔是正常的現象。
- **清除日誌**：請選取此動作項目，以刪除事件日誌。
- **重新整理**：請選取此動作項目，以更新自從上一次顯示頁面後，其間可能已發生的所有事件日誌項目。
- **類型**：選取要顯示的事件類型。事件類型如下：

  
  在日誌中顯示錯誤項目

  
  在日誌中顯示警告項目

  
  在日誌中顯示參考項目

  按一下每個圖示，以關閉或開啟要顯示的錯誤類型。連續地按一下圖示，可在顯示和隱藏事件之間切換。圖示周圍的藍色方框表示將顯示的事件類型。
- **來源類型過濾器**：從下拉功能表選取某個項目，僅會出現您欲顯示的事件日誌項目類型。
- **時間過濾器**：請選取此動作項目，來指定您要顯示的事件間隔。

- **搜尋**：若要搜尋事件或關鍵字的特定類型，請按一下放大鏡圖示，然後在**搜尋**方框中輸入要搜尋的單字。請注意，輸入區分大小寫。

附註：事件日誌記錄的數目上限是 1024。事件日誌已滿時，新的日誌項目將會自動改寫最舊的項目。

檢視審核日誌

審核日誌提供使用者動作的歷程記錄，例如登入 XClarity Controller、建立新使用者和變更使用者密碼。

您可以使用審核日誌來追蹤及記錄鑑別、變更和系統動作。

事件日誌和審核日誌都支援類似的維護和檢視動作。若要查看「審核日誌」頁面上可執行的顯示說明和過濾動作，請參閱第 46 頁 「檢視事件日誌」。

附註：

- 在您的伺服器作業系統上執行 Lenovo 工具之後，審核日誌可能會包含記錄，顯示由您可能無法辨識的使用者名稱（例如使用者「20luN4SB」）執行的動作。部分工具在伺服器作業系統上執行時，可能會建立暫時的使用者帳戶，用於存取 XClarity Controller。該帳戶是使用隨機的使用者名稱和密碼建立的，只能用於在內部 Ethernet over USB 介面上存取 XClarity Controller。該帳戶只能用於存取 XClarity Controller CIM-XML 和 SFTP 介面。此暫時帳戶的建立和移除，以及工具使用這些認證執行的任何動作都會記錄在審核日誌中。
- 審核日誌記錄的數目上限是 1024。審核日誌已滿時，新的日誌項目將會自動改寫最舊的項目。

檢視維護歷程

維護歷程頁面包含韌體更新、配置及硬體更換歷程的相關資訊。

可以過濾維護歷程的內容，以顯示特定事件類型或特定時間間隔。

附註：維護歷程記錄的數目上限是 250。維護歷程日誌已滿時，新的日誌項目將會自動改寫最舊的項目。

配置警示接收者

若要新增和修改電子郵件和 Syslog 通知或 SNMP 設陷接收者，請使用本主題中的資訊。

以下是可在**警示接收者**標籤中執行的動作說明。

下列動作項目可以在**電子郵件/Syslog** 接收者區段中執行。

- **建立**：選取此動作項目可建立其他新的電子郵件接收者和 Syslog 接收者。最多可配置 12 個電子郵件和 Syslog 接收者。
  - **建立電子郵件收件者**：選取此動作項目可建立電子郵件收件者。
    - 輸入收件者的名稱和電子郵件位址。
    - 選取要啟用或停用事件通知。如果選取停用，將會保留配置的帳戶，但不會傳送任何電子郵件。
    - 選取要通知接收者的事件類型。如果按一下「嚴重」、「注意」或「系統」種類標籤旁的下拉功能表，則您可以選取或取消選取該種類中特定元件的通知。
    - 您可以選擇是否在電子郵件警示中附上事件日誌內容。
    - 該索引會指定要指派 12 個接收者插槽中的某一個。
    - 您可以在此配置要接受事件轉遞的電子郵件伺服器，或按一下區段上方的「SMTP 伺服器」動作。請參閱下方「SMTP 伺服器」以取得詳細配置資料。
  - **建立 Syslog 接收者**：選取此動作項目可建立 Syslog 接收者。

— 輸入 Syslog 伺服器的名稱和 IP 位址或主機名稱。

— 選取要啟用或停用事件通知。如果選取停用，將會保留配置的帳戶，但不會傳送任何電子郵件。

— 該索引會指定要指派 12 個接收者插槽中的某一個。

— 選取要傳送至 Syslog 伺服器的事件類型。如果按一下「嚴重」、「注意」或「系統」種類標籤旁的下拉功能表，則您可以選取或取消選取該種類中特定元件的通知。

- **SMTP 伺服器**：選取此動作項目可配置 SMTP 電子郵件伺服器的相關設定。只能配置一個電子郵件伺服器。將警示傳送給所有配置的電子郵件收件者時，會使用相同的電子郵件配置。如果目標郵件伺服器支援的話，BMC 會透過埠 587 統一使用 STARTTLS 指令，自動從安全連線切換至加密連線進行郵件傳輸。

  — 輸入電子郵件伺服器的主機名稱或 IP 位址及網路埠號。

  — 如果電子郵件伺服器需要鑑別，請選取**需要鑑別**勾選框，然後輸入使用者名稱和密碼。選取電子郵件伺服器所需的鑑別類型，可以是盤查 - 回應方法 (**CRAM MD5**) 或簡易認證 (**LOGIN**)。

  — 如果反向路徑值不符合預期，部分網路可能會阻擋外寄的電子郵件。依預設，XClarity Controller 會使用 alertmgr@domain，其中 domain 是 XClarity Controller 網頁中 DDNS 區段所指定的網域名稱。您可以指定寄件者資訊以取代預設值。

  — 您可以測試與電子郵件伺服器的連線，以確保正確配置電子郵件設定。XClarity Controller 會顯示連線是否成功的訊息。

- **重試和延遲**：選取此動作項目可配置重試和延遲選項的相關設定。

  — 「重試限制」可指定在初始嘗試失敗後，XClarity Controller 可嘗試傳送警示的次數。

  — 「輸入之間的延遲」可指定 XClarity Controller 將警示傳送給前後兩位接收者之間的等待時間。

  — 「嘗試之間的延遲」可指定嘗試失敗之後，重試傳送警示之前，XClarity Controller 的等待時間。

- **通訊協定**：選取此動作項目可配置連線通訊協定的相關設定。

  — 您可以選擇「**TCP 通訊協定**」或「**UDP 通訊協定**」，請注意，此設定將套用至所有 syslog 接收者。

- 如果已建立電子郵件或 Syslog 接收者，則會在本區段中列出這些接收者。

  — 若要編輯電子郵件或 Syslog 接收者的設定，請在要配置之接收者旁邊的橫列上，按一下動作標題下方的鉛筆圖示。

  — 若要刪除電子郵件或 Syslog 接收者，請按一下垃圾桶圖示。

  — 如果要傳送測試警示給電子郵件或 Syslog 接收者，請按一下紙飛機圖示。

以下是可在 **SNMPv3** 使用者區段中執行的動作。

- **建立**：選取此動作項目可建立 SNMPv3 設陷接收者。

  — 選取要與 SNMPv3 設陷相關聯的使用者帳戶。使用者帳戶必須是十二個本端使用者帳戶的其中一個。

  — 指定會收到 SNMPv3 設陷的 SNMPv3 管理程式的主機名稱或 IP 位址。

  — XClarity Controller 使用 HMAC-SHA 雜湊演算法向 SNMPv3 管理程式進行鑑別。這是唯一受支援的演算法。

  — 保密密碼與保密通訊協定搭配使用，以加密 SNMP 資料。

  — **SNMPv3 廣域設定**套用至所有 SNMPv3 設陷接收者。您可以在建立 SNMPv3 設陷接收者時，或藉由按一下 **SNMPv3** 使用者區段上方的「SNMPv3 設定」動作，配置這些設定。

    — 選取要啟用或停用 SNMPv3 設陷。如果停用，則會保留配置的設定，但不會傳送 SNMPv3 設陷。

    — 必須在「伺服器內容」網頁配置 BMC 聯絡人和位置資訊。如需相關資訊，請參閱第 69 頁 「設定位置和聯絡人」。

    — 選取會導致設陷傳送至 SNMPv3 管理程式的事件類型。如果按一下「嚴重」、「注意」或「系統」種類標籤旁的下拉功能表，則您可以選取或取消選取該種類中特定元件的通知。

  附註：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**保密通訊協定**方法是 CBC-DES 和 AES。

- 如果已建立 SNMPv3 設陷接收者，則會在本區段中列出這些接收者。
  - 如果要編輯 SNMPv3 接收者的設定，請在要配置之接收者旁邊的橫列上，按一下動作標題下方的鉛筆圖示。
  - 如果要刪除 SNMPv3 接收者，請按一下垃圾桶圖示。

擷取上次 OS 失敗畫面資料

使用本主題中的資訊來擷取及檢視作業系統失敗畫面。

發生「OS 監視器」逾時時，會自動擷取作業系統畫面。如果發生導致 OS 停止執行的事件，會觸發「OS 監視器」特性，並擷取畫面內容。XClarity Controller 只會儲存一個畫面擷取。發生「OS 監視器」逾時時，新的畫面擷取會改寫前一個畫面擷取。必須啟用「OS 監視器」特性，才會擷取 OS 失敗畫面。若要設定「OS 監視器時間」，請參閱第 70 頁 「設定伺服器逾時」，以取得相關資訊。只有 XClarity Controller 進階版或企業版層次的功能，才有提供 OS 失敗畫面擷取特性。若要瞭解伺服器中安裝的 XClarity Controller 功能層次，請參閱伺服器的文件。

在 XClarity Controller 首頁的**遠端主控台**區段中，按一下**上次失敗畫面**動作，以檢視發生「OS 監視器」逾時時，所擷取的作業系統顯示影像。在首頁的**快速動作**區段中，依序按一下**服務**和**上次失敗畫面**，也可以檢視該擷取。如果系統未發生過「OS 監視器」逾時並擷取 OS 畫面，則會顯示訊息，指出尚未建立失敗畫面。

第 5 章 配置伺服器

使用本章的資訊，可瞭解伺服器可用的配置選項。

配置伺服器時，可用的選項如下：

- 配接卡
- 開機選項
- 電源原則
- 伺服器內容

檢視配接卡資訊和配置設定

使用本主題中的資訊來檢視伺服器中安裝之配接卡的相關資訊。

按一下**伺服器配置**下的**配接卡**，可檢視伺服器中安裝之配接卡的相關資訊。

附註：

- 如果配接卡不支援狀態監視，則不會顯示其監視或配置資訊。如需所有已安裝之 PCI 配接卡的庫存相關資訊，請參閱**庫存**頁面。

配置系統開機模式和順序

如果要配置系統開機模式和順序，請使用本主題中的資訊。

當您選取**伺服器配置**下的**開機選項**時，您可以配置系統開機模式和順序。

附註：未經鑑別的頻內方法不能變更安全性相關系統設定。例如，不能透過 OS 或 UEFI Shell 上的未經鑑別頻內 API 來配置安全開機。這包括頻內執行的 OneCLI，並使用 IPMI 或任何工具和 API 來配置安全開機、TPM、UEFI 設定密碼相關設定。所有安全性相關設定都需要具有足夠專用權的正確鑑別。

針對系統開機模式，有下列兩個選項：

UEFI 開機
選取此選項可配置支援 Unified Extensible Firmware Interface (UEFI) 的伺服器。如果是啟動已啟用 UEFI 的作業系統，此選項可藉由停用舊式 Option ROM 縮短開機時間。

舊式開機
如果要將伺服器配置為啟動需要舊式 (BIOS) 韌體的作業系統，請選取此選項。僅在您要啟動未啟用 UEFI 的作業系統時，才選取此選項。

如果要配置系統開機順序，請從**可用的裝置**清單中選取裝置，然後按一下向右箭頭，將裝置新增至開機順序中。如果要從開機順序中移除裝置，請從開機順序清單中選取裝置，然後按一下向左箭頭，將裝置移回可用的裝置清單中。如果要變更開機順序，請選取裝置，然後按一下向上或向下鍵，將裝置依優先順序向上或向下移動。

當您變更開機順序時，必須先選取重新啟動選項，才能套用變更。下列選項可供使用：

- **立即重新啟動伺服器**：儲存開機順序變更後立即重新啟動伺服器，不需關閉作業系統。
- **正常重新啟動伺服器**：儲存開機順序變更後，會先關閉作業系統，再重新啟動伺服器。
- **稍後手動重新啟動**：將儲存開機順序變更，但是要到下次重新啟動伺服器之後才會生效。

配置單次開機

如果要暫時忽略配置的開機，而改為單次開機至指定裝置，請使用本主題中的資訊。

按一下**伺服器配置**下的**開機選項**，然後從下拉功能表中選取裝置，配置系統將在下一次伺服器重新啟動時單次開機的裝置。下列選項可供使用：

PXE 網路
將您的伺服器設定為嘗試開機前執行環境網路開機。

主要抽取式媒體
伺服器會從預設的 USB 裝置啟動。

預設 CD/DVD
伺服器會從預設的 CD/DVD 光碟機啟動。

F1 系統設定
伺服器會開機至 Lenovo XClarity Provisioning Manager。

診斷分割區
伺服器會開機至 Lenovo XClarity Provisioning Manager 的「診斷」區段。

預設硬碟
伺服器會從預設的硬碟啟動。

主要遠端媒體
伺服器從裝載的虛擬媒體開機。

無單次開機
使用配置的開機順序。不會使用單次開機來置換配置的開機順序。

當您變更要使用單次開機裝置執行的開機類型時，您也可以將開機指定為舊式開機或 UEFI 開機。如果您希望開機是舊式 BIOS 開機，請按一下**偏好舊式開機**。如果想要 UEFI 開機，則取消勾選方框。當您選取單次變更開機順序時，必須先選取重新啟動選項，才能套用變更。

- **立即重新啟動伺服器**：儲存開機順序變更後立即重新啟動伺服器，不需關閉作業系統。
- **正常重新啟動伺服器**：儲存開機順序變更後，會先關閉作業系統，再重新啟動伺服器。
- **稍後手動重新啟動**：儲存開機順序變更，但是要到下次重新啟動伺服器之後才會生效。

管理伺服器電源

若要檢視電源管理資訊及執行電源管理功能，請使用本主題中的資訊。

選取**伺服器配置**下的**電源原則**，以檢視電源管理資訊和執行電源管理功能。

附註：在內含刀鋒伺服器或高密度伺服器節點的機箱中，機箱冷卻和電源是由機箱管理控制器而非 XClarity Controller 來控制。

配置電源備援

如果要配置電源備援，請使用本主題中的資訊。

「電源備援」區段中的可用欄位包括：

- **備用 (N+N)**：在此模式中，伺服器在失去一個電源供應器後仍可維持運作。
  - **零輸出模式**：在備援配置下啟用後，某些 PSU 會自動進入輕載條件下的待命狀態。以這種方式，其餘 PSU 可以提供整個電源負載以提高效率。

- **備用 (N+1)**：在此模式中，安裝四個電源供應器時，伺服器在失去一個電源供應器後仍可維持運作。
- **非備用模式**：在此模式中，無法保證伺服器若失去電源供應器仍可維持運作。如果電源供應器嘗試維持運轉時失敗，伺服器將進行節流控制。

變更配置後，按一下**套用**。

配置功率上限原則

若要配置功率上限原則，請使用本主題中的資訊。

您可以選擇啟用或停用功率上限功能。如果已啟用功率上限，可選取限制伺服器用電量的選項。如果已停用功率上限，伺服器使用的最大功率則由電源備援原則決定。如果要變更設定，請先按一下**重設**。選擇您偏好的設定，然後按一下**套用**。

您可以使用 AC 耗電量測量或 DC 耗電量測量來啟用功率上限。從下拉功能表中選取用於決定功率上限限制的測量類型。在 AC 和 DC 之間切換時，調節器上的數字也會隨之改變。

有兩種方法可變更功率上限值：

- **方法 1**： 將調節器標記移至所需的瓦特數，以設定整體伺服器電源限制。
- **方法 2**：在輸入方框中輸入值。調節器標記將會自動移至對應的位置。

變更配置後，按一下**套用**。

附註：當 XClarity Controller 位於內含刀鋒伺服器或高密度伺服器節點的機箱中時，無法使用**電源原則**選項。電源原則是由機箱管理控制器而非 XClarity Controller 所控制。

配置電源還原原則

如果要配置伺服器在電源中斷後還原時的反應方式，請使用本主題中的資訊。

配置電源還原原則時，有下列三個選項：

一律關閉
即使電源已還原，伺服器電源仍維持關閉。

還原
如果伺服器電源在發生電源故障時是開啟的，則當電源還原時，將會自動開啟伺服器電源。否則當電源還原時，伺服器電源仍會維持關閉。

一律開啟
伺服器將在電源還原時自動開啟電源。

變更配置後，按一下**套用**。

附註：在內含刀鋒伺服器或高密度伺服器節點的機箱中，無法使用**電源還原原則**選項。電源還原原則是由機箱管理控制器而非 XClarity Controller 所控制。

電源動作

查看本主題中的資訊，以瞭解可以對伺服器執行的電源動作。

按一下 XClarity Controller 首頁的**快速動作**區段中的**電源動作**。

下表包含可以在伺服器上執行的電源和重新啟動動作的說明。

表格 6. 電源動作和說明

兩欄表格，包含伺服器電源和重新啟動動作的說明。

電源動作	**說明**
開啟伺服器電源	選取此動作項目可開啟伺服器電源及啟動作業系統。
正常關閉伺服器電源	選取此動作項目可關閉作業系統和關閉伺服器電源。
立即關閉伺服器電源	選取此動作項目可關閉伺服器電源，而不需先關閉作業系統。
正常重新啟動伺服器	選取此動作項目可關閉作業系統，並關閉後再開啟伺服器電源。
立即重新啟動伺服器	選取此動作項目可立即關閉伺服器電源後再開啟電源，而不需先關閉作業系統。
將伺服器開機至系統設定	選取此項目可開啟伺服器電源或重新啟動伺服器，並自動開機至系統設定，而不需在開機期間按 F1。
觸發不可遮罩式岔斷 (NMI)	選取此動作項目可在「當機」系統上強制執行不可遮罩式岔斷 (NMI)。選取此動作項目可讓平台作業系統執行記憶體傾出，記憶體傾出可用於系統當機狀況的除錯用途。F1 系統設定功能表中 NMI 設定上的自動重新啟動會決定 XClarity Controller 是否將在 NMI 之後重新啟動伺服器。
排程電源動作	選取此動作項目可為伺服器排定每日和每週電源和重新啟動動作。
重新啟動管理控制器	選取此動作項目可重新啟動 XClarity Controller
關閉再開啟伺服器的 AC 電源	選取此動作以關閉再開啟伺服器的電源。
附註：如果在嘗試關閉作業系統時，作業系統處於螢幕保護程式或鎖定模式，XClarity Controller 可能無法起始正常關機。XClarity Controller 會在電源關閉延遲間隔到期後執行硬重設或關機，而作業系統可能仍處於執行中狀態。	

使用 IPMI 指令來管理及監視耗電量

使用本主題中的資訊，以 IPMI 指令來管理及監視耗電量。

本主題說明如何使用 Intel Intelligent Power Node Manager 和資料中心可管理性介面規格 (DCMI)，利用智慧型平台管理介面 (IPMI) 電源管理指令為伺服器提供電源和散熱監視以及原則式電源管理。

針對使用 Intel Node Manager SPS 3.0 的伺服器，XClarity Controller 使用者可以使用 Intel Management Engine (ME) 提供的 IPMI 電源管理指令來控制 Node Manager 功能，以及監視伺服器耗電量。伺服器電源管理也可以使用 DCMI 電源管理指令來達成。本主題中提供 Node Manager 和 DCMI 電源管理指令的範例。

使用 Node Manager 指令管理伺服器電源

使用本主題中的資訊，以「節點管理程式」來管理伺服器電源。

Intel Node Manager 韌體沒有外部介面；因此，Node Manager 指令必須先被 XClarity Controller 接收，再傳送至 Intel Node Manager。XClarity Controller 使用標準 IPMI 橋接來擔任 IPMI 指令的轉送和傳輸裝置。

附註：使用 Node Manager IPMI 指令變更 Node Manager 原則可能會與 XClarity Controller 電源管理功能產生衝突。依預設已停用 Node Manager 指令的橋接，以防止任何衝突。

對於想要使用 Node Manager 取代 XClarity Controller 來管理伺服器電源的使用者，可以使用由（網路功能：**0x3A**）和（指令：**0xC7**）組成的 OEM IPMI 指令。

如果要啟用原生 Node Manager IPMI 指令類型：ipmitool -H **<$XClarity_Controller_IP>** -U **<USERID>** -P **<PASSW0RD>** raw **0x3a 0xc7 0x01**

如果要停用原生 Node Manager IPMI 指令類型：ipmitool -H **<$XClarity_Controller_IP>** -U **<USERID>** -P **<PASSW0RD>** raw **0x3a 0xc7 0x00**

下列資訊是 Node Manager 電源管理指令的範例。

附註：

- 透過指定 IPMI **通道 0** 和 **0x2c** 的目標位址，您可以使用 IPMITOOL 將指令傳送至 Intel Node Manager 以進行處理。要求訊息是用於起始動作，然後將回應訊息送回給要求者。
- 由於空間限制，因此指令會以下列格式顯示。

使用「取得廣域系統電源統計資料」的電源監視，（指令碼 0xC8）：要求：ipmitool -H **<$XClarity_Controller_IP>** -U **<USERID>** -P **<PASSW0RD>** -b **0x00** -t **0x2c** raw **0x2E 0xC8 0x57 0x01 0x00 0x01 0x00 0x00** 回應：57 01 00 38 00 04 00 41 00 39 00 ec 56 f7 53 5a 86 00 00 50

使用「設定 Intel Node Manager 原則」的功率上限，（指令碼 0xC1）： Request:ipmitool -H **<$XClarity_Controller_IP>** -U **<USERID>** -P **<PASSW0RD>** -b **0x00** -t **0x2c** raw **0x2e 0xC1 0x57 0x01 0x00 0x10 0x01 0xA0 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00 0x00 0x1e 0x00**Response:57 01 00

使用「設定 Intel Node Manager 原則」的省電，（指令碼 0xC1）： Request:ipmitool -H **<$XClarity_Controller_IP>** -U **<USERID>** -P **<PASSW0RD>** -b **0x00** -t **0x2c** raw **0x2e 0xC1 0x57 0x01 0x00 0x10 0x01 0x00 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00 0x00 0x1e 0x00**

使用「取得 Intel 管理引擎裝置 ID」取得裝置 ID 功能：Request:ipmitool -H **<$XClarity_Controller_IP>** -U **<USERID>** -P **<PASSW0RD>** -b **0x00** -t **0x2c** raw **0x06 0x01**Response:50 01 03 05 02 21 57 01 00 05 0b 03 40 20 01

如需其他的 Intel Node Manager 指令，請參閱最新版本的**使用 IPMI 的 Intel Intelligent Power Node Manager 外部介面規格**，網址為 https://businessportal.intel.com。

使用 DCMI 指令管理伺服器電源

使用本主題中的資訊，以 DCMI 指令來管理伺服器電源。

DCMI 提供可以透過標準管理軟體介面公開的監視及控制功能。伺服器電源管理功能也可以使用 DCMI 指令來達成。

下列資訊是常用的 DCMI 電源管理功能和指令的範例。要求訊息是用於起始動作，然後將回應訊息送回給要求者。

附註：由於空間限制，因此指令會以下列格式顯示。

取得電源讀數： Request:ipmitool -H **<$XClarity_Controller_IP>** -U **<USERID>** -P **<PASSW0RD>** raw **0x2c 0x02 0xdc 0x01 0x00 0x00** Response:dc 39 00 38 00 3b 00 39 00 e3 6f 0a 39 e8 03 00 00 40

設定電源限制： Request:ipmitool -H **<$XClarity_Controller_IP>** -U **<USERID>** -P **PASSW0RD** raw **0x2c 0x04 0xdc 0x00 0x00 0x00 0x00 0xA0 0x00 0xe8 0x03 0x00 0x00 0x00 0x00 0xe8 0x03** Response:dc

取得功率限制： Request:ipmitool -H **<$XClarity_Controller_IP>** -U **<USERID>** -P **<PASSW0RD>** raw **0x2c 0x03 0xdc 0x00 0x00** Response:dc 00 00 00 a0 00 e8 03 00 00 00 00 01 00

啟動電源限制： Request:ipmitool -H **<$XClarity_Controller_IP>** -U **<USERID>** -P **<PASSW0RD>** raw **0x2c 0x05 0xdc 0x01 0x00 0x00** Response:dc

停用電源限制： Request:`ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSW0RD> raw 0x2c 0x05 0xdc 0x00 0x00 0x00` Response:`dc`

附註：在部分伺服器上，可能不支援**設定電源限制**指令的例外動作。例如，可能不支援**硬關閉系統電源並將事件記錄至 SEL** 參數。

如需 DCMI 規格支援的指令的完整清單，請參閱最新版的**資料中心可管理性介面規格**，網址為 https://www.intel.com/content/dam/www/public/us/en/documents/technical-specifications/dcmi-v1-5-rev-spec.pdf。

遠端主控台功能

使用本主題中的資訊，以瞭解如何從遠端檢視伺服器主控台，以及與其互動。

您可以使用 XClarity Controller Web 介面中的遠端主控台功能，以檢視並與伺服器主控台互動。您可以將磁碟映像檔（ISO 或 IMG 檔案）指派為伺服器上的虛擬硬碟。遠端主控台是 XClarity Controller 進階版和 XClarity Controller 企業版提供的功能，而且僅可透過 Web 介面使用。您必須使用具有監督者存取權或遠端主控台存取權限的使用者 ID 登入 XClarity Controller，才能使用遠端主控台功能。如需從 XClarity Controller 標準版升級為 XClarity Controller 進階版或 XClarity Controller 企業版的相關資訊，請參閱第 5 頁「升級 XClarity Controller」。

使用遠端主控台功能來執行下列動作：

- 無論伺服器狀態為何，都能以最高達 1280 x 1024（72 或 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，從遠端存取伺服器。
- 裝載位於您本端系統或遠端系統上的 ISO 和 IMG 檔案，做為可供伺服器使用的虛擬硬碟。
- 將 IMG 或 ISO 映像檔上傳至 XClarity Controller 記憶體，並將它裝載至伺服器做為虛擬硬碟。最多可上傳兩個檔案（大小總計上限為 50 MB）至 XClarity Controller 記憶體。

附註：

- 在多使用者模式中啟動遠端主控台功能時（具有 XClarity Controller 企業版功能集的 XClarity Controller 最多可支援六個同步階段作業），遠端磁碟功能每次只能由一個階段作業執行。
- 遠端主控台只能顯示由主機板上的視訊控制器產生的視訊。如果安裝並使用個別的視訊控制器配接卡來取代系統的視訊控制器，則 XClarity Controller 遠端主控台無法顯示來自新增配接卡的視訊內容。
- 如果您的網路中有防火牆，必須開啟網路埠才能支援遠端主控台功能。如果要檢視或變更遠端主控台功能所使用的網路埠號，請參閱第 31 頁「服務啟用和埠指派」。
- 遠端主控台功能使用 HTML5 在網頁上顯示伺服器視訊。如果要使用此功能，您的瀏覽器必須支援顯示使用 HTML5 元素的視訊內容。
- 如果您是使用自簽憑證和 IPv6 位址透過 Internet Explorer 瀏覽器來存取 BMC，可能會因憑證錯誤而無法啟動遠端主控台階段作業。為避免此問題，自簽憑證可以新增至 Internet Explorer 授信主要憑證授權單位：
  - 選取 **BMC 配置**下的**安全性**並下載自簽憑證。
  - 將憑證副檔名變更為 *.crt，然後按兩下 Web 憑證檔案。
  - 清除 IE11 瀏覽器快取。
  - 依照憑證匯入精靈的步驟，按一下**安裝憑證**將憑證安裝至憑證存放區。

啟用遠端主控台功能

此主題提供遠端主控台功能的相關資訊。

如稍早所述，XClarity Controller 遠端主控台功能僅在 XClarity Controller 進階版和 XClarity Controller 企業版功能中提供。如果您沒有操作遠端主控台的專用權，將會看到鎖定圖示。

在您購買並取得 XClarity Controller 進階版升級的啟動金鑰之後，使用第 79 頁 「安裝啟動金鑰」下的指示進行安裝。

如果要使用遠端主控台功能，請完成下列步驟：

1. 在 XClarity Controller 首頁或遠端主控台網頁的「遠端主控台」區段中，按一下有白色斜箭頭的影像。
2. 請選取下列其中一種模式：
   - 在單一使用者模式中啟動遠端主控台
   - 在多使用者模式中啟動遠端主控台

   附註：具有 XClarity Controller 企業版功能集的 XClarity Controller 在多使用者模式中最多可支援六個同步視訊階段作業。
3. 選取當有人希望使用遠端主控台功能，且在單一使用者模式中已使用此功能時，或當最大數目的使用者正在多使用者模式中使用遠端主控台功能時，是否允許他人要求將斷線要求傳送給遠端主控台使用者。**無回應時間間隔**會指定若斷線要求未收到回應時，XClarity Controller 在與使用者自動斷線之前等待的時間。
4. 選取是否允許記錄最近三個伺服器開機視訊。
5. 選取是否允許記錄最近三個伺服器當機視訊。
6. 選取是否允許含有硬體錯誤的 OS 失敗畫面擷取。
7. 按一下**啟動遠端主控台**，在另一個標籤中開啟遠端主控台頁面。當所有可能的遠端主控台階段作業都在使用中時，即會蹦現對話框。使用者可以從這個對話框將斷線要求傳送給遠端主控台使用者，該使用者已啟用**允許他人要求我的遠端階段作業中斷連線**的設定。使用者可以接受或拒絕要中斷連線的要求。如果使用者未在**無回應時間間隔**設定所指定的間隔內回應，XClarity Controller 將會自動結束使用者階段作業。

遠端電源控制

本主題說明如何從遠端主控台視窗傳送伺服器電源和重新啟動指令。

您可以從遠端主控台視窗傳送伺服器電源和重新啟動指令，而無須返回主網頁。如果要透過遠端主控台來控制伺服器電源，請按一下**電源**並選取下列其中一個指令：

開啟伺服器電源
選取此動作項目可開啟伺服器電源及啟動作業系統。

正常關閉伺服器電源
選取此動作項目可關閉作業系統和關閉伺服器電源。

立即關閉伺服器電源
選取此動作項目可關閉伺服器電源，而不需先關閉作業系統。

正常重新啟動伺服器
選取此動作項目可關閉作業系統，並關閉後再開啟伺服器電源。

立即重新啟動伺服器
選取此動作項目可立即關閉伺服器電源後再開啟電源，而不需先關閉作業系統。

將伺服器開機至系統設定
選取此項目可開啟伺服器電源或重新啟動伺服器，並自動開機至系統設定，而不需在開機期間按 F1。

遠端主控台擷取畫面

使用本主題中的資訊來瞭解如何使用遠端主控台畫面擷取功能。

遠端主控台視窗中的畫面擷取功能可擷取伺服器的視訊顯示內容。如果要擷取並儲存畫面影像，請完成下列步驟：

步驟 1. 在遠端主控台視窗中，按一下**擷取畫面**。

步驟 2. 在蹦現視窗中，按一下**儲存檔案**，然後按**確定**。檔案將命名為 rpviewer.png，並儲存至您的預設下載資料夾。

附註：畫面擷取影像會儲存為 PNG 檔案類型。

遠端主控台鍵盤支援

在遠端主控台視窗的**鍵盤**下，提供下列選項：

- 按一下**虛擬鍵盤**啟動虛擬鍵盤。如果您是使用無實體鍵盤的平板裝置，此功能很有用。下列選項可用來建立可傳送至伺服器的巨集和按鍵組合。您所使用的用戶端系統上的作業系統可能會設陷捕捉特定按鍵組合（例如 Ctrl+Alt+Del），而非將它們傳輸至伺服器。其他按鍵（例如 F1 或 Esc）可能被您正在使用的程式或瀏覽器攔截。巨集提供一種機制，可將按鍵傳送至使用者可能無法傳送的伺服器。
- 按一下**伺服器巨集**以使用伺服器定義的巨集。部分伺服器巨集是由 XClarity Controller 韌體預先定義。其他伺服器定義的巨集可以使用 Lenovo XClarity Essentials 來定義，並從 XClarity Controller 下載。這些巨集是針對遠端主控台功能的所有使用者來定義。
- 按一下**配置**以新增或移除使用者定義的巨集。使用者定義的巨集僅針對目前的遠端主控台使用者來定義。其他的遠端主控台使用者不會看到彼此的使用者定義的巨集。
  - 按一下「新增巨集」圖示，然後按下您所需的按鍵順序；然後，按一下**新增**以新增巨集。
  - 如果要移除使用者定義的巨集，請從清單中選取巨集，然後按一下垃圾桶圖示。
  - 如果要將使用者定義的巨集傳送至伺服器，請選取**使用者定義的巨集**選項，然後按一下要傳送的巨集。

遠端主控台滑鼠支援

使用此資訊來瞭解滑鼠遠端控制選項。

遠端主控台視窗針對滑鼠控制提供數個選項，包括絕對滑鼠控制、相對滑鼠控制（無加速）和滑鼠控制（RHEL、較舊的 Linux）。

絕對和相對滑鼠控制

使用此資訊存取用於控制滑鼠的絕對和相對選項。

如果要存取用於控制滑鼠的絕對和相對選項，請完成下列步驟：

步驟 1. 在遠端主控台視窗中，按一下**滑鼠**。

步驟 2. 在下拉功能表中，按一下**滑鼠設定**。

步驟 3. 選取下列其中一個**滑鼠加速**模式：

絕對位置（Windows、較新的 Linux 和 Mac OS X）
用戶端會將滑鼠位置訊息傳送至與檢視區域的原點（左上方區域）相對的伺服器。

相對位置，無加速
用戶端傳送滑鼠位置做為距先前滑鼠位置的偏移。

相對位置（較舊的 Linux）
此模式會套用加速因素，以便在部分 Linux 目標上更好地對齊滑鼠。已選取加速設定，以最大化與舊的 Linux 發行套件的相容性。

畫面錄影/重播

使用本主題中的資訊，錄製或重播遠端顯示畫面視訊。

XClarity Controller Web 介面提供了類似 DVR 的功能，可支援錄製和播放遠端顯示畫面視訊。此功能僅支援錄製視訊到網路資料夾。目前支援 NFS 和 CIFS 通訊協定。使用錄製和重播功能的步驟如下。

1. 在遠端主控台網頁上，按一下**畫面錄製**開啟設定視窗。
2. 在設定視窗中，可能需要指定下列資訊。
   - 如果選取了「CIFS」裝載類型，請指定**遠端資料夾**、**使用者名稱**和**密碼**參數。CIFS 遠端資料夾的格式為「**//<遠端 IP 位址>/<資料夾名稱>**」。例如：//xxx.xxx.xxx.xxx/folder。
   - 如果選取了「NFS」裝載類型，請指定**遠端資料夾**參數。NFS 遠端資料夾的格式為「**<遠端 IP 位址>:/<資料夾名稱>**」。例如：xxx.xxx.xxx.xxx:/folder。
   - 視需要指定視訊檔案名稱。如果已經提供檔案名稱，則會顯示錯誤訊息框。若要改寫現有檔案名稱，請選擇「改寫檔案名稱」。如果核取了「自動」勾選框，將自動產生視訊檔案名稱。
   - 「檔案大小上限」表示自動停止錄製視訊之前將形成的最大視訊檔案大小。
   - 「錄製期間上限」表示自動停止錄製之前將持續錄製視訊的最長時間。
3. 按一下**開始錄製**開始視訊錄製。
4. 按一下**停止錄製**停止視訊錄製。蹦現視窗隨即出現，提示「視訊錄製已完成」並顯示相關的視訊錄製資訊。
5. 從 NFS 或 CIFS 將錄製的視訊下載到本端資料夾。在 XClarity Controller 首頁的「遠端主控台預覽」區段，按一下**錄製的視訊**並選取要重播的視訊檔案。

遠端主控台畫面模式

使用本主題中的資訊來配置遠端主控台畫面模式。

如果要配置遠端主控台畫面模式，請按一下**螢幕模式**。

下列功能表選項可供使用：

全螢幕
此模式使用視訊顯示畫面填滿用戶端桌面。在此模式中按 Esc 鍵將結束全螢幕模式。由於在全螢幕模式中看不到遠端主控台功能表，因此您必須結束全螢幕模式才能使用遠端主控台功能表提供的功能，例如鍵盤巨集。

適合螢幕
這是遠端主控台啟動時的預設值。在此設定中會完全顯示目標桌面，而沒有捲軸，並維持長寬比。

縮放螢幕
啟用縮放後，會調整視訊影像的大小，讓完整影像能夠填滿主控台視窗。

原始螢幕
視訊影像的尺寸與伺服器端相同。捲軸會視需要顯示，以便檢視視窗無法容納的視訊影像區域。

色彩模式
調整遠端主控台視窗的色彩深度。有兩種色彩模式選擇：

- 顏色：7、9、12、15 和 23 位元
- 灰階：16、32、64 和 128 網底

附註：如果您與遠端伺服器連線的頻寬受限，而您希望減少頻寬需求，通常會進行色彩模式調整。

媒體裝載方法

使用本主題中的資訊，以瞭解如何執行媒體裝載。

提供三種可將 ISO 和 IMG 檔案裝載為虛擬硬碟的機制。

- 按一下**媒體**，即可從遠端主控台階段作業將虛擬硬碟新增至伺服器。
- 直接從遠端主控台網頁，不需建立遠端主控台階段作業。
- 獨立工具

使用者需要**遠端主控台及遠端硬碟存取**專用權才能使用虛擬媒體功能。

檔案可以從本端系統或遠端伺服器裝載為虛擬媒體，並且可透過網路加以存取，或使用 RDOC 功能上傳至 XClarity Controller 記憶體。這些機制如下所述。

- 本端媒體是位於您用於存取 XClarity Controller 的系統上的 ISO 或 IMG 檔案。此機制僅透過遠端主控台階段作業提供，無法直接從遠端主控台網頁使用，且僅限搭配 XClarity Controller 企業版功能使用。如果要裝載本端媒體，請按一下**裝載本端媒體**區段中的**啟動**。最多可以將四個檔案同時裝載到伺服器。

  附註：

  — 使用 Google Chrome 瀏覽器時，系統會額外提供一個名為**裝載檔案/資料夾**的裝載選項，讓您拖放檔案/資料夾。

  — 如果多個同時遠端主控台階段作業正與 XClarity Controller 一起進行，此功能只能由其中一個階段作業啟動。

- 也可以裝載位於遠端系統上的檔案做為虛擬媒體。最多可以同時裝載四個檔案做為虛擬硬碟。XClarity Controller 支援下列檔案共用通訊協定：

  — CIFS – 一般網際網路檔案系統：

  — 輸入為遠端系統上的檔案定位的 URL。

  — 如果您要讓檔案向伺服器展示為唯讀虛擬媒體，請勾選勾選框。

  — 輸入 XClarity Controller 存取遠端系統上的檔案所需的認證。

  附註：XClarity Controller 不支援使用者名稱、密碼或 URL 中包含空格。請確定為 CIFS 伺服器配置登入認證的使用者名稱或密碼中沒有空格，且 URL 不包含空格。

  — 裝載選項是選用的，而且是由 CIFS 通訊協定所定義。

  — 如果遠端伺服器屬於一組集中處理安全性的伺服器，請輸入遠端伺服器所屬的網域名稱。

  — NFS – 網路檔案系統：

  — 輸入為遠端系統上的檔案定位的 URL。

  — 如果希望檔案向伺服器顯示為唯讀虛擬媒體，請核取勾選框。

  — 裝載選項是選用的，而且是由 NFS 通訊協定所定義。支援 NFSv3 與 NFSv4。例如，若要使用 NFSv3，您必須指定「nfsvers=3」選項。如果 NFS 伺服器會使用 AUTH_SYS 安全特點來鑑別 NFS 作業，您就必須指定「sec=sys」選項。

  — HTTPFS — HTTP Fuse 型檔案系統：

  — 輸入為遠端系統上的檔案定位的 URL

  — 如果您要讓檔案向伺服器展示為唯讀虛擬媒體，請勾選勾選框。

  附註：裝載 Microsoft IIS 所產生的安全憑證期間，可能會發生錯誤。如果發生這種情況，請參閱第 67 頁 「媒體裝載錯誤問題」。

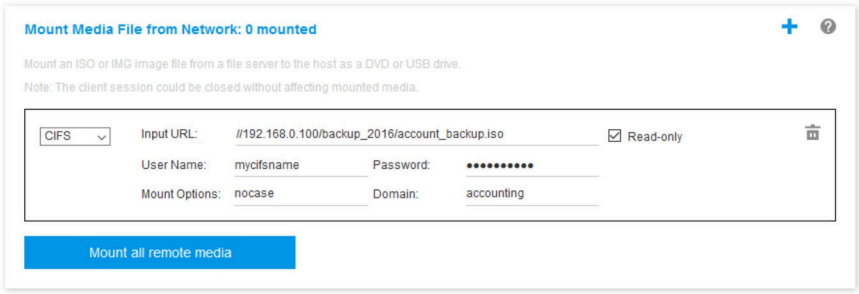
  按一下**裝載所有遠端媒體**，以裝載檔案做為虛擬媒體。如果要移除虛擬媒體，請按一下裝載的媒體右側的垃圾桶圖示。

- 最多可以在 XClarity Controller 記憶體中上傳兩個檔案，並使用 XClarity Controller RDOC 功能裝載做為虛擬媒體。兩個檔案的大小總計不得超過 50 MB。這些檔案將會保留在 XClarity Controller 記憶體中，直到檔案遭移除；在此之前，即使遠端主控台階段作業已結束，仍會保留。上傳檔案時，RDOC 功能支援下列機制：

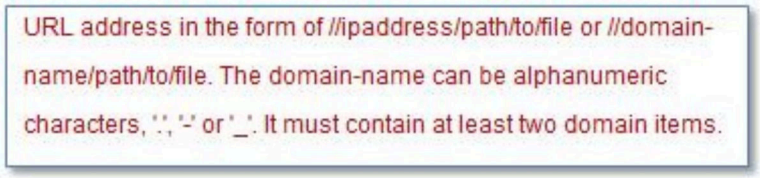
— **CIFS – 一般網際網路檔案系統**：如需詳細資料，請參閱上述說明。

範例：

若要將 ISO 檔案 account_backup.iso（位於 IP 位址為 192.168.0.100 之 CIFS 伺服器的 backup_2016 目錄）裝載為伺服器上的唯讀虛擬硬碟，您可以在下圖所示的欄位中填入資訊。在此範例中，位於 192.168.0.100 的伺服器是在「accounting」網域下的伺服器集合成員。網域名稱為選用，可省略。如果您的 CIFS 伺服器不屬於網域，請讓**網域**欄位保留空白。此範例中的**裝載選項**欄位指定了 CIFS「nocase」裝載選項，指示 CIFS 伺服器應忽略檔案名稱的大寫/小寫檢查。**裝載選項**欄位為選用，可省略。使用者在此欄位輸入的資訊並非由 BMC 使用，只是會在提出裝載要求時傳遞給 CIFS 伺服器。請參閱 CIFS 伺服器實作文件，以判斷您的 CIFS 伺服器支援哪些選項。



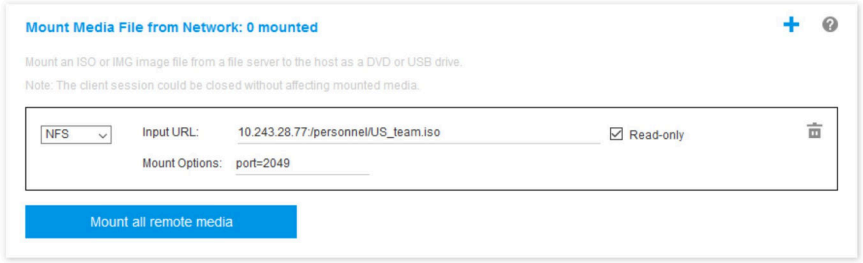
BMC 會在指定 URL 時提供指引。如果輸入的 URL 不正確，裝載按鈕就會變成灰色，而且 URL 欄位下方會顯示紅色文字，指出預期的 URL 格式。



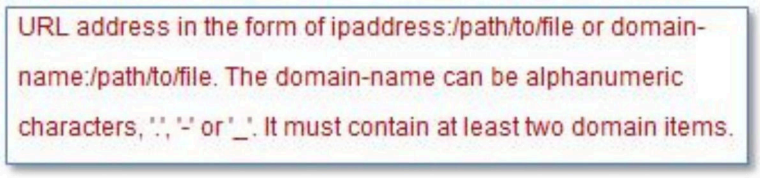
— **NFS – 網路檔案系統**：如需詳細資料，請參閱上述說明。

範例：

若要將 ISO 檔案 US_team.iso (位於 IP 位址為 10.243.28.77 之 NFS 伺服器的「personnel」目錄) 裝載為伺服器上的唯讀虛擬硬碟，您可以在下圖所示的欄位中填入資訊。NFS「port=2049」裝載選項會指定應使用網路埠 2049 來傳輸資料。**裝載選項**欄位為選用，可省略。使用者在此欄位輸入的資訊會在提出裝載要求時傳遞給 NFS 伺服器。請參閱 NFS 伺服器實作文件，以判斷您的 NFS 伺服器支援哪些選項。



BMC 會在指定 URL 時提供指引。如果輸入的 URL 不正確，裝載按鈕就會變成灰色，而且 URL 欄位下方會顯示紅色文字，指出預期的 URL 格式。



— **HTTPS — 超文字安全傳輸通訊協定**：

— 輸入為遠端系統上的檔案定位的 URL。

— 如果您要讓檔案向伺服器展示為唯讀虛擬媒體，請勾選勾選框。

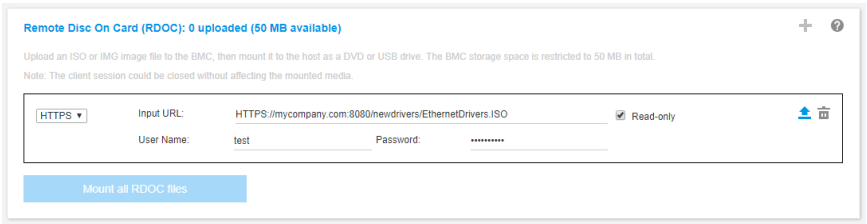
— 輸入 XClarity Controller 存取遠端系統上的檔案所需的認證。

附註：

— 裝載 Microsoft IIS 所產生的安全憑證期間，可能會發生錯誤。如果發生這種情況，請參閱第 67 頁「媒體裝載錯誤問題」。

— XClarity Controller 不支援使用者名稱、密碼或 URL 中包含空格。請確定為 CIFS 伺服器配置登入認證的使用者名稱或密碼中沒有空格，且 URL 不包含空格。**範例**：

若要使用網路埠 8080 將 ISO 檔案 EthernetDrivers.ISO（位於網域名稱為「mycompany.com」之 HTTPS 伺服器的「newdrivers」目錄）裝載為伺服器上的唯讀虛擬硬碟，您可以在下圖所示的欄位中填入資訊。



BMC 會在指定 URL 時提供指引。如果輸入的 URL 不正確，裝載按鈕就會變成灰色，而且 URL 欄位下方會顯示紅色文字，指出預期的 URL 格式。

URL address in the form of https://ipaddress[:port]/path/to/file or HTTPS://domain-name[:port]/path/to/file. The domain-name can be alphanumeric characters, '.', '-' or '_'. It must contain at least two domain items. The port number is optional

— **SFTP — SSH 檔案傳送通訊協定**

— 輸入為遠端系統上的檔案定位的 URL。

— 如果希望檔案向伺服器顯示為唯讀虛擬媒體，請核取勾選框。

— 輸入 XClarity Controller 存取遠端系統上的檔案所需的認證。

附註：

— XClarity Controller 不支援使用者名稱、密碼或 URL 中包含空格。請確定為 CIFS 伺服器配置登入認證的使用者名稱或密碼中沒有空格，且 URL 不包含空格。

— 當 XClarity Controller 連線至 HTTPS 伺服器時，將會出現蹦現視窗，顯示 HTTPS 伺服器所使用的安全憑證的資訊。XClarity Controller 無法驗證安全憑證的真實性。

— **LOCAL – 一般網際網路檔案系統**：

— 瀏覽系統中您想要裝載的 ISO 或 IMG 檔案。

— 如果希望檔案向伺服器顯示為唯讀虛擬媒體，請勾選勾選框。

按一下**裝載所有 RDOC 檔案**，以裝載檔案做為虛擬媒體。若要移除虛擬媒體，請按一下已裝載媒體右側的垃圾桶圖示。

獨立工具

需要使用 XClarity Controller 裝載裝置或映像檔 (.iso / .img) 的使用者，可以使用 OneCLI 套件的 rdmount 獨立程式碼部分。具體而言，rdmount 將會開啟 XClarity Controller 的連線，並將裝置或映像檔裝載至主機。

rdmount 的語法如下：

```
rdmount -s ip_address -d <iso or device path> -l <userid> -p <password> -w port (443)
```

裝載 iso 檔案的範例：

```
$sudo ./rdmount -s 10.243.11.212 -d /home/user/temp/SLE-15-Installer-DVD-x86_64-RC2-DVD1.iso -l userid -p password -w 443
```

使用 Java 用戶端的遠端硬碟

本節說明如何使用 Java 用戶端裝載本端媒體。

您可以使用 Java 用戶端為伺服器指派您電腦上的 CD 或 DVD 光碟機、軟式磁碟機、USB 快閃記憶體隨身碟，或者，您可以指定電腦上的磁碟映像檔供伺服器使用。您可以將硬碟用於各種功能，如重新啟動（啟動）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。您可以存取遠端磁碟。硬碟和磁碟映像檔在伺服器上顯示為 USB 隨身碟。

附註：遠端主控台 Java 支援下列其中一種 Java 環境，而且只有在未執行 HTML5 用戶端時才能開啟。

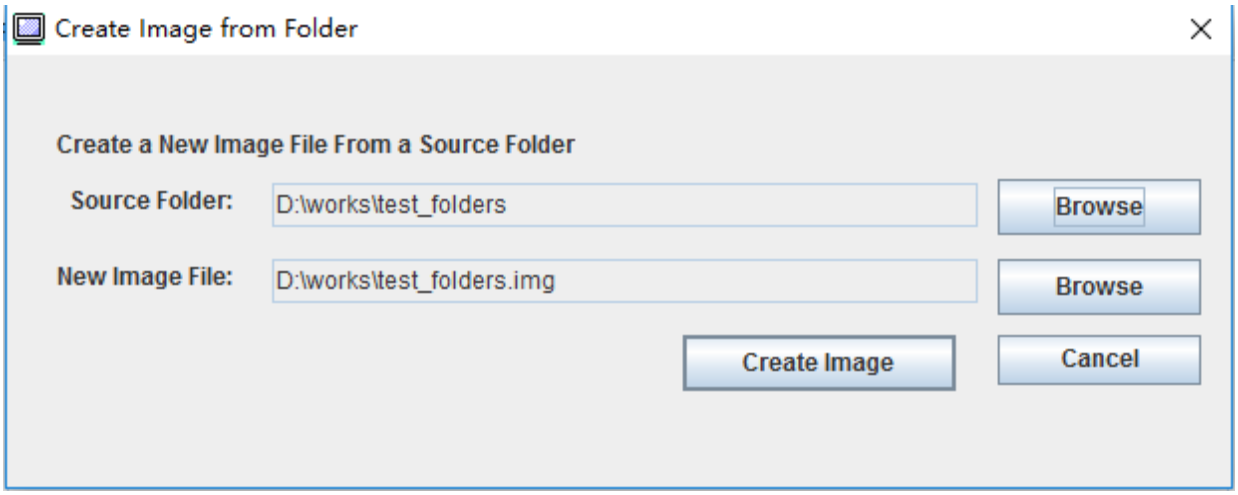
1. Oracle Java Runtime Environment 1.8/Java SE 8 或更新版本
2. OpenJDK 8。支援 AdoptOpenJDK 含 HotSpot JVM 的發佈版本。

如果您使用 AdoptOpenJDK，在 OSX、Windows 和 Linux 下則必須使用 https://openwebstart.com/。

建立映像檔

若要從指定的來源資料夾建立新的映像檔，請完成下列步驟：

1. 在「虛擬媒體 Java 用戶端」視窗的**虛擬媒體**標籤下，按一下**建立映像檔**選項。「從資料夾建立映像檔」視窗隨即顯示。
2. 按一下與**來源資料夾**欄位相關聯的**瀏覽**按鈕以選取特定的來源資料夾。
3. 按一下與**新建映像檔**欄位相關聯的**瀏覽**按鈕以選取要使用的映像檔。
4. 按一下**建立映像檔**按鈕。

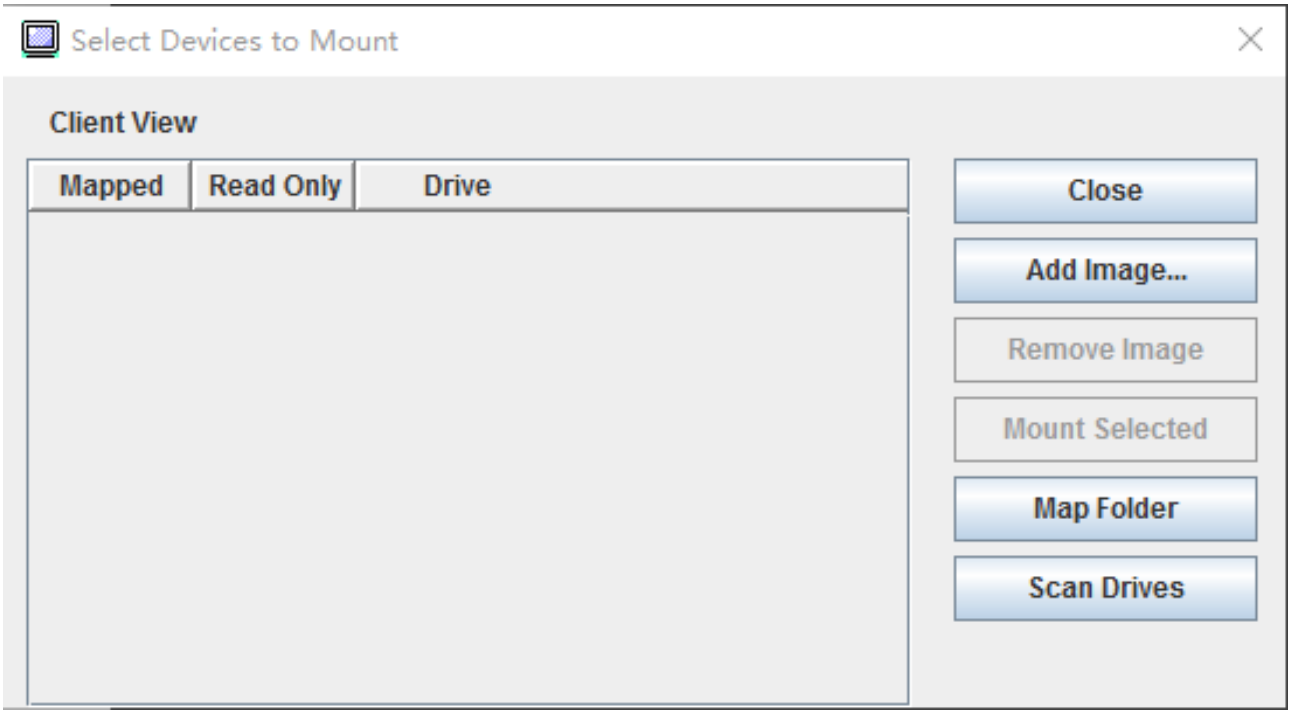


圖例 1. 建立映像檔

選取要裝載的裝置

若要裝載本端映像檔、資料夾和 CD/DVD/USB 磁碟機，請完成下列步驟：

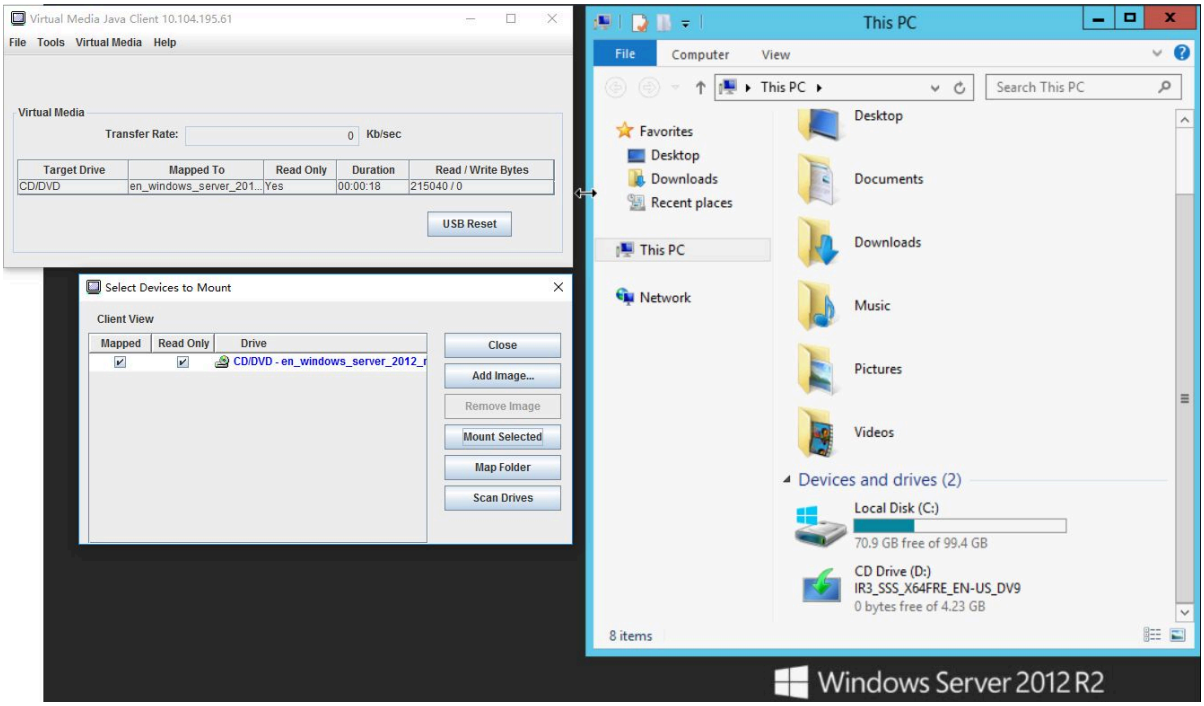
在「虛擬媒體 Java 用戶端」視窗的**虛擬媒體**標籤下，按一下**選取要裝載的裝置**選項。「選取要裝載的裝置」視窗隨即顯示。



圖例 2. 「選取要裝載的裝置」視窗

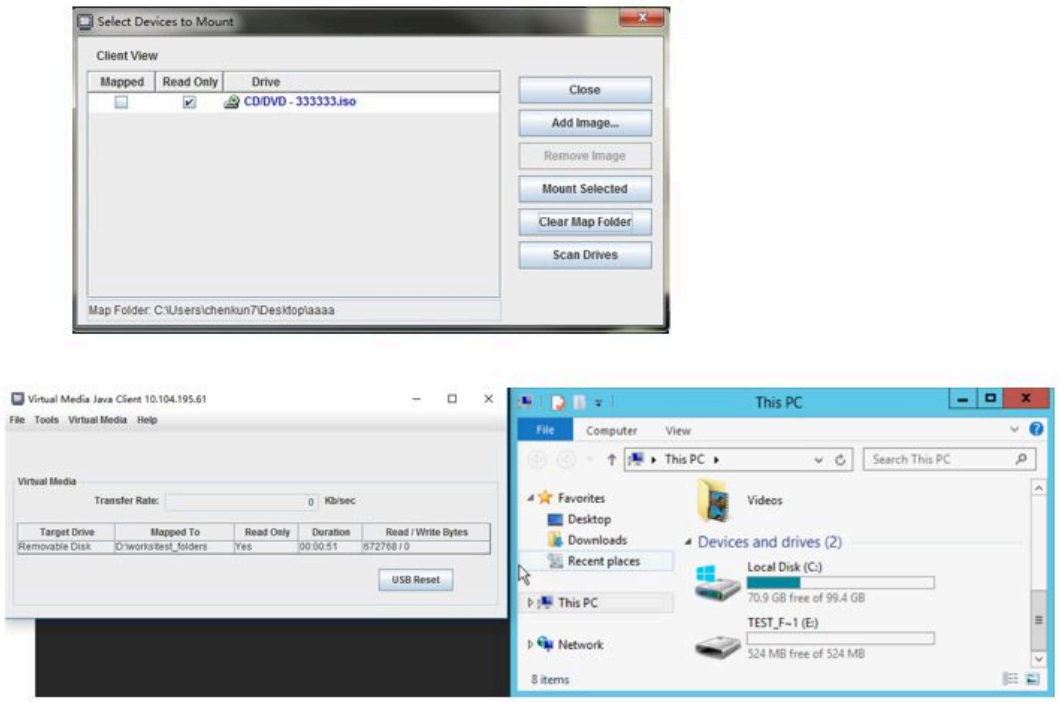
透過執行下列步驟，裝載本端映像檔、資料夾和 CD/DVD/USB 磁碟機：

- **裝載本端映像檔**：
  1. 按一下**新增映像檔**按鈕以選取要裝載的映像檔。
  2. 勾選**已對映**選項。
  3. 勾選**唯讀**選項，視需要啟用該功能。
  4. 按一下**裝載所選項目**按鈕即可順利裝載本端映像檔。



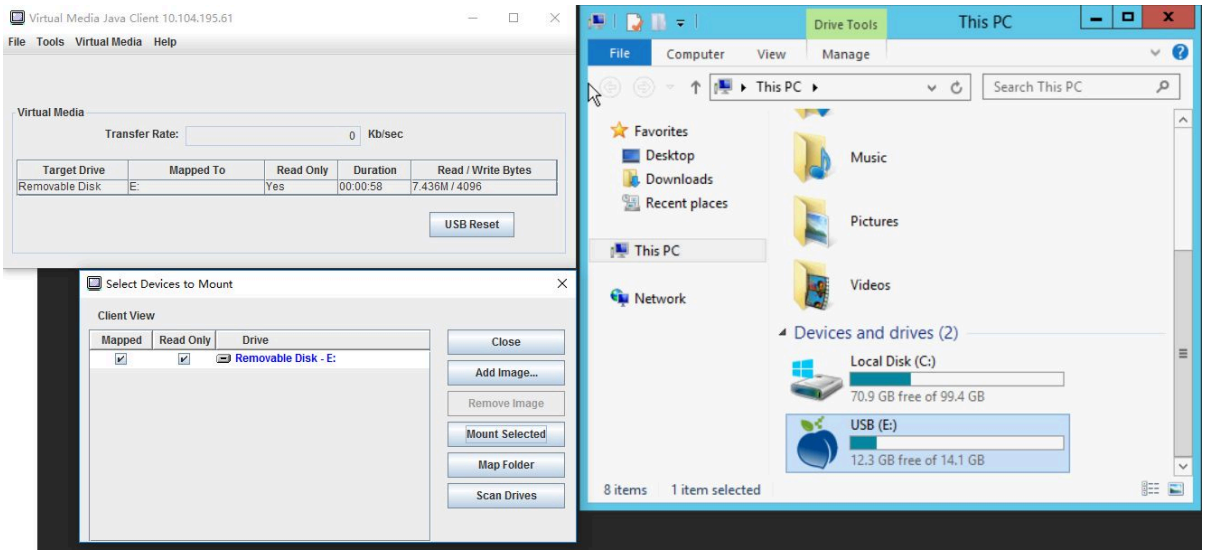
圖例 3. 裝載本端映像檔

- **裝載本端資料夾**：
  1. 按一下**對映資料夾**按鈕以選取要裝載的本端資料夾。
  2. 按一下**裝載所選項目**按鈕即可順利裝載本端資料夾。



圖例 4. 裝載本端資料夾

- **裝載 CD/DVD 光碟機或 USB 隨身碟**：
  1. 按一下**掃描硬碟**按鈕以偵測已插入的 CD/DVD 光碟機或 USB 隨身碟。
  2. 勾選**已對映**選項。
  3. 勾選**唯讀**選項，視需要啟用該功能。
  4. 按一下**裝載所選項目**按鈕即可順利裝載本端映像檔。



圖例 5. 裝載 CD/DVD 光碟機或 USB 隨身碟

「選取要裝載的裝置」視窗包含了目前可供裝載的本端裝置的清單。該視窗內有以下欄位和按鈕：

- **已對映**欄位包含的勾選框可讓您選取要裝載或對映的裝置。
- **唯讀**欄位包含的勾選框可讓您選取將在主伺服器上**唯讀**的對映裝置或裝載的裝置。
- **硬碟**欄位包含各裝置在本端機器上的路徑。
- 按一下**關閉**按鈕可關閉「選取要裝載的裝置」視窗。
- 按一下**新增映像檔**按鈕可瀏覽本端檔案系統，找出要新增至裝置清單的磁片映像檔和 ISO 映像檔。
- 按一下**移除映像檔**按鈕可移除已新增至裝置清單的映像檔。
- 按一下**裝載所選項目**按鈕可裝載或對映**已對映**欄位所勾選要裝載或對映的所有裝置。

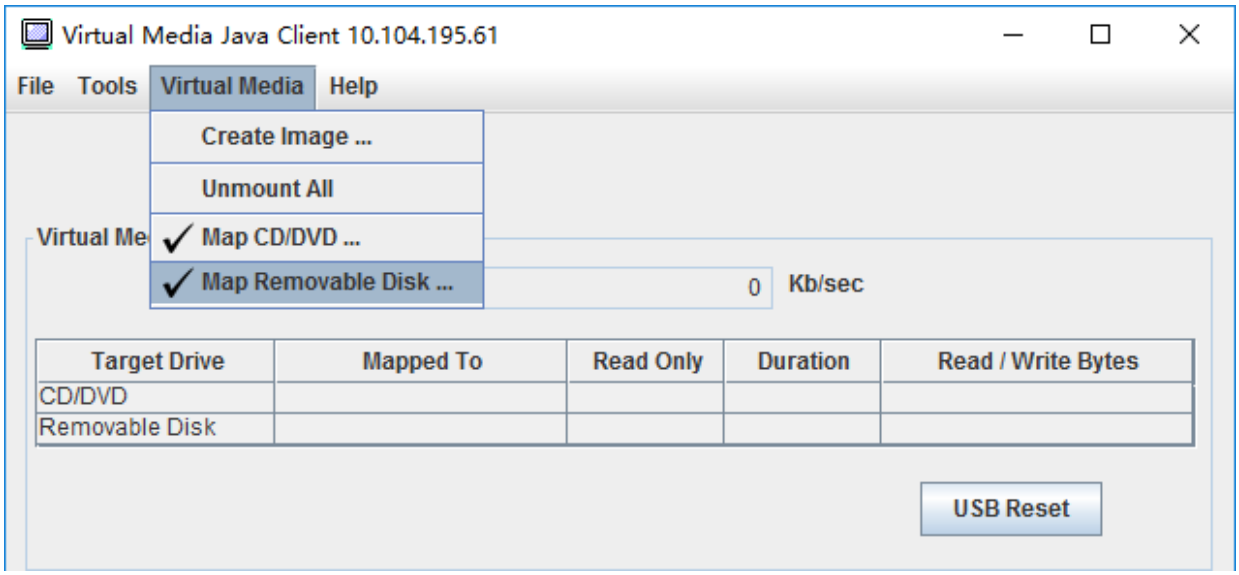
  附註：資料夾將以唯讀形式裝載。
- 按一下**掃描硬碟**按鈕可重新整理本端裝置清單。

選取要卸載的裝置

若要卸載主伺服器裝置，請完成下列步驟：

1. 在「虛擬媒體 Java 用戶端」視窗的**虛擬媒體**標籤下，按一下**全部卸載**選項。
2. 選取**全部卸載**選項後，您將看到「全部卸載」確認視窗。如果您接受，即會卸載伺服器上的**所有**主伺服器裝置。

   附註：您無法卸載個別的硬碟。



圖例 6. 全部卸載

媒體裝載錯誤問題

使用本主題中的資訊，對媒體裝載錯誤問題進行疑難排解。

使用 Microsoft IIS 所產生的安全憑證時，您可能會在裝載程序期間遇到錯誤。如果發生這種情況，請用 openssl 所產生的新憑證來更換此安全憑證。具體而言，新產生的 pfx 檔案會載入 Microsoft IIS 伺服器中。

以下範例將示範如何透過 Linux 作業系統中的 openssl 產生新的安全憑證。

```
$ openssl
```

```
OpenSSL>

$ openssl genrsa 1024 > server.key
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)

$ openssl req -new -key server.key > server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:BJ
Locality Name (eg, city) []:HD
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Lenovo
Organizational Unit Name (eg, section) []:Lenovo
Common Name (e.g. server FQDN or YOUR name) []:10.245.18.66
Email Address []:test@test.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:LNV

$ ls
server.csr  server.key

$ openssl req -x509 -days 3650 -key server.key -in server.csr > server.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:BJ
Locality Name (eg, city) []:BJ
Organization Name (eg, company) [Internet Widgits Pty Ltd]:LNV
Organizational Unit Name (eg, section) []:LNV
Common Name (e.g. server FQDN or YOUR name) []:10.245.18.66
Email Address []:test@test.com

$ ls
server.crt  server.csr  server.key

$ openssl pkcs12 -export -out server.pfx -inkey server.key -in server.crt
Enter Export Password:
Verifying - Enter Export Password:

$ ls
server.crt  server.csr  server.key  server.pfx
```

結束遠端主控台階段作業

本主題說明如何結束遠端主控台階段作業。

如果要結束遠端主控台階段作業，請關閉遠端主控台和虛擬媒體階段作業視窗。

下載服務資料

使用本主題中的資訊來收集伺服器的相關服務資訊。此程序通常只有在服務人員為了協助解決伺服器問題而提出要求時，才會執行。

在 XClarity Controller 首頁中，按一下**快速動作**區段中的**服務**選項，然後選取**下載服務資料**。按一下**確定**以下載服務資料。

收集服務及支援資料的程序需要數分鐘才能產生服務資料。檔案將會儲存至您的預設下載資料夾。服務資料檔案的命名慣例遵循此慣例：<machine type and model>_<serial number>_xcc_<date>-<time>.tgz

例如：7X2106Z01A_2345678_xcc_170511-175656.tgz。

除了 tgz 格式，也可以使用 tzz 格式下載服務資料。Tzz 使用另一種壓縮演算法，而且可以使用「lzop」等公用程式解壓縮。

伺服器內容

使用本主題中的資訊來變更或檢視相關的伺服器內容。

設定位置和聯絡人

使用本主題中的資訊來設定各種參數，以幫助識別適用於作業和支援人員的系統。

選取**伺服器配置**下的**伺服器內容**，以配置**位置和聯絡人**資訊。

聯絡人
可讓您指定若此系統遇到問題時，應聯絡的人員姓名和電話號碼。

附註：此欄位與 SNMPv3 配置中的「聯絡人」欄位相同，且為啟用 SNMPv3 的必要欄位。

機架名稱
可讓您透過指定其所在機架，更輕鬆地找到伺服器。

附註：此欄位為選用，而且在 Flex 節點中不可配置。

機房號碼
可讓您透過指定其所在機房，更輕鬆地找到伺服器。

建築物
可讓您透過指定其所在建築物，更輕鬆地找到伺服器。

最低 U
可讓您透過指定在機架中的位置，更輕鬆地找到伺服器。

附註：此欄位為選用，而且在 Flex 節點中不可配置。

地址
可讓您指定伺服器所在的完整郵寄地址。

附註：輸入相關資訊之後，這些資訊將在 SNMPv3 區段和 XClarity Controller 首頁的**位置**欄位中以單獨一行顯示。

設定伺服器逾時

使用本主題中的資訊來設定伺服器的逾時值。

這些逾時用於將作業還原至已當機的伺服器。

選取**伺服器配置**下的**伺服器內容**，以配置伺服器逾時。提供下列伺服器逾時選項：

OS 監視器

OS 監視器是用於監視作業系統，以確定未當機。此功能必須啟用 Ethernet over USB 介面。請參閱第 29 頁 「配置 Ethernet over USB」，以取得相關詳細資料。XClarity Controller 會依 **OS 監視器時間**選項中配置的間隔來聯絡作業系統。如果作業系統未在下次檢查的時間之前回應，XClarity Controller 則假設作業系統已當機。XClarity Controller 將擷取伺服器顯示器的內容，然後重新啟動伺服器，以嘗試還原作業。XClarity Controller 只會重新啟動伺服器一次。如果作業系統在重新啟動之後仍然當機，則不會再繼續重新啟動伺服器，伺服器將停留在當機狀態，以便能夠調查並更正問題。如果要重設 OS 監視器的授權狀態，請關閉伺服器電源後再開啟。如果要啟用 OS 監視器，請從「OS 監視器時間」下拉清單中選取間隔，然後按一下**套用**。如果要停用 OS 監視器，請選取「OS 監視器時間」下拉功能表上的**無**。

載入器監視器

載入器監視器會監視完成 POST 和作業系統開始執行之間的間隔。此功能必須啟用 Ethernet over USB 介面。請參閱第 29 頁 「配置 Ethernet over USB」，以取得相關詳細資料。POST 完成時，XClarity Controller 會啟動計時器並開始聯絡作業系統。如果作業系統未在「載入器監視器」選項中配置的時間回應，XClarity Controller 則假設作業系統開機已當機。然後 XClarity Controller 將重新啟動伺服器，以嘗試還原作業。XClarity Controller 只會重新啟動伺服器一次。如果作業系統開機在重新啟動之後仍然當機，則不會再繼續重新啟動伺服器，伺服器將停留在當機狀態，以便能夠調查並更正問題。當關閉伺服器後再開啟時，或伺服器成功開機至作業系統時，會重設載入器監視器的授權狀態。如果要啟用載入器監視器，請從「載入器監視器」下拉清單中選取間隔，然後按一下**套用**。如果要停用載入器監視器，請選取「載入器監視器」下拉清單上的**無**。

啟用關閉電源延遲

使用「關閉電源延遲」欄位，可指定 XClarity Controller 子系統在強制關閉電源之前等待作業系統關閉的分鐘數。如果要設定關閉電源延遲逾時值，請從下拉清單中選取時間間隔，然後按一下**套用**。如果要停用 XClarity Controller 的強制關閉電源，請從下拉選項中選取**無**。

侵害訊息

如果要建立當使用者登入 XClarity Controller 時所顯示的訊息，請使用本主題中的資訊。

選取**伺服器配置**下的**伺服器內容**。使用**侵害訊息**選項來配置您希望向使用者顯示的訊息。完成時，按一下**套用**。

使用者登入時，在 XClarity Controller 登入頁面的「訊息」區域中將會顯示訊息文字。

設定 XClarity Controller 日期和時間

使用本主題中的資訊，以瞭解 XClarity Controller 日期和時間設定。其中包含配置 XClarity Controller 日期和時間的指示。XClarity Controller 日期和時間會用來為事件日誌中記載的所有事件和傳送的警示加上時間戳記。

在 XClarity Controller 首頁，按一下右上角的時鐘圖示以檢視或變更 XClarity Controller 日期和時間。XClarity Controller 沒有自己的即時時鐘。您可以配置 XClarity Controller，將其時間和日期與「網路時間通訊協定」伺服器或伺服器的即時時鐘硬體同步。

與 NTP 同步

請完成下列步驟，將 XClarity Controller 時鐘與 NTP 伺服器同步：

- 選取**將時間與 NTP 同步**，並指定 NTP 伺服器位址。

- 按一下「+」圖示可以指定其他 NTP 伺服器。
- 指定您希望 XClarity Controller 與 NTP 伺服器同步的頻率。
- 從 NTP 伺服器取得的時間格式為國際標準時間 (UTC)。
  - 如果您希望 XClarity Controller 針對您所在的地區調整時間和日期，請從下拉功能表中選取您的語言環境的時區偏移。
  - 如果您所在位置採用日光節約時間，請核取**自動調整日光節約時間 (DST)** 勾選框。
- 配置變更完成時，按一下**套用**。

與主機同步

保存在伺服器的即時時鐘硬體中的時間格式可能是國際標準時間 (UTC)，或可能已使用當地時間格式調整及儲存。有些作業系統會使用 UTC 格式來儲存即時時鐘，有些則將時間儲存為當地時間。伺服器即時時鐘不會指出使用何種時間格式。因此，當 XClarity Controller 配置為與主機的即時時鐘同步時，使用者可以選擇 XClarity Controller 如何使用從即時時鐘取得的時間和日期。

- 當地（範例：Windows）：在此模式中，XClarity Controller 會將從即時時鐘取得的時間和日期視為當地時間，而且已經套用適用的時區和 DST 偏移。
- UTC（範例：Linux）：在此模式中，XClarity Controller 會將從即時時鐘取得的時間和日期視為國際標準時間，而且未套用任何時區或 DST 偏移。在此模式中，您可以從下拉功能表中選取您的語言環境的時區偏移，以針對您所在的地區調整時間和日期。如果您所在位置採用日光節約時間，也可以核取**自動調整日光節約時間 (DST)** 勾選框.
- 配置變更完成時，按一下**套用**。

附註：

- 在日光節約期間，將不會執行 XClarity Controller 排定要在時鐘調快期間內執行的任何動作。例如，如果美國日光節約是從 3 月 12 日早上 2:00 開始，而電源動作是排定在 3 月 12 日的早上 2:10，則不會發生此動作。時間到早上 2:00 時，XClarity Controller 會將時間視為是早上 3:00。
- 在 Flex System 中，無法修改 XClarity Controller 日期和時間設定。

第 6 章　配置儲存體

使用本章的資訊，可瞭解儲存體可用的配置選項。

配置儲存體時，可用的選項如下：

- 詳細資料
- 設定 RAID

RAID 詳細資料

若要使用 RAID 詳細資料功能，請使用本主題中的資訊。

此功能顯示儲存裝置的實體結構和儲存體配置，以及諸如其所在位置、製造商、產品名稱、狀態、容量、介面、媒體、尺寸外型等詳細資料和其他資訊。

設定 RAID

若要執行「設定 RAID」功能，請使用本主題中的資訊。

使用本主題中的資訊來檢視及配置 RAID 配接卡的儲存區、相關聯的虛擬磁碟和硬碟。如果系統電源已關閉，請開啟電源以便檢視 RAID 資訊。

檢視及配置虛擬硬碟

使用本主題中的資訊來檢視及配置虛擬硬碟。

當您選取**伺服器配置**下的**設定 RAID** 時，將會選擇**陣列配置**標籤，而且依預設會顯示現有的虛擬磁碟。邏輯硬碟是依磁碟陣列和控制器來排序。畫面上會顯示虛擬磁碟的詳細資訊，例如虛擬磁碟磁區帶大小和可開機資訊。

如果要配置 RAID 設定，請按一下**啟用編輯模式**。

在編輯模式中，您可以按一下控制器動作功能表，檢視目前的 RAID 虛擬磁碟及建立新的 RAID 虛擬磁碟。

您可以從「控制器動作」功能表來執行下列動作：

清除 RAID 配置
清除選定控制器上所有的配置和資料。

管理外部配置
匯入偵測到的外部硬碟。外部硬碟是從不同的 RAID 配置移至目前 RAID 控制器的硬碟

附註：如果未偵測到外部硬碟，將會通知您。

特定控制器的目前 RAID 虛擬磁碟資訊會分別顯示為「虛擬磁碟卡」。各卡都會顯示如虛擬磁碟名稱、狀態、容量及動作等資訊。鉛筆圖示可讓您編輯資訊，垃圾桶圖示可讓您刪除「虛擬磁碟卡」。

附註：容量和 RAID 層級無法變更。

如果您按一下虛擬磁碟名稱，將會出現虛擬磁碟內容視窗。

如果要建立新的 RAID 虛擬磁碟，請遵循下列步驟：

附註： 如果沒有剩餘的儲存容量，您就無法建立新的虛擬磁碟。

1. **選取有可用儲存容量的硬碟或磁碟陣列**
   a. 在新的磁碟陣列中建立虛擬磁碟時，您必須指定 RAID 層級。如果沒有足夠的硬碟可供選取，而您按一下**下一步**，RAID 層級欄位下方將會出現錯誤訊息。

      對於部分 RAID 層級，跨距是必要的。跨距中也需要有最低硬碟數量。

      1) 針對這些類型的情況，Web 介面依預設將會顯示**跨距 1**。
      2) 選取硬碟，然後按一下**新增成員**，將硬碟新增至**跨距 1**。當**跨距 1** 沒有足夠的硬碟時，則停用**新增跨距**鏈結。
      3) 按一下**新增跨距**以新增**跨距 2**。選取硬碟，然後按一下**新增成員**以新增至**跨距 2**。
      4) 按一下**新增成員**，將硬碟新增至最後一個跨距。如果要再次將硬碟新增至**跨距 1**，您必須按一下「跨距 1」，並選取要新增至**跨距 1** 的硬碟。
      5) 如果跨距數目到達上限，則停用**新增跨距**。

   b. 如果要在現有的磁碟陣列中建立虛擬磁碟，您必須選取具有可用容量的磁碟陣列。
2. **建立虛擬磁碟**
   a. 依預設，建立使用所有儲存容量的虛擬磁碟。所有儲存體都已使用時，就會停用**新增**圖示。您可以按一下鉛筆圖示，以變更容量或其他內容。
   b. 當您將第一個虛擬磁碟編輯為僅使用部分的儲存容量時，將會啟用**新增**圖示。按一下圖示以顯示**新增虛擬磁碟**視窗。
   c. 如果有一個以上的虛擬磁碟，將會啟用**移除**圖示。如果只有一個虛擬磁碟，則不會顯示此圖示。當您按一下**移除**圖示時，將會立即刪除選取的列。由於尚未建立虛擬磁碟，因此不會有確認視窗。
   d. 按一下**開始建立虛擬磁碟**以啟動程序。

附註：不支援控制器時，會出現一則訊息。

檢視及配置儲存體庫存

使用本主題中的資訊來檢視及配置儲存體庫存。

在**儲存體庫存**標籤下方，您可以檢視及配置磁碟陣列、相關聯的虛擬硬碟以及 RAID 控制器的硬碟。

- **支援 RAID 配置的儲存裝置**：
  1. 如果控制器包含配置的磁碟陣列，將會根據磁碟陣列顯示已安裝的硬碟。以下說明出現在視窗中的項目。

     — **表格標題**：顯示磁碟陣列 ID、RAID 層級及硬碟的總數。

     — **表格內容**：列出基本內容 - 硬碟名稱、RAID 狀態、類型、序號、零件編號、FRU 號碼和動作。您可以移至**庫存**頁面，檢視 XClarity Controller 可以偵測到的所有內容。

     — **動作**：以下顯示可以執行的動作項目。當硬碟處於不同狀態時，部分動作將無法使用。

     — **指派緊急備用**：將硬碟指定為廣域緊急備用或專用緊急備用。

     — **移除緊急備用**：從緊急備用中移除硬碟。

     — **將硬碟設為離線**：將硬碟設定為離線。

     — **將硬碟設為線上**：將硬碟設定為在線上。

     — **將硬碟設為可重複使用**： 將硬碟設定為可重複使用。

     — **將硬碟設為遺漏**：將硬碟設定為遺漏。

     — **將硬碟設定為支援 JBOD**：將硬碟新增至 JBOD 磁碟排列。

     — **將硬碟設定為未配置的良好**：可讓硬碟配置到陣列中，或用來做為緊急備用。

     — **將硬碟設定為未配置的不良**：標示硬碟有損壞、無法用於陣列中或做為緊急備用。

     — **讓硬碟做好卸下準備**：設定硬碟以進行卸除。

2. 如果控制器包含尚未配置的硬碟，這些硬碟將會顯示在**非 RAID 硬碟**表格中。按一下**將 JBOD 轉換為已做好配置準備**選項，將會出現視窗，顯示所有支援此動作項目的硬碟。您可以選取一個或多個要轉換的硬碟。

不支援 RAID 配置的儲存裝置：XClarity Controller 可能無法偵測部分硬碟的內容。

第 7 章　更新伺服器韌體

如果要更新伺服器韌體，請使用本主題中的資訊。

概觀

與更新伺服器韌體有關的一般資訊。

導覽面板上的**韌體更新**選項有 4 個功能：

- **系統韌體：**系統韌體狀態和版本的概觀。而且可執行系統韌體更新。
- **自動將主要 XCC 升級為備份：**啟用後，在主要儲存庫通過映像檔穩定性衡量標準 (ISM) 量測後，擱置的備份儲存庫韌體將與主要儲存庫同步。
- **配接卡韌體：**已安裝之配接卡的狀態和版本的概觀。而且可執行配接卡韌體更新。

BMC、UEFI、LXPM、LXPM 驅動程式和配接卡的韌體目前狀態和版本都會顯示，包括 BMC 主要和備份版本。韌體狀態有四個種類：

- **作用中：**韌體處於作用中狀態。
- **非作用中：**韌體處於非作用中狀態。
- **擱置中：**韌體正在等待變成作用中狀態。
- **不適用：**未為此元件安裝韌體。

注意：

- 更新 UEFI 之前，XCC 和 IMM 必須更新為最新版本。以不同的順序進行更新可能會導致奇怪或不正確的行為。
- 安裝錯誤的韌體更新可能會導致伺服器故障。在安裝韌體或裝置驅動程式更新之前，請先閱讀隨所下載更新一同提供的任何 Readme 或變更歷程檔案。這些檔案包含更新的重要資訊和安裝更新的程序，包括從早期韌體或裝置驅動程式版本更新至最新版本的任何特殊程序。由於 Web 瀏覽器可能包含 XCC 快取資料，建議您在 XCC 韌體升級後重新載入網頁。
- 某些韌體更新需要重新啟動系統，這會執行韌體啟動或內部更新。此程序在系統開機中稱為「系統維護模式」，在該模式下暫時不允許使用者電源動作。在韌體更新期間，也會啟用該模式。當系統進入維護模式時，使用者不應中斷 AC 電源的連接。

系統、配接卡和 PSU 韌體更新

更新系統韌體、配接卡韌體和 PSU 韌體的步驟。

若要為**系統韌體**、**配接卡韌體**和 **PSU 韌體**手動套用更新，請完成下列步驟：

1. 按一下每個功能中的**更新韌體**。「更新伺服器韌體」視窗隨即開啟。
2. 按一下**瀏覽**，以選取您要使用的韌體更新檔案。
3. 導覽至您要選取的檔案，然後按一下**開啟**。您會回到「更新伺服器韌體」視窗，其中會顯示所選取的檔案。
4. 按一下**下一步 >** 以開始上傳，並驗證所選檔案的處理程序。在上傳及驗證檔案時，會顯示進度表。您可以檢視此狀態視窗，以驗證您選取要更新的檔案是正確的檔案。若是**系統韌體**，狀態視窗中會有所要更新之韌體檔案類型的相關資訊，例如 BMC、UEFI 或 LXPM。上傳並成功驗證韌體檔案之後，請按一下**下一步**選取您要更新的裝置。

5. 按一下**更新**，以開始韌體更新。進度表會顯示更新進度。順利完成韌體更新之後，按一下**完成**。如果更新需要 XClarity Controller 重新啟動，才會生效，將會顯示警告訊息。如需有關如何重新啟動 XClarity Controller 的詳細資訊，請參閱第 53 頁 「電源動作」。

第 8 章　授權管理

Lenovo XClarity Controller 授權管理可讓您安裝及管理選配伺服器和系統管理功能。

有多種版本的 XClarity Controller 韌體功能和特性可用於您的伺服器。您的伺服器安裝的韌體功能版本視硬體類型而異。

您可以購買和安裝啟動金鑰，以升級 XClarity Controller 功能。

如果要訂購啟動金鑰，請聯絡您的銷售代表或事業夥伴。

使用 XClarity Controller Web 介面或 XClarity Controller CLI 來手動安裝啟動金鑰，此金鑰可讓您使用已購買的選配功能。在啟動金鑰之前：

- 啟動金鑰必須在您用於登入 XClarity Controller 的系統上。
- 您必須已購買授權金鑰，及透過郵件或電子郵件接收其授權碼。

如需使用 XClarity Controller Web 介面管理啟動金鑰的相關資訊，請參閱第 79 頁 「安裝啟動金鑰」、第 80 頁 「卸下啟動金鑰」或第 80 頁 「匯出啟動金鑰」。如需使用 XClarity Controller CLI 管理啟動金鑰的相關資訊，請參閱第 113 頁 「keycfg 指令」。

如果要註冊 ID 以管理 XClarity Controller 授權，請按一下下列連結：https://fod.lenovo.com/lkms/angular/app/pages/index.htm#/welcome

下列 **Lenovo Press** 網站提供 Lenovo 伺服器授權管理的其他相關資訊：

https://lenovopress.com/redp4895-using-lenovo-features-on-demand

注意：您無法從標準 XClarity Controller 直接升級為企業版功能。您必須先升級為進階版，然後才能啟動企業版功能。

安裝啟動金鑰

使用本主題中的資訊，可將選用功能新增至您的伺服器。

若要安裝啟動金鑰，請完成下列步驟：

步驟 1. 按一下 **BMC 配置**下的**授權**。

步驟 2. 按一下**升級授權**。

步驟 3. 在**新增授權**視窗中，按一下**瀏覽**，然後在「檔案上傳」視窗中選取要新增的啟動金鑰檔，並按一下**開啟**以新增檔案，或按一下**取消**以停止安裝。要完成新增金鑰，請在「新增啟動金鑰」視窗中按一下**確定**，或按一下**取消**以停止安裝。

「成功」視窗表示已安裝啟動金鑰。

附註：

- 如果啟動金鑰無效，則會出現錯誤視窗。

步驟 4. 按一下**確定**以關閉「成功」視窗。

卸下啟動金鑰

使用本主題中的資訊，可刪除您伺服器中的選用功能。

若要移除啟動金鑰，請完成下列步驟：

步驟 1. 按一下 **BMC 配置**下的**授權**。

步驟 2. 選取要移除的啟動金鑰，然後按一下**刪除**。

步驟 3. 在「確認刪除啟動金鑰」視窗中，按一下**確定**以確認刪除啟動金鑰，或按一下**取消**以保留金鑰檔。
選取的啟動金鑰會從伺服器中移除，不再出現在「授權管理」頁面中。

匯出啟動金鑰

使用本主題中的資訊，以從伺服器匯出選用特性。

若要匯出啟動金鑰，請完成下列步驟：

步驟 1. 按一下 **BMC 配置**下的**授權**。

步驟 2. 從「授權管理」頁面中選取要匯出的啟動金鑰，然後按一下**匯出**。

步驟 3. 在**匯出選取的授權**視窗中，按一下**匯出**以確認匯出啟動金鑰，或按一下**取消**以取消金鑰匯出要求。

步驟 4. 選取要用來儲存檔案的目錄。
從伺服器匯出所選取的啟動金鑰。

第 9 章 Lenovo XClarity Controller Redfish REST API

Lenovo XClarity Controller 提供了一組與 Redfish 相容且簡單易用的 REST API，可用於從 Lenovo XClarity Controller 架構外部執行的應用程式存取 Lenovo XClarity Controller 資料和服務。

不論是與 Lenovo XClarity Controller 伺服器在相同系統上執行的軟體，還是在相同網路之遠端系統上執行的軟體，您都可以輕鬆地將 Lenovo XClarity Controller 功能整合到其他軟體中。這些 API 是以業界標準 Redfish REST API 為基礎，透過 HTTPS 通訊協定存取。

《XClarity Controller Redfish REST API 使用手冊》位於下列網址：
https://pubs.lenovo.com/xcc-restapi/xcc_restapi_book.pdf。

Lenovo 提供了開放原始碼 Redfish Script 範例，在開發軟體與 Lenovo Redfish REST API 進行通訊時可用作參考。這些 Script 範例位於下列網址：

- Python： https://github.com/lenovo/python-redfish-lenovo
- PowerShell： https://github.com/lenovo/powershell-redfish-lenovo

與 Redfish API 相關的 DMTF 規格位於下列網址：https://redfish.dmtf.org/。該網站提供了 Redfish REST API 的一般規格及其他參考資料。

第 10 章　指令行介面

使用本主題的資訊，可輸入管理及監視 XClarity Controller 的指令，不需要使用 XClarity Controller Web 介面。

使用 XClarity Controller 指令行介面 (CLI) 可存取 XClarity Controller，不需要使用 Web 介面。它有 Web 介面提供的管理功能子集。

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

存取指令行介面

使用本主題中的資訊來存取 CLI。

如果要存取 CLI，請將 SSH 階段作業啟動至 XClarity Controller IP 位址（如需相關資訊，請參閱第 83 頁「配置 serial-to-SSH 重新導向」）。

登入指令行階段作業

使用本主題中的資訊來登入指令行階段作業。

若要登入指令行，請完成下列步驟：

步驟 1. 建立與 XClarity Controller 的連線。

步驟 2. 在「使用者名稱」提示處輸入使用者 ID。

步驟 3. 在密碼提示處，輸入您登入 XClarity Controller 所使用的密碼。

您已登入指令行。指令行提示為 `system>`。指令行階段作業會繼續進行，直到您在指令行中輸入 `exit` 為止。您已登出，並結束階段作業。

配置 serial-to-SSH 重新導向

本主題提供使用 XClarity Controller 作為序列終端伺服器的相關資訊。

serial-to-SSH 重新導向可讓系統管理者使用 XClarity Controller 做為序列終端伺服器。在啟用序列重新導向時，您可以從 SSH 連線存取伺服器序列埠。

附註：CLI **console 1** 指令用於透過 COM 埠啟動序列重新導向階段作業。

階段作業範例

```
$ ssh USERID@10.240.1.12
Password:

system>
```

來自 SSH 階段作業的所有資料流量都會遞送至 COM2。

```
ESC (
```

鍵入結束按鍵順序，以返回 CLI。在此範例中，按 Esc 鍵，然後鍵入左括弧。CLI 提示會顯示，以指示返回 IMM CLI。

```
system>
```

指令語法

檢閱本主題中的準則，可瞭解如何在 CLI 中輸入指令。

在使用指令之前，請先閱讀下列準則：

- 每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選用的。方括弧不是您輸入指令的一部分。

功能和限制

本主題包含 CLI 功能和限制的相關資訊。

CLI 具有下列功能和限制：

- 允許透過 SSH 進行多個並行 CLI 階段作業。
- 每行容許一個指令（1024 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，然後您可以用來做為執行指令的捷徑，如以下範例：

```
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 XClarity ControllerA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system >
```

- 在 CLI 中，輸出緩衝區限制為 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）。
- 簡式文字訊息用於表示指令執行狀態，如以下範例：

```
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` 語法不正確。正確語法為 `ifconfig eth0 -i 192.168.70.133`。
- 所有指令都有提供語法協助的 `-h`, `-help` 和 `?` 選項。下列所有範例都提供相同結果：
  ```
  system> power -h
  system> power -help
  system> power ?
  ```
- 接下來的章節所描述的部分指令可能不適用於您的系統配置。如果要查看您的配置支援的指令清單，請使用 `help` 或 `?` 選項，如下列範例所示：
  ```
  system> help
  system> ?
  ```
- 在 Flex System 中，部分設定由 CMM 管理，且無法在 XClarity Controller 中修改。

按字母順序排序的指令清單

本主題包含按字母順序排序的 CLI 指令清單。每項指令都提供主題鏈結。每個指令主題包含指令及其功能、語法和使用的相關資訊。

所有 XClarity Controller CLI 指令的完整清單（按字母順序排序）如下：

- 第 136 頁 「trespass 指令」
- 第 137 頁 「uefipw 指令」
- 第 138 頁 「usbeth 指令」
- 第 138 頁 「usbfp 指令」
- 第 138 頁 「users 指令」
- 第 95 頁 「volts 指令」
- 第 95 頁 「vpd 指令」

公用程式指令

本主題提供按字母順序排序的公用程式 CLI 指令清單。

目前有 3 個公用程式指令：

exit 指令

使用此指令登出 CLI 階段作業。

使用 **exit** 指令可登出並結束 CLI 階段作業。

help 指令

此指令可顯示所有指令清單。

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輸入 ?。

history 指令

此指令可提供先前已發出的指令清單。

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 !），才能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
HISTORY-g 0.0.0.0
-s 255.255.255.0
-n XCCA00096B9E003A
-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

本主題提供按字母順序排序的監視 CLI 指令清單。

目前有 11 個監視指令：

clearlog 指令

此指令是用於清除 IMM 事件日誌。

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。

附註：此指令僅供支援人員使用。

下表顯示各選項的引數。

表格 7. clearlog 指令

下表是由一個橫列與兩個直欄組成的表格，其中包含選項及選項說明。

選項	說明
-t <all | platform | audit>	事件類型，選擇要清除的事件類型。如果未指定，則選取所有事件類型。

事件類型說明

- all：所有事件類型，包括平台事件和審核事件。
- platform：平台事件類型。
- audit：審核事件類型。

範例：

```
system> clearlog
All event log cleared successfully
system> clearlog -t all
All event log cleared successfully
system> clearlog -t platform
Platform event log cleared successfully
system> clearlog -t audit
Audit event log cleared successfully
```

fans 指令

此指令可用來顯示伺服器風扇的速度。

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>
```

ffdc 指令

此指令可用來產生新的服務資料檔。

使用第一次失敗資料擷取 (**ffdc**) 指令可產生服務資料，並傳送至「支援中心」。

下列清單包含要與 **ffdc** 指令搭配使用的指令：

- **generate**，可建立新的服務資料檔
- **status**，可檢查服務資料檔的狀態
- **copy**，可複製現有的服務資料
- **delete**，可刪除現有的服務資料

下表顯示各選項的引數。

表格 8. ffdc 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-t	類型號碼	1（處理器傾出）和 4（服務資料）。處理器傾出包含所有可用的日誌及檔案。服務資料只包含日誌及檔案的子集。預設值是 1。
-f [1]	遠端檔名或 sftp 目標目錄。	針對 sftp，請使用完整路徑，或是在目錄名稱尾端加上 /（~/ 或 /tmp/）。預設值是系統產生的名稱。
-ip [1]	tftp/sftp 伺服器的位址	
-pn [1]	tftp/sftp 伺服器的埠號	預設值為 69/22。
-u [1]	sftp 伺服器的使用者名稱	
-pw [1]	sftp 伺服器的密碼	
1. **generate** 和 **copy** 指令的其他引數		

語法：

```
ffdc [options]
option:
 -t 1 or 4
 -f
 -ip ip_address
 -pn port_number
 -u username
  -pw password
```

範例：

```
system> ffdc generate
Generating ffdc...
system> ffdc status
Type 1 ffdc: in progress
system> ffdc copy -t 1 -ip 192.168.70.230 -u User2 -pw Passw0rd -f /tmp/
Waiting for ffdc.....
Copying ffdc...
ok
system> ffdc status
Type 1 ffdc: completed
8737AC1_DSY0123_xcc_120317-153327.tgz


system> ffdc generate
Generating ffdc...
system> ffdc status
Type 1 ffdc: in progress
```

```
system> ffdc status
Type 1 ffdc: in progress
system> ffdc copy -ip 192.168.70.230
Copying ffdc...
ok
system> ffdc status
Type 1 ffdc: completed
8737AC1_DSY0123_xcc_120926-105320.tgz
system>
```

hreport 指令

使用此指令可顯示內嵌性能報告。

下表顯示 hreport 指令。

表格 9. hreport 指令

下表是由多個橫列與兩個直欄組成的表格，其中包含不同的 hreport 指令說明。

選項	說明
generate	建立新的性能報告
status	檢查狀態
copy	複製現有的性能報告
delete	刪除現有的性能報告

下表顯示 generate 和 copy 選項的引數。

表格 10. generate 和 copy 指令

下表是由多個橫列與兩個直欄組成的表格，其中包含 generate 和 copy 指令選項和選項說明。

選項	說明
-f	遠端檔名或 sftp 目標目錄，預設值是系統產生的名稱（針對 sftp，請使用完整路徑，或是在目錄名稱尾端加上 /（~/ 或 /tmp/））
-ip	tftp/sftp 伺服器的位址
-pn	tftp/sftp 伺服器的埠號（預設值 69/22）
-u	sftp 伺服器的使用者名稱
-pw	sftp 伺服器的密碼

mhlog 指令

使用此指令可顯示維護歷程活動日誌項目。

下表顯示各選項的引數。

表格 11. mhlog 指令

下表是由多個橫列與兩個直欄組成的表格，其中包含選項及選項說明。

表格 11. mhlog 指令（繼續）

選項	說明
-c <count>	顯示「計數」項目 (1-250)
-i <index>	顯示從索引 (1-250) 開始的項目
-f	遠端日誌檔案的檔名
-ip	tftp/sftp 伺服器的位址
-pn	tftp/sftp 伺服器的埠號（預設值 69/22）
-u	sftp 伺服器的使用者名稱
-pw	sftp 伺服器的密碼

範例

顯示將會如下所示：

```
Type       Message                                                Time
-------------  ------------                                           ----
Hardware     SAS Backplane1(SN: XXXX9CE009L) is added.                    05/08/2020,04:23:18
Hardware     CPU 1(SKU NO: 50844440) is added.                          05/08/2020,04:23:22
Hardware     CPU 2(SKU NO: 50844440) is added.                          05/08/2020,04:23:22
Hardware     M2 Card(SN: R1SH9AJ0037) is added.                          05/08/2020,04:23:22
Firmware     Primary XCC firmware is updated to TGBT99T by XCC Web.              05/08/2020,06:40:37
Firmware     Primary XCC firmware is activated to TGBT99T .                 05/08/2020,06:41:26
Hardware     PSU1(SN: D1DG94C0075) is added.                            05/08/2020,06:43:28
```

led 指令

使用此指令可顯示和設定 LED 狀態。

此 **led** 指令可顯示並設定伺服器的 LED 狀態。

- 在沒有選項的情況下執行 **led** 指令，可顯示前方面板 LED 的狀態。
- **led -d** 指令選項必須與 **led -identify on** 指令選項搭配使用。

下表顯示各選項的引數。

表格 12. led 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-l	取得所有系統及系統子元件 LED 的狀態	
-chklog	關閉檢查日誌 LED	off
-identify	變更機體識別 LED 的狀態	off、on、blink
-d	開啟所指定時段的識別 LED	時段（秒）

語法：

```
led [options]
option:
 -l
 -chklog off
```

-identify **state**
-d **time**

範例：

```
system> led
Fault          Off
Identify        On       Blue
Chklog         Off
Power          Off

system> led -l
Label          Location           State     Color
Battery         Planar            Off
BMC Heartbeat      Planar            Blink     Green
BRD            Lightpath Card       Off
Channel A        Planar            Off
Channel B        Planar            Off
Channel C        Planar            Off
Channel D        Planar            Off
Channel E        Planar            Off
Chklog          Front Panel         Off
CNFG           Lightpath Card       Off
CPU            Lightpath Card       Off
CPU 1           Planar            Off
CPU 2           Planar            Off
DASD           Lightpath Card       Off
DIMM           Lightpath Card       Off
DIMM 1          Planar            Off
DIMM 10          Planar            Off
DIMM 11          Planar            Off
DIMM 12          Planar            Off
DIMM 13          Planar            Off
DIMM 14          Planar            Off
DIMM 15          Planar            Off
DIMM 16          Planar            Off
DIMM 2          Planar            Off
DIMM 3          Planar            Off
DIMM 4          Planar            Off
DIMM 5          Planar            Off
DIMM 6          Planar            Off
DIMM 7          Planar            Off
DIMM 8          Planar            Off
DIMM 9          Planar            Off
FAN            Lightpath Card       Off
FAN 1           Planar            Off
FAN 2           Planar            Off
FAN 3           Planar            Off
Fault          Front Panel (+)      Off
Identify        Front Panel (+)       On       Blue
LINK           Lightpath Card       Off
LOG            Lightpath Card       Off
NMI            Lightpath Card       Off
OVER SPEC        Lightpath Card       Off
PCI 1          FRU              Off
PCI 2          FRU              Off
PCI 3          FRU              Off
PCI 4          FRU              Off
Planar          Planar            Off
Power          Front Panel (+)      Off
PS             Lightpath Card       Off
RAID           Lightpath Card       Off
```

```
Riser 1          Planar            Off
Riser 2          Planar            Off
SAS ERR          FRU               Off
SAS MISSING       Planar             Off
SP             Lightpath Card        Off
TEMP           Lightpath Card         Off
VRM            Lightpath Card         Off
system>
```

readlog 指令

此指令可顯示 IMM 事件日誌。

使用 **readlog** 指令可顯示 IMM 事件日誌項目。每次顯示五個事件日誌。這些項目將按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 -a 會顯示事件日誌中的所有項目（從最新項目開始）。

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）。

readlog -date date 會顯示所指定日期（以 mm/dd/yy 格式指定）的事件日誌項目。它可以是垂直線 (|) 區隔的日期清單。

readlog -sev severity 會顯示所指定嚴重性等級（E、W、I）的事件日誌項目。它可以是垂直線 (|) 區隔的嚴重性等級清單。

readlog -i ip_address 會設定儲存事件日誌的 TFTP 或 SFTP 伺服器的 IPv4 或 IPv6 IP 位址。一併使用 **-i** 和 **-l** 指令選項可指定位置。

readlog -l filename 會設定事件日誌檔案的檔名。一併使用 **-i** 和 **-l** 指令選項可指定位置。

readlog -pn port_number 會顯示或設定 TFTP 或 SFTP 伺服器的埠號（預設值 69/22）。

readlog -u username 會指定 SFTP 伺服器的使用者名稱。

readlog -pw password 會指定 SFTP 伺服器的密碼。

語法：

```
readlog [options]
option:
 -a
 -f
 -date date
 -sev severity
 -i ip_address
 -l filename
 -pn port_number
 -u username
  -pw password
```

範例：

```
system> readlog -f
1 I 2017-06-17T09:31:59.217  Remote Login Successful. Login ID: USERID
from SSH at IP address 10.134.78.180
2 I 2017-06-17T07:23:04.685  Remote Login Successful. Login ID: USERID
from webguis at IP address 10.134.78.180.
3 I 2017-06-16T11:00:35.581  Login ID: USERID from webguis at IP address 10.134.78.180 has logged off.
4 I 2017-06-16T11:00:15.174  Login ID: USERID from webguis at IP address 10.104.209.144 has logged off.
5  I 2017-06-16T10:40:14.352  Login ID: USERID from webguis at IP address 10.104.209.144 has logged off.
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

此指令提供性能或作用中事件的摘要。

使用 **syshealth** 指令可顯示伺服器性能或作用中事件的摘要。電源狀態、系統狀態、硬體狀態（包括風扇、電源供應器、儲存體、處理器、記憶體）、重新啟動計數和 IMM 軟體狀態都會顯示。

語法：

```
syshealth [argument]
argument:
 summary    -display the system health summary
 activeevents -display active events
 cooling - display cooling devices health status
 power - display power modules health status
 storage - display local storage health status
 processors - display processors health status
 memory - display memory health status
```

範例：

```
system> syshealth summary
Power  On
State  OS booted
Restarts 29

system> syshealth activeevents
No Active Event Available!
```

temps 指令

此指令可顯示所有溫度和溫度臨界值資訊。

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。

```
Example
system> temps
Temperatures are displayed in degrees Fahrenheit/Celsius

        WR      W       T       SS      HS
-------------------------------------------
CPU1    N/A     N/A     80/27   N/A     N/A
CPU2    N/A     N/A     80/27   N/A     N/A
DASD1   66/19   73/23   82/28   88/31   92/33
Amb     59/15   70/21   83/28   90/32   95/35
system>
```

附註：

1. 此輸出具有下列直欄標題：

   WR：警告重設（正向臨界遲滯值）

   W：警告（非嚴重臨界值上限）

T：溫度（現行值）

SS：正常關機（嚴重臨界值上限）

HS：強迫關機（不可回復臨界值上限）

2. 所有溫度值均以華氏度/攝氏度為單位。
3. N/A 表示「不適用」。

volts 指令

使用此指令來顯示伺服器電壓資訊。

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。

```
Example:
system> volts

     i 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>
```

附註：此輸出具有下列直欄標題：

HSL：強迫關機（低）（不可回復臨界值下限）

SSL：正常關機（低）（嚴重臨界值下限）

WL：警告（低）（非嚴重臨界值下限）

WRL：警告重設（低）（負向臨界遲滯值）

V：電壓（現行值）

WRH：警告重設（高）（正向臨界遲滯值）

WH：警告（高）（非嚴重臨界值上限）

SSH：正常關機（高）（嚴重臨界值上限）

HSH：強迫關機（高）（不可回復臨界值上限）

vpd 指令

此指令可顯示與伺服器軟硬體相關的配置及參考資料（重要產品資料）。

使用 **vpd** 指令可顯示系統 (sys)、IMM (bmc)、伺服器 BIOS (uefi)、Lenovo XClarity Provisioning Manager (lxpm)、伺服器韌體 (fw)、伺服器元件 (comp) 和 PCIe 裝置 (pcie) 的重要產品資料。此資訊與 Web 介面中顯示的相同。

語法：

```
vpd sys  - displays Vital Product Data for the system
vpd bmc  - displays Vital Product Data for the management controller
vpd uefi - displays Vital Product Data for system BIOS
vpd lxpm  - displays Vital Product Data for system LXPM
vpd fw  - displays Vital Product Data for the system firmware
vpd comp - displays Vital Product Data for the system components
```

```
vpd pmem - displays Vital Product Data for Intel Optane PMem
vpd pcie - displays Vital Product Data for PCIe devices
```

範例：

```
system> vpd bmc
Type      Status    Version   Build   ReleaseDate
----      -------   -----    ------
BMC (Primary)  Active    0.00    DVI399T  2017/06/06
BMC (Backup)  Inactive  1.00    TEI305J  2017/04/13

system>
```

伺服器電源和重新啟動控制指令

本主題提供按字母順序排序的電源和重新啟動 CLI 指令清單。

目前有 4 個伺服器電源和重新啟動指令：

power 指令

此指令說明如何控制伺服器電源。

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「遠端伺服器電源」/「重新啟動」存取權層次。

下表包含可以與 **power** 指令搭配使用的指令子集。

表格 13. power 指令

下表是由多個橫列與三個直欄組成的表格，其中包括 power 指令、指令描述和指令的相關值。

指令	說明	值
power on	使用此指令可開啟伺服器電源。	on、off
power off	使用此指令可關閉伺服器電源。 **附註：-s** 選項用於在關閉伺服器電源之前關閉作業系統。	on、off
power cycle	使用此指令可先關閉伺服器電源，然後再開啟伺服器電源。 **附註：-s** 選項用於在關閉伺服器電源之前關閉作業系統。	
power enterS3	使用此指令可讓作業系統置於 S3（休眠）模式。 **附註：**此指令僅在作業系統開啟時使用。並非在所有伺服器上均支援 S3 模式。	
power rp	使用此選項可指定主機電源還原原則。	alwayson|alwaysoff|restore
power S3resume	使用此指令可喚醒 S3（休眠）模式中的作業系統。 **附註：**此指令僅在作業系統開啟時使用。並非在所有伺服器上均支援 S3 模式。	
power state	使用此指令可顯示伺服器電源狀態及伺服器的現行狀態。	on、off

下表包含 **power on**、**power off** 及 **power cycle** 的指令選項。

表格 14. power 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

表格 14. power 指令（繼續）

選項	說明	值
-s	使用此選項可在關閉伺服器電源之前先關閉作業系統。 **附註：**在對 **power off** 及 **power cycle** 指令使用 **-every** 選項時，會隱含 **-s** 選項。	
-every	對 **power on**、**power off** 及 **power cycle** 指令使用此選項，可控制伺服器電源。您可以設定伺服器電源開啟、電源關閉或關機後再開啟的日期、時間及頻率（每日或每週）。	**附註：**此選項的值由於空間限制會在其他行呈現。 Sun|Mon|Tue|Wed|Thu| Fri|Sat|Day|clear
-t	使用此選項可指定伺服器電源開啟、關閉作業系統及關閉或重新啟動伺服器的時間（小時和分鐘）。	使用下列格式：hh:mm
-d	使用此選項可指定開啟伺服器電源的日期。此為 **power on** 指令的其他選項。 **附註：-d** 與 **-every** 選項無法在同一指令中使用。	使用下列格式：mm/dd/yyyy
-clear	使用此選項可清除已排程的電源開啟日期。此為 **power on** 指令的其他選項。	

語法：

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

下列資訊為 **power** 指令的範例。

若要在每個星期日 1:30 關閉作業系統及伺服器電源，請輸入下列指令：

```
system> power off
-every Sun -t 01:30
```

若要在每天 1:30 關閉作業系統並重新啟動伺服器，請輸入下列指令：

```
system> power cycle
-every Day -t 01:30
```

若要在每個星期一 1:30 開啟伺服器電源，請輸入下列指令：

```
system> power on
-every Mon -t 13:00
```

若要在 2013 年 12 月 31 日晚上 11:30 開啟伺服器電源，請輸入下列指令：

```
system> power on
-d 12/31/2013 -t 23:30
```

若要清除每週關機後再開啟，請輸入下列指令：

```
system> power cycle
-every clear
```

reset 指令

此指令說明如何重設伺服器。

使用 **reset** 指令可重新啟動伺服器。若要使用此指令，您必須具有電源和重新啟動存取權。

下表顯示各選項的引數。

表格 15. reset 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-s	重設伺服器之前，請先關閉作業系統。	
-d	延遲重設給定的秒數。	0 - 120
-nmi	在伺服器上產生不可遮罩式岔斷 (NMI)。	

語法：

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

fuelg 指令

此指令會顯示伺服器電源的相關資訊。

使用 **fuelg** 指令可顯示伺服器電源使用情形的相關資訊，以及配置伺服器電源管理。此指令還可以配置電源備援喪失原則。下表顯示各選項的引數。

表格 16. fuelg 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-pme	在伺服器中啟用或停用電源管理和上限設定。	on、off
-pcapmode	設定伺服器的功率上限模式。	input、output
-pcap	在目標上執行 fuelg 指令，而不使用任何選項時，會顯示落在功率上限值範圍內的數值。	瓦特數值
-history	顯示耗電量或效能歷程	pc、perf
-period	顯示歷程的數值（1、6、12、24 小時）	以小時為單位的數值
-pm	設定備援電源喪失的原則模式。	• **bt** - 基本且使用節流控制 • **rt** - 備援且不使用節流控制（預設） • **ort**- N_1 備援且使用節流控制
-zm	啟用或停用零輸出模式。原則模式設定為備援且使用節流控制時，才能設定此設定。	on、off
-perf	顯示目前的計算使用率，包括系統、微處理器和 I/O。	百分比
-pc	顯示目前耗電量	• **output** - 顯示目前 DC 耗電量。對於機架式和直立式伺服器，這將包括系統、CPU、記憶體和其他元件的耗電量；對於 ITE 刀鋒伺服器，這只會包括系統耗電量。 • **input** - 顯示目前輸入耗電量，包括系統耗電量。

語法：
```
fuelg [options]
option:
 -pme on|off
 -pcapmode input|output
 -pcap
 -history
 -period
 -pm bt|r|rt
 -zm on|off
 -perf
 -pc input|output
```

範例：
```
system> fuelg
-pme: on
system>
```

pxeboot 指令

此指令可顯示和設定「開機前執行環境」的狀況。

在沒有選項的情況下執行 **pxeboot** 可傳回現行「開機前執行環境」設定。下表顯示各選項的引數。

表格 17. pxeboot 指令

下表是由一個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-en	設定下次系統重新啟動的「開機前執行環境」狀況。	enabled、disabled

語法：
```
pxeboot [options]
option:
 -en state
```

範例：
```
system> pxeboot
-en disabled
system>
```

序列重新導向指令

本主題包含序列重新導向指令。

只有一個序列重新導向指令：第 99 頁 「console 指令」。

console 指令

此指令可用來啟動序列重新導向主控台階段作業。

使用 **console** 指令可啟動 IMM 的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

本主題提供按字母順序排序的配置 CLI 指令清單。

目前有 41 個配置指令：

accseccfg 指令

使用此指令可顯示和配置帳戶安全性設定。

在沒有選項的情況下執行 **accseccfg** 指令，可顯示所有帳戶安全資訊。下表顯示各選項的引數。

表格 18. accseccfg 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-am	設定使用者鑑別方法。	local、ldap、localldap、ldaplocal
-lp	已達登入失敗數目上限後的鎖定期間（分鐘）。	介於 0 和 2880 之間，0 = 鎖定期不會到期
-pe	密碼有效期限（天）。	介於 0 和 365 之間，0 = 永不到期
-pew	密碼有效警告期間 **附註：**密碼有效警告期間必須小於密碼有效期限。	介於 0 和 30 之間，0 = 永不警告
-pc	已啟用密碼複雜性規則。	on、off
-pl	密碼長度。	如果密碼複雜性規則為已啟用，則密碼長度為介於 8 到 32 之間。否則為介於 0 到 32 之間。
-ci	最短密碼變更間隔（小時）。	介於 0 和 240 之間，0 = 立即變更
-lf	登入失敗次數上限。	介於 0 和 10 之間，0 = 永不鎖定
-chgdft	在第一次登入之後變更預設密碼。	on、off
-chgnew	在第一次登入之後變更新的使用者密碼。	on、off
-rc	密碼重複使用週期。	介於 0 和 10 之間，0 = 立即重複使用
-wt	Web 和 Secure Shell 閒置階段作業逾時（分鐘）。	介於 0 和 1440 之間

Syntax:
```
accseccfg [options]
option:
   -legacy
   -high
   -custom
   -am authentication method
   -lp lockout_period
   -pe time_period
   -pr state
   -pc state
   -pd number_characters
   -pl number_characters
   -ci minimum_interval
   -lf number_failures
   -chgdft state
   -chgnew state
   -rc reuse_cycle
   -wt timeout
```

範例：
```
system> accseccfg
-legacy
-am local
-lp 2
-pe 0
-pr off
-pd 1
-pl 4
-ci 0
-lf 0
-chgdft off
-chgnew off
-rc 0
-wt user
system>
```

alertcfg 指令

使用此指令可顯示和配置 IMM 廣域遠端警示參數。

在沒有選項的情況下執行 **alertcfg** 指令，可顯示所有廣域遠端警示參數。下表顯示各選項的引數。

表格 19. alertcfg 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-dr	設定在 IMM 重新傳送警示之前重試之間的等待時間。	0 至 4.0 分鐘（以 0.5 分鐘為增量）
-da	設定在 IMM 將警示傳送至清單中的下一個接收者之前的等待時間。	0 至 4.0 分鐘（以 0.5 分鐘為增量）
-rl	設定 IMM 嘗試傳送警示的額外次數（如果先前的嘗試不成功）。	0 至 8

語法：

```
alertcfg [options]
 options:
  -rl retry_limit
  -dr retry_delay
  -da agent_delay
```

範例：

```
system>alertcfg
-dr 1.0
-da 2.5
-rl 5
system>
```

asu 指令

此指令可用來配置 UEFI 設定。

Advanced Settings Utility 指令 (ASU) 可用來配置 UEFI 設定。主機系統必須重新啟動，才能使任何 UEFI 設定變更生效。

下表包含可以與 **asu** 指令搭配使用的指令子集。

表格 20. asu 指令

下表是由多個橫列與三個直欄組成的表格，其中包含可與 **asu** 指令搭配使用的指令子集。有提供指令的說明資訊和相關聯的值。

指令	說明	值
delete	使用此指令可刪除設定的實例或記錄。設定必須是可刪除的實例，例如，iSCSI.AttemptName.1。	**setting_instance**
help	使用此指令可顯示一個或多個設定的說明資訊。	**setting**
set	使用此指令可變更設定的值。將 UEFI 設定設為輸入值。 **附註：** • 設定一個或多個設定/值配對。 • 如果設定展開成單一設定，則可包含萬用字元。 • 如果值包含空格，則必須用引號括住。 • 排序的清單值以等號 (=) 分隔。例如，set B*.Bootorder "CD/DVD Rom=Hard Disk 0=PXE Network"。	**setting value**
showgroups	使用此指令可顯示可用的設定群組。此指令顯示已知群組的名稱。群組名稱可能會依所安裝的裝置而異。	**setting**
show	使用此指令可顯示一個或多個設定的現行值。	**setting**
showvalues	使用此指令可顯示一個或多個設定的所有可能值。 **附註：** • 此指令會顯示設定的容許值的相關資訊。 • 會顯示設定所容許的實例數目下限和上限。 • 將會顯示預設值（如果有）。 • 預設值會以左右角括弧（< 和 >）括住。 • 文字值顯示長度下限和上限，以及正規表示式。	**setting**
附註： • 在指令語法中，**setting** 是您要檢視或變更的設定名稱，**value** 是您要設定的值。 • **Setting** 可以是多個名稱，但使用 **set** 指令時除外。		

表格 20. asu 指令（繼續）

指令	說明	值
• **Setting** 可以包含萬用字元，例如星號 (*) 或問號 (?)。 • **Setting** 可以是群組、設定名稱或 **all**。		

下列清單顯示 **asu** 指令的語法範例：

- 若要顯示所有 asu 指令選項，請輸入 `asu –help`。
- 若要顯示所有指令的詳細說明，請輸入 `asu -v –help`。
- 若要顯示一個指令的詳細說明，請輸入 `asu -v set –help`。
- 若要變更值，請輸入 `asu set` **setting value**。
- 若要顯示現行值，請輸入 `asu show` **setting**。
- 若要以長批次格式顯示設定，請輸入 `asu show -l -b all`
- 若要顯示設定的所有可能值，請輸入 `asu showvalues` **setting**。**show values** 指令範例：
```
system> asu showvalues S*.POST*
SystemRecovery.POSTWatchdogTimer==<Disable>=Enable
SystemRecovery.POSTWatchdogTimerValue=numeric min=5 max=20 step=1 default=5
system>
```

下表顯示各選項的引數。

表格 21. asu 選項

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-b	以批次格式顯示。	
--help[1]	顯示指令用法和選項。--help 選項置於指令之前，例如，**asu --help show**。	
--help[1]	顯示指令的說明。--help 選項置於指令之後，例如，**asu show --help**。	
-l	長格式設定名稱（包括配置設定）。	
-m	混合格式設定名稱（使用配置 ID）。	
-v[2]	詳細輸出。	

1. --help 選項可與任何指令搭配使用。
2. -v 選項僅限用在 **asu** 與指令之間。

語法：
```
asu [options] command [cmdopts]
options:
  -v verbose output
  --help display main help
cmdopts:
  --help help for the command
```

附註：如需更多指令選項，請參閱個別指令。

使用 asu 交易指令可設定多個 UEFI 設定，以及建立和執行批次模式指令。使用 **tropen** 和 **trset** 指令可建立包含所要套用之多個設定的交易檔。使用 **tropen** 指令可開啟具有給定 ID 的交易。使用 **trset** 指令可將設定新增至該集。使用 **trcommit** 指令可確定已完成的交易。完成交易時，可以使用 **trrm** 指令將其刪除。

附註：UEFI 設定還原作業會建立 ID 為三位隨機碼的交易。

下表包含可與 **asu** 指令搭配使用的交易指令。

表格 22. asu 交易指令

下表是由多個橫列與三個直欄組成的表格，其中包含 transactions 指令、指令說明和指令的相關值。

指令	說明	值
tropen **id**	此指令可建立新的交易檔，其中包含數個所要設定的設定。	**Id** 是識別字串，句含 1 - 3 個英數字元。
trset **id**	此指令可將一個或多個設定或值配對新增至交易。	**Id** 是識別字串，句含 1 - 3 個英數字元。
trlist **id**	此指令會先顯示交易檔的內容。如果交易檔是在 CLI Shell 中建立的，這會很有用。	**Id** 是識別字串，句含 1 - 3 個英數字元。
trcommit **id**	此指令可確定並執行交易檔的內容。將會顯示執行的結果和任何錯誤。	**Id** 是識別字串，句含 1 - 3 個英數字元。
trrm **id**	此指令會在確定交易檔後，移除交易檔。	**Id** 是識別字串，句含 1 - 3 個英數字元。

建立多個 UEFI 設定的範例：

```
asu tropen TR1
asu trset TR1 UEFI.BootModes.SystemBootMode "UEFI and Legacy"
asu trset TR1 BootOrder.BootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 BootOrder.WolBootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 UEFI.DevicesandIOPorts.Com1BaudRate 115200
asu trset TR1 UEFI.DevicesandIOPorts.Com1DataBits 8
asu trset TR1 UEFI.DevicesandIOPorts.Com1FlowControl Disable
asu trset TR1 UEFI.DevicesandIOPorts.Com1Parity None
asu trset TR1 UEFI.DevicesandIOPorts.Com1StopBits 1
asu trset TR1 UEFI.DevicesandIOPorts.COMPort1 Enable
asu trcommit TR1
```

backup 指令

使用此指令可建立包含現行系統安全設定的備份檔。

下表顯示各選項的引數。

表格 23. backup 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-f	備份檔名稱	有效的檔名
-pp	用於加密備份檔內部密碼的密碼或通行詞組	有效的密碼或引號定界的通行詞組
-ip	TFTP/SFTP 伺服器的 IP 位址	有效的 IP 位址
-pn	TFTP/SFTP 伺服器的埠號	有效的埠號（預設值 69/22）

表格 23. backup 指令（繼續）

選項	說明	值
-u	SFTP 伺服器的使用者名稱	有效的使用者名稱
-pw	SFTP 伺服器的密碼	有效的密碼
-fd	備份 CLI 指令的 XML 說明檔名	有效的檔名

語法：

```
backup [options]
  option:
   -f    filename
   -pp   password
   -ip   ip address
   -pn   port number
   -u    username
   -pw   password
   -fd   filename
```

範例：

```
system> backup f xcc-back.cli pp xxxxxx ip 192.168.70.200
ok
system>
```

dhcpinfo 指令

使用此指令可檢視 DHCP 伺服器為 eth0 指派的 IP 配置。

使用 **dhcpinfo** 指令可檢視 DHCP 伺服器為 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** 指令來啟用或停用 DHCP。

語法：

```
dhcpinfo eth0
```

Example:

```
system> dhcpinfo eth0
   -server :  10.240.0.10
   -n      :  XCC-7X19-123456789A
   -i      :  10.243.4.66
   -i6     :  ::
   -g      :  10.243.0.1
   -s      :  255.255.240.0
   -d      :  labs.lenovo.com
   -d6     :
   -dns1   :  10.240.0.10
   -dns2   :  10.240.0.11
   -dns3   :  0.0.0.0
   -dns61  :  ::
   -dns62  :  ::
   -dns63  :  ::
```

下表說明此範例的輸出。

表格 24. dhcpinfo 指令

下表是由多個橫列與兩個直欄組成的表格，說明前述範例中所使用的選項。

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	第三級 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	第三級 IPv6 DNS 伺服器 IP 位址

dns 指令

使用此指令可檢視和設定 IMM 的 DNS 配置。

附註：在 Flex System 中，無法修改 IMM 上的 DNS 設定。DNS 設定由 CMM 管理。

在沒有選項的情況下執行 **dns** 指令，可顯示所有 DNS 配置資訊。下表顯示各選項的引數。

表格 25. dns 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-state	DNS 狀態	on、off
-ddns	DDNS 狀態	enabled、disabled
-i1	主要 IPv4 DNS 伺服器 IP 位址	帶點十進位 IP 位址格式的 IP 位址。
-i2	次要 IPv4 DNS IP 位址	帶點十進位 IP 位址格式的 IP 位址。
-i3	第三級 IPv4 DNS 伺服器 IP 位址	帶點十進位 IP 位址格式的 IP 位址。
-i61	主要 IPv6 DNS 伺服器 IP 位址	IPv6 格式的 IP 位址。
-i62	次要 IPv6 DNS IP 位址	IPv6 格式的 IP 位址。
-i63	第三級 IPv6 DNS 伺服器 IP 位址	IPv6 格式的 IP 位址。
-p	IPv4/IPv6 優先順序	ipv4、ipv6

語法：

```
dns [options]
```

```
option:
 -state state
 -ddns state
 -i1 first_ipv4_ip_address
 -i2 second_ipv4_ip_address
 -i3 third_ipv4_ip_address
 -i61 first_ipv6_ip_address
 -i62 second_ipv6_ip_address
 -i63 third_ipv6_ip_address
  -p priority
```

附註：下列範例顯示已停用 DNS 的 IMM 配置。

範例：

```
system> dns
  -state  : disabled
  -i1     : 0.0.0.0
  -i2     : 0.0.0.0
  -i3     : 0.0.0.0
  -i61    : ::
  -i62    : ::
  -i63    : ::
  -ddns   : enabled
  -dnsrc  : DHCP
  -ddn    :
  -ddncur : labs.lenovo.com
  -p      : ipv6
  -dscvry : enabled

system>
```

下表說明在前述範例中所使用的選項。

表格 26. dns 指令的輸出

下表是由多個橫列與兩個直欄組成的表格，說明在前述範例中使用的選項。

選項	說明
-state	DNS 狀態（on 或 off）
-i1	主要 IPv4 DNS 伺服器 IP 位址
-i2	次要 IPv4 DNS IP 位址
-i3	第三級 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	第三級 IPv6 DNS 伺服器 IP 位址
-ddns	DDNS 狀態（enabled 或 disabled）
-dnsrc	DDNS 慣用的網域名稱（dhcp 或 manual）
-ddn	手動指定的 DDN
-ddncur	現行 DDN（唯讀）
-p	慣用的 DNS 伺服器（ipv4 或 ipv6）

encaps 指令

使用此指令可讓 BMC 結束 encapsulation 模式。

下表顯示各選項的引數。

表格 27. encaps 指令

下表是由一個橫列與兩個直欄組成的表格，其中包含選項及選項說明。

選項	說明
lite off	讓 BMC 結束 encapsulation 模式，並開啟對所有使用者的廣域存取

ethtousb 指令

使用 **ethtousb** 指令可顯示和配置乙太網路至 Ethernet-over-USB 埠對映。

此指令可讓您將外部乙太網路埠號對映至 Ethernet-over-USB 的不同埠號。

在沒有選項的情況下執行 **ethtousb** 指令，可顯示 Ethernet-over-USB 資訊。下表顯示各選項的引數。

表格 28. ethtousb 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-en	Ethernet-over-USB 狀態	enabled、disabled
-m**x**	配置索引 **x** 的埠對映	以冒號 (:) 區隔的埠配對，格式為 **port1:port2** 其中： • 在指令選項中，埠索引編號 (**x**) 指定為 1 至 10 的整數。 • 埠配對的 **port1** 是外部乙太網路埠號。 • 埠配對的 **port2** 是 Ethernet-over-USB 埠號。
-rm	移除所指定索引的埠對映	1 至 10 在沒有選項的情況下使用 **ethtousb** 指令，將顯示埠對映索引。

語法：

```
ethtousb [options]
option:
 -en state
 -mxport_pair
 -rm map_index
```

範例：

```
system> ethtousb  -en enabled -m1 100:200 -m2 101:201
system> ethtousb
 -en enabled
 -m1 100:200
 -m2 101:201
system> ethtousb -rm 1
system>
```

firewall 指令

使用此指令配置防火牆以限制來自某些位址的存取，並可以選擇限制存取時間範圍。如果未指定選項，則將顯示目前的設定。

下表顯示各選項的引數。

表格 29. firewall 指令

下表是由多個橫列與三個直欄組成的表格，其中包含選項及選項說明。

選項	說明	值
-bips	封鎖 1-3 個 IP 位址（以逗點分隔、CIDR 或範圍）	有效的 IP 位址 **附註：**IPv4 和 IPv6 位址可以使用 CIDR 格式來封鎖一系列位址。
-bmacs	封鎖 1-3 個 MAC 位址（以逗點分隔）	有效的 MAC 位址 **附註：**MAC 位址過濾僅適用於特定位址。
-bbd	封鎖開始日期	日期格式為 <YYYY-MM-DD>
-bed	封鎖結束日期	日期格式為 <YYYY-MM-DD>
-bbt	封鎖開始時間	時間格式為 <HH:MM>
-bet	封鎖結束時間	時間格式為 <HH:MM>
-bti	封鎖 1-3 個時間間隔（以逗號分隔） 例如，**firewall - bti 01:00—02:00,05:05—10:30** 會封鎖每天 01:00-02:00 和 05:05-10:30 期間的存取	時間範圍格式為 <HH:MM-HH:MM>
-clr	清除給定類型的防火牆規則	ip、mac、datetime、interval、all
以下選項用於 IP 位址封鎖		
-iplp	IP 位址鎖定期（以分鐘為單位）。	介於 0 和 2880 之間的數值，0 = 永不到期
-iplf	IP 位址被鎖定之前的登入失敗數目上限。 **附註：**如果此值不為 0，則它必須大於或等於由 **<accseccfg -lf>** 設定的 <登入失敗數目上限>	介於 0 和 32 之間的數值，0 = 永不鎖定
-ipbl	顯示/配置要鎖定的 IP 位址清單。	del、clrall、show • **-del**：刪除封鎖清單中的 IPv4 或 IPv6 位址 • **-clrall**：清除所有封鎖 IP • **-show**：顯示所有封鎖 IP

範例：

```
· “firewall”: Show all options’ value and IP addresses blocking list.
· “firewall -bips  192.168.1.1,192.168.1.0/24,192.168.1.1-192.168.1.5”: Block the access from multi IPs
· “firewall -bti 01:00-02:00,05:05-10:30,14:15-20:00”: Block all access during 01:00-02:00,05:05-10:30,14:15-20:00 every day.
· “firewall –clr all”: Clear all rules of “Block List and Time Restriction”.
· “firewall -iplp 60”:Set IP address lockout period to 60 minutes.
· “firewall -iplf 5”:Set maximum number of login failures to 5 timesi.
· “firewall -ipbl -del 192.168.100.1”:Delete 192.168.100.1 from IP address blocking list.
· “firewall –ipbl -del 3fcc:1234::2”:Delete 3fcc:1234::2 from IP address blocking list.
· “firewall –ipbl –clrall”:  Delete all blocking IP addresses.
· “firewall –ipbl –show”:   Show all blocking IP addresses.
```

gprofile 指令

使用此指令可顯示及配置 IMM 的 Group Profile。

下表顯示各選項的引數。

表格 30. gprofile 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-clear	刪除群組	enabled、disabled
-n	群組名稱	**group_name** 為最多 63 個字元的字串。**group_name** 必須是唯一的。
-a	角色型權限層級	supervisor、operator、rbs <role list>： nsc|am|rca|rcvma|pr|bc|cel|ac 角色清單值是使用以垂直線分隔的值清單來指定。
-h	顯示指令用法和選項	

語法：

```
gprofile [1 – 16 group_profile_slot_number] [options]
options:
-clear state
-n group_name
-a authority level:
  -nsc network and security
  -am user account management
  -rca remote console access
  -rcvma remote console and remote disk access
  -pr remote server power/restart access
  -bc basic adapter configuration
  -cel ability to clear event logs
  -ac advanced adapter configuration
-h help
```

hashpw 指令

將此指令與 -sw 選項搭配使用可啟用/停用協力廠商密碼功能，與 -re 選項搭配使用可啟用/停用允許擷取協力廠商密碼。

下表顯示各選項的引數。

表格 31. hashpw 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-sw	協力廠商密碼開關狀態	enabled、disabled
-re	協力廠商密碼讀取狀態 **附註：**如果已啟用開關，則可以設定讀取。	enabled、disabled

範例：

```
system> hashpw -sw enabled -re enabled
system> users -5 -n guest5 -shp ef92b778bafe771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f -a super
system> users -5 ghp
ef92b778bafe771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f
system> users
Account    Login ID    Advanced Attribute        Role       Password Expires
```

```
-------   --------   ------------------       ------      ----------------
  1       USERID          Native          Administrator    Password doesn't expire
5       guest5   Third-party Password        Administrator          90 day(s)
```

ifconfig 指令

使用此指令可配置乙太網路介面。

輸入 **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，請依次輸入選項和值。若要變更介面配置，您必須至少具有「配接器網路連線和安全性配置」權限。

附註：在 Flex System 中，VLAN 設定由 Flex System CMM 管理，且無法在 IMM 上修改。

下表顯示各選項的引數。

表格 32. ifconfig 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-b	燒錄 MAC 位址（唯讀且不可配置）	
-state	介面狀態	disabled、enabled
-c	配置方法	dhcp、static、dthens（dthens 對應於 Web 介面上的**嘗試 dhcp 伺服器，如果失敗請使用靜態配置**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。
-r	資料傳輸率	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（第一個位元組必須為偶數）。
-dn	網域名稱	有效格式的網域名稱。
-auto	決定是否可配置資料傳輸率和雙工網路設定的自動協調設定	true、false
-ghn	從 DHCP 取得主機名稱	disabled、enabled
-nic	交換器 NIC 模式[1]	shared、dedicated、shared:nixX[2]
-failover[2]	失效接手模式	none、shared、shared:nicX
-nssync[3]	網路設定同步化	enabled、disabled
-address_table	自動產生的 IPv6 位址及其字首長度表格 **附註：**僅在啟用 IPv6 和無狀態自動配置時，此選項才可見。	此值是唯讀且不可配置。
-ipv6	IPv6 狀態	disabled、enabled

表格 32. ifconfig 指令（繼續）

選項	說明	值
-lla	鏈結本端位址 **附註：**僅在啟用 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	IPv6 格式的乙太網路通道 0 靜態 IP 位址。
-p6	位址字首長度	介於 1 與 128 之間的數值。
-g6	閘道或預設路由	閘道 IP 位址或 IPv6 格式之乙太網路通道 0 的預設路由。
-dhcp6	DHCPv6 狀態	enabled、disabled
-sa6	IPv6 無狀態自動配置狀態	enabled、disabled
-vlan	啟用或停用 VLAN 標記	enabled、disabled
-vlanid	用於 IMM 的網路封包識別標籤	介於 1 與 4094 之間的數值。

附註：

1. -nic 也將顯示 nic 的狀態。[active] 指出目前正在使用哪個 nic XCC

   例如：

   ```
   -nic: shared:nic3
    nic1: dedicate
    nic2: ext card slot #3
    nic3: ext card slot 5 [active]
   ```

   指出 nic3 處於共用模式、位於插槽 5，nic2 位於插槽 3，nic1 是 XCC 專用埠，並且 XCC 正在使用 nic3。
2. 在安裝選配 Mezzanine 網路卡的伺服器上，可以使用 shared:nicX 值。IMM 可以使用此 Mezzanine 網路卡。
3. 當 IMM 配置為使用專用管理網路埠時，若是中斷連接專用網路埠，則 -failover 選項會將 IMM 導向切換為共用網路埠。
4. 如果已啟用失效接手模式，則 -nssync 選項會將 IMM 導向使用與專用管理網路埠上共用網路埠所用的相同網路設定。

語法：

```
ifconfig eth0 [options]
options:

 -state interface_state
 -c config_method
 -i static_ipv4_ip_address
 -g ipv4_gateway_address
 -s subnet_mask
 -n hostname
 -r data_rate
 -d duplex_mode
 -m max_transmission_unit
 -l locally_administered_MAC
 -b burned_in_MAC_address
 -dn domain_name
 -auto state
 -nic state
 -failover mode
 -nssync state
 -address_table
 -lla ipv6_link_local_addr
 -dhcp6 state
 -ipv6 state
 -ipv6static state
```

```
 -sa6 state
 -i6 static_ipv6_ip_address
 -g6 ipv6_gateway_address
 -p6 length
 -vlan state
 -vlanid VLAN ID
```

範例：

```
system> ifconfig eth0
-state  : enabled
-c    : dthens
-ghn   : disabled
-i    : 192.168.70.125
-g    : 0.0.0.0
-s    : 255.255.255.0
-n    : IMM00096B9E003A
-auto   : true
-r    : auto
-d    : auto
-vlan   : disabled
-vlanid : 1
-m    : 1500
-b    : 00:09:6B:9E:00:3A
-l    : 00:00:00:00:00:00
-dn    :
-ipv6   : enabled
-ipv6static : disabled
-i6    : ::
-p6    : 64
-g6    : ::
-dhcp6  : enabled
-sa6   : enabled
-lla   : fe80::6eae:8bff:fe23:91ae
-nic : shared:nic3
   nic1: dedicate
   nic2: ext card slot #3
   nic3: ext card slot #5 [active]
-address_table  :

system> ifconfig eth0 -c static -i 192.168.70.133
These configuration changes will become active after the next reset of the IMM.
```

keycfg 指令

使用此指令可顯示、新增或刪除啟動金鑰。

啟動金鑰可控制對選用 IMM 功能的存取。

附註：

- 在沒有任何選項的情況下執行 **keycfg** 指令時，會顯示已安裝啟動金鑰的清單。顯示的金鑰資訊包括每一個啟動金鑰的索引編號、啟動金鑰的類型、金鑰的有效日期、剩餘的使用數目、金鑰狀態，以及金鑰說明。
- 透過檔案傳送新增啟動金鑰。
- 透過指定金鑰號碼或金鑰類型來刪除舊的金鑰。按類型刪除金鑰時，僅刪除給定類型的第一個金鑰。

下表顯示各選項的引數。

表格 33. keycfg 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-add	新增啟動金鑰	-ip、-pn、-u、-pw 及 -f 指令選項的值
-ip	具有要新增啟動金鑰的 TFTP 伺服器 IP 位址	TFTP 伺服器的有效 IP 位址
-pn	具有要新增啟動金鑰的 TFTP/SFTP 伺服器埠號	TFTP/SFTP 伺服器的有效埠號（預設值 69/22）
-u	具有要新增啟動金鑰的 SFTP 伺服器使用者名稱	SFTP 伺服器的有效使用者名稱
-pw	具有要新增啟動金鑰的 SFTP 伺服器密碼	SFTP 伺服器的有效密碼
-f	要新增啟動金鑰的檔名	啟動金鑰檔的有效檔名
-del	按索引編號刪除啟動金鑰	**keycfg** 清單中的有效啟動金鑰索引編號
-deltype	按金鑰類型刪除啟動金鑰	有效的金鑰類型值

語法：

```
keycfg [options]
option:
 -add
   -ip tftp/sftp server ip address
   -pn pn port number of tftp/sftp server (default 69/22)
   -u  username for sftp server
   -pw password for sftp server
   -f  filename
   -del  n ( where n is a valid ID number from listing)
    -deltype x ( where x is a Type value)
```

範例：

```
system> keycfg
ID Type Valid      Uses      Status  Description
1  4   10/10/2010   5        "valid"  "IMM remote presence"
2  3   10/20/2010   2        "valid"  "IMM feature
3  32796 NO CONSTRAINTS  NO CONSTRAINTS "valid"  "IBM Security Key Lifecycle Manager for SEDs FoD"
system>
```

附註：由於空間限制，ID 號碼 3 的**說明**欄位會顯示在其他行。

ldap 指令

使用此指令可顯示和配置 LDAP 通訊協定配置參數。

下表顯示各選項的引數。

表格 34. ldap 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-a	使用者鑑別方法	local only、LDAP only、local first then LDAP、LDAP first then local
-aom	僅限鑑別模式	enabled、disabled

表格 34. ldap 指令（繼續）

選項	說明	值
-b	連結方法	anonymous、bind with ClientDN and password、bind with Login Credential
-c	用戶端識別名稱	最多 127 個字元的 **client_dn** 字串
-d	搜尋網域	最多 63 個字元的 **search_domain** 字串
-f	群組過濾器	最多 127 個字元的 **group_filter** 字串
-fn	樹系名稱	適用於 Active Directory 環境。最多 127 個字元的字串。
-g	群組搜尋屬性	最多 63 個字元的 **group_search_attr** 字串
-l	登入權限屬性	最多 63 個字元的 **string** 字串
-p	用戶端密碼	最多 15 個字元的 **client_pw** 字串
-pc	確認用戶端密碼	最多 15 個字元的 **confirm_pw** 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。如果這些引數不相符，此指令將會失敗。
-ep	加密密碼	備份/還原密碼（僅限內部使用）
-r	根項目識別名稱 (DN)	最多 127 個字元的 **root_dn** 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	最多 127 個字元的 **host name/ip_addr** 字串或 IP 位址
-s2ip	伺服器 2 的主機名稱/IP 位址	最多 127 個字元的 **host name/ip_addr** 字串或 IP 位址
-s3ip	伺服器 3 的主機名稱/IP 位址	最多 127 個字元的 **host name/ip_addr** 字串或 IP 位址
-s4ip	伺服器 4 的主機名稱/IP 位址	最多 127 個字元的 **host name/ip_addr** 字串或 IP 位址
-s1pn	伺服器 1 的埠號	最多 5 位數的 **port_number** 數字埠號
-s2pn	伺服器 2 的埠號	最多 5 位數的 **port_number** 數字埠號
-s3pn	伺服器 3 的埠號	最多 5 位數的 **port_number** 數字埠號
-s4pn	伺服器 4 的埠號	最多 5 位數的 **port_number** 數字埠號
-t	伺服器目標名稱	啟用 rbs 選項時，此欄位將指定可透過「角色型安全 (RBS) 嵌入式管理單元」工具與 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	最多 63 個字元的 **search_attrib** 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:
  -a loc|ldap|locld|ldloc
  -aom enable/disabled
  -b anon|client|login
  -c client_dn
  -d search_domain
  -f group_filter
  -fn forest_name
```

-g **group_search_attr**
-l **string**
-p **client_pw**
-pc **confirm_pw**
-ep **encrypted_pw**
-r **root_dn**
-rbs **enable|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

使用此指令可顯示和配置「網路時間通訊協定 (NTP)」。

下表顯示各選項的引數。

表格 35. ntp 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-en	啟用或停用「網路時間通訊協定」。	enabled、disabled
-i[1]	「網路時間通訊協定」伺服器的名稱或 IP 位址。這是「網路時間通訊協定」伺服器的索引編號。	用於時鐘同步化的 NTP 伺服器名稱。NTP 伺服器的索引編號範圍為 -i1 至 -i4。
-f	IMM 時鐘與網路時間通訊協定伺服器同步化的頻率（單位為分鐘）。	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。

1. -i 與 i1 相同。

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

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

portcfg 指令

使用此指令可針對序列重新導向功能配置 IMM。

IMM 必須配置為與伺服器內部序列埠設定相符。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「配接器網路連線和安全性配置」權限。

附註：伺服器外部序列埠只能供 IMM 用於 IPMI 功能。序列埠不支援 CLI。不支援 Remote Supervisor Adapter II CLI 中呈現的 **serred** 和 **cliauth** 選項。

在沒有選項的情況下執行 **portcfg** 指令可顯示序列埠配置。下表顯示各選項的引數。

附註：資料位元數 (8) 設定於硬體中，且無法變更。

表格 36. portcfg 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-b	傳輸速率	9600, 19200, 38400, 57600, 115200
-p	同位	none、odd、even
-s	停止位元	1, 2
-climode	CLI 模式	0, 1, 2 其中： • 0 = none：停用 CLI • 1 = cliems：使用 EMS 相容按鍵順序來啟用 CLI • 2 = cliuser：利用使用者定義的按鍵順序來啟用 CLI

語法：

```
portcfg [options]
 options:
  -b baud_rate
  -p parity
  -s stopbits
   -climode mode
```

範例：

```
system> portcfg
-b: 57600
-climode: 2 (CLI with user defined keystroke sequence)
-p: even
-s: 1
system> portcfg -b 38400
ok
system>
```

portcontrol 指令

使用此指令可開啟或關閉網路服務埠。

目前此指令僅支援對 IPMI 通訊協定的埠進行控制。輸入 **portcontrol** 可顯示 IPMI 埠狀態。若要啟用或停用 IPMI 網路埠，請輸入 **-ipmi** 選項，後面接著 **on** 或 **off** 值。

表格 37. portcontrol 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

表格 37. portcontrol 指令（繼續）

選項	說明	值
-all	啟用或停用所有介面和探索通訊協定	on、off
-cim	啟用或停用 CIM 探索	on、off
-ipmi	啟用或停用透過 LAN 的 ipmi 存取	on、off
-ipmi-kcs	啟用或停用來自伺服器的 ipmi 存取	on、off
-rest	啟用或停用 REST 探索	on、off
-slp	啟用或停用 SLP 探索	on、off
-snmp	啟用或停用 SNMP 探索	on、off
-ssdp	啟用或停用 SSDP 探索	on、off
-cli	啟用或停用 CLI 探索	on、off
-web	啟用或停用 WEB 探索	on、off

語法：
```
portcontrol [options]
 options:
  -ipmi on/off
```

範例：
```
system> portcontrol
cim：on
ipmi：on
ipmi-kcs：on
rest：on
slp：on
snmp：off
ssdp：on
cli：on
web：on
```

ports 指令

使用此指令可顯示和配置 IMM 埠。

在沒有選項的情況下執行 **ports** 指令，可顯示所有 IMM 埠的資訊。下表顯示各選項的引數。

表格 38. ports 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-open	顯示開啟的埠	
-reset	將埠重設為預設值	
-httpp	HTTP 埠號	預設埠號：80

表格 38. ports 指令（繼續）

選項	說明	值
-httpsp	HTTPS 埠號	預設埠號：443
-sshp	SSH 舊式 CLI 埠號	預設埠號：22
-snmpap	SNMP 代理程式埠號	預設埠號：161
-snmptp	SNMP 設陷埠號	預設埠號：162
-rpp	遠端顯示埠號	預設埠號：3900
-cimhp	CIM over HTTP 埠號	預設埠號：5988
-cimhsp	CIM over HTTPS 埠號	預設埠號：5989

語法：

```
ports [options]
option:
 -open
 -reset
 -httpp port_number
 -httpsp port_number
 -sshp port_number
 -snmpap port_number
 -snmptp port_number
 -rpp port_number
 -cimhp port_number
  -cimhsp port_number
```

範例：

```
system> ports
-httpp 80
-httpsp 443
-rpp 3900
-snmpap 161
-snmptp 162
-sshp 22
-cimhp 5988
-cimhsp 5989
system>
```

rdmount 指令

使用此指令可裝載遠端磁碟映像檔或網路共用

下表顯示各選項的引數。

表格 39. rdmount 指令

下表是由多個橫列與兩個直欄組成的表格，其中包含選項及選項說明。

附註：

- 最多可以在 XClarity Controller 記憶體中上傳兩個檔案，並使用 XClarity Controller RDOC 功能裝載做為虛擬媒體。兩個檔案的大小總計不得超過 50 MB。除非使用了 —rw 選項，否則上傳的映像檔是唯讀的。
- 使用 HTTP、SFTP 或 FTP 通訊協定裝載或對映映像檔時，所有映像檔的大小合計不得超過 50 MB。如果是使用 NFS 或 SAMBA 通訊協定，則沒有大小限制。

表格 39. rdmount 指令（繼續）

選項	說明
-r	rdoc 作業（如果使用，則必須是第一個選項） -r -map：裝載 RDOC 映像檔 -r -unmap<檔名>：卸載已裝載的 RDOC 映像檔 -r -maplist：顯示透過 XClarity Controller Web 瀏覽器和 CLI 介面裝載的 RDOC 映像檔
-map	-t <samba|nfs|http|sftp|ftp> 檔案系統類型 -ro 唯讀 -rw 讀寫 -u 使用者 -p 密碼 -l 檔案位置（URL 格式） -o 選項（samba 和 nfs 裝載的額外選項字串） -d 網域（samba 裝載的網域）
-maplist	顯示對映的映像檔
-unmap <id|fname>	對網路映像檔使用 id，對 rdoc 使用檔名
-mount	裝載對映的映像檔
-unmount	卸載已裝載的映像檔

restore 指令

使用此指令可從備份檔還原系統設定。

下表顯示各選項的引數。

表格 40. restore 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-f	備份檔名稱	有效的檔名
-pp	用於加密備份檔內部密碼的密碼或通行詞組	有效的密碼或引號定界的通行詞組
-ip	TFTP/SFTP 伺服器的 IP 位址	有效的 IP 位址
-pn	TFTP/SFTP 伺服器的埠號	有效的埠號（預設值 69/22）
-u	SFTP 伺服器的使用者名稱	有效的使用者名稱
-pw	SFTP 伺服器的密碼	有效的密碼

語法：

```
restore [options]
option:
 -f filename
```

-pp **password**
-ip **ip_address**
-pn **port_number**
-u **username**
-pw **password**

範例：
system> **restore f xcc-back.cli pp xxxxxx ip 192.168.70.200**
ok
system>

restoredefaults 指令

使用此指令可將所有 IMM 設定還原為原廠預設值。

- 沒有用於 **restoredefaults** 指令的選項。
- 在處理此指令之前，系統會要求您確認此指令。

語法：
restoredefaults

範例：
system> **restoredefaults**

This action will cause all IMM settings to be set to factory defaults.

If this is the local system, you will lose your TCP/IP connection as a result.
You will need to reconfigure the IMM network interface to restore connectivity.
After the IMM configuration is cleared, the IMM will be restarted.

Proceed? (y/n)
Y
Restoring defaults

roles 指令

使用此指令可顯示或配置角色。

下表顯示各選項的引數。

表格 41. roles 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-n	要配置的角色	限制在 32 個字元內
-p	設定權限	custom:am|rca|rcvma|pr|cel|bc|nsc|ac|us • **am**：使用者帳戶管理存取 • **rca**：遠端主控台存取 • **rcvma**：遠端主控台和遠端磁碟（虛擬媒體）存取 • **pr**：遠端伺服器電源/重新啟動存取 • **cel**：清除事件日誌的能力 • **bc**：配接器配置（基本） • **nsc**：配接器配置（網路和安全性）

表格 41. roles 指令（繼續）

選項	說明	值
		• **ac**：配接器配置（進階） • **us**：UEFI 安全性 **附註：**上面的自訂權限旗標可以任意組合使用
d	刪除列	

語法

```
 roles [-options] - display/configure roles
  - role_account -role number[3-31]
options:
  -n     - role name (limited to 32 characters)
  -p     - privilege (custom:am|rca|rcvma|pr|cel|bc|nsc|ac|us)
    am   - User account management access
    rca  - Remote console access
    rcvma - Remote console and remote disk (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)
    us   - UEFI Security
    Note: the above custom permission flags can be used in any combination
  -d     - delete a row
```

範例

```
system> roles -3 -n test1 -p custom:am|rca|rcvma
ok


system> roles
Account        Role                Privilege            Assigned To
------- ---------------------------------  -------------------------   -------------------------------
  0          Administrator           all              USERID
  1             ReadOnly            none
  2             Operator      custom:pr|cel|bc|nsc
  3               test1      custom:am|rca|rcvma
```

seccfg 指令

使用此指令可執行韌體回復。

下表顯示各選項的引數。

表格 42. seccfg 指令

下表是由多個橫列與兩個直欄組成的表格，其中包含選項及選項說明。

選項	說明	值
-fwrb	允許韌體回復至舊版	yes、no
-rppen	遠端物理現場授權啟用（唯讀）	/

表格 42. seccfg 指令（繼續）

選項	說明	值
-rppto	遠端物理現場授權逾時（唯讀）	/
-rpp	物理現場授權（若已由 BIOS 啟用）	yes、no
-aubp	啟用或停用自動備份至主要升級的功能	enabled、disabled

set 指令

使用此指令可變更部分 IMM 設定。

- 您可以使用簡單的 **set** 指令來變更部分 IMM 設定。
- 其中部分設定（如環境變數）由 CLI 使用。

下表顯示各選項的引數。

表格 43. set 指令

下表是由一個橫列與三個直欄組成的表格，其中包括指令說明及相關聯的資訊。

選項	說明	值
值	設定所指定路徑或設定的值	所指定路徑或設定的適當值。

語法：

```
set [options]
option:
 value
```

smtp 指令

使用此指令可顯示和配置 SMTP 介面的設定。

在沒有選項的情況下執行 **smtp** 指令可顯示所有 SMTP 介面資訊。下表顯示各選項的引數。

表格 44. smtp 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-auth	SMTP 鑑別支援	enabled、disabled
-authepw	SMTP 鑑別加密的密碼	有效的密碼字串
-authmd	SMTP 鑑別方法	CRAM-MD5、LOGIN
-authn	SMTP 鑑別使用者名稱	字串（限制在 256 個字元內）
-authpw	SMTP 鑑別密碼	字串（限制在 256 個字元內）
-pn	SMTP 埠號	有效的埠號
-s	SMTP 伺服器 IP 位址或主機名稱	有效的 IP 位址或主機名稱（63 個字元限制）

語法：

```
smtp [options]
option:
 -auth enabled|disabled
```

```
-authepw password
-authmd CRAM-MD5|LOGIN
-authn username
-authpw password
-s ip_address_or_hostname
 -pn port_number
```

範例：

```
system> smtp
-s test.com
-pn 25
system>
```

snmp 指令

使用此指令可顯示和配置 SNMP 介面資訊。

在沒有選項的情況下執行 **snmp** 指令可顯示所有 SNMP 介面資訊。下表顯示各選項的引數。

表格 45. snmp 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-a3	SNMPv3 代理程式	on、off **附註：**若要啟用 SNMPv3 代理程式，必須符合下列準則： • 使用 -cn 指令選項指定 IMM 聯絡人。 • 使用 -l 指令選項指定 IMM 位置。
-t1	SNMPv1 設陷	on、off
-t2	SNMPv2 設陷	on、off
-t	SNMPv3 設陷	on、off
-l	IMM 位置	字串（限制在 47 個字元內）。 **附註：** • 含有空格的引數必須括在引號中。引數中不允許前導空格或尾端空格。 • 透過不指定任何引數或將空字串指定為引數（例如 ""），來清除 IMM 位置。
-cn	IMM 聯絡人名稱	字串（限制在 47 個字元內）。 **附註：** • 含有空格的引數必須括在引號中。引數中不允許前導空格或尾端空格。 • 透過不指定任何引數或將空字串指定為引數（例如 ""），來清除 IMM 聯絡人名稱。
-c	SNMP 社群名稱	字串（限制在 15 個字元內）。 **附註：** • 含有空格的引數必須括在引號中。引數中不允許前導空格或尾端空格。 • 透過不指定任何引數或將空字串指定為引數（例如 ""），來清除 SNMP 社群名稱。

表格 45. snmp 指令（繼續）

選項	說明	值
-ct	SNMPv2 設陷社群名稱	字串（限制在 15 個字元內）。 **附註：** • 含有空格的引數必須括在引號中。引數中不允許前導空格或尾端空格。 • 透過不指定任何引數或將空字串指定為引數（例如 ""），來清除 IMM 聯絡人名稱。
-ci	SNMP 社群 IP 位址/主機名稱	有效的 IP 位址或主機名稱（限制在 63 個字元內）。 **附註：** • IP 位址或主機名稱只能包含點、底線、減號、字母及數字。不允許內含空格或連續句點。 • 透過不指定任何引數，來清除 SNMP 社群 IP 位址或主機名稱。
-cti	SNMPv2 設陷社群 IP 位址/主機名稱	有效的 IP 位址或主機名稱（限制在 63 個字元內）。 **附註：** • IP 位址或主機名稱只能包含點、底線、減號、字母及數字。不允許內含空格或連續句點。 • 透過不指定任何引數，來清除 SNMP 社群 IP 位址或主機名稱。
-eid	SNMP 引擎 ID	字串（限制在 1 至 27 個字元）

語法：

```
snmp [options]
option:
 -a3 state
 -t state
 -l location
 -cn contact_name
 -t1 state
 -c community name
 -ci community IP address/hostname
 -t2 state
 -ct community name
 -cti community IP address/hostname
  -eid engine id
```

範例：

```
system> snmp
-t enabled
-a3 enabled
-l ZhangjiangMansion
-cn Kelvin
-t1 enabled
-c community1
-ci host1
-t2 enabled
-ct community2
-cti host2
-eid XCC-7Z70-DSYM09X
system>
```

snmpalerts 指令

使用此指令可管理透過 SNMP 傳送的警示。

在沒有選項的情況下執行 **snmpalerts** 可顯示所有 SNMP 警示設定。下表顯示各選項的引數。

表格 46. snmpalerts 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-status	SNMP 警示狀態	on、off
-crt	設定會傳送警示的重大事件	all、none、custom:te|vo|po|di|fa|cp|me|in|re|ot 使用格式 **snmpalerts -crt custom:te|vo** 的垂直線區隔的值清單指定自訂嚴重警示設定，其中自訂值為： • te：已超出嚴重溫度臨界值 • vo：已超出嚴重電壓臨界值 • po：嚴重電源故障 • di：硬碟故障 • fa：風扇故障 • cp：微處理器故障 • me：記憶體故障 • in：硬體不相容 • re：電源備援故障 • ot：其他所有重大事件
-crten	傳送重大事件警示	enabled、disabled
-wrn	設定會傳送警示的警告事件	all、none、custom:rp|te|vo|po|fa|cp|me|ot 使用格式 **snmpalerts -wrn custom:rp|te** 的垂直線區隔的值清單指定自訂警告警示設定，其中自訂值為： • rp：電源備援警告 • te：已超出警告溫度臨界值 • vo：已超出警告電壓臨界值 • po：已超出警告電源臨界值 • fa：非重大風扇事件 • cp：微處理器處於欠佳狀態 • me：記憶體警告 • ot：其他所有警告事件
-wrnen	傳送警告事件警示	enabled、disabled
-sys	設定會傳送警示的常式事件	all、none、custom:lo|tio|ot|po|bf|til|pf|el|ne 使用格式 **snmpalerts -sys custom:lo|tio** 的垂直線區隔的值清單指定自訂常式警示設定，其中自訂值為： • lo：遠端登入成功 • tio：作業系統逾時 • ot：其他所有參考和系統事件 • po：系統電源開啟/關閉 • bf：作業系統啟動失敗 • til：作業系統載入器監視器逾時 • pf：預期的故障 (PFA) • el：事件日誌 75% 完整

表格 46. snmpalerts 指令（繼續）

選項	說明	值
		• ne：網路變更
-sysen	傳送常式事件警示	enabled、disabled

語法：
```
snmpalerts [options]
  options:
    -status status
    -crt event_type
    -crten state
    -wrn event_type
    -wrnen state
    -sys event_type
     -sysen state
```

srcfg 指令

使用此指令可指示從序列重新導向模式進入 CLI 的按鍵順序。

若要變更序列重新導向配置，請依次輸入選項和值。若要變更序列重新導向配置，您必須至少具有「配接器網路連線和安全性配置」權限。

附註：IMM 硬體未為序列埠提供序列埠透通功能。因此，不支援 Remote Supervisor Adapter II CLI 中呈現的 `-passthru` 和 `entercliseq` 選項。

在沒有選項的情況下執行 **srcfg** 指令，可顯示現行序列重新導向按鍵順序。下表顯示 `srcfg -entercliseq` 指令選項的引數。

表格 47. srcfg 指令

下表是由一個橫列與三個直欄組成的表格，其中包括選項、選項描述和選項的值資訊。

選項	說明	值
-entercliseq	輸入 CLI 按鍵順序	用於進入 CLI 的使用者定義按鍵順序。 **附註：**此順序必須具有至少一個字元，最多 15 個字元。在此順序中，脫字符號 (^) 具有特殊意義。它表示用於對映至 Ctrl 順序的按鍵 Ctrl（例如，^[表示跳出鍵，^M 表示換行）。出現的所有 ^ 都解譯為 Ctrl 順序的一部分。如需 Ctrl 順序的完整清單，請參閱 ASCII 至按鍵轉換表。此欄位的預設值為 ^[(，它是 Esc 後接 (。

語法：
```
srcfg [options]
options:
-entercliseq entercli_keyseq
```

範例：
```
system> srcfg
-entercliseq ^[Q
system>
```

sshcfg 指令

使用此指令可顯示和配置 SSH 參數。

在沒有選項的情況下執行 **sshcfg** 指令可顯示所有 SSH 參數。下表顯示各選項的引數。

表格 48. sshcfg 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-cstatus	SSH CLI 的狀態	enabled、disabled
-hk gen	產生 SSH 伺服器私密金鑰	
-hk rsa	顯示伺服器 RSA 公開金鑰	

語法：

```
sshcfg [options]
option:
 -cstatus state
 -hk gen
 -hk rsa
```

範例：

```
system> sshcfg
-cstatus enabled
CLI SSH port 22
ssh-rsa 2048 bit fingerprint: b4:a3:5d:df:0f:87:0a:95:f4:d4:7d:c1:8c:27:51:61
1 SSH public keys installed
system>
```

ssl 指令

使用此指令可顯示和配置 SSL 參數。

必須安裝用戶端憑證，才能啟用 SSL 用戶端。在沒有選項的情況下執行 **ssl** 指令可顯示 SSL 參數。下表顯示各選項的引數。

表格 49. ssl 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-ce	啟用或停用 SSL 用戶端	on、off
-se	啟用或停用 SSL 伺服器	on、off
-cime	在 SSL 伺服器上啟用或停用 CIM over HTTPS	on、off

語法：

```
portcfg [options]
 options:
  -ce state
  -se state
   -cime state
```

參數：下列參數會呈現在 **ssl** 指令的選項狀態顯示畫面中，並且僅從 CLI 進行輸出：

啟用伺服器安全傳輸

此狀態顯示是唯讀且無法直接設定。

伺服器 Web/CMD 金鑰狀態
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 伺服器 CSR 金鑰狀態
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 用戶端 LDAP 金鑰狀態
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 用戶端 CSR 金鑰狀態
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

sslcfg 指令

使用此指令可顯示和配置 IMM 適用的 SSL 及管理憑證。

在沒有選項的情況下執行 **sslcfg** 指令，可顯示所有 SSL 配置資訊。**sslcfg** 指令用來產生新的加密金鑰及自簽憑證或憑證簽章要求 (CSR)。下表顯示各選項的引數。

表格 50. sslcfg 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-server	SSL 伺服器狀態	enabled、disabled **附註：**僅在有效憑證就緒時，才能啟用 SSL 伺服器。
-client	SSL 用戶端狀態	enabled、disabled **附註：**僅在有效伺服器或用戶端憑證就緒時，才能啟用 SSL 用戶端。

表格 50. sslcfg 指令（繼續）

選項	說明	值
-cim	CIM over HTTPS 狀態	enabled、disabled **附註：**僅在有效伺服器或用戶端憑證就緒時，才能啟用 CIM over HTTPS。
-cert	產生自簽憑證	server、client、sysdir、storekey **附註：** • 產生自簽憑證時，需要 **-c**、**-sp**、**-cl**、**-on** 及 **-hn** 指令選項的值。 • 產生自簽憑證時，**-cp**、**-ea**、**-ou**、**-s**、**-gn**、**-in** 及 **-dq** 指令選項的值是選用的。
-csr	產生 CSR	server、client、sysdir、storekey **附註：** • 產生 CSR 時，需要 **-c**、**-sp**、**-cl**、**-on** 及 **-hn** 指令選項的值。 • 產生 CSR 時，**-cp**、**-ea**、**-ou**、**-s**、**-gn**、**-in**、**-dq**、**-cpwd** 及 **-un** 指令選項的值是選用的。
-i	TFTP/SFTP 伺服器的 IP 位址	有效的 IP 位址 **附註：**在上傳憑證，或下載憑證或 CSR 時，必須指定 TFTP 或 SFTP 伺服器的 IP 位址。
-pn	TFTP/SFTP 伺服器的埠號	有效的埠號（預設值 69/22）
-u	SFTP 伺服器的使用者名稱	有效的使用者名稱
-pw	SFTP 伺服器的密碼	有效的密碼
-l	憑證檔名	有效的檔名 **附註：**下載或上傳憑證或 CSR 時需要檔名。如果未為下載指定任何檔名，則使用及顯示檔案的預設名稱。
-dnld	下載憑證檔案	此選項未採用任何引數；但也必須指定 **-cert** 或 **-csr** 指令選項的值（視要下載的憑證類型而定）。此選項未採用任何引數；但也必須指定 **-i** 指令選項和 **-l**（選用）指令選項的值。
-upld	匯入憑證檔案	此選項未採用任何引數；但也必須指定 **-cert**、**-i** 及 **-l** 指令選項的值。
-tc**x**	SSL 用戶端的授信憑證 **x**	import、download、remove **附註：**在指令選項中，授信憑證號碼 (**x**) 指定為 1 至 3 的整數。
-c	國家/地區	國碼（2 個字母） **附註：**產生自簽憑證或 CSR 時需要。
-sp	州/省（縣/市）	引號定界的字串（最多 60 個字元） **附註：**產生自簽憑證或 CSR 時需要。
-cl	鄉鎮/市區	引號定界的字串（最多 50 個字元） **附註：**產生自簽憑證或 CSR 時需要。
-on	組織名稱	引號定界的字串（最多 60 個字元） **附註：**產生自簽憑證或 CSR 時需要。
-hn	IMM 主機名稱	字串（最多 60 個字元） **附註：**產生自簽憑證或 CSR 時需要。
-cp	聯絡人	引號定界的字串（最多 60 個字元） **附註：**產生自簽憑證或 CSR 時選用。
-ea	聯絡人電子郵件位址	有效的電子郵件位址（最多 60 個字元） **附註：**產生自簽憑證或 CSR 時選用。
-ou	組織單位	引號定界的字串（最多 60 個字元） **附註：**產生自簽憑證或 CSR 時選用。

表格 50. sslcfg 指令（繼續）

選項	說明	值
-s	姓氏	引號定界的字串（最多 60 個字元） **附註：**產生自簽憑證或 CSR 時選用。
-gn	名字	引號定界的字串（最多 60 個字元） **附註：**產生自簽憑證或 CSR 時選用。
-in	姓名縮寫	引號定界的字串（最多 20 個字元） **附註：**產生自簽憑證或 CSR 時選用。
-dq	網域名稱限定元	引號定界的字串（最多 60 個字元） **附註：**產生自簽憑證或 CSR 時選用。
-cpwd	盤查密碼	字串（最少 6 個字元，最多 30 個字元） **附註：**產生 CSR 時選用。
-un	未結構化的名稱	引號定界的字串（最多 60 個字元） **附註：**產生 CSR 時選用。

語法：

```
sslcfg [options]
option:
 -server state
 -client state
 -cim state
 -cert certificate_type
 -csr certificate_type
 -i ip_address
 -pn port_number
 -u username
 -pw password
 -l filename
 -dnld
 -upld
 -tc xaction
 -c country_code
 -sp state_or_province
 -cl city_or_locality
 -on organization_name
 -hn bmc_hostname
 -cp contact_person
 -ea email_address
 -ou organizational_unit
 -s surname
 -gn given_name
 -in initials
 -dq dn_qualifier
 -cpwd challenge_password
  -un unstructured_name
```

範例：

```
system> sslcfg
-server enabled
-client disabled
-sysdir enabled
SSL Server Certificate status:
 A self-signed certificate is installed
SSL Client Certificate status:
 A self-signed certificate is installed
```

```
SSL CIM Certificate status:
 A self-signed certificate is installed
SSL Client Trusted Certificate status:
 Trusted Certificate 1: Not available
 Trusted Certificate 2: Not available
 Trusted Certificate 3: Not available
 Trusted Certificate 4: Not available
```

用戶端憑證範例：

- 若要產生儲存金鑰的 CSR，請輸入下列指令：
  ```
  system> sslcfg
  -csr storekey -c US -sp NC -cl rtp -on Lenovo -hn XCC-5cf3fc6e0c9d
  -cp Contact -ea "" -ou""
  ok
  ```

由於空間限制，上述範例會顯示在數行中。

- 如果要從 IMM 將憑證下載至其他伺服器，請輸入下列指令：
  ```
  system> sslcfg
  -csr storekey -dnld -i 192.168.70.230 -l storekey.csr
  ok
  ```
- 若要上傳憑證管理中心 (CA) 處理的憑證，請輸入下列指令：
  ```
  system> sslcfg
  -cert storekey -upld -i 192.168.70.230 -l tklm.der
  ```
- 若要產生自簽憑證，請輸入下列指令：
  ```
  system> sslcfg
  -cert storekey -c US -sp NC -cl rtp -on Lenovo -hn XCC-5cf3fc6e0c9d
  -cp Contact -ea "" -ou "
  ok
  ```
  由於空間限制，上述範例會顯示在數行中。

SKLM 伺服器憑證範例：

- 若要匯入 SKLM 伺服器憑證，請輸入下列指令：
  ```
  system> storekeycfg
  -add -ip 192.168.70.200 -f tklm-server.der
  ok
  ```

storekeycfg 指令

使用此指令可配置 SKLM 伺服器的主機名稱或 IP 位址和網路埠。

您最多可以配置四個 SKLM 伺服器目標。**storekeycfg** 指令也可以用來安裝及移除 IMM 用於鑑別 SKLM 伺服器的憑證。

下表顯示各選項的引數。

表格 51. storekeycfg 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

表格 51. storekeycfg 指令（繼續）

選項	說明	值
-add	新增啟動金鑰	值為 -ip、-pn、-u、-pw 和 -f 指令選項
-ip	TFTP/SFTP 伺服器的主機名稱或 IP 位址	TFTP/SFTP 伺服器的有效主機名稱或 IP 位址
-pn	TFTP 或 SFTP 伺服器的埠號	TFTP/SFTP 伺服器的有效埠號（預設值為 69/22）
-u	SFTP 伺服器的使用者名稱	SFTP 伺服器的有效使用者名稱
-pw	SFTP 伺服器的密碼	SFTP 伺服器的有效密碼
-f	啟動金鑰的檔名	啟動金鑰檔名的有效檔名
-del	使用此指令可依索引號碼刪除啟動金鑰	keycfg 清單中的有效啟動金鑰索引號碼
-dgrp	新增裝置群組	裝置群組名稱
-sxip	新增 SKLM 伺服器的主機名稱或 IP 位址	SKLM 伺服器的有效主機名稱或 IP 位址。數值 1、2、3 或 4。
-sxpn	新增 SKLM 伺服器的埠號	SKLM 伺服器的有效埠號。數值 1、2、3 或 4。
-testx	測試 SKLM 伺服器的配置和連線	數值 1、2、3 或 4
-h	顯示指令用法和選項	

語法：

```
storekeycfg [options]
 options:
  -add state
  -ip ip_address
  -pn port_number
  -u username
  -pw password
  -f filename
  -del key_index
  -dgrp device_group_name
  -sxip ip_address
  -sxpn port_number
  -testx numeric value of SKLM server
  -h
```

範例：

若要匯入 SKLM 伺服器憑證，請輸入下列指令：

```
system> storekeycfg
add -ip 192.168.70.200 -f tklm-server.der
system> ok
```

若要配置 SKLM 伺服器位址和埠號，請輸入下列指令：

```
system> storekeycfg
-s1ip 192.168.70.249
system> ok
```

若要設定裝置群組名稱，請輸入下列指令：

```
system> storekeycfg
-dgrp IBM_SYSTEM_X_SED
```

```
system> ok
```

syncrep 指令

使用此指令可從遠端儲存庫啟動韌體同步。

下表顯示各選項的引數。

表格 52. syncrep 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-t	連接儲存庫的通訊協定	samba、nfs
-l	遠端儲存庫的位置	使用 URL 格式
-u	使用者	
-p	密碼	
-o	選項	samba 和 nfs 裝載的額外選項字串
-d	網域	samba 裝載的網域
-q	查詢目前更新狀態	
-c	取消同步程序	

語法

```
syncrep [options]  Launch firmware sync from remote repository
 options:
    -t <samba|nfs> protocol to connect repository
    -l location of remote repository (URL format)
    -u User
    -p Password
    -o option (extra option string for samba and nfs mounts)
    -d domain (domain for samba mount)
    -q query current update status
    -c cancel the sync process
```

範例

```
(1) start sync with repository
system> syncrep -t samba -l url -u user -p password
(2) query current update status
system> syncrep -q
(3)cancel the sync process
system> syncrep -c
```

thermal 指令

使用此指令可顯示和配置主機系統的散熱模式原則。

在沒有選項的情況下執行 **thermal** 指令可顯示散熱模式原則。下表顯示各選項的引數。

表格 53. thermal 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

表格 53. thermal 指令（繼續）

選項	說明	值
-mode	散熱模式選項	normal、performance、minimal、efficiency、custom
-table	供應商、裝置 ID 及替代散熱表	

語法：
```
thermal [options]
option:
 -mode thermal_mode
 -table vendorID_devicetable_number
```

範例：
```
system> thermal
-mode normal
-table 80860126 1 10DE0DFA 3
system>
```

timeouts 指令

使用此指令可顯示或變更逾時值。

- 若要顯示逾時，請輸入 timeouts。
- 若要變更逾時值，請依次輸入選項和值。
- 若要變更逾時值，您必須至少具有「配接器配置」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。

表格 54. timeouts 指令

下表是由多個橫列與四個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	逾時	單位	值
-f	關閉電源延遲	分鐘	disabled、0.5、1、2、3、4、5、7.5、10、15、20、30、60、120
-l	載入器逾時	分鐘	disabled、0.5、1、1.5、2、2.5、3、3.5、4、4.5、5、7.5、10、15、20、30、60、120
-o	作業系統逾時	分鐘	disabled、2.5、3、3.5、4
-s	含有硬體錯誤的 OS 失敗畫面擷取	/	disabled、enabled

語法：
```
timeouts [options]
options:
-f power_off_delay_watchdog_option
-o OS_watchdog_option
-l loader_watchdog_option
-s OS failure screen capture with HW error
```

範例：
```
system> timeouts
-o disabled
```

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

tls 指令

使用此指令可設定最低 TLS 層級。

下表顯示各選項的引數。

表格 55. tls 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-min	選取最低 TLS 層級	1.0, 1.1, 1.2[1], 1.3
-h	列出用法和選項	
附註： 1. 當加密模式設定為 NIST-800-131A 相符性模式，TLS 版本必須設定為 1.2。		

用法：

```
tls [-options] - configures the minimum TLS level
  -min <1.0 | 1.1 | 1.2 | 1.3> - Selects the minimum TLS level
  -h - Lists usage and options
```

範例：

若要取得 tls 指令的用法，請發出下列指令：

```
system> tls
-h
system>
```

若要取得現行 tls 版本，請發出下列指令：

```
system> tls
-min 1.2
system>
```

若要將現行 tls 版本變更為 1.2，請發出下列指令：

```
system> tls
-min 1.2
ok
system>
```

trespass 指令

使用此指令可配置和顯示侵害訊息。

trespass 指令可用來配置和顯示侵害訊息。侵害訊息將透過 Web 或 CLI 介面顯示給所有登入的使用者。

下表顯示各選項的引數。

表格 56. uefipw 指令

下表是由多個橫列與兩個直欄組成的表格，其中包含選項及選項說明。

選項	說明
-s	配置侵害訊息
-h	列出用法和選項

語法：

```
usage:
  trespass display the trespass message
  -s <trespass message> configure trespass message
  -h - Lists usage and options
```

範例：

附註：侵害訊息不包含任何空格。

```
system> trespass -s testingmessage
ok
system> trespass
testingmessage

The trespass message contains spaces:
system> trespass -s "testing message"
ok
system> trespass
testing message
```

uefipw 指令

使用此指令可配置 UEFI 管理者密碼。密碼是唯寫的。

uefipw 指令可以與「-p」選項搭配使用來配置 XCC 的 UEFI 管理者密碼，也可以與 LXCA 的「-ep」選項搭配用於透過 CLI 介面配置 UEFI 管理者密碼。密碼是唯寫的。

下表顯示各選項的引數。

表格 57. uefipw 指令

下表是由多個橫列與兩個直欄組成的表格，其中包含選項及選項說明。

選項	說明
-cp	目前密碼（限制在 20 個字元內）
-p	新密碼（限制在 20 個字元內）
-cep	加密目前密碼
-ep	加密新密碼

語法：

```
usage:
  uefipw [-options] - Configure the UEFI admin password
options:
```

```
-cp    - current password (limited to 20 characters)
-p     - new password (limited to 20 characters)
-cep   - current password encrypted
-ep    - new password encrypted
```

usbeth 指令

使用此指令可啟用或停用頻內 LAN over USB 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
```

usbfp 指令

使用此指令可控制 BMC 使用前方面板 USB 埠的方式

下表顯示各選項的引數。

表格 58. usbfp 指令

下表是由多個橫列與兩個直欄組成的表格，其中包含選項及選項說明。

選項	說明
-mode <bmc | server | shared>	將使用模式設定為 BMC、伺服器或共用
-it <minutes>	以分鐘為單位的閒置逾時（共用模式）
-btn <on | off>	允許使用 ID 按鈕來切換擁有者（共用模式）
-own <bmc | server >	將擁有者設定為 bmc 或伺服器（共用模式）

users 指令

使用此指令可存取所有使用者帳戶及其權限層級。

users 指令也用於建立新的使用者帳戶和修改現有帳戶。在沒有選項的情況下執行 **users** 指令可顯示使用者清單和部分基本使用者資訊。下表顯示各選項的引數。

表格 59. users 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-user_index	使用者帳戶索引編號	1（含）至 12（含），或 all（對於所有使用者）。
-n	使用者帳戶名稱	僅包含數字、字母、句點及底線的唯一字串。最少 4 個字元，最多 16 個字元。

表格 59. users 指令（繼續）

選項	說明	值
-p	使用者帳戶密碼	包含至少一個英文字母和一個非英文字母的字串。最少 6 個字元，最多 20 個字元。空值會建立沒有密碼的帳戶，使用者在第一次登入期間必須設定密碼。
-a	權限層級	權限層級可以是下列其中一個層級： • super（監督者） • ro（唯讀） • 下列值的任意組合（以 | 區隔）： — am（使用者帳戶管理存取） — rca（遠端主控台存取） — rcvma（遠端主控台及虛擬媒體存取） — pr（遠端伺服器電源/重新啟動存取） — cel（清除事件日誌的能力） — bc（配接器配置 [基本]） — nsc（配接器配置 [網路和安全性]） — ac（配接器配置 [進階]）
-ep	加密密碼（用於備份/還原）	有效的密碼
-clear	消除指定的使用者帳戶 如果您獲得授權，您可以移除自己的帳戶或其他使用者的帳戶（即使他們目前已登入），除非這是剩下唯一具有「使用者帳戶管理」權限的帳戶。刪除使用者帳戶時已在進行中的階段作業將不會自動終止。	必須遵循下列格式指定要消除的使用者帳戶索引編號： users -clear -**user_index**
-curr	顯示目前登入的使用者	
-sauth	SNMPv3 鑑別通訊協定	HMAC-SHA、none
-spriv	SNMPv3 保密通訊協定	CBC-DES、AES、none
-spw	SNMPv3 保密密碼	有效的密碼
-sepw	SNMPv3 保密密碼（已加密）	有效的密碼
-sacc	SNMPv3 存取類型	get、set
-strap	SNMPv3 設陷主機名稱	有效的主機名稱
-pk	顯示使用者的 SSH 公開金鑰	使用者帳戶索引編號。 **附註：** • 顯示指派給使用者的每一個 SSH 金鑰，以及識別金鑰索引編號。 • 使用 SSH 公開金鑰選項時，必須在使用者索引（-**userindex** 選項）之後使用 -pk 選項，格式為：users -2 -pk。 • 所有金鑰採用 OpenSSH 格式。 • 對於 Flex 節點，使用者指令僅限用於本端 IPMI 和 SNMP 帳戶。Flex 系統不支援 -pk 選項。

表格 59. users 指令（繼續）

選項	說明	值
-e	以 OpenSSH 格式顯示整個 SSH 金鑰 **（SSH 公開金鑰選項）**	此選項未採用任何引數，且必須使用此選項，不包括所有其他 users -pk 選項。 **附註：**使用 SSH 公開金鑰選項時，必須在使用者索引（-**userindex** 選項）之後使用 -pk 選項，格式為：users -2 -pk -e。
-remove	從使用者移除 SSH 公開金鑰 **（SSH 公開金鑰選項）**	必須提供要移除的公開金鑰索引編號作為特定的 -**key_index** 或 -all（對於指派給使用者的所有金鑰）。 **附註：** • 使用 SSH 公開金鑰選項時，必須在使用者索引（-**userindex** 選項）之後使用 -pk 選項，格式為：users -2 -pk -remove -1。 • 對於 Flex 節點，使用者指令僅限用於本端 IPMI 和 SNMP 帳戶。Flex 系統不支援 -remove 選項。
-add	新增使用者的 SSH 公開金鑰 **（SSH 公開金鑰選項）**	OpenSSH 格式的引號定界金鑰 **附註：** • 使用 -add 選項，不包括所有其他 users -pk 指令選項。 • 使用 SSH 公開金鑰選項時，必須在使用者索引（-**userindex** 選項）之後使用 -pk 選項，格式為：users -2 -pk -add "AAAAB3NzC1yc2EAAAABIwAAAQEAvfnTUzRF7pdBuaBy4dO/aIFasa/Gtc+o/wlZnuC4aDHMA1UmnMyLOCiIaNOy4OOICEKCqjKEhrYymtAoVtfKApvY39GpnSGRC/qcLGWLM4cmirKL5kxHNOqIcwbT1NPceoKHj46X7E+mqlfWnAhhjDpcVFjagM3Ek2y7w/tBGrwGgN7DPHJU1tzcJy68mEAnIrzjUoR98Q3/B9cJD77ydGKe8rPdI2hIEpXR5dNUiupA1Yd8PSSMgdukASKEd3eRRZTBl3SAtMucUsTkYjlXcqex1OQz4+N5OR6MbNcwlsx+mTEAvvcpJhuga7OUNPGhLJMl6k7jeJiQ8Xd2p XbOZQ==" • 對於 Flex 節點，使用者指令僅限用於本端 IPMI 和 SNMP 帳戶。Flex 系統不支援 -add 選項。
-upld	上傳 SSH 公開金鑰 **（SSH 公開金鑰選項）**	需要 -i 和 -l 選項以指定金鑰位置。 **附註：** • 使用 -upld 選項，不包括所有其他 users -pk 指令選項（-i 和 -l 除外）。 • 若要用新金鑰取代某個金鑰，您必須指定 -**key_index**。若要在現行金鑰清單結尾新增金鑰，請勿指定金鑰索引。 • 使用 SSH 公開金鑰選項時，必須在使用者索引（-**userindex** 選項）之後使用 -pk 選項，格式為：users -2 -pk -upld -i tftp://9.72.216.40/ -l file.key。 • 對於 Flex 節點，使用者指令僅限用於本端 IPMI 和 SNMP 帳戶。Flex 系統不支援 -upld 選項。
-dnld	下載指定的 SSH 公開金鑰 **（SSH 公開金鑰選項）**	需要 -**key_index** 以指定要下載的金鑰，及需要 -i 和 -l 選項以指定其他執行 TFTP 伺服器電腦上的下載位置。 **附註：** • 使用 -dnld 選項，不包括所有其他 users -pk 指令選項（-i、-l 和 -**key_index** 除外）。 • 使用 SSH 公開金鑰選項時，必須在使用者索引（-**userindex** 選項）之後使用 -pk 選項，格式為：users -2 -pk -dnld -1 -i tftp://9.72.216.40/ -l file.key。
-i	用於上傳或下載金鑰檔的 TFTP/SFTP 伺服器 IP 位址 **（SSH 公開金鑰選項）**	有效的 IP 位址 **附註：**users -pk -upld 和 users -pk -dnld 指令選項需要 -i 選項。

表格 59. users 指令（繼續）

選項	說明	值
-pn	TFTP/SFTP 伺服器的埠號 **（SSH 公開金鑰選項）**	有效的埠號（預設值 69/22） **附註：**users -pk -upld 和 users -pk -dnld 指令選項的選用參數。
-u	SFTP 伺服器的使用者名稱 **（SSH 公開金鑰選項）**	有效的使用者名稱 **附註：**users -pk -upld 和 users -pk -dnld 指令選項的選用參數。
-pw	SFTP 伺服器的密碼 **（SSH 公開金鑰選項）**	有效的密碼 **附註：**users -pk -upld 和 users -pk -dnld 指令選項的選用參數。
-l	透過 TFTP 或 SFTP 上傳或下載金鑰檔的檔名 **（SSH 公開金鑰選項）**	有效的檔名 **附註：**users -pk -upld 和 users -pk -dnld 指令選項需要 -l 選項。
-af	接受來自主機的連線 **（SSH 公開金鑰選項）**	以逗點區隔的主機名稱和 IP 位址清單（限制在 511 個字元內）。有效的字元包括：英數、逗點、星號、問號、驚嘆號、句點、連字號、冒號及百分比符號。
-cm	註解 **（SSH 公開金鑰選項）**	引號定界的字串（最多 255 個字元）。 **附註：**使用 SSH 公開金鑰選項時，必須在使用者索引（**-userindex** 選項）之後使用 -pk 選項，格式為：users -2 -pk -cm "This is my comment."。

語法：

```
users [-options] - display/configure user accounts
options:
  -[1-12] - user account number
  -l    - display password expiration days
  -n    - username (limited to 16 characters)
  -p    - password (limited to 32 characters)
  -shp   - set hashpassword (total 64 characters)
  -ssalt  - set salt (limited to 64 characters)
  -ghp   - get hashpassword
  -gsalt  - get salt
  -ep    - encrypted password (used with backup/restore )

  -a    - authority level (super, ro, custom:am|rca|rcvma|pr|cel|bc|nsc|ac)
    -am   - User account management access
    -rca  - Remote console access
    -rcvma - Remote console and remote disk (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)

  -clear  - clear user account
  -curr   - display current users
  -sauth  (none|HMAC-SHA)       - snmpv3 authentication protocol
  -spriv  (none|CBC-DES|AES)     - snmpv3 privacy protocol
  -spw   password           - snmpv3 privacy password
  -sepw   encryptedpassword      - snmpv3 privacy password (encrypted)
  -sacc  (Get)          - snmpv3 Access type
  -strap  hostname           - snmpv3 trap hostname

  -pk    - SSH public keys options:
    -e     - Displays the entire key in OpenSSH format
    -remove  - Removes the specified key for the specified user
    -add    - Adds a public key for the specified user
    -upld   - Used to upload a public key in OpenSSH/RFC4716 format
```

```
    -dnld   - Used to download the specified public key to a TFTP/SFTP server
    -i    - IP address of the TFTP/SFTP
    -pn    - port number of tftp/sftp server (default 69/22)
    -u    - username for sftp server
    -pw    - password for sftp server
    -l    - Filename of the key file when uploading or downloading via TFTP/SFTP
    -af    - accept connections from host, in the format: from="<list>", where
           <list> is a comma-separated list of hostnames and IP addresses
           (limited to 511 characters)
    -cm    - comment (limited to 255 characters, must be quote-delimited)
```

附註：-a 自訂權限旗標可以任意組合使用。

範例：

```
system> users
 Account    Login ID    Advanced Attribute        Role       Password Expires
 -------    --------    ------------------       ------      ----------------
   1       USERID           Native          Administrator          89 day(s)
system> users -2 -n sptest -p PasswOrd12 -a super
The user is required to change the password when the user logs in to the management server for the first time
ok
system> users
 Account    Login ID    Advanced Attribute       Role        Password Expires
 -------    --------    ------------------      ------       ----------------
   1       USERID           Native       Administrator           90 day(s)
2       sptest           Native          Administrator       Password expired
system> hashpw -sw enabled -re enabled
system> users -5 -n guest5 -shp 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee -ssalt abc -a super
system> users -5 ghp
292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
system> users -5 gsalt
abc
system> users -2 -n sptest -p PasswOrd12 -a custom:am|rca
The user is required to change the password when the user logs in to the management server for the first time
ok
```

IMM 控制指令

本主題提供按字母順序排序的 IMM 控制 CLI 指令清單。

目前有 7 個 IMM 控制指令：

alertentries 指令

使用此指令可管理警示接收者。

- **alertentries** 在沒有選項的情況下，可顯示所有警示項目設定。
- **alertentries -number -test** 可為給定的接收者索引編號產生測試警示。
- **alertentries -number**（其中號碼為 0 - 12）可為指定的接收者索引編號顯示警示項目設定，或可讓您修改該接收者的警示設定。

下表顯示各選項的引數。

表格 60. alertentries 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

表格 60. alertentries 指令（繼續）

選項	說明	值
-number	要顯示、新增、修改或刪除的警示接收者索引編號	1 至 12
-status	警示接收者狀態	on、off
-type	警示類型	email、syslog
-log	將事件日誌包括在警示電子郵件中	on、off
-n	警示接收者名稱	字串
-e	警示接收者電子郵件位址	有效的電子郵件位址
-ip	Syslog IP 位址或主機名稱	有效的 IP 位址或主機名稱
-pn	Syslog 埠號	有效的埠號
-del	刪除指定的接收者索引編號	
-test	為指定的接收者索引編號產生測試警示	
-crt	設定會傳送警示的重大事件	all、none、custom:te|vo|po|di|fa|cp|me|in|re|ot 使用格式 **alertentries -crt custom:te|vo** 的垂直線區隔的值清單指定自訂嚴重警示設定，其中自訂值為： • te：已超出嚴重溫度臨界值 • vo：已超出嚴重電壓臨界值 • po：嚴重電源故障 • di：硬碟故障 • fa：風扇故障 • cp：微處理器故障 • me：記憶體故障 • in：硬體不相容 • re：電源備援故障 • ot：其他所有重大事件
-crten	傳送重大事件警示	enabled、disabled
-wrn	設定會傳送警示的警告事件	all、none、custom:rp|te|vo|po|fa|cp|me|ot 使用格式 **alertentries -wrn custom:rp|te** 的垂直線區隔的值清單指定自訂警告警示設定，其中自訂值為： • rp：電源備援警告 • te：已超出警告溫度臨界值 • vo：已超出警告電壓臨界值 • po：已超出警告電源臨界值 • fa：非重大風扇事件 • cp：微處理器處於欠佳狀態 • me：記憶體警告 • ot：其他所有警告事件
-wrnen	傳送警告事件警示	enabled、disabled

表格 60. alertentries 指令（繼續）

選項	說明	值
-sys	設定會傳送警示的常式事件	all、none、custom:lo|tio|ot|po|bf|til|pf|el|ne 使用格式 **alertentries –sys custom:lo|tio** 的垂直線區隔的值清單指定自訂常式警示設定，其中自訂值為： • lo：遠端登入成功 • tio：作業系統逾時 • ot：其他所有參考和系統事件 • po：系統電源開啟/關閉 • bf：作業系統啟動失敗 • til：作業系統載入器監視器逾時 • pf：預期的故障 (PFA) • el：事件日誌 75% 完整 • ne：網路變更
-sysen	傳送常式事件警示	enabled、disabled

語法：

```
alertentries [options]
 options:
 -number recipient_number
   -status status
   -type alert_type
   -log include_log_state
   -n recipient_name
   -e email_address
   -ip ip_addr_or_hostname
   -pn port_number
   -del
   -test
   -crt event_type
   -crten state
   -wrn event_type
   -wrnen state
   -sys event_type
    -sysen state
```

範例：

```
system> alertentries
1. test
2. <not used>
3. <not used>
4. <not used>
5. <not used>
6. <not used>
7. <not used>
8. <not used>
9. <not used>
10. <not used>
11. <not used>
12. <not used>

system> alertentries -1
-status off
-log off
```

```
-n test
-e test@mytest.com
-crt all
-wrn all
-sys none
system>
```

batch 指令

使用此指令可執行包含在檔案中的一個或多個 CLI 指令。

- 批次檔中的備註行以 # 開頭。
- 執行批次檔時，會隨失敗回覆碼傳回失敗的指令。
- 包含無法辨識指令選項的批次檔指令可能會產生警告。

下表顯示各選項的引數。

表格 61. batch 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-f	批次檔名稱	有效的檔名
-ip	TFTP/SFTP 伺服器的 IP 位址	有效的 IP 位址
-pn	TFTP/SFTP 伺服器的埠號	有效的埠號（預設值 69/22）
-u	SFTP 伺服器的使用者名稱	有效的使用者名稱
-pw	SFTP 伺服器的密碼	有效的密碼

語法：

```
batch [options]
option:
 -f filename
 -ip ip_address
 -pn port_number
 -u username
  -pw password
```

範例：

```
system> batch -f sslcfg.cli -ip 192.168.70.200
1 : sslcfg client dnld ip 192.168.70.20
Command total/errors/warnings: 8 / 1 / 0
system>
```

clearcfg 指令

使用此指令可將 IMM 配置設定為其原廠預設值。

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 的配置之後，將會重新啟動 IMM。

clock 指令

使用此指令可顯示目前的日期和時間。您可以設定 UTC 偏移和日光節約時間設定

BMC 從主機伺服器或 NTP 伺服器取得時間。

從主機取得的時間可能是當地時間或 UTC 時間。如果未使用 NTP 且主機使用 UTC 格式，主機選項應設定為 UTC。若為正偏移，則 UTC 偏移格式可以是 +0200、+2:00、+2 或 2；若為負偏移，則其格式可以是 -0500、-5:00 或 -5。UTC 偏移和日光節約時間是搭配 NTP 使用，或主機模式為 UTC 時使用。

若 UTC 偏移為 +2、-7、-6、-5、-4 和 -3，則需要設定特殊日光節約時間。

- 若為 +2，則日光節約時間選項如下：off（關閉）、ee（歐洲東部）、tky（土耳其）、bei（貝魯特）、amm（安曼）、jem（耶路撒冷）。
- 若為 -7，則日光節約時間設定如下：off（關閉）、mtn（山區）、maz（馬薩特蘭）。
- 若為 -6，則日光節約時間設定如下：off（關閉）、mex（墨西哥）、cna（中北美洲）。
- 若為 -5，則日光節約時間設定如下：off（關閉）、cub（古巴）、ena（東北美洲）。
- 若為 -4，則日光節約時間設定如下：off（關閉）、asu（亞松森）、cui（庫亞巴）、san（聖地牙哥）、cat（加拿大 - 大西洋）。
- 若為 -3，則日光節約時間設定如下：off（關閉）、gtb（哥特哈布）、bre（巴西 - 東部）。

語法：
```
clock [options]
options:
-u UTC offset
-dst on/off/special case
-host - local | utc , format of time obtained from host (default: utc)
Windows systems use local, Linux uses utc
```

範例：
```
system> clock
12/12/2011 13:15:23 GMT-5:00 dst on
```

identify 指令

使用此指令可亮起或熄滅機箱識別 LED，或使其閃爍。

-d 選項可與 **-s on** 選項搭配使用以開啟 LED，不過只能維持 **-d** 選項所指定的秒數。該秒數結束後，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>
```

info 指令

使用此指令可顯示和配置 IMM 的相關資訊。

在沒有選項的情況下執行 **info** 指令，可顯示所有 IMM 位置和聯絡資訊。下表顯示各選項的引數。

表格 62. info 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

表格 62. info 指令（繼續）

選項	說明	值
-name	IMM 名稱	字串
-contact	IMM 聯絡人的名稱	字串
-location	IMM 位置	字串
-room[1]	IMM 會議室 ID	字串
-rack[1]	IMM 機架 ID	字串
-rup[1]	機架中 IMM 的位置	字串
-ruh	機架裝置高度	唯讀
-bbay	刀鋒伺服器機槽位置	唯讀
1. 如果 IMM 位於 Flex System 中，則值為唯讀，且無法重設。		

語法：

```
info [options]
option:
 -name xcc_name
 -contact contact_name
 -location xcc_location
 -room room_id
 -rack rack_id
 -rup rack_unit_position
 -ruh rack_unit_height
  -bbay blade_bay
```

spreset 指令

使用此指令可重新啟動 IMM。

您必須至少具有「進階配接器配置」權限才能發出此指令。

無代理程式指令

本主題提供按字母順序排序的無代理程式指令清單。

目前有 3 個 無代理程式指令：

storage 指令

使用此指令可顯示和配置（如果平台支援）由 IMM 管理之伺服器儲存裝置的相關資訊。

下表顯示各選項的引數。

表格 63. storage 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

表格 63. storage 指令（繼續）

選項	說明	值
-list	列出由 IMM 管理的儲存體目標。	**controllers|pools|volumes|drives** 其中 **target** 為： • **controllers**：列出所支援的 RAID 控制器[1] • **pools**：列出與 RAID 控制器相關聯的儲存區[1] • **volumes**：列出與 RAID 控制器相關聯的儲存磁區[1] • **drives**：列出與 RAID 控制器相關聯的儲存硬碟[1]
-list -target **target_id**	根據 **target_id**，列出由 IMM 管理的儲存體**目標**。	**pools|volumes|drives ctrl[x]|pool[x]** 其中 **target** 和 **target_id** 是： • **pools ctrl[x]**：根據 target_id，列出與 RAID 控制器相關聯的儲存區[1] • **volumes ctrl[x]|pool[x]**：根據 target_id，列出與 RAID 控制器相關聯的儲存磁區[1] • **drives ctrl[x]|pool[x]**：根據 target_id，列出與 RAID 控制器相關聯的儲存硬碟[1]
-list flashdimms	列出由 IMM 管理的快閃記憶體 DIMM。	
-list devices	顯示由 IMM 管理的所有磁碟和快閃記憶體 DIMM 的狀態。	
-show **target_id**	顯示由 IMM 管理之選定目標的資訊。	其中 **target_id** 為： **ctrl[x]|vol[x]|disk[x]|pool[x]** **|flashdimm[x]** [3]
-show **target_id** info	顯示由 IMM 管理之選定目標的詳細資訊。	其中 **target_id** 為： **ctrl[x]|vol[x]|disk[x]|pool[x]** **|flashdimm[x]** [3]
-show **target_id firmware**[3]	顯示由 IMM 管理之選定目標的韌體資訊。	其中 **target_id** 為： **ctrl[x]|disk[x]|flashdimm[x]**[2]
-showlog **target_id<m:n|all>**[3]	顯示由 IMM 管理之選定目標的事件日誌。	其中 **target_id** 為：**ctrl[x]**[4] **m:n|all** 其中 **m:n** 是一到事件日誌數目上限 其中 **all** 是所有事件日誌
-config ctrl -scanforgn -target **target_id**[3]	偵測外部 RAID 配置。	其中 **target_id** 為：**ctrl[x]**[5]
-config ctrl -imptforgn -target **target_id**[3]	匯入外部 RAID 配置。	其中 **target_id** 為：**ctrl[x]**[5]
-config ctrl -clrforgn -target **target_id**[3]	清除外部 RAID 配置。	其中 **target_id** 為：**ctrl[x]**[5]
-config ctrl -clrcfg -target **target_id**[3]	清除 RAID 配置。	其中 **target_id** 為：**ctrl[x]**[5]

表格 63. storage 指令（繼續）

選項	說明	值
-config drv -mkoffline -target **target_id**[3]	將硬碟狀態從線上變更為離線。	其中 **target_id** 為：**disk[x]**[5]
-config drv -mkonline -target **target_id**[3]	將硬碟狀態從離線變更為線上。	其中 **target_id** 為：**disk[x]**[5]
-config drv -mkmissing -target **target_id**[3]	將離線硬碟標示為未配置的良好硬碟。	其中 **target_id** 為：**disk[x]**[5]
-config drv -prprm -target **target_id**[3]	準備未配置的良好硬碟以進行移除。	其中 **target_id** 為：**disk[x]**[5]
-config drv -undoprprm -target **target_id**[3]	取消準備未配置的良好硬碟以進行移除的作業。	其中 **target_id** 為：**disk[x]**[5]
-config drv -mkbad -target **target_id**[3]	將未配置的良好硬碟變更為未配置的不良硬碟。	其中 **target_id** 為：**disk[x]**[5]
-config drv -mkgood -target **target_id**[3]	將未配置的不良硬碟變更為未配置的良好硬碟。 或 將集束磁碟 (JBOD) 硬碟轉換成未配置的良好硬碟。	其中 **target_id** 為：**disk[x]**[5]
-config drv -addhsp -**[dedicated pools]** -target **target_id**[3]	將選定硬碟指派給一個控制器或現有儲存區，做為緊急備用。	其中 **target_id** 為：**disk[x]**[5]
-config drv -rmhsp -target **target_id**[3]	移除緊急備用。	其中 **target_id** 為：**disk[x]**[5]
-config vol -remove -target **target_id**[3]	移除一個磁區。	其中 **target_id** 為：**vol[x]**[5]
-config vol -set [-N] [-w] [-r] [-i] [-a] [-d] [-b] -target **target_id**[3]	修改一個磁區的內容。	• [-N **volume_name**] 是磁區的名稱 • [-w **<0|1|2>**] 是快取寫入原則： — 類型 **0** 為「直接寫入」原則 — 類型 **1** 為「寫回」原則 — 類型 **2** 為「以備用電池組件 (BBU) 寫入」原則 • [-r **<0|1|2>**] 為快取讀取原則： — 類型 **0** 為「無預先讀取」原則 — 類型 **1** 為「預先讀取」原則 — 類型 **2** 為「調適性預先讀取」原則 • [-i **<0|1>**] 為快取 I/O 原則： — 類型 **0** 為「直接 I/O」原則 — 類型 **1** 為「快取 I/O」原則 • [-a **<0|2|3>**] 為存取原則： — 類型 **0** 為「讀寫」原則 — 類型 **2** 為「唯讀」原則 — 類型 **3** 為「已封鎖」原則 • [-d **<0|1|2>**] 為磁碟快取原則： — 如果原則未變更，則為類型 **0** — 類型 **1** 可啟用原則[6]

表格 63. storage 指令（繼續）

選項	說明	值
		— 類型 **2** 可停用原則 • [-b **<0|1>**] 為背景起始設定： — 類型 **0** 可啟用起始設定 — 類型 **1** 可停用起始設定 • **-target_id** 為 **vol[x]**[5]
-config vol -add<[-R] [-D disk] [-H disk] [-l hole]> [-N] [-w] [-r][3,7]	當目標為控制器時，為新的儲存區建立一個磁區。 或 當目標為儲存區時，以現有的儲存區來建立一個磁區。	• [-R **<0|1|5|1E|6|10|50|60|00|1ERLQ0|1E0RLQ0>**] 此選項可定義 RAID 層次，並且僅用於新的儲存區 • [-D disk **[id11]:disk[id12]:..disk[id21]:disk[id22]:..**] 此選項可定義硬碟群組（包括跨距），並且僅用於新的儲存區 • [-H disk **[id1]:disk[id2]:..**]此選項可定義緊急備用群組，並且僅用於新的儲存區 • [-l hole] 此選項可為現有的儲存區定義可用孔空間的索引編號 • [-N **volume_name**] 是磁區的名稱 • [-w **<0|1|2>**] 是快取寫入原則： — 類型 **0** 為「直接寫入」原則 — 類型 **1** 為「寫回」原則 — 類型 **2** 為「以備用電池組件 (BBU) 寫入」原則 • [-r **<0|1|2>**] 為快取讀取原則： — 類型 **0** 為「無預先讀取」原則 — 類型 **1** 為「預先讀取」原則 — 類型 **2** 為「調適性預先讀取」原則
-config vol -add[-i] [-a] [-d] [-f] [-S] [-P] -target **target_id**[3]	當目標為控制器時，為新的儲存區建立一個磁區。 或 當目標為儲存區時，以現有的儲存區來建立一個磁區。	• [-i **<0|1>**] 為快取 I/O 原則： — 類型 **0** 為「直接 I/O」原則 — 類型 **1** 為「快取 I/O」原則 • [-a **<0|2|3>**] 為存取原則： — 類型 **0** 為「讀寫」原則 — 類型 **2** 為「唯讀」原則 — 類型 **3** 為「已封鎖」原則 • [-d **<0|1|2>**] 為磁碟快取原則： — 如果原則仍未變更，則為類型 **0** — 類型 **1** 可啟用原則[6] — 類型 **2** 可停用原則 • [-f **<0/1/2>**] 為起始設定的類型： — 類型 **0** 為無起始設定 — 類型 **1** 為快速起始設定 — 類型 **2** 為完整起始設定 • [-S **volume_size**] 是新磁區的大小（以 MB 為單位）

表格 63. storage 指令（繼續）

選項	說明	值
		• [-P **strip_size**] 為磁區帶大小，例如 128K 或 1M • -target **target_id** 為： — **ctrl[x]**（新儲存區）[5] — **pool[x]**（現有儲存區）[5]
-config vol -getfreecap[-R] [-D disk] [-H disk] -target **target_id**[3]	取得硬碟群組的可用容量。	• [-R **<0|1|5|1E|6|10|50|60|00|1ERLQ0|1E0RLQ0>**] 此選項可定義 RAID 層次，並且僅用於新的儲存區 • [-D disk **[id11]:[id12]:..[id21]:[id22]:..**]此選項可定義硬碟群組（包括跨距），並且僅用於新的儲存區 • [-H disk **[id1]:[id2]:..**]此選項可定義緊急備用群組，並且僅用於新的儲存區 • -target **target_id** 為： — **ctrl[x]**[5]
-help	顯示指令用法和選項	

附註：

1. 只有在 IMM 可存取 RAID 控制器的伺服器上，才支援此指令。
2. 只會針對相關聯的控制器、磁碟和快閃記憶體 DIMM 顯示韌體資訊。不會針對相關聯的儲存區和磁區顯示韌體資訊。
3. 由於空間限制，資訊會以數行顯示。
4. 只有在支援 RAID 日誌的伺服器上，可支援此指令。
5. 只有在支援 RAID 配置的伺服器上，可支援此指令。
6. **Enable** 值不支援 RAID 層次 1 配置。
7. 以下列出可用選項的部分清單。**storage –config vol –add** 指令的其餘選項列示如下。

語法：

```
storage [options]
option:
 -config ctrl|drv|vol -option [–options] -target target_id
 -list controllers|pools|volumes|drives
 -list pools -target ctrl[x]
 -list volumes -target ctrl[x]|pool[x]
 -list drives -target ctrl[x]|pool[x]
 -list devices
 -list flashdimms
 -show target_id
 -show {ctrl[x]|pool[x]|disk[x]|vol[x]|flashdimm[x]} info
 -show {ctrl[x]|disk[x]|flashdimm[x]}firmware
 -showlog ctrl[x]m:n|all
  -h help
```

範例：

```
system> storage
-config ctrl -clrcfg -target ctrl[0]
ok
system>
system> storage
-config ctrl -clrforgn -target ctrl[0]
ok
system>
system> storage
```

```
-config ctrl -imptforgn -target ctrl[0]
ok
system>
system> storage
-config ctrl -scanforgn -target ctrl[0]
Detect 1 foreign configuration(s) on controller ctrl[0]
system>
system> storage
-config drv -addhsp -dedicated pool[0-1] -target disk[0-0]
ok
system>
system> storage
-config drv -addhsp -target disk[0-0]
ok
system>
system> storage
-config drv -mkbad -target disk[0-0]
ok
system>
system> storage
-config drv -mkgood -target disk[0-0]
ok
system>
system> storage
-config drv -mkmissing -target disk[0-0]
ok
system>
system> storage
-config drv -mkoffline -target disk[0-0]
ok
system>
system> storage
-config drv -mkonline -target disk[0-0]
ok
system>
system> storage
-config drv -prprm -target disk[0-0]
ok
system>
system> storage
-config drv -rmhsp -target disk[0-0]
ok
system>
system> storage
-config drv -undoprprm -target disk[0-0]
ok
system>
system> storage
-config vol -add -1 1 -target pool[0-1]
ok
system>
system> storage
-config vol -add -R 1 -D disk[0-0]:disk[0-1] -w 1 -r 2 -i 0 -a 0 -d 0 -f 0
-N LD_volume -S 100000 -P 64K -H disk[0-2] -target ctrl[0]
ok
system>
system> storage
-config vol -getfreecap -R 1 -D disk[0-0]:disk[0-1] -H disk[0-2] -target ctrl[0]
The drive group configuration is good with free capacity 500000MB
system>
system> storage
```

```
-config vol -remove -target vol[0-1]
ok
system>
system> storage
-config vol -set -N LD_volume -w 0 -target vol[0-0]
ok
system>
system> storage
-list controllers
ctrl[0]   ServerRAID M5110e(Slot No. 0)
ctrl[1]   ServerRAID M5110f(Slot No. 1)
system>
system> storage
-list drives
disk[0-0]   Drive 0
disk[0-1]   Drive 1
disk[0-2]   Drive 2
system>
system> storage
-list flashdimms
flashdimm[1]   Flash DIMM 1
flashdimm[4]   Flash DIMM 4
flashdimm[9]   Flash DIMM 9
system>
system> storage
-list pools
pool[0-0]   Storage Pool 0
pool[0-1]   Storage Pool 1
system>
system> storage
-list volumes
system>storage -list volumes
vol[0-0]   Volume 0
vol[0-1]   Volume 1
Vol[0-2]   Volume 2
system>
system> storage
-list drives -target ctrl[0]
disk[0-0]   Drive 0
disk[0-1]   Drive 1
disk[0-2]   Drive 2
system>
system> storage
-list drives -target pool[0-0]
disk[0-0]   Drive 0
disk[0-1]   Drive 1
system>
system> storage
-list pools -target ctrl[0]
pool[0-0]   Storage Pool 0
system>
system> storage
-list volumes -target ctrl[0]
vol[0-0]   Volume 0
vol[0-1]   Volume 1
system>
system> storage
-list volumes -target pool[0-0]
vol[0-0]   Volume 0
vol[0-1]   Volume 1
system>
```

```
system> storage
-show ctrl[0] firmware
Total Firmware number: 2
Name: RAID Firmware1
Description: RAID Firmware
Manfacture: IBM
Version: 4.01(3)T
Release Date: 01/05/2013
Name: RAID Firmware2
Description: RAID Firmware
system>
system> storage
-show ctrl[0] info
Product Name: ServerRAID M5110e
Firmware Package Version: 23.7.0.1.2
Battery Backup: Installed
Manufacture: IBM
UUID: 1234567890123456
Model Type / Model: 1234AHH
Serial No.: 1234567890
FRU No.: 5005076049CC4
Part No.: LSI2004
Cache Model Status: Unknown
Cache Model Memory Size: 300MB
Cache Model Serial No.: PBKUD0XTA0P04Y
PCI Slot Number: 0
PCI Bus Number: 2
PCI Device Number: 2
PCI Function Number: 10
PCI Device ID: 0x1000
PCI Subsystem Device ID: 0x1413
Ports: 2
Port 1: 12345678901234
Port 2: 12345678901235
Storage Pools: 2
pool[0-0] Storage Pool 0
pool[0-1] Storage Pool 1
Drives: 3
disk[0-0]  Drive 0
disk[0-1]  Drive 1
disk[0-2]  Drive 2
system>
system> storage
-show disk[0-0] firmware
Total Firmware number: 1
Name: Drive
Description:
Manufacture:
Version: BE24
Release Date:
system>
system> storage
-show disk[0-0] info
Product Name: ST98394893
State: Online
Slot No.: 0
Disk Type: SATA
Media Type: HHD
Health Status: Normal
Capacity: 100.000GB
Speed: 6.0Gb/s
```

```
Current Temperature: 33C
Manufacture: ATA
Device ID: 5
Enclusure ID: 0x00FC
Machine Type:
Model:
Serial No.: 9XKJKL
FRU No.:
Part No.:
system>
system> storage
-show flashdimm[15]
Name: CPU1 DIMM 15
Health Status: Normal
Operational Status: Online
Capacity(GB): 400GB
Model Type: DDR3
Part Number: 93E40400GGM101PAT
FRU S/N: 44000000
Manuf ID: Diablo Technologies
Temperature: 0C
Warranty Writes: 100%
Write Endurance: 100%
F/W Level: A201.0.0.49152
system>
system> storage
-show pool[0-0]
RAID State: RAID 0
RAID Capacity: 67.000GB (0.000GB free)
Drives: 2
disk[0-0]   Drive 0
disk[0-1]   Drive 1
Volumes: 2
vol[0-0]   Volume 0
vol[0-1]   Volume 1
system>
system> storage
-show pool[0-1] info
RAID State: RAID 1
RAID Capacity: 231.898GB (200.000GB free)
Holes: 2
#1 Free Capacity: 100.000GB
#2 Free Capacity: 100.000GB

Drives: 2
disk[0-1]   Drive 1
disk[0-2]   Drive 2

Volume: 1
vol[0-1]   LD_volume
system>
system> storage
-show vol[0-0]
Name: Volume 0
Stripe Size: 64KB
Status: Offline
Capacity: 100.000GB
system>
system> storage
-show vol[0-0] info
Name: LD_volume
```

```
Status: Optimal
Stripe Size: 64KB
Bootable: Not Bootable
Capacity: 231.898GB
Read Policy: No Read Ahead
Write Policy: Write Through
I/O Policy: Direct I/O
Access Policy: Read Write
Disk Cache Policy: Unchanged
Background Initialization: Enable
system>
```

adapter 指令

此指令可用來顯示 PCIe 配接卡庫存資訊。

如果不支援 **adapter** 指令，發出此指令時，伺服器會以下列訊息回應：
`Your platform does not support this command.`
如果您移除、更換或配置任何配接卡，則必須重新啟動伺服器（至少一次），才能檢視更新的配接卡資訊。

下表顯示各選項的引數。

表格 64. adapter 指令

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

選項	說明	值
-list	列出伺服器中的所有 PCIe 配接卡	
-show **target_id**	顯示目標 PCIe 配接卡的詳細資訊	**target_id [info|firmware|ports|chips]** 其中： • **info**：顯示配接卡的硬體資訊 • **firmware**：顯示配接卡的所有韌體資訊 • **ports**：顯示配接卡的所有乙太網路埠資訊 • **chips**：顯示配接卡的所有 GPU 晶片資訊
-h	顯示指令用法和選項	

語法：
```
adapter [options]
option:
 -list
 -show target_id [info|firmware|ports|chips]
  -h help
```

範例：
```
system> adapter
list
ob-1   Flex System CN4054 10Gbps Virtual Fabric Adapter
ob-2   GPU Card 1
slot-1  Raid Controller 1
slot-2  Adapter 01:02:03

system> adapter
show ob-1 info
Product Name: Flex System CN4054 10Gbps Virtual Fabric Adapter
Card Interface: PCIe x 16
```

```
Function Count: 2

Function Name: xxx Emulx xx component1
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1
Class Code: 2
Sub Vendor: 334
Sub Device: 223
Slot Description: a slot
Slot Type: 23
Slot Data Bus Width: 0
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
Model: 345
Function Sku: 221
Fod Uid: 2355
Required Daughter: 0
Max Data Width: 0
Connector Layout: pci x

Package Type: dici
Function Name: xxx nVidia xx component2
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1
Class Code: 2
Sub Vendor: 334
Sub Device: 223
Slot Description: a slot
Slot Type: 23
Slot Data Bus Width: 0
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
Model: 345
Function Sku: 221
Fod Uid: 2355
Required Daughter: 0
Max Data Width: 0
Connector Layout: pci x
Package Type: dici
```

m2raid 指令

使用此指令可取得與 M.2 相關的庫存資訊和管理虛擬磁區。

下表顯示各選項的引數。

表格 65. m2raid 指令

下表是由多個橫列與兩個直欄組成的表格，其中包含選項及選項說明。

選項	說明
-h/?	列印此指令的說明資訊
-version	顯示控制器韌體資訊
-disks	顯示媒體硬碟資訊
-volumes	顯示虛擬磁區資訊
-create	建立虛擬磁區，可以指定 VD_Name、RaidLevel 和 StripeSize
-delete	刪除虛擬磁區
-import	匯入外部虛擬磁區。匯入虛擬磁區後，系統重新開機將自動重建虛擬磁區。

用法

```
m2raid [-options] - raid configuration for M.2 adapter with Mirroring Enablem
options:
  -version            - displays controller firmware version.
  -disks             - displays information of media disks.
  -volumes            - displays information of virtual volumes
  -create -VD_Name <nameStr> -RaidLevel <0|1> -StripeSize <32|64>  - create virt
  -delete -VD_ID <0|1>     - delete the virtual volume
  -import -VD_ID <0|1>     - import a foreign virtual volume
```

範例

```
system> m2raid -version
   ThinkSystem M.2 with Mirroring Enablement Kit
 Firmware Version = 2.3.10.1193

system> m2raid -disks
   M.2 Bay0      32GB M.2 SATA SSD    LEN    100%
M.2 Bay1      32GB M.2 SATA SSD    LEN    100%

system> m2raid -volumes
   VD_ID   VD_Name   RaidLevel   StripSize   VD Capacity   Status
    0     M2RAID     1         64k       29 GB       Optimal

system> m2raid -delete -VD_ID 0
VD_ID 0 is deleted

system> m2raid -create -VD_Name M2RAID -RaidLevel 1 -StripeSize 64
New volume is created

system> m2raid -import -VD_ID 0
VD_ID 0 is imported
```

支援指令

本主題提供按字母順序排序的支援指令清單。

只有一個支援指令：第 159 頁 「dbgshimm 指令」。

dbgshimm 指令

使用此指令可解除鎖定安全除錯 Shell 的網路存取。

附註：此指令僅供支援人員使用。

下表顯示各選項的引數。

表格 66. dbgshimm 指令

下表是由多個橫列與兩個直欄組成的表格，其中包含選項及選項說明。

選項	說明
status	顯示狀態
enable	啟用除錯存取（若無指定選項時的預設值）
disable	停用除錯存取

第 11 章　IPMI 介面

本章說明 XClarity Controller 所支援的 IPMI 介面。

如需標準 IPMI 指令的詳細資料，請參閱智慧型平台管理介面 (IPMI) 規格文件（2.0 或更高版本）。本文件提供與 XClarity Controller 韌體所支援的標準 IPMI 和 OEM IPMI 指令搭配使用的 OEM 參數的說明。

使用 IPMI 管理 XClarity Controller

使用本主題中的資訊，可運用「智慧型平台管理介面 (IPMI)」管理 XClarity Controller。

XClarity Controller 隨附使用者 ID，最初設定的使用者名稱和密碼分別為 USERID 和 PASSW0RD（所含的是數字 0，不是字母 O）。此使用者具有監督者存取權。

重要事項：請在起始配置期間變更此使用者名稱和密碼，以加強安全性。

在 Flex System 中，使用者可以配置 Flex System CMM 以集中管理 XClarity Controller IPMI 使用者帳戶。在此情況下，直至 CMM 配置了 IPMI 使用者 ID，您才能夠使用 IPMI 存取 XClarity Controller。

附註：CMM 配置的使用者 ID 認證可能與上述 USERID/PASSW0RD 組合不同。如果 CMM 未配置 IPMI 使用者 ID，則與 IPMI 通訊協定相關的網路埠將會關閉。

XClarity Controller 也提供以下 IPMI 遠端伺服器管理功能：

IPMI 指令行介面
IPMI 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 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。如需 IPMItool 的相關資訊，請參閱第 161 頁 「使用 IPMItool」。

Serial over LAN
若要從遠端位置管理伺服器，請使用 IPMItool 來建立 Serial over LAN (SOL) 連線。如需 IPMItool 的相關資訊，請參閱第 161 頁 「使用 IPMItool」。

使用 IPMItool

使用本主題中的資訊來存取 IPMItool 的相關資訊。

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 XClarity Controller。

如需 IPMItool 的相關資訊，或要下載 IPMItool，請造訪 https://github.com/ipmitool/ipmitool。

IPMI 指令與 OEM 參數

取得/設定 LAN 配置參數

為了反映 XCC 就某些網路設定所提供的功能，部分參數資料的值定義如下所示。

DHCP
除了透過常用方法取得 IP 位址，XCC 還提供一種模式，其將在一段時間內嘗試從 DHCP 伺服器取得 IP 位址，若未成功即由使用靜態 IP 位址失效接手。

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

參數	#	參數資料
IP 位址來源	4	資料 1 [7:4] — 保留 [3:0] — 位址來源 0h = 未指定 1h = 靜態位址（手動配置） 2h = 由 XCC 執行 DHCP 取得的位址 3h = 由 BIOS 或系統軟體取得的位址 4h = 由 XCC 執行其他位址指派通訊協定取得的位址。 XCC 使用 4h 的值表示 DHCP 由靜態位址失效接手的位址模式。

乙太網路介面選擇

XCC 硬體包含具有 RMII 介面的雙 10/100 乙太網路 MAC。XCC 硬體還包含具有 RGMII 介面的雙 1Gbps 乙太網路 MAC。其中一個 MAC 通常連接到共用伺服器 NIC，另一個 MAC 則用作專用系統管理埠。任何一段時間內，伺服器上只有一個乙太網路埠處於作用狀態。兩個埠不會同時啟用。

對於部分伺服器，系統設計者可選擇僅連接系統介面板上這些乙太網路介面的其中一個或另一個。如為這類系統，XCC 僅支援由介面板上連接的乙太網路介面。要求使用未連接的埠將傳回 CCh 完成碼。

所有選配網路卡的套件 IDS 編號如下：

- 選配卡 #1，套件 ID = 03h (eth2)，
- 選配卡 #2，套件 ID = 04h (eth3)，

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

參數	#	參數資料
OEM 參數 XCC 使用此參數號碼表示應使用哪個可行的乙太網路埠（邏輯套件）。 在「取得/設定 LAN 配置參數」指令中，此參數不使用設定選取器或不需要區塊選取器，所以其各欄位應設為 00h。 回應資料將傳回 3 個位元組，若裝置位於 NCSI 套件內，則傳回 4 個位元組。 位元組 1 = 完成碼 位元組 2 = 修訂 位元組 3 = eth0 為 00h、eth1 為 01h，依此類推… 位元組 4 =（選用）若裝置是 NCSI 套件，即為通道號碼	C0h	資料 1 00h = eth0 01h = eth1 02h = eth2 依此類推… FFh = 停用所有外部網路埠 XCC 還支援另一個選用資料位元組，以指定要使用套件內的哪個通道 資料 2 00h = 通道 0 01h = 通道 1 依此類推…

參數	#	參數資料
		如果要求中未指定資料 2，即假定為通道 0

資料 1 位元組用於指定邏輯套件。這可能是專用系統管理 NIC 或與伺服器共用的 NIC 中的 NCSI 介面。

資料 2 位元組用於為邏輯套件指定通道（若套件是 NCSI 裝置）。如果要求中未指定資料 2 且邏輯套件是 NCSI 裝置，即假定為通道 0。如果要求中指定了資料 2 但邏輯套件不是 NCSI 裝置，則會忽略通道資訊。

範例：

附錄 A：如果將介面板上共用 NIC 的通道 2（套件 ID = 0，eth0）用作管理埠，則輸入資料為：0xC0 0x00 0x02

附錄 B：如果要使用第一張 Mezzanine 網路卡的第一個通道，則輸入為：0xC0 0x02 0x0

啟用/停用 Ethernet over USB

以下參數用於啟用或停用 XCC 頻內介面。

下表是由多個橫列與三個直欄組成的表格，其中包括各選項、選項描述和選項的相關值。

參數	#	參數資料
OEM 參數 （XCC 使用此參數號碼以啟用或停用 Ethernet over USB 介面）。 在「取得 LAN 配置參數」指令中，此參數不使用設定選取器或不需要區塊選取器，所以其各欄位應設為 00h。 回應資料將傳回 3 個位元組： 位元組 1 = 完成碼 位元組 2 = 修訂 位元組 3 = 00h（已停用）或 01h（已啟用）	C1h	資料 1 0x00 = 已停用 0x01 = 已啟用

資料 1 位元組用於指定邏輯套件。這可能是專用系統管理 NIC 或與伺服器共用的 NIC 中的 NCSI 介面。

資料 2 位元組用於為邏輯套件指定通道（若套件是 NCSI 裝置）。如果要求中未指定資料 2 且邏輯套件是 NCSI 裝置，即假定為通道 0。如果要求中指定了資料 2 但邏輯套件不是 NCSI 裝置，則會忽略通道資訊。

範例：

附錄 A：如果將介面板上共用 NIC 的通道 2（套件 ID = 0，eth0）用作管理埠，則輸入資料為：0xC0 0x00 0x02

附錄 B：如果要使用第一張 Mezzanine 網路卡的第一個通道，則輸入為：0xC0 0x02 0x0

用於取得 DUID-LLT 的 IPMI 選項

另一個需要透過 IPMI 公開的唯讀值是 DUID。根據 RFC3315，這種格式的 DUID 是基於鏈結層位址加上時間。

參數	#	參數資料
OEM 參數 （XCC 使用此參數號碼以啟用或停用 Ethernet over USB 介面）。 在「取得 LAN 配置參數」指令中，此參數不使用設定選取器或不需要區塊選取器，所以其各欄位應設為 00h。 回應資料將傳回 3 個位元組： 位元組 1 = 完成碼 位元組 2 = 參數修訂（如 IPMI 規格） 位元組 3 = 後續資料位元組的長度（目前為 16 個位元組） 位元組 4 至 n = DUID_LLT	C2h	

乙太網路配置參數

以下參數可用於配置特定的乙太網路設定。

參數	#	參數資料
OEM 參數 （XCC 使用此參數號碼以啟用或停用乙太網路介面的自動協調設定）。 回應資料將傳回 3 個位元組： 位元組 1 = 完成碼 位元組 2 = 修訂 位元組 3 = 00h（已停用）或 01h（已啟用）	C3h	資料 1 0x00 = 已停用 0x01 = 已啟用 附註：在 Flex 和 ThinkSystem D2 Enclosure (ThinkSystem SD530 Compute Node) 系統上，自動協調設定無法變更，因為這可能會破壞經過 CMM 和 SMM 的網路通訊路徑。
OEM 參數 （XCC 使用此參數號碼以取得或設定乙太網路介面的資料傳輸率）。 回應資料將傳回 3 個位元組： 位元組 1 = 完成碼 位元組 2 = 修訂 位元組 3 = 00h (10Mb) 或 01h (100Mb)	C4h	資料 1 0x00 = 10Mbit 0x01 = 100Mbit

參數	#	參數資料
OEM 參數 （XCC 使用此參數號碼以取得或設定乙太網路介面的雙工設定）。 回應資料將傳回 3 個位元組： 位元組 1 = 完成碼 位元組 2 = 修訂 位元組 3 = 00h（半雙工）或 01h（全雙工）	C5h	資料 1 0x00 = 半雙工 0x01 = 全雙工
OEM 參數 （XCC 使用此參數號碼以取得或設定乙太網路介面的最大傳輸單位 (MTU)）。 回應資料將傳回 3 個位元組： 位元組 1 = 完成碼 位元組 2 = 修訂 位元組 3 至 4 = MTU 的大小	C6h	資料 1 MTU 的大小
OEM 參數 （XCC 使用此參數號碼以取得或設定本端管理 MAC 位址）。 回應資料將傳回 3 個位元組： 位元組 1 = 完成碼 位元組 2 = 修訂 位元組 3 至 8 = MAC 位址	C7h	資料 1 至 6 MAC 位址

用於取得鏈結本端位址的 IPMI 選項

此為唯讀參數，用於擷取 IPV6 鏈結本端位址。

參數	#	參數資料
OEM 參數 此參數用於取得 XCC 的鏈結本端位址： 回應資料將傳回以下內容： 位元組 1 = 完成碼 位元組 2 = 參數修訂（如 IPMI 規格） 位元組 3 = IPV6 位址字首長度 位元組 4 至 19 = 鏈結本端位址（二進位格式）	C8h	

用於啟用/停用 IPv6 的 IPMI 選項

此為可讀寫參數，用於在 XCC 中啟用/停用 IPV6。

參數	#	參數資料
OEM 參數 此參數用於在 XCC 中啟用/停用 IPv6 回應資料將傳回以下內容： 位元組 1 = 完成碼 位元組 2 = 參數修訂（如 IPMI 規格） 位元組 3 = 00h（已停用）或 01h（已啟用）	C9h	資料 1 0x00 = 已停用 0x01 = 已啟用

Ethernet over USB 透通外部網路

以下參數用於將 Ethernet over USB 配置為外部乙太網路透通。

參數	#	參數資料
OEM 參數 在「取得/設定 LAN 配置參數」指令中，此參數不使用設定選取器或不需要區塊選取器，所以其各欄位應設為 00h。 Get 回應資料將傳回以下內容： 位元組 1 = 完成碼 位元組 2 = 修訂 位元組 3 = 保留 (00h) 位元組 4:5 = Ethernet over USB 埠號（LSByte 在前） 位元組 6:7 = 外部乙太網路埠號（LSByte 在前） 後續位元組的數目因定址模式而異，可能是 1、4 或 16 個位元組： • 位元組 8 = 預先定義的模式： 00h = 透通已停用 01h = 使用了 CMM 的 IP 位址 位元組 8:11 = IPv4 外部網路 IP 位址（二進位格式） 位元組 8:23 = IPv6 外部網路 IP 位址（二進位格式） 完成碼： 00h — 成功 80h — 參數不受支援 C1h — 指令不受支援	CAh	設定 LAN 配置參數： 資料 1 保留 (= 00h) 資料 2:3 Ethernet over USB 埠號，LSByte 在前 資料 4:5 外部乙太網路埠號，LSByte 在前 後續位元組的數目因定址模式而異，可能是 1、4 或 16 個位元組： 資料 6 00h = 停用透通 01h = 使用 CMM 的 IP 位址 資料 6:9 IPv4 外部網路 IP 位址（二進位格式） 資料 6:21 IPv6 外部網路 IP 位址（二進位格式）

參數	#	參數資料
C7h — 要求資料長度無效		
OEM 參數 此參數用於設定和取得 XCC 的 LAN over USB IP 位址及網路遮罩： 回應資料將傳回以下內容： 位元組 1 = 完成碼 位元組 2 = 參數修訂（如 IPMI 規格） 位元組 3:10 = IP 位址及網路遮罩值（MS-byte 在前）	CBh	資料 1:4 XCC 側 LAN over USB 介面的 IP 位址。 資料 5:8 XCC 側 LAN over USB 介面的網路遮罩
OEM 參數 此參數用於設定和取得主機作業系統的 LAN over USB IP 位址： 回應資料將傳回以下內容： 位元組 1 = 完成碼 位元組 2 = 參數修訂（如 IPMI 規格） 位元組 3:6 = IP 位址（MS-byte 在前）	CCh	資料 1:4 主機側 LAN over USB 介面的 IP 位址。

查詢邏輯套件庫存

以下參數用於查詢 NCSI 套件庫存。

參數	#	參數資料
OEM 參數 在「取得/設定 LAN 配置參數」指令中，此參數不使用設定選取器或不需要區塊選取器，所以其各欄位應設為 00h。 查詢套件庫存作業 透過發出帶有 D3h 參數號碼和兩個 0x00 資料位元組的要求，執行查詢套件資訊作業。 查詢套件庫存： --> 0x0C 0x02 0x00 0xD3 0x00 0x00 對於每個存在的套件，XCC 回應各包括一個位元組的資訊： 位元 7:4 = 套件中 NCSI 通道的數目	D3h	取得/設定 LAN 配置參數：

參數	#	參數資料
位元 3:0 = 邏輯套件號碼 回應 --> 0x00 0x00 0x40 0x01 0x32 表示存在 3 個邏輯套件： 套件 0 有 4 個 NCSI 通道 套件 1 不是 NCSI NIC，所以不支援 NCSI 通道 套件 2 有 3 個 NCSI 通道		

取得/設定邏輯套件資料

以下參數用於讀取及設定指派給每個套件的優先順序。

參數	#	參數資料
OEM 參數 在「取得/設定 LAN 配置參數」指令中，此參數不使用設定選取器或不需要區塊選取器，所以其各欄位應設為 00h。 本指令支援 2 種作業： • 讀取套件優先順序 • 設定套件優先順序 讀取套件優先順序作業 透過發出帶有 D4h 參數號碼和兩個 0x00 資料位元組的要求，執行讀取套件優先順序作業。 讀取套件優先順序： --> 0x0C 0x02 0x01 0xD4 0x00 0x00 回應 --> 0x00 0x00 0x00 0x12 0x23 邏輯套件 0 = 優先順序 0 邏輯套件 2 = 優先順序 1 邏輯套件 3 = 優先順序 2 設定套件優先順序作業 透過發出帶有 D4h 參數號碼和一個或多個參數的要求，執行設定套件優先順序作業。	D4	取得/設定 LAN 配置參數： 位元 [7-4] = 邏輯套件的優先順序（1 = 最高，15 = 最低） 位元 [3-0] = 邏輯套件號碼

參數	#	參數資料
設定套件優先順序： --> 0x0C 0x01 0x01 0xD4 0x00 0x12 0x23 設定邏輯套件 0 = 優先順序 0 設定邏輯套件 2 = 優先順序 1 設定邏輯套件 3 = 優先順序 2 回應： 僅完成碼，無其他資料		

取得/設定 XCC 網路同步狀態

參數	#	參數資料
OEM 參數 此位元組用於配置在專用和共用 NIC 模式之間同步網路設定 在「取得 LAN 配置參數」指令中，此參數不使用設定選取器或不需要區塊選取器，所以其各欄位應設為 00h。 回應資料將傳回 3 個位元組： 位元組 1 = 完成碼 位元組 2 = 修訂 位元組 3 = 00h（已啟用）或 01h（已停用）	D5h	資料 1 0x00 = 同步 0x01 = 獨立

此位元組用於配置在專用和共用 NIC 模式之間同步網路設定。上例的預設值為 0h，表示 XCC 將隨著模式變更而自動更新網路設定，並且使用共用 NIC（機載）做為主要參考。如果設為 1h，每項網路設定則均為獨立，各模式間即可配置不同的網路設定，例如專用模式啟用 VLAN 而共用 NIC 模式設定 VLAN 停用。

取得/設定 XCC 網路模式

參數	#	參數資料
OEM 參數 此參數用於取得/設定 XCC 管理 NIC 的網路模式。 回應資料將傳回 4 個位元組： 位元組 1 = 完成碼 位元組 2 = 修訂 位元組 3 = 已套用/指定的網路模式	D6h	設定 LAN 配置參數： 資料 1 要設定的網路模式 取得 LAN 配置參數： 資料 1

參數	#	參數資料
位元組 4 = 套用的網路模式其套件 ID 位元組 5 = 套用的網路模式其通道 ID		要取得的網路模式。此為選用資料，預設將查詢目前的網路模式

OEM IPMI 指令

XCC 支援下列 IPMI OEM 指令。各指令需要不同層級的專用權，如下所示。

代碼	Netfn 0x2E 指令	專用權
0xCC	將 XCC 重設為預設值	PRIV_USR

代碼	Netfn 0x3A 指令	專用權
0x00	查詢韌體版本	PRIV_USR
0x0D	主機板資訊	PRIV_USR
0x1E	機箱電源還原延遲選項	PRIV_USR
0x38	NMI 與重設	PRIV_USR
0x49	起始資料收集	PRIV_USR
0x4A	推送檔案	PRIV_USR
0x4D	資料收集狀態	PRIV_USR
0x50	取得 Build 資訊	PRIV_USR
0x55	取得/設定主機名稱	PRIV_USR
0x6B	查詢 FPGA 韌體修訂層次	PRIV_USR
0x6C	查詢主機板硬體修訂層次	PRIV_USR
0x6D	查詢 PSoC 韌體修訂層次	PRIV_USR
0x98	前方面板 USB 埠控制	PRIV_USR
0xC7	原生 NM IPMI 交換器	PRIV_ADM

將 XCC 重設為預設值指令

此指令會將 XCC 配置設定重設為預設值。

網路功能 = 0x2E			
代碼	**指令**	**要求、回應資料**	**說明**
0xCC	將 XCC 重設為預設值	**要求：** 位元組 1 — 0x5E，位元組 2 — 0x2B 位元組 3 — 0x00 位元組 4 — 0x0A，位元組 5 — 0x01 位元組 6 — 0xFF 位元組 7 — 0x00，位元組 8 — 0x00 位元組 9 — 0x00 **回應：** 位元組 1 — 完成碼，位元組 2 — 0x5E，位元組 3 — 0x2B 位元組 4 — 0x00 位元組 5 — 0x0A，位元組 6 — 0x01 位元組 7 — 回應資料 0 = 成功 非 0 = 失敗	此指令會將 XCC 配置設定重設為預設值。

主機板/韌體資訊指令

本節列出用於查詢主機板和韌體資訊的指令。

網路功能 = 0x3A			
代碼	**指令**	**要求、回應資料**	**說明**
0x00	查詢韌體版本	**要求**： 無任何要求的資料 **回應**： 位元組 1 — 完成碼 位元組 2 — 主要版本 位元組 3 — 次要版本	此指令傳回韌體的主要版本及次要版本號碼。如果使用選用 1 位元組的要求資料發出指令，XCC 回應還會傳回版本的第三個欄位（修訂號碼）。 （主要.次要.修訂）
0x0D	查詢主機板資訊	**要求**：不適用 **回應**： 位元組 1 — 系統 ID	此指令傳回主機板 ID 及介面板修訂號碼。

網路功能 = 0x3A			
代碼	**指令**	**要求、回應資料**	**說明**
		位元組 2 — 主機板修訂號碼	
0x50	查詢 Build 資訊	**要求**：不適用 **回應**： 位元組 1 — 完成碼。 位元組 2:10 — ASCIIZ Build 名稱 位元組 11:23 — ASCIIZ Build 日期 位元組 24:31 — ASCII Build 時間	此指令傳回 Build 名稱、Build 日期和 Build 時間。Build 名稱和 Build 日期字串以零結尾。 Build 日期的格式為 YYYY-MM-DD。 例如「ZUBT99A」 “2005-03-07” “23:59:59”
0x6B	查詢 FPGA 韌體修訂層次	**要求**： 位元組 1 — FPGA 裝置類型* FPGA 裝置類型 0 = 本端（作用中層級） 1 = CPU 卡 1（作用中層級） 2 = CPU 卡 2（作用中層級） 3 = CPU 卡 3（作用中層級） 4 = CPU 卡 4（作用中層級） 5 = 本端主要 ROM 6 = 本端復原 ROM **回應**： 位元組 1 — 完成碼 位元組 2 — 主要修訂層次 位元組 3 — 次要修訂層次 位元組 4 — 附屬次要修訂層次 （XCC 平台上的測試位元組）	此指令傳回 FPGA 韌體的修訂層次。 如果省略位元組 1，則會選取本端（作用中層級）

網路功能 = 0x3A			
代碼	**指令**	**要求、回應資料**	**說明**
0x6C	查詢主機板硬體修訂層次	**要求**： 無資料。 **回應**： 位元組 1 — 完成碼 位元組 2 — 修訂層次	此指令傳回 FPGA 所在主機板硬體的修訂層次。
0x6D	查詢 PSoC 韌體修訂層次	**要求**： 無 **回應**： 位元組 1 — 完成碼 位元組 2 — bin# 位元組 3 — APID 位元組 4 — 修訂號碼 位元組 5 至 6 — FRU ID 位元組 6:N — 對每個偵測到的 PSoC 重複位元組 2 至 6	此指令傳回所有偵測到的 PSoC 裝置的修訂層次。 附註：bin# 代表實體位置。詳細資料請查閱系統規格。

系統控制指令

IPMI 規格提供了基本電源和重設控制。Lenovo 增加了其他控制功能。

<table>
<tr><th colspan="4">網路功能 = 0x3A</th></tr>
<tr><th>代碼</th><th>指令</th><th>要求、回應資料</th><th>說明</th></tr>
<tr><td>0x1E</td><td>機箱電源還原延遲選項</td><td>要求：
<table><tr><td>位元組 1</td><td>要求類型：
0x00 = 設定延遲選項
0x01 = 查詢延遲選項</td></tr><tr><td>位元組 2</td><td>（如果位元組 1 = 0x00）
0x00 = 已停用（預設）
0x01 = 隨機
0x02 - 0xFF 保留</td></tr></table></td><td>如果機箱電源還原原則設為在 AC 電源接通/恢復供電後始終開啟電源或恢復為開啟電源（若原先已開啟電源），將使用此設定。共有 2 種選擇：已停用（預設值，開啟電源時無延遲）和隨機。隨機延遲設定將自 AC 電源接通/恢復供電以及伺服器自動開啟電源之時起隨機提供 1 至 15 秒不等的延遲。
此指令僅限機架式伺服器上的 XCC 才有支援。</td></tr>
</table>

網路功能 = 0x3A			
代碼	**指令**	**要求、回應資料**	**說明**
		回應： 位元組 1 — 完成碼 位元組 2 — 延遲選項（僅限「查詢」要求）	
0x38	NMI 與重設	**要求**： 位元組 1 — 秒數 0 = 僅限 NMI 位元組 2 — 重設類型 0 = 正常重設 1 = 關閉再開啟電源 **回應**： 位元組 1 — 完成碼	此指令用於執行系統 NMI。或者，在 NMI 後可將系統重設（重新開機）或關閉再開啟電源。 若「秒數」欄位非 0，系統將在指定的秒數過後重設或關閉再開啟電源。 要求的位元組 2 為選用。如果未提供位元組 2，或者其值為 0x00，則將執行正常重設。如果位元組 2 為 0x01，系統將關閉再開啟電源。

其他指令

本節提供不屬於任何其他各節內容的指令。

<table>
<tr><th colspan="4">網路功能 = 0x3A</th></tr>
<tr><th>代碼</th><th>指令</th><th>要求、回應資料</th><th>說明</th></tr>
<tr><td>0x55</td><td>取得/設定主機名稱</td><td>要求長度 = 0：
要求資料為空
回應：<table><tr><td>位元組 1</td><td>完成碼</td></tr><tr><td>位元組 2 至 65</td><td>目前主機名稱。
ASCIIZ，以空值結尾的字串。</td></tr></table>要求長度 1-64：<table><tr><td>位元組 1 至 64</td><td>DHCP 主機名稱
ASCIIZ 以 00h 結尾</td></tr></table></td><td>使用此指令可取得/設定主機名稱。
設定主機名稱時，所需的值必須以 00h 結尾。主機名稱的字元數限制為 63 個（包括空值在內）。</td></tr>
<tr><td>0x98</td><td>前方面板 USB 埠控制</td><td>要求：
位元組 1</td><td>此指令用於查詢前方面板 USB 埠的狀態/配置、配置前方面板 USB 埠的模式/逾時，以及將 USB 埠的擁有者切換至主機或 BMC</td></tr>
</table>

<table>
<tr><th colspan="4">網路功能 = 0x3A</th></tr>
<tr><th>代碼</th><th>指令</th><th>要求、回應資料</th><th>說明</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>01h：</td><td>取得前方面板 USB 埠的現行擁有者</td></tr>
</table>
回應：
位元組 1 — 完成碼
位元組 2
<table>
<tr><td>00h：</td><td>主機所擁有</td></tr>
<tr><td>01h：</td><td>BMC 所擁有</td></tr>
</table>
要求：
位元組 1
<table>
<tr><td>02h：</td><td>取得前方面板 USB 埠的配置</td></tr>
</table>
回應：
位元組 1 — 完成碼
位元組 2
<table>
<tr><td>00h：</td><td>主機專用</td></tr>
<tr><td>01h：</td><td>BMC 專用</td></tr>
<tr><td>02h：</td><td>共用模式</td></tr>
</table>
位元組 3:4 — 以分鐘為單位的閒置逾時（MSB 在前）
位元組 5 — 啟用 ID 按鈕
<table>
<tr><td>00h：</td><td>已停用</td></tr>
<tr><td>01h：</td><td>已啟用</td></tr>
</table>
位元組 6 — 遲滯（選用）秒數
要求：
位元組 1
03h：設定前方面板 USB 埠的配置
位元組 2</td><td>在配置中，前方面板 USB 可分為 3 種模式 — 主機專用、BMC 獨佔或允許切換擁有者至主機或 BMC 的共用模式。

如果啟用了共用模式，USB 埠將於伺服器電源關閉時連接到 BMC，並於伺服器電源開啟時連接到伺服器。

啟用共用模式並已開啟伺服器電源後，若發生了配置的閒置逾時，BMC 會將 USB 埠交還給伺服器。

如果伺服器具有識別按鈕，使用者可以啟用/停用 ID 按鈕，透過按住 ID 按鈕 3 秒以上，切換前方面板 USB 埠的擁有者。

關閉再開啟電源期間自動切換埠時，將設定遲滯秒數。此為選用參數。

SD530 伺服器

在 SD530 平台上，該埠為選用性質，若有則會直接佈線至 XCC，而且僅連到 XCC。切換該埠至主機不可行。
• 發出的指令若位元組 1 = 1，XCC 將一律回應以該埠由 BMC 所擁有。
• 發出的指令若位元組 1 = 2，XCC 將一律回應以該埠由 BMC 專用。
• 發出的指令若位元組 1 = 3 或位元組 1 = 4，XCC 將回應以完成碼 D6h。

非 SD530 伺服器

在非 SD530 平台上，透過切換到「僅限主機」模式可停用 XCC 對前方面板 USB 埠的使用。

發出的指令若位元組 1 = 5 或位元組 1 = 6，XCC 將回應以完成碼 D6h。</td></tr>
</table>

<table>
<tr><th colspan="4">網路功能 = 0x3A</th></tr>
<tr><th>代碼</th><th>指令</th><th>要求、回應資料</th><th>說明</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>00h：</td><td>主機專用</td></tr>
<tr><td>01h：</td><td>BMC 專用</td></tr>
<tr><td>02h：</td><td>共用模式</td></tr>
</table>
位元組 3:4 — 以分鐘為單位的閒置逾時（MSB 在前）

位元組 5 — 啟用 ID 按鈕
<table>
<tr><td>00h：</td><td>已停用</td></tr>
<tr><td>01h：</td><td>已啟用</td></tr>
</table>
位元組 6 — 遲滯（選用）秒數

回應：

位元組 1 — 完成碼，位元組 2
<table>
<tr><td>00h：</td><td>切換至主機</td></tr>
<tr><td>01h：</td><td>切換至 BMC</td></tr>
</table>
回應：

位元組 1 — 完成碼

位元組 1
<table>
<tr><td>05h：</td><td>啟用/停用前方面板 USB 埠</td></tr>
</table>
位元組 2
<table>
<tr><td>00h：</td><td>停用</td></tr>
<tr><td>01h：</td><td>啟用</td></tr>
</table>
回應：

位元組 1 — 完成碼

要求：

位元組 1
<table>
<tr><td>06h：</td><td>讀取前方面板 USB 埠的啟用/停用狀態</td></tr>
</table>
回應：

位元組 1 - 完成碼
</td><td></td></tr>
</table>

<table>
<tr><th colspan="4">網路功能 = 0x3A</th></tr>
<tr><th>代碼</th><th>指令</th><th>要求、回應資料</th><th>說明</th></tr>
<tr><td></td><td></td><td>位元組 2</td><td></td></tr>
<tr><td>0xC7</td><td>原生 NM IPMI 交換器</td><td>要求長度 = 0：
要求資料為空
回應：<table><tr><td>位元組 1</td><td>完成碼</td></tr><tr><td>位元組 2</td><td>目前啟用/停用狀態</td></tr></table>要求長度 = 1：<table><tr><td>位元組 1</td><td>原生 NM IPMI 介面啟用/停用屬性
00h — 停用
01h — 啟用</td></tr></table>回應：<table><tr><td>位元組 1</td><td>完成碼</td></tr></table></td><td>此指令用於啟用/停用 XCC 對原生 Intel IPMI 指令的橋接功能。</td></tr>
</table>

第 12 章 Edge 伺服器

本主題說明 Edge 伺服器的具體功能。

附註：

1. 第一次登入時，系統將要求您變更 XCC 密碼。
2. IPMI over LAN 預設為停用。
3. IPMI over KCS 預設為停用。

系統鎖定模式

系統鎖定模式處於作用中狀態時，表示系統正處於鎖定模式。您可以啟動系統並將其解除鎖定，否則不允許主機系統開機。

附註：系統鎖定模式僅適用於配備安全性套件的 SE350，但不適用於 SE350 標準。您可以在**首頁**標籤的**系統資訊和設定**下查看版本。

按一下 **BMC 配置**下方的**安全性**，然後捲動至 **系統鎖定模式**。

系統鎖定模式

若要啟動系統並結束**系統鎖定模式**，請完成下列步驟。

1. 按一下**非作用中**按鈕，隨即會蹦現 **Key Vault 啟動**視窗以顯示**挑戰文字**。
2. 聯絡您的 IT 管理者並提供**挑戰文字**。
3. 向您的 IT 管理者取得**挑戰回應**，然後在 **Key Vault 啟動**視窗中輸入.
4. 按一下**確定**按鈕，然後按一下**套用**。
5. 如果所有設定都正常運作，您將看到**系統鎖定模式**變更為**非作用中**。

附註：系統鎖定模式處於作用中狀態時，對系統機密（例如 SED 金鑰）進行任何存取都將**遭拒**。

若要強制系統進入系統鎖定模式，請完成下列步驟。

1. 按一下**作用中**按鈕。
2. 按一下**確定**按鈕，然後按一下**套用**。

動作偵測

您可以啟用此功能，透過偵測伺服器的任何實體移動來保護伺服器。
啟用動作偵測之後，您可以根據自身喜好和配置，設定以下各項目。

- **靈敏度等級**：根據您的喜好，選取靈敏度等級為**低**、**中**或**高**
- **方向**：選取您的配置，如**立式桌面**、**壁掛式（水平）**、**壁掛式（垂直）**、**書架式**或**天花板掛式**。

附註：系統進入鎖定模式時，將自動停用動作偵測。

機箱侵入偵測

您可以啟用此功能，透過偵測上蓋的任何實體移動來保護伺服器。

其他配置

如果安裝了已啟用無線功能的 LOM 保護袋，您即可就偵測到的篡改事件選擇三種設定。
在某些特殊情況下，**挑戰文字**可能無法通過 ThinkShield Key Vault Portal 的驗證，以致在按照 IT 管理者的要求啟動裝置之前可能需要先重設裝置內部計數器。

SED 鑑別金鑰 (AK) 管理員

對於安裝了 SED（自我加密型硬碟）的系統，此功能將控制 BMC 以部署 SED 金鑰。您可以使用 SED 金鑰將開機硬碟和資料硬碟加密，且無須人為介入即可將系統開機

附註：系統未啟動（系統鎖定模式生效）或現行使用者無權管理 SED 金鑰時，不允許執行此作業。

附註：系統鎖定模式僅適用於配備安全性套件的 SE350，但不適用於 SE350 標準。您可以在**首頁**標籤的**系統資訊和設定**下查看版本。

附註：只要 ThinkSystem M.2 Enablement Kit 或 ThinkSystem M.2 Mirroring Enablement Kit 性能良好，SE350 亦支援自動備份功能。如果硬體損壞，但 SED 和 M.2 套件性能良好，可以將它們安裝到另一個 SE350 中，然後即可還原 SED AK。不過，為了針對硬體徹底毀損做好準備，Lenovo 建議您製作 SED AK 備份。

按一下 **BMC 配置**下方的**安全性**，然後捲動至 **SED 鑑別金鑰 (AK) 管理員**。

變更 SED AK

從通行詞組產生 SED AK：設定密碼並再次輸入以便確認。按一下**重新產生**以取得新的 SED AK。
產生隨機 SED AK：按一下**重新產生**以取得隨機 SED AK。
備份 SED AK：設定密碼並再次輸入以便確認。按一下**開始備份**以備份 SED AK；然後下載 SED AK 檔案並妥善保存，以供日後使用。

附註：如果您使用備份 SED AK 檔案來還原配置，系統將詢問您在此處設定的密碼。

回復 SED AK：僅當 SED 無法正常運作時，才能執行此作業。有兩種方式可回復 SED AK：

- **使用通行詞組回復 SED AK**：使用在**從通行詞組產生 SED AK** 模式下設定的密碼回復 SED AK。
- **從備份檔案回復 SED AK**：上傳在**備份 SED AK** 模式下產生的備份檔案，然後輸入對應的備份檔案密碼以回復 SED AK。

Edge 網路功能

此功能頁面僅在安裝了已啟用無線功能的 LOM 保護袋時才受支援。

如需網路拓撲預設表的詳細資料，請參閱 https://thinksystem.lenovofiles.com/help/topic/SE350/pdf_files.html。

Wi-Fi 連線功能

按一下**已啟用**後，即可根據您的 Wi-Fi 配置進行各項設定的配置。

LTE 連線功能

這使您能夠控制 Edge 網路板的 LTE 連線功能。

Edge 網路板位址

IPv4 或 IPv6 狀態	DHCP 伺服器狀態	方法
已停用	已停用	從 DHCP 取得 IP
已啟用	已啟用	使用靜態 IP 位址
已啟用	已停用	從 DHCP 取得 IP 或使用靜態 IP 位址，視您的用法而定。

BMC 網路橋接器

您可以透過**下行鏈結埠**、**Wi-Fi 埠**、**上行鏈結埠**或**無**存取 BMC。

附註：選取**無**表示已停用此功能。

Edge 網路板疑難排解

立即重新啟動：透過此按鈕可以重新啟動網路板。

重設為原廠預設值：透過此按鈕可以將網路板重設為預設值。

附錄 A　取得說明和技術協助

若您需要說明、服務或技術協助，或想取得更多有關 Lenovo 產品的相關資訊，您可從 Lenovo 獲得許多相關資源來協助您。

在「全球資訊網 (WWW)」上，提供了 Lenovo 系統、選配裝置、維修及支援的最新相關資訊：

http://datacentersupport.lenovo.com

附註：本節包含 IBM 網站參考及相關資訊，協助您尋求支援服務。IBM 是 Lenovo 處理 ThinkSystem 所偏好的服務供應商。

致電之前

致電之前，您可以採取幾項步驟來嘗試自行解決問題。如果您確定需要致電尋求協助，請收集維修技術人員需要的資訊，以便更快地解決您的問題。

嘗試自行解決問題

只要遵照 Lenovo 線上說明或產品文件內的疑難排解程序，您就可以自行解決許多問題，而不需要向外尋求協助。Lenovo 產品文件也說明了您可執行的診斷測試。大部分的系統、作業系統和程式文件都提供了疑難排解程序以及錯誤訊息和錯誤碼的說明。如果您懷疑軟體有問題，請參閱作業系統文件或程式的文件。

您可以在以下位置找到 ThinkSystem 產品的產品文件：

https://pubs.lenovo.com/

您可以採取這些步驟來嘗試自行解決問題：

- 檢查所有的纜線，確定纜線已經連接。
- 檢查電源開關，確定系統及所有選配裝置都已開啟。
- 檢查是否有適用於 Lenovo 產品的更新軟體、韌體和作業系統裝置驅動程式。「Lenovo 保固」條款聲明，作為 Lenovo 產品的擁有者，您必須負責維護並更新產品的所有軟體及韌體（除非其他維護合約涵蓋此項服務）。如果軟體升級中已記載問題的解決方案，維修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，請查看http://www.lenovo.com/serverproven/，以確定您的產品支援此硬體或軟體。
- 請造訪 http://datacentersupport.lenovo.com，並查看是否有資訊可協助您解決問題。
  - 請查閱 https://forums.lenovo.com/t5/Datacenter-Systems/ct-p/sv_eg 上的 Lenovo 論壇，瞭解是否有其他人遇到類似的問題。

只要遵照 Lenovo 線上說明或產品文件內的疑難排解程序，您就可以自行解決許多問題，而不需要向外尋求協助。Lenovo 產品文件也說明了您可執行的診斷測試。大部分的系統、作業系統和程式文件都提供了疑難排解程序以及錯誤訊息和錯誤碼的說明。如果您懷疑軟體有問題，請參閱作業系統文件或程式的文件。

收集致電支援中心所需要的資訊

在您認為需要尋求 Lenovo 產品的保固服務時，若在電話詢問之前做好相應準備，維修技術人員將會更有效地協助您解決問題。您也可以查看http://datacentersupport.lenovo.com/warrantylookup，以取得有關產品保固的詳細資訊。

收集下列資訊，提供給維修技術人員。此資料將會協助維修技術人員快速提供問題的解決方案，確保您能獲得所約定的服務等級。

- 軟硬體維護合約號碼（如其適用）
- 機型號碼（Lenovo 4 位數的機器 ID）
- 型號
- 序號
- 現行系統 UEFI 及韌體版本
- 其他相關資訊，例如錯誤訊息及日誌

如不致電 Lenovo 支援中心，您可以前往 https://www-947.ibm.com/support/servicerequest/Home.action 提交電子服務要求。提交「電子服務要求」即會開始透過向維修技術人員提供相關資訊以決定問題解決方案的程序。一旦您已經完成並提交「電子服務要求」，Lenovo 維修技術人員即可開始制定解決方案。

收集服務資料

若要明確識別伺服器問題的根本原因或回應 Lenovo 支援中心的要求，您可能需要收集能夠用於進一步分析的服務資料。服務資料包含事件日誌和硬體庫存等資訊。

您可以透過下列工具收集服務資料：

- **Lenovo XClarity Controller**

  您可以使用 Lenovo XClarity Controller Web 介面或 CLI 收集伺服器的服務資料。您可以儲存此檔案，並將其傳送至 Lenovo 支援中心。

  — 如需使用 Web 介面收集服務資料的相關資訊，請參閱 https://pubs.lenovo.com/xcc/NN1ia_c_servicesandsupport.html。

  — 如需使用 CLI 收集服務資料的相關資訊，請參閱 https://pubs.lenovo.com/xcc/nn1ia_r_ffdccommand.html。

- **Lenovo XClarity Administrator**

  您可以將 Lenovo XClarity Administrator 設定為當 Lenovo XClarity Administrator 和受管理端點中發生某些可服務事件時，自動收集並傳送診斷檔案至 Lenovo 支援中心。您可以選擇使用 Call Home 將診斷檔案傳送給 Lenovo 支援中心，或使用 SFTP 傳送至其他服務供應商。也可以手動收集診斷檔案、提出問題記錄並將診斷檔案傳送給 Lenovo 支援中心。

  您可以在下列網址找到在 Lenovo XClarity Administrator 內設定自動問題通知的相關資訊：https://pubs.lenovo.com/lxca/admin_setupcallhome.html。

- **Lenovo XClarity Provisioning Manager**

  使用 Lenovo XClarity Provisioning Manager 的「收集服務資料」功能收集系統服務資料。您可以收集現有的系統日誌資料，或執行新診斷以收集新資料。

- **Lenovo XClarity Essentials**

  Lenovo XClarity Essentials 可以在頻內從作業系統執行。除了硬體服務資料之外，Lenovo XClarity Essentials 還可以收集作業系統的相關資訊，例如作業系統事件日誌。

  若要取得服務資料，您可以執行 `getinfor` 指令。如需執行 `getinfor` 的相關資訊，請參閱 https://pubs.lenovo.com/lxce-onecli/onecli_r_getinfor_command.html。

聯絡支援中心

您可以聯絡支援中心，針對您的問題取得協助。

您可以透過 Lenovo 授權服務供應商來獲得硬體服務。如果要尋找 Lenovo 授權服務供應商提供保固服務，請造訪 https://datacentersupport.lenovo.com/us/en/serviceprovider，並使用過濾器搜尋不同的國家/地區。對於 Lenovo 支援電話號碼，請參閱 https://datacentersupport.lenovo.com/us/en/supportphonelist 以取得您的地區支援詳細資料。

附錄 B　聲明

Lenovo 不見得會對所有國家或地區都提供本文件所提的各項產品、服務或功能。請洽詢當地的 Lenovo 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 Lenovo 的產品、程式或服務時，不表示或暗示只能使用 Lenovo 的產品、程式或服務。只要未侵犯 Lenovo 之智慧財產權，任何功能相當之產品、程式或服務皆可取代 Lenovo 之產品、程式或服務。不過，其他產品、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，Lenovo 可能擁有其專利或正在進行專利申請。本文件之提供不代表使用者享有優惠，並且未提供任何專利或專利申請之授權。您可以書面提出查詢，來函請寄到：

Lenovo (United States), Inc.
1009 Think Place
Morrisville, NC 27560
U.S.A.
Attention: Lenovo VP of Intellectual Property

LENOVO 係以「現狀」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、可商用性或特定目的之適用性的隱含保證。有些轄區在特定交易上，不允許排除明示或暗示的保證，因此，這項聲明不一定適合您。

本資訊中可能會有技術上或排版印刷上的訛誤。因此，Lenovo 會定期修訂；並將修訂後的內容納入新版中。Lenovo 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。

本文件中所述產品不適用於移植手術或其他的生命維持應用，因其功能失常有造成人員傷亡的可能。本文件中所包含的資訊不影響或變更 Lenovo 產品的規格或保證。本文件不會在 Lenovo 或協力廠商的智慧財產權以外提供任何明示或暗示的保證。本文件中包含的所有資訊均由特定環境取得，而且僅作為說明用途。在其他作業環境中獲得的結果可能有所差異。

Lenovo 得以各種 Lenovo 認為適當的方式使用或散佈貴客戶提供的任何資訊，而無需對貴客戶負責。

本資訊中任何對非 Lenovo 網站的敘述僅供參考，Lenovo 對該網站並不提供保證。該等網站提供之資料不屬於本產品著作物，若要使用該等網站之資料，貴客戶必須自行承擔風險。

本文件中所含的任何效能資料是在控制環境中得出。因此，在其他作業環境中獲得的結果可能有明顯的差異。在開發層次的系統上可能有做過一些測量，但不保證這些測量在市面上普遍發行的系統上有相同的結果。再者，有些測定可能是透過推測方式來評估。實際結果可能不同。本文件的使用者應驗證其特定環境適用的資料。

商標

Lenovo、Lenovo 標誌、ThinkSystem、Flex System、System x、NeXtScale System 及 x Architecture 是 Lenovo 於美國及（或）其他國家/地區之商標。

Intel 和 Intel Xeon 是 Intel Corporation 於美國及（或）其他國家或地區之商標。

Internet Explorer、Microsoft 和 Windows 是 Microsoft 集團旗下公司的商標。

Linux 是 Linus Torvalds 的註冊商標。

其他公司、產品或服務名稱，可能是第三者的商標或服務標誌。

重要聲明

處理器速度表示微處理器的內部時脈速度；其他因素也會影響應用程式效能。

CD 或 DVD 光碟機速度是可變的讀取速率。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量時，KB 代表 1,024 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量時，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用 Lenovo 提供的目前所支援最大容量的硬碟來替換任何標準硬碟，並裝滿所有硬碟機槽時的容量。

記憶體上限的計算可能需要使用選配記憶體模組，來更換標準記憶體。

每一個固態記憶體蜂巢都具有本質上可以引起且數目固定的寫入循環。因此，固態裝置具有可以承受的寫入週期數上限，並以 **total bytes written** (TBW) 表示。超出此限制的裝置可能無法回應系統產生的指令，或資料可能無法接受寫入。Lenovo 將依裝置的「正式發佈規格」中所載明，不負責更換已超出其保證的程式/消除循環數目上限的裝置。

Lenovo 對於非 Lenovo 產品不負有責任或保固。非 Lenovo 產品皆由協力廠商提供支援，Lenovo 不提供任何支援。

部分軟體可能與其零售版（若有）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（包括金屬碎屑或微粒），以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，可能會對本文件中所說明的裝置造成危險。

由於過度密集的微粒或過高濃度的有害氣體所引發的危險，其所造成的損壞包括可能導致裝置故障或完全停止運作。此規格提出微粒及氣體的限制，以避免這類的損壞。這些限制不得視為或是用來作為明確的限制，因為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。在欠缺本文件提出之特定限制的情況下，您必須實作維護符合人類健康與安全之微粒和氣體層次的實務。如果 Lenovo 判定您環境中的微粒或氣體等級已經對裝置造成損害，Lenovo 可能會在實作適當補救措施以減輕這類環境污染時，視狀況修復或更換裝置或零件。實作這類矯正性測量是客戶的責任。

表格 67. 微粒及氣體的限制

污染	限制
微粒	• 根據「ASHRAE 標準 52.2[1]」，室內空氣必須以 40% 大氣灰塵點效率 (MERV 9) 持續過濾。 • 進入資料中心的空氣，必須使用符合 MIL-STD-282 的高效率微粒空氣 (HEPA) 過濾器來過濾達到 99.97% 的效率或更高。 • 微粒污染的溶解相對濕度必須超過 60%[2]。 • 室內不可以有傳導性污染物，如鋅鬚晶。
氣體	• 銅：G1 級，根據 ANSI/ISA 71.04-1985[3] • 銀：30 天內少於 300 Å 的腐蝕率
[1] ASHRAE 52.2-2008 - **依微粒大小測試一般通風空氣清靜裝置之清除效率的方法**。Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc. [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。	

表格 67. 微粒及氣體的限制（繼續）

污染	限制
[3] ANSI/ISA-71.04-1985。**處理測量及控制系統的環境條件：空氣污染**。Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.	

電信法規聲明

我們無法保證您所在國家/地區中，本產品連線至公用電信網路介面之絕對性。在進行任何此類連線之前，可能需要進行進一步的檢定。若有任何問題，請聯絡 Lenovo 業務代表或轉銷商。

電子放射聲明

將監視器連接至設備時，您必須使用指定的監視器纜線與監視器隨附的任何抗干擾裝置。

如需其他電子放射聲明，請參閱：

https://pubs.lenovo.com/

台灣 BSMI RoHS 宣告

單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛Lead (Pb)	汞Mercury (Hg)	鎘Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr^{+6})	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
機架	○	○	○	○	○	○
外部蓋板	○	○	○	○	○	○
機械組合件	–	○	○	○	○	○
空氣傳動設備	–	○	○	○	○	○
冷卻組合件	–	○	○	○	○	○
內存模塊	–	○	○	○	○	○
處理器模塊	–	○	○	○	○	○
鍵盤	–	○	○	○	○	○
調製解調器	–	○	○	○	○	○
監視器	–	○	○	○	○	○
滑鼠	–	○	○	○	○	○
電纜組合件	–	○	○	○	○	○
電源	–	○	○	○	○	○
儲備設備	–	○	○	○	○	○
電池匣組合件	–	○	○	○	○	○
有mech的電路卡	–	○	○	○	○	○
無mech的電路卡	–	○	○	○	○	○
雷射器	–	○	○	○	○	○

備考1.〝超出0.1 wt %〞及〝超出0.01 wt %〞係指限用物質之百分比含量超出百分比含量基準值。

Note1 : “exceeding 0.1wt%” and “exceeding 0.01 wt%” indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.

備考2.〝○〞係指該項限用物質之百分比含量未超出百分比含量基準值。

Note2 : “○”indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.

備考3.〝-〞係指該項限用物質為排除項目。

Note3 : The “-“ indicates that the restricted substance corresponds to the exemption.

台灣進出口聯絡資訊

您可以向相關聯絡人取得台灣進出口資訊。

委製商/進口商名稱: 台灣聯想環球科技股份有限公司
進口商地址: 台北市南港區三重路 66 號 8 樓
進口商電話: 0800-000-702

索引

i

k

l

m

n

o

p

r

s

t

u

v

w

X

、

乙

丨

人

广

延

微

心

手

支

攴

斤

日

曰

月

木

气

水

火

用

田

癶

皿

目

石

禾

竹

糸

羊

耒

耳

自

艸

衣

見

角

言

車

辵

酉

里

金

阜

隹

雨

青

韋

頁

Lenovo

產品編號：SP47A30085

Printed in China

(1P) P/N: SP47A30085