# Lenovo XClarity Administrator 規劃與安裝手冊，適用於 Docker 環境

4.3 版

**注意事項**

在使用本資訊及其支援的產品之前，請先閱讀 XClarity Administrator 線上文件中的一般和法律聲明。

**第四版 (2025 4 月)**

**© Copyright Lenovo 2022.**
**有限及限制權利注意事項：倘若資料或軟體係依據美國聯邦總務署 (General Services Administration, GSA) 的合約交付，其使用、重製或揭露須符合合約編號 GS-35F-05925 之規定。**

# 目錄


**目錄 . . . . . i**

**圖例 . . . . . iii**

**表格 . . . . . v**

**變更摘要 . . . . . vii**

**第 1 章. Lenovo XClarity Administrator 概觀 . . . . . 1**

**第 2 章. 規劃 XClarity Administrator . . 5**

授權和 90 天免費試用 . . . . . 5
硬體和軟體必要條件 . . . . . 5
防火牆和代理伺服器 . . . . . 8
埠可用性 . . . . . 8
管理考量 . . . . . 12
網路考量 . . . . . 13
IP 配置限制 . . . . . 13
網路類型 . . . . . 13
網路配置 . . . . . 14
安全考量 . . . . . 23
encapsulation 管理 . . . . . 23
加密管理 . . . . . 23
安全憑證 . . . . . 25
鑑別 . . . . . 26
使用者帳戶和角色群組 . . . . . 28
使用者帳戶安全 . . . . . 28
高可用性考量 . . . . . 28
Features on Demand . . . . . 29

**第 3 章. 安裝 Lenovo XClarity Administrator . . . . . 31**

單一資料和管理網路 . . . . . 31
步驟 1：將機箱、機架式伺服器及 Lenovo XClarity Administrator 主機的纜線連接到機架頂端交換器 . . . . . 33
步驟 2：配置機架頂端交換器 . . . . . 34
步驟 3：配置 Chassis Management Module (CMM) . . . . . 34
步驟 4：配置 Flex 交換器 . . . . . 35
步驟 5：安裝及配置主機 . . . . . 36
步驟 6. 安裝和配置 XClarity Administrator . . 37
實體分離資料和管理網路 . . . . . 40
步驟 1：將機箱、機架式伺服器及 Lenovo XClarity Administrator 主機的纜線連接到機架頂端交換器 . . . . . 42
步驟 2：配置機架頂端交換器 . . . . . 42
步驟 3：配置 Chassis Management Module (CMM) . . . . . 43
步驟 4：配置 Flex 交換器 . . . . . 44
步驟 5：安裝及配置主機 . . . . . 45
步驟 6. 安裝和配置 XClarity Administrator . . 46
虛擬分離資料和管理網路拓撲 . . . . . 49
步驟 1：將機箱和機架式伺服器的纜線連接到機架頂端交換器 . . . . . 52
步驟 2：配置機架頂端交換器 . . . . . 52
步驟 3：配置 Chassis Management Module (CMM) . . . . . 53
步驟 4：配置 Flex 交換器 . . . . . 55
步驟 5：安裝及配置主機 . . . . . 56
步驟 6. 安裝和配置 XClarity Administrator . . 57
管理專用網路拓撲 . . . . . 60
步驟 1：將機箱、機架式伺服器及 Lenovo XClarity Administrator 主機的纜線連接到機架頂端交換器 . . . . . 62
步驟 2：配置機架頂端交換器 . . . . . 62
步驟 3：配置 Chassis Management Module (CMM) . . . . . 63
步驟 4：配置 Flex 交換器 . . . . . 64
步驟 5：安裝及配置主機 . . . . . 65
步驟 6. 安裝和配置 XClarity Administrator . . 65
實作高可用性 . . . . . 69

**第 4 章. 配置 Lenovo XClarity Administrator . . . . . 71**

初次存取 Lenovo XClarity Administrator Web 介面 . 71
建立使用者帳戶 . . . . . 74
配置網路存取 . . . . . 75
正在配置日期和時間 . . . . . 80
配置服務和支援 . . . . . 82
配置安全 . . . . . 84
管理裝置 . . . . . 84

**第 5 章. 註冊 XClarity Administrator . . . . . 95**

**第 6 章. 安裝可啟用完整功能的授權 . . 97**

使用 XClarity Administrator Web 介面安裝可啟用完整功能的授權 . . . . . 98
使用 Features on Demand 入口網站安裝啟用完整功能的授權 . . . . . 101

**第 7 章. 將 XClarity Administrator 做為容器更新 . . . . . 105**

將 XClarity Administrator 做為容器從 v4.0 更新到 v4.1 . . . . . 107


© Copyright Lenovo 2022

**第 8 章. 解除安裝 XClarity Administrator . . . . . 111**

# 圖例


1. 用於管理、資料和作業系統部署的單一網路實作範例 . . . . . 17
2. 實體分離資料和管理網路的實作範例，其中作業系統網路是資料網路的一部分 . . . . . 18
3. 實體分離資料和管理網路的實作範例，其中作業系統網路是管理網路的一部分 . . . . . 19
4. 虛擬分離資料和管理網路的實作範例，其中作業系統網路是資料網路的一部分 . . . . . 20
5. 虛擬分開的管理和資料網路實作範例，其中作業系統網路是管理網路的一部分 . . . . . 21
6. 不支援作業系統部署的管理專用網路範例實作 . . . . . 22
7. 支援作業系統部署的管理專用網路範例實作 . . . . . 22
8. 虛擬裝置的單一資料和管理網路拓撲範例 . . 32
9. 容器的單一資料和管理網路拓撲範例 . . . . 32
10. 單一資料和管理網路的纜線佈線範例 . . . . 33
11. Flex 交換器 在機箱中的位置 . . . . . 36
12. 虛擬裝置的實體分離資料和管理網路拓撲範例 . . . . . 41
13. 容器的實體分離資料和管理網路拓撲範例 . . 41
14. 實體分離資料和管理網路的纜線佈線範例 . . 42
15. Flex 交換器 在機箱中的位置 . . . . . 45
16. 虛擬裝置的虛擬分離資料和管理網路拓撲範例 . . . . . 50
17. 容器的虛擬分離資料和管理網路拓撲範例 . . 51
18. 虛擬分離資料和管理網路的纜線佈線範例 . . 52
19. 虛擬分離資料和管理網路 (VMware ESXi) 上的 Flex 交換器 範例配置，其中 VLAN 標記是在管理網路上啟用 . . . . . 53
20. 虛擬分離資料和管理網路 (VMware ESXi) 上的 Flex 交換器 範例配置，其中 VLAN 標記是在管理網路上啟用 . . . . . 56
21. 虛擬裝置的管理專用網路拓撲範例 . . . . . 61
22. 容器的管理專用網路拓撲範例 . . . . . 61
23. 管理專用網路的纜線連接範例 . . . . . 62
24. Flex 交換器 在機箱中的位置 . . . . . 65


© Copyright Lenovo 2022

# 表格

1. 根據網路拓撲的每個網路介面角色 . . . . 15
2. 根據網路拓撲的每個網路介面角色 . . . . 76

© Copyright Lenovo 2022

# 變更摘要

Lenovo XClarity Administrator 管理軟體的後續版本提供新硬體、軟體加強功能及修正程式的支援。

請參閱更新套件中提供的變更歷程檔案 (*.chg)，以取得修正程式的相關資訊。

如需所有支援硬體（包括伺服器、機箱及 Flex 交換器）的相關資訊，請參閱硬體和軟體必要條件。

如需舊版中的變更相關資訊，請參閱 XClarity Administrator 線上文件中的新功能。

此版本支援下列新硬體。

- **伺服器和設備**
  - ThinkEdge SE100 (7DGR)
  - ThinkSystem SC750 V4 (7DDJ)
  - ThinkSystem SR630 V4 (7DGA、7DGB、7DG8、7DG、7DLM)
  - ThinkSystem SR650 V4 (7DGC、7DGD、7DGE、7DGF、7DLN)
  - ThinkSystem SR680a V3 (7DM9)
- **交換器**
  - ThinkSystem DB710S (7DHN)
- **儲存裝置**
  - ThinkSystem DE4200H 混合 SAS（7DCA、7DCQ）
  - ThinkSystem DE4800F 全快閃儲存陣列（7DCC）
  - ThinkSystem DE4800H 混合 SAS（7DCB、7DCR、7DCS）
  - ThinkSystem DG5200 全快閃儲存陣列 (7DHY)
  - ThinkSystem DG7200 全快閃儲存陣列 (7DHZ)
  - ThinkSystem DM3200F 全快閃儲存陣列 (7DJ0)
  - ThinkSystem DM5200F 全快閃儲存陣列 (7DJ2)
  - ThinkSystem DM5200H 混合式快閃儲存陣列 (7DJ1)
  - ThinkSystem DM7200F 全快閃儲存陣列 (7DJ3)

此版本未增加規劃和安裝加強功能。

© Copyright Lenovo 2022

# 第 1 章　Lenovo XClarity Administrator 概觀

Lenovo XClarity Administrator 是一套集中式資源管理解決方案，可簡化基礎架構管理、加速回應以及提高 Lenovo® 伺服器系統和解決方案的可用性。其作用如同虛擬裝置，可以在安全的環境中為伺服器、網路和儲存硬體執行自動化探索、庫存、追蹤、監視以及供應程序。

**進一步瞭解：**

- XClarity Administrator：管理硬體就像管理 軟體
- XClarity Administrator：概觀

XClarity Administrator 為您提供集中式介面，方便您針對所有受管理的裝置執行下列功能。

**硬體管理**

XClarity Administrator 無須代理程式即可管理硬體。它可以自動探索可管理的裝置，包括伺服器、網路和儲存硬體。它會收集受管理裝置的庫存資料，可讓您快速檢視受管理硬體的庫存和狀態。

每一部支援的裝置各有數個管理作業，包括檢視狀態和內容，以及配置系統和網路設定、啟動管理介面、開關電源及遠端控制。如需管理裝置的相關資訊，請參閱管理機箱、管理伺服器和管理交換器（在 XClarity Administrator 線上文件中）。

**要訣：**XClarity Administrator 可管理的伺服器、網路和儲存硬體稱為*裝置*。受到 XClarity Administrator 管理的硬體則稱為*受管理的裝置*。

您可以使用 XClarity Administrator 中的機架檢視將受管理的裝置分組，以反映資料中心實際的機架設定。如需機架的相關資訊，請參閱管理機架（在 XClarity Administrator 線上文件中）。

**進一步瞭解：**

- XClarity Administrator：探索
- XClarity Administrator：庫存

© Copyright Lenovo 2022

- XClarity Administrator：遠端控制

**硬體監視**

XClarity Administrator 可讓您集中檢視受管理裝置產生的所有事件和警示。事件或警示會傳遞到 XClarity Administrator，並顯示在事件或警示日誌中。您可以從「儀表板」和「狀態列」檢視所有事件和警示的摘要資訊。此外，您也可以從裝置的「警示和事件」詳細資料頁面檢視特定裝置的事件和警示。

如需監視硬體的相關資訊，請參閱使用事件和使用警示（在 XClarity Administrator 線上文件中）。

**進一步瞭解：** XClarity Administrator：監視

**配置管理**

您可以使用一致的配置，為所有伺服器快速進行佈建和預先佈建。您可以將配置設定（例如本端儲存體、I/O 配接卡、開機設定、韌體、埠、管理控制器和 UEFI 設定）儲存為 Server Pattern，方便套用到一部或多部受管理的伺服器。當 Server Patterns 更新時，變更內容會自動部署至套用的伺服器。

此外，Server Pattern 也整合了虛擬化 I/O 位址的支援，所以您不必中斷光纖即可虛擬化 Flex System 光纖連線或重新規劃伺服器。

如需配置伺服器的相關資訊，請參閱使用 XClarity Administrator 配置伺服器（在 XClarity Administrator 線上文件中）。

**進一步瞭解：**

- XClarity Administrator：裸機到叢集
- XClarity Administrator：Configuration Patterns

**韌體相容性和更新**

為受管理的裝置指派韌體相符性原則，可簡化韌體管理。當您建立相符性原則並指派給受管理的裝置時，XClarity Administrator 會監視這些裝置的庫存變更，並標示出不符合標準的裝置。

當裝置不符合標準時，您可以使用 XClarity Administrator，從您管理的韌體更新儲存庫在該裝置中套用並啟動所有裝置的韌體更新。

**附註：**重新整理儲存庫及下載韌體更新時必須有網際網路連線。如果 XClarity Administrator 沒有網際網路連線，您可以手動將韌體更新匯入儲存庫。

如需韌體更新的相關資訊，請參閱更新受管理裝置上的韌體（在 XClarity Administrator 線上文件中）。

**進一步瞭解：**

- XClarity Administrator：裸機到叢集
- XClarity Administrator：韌體更新
- XClarity Administrator：供應韌體 安全更新

**作業系統部署**

您可以使用 XClarity Administrator 管理作業系統映像檔儲存庫，以及將作業系統映像檔同時部署至最多 28 部受管理的伺服器。

如需部署作業系統的相關資訊，請參閱部署作業系統映像檔（在 XClarity Administrator 線上文件中）。

**進一步瞭解：**

- XClarity Administrator：裸機到叢集
- XClarity Administrator：作業系統部署

**裝置鑑別**

XClarity Administrator 會使用下列方法向受管理機箱和伺服器進行鑑別。

- **受管理鑑別**。啟用受管理鑑別時，您在 XClarity Administrator 中建立的使用者帳戶就會用來鑑別受管理機箱和伺服器。

  如需使用者的相關資訊，請參閱管理使用者帳戶（在 XClarity Administrator線上文件中）。

- **本端鑑別**。停用受管理鑑別時，XClarity Administrator 中所定義的已儲存認證就會用來鑑別受管理伺服器。已儲存的認證必須對應至裝置上或 Active Directory 中的作用中使用者帳戶。

  如需已儲存認證的相關資訊，請參閱 XClarity Administrator 線上文件中的管理儲存的認證。

### 鑑別管理

XClarity Administrator 提供集中式驗證伺服器，方便建立和管理使用者帳戶，以及管理和驗證使用者認證。當您第一次啟動管理伺服器時，就會自動建立驗證伺服器。您為 XClarity Administrator 建立的使用者帳戶也可以在受管理鑑別模式下，用來登入受管理機箱和伺服器。如需使用者的相關資訊，請參閱管理使用者帳戶（在 XClarity Administrator線上文件中）。

XClarity Administrator 支援三種鑑別伺服器類型：

- **本端鑑別伺服器**。XClarity Administrator 預設配置為使用位於管理節點的本端鑑別伺服器。
- **外部 LDAP 伺服器**。目前只支援 Microsoft Active Directory。此伺服器必須位於連線至管理網路的外接式 Microsoft Windows 伺服器。使用外部 LDAP 伺服器時，會停用本端鑑別伺服器。
- **外部 SAML 2.0 識別提供者**。目前支援 Microsoft Active Directory Federation Services (AD FS)。除了輸入使用者名稱及密碼外，還可以設定多重要素鑑別，透過要求 PIN 碼、讀取智慧卡和用戶端憑證等方式提供額外的安全性。

如需鑑別類型的相關資訊，請參閱管理鑑別伺服器（在 XClarity Administrator線上文件中）。

建立使用者帳戶時，您會為使用者帳戶指派預先定義或自訂的角色群組，以控制該使用者的存取層次。如需角色群組的相關資訊，請參閱建立角色群組（在 XClarity Administrator 線上文件中）。

XClarity Administrator 包含審核日誌，可提供使用者動作的歷程記錄，例如登入、建立新使用者或變更使用者密碼。如需審核日誌的相關資訊，請參閱使用事件（在 XClarity Administrator 線上文件中）。

### 安全性

如果您的環境必須符合 NIST SP 800-131A 標準，XClarity Administrator 可以協助您建構完全符合標準的環境。

XClarity Administrator 支援自簽 SSL 憑證（由內部憑證管理中心發出）和外部 SSL 憑證（由私人或商用 CA 發出）。

機箱與伺服器上的防火牆可以設定為僅接受來自 XClarity Administrator 的內送要求。

如需安全性的相關資訊，請參閱實作安全環境（在 XClarity Administrator 線上文件中）。

### 服務和支援

您可以將 XClarity Administrator 設定為當 XClarity Administrator 和受管理裝置中發生某些可服務事件時，自動收集並傳送診斷檔案給您偏好的服務供應商。您可以選擇透過 Call Home 將診斷檔案傳送給 Lenovo 支援 或使用 SFTP 傳送給其他服務供應商，也可以手動收集診斷檔案、開啟問題記錄並將診斷檔案傳送給 Lenovo 支援中心。

**進一步瞭解：** XClarity Administrator：服務和支援

### 使用 Script 達到作業自動化

XClarity Administrator 可以透過開放式 REST 應用程式開發介面 (API) 與更高階的外部管理和自動化平台整合。XClarity Administrator 透過 REST API 能輕易地整合您現有的管理基礎架構。

PowerShell 工具箱提供豐富的 cmdlet 庫，讓您從 Microsoft PowerShell 階段作業執行自動化供應和資源管理工作。Python 工具箱提供以 Python 為基礎的指令和 API 庫，讓您從 OpenStack 環境（例如

Ansible 或 Puppet）執行自動化供應和資源管理工作。這兩種工具箱都會為 XClarity Administrator REST API 提供介面，以便將下列功能自動化，例如：

- 登入 XClarity Administrator
- 管理和解除管理機箱、伺服器、儲存裝置和機架頂端交換器（裝置）
- 收集和檢視裝置和元件的庫存資料
- 在一部或多部伺服器上部署作業系統映像檔
- 使用 Configuration Patterns 來配置伺服器
- 將韌體更新套用至裝置

### 與其他受管理的軟體整合

XClarity Administrator 模組整合 XClarity Administrator 與協力廠商管理軟體，提供探索、監視、配置及管理功能，以降低支援裝置之日常系統管理工作的成本和複雜度。

如需 XClarity Administrator 的相關資訊，請參閱下列文件：

- Microsoft System Center 適用的 Lenovo XClarity Integrator
- VMware vCenter 適用的 Lenovo XClarity Integrator

如需其他考量，請參閱管理考量。

**進一步瞭解：**

- Microsoft System Center 適用的 Lenovo XClarity Integrator 概觀
- VMware vCenter 適用的 Lenovo XClarity Integrator

### 文件

XClarity Administrator 的英文版文件定期於線上更新。如需最新資訊和程序，請參閱XClarity Administrator 線上文件。

線上文件提供下列語言版本：

- 德文 (de)
- 英文 (en)
- 西班牙文 (es)
- 法文 (fr)
- 義大利文 (it)
- 日文 (ja)
- 韓文 (ko)
- 巴西葡萄牙文 (pt-BR)
- 俄文 (ru)
- 泰文 (th)
- 簡體中文 (zh-CN)
- 繁體中文 (zh-TW)

預設顯示英文。您可以用下列方式來變更線上文件的語言。

- 從橫幅中的語言下拉功能表中選取您的語言。
- 在 `https://pubs.lenovo.com/lxca/` 之後加上 *`<language_code>`*，例如，若要顯示簡體中文版的線上文件。
  `https://pubs.lenovo.com/lxca/zh-CN/lxca_overview`

# 第 2 章　規劃 XClarity Administrator

安裝 Lenovo XClarity Administrator 前，請檢閱下列考量以協助您規劃安裝和日常管理。

## 授權和 90 天免費試用

Lenovo XClarity Administrator 提供免費的 90 天試用版授權，您可以在這段期間內充分利用所有可用功能。

您可以按一下 XClarity Administrator 標題列上的使用者動作功能表 (ADMIN_USER)，然後按一下**關於**，以判斷授權狀態，包括試用授權的剩餘天數。

XClarity Administrator 支援下列授權。

- **Lenovo XClarity Pro**。每份授權都會為單一裝置提供以下權利。
  - Lenovo XClarity Integrator 服務和支援
  - XClarity Administrator 服務和支援
  - XClarity Administrator 的進階功能：
    - 使用 Configuration Patterns 配置伺服器
    - 部署作業系統
    - 使用 Call Home 報告 XClarity Administrator 問題（硬體警示的 Call Home 不受影響。）

您必須為每個支援進階功能的受管理裝置購買授權。授權未與特定裝置連結。

授權的相符性由支援進階功能的受管理裝置數量決定。受管理裝置的數量不得超過所有作用中授權金鑰中的授權總數。如果 XClarity Administrator 不符合已安裝的授權（例如，授權過期或管理的其他裝置數量超過作用中授權總數），您將有 90 天的寬限期來安裝適當的授權。每當 XClarity Administrator 變成不符合標準時，寬限期便會重設為 90 天。如果寬限期 (包括免費試用) 結束時間在授權符合標準之前，則所有裝置上都會停用進階功能。

**附註：**

- 寬限期到期時，伺服器配置和作業系統部署功能便會停用。
- 授權不符合標準時，XClarity Administrator 問題的 Call Home（軟體 Call Home 功能）便會停用。此功能沒有寬限期。但是，硬體警示的 Call Home 不受影響。

如果已安裝授權，升級至新版 XClarity Administrator 時就*不*需要新授權。

如需購買 Lenovo XClarity Pro 授權的相關資訊，請聯絡您的 Lenovo 業務代表或授權事業夥伴。

如需安裝授權的相關資訊，請參閱 XClarity Administrator 線上文件中的安裝可啟用完整功能的授權 。

## 硬體和軟體必要條件

Lenovo XClarity Administrator 管理裝置會在主機系統上的虛擬機器中執行。

### Hypervisor 需求

#### 容器環境

將 XClarity Administrator 做為容器執行時，支援下列容器環境。

- Docker v20.10.9
- Docker-compose v1.29.2

© Copyright Lenovo 2022

### Hypervisor

將 XClarity Administrator 做為虛擬裝置執行時，支援下列 Hypervisor。

- Citrix Hypervisor v8.2
- Citrix XenServer v7.6
- CentOS 8[1]
- 已安裝 Hyper-V 的 Microsoft Windows Server 2022
- 已安裝 Hyper-V 的 Microsoft Windows Server 2019
- Nutanix Acropolis Hypervisor (AHV)
- 已安裝核心型虛擬機器 (KVM) v6.2.0 的 Red Hat Enterprise Linux v9.x
- 已安裝 KVM v2.12.0 的 RedHat Enterprise Linux v8.x
- 已安裝 KVM v7.0.0 的 Rocky Linux 8.x 和 9.x
- 已安裝 KVM v6.2.0 的 Ubuntu Server 22.04.x
- 已安裝 KVM v4.2.3 的 Ubuntu Server 20.04.2 LTS
- VMware ESXi 8.0
- VMware ESXi 7.0、U1、U2 和 U3
- VMware ESXi 6.7、U1、U2[2] 和 U3

**附註：**

1. Red Hat 不再更新 CentOS Linux。請考慮遷移至 Red Hat Enterprise Linux（請參閱 Red Hat：如何從 CentOS 或 Oracle Linux 轉換為 RHEL 網頁）。
2. 若是 VMware ESXi 6.7 U2，您必須使用 ISO 映像檔 VMware-ESXi-6.7.0.update02-13981272-LNV-20190630.iso 或更高版本。

針對 VMware 和 Citrix，虛擬機器是做為 OVF 範本提供。針對 Hyper-V 和 Nutanix AHV，虛擬機器為虛擬磁碟映像檔 (VHD)。針對 CentOS 和 KVM，虛擬機器是以 qcow2 格式提供。

**重要事項：**若是以採用 2.6 核心基底的 Linux 來賓身分執行，且針對虛擬裝置使用大量記憶體的 Hyper-V 環境，您必須在 Hyper-V 管理員中的 Hyper-V 設定面板上停用非一致記憶體存取 (NUMA)。變更此設定後需要重新啟動 Hyper-V 服務，這樣做也會重新啟動所有執行中的虛擬機器。如果未停用此設定，XClarity Administrator 虛擬機器可能會在初次啟動期間發生問題。

### 硬體需求

XClarity Administrator 必須符合下列*最低需求*。根據您的環境規模和您使用的 Configuration Patterns 而定，可能會需要其他資源才能獲得最佳效能。

- 兩顆虛擬微處理器

  **附註：**XClarity Administrator v4.2 和更新版本需要使用 AVX 指令集。
  — Intel：Sandy Bridge 或更新版本的核心處理器、Tiger Lake 或更新版本的 Celeron 或 Pentium 處理器
  — AMD：Bulldozer 或更新版本的處理器
- 8 GB 記憶體
- 至少 192 GB 儲存空間供 XClarity Administrator 虛擬裝置使用。
- 以寬度 1024 像素的最低解析度顯示 (XGA)

下表列出根據裝置數目建議的最低配置。請切記，如果您執行最低配置，完成管理作業所花費的時間可能會比預期更久。對於供應作業（例如作業系統部署、韌體更新和伺服器配置），您可能需要暫時增加資源。

| 受管理裝置數目 | 虛擬 CPU/記憶體配置 |
|---|---|
| 0 - 100 部裝置 | 2 vCPU、8 GB RAM |
| 100 - 200 部裝置 | 4 vCPU、10 GB RAM |
| 200 - 400 部裝置 | 6 vCPU、12 GB RAM |
| 400 - 600 部裝置 | 8 vCPU、16 GB RAM |

| 受管理裝置數目 | 虛擬 CPU/記憶體配置 |
| --- | --- |
| 600 - 800 部裝置 | 10 vCPU、20 GB RAM |
| 800 - 1,000 部裝置 | 12 vCPU、24 GB RAM |

**附註：**

- 單一 XClarity Administrator 實例最多可支援 1,000 個裝置。
- 如需最新的建議事項及其他效能考量，請參閱 XClarity Administrator：效能指南 （白皮書）。
- 視受管理環境的規模以及安裝所用的 Pattern 而定，您可能需要增加資源以使效能維持在可接受的程度。若您經常由系統資源儀表板看到處理器使用情形顯示偏高或超高的值，請考慮增加 1 到 2 個虛擬處理器核心。如果記憶體用量在閒置時持續超過 80%，請考慮增加 1-2 GB 的 RAM。若您的系統按照上表定義的方式配置而有靈敏回應，請考慮延長虛擬機器的執行時間以便評估系統效能。
- 如需如何透過刪除不再需要的 XClarity Administrator 資源釋出磁碟空間的相關資訊，請參閱 XClarity Administrator 線上文件中的管理磁碟空間。

### 軟體需求

- **Orchestrator 伺服器**

  如果您使用多個 XClarity Administrator 實例管理大量裝置，可以使用 Lenovo XClarity Orchestrator 集中監視、管理、供應和分析。XClarity Orchestrator 可以支援不限數量的 XClarity Administrator 實例，這些實例可共同管理多達 **10,000** 個非 ThinkEdge 用戶端裝置。

  若要使用 Lenovo XClarity Orchestrator 管理 XClarity Administrator v4.0 或更新版本的實例，需要使用 XClarity Orchestrator v2.0 或更新版本。

- **鑑別伺服器**

  根據預設，XClarity Administrator 會使用本端「輕量型目錄存取通訊協定 (LDAP)」伺服器來鑑別使用者認證。您可以選擇使用外部鑑別伺服器。

  如果您選擇使用外部鑑別伺服器，則僅支援在 Windows Server 2008 或更新版本上執行的 Microsoft Active Directory。

  如果您選擇使用 SAML 識別提供者，則僅支援在 Windows Server 2012 上執行的 Microsoft Active Directory Federation Services (AD FS) 2.0 或更新版本。

- **NTP 伺服器**

  需有「網路時間通訊協定 (NTP)」伺服器，才能確保從受管理裝置收到之所有事件和警示的時間戳記與 XClarity Administrator 同步。確定可透過管理網路（通常是 Eth0 介面）存取 NTP 伺服器。

  **要訣：**請考慮使用 XClarity Administrator 安裝所在的主機系統做為 NTP 伺服器。這樣做就可確保能夠透過管理網路存取主機系統。

### 可管理的資源

一個 XClarity Administrator 實例可以管理、監視和供應最多 **1,000** 個實體裝置。

您可以從 XClarity Administrator 支援 — 相容性 網頁找到受支援裝置和選配產品（例如 I/O、DIMM 和儲存體配接卡）、最低所需韌體版本和限制考量的完整清單，方法是按一下 **Compatibility（相容性）**標籤，然後按一下適當裝置類型的鏈結。

如需特定裝置的硬體配置與選項的一般資訊，請參閱 Lenovo Server Proven 網頁。

**限制：**如果 XClarity Administrator 安裝所在的主機系統是受管理機架式伺服器或計算節點，您就無法使用 XClarity Administrator 一次將韌體更新套用至該主機系統或整個機箱。將韌體更新套用至主機系統時，必須重新啟動主機系統。重新啟動主機系統也會一併重新啟動 XClarity Administrator，如此就無法使用 XClarity Administrator 來完成主機系統上的更新。

### 支援的 Web 瀏覽器

XClarity Administrator Web 介面可搭配下列 Web 瀏覽器使用。

- Chrome™ 48.0 或更新版本（對於遠端主控台，則需要 55.0 或更高版本）
- Firefox® ESR 38.6.0 或更新版本
- Microsoft® Internet Explorer® 11
- Microsoft Edge
- Safari® 9.0.2 或更新版本（IOS7 或更新版本和 OS X）

## 防火牆和代理伺服器

Lenovo XClarity Administrator 的部分功能需要存取網際網路，包括管理伺服器更新、韌體更新、服務與支援。如果您的網路中有防火牆，請配置防火牆，好讓 XClarity Administrator 管理伺服器能夠執行這些作業。如果管理伺服器無法直接存取網際網路，請將 XClarity Administrator 配置為使用代理伺服器。

### 防火牆

確認已在防火牆上開啟下列 DNS 名稱和連接埠。每個 DNS 代表一個具有動態 IP 位址且地理位置分散的系統。

| DNS 名稱 | 埠 | 通訊協定 |
|---|---|---|
| **下載授權啟動金鑰** | | |
| fod.lenovo.com | 443 | https |
| **擷取服務公告** | | |
| download.lenovo.com/servers/LXCA_Bulletin_Service.json | 443 | https |
| **下載更新（管理伺服器更新、韌體更新、UpdateXpress System Packs（OS 裝置驅動程式）和儲存庫套件）** | | |
| download.lenovo.com | 443 | https |
| support.lenovo.com | 443 | https 和 http |
| **將服務資料傳送至 Lenovo 支援中心 (Call Home)** | | |
| soaus.lenovo.com | 443 | https |
| logupload.lenovo.com/BLL/Logupload.ashx | 443 和 80 | https |
| **將服務資料傳送至 Lenovo 更新設備** | | |
| esupportwebapi.lenovo.com | 443 和 80 | https |
| **擷取保固資訊** | | |
| csapi.lenovo.com.cn（僅限中國） | 443 | https |
| supportapi.lenovo.com（全球） | 443 和 80 | https 和 http |

### 代理伺服器

如果管理伺服器無法直接存取網際網路，請確定將管理伺服器配置為使用 HTTP 代理伺服器（請參閱第 75 頁 「配置網路存取」）。

- 請確認代理伺服器設定為使用基本鑑別。
- 請確認 Proxy 伺服器設定為非終止的代理伺服器。
- 請確認代理伺服器設定為轉遞代理。
- 確認已配置負載平衡器維持與 Proxy 伺服器的階段作業，而不在其間切換。

## 埠可用性

根據在環境中實作防火牆的方式，必須可以使用數個埠。如果需要的埠遭到封鎖或由另一個程序使用，則部分 Lenovo XClarity Administrator 功能可能無法運作。

若要根據您的環境決定必須開放哪些埠，請檢閱下列幾節。下面幾節中的表格包含 XClarity Administrator 中如何使用各埠、受影響的受管理裝置、通訊協定 (TCP 或 UDP) 以及流量方向的相關資訊。*入埠*流量會辨識從受管理裝置或外部系統流向 XClarity Administrator 的流量，所以 XClarity Administrator 設備上一定要開啟這些埠。*出埠*流量是從 XClarity Administrator 流向受管理裝置。

- 存取 XClarity Administrator 伺服器
- XClarity Administrator 和受管理裝置之間的存取
- XClarity Administrator 和資料網路之間用於作業系統部署和裝置驅動程式更新的存取權

### 存取 XClarity Administrator 伺服器

如果 XClarity Administrator 伺服器和所有受管理裝置在防火牆後面，而且您想要從防火牆外部的瀏覽器存取這些裝置，則您必須確定 XClarity Administrator 埠已開放。如果您要使用 SNMP 和 SMTP 進行事件管理，可能還需要確定 XClarity Administrator 伺服器用於事件轉遞的埠已開放。

XClarity Administrator 伺服器會接聽下表中所列的埠，並透過這些埠回應。

**附註：**

- XClarity Administrator 是一個 RESTful 應用程式，在埠 443 透過 TCP 進行安全通訊。
- XClarity Administrator 可以選擇性地配置為與數個外部服務 (例如 LDAP、SMTP 或 Syslog) 建立出埠連線。這些連線可能需要使用者通常可配置且不包含在此清單中的其他埠，這些連線也可能需要對 TCP 或 UDP 埠 53 上網域名稱服務 (DNS) 伺服器的存取權，才能解析外部伺服器名稱。

| 服務 | 出埠 (外部系統的已開啟埠) | 入埠（XClarity Administrator 裝置的已開啟埠） |
|---|---|---|
| XClarity Administrator 裝置 | • DNS — TCP/UDP，埠 **53** | • HTTPS — TCP，埠 **443** |
| 外部鑑別伺服器 | • LDAP — TCP，埠 **389**[1]<br>• LDAPS — TCP，埠 **636**<br>• SAML 鑑別 — TCP，埠 **3268, 3269** | 不適用 |
| 事件轉遞服務 | • FTP 伺服器 — TCP，埠 **21**[1]<br>• 電子郵件伺服器 (SMTP) — UDP，埠 **25**[1]<br>• REST Web 服務 (HTTP) — TCP，埠 **80**[1]<br>• SNMP 管理程式 — UDP，埠 **161**[2]、**162**[1]<br>• MS Azure — UDP，埠 **443**[1]<br>• Syslog — UDP，埠 **514**[1]<br>• Apple 推送 [3] — TCP，埠 **443**、**2195**、**5223**<br>• Google 推送 [4] — TCP，埠 **443**、**5288**、**5299**、**5230** | • SNMP — UDP，埠 **161** |
| Lenovo 服務 (包括 Call Home) | • Warranty (僅限中國) — TCP，埠 **83**[5]<br>• HTTPS (Call Home) — TCP，埠 **443** | 不適用 |

1. 這是預設埠。您可從使用者介面設定這個埠。
2. 搭配使用者鑑別進行 SNMP 事件轉遞時將會使用這個埠。

3. 當防火牆或者行動資料專用的私人存取點名稱 (APN) 使用 Wi-Fi 時，開啟這個埠。此埠上的 APN 伺服器需要有直接的非代理連線。當裝置無法聯繫埠 5223 上的 Apple 推送通知服務時，此埠將僅用於 Wi-Fi 容錯回復。IP 位址範圍是 17.0.0.0/8。
4. 如需了解 IP 位址範圍，請參閱 Google ASN 15169。網域為 android.googleapis.com。
5. 雖然在中國境外不需要，但是 XClarity Administrator 可能還是會嘗試在其他國家或地區連線至此服務。

### XClarity Administrator 和受管理裝置之間的存取

如果受管理的裝置（如計算節點或機架式伺服器）在防火牆後面，而且如果您想要從該防火牆外部的 XClarity Administrator 伺服器管理這些裝置，您必須確定涉及 XClarity Administrator 和每個受管理裝置中的基板管理控制器之間通訊的所有埠都已開放。

如果您想要在受管理裝置上使用 XClarity Administrator 安裝作業系統，請務必在XClarity Administrator 和資料網路之間用於作業系統部署和裝置驅動程式更新的存取權中檢閱埠清單。

- **Flex chassis CMM**

| 裝置類型 | 出埠 (外部系統的已開啟埠) | 入埠（XClarity Administrator 裝置的已開啟埠） |
|---|---|---|
| Flex Chassis CMMs | — SLP — UDP/TCP，埠 **427**<br>— CIM HTTP — TCP，埠 **5988**[2]<br>— CIM HTTPS — TCP，埠 **5989**<br>— TCP 指令 — TCP，埠 **6090**[2]<br>— 安全 TCP 指令 — TCP，埠 **6091** | — SFTP — TCP，埠 **22**[1]<br>— CIM 指示 HTTPS — TCP **9090**<br>— LDAPS — TCP，埠 **50637** |

1. 此埠用於透過 SFTP 傳輸韌體更新。
2. 依預設，管理是透過安全埠執行。非安全埠則是可選的。

- **伺服器和計算節點**

| 裝置類型 | 出埠 (外部系統的已開啟埠) | 入埠（XClarity Administrator 裝置的已開啟埠） |
|---|---|---|
| ThinkSystem 和 ThinkAgile | — SSDP 探索 — UDP，埠 **1900**<br>— SFTP — TCP，埠 **115**[4]<br>— HTTPS — TCP，埠 **443**<br>— 遠端控制 — TCP，埠 **3888**[3]<br>— CIM HTTPS — TCP，埠 **5989**[8]<br>— 韌體更新 - TCP，埠 **6990**[4、7]<br>— SLP — UDP/TCP，埠 **427**[6] | — SFTP — TCP，埠 **22**[1]<br>— HTTPS — TCP，埠 **443**<br>— 韌體更新 - TCP，埠 **6990**[4、7]<br>— CIM 指示 HTTPS — TCP **9090**<br>— LDAPS — TCP，埠 **50636**[5]<br>— LDAPS — TCP，埠 **50637**[9] |
| System x | — SLP — UDP/TCP，埠 **427**<br>— HTTPS — TCP，埠 **443**<br>— IPMI — TCP，埠 **623**<br>— 遠端控制 — TCP，埠 **3888**[3]<br>— CIM HTTP — TCP，埠 **5988**[2]<br>— CIM HTTPS — TCP，埠 **5989**[2、8]<br>— 韌體更新 - TCP，埠 **6990**[4、7] | — SFTP — TCP，埠 **22**[1]<br>— HTTPS — TCP，埠 **443**<br>— 韌體更新 - TCP，埠 **6990**[4、7]<br>— CIM 指示 HTTPS — TCP **9090**[8]<br>— LDAPS — TCP，埠 **50636**[5]<br>— LDAPS — TCP，埠 **50637**[9] |

| 裝置類型 | 出埠 (外部系統的已開啟埠) | 入埠（XClarity Administrator 裝置的已開啟埠） |
|---|---|---|
| Flex System | — SLP — UDP/TCP，埠 **427**<br>— 遠端控制 — TCP，埠 **3888**[3]<br>— CIM HTTP — TCP，埠 **5988**[2]<br>— CIM HTTPS — TCP，埠 **5989**[2、8]<br>— 韌體更新 - TCP，埠 **6990**[4、7] | — SFTP — TCP，埠 **22**[1]<br>— HTTPS — TCP，埠 **443**<br>— 韌體更新 - TCP，埠 **6990**[4、7]<br>— CIM 指示 HTTPS — TCP **9090**<br>— LDAPS — TCP，埠 **50636**[5]<br>— LDAPS — TCP，埠 **50637**[9] |
| ThinkServer | — SNMP 設陷 — UDP，埠 **162**<br>— IPMI — UDP，埠 **623** | — SNMP 設陷 — UDP，埠 **162** |

1. 此埠用於透過 SFTP 傳輸韌體更新，上傳、下載和移除服務資料檔案，以及儲存由 BMU OS 在安全消除磁碟機資料時擷取的磁碟機清除工具。
2. 依預設，管理是透過安全埠執行。非安全埠則是可選的。
3. 遠端控制和遠端 KVM 是從 Web 瀏覽器啟動，而不是從 XClarity Administrator 伺服器啟動。
4. BMU 韌體更新需要使用此埠將韌體更新套件上傳到管理控制器。
5. 必須使用此埠才能使用 Configuration Patterns 配置伺服器。
6. 只有 ThinkSystem SR635 和 SR655 伺服器才需要此埠。
7. 在安全消除磁碟機資料時，需要使用此埠裝載 BMU 映像檔。此埠必須在基板管理控制器和 XClarity Administrator 設備中都保持開啟狀態。
8. 只有 ThinkSystem V1 伺服器才需要此埠。System X、Flex System 和 ThinkSystem V1 伺服器都需要此埠。
9. 使用受管理鑑別時需要此埠。

- **機架交換器和 Flex 交換器**

| 裝置類型 | 出埠 (外部系統的已開啟埠) | 入埠（XClarity Administrator 裝置的已開啟埠） |
|---|---|---|
| 機架交換器 | — SSH — TCP，埠 **22**[1、3]<br>— SNMP - UDP，埠 **161**[2]<br>— SLP — UDP/TCP，埠 **427**[6]<br>— HTTPS — TCP，埠 **443**[7] | — SFTP — TCP，埠 **22**[4]<br>— SNMP 設陷 — TCP，埠 **162**[2] |
| Flex 交換器 | — SSH — TCP，埠 **22**[3]<br>— SNMP - UDP，埠 **161**[5] | — SFTP — TCP，埠 **22**[4]<br>— SNMP 設陷 — TCP，埠 **162**[2] |

1. 使用 ENOS 機架交換器時，這個埠會用於配置 CMM 和 Flex 交換器之間使用的堆疊頭 (HoS) 認證、啟動韌體插槽，以及清除 SSH 主機金鑰，接著就能進行 SFTP 檔案傳輸作業。
2. 如果交換器位於不同於 XClarity Administrator 的網路上，XClarity Administrator 設備必須開啟這個埠（入埠），以便 XClarity Administrator 能接收這些裝置的事件。
3. 此埠用於管理 (SSH)。
4. 此埠用於透過 SFTP 傳輸韌體更新。
5. 使用 ENOS 機架交換器時，此埠用於傳輸庫存資料。
6. 此埠用於探索。
7. 此埠用於套用韌體更新。

- **儲存裝置**

| 裝置類型 | 出埠 (外部系統的已開啟埠) | 入埠（XClarity Administrator 裝置的已開啟埠） |
|---|---|---|
| 儲存裝置 | — FTP — TCP，埠 **21**<br>— SFTP— TCP，埠 **22**[2]<br>— SLP — UDP/TCP，埠 **427**<br>— HTTPS — TCP，埠 **443**[1]<br>— HTTPS — TCP，埠 **3031**[3] | — HTTPS — TCP，埠 **443**[2]<br>— SNMP 設陷 — UDP，埠 **115** |

1. 此埠用於傳輸韌體更新。
2. 此埠用於傳輸和套用韌體更新。
3. 此埠用於探索磁帶庫儲存裝置。

XClarity Administrator 和資料網路之間用於作業系統部署和裝置驅動程式更新的存取權

| 裝置類型 | 出埠 (外部系統的已開啟埠) | 入埠（XClarity Administrator 裝置的已開啟埠） |
|---|---|---|
| OS 部署[1、2、3] | | • SMB 通訊 — TCP，埠 **445**[4]<br>• HTTPS（ThinkServer 除外）— TCP，埠 **8443**[6] |
| OS 裝置驅動程式更新項目[2] | • WinRM over HTTP — TCP，埠 **5985**[5]<br>• WinRM over HTTPS — TCP，埠 **5986**[6] | • SMB 通訊 — TCP，埠 **445**[4] |

1. 如果您已為了使用作業系統部署網路而配置 XClarity Administrator 網路，則請務必開啟其相關埠。
2. 如需必須可供部署作業系統使用的埠清單，請參閱 XClarity Administrator 線上文件中的部署之作業系統的埠可用性。 例如，如果作業系統部署已配置為使用資料網路 (eth1)，則必須在該網路上開啟這些埠。
3. 每個 XClarity Administrator 實例具有僅用於 OS 部署的唯一憑證管理中心 (CA)。該 CA 會簽署用於埠 8443 上目標伺服器的憑證。起始 OS 部署時，會在推送至目標伺服器的 OS 映像檔中包含 CA 憑證。在部署程序期間，該伺服器會連回埠 8443，並確認埠 8443 在信號交換期間所提供的憑證，因為其具有 CA 憑證。
4. 此埠用於傳輸 Windows 驅動程式檔案。
5. 此埠用於連線至目標伺服器 WinRM。
6. 此埠用於在目標 OS 和 XClarity Administrator 之間交換資料，包括 OS 映像檔和狀態。

## 管理考量

管理裝置時，有數種不同的替代選項可供選擇。根據所要管理的裝置而定，您可能需要同時執行多個管理解決方案。

裝置只能由一個 Lenovo XClarity Administrator 實例管理。不過，您可以使用其他管理軟體（例如 VMware vRealize Operations Manager）搭配 Lenovo XClarity Administrator 來*監視* XClarity Administrator 管理的裝置。

**注意：**使用多種管理工具管理裝置時，應特別注意防止非預期的衝突發生。例如，使用其他工具提交電源狀態變更，可能會與 XClarity Administrator 中執行的配置或更新工作發生衝突。

### ThinkSystem、ThinkServer 和 System x 裝置

如果您打算使用其他管理軟體監視受管理裝置，請從 IMM 介面透過正確的 SNMP 或 IPMI 設定建立新的本端使用者。務必根據您的需要授與 SNMP 或 IPMI 專用權。

### Flex System 裝置

如果您想要使用其他管理軟體來監視受管理裝置，而該管理軟體使用 SNMPv3 或 IPMI 通訊，您必須針對每一個受管理 CMM 執行下列步驟讓您的環境準備就緒：

1. 使用 RECOVERY_ID 使用者名稱和密碼登入機箱的管理控制器 Web 介面。
2. 如果安全原則設定為**安全**，請變更使用者鑑別方法。
   a. 按一下 **Mgt Module Management → 使用者帳戶**。
   b. 按一下**帳戶**標籤。
   c. 按一下**廣域登入設定**。
   d. 按一下**一般**標籤。
   e. 選取**先外部，然後本端鑑別**做為使用者鑑別方法。
   f. 按一下**確定**。
3. 使用管理控制器 Web 介面上正確的 SNMP 或 IPMI 設定，建立新的本端使用者。
4. 如果您的安全原則設定為**安全**，請先登出管理控制器 Web 介面，再使用新的使用者名稱和密碼登入。出現提示時，變更新使用者的密碼。

您現在可以使用新使用者做為作用中 SNMP 或 IPMI 使用者。

**附註：**如果您解除管理機箱後，再次管理機箱，這個新使用者帳戶就會變成鎖定狀態並停用。在此情況下，請重複這些步驟以建立新的使用者帳戶。

## 網路考量

規劃 Lenovo XClarity Administrator 安裝時，請考慮您環境中實作的網路拓蹼，以及如何在該拓蹼中安排 XClarity Administrator。

**重要事項：**配置裝置和元件，以盡量減少 IP 位址變更。考慮使用靜態 IP 位址，而不使用動態主機配置通訊協定 (DHCP)。如果使用 DHCP，務必盡量減少 IP 位址變更。

## IP 配置限制

針對下列功能和受管理裝置，必須使用 IPv4 位址配置網路介面。不支援 IPv6 位址。
- Lenovo Storage 裝置的韌體更新
- ThinkServer 伺服器
- Lenovo Storage 裝置

不支援透過資料埠或管理埠使用 IPv6 鏈結本端來管理 RackSwitch 裝置。

不支援網路位址轉譯 (NAT)，它會將某一個 IP 位址空間重新對應到另一個。

## 網路類型

一般而言，大部分的環境會實作下列類型的網路。根據您的需求，您可能只會實作其中一個網路，或者您可能會實作全部三個網路。

- **管理網路**

  管理網路通常會保留給 Lenovo XClarity Administrator 和受管理裝置的管理處理器之間的通訊。例如，系統可能會將管理網路配置為包含 XClarity Administrator、每個受管理機箱的 CMM，以及 XClarity Administrator 所管理的每個伺服器的基板管理控制器。

- **資料網路**

  資料網路通常用於伺服器上所安裝的作業系統和公司內部網路、網際網路或兩者之間的通訊。

- **作業系統部署網路**

  在某些情況下，作業系統部署網路的設定會將在伺服器上部署作業系統所需的通訊區隔開。如果經過實作，此網路通常包含 XClarity Administrator 和所有伺服器主機。

您可以選擇在管理網路或資料網路中結合這個功能，而不實作個別的作業系統部署網路。

## 網路配置

您可以配置 Lenovo XClarity Administrator 使用一個或兩個網路介面。

**注意：**

- 管理裝置後變更 XClarity Administrator 的 IP 位址可能導致 XClarity Administrator 中的裝置處於離線狀態。請確定變更 IP 位址之前，已解除管理所有裝置。
- 按一下**重複 IP 位址檢查**切換開關，可以啟用或停用檢查相同子網路的重複 IP 位址。預設為停用。啟用時，如果您嘗試變更 XClarity Administrator 的 IP 位址，或管理的裝置與管理中的其他裝置或相同子網路中找到的其他裝置具有相同的 IP 位址，則 XClarity Administrator 會發出警示。

  **附註：**啟用後，XClarity Administrator 會執行 ARP 掃描來尋找同一個子網路中的作用中 IPv4 裝置。若要防止 ARP 掃描，請停用**重複的 IP 位址檢查**。
- 將 XClarity Administrator 做為虛擬裝置執行時，如果管理網路的網路介面配置為使用動態主機配置通訊協定 (DHCP)，則 DHCP 租賃到期時，管理介面 IP 位址可能會變更。如果 IP 位址變更，您必須將機箱、機架式和直立式伺服器解除管理，然後再次將它們納入管理。為避免此問題發生，請將管理介面變更為靜態 IP 位址，或確認已設定 DHCP 伺服器配置，讓 DHCP 位址依據 MAC 位址，或使 DHCP 租賃不會到期。
- 如果您*不想*使用 XClarity Administrator 來部署作業系統或更新 OS 裝置驅動程式，您可以停用 Samba 和 Apache 伺服器，方法是將網路介面變更為使用**僅探索和管理硬體**選項。請注意，變更網路介面之後會重新啟動管理伺服器。
- 將 XClarity Administrator 做為容器執行時，請確保在主機系統上設定了 macvlan 網路。

XClarity Administrator 有兩個單獨的網路介面可為您的環境定義，具體取決於您實作的網路拓撲。若是虛擬裝置，這些網路命名為 eth0 和 eth1。若是容器，您可以選擇自訂名稱。

- 只有一個網路介面 (eth0) 存在時：
  - 介面必須配置為可支援裝置探索和管理（例如伺服器配置和韌體更新）。它必須能與每一個受管理機箱中的 CMM 和 Flex 交換器、每一部受管理伺服器中的基板管理控制器，以及每個 RackSwitch 交換器進行通訊。
  - 如果您想要使用 XClarity Administrator 取得韌體和 OS 裝置驅動程式更新，至少一個網路介面必須連線至網際網路，最好是透過防火牆。否則，您必須將更新項目匯入儲存庫。
  - 如果您想要收集服務資料或使用自動問題通知（包括 Call Home 及 Lenovo 上傳設備），則至少一個網路介面必須連線至網際網路，最好是透過防火牆。
  - 如果您想要部署作業系統映像檔及更新 OS 裝置驅動程式，則介面必須具有可用於連接伺服器網路介面、存取主機作業系統的 IP 網路連線功能。

    **附註：**如果您實作另一網路進行 OS 部署及 OS 裝置驅動程式更新，可以將第二個網路介面配置為連線至該網路，而非資料網路。不過，如果各伺服器的作業系統無法存取資料網路，請在伺服器上配置其他介面，讓主機作業系統能夠連線至資料網路以進行 OS 部署及 OS 裝置驅動程式更新（如有需要）。
- 有兩個網路介面（eth0 和 eth1）存在時：
  - 第一個網路介面（通常是 Eth0 介面）必須連線至管理網路，並且配置為可支援裝置探索和管理（包括伺服器配置和韌體更新）。它必須能與每一個受管理機箱中的 CMM 和 Flex 交換器、每一部受管理伺服器中的管理控制器，以及每個 RackSwitch 交換器進行通訊。
  - 第二個網路介面（通常是 eth1 介面）可以配置為與內部資料網路、公用資料網路或兩者進行通訊。
  - 如果您想要使用 XClarity Administrator 取得韌體和 OS 裝置驅動程式更新，至少一個網路介面必須連線至網際網路，最好是透過防火牆。否則，您必須將更新項目匯入儲存庫。
  - 如果您想要收集服務資料或使用自動問題通知（包括 Call Home 及 Lenovo 上傳設備），則至少一個網路介面必須連線至網際網路，最好是透過防火牆。

— 如果您想要部署作業系統映像檔及更新 OS 裝置驅動程式，可以選擇使用 eth1 或 eth0 介面。不過，您所使用的介面必須具有連接伺服器網路介面、存取主機作業系統的 IP 網路連線功能。

**附註：**如果您實作另一網路進行 OS 部署及 OS 裝置驅動程式更新，可以將第二個網路介面配置為連線至該網路，而非資料網路。不過，如果各伺服器的作業系統無法存取資料網路，請在伺服器上配置其他介面，讓主機作業系統能夠連線至資料網路以進行 OS 部署及 OS 裝置驅動程式更新（如有需要）。

下表根據您環境中實作的網路拓蹼類型，顯示 XClarity Administrator 網路介面可能的配置。請使用此表判斷如何定義每個網路介面。

*表格 1. 根據網路拓撲的每個網路介面角色*

| 網路拓蹼 | 介面 1 (eth0) 的角色 | 介面 2 (eth1) 的角色 |
|---|---|---|
| 聚合網路（支援 OS 部署及 OS 裝置驅動程式更新的管理和資料網路） | 管理網路<br>• 探索和管理<br>• 伺服器配置<br>• 韌體更新<br>• 服務資料收集<br>• 自動問題通知（如 Call Home 及 Lenovo 更新設備）<br>• 保固資料擷取<br>• 作業系統部署<br>• OS 裝置驅動程式更新項目 | 無 |
| 單獨的管理網路支援 OS 部署及 OS 裝置驅動程式更新和資料網路 | 管理網路<br>• 探索和管理<br>• 伺服器配置<br>• 韌體更新<br>• 服務資料收集<br>• 自動問題通知（如 Call Home 及 Lenovo 更新設備）<br>• 保固資料擷取<br>• 作業系統部署<br>• OS 裝置驅動程式更新項目 | 資料網路<br>• 無 |
| 單獨的管理網路和支援 OS 部署及 OS 裝置驅動程式更新的資料網路 | 管理網路<br>• 探索和管理<br>• 伺服器配置<br>• 韌體更新<br>• 服務資料收集<br>• 自動問題通知（如 Call Home 及 Lenovo 更新設備）<br>• 保固資料擷取 | 資料網路<br>• 作業系統部署<br>• OS 裝置驅動程式更新項目 |
| 單獨的管理網路和未支援 OS 部署及 OS 裝置驅動程式更新的資料網路 | 管理網路<br>• 探索和管理<br>• 伺服器配置<br>• 韌體更新<br>• 服務資料收集<br>• 自動問題通知（如 Call Home 及 Lenovo 更新設備）<br>• 保固資料擷取 | 資料網路<br>• 無 |
| 僅管理網路（不支援 OS 部署及 OS 裝置驅動程式更新） | 管理網路<br>• 探索和管理<br>• 伺服器配置<br>• 韌體更新<br>• 服務資料收集<br>• 自動問題通知（如 Call Home 及 Lenovo 更新設備）<br>• 保固資料擷取 | 無 |

## 單一資料和管理網路

在此網路拓撲中，管理通訊、資料通訊和作業系統部署可以在相同的網路進行。此拓撲也稱為*聚合*網路。

**重要事項：**根據您的網路配置（例如，如果來自伺服器的資料流量有高優先順序，而來自管理控制器的資料流量有低優先順序），實作共用資料和管理網路可能會導致資料流量中斷，例如，封包遭到丟棄或管理網路連線問題。管理網路除了 TCP 之外，還會使用 UDP 資料流量。當網路資料流量高時，UDP 資料流量的優先順序可能會比較低。

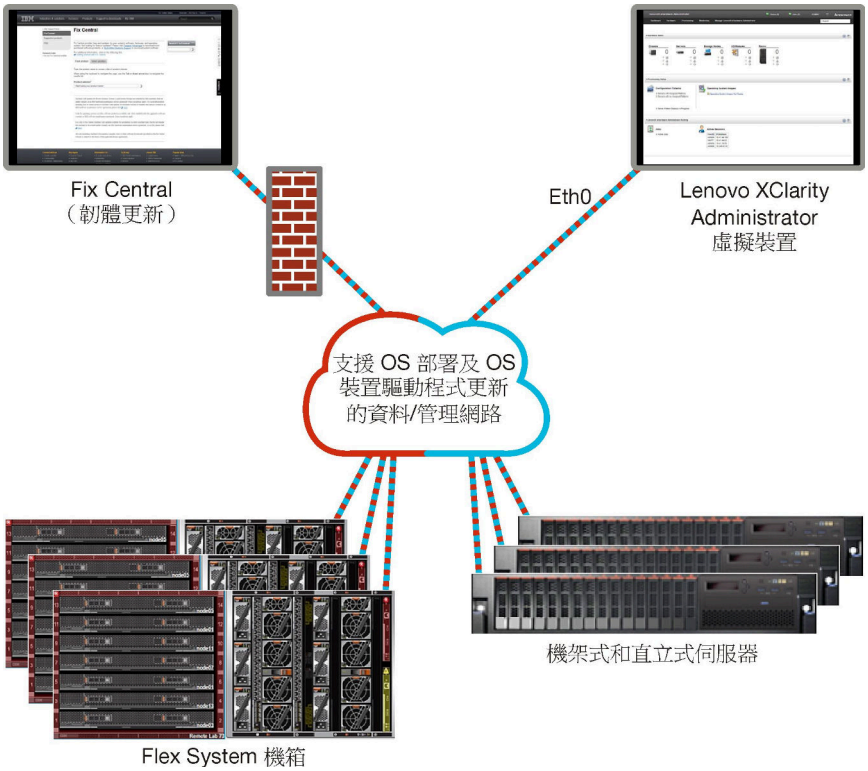
當您安裝 Lenovo XClarity Administrator 時，請使用下列考量定義 eth0 網路介面：

- 介面必須配置為可支援裝置探索和管理（例如伺服器配置和韌體更新）。它必須能與每一個受管理機箱中的 CMM 和 Flex 交換器、每一部受管理伺服器中的基板管理控制器，以及每個 RackSwitch 交換器進行通訊。
- 如果您想要使用 XClarity Administrator 取得韌體和 OS 裝置驅動程式更新，至少一個網路介面必須連線至網際網路，最好是透過防火牆。否則，您必須將更新項目匯入儲存庫。
- 如果您想要收集服務資料或使用自動問題通知（包括 Call Home 及 Lenovo 上傳設備），則至少一個網路介面必須連線至網際網路，最好是透過防火牆。
- 如果您想要部署作業系統映像檔及更新 OS 裝置驅動程式，則介面必須具有可用於連接伺服器網路介面、存取主機作業系統的 IP 網路連線功能。

  **附註：**如果您實作另一網路進行 OS 部署及 OS 裝置驅動程式更新，可以將第二個網路介面配置為連線至該網路，而非資料網路。不過，如果各伺服器的作業系統無法存取資料網路，請在伺服器上配置其他介面，讓主機作業系統能夠連線至資料網路以進行 OS 部署及 OS 裝置驅動程式更新（如有需要）。
- 只有在您實作單一資料和管理網路拓撲，或虛擬分離資料和管理網路拓撲時，您才可以在符合 XClarity Administrator 需求的任何系統上設定 XClarity Administrator，包括受管理伺服器，但是您無法使用 XClarity Administrator 將韌體更新套用到該受管理伺服器。即使是這樣，使用立即啟動才能套用部分韌體，而且 XClarity Administrator 會強制目標伺服器重新啟動，這也會重新啟動 XClarity Administrator。使用延遲啟動套用時，只有在重新啟動 XClarity Administrator 主機時，才會套用部分韌體。

您也可以配置第二個網路介面，從 XClarity Administrator 連線至同一網路以支援備援。

下圖顯示聚合網路拓撲的實作範例。




*圖例 1. 用於管理、資料和作業系統部署的單一網路實作範例*

## 實體分離資料和管理網路

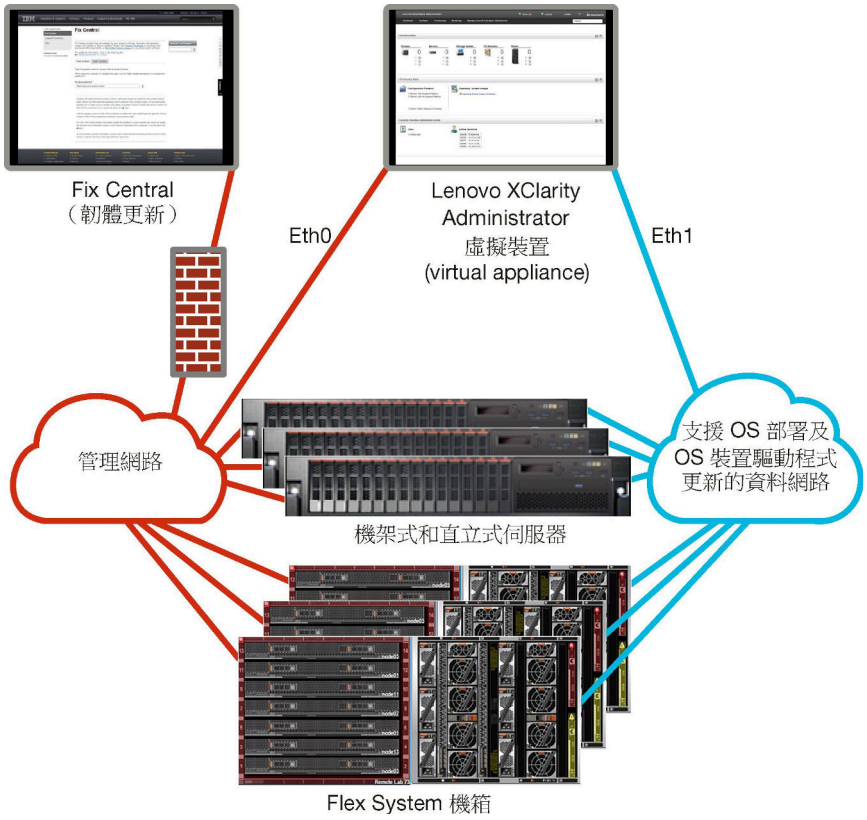
在此網路拓撲中，管理網路與資料網路實際上是分開的網路，而且作業系統部署網路會配置為管理網路或資料網路的一部分。

當您安裝 Lenovo XClarity Administrator 時，請使用下列考量定義網路設定：

- 第一個網路介面（通常是 Eth0 介面）必須連線至管理網路，並且配置為可支援裝置探索和管理（包括伺服器配置和韌體更新）。它必須能與每一個受管理機箱中的 CMM 和 Flex 交換器、每一部受管理伺服器中的管理控制器，以及每個 RackSwitch 交換器進行通訊。
- 第二個網路介面（通常是 eth1 介面）可以配置為與內部資料網路、公用資料網路或兩者進行通訊。
- 如果您想要使用 XClarity Administrator 取得韌體和 OS 裝置驅動程式更新，至少一個網路介面必須連線至網際網路，最好是透過防火牆。否則，您必須將更新項目匯入儲存庫。
- 如果您想要收集服務資料或使用自動問題通知（包括 Call Home 及 Lenovo 上傳設備），則至少一個網路介面必須連線至網際網路，最好是透過防火牆。
- 如果您想要部署作業系統映像檔及更新 OS 裝置驅動程式，可以選擇使用 eth1 或 eth0 介面。不過，您所使用的介面必須具有連接伺服器網路介面、存取主機作業系統的 IP 網路連線功能。

  **附註：**如果您實作另一網路進行 OS 部署及 OS 裝置驅動程式更新，可以將第二個網路介面配置為連線至該網路，而非資料網路。不過，如果各伺服器的作業系統無法存取資料網路，請在伺服器上配置其他介面，讓主機作業系統能夠連線至資料網路以進行 OS 部署及 OS 裝置驅動程式更新（如有需要）。

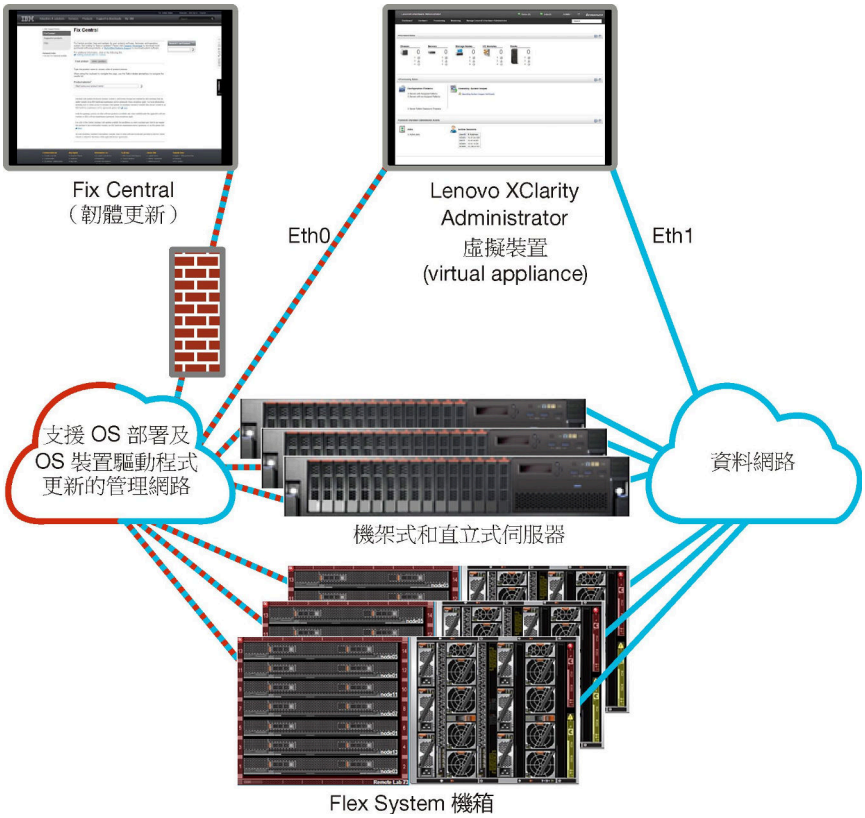
第 18 頁圖例 2 「實體分離資料和管理網路的實作範例，其中作業系統網路是資料網路的一部分」 顯示分開管理和資料網路的實作範例，其中作業系統部署網路會配置為資料網路的一部分。




*圖例 2. 實體分離資料和管理網路的實作範例，其中作業系統網路是資料網路的一部分*

第 19 頁圖例 3 「實體分離資料和管理網路的實作範例，其中作業系統網路是管理網路的一部分」 顯示分開管理和資料網路的另一個實作範例，其中作業系統部署網路會配置為管理網路的一部分。在此實作中，XClarity Administrator 不需要連線至資料網路。

**附註：**如果作業系統部署網路無法存取資料網路，請在伺服器上配置其他介面，讓伺服器上的主機作業系統可以連線至資料網路（如有需要）。




*圖例 3. 實體分離資料和管理網路的實作範例，其中作業系統網路是管理網路的一部分*

## 虛擬分離資料和管理網路

在此拓撲中，資料網路與管理網路是虛擬分開的。來自資料網路的封包以及來自管理網路的封包會透過相同的實體連線傳送。VLAN 標記用於所有管理網路資料封包以保留兩個分隔網路之間的資料流量。

**附註：**如果 Lenovo XClarity Administrator 是安裝在機箱中受管理伺服器上執行的主機上，則您無法使用 XClarity Administrator 一次將韌體更新套用到該整個機箱中。套用韌體更新時、必須重新啟動主機系統。

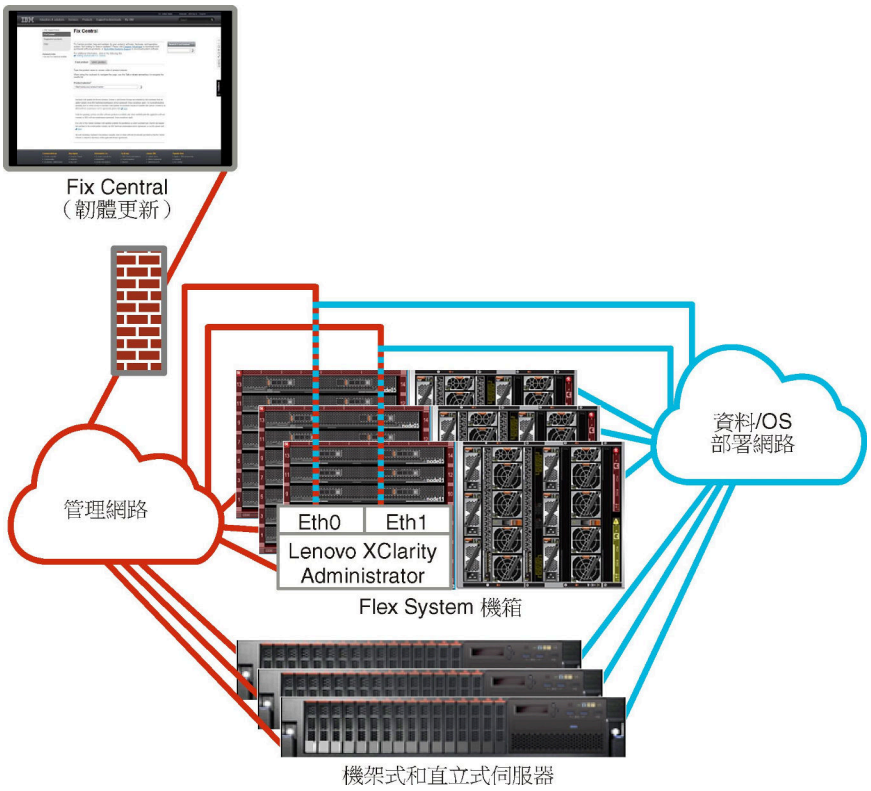
當您安裝 XClarity Administrator 時，請使用下列考量定義網路設定：

- 第一個網路介面（通常是 Eth0 介面）必須連線至管理網路，並且配置為可支援裝置探索和管理（包括伺服器配置和韌體更新）。它必須能與每一個受管理機箱中的 CMM 和 Flex 交換器、每一部受管理伺服器中的管理控制器，以及每個 RackSwitch 交換器進行通訊。
- 第二個網路介面（通常是 eth1 介面）可以配置為與內部資料網路、公用資料網路或兩者進行通訊。
- 如果您想要使用 XClarity Administrator 取得韌體和 OS 裝置驅動程式更新，至少一個網路介面必須連線至網際網路，最好是透過防火牆。否則，您必須將更新項目匯入儲存庫。
- 如果您想要收集服務資料或使用自動問題通知（包括 Call Home 及 Lenovo 上傳設備），則至少一個網路介面必須連線至網際網路，最好是透過防火牆。
- 如果您想要部署作業系統映像檔及更新 OS 裝置驅動程式，可以選擇使用 eth1 或 eth0 介面。不過，您所使用的介面必須具有連接伺服器網路介面、存取主機作業系統的 IP 網路連線功能。

  **附註：**如果您實作另一網路進行 OS 部署及 OS 裝置驅動程式更新，可以將第二個網路介面配置為連線至該網路，而非資料網路。不過，如果各伺服器的作業系統無法存取資料網路，請在伺服器上配置其他介面，讓主機作業系統能夠連線至資料網路以進行 OS 部署及 OS 裝置驅動程式更新（如有需要）。

- 只有在您實作單一資料和管理網路拓撲，或虛擬分離資料和管理網路拓撲時，您才可以在符合 XClarity Administrator 需求的任何系統上設定 XClarity Administrator，包括受管理伺服器，但是您無法使用 XClarity Administrator 將韌體更新套用到該受管理伺服器。即使是這樣，使用立即啟動才能套用部分韌體，而且 XClarity Administrator 會強制目標伺服器重新啟動，這也會重新啟動 XClarity Administrator。使用延遲啟動套用時，只有在重新啟動 XClarity Administrator 主機時，才會套用部分韌體。

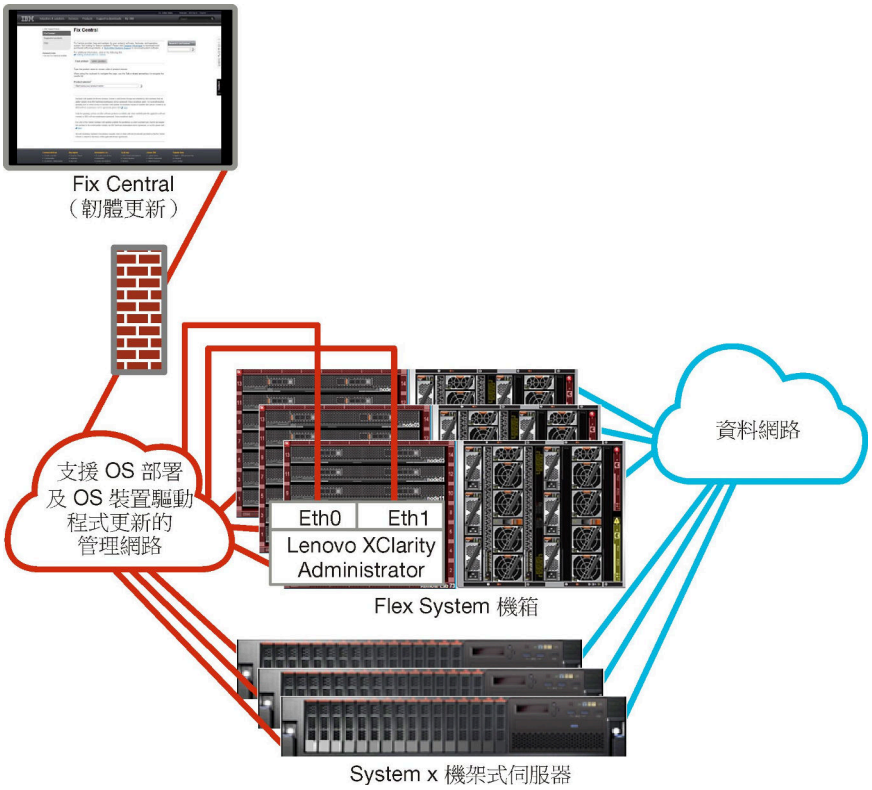
第 20 頁圖例 4 「虛擬分離資料和管理網路的實作範例，其中作業系統網路是資料網路的一部分」 顯示虛擬分開管理和資料網路的實作範例，其中作業系統部署網路會配置為資料網路的一部分。在此範例中，XClarity Administrator 是安裝在機箱內的受管理伺服器上。




*圖例 4. 虛擬分離資料和管理網路的實作範例，其中作業系統網路是資料網路的一部分*

第 21 頁圖例 5 「虛擬分開的管理和資料網路實作範例，其中作業系統網路是管理網路的一部分」 顯示虛擬分開管理和資料網路的實作範例，其中作業系統部署網路會配置為管理網路的一部分，而且 XClarity Administrator 是安裝在機箱內的受管理伺服器上。在此實作中，XClarity Administrator 不需要連線至資料網路。

**附註：**如果作業系統部署網路無法存取資料網路，請在伺服器上配置其他介面，讓伺服器上的主機作業系統可以連線至資料網路（如有需要）。




*圖例 5. 虛擬分開的管理和資料網路實作範例，其中作業系統網路是管理網路的一部分*

## 管理專用網路

在此拓蹼中，Lenovo XClarity Administrator 只能存取管理網路。它無法存取資料網路。不過，如果您想要從 XClarity Administrator 將作業系統映像檔部署至受管理伺服器，則 XClarity Administrator 必須能夠存取作業系統部署網路。

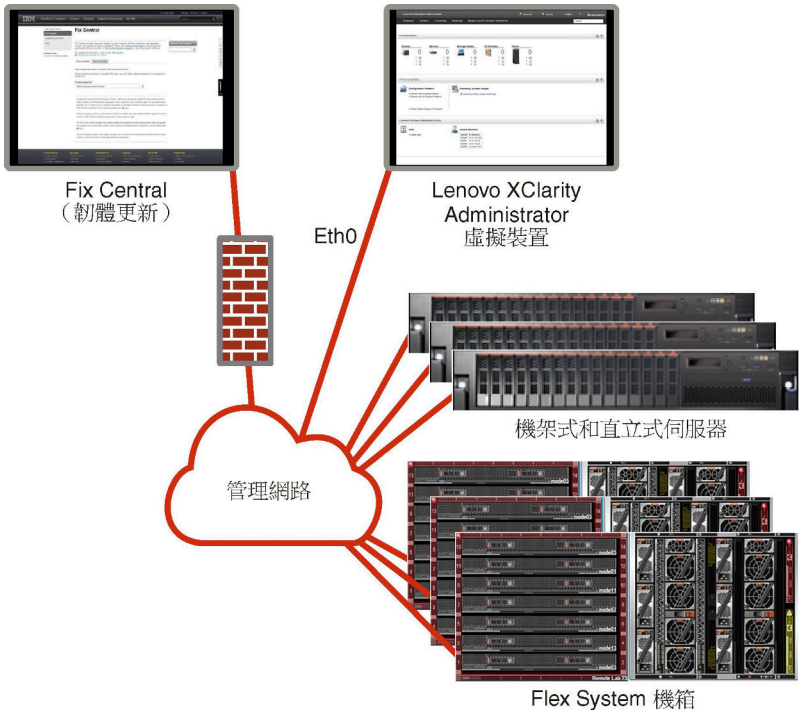
當您安裝 XClarity Administrator 並定義網路設定時，eth0 網路介面必須配置為：

- 介面必須配置為可支援裝置探索和管理（例如伺服器配置和韌體更新）。它必須能與每一個受管理機箱中的 CMM 和 Flex 交換器、每一部受管理伺服器中的基板管理控制器，以及每個 RackSwitch 交換器進行通訊。
- 如果您想要使用 XClarity Administrator 取得韌體和 OS 裝置驅動程式更新，至少一個網路介面必須連線至網際網路，最好是透過防火牆。否則，您必須將更新項目匯入儲存庫。
- 如果您想要收集服務資料或使用自動問題通知（包括 Call Home 及 Lenovo 上傳設備），則至少一個網路介面必須連線至網際網路，最好是透過防火牆。
- 如果您想要部署作業系統映像檔及更新 OS 裝置驅動程式，則介面必須具有可用於連接伺服器網路介面、存取主機作業系統的 IP 網路連線功能。

  **附註：**如果您實作另一網路進行 OS 部署及 OS 裝置驅動程式更新，可以將第二個網路介面配置為連線至該網路，而非資料網路。不過，如果各伺服器的作業系統無法存取資料網路，請在伺服器上配置其他介面，讓主機作業系統能夠連線至資料網路以進行 OS 部署及 OS 裝置驅動程式更新（如有需要）。

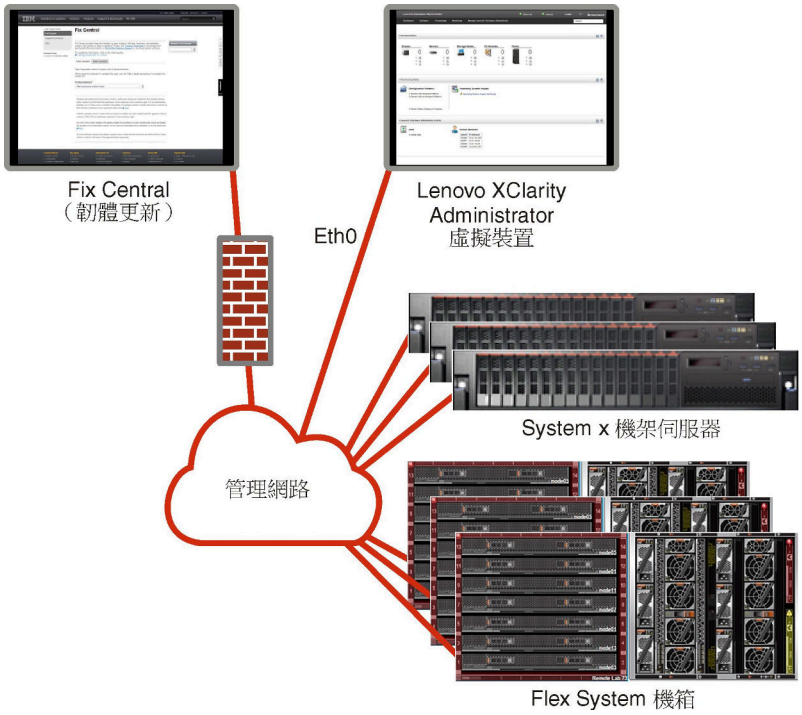
您也可以配置第二個網路介面，從 XClarity Administrator 連線至同一網路以支援備援。

第 22 頁圖例 6 「不支援作業系統部署的管理專用網路範例實作」 會顯示管理專用網路的範例實作，當中不支援從 XClarity Administrator 進行作業系統部署。




*圖例 6. 不支援作業系統部署的管理專用網路範例實作*

第 22 頁圖例 6 「不支援作業系統部署的管理專用網路範例實作」 會顯示管理專用網路的範例實作，當中可支援從 XClarity Administrator 進行作業系統部署。




*圖例 7. 支援作業系統部署的管理專用網路範例實作*

## 安全考量

規劃 Lenovo XClarity Administrator 及所有受管理裝置的安全。

## encapsulation 管理

在 Lenovo XClarity Administrator 中管理 Lenovo 機箱及伺服器時，可以配置 Lenovo XClarity Administrator 來變更裝置的防火牆規則，以便只接受從 Lenovo XClarity Administrator 傳入的要求。這稱為 *encapsulation*。您也可以在已經由 Lenovo XClarity Administrator 管理的機箱和伺服器啟用或停用 encapsulation。

在支援 encapsulation 的裝置上啟用時，Lenovo XClarity Administrator 會將裝置 encapsulation 模式變更為「encapsulationLite」，並會變更裝置的防火牆規則，以便只接受從此 Lenovo XClarity Administrator 傳入的要求。

停用時，encapsulation 模式會設為「正常」。如果先前已在裝置上啟用 encapsulation，便會移除 encapsulation 防火牆規則。

**注意：**如果已啟用 encapsulation，而且 XClarity Administrator 在裝置解除管理之前無法使用，則必須採取必要的步驟，停用 encapsulation 以建立與裝置的通訊。如需回復程序，請參閱 XClarity Administrator 線上文件中的在管理伺服器故障之後， 使用 CMM 回復機箱管理和在管理伺服器故障之後，回復機架式或直立式 伺服器管理。

**附註：**

- 交換器、儲存裝置、非 Lenovo 機箱和伺服器不支援 encapsulation。
- 當管理網路介面配置為使用動態主機配置通訊協定 (DHCP) 以及啟用 Encapsulation 時，管理機架式伺服器可能需要一段時間。

如需 Encapsulation 的相關資訊，請參閱 XClarity Administrator 線上文件中的啟用 encapsulation。

## 加密管理

加密管理是由通訊模式及通訊協定所構成，這些通訊模式及通訊協定可控制 Lenovo XClarity Administrator 和受管理裝置（例如，機箱、伺服器及 Flex 交換器）間處理安全通訊的方式。

### 加密演算法

XClarity Administrator 支援 TLS 1.2 和更強大的加密演算法以實現安全網路連線。

為了增加安全性，僅支援高強度密碼。用戶端作業系統和 Web 瀏覽器必須支援下列其中一個密碼組合。

- SSH-ED25519
- SSH-ED25519-CERT-V01@OPENSSH.COM
- ECDSA-SHA2-NISTP256
- ECDSA-SHA2-NISTP256-CERT-V01@OPENSSH.COM
- ECDSA-SHA2-NISTP384
- ECDSA-SHA2-NISTP384-CERT-V01@OPENSSH.COM
- ECDSA-SHA2-NISTP521
- ECDSA-SHA2-NISTP521-CERT-V01@OPENSSH.COM
- RSA-SHA2-512
- RSA-SHA2-256
- RSA-SHA2-384

### 管理伺服器的加密模式

此設定決定了從管理伺服器進行安全通訊所使用的模式。

- **相容性**。此模式是預設值。此模式與舊版韌體、瀏覽器，以及未實作為符合 NIST SP 800-131A 而需要之嚴密安全標準的其他網路用戶端相容。

- **NIST SP 800-131A**。此模式是針對符合 NIST SP 800-131A 標準而設計。XClarity Administrator 的設計是一律在內部使用強式加密法，並使用強式加密法網路連線（如果有的話）。不過，在此模式下，使用 NIST SP 800-131A 未核准之加密法的網路連線則在禁止之列，包括拒絕使用 SHA-1 或更弱雜湊簽章的傳輸層安全 (TLS) 憑證。

  如果您選取此模式：

  — 對於埠 8443 以外的所有埠，所有 TLS CBC 密碼和所有不支援完整轉寄密碼的密碼都會遭停用。

  — 事件通知可能不會成功推送到部分行動裝置訂閱（請參閱XClarity Administrator 線上文件中的轉遞事件至行動裝置）。外部服務（例如 Android 及 iOS）會呈現使用 SHA-1 簽章的憑證，而 SHA-1 是不符合需求較嚴密之 NIST SP 800-131A 模式的演算法。因此，與這些服務的任何連線都可能會失敗，並出現憑證異常狀況或信號交換失敗。

  如需 NIST SP 800-131A 相符性的相關資訊，請參閱XClarity Administrator 線上文件中的實作 NIST 800-131A 相符性。

如需在管理伺服器上設定安全性模式的相關資訊，請參閱 XClarity Administrator 線上文件中的設定加密法模式和通訊 協定。

### 受管理伺服器的安全性模式

此設定決定了從受管理伺服器進行安全通訊所使用的模式。

- **相容性安全性**。當服務和用戶端需要不符合 CNSA/FIPS 標準的加密法時，請選取此模式。此模式支援廣泛的加密演算法，並允許啟用所有服務。
- **NIST SP 800-131A**。請選取此模式以確定符合 NIST SP 800-131A 標準。這包括將 RSA 金鑰限制為 2048 位元或更大，將用於數位簽章的雜湊限制為 SHA-256 或更長，並確定只使用 NIST 核准的對稱加密演算法。此模式需要將 SSL/TLS 模式設定為 **TLS 1.2 伺服器用戶端**。

  ThinkSystem V1 和 V2 伺服器支援此模式。
- **標準安全性**。這是 ThinkSystem V3 和 V4 伺服器的預設安全性模式。請選取此模式以確定符合 FIPS 140-3 標準。為了使 XCC 在 FIPS 140-3 驗證模式下運作，只能啟用支援 FIPS 140-3 級加密法的服務。不支援 FIPS 140-2/140-3 級加密法的服務預設為停用，但可視需要啟用。如果啟用了任何使用非 FIPS 140-3 級加密法的服務，XCC 將無法在 FIPS 140-3 驗證模式下運作。此模式需要 FIP 層級憑證。
- **企業嚴格安全性**。這是 ThinkSystem V3 和 V4 伺服器最安全的模式。請選取此模式以確定符合 CNSA 標準。僅允許支援 CNSA 層級加密法的服務。非安全服務預設為停用，而且無法啟用。此模式需要 CNSA 層級憑證。

  XClarity Administrator 會對採用**企業嚴格安全性**模式的伺服器使用 RSA 3072 位元/SHA-384 憑證簽章。

  **重要事項：**

  — 要使用此模式，必須在每個選取的 ThinkSystem V3 和 V4 伺服器（搭載 XCC2 或 XCC3）上安裝 XCC Feature On Demand 金鑰。

  — 在此模式下，如果 XClarity Administrator 使用自簽憑證，則 XClarity Administrator 必須使用基於 RSA 3072 位元/SHA-384 的主要憑證和伺服器憑證。如果 XClarity Administrator 使用外部簽署憑證，則 XClarity Administrator 必須產生基於 RSA 3072 位元/SHA-384 的 CSR，並聯絡外部 CA 以簽署基於 RSA 3072 位元/SHA-384 的新伺服器憑證。

  — 當 XClarity Administrator 使用基於 RSA 3072 位元/SHA-384 的憑證時，XClarity Administrator 可能會中斷與裝置的連線，但下列裝置除外：Flex System 機箱 (CMMS) 和伺服器、ThinkSystem 伺服器、ThinkServer 伺服器、System x M4 和 M5 伺服器、Lenovo ThinkSystem DB 系列交換器、Lenovo RackSwitch、Flex System 交換器、Mellanox 交換器、ThinkSystem DE/DM 儲存裝置、IBM 磁帶庫儲存體，以及使用低於 22C 的韌體刷新的 ThinkSystem SR635/SR655 伺服器。若要繼續管理中斷連線的裝置，請設定另一個採用基於 2048 位元/SHA-256 的憑證的 XClarity Administrator 實例。
- **高安全性**。這是 ThinkSystem V1 和 V2 伺服器最安全的模式。選取此模式可確保符合 NIST 和 PFS（完全前向保密）標準。

  僅 ThinkSystem V1 和 V2 伺服器支援此模式。需要使用 2023 年第二季或之後發佈的 XCC 韌體版本。

請考慮變更加密模式的下列含意。

- 對於 XClarity Administrator v4.2 和更舊版本：
  - 當 XCC 上的 TLS 版本設定為 v1.3 時，若要使用受管理鑑別來管理 ThinkSystem 或 ThinkAgile 伺服器，XClarity Administrator 中的**最低伺服器 TLS 版本**也必須設定為 TLS v1.3（請參閱線上文件中的設定加密法模式和通訊 協定）。
- 對於 XClarity Administrator v4.0 和更舊版本：
  - 當 XCC 的安全性模式設定為 **TLS v1.3** 時，無法使用*受管理鑑別*管理 ThinkSystem 或 ThinkAgile 伺服器。
  - 對於使用*受管理鑑別*管理的 ThinkSystem 或 ThinkAgile 伺服器，使用 XClarity Administrator 或 XCC 將 XCC 的安全性模式變更為 **TLS v1.3** 將導致伺服器離線。
- 不支援從**相容性安全性**模式或**標準安全性**模式變更為**企業嚴格安全性**模式。
- 當您從**相容性安全性**模式升級到**標準安全性**模式時，如果匯入的憑證或 SSH 公用金鑰不符合標準，您會收到警告，但仍然可以升級到**標準安全性**模式。
- 如果從**企業嚴格安全性**模式降級到**相容性安全性**模式或**標準安全性**模式：
  - 伺服器會自動重新啟動以使安全性模式生效。
  - 對於 ThinkSystem V3 和 V4 伺服器：如果 XCC 上的嚴格模式 FoD 金鑰遺失或過期，而且 XCC 使用自簽 TLS 憑證，則 XCC 會根據符合標準嚴格規格的演算法重新產生自簽 TLS 憑證。XClarity Administrator 因憑證錯誤出現連線失敗。若要解決不受信任的憑證錯誤，請參閱 XClarity Administrator 線上文件中的解決不受信任的伺服器憑證。如果 XCC 使用自訂 TLS 憑證，則 XCC 允許降級，而且會警告您需要匯入基於**標準安全性**模式加密法的伺服器憑證。

您可以變更下列裝置的安全性設定。

- 配備 Intel 或 AMD 處理器的 Lenovo ThinkSystem 伺服器（SR635/SR655 除外）
- Lenovo ThinkSystem V2 伺服器
- 配備 Intel 或 AMD 處理器的 Lenovo ThinkSystem V3 伺服器
- Lenovo ThinkSystem V4 伺服器
- Lenovo ThinkEdge SE350 和 SE450 伺服器
- Lenovo System x 伺服器

如需在受管理伺服器上設定安全性模式的相關資訊，請參閱 XClarity Administrator 線上文件中的配置伺服器的安全性設定。

## 安全憑證

Lenovo XClarity Administrator 使用 SSL 憑證建立 XClarity Administrator 及其受管理裝置（例如，System x 伺服器中的機箱和服務處理器）之間安全、信任的通訊，以及使用者與 XClarity Administrator 或與不同服務之間的通訊。依預設，XClarity Administrator、CMM 和基板管理控制器使用內部憑證管理中心自行簽署並發出的 XClarity Administrator 產生的憑證。

在每個 XClarity Administrator 實例唯一產生的預設自簽伺服器憑證可為許多環境提供足夠的安全。您可以選擇讓 XClarity Administrator 為您管理憑證，或者您可以採取更積極的角色，自訂或取代伺服器憑證。XClarity Administrator 會針對您的環境提供自訂憑證的選項。例如，您可以選擇：

- 透過重新產生內部憑證管理中心和/或使用組織特有值的最終伺服器憑證來產生一對新金鑰。
- 產生憑證簽章要求 (CSR)，然後將之傳送至您選擇的憑證管理中心以簽署自訂憑證，再將該自訂憑證上傳至 XClarity Administrator 以用來做為其所有裝載服務的最終伺服器憑證。
- 將伺服器憑證下載至本端系統，讓您可以將該憑證匯入 Web 瀏覽器的受信任憑證清單。

如需憑證的相關資訊，請參閱 XClarity Administrator 線上文件中的使用安全憑證。

# 鑑別

## 支援的鑑別伺服器

*鑑別伺服器*是用來鑑別使用者認證的使用者登錄。Lenovo XClarity Administrator 支援以下類型的鑑別伺服器。

- **本端鑑別伺服器**。依預設，XClarity Administrator配置為使用位於管理伺服器中的內嵌輕量型目錄存取通訊協定 (LDAP) 伺服器。
- **外部 LDAP 伺服器**。目前支援 Microsoft Active Directory 和 OpenLDAP。此伺服器必須位於連線至管理網路的外接式 Microsoft Windows 伺服器。使用外部 LDAP 伺服器時，會停用本端鑑別伺服器。

  **注意：**若要配置 Active Directory 連結方法以使用登入認證，每一部受管理伺服器的基板管理控制器都必須執行 2016 年 9 月或更新版本的韌體。
- **外部識別管理系統**。目前只支援 CyberArk。

  如果將 ThinkSystem 或 ThinkAgile 伺服器的使用者帳戶加入 CyberArk，則可以在初次設定管理伺服器時選擇讓 XClarity Administrator 從 CyberArk 擷取認證，以登入伺服器（使用受管理或本端鑑別）。在可以從 CyberArk 擷取認證之前，必須在 XClarity Administrator 中定義 CyberArk 路徑，而且必須使用 TLS 交互鑑別透過用戶端憑證在 CyberArk 和 XClarity Administrator 之間建立互信。
- **外部 SAML 識別提供者**。目前支援 Microsoft Active Directory Federation Services (AD FS)。除了輸入使用者名稱及密碼外，還可以設定多重要素鑑別，透過要求 PIN 碼、讀取智慧卡和用戶端憑證等方式提供額外的安全性。使用 SAML 識別提供者時，不會停用本端鑑別伺服器。您需要有本端使用者帳戶，才能直接登入受管理機箱或伺服器（除非該裝置上已啟用 Encapsulation），進行 PowerShell 和 REST API 鑑別，以及回復（如果無法使用外部鑑別）。

  您可以選擇同時使用外部 LDAP 伺服器和外部識別提供者。如果兩者都已啟用，則使用外部 LDAP 伺服器直接登入受管理的裝置，並使用識別提供者登入管理伺服器。

如需鑑別伺服器的相關資訊，請參閱 XClarity Administrator 線上文件中的管理鑑別伺服器。

## 裝置鑑別

依預設，系統會使用 XClarity Administrator 受管理鑑別登入裝置來管理裝置。管理機架式伺服器和 Lenovo 機箱時，您可以選擇使用本端鑑別或受管理鑑別登入裝置。

- 當*本端鑑別*用於機架式伺服器、Lenovo 機箱和 Lenovo 機架式交換器時，XClarity Administrator 會使用已儲存認證向裝置進行鑑別。*已儲存認證*可以是裝置上的作用中使用者帳戶，或是 Active Directory 伺服器中的使用者帳戶。

  使用本端鑑別管理裝置之前，您應先在 XClarity Administrator 建立已儲存認證，其必須與裝置上的作用中使用者帳戶或 Active Directory 伺服器中的使用者帳戶相符（請參閱 XClarity Administrator 線上文件中的管理儲存的認證）。

  **附註：**

  — 裝置的本端鑑別啟用時，您無法使用 XClarity Administrator 編輯該裝置的已儲存認證。

  — RackSwitch 裝置僅支援已儲存認證進行鑑別，不支援 XClarity Administrator 使用者認證。
- 使用*受管理鑑別*讓您能夠利用 XClarity Administrator 鑑別伺服器中的認證來管理及監視多個裝置，而不使用本端認證。當受管理鑑別用於裝置（非 ThinkServer 伺服器、System x M4 伺服器和交換器）時，XClarity Administrator 會配置裝置及其所安裝的元件，以使用 XClarity Administrator 鑑別伺服器進行集中管理。

  — 啟用受管理鑑別時，您可以使用手動輸入或已儲存認證來管理裝置（請參閱 管理使用者帳戶 以及 XClarity Administrator 線上文件中的管理儲存的認證）。要等到 XClarity Administrator 配置了裝置的 LDAP 設定後才會使用已儲存認證。之後，已儲存認證的任何變更都不會影響對該裝置的管理或監視。

  — 如果使用本端或外部 LDAP 伺服器做為 XClarity Administrator 鑑別伺服器，則會使用鑑別伺服器中定義的使用者帳戶登入 XClarity Administrator、CMM 和 XClarity Administrator 網域內的基板管理控制器。已停用本端 CMM 和管理控制器使用者帳戶。

**附註：**對於 Think Edge SE450、SE350 V2 和 SE360 V2 伺服器，預設本端使用者帳戶保持啟用，所有其他本端帳戶均為停用。

— 如果使用 SAML 2.0 識別提供者做為 XClarity Administrator 鑑別伺服器，受管理裝置將無法存取 SAML 帳戶。不過，當同時使用 SAML 識別提供者和 LDAP 伺服器時，如果識別提供者使用存在於 LDAP 伺服器的帳戶，則可以使用 LDAP 使用者帳戶登入受管理裝置；而 SAML 2.0 所提供更進階的鑑別方法（例如，多重要素鑑別和單一登入），則可以用來登入 XClarity Administrator。

— 單一登入可以讓已登入 XClarity Administrator 的使用者自動登入基板管理控制器。依預設，將 ThinkSystem 或 ThinkAgile 伺服器設定為受 XClarity Administrator 管理後，會啟用單一登入（使用 CyberArk 密碼管理伺服器的情況除外）。您可以配置廣域設定來啟用或停用所有受管理 ThinkSystem 和 ThinkAgile 伺服器的單一登入。為特定 ThinkSystem 和 ThinkAgile 伺服器啟用單一登入會置換所有 ThinkSystem 和 ThinkAgile 伺服器的廣域設定 (請參閱 XClarity Administrator 線上文件中的 管理伺服器)。

**附註：**使用 CyberArk 識別管理系統進行鑑別時，單一登入會自動停用。

— 為 ThinkSystem SR635 和 SR655 伺服器啟用受管理鑑別時：

  — 基板管理控制器韌體支援最多五個 LDAP 使用者角色。XClarity Administrator 會在管理期間，將這些 LDAP 使用者角色新增至伺服器：**lxc-supervisor**、**lxc-sysmgr**、**lxc-admin**、**lxc-fw-admin** 和 **lxc-os-admin**。使用者必須獲指派至少其中一個指定的 LDAP 使用者角色，才能與 ThinkSystem SR635 和 SR655 通訊。

  — 管理控制器韌體不支援與伺服器本端使用者具有相同使用者名稱的 LDAP 使用者。

— 若是 ThinkServer 和 System x M4 伺服器，則不會使用 XClarity Administrator 鑑別伺服器。但是會在裝置上建立字首為「LXCA_」，後面緊接著隨機字串的 IPMI 帳戶（現有的本端 IPMI 使用者帳戶不會遭到停用）。當您解除管理 ThinkServer 伺服器時，會停用「LXCA_」使用者帳戶，並將字首「LXCA_」取代為字首「DISABLED_」。若要判斷 ThinkServer 伺服器是否受另一個實例管理，XClarity Administrator 會檢查字首為「LXCA_」的 IPMI 帳戶。如果您選擇強制管理受管理的 ThinkServer 伺服器，則會停用並重新命名裝置上字首為「LXCA_」的所有 IPMI 帳戶。請考慮手動清除不再使用的 IPMI 帳戶。

  如果您使用手動輸入的認證，XClarity Administrator 會自動建立已儲存認證，並且使用該份已儲存認證來管理裝置。

  **附註：**裝置的受管理鑑別啟用時，您無法使用 XClarity Administrator 編輯該裝置的已儲存認證。

  — 每次使用手動輸入的認證來管理裝置時，都將為該裝置建立一份新的已儲存認證，即使前次管理程序期間已為該裝置建立了另一份已儲存認證亦同。

  — 當您解除管理裝置時，XClarity Administrator 不會刪除在管理程序期間為該裝置自動建立的已儲存認證。

### 回復使用者帳戶

如果您指定回復密碼，XClarity Administrator 會停用本端 CMM 或管理控制器使用者帳戶，並在裝置上建立新的回復使用者帳戶 (`RECOVERY_ID`) 以供日後鑑別之用。如果管理伺服器發生故障，您可以使用 `RECOVERY_ID` 帳戶登入裝置採取回復動作，以還原裝置上的帳戶管理功能，直到還原或更換管理節點為止。

如果您解除管理具有 `RECOVERY_ID` 使用者帳戶的裝置，則會啟用所有本端使用者帳戶，並刪除 `RECOVERY_ID` 帳戶。

- 如果您變更已停用的本端使用者帳戶（例如，如果您變更密碼），則這些變更對於 `RECOVERY_ID` 帳戶沒有任何影響。在受管理鑑別模式下，`RECOVERY_ID` 帳戶是已啟動並可運作的唯一使用者帳戶。
- 請僅在緊急狀況下使用 `RECOVERY_ID` 帳戶，例如，管理伺服器發生故障時，或是網路問題使裝置無法與 XClarity Administrator 進行通訊以鑑別使用者時。
- 當您探索裝置時，會指定 `RECOVERY_ID` 密碼。請務必記下密碼以供日後使用。
- RackSwitch 裝置僅支援已儲存認證進行鑑別，不支援 XClarity Administrator 使用者認證。

如需回復裝置管理的相關資訊，請參閱XClarity Administrator 線上文件中的在管理伺服器故障之後， 使用 CMM 回復機箱管理和在管理伺服器故障之後，回復機架式或直立式 伺服器管理。

## 使用者帳戶和角色群組

*使用者帳戶*用於登入並管理 Lenovo XClarity Administrator 和所有受管理機箱及伺服器。XClarity Administrator 使用者帳戶可以承受兩個相互依存的程序：鑑別及授權。

*鑑別*是驗證使用者認證所使用的安全機制。鑑別程序使用儲存在已配置之鑑別伺服器中的使用者認證。它也可以防止未經授權的管理伺服器或惡意的受管理系統應用程式存取資源。鑑別之後，使用者可以存取 XClarity Administrator。不過，若要存取特定的資源或執行特定的工作，使用者也必須具備適當的授權。

*授權*可檢查經鑑別使用者的權限，並根據角色群組中的使用者成員資格，控制對資源的存取。*角色群組*用於將特定角色指派給在鑑別伺服器中定義並管理的一組使用者帳戶。例如，如果使用者是具有 Supervisor 權限之角色群組的成員，則該使用者可以從 XClarity Administrator 建立、編輯與刪除使用者帳戶。如果使用者具有 Operator 權限，則該使用者只能檢視使用者帳戶資訊。

如需使用者帳戶和角色群組的相關資訊，請參閱 XClarity Administrator 線上文件中的管理使用者帳戶。

## 使用者帳戶安全

使用者帳戶設定可控制密碼複雜性、帳戶鎖定與 Web 階段作業閒置逾時。您可以變更帳戶安全設定的值。

如需帳戶安全性設定的相關資訊，請參閱 Lenovo XClarity Administrator 線上文件中的變更使用者帳戶安全性設定。

# 高可用性考量

若要為 Lenovo XClarity Administrator 設定高可用性，請使用主機作業系統或容器環境中的高可用性功能。

### Docker

您可以使用 Docker Datacenter 為 Docker Engine 中執行的 XClarity Administrator 容器設定高可用性環境。如需 Docker Datacenter 高可用性的相關資訊，請參閱 使用 Docker Datacenter 實現高可用性架構和應用程式 網頁。

### Citrix

使用針對 Citrix 環境提供的高可用性功能。如需相關資訊，請參閱 XClarity Administrator 線上文件中的實作高可用性 (Citrix)。

### KVM（CentOS、RedHat、Rocky 和 Ubuntu）

您可以使用 OpenStack，或者如果您已有高可用性環境，則繼續使用您的內部程序。如需 OpenStack 高可用性的相關資訊，請參閱 XClarity Administrator 線上文件中的實作高可用性 (KVM)。

### Microsoft Hyper-V

使用針對 ESXi 環境提供的高可用性功能。如需相關資訊，請參閱 XClarity Administrator 線上文件中的實作高可用性 (Microsoft Hyper-V)。

### Nutanix AHV

使用針對 Nutanix AHV 環境提供的虛擬機器高可用性功能。如需相關資訊，請參閱 XClarity Administrator 線上文件中的實作高可用性 (Nutanix)。

### VMware ESXi

在 VMware High Availability 中，會將多部主機配置為叢集。共用儲存體會用來將虛擬機器 (VM) 的磁碟映像檔提供給叢集中的主機。虛擬機器一次只會在一部主機上執行。當虛擬機器發生問題時，該虛擬機器的另一個實例就會在備用主機上啟動。

VMware High Availability 需要下列元件：

- 至少兩部已安裝 ESXi 的主機。這些主機會成為 VMware 叢集的一部分。
- 安裝 VMware vCenter 的第三部主機。

  **要訣：**確認您安裝的 VMware vCenter 版本與叢集中要使用的主機上安裝的 ESXi 版本相容。

  VMware vCenter 可以安裝在叢集中使用的其中一部主機上。不過，如果該主機電源關閉或無法使用，您就無法存取 VMware vCenter 介面。
- 共用儲存體（資料存放區），可供叢集中的所有主機存取。您可以使用 VMware 支援的任何一種共用儲存體。VMware 會使用資料存放區來判斷虛擬機器是否應進行失效接手，以轉換至另一部主機（活動訊號）。

如需設定 VMware High Availability 叢集的相關詳細資料，請參閱 XClarity Administrator 線上文件中的實作高可用性 (VMware ESXi)。

## Features on Demand

Features on Demand 會啟動功能，而不需安裝硬體或購買新設備。啟動透過取得並安裝對應的 Features on Demand 金鑰完成。

若要使用 Lenovo XClarity Administrator 中的遠端控制和作業系統部署作業，而伺服器隨附的這些功能未預設為已啟動，則您必須為伺服器啟用 XClarity Controller 企業版或 MM Advanced Upgrade。這些作業也會要求在 ThinkSystem、Converged 和 System x 伺服器上必須安裝用於遠端顯示功能的 Features on Demand 金鑰。您可以從「伺服器」頁面判斷伺服器是否已啟用、停用或未安裝遠端顯示功能（請參閱 XClarity Administrator 線上文件中的檢視受管理伺服器的狀態）。

部分進階伺服器功能是使用 Features on Demand 金鑰啟動。如果功能有可配置的設定，並且在 UEFI 設定期間公開，您就可以使用 Configuration Patterns 配置設定；不過，在安裝對應的 Features on Demand 金鑰之前，不會啟動產生的配置。

**附註：**您無法從 XClarity Administrator 安裝或管理 Features on Demand 金鑰，但是可以檢視受管理伺服器上目前已安裝的 Features on Demand 金鑰清單。如需檢視已安裝 Features on Demand 金鑰的相關資訊，請參閱 XClarity Administrator 線上文件中的檢視 Feature on Demand 金鑰。

若要取得並安裝 Features on Demand 金鑰：

1. 使用適當的零件編號購買 Features on Demand 升級。

   您可以從 Features on Demand 入口網站 購買金鑰。購買完成時，您會收到包含授權碼的電子郵件。
2. 在 Features on Demand 入口網站 上，輸入收到的授權碼，以及您要升級之伺服器的唯一系統 ID。
3. 下載 .KEY 檔案形式的啟動金鑰。
4. 將啟動金鑰上傳至伺服器的管理控制器。
5. 重新啟動伺服器。重新啟動完成時，功能就會啟動。

如需 Features on Demand 金鑰的相關資訊，請參閱 使用 Lenovo Features on Demand。

# 第 3 章　安裝 Lenovo XClarity Administrator

有數種方法能夠將可管理裝置連接至網路，並設定 Lenovo XClarity Administrator 虛擬裝置來管理這些裝置。使用本節中的資訊做為指南，設定可管理裝置及安裝 XClarity Administrator

本節說明如何設定數種常見的拓撲。但本節並未涵蓋每一種可能的網路拓撲。

**注意：**如果要管理裝置，XClarity Administrator 必須具有管理網路的存取權。

**進一步瞭解：**

- 在 VMware vCenter 上安裝 Lenovo XClarity Administrator
- 在 VMware vSphere 上安裝 Lenovo XClarity Administrator
- 在 Windows Hyper-V 上安裝 Lenovo XClarity Administrator
- 在 Red Hat KVM 上安裝 Lenovo XClarity Administrator

## 單一資料和管理網路

在此網路拓撲中，資料網路與管理網路兩者是相同的網路。

### 開始之前

確定已啟用所有適用的埠，包括 XClarity Administrator 所需的埠（請參閱 XClarity Administrator 線上文件中的埠可用性）。

確定您要使用 XClarity Administrator 管理的每個裝置上都已安裝最低需求韌體。您可以從 XClarity Administrator 支援 — 相容性 網頁找到最低所需韌體版本，方法是按一下 **Compatibility（相容性）**標籤，然後按一下適當裝置類型的鏈結。

**重要事項：**配置裝置和元件，以盡量減少 IP 位址變更。考慮使用靜態 IP 位址，而不使用動態主機配置通訊協定 (DHCP)。如果使用 DHCP，務必盡量減少 IP 位址變更。

### 關於此作業

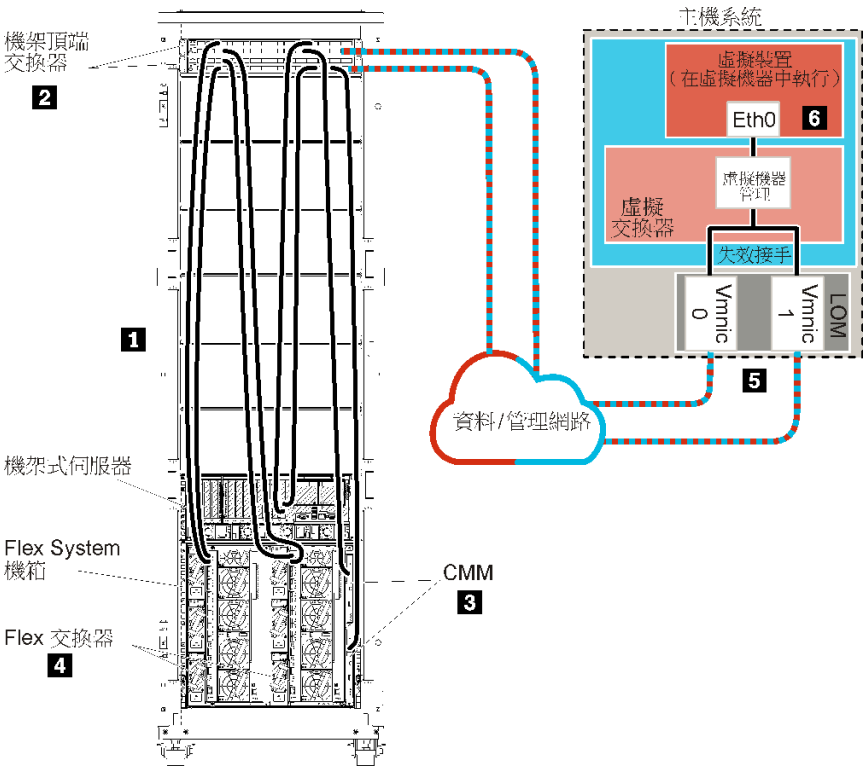
若是虛擬裝置，XClarity Administrator 與網路之間的所有通訊都是透過主機上的 eth0 網路介面進行。若是容器，您可以使用自訂名稱；但是，此案例使用的是 eth0。

**重要事項：**根據您的網路配置（例如，如果來自伺服器的資料流量有高優先順序，而來自管理控制器的資料流量有低優先順序），實作共用資料和管理網路可能會導致資料流量中斷，例如，封包遭到丟棄或管理網路連線問題。管理網路除了 TCP 之外，還會使用 UDP 資料流量。當網路資料流量高時，UDP 資料流量的優先順序可能會比較低。

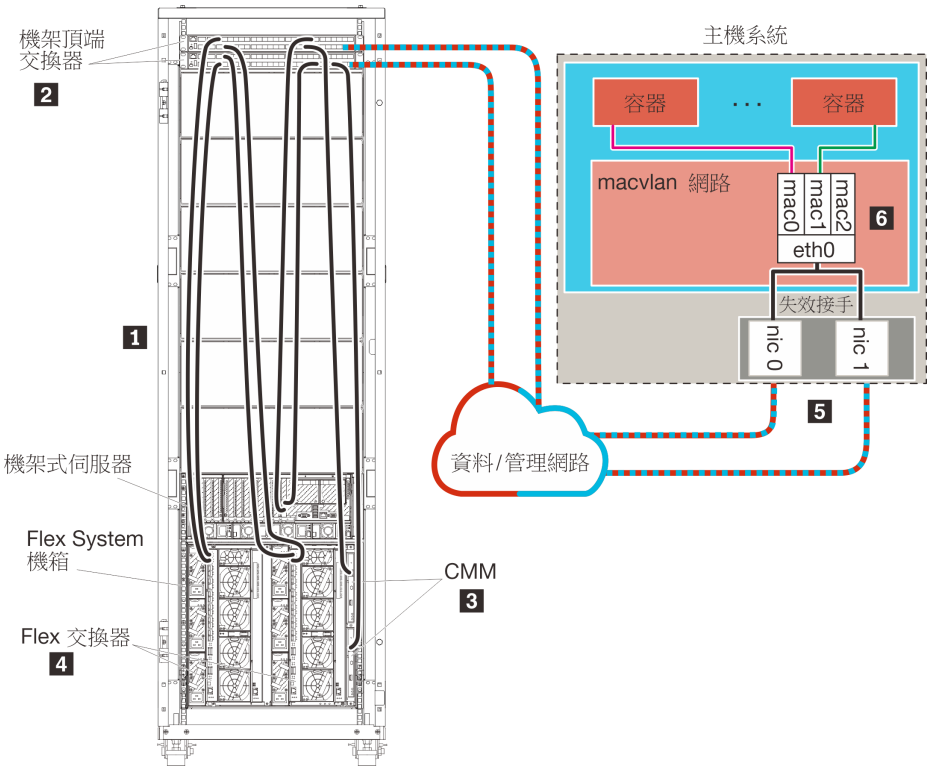
下圖說明在資料網路和管理網路為相同網路的情況下，設定環境的方式。圖中的數字對應下列各節的編號步驟。

**附註：**此圖中並未描述您環境中可能需要的所有佈線選項。此圖僅顯示機架式伺服器、機架式交換器、Flex 交換器和 CMM 的佈線選項需求，因為它們與設定單一資料/管理網路相關。

© Copyright Lenovo 2022




*圖例 8. 虛擬裝置的單一資料和管理網路拓撲範例*




*圖例 9. 容器的單一資料和管理網路拓撲範例*

**重要事項：**您可以在符合 XClarity Administrator 需求的任何系統上設定 XClarity Administrator，包括受管理伺服器在內。如果您使用受管理伺服器做為 XClarity Administrator 主機：

- 您必須實作虛擬分離資料和管理網路拓撲，或是單一資料和管理網路拓撲。
- 您無法使用 XClarity Administrator 將韌體更新套用至該受管理伺服器。即使只能透過立即啟動套用部分硬體，XClarity Administrator 仍會強制目標伺服器重新啟動，這也會重新啟動 XClarity Administrator。透過延遲啟動套用時，在 XClarity Administrator 主機重新啟動時只會套用部分韌體。
- 如果您使用 Flex System 機箱內的伺服器，請確定伺服器設定為自動開啟電源。您可以從 CMM Web 介面中設定此選項，方法是按一下**機箱管理 → 計算節點**，然後選取伺服器，再選取**自動電源**做為**自動開啟電源模式**。

如果您想要安裝 XClarity Administrator，用來管理已配置的現有機箱和機架式伺服器，請繼續執行步驟 5：安裝及配置主機。

如需有關規劃此拓撲的其他資訊，包括網路設定和 Eth1 與 Eth0 配置的相關資訊，請參閱單一資料和管理網路。

## 步驟 1：將機箱、機架式伺服器及 Lenovo XClarity Administrator 主機的纜線連接到機架頂端交換器

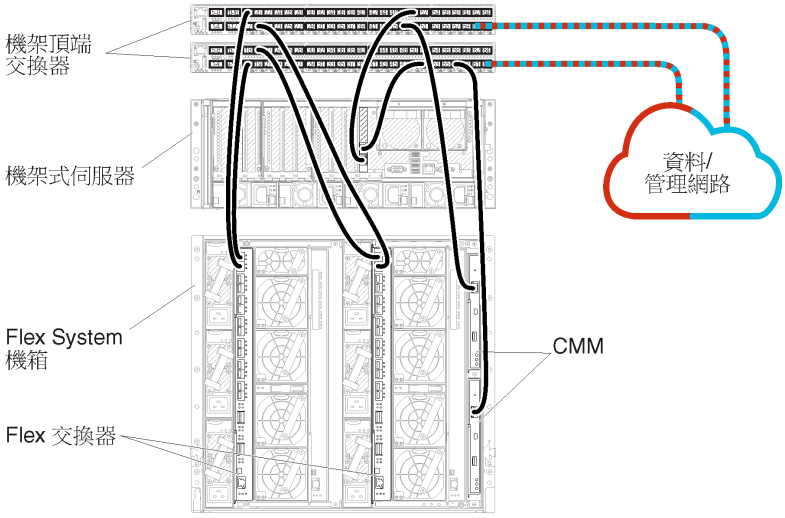
將機箱、機架式伺服器及 XClarity Administrator 主機的纜線連接到機架頂端交換器，以啟用裝置與網路之間的通訊。

### 程序

將每個機箱中的每一部 Flex 交換器和 CMM、每一部機架式伺服器及 XClarity Administrator 主機的纜線連接到兩台機架頂端交換器。您可以選擇機架頂端交換器的任何埠。

下圖的範例說明將纜線從機箱（Flex 交換器 及 CMM）、機架式伺服器及 XClarity Administrator 主機連接到機架頂端交換器。

**附註：**此圖中並未描述您環境中可能需要的所有佈線選項。此圖僅顯示機架式伺服器、機架式交換器、Flex 交換器和 CMM 的佈線選項需求，因為它們與設定單一資料/管理網路相關。




*圖例 10. 單一資料和管理網路的纜線佈線範例*

## 步驟 2：配置機架頂端交換器

配置機架頂端交換器。

### 開始之前

除了機架頂端交換器的一般配置需求之外，請確定已啟用所有適當的埠，包括用於 Flex 交換器、機架式伺服器和網路的外部埠，以及用於 CMM、機架式伺服器和網路的內部埠。

### 程序

配置步驟可能會隨著所安裝的機架交換器類型而有所不同。

如需配置 Lenovo 機架頂端交換器的相關資訊，請參閱 System x 中的機架交換器線上文件。如果安裝其他機架頂端交換器，請參閱該交換器隨附的文件。

## 步驟 3：配置 Chassis Management Module (CMM)

在您的機箱中配置主要 Chassis Management Module (CMM)，用來管理機箱內的所有裝置。

### 關於此作業

如需配置 CMM 的詳細資訊，請參閱 Flex System 線上文件中的「配置機箱元件」。

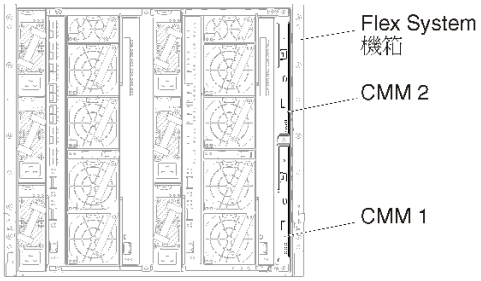
此外，請參閱機箱隨附說明書上的步驟 4.1 - 4.5。

### 程序

請完成下列步驟以配置 CMM。

如果安裝兩個 CMM，請僅配置*主要* CMM，它會自動將配置與待命 CMM 同步。

步驟 1. 將機槽 1 中 CMM 的乙太網路纜線連接到用戶端工作站，以建立直接連線。




第一次連接至 CMM 時，您可能需要變更用戶端工作站上的「網際網路通訊協定」內容。

**重要事項：**請確定用戶端工作站子網路與 CMM 子網路相同。（預設 CMM 子網路為 255.255.255.0）。為用戶端工作站選擇的 IP 位址必須與 CMM 位於相同網路上（例如 192.168.70.0 - 192.168.70.24）。

步驟 2. 若要啟動 CMM 管理介面，請在用戶端工作站上開啟 Web 瀏覽器，並且將它指向 CMM IP 位址。

**附註：**

- 請確定您使用的是安全連線，且 URL 中包含 **https**（例如 https://192.168.70.100）。如果未包含 https，您將會收到找不到頁面的錯誤訊息。
- 如果您使用預設 IP 位址 192.168.70.100，CMM 管理介面可能需要花幾分鐘才能使用。這個延遲情況是因為 CMM 會花兩分鐘嘗試取得 DHCP 位址，然後才回復為預設靜態位址。

步驟 3. 使用預設使用者 ID `USERID` 和密碼 `PASSWORD` 登入 CMM 管理介面。登入後，您必須變更預設密碼。

步驟 4. 完成「CMM 起始設定精靈」，以指定環境的詳細資料。「起始設定精靈」包括下列選項：

- 檢視機箱庫存和性能。
- 從現行的配置檔匯入配置。
- 配置一般 CMM 設定。
- 配置 CMM 日期和時間。

  **要訣：**當您安裝 XClarity Administrator 時，您會將 XClarity Administrator 及 XClarity Administrator 管理的所有機箱配置為使用 NTP 伺服器。
- 配置 CMM IP 資訊。
- 配置 CMM 安全原則。
- 配置網域名稱系統 (DNS)。
- 配置事件轉遞器。

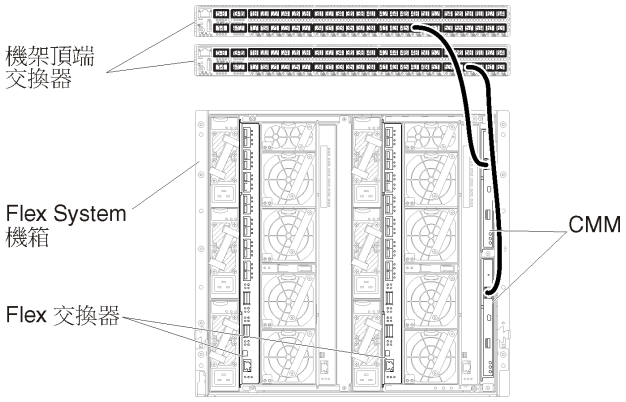
步驟 5. 儲存設定精靈設定並套用變更後，配置機箱中所有元件的 IP 位址。

請參閱機箱隨附說明書上的步驟 4.6。

**附註：**您必須重設每個計算節點的系統管理處理器，並重新啟動 Flex 交換器，才會顯示新的 IP 位址。

步驟 6. 使用 CMM 管理介面重新啟動 CMM。

步驟 7. CMM 重新啟動時，將纜線分別連接到 CMM 上的乙太網路埠和您的網路。




步驟 8. 使用新的 IP 位址登入 CMM 管理介面。

## 在您完成之後

您也可以配置 CMM，使其支援備援。請使用 CMM 說明系統進一步瞭解下列每一個頁面上提供的欄位。

- 為 CMM 配置失效接手，以防主要 CMM 發生硬體故障。在 CMM 管理介面中，按一下 **Mgt Module Management → 內容 → 進階失效接手**。
- 配置失效接手做為網路問題的最終解決方法（上行）。在 CMM 管理介面中，按一下 **Mgt Module Management → 網路**，按一下**乙太網路**標籤，然後按一下**進階乙太網路**。請確定至少要選取**喪失實體網路鏈結時失效接手**。

# 步驟 4：配置 Flex 交換器

配置每個機箱中的 Flex 交換器（I/O 模組）。

## 開始之前

確定已啟用所有適當的埠，包括從 Flex 交換器到機架頂端交換器的外部埠，以及連接到 CMM 的內部埠。

如果 Flex 交換器設定為透過 DHCP 取得動態網路設定（IP 位址、網路遮罩、閘道和 DNS 位址），請確定 Flex 交換器的設定一致（例如，確認 IP 位址與 CMM 位於相同的子網路）。

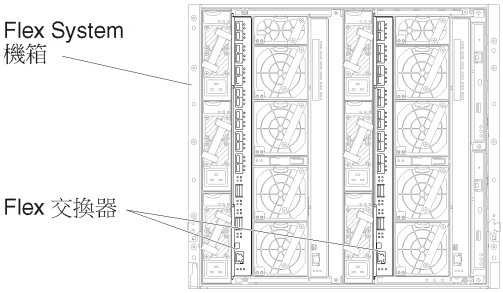
**重要事項：**對於每個 Flex System 機箱，請確定機箱內的每一部伺服器中擴充卡的光纖類型，能夠與相同機箱中所有 Flex 交換器的光纖類型相容。例如，如果乙太網路交換器安裝在機箱中，則該機箱中的所有伺服器都必須具備透過主機板上 LAN 接頭或乙太網路擴充卡連線到乙太網路的功能。如需配置 Flex 交換器的相關資訊，請參閱 Flex Systems 線上文件中的「配置 I/O 模組」。

## 程序

配置步驟可能會隨著所安裝的 Flex 交換器 類型而有所不同。如需支援的每一種 Flex 交換器 的相關資訊，請參閱 Flex Systems 線上文件中的「Flex System 網路交換器」。

一般而言，您必須將 Flex 交換器配置在 Flex 交換器機槽 1 和 2 中。

**要訣：**Flex 交換器機槽 2 是機箱背面的第三個模組機槽。




*圖例 11. Flex 交換器 在機箱中的位置*

# 步驟 5：安裝及配置主機

您可以在符合 Lenovo XClarity Administrator 需求的任何伺服器上安裝 Docker。

## 開始之前

您可以使用 Docker Datacenter 為 Docker Engine 中執行的 XClarity Administrator 容器設定高可用性環境。如需 Docker Datacenter 高可用性的相關資訊，請參閱 使用 Docker Datacenter 實現高可用性架構和應用程式 網頁。

確認主機符合 XClarity Administrator 線上文件的硬體和軟體必要條件。

確認主機系統與您要管理的裝置位於相同網路中。

**重要事項：**您可以在符合 XClarity Administrator 需求的任何系統上設定 XClarity Administrator，包括受管理伺服器在內。如果您使用受管理伺服器做為 XClarity Administrator 主機：

- 您必須實作虛擬分離資料和管理網路拓撲，或是單一資料和管理網路拓撲。
- 您無法使用 XClarity Administrator 將韌體更新套用至該受管理伺服器。即使只能透過立即啟動套用部分硬體，XClarity Administrator 仍會強制目標伺服器重新啟動，這也會重新啟動 XClarity Administrator。透過延遲啟動套用時，在 XClarity Administrator 主機重新啟動時只會套用部分韌體。
- 如果您使用 Flex System 機箱內的伺服器，請確定伺服器設定為自動開啟電源。您可以從 CMM Web 介面中設定此選項，方法是按一下**機箱管理 → 計算節點**，然後選取伺服器，再選取**自動電源**做為**自動開啟電源模式**。

## 程序

使用隨著 Docker 分配提供的指示，在主機上安裝及配置 Docker。

# 步驟 6. 安裝和配置 XClarity Administrator

在剛安裝的 Docker 主機上安裝及配置 Lenovo XClarity Administrator 容器。

## 開始之前

確定主機系統符合最低的硬體和軟體需求（請參閱硬體和軟體必要條件）。

確定已啟用所有適用的埠，包括 XClarity Administrator 所需的埠（請參閱埠可用性）。

確認主機系統與您要管理的裝置位於相同網路中。

確保主機 OS 和 XClarity Administrator 使用相同的 NTP 伺服器。

XClarity Administrator 允許用於資料管理、硬體管理和 OS 部署的網路使用自訂名稱（請參閱網路配置）。以下程序中的範例使用的是 eth0。

確定主機系統上的核心中載入了 macvlan 網路。若要檢查是否已載入，請使用 **lsmod | grep macvlan** 指令。若要將 macvlan 載入核心中，請執行 **modprobe macvlan** 指令。

在同一個主機上執行多個 XClarity Administrator 容器時，確保為每個容器使用唯一的名稱和 IP 位址。

如果您打算管理 ThinkServer 和其他舊式裝置，請確保啟用 Docker 以支援 IPv6。

1. 編輯 /etc/docker/daemon.json 檔案，將 **ipv6** 機碼設定為 true，並將 **fixed-cidr-v6** 機碼設定為您的 IPv6 子網路。以下是 daemon 檔案的範例。
```
{
  "ipv6": true,
  "fixed-cidr-v6": "2001:db8:1::/64",
  "experimental": true,
  "ip6tables": true
}
```
2. 執行下列指令以重新載入 Docker 配置檔。
```
systemctl reload docker
```

**附註：**XClarity Administrator *不是*做為特殊權限容器執行。

XClarity Administrator 容器中未配置防火牆規則。若要為主機系統上的容器新增防火牆規則，請完成下列步驟。

1. 透過執行下列指令取得由「NSPID」識別的 Docker 程序 ID。
```
docker inspect --format='{{ .State.Pid }}' "$CONTAINER_NAME"
```
2. 透過執行下列指令建立符號鏈結。
```
LINKFILE="/var/run/netns/$NSPID"
mkdir -p /var/run/netns
/bin/rm -f "$LINKFILE"
ln -s "/proc/$NSPID/ns/net" "$LINKFILE"
```
3. 透過執行下列指令配置適當的 iptables 規則。
```
ip netns exec $NSPID iptables -I OUTPUT -j DROP
```
4. 透過執行下列指令確保所有鏈結都已移除。
```
/bin/rm -f "$LINKFILE"
```

## 程序

若要使用 Docker compose 安裝 XClarity Administrator 容器，請完成下列步驟。

步驟 1. 從 XClarity Administrator 下載網頁將 XClarity Administrator 虛擬裝置映像檔、環境檔案和 YAML 檔案下載到用戶端工作站。登入網站，然後使用提供給您的存取金鑰以下載映像檔。

步驟 2. 透過執行下列指令，將 XClarity Administrator 容器映像檔匯入 Docker 主機。

```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

步驟 3. 編輯 `docker_compose.env` 檔案，並更新下列環境變數。

- **CONTAINER_NAME**。唯一的容器名稱，用於為每個 XClarity Administrator 實例建立 Docker 磁區（例如，`CONTAINER_NAME=LXCA-203`）
- **ADDRESS**。容器的靜態 IPv4 位址（例如，`ADDRESS=192.0.2.0`）
- **BACKUP_MOUNT**。（選用）可用於儲存 XClarity Administrator 備份的遠端共用路徑。這必須是 `/mnt/backup_share`。
- **FIRMWARE_MOUNT**。（選用）可用來做為韌體更新遠端儲存庫的遠端共用路徑。這必須是 `/mnt/fw_share`。

以下是環境檔案的範例。

```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

步驟 4. 編輯 `docker_compose.yml`，並更新以下內容。

- 將 **image** 內容設定為步驟 2 中使用的安裝映像檔的名稱。

  **附註：**您可以使用 `docker tag` 指令變更映像檔名稱（例如，變更為「latest」）。
- 如果要使用遠端共用做為遠端韌體儲存庫並儲存 XClarity Administrator 備份，請在 **volumes** 內容中為每個遠端共用設定主機裝載點。
- 將 **dns** 內容設定為 DNS 伺服器的 IP 位址。
- 容器共用主機可用的處理器和記憶體資源儲存區。（選用）透過設定 **cpus** 和 **memory** 內容，定義資源使用限制。
- 將 **parent** 內容設定為主機系統上的網路介面名稱，以用來做為容器中 macvlan 介面的父介面。此介面必須可以直接存取指派給容器的子網路。
- 根據您的網路拓撲設定 **subnet** 和 **gateway**。通常，子網路和閘道用於 ${ADDRESS} 所屬的管理網路。
- 如果要支援 IPv6，請將 **enable_ipv6** 內容設定為 true，將 **ipv6_address** 內容設定為 IPv6 位址，並根據您的網路拓撲新增另一組 **subnet** 和 **gateway** 內容（通常是該 IPv6 位址所屬的管理網路）。

**附註：**XClarity Administrator 使用 macvlan 配置容器網路。如需相關資訊，請參閱「使用 macvlan 網路」網頁

下面是啟用了 IPv6 的 YML 檔案範例。

```
version: '3.8'

services:

 lxca:
  image: lenovo/lxca:4.1.0-124
  container_name: ${CONTAINER_NAME}
  tty: true
  stop_grace_period: 60s
```

```
    volumes:
     #bind mount example
     - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
     - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
     #docker volume mount
     - data:/opt/lenovo/lxca/data
     - postgresql:/var/lib/postgresql
     - log:/var/log
     - confluent-etc:/etc/confluent
     - confluent-log:/var/log/confluent
     - confluent:/var/lib/confluent
     - propconf:/opt/lenovo/lxca/bin/conf
     - ssh:/etc/ssh
     - xcat:/etc/xcat
    networks:
     lan:
      ipv4_address: ${ADDRESS}
      ipv6_address: "2001:8003:7d51:2003::2"
    dns:
     - 192.0.2.10
     - 192.0.2.11
    deploy:
     resources:
      limits:
       cpus: "2.0"
       memory: "8g"

volumes:
 data:
  name: ${CONTAINER_NAME}-data
 postgresql:
  name: ${CONTAINER_NAME}-postgresql
 log:
  name: ${CONTAINER_NAME}-log
 confluent-etc:
  name: ${CONTAINER_NAME}-confluent-etc
 confluent-log:
  name: ${CONTAINER_NAME}-confluent-log
 confluent:
  name: ${CONTAINER_NAME}-confluent
 propconf:
  name: ${CONTAINER_NAME}-propconf
 ssh:
  name: ${CONTAINER_NAME}-ssh
 xcat:
  name: ${CONTAINER_NAME}-xcat

networks:
 lan:
  name: lan
  driver: macvlan
  enable_ipv6: true
  driver_opts:
   parent: eth0
  ipam:
   config:
    - subnet: 192.0.0.0/19
      gateway: 192.0.30.1
    - subnet: "2001:8003:7d51:2000::/80"
      gateway: "2001:8003:7d51:2000::1"
```

步驟 5. 透過執行下列指令在 Docker 中部署映像檔，其中 *<ENV_FILENAME>* 是您在步驟 2 中建立的環境變數檔案的名稱。

```
COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d
```

## 在您完成之後

登入並配置 XClarity Administrator（請參閱初次存取 Lenovo XClarity Administrator Web 介面和配置 Lenovo XClarity Administrator）。

# 實體分離資料和管理網路

在此拓撲中，資料網路與管理網路是實體分離的網路。Lenovo XClarity Administrator 與網路之間通訊的管理工作是透過主機上的 Eth0 網路介面進行。資料通訊則是透過 Eth1 網路介面進行。

## 開始之前

確定已啟用所有適用的埠，包括 XClarity Administrator 所需的埠（請參閱 XClarity Administrator 線上文件中的埠可用性）。

確定您要使用 XClarity Administrator 管理的每個裝置上都已安裝最低需求韌體。您可以從 XClarity Administrator 支援 — 相容性 網頁找到最低所需韌體版本，方法是按一下 **Compatibility（相容性）**標籤，然後按一下適當裝置類型的鏈結。

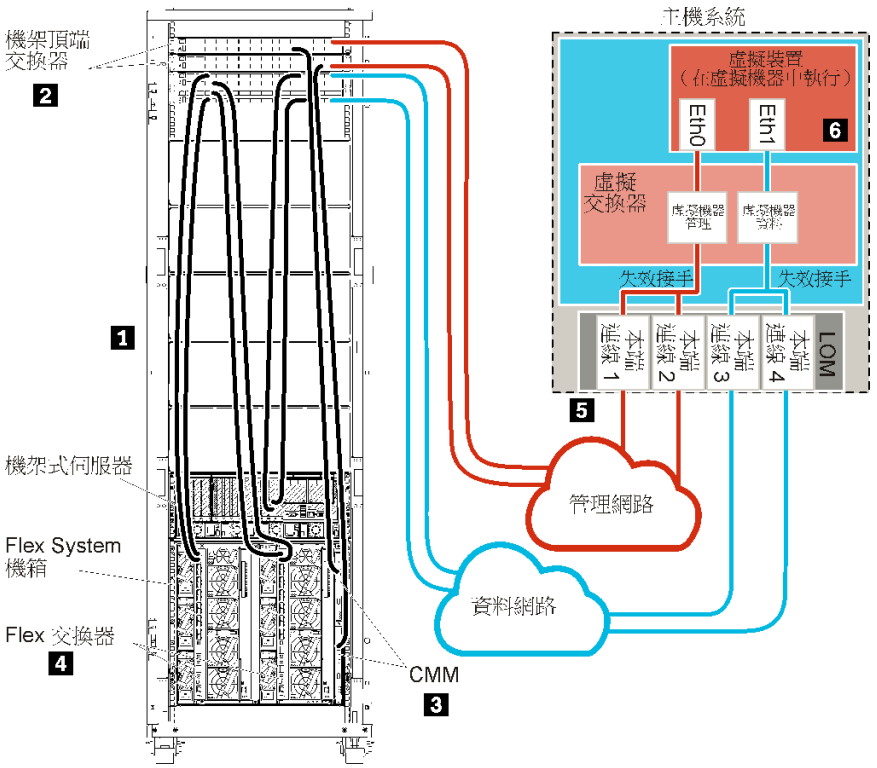
**重要事項：**配置裝置和元件，以盡量減少 IP 位址變更。考慮使用靜態 IP 位址，而不使用動態主機配置通訊協定 (DHCP)。如果使用 DHCP，務必盡量減少 IP 位址變更。

## 關於此作業

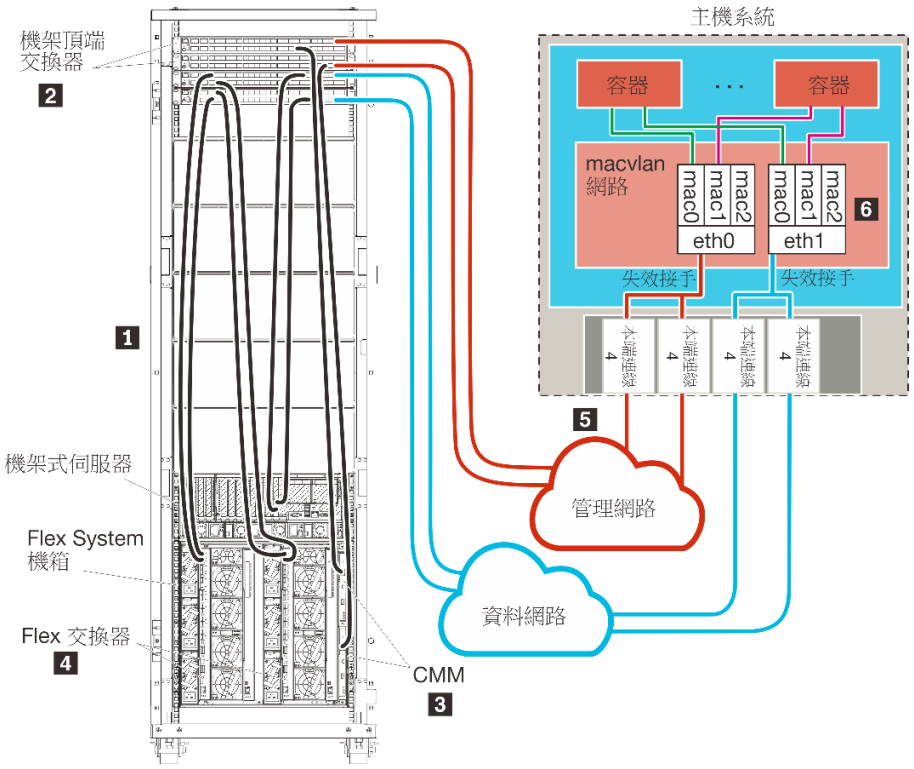
下圖說明在資料和管理網路實際上是不同網路的情況下，設定環境的方式。圖中的數字對應下列各節的編號步驟。

**附註：**此圖中並未描述您環境中可能需要的所有佈線選項。此圖僅顯示 Flex 交換器、CMM 及機架式伺服器的佈線選項需求，因為它們與設定實體分離資料和管理網路相關。

**要訣：**您可以設定一部連線至每個網路的實體交換器（總共兩部交換器），而不要設定兩部連線至每個網路以提供備援的實體交換器（總共四部交換器）。這種情況下，每一部交換器都會連線至兩個網路，而且您可以實作兩個 VLAN：一個用於資料網路，另一個用於管理網路，藉此分隔資料流量。




*圖例 12. 虛擬裝置的實體分離資料和管理網路拓撲範例*




*圖例 13. 容器的實體分離資料和管理網路拓撲範例*

如果您想要安裝 XClarity Administrator，用來管理已配置的現有機箱和機架式伺服器，請繼續執行步驟 5：安裝及配置主機。

如需有關規劃此拓撲的其他資訊，包括網路設定和 Eth1 與 Eth0 配置的相關資訊，請參閱實體分離資料和管理網路。

## 步驟 1：將機箱、機架式伺服器及 Lenovo XClarity Administrator 主機的纜線連接到機架頂端交換器

將機箱、機架式伺服器及 XClarity Administrator 主機的纜線連接到機架頂端交換器，以啟用裝置與網路之間的通訊。

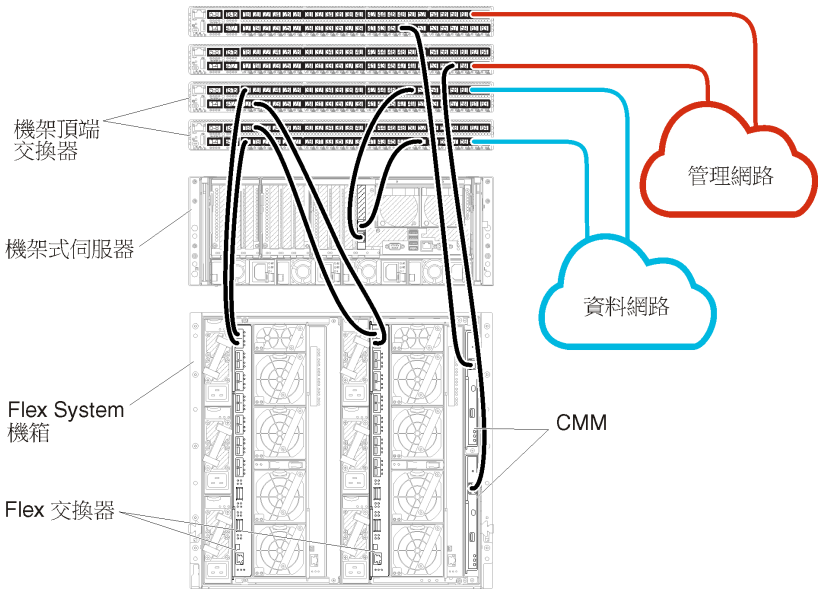
### 程序

將每個機箱中的每一部 Flex 交換器和 CMM、每一部機架式伺服器及 XClarity Administrator 主機的纜線連接到兩台機架頂端交換器。您可以選擇機架頂端交換器的任何埠。

下圖的範例說明將纜線從機箱（Flex 交換器 及 CMM）、機架式伺服器及 XClarity Administrator 主機連接到機架頂端交換器。

**附註：**此圖中並未描述您環境中可能需要的所有佈線選項。此圖僅顯示 Flex 交換器、CMM 及機架式伺服器的佈線選項需求，因為它們與設定實體分離資料和管理網路相關。

**要訣：**您可以設定一部連線至每個網路的實體交換器（總共兩部交換器），而不要設定兩部連線至每個網路以提供備援的實體交換器（總共四部交換器）。這種情況下，每一部交換器都會連線至兩個網路，而且您可以實作兩個 VLAN：一個用於資料網路，另一個用於管理網路，藉此分隔資料流量。




*圖例 14. 實體分離資料和管理網路的纜線佈線範例*

## 步驟 2：配置機架頂端交換器

配置機架頂端交換器。

### 開始之前

除了機架頂端交換器的一般配置需求之外，請確定已啟用所有適當的埠，包括用於 Flex 交換器、機架式伺服器和網路的外部埠，以及用於 CMM、機架式伺服器和網路的內部埠。

### 程序

配置步驟可能會隨著所安裝的機架交換器類型而有所不同。

如需配置 Lenovo 機架頂端交換器的相關資訊，請參閱 System x 中的機架交換器線上文件。如果安裝其他機架頂端交換器，請參閱該交換器隨附的文件。

## 步驟 3：配置 Chassis Management Module (CMM)

在您的機箱中配置主要 Chassis Management Module (CMM)，用來管理機箱內的所有裝置。

### 關於此作業

如需配置 CMM 的詳細資訊，請參閱 Flex System 線上文件中的 「配置機箱元件」 。

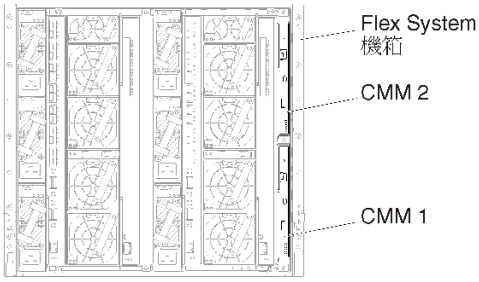
此外，請參閱機箱隨附說明書上的步驟 4.1 - 4.5。

### 程序

請完成下列步驟以配置 CMM。

如果安裝兩個 CMM，請僅配置*主要* CMM，它會自動將配置與待命 CMM 同步。

步驟 1. 將機槽 1 中 CMM 的乙太網路纜線連接到用戶端工作站，以建立直接連線。




第一次連接至 CMM 時，您可能需要變更用戶端工作站上的「網際網路通訊協定」內容。

**重要事項：**請確定用戶端工作站子網路與 CMM 子網路相同。（預設 CMM 子網路為 255.255.255.0）。為用戶端工作站選擇的 IP 位址必須與 CMM 位於相同網路上（例如 192.168.70.0 - 192.168.70.24）。

步驟 2. 若要啟動 CMM 管理介面，請在用戶端工作站上開啟 Web 瀏覽器，並且將它指向 CMM IP 位址。

**附註：**

- 請確定您使用的是安全連線，且 URL 中包含 **https**（例如 https://192.168.70.100）。如果未包含 https，您將會收到找不到頁面的錯誤訊息。
- 如果您使用預設 IP 位址 192.168.70.100，CMM 管理介面可能需要花幾分鐘才能使用。這個延遲情況是因為 CMM 會花兩分鐘嘗試取得 DHCP 位址，然後才回復為預設靜態位址。

步驟 3. 使用預設使用者 ID `USERID` 和密碼 `PASSWORD` 登入 CMM 管理介面。登入後，您必須變更預設密碼。

步驟 4. 完成「CMM 起始設定精靈」，以指定環境的詳細資料。「起始設定精靈」包括下列選項：

- 檢視機箱庫存和性能。
- 從現行的配置檔匯入配置。
- 配置一般 CMM 設定。

- 配置 CMM 日期和時間。

  **要訣：**當您安裝 XClarity Administrator 時，您會將 XClarity Administrator 及 XClarity Administrator 管理的所有機箱配置為使用 NTP 伺服器。
- 配置 CMM IP 資訊。
- 配置 CMM 安全原則。
- 配置網域名稱系統 (DNS)。
- 配置事件轉遞器。

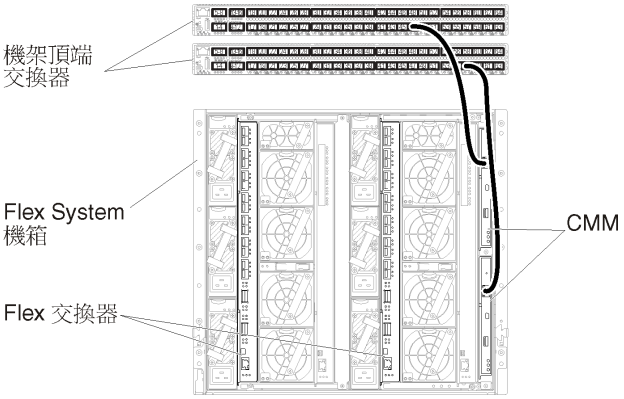
步驟 5. 儲存設定精靈設定並套用變更後，配置機箱中所有元件的 IP 位址。

請參閱機箱隨附說明書上的步驟 4.6。

**附註：**您必須重設每個計算節點的系統管理處理器，並重新啟動 Flex 交換器，才會顯示新的 IP 位址。

步驟 6. 使用 CMM 管理介面重新啟動 CMM。

步驟 7. CMM 重新啟動時，將纜線分別連接到 CMM 上的乙太網路埠和您的網路。




步驟 8. 使用新的 IP 位址登入 CMM 管理介面。

## 在您完成之後

您也可以配置 CMM，使其支援備援。請使用 CMM 說明系統進一步瞭解下列每一個頁面上提供的欄位。

- 為 CMM 配置失效接手，以防主要 CMM 發生硬體故障。在 CMM 管理介面中，按一下 **Mgt Module Management → 內容 → 進階失效接手**。
- 配置失效接手做為網路問題的最終解決方法（上行）。在 CMM 管理介面中，按一下 **Mgt Module Management → 網路**，按一下**乙太網路**標籤，然後按一下**進階乙太網路**。請確定至少要選取**喪失實體網路鏈結時失效接手**。

# 步驟 4：配置 Flex 交換器

配置每個機箱中的 Flex 交換器。

## 開始之前

確定已啟用所有適當的埠，包括從 Flex 交換器到機架頂端交換器的外部埠，以及連接到 CMM 的內部埠。

如果 Flex 交換器設定為透過 DHCP 取得動態網路設定（IP 位址、網路遮罩、閘道和 DNS 位址），請確定 Flex 交換器的設定一致（例如，確認 IP 位址與 CMM 位於相同的子網路）。

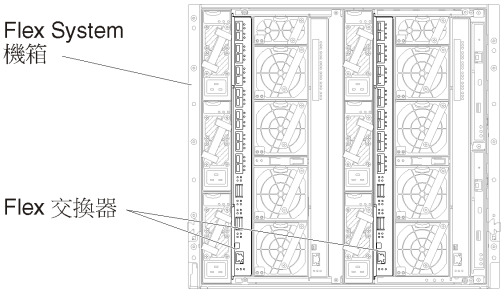
**重要事項：**對於每個 Flex System 機箱，請確定機箱內的每一部伺服器中擴充卡的光纖類型，能夠與相同機箱中所有 Flex 交換器的光纖類型相容。例如，如果乙太網路交換器安裝在機箱中，則該機箱中的所有伺服器都必須具備透過主機板上 LAN 接頭或乙太網路擴充卡連線到乙太網路的功能。如需配置 Flex 交換器的相關資訊，請參閱 Flex Systems 線上文件中的「配置 I/O 模組」 。

## 程序

配置步驟可能會隨著所安裝的 Flex 交換器 類型而有所不同。如需支援的每一種 Flex 交換器 的相關資訊，請參閱 Flex Systems 線上文件中的「Flex System 網路交換器」 。

一般而言，您必須將 Flex 交換器配置在 Flex 交換器機槽 1 和 2 中。

**要訣：**Flex 交換器機槽 2 是機箱背面的第三個模組機槽。




*圖例 15. Flex 交換器 在機箱中的位置*

# 步驟 5：安裝及配置主機

您可以在符合 Lenovo XClarity Administrator 需求的任何伺服器上安裝 Docker

## 開始之前

您可以使用 Docker Datacenter 為 Docker Engine 中執行的 XClarity Administrator 容器設定高可用性環境。如需 Docker Datacenter 高可用性的相關資訊，請參閱 使用 Docker Datacenter 實現高可用性架構和應用程式 網頁。

確認主機符合 XClarity Administrator 線上文件的硬體和軟體必要條件。

確認主機系統與您要管理的裝置位於相同網路中。

**重要事項：**您可以在符合 XClarity Administrator 需求的任何系統上設定 XClarity Administrator，包括受管理伺服器在內。如果您使用受管理伺服器做為 XClarity Administrator 主機：

- 您必須實作虛擬分離資料和管理網路拓撲，或是單一資料和管理網路拓撲。
- 您無法使用 XClarity Administrator 將韌體更新套用至該受管理伺服器。即使只能透過立即啟動套用部分硬體，XClarity Administrator 仍會強制目標伺服器重新啟動，這也會重新啟動 XClarity Administrator。透過延遲啟動套用時，在 XClarity Administrator 主機重新啟動時只會套用部分韌體。
- 如果您使用 Flex System 機箱內的伺服器，請確定伺服器設定為自動開啟電源。您可以從 CMM Web 介面中設定此選項，方法是按一下**機箱管理 → 計算節點**，然後選取伺服器，再選取**自動電源**做為**自動開啟電源模式**。

## 程序

使用隨著 Docker 分配提供的指示，在主機上安裝及配置 Docker。

## 步驟 6. 安裝和配置 XClarity Administrator

在剛安裝的 Docker 主機上安裝及配置 Lenovo XClarity Administrator 容器。

### 開始之前

確定主機系統符合最低的硬體和軟體需求（請參閱硬體和軟體必要條件）。

確定已啟用所有適用的埠，包括 XClarity Administrator 所需的埠（請參閱埠可用性）。

確認主機系統與您要管理的裝置位於相同網路中。

確保主機 OS 和 XClarity Administrator 使用相同的 NTP 伺服器。

XClarity Administrator 允許用於資料管理、硬體管理和 OS 部署的網路使用自訂名稱（請參閱網路配置）。以下程序中的範例使用的是 eth0。

XClarity Administrator 允許用於資料和硬體管理的網路和用於 OS 部署的網路使用自訂名稱（請參閱網路配置）。以下程序中的範例使用的分別是 eth0 和 eth1

確定主機系統上的核心中載入了 macvlan 網路。若要檢查是否已載入，請使用 **lsmod | grep macvlan** 指令。若要將 macvlan 載入核心中，請執行 **modprobe macvlan** 指令。

在同一個主機上執行多個 XClarity Administrator 容器時，確保為每個容器使用唯一的名稱和 IP 位址。

如果您打算管理 ThinkServer 和其他舊式裝置，請確保啟用 Docker 以支援 IPv6。

1. 編輯 /etc/docker/daemon.json 檔案，將 **ipv6** 機碼設定為 true，並將 **fixed-cidr-v6** 機碼設定為您的 IPv6 子網路。以下是 daemon 檔案的範例。
```
{
  "ipv6": true,
  "fixed-cidr-v6": "2001:db8:1::/64",
  "experimental": true,
  "ip6tables": true
}
```
2. 執行下列指令以重新載入 Docker 配置檔。
```
systemctl reload docker
```

**附註：**XClarity Administrator *不是*做為特殊權限容器執行。

XClarity Administrator 容器中未配置防火牆規則。若要為主機系統上的容器新增防火牆規則，請完成下列步驟。

1. 透過執行下列指令取得由「NSPID」識別的 Docker 程序 ID。
```
docker inspect --format='{{ .State.Pid }}' "$CONTAINER_NAME"
```
2. 透過執行下列指令建立符號鏈結。
```
LINKFILE="/var/run/netns/$NSPID"
mkdir -p /var/run/netns
/bin/rm -f "$LINKFILE"
ln -s "/proc/$NSPID/ns/net" "$LINKFILE"
```
3. 透過執行下列指令配置適當的 iptables 規則。
```
ip netns exec $NSPID iptables -I OUTPUT -j DROP
```
4. 透過執行下列指令確保所有鏈結都已移除。
```
/bin/rm -f "$LINKFILE"
```

### 程序

若要使用 Docker compose 安裝 XClarity Administrator 容器，請完成下列步驟。

步驟 1. 從 XClarity Administrator 下載網頁將 XClarity Administrator 虛擬裝置映像檔、環境檔案和 YAML 檔案下載到用戶端工作站。登入網站，然後使用提供給您的存取金鑰以下載映像檔。

步驟 2. 透過執行下列指令，將 XClarity Administrator 容器映像檔匯入 Docker 主機。

```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

步驟 3. 編輯 `docker_compose.env` 檔案，並更新下列環境變數。

- **CONTAINER_NAME**。唯一的容器名稱，用於為每個 XClarity Administrator 實例建立 Docker 磁區（例如，`CONTAINER_NAME=LXCA-203`）
- **ADDRESS**。容器的靜態 IPv4 位址（例如，`ADDRESS=192.0.2.0`）
- **BACKUP_MOUNT**。（選用）可用於儲存 XClarity Administrator 備份的遠端共用路徑。這必須是 `/mnt/backup_share`。
- **FIRMWARE_MOUNT**。（選用）可用來做為韌體更新遠端儲存庫的遠端共用路徑。這必須是 `/mnt/fw_share`。

以下是環境檔案的範例。

```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

步驟 4. 編輯 `docker_compose.yml`，並更新以下內容。

- 將 **image** 內容設定為步驟 2 中使用的安裝映像檔的名稱。

  **附註：**您可以使用 `docker tag` 指令變更映像檔名稱（例如，變更為「latest」）。
- 如果要使用遠端共用做為遠端韌體儲存庫並儲存 XClarity Administrator 備份，請在 **volumes** 內容中為每個遠端共用設定主機裝載點。
- 將 **dns** 內容設定為 DNS 伺服器的 IP 位址。
- 容器共用主機可用的處理器和記憶體資源儲存區。（選用）透過設定 **cpus** 和 **memory** 內容，定義資源使用限制。
- 將 **parent** 內容設定為主機系統上的網路介面名稱，以用來做為容器中 macvlan 介面的父介面。此介面必須可以直接存取指派給容器的子網路。
- 根據您的網路拓撲設定 **subnet** 和 **gateway**。通常，子網路和閘道用於 ${ADDRESS} 所屬的管理網路。
- 如果要支援 IPv6，請將 **enable_ipv6** 內容設定為 true，將 **ipv6_address** 內容設定為 IPv6 位址，並根據您的網路拓撲新增另一組 **subnet** 和 **gateway** 內容（通常是該 IPv6 位址所屬的管理網路）。

下面是啟用了 IPv6 的 YML 檔案範例。

```
version: '3.8'

services:

 lxca:
  image: lenovo/lxca:4.1.0-124
  container_name: ${CONTAINER_NAME}
  tty: true
  stop_grace_period: 60s
  volumes:
   #bind mount example
   - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
```

```
    - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
    #docker volume mount
    - data:/opt/lenovo/lxca/data
    - postgresql:/var/lib/postgresql
    - log:/var/log
    - confluent-etc:/etc/confluent
    - confluent-log:/var/log/confluent
    - confluent:/var/lib/confluent
    - propconf:/opt/lenovo/lxca/bin/conf
    - ssh:/etc/ssh
    - xcat:/etc/xcat
  networks:
   lan1:
    ipv4_address: ${ADDRESS}
    ipv6_address: "2001:8003:7d51:2000::2"
   lan2:
    ipv4_address: 192.0.1.3
    ipv6_address: "2001:8003:7d51:2003::2"
  dns:
   - 192.0.40.10
   - 192.0.50.11
  deploy:
   resources:
    limits:
     cpus: "2.0"
     memory: "8g"

volumes:
 data:
  name: ${CONTAINER_NAME}-data
 postgresql:
  name: ${CONTAINER_NAME}-postgresql
 log:
  name: ${CONTAINER_NAME}-log
 confluent-etc:
  name: ${CONTAINER_NAME}-confluent-etc
 confluent-log:
  name: ${CONTAINER_NAME}-confluent-log
 confluent:
  name: ${CONTAINER_NAME}-confluent
 propconf:
  name: ${CONTAINER_NAME}-propconf
 ssh:
  name: ${CONTAINER_NAME}-ssh
 xcat:
  name: ${CONTAINER_NAME}-xcat

networks:
 lan1:
  name: lan1
  driver: macvlan
  enable_ipv6: true
  driver_opts:
   parent: eno1
  ipam:
   config:
    - subnet: 192.0.0.0/19
      gateway: 192.0.30.1
    - subnet: "2001:8003:7d51:2000::/80"
      gateway: "2001:8003:7d51:2000::1"
 lan2:
```

```
name: lan2
driver: macvlan
enable_ipv6: true
driver_opts:
 parent: virbr0
ipam:
 config:
  - subnet: 192.0.122.0/24
  - subnet: "2001:8003:7d51:2005::/80"
```

步驟 5. 透過執行下列指令在 Docker 中部署映像檔，其中 *<ENV_FILENAME>* 是您在步驟 2 中建立的環境變數檔案的名稱。

```
COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d
```

### 在您完成之後

登入並配置 XClarity Administrator（請參閱初次存取 Lenovo XClarity Administrator Web 介面和配置 Lenovo XClarity Administrator）。

## 虛擬分離資料和管理網路拓撲

在此拓撲中，資料網路與管理網路是虛擬分開的。來自資料網路的封包以及來自管理網路的封包會透過相同的實體連線傳送。位於所有管理網路資料封包上的 VLAN 標記是用來分隔兩個網路之間的資料流量。

### 開始之前

確定已啟用所有適用的埠，包括 XClarity Administrator 所需的埠（請參閱 XClarity Administrator 線上文件中的埠可用性）。

確定您要使用 XClarity Administrator 管理的每個裝置上都已安裝最低需求韌體。您可以從 XClarity Administrator 支援 — 相容性 網頁找到最低所需韌體版本，方法是按一下 **Compatibility（相容性）**標籤，然後按一下適當裝置類型的鏈結。

確認已設定資料網路和管理網路的 VLAN ID。或者，如果您從 Flex 交換器 實作標記，則在 Flex 交換器 中啟用 VLAN 標記，如果您從機架頂端交換器實作標記，則從機架頂端交換器啟用。

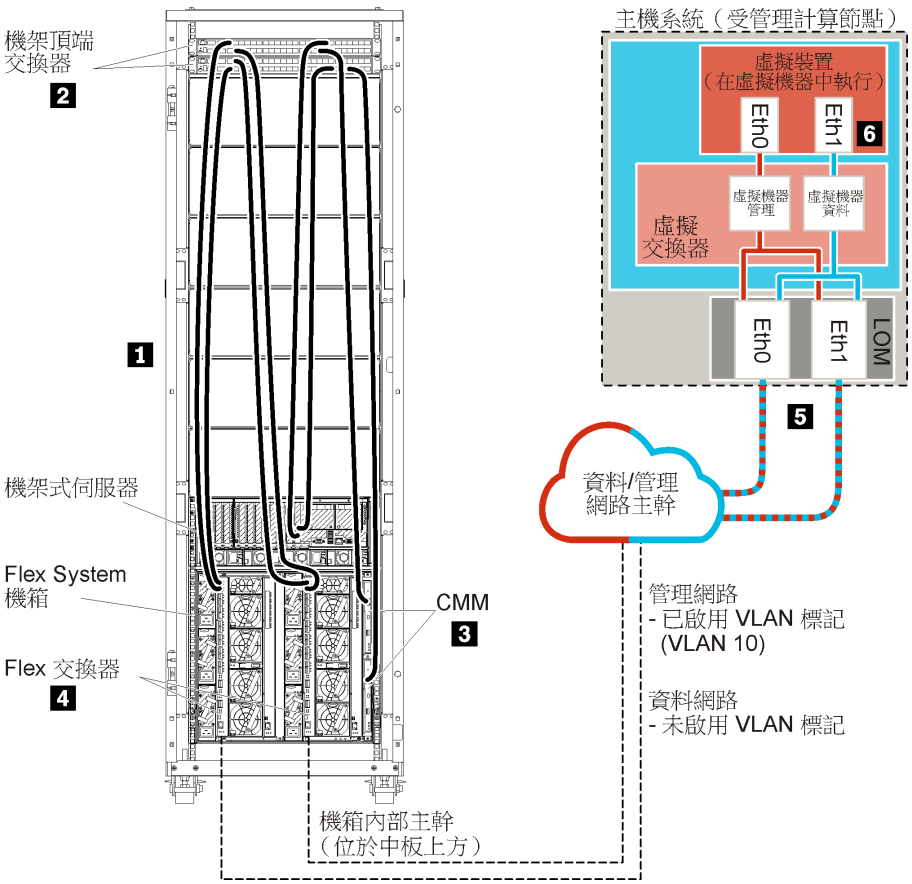
確定您將 CMM 連接的埠定義為隸屬於管理 VLAN。

**重要事項：**配置裝置和元件，以盡量減少 IP 位址變更。考慮使用靜態 IP 位址，而不使用動態主機配置通訊協定 (DHCP)。如果使用 DHCP，務必盡量減少 IP 位址變更。

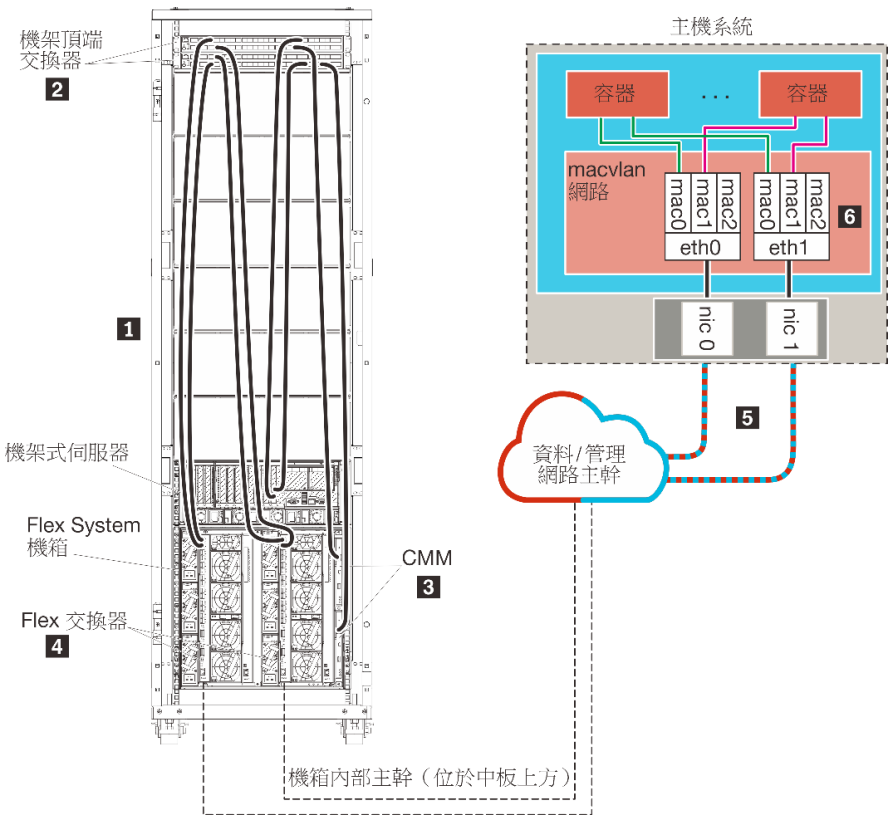
### 關於此作業

下圖說明的環境設定方式，可將管理網路與虛擬網路分開。圖中的數字對應下列各節的編號步驟。

**附註：**此圖中並未描述您環境中可能需要的所有佈線選項。此圖僅顯示 Flex 交換器、CMM 及機架式伺服器的佈線選項需求，因為它們與設定虛擬分離資料和管理網路相關。




*圖例 16. 虛擬裝置的虛擬分離資料和管理網路拓撲範例*




*圖例 17. 容器的虛擬分離資料和管理網路拓撲範例*

在此情景中，XClarity Administrator 是安裝在 Flex System 機箱內 XClarity Administrator 所管理的伺服器上。

**重要事項：**您可以在符合 XClarity Administrator 需求的任何系統上設定 XClarity Administrator，包括受管理伺服器在內。如果您使用受管理伺服器做為 XClarity Administrator 主機：

- 您必須實作虛擬分離資料和管理網路拓撲，或是單一資料和管理網路拓撲。
- 您無法使用 XClarity Administrator 將韌體更新套用至該受管理伺服器。即使只能透過立即啟動套用部分硬體，XClarity Administrator 仍會強制目標伺服器重新啟動，這也會重新啟動 XClarity Administrator。透過延遲啟動套用時，在 XClarity Administrator 主機重新啟動時只會套用部分韌體。
- 如果您使用 Flex System 機箱內的伺服器，請確定伺服器設定為自動開啟電源。您可以從 CMM Web 介面中設定此選項，方法是按一下**機箱管理 → 計算節點**，然後選取伺服器，再選取**自動電源**做為**自動開啟電源模式**。

同樣在此情景中，所有資料都是透過相同的實體連線傳送。管理網路與資料網路是透過 VLAN 標記加以分開，當中對應管理網路的特定標記會附加至傳入的資料封包，以確保正確佈置到適當的介面。輸出資料封包中的標記則會移除。

VLAN 標記可在下列其中一個裝置上啟用：

- **機架頂端交換器**。對應管理網路的 VLAN 標記會在進入機架頂端交換器時新增至封包，然後通過 Flex 交換器 並前往 Flex System 機箱內的伺服器。在傳回路由上會將 VLAN 標記移除，因為它們是從機架頂端交換器傳送至管理控制器。
- **Flex 交換器**。對應管理網路的 VLAN 標記會在進入 Flex 交換器 時新增至封包，然後傳遞至 Flex System 機箱內的伺服器。在傳回路由上，伺服器會新增 VLAN 標記，並將其傳遞至 Flex 交換器，然後在轉遞至管理控制器時將它們移除。

是否要實作 VLAN 標記取決於您環境的需要與複雜度。

如果您想要安裝 XClarity Administrator，用來管理已配置的現有機箱和機架式伺服器，請繼續執行步驟 5：安裝及配置主機。

如需有關規劃此拓撲的其他資訊，包括網路設定和 Eth1 與 Eth0 配置的相關資訊，請參閱虛擬分離資料和管理網路。

## 步驟 1：將機箱和機架式伺服器的纜線連接到機架頂端交換器

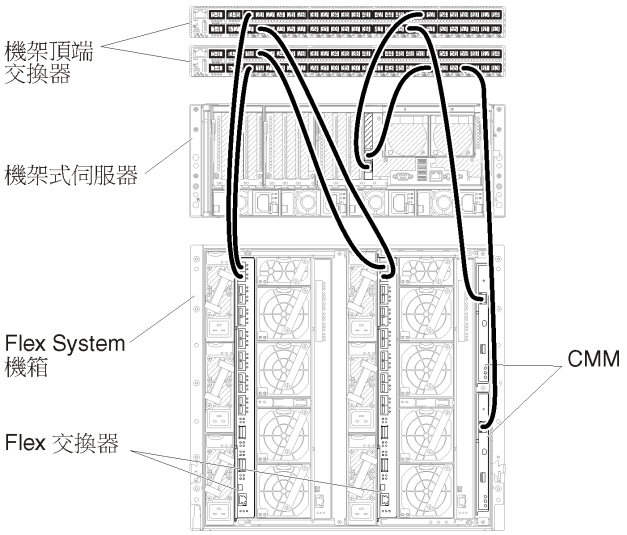
將機箱和機架式伺服器的纜線連接到相同的機架頂端交換器，以啟用裝置之間的通訊。

### 程序

將每個機箱中的每一部 Flex 交換器和 CMM 及每一部機架式伺服器的纜線連接到兩台機架頂端交換器。您可以選擇該機架頂端交換器的任何埠。

下圖的範例說明，當 Lenovo XClarity Administrator 安裝在 XClarity Administrator 所管理的機箱內伺服器上時，從機箱（Flex 交換器和 CMM）和機架式伺服器將纜線連接到機架頂端交換器的範例。

**附註：**此圖中並未描述您環境中可能需要的所有佈線選項。此圖僅顯示 Flex 交換器、CMM 及機架式伺服器的佈線選項需求，因為它們與設定虛擬分離資料和管理網路相關。




*圖例 18. 虛擬分離資料和管理網路的纜線佈線範例*

## 步驟 2：配置機架頂端交換器

配置機架頂端交換器。

### 開始之前

除了機架頂端交換器的一般配置需求之外，請確定已啟用所有適當的埠，包括用於 Flex 交換器、機架式伺服器和網路的外部埠，以及用於 CMM、機架式伺服器和網路的內部埠。

您可以根據環境的需要和複雜度，在 Flex 交換器或機架頂端交換器中實作 VLAN 標記。如果您從機架頂端交換器實作標記，請從機架頂端交換器啟用 VLAN 標記。

確認已設定管理和資料網路的 VLAN ID。

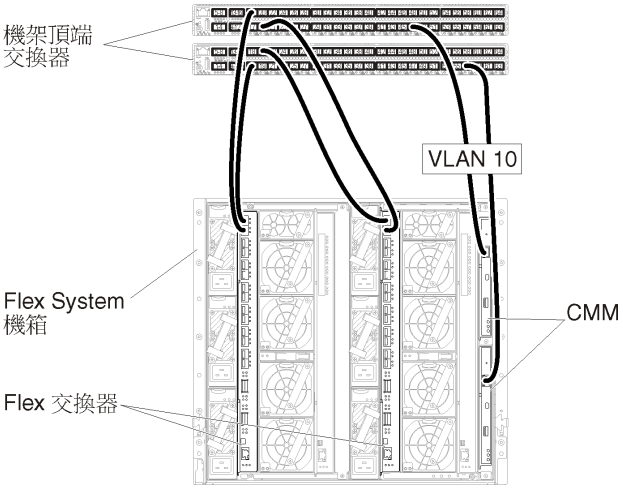
## 程序

配置步驟可能會隨著所安裝的機架交換器類型而有所不同。

下圖的範例情景說明在機架頂端交換器中實作且只在管理網路上啟用的 VLAN 標記。管理 VLAN 設定為 VLAN 10。

在此情景中，您必須將 CMM 連接的埠定義為隸屬於管理 VLAN。

**附註：**您也可以在資料網路上啟用 VLAN 標記，以配置資料 VLAN。




*圖例 19. 虛擬分離資料和管理網路 (VMware ESXi) 上的 Flex 交換器 範例配置，其中 VLAN 標記是在管理網路上啟用*

如需配置 Lenovo 機架頂端交換器的相關資訊，請參閱 System x 中的機架交換器線上文件。如果安裝其他機架頂端交換器，請參閱該交換器隨附的文件。

# 步驟 3：配置 Chassis Management Module (CMM)

在您的機箱中配置主要 Chassis Management Module (CMM)，用來管理機箱內的所有裝置。

## 關於此作業

如需配置 CMM 的詳細資訊，請參閱 Flex System 線上文件中的 「配置機箱元件」。

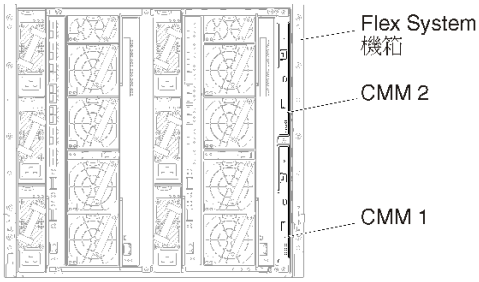
此外，請參閱機箱隨附說明書上的步驟 4.1 - 4.5。

## 程序

請完成下列步驟以配置 CMM。

如果安裝兩個 CMM，請僅配置*主要* CMM，它會自動將配置與待命 CMM 同步。

步驟 1. 將機槽 1 中 CMM 的乙太網路纜線連接到用戶端工作站，以建立直接連線。




第一次連接至 CMM 時，您可能需要變更用戶端工作站上的「網際網路通訊協定」內容。

**重要事項：**請確定用戶端工作站子網路與 CMM 子網路相同。（預設 CMM 子網路為 255.255.255.0）。為用戶端工作站選擇的 IP 位址必須與 CMM 位於相同網路上（例如 192.168.70.0 - 192.168.70.24）。

步驟 2. 若要啟動 CMM 管理介面，請在用戶端工作站上開啟 Web 瀏覽器，並且將它指向 CMM IP 位址。

**附註：**

- 請確定您使用的是安全連線，且 URL 中包含 **https**（例如 https://192.168.70.100）。如果未包含 https，您將會收到找不到頁面的錯誤訊息。
- 如果您使用預設 IP 位址 192.168.70.100，CMM 管理介面可能需要花幾分鐘才能使用。這個延遲情況是因為 CMM 會花兩分鐘嘗試取得 DHCP 位址，然後才回復為預設靜態位址。

步驟 3. 使用預設使用者 ID `USERID` 和密碼 `PASSWORD` 登入 CMM 管理介面。登入後，您必須變更預設密碼。

步驟 4. 完成「CMM 起始設定精靈」，以指定環境的詳細資料。「起始設定精靈」包括下列選項：

- 檢視機箱庫存和性能。
- 從現行的配置檔匯入配置。
- 配置一般 CMM 設定。
- 配置 CMM 日期和時間。

  **要訣：**當您安裝 XClarity Administrator 時，您會將 XClarity Administrator 及 XClarity Administrator 管理的所有機箱配置為使用 NTP 伺服器。
- 配置 CMM IP 資訊。
- 配置 CMM 安全原則。
- 配置網域名稱系統 (DNS)。
- 配置事件轉遞器。

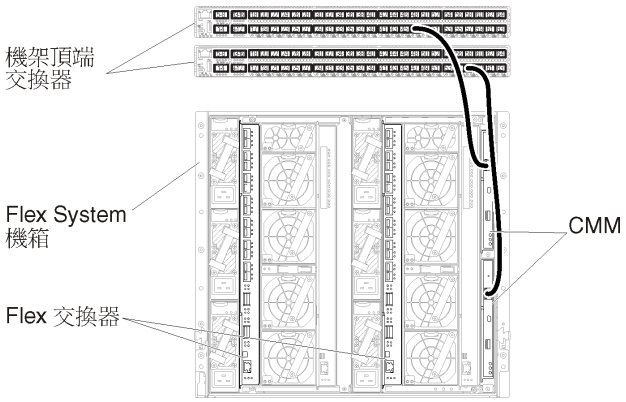
步驟 5. 儲存設定精靈設定並套用變更後，配置機箱中所有元件的 IP 位址。

請參閱機箱隨附說明書上的步驟 4.6。

**附註：**您必須重設每個計算節點的系統管理處理器，並重新啟動 Flex 交換器，才會顯示新的 IP 位址。

步驟 6. 使用 CMM 管理介面重新啟動 CMM。

步驟 7. CMM 重新啟動時，將纜線分別連接到 CMM 上的乙太網路埠和您的網路。




步驟 8. 使用新的 IP 位址登入 CMM 管理介面。

## 在您完成之後

您也可以配置 CMM，使其支援備援。請使用 CMM 說明系統進一步瞭解下列每一個頁面上提供的欄位。

- 為 CMM 配置失效接手，以防主要 CMM 發生硬體故障。在 CMM 管理介面中，按一下 **Mgt Module Management → 內容 → 進階失效接手**。
- 配置失效接手做為網路問題的最終解決方法（上行）。在 CMM 管理介面中，按一下 **Mgt Module Management → 網路**，按一下**乙太網路**標籤，然後按一下**進階乙太網路**。請確定至少要選取**喪失實體網路鏈結時失效接手**。

# 步驟 4：配置 Flex 交換器

配置每個機箱中的 Flex 交換器。

## 開始之前

確定已啟用所有適當的埠，包括從 Flex 交換器到機架頂端交換器的外部埠，以及連接到 CMM 的內部埠。

您可以根據環境的需要和複雜度，在 Flex 交換器或機架頂端交換器中實作 VLAN 標記。如果您從 Flex 交換器實作標記，請從 Flex 交換器啟用 VLAN 標記。

確認已設定管理和資料網路的 VLAN ID。

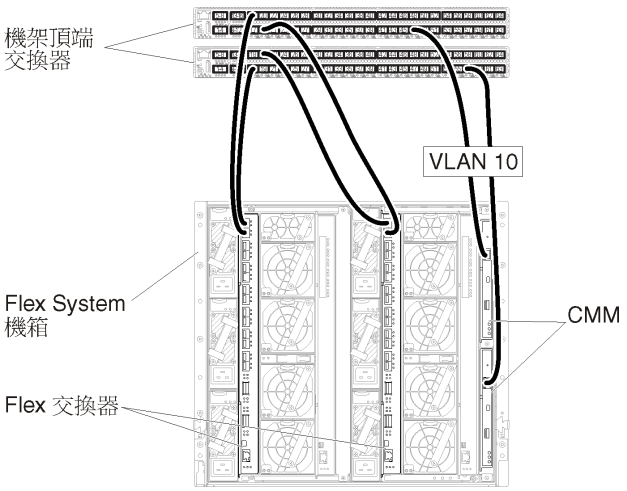
**重要事項：**對於每個 Flex System 機箱，請確定機箱內的每一部伺服器中擴充卡的光纖類型，能夠與相同機箱中所有 Flex 交換器的光纖類型相容。例如，如果乙太網路交換器安裝在機箱中，則該機箱中的所有伺服器都必須具備透過主機板上 LAN 接頭或乙太網路擴充卡連線到乙太網路的功能。如需配置 Flex 交換器的相關資訊，請參閱 Flex Systems 線上文件中的「配置 I/O 模組」。

## 程序

配置步驟可能會隨著所安裝的 Flex 交換器 類型而有所不同。如需支援的每一種 Flex 交換器 的相關資訊，請參閱 Flex Systems 線上文件中的「Flex System 網路交換器」。

下圖的範例情景說明在 Flex 交換器中實作且只在管理網路上啟用的 VLAN 標記。管理 VLAN 設定為 VLAN 10。

**附註：**您可以在資料網路上啟用 VLAN 標記，藉此配置資料 VLAN。




*圖例 20. 虛擬分離資料和管理網路 (VMware ESXi) 上的 Flex 交換器 範例配置，其中 VLAN 標記是在管理網路上啟用*

若要配置此情景的 Flex 交換器，請完成下列步驟：

步驟 1. 在 Flex 交換器機槽 1 中配置 Flex 交換器：

a. 定義管理 VLAN（在此範例中，我們選擇了 VLAN 10）以包含外部埠，其中纜線是佈置到機架頂端管理交換器 (Ext1)。

b. 將內部埠定義為 VLAN 10（管理 VLAN）的一部分。確認已在該埠上啟用 VLAN 主幹連線。

步驟 2. 在 Flex 交換器機槽 2 中配置 Flex 交換器：

**要訣：**Flex 交換器機槽 2 實際上是機箱背面的第三個模組機槽：

a. 定義管理 VLAN（在此範例中，我們選擇了 VLAN 10）以包含外部埠，其中纜線是佈置到機架頂端管理交換器。

b. 將內部埠定義為 VLAN 10（管理 VLAN）的一部分。確認已在該埠上啟用 VLAN 主幹連線。

## 步驟 5：安裝及配置主機

您可以在符合 Lenovo XClarity Administrator 需求的任何系統上安裝 Docker。

### 開始之前

您可以使用 Docker Datacenter 為 Docker Engine 中執行的 XClarity Administrator 容器設定高可用性環境。如需 Docker Datacenter 高可用性的相關資訊，請參閱 使用 Docker Datacenter 實現高可用性架構和應用程式 網頁。

確認主機符合 XClarity Administrator 線上文件的硬體和軟體必要條件。

確認主機系統與您要管理的裝置位於相同網路中。

**重要事項：**您可以在符合 XClarity Administrator 需求的任何系統上設定 XClarity Administrator，包括受管理伺服器在內。如果您使用受管理伺服器做為 XClarity Administrator 主機：

- 您必須實作虛擬分離資料和管理網路拓撲，或是單一資料和管理網路拓撲。
- 您無法使用 XClarity Administrator 將韌體更新套用至該受管理伺服器。即使只能透過立即啟動套用部分硬體，XClarity Administrator 仍會強制目標伺服器重新啟動，這也會重新啟動 XClarity Administrator。透過延遲啟動套用時，在 XClarity Administrator 主機重新啟動時只會套用部分韌體。

- 如果您使用 Flex System 機箱內的伺服器，請確定伺服器設定為自動開啟電源。您可以從 CMM Web 介面中設定此選項，方法是按一下**機箱管理 → 計算節點**，然後選取伺服器，再選取**自動電源**做為**自動開啟電源模式**。

### 程序

使用隨著 Docker 分配提供的指示，在主機上安裝及配置 Docker。

## 步驟 6. 安裝和配置 XClarity Administrator

在剛安裝的 Docker 主機上安裝及配置 Lenovo XClarity Administrator 容器。

### 開始之前

確定主機系統符合最低的硬體和軟體需求（請參閱硬體和軟體必要條件）。

確定已啟用所有適用的埠，包括 XClarity Administrator 所需的埠（請參閱埠可用性）。

確認主機系統與您要管理的裝置位於相同網路中。

確保主機 OS 和 XClarity Administrator 使用相同的 NTP 伺服器。

XClarity Administrator 允許用於資料管理、硬體管理和 OS 部署的網路使用自訂名稱（請參閱網路配置）。以下程序中的範例使用的是 eth0。

XClarity Administrator 允許用於資料和硬體管理的網路和用於 OS 部署的網路使用自訂名稱（請參閱網路配置）。以下程序中的範例使用的分別是 eth0 和 eth1。

確定主機系統上的核心中載入了 macvlan 網路。若要檢查是否已載入，請使用 **lsmod | grep macvlan** 指令。若要將 macvlan 載入核心中，請執行 **modprobe macvlan** 指令。

在同一個主機上執行多個 XClarity Administrator 容器時，確保為每個容器使用唯一的名稱和 IP 位址。

如果您打算管理 ThinkServer 和其他舊式裝置，請確保啟用 Docker 以支援 IPv6。

1. 編輯 /etc/docker/daemon.json 檔案，將 **ipv6** 機碼設定為 true，並將 **fixed-cidr-v6** 機碼設定為您的 IPv6 子網路。以下是 daemon 檔案的範例。
```
{
  "ipv6": true,
  "fixed-cidr-v6": "2001:db8:1::/64",
  "experimental": true,
  "ip6tables": true
}
```
2. 執行下列指令以重新載入 Docker 配置檔。
```
systemctl reload docker
```

**附註：**XClarity Administrator *不是*做為特殊權限容器執行。

XClarity Administrator 容器中未配置防火牆規則。若要為主機系統上的容器新增防火牆規則，請完成下列步驟。

1. 透過執行下列指令取得由「NSPID」識別的 Docker 程序 ID。
```
docker inspect --format='{{ .State.Pid }}' "$CONTAINER_NAME"
```
2. 透過執行下列指令建立符號鏈結。
```
LINKFILE="/var/run/netns/$NSPID"
mkdir -p /var/run/netns
/bin/rm -f "$LINKFILE"
```

```
ln -s "/proc/$NSPID/ns/net" "$LINKFILE"
```

3. 透過執行下列指令配置適當的 iptables 規則。
```
ip netns exec $NSPID iptables -I OUTPUT -j DROP
```
4. 透過執行下列指令確保所有鏈結都已移除。
```
/bin/rm -f "$LINKFILE"
```

## 程序

若要使用 Docker compose 安裝 XClarity Administrator 容器，請完成下列步驟。

步驟 1. 從 XClarity Administrator 下載網頁將 XClarity Administrator 虛擬裝置映像檔、環境檔案和 YAML 檔案下載到用戶端工作站。登入網站，然後使用提供給您的存取金鑰以下載映像檔。

步驟 2. 透過執行下列指令，將 XClarity Administrator 容器映像檔匯入 Docker 主機。
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

步驟 3. 編輯 `docker_compose.env` 檔案，並更新下列環境變數。

- **CONTAINER_NAME**。唯一的容器名稱，用於為每個 XClarity Administrator 實例建立 Docker 磁區（例如，`CONTAINER_NAME=LXCA-203`）
- **ADDRESS**。容器的靜態 IPv4 位址（例如，`ADDRESS=192.0.2.0`）
- **BACKUP_MOUNT**。（選用）可用於儲存 XClarity Administrator 備份的遠端共用路徑。這必須是 `/mnt/backup_share`。
- **FIRMWARE_MOUNT**。（選用）可用來做為韌體更新遠端儲存庫的遠端共用路徑。這必須是 `/mnt/fw_share`。

以下是環境檔案的範例。
```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

步驟 4. 編輯 `docker_compose.yml`，並更新以下內容。

- 將 **image** 內容設定為步驟 2 中使用的安裝映像檔的名稱。

  **附註：**您可以使用 `docker tag` 指令變更映像檔名稱（例如，變更為「latest」）。
- 如果要使用遠端共用做為遠端韌體儲存庫並儲存 XClarity Administrator 備份，請在 **volumes** 內容中為每個遠端共用設定主機裝載點。
- 將 **dns** 內容設定為 DNS 伺服器的 IP 位址。
- 容器共用主機可用的處理器和記憶體資源儲存區。（選用）透過設定 **cpus** 和 **memory** 內容，定義資源使用限制。
- 將 **parent** 內容設定為主機系統上的網路介面名稱，以用來做為容器中 macvlan 介面的父介面。此介面必須可以直接存取指派給容器的子網路。
- 根據您的網路拓撲設定 **subnet** 和 **gateway**。通常，子網路和閘道用於 ${ADDRESS} 所屬的管理網路。
- 如果要支援 IPv6，請將 **enable_ipv6** 內容設定為 true，將 **ipv6_address** 內容設定為 IPv6 位址，並根據您的網路拓撲新增另一組 **subnet** 和 **gateway** 內容（通常是該 IPv6 位址所屬的管理網路）。

下面是啟用了 IPv6 的 YML 檔案範例。

```
version: '3.8'

services:
```

```
  lxca:
   image: lenovo/lxca:4.1.0-124
   container_name: ${CONTAINER_NAME}
   tty: true
   stop_grace_period: 60s
   volumes:
    #bind mount example
    - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
    - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
    #docker volume mount
    - data:/opt/lenovo/lxca/data
    - postgresql:/var/lib/postgresql
    - log:/var/log
    - confluent-etc:/etc/confluent
    - confluent-log:/var/log/confluent
    - confluent:/var/lib/confluent
    - propconf:/opt/lenovo/lxca/bin/conf
    - ssh:/etc/ssh
    - xcat:/etc/xcat
   networks:
    lan1:
     ipv4_address: ${ADDRESS}
     ipv6_address: "2001:8003:7d51:2000::2"
    lan2:
     ipv4_address: 192.0.1.3
     ipv6_address: "2001:8003:7d51:2003::2"
   dns:
    - 192.0.40.10
    - 192.0.50.11
   deploy:
    resources:
     limits:
      cpus: "2.0"
      memory: "8g"

volumes:
  data:
   name: ${CONTAINER_NAME}-data
  postgresql:
   name: ${CONTAINER_NAME}-postgresql
  log:
   name: ${CONTAINER_NAME}-log
  confluent-etc:
   name: ${CONTAINER_NAME}-confluent-etc
  confluent-log:
   name: ${CONTAINER_NAME}-confluent-log
  confluent:
   name: ${CONTAINER_NAME}-confluent
  propconf:
   name: ${CONTAINER_NAME}-propconf
  ssh:
   name: ${CONTAINER_NAME}-ssh
  xcat:
   name: ${CONTAINER_NAME}-xcat

networks:
  lan1:
   name: lan1
   driver: macvlan
   enable_ipv6: true
   driver_opts:
```

```
    parent: eno1
  ipam:
    config:
      - subnet: 192.0.0.0/19
        gateway: 192.0.30.1
      - subnet: "2001:8003:7d51:2000::/80"
        gateway: "2001:8003:7d51:2000::1"
lan2:
  name: lan2
  driver: macvlan
  enable_ipv6: true
  driver_opts:
    parent: virbr0
  ipam:
    config:
      - subnet: 192.0.122.0/24
        gateway: 192.0.122.1
      - subnet: "2001:8003:7d51:2003::/80"
        gateway: "2001:8003:7d51:2003::1"
```

步驟 5. 透過執行下列指令在 Docker 中部署映像檔，其中 *<ENV_FILENAME>* 是您在步驟 2 中建立的環境變數檔案的名稱。

```
COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d
```

## 在您完成之後

登入並配置 XClarity Administrator（請參閱初次存取 Lenovo XClarity Administrator Web 介面和配置 Lenovo XClarity Administrator）。

# 管理專用網路拓撲

在此拓撲中，Lenovo XClarity Administrator 只有管理網路。它沒有資料網路。

## 開始之前

確定已啟用所有適當的埠，包括：

- XClarity Administrator 所需的埠（請參閱 XClarity Administrator 線上文件中的埠可用性）
- 網路用的外部埠
- CMM 用的內部埠

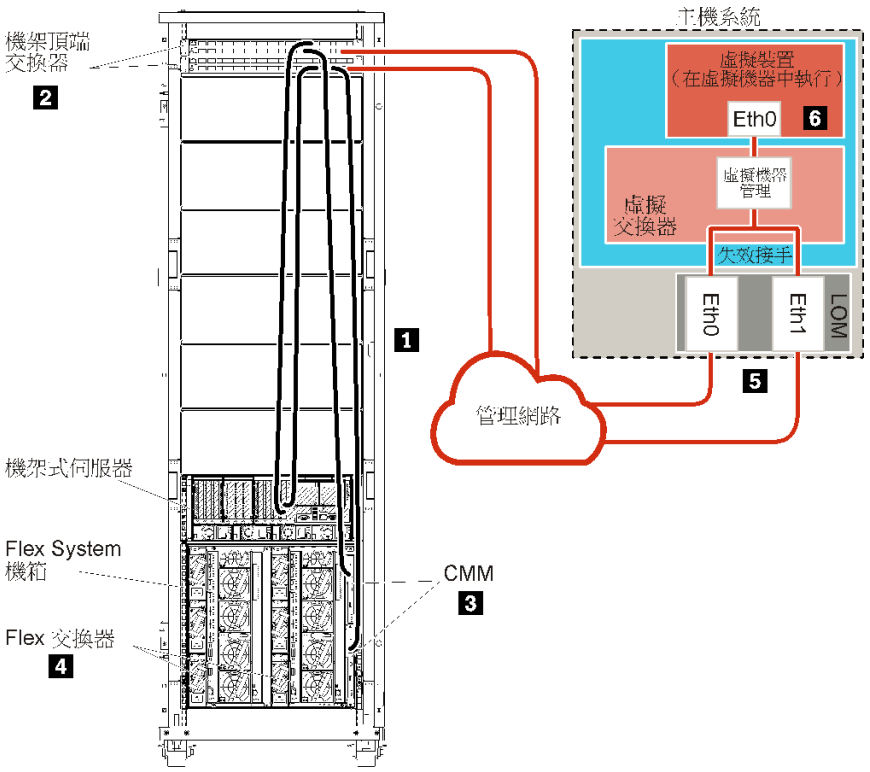
確定您要使用 XClarity Administrator 管理的每個裝置上都已安裝最低需求韌體。您可以從 XClarity Administrator 支援 — 相容性 網頁找到最低所需韌體版本，方法是按一下 **Compatibility（相容性）**標籤，然後按一下適當裝置類型的鏈結。

**重要事項：**配置裝置和元件，以盡量減少 IP 位址變更。考慮使用靜態 IP 位址，而不使用動態主機配置通訊協定 (DHCP)。如果使用 DHCP，務必盡量減少 IP 位址變更。

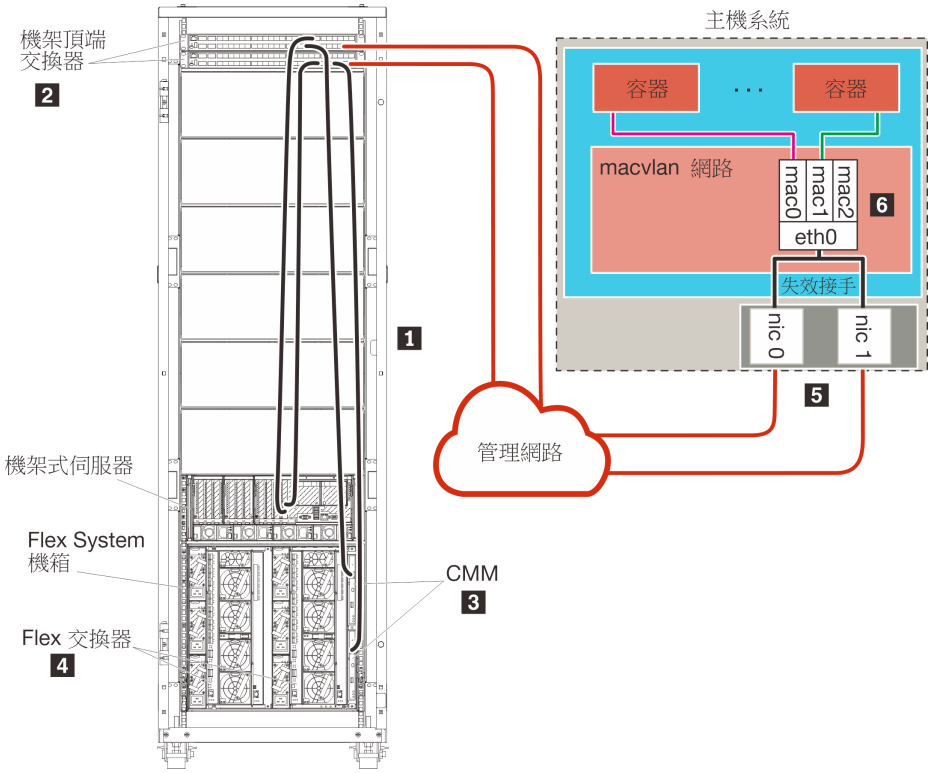
## 關於此作業

下圖說明在 Lenovo XClarity Administrator 只有管理網路（沒有資料網路）的情況下，設定環境的方式。圖中的數字對應下列各節的編號步驟。

**附註：**此圖中並未描述您環境中可能需要的所有佈線選項。此圖僅顯示 Flex 交換器、CMM 及機架式伺服器的佈線選項需求，因為它們與設定管理專用網路相關。




*圖例 21. 虛擬裝置的管理專用網路拓撲範例*




*圖例 22. 容器的管理專用網路拓撲範例*

如果您想要安裝 XClarity Administrator，用來管理已配置的現有機箱和機架式伺服器，請繼續執行步驟 5：安裝及配置主機。

如需有關規劃此拓撲的其他資訊，包括網路設定和 Eth1 與 Eth0 配置的相關資訊，請參閱管理專用網路。

## 步驟 1：將機箱、機架式伺服器及 Lenovo XClarity Administrator 主機的纜線連接到機架頂端交換器

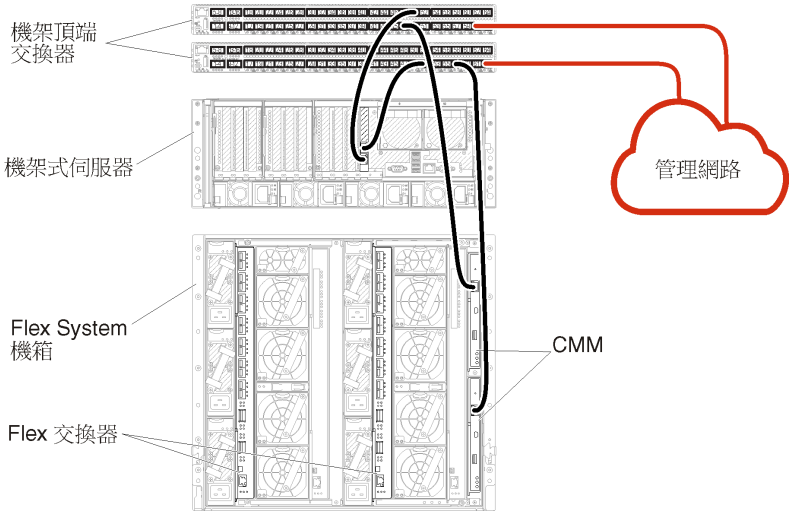
將機箱、機架式伺服器及 XClarity Administrator 主機的纜線連接到機架頂端交換器，以啟用裝置與網路之間的通訊。

### 程序

將每個機箱中的每一部 Flex 交換器和 CMM、每一部機架式伺服器及 XClarity Administrator 主機的纜線連接到兩台機架頂端交換器。您可以選擇機架頂端交換器的任何埠。

下圖的範例說明將纜線從機箱（Flex 交換器及 CMM）、機架式伺服器及 XClarity Administrator 主機連接到機架頂端交換器。

**附註：**此圖中並未描述您環境中可能需要的所有佈線選項。此圖僅顯示 Flex 交換器、CMM 及機架式伺服器的佈線選項需求，因為它們與設定管理專用網路相關。




*圖例 23. 管理專用網路的纜線連接範例*

## 步驟 2：配置機架頂端交換器

配置機架頂端交換器。

### 開始之前

除了機架頂端交換器的一般配置需求之外，請確定已啟用所有適當的埠，包括用於 Flex 交換器、機架式伺服器和網路的外部埠，以及用於 CMM、機架式伺服器和網路的內部埠。

### 程序

配置步驟可能會隨著所安裝的機架交換器類型而有所不同。

如需配置 Lenovo 機架頂端交換器的相關資訊，請參閱 System x 中的機架交換器線上文件。如果安裝其他機架頂端交換器，請參閱該交換器隨附的文件。

## 步驟 3：配置 Chassis Management Module (CMM)

在您的機箱中配置主要 Chassis Management Module (CMM)，用來管理機箱內的所有裝置。

### 關於此作業

如需配置 CMM 的詳細資訊，請參閱 Flex System 線上文件中的 「配置機箱元件」 。

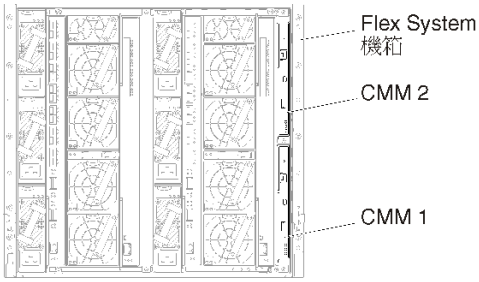
此外，請參閱機箱隨附說明書上的步驟 4.1 - 4.5。

### 程序

請完成下列步驟以配置 CMM。

如果安裝兩個 CMM，請僅配置*主要* CMM，它會自動將配置與待命 CMM 同步。

步驟 1. 將機槽 1 中 CMM 的乙太網路纜線連接到用戶端工作站，以建立直接連線。




第一次連接至 CMM 時，您可能需要變更用戶端工作站上的「網際網路通訊協定」內容。

**重要事項：**請確定用戶端工作站子網路與 CMM 子網路相同。（預設 CMM 子網路為 255.255.255.0）。為用戶端工作站選擇的 IP 位址必須與 CMM 位於相同網路上（例如 192.168.70.0 - 192.168.70.24）。

步驟 2. 若要啟動 CMM 管理介面，請在用戶端工作站上開啟 Web 瀏覽器，並且將它指向 CMM IP 位址。

**附註：**

- 請確定您使用的是安全連線，且 URL 中包含 **https**（例如 https://192.168.70.100）。如果未包含 https，您將會收到找不到頁面的錯誤訊息。
- 如果您使用預設 IP 位址 192.168.70.100，CMM 管理介面可能需要花幾分鐘才能使用。這個延遲情況是因為 CMM 會花兩分鐘嘗試取得 DHCP 位址，然後才回復為預設靜態位址。

步驟 3. 使用預設使用者 ID `USERID` 和密碼 `PASSWORD` 登入 CMM 管理介面。登入後，您必須變更預設密碼。

步驟 4. 完成「CMM 起始設定精靈」，以指定環境的詳細資料。「起始設定精靈」包括下列選項：

- 檢視機箱庫存和性能。
- 從現行的配置檔匯入配置。
- 配置一般 CMM 設定。
- 配置 CMM 日期和時間。

  **要訣：**當您安裝 XClarity Administrator 時，您會將 XClarity Administrator 及 XClarity Administrator 管理的所有機箱配置為使用 NTP 伺服器。

- 配置 CMM IP 資訊。
- 配置 CMM 安全原則。

- 配置網域名稱系統 (DNS)。
- 配置事件轉遞器。

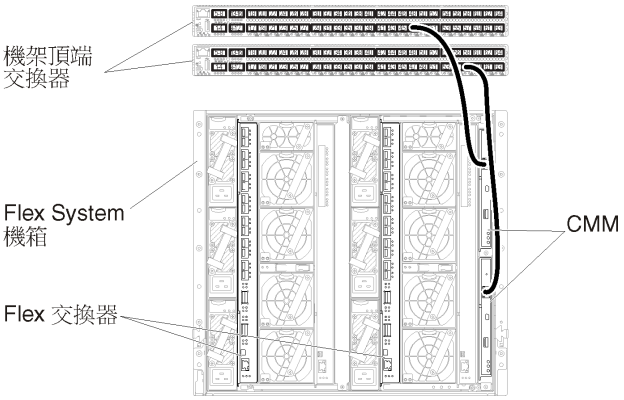
步驟 5. 儲存設定精靈設定並套用變更後，配置機箱中所有元件的 IP 位址。

請參閱機箱隨附說明書上的步驟 4.6。

**附註：**您必須重設每個計算節點的系統管理處理器，並重新啟動 Flex 交換器，才會顯示新的 IP 位址。

步驟 6. 使用 CMM 管理介面重新啟動 CMM。

步驟 7. CMM 重新啟動時，將纜線分別連接到 CMM 上的乙太網路埠和您的網路。




步驟 8. 使用新的 IP 位址登入 CMM 管理介面。

## 在您完成之後

您也可以配置 CMM，使其支援備援。請使用 CMM 說明系統進一步瞭解下列每一個頁面上提供的欄位。

- 為 CMM 配置失效接手，以防主要 CMM 發生硬體故障。在 CMM 管理介面中，按一下 **Mgt Module Management → 內容 → 進階失效接手**。
- 配置失效接手做為網路問題的最終解決方法（上行）。在 CMM 管理介面中，按一下 **Mgt Module Management → 網路**，按一下**乙太網路**標籤，然後按一下**進階乙太網路**。請確定至少要選取**喪失實體網路鏈結時失效接手**。

# 步驟 4：配置 Flex 交換器

配置每個機箱中的 Flex 交換器。

## 開始之前

確定已啟用所有適當的埠，包括從 Flex 交換器到機架頂端交換器的外部埠，以及連接到 CMM 的內部埠。

如果 Flex 交換器設定為透過 DHCP 取得動態網路設定（IP 位址、網路遮罩、閘道和 DNS 位址），請確定 Flex 交換器的設定一致（例如，確認 IP 位址與 CMM 位於相同的子網路）。

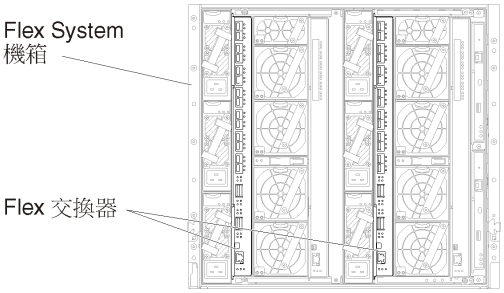
**重要事項：**對於每個 Flex System 機箱，請確定機箱內的每一部伺服器中擴充卡的光纖類型，能夠與相同機箱中所有 Flex 交換器的光纖類型相容。例如，如果乙太網路交換器安裝在機箱中，則該機箱中的所有伺服器都必須具備透過主機板上 LAN 接頭或乙太網路擴充卡連線到乙太網路的功能。如需配置 Flex 交換器的相關資訊，請參閱 Flex Systems 線上文件中的「配置 I/O 模組」。

## 程序

配置步驟可能會隨著所安裝的 Flex 交換器 類型而有所不同。如需支援的每一種 Flex 交換器 的相關資訊，請參閱 Flex Systems 線上文件中的「Flex System 網路交換器」 。

一般而言，您必須將 Flex 交換器配置在 Flex 交換器機槽 1 和 2 中。

**要訣：**Flex 交換器機槽 2 是機箱背面的第三個模組機槽。




*圖例 24. Flex 交換器 在機箱中的位置*

## 步驟 5：安裝及配置主機

您可以在符合 Lenovo XClarity Administrator 需求的任何系統上安裝 Docker。

### 開始之前

您可以使用 Docker Datacenter 為 Docker Engine 中執行的 XClarity Administrator 容器設定高可用性環境。如需 Docker Datacenter 高可用性的相關資訊，請參閱 使用 Docker Datacenter 實現高可用性架構和應用程式 網頁。

確認主機符合 XClarity Administrator 線上文件的硬體和軟體必要條件。

確認主機系統與您要管理的裝置位於相同網路中。

**重要事項：**您可以在符合 XClarity Administrator 需求的任何系統上設定 XClarity Administrator，包括受管理伺服器在內。如果您使用受管理伺服器做為 XClarity Administrator 主機：

- 您必須實作虛擬分離資料和管理網路拓撲，或是單一資料和管理網路拓撲。
- 您無法使用 XClarity Administrator 將韌體更新套用至該受管理伺服器。即使只能透過立即啟動套用部分硬體，XClarity Administrator 仍會強制目標伺服器重新啟動，這也會重新啟動 XClarity Administrator。透過延遲啟動套用時，在 XClarity Administrator 主機重新啟動時只會套用部分韌體。
- 如果您使用 Flex System 機箱內的伺服器，請確定伺服器設定為自動開啟電源。您可以從 CMM Web 介面中設定此選項，方法是按一下**機箱管理 → 計算節點**，然後選取伺服器，再選取**自動電源**做為**自動開啟電源模式**。

### 程序

使用隨著 Docker 分配提供的指示，在主機上安裝及配置 Docker。

## 步驟 6. 安裝和配置 XClarity Administrator

在剛安裝的 Docker 主機上安裝及配置 Lenovo XClarity Administrator 容器。

### 開始之前

確定主機系統符合最低的硬體和軟體需求（請參閱硬體和軟體必要條件）。

確定已啟用所有適用的埠，包括 XClarity Administrator 所需的埠（請參閱埠可用性）。

確認主機系統與您要管理的裝置位於相同網路中。

確保主機 OS 和 XClarity Administrator 使用相同的 NTP 伺服器。

XClarity Administrator 允許用於資料管理、硬體管理和 OS 部署的網路使用自訂名稱（請參閱網路配置）。以下程序中的範例使用的是 eth0。

XClarity Administrator 允許用於資料和硬體管理的網路使用自訂名稱（請參閱網路配置）。以下程序中的範例使用的是 eth0

確定主機系統上的核心中載入了 macvlan 網路。若要檢查是否已載入，請使用 **lsmod | grep macvlan** 指令。若要將 macvlan 載入核心中，請執行 **modprobe macvlan** 指令。

在同一個主機上執行多個 XClarity Administrator 容器時，確保為每個容器使用唯一的名稱和 IP 位址。

如果您打算管理 ThinkServer 和其他舊式裝置，請確保啟用 Docker 以支援 IPv6。

1. 編輯 /etc/docker/daemon.json 檔案，將 **ipv6** 機碼設定為 true，並將 **fixed-cidr-v6** 機碼設定為您的 IPv6 子網路。以下是 daemon 檔案的範例。
```
{
  "ipv6": true,
  "fixed-cidr-v6": "2001:db8:1::/64",
  "experimental": true,
  "ip6tables": true
}
```
2. 執行下列指令以重新載入 Docker 配置檔。
```
systemctl reload docker
```

**附註：**XClarity Administrator *不是*做為特殊權限容器執行。

XClarity Administrator 容器中未配置防火牆規則。若要為主機系統上的容器新增防火牆規則，請完成下列步驟。

1. 透過執行下列指令取得由「NSPID」識別的 Docker 程序 ID。
```
docker inspect --format='{{ .State.Pid }}' "$CONTAINER_NAME"
```
2. 透過執行下列指令建立符號鏈結。
```
LINKFILE="/var/run/netns/$NSPID"
mkdir -p /var/run/netns
/bin/rm -f "$LINKFILE"
ln -s "/proc/$NSPID/ns/net" "$LINKFILE"
```
3. 透過執行下列指令配置適當的 iptables 規則。
```
ip netns exec $NSPID iptables -I OUTPUT -j DROP
```
4. 透過執行下列指令確保所有鏈結都已移除。
```
/bin/rm -f "$LINKFILE"
```

## 程序

若要使用 Docker compose 安裝 XClarity Administrator 容器，請完成下列步驟。

步驟 1. 從 XClarity Administrator 下載網頁將 XClarity Administrator 虛擬裝置映像檔、環境檔案和 YAML 檔案下載到用戶端工作站。登入網站，然後使用提供給您的存取金鑰以下載映像檔。

步驟 2. 透過執行下列指令，將 XClarity Administrator 容器映像檔匯入 Docker 主機。
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

步驟 3. 編輯 `docker_compose.env` 檔案，並更新下列環境變數。

- **CONTAINER_NAME**。唯一的容器名稱，用於為每個 XClarity Administrator 實例建立 Docker 磁區（例如，`CONTAINER_NAME=LXCA-203`）
- **ADDRESS**。容器的靜態 IPv4 位址（例如，`ADDRESS=192.0.2.0`）
- **BACKUP_MOUNT**。（選用）可用於儲存 XClarity Administrator 備份的遠端共用路徑。這必須是 `/mnt/backup_share`。
- **FIRMWARE_MOUNT**。（選用）可用來做為韌體更新遠端儲存庫的遠端共用路徑。這必須是 `/mnt/fw_share`。

以下是環境檔案的範例。

```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

步驟 4. 編輯 `docker_compose.yml`，並更新以下內容。

- 將 **image** 內容設定為步驟 2 中使用的安裝映像檔的名稱。

  **附註：**您可以使用 `docker tag` 指令變更映像檔名稱（例如，變更為「latest」）。
- 如果要使用遠端共用做為遠端韌體儲存庫並儲存 XClarity Administrator 備份，請在 **volumes** 內容中為每個遠端共用設定主機裝載點。
- 將 **dns** 內容設定為 DNS 伺服器的 IP 位址。
- 容器共用主機可用的處理器和記憶體資源儲存區。（選用）透過設定 **cpus** 和 **memory** 內容，定義資源使用限制。
- 將 **parent** 內容設定為主機系統上的網路介面名稱，以用來做為容器中 macvlan 介面的父介面。此介面必須可以直接存取指派給容器的子網路。
- 根據您的網路拓撲設定 **subnet** 和 **gateway**。通常，子網路和閘道用於 ${ADDRESS} 所屬的管理網路。
- 如果要支援 IPv6，請將 **enable_ipv6** 內容設定為 true，將 **ipv6_address** 內容設定為 IPv6 位址，並根據您的網路拓撲新增另一組 **subnet** 和 **gateway** 內容（通常是該 IPv6 位址所屬的管理網路）。

下面是啟用了 IPv6 的 YML 檔案範例。

```
version: '3.8'

services:

 lxca:
  image: lenovo/lxca:4.1.0-124
  container_name: ${CONTAINER_NAME}
  tty: true
  stop_grace_period: 60s
  volumes:
   #bind mount example
   - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
   - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
   #docker volume mount
   - data:/opt/lenovo/lxca/data
   - postgresql:/var/lib/postgresql
   - log:/var/log
   - confluent-etc:/etc/confluent
   - confluent-log:/var/log/confluent
   - confluent:/var/lib/confluent
   - propconf:/opt/lenovo/lxca/bin/conf
```

```
    - ssh:/etc/ssh
    - xcat:/etc/xcat
  networks:
   lan:
    ipv4_address: ${ADDRESS}
    ipv6_address: "2001:8003:7d51:2003::2"
  dns:
    - 192.0.2.10
    - 192.0.2.11
  deploy:
   resources:
    limits:
     cpus: "2.0"
     memory: "8g"

volumes:
 data:
  name: ${CONTAINER_NAME}-data
 postgresql:
  name: ${CONTAINER_NAME}-postgresql
 log:
  name: ${CONTAINER_NAME}-log
 confluent-etc:
  name: ${CONTAINER_NAME}-confluent-etc
 confluent-log:
  name: ${CONTAINER_NAME}-confluent-log
 confluent:
  name: ${CONTAINER_NAME}-confluent
 propconf:
  name: ${CONTAINER_NAME}-propconf
 ssh:
  name: ${CONTAINER_NAME}-ssh
 xcat:
  name: ${CONTAINER_NAME}-xcat

networks:
 lan:
  name: lan
  driver: macvlan
  enable_ipv6: true
  driver_opts:
   parent: eth0
  ipam:
   config:
    - subnet: 192.0.0.0/19
      gateway: 192.0.30.1
    - subnet: "2001:8003:7d51:2000::/80"
      gateway: "2001:8003:7d51:2000::1"
```

步驟 5. 透過執行下列指令在 Docker 中部署映像檔，其中 *<ENV_FILENAME>* 是您在步驟 2 中建立的環境變數檔案的名稱。

```
COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d
```

## 在您完成之後

登入並配置 XClarity Administrator（請參閱初次存取 Lenovo XClarity Administrator Web 介面和配置 Lenovo XClarity Administrator）。

## 實作高可用性

您可以使用 Docker Datacenter 為 Docker Engine 中執行的 Lenovo XClarity Administrator 容器設定高可用性環境。

如需 Docker Datacenter 高可用性的相關資訊，請參閱 使用 Docker Datacenter 實現高可用性架構和應用程式 網頁。

# 第 4 章　配置 Lenovo XClarity Administrator

當您初次存取 Lenovo XClarity Administrator，必須完成幾個步驟以起始設定XClarity Administrator。

**進一步瞭解：** XClarity Administrator：初次 配置

## 程序

完成下列步驟，以初次設定 XClarity Administrator。

步驟 1. 存取 XClarity Administrator Web 介面。

步驟 2. 閱讀並接受授權合約。

步驟 3. 建立具備監督者權限的使用者帳戶。

**要訣：**如有需要，請考量建立至少兩個具有監督者權限的使用者帳戶，以便備份。

步驟 4. 配置網路存取，包括資料和管理網路的 IP 位址。

步驟 5. 配置日期和時間。

步驟 6. 配置服務與支援設定，包括隱私權聲明、用量和硬體資料、Lenovo 支援中心 (Call Home)、Lenovo 上傳設備和產品保固。

步驟 7. 配置安全性設定，包括鑑別伺服器、使用者群組、伺服器憑證和加密法模式。

步驟 8. 管理機箱、伺服器、交換器和儲存裝置。

## 初次存取 Lenovo XClarity Administrator Web 介面

您可以從能網路連線虛擬機器 XClarity Administrator 的任何電腦啟動 XClarity Administrator Web 介面。

### 開始之前

確定您使用的是下列其中一個支援的 Web 瀏覽器：

- Chrome™ 48.0 或更新版本（對於遠端主控台，則需要 55.0 或更高版本）
- Firefox® ESR 38.6.0 或更新版本
- Microsoft® Internet Explorer® 11
- Microsoft Edge
- Safari® 9.0.2 或更新版本（IOS7 或更新版本和 OS X）

**附註：**不支援使用 Safari Web 瀏覽器從 XClarity Administrator 啟動管理控制器介面。

確定您用來登入 XClarity Administrator Web 介面的系統有網路連線可連線到 XClarity Administrator 管理節點。

### 程序

完成下列步驟以初次存取 XClarity Administrator Web 介面。

步驟 1. 將瀏覽器指向 XClarity Administrator 的 IP 位址。

© Copyright Lenovo 2022

**要訣：**存取 Web 介面時是透過安全連線完成。請確定使用 **https**。

- **若是容器**，請使用為 ${ADDRESS} 變數指定的 IPv4 位址，以使用下列 URL 存取 XClarity Administrator：
  `https://<IPv4_address>/ui/login.html`

  例如：
  `https://192.0.2.10/ui/login.html`

- **若是虛擬裝置**，您使用的 IP 位址取決於您的環境設定。

  如果您的 Eth0 及 Eth1 網路位於不同子網路，而且兩個子網路都使用 DHCP，則在存取用於起始設定的 Web 介面時，請使用 *Eth1* IP 位址。初次啟動 XClarity Administrator 時，Eth0 和 Eth1 都會取得由 DHCP 指派的 IP 位址，而且 XClarity Administrator 預設閘道設定為 *Eth1* 的 DHCP 指派閘道。

  **使用靜態 IPv4 位址**

  如果您在 eth0_config 中指定了 IPv4 位址，請利用下列 URL，使用該 IPv4 位址存取 XClarity Administrator：
  `https://<IPv4_address>/ui/login.html`

  例如：
  `https://192.0.2.10/ui/login.html`

  **使用相同廣播網域中的 DHCP 伺服器作為 XClarity Administrator**

  如果將 DHCP 伺服器與 XClarity Administrator 設定在相同廣播網域中，請利用下列 URL，使用 XClarity Administrator 虛擬機器主控台中顯示的 IPv4 位址存取 XClarity Administrator：
  `https://<IPv4_address>/ui/login.html`

  例如：
  `https://192.0.2.10/ui/login.html`

  **使用不同廣播網域中的 DHCP 伺服器作為 XClarity Administrator**

  如果 DHCP 伺服器*不是*設定在相同廣播網域，請使用 XClarity Administrator 虛擬機器主控台中針對 eEth0（管理網路）顯示的 IPv6 鏈結本端位址 (LLA) 存取 XClarity Administrator，例如：

```
---------------
Lenovo XClarity Administrator  Version x.x.x
---------------

eth0  flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
     inet 192.0.2.10  netmask 255.255.255.0  broadcast 192.0.2.55
     inet6 2001:db8:56ff:fe80:bea3  prefixlen 64  scopeid 0x20<link>
     ether 00:15:5d:0c:d1:92   txqueuelen 1000 (Ethernet)
     RX errors 0  dropped 0  overruns 0  frame 0

eth1  flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
     inet 192.0.2.20  netmask 255.255.255.0  broadcast 192.0.2.130
     inet6 2001:db8:56ff:fe80:bea3  prefixlen 64  scopeid 0x20<link>

==============================================================================
==============================================================================

You have 150 seconds to change IP settings. Enter one of the following:
 1. To set a static IP address for Lenovo XClarity virtual appliance eth0 port
 2. To use a DHCP address for Lenovo XClarity virtual appliance eth0 port
 x. To continue without changing IP settings
 ... ...
```

  **要訣：**IPv6 鏈結本端位址 (LLA) 衍生自介面的 MAC 位址。

  **注意：**如果從遠端配置 XClarity Administrator，您必須連線到同一個 Layer 2 網路。未完成起始設定之前，都必須從非路由位址存取它。因此，請考慮從具有 XClarity Administrator

連線的其他虛擬機器存取 XClarity Administrator。例如，您可以從 XClarity Administrator 安裝主機上的其他虛擬機器存取 XClarity Administrator。

— **Firefox：**

若要從 Firefox 瀏覽器存取 XClarity Administrator Web 介面，請使用下列 URL 登入。請注意，輸入 IPv6 位址時必須使用方括號。

```
https://[<IPv6_LLA>/ui/login.html]
```

例如，根據先前顯示的 Eth0 範例，請在 Web 瀏覽器中輸入下列 URL：

```
https://[fe80:21a:64ff:fe12:3456]/ui/login.html
```

— **Internet Explorer：**

若要從 Internet Explorer 瀏覽器存取 XClarity Administrator Web 介面，請使用下列 URL 登入。請注意，輸入 IPv6 位址時必須使用方括號。

```
https://[<IPv6_LLA>%25<zone_index>]/ui/login.html
```

其中，*<zone_index>* 是從您啟動 Web 瀏覽器的電腦連線到管理網路的乙太網路配接卡 ID。如果您在 Windows 中使用瀏覽器，請使用 `ipconfig` 指令尋找區域索引，這個索引顯示在配接卡的**鏈結-本端 IPv6 位址**欄位中的百分比符號 (%) 之後。在下列範例中，區域索引是「30」。

```
PS C:> ipconfig
Windows IP Configuration

Ethernet adapter vEthernet (teamVirtualSwitch):

  Connection-specific DNS Suffix  . :
  Link-local IPv6 Address . . . . . : 2001:db8:56ff:fe80:bea3%30
  Autoconfiguration IPv4 Address. . : 192.0.2.30
  Default Gateway . . . . . . . . . :
```

如果您在 Linux 中使用瀏覽器，請使用 `ifconfig` 指令來尋找區域索引。您也可以使用配接卡的名稱（通常是 Eth0）做為區域索引。

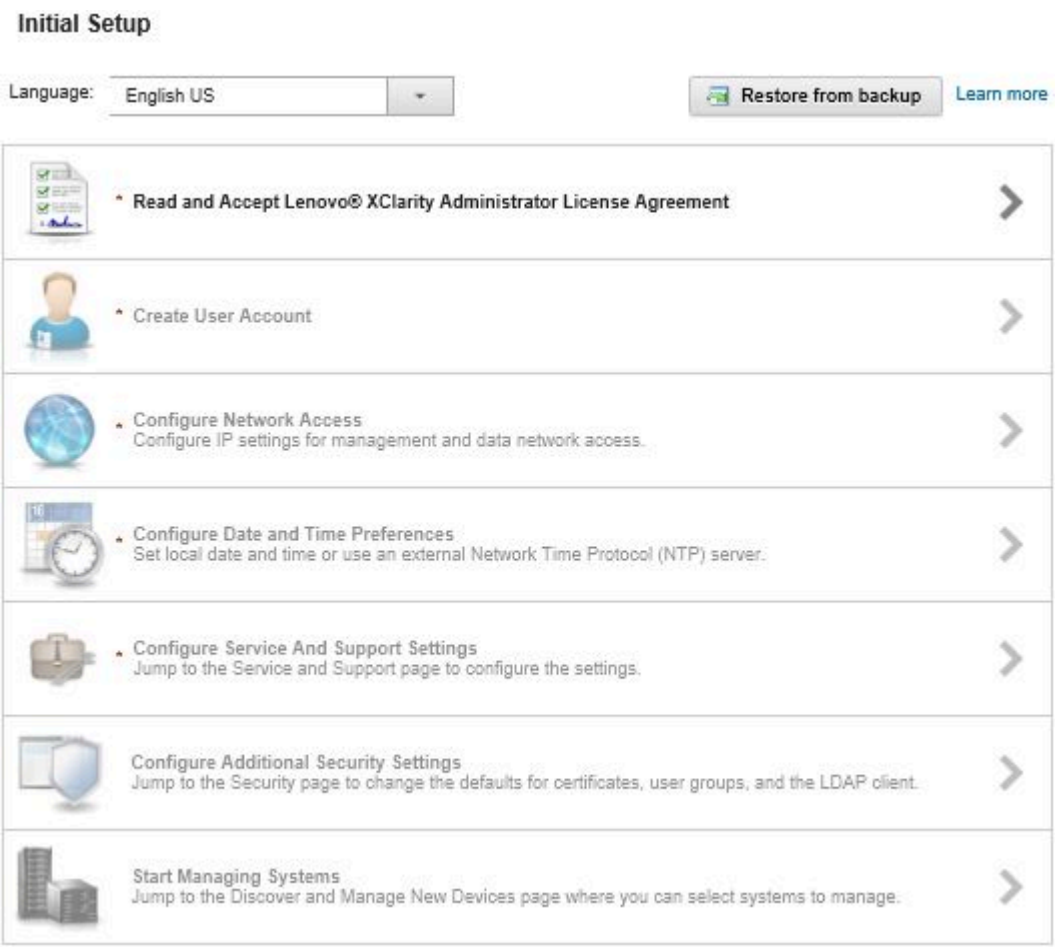
例如，根據顯示的 Eth0 和區域索引範例，請在 Web 瀏覽器中輸入下列 URL：

```
https://[2001:db8:56ff:fe80:bea3%2530]/ui/login.html
```

步驟 2. 您在初次存取 Lenovo XClarity Administrator 時，可能會收到安全性或憑證警告。您可以忽略這個警告。

## 結果

畫面上會顯示起始設定頁面。




### 在您完成之後

完成起始設定步驟以配置 XClarity Administrator（請參閱配置 Lenovo XClarity Administrator）。

## 建立使用者帳戶

使用者帳戶用於管理授權並存取 Lenovo XClarity Administrator 以及使用受管理鑑別的裝置。

### 關於此作業

您建立的第一個使用者帳戶必須具有「監督者」角色，且必須啟動（啟用）。

為了增加安全性，請至少建立兩個具有**監督者**角色的使用者帳戶。請務必記下這些使用者帳戶的密碼，並將其儲存在安全的位置，以備您必須還原 Lenovo XClarity Administrator 時使用。

### 程序

若要建立使用者帳戶，請完成下列步驟。

步驟 1. 在「建立新的監督者使用者」對話框中，填寫下列資訊。

- 輸入使用者名稱和該使用者的說明。
- 輸入新密碼和確認新密碼。密碼規則取決於現行的帳戶安全性設定。
- 選取一個或多個角色群組，以授權使用者執行適當的作業。

如需角色群組以及如何建立自訂角色群組的相關資訊，請參閱 XClarity Administrator 線上文件中的建立角色群組。

- （選用）如果您要強制使用者在第一次登入 XClarity Administrator 時變更密碼，請將**第一次存取時變更密碼**設為 Yes。

步驟 2. 按一下**建立**。

步驟 3. 按一下**建立**圖示 ( )，然後重複先前的步驟，建立其他使用者。

步驟 4. 按一下**回到起始設定**。

## 配置網路存取

若要配置網路存取，您可以配置最多兩個網路介面、Lenovo XClarity Administrator 的主機名稱和要使用的 DNS 伺服器。

### 關於此作業

XClarity Administrator 有兩個單獨的網路介面可為您的環境定義，具體取決於您實作的網路拓撲。若是虛擬裝置，這些網路命名為 eth0 和 eth1。若是容器，您可以選擇自訂名稱。

- 只有一個網路介面 (eth0) 存在時：
  - 介面必須配置為可支援裝置探索和管理（例如伺服器配置和韌體更新）。它必須能與每一個受管理機箱中的 CMM 和 Flex 交換器、每一部受管理伺服器中的基板管理控制器，以及每個 RackSwitch 交換器進行通訊。
  - 如果您想要使用 XClarity Administrator 取得韌體和 OS 裝置驅動程式更新，至少一個網路介面必須連線至網際網路，最好是透過防火牆。否則，您必須將更新項目匯入儲存庫。
  - 如果您想要收集服務資料或使用自動問題通知（包括 Call Home 及 Lenovo 上傳設備），則至少一個網路介面必須連線至網際網路，最好是透過防火牆。
  - 如果您想要部署作業系統映像檔及更新 OS 裝置驅動程式，則介面必須具有可用於連接伺服器網路介面、存取主機作業系統的 IP 網路連線功能。

    **附註：**如果您實作另一網路進行 OS 部署及 OS 裝置驅動程式更新，可以將第二個網路介面配置為連線至該網路，而非資料網路。不過，如果各伺服器的作業系統無法存取資料網路，請在伺服器上配置其他介面，讓主機作業系統能夠連線至資料網路以進行 OS 部署及 OS 裝置驅動程式更新（如有需要）。
- 有兩個網路介面（eth0 和 eth1）存在時：
  - 第一個網路介面（通常是 Eth0 介面）必須連線至管理網路，並且配置為可支援裝置探索和管理（包括伺服器配置和韌體更新）。它必須能與每一個受管理機箱中的 CMM 和 Flex 交換器、每一部受管理伺服器中的管理控制器，以及每個 RackSwitch 交換器進行通訊。
  - 第二個網路介面（通常是 eth1 介面）可以配置為與內部資料網路、公用資料網路或兩者進行通訊。
  - 如果您想要使用 XClarity Administrator 取得韌體和 OS 裝置驅動程式更新，至少一個網路介面必須連線至網際網路，最好是透過防火牆。否則，您必須將更新項目匯入儲存庫。
  - 如果您想要收集服務資料或使用自動問題通知（包括 Call Home 及 Lenovo 上傳設備），則至少一個網路介面必須連線至網際網路，最好是透過防火牆。
  - 如果您想要部署作業系統映像檔及更新 OS 裝置驅動程式，可以選擇使用 eth1 或 eth0 介面。不過，您所使用的介面必須具有連接伺服器網路介面、存取主機作業系統的 IP 網路連線功能。

    **附註：**如果您實作另一網路進行 OS 部署及 OS 裝置驅動程式更新，可以將第二個網路介面配置為連線至該網路，而非資料網路。不過，如果各伺服器的作業系統無法存取資料網路，請在伺服器上配置其他介面，讓主機作業系統能夠連線至資料網路以進行 OS 部署及 OS 裝置驅動程式更新（如有需要）。

下表根據您環境中實作的網路拓蹼類型，顯示 XClarity Administrator 網路介面可能的配置。請使用此表判斷如何定義每個網路介面。

*表格 2. 根據網路拓撲的每個網路介面角色*

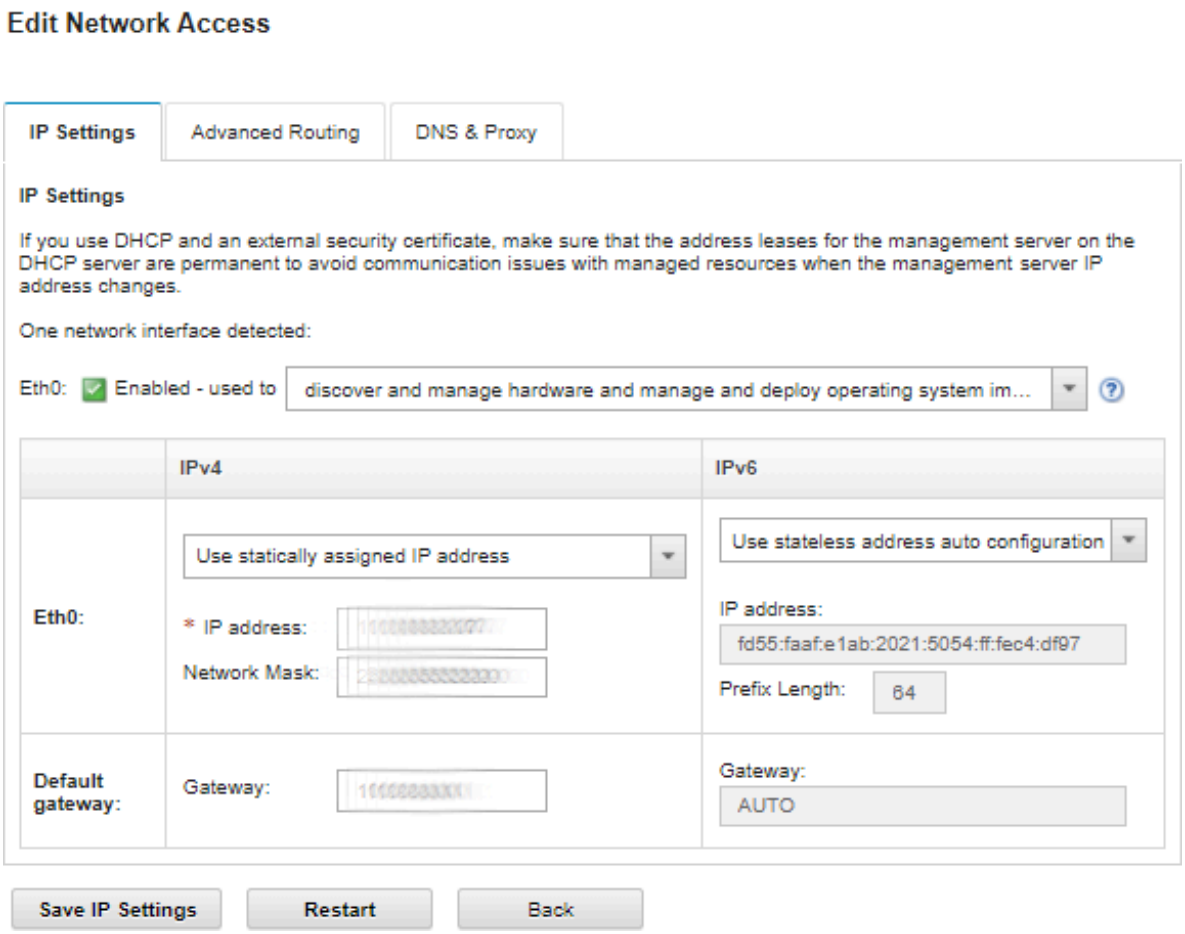
| 網路拓蹼 | 介面 1 (eth0) 的角色 | 介面 2 (eth1) 的角色 |
|---|---|---|
| 聚合網路（支援 OS 部署及 OS 裝置驅動程式更新的管理和資料網路） | 管理網路<br>• 探索和管理<br>• 伺服器配置<br>• 韌體更新<br>• 服務資料收集<br>• 自動問題通知（如 Call Home 及 Lenovo 更新設備）<br>• 保固資料擷取<br>• 作業系統部署<br>• OS 裝置驅動程式更新項目 | 無 |
| 單獨的管理網路支援 OS 部署及 OS 裝置驅動程式更新和資料網路 | 管理網路<br>• 探索和管理<br>• 伺服器配置<br>• 韌體更新<br>• 服務資料收集<br>• 自動問題通知（如 Call Home 及 Lenovo 更新設備）<br>• 保固資料擷取<br>• 作業系統部署<br>• OS 裝置驅動程式更新項目 | 資料網路<br>• 無 |
| 單獨的管理網路和支援 OS 部署及 OS 裝置驅動程式更新的資料網路 | 管理網路<br>• 探索和管理<br>• 伺服器配置<br>• 韌體更新<br>• 服務資料收集<br>• 自動問題通知（如 Call Home 及 Lenovo 更新設備）<br>• 保固資料擷取 | 資料網路<br>• 作業系統部署<br>• OS 裝置驅動程式更新項目 |
| 單獨的管理網路和未支援 OS 部署及 OS 裝置驅動程式更新的資料網路 | 管理網路<br>• 探索和管理<br>• 伺服器配置<br>• 韌體更新<br>• 服務資料收集<br>• 自動問題通知（如 Call Home 及 Lenovo 更新設備）<br>• 保固資料擷取 | 資料網路<br>• 無 |
| 僅管理網路（不支援 OS 部署及 OS 裝置驅動程式更新） | 管理網路<br>• 探索和管理<br>• 伺服器配置<br>• 韌體更新<br>• 服務資料收集<br>• 自動問題通知（如 Call Home 及 Lenovo 更新設備）<br>• 保固資料擷取 | 無 |

如需 XClarity Administrator 網路介面的相關資訊，請參閱 XClarity Administrator 線上文件中的網路考量。

## 程序

若要配置網路存取，請完成下列步驟。

步驟 1. 在起始設定頁面上按一下**配置網路存取**。畫面上會顯示編輯網路存取頁面。




步驟 2. 如果您想要使用 XClarity Administrator 部署作業系統和更新 OS 裝置驅動程式，請選擇要用於管理作業系統的網路介面。

- 如果只為 XClarity Administrator 定義一個介面，請選擇該介面是否僅用於探索及管理硬體，或者也要用來管理作業系統。
- 如果為 XClarity Administrator 定義了兩個介面（Eth0 和 Eth1），請決定使用哪一個介面來管理作業系統。如果您選擇「無」，則*無法*從 XClarity Administrator 在受管理伺服器上部署作業系統映像檔或更新 OS 裝置驅動程式。

步驟 3. 指定 IP 設定。

a. 針對第一個介面，指定 IPv4 位址、IPv6 位址或這兩個位址。

- **IPv4**。您必須指派 IPv4 位址給介面。您可以選擇使用靜態指派 IP 位址或從 DHCP 伺服器取得 IP 位址。
- **IPv6**。或者，您可以使用下列其中一種指派方法，將 IPv6 位址指派給介面：
  — 使用靜態指派的 IP 位址
  — 使用有狀態位址配置 (DHCPv6)
  — 使用無狀態位址自動配置

  **附註：**如需 IPv6 位址限制的相關資訊，請參閱 XClarity Administrator 線上文件中的 IP 配置限制。

b. 如果第二個介面可用，請指定 IPv4 位址、IPv6 位址或這兩種位址。

**附註：**指派給這個介面的 IP 位址必須與指派給第一個介面的 IP 位址分屬不同的子網路。如果您選擇使用 DHCP 來指派兩個介面（Eth0 和 Eth1）的 IP 位址，則 DHCP 伺服器必須為這兩個介面的 IP 位址指派不同的子網路。

- **IPv4**。您可以選擇使用靜態指派 IP 位址或從 DHCP 伺服器取得 IP 位址。
- **IPv6**。或者，您可以使用下列其中一種指派方法，將 IPv6 位址指派給介面：
  — 使用靜態指派的 IP 位址
  — 使用有狀態位址配置 (DHCPv6)
  — 使用無狀態位址自動配置

c. 指定預設閘道。

如果指定預設閘道，則必須為有效的 IP 位址，而且必須與其中一個網路介面（Eth0 或 Eth1）的 IP 位址使用相同的網路遮罩（相同的子網路）。如果使用單一介面，預設閘道則必須與網路介面在相同的子網路中。

如果其中一個介面使用 DHCP 取得 IP 位址，則預設閘道也會使用 DHCP。若要手動輸入預設閘道位址以置換從 DHCP 伺服器接收的位址，請選取**置換閘道**勾選框。

**要訣：**

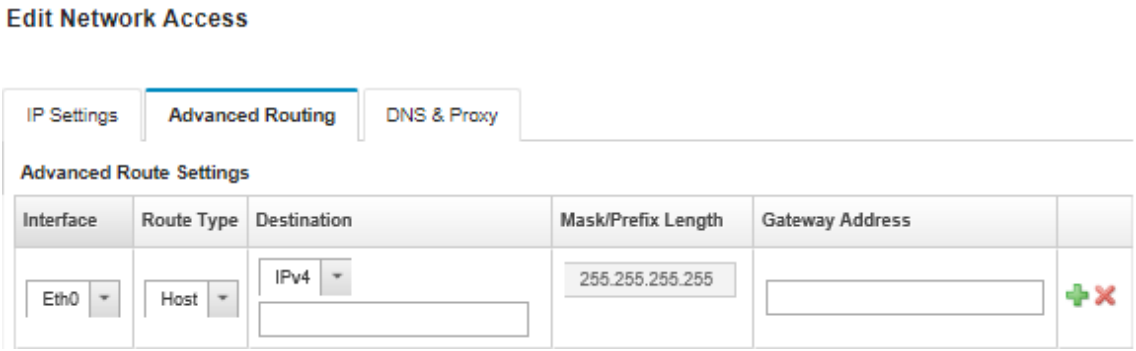
- 確保閘道符合其中一個網路介面的子網路。預設閘道是透過網路介面自動設定。
- 若要恢復成使用 DHCP 提供的閘道，請清除**置換閘道**勾選框。

**警告：**
**如果您選擇置換閘道，請注意輸入正確的閘道位址；否則，此管理伺服器將無法存取，而且無法遠端登入加以更正。**

d. 按一下**儲存 IP 設定**。

步驟 4. **選用：**配置進階設定。

a. 按一下**進階路由**標籤。



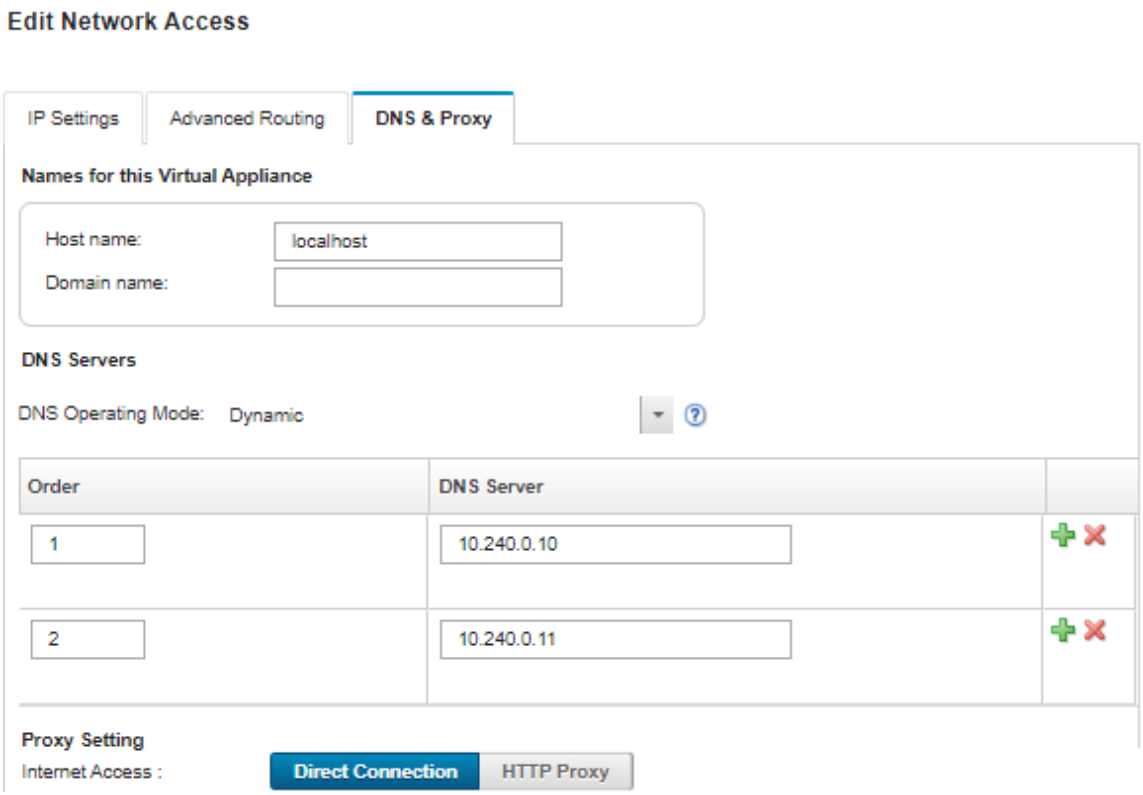

b. 在**進階路由設定**表中，指定這個介面要使用的一個或多個路由項目。

若要定義一個或多個路由項目，請完成下列步驟。
1. 選擇介面。
2. 指定可以到其他主機或網路的路由類型。
3. 指定要引導路由的目的地主機或網路位址。
4. 指定目的地位址的子網路遮罩。
5. 指定封包要定址的閘道位址。

c. 按一下**儲存進階路由**。

步驟 5. 選擇性地修改 DNS 和代理設定。

a. 按一下 **DNS 和代理**標籤。




b. 指定 XClarity Administrator 要使用的主機名稱及網域名稱。

c. 選取 DNS 作業模式。這可以是**靜態**或 **DHCP**。

**注意：**當您變更 DNS 作業模式時，必須重新啟動管理伺服器。

**附註：**如果選擇使用 DHCP 伺服器取得 IP 位址，則下次XClarity Administrator更新 DHCP 租賃時，會改寫在**DNS 伺服器**欄位所做的所有變更。

d. 指定要使用的一個或多個網域名稱系統 (DNS) 伺服器的 IP 位址，以及每個伺服器的優先順序。

e. 指定存取網際網路是透過直接連線還是透過 HTTP 代理（如果 XClarity Administrator 可以存取網際網路）。

**附註：**如果透過 HTTP 代理，請確定滿足下列需求。
- 請確認代理伺服器設定為使用基本鑑別。
- 請確認 Proxy 伺服器設定為非終止的代理伺服器。
- 請確認代理伺服器設定為轉遞代理。
- 確認已配置負載平衡器維持與 Proxy 伺服器的階段作業，而不在其間切換。

如果選擇使用 HTTP Proxy，請完成必要欄位：
1. 指定 Proxy 伺服器的主機名稱及埠。
2. 選擇是否使用鑑別，並指定使用者名稱及密碼（如有需要）。
3. 指定 Proxy 測試 URL。
4. 按一下**文字 Proxy**，驗證已配置 Proxy 設定而且運作正常。

f. 按一下**儲存 DNS 和代理**。

g. 將 XClarity Administrator 管理伺服器完整網域名稱 (FQDN) 和 DNS 資訊推送至配備 IMM2、XCC、XCC2 和 XCC3 的受管理伺服器，以便受管理伺服器可以使用這些資訊找到管理伺服器。

1. 按一下**將 FQDN/DNS 推送至 BMC**。
2. 選擇如何處理基板管理控制器中的現有 DNS 項目。
   - 保留現有的 DNS 項目，並將管理伺服器 DNS 項目附加到下一個可用槽位中。

- 將所有現有 DNS 項目取代為管理伺服器 DNS 項目。

3. 在編輯欄位中輸入**是**。
4. 按一下**套用**。

建立一項工作以執行此作業。您可以從**監視 → 工作**卡片監視工作的進度。如果工作未成功完成，請按一下工作連結以顯示工作的詳細資料 (請參閱 XClarity Administrator 線上文件的 使用工作)。

您也可以從配備 IMM2、XCC、XCC2 和 XCC3 的受管理伺服器中移除管理伺服器 FQDN 和 DNS 資訊，方法是按一下**從 BMC 移除 FQDN/DNS**。您可以選擇保留其他現有 DNS 項目、移除所有 DNS 項目，或僅移除與管理伺服器資訊相符的項目。

步驟 6. 按一下**上一步**。

步驟 7. 按一下**測試連線**以驗證網路設定。

## 正在配置日期和時間

雖然可以手動設定 Lenovo XClarity Administrator 的日期和時間，但是更好的方法是設定網路時間協定 (NTP) 伺服器，用來同步 XClarity Administrator 和所有受管理裝置之間的時間戳記。

### 開始之前

您必須使用至少一個（最多四個）網路時間通訊協定 (NTP) 伺服器，將從受管理裝置收到的所有事件的時間戳記同步到 XClarity Administrator。

**要訣：**務必能夠透過管理網路（通常是 Eth0 介面）存取 NTP 伺服器。請考量在執行 XClarity Administrator 的主機上設定 NTP 伺服器。

如果變更 NTP 伺服器上的時間，XClarity Administrator 可能需要一些時間才能與新的時間同步。

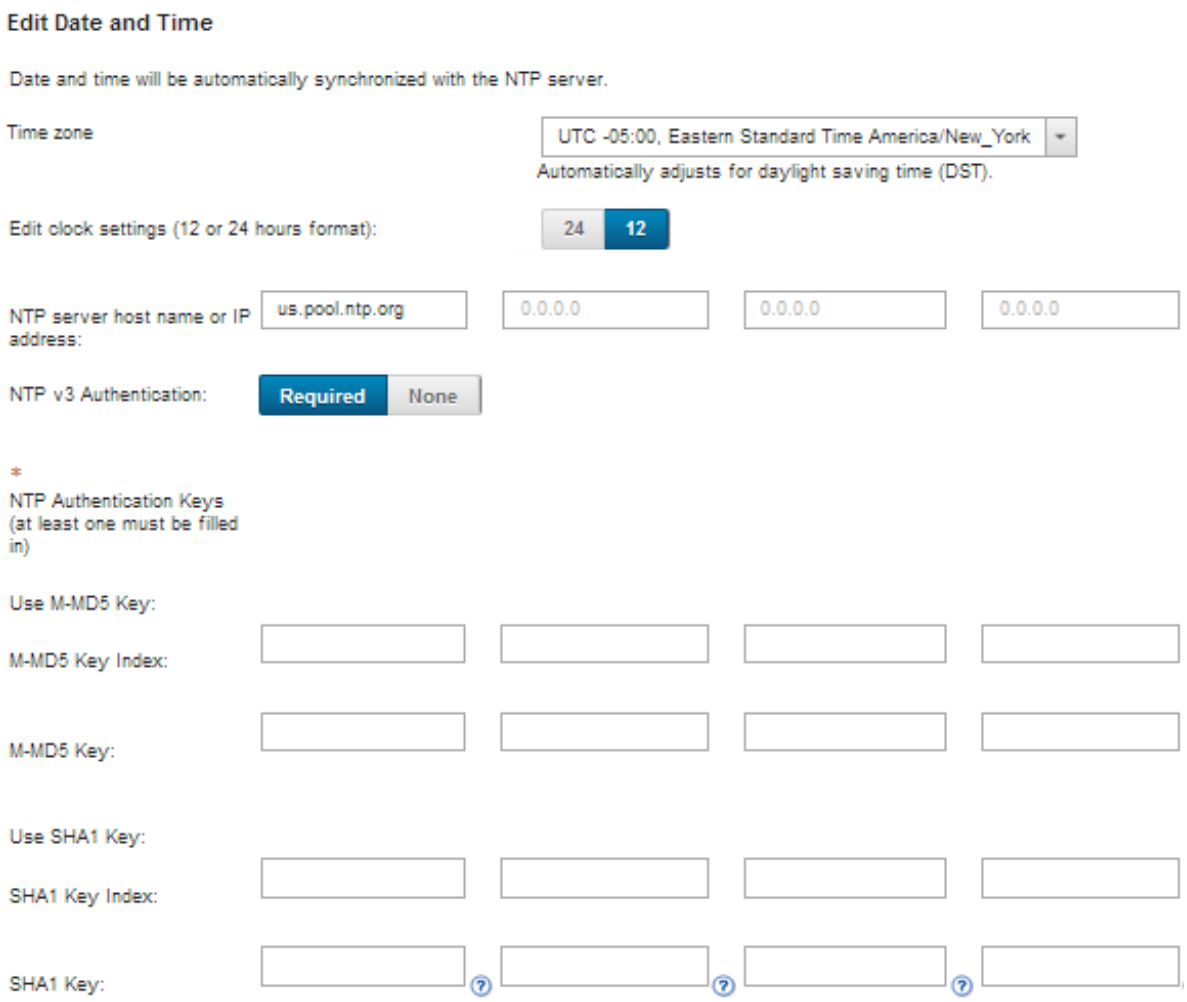
**注意：**XClarity Administrator 虛擬裝置和其主機必須設為同步至相同時間來源，避免 XClarity Administrator 與其主機之間意外發生時間不同步。通常主機已配置為與其虛擬裝置的時間同步。如果 XClarity Administrator 設定為與其主機不同的來源同步，您必須停用 XClarity Administrator 虛擬裝置和其主機之間的主機時間同步。

- 針對 ESXi，請依照VMware — 停用時間同步網頁上的指示進行。
- 針對 Hyper-V，在 Hyper-V 管理員中用滑鼠右鍵按一下 XClarity Administrator 虛擬機器，然後按一下**設定**。在對話框中，按一下導覽窗格中的**管理 > 整合服務**，然後清除**時間同步**。

### 程序

如要為 XClarity Administrator 設定 NTP 伺服器，請完成下列步驟。

步驟 1. 在「起始設定」頁面上按一下**配置日期和時間喜好設定**。畫面上會顯示編輯日期和時間頁面。




步驟 2. 填寫「日期和時間」對話框。

1. 選擇 XClarity Administrator 的主機所在的時區。

   如果所選取的時區遵循日光節約時間 (DST)，則會自動為 DST 調整時間。

2. 選擇使用 12 小時或 24 小時制。
3. 指定網路中每個 NTP 伺服器的主機名稱或 IP 位址。您最多可以定義四個 NTP 伺服器。
4. 選取**必要**在 XClarity Administrator 和您網路中的 NTP 伺服器之間啟用 NTP v3 鑑別，或選取**無**使用 NTP v1 鑑別。

   如果受管理的 Flex System CMM 和基板管理控制器的韌體需要 v3 鑑別，且 XClarity Administrator 與您網路中一個或多個 NTP 伺服器之間需要 NTP v3 鑑別，您可以使用 v3 鑑別

5. 如果啟用 NTP v3 鑑別，請設定每個適用的 NTP 伺服器的鑑別金鑰和索引。您可以指定 M-MD5 金鑰、SHA1 金鑰或兩者。若有指定 M-MD5 和 SHA1 兩種金鑰，XClarity Administrator 會將 M-MD5 或 SHA1 金鑰推送至支援該金鑰的受管理 Flex System CMM 和管理控制器。XClarity Administrator 會使用該金鑰向 NTP 伺服器進行鑑別
   - 為 M-MD5 金鑰指定僅包含大小寫字母（a-z、A-Z）、數字 (0-9) 和下列特殊字元的 ASCII 字串：@#。
   - 為 SHA1 金鑰指定一個 40 字元的 ASCII 字串，只能包含 0-9 和 a-f。
   - 指定的金鑰索引和鑑別金鑰必須符合 NTP 伺服器上設定的金鑰 ID 及密碼值。例如，若輸入的 SHA1 金鑰其金鑰索引在 NTP 伺服器上為 5，則 XClarity Administrator SHA1 金鑰所指定的金鑰索引也必須是 5。如需設定金鑰 ID 及密碼的相關資訊，請參閱 NTP 伺服器的文件。

- 即使兩個或多個 NTP 伺服器皆使用相同的金鑰，您仍然必須為使用 v3 鑑別的每個 NTP 伺服器指定金鑰。
- 如果您啟用 v3 鑑別，但不為 NTP 伺服器提供鑑別金鑰和索引，依預設會使用 v1 鑑別。
- 如果您指定多個 NTP 伺服器，NTP 伺服器必須全部採用 v3 鑑別或全部採用 v1 鑑別。不支援混用 v3 鑑別和 v1 鑑別的 NTP 伺服器。
- 如果您指定了多個採用 v3 鑑別的 NTP 伺服器，但金鑰不相同，金鑰索引必須是唯一的。例如，如果 NTP 伺服器 1 和 2 中的 SHA1 金鑰不同，NTP 伺服器 1 和 2 就不能具有 1 的 SHA1 金鑰索引。您必須重新配置其中一個 NTP 伺服器，才能接受其金鑰索引與另一個 NTP 伺服器不同的金鑰；否則，將會為所有具有相同金鑰索引的 NTP 伺服器配置與金鑰索引相關聯的最後一個定義的金鑰。

步驟 3. 按一下**儲存**。

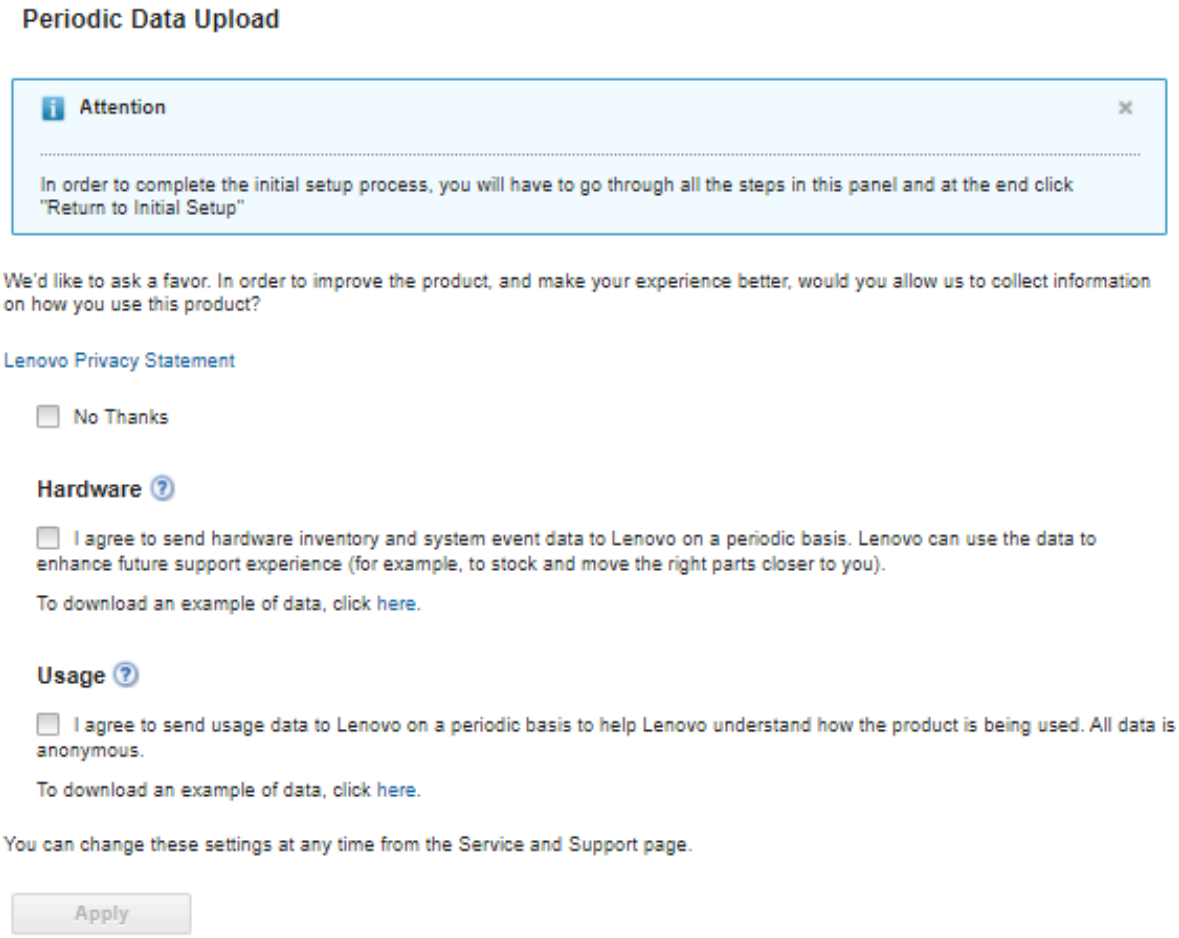
## 配置服務和支援

您可以配置服務與支援設定，包括用量資料、Lenovo 支援中心 (Call Home)、Lenovo 上傳設備和產品保固。

### 程序

完成下列步驟以配置安全性。

步驟 1. 在「起始設定」頁面上按一下**配置服務與支援設定**。畫面上會顯示服務與支援頁面。




步驟 2. 閱讀並接受 Lenovo 隱私權聲明。

**附註：**如果沒有先接受 Lenovo 隱私權聲明，就不能收集資料並傳送至 Lenovo。如果您選擇拒絕隱私權聲明，日後可以從**服務與支援 → Call Home 配置**頁面檢閱並接受隱私權聲明。

步驟 3. 選擇性地選擇允許 Lenovo XClarity Administrator 收集使用情形和硬體資訊，然後按一下**套用**。

您可以收集下列類型的資料並傳送至 Lenovo。

- **使用資料**

  當您同意將使用資料傳送到 Lenovo 後，系統將每週收集並傳送下列資料。此資料*匿名*。不會收集或向 Lenovo 傳送私人資料（包括序號、UUID、主機名稱、IP 位址和使用者名稱）。
  — 已執行之動作的日誌
  — 引發的事件的清單，以及引發時的時間戳記
  — 引發的審核事件的清單，以及引發時的時間戳記
  — 已執行之工作的清單，以及每個工作的成功/失敗資訊
  — XClarity Administrator 計量，包括記憶體用量、處理器使用情形和磁碟空間
  — 所有受管理裝置的有限庫存資料

- **硬體資料**

  當您同意將硬體資料傳送到 Lenovo 後，系統將定期收集並傳送下列資料。此資料*不匿名*。硬體資料包括屬性，例如 UUID 和序號。不包括 IP 位址或主機名稱。

  — **每日硬體資料**。包含每次庫存變更的下列資料。
    — 庫存變更事件 (FQXHMDM0001I)
    — 與該事件相關聯的裝置庫存資料變更

  — **每週硬體資料**。包含所有受管理裝置的庫存資料。

當使用情形和硬體資料傳送至 Lenovo 時，系統會在審核日誌中記錄一個事件。

您可以隨時變更此設定，並使用鏈結下載最近收集並傳送到 Lenovo 的保存檔，方法是按一下**管理 → 服務與支援**，然後按一下**定期資料上傳**標籤。

步驟 4. 選擇性地按一下 **Call Home 配置**，設定自動將問題通知傳送至 Lenovo 支援中心 (Call Home)。接著，按一下**套用並啟用**，建立預設的 Call Home 服務轉遞器，或按一下**僅套用**，儲存聯絡資訊。

如需設定自動將問題通知傳送至 Lenovo 支援中心的相關資訊，請參閱 XClarity Administrator 線上文件中的設定 Call Home。

步驟 5. 選擇性地按一下 **Lenovo 上傳設備**，設定自動將問題通知傳送至 Lenovo 上傳設備。接著，按一下**套用並啟用**，建立預設的 Lenovo 上傳設備服務轉遞器，或按一下**僅套用**，儲存設定資訊。

如需設定自動將問題通知傳送至 Lenovo 上傳設備的相關資訊，請參閱 XClarity Administrator 線上文件中的設定自動將問題通知傳送至 Lenovo 上傳設備。

步驟 6. 選擇性地按一下**保固**，啟用收集受管理裝置保固資訊的外部連線。

如需檢視受管理裝置保固狀態（包括延長保固）的相關資訊，請參閱 XClarity Administrator 線上文件中的檢視保固資訊。

步驟 7. （選擇性）按一下 **Lenovo 公告服務**以允許 Lenovo 傳送服務公告至 XClarity Administrator，然後按一下**套用**

如需 Lenovo 傳送的服務公告類型相關資訊，請參閱 XClarity Administrator 線上文件的 從 Lenovo 取得公告。

步驟 8. 指定若 XClarity Administrator 沒有回應且無法回復時，可以用於收集並下載服務資料及日誌的服務回復密碼。

如需服務回復密碼的相關資訊，請參閱 XClarity Administrator 線上文件中的變更服務回復密碼。

步驟 9. 按一下**回到起始設定**。

## 配置安全

您可以配置安全性，包括角色群組、鑑別伺服器、使用者帳戶安全性設定、加密法和憑證。

### 程序

完成下列步驟以配置安全性。

步驟 1. 在「起始設定」頁面上按一下**配置其他安全性設定**。畫面上會顯示安全性頁面。

步驟 2. 建立自訂的角色群組，以管理授權和資源存取權（請參閱 XClarity Administrator 線上文件中的建立角色群組）。

*角色群組*則是一個或多個角色的集合，用於將這些角色指派給多個使用者。您為角色群組配置的角色會決定授與該角色群組所屬成員之每個使用者的存取層次。每個 XClarity Administrator 使用者都必須是至少一個角色群組的成員。

步驟 3. 配置鑑別伺服器（請參閱 XClarity Administrator 線上文件中的管理鑑別伺服器）。

*鑑別伺服器*是用來鑑別使用者認證的Microsoft Active Directory (LDAP) 伺服器。XClarity Administrator 使用單一鑑別伺服器，進行所有受管理裝置（Flex 交換器除外）的集中式使用者管理。當某個裝置受 XClarity Administrator 管理，則受管理的裝置及其已安裝的元件（Flex 交換器除外）會配置為使用 XClarity Administrator 鑑別伺服器。使用鑑別伺服器中定義的使用者帳戶登入 XClarity Administrator、CMM 和基板管理控制器。

您可以選擇使用外部鑑別伺服器，而不使用管理節點上的本端鑑別伺服器。

步驟 4. 配置使用者帳戶安全性設定，以控制密碼複雜性、帳戶鎖定與 Web 階段作業閒置逾時（請參閱 XClarity Administrator 線上文件中的變更使用者帳戶安全性設定）。

步驟 5. 配置加密法設定，定義控制 XClarity Administrator 和受管理裝置之間處理安全通訊方式的通訊模式和通訊協定（請參閱 XClarity Administrator 線上文件中的設定加密法模式和通訊 協定）

步驟 6. 如果您打算使用本端鑑別（而非 XClarity Administrator 受管理鑑別）管理機架式伺服器，請在裝置上或 Active Directory 中，建立一個或多個可與管理程序中登入裝置所使用的作用中使用者帳戶相對應的儲存認證。如需已儲存認證的相關資訊，請參閱 XClarity Administrator 線上文件中的管理儲存的認證。

步驟 7. 如果您計劃使用包含本身資訊的自訂伺服器憑證或使用外部簽署憑證，請先產生並部署新憑證，再開始管理系統。如需產生您專屬安全憑證的相關資訊，請參閱 XClarity Administrator 線上文件中的使用安全憑證。

步驟 8. 在「安全性」頁面的垂直功能表上，請按一下**回到起始設定**。

## 管理裝置

Lenovo XClarity Administrator 可以管理數種類型的系統，包括 Flex System 機箱、機架式和直立式伺服器、RackSwitch 交換器及儲存裝置。您可以使用大量匯入檔案，透過匯入裝置相關資訊的方式，輕鬆探索和管理您環境中的大量裝置。

### 開始之前

**重要事項：**

- 您可以一次管理或解除管理最多 300 個裝置。大量匯入檔案中包含的裝置不得超過 300 個。
- 起始裝置管理或解除管理作業後，請等待整個管理工作完成後再起始另一個裝置管理作業。

在管理包含機箱元件的機箱時，會自動探索及管理機箱元件（例如 CMM、計算節點、交換器和儲存裝置）。您無法探索及管理脫離機箱的機箱元件。

某些埠必須開放使用，才能與機箱中的 CMM 及伺服器中的基板管理控制器進行通訊。在您嘗試管理系統前，請確定能使用這些埠。如需埠的相關資訊，請參閱 XClarity Administrator 線上文件中的埠可用性。

確定您要使用 XClarity Administrator 管理的每個系統上都已安裝最低需求韌體。您可以從 XClarity Administrator 支援 — 相容性 網頁找到最低所需韌體版本，方法是按一下 **Compatibility（相容性）**標籤，然後按一下適當裝置類型的鏈結。

確定與 CMM 的頻外通訊至少有三個 TCP 指令模式的階段作業設定。如需設定階段作業數的相關資訊，請參閱CMM 線上文件中的「tcpcmdmode 指令」。

請考慮為 XClarity Administrator 管理的所有 CMM 和 Flex 交換器實作 IPv4 *或* IPv6 位址。如果部分 CMM 和 Flex 交換器實作 IPv4，而其他實作 IPv6，則可能在審核日誌（或是審核設陷）中無法收到部份事件。

請確定已啟用機架頂端交換器的多重播送 SLP 轉遞，以及環境中的路由器。請參閱隨特定交換器或路由器提供的文件，以判斷是否已啟用多重播送 SLP 轉遞；如果已停用，則找出啟用的程序。

**重要事項：**

- 根據 RackSwitch 交換器的韌體版本而定，您可能需要在每一個 RackSwitch 交換器上手動使用下列指令啟用多重播送 SLP 轉遞和 SSH，如此 XClarity Administrator 才能探索到交換器並進行管理。如需相關資訊，請參閱System x 中的機架交換器線上文件。
- 每個儲存裝置都必須啟用多重播送 SLP 轉遞，XClarity Administrator 才能探索到該裝置。
- 如果您計劃使用包含本身資訊的自訂伺服器憑證或使用外部簽署憑證，請先產生並部署新憑證，再開始管理系統。如需產生您專屬安全憑證的相關資訊，請參閱 XClarity Administrator 線上文件中的使用安全憑證。
- 除了 Lenovo XClarity Administrator 之外，如果您要使用其他管理軟體監視機箱，而且該管理軟體使用 SNMPv3 通訊，您必須先建立配置適當 SNMPv3 資訊的本端 CMM 使用者 ID，然後以該使用者 ID 登入 CMM 並變更密碼。如需相關資訊，請參閱XClarity Administrator 線上文件中的管理考量。
- 服務探索通訊協定（例如 SLP 和 SSDP）會啟用 XClarity Administrator 自動探索即將接受管理之裝置的類型，然後使用適當的機制管理裝置。某些裝置類型不支援服務探索通訊協定，而且在某些環境中會故意關閉服務探索通訊協定。無論哪種情況，您都必須選擇適當的裝置類型來完成管理程序。必須明確指出以下裝置類型。
  — Lenovo ThinkSystem DB 系列交換器
  — NVIDIA Mellanox 交換器

## 關於此作業

XClarity Administrator 可透過探測與 XClarity Administrator 位於相同 IP 子網路上的可管理裝置、使用指定的 IP 位址或 IP 位址範圍，或是從試算表匯入資訊的方式，探索您環境中可管理的系統。

依預設，系統會使用 XClarity Administrator 受管理鑑別登入裝置來管理裝置。管理機架式伺服器和 Lenovo 機箱時，您可以選擇使用本端鑑別或受管理鑑別登入裝置。

- 當*本端鑑別*用於機架式伺服器、Lenovo 機箱和 Lenovo 機架式交換器時，XClarity Administrator 會使用已儲存認證向裝置進行鑑別。*已儲存認證*可以是裝置上的作用中使用者帳戶，或是 Active Directory 伺服器中的使用者帳戶。

  使用本端鑑別管理裝置之前，您應先在 XClarity Administrator 建立已儲存認證，其必須與裝置上的作用中使用者帳戶或 Active Directory 伺服器中的使用者帳戶相符（請參閱 XClarity Administrator 線上文件中的管理儲存的認證）。

  **附註：**

  — 裝置的本端鑑別啟用時，您無法使用 XClarity Administrator 編輯該裝置的已儲存認證。

  — RackSwitch 裝置僅支援已儲存認證進行鑑別，不支援 XClarity Administrator 使用者認證。

- 使用*受管理鑑別*讓您能夠利用 XClarity Administrator 鑑別伺服器中的認證來管理及監視多個裝置，而不使用本端認證。當受管理鑑別用於裝置（非 ThinkServer 伺服器、System x M4 伺服器和交換器）時，XClarity Administrator 會配置裝置及其所安裝的元件，以使用 XClarity Administrator 鑑別伺服器進行集中管理。
  - 啟用受管理鑑別時，您可以使用手動輸入或已儲存認證來管理裝置（請參閱 管理使用者帳戶 以及 XClarity Administrator 線上文件中的管理儲存的認證）。要等到 XClarity Administrator 配置了裝置的 LDAP 設定後才會使用已儲存認證。之後，已儲存認證的任何變更都不會影響對該裝置的管理或監視。
  - 如果使用本端或外部 LDAP 伺服器做為 XClarity Administrator 鑑別伺服器，則會使用鑑別伺服器中定義的使用者帳戶登入 XClarity Administrator、CMM 和 XClarity Administrator 網域內的基板管理控制器。已停用本端 CMM 和管理控制器使用者帳戶。

    **附註：**對於 Think Edge SE450、SE350 V2 和 SE360 V2 伺服器，預設本端使用者帳戶保持啟用，所有其他本端帳戶均為停用。
  - 如果使用 SAML 2.0 識別提供者做為 XClarity Administrator 鑑別伺服器，受管理裝置將無法存取 SAML 帳戶。不過，當同時使用 SAML 識別提供者和 LDAP 伺服器時，如果識別提供者使用存在於 LDAP 伺服器的帳戶，則可以使用 LDAP 使用者帳戶登入受管理裝置；而 SAML 2.0 所提供更進階的鑑別方法（例如，多重要素鑑別和單一登入），則可以用來登入 XClarity Administrator。
  - 單一登入可以讓已登入 XClarity Administrator 的使用者自動登入基板管理控制器。依預設，將 ThinkSystem 或 ThinkAgile 伺服器設定為受 XClarity Administrator 管理後，會啟用單一登入（使用 CyberArk 密碼管理伺服器的情況除外）。您可以配置廣域設定來啟用或停用所有受管理 ThinkSystem 和 ThinkAgile 伺服器的單一登入。為特定 ThinkSystem 和 ThinkAgile 伺服器啟用單一登入會置換所有 ThinkSystem 和 ThinkAgile 伺服器的廣域設定 (請參閱 XClarity Administrator 線上文件中的 管理伺服器)。

    **附註：**使用 CyberArk 識別管理系統進行鑑別時，單一登入會自動停用。
  - 為 ThinkSystem SR635 和 SR655 伺服器啟用受管理鑑別時：
    - 基板管理控制器韌體支援最多五個 LDAP 使用者角色。XClarity Administrator 會在管理期間，將這些 LDAP 使用者角色新增至伺服器：**lxc-supervisor**、**lxc-sysmgr**、**lxc-admin**、**lxc-fw-admin** 和 **lxc-os-admin**。使用者必須獲指派至少其中一個指定的 LDAP 使用者角色，才能與 ThinkSystem SR635 和 SR655 通訊。
    - 管理控制器韌體不支援與伺服器本端使用者具有相同使用者名稱的 LDAP 使用者。
  - 若是 ThinkServer 和 System x M4 伺服器，則不會使用 XClarity Administrator 鑑別伺服器。但是會在裝置上建立字首為「LXCA_」，後面緊接著隨機字串的 IPMI 帳戶（現有的本端 IPMI 使用者帳戶不會遭到停用）。當您解除管理 ThinkServer 伺服器時，會停用「LXCA_」使用者帳戶，並將字首「LXCA_」取代為字首「DISABLED_」。若要判斷 ThinkServer 伺服器是否受另一個實例管理，XClarity Administrator 會檢查字首為「LXCA_」的 IPMI 帳戶。如果您選擇強制管理受管理的 ThinkServer 伺服器，則會停用並重新命名裝置上字首為「LXCA_」的所有 IPMI 帳戶。請考慮手動清除不再使用的 IPMI 帳戶。

    如果您使用手動輸入的認證，XClarity Administrator 會自動建立已儲存認證，並且使用該份已儲存認證來管理裝置。

    **附註：**裝置的受管理鑑別啟用時，您無法使用 XClarity Administrator 編輯該裝置的已儲存認證。
    - 每次使用手動輸入的認證來管理裝置時，都將為該裝置建立一份新的已儲存認證，即使前次管理程序期間已為該裝置建立了另一份已儲存認證亦同。
    - 當您解除管理裝置時，XClarity Administrator 不會刪除在管理程序期間為該裝置自動建立的已儲存認證。

在 XClarity Administrator 管理系統後，XClarity Administrator 會定期輪詢每個受管理系統以收集資訊，例如庫存、重要產品資料和狀態。您可以檢視和監控每個受管理系統並執行管理動作（例如配置系統設定、部署作業系統映像檔，以及開啟和關閉電源）。

一個 XClarity Administrator 一次只能管理一個系統。不支援由多個管理員進行的管理。如果系統已受到一個 XClarity Administrator 管理，而您想要透過另一個 XClarity Administrator 管理它，則必須先在現行的

XClarity Administrator 上解除管理系統。接著您就可以透過另一個 XClarity Administrator 管理系統。如需解除管理系統的相關資訊，請參閱 XClarity Administrator 線上文件中的解除機箱管理、解除伺服器管理、解除管理 RackSwitch 交換器和解除管理 Lenovo Storage 儲存體系統。

**附註：**XClarity Administrator 不會在管理程序中修改安全設定或加密設定（加密模式和用於安全通訊的模式）。您可以在系統受到管理後修改加密設定（請參閱 XClarity Administrator 線上文件中的設定加密法模式和通訊 協定）。

**附註：**XClarity Administrator 可預先填入示範機箱（包括 CMM、計算節點及交換器）以及模擬真實硬體的示範機架式或直立式伺服器的硬體庫存。示範裝置已填入 Web 介面頁面中，可用於示範管理作業；不過，管理作業都會失敗。例如，您可以建立 Configuration Pattern 並將 Pattern 部署在展示伺服器，但部署都會失敗。您可以解除管理示範裝置來進行移除（請參閱 XClarity Administrator 線上文件中的解除機箱管理和解除伺服器管理）。刪除示範裝置之後，就無法再次管理。

## 程序

若要在 XClarity Administrator 中使用大量匯入檔案來探索和管理您的系統，請完成下列步驟。

**附註：**使用大量匯入管理交換器時，交換器上會啟用 HTTPS，並且會將交換器上的 NTP 用戶端配置為使用管理伺服器的 NTP 設定。若要變更這些設定，您必須手動管理交換器。

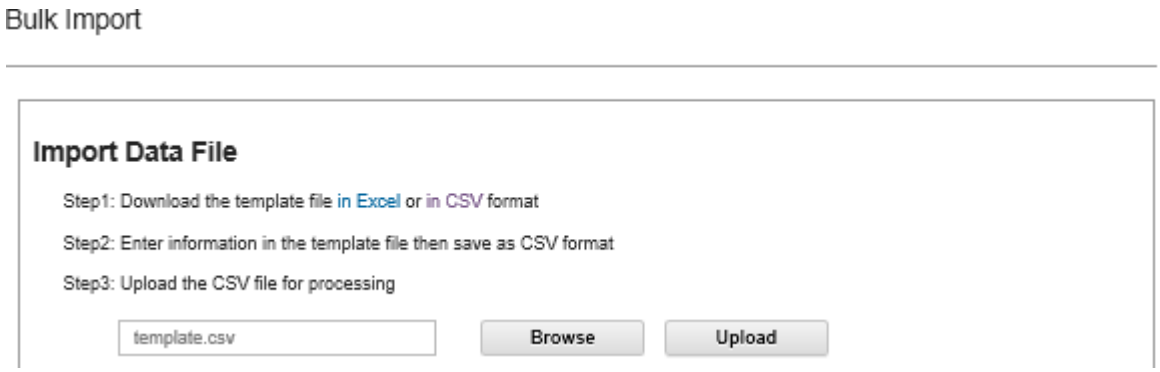
1. 在 XClarity Administrator 功能表列上，按一下**硬體 → 探索和管理新裝置**。顯示探索和管理頁面。
2. 按一下**在未來所有受管理裝置上啟用 Encapsulation** 勾選框，以變更管理程序期間所有裝置的防火牆規則，以便只接受從 XClarity Administrator 傳入的要求。

   **附註：**

   - 交換器、儲存裝置、非 Lenovo 機箱和伺服器不支援 encapsulation。
   - 當管理網路介面配置為使用動態主機配置通訊協定 (DHCP) 以及啟用 Encapsulation 時，管理機架式伺服器可能需要一段時間。

   管理特定裝置後，可以在特定裝置上啟用或停用 encapsulation。

   **注意：**如果已啟用 encapsulation，而且 XClarity Administrator 在裝置解除管理之前無法使用，則必須採取必要的步驟，停用 encapsulation 以建立與裝置的通訊。如需回復程序，請參閱 XClarity Administrator 線上文件中的在管理伺服器故障之後， 使用 CMM 回復機箱管理和在管理伺服器故障之後，回復機架式或直立式 伺服器管理。
3. 按一下**大量匯入**。大量匯入精靈隨即顯示。




4. 按一下「匯入資料檔」頁面上的 **Excel 格式**或 **CSV 格式**連結，下載 Excel 或 CSV 格式的大量匯入範本檔。

   **重要事項：**範本檔案可能會變更發佈版本。請確認一律使用最新版範本。
5. 填寫範本檔案中的資料表，並以*逗點區隔的* CSV 格式儲存檔案。

**要訣：**Excel 範本包括**資料**表和 **Readme** 表。請使用**資料**表填寫您的裝置資料。**Readme** 表提供如何填寫**資料**表各個欄位的相關資訊（包括必填欄位）和範例資料。

**重要事項：**

- 裝置將按照大量匯入檔案中所列的順序受到管理。
- 裝置受到管理時，XClarity Administrator 會使用裝置配置中定義的機架指派資訊。如果您在 XClarity Administrator 中變更機架指派，XClarity Administrator 將更新裝置配置。如果您在裝置受到管理之後更新裝置配置，所做的變更會反映在 XClarity Administrator 中。
- 建議（但非必要）對裝置指派機架之前先由試算表中明確建立機架。若未明確定義機架且 XClarity Administrator 中並無該機架，則將使用為裝置指定的機架指派資訊建立預設高度為 52U 的機架。

  如果您要使用另一款高度的機架，就必須先由試算表中明確定義機架後再將其指派給裝置。

若要由大量匯入檔案中定義裝置，請填妥下列各欄。

- （A - C 欄）基本探索：必須指定裝置類型和裝置目前的 IP 位址或序號。支援下列類型：
  - **填充板**。預留給已解除管理的裝置。在機架檢視中，此裝置顯示為一般填充板圖形。其他填充板類型請參閱 Excel 範本的 **Readme** 表。
  - **flexchassis**。10U Flex System 機箱
  - **伺服器**。XClarity Administrator 支援機架式和直立式伺服器
  - **機架**。6U、12U、18U、25U、37U、42U、45U、46U、48U、50U 和 52U 機架。不支援其他機架高度。預設會使用 52U。
  - **儲存體**。儲存裝置
  - **交換器**。RackSwitch 交換器

  **附註：**Flex System 計算節點、交換器和儲存裝置被視為機箱探索與管理程序的一部分。
- （D - H 欄）如果您選擇使用手動輸入的認證而不是已儲存認證（Z 欄）或識別（AF — AJ 欄），請指定目前的使用者名稱和密碼。如果部分裝置的認證不同，手動輸入的認證很實用。如果在大量匯入的檔案中沒有為一個或多個裝置指定認證，則會改用在大量匯入對話框中所指定的廣域認證。如需手動輸入的使用者和受管理鑑別的相關資訊，請參閱 XClarity Administrator 線上文件中的管理使用者帳戶。

  **附註：**
  - 若要使用手動輸入的認證，您必須選取 XClarity Administrator 受管理鑑別。
  - 某些欄位不適用於部分裝置。
  - （若是機箱）如果選擇受管理鑑別（在 AA 欄或大量匯入對話框中），則可以選擇在大量匯入檔案的 G 欄中或大量匯入對話框中指定 `RECOVERY_ID` 密碼。如果選擇本端鑑別，則不允許回復密碼。請勿在大量匯入檔案的 G 欄中或大量匯入對話框中指定回復密碼。
  - （若是機架式伺服器）如果選擇受管理鑑別（在 AA 欄或大量匯入對話框中），則可以選擇在大量匯入檔案的 G 欄中或大量匯入對話框中指定回復密碼。如果選擇本端鑑別，則不允許回復密碼。請勿在大量匯入檔案的 G 欄中或大量匯入對話框中指定回復密碼。
  - （若是機架式交換器）RackSwitch 裝置僅支援已儲存認證（Z 欄）對交換器進行鑑別。不支援手動輸入的使用者認證。
- （I - U 欄）如果要在成功管理後將裝置套用變更，則可選擇提供其他資訊。

  **附註：**某些欄位不適用於部分裝置。這些欄位不適用於 RackSwitch 交換器。
- （V - Z 欄）您可以選擇提供機架建立和指派的資訊，包括機架名稱、位置、機房、最低機架裝置和高度。

  **附註：**

— 建立機架時，務必指定機架名稱和機架高度。支援下列機架高度：6U、12U、18U、25U、37U、42U、45U、46U、48U、50U 和 52U。不支援其他機架高度。

— 建立一般填充板時，務必指定機架名稱和填充板高度。支援下列填充板高度：1U、2U 和 4U。

— 建立特定填充板時，將忽略填充板高度。XClarity Administrator 已知每一款特定填充板的高度。各款填充板類型和高度請參閱範本試算表。

— 對機架指派裝置時，將忽略裝置高度。裝置高度是從裝置庫存中擷取。

- （AA 欄）如果由於下列任一錯誤狀況導致管理未成功，請使用強制管理選項重複此程序。

  — 如果管理的 XClarity Administrator 發生故障且無法回復。

  **附註：**如果更換的 XClarity Administrator 實例使用與故障的 XClarity Administrator 相同的 IP 位址，您可以使用 RECOVERY_ID 帳戶和密碼（如適用）及強制管理選項再次管理裝置。

  — 如果管理的 XClarity Administrator 在裝置解除管理之前已停機。

  — 如果未能成功將裝置解除管理。

  裝置一次只能由一個 XClarity Administrator 實例管理。不支援由多個 XClarity Administrator 實例進行管理。如果裝置已由某個 XClarity Administrator 管理，而您想要透過另一個 XClarity Administrator 加以管理，則必須先從原始 XClarity Administrator 上解除管理該裝置，然後透過新的 XClarity Administrator 進行管理。

  **重要事項：**如果在 XClarity Administrator 管理伺服器之後變更伺服器的 IP 位址，則 XClarity Administrator 會辨識新的 IP 位址並繼續管理伺服器。不過，XClarity Administrator 無法辨識部分伺服器的 IP 位址變更。如果 XClarity Administrator 顯示伺服器在變更 IP 位址之後離線，請再次使用強制管理選項管理伺服器。

- （AB 欄）如果您選擇使用已儲存認證而不是手動輸入的認證（D — H 欄）或識別（AF — AJ 欄），請指定已儲存認證 ID。您可以在「已儲存認證」頁面找到已儲存認證 ID，方法是按一下 XClarity Administrator 功能表中的**管理 → 安全性**，然後按一下左側導覽中的**已儲存認證**。如需已儲存認證及本端鑑別的相關資訊，請參閱 XClarity Administrator 線上文件中的管理儲存的認證。

  **附註：**

  — RackSwtich 裝置僅支援使用已儲存認證進行鑑別。不支援手動輸入的使用者認證（D 欄）。

  — 如果使用已儲存認證來管理裝置並啟用受管理鑑別，您將無法編輯所用的已儲存認證。

- （AC 欄）對於機箱和機架式伺服器，如果選擇使用受管理鑑別，則必須在大量匯入檔案的 G 欄中或大量匯入對話框中指定 RECOVERY_ID 密碼。如果選擇本端鑑別，則不允許回復密碼。請勿在大量匯入檔案的 G 欄中或大量匯入對話框中指定回復密碼。

- （AD 欄）若是機架式伺服器，您可以選擇透過在此欄中指定 FALSE 以使用本端鑑別，而不使用 XClarity Administrator 受管理鑑別。如需受管理和本端鑑別的相關資訊，請參閱 XClarity Administrator 線上文件中的管理鑑別伺服器。

- （AE 欄）您可以選擇指定允許檢視及管理裝置的角色群組清單。僅能指定目前使用者所屬的角色群組。

  **附註：**如果您新增裝置到受管理機箱，新裝置將與該機箱屬於同一角色群組。

- （AF — AJ 欄）如果您選擇使用識別管理系統而不是手動輸入的認證（D — H 欄）或已儲存認證（AB 欄），請指定受管理伺服器的 IP 位址或主機名稱、使用者名稱，以及選用的應用程式 ID、保險箱和資料夾。

  如果指定了應用程式 ID，則還必須指定保險箱和資料夾（如果適用）。

  如果未指定應用程式 ID，XClarity Administrator 會使用您在設定 CyberArk 時使用的路徑來識別已加入 CyberArk 中的帳戶 (請參閱 XClarity Administrator 線上文件的 設定 CyberArk 識別管理系統)。

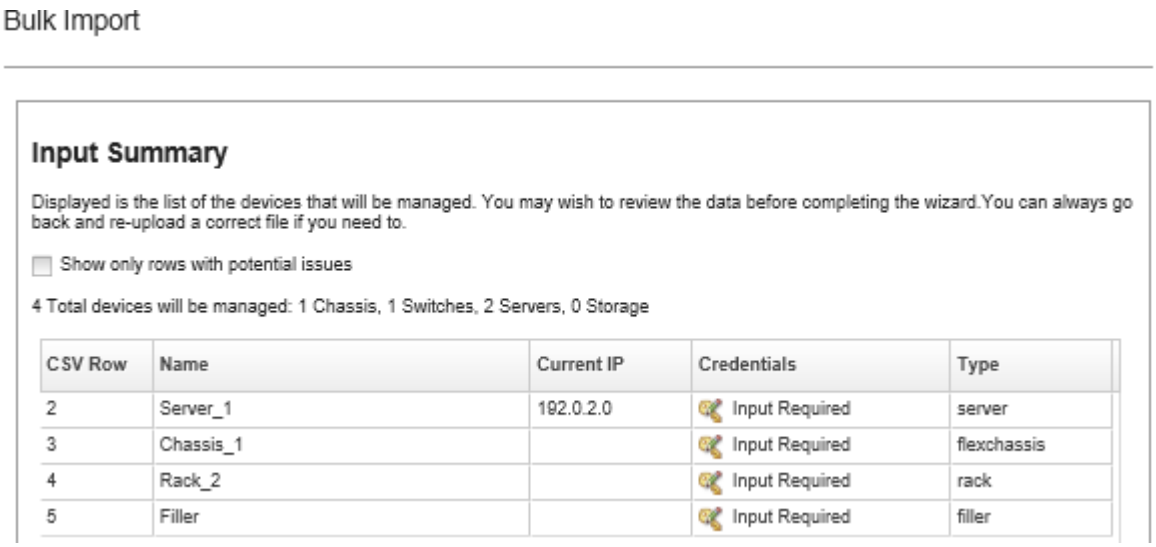
  **附註：**僅支援 ThinkSystem 或 ThinkAgile 伺服器。必須在 XClarity Administrator 中配置識別管理系統，而且受管理 ThinkSystem 或 ThinkAgile 伺服器的 Lenovo XClarity Controller 必須與 CyberArk 整合（請參閱 XClarity Administrator 線上文件中的設定 CyberArk 識別管理系統）。

下圖顯示大量匯入檔案的範例：

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Required fields (Type + SN or IP) | | | Optional fields | | | | | | | | | | | | | | | |
| Type | Serial Number | Current IP | Current username | Current password | New password | Recovery password | Switch enable password | New IPv4 | IPv4 subnet mask | IPv4 default gateway | IPv4 DNS1 | IPv4 DNS2 | New IPv6 | IPv6 prefix | IPv6 gateway | IPv6 DNS1 | IPv6 DNS2 | Domain |
| server | | 10.1.0.198 | | | | | | | | | | | | | | | | |
| server | P67X3OEL | | | | | | | | | | | | | | | | | |
| flexchassis | | 10.1.0.213 | USERID | passw0rdx | Pa55word@ | abcd1234 | | | | | | | | | | | | |
| flexchassis | Z3499DD | | | | Pa55word@ | abcd1234 | | 9.27.20.51 | 255.255.255.0 | 9.27.20.1 | 9.0.148.50 | 9.0.146.50 | | | | | | ebg.lenovo.com |
| server | 35T88XP | | | | | | | | | | | | 2002:939 | 2002:9 | 2002:939: | 2002:9 | 2002:9 | ebg.lenovo.com |
| server | | 10.1.0.214 | | | | | | 10.1.2.213 | 255.255.255.0 | 10.1.2.1 | 9.0.148.50 | 9.0.146.50 | | | | | | ebg.lenovo.com |
| rack | | | | | | | | | | | | | | | | | | |
| rack | | | | | | | | | | | | | | | | | | |
| filler | | | | | | | | | | | | | | | | | | |
| filler | | | | | | | | | | | | | | | | | | |
| filler | | | | | | | | | | | | | | | | | | |

| R | S | T | U | V | W | X | Y | Z | AA | AB | AC | AD | AE | AF | AG | AH | AI | AJ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| IPv6 DNS2 | Domain | Host name | User-defined name | Rack name | Location | Room | Lowest rack unit | Height | Force | Stored credentials ID | Stored credentials ID for RECOVERY_ID | Managed authentication | Role Groups | IdentityManagementSystemEnabled | IMS type | IMS AppID | Folder | Safe |
| | | | | | | | | | | | | | | TRUE | CyberArk | LXCA | | Test |
| | | | | | | | | | | | | | | | | | | |
| | | | chassis03 | SH3G05A34 | | | 25 | | TRUE | | | | | | | | | |
| | ebg.lenovo.com | chassis01 | chassis01 | SH3G05A34 | | | 5 | | | | | | | | | | | |
| 2002:9 | ebg.lenovo.com | host4 | c02node01 | SH3G05B12 | | | 38 | | | 2 | 3 | FALSE | | | | | | |
| | ebg.lenovo.com | host5 | web02 | SH3G05B12 | | | 10 | | | | | | | | | | | |
| | | | SG2R01A01 | | | | | 37 | | | | | | | | | | |
| | | | SH3G05A34 | | | | | 46 | | | | | | | | | | |
| | | | APC UPS | SH3G05A34 | | | 1 | 4 | | | | | | | | | | |
| | | | FC switch | SH3G05A34 | | | 40 | 2 | | | | | | | | | | |
| | | | KVM switch | SH3G05B12 | | | 22 | 1 | | | | | | | | | | |

6. 從大量匯入精靈中，輸入要上傳處理的 CSV 檔案名稱。請按**瀏覽**，協助您找出該檔案。
7. 按一下**上傳**，上傳並驗證檔案。
8. 按**下一步**以顯示「輸入摘要」頁面，列出將受管理的裝置。

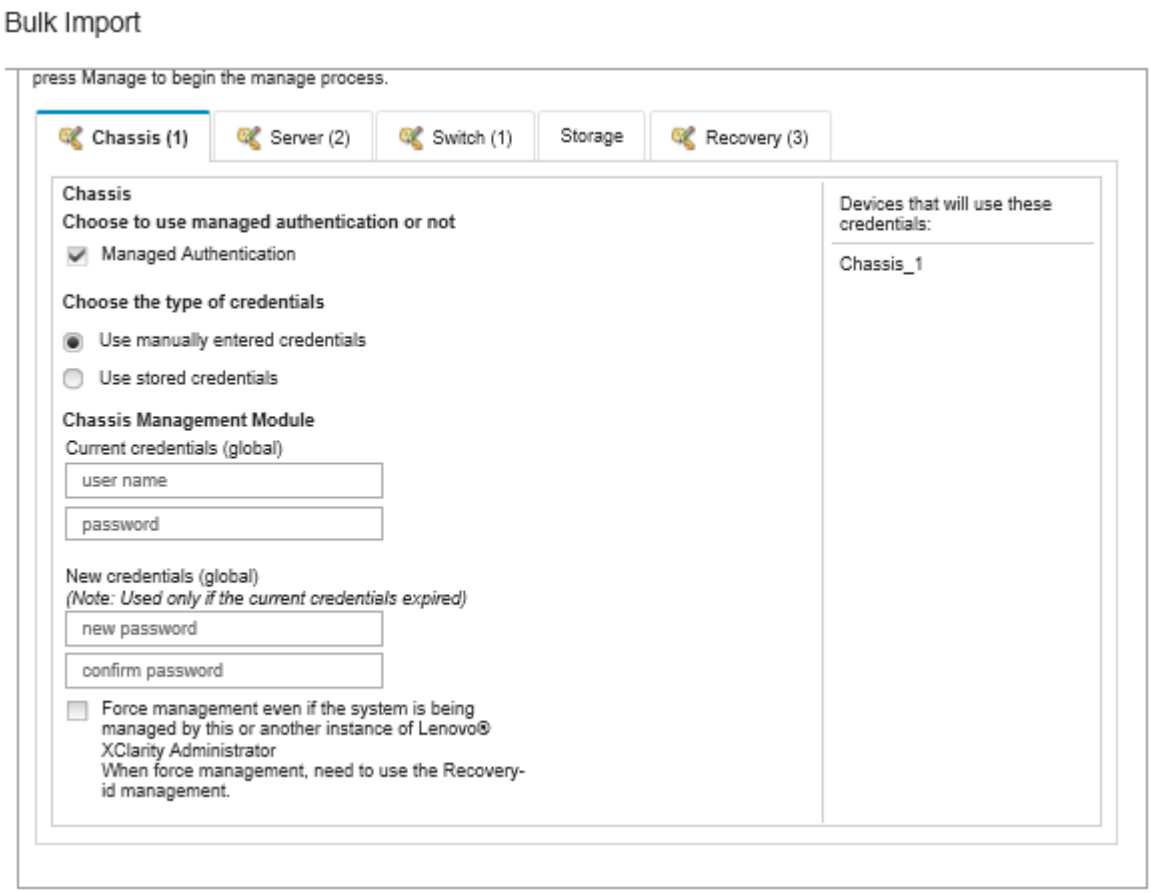



9. 檢閱您要管理的裝置摘要。

   選取**僅顯示有潛在問題的列**，列出資料不完整的列。由大量匯入檔案中修正任何問題，然後按**上一步**上傳已更正的 CSV 檔案。

   **附註：**

   - 如果大量匯入檔案未提供必填資料，相關聯的裝置將不會受到管理。
   - 輸入摘要頁面會標出無認證資訊的列。如果大量匯入檔案中未指定認證，則會改用您在大量匯入精靈中所指定的廣域認證。
10. 按**下一步**以顯示「裝置認證」頁面。




11. **選填：**按一下各個標籤，選擇性指定特定類型的所有裝置要使用的廣域設定和認證。各個標籤的右側會列出將使用廣域設定和認證的裝置。

    如果選擇使用廣域認證，則特定裝置類型的認證必須與未在大量匯入檔案中輸入認證的所有同類型裝置相同。例如，所有機箱的 CMM 認證必須相同，而所有儲存裝置的儲存體管理認證也必須一樣。如果認證不相同，則必須輸入大量匯入檔案中的認證。

    - **機箱**。指定鑑別模式和認證類型。指定用於登入大量匯入檔案中列出的所有機箱的目前認證。如果目前的 CMM 認證已過期，請指定要使用的新密碼。

      如果您強制管理機箱，請為裝置認證指定 RECOVERY_ID 帳戶及密碼。
    - **伺服器**。指定鑑別模式和認證類型。指定用於登入大量匯入檔案中列出的所有機架和直立式伺服器的目前認證。如果目前的基板管理控制器認證已過期，請指定要使用的新密碼。

      如果您強制管理伺服器，請為裝置認證指定 RECOVERY_ID 帳戶及密碼。
    - **交換器**。指定用於登入大量匯入檔案中列出的所有 RackSwitch 交換器的已儲存認證。如已設定，請同時指定用於進入交換器特殊權限執行模式的「啟用」密碼。
    - **儲存體**。指定用於登入大量匯入檔案中列出的所有儲存裝置的目前認證。
    - **回復**。指定用於登入大量匯入檔案中列出的所有伺服器和機箱的回復密碼。

      您可以選擇使用本端使用者帳戶或儲存的回復認證。無論哪種情況，使用者名稱始終為 `RECOVERY_ID`。

      指定密碼後，就會建立裝置上的 `RECOVERY_ID` 帳戶，並停用所有本端使用者帳戶。

      — 若是機箱，則需要回復密碼。

      — 若是伺服器，如果選擇使用受管理鑑別，則可選用回復密碼；若是選擇使用本端鑑別，則不允許使用回復密碼。

      — 確定密碼遵循裝置的安全原則和密碼原則。安全原則和密碼原則可能不同。

      — 請務必記下回復密碼以供日後使用。

— ThinkServer 和 System x M4 伺服器不支援回復帳戶。

您在大量匯入檔案中指定的資訊將會置換您在「裝置認證」頁面上指定的類似資訊。

如有下列情況，您可以選擇強制管理每一類型的裝置：

- 裝置目前正由其他管理系統（例如另一個 XClarity Administrator 實例或 IBM Flex System Manager）管理
- XClarity Administrator 已停機，但在停機前未解除管理裝置
- 裝置未正確解除管理，CIM 訂閱也未清除

**附註：**如果由另一個 XClarity Administrator 實例管理裝置，在發生強制管理後，該裝置似乎仍由原始實例管理一段時間。您可以解除管理裝置，以從原始 XClarity Administrator 實例中移除裝置。

12. 按一下**管理**。「監視結果」頁面隨即顯示，提供大量匯入檔案中各裝置的管理狀態相關資訊。

    將建立一項工作以進行管理程序。如果您關閉大量匯入精靈，管理程序將繼續在背景執行。您可以從工作日誌監視管理程序的狀態。如需工作日誌的相關資訊，請參閱監視工作（在 XClarity Administrator 線上文件中）。

    如果 XClarity Administrator 無法使用在大量匯入檔案中所指定的認證，或是在對話框中所指定的廣域認證登入裝置，就無法管理該裝置，XClarity Administrator 會移到大量匯入檔案中的下一個裝置。

    **附註：**如果由於下列任一錯誤狀況導致管理未成功，請使用**強制管理**選項重複此程序。

    - 如果管理的 XClarity Administrator 發生故障且無法回復。

      **附註：**如果更換的 XClarity Administrator 實例使用與故障的 XClarity Administrator 相同的 IP 位址，您可以使用 RECOVERY_ID 帳戶和密碼（如適用）及**強制管理**選項再次管理裝置。
    - 如果管理的 XClarity Administrator 在裝置解除管理之前已停機。
    - 如果未能成功將裝置解除管理。

    **注意：**裝置一次只能由一個 XClarity Administrator 實例管理。不支援由多個 XClarity Administrator 實例進行管理。如果裝置已由某個 XClarity Administrator 管理，而您想要透過另一個 XClarity Administrator 加以管理，則必須先從原始 XClarity Administrator 上解除管理該裝置，然後透過新的 XClarity Administrator 進行管理。

13. 如果大量匯入檔案包含新機箱，請透過建立及部署 Server Patterns，驗證和變更整個機箱（包括計算節點和 Flex 交換器）的管理網路設定，並配置計算節點資訊、本端儲存體、I/O 配接卡、開機目標及韌體設定。如需相關資訊，請參閱修改機箱的管理 IP 設定和使用 XClarity Administrator 配置伺服器（在 XClarity Administrator 線上文件中）。

## 在您完成之後

在您管理各系統後，可以執行下列動作：

- 探索和管理其他系統（請參閱 Lenovo XClarity Administrator 線上文件中的管理機箱、管理機架、管理伺服器、管理儲存裝置和管理交換器）。
- 建立及部署 Server Patterns，藉此配置系統資訊、本端儲存體、I/O 配接卡、開機設定及韌體設定（請參閱 Lenovo XClarity Administrator 線上文件中的使用 XClarity Administrator 配置伺服器）。
- 將作業系統映像檔部署至尚未安裝作業系統的伺服器（請參閱 XClarity Administrator 線上文件中的部署作業系統映像檔）。
- 為未遵循現行原則的裝置更新韌體（請參閱 XClarity Administrator 線上文件中的更新受管理裝置上的韌體）。
- 將新管理的系統新增到適當的機架，以反映實體環境（請參閱 XClarity Administrator 線上文件中的管理機架）。
- 監視硬體狀態和詳細資料（請參閱 XClarity Administrator 線上文件中的檢視受管理伺服器的狀態）。

- 監視事件和警示（請參閱 XClarity Administrator 線上文件中的使用事件和使用警示）。
- 為受管理 ThinkSystem 和 ThinkAgile 伺服器停用或啟用單一登入。
  - 對於所有受管理 ThinkSystem 和 ThinkAgile 伺服器（廣域），在 XClarity Administrator 功能表列中按一下**管理 → 安全性**，按一下**作用中階段作業數**，然後啟用或停用**單一登入**
  - 對於特定 ThinkSystem 和 ThinkAgile 伺服器，在 XClarity Administrator 功能表列中按一下**硬體 → 伺服器**，然後按一下**所有動作 → 安全性 → 啟用單一登入**，或**所有動作 → 安全性 → 停用單一登入**。

**附註：**單一登入可以讓已登入 XClarity Administrator 的使用者自動登入基板管理控制器。依預設，將 ThinkSystem 或 ThinkAgile 伺服器設定為受 XClarity Administrator 管理後，會啟用單一登入（使用 CyberArk 密碼管理伺服器的情況除外）。您可以配置廣域設定來啟用或停用所有受管理 ThinkSystem 和 ThinkAgile 伺服器的單一登入。為特定 ThinkSystem 和 ThinkAgile 伺服器啟用單一登入會置換所有 ThinkSystem 和 ThinkAgile 伺服器的廣域設定。

# 第 5 章 註冊 XClarity Administrator

透過註冊您的 Lenovo XClarity Administrator 實例，您可以使用基本功能，而不會收到關於試用期滿和不符合標準授權的重複警告。註冊後，不符合標準的授權警告將不再顯示；然而，需要授權的所有功能都保持停用狀態，直到您購買並安裝與受管理裝置數量相符的授權。

## 關於此作業

註冊您的 XClarity Administrator 實例不需要共用您的聯絡資訊。Lenovo 不會與其他外部實體共用您提供的資訊。

如果您已經安裝了進階功能的授權，則無需註冊您的 XClarity Administrator 實例。如需授權和進階功能的相關資訊，請參閱安裝可啟用完整功能的授權。

## 程序

若要註冊 XClarity Administrator，請完成下列步驟。

- 如果 XClarity Administrator 已連接至網際網路
  1. 在 Lenovo XClarity Administrator 功能表列上，按一下**管理 → 註冊**，以顯示「註冊」頁面。
  2. 按一下**註冊**以註冊新的 XClarity Administrator 實例。
  3. 填寫公司名稱、要由 XClarity Administrator 管理的裝置數量，以及 XClarity Administrator 所在的國家/地區。
  4. 按一下**提交**。
- 如果 XClarity Administrator 未連接至網際網路
  1. 註冊 XClarity Administrator。
     a. 在 Web 瀏覽器中開啟 Lenovo XClarity 註冊入口網站。
     b. 填寫公司名稱、要由 XClarity Administrator 管理的裝置數量，以及 XClarity Administrator 所在的國家/地區。
     c. 按一下**提交**以接收註冊權杖。
  2. 在 Lenovo XClarity Administrator 功能表列上，按一下**管理 → 註冊**，以顯示「註冊」頁面。
  3. 按一下**匯入**以匯入註冊權杖。
  4. 填寫您在步驟 1 中收到的註冊權杖。
  5. 按一下**提交**。

© Copyright Lenovo 2022

# 第 6 章 安裝可啟用完整功能的授權

90 天免費試用到期後，您必須為所有支援進階功能之受管理裝置購買並安裝 Lenovo XClarity Pro 授權，才能繼續使用 Lenovo XClarity Administrator 中的作業系統部署和裝置配置功能。*所有*受管理裝置必須都安裝 Lenovo XClarity Pro 授權，您才可以獲得 XClarity Administrator 服務與支援。

## 開始之前

**進一步瞭解：** XClarity Administrator：安裝授權

請查看下面授權考量。

- 授權*未*與特定裝置連結。
- 機箱授權提供 14 個裝置的授權。
- 對於 System x3850 X6 (6241) 可調式複合體伺服器，每個伺服器都需要個別授權，與分割區無關。
- 對於 System x3950 X6 (6241) 可調式複合體伺服器，如未分割處理，則每個伺服器都需要單獨的授權。如已經過分割處理，每個分割區都需要單獨的許可證。
- 以下裝置*不支援*進階功能，因此*不需要*這些功能的授權；但是，必須為每個裝置購買授權才能獲得 XClarity Administrator 服務和支援。
  — ThinkServer 伺服器
  — System x M4 伺服器
  — System x X5 伺服器
  — System x3850 X6 和 x3950 X6 (3837) 伺服器
  — 儲存裝置
  — 交換器

您必須具備 **lxc-supervisor** 或 **lxc-security-admin** 權限才能安裝授權。

## 關於此作業

XClarity Administrator 支援下列授權。

- **Lenovo XClarity Pro**。每份授權都會為單一裝置提供以下權利。
  — Lenovo XClarity Integrator 服務和支援
  — XClarity Administrator 服務和支援
  — XClarity Administrator 的進階功能：
    — 使用 Configuration Patterns 配置伺服器
    — 部署作業系統
    — 使用 Call Home 報告 XClarity Administrator 問題（硬體警示的 Call Home 不受影響。）

授權的啟動期間從購買授權並建立授權碼時開始。

授權的相符性由支援進階功能的受管理裝置數量決定。受管理裝置的數量不得超過所有作用中授權金鑰中的授權總數。如果 XClarity Administrator 不符合已安裝的授權（例如，授權過期或管理的其他裝置數量超過作用中授權總數），您將有 90 天的寬限期來安裝適當的授權。每當 XClarity Administrator 變成不符合標準時，寬限期便會重設為 90 天。如果寬限期 (包括免費試用) 結束時間在授權符合標準之前，則所有裝置上都會停用進階功能。

例如，如果您在現有 XClarity Administrator 實例中額外管理 100 部 ThinkSystem 伺服器和 20 部機架交換器，則在使用者介面中的進階功能停用之前，您有 90 天可購買和安裝 100 個額外授權。使用進階功能時並

© Copyright Lenovo 2022

不需要 20 個機架交換器的授權；但是，如果想要使用和服務，則需要這些授權。如果進階功能停用，則當您安裝足夠授權而回復相符性之後，這些進階功能將會重新啟用。

如果您使用的是免費試用授權，或者您有符合標準前的寬限期，而您升級到較新版本的 XClarity Administrator，則試用授權或寬限期會重設為 90 天。

**附註：**

- 寬限期到期時，伺服器配置和作業系統部署功能便會停用。
- 授權不符合標準時，XClarity Administrator 問題的 Call Home（軟體 Call Home 功能）便會停用。此功能沒有寬限期。但是，硬體警示的 Call Home 不受影響。

如果已安裝授權，升級至新版 XClarity Administrator 時就*不*需要新授權。

您可以按一下 XClarity Administrator 標題列上的使用者動作功能表（ADMIN_USER），然後按一下**關於**，以判斷授權狀態，包括試用授權的剩餘天數。

**取得協助**

- 如果您是向事業夥伴訂購而有任何問題，請聯絡您的事業夥伴以查證交易與啟用狀況。
- 如果您未收到電子權利證明、授權碼或啟動金鑰，或是郵件誤寄給了其他人，請根據您的所在地聯絡區域代表。
  — ESDNA@lenovo.com（北美地區）
  — ESDAP@lenovo.com（亞太地區）
  — ESDEMEA@lenovo.com（歐洲、中東暨非洲地區）
  — ESDLA@lenovo.com（拉丁美洲地區）
  — ESDChina@Lenovo.com（中國）
- 如果有關權利的資訊有誤，請傳送電子郵件至 SW_override@lenovo.com 聯絡 Lenovo 支援中心，並在其中包含下列資訊：
  — 訂購號碼
  — 您的聯絡資訊，包括電子郵件位址。
  — 您的郵寄地址
  — 您要進行的變更
- 如果您對下載授權有任何問題或疑問，請傳送電子郵件至 -eSupport_-_Ops@lenovo.com 聯絡 Lenovo 支援中心。

## 使用 XClarity Administrator Web 介面安裝可啟用完整功能的授權

如果 XClarity Administrator 可存取網際網路，您可以使用 XClarity Administrator Web 介面兌換和擷取現有授權的授權，然後匯入並安裝兌換的授權。

### 開始之前

聯絡您的 Lenovo 業務代表或授權事業夥伴，以根據您要啟用的功能和要管理的裝置數量購買 Lenovo XClarity Pro 授權。購買授權之後，您將透過*電子權利證明*電子郵件收到授權碼。授權碼是 22 個字元的英數字串，您需要用它來兌換和安裝授權。如果您是透過事業夥伴購買授權而未收到該電子郵件，請聯絡您的事業夥伴以申請授權碼。

您也可以按一下**擷取授權碼**，從 Features on Demand 入口網站擷取您的授權碼。

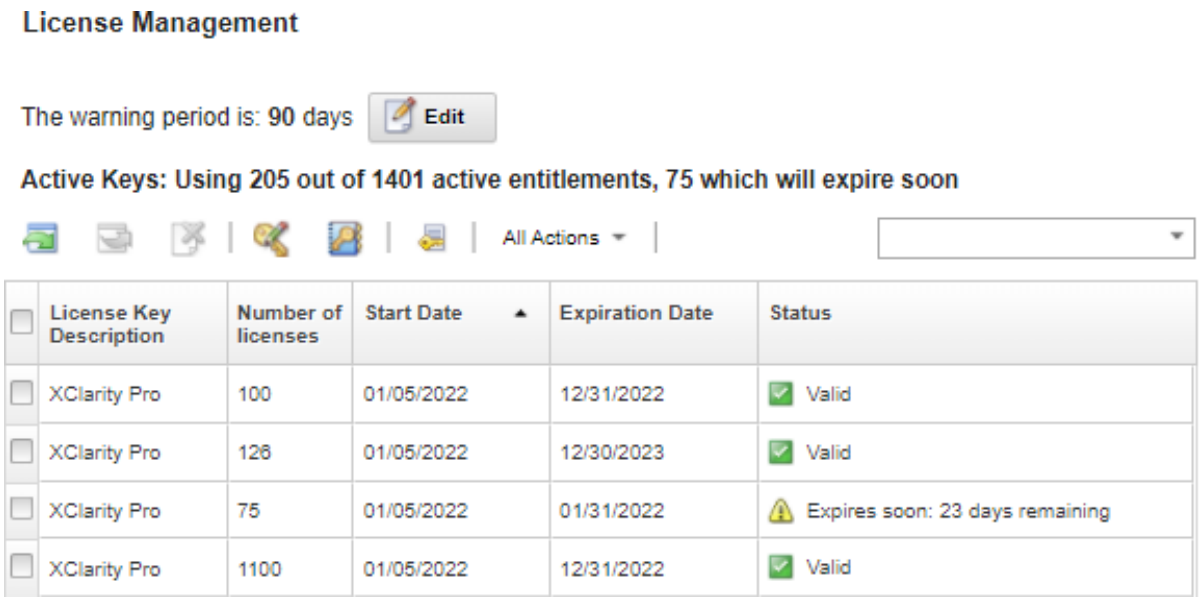
### 程序

如果要在管理伺服器中安裝 Lenovo XClarity Pro 授權，請完成下列其中一個程序。

- **兌換並安裝單一授權碼中的所有或部分剩餘授權**

您可以兌換單一授權碼所有或部分的可用授權以建立授權啟動金鑰，該金鑰是包含已兌換授權的所有資訊的檔案。然後，您可以使用該授權啟動金鑰安裝已兌換的授權。

1. 在 XClarity Administrator 功能表列上，按一下**管理** → **授權**以顯示授權管理頁面。




2. 按一下**申請啟動金鑰**圖示 ( ) 以顯示申請啟動金鑰對話框。
3. 按一下**單一授權碼**。
4. 輸入 22 個字元的授權碼，然後按一下**搜尋**，從 Features on Demand 網站擷取該指定授權碼的已購買授權的相關資訊。

   如果您收到的授權碼不被接受，請聯絡 Lenovo 支援中心。
5. 在 **Lenovo 客戶號碼**欄位中輸入您的 10 位數 Lenovo 客戶號碼。
6. 在**兌換數量**欄位中輸入您要兌換的授權數量，然後按一下**繼續**。

   若要兌換授權碼中的所有可用授權，請在**可用授權**欄位中輸入相符的數字。

   如果兌換一部分可用授權，則可以在稍後使用同一個授權碼兌換其餘的授權。

   **要訣：**每個 XClarity Administrator 最多支援 1,000 個受管理裝置。因此，可安裝在一個 XClarity Administrator 實例中的單一授權啟動金鑰擁有的授權數量不能超過 1,000 個。
7. 檢查聯絡資訊的準確性，並視需要進行修改。
8. 按一下**提交要求**以兌換授權並建立授權啟動金鑰。
9. 選取包含要安裝的授權的授權啟動金鑰。
10. 按一下**安裝**，在管理伺服器中安裝授權。
11. 按一下**關閉**。

- **兌換並安裝多個授權碼中的所有剩餘授權**

您可以兌換多個授權碼的所有剩餘授權。每個授權碼都會建立一個授權啟動金鑰。然後，您可以使用授權啟動金鑰安裝已兌換的授權。必須使用提供的範本在 CSV 格式的檔案中提供授權碼。

1. 在 XClarity Administrator 功能表列上，按一下**管理** → **授權**以顯示授權管理頁面。
2. 按一下**申請啟動金鑰**圖示 ( ) 以顯示申請啟動金鑰對話框。
3. 按一下**多個授權碼**。
4. 按一下**下載範本**鏈結以開啟 Excel 檔案。將每個授權碼加入檔案中，然後將檔案以 CSV 格式儲存在本端系統。

5. 按一下**瀏覽**以尋找並選取授權碼 CSV 檔案，然後按一下**搜尋**，從 Lenovo 支援中心網站擷取授權碼的相關資訊。
6. 檢閱與每個授權碼相關聯的已購買授權和可用授權啟動金鑰的相關資訊。
7. 在 **Lenovo 客戶號碼**欄位中輸入您的 10 位數 Lenovo 客戶號碼。
8. 檢查聯絡資訊的準確性，並視需要進行修改。然後，按一下**繼續**。
9. 選取**是的，我想兌換所有有效的授權碼**，然後按一下**提交要求**以產生授權啟動金鑰。
10. 選取要安裝的授權啟動金鑰。
11. 按一下**安裝**，在管理伺服器中安裝授權啟動金鑰。
12. 按一下**關閉**。

- **擷取並安裝已兌換的授權**

  您可以從能夠存取 Features on Demand 入口網站的 XClarity Administrator 實例將授權啟動金鑰下載到本端系統，然後將這些授權啟動金鑰匯入並安裝到另一個 XClarity Administrator 實例中。當您想要將授權安裝在無法存取網際網路的 XClarity Administrator 實例時，或您重新安裝了 XClarity Administrator 並需要還原已安裝的授權時，這個方法很實用。

  1. 在 XClarity Administrator 功能表列上，按一下**管理** → **授權**以顯示授權管理頁面。
  2. 按一下**擷取歷程**圖示 ( ) 以顯示擷取歷程對話框。
  3. 輸入您的 Lenovo 客戶號碼或 22 個字元的授權碼。
  4. 按一下**搜尋**以擷取有關可用授權和已兌換授權的資訊。

     如果您收到的授權碼不被接受，請聯絡 Lenovo 支援中心。
  5. 選取要安裝的授權金鑰檔案。
  6. 按一下**安裝**，在 XClarity Administrator 中安裝授權啟動金鑰。
  7. 按一下**關閉**。

- **在另一個 XClarity Administrator 實例中匯入並安裝已兌換的授權**

  如果已使用一個 XClarity Administrator 實例兌換授權，並希望在另一個 XClarity Administrator 實例上安裝那些授權，或者如果發生錯誤狀況而需要您還原已安裝的授權，則可以將授權金鑰檔案從本端系統匯入到另一個 XClarity Administrator 實例。

  1. 在可以存取 Features on Demand 入口網站的 XClarity Administrator 實例中，從 Features on Demand 入口網站擷取授權啟動金鑰，然後將授權啟動金鑰另存為本端系統中的檔案。
     a. 在 XClarity Administrator 功能表列上，按一下**管理** → **授權**以顯示授權管理頁面。
     b. 按一下**擷取歷程**圖示 ( ) 以顯示擷取歷程對話框。
     c. 輸入 22 個字元的授權碼。
     d. 按一下**搜尋**以擷取該授權碼的可用授權和已兌換授權的相關資訊。

        如果您收到的授權碼不被接受，請聯絡 Lenovo 支援中心。
     e. 選取要安裝的授權啟動金鑰檔案。
     f. 按一下**下載**，將授權金鑰檔案儲存到本端系統。
  2. 在您要安裝授權啟動金鑰的 XClarity Administrator 實例中：
     a. 在 XClarity Administrator 功能表列上，按一下**管理** → **授權**以顯示授權管理頁面。
     b. 按一下**匯入並套用**圖示 ( ) 以匯入並安裝授權。
     c. 按一下**瀏覽**，選取您要安裝的授權的授權啟動金鑰。

        如果要匯入多個授權啟動金鑰，請將 .KEY 檔案壓縮成 ZIP 檔案，然後選取該 ZIP 檔案進行匯入。
     d. 按一下**接受授權**以匯入並套用授權。

安裝完成後，表格中會列出授權啟動金鑰，以及已安裝授權的數量和啟動期間（開始日期和到期日）。

## 在您完成之後

您可以在授權頁面上執行下列動作。

- 按一下**匯出**圖示 ( )，將一個或多個特定授權啟動金鑰下載至本端系統。

  **附註：**匯出多個授權啟動金鑰時，檔案將以單一 ZIP 檔案下載。
- 按一下**刪除**圖示 ( ) 以刪除特定授權啟動金鑰。
- 按一下頁面頂端的**編輯**按鈕以配置授權警告期間。授權警告期間是 XClarity Administrator 觸發警告到授權到期前的天數。

### 取得協助

- 如果您是向事業夥伴訂購而有任何問題，請聯絡您的事業夥伴以查證交易與啟用狀況。
- 如果您未收到電子權利證明、授權碼或啟動金鑰，或是郵件誤寄給了其他人，請根據您的所在地聯絡區域代表。
  — ESDNA@lenovo.com（北美地區）
  — ESDAP@lenovo.com（亞太地區）
  — ESDEMEA@lenovo.com（歐洲、中東暨非洲地區）
  — ESDLA@lenovo.com（拉丁美洲地區）
  — ESDChina@Lenovo.com（中國）
- 如果有關權利的資訊有誤，請傳送電子郵件至 SW_override@lenovo.com 聯絡 Lenovo 支援中心，並在其中包含下列資訊：
  — 訂購號碼
  — 您的聯絡資訊，包括電子郵件位址。
  — 您的郵寄地址
  — 您要進行的變更
- 如果您對下載授權有任何問題或疑問，請傳送電子郵件至 -eSupport_-_Ops@lenovo.com 聯絡 Lenovo 支援中心。

# 使用 Features on Demand 入口網站安裝啟用完整功能的授權

如果 XClarity Administrator *無法*存取網際網路，您可以從另一個可透過網路存取 XClarity Administrator 的系統，使用 Features on Demand 入口網站來兌換和擷取現有授權碼的授權。然後，您可以使用 XClarity Administrator Web 介面匯入並安裝兌換的授權。

## 程序

如果要在管理伺服器中安裝 Lenovo XClarity Pro 授權，請完成下列步驟。

步驟 1. 為每個受管理裝置購買 Lenovo XClarity Pro 授權。

聯絡您的 Lenovo 業務代表或授權事業夥伴，以根據您要啟用的功能和要管理的裝置數量購買 Lenovo XClarity Pro 授權。購買授權之後，您將透過*電子權利證明*電子郵件收到授權碼。授權碼是 22 個字元的英數字串，您需要用它來兌換和安裝授權。如果您是透過事業夥伴購買授權而未收到該電子郵件，請聯絡您的事業夥伴以申請授權碼。

您也可以按一下**擷取授權碼**，從 Features on Demand 入口網站擷取您的授權碼。

步驟 2. 使用授權碼兌換所有或部分授權。兌換授權時，會產生一個授權啟動金鑰檔案。

1. 從 Web 瀏覽器開啟 Features on Demand 入口網站，使用電子郵件地址做為使用者 ID 登入入口網站。

2. 按一下**申請啟動金鑰**。
3. 選取**輸入單一授權碼**。
4. 輸入 22 個字元的授權碼，然後按一下**繼續**。
5. 在 **Lenovo 客戶號碼**欄位中輸入您的 Lenovo 客戶號碼。
6. 在**兌換數量**欄位中輸入您要兌換的授權數量，然後按一下**繼續**。

   若要兌換此授權碼中的所有可用授權，請在**可用授權**欄位中輸入相符的數字。

   如果兌換一部分可用授權，則可以使用同一個授權碼在另一個授權啟動金鑰中兌換其餘的授權。

   **要訣：**每個 XClarity Administrator 最多支援 1,000 個受管理裝置。因此，可安裝在一個 XClarity Administrator 實例中的單一授權啟動金鑰擁有的授權數量不得超過 1,000 個。
7. 依照提示輸入產品詳細資料和聯絡資訊，然後按一下**繼續**以產生授權啟動金鑰。
8. 您可以選擇指定其他收件者以接收授權啟動金鑰。
9. 按一下**提交**傳送授權啟動金鑰。

   採購單上指派的人員和其他收件者將收到含有授權啟動金鑰的電子郵件。金鑰是 .KEY 格式的檔案。

   **附註：**您也可以從 Features on Demand 入口網站下載授權啟動金鑰（個別或批次），方法是按一下**擷取歷程**，使用您的 Lenovo 客戶號碼尋找您的授權啟動金鑰，然後下載所有或部分金鑰。然後，按一下**電子郵件**透過電子郵件將金鑰傳送給您，或按**下載**將金鑰下載到您的本端系統。

步驟 3. 在 XClarity Administrator 中匯入並安裝授權。

1. 在 XClarity Administrator 功能表列上，按一下**管理 → 授權**以顯示授權管理頁面。
2. 按一下**匯入並套用**圖示 ( ) 以安裝授權。
3. 按一下**瀏覽**，選取您要安裝的授權的授權啟動金鑰檔案。

   **要訣：**如果要匯入多個授權啟動金鑰，請將 .KEY 檔案壓縮成 ZIP 檔案，然後選取該 ZIP 檔案進行匯入。
4. 按一下**接受授權**以匯入並套用授權。

   安裝完成後，表格中會列出授權啟動金鑰，以及已安裝授權的數量和啟動期間（開始日期和到期日）。

## 在您完成之後

您可以在授權頁面上執行下列動作。

- 按一下**匯出**圖示 ( )，將一個或多個特定授權啟動金鑰下載至本端系統。

  **附註：**匯出多個授權啟動金鑰時，檔案將以單一 ZIP 檔案下載。
- 按一下**刪除**圖示 ( ) 以刪除特定授權啟動金鑰。
- 按一下頁面頂端的**編輯**按鈕以配置授權警告期間。授權警告期間是 XClarity Administrator 觸發警告到授權到期前的天數。

### 取得協助

- 如果您是向事業夥伴訂購而有任何問題，請聯絡您的事業夥伴以查證交易與啟用狀況。
- 如果您未收到電子權利證明、授權碼或啟動金鑰，或是郵件誤寄給了其他人，請根據您的所在地聯絡區域代表。
  — ESDNA@lenovo.com（北美地區）
  — ESDAP@lenovo.com（亞太地區）
  — ESDEMEA@lenovo.com（歐洲、中東暨非洲地區）

— ESDLA@lenovo.com（拉丁美洲地區）
— ESDChina@Lenovo.com（中國）

- 如果有關權利的資訊有誤，請傳送電子郵件至 SW_override@lenovo.com 聯絡 Lenovo 支援中心，並在其中包含下列資訊：
  — 訂購號碼
  — 您的聯絡資訊，包括電子郵件位址。
  — 您的郵寄地址
  — 您要進行的變更
- 如果您對下載授權有任何問題或疑問，請傳送電子郵件至 -eSupport_-_Ops@lenovo.com 聯絡 Lenovo 支援中心。

# 第 7 章　將 XClarity Administrator 做為容器更新

將 Lenovo XClarity Administrator 做為容器執行時，請使用此更新程序安裝最新軟體以做為新容器，並將原始容器的磁區連結至新容器。

## 開始之前

若要將 XClarity Administrator 做為 Docker 容器從 **v4.0** 更新到 **v4.1**，請參閱將 XClarity Administrator 做為容器從 v4.0 更新到 v4.1。

您無法將舊版的 XClarity Administrator 做為 Docker 容器更新到 XClarity Administrator **v4.0**。您必須安裝 XClarity Administrator **v4.0** 的*完整映像檔*（請參閱安裝 Lenovo XClarity Administrator）。

若要使用 Lenovo XClarity Orchestrator 管理 XClarity Administrator **v4.0** 或更新版本實例，需要使用 XClarity Orchestrator **v2.0** 或更新版本。如果要將 XClarity Administrator 更新到 v4.0 或更新版本，請確保 XClarity Orchestrator 已是 v2.0 或更新版本。

## 關於此作業

`docker-compose.yml` 檔案使用下列環境變數，這些變數是您在安裝*原始*容器的期間所設定。新容器也使用這些環境變數。

- **CONTAINER_NAME**。唯一的容器名稱，用於為每個 XClarity Administrator 實例建立 Docker 磁區（例如，`CONTAINER_NAME=LXCA-203`）

  XClarity Administrator 使用容器名稱為容器建立磁區。如果為新容器使用相同的容器名稱，則新的 XClarity Administrator 實例將使用相同的磁區，因此可以存取與原始 XClarity Administrator 實例（容器）相同的系統資料和設定。

  如果變更容器名稱，則會為容器建立新磁區，而新的 XClarity Administrator 實例將無法存取與原始 XClarity Administrator 實例（容器）相同的系統資料和設定。如果您需要變更容器名稱或 IP 位址，請在安裝新容器之前備份原始 XClarity Administrator 實例的系統資料和設定，然後使用該備份在新容器中還原系統資料和設定。

- **ADDRESS**。容器的靜態 IPv4 或 IPv6 位址（例如，`ADDRESS=192.0.2.0`）

  管理裝置後變更 XClarity Administrator 的 IP 位址可能導致 XClarity Administrator 中的裝置處於離線狀態。請確定變更 IP 位址之前，已解除管理所有裝置。

- **BACKUP_MOUNT** 和 **FIRMWARE_MOUNT**。（選用）可用於儲存 XClarity Administrator 備份或用來做為韌體更新遠端儲存庫的遠端共用路徑。路徑必須分別為 `/mnt/backup_share` 和 `/mnt/fw_share`。

**附註：**XClarity Administrator *不是*做為特殊權限容器執行。

## 程序

若要更新 XClarity Administrator 容器，請完成下列步驟。

步驟 1. 從 XClarity Administrator 下載網頁將 XClarity Administrator 容器映像檔下載到用戶端工作站。登入網站，然後使用提供給您的存取金鑰以下載映像檔。

步驟 2. 透過執行下列指令，將 XClarity Administrator 容器映像檔匯入 Docker 主機。
```
docker load -i lnvgy_sw_lxca_110-3.5.0_anyos_noarch
```

步驟 3. 編輯用於原始容器的同一個 `docker-compose.yml`。更新檔案頂部的映像檔內容，以指向步驟 2 中的新 Docker 映像檔。您可以使用 `docker tag` 指令變更映像檔標記。

以下顯示 yml 檔案的範例。

© Copyright Lenovo 2022

```
version: '3.8'

services:

 lxca:
  image: lenovo/lxca:lnvgy_sw_lxca_container_111-4.0.0_anyos_noarch
  container_name: ${CONTAINER_NAME}
  tty: true
  stop_grace_period: 60s
  volumes:
   # Bind mount remote shares to the container
   - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
   - /home/<<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
   # Docker volume mount
   - data:/opt/lenovo/lxca/data
   - postgresql:/var/lib/postgresql/data
   - log:/var/log
   - confluent-etc:/etc/confluent
   - confluent-log:/var/log/confluent
   - confluent:/var/lib/confluent
   - propconf:/opt/lenovo/lxca/bin/conf
  networks:
   lan:
    ipv4_address: ${ADDRESS}

volumes:
 data:
  name: ${CONTAINER_NAME}-data
 postgresql:
  name: ${CONTAINER_NAME}-postgresql
 log:
  name: ${CONTAINER_NAME}-log
 confluent-etc:
  name: ${CONTAINER_NAME}-confluent-etc
 confluent-log:
  name: ${CONTAINER_NAME}-confluent-log
 confluent:
  name: ${CONTAINER_NAME}-confluent
 propconf:
  name: ${CONTAINER_NAME}-propconf

networks:
 lan:
  name: lan
  driver: macvlan
  driver_opts:
   parent: eth0
  ipam:
   config:
    - subnet: 192.0.0.0/19
      gateway: 192.0.30.1
```

步驟 4. 透過執行下列指令將*原始*容器關機。

```
docker-compose -p ${CONTAINER_NAME} down
```

步驟 5. 透過執行下列指令在 Docker 中部署*新*映像檔，其中 *<ENV_FILENAME>* 是環境變數檔案的名稱。

```
COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d
```

## 將 XClarity Administrator 做為容器從 v4.0 更新到 v4.1

將 Lenovo XClarity Administrator 做為 Docker 容器執行時，請使用此更新程序安裝最新軟體以做為新容器，並將原始容器的磁區連結至新容器。

### 開始之前

將 XClarity Administrator 做為容器從 v4.0 更新到 v4.1 時，需要使用特殊的更新指令碼使某些非持續性檔案持久化。

更新完成後，日誌層級會還原為預設值。

確保主機系統上存在非 Root Linux 使用者，而且該非 Root 使用者可以執行 Docker 指令。如果沒有，請透過執行下列指令將使用者新增到 Docker 群組。

```
bash
sudo groupadd docker
sudo gpasswd -a $USER docker
newgrp docker
docker ps
```

### 關於此作業

**附註：**XClarity Administrator *不是*做為特殊權限容器執行。

### 程序

若要更新 XClarity Administrator 容器，請完成下列步驟。

步驟 1. 切換到 Docker 群組中的非 Root 使用者。

步驟 2. 從 XClarity Administrator 下載網頁將 XClarity Administrator 容器映像檔（`do-container-update.sh`、`docker-compose.env`、`docker-compose.yml`、`lnvgy_sw_lxca_*.tar.gz`）下載到本端系統的新目錄中。登入網站，然後使用提供給您的存取金鑰以下載映像檔。

步驟 3. 透過執行下列指令，將 XClarity Administrator 容器映像檔匯入 Docker 主機。

```
docker load -i <CONTAINER-IMAGE-FILENAME>
```

例如：

```
docker load -i lnvgy_sw_lxca_110-4.1.0_anyos_noarch
```

步驟 4. 編輯*新的* `docker-compose.env` 檔案，更新以下環境變數以符合*原始* `docker-compose.env` 檔案中的值。

以下是環境檔案的範例。

```
CONTAINER_NAME="LXCA-400"
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

步驟 5. 編輯*新的* `docker-compose.yml` 檔案。將檔案頂部的 **image** 內容更新為新的 Docker 映像檔的檔案名稱，並更新網路配置設定（子網路、閘道和 DNS）以符合*原始* `docker-compose.yml` 檔案中的值。

以下顯示 yml 檔案的範例。

```
version: '3.8'

services:
```

```
  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan:
        ipv4_address: ${ADDRESS}
    dns: 192.0.30.10
         192.0.30.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

volumes:
  data:
    name: ${CONTAINER_NAME}-data
  postgresql:
    name: ${CONTAINER_NAME}-postgresql
  log:
    name: ${CONTAINER_NAME}-log
  confluent-etc:
    name: ${CONTAINER_NAME}-confluent-etc
  confluent-log:
    name: ${CONTAINER_NAME}-confluent-log
  confluent:
    name: ${CONTAINER_NAME}-confluent
  propconf:
    name: ${CONTAINER_NAME}-propconf
  ssh:
    name: ${CONTAINER_NAME}-ssh
  xcat:
    name: ${CONTAINER_NAME}-xcat
networks:
  lan:
    name: lan
    driver: macvlan
    driver_opts:
      parent: eth0
    ipam:
      config:
        - subnet: 192.0.0.0/19
          gateway: 192.0.30.1
```

步驟 6. 透過執行以下指令升級 Docker 中的容器映像檔，其中 *<ORIGINAL-CONTAINER-IMAGE-PATH>* 是原容器檔案的位置，*<NEW-CONTAINER-IMAGE-PATH>* 是您在步驟 2 中下載的新容器映像檔的位置。

```
bash do-container-update.sh <ORIGINAL-CONTAINER-IMAGE-PATH> <NEW-CONTAINER-IMAGE-PATH>
```

例如：

```
bash do-container-update.sh /home/$USER/lxca-400 /home/$USER/lxca-410
```

**附註：**在升級程序期間，系統會提示您輸入 `sudo` 指令的密碼。您必須輸入密碼才能繼續。

# 第 8 章 解除安裝 XClarity Administrator

完成這些步驟以解除安裝 Lenovo XClarity Administrator 虛擬裝置或容器。

## 程序

若要解除安裝 XClarity Administrator 虛擬裝置，請完成下列步驟。

步驟 1. 解除管理目前由 XClarity Administrator 管理的所有裝置（請參閱 XClarity Administrator 線上文件中的管理機箱、管理伺服器和管理交換器）。

步驟 2. 根據作業系統解除安裝 XClarity Administrator：

- **Docker-compose**執行下列指令以停止容器並移除網路和磁區。
  `docker-compose down -v`
- **CentOS、Red Hat、Rocky 和 Ubuntu**
  1. 使用虛擬機器管理員連線至主機。
  2. 用滑鼠右鍵按一下虛擬機器，然後按一下**關機 → 強制關機**。
  3. 再次用滑鼠右鍵按一下虛擬機器，然後按一下**刪除**。刪除確認對話框隨即顯示。
  4. 選取所有勾選框，然後按一下**刪除**。
- **ESXi**
  1. 透過 VMware vSphere Client 連線至主機。
  2. 用滑鼠右鍵按一下虛擬機器，然後按一下**電源 → 關閉電源**。
  3. 再次用滑鼠右鍵按一下虛擬機器，然後按一下**從磁碟刪除**。
- **Hyper-V**
  1. 在「伺服器管理員儀表板」中按一下 **Hyper-V**。
  2. 用滑鼠右鍵按一下伺服器，然後按一下 **Hyper-V 管理員**。
  3. 用滑鼠右鍵按一下虛擬機器，然後按一下**關機**。
  4. 再次用滑鼠右鍵按一下虛擬機器，然後按一下**刪除**。

© Copyright Lenovo 2022