适用于 Docker 环境的 Lenovo XClarity Administrator 规划和安装指南

版本 4.0.0

注

使用此信息及其支持的产品之前，请阅读一般声明和法律声明（位于 **XClarity Administrator** 在线文档）。

第一版 (2023 年 2 月)

目录

图

表

更改摘要

Lenovo XClarity Administrator 管理软件的后续版本支持新硬件，并提供软件增强功能和修订。

有关修订的信息，请参阅更新包中提供的变更历史记录文件（***.chg**）。

有关所有支持的硬件（包括服务器、机箱和 **Flex** 交换机）的信息，请参阅硬件和软件先决条件。

有关早期版本中的更改的信息，请参阅 **XClarity Administrator** 在线文档中的新增功能。

此版本支持以下硬件。

- **机箱和设备**
  - **ThinkAgile HX630 V3（7D6M）**
  - **ThinkAgile HX645 V3（7D9M）**
  - **ThinkAgile HX650 V3（7D6N）**
  - **ThinkAgile HX665 V3（7D9N）**
  - **ThinkAgile MX630 V3（7D6U）**
  - **ThinkAgile MX650 V3（7D6S）**
  - **ThinkAgile VX630 V3（7D6X、7Z63）**
  - **ThinkAgile VX635 V3（7D9V）**
  - **ThinkAgile VX645 V3（7D9K）**
  - **ThinkAgile VX650 V2-DPU（7Z63）**
  - **ThinkAgile VX650 V3（7D6W）**
  - **ThinkAgile VX650 V3-DPU（7D6W）**
  - **ThinkAgile VX655 V3（7D9W）**
  - **ThinkAgile VX665 V3（7D9L）**
  - **ThinkAgile VX850 V3（7DDK）**
  - **ThinkEdge SE350 V2（7DA9）**
  - **ThinkEdge SE455 V3（7DBY）**
  - **ThinkEdge SE360 V2（7DAM）**
  - **ThinkSystem SD555 V3（7DDP、7DDQ）**
  - **ThinkSystem SD650 V3（7D7M）**
  - **ThinkSystem SD650-I V3（7D7L）**
  - **ThinkSystem SD650-N V3（7D7L）**
  - **ThinkSystem SD665 V3（7D9P）**
  - **ThinkSystem SD665-N V3（7DAZ）**
  - **ThinkSystem SR630 V3（7D72、7D73、7D74）**
  - **ThinkSystem SR635 V3（7D9G、7D9H）**
  - **ThinkSystem SR645 V3（7D9C、7D9D）**
  - **ThinkSystem SR650 V3（7D75、7D76、7D77）**
  - **ThinkSystem SR655 V3（7D9E、7D9F）**
  - **ThinkSystem SR665 V3（7D9B、7D9A）**
  - **ThinkSystem SR675 V3（7D9Q、7D9R）**
  - **ThinkSystem SR850 V3（7D96、7D97、7D98）**
  - **ThinkSystem SR860 V3（7D93、7D94、7D95）**
  - **ThinkSystem SR950 V3（7DC4、7DC5、7DC6）**
  - **ThinkSystem ST650 V3（7D7A、7D7B）**

- **存储设备**
  - **ThinkSystem DE6400F 全闪存阵列（7DB6）**
  - **ThinkSystem DE6400H 混合闪存阵列（7DB6）**
  - **ThinkSystem DE6600F 全闪存阵列（7DB7）**
  - **ThinkSystem DE6600H 混合闪存阵列（7DB7）**
- **交换机**
  - **ThinkSystem DB730S FC SAN 交换机（7D9J）**
  - **ThinkSystem DB400D FC SAN Director（6684）**
  - **ThinkSystem DB800D FC SAN Director（6682）**

此版本支持以下适用于管理软件的规划和安装增强功能。

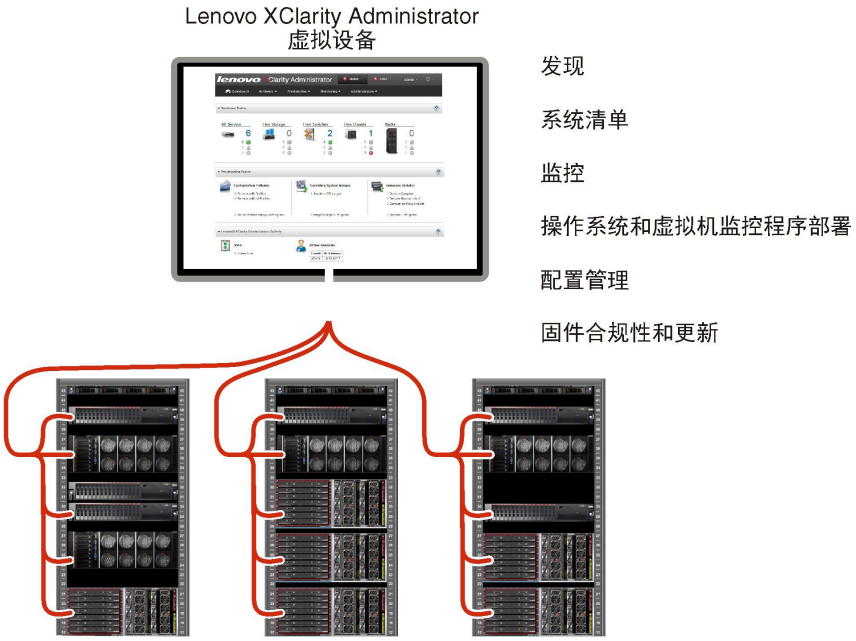
函数	描述
规划和安装	从支持的主机密钥算法列表中删除了 **ssh-rsa**，并添加了 **ssh-ed25519**、**ecdsa-sha2-nistp256**、**ecdsa-sha2-nistp384** 和 **ecdsa-sha2-nistp521**（请参阅加密管理）。

第 1 章　Lenovo XClarity Administrator 概述

Lenovo XClarity Administrator 是一种集中式资源管理解决方案，可简化基础结构管理、加快响应和提高 **Lenovo®** 服务器系统和解决方案的可用性。它在安全环境中以虚拟设备的形式运行，可自动发现、清点、跟踪、监控和配置服务器、网络和存储硬件。

了解更多：

- **XClarity Administrator：如管理软件般 管理硬件**
- **XClarity Administrator：概述**



XClarity Administrator 提供一个集中式界面，从中可对所有受管设备执行以下功能。

硬件管理

XClarity Administrator 可免代理进行硬件管理。它可自动发现可管理的设备，包括服务器、网络和存储硬件。它会收集受管设备的清单数据，使受管硬件清单及状态一目了然。

所支持的每个设备均有多种管理任务，包括查看状态和属性、配置系统和网络设置、启动管理界面、打开和关闭电源以及远程控制。有关管理设备的详细信息，请参阅 **XClarity Administrator** 在线文档中的管理机箱、管理服务器和管理交换机。

提示：可由 **XClarity Administrator** 管理的服务器、网络和存储硬件称为*设备*。处于 **XClarity Administrator** 管理之下的硬件称为*受管设备*。

可在 **XClarity Administrator** 中使用机架视图将受管设备进行分组，以反映数据中心内真实的机架安装情况。有关机架的详细信息，请参阅 **XClarity Administrator** 在线文档中的管理机架。

了解更多：

- **XClarity Administrator：发现**

- XClarity Administrator：清单
- XClarity Administrator：远程控制

硬件监控

XClarity Administrator 可集中查看从受管设备生成的所有事件和警报。事件或警报将传递到 XClarity Administrator，并显示在事件或警报日志中。可从仪表板和状态栏中查看所有事件和警报的摘要。可从特定设备的“警报和事件详细信息”页面获取该设备的事件和警报。

有关监控硬件的详细信息，请参阅 XClarity Administrator 在线文档中的使用事件和使用警报。

了解更多： XClarity Administrator：监控

配置管理

可使用一致的配置快速配置和预先配置所有服务器。配置设置（如本地存储、I/O 适配器、引导设置、固件、端口以及管理控制器和 UEFI 设置）保存为 Server Pattern，可应用于一个或多个受管服务器。更新 Server Patterns 后，这些更改将自动部署到所应用的服务器。

Server Patterns 还支持将 I/O 地址虚拟化，因此可将 Flex System 构造连接虚拟化，或改变服务器用途而不中断构造。

有关配置服务器的详细信息，请参阅 XClarity Administrator 在线文档中的使用 XClarity Administrator 配置服务器。

了解更多：
- XClarity Administrator：从裸机到集群
- XClarity Administrator：Configuration Pattern

固件合规性和更新

通过将固件合规性策略分配给受管设备，简化固件管理。创建合规性策略并将其分配给受管设备时，XClarity Administrator 监控对这些设备的清单作出的更改，并标记任何不合规的设备。

当设备不合规时，可使用 XClarity Administrator 从所管理的固件更新的存储库为该设备中的所有设备应用并激活固件更新。

注：刷新存储库和下载固件更新需要 Internet 连接。如果 XClarity Administrator 未连接到 Internet，则可手动将固件更新导入到存储库。

有关更新固件的详细信息，请参阅 XClarity Administrator 在线文档中的更新受管设备上的固件。

了解更多：
- XClarity Administrator：从裸机到集群
- XClarity Administrator：固件更新
- XClarity Administrator：配置固件 安全更新

操作系统部署

可使用 XClarity Administrator 管理操作系统映像的存储库以及同时将操作系统映像部署到多达 28 个受管服务器。

有关部署操作系统的详细信息，请参阅 XClarity Administrator 在线文档中的部署操作系统映像。

了解更多：

- XClarity Administrator：从裸机到集群
- XClarity Administrator：操作系统部署

用户管理

XClarity Administrator 提供一个集中认证服务器以创建和管理用户帐户以及管理和认证用户凭证。首次启动管理软件时，将自动创建该认证服务器。为 XClarity Administrator 创建的用户帐户还可用于以受管认证模式登录到受管机箱和服务器。有关用户的详细信息，请参阅 XClarity Administrator 在线文档中的管理用户帐户。

XClarity Administrator 支持三种类型的认证服务器：

- **本地认证服务器**。默认情况下，将 XClarity Administrator 配置为使用位于管理节点上的本地认证服务器。
- **外部 LDAP 服务器**。目前，仅支持 Microsoft Active Directory。此服务器必须位于连接到管理网络的外侧 Microsoft Windows Server 上。当使用外部 LDAP 服务器时，将禁用本地认证服务器。
- **外部 SAML 2.0 身份提供商**。目前，仅支持 Microsoft Active Directory 联合身份验证服务（AD FS）。除了输入用户名和密码之外，还可设置多重认证，通过要求输入 PIN 码、读取智能卡和客户端证书而增强安全性。

有关认证类型的详细信息，请参阅 XClarity Administrator 在线文档中的“管理认证服务器”。

创建用户帐户时，将向该用户帐户分配预定义或定制的角色组以控制该用户的访问级别。有关角色组的详细信息，请参阅 XClarity Administrator 在线文档中的创建角色组。

XClarity Administrator 包括一个审核日志，其中提供用户操作（如登录、创建新用户或更改用户密码）的历史记录。有关审核日志的详细信息，请参阅 XClarity Administrator 在线文档中的使用事件。

设备认证

XClarity Administrator使用以下方法向受管机箱和服务器进行认证。

- **受管认证**。启用了受管认证后，在 XClarity Administrator 中创建的用户帐户用于对受管机箱和服务器进行认证。

  有关用户的详细信息，请参阅 XClarity Administrator 在线文档中的管理用户帐户。
- **本地认证**。启用受管认证后，在 XClarity Administrator 中创建的存储的凭证将用于对受管服务器进行认证。存储的凭证必须对应于设备上或 Active Directory 中的活动用户帐户。

  有关存储的凭证的详细信息，请参阅 XClarity Administrator 在线文档中的管理存储的凭证。

安全性

如果所处环境必须符合 NIST SP 800-131A 标准，则 XClarity Administrator 可帮助实现环境完全合规。

XClarity Administrator 支持自签名 SSL 证书（由内部证书颁发机构颁发）和外部 SSL 证书（由私有或商业 CA 颁发）。

可配置机箱和服务器上的防火墙，使其仅接受来自 XClarity Administrator 的传入请求。

有关安全性的详细信息，请参阅 XClarity Administrator 在线文档中的实现安全环境。

服务与支持

可设置 XClarity Administrator，使其在 XClarity Administrator 和受管设备中发生某些可维护事件时自动收集诊断文件并发送到首选服务提供商。可选择将诊断文件使用 Call Home 发送到 Lenovo Support 或使用 SFTP 发送到其他服务提供商。也可手动收集诊断文件，开立问题记录，然后将诊断文件发送到 Lenovo 支持中心。

了解更多： XClarity Administrator：服务与支持

使用脚本自动执行任务

XClarity Administrator 可通过开放式 REST 应用程序编程接口（API）集成到外部、更高级别的管理和自动化平台。使用 REST API，XClarity Administrator 可轻松地与现有的管理基础结构集成。

PowerShell 工具包提供一个 cmdlet 库，用于从 Microsoft PowerShell 会话中自动执行配置和资源管理。Python 工具包提供一个基于 Python 的命令和 API 库，用于从 OpenStack 环境（例如 Ansible 或 Puppet）自动执行配置和资源管理。这两个工具包均提供一个访问 XClarity Administrator REST API 的接口以便自动执行如下功能：

- 登录到 XClarity Administrator
- 管理和终止管理机箱、服务器、存储设备和架顶交换机（设备）
- 收集和查看设备和组件的清单数据
- 将操作系统映像部署到一个或多个服务器
- 使用 Configuration Patterns 配置服务器
- 将固件更新应用到设备

与其他受管软件集成

XClarity Administrator 模块将 XClarity Administrator 与第三方管理软件集成，可提供发现、监控、配置和管理功能，从而降低对支持的设备进行日常系统管理所需的成本和复杂性。

有关 XClarity Administrator 的详细信息，请参阅以下文档：

- 适用于 Microsoft System Center 的 Lenovo XClarity Integrator
- 适用于 VMware vCenter 的 Lenovo XClarity Integrator

有关其他注意事项，请参阅管理注意事项。

了解更多：

- 适用于 Microsoft System Center 的 Lenovo XClarity Integrator 概述
- 适用于 VMware vCenter 的 Lenovo XClarity Integrator

文档

XClarity Administrator 文档为英文，并定期在线更新。有关最新信息和过程，请参阅XClarity Administrator 在线文档。

在线文档提供以下语言版本：

- 德语（de）
- 英语（en）
- 西班牙语（es）
- 法语（fr）
- 意大利语（it）

- 日语（**ja**）
- 韩语（**ko**）
- 巴西葡萄牙语（**pt_BR**）
- 俄语（**ru**）
- 泰语（**th**）
- 简体中文（**zh_CN**）
- 繁体中文（**zh_TW**）

可通过以下方式更改在线文档的语言：

- 在 **Web** 浏览器中更改语言设置
- 将 ?lang=*<language_code>* 添加到 **URL** 末尾，例如，要显示简体中文的在线文档：
  http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/aug_product_page.html?**lang=zh_CN**

第 2 章　规划 XClarity Administrator

安装 **Lenovo XClarity Administrator** 之前，请仔细研究以下注意事项以帮助您规划安装和日常管理。

许可证和 90 天免费试用

Lenovo XClarity Administrator 提供一个免费的 **90** 天试用许可证，可用于在一段有限的时间内充分使用所有可用功能。

可通过单击 **XClarity Administrator** 标题栏中的用户操作菜单（  ），然后单击**关于**，确定许可证状态，包括试用许可证还剩多少天。

XClarity Administrator 支持以下许可证。

- **Lenovo XClarity Pro**。每个许可证为一台设备提供以下权利。
  - **Lenovo XClarity Integrator** 服务与支持
  - **XClarity Administrator** 服务与支持
  - **XClarity Administrator** 的高级功能：
    - 使用 **Configuration Patterns** 配置服务器
    - 部署操作系统
    - 使用 **Call Home** 报告 **XClarity Administrator** 问题（用于硬件警报的 **Call Home** 不受影响。）

必须为每个支持高级功能的受管设备购买许可证。许可证未 与特定设备绑定。

许可证的合规性由支持高级功能的受管设备数量来决定。受管设备数量不得超过所有有效许可证密钥中的许可证总数。如果 **XClarity Administrator** 不符合已安装的许可证（例如，许可证过期或管理的其他设备数量超出有效许可证总数），您将有 **90** 天的宽限期来安装合适的许可证。只要 **XClarity Administrator** 不合规，宽限期都将恢复为 **90** 天。如果宽限期（包括免费试用）在许可证合规之前结束，则将禁用所有设备的高级功能。

注：

- 宽限期过后，服务器配置和操作系统部署功能会被禁用。
- 许可证不合规时，会禁用针对 **XClarity Administrator** 问题的 **Call Home**（软件 **Call Home** 功能）。该功能没有宽限期。但是，用于硬件警报的 **Call Home** 不受影响。

如果已安装许可证，那么在升级到 **XClarity Administrator** 新版本时*不*需要新许可证。

有关购买 **Lenovo XClarity Pro** 许可证的信息，请与 **Lenovo** 代表或授权业务合作伙伴联系。

有关安装许可证的信息，请参阅安装启用全功能的许可证（位于 **XClarity Administrator** 在线文档）。

硬件和软件先决条件

Lenovo XClarity Administrator 管理设备在主机系统上的虚拟机中运行。

虚拟机监控程序要求

容器环境

在将 XClarity Administrator 作为容器运行时支持以下容器环境。

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

虚拟机监控程序

在将 XClarity Administrator 作为虚拟设备运行时支持以下虚拟机监控程序。

- Citrix Hypervisor 8.2
- Citrix XenServer v7.6
- CentOS 7 和 8[1]
- 装有 Hyper-V 的 Microsoft Windows Server 2022
- 装有 Hyper-V 的 Microsoft Windows Server 2019
- 装有 Hyper-V 的 Microsoft Windows Server 2016
- 装有 Hyper-V 的 Microsoft Windows Server 2012 R2
- 装有 Hyper-V 的 Microsoft Windows Server 2012
- Nutanix Acropolis 虚拟机监控程序（AHV）
- 装有基于内核的虚拟机（KVM）v2.12.0 的 Red Hat v8.x
- 装有 KVM v1.2.17 的 Red Hat v7.x
- 装有 KVM v4.2.3 的 Ubuntu 20.04.2 LTS
- VMware ESXi 7.0、U1、U2 和 U3
- VMware ESXi 6.7、U1、U2[2] 和 U3

注：

1. Red Hat 不再更新 CentOS Linux。考虑迁移到 Red Hat Enterprise Linux（请参阅 Red Hat：如何从 CentOS 或 Oracle Linux 转换为 RHEL 网页）。
2. 对于 VMware ESXi 6.7 U2，必须使用 ISO 映像 VMware-ESXi-6.7.0.update02-13981272-LNV-20190630.iso 或更高版本。

对于 VMware 和 Citrix，虚拟机为 OVF 模板。对于 Hyper-V 和 Nutanix AHV，虚拟机为虚拟磁盘映像（VHD）。对于 CentOS 和 KVM，虚拟机以 qcow2 格式提供。

重要：对于在内核为 2.6 的 Linux 来宾上运行并将大量内存用于虚拟设备的 Hyper-V 环境，必须从 Hyper-V Manager 的 Hyper-V 设置面板上禁止使用非统一内存访问（NUMA）。更改此设置需要重新启动 Hyper-V 服务，而这还将重新启动所有正在运行的虚拟机。如果未禁用此设置，则 XClarity Administrator 虚拟设备可能会在初始启动期间遇到问题。

硬件要求

XClarity Administrator 必须满足以下*最低要求*。根据环境的大小和所使用的 Configuration Patterns，可能需要其他资源才能达到最佳性能。

- 两个虚拟微处理器
- 8 GB 内存
- 192 GB 的存储空间供 XClarity Administrator 虚拟设备使用。
- 以 1024 像素（宽度）的最小分辨率显示（XGA）

以下表格列出了指定设备数量对应的建议最低配置。请注意，运行最低配置时，管理任务持续的时间可能长于预期完成时间。对于配置任务（如操作系统部署、固件更新和服务器配置），可能需要临时增加资源。

受管设备数	虚拟 CPU/内存配置
0 - 100 个设备	2 个 vCPU，8 GB RAM
100 - 200 个设备	4 个 vCPU，10 GB RAM
200 - 400 个设备	6 个 vCPU，12 GB RAM
400 - 600 个设备	8 个 vCPU，16 GB RAM
600 - 800 个设备	10 个 vCPU，20 GB RAM
800 - 1000 个设备	12 个 vCPU，24 GB RAM

注：

- 一个 XClarity Administrator 实例最多可支持 1000 个设备。
- 有关最新建议和其他性能注意事项，请参阅《XClarity Administrator：性能指南》（白皮书）。
- 根据受管环境的大小和安装时使用的 pattern，可能需要添加资源来确保性能处于可接受范围内。如果系统资源仪表板内的处理器使用情况频繁显示较高或非常高的值，请考虑添加 1 - 2 个虚拟处理器核。如果空闲时的内存使用情况持续超过 80%，请考虑添加 1 - 2 GB RAM。如果系统以表格中定义的配置运行时能迅速响应，请考虑延长虚拟机的运行时间，以评估系统性能。
- 有关如何通过删除不再需要的 XClarity Administrator 资源而释放磁盘空间的信息，请参阅 XClarity Administrator 在线文档中的管理磁盘空间。

软件要求

- **Orchestrator 服务器**

  如果您使用多个 XClarity Administrator 实例管理大量设备，则可以使用 Lenovo XClarity Orchestrator 集中进行监控、管理、配置和分析。XClarity Orchestrator 可以支持不限数量的 XClarity Administrator 实例，这些实例总共可管理多达 10000 个非 ThinkEdge 客户端设备。

  要使用 Lenovo XClarity Orchestrator 管理 XClarity Administrator v4.0 或更高版本的实例，需要安装 XClarity Orchestrator v2.0 或更高版本。

- **认证服务器**

  如果选择使用外部认证服务器，则仅支持 Windows Server 2008 或更高版本上运行的 Microsoft Active Directory。

  如果选择使用 SAML 身份提供商，则仅支持 Windows Server 2012 上运行的 Microsoft Active Directory 联合身份验证服务（AD FS） 版本 2.0 或更高版本。

- **NTP 服务器**

  需要网络时间协议（NTP）服务器以确保从受管设备收到的所有事件和警报的时间戳与 XClarity Administrator 同步。确保可通过管理网络（通常为 Eth0 接口）访问 NTP 服务器。

  提示：考虑使用装有 XClarity Administrator 的主机系统作为 NTP 服务器。如果这样做，则确保可通过管理网络访问主机系统。

可管理的资源

单个 XClarity Administrator 实例可以管理、监控和配置最多 1000 个物理设备。

可从 “XClarity Administrator 支持 – 兼容性” Web 页面中单击 Compatibility（兼容性）选项卡，然后单击相应设备类型的链接，查找支持的设备和选件（例如 I/O、DIMM 和存储适配器）、所需的最低固件级别和限制注意事项的完整列表。

有关特定设备的硬件配置和选项的常规信息，请参阅Lenovo Server Proven 网页。

限制：如果装有 XClarity Administrator 的主机系统为受管机架服务器或计算节点，则无法使用 XClarity Administrator 将固件更新应用于该主机系统或一次应用于整个机箱。将固件更新应用于主机系统后，必须重新启动主机系统。重新启动主机系统还将重新启动 XClarity Administrator，使 XClarity Administrator 无法在主机系统上完成更新。

支持的 Web 浏览器

XClarity Administrator Web 界面可与以下 Web 浏览器搭配使用。

- Chrome™ 48.0 或更高版本（对于远程控制台，使用 55.0 或更高版本）
- Firefox® ESR 38.6.0 或更高版本
- Microsoft® Internet Explorer® 11
- Microsoft Edge
- Safari® 9.0.2 或更高版本（iOS7 或更高版本和 OS X）

防火墙和代理服务器

Lenovo XClarity Administrator 的某些功能（包括管理软件更新、固件更新、维护和支持）需要访问 Internet。如果网络中有防火墙，请配置防火墙以允许 XClarity Administrator 管理软件执行上述操作。如果管理软件没有 Internet 直接访问权限，请配置 XClarity Administrator 以使用代理服务器。

防火墙

确保防火墙开放了以下 DNS 名称和端口。

注：IP 地址可能发生变化。请尽可能使用 DNS 名称。

表 1. 需要 Internet 连接

DNS 名称	IPv4 地址	IPv6 地址	端口	协议
下载许可证激活密钥				
fod.lenovo.com	不适用	不适用	443	https
下载服务公告				
download.lenovo.com/servers/LXCA_Bulletin_Service.json	不适用	不适用	443 和 80	https
下载更新（管理软件更新、固件更新、UpdateXpress System Pack（操作系统设备驱动程序）和存储库包）				
datacentersupport.lenovo.com	不适用	不适用	443 和 80	https
download.lenovo.com	不适用	不适用	443 和 80	https
filedownload.lenovo.com	不适用	不适用	443 和 80	https
support.lenovo.com	不适用	不适用	443 和 80	https 和 http
supportapi.lenovo.com	不适用	不适用	443 和 80	https
下载固件（仅限 Flex System x220、x222、x240、x280 X6、x440、x480 X6、x880 X6、某些 Flex 交换机和第一代 CMM）				

表 1. 需要 Internet 连接 （续）

DNS 名称	IPv4 地址	IPv6 地址	端口	协议
www.ibm.com	129.42.56.216, 129.42.58.216, 129.42.60.216, 129.42.160.51, 207.25.252.197	不适用	443 和 80	https 和 http
www-03.ibm.com	204.146.30.17	不适用	443 和 80	https 和 http
download3.boulder.ibm.com	170.225.126.24	不适用	443	https
download4.boulder.ibm.com	170.225.126.43	不适用	443 和 80	https 和 http
delivery04-bld.dhe.ibm.com	170.225.126.45	不适用	443 和 80	https 和 http
delivery04-mul.dhe.ibm.com	170.225.126.46	不适用	443 和 80	https 和 http
delivery04.dhe.ibm.com	170.225.126.44	不适用	443 和 80	https 和 http
将服务数据上传到 Lenovo 支持中心（Call Home）				
soaus.lenovo.com	3.222.8.29, 52.6.14.20	不适用	443	https
logupload.lenovo.com/BLL/Logupload.ashx	不适用	不适用	443 和 80	https
将服务数据上传到 Lenovo 更新设施				
logupload.lenovo.com/BLL/Logupload.ashx	不适用	不适用	443 和 80	https
下载保修信息				
ibase.lenovo.com（全球）	不适用	不适用	443 和 80	https 和 http
service.lenovo.com.cn（仅限中国）	114.247.140.212（仅限中国）	不适用	83	http
supportapi.lenovo.com	不适用	不适用	443 和 80	https 和 http

注意：对于中国境内的用户，如要使用 XClarity Administrator 检索受管设备的保修信息，必须先升级到 XClarity Administrator v1.3.1 或更高版本。

代理服务器

如果管理软件没有 Internet 直接访问权限，请务必配置管理软件使用 HTTP 代理服务器（请参阅配置网络访问权限）。

- 确保代理服务器设置为使用基本认证。
- 务必将代理服务器设置为非终止代理。
- 务必将代理服务器设置为转发代理。
- 确保负载均衡器配置为保持与一个代理服务器之间的会话而不在二者之间切换。

端口可用性

根据在所处环境中实现防火墙的方式，有若干端口必须可用。如果所需的端口被阻止或由另一进程使用，则某些 **Lenovo XClarity Administrator** 功能可能不起作用。

要判断根据所处环境必须开放哪些端口，请参阅以下章节。这些章节中的表里包含了如下信息：**XClarity Administrator** 中如何使用各端口、受影响的受管设备、协议（**TCP** 或 **UDP**），以及流量传输方向。*入站* 流量标识从受管设备或外部系统到 **XClarity Administrator** 的流量，因此端口需要在 **XClarity Administrator** 设备上打开。*出站* 流量从 **XClarity Administrator** 传输到受管设备。

- 访问 **XClarity Administrator** 服务器
- 在 **XClarity Administrator** 与受管设备之间访问
- 在 **XClarity Administrator** 与数据网络之间访问，以便进行操作系统部署和设备驱动程序更新

访问 XClarity Administrator 服务器

如果 **XClarity Administrator** 服务器和所有受管设备在防火墙后，而您要从防火墙以外的浏览器访问这些设备，则必须确保这些 **XClarity Administrator** 端口开放。如果使用 **SNMP** 和 **SMTP** 进行事件管理，则可能还需要确保 **XClarity Administrator** 服务器用于事件转发的端口开放。

XClarity Administrator 服务器通过下表中列出的端口进行侦听和响应。

注：

- **XClarity Administrator** 是一个 **RESTful** 应用程序，使用端口 **443** 通过 **TCP** 进行安全通信。
- 可以选择将 **XClarity Administrator** 配置为建立与外部服务（如 **LDAP**、**SMTP** 或 **syslog**）的出站连接。这些连接可能需要未包含在该列表中的其他常规用户可配置端口。这些连接也可能需要在 **TCP** 或 **UDP** 端口 **53** 上访问域名服务（**DNS**）服务器以解析外部服务器名称。

通信	XClarity Administrator 设备	外部认证服务器	事件转发服务	Lenovo 服务（包含 Call Home）
出站（端口在外部系统上打开）	• **DNS – 端口 53 上的 TCP/UDP**	• **LDAP– 端口 389[1] 上的 TCP** • **LDAPS – 端口 636 上的 TCP** • **SAML 认证 – 端口 3268 和 3269 上的 TCP**	• **FTP 服务器 – 端口 21[1] 上的 TCP** • **电子邮件服务器（SMTP） – 端口 25[1] 上的 UDP** • **REST Web 服务（HTTP） – 端口 80[1] 上的 UDP** • **SNMP 管理器 – 端口 161[2] 和 162[1] 上的 UDP** • **MS Azure – 端口 443[1] 上的 UDP**	• **保修（仅限中国） – 端口 83[5] 上的 TCP** • **HTTPS（Call Home） – 端口 443 上的 TCP**

通信	XClarity Administrator 设备	外部认证服务器	事件转发服务	Lenovo 服务（包含 Call Home）
			• Syslog – 端口 514[1] 上的 UDP • Apple 推送[3] – 端口 443、2195 和 5223 上的 TCP • Google 推送[4] – 端口 443、5288、5299 和 5230 上的 TCP	
入站（端口在 XClarity Administrator 设备上打开）	• HTTPS – 端口 443 上的 TCP	不适用	• SNMP – 端口 161 上的 UDP	不适用

1. 这是默认端口。您可以从用户界面中配置此端口。
2. 在配置了具有用户认证的 SNMP 事件转发时使用此端口。
3. 当 Wi-Fi 位于防火墙或蜂窝数据专用接入点名称（APN）后方时，打开此端口。在此端口上需要以直接、无代理的方式连接到 APN 服务器。当设备无法在端口 5223 上访问 Apple 推送通知服务时，此端口仅用作 Wi-Fi 上的故障恢复端口。IP 地址范围是 17.0.0.0/8。
4. 有关 IP 地址范围，请参阅 Google ASN 15169。域为 android.googleapis.com。
5. 尽管在中国以外的国家/地区不需要，但 XClarity Administrator 可能会尝试在其他国家/地区连接到该服务。

在 XClarity Administrator 与受管设备之间访问

如果受管设备（如计算节点或机架服务器）在防火墙后，并且如果要从该防火墙以外的 XClarity Administrator 服务器管理这些设备，则必须确保 XClarity Administrator 与每个受管设备上的主板管理控制器之间进行通信所涉及的所有端口均开放。

如果要使用 XClarity Administrator 在受管设备上安装操作系统，请务必查看在 XClarity Administrator 与数据网络之间访问，以便进行操作系统部署和设备驱动程序更新中的端口列表。

- Flex 机箱 CMM

通信	Flex 机箱 CMM
出站（端口在外部系统上打开）	– SLP – 端口 427 上的 UDP/TCP – CIM HTTP – 端口 5988[2] 上的 TCP – CIM HTTPS – 端口 5989 上的 TCP – TCP 命令 – 端口 6090[2] 上的 TCP – Secure TCP command – 端口 6091 上的 TCP
入站（端口在 XClarity Administrator 设备上打开）	– SFTP – 端口 22[1] 上的 TCP – CIM 指示 HTTPS – 端口 9090 上的 TCP – LDAPS – 端口 50637 上的 TCP

1. 此端口用于通过 SFTP 传输固件更新。
2. 默认情况下，通过安全端口进行管理。非安全端口是可选的。

- **服务器和计算节点**

通信	ThinkSystem 和 ThinkAgile	System x	Flex System	ThinkServer
出站（端口在外部系统上打开）	– SFTP – 端口 115 上的 TCP – SLP – 端口 427 上的 UDP/TCP – HTTPS – 端口 443 上的 TCP – SSDP 发现 – 端口 1900 上的 UDP – 远程控制 – 端口 3888[4] 上的 TCP – 远程 KVM – 端口 3889[4] 上的 TCP – CIM HTTPS – 端口 5989 上的 TCP – 固件更新 – 端口 6990[5] 上的 TCP	– SLP – 端口 427 上的 UDP/TCP – HTTPS – 端口 443 上的 TCP – IPMI – 端口 623 上的 TCP – 远程控制 – 端口 3888[4] 上的 TCP – 远程 KVM – 端口 3889[4] 上的 TCP – CIM HTTP – 端口 5988[3] 上的 TCP – CIM HTTPS – 端口 5989[3] 上的 TCP – 固件更新 – 端口 6990[5] 上的 TCP	– SLP – 端口 427 上的 UDP/TCP – 远程控制 – 端口 3888[4] 上的 TCP – 远程 KVM – 端口 3889[1,4] 上的 TCP – CIM HTTP – 端口 5988[3] 上的 TCP – CIM HTTPS – 端口 5989[3] 上的 TCP – 固件更新 – 端口 6990[5] 上的 TCP	– SNMP 警报 – 端口 162 上的 UDP – IPMI – 端口 623 上的 UDP
入站（端口在 XClarity Administrator 设备上打开）	– SFTP – 端口 22[2] 上的 TCP – HTTPS – 端口 443 上的 TCP – SSDP 发现 – 端口 1900 上的 UDP – 固件更新 – 端口 6990[5] 上的 TCP – CIM 指示 HTTPS – 端口 9090 上的 TCP – LDAPS – 端口 50636[6] 和 50637 上的 TCP	– SFTP – 端口 22[2] 上的 TCP – HTTPS – 端口 443 上的 TCP – 固件更新 – 端口 6990[5] 上的 TCP – CIM 指示 HTTPS – 端口 9090 上的 TCP – LDAPS – 端口 50636[6] 和 50637 上的 TCP	– SFTP – 端口 22[2] 上的 TCP – HTTPS – 端口 443 上的 TCP – 固件更新 – 端口 6990[5] 上的 TCP – CIM 指示 HTTPS – 端口 9090 上的 TCP – LDAPS – 端口 50636[6] 和 50637 上的 TCP	– SNMP 警报 – 端口 162 上的 UDP

1. 此端口仅要求对带有 IMM2 的服务器开放。
2. 此端口用于通过 SFTP 传输固件更新。
3. 默认情况下，通过安全端口进行管理。非安全端口是可选的。
4. 远程控制和远程 KVM 是从 Web 浏览器启动，而不是从 XClarity Administrator 服务器启动。
5. 此端口用于连接到 BMU 操作系统，以传输文件和运行更新命令。
6. 使用 Configuration Patterns 配置服务器时需要此端口。

- **机架和 Flex 交换机**

通信	机架交换机	Flex 交换机
出站（端口在外部系统上打开）	– SSH – 端口 22[1, 3] 上的 TCP – SNMP – 端口 161[2] 上的 UDP – SLP – 端口 427[6] 上的 UDP/TCP – HTTPS – 端口 443[7] 上的 TCP	– SSH – 端口 22[3] 上的 TCP – SNMP – 端口 161[5] 上的 UDP
入站（端口在 XClarity Administrator 设备上打开）	– SFTP – 端口 22[4] 上的 TCP – SNMP 警报 – 端口 162[2] 上的 TCP	– SFTP – 端口 22[4] 上的 TCP – SNMP 警报 – 端口 162[2] 上的 TCP

1. 对于 ENOS 机架交换机而言，此端口用于在执行 SFTP 文件传输操作之前配置 CMM 和 Flex 交换机之间使用的栈头（HoS）凭证、激活固件插槽和清除 SSH 主机密钥。
2. 当交换机与 XClarity Administrator 不在同一网络时，此端口必须在 XClarity Administrator 设备上打开（入站），这样，XClarity Administrator 才能接收那些设备的事件。
3. 此端口用于管理（SSH）。
4. 此端口用于通过 SFTP 传输固件更新。
5. 对于 ENOS 机架交换机来说，此端口用于传输清单数据。
6. 此端口用于发现。
7. 此端口用于应用固件更新。

- **存储设备**

通信	存储设备
出站（端口在外部系统上打开）	– FTP – 端口 21 上的 TCP – SFTP – 端口 22[2] 上的 TCP – SLP – 端口 427 上的 UDP/TCP – HTTPS – 端口 443[1] 上的 TCP
入站（端口在 XClarity Administrator 设备上打开）	– HTTPS – 端口 443[2] 上的 TCP – SNMP 警报 – 端口 115 上的 UDP

1. 此端口用于传输固件更新。
2. 此端口用于传输和应用固件更新。

在 XClarity Administrator 与数据网络之间访问，以便进行操作系统部署和设备驱动程序更新

通信	操作系统部署[1、2、3]	操作系统设备驱动程序更新[2]
出站（端口在外部系统上打开）		• WinRM over HTTP – 端口 5985[5] 上的 TCP • WinRM over HTTPS – 端口 5986[6] 上的 TCP
入站（端口在 XClarity Administrator 设备上打开）	• SMB 通信 – 端口 445 上的 TCP[4] • HTTPS（ThinkServer 除外）– 端口 8443[6] 上的 TCP	• SMB 通信 – 端口 445 上的 TCP[4]

1. 如果将 **XClarity Administrator** 配置为使用操作系统部署网络，则必须在该网络上打开端口。
2. 有关对于部署操作系统必须可用的端口的列表，请参阅 **XClarity Administrator** 在线文档中的“所部署的操作系统的端口可用性”。 例如，如果将操作系统配置为使用数据网络（**eth1**），则必须在连接到该网络时打开以下端口。
3. 每个 **XClarity Administrator** 实例有一个仅用于部署操作系统的唯一证书颁发机构（**CA**）。该 **CA** 会在端口 **8443** 上签署用于目标服务器的证书。开始执行操作系统部署后，该 **CA** 证书会被添加到要推送至目标服务器的操作系统映像中。在部署过程中，该服务器会连接回端口 **8443**，并在握手期间验证端口 **8443** 提供的证书，因为它们拥有该 **CA** 证书。
4. 此端口用于传输 **Windows** 驱动程序文件。
5. 此端口用于连接到目标服务器 **WinRM**。
6. 此端口用于在目标操作系统与 **XClarity Administrator** 之间交换数据（包括操作系统映像和状态）。

管理注意事项

管理设备时有多种备用方案可供选择。根据所管理的设备的不同，可能需要同时运行多种管理解决方案。

一个设备只能受 **Lenovo XClarity Administrator** 的一个实例管理。但是，可将其他管理软件（例如 **VMware vRealize Operations Manager**）与 **Lenovo XClarity Administrator** 一起用于*监控* **XClarity Administrator** 管理的设备。

注意：使用多个管理工具管理设备时，请务必小心，以避免意外冲突。例如，使用另一个工具提交电源状态更改可能会与 **XClarity Administrator** 中正在运行的配置或更新作业冲突。

ThinkSystem、ThinkServer 和 System x 设备

如果要使用另一个管理软件监控受管设备，请从 **IMM** 界面使用正确的 **SNMP** 或 **IPMI** 设置创建一个新的本地用户。确保授予 **SNMP** 或 **IPMI** 权限，具体取决于您的需求。

Flex System 设备

如果打算使用另一管理软件来监控受管设备，并且该管理软件使用 **SNMPv3** 或 **IPMI** 通信，则必须对每个受管 **CMM** 执行以下步骤来准备环境：

1. 可使用 `RECOVERY_ID` 用户名和帐户登录机箱的管理控制器 **Web** 界面。
2. 如果安全策略设置为**安全**，请更改用户认证方法。
   a. 单击**管理模块的管理 → 用户帐户**。
   b. 单击**帐户**选项卡。
   c. 单击**全局登录设置**。
   d. 单击**常规**选项卡。
   e. 选择**先进行外部认证，然后进行本地认证**的用户认证方法。
   f. 单击**确定**。
3. 从管理控制器 **Web** 界面中新建具有正确 **SNMP** 或 **IPMI** 设置的本地用户。
4. 如果安全策略设置为**安全**，请注销再使用新的用户名和密码来登录管理控制器 **Web** 界面。提示更改新用户的密码时，请照做。

现在可将新用户用作活动的 **SNMP** 或 **IPMI** 用户。

注：如果终止管理机箱再重新管理该机箱，则会锁定并禁用这个新用户帐户。在这种情况下，请重复这些步骤以创建新用户帐户。

网络注意事项

打算安装 **Lenovo XClarity Administrator** 时，请考虑所处环境中实现的网络拓扑以及 **XClarity Administrator** 如何融入该拓扑。

重要：配置设备和组件时尽量少更改 **IP** 地址。考虑使用静态 **IP** 地址代替动态主机配置协议（**DHCP**）。如果使用 **DHCP**，则务必尽量少更改 **IP** 地址。

IP 配置限制

对于以下功能和受管设备，必须为网络接口配置 **IPv4** 地址。不支持 **IPv6** 地址。

- **Lenovo Storage** 设备的固件更新
- **ThinkServer** 服务器
- **Lenovo Storage** 设备

不支持使用 **IPv6** 链路本地地址通过数据端口或管理端口来管理 **RackSwitch** 设备。

不支持网络地址转换（**NAT**，用于将一个 **IP** 地址空间映射到另一个中）。

网络类型

一般而言，大多数环境实现以下几种类型的网络。根据要求，可仅实现其中某个网络，也可实现全部三者。

- **管理网络**

  管理网络通常保留用于在 **Lenovo XClarity Administrator** 与受管设备的管理处理器之间进行通信。例如，可将管理网络配置为包括 **XClarity Administrator**、每个受管机箱的 **CMM**，以及 **XClarity Administrator** 管理的每个服务器的主板管理控制器。

- **数据网络**

  数据网络通常用于在服务器上安装的操作系统与公司内部网和/或 **Internet** 之间进行通信。

- **操作系统部署网络**

  在某些情况下，设置一个操作系统部署网络以隔离在服务器上部署操作系统所需的通信。如果实现了此网络，则其中通常包括 **XClarity Administrator** 和所有服务器主机。

  除了实现单独的操作系统部署网络之外，还可决定将此功能融入管理网络或数据网络。

网络配置

可配置 **Lenovo XClarity Administrator** 使用一个或两个网络接口。

注意：

- 如果管理设备后再更改 **XClarity Administrator** 的 **IP** 地址，可能会使设备在 **XClarity Administrator** 中处于脱机状态。确保更改 **IP** 地址前先终止管理所有设备。
- 通过单击**重复 IP 地址检查**切换开关可启用或禁用同一子网的重复 **IP** 地址检查。默认情况下禁用此功能。启用后，如果尝试更改 **XClarity Administrator** 的 **IP** 地址或者要管理的设备 **IP** 地址与另一受管设备或同一子网的其他设备相同，**XClarity Administrator** 将发出警报。

注：启用后，**XClarity Administrator** 会运行 **ARP** 扫描来查找同一子网内的活动 **IPv4** 设备。要阻止 **ARP** 扫描，请禁用**重复 IP 地址检查**。

- 在将 **XClarity Administrator** 作为虚拟设备运行时，如果管理网络的网络接口配置为使用 **DHCP**，则 **DHCP** 租约到期时可能会更改管理界面 **IP** 地址。如果 **IP** 地址更改，则必须终止管理机箱、机架和立式服务器，然后再次管理它们。为避免发生此问题，请将管理界面改为静态 **IP** 地址，或确保设置 **DHCP** 服务器配置，以使 **DHCP** 地址基于 **MAC** 地址或 **DHCP** 租约不会到期。
- 如果*不*计划使用 **XClarity Administrator** 来部署操作系统或更新操作系统设备驱动程序，可通过将网络接口更改为使用**仅发现和管理硬件**选项来禁用 **Samba** 和 **Apache** 服务器。请注意，更改网络接口后将重新启动管理软件。
- 将 **XClarity Administrator** 作为容器运行时。
  - 只能启用或禁用重复 **IP** 地址检查、修改网络接口角色以及修改代理设置。所有其他网络设置（包括 **IP** 地址、网关和 **DNS**）都是在容器设置中定义。
  - 确保在主机系统上设置了 **macvlan** 网络。

XClarity Administrator 有两个单独的网络接口可为所处环境定义，具体取决于所实现的网络拓扑。对于虚拟设备，这些网络命名为 **eth0** 和 **eth1**。对于容器，可以选择自定义名称。

- 仅存在一个网络接口（**eth0**）时：
  - 必须配置接口以支持设备发现和管理（如服务器配置和固件更新）。它必须可与每个受管机箱中的 **CMM** 和 **Flex** 交换机、每个受管服务器中的主板管理控制器，以及每个 **RackSwitch** 交换机通信。
  - 如果要使用 **XClarity Administrator** 获取固件和操作系统设备驱动程序更新，则必须有至少一个网络接口连接到 **Internet**，且最好通过防火墙。否则，必须将更新导入到存储库中。
  - 如果要收集服务数据或使用自动问题通知（包括 **Call Home** 和 **Lenovo** 上传设施），至少一个网络接口必须连接到 **Internet**，且最好通过防火墙。
  - 如果要部署操作系统映像并更新操作系统设备驱动程序，则此接口必须通过 **IP** 网络连接到用于访问主机操作系统的服务器网络接口。

    注：如果已实现一个单独的网络用于部署操作系统和更新操作系统设备驱动程序，则可将第二个网络接口配置为连接到该网络而非数据网络。但是，如果每个服务器上的操作系统均无权访问数据网络，则在服务器上另外配置一个接口以从主机操作系统连接到用于操作系统部署和操作系统设备驱动程序更新的数据网络（如果需要）
- 存在两个网络接口（**eth0** 和 **eth1**）时：
  - 第一个网络接口（通常是 **Eth0** 接口）必须连接到管理网络并配置为支持设备发现和管理（包括服务器配置和固件更新）。它必须可与每个受管机箱中的 **CMM** 和 **Flex** 交换机、每个受管服务器中的管理控制器，以及每个 **RackSwitch** 交换机通信。
  - 第二个网络接口（通常是 **eth1** 接口）可配置为与内部数据网络和/或公共数据网络进行通信。
  - 如果要使用 **XClarity Administrator** 获取固件和操作系统设备驱动程序更新，则必须有至少一个网络接口连接到 **Internet**，且最好通过防火墙。否则，必须将更新导入到存储库中。
  - 如果要收集服务数据或使用自动问题通知（包括 **Call Home** 和 **Lenovo** 上传设施），至少一个网络接口必须连接到 **Internet**，且最好通过防火墙。
  - 如果要部署操作系统映像并更新设备驱动程序，可选择使用 **eth1** 或 **eth0** 接口。但是，使用的接口必须通过 **IP** 网络连接到用于访问主机操作系统的服务器网络接口。

注：如果已实现一个单独的网络用于部署操作系统和更新操作系统设备驱动程序，则可将第二个网络接口配置为连接到该网络而非数据网络。但是，如果每个服务器上的操作系统均无权访问数据网络，则在服务器上另外配置一个接口以从主机操作系统连接到用于操作系统部署和操作系统设备驱动程序更新的数据网络（如果需要）

下表根据已在所处环境中实现的网络拓扑类型，显示 **XClarity Administrator** 网络接口可采用的配置。根据此表决定如何定义各网络接口。

表 2. 各网络接口的角色（基于网络拓扑）

网络拓扑	接口 1（eth0）的角色	接口 2（eth1）的角色
聚合网络（支持操作系统部署和操作系统设备驱动程序更新的管理和数据网络）	管理网络 • 发现和管理 • 服务器配置 • 固件更新 • 服务数据集合 • 自动通知问题（如 **Call Home** 和 **Lenovo** 更新设施） • 保修数据检索 • 操作系统部署 • 操作系统设备驱动程序更新	无
数据网络和支持操作系统部署和操作系统设备驱动程序更新的单独管理网络	管理网络 • 发现和管理 • 服务器配置 • 固件更新 • 服务数据集合 • 自动通知问题（如 **Call Home** 和 **Lenovo** 更新设施） • 保修数据检索 • 操作系统部署 • 操作系统设备驱动程序更新	数据网络 • 无
单独的管理网络和支持操作系统部署和操作系统设备驱动程序更新的数据网络	管理网络 • 发现和管理 • 服务器配置 • 固件更新 • 服务数据集合 • 自动通知问题（如 **Call Home** 和 **Lenovo** 更新设施） • 保修数据检索	数据网络 • 操作系统部署 • 操作系统设备驱动程序更新
单独的管理网络和不支持操作系统部署和操作系统设备驱动程序更新的数据网络	管理网络 • 发现和管理 • 服务器配置 • 固件更新 • 服务数据集合 • 自动通知问题（如 **Call Home** 和 **Lenovo** 更新设施） • 保修数据检索	数据网络 • 无
仅管理网络（不支持操作系统部署和操作系统设备驱动程序更新）	管理网络 • 发现和管理 • 服务器配置 • 固件更新 • 服务数据集合	无

表 2. 各网络接口的角色（基于网络拓扑）（续）

网络拓扑	接口 1（eth0）的角色	接口 2（eth1）的角色
	• 自动通知问题（如 **Call Home** 和 **Lenovo** 更新设施） • 保修数据检索	

单一数据和管理网络

在此网络拓扑中，通过同一网络进行管理通信、数据通信和操作系统部署。此拓扑称为*聚合*网络。

重要：实现共享数据和管理网络可能会导致流量中断，如丢弃数据包或管理网络连接问题，具体取决于网络配置（例如，来自服务器的流量具有高优先级，而来自管理控制器的流量具有低优先级）。除 **TCP** 之外，管理网络还使用 **UDP** 流量。当网络流量较高时，**UDP** 流量可能具有较低的优先级。

安装 **Lenovo XClarity Administrator** 时，请遵照以下注意事项定义 **eth0** 网络接口：

- 必须配置接口以支持设备发现和管理（如服务器配置和固件更新）。它必须可与每个受管机箱中的 **CMM** 和 **Flex** 交换机、每个受管服务器中的主板管理控制器，以及每个 **RackSwitch** 交换机通信。
- 如果要使用 **XClarity Administrator** 获取固件和操作系统设备驱动程序更新，则必须有至少一个网络接口连接到 **Internet**，且最好通过防火墙。否则，必须将更新导入到存储库中。
- 如果要收集服务数据或使用自动问题通知（包括 **Call Home** 和 **Lenovo** 上传设施），至少一个网络接口必须连接到 **Internet**，且最好通过防火墙。
- 如果要部署操作系统映像并更新操作系统设备驱动程序，则此接口必须通过 **IP** 网络连接到用于访问主机操作系统的服务器网络接口。

  注：如果已实现一个单独的网络用于部署操作系统和更新操作系统设备驱动程序，则可将第二个网络接口配置为连接到该网络而非数据网络。但是，如果每个服务器上的操作系统均无权访问数据网络，则在服务器上另外配置一个接口以从主机操作系统连接到用于操作系统部署和操作系统设备驱动程序更新的数据网络（如果需要）
- 只有在实现单一数据和管理网络拓扑或虚拟隔离的数据和管理网络拓扑时，才能在满足 **XClarity Administrator** 要求的包括受管服务器在内的任何系统上设置 **XClarity Administrator**；但是，无法使用 **XClarity Administrator** 将固件更新应用于该受管服务器。甚至，此时仅有某些固件在应用时立即激活，并且 **XClarity Administrator** 强制目标服务器重新启动，而这还将重新启动 **XClarity Administrator**。在应用但延迟激活时，重新启动 **XClarity Administrator** 主机后仅应用某些固件。

还可从 **XClarity Administrator** 配置第二个网络接口以连接到同一网络来支持冗余。

下图显示聚合网络拓扑的示例实现。

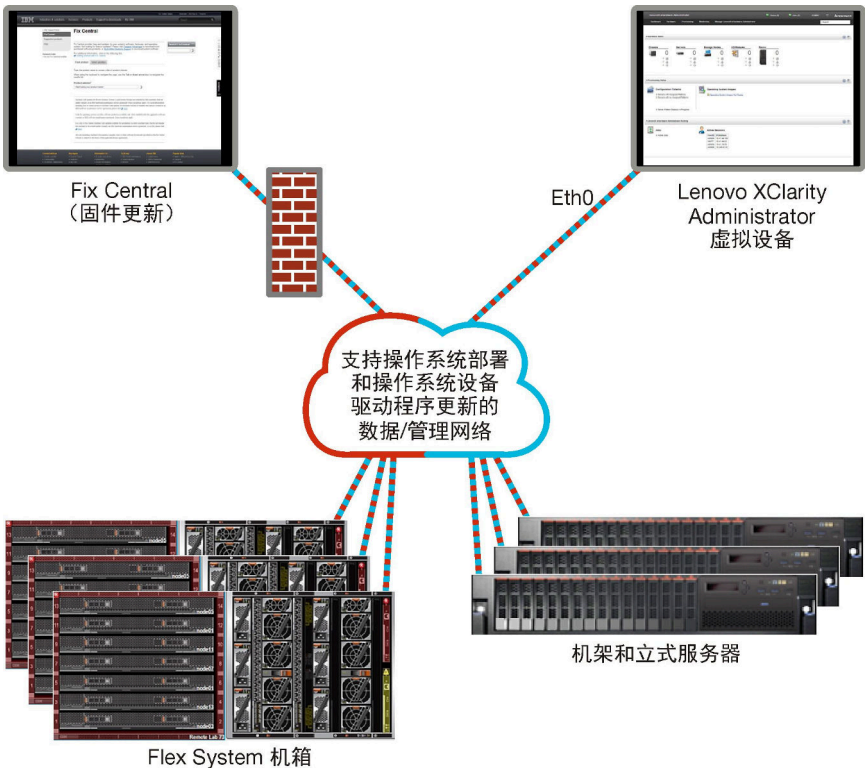


图 1. 单一管理、数据和操作系统部署的示例实现

物理隔离的数据和管理网络

在此网络拓扑中，管理网络和数据网络是两个物理隔离的网络，而将操作系统部署网络配置为管理网络或数据网络的一部分。

安装 **Lenovo XClarity Administrator** 时，遵照以下注意事项定义网络设置：

- 第一个网络接口（通常是 **Eth0** 接口）必须连接到管理网络并配置为支持设备发现和管理（包括服务器配置和固件更新）。它必须可与每个受管机箱中的 **CMM** 和 **Flex** 交换机、每个受管服务器中的管理控制器，以及每个 **RackSwitch** 交换机通信。
- 第二个网络接口（通常是 **eth1** 接口）可配置为与内部数据网络和/或公共数据网络进行通信。
- 如果要使用 **XClarity Administrator** 获取固件和操作系统设备驱动程序更新，则必须有至少一个网络接口连接到 **Internet**，且最好通过防火墙。否则，必须将更新导入到存储库中。
- 如果要收集服务数据或使用自动问题通知（包括 **Call Home** 和 **Lenovo** 上传设施），至少一个网络接口必须连接到 **Internet**，且最好通过防火墙。
- 如果要部署操作系统映像并更新设备驱动程序，可选择使用 **eth1** 或 **eth0** 接口。但是，使用的接口必须通过 **IP** 网络连接到用于访问主机操作系统的服务器网络接口。

  注：如果已实现一个单独的网络用于部署操作系统和更新操作系统设备驱动程序，则可将第二个网络接口配置为连接到该网络而非数据网络。但是，如果每个服务器上的操作系统均无权访问数据网络，则在服务器上另外配置一个接口以从主机操作系统连接到用于操作系统部署和操作系统设备驱动程序更新的数据网络（如果需要）

第 22 页图 2 “物理隔离的数据网络和管理网络的示例实现，其中操作系统网络作为数据网络的一部分” 显示物理隔离的管理网络和数据网络的一个示例实现，其中将操作系统部署网络配置为数据网络的一部分。

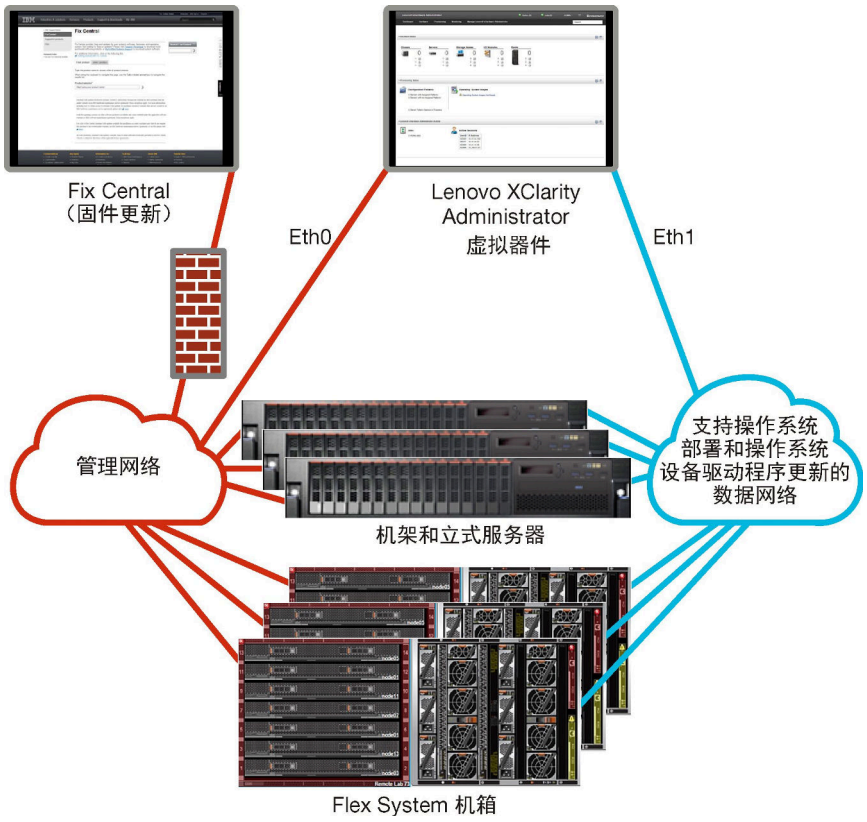


图 2. 物理隔离的数据网络和管理网络的示例实现，其中操作系统网络作为数据网络的一部分

第 23 页图 3 “物理隔离的数据网络和管理网络的示例实现，其中操作系统网络作为管理网络的一部分” 显示隔离管理网络和数据网络的另一个示例实现，其中将操作系统部署网络配置为管理网络的一部分。在此实现中，**XClarity Administrator** 不需要连接到数据网络。

注：如果操作系统部署网络无权访问数据网络，则在服务器上另外配置一个接口以从服务器上的主机操作系统连接到数据网络（如果需要）。

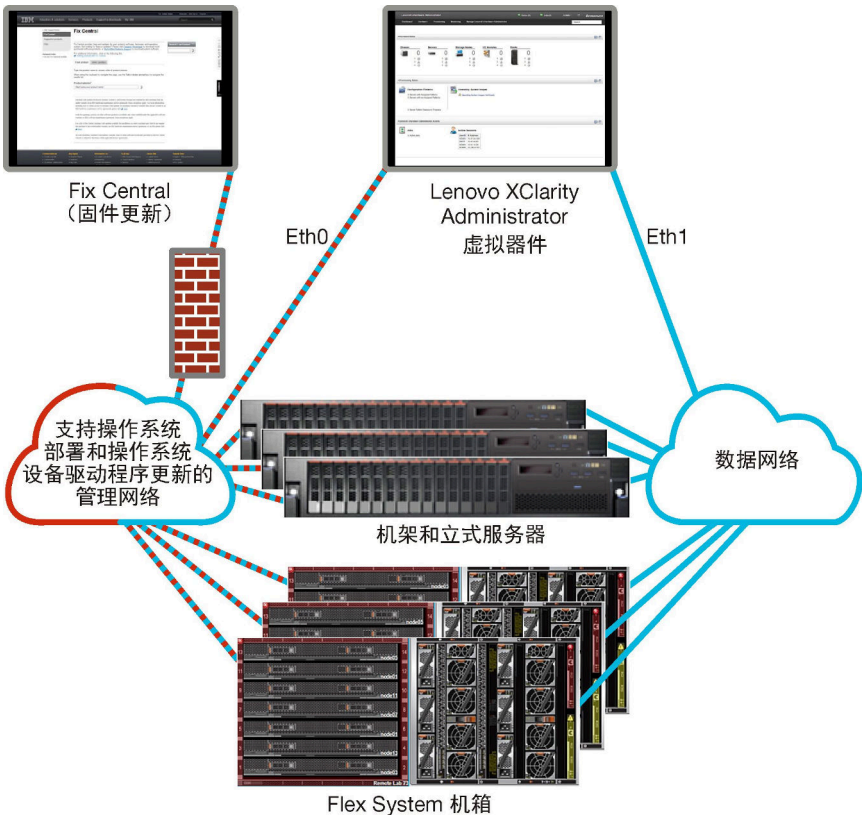


图 3. 物理隔离的数据网络和管理网络的示例实现，其中操作系统网络作为管理网络的一部分

虚拟隔离的数据和管理网络

在此拓扑中，虚拟地将数据网络与管理网络隔离。通过同一物理连接发送来自数据网络的数据包和来自管理网络的数据包。对所有管理网络数据包使用 **VLAN** 标记以隔离两个网络之间的流量。

注：如果 **Lenovo XClarity Administrator** 安装在某个主机上，而该主机在机箱中的受管服务器上运行，则无法同时使用 **XClarity Administrator** 将固件更新应用于整个机箱。应用固件更新后，必须重新启动主机系统。

安装 **XClarity Administrator** 时，遵照以下注意事项定义网络设置：

- 第一个网络接口（通常是 **Eth0** 接口）必须连接到管理网络并配置为支持设备发现和管理（包括服务器配置和固件更新）。它必须可与每个受管机箱中的 **CMM** 和 **Flex** 交换机、每个受管服务器中的管理控制器，以及每个 **RackSwitch** 交换机通信。
- 第二个网络接口（通常是 **eth1** 接口）可配置为与内部数据网络和/或公共数据网络进行通信。
- 如果要使用 **XClarity Administrator** 获取固件和操作系统设备驱动程序更新，则必须有至少一个网络接口连接到 **Internet**，且最好通过防火墙。否则，必须将更新导入到存储库中。
- 如果要收集服务数据或使用自动问题通知（包括 **Call Home** 和 **Lenovo** 上传设施），至少一个网络接口必须连接到 **Internet**，且最好通过防火墙。
- 如果要部署操作系统映像并更新设备驱动程序，可选择使用 **eth1** 或 **eth0** 接口。但是，使用的接口必须通过 **IP** 网络连接到用于访问主机操作系统的服务器网络接口。

  注：如果已实现一个单独的网络用于部署操作系统和更新操作系统设备驱动程序，则可将第二个网络接口配置为连接到该网络而非数据网络。但是，如果每个服务器上的操作系统均无权访

问数据网络，则在服务器上另外配置一个接口以从主机操作系统连接到用于操作系统部署和操作系统设备驱动程序更新的数据网络（如果需要）

- 只有在实现单一数据和管理网络拓扑或虚拟隔离的数据和管理网络拓扑时，才能在满足 XClarity Administrator 要求的包括受管服务器在内的任何系统上设置 XClarity Administrator；但是，无法使用 XClarity Administrator 将固件更新应用于该受管服务器。甚至，此时仅有某些固件在应用时立即激活，并且 XClarity Administrator 强制目标服务器重新启动，而这还将重新启动 XClarity Administrator。在应用但延迟激活时，重新启动 XClarity Administrator 主机后仅应用某些固件。

第 24 页图 4 “虚拟隔离的数据网络和管理网络的示例实现，其中操作系统网络作为数据网络的一部分” 显示虚拟隔离管理网络和数据网络的一个示例实现，其中将操作系统部署网络配置为数据网络的一部分。在此示例中，XClarity Administrator 安装在机箱中的受管服务器上。

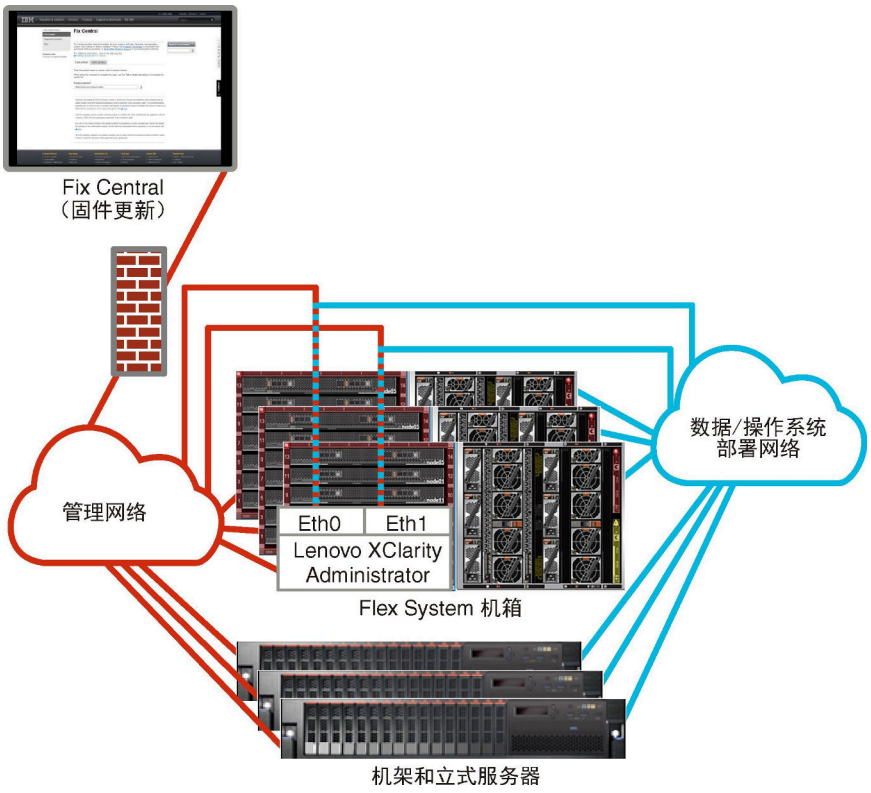


图 4. 虚拟隔离的数据网络和管理网络的示例实现，其中操作系统网络作为数据网络的一部分

第 25 页图 5 “虚拟隔离的管理网络和数据网络的示例实现，其中操作系统网络作为管理网络的一部分” 显示虚拟隔离的管理网络和数据网络的一个示例实现，其中将操作系统部署网络配置为管理网络的一部分，而 XClarity Administrator 安装在机箱中的受管服务器上。在此实现中，XClarity Administrator 不需要连接到数据网络。

注：如果操作系统部署网络无权访问数据网络，则在服务器上另外配置一个接口以从服务器上的主机操作系统连接到数据网络（如果需要）。

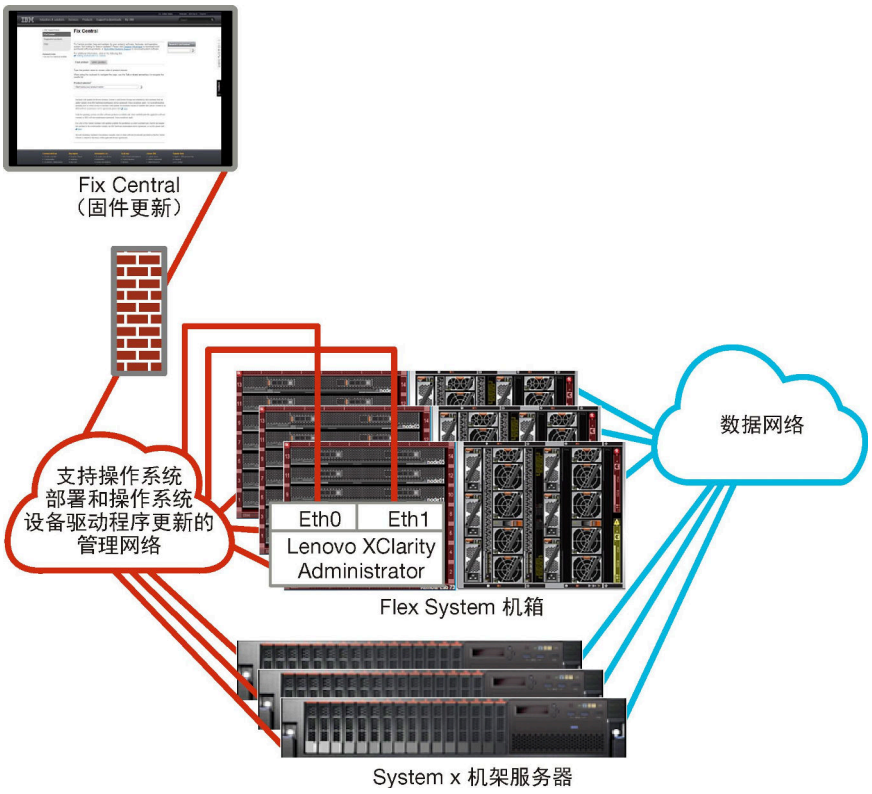


图 5. 虚拟隔离的管理网络和数据网络的示例实现，其中操作系统网络作为管理网络的一部分

仅限于管理的网络

在此拓扑中，**Lenovo XClarity Administrator** 仅有权访问管理网络。它不能访问数据网络。但是，如果要将操作系统映像从 **XClarity Administrator** 部署到受管服务器，则 **XClarity Administrator** 必须有权访问操作系统部署网络。

在安装 **XClarity Administrator** 和定义网络设置时，**eth0** 网络接口必须配置为：

- 必须配置接口以支持设备发现和管理（如服务器配置和固件更新）。它必须可与每个受管机箱中的 **CMM** 和 **Flex** 交换机、每个受管服务器中的主板管理控制器，以及每个 **RackSwitch** 交换机通信。
- 如果要使用 **XClarity Administrator** 获取固件和操作系统设备驱动程序更新，则必须有至少一个网络接口连接到 **Internet**，且最好通过防火墙。否则，必须将更新导入到存储库中。
- 如果要收集服务数据或使用自动问题通知（包括 **Call Home** 和 **Lenovo** 上传设施），至少一个网络接口必须连接到 **Internet**，且最好通过防火墙。
- 如果要部署操作系统映像并更新操作系统设备驱动程序，则此接口必须通过 **IP** 网络连接到用于访问主机操作系统的服务器网络接口。

  注：如果已实现一个单独的网络用于部署操作系统和更新操作系统设备驱动程序，则可将第二个网络接口配置为连接到该网络而非数据网络。但是，如果每个服务器上的操作系统均无权访问数据网络，则在服务器上另外配置一个接口以从主机操作系统连接到用于操作系统部署和操作系统设备驱动程序更新的数据网络（如果需要）

还可从 **XClarity Administrator** 配置第二个网络接口以连接到同一网络来支持冗余。

第 26 页图 6 “不支持操作系统部署的仅限于管理的网络的示例实现”展示一个示例实现，这是一个仅限于管理的网络，其中不支持从 **XClarity Administrator** 部署操作系统。

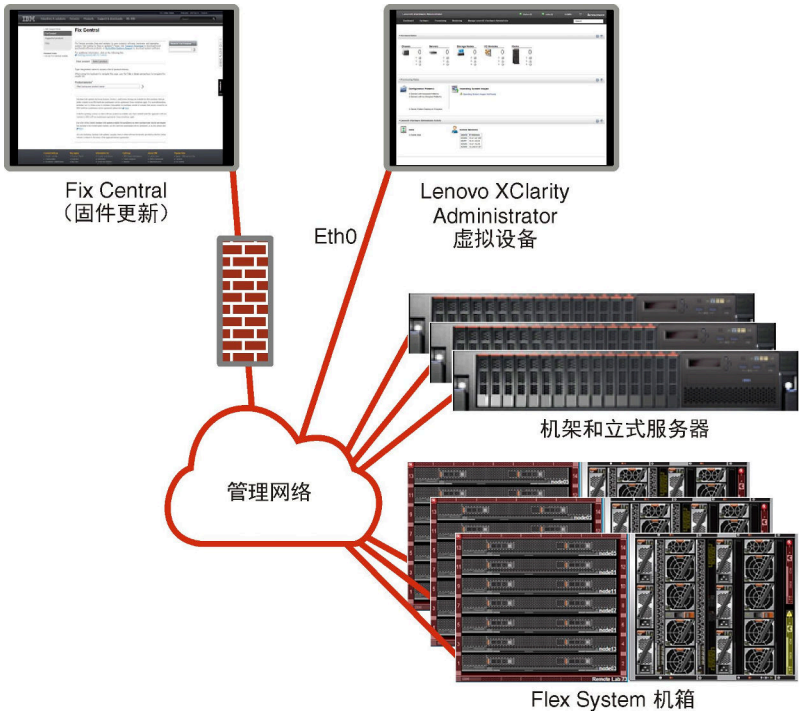


图 6. 不支持操作系统部署的仅限于管理的网络的示例实现

第 26 页图 6 “不支持操作系统部署的仅限于管理的网络的示例实现”展示一个示例实现，这是一个仅限于管理的网络，其中支持从 **XClarity Administrator** 部署操作系统。

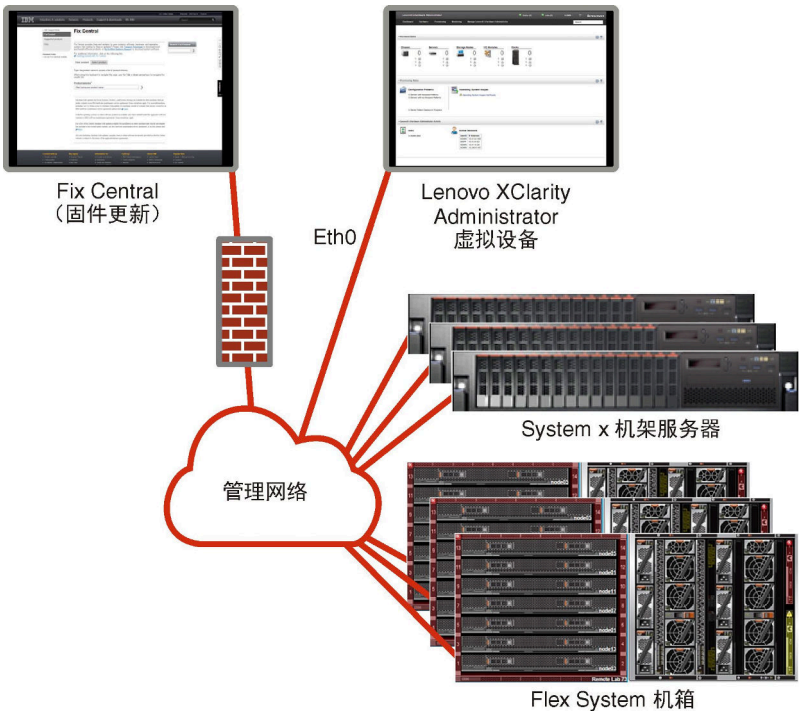


图 7. 支持操作系统部署的仅限于管理的网络的示例实现

安全注意事项

规划 Lenovo XClarity Administrator 和所有受管设备的安全性。

Encapsulation 管理

在 Lenovo XClarity Administrator 中管理 Lenovo 机箱和服务器时，可配置 Lenovo XClarity Administrator 以更改设备的防火墙规则，以便仅接受来自 Lenovo XClarity Administrator 的传入请求。这称为 ***Encapsulation***。也可在已受 Lenovo XClarity Administrator 管理的机箱和服务器上启用或禁用 Encapsulation。

在支持 Encapsulation 的设备上启用 Encapsulation 模式后，Lenovo XClarity Administrator 会将设备 Encapsulation 模式更改为“encapsulationLite”并更改设备上的防火墙规则以将传入请求限制为仅限来自此 Lenovo XClarity Administrator 的请求。

禁用后，Encapsulation 模式设置为“normal”。如果先前在设备上启用了 Encapsulation，则会删除 Encapsulation 防火墙规则。

注意：如果启用了 Encapsulation，但 XClarity Administrator 在终止管理设备之前变为不可用状态，则必须采取必要步骤来禁用 Encapsulation 以便建立与设备的通信。有关恢复过程，请参阅 XClarity Administrator 在线文档中的在发生管理软件故障后用 CMM 恢复 管理机箱和在发生管理软件故障后恢复管理 机架或立式服务器。

注：

- 交换机、存储设备以及非 Lenovo 机箱和服务器不支持 Encapsulation。

- 配置管理网络接口以使用动态主机配置协议（DHCP）并启用了 Encapsulation 时，管理机架服务器可能需要很长时间。

有关 Encapsulation 的详细信息，请参阅 XClarity Administrator 在线文档中的“启用 Encapsulation”。

加密管理

加密管理由多种通信模式和协议构成，它们控制如何处理 Lenovo XClarity Administrator 与受管设备（如机箱、服务器和 Flex 交换机）之间的安全通信。

加密算法

XClarity Administrator 支持 TLS 1.2 和更强大的加密算法，以实现安全网络连接。

为了提高安全性，仅支持高强度密码。客户端操作系统和 Web 浏览器的组合必须支持以下密码套件之一。

- **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**

管理软件的加密模式

此设置将决定用于从管理软件进行安全通信的模式。

- **兼容性**。此模式为默认模式。它与较旧的固件版本、浏览器和其他网络客户端兼容，但这些旧版本未实现符合 NIST SP 800-131A 所需的严格安全性标准。
- **NIST SP 800-131A**。此模式旨在遵从 NIST SP 800-131A 标准。XClarity Administrator 旨在始终在内部使用强加密，如有强加密网络连接，还要使用这些连接。但是，在此模式下，不允许使用未经 NIST SP 800-131A 认可的加密模式进行网络连接，其中包括拒绝接受用 SHA-1 或更弱的散列签署的传输层安全性（TLS）证书。

  如果选择此模式：

  – 对于除端口 8443 以外的所有端口，所有 TLS CBC 密码和所有不支持完美前向保密的密码都会被禁用。
  – 事件通知可能未成功推送到某些移动设备订阅。请参阅将事件转发到移动设备（位于 XClarity Administrator 在线文档中）。外部服务（如 Android 和 iOS）存在用 SHA-1 签署的证书，而 SHA-1 是一种不符合 NIST SP 800-131A 模式的更严格要求的算法。因此，连接到这些服务可能会失败并返回证书异常或握手故障。

  有关 NIST SP 800-131A 合规性的详细信息，请参阅 XClarity Administrator 在线文档中的实现 NIST 800-131A 合规性。

有关在管理软件上设置安全模式的更多信息，请参阅 XClarity Administrator 线文档中的设置加密模式和通信 协议。

受管服务器的安全模式

此设置将决定用于从受管服务器进行安全通信的模式。

- **兼容性安全**。当服务和客户端需要不符合 CNSA/FIPS 的加密算法时，请选择此模式。该模式支持广泛的加密算法，并允许启用所有服务。
- **NIST SP 800-131A**。选择此模式可确保符合 NIST SP 800-131A 标准。这包括将 RSA 密钥限制在 2048 位或更长，将用于数字签名的散列限制在 SHA-256 或更长，并确保仅使用 NIST 批准的对称加密算法。此模式需要将 SSL/TLS 模式设为 **TLS 1.2 服务器和客户端**。

  配备 XCC2 的服务器*不*支持此模式。
- **标准安全**。（仅限配备 XCC2 的服务器）这是配备 XCC2 的服务器的默认安全模式。选择此模式可确保符合 FIPS 140-3 标准。要使 XCC 在 FIPS 140-3 验证模式下运行，只能启用支持 FIPS 140-3 级加密的服务。默认情况下，不支持 FIPS 140-2/140-3 级加密的服务处于禁用状态，但可以根据需要启用。如果启用了任何使用非 FIPS 140-3 级加密的服务，XCC 将无法在 FIPS 140-3 验证模式下运行。此模式需要 FIP 级证书。
- **企业级严格安全**。（仅限配备 XCC2 的服务器）这是最安全的模式。选择此模式可确保符合 CNSA 标准。仅允许支持 CNSA 级加密的服务。非安全服务默认处于禁用状态且无法启用。此模式需要 CNSA 级证书。

  XClarity Administrator 会对采用**企业级严格安全**模式的服务器使用 RSA-3072/SHA-384 证书签名。

  重要：

  - 要使用此模式，必须在每个选定的配备 XCC2 的服务器上都安装 XCC2 Feature On Demand 密钥。
  - 在该模式下，如果 XClarity Administrator 使用自签名证书，则 XClarity Administrator 必须使用基于 RSA3072/SHA384 的根证书和服务器证书。如果 XClarity Administrator 使用外部签名证书，则 XClarity Administrator 必须生成基于 RSA3072/SHA384 的 CSR，并联系外部 CA 以签署基于 RSA3072/SHA384 的新服务器证书。
  - 当 XClarity Administrator 使用基于 RSA3072/SHA384 的证书时，XClarity Administrator 可能会断开与设备的连接，但下列设备除外：Flex System 机箱（CMMS）和服务器、ThinkSystem 服务器、ThinkServer 服务器、System x M4 和 M5 服务器、Lenovo ThinkSystem DB 系列交换机、Lenovo RackSwitch, Flex System 交换机、Mellanox 交换机、ThinkSystem DE/DM 存储设备、IBM 磁带库存储，以及已刷写 22C 之前版本固件的 ThinkSystem SR635/SR655 服务器。要继续管理断开连接的设备，请设置另一个采用基于 RSA2048/SHA384 的证书的 XClarity Administrator 实例。

更改加密模式时，请考虑以下影响。

- 不支持从**兼容性安全**模式或**标准安全**模式更改为**企业级严格安全**模式。
- 当从**兼容性安全**模式升级到**标准安全**模式时，如果导入的证书或 SSH 公钥不合规，您会收到警告，但仍然可以升级到**标准安全**模式。
- 如果从**企业级严格安全**模式降级到**兼容性安全**模式或**标准安全**模式，则：
  - 服务器会自动重启以使该安全模式生效。
  - 如果 XCC2 上的严格模式 FoD 密钥丢失或过期，并且 XCC2 使用自签名 TLS 证书，则 XCC2 会根据符合标准严格模式的算法重新生成自签名 TLS 证书。这会导致 XClarity Administrator 因证书错误出现连接故障。要解决不受信任的证书错误，请参阅 XClarity Administrator 在线文档中的解析不受信任的服务器证书。如果 XCC2 使用自定义 TLS 证书，XCC2 会允许降级，并且会警告您需要导入基于**标准安全**模式密码的服务器证书。

- 配备 XCC2 的服务器不支持 NIST SP 800-131A 模式。
- 如果将 XClarity Administrator 的加密模式设为 TLS v1.2，并且使用受管认证的受管服务器的安全模式设为 TLS v1.2，则使用 XClarity Administrator 或 XCC 将服务器安全模式更改为 TLS v1.3 将导致服务器永久脱机。
- 如果 XClarity Administrator 的加密模式设为 TLS v1.2 并且您尝试使用 XCC 管理安全模式设为 TLS v1.3 的服务器，则无法使用受管认证管理该服务器。

您可以更改以下设备的安全设置。
- 采用 Intel 或 AMD 处理器的 Lenovo ThinkSystem 服务器（SR635/SR655 除外）
- Lenovo ThinkSystem V2 服务器
- 采用 Intel 或 AMD 处理器的 Lenovo ThinkSystem V3 服务器
- Lenovo ThinkEdge SE350/SE450 服务器
- Lenovo System x 服务器

有关在受管服务器上设置安全模式的更多信息，请参阅 XClarity Administrator 在线文档中的配置服务器的安全设置。

安全证书

Lenovo XClarity Administrator 使用 SSL 证书建立 XClarity Administrator 与其受管设备（如 System x 服务器中的机箱和服务处理器）之间的安全可信的通信，以及用户与 XClarity Administrator 或其他服务之间的通信。默认情况下，XClarity Administrator、CMM 和主板管理控制器使用 XClarity Administrator 生成的由内部证书颁发机构颁发的自签名证书。

在每个 XClarity Administrator 实例中唯一生成的默认自签名服务器证书为多种环境提供充分的安全性。可让 XClarity Administrator 为您管理证书，也可更主动地定制或替换服务器证书。XClarity Administrator 可根据所处环境定制证书。例如，可决定：

- 通过重新生成内部证书颁发机构证书和/或具有组织特定值的最终服务器证书来生成一对新密钥。
- 生成证书签名请求（CSR），该 CSR 可发送到所选的证书颁发机构以签署自定义证书并上传到 XClarity Administrator，用作其所有托管服务的最终服务器证书。
- 将服务器证书下载到本地系统，以便将该证书导入到 Web 浏览器的可信证书列表中。

有关证书的更多信息，请参阅 XClarity Administrator 在线文档中的使用安全证书。

认证

支持的认证服务器

认证服务器 是用于认证用户凭证的用户注册表。Lenovo XClarity Administrator 支持以下类型的认证服务器。

- **本地认证服务器**。默认情况下，XClarity Administrator 配置为使用管理软件中驻留的嵌入式轻型目录访问协议（LDAP）服务器。
- **外部 LDAP 服务器**。目前仅支持 Microsoft Active Directory 和 OpenLDAP。此服务器必须位于连接到管理网络的外侧 Microsoft Windows Server 上。当使用外部 LDAP 服务器时，将禁用本地认证服务器。

  注意：要将 Active Directory 绑定方法配置为使用登录凭证，每个受管服务器的主板管理控制器必须运行 2016 年 9 月或更高版本的固件。

- **外部标识管理系统**。目前仅支持 CyberArk。

  如果在 CyberArk 上为 ThinkSystem 或 ThinkAgile 服务器注册了用户帐户，则可以在首次设置管理服务器时选择让 XClarity Administrator 从 CyberArk 检索凭证，从而登录服务器（使用受管或本地认证）。在从 CyberArk 检索凭证之前，必须在 XClarity Administrator 中定义 CyberArk 路径，并且必须使用 TLS 相互认证通过客户端证书在 CyberArk 和 XClarity Administrator 之间建立相互信任。
- **外部 SAML 身份提供商**。目前，仅支持 Microsoft Active Directory 联合身份验证服务（AD FS）。除了输入用户名和密码之外，还可设置多重认证，通过要求输入 PIN 码、读取智能卡和客户端证书而增强安全性。当使用 SAML 身份提供商 时，不会禁用本地认证服务器。必须使用本地用户帐户直接登录到受管机箱或服务器（除非在该设备上启用 Encapsulation）进行 PowerShell 和 REST API 认证，如果外部认证不可用，还要以此方式进行恢复。

  可决定同时使用外部 LDAP 服务器和外部 身份提供商。如果两者均启用，则应使用外部 LDAP 服务器直接登录到受管设备，并使用 身份提供商 登录到管理软件。

有关认证服务器的更多信息，请参阅 XClarity Administrator 在线文档中的管理认证服务器。

设备认证

默认情况下，设备的管理方式是使用 XClarity Administrator 受管认证登录。管理机架服务器和 Lenovo 机箱时，可选择使用本地认证或受管认证登录设备。

- 对机架服务器、Lenovo 机箱及 Lenovo 机架交换机使用*本地认证* 时，XClarity Administrator 使用存储的凭证对设备进行认证。*存储的凭证* 可以是设备上的活动用户帐户或 Active Directory 服务器中的用户帐户。

  使用本地认证管理设备之前必须在 XClarity Administrator 中创建中存储的凭证，且凭证须匹配设备上的活动用户帐户或者 Active Directory 服务器中的用户帐户（请参阅 XClarity Administrator 在线文档中的管理存储的凭证）。

  注：

  – RackSwitch 设备仅支持使用存储的凭证进行认证。XClarity Administrator 用户凭证不受支持。
- 借助*受管认证*，可使用 XClarity Administrator 认证服务器中的凭证（而非本地凭证）来管理和监控多个设备。对设备（而不是 ThinkServer 服务器、System x M4 服务器和交换机）使用受管认证时，XClarity Administrator 将设备及其安装的组件配置为使用 XClarity Administrator 认证服务器进行集中管理。

  – 启用受管认证后，可使用手动输入的凭证或存储的凭证管理设备（请参阅 XClarity Administrator 在线文档中的管理用户帐户以及管理存储的凭证）。

    仅当 XClarity Administrator 在设备上配置了 LDAP 设置，才会使用存储的凭证。此后，存储的凭证发生的任何更改都不会影响该设备的管理或监控。

    注：如果为设备启用了受管认证，则不能使用 XClarity Administrator 编辑该设备的存储的凭证。
  – 如果使用本地或外部 LDAP 服务器作为 XClarity Administrator 认证服务器，则应使用在该认证服务器中定义的用户帐户登录到 XClarity Administrator 域中的 XClarity Administrator、CMM 和主板管理控制器。而本地 CMM 和管理控制器用户帐户被禁用。
  – 如果使用 SAML 2.0 身份供应商作为 XClarity Administrator 认证服务器，则 SAML 帐户无法访问受管设备。但是，当 SAML 身份供应商与 LDAP 服务器一起使用时，如果该身份供应商使用存在于 LDAP 服务器中的 LDAP 帐户，则可使用 LDAP 用户帐户登录受

管设备，而 SAML 2.0 提供的更高级认证方法（例如多重认证和单点登录）可用于登录 XClarity Administrator。

- 借助单点登录功能，已登录 XClarity Administrator 的用户将可以自动登录到主板管理控制器。默认情况下，将 ThinkSystem 或 ThinkAgile 服务器设置为受 XClarity Administrator 管理的服务器后，即可启用单点登录（使用 CyberArk 密码管理服务器的情况除外）。可以通过配置全局设置来对所有受管 ThinkSystem 和 ThinkAgile 服务器启用或禁用单点登录。对特定 ThinkSystem 和 ThinkAgile 服务器启用单点登录会覆盖适用于所有 ThinkSystem 和 ThinkAgile 服务器的全局设置（请参阅 XClarity Administrator 在线文档中的“管理服务器”）。

  注：使用 CyberArk 标识管理系统进行认证时会自动禁用单点登录。

- 为 ThinkSystem SR635 和 SR655 服务器启用受管认证时：
  - 主板管理控制器固件最多支持五个 LDAP 用户角色。XClarity Administrator 在管理期间将这些 LDAP 用户角色添加到服务器中：lxc-supervisor、lxc-sysmgr、lxc-admin、lxc-fw-admin 和 lxc-os-admin。

    必须至少为用户分配一个指定的 LDAP 用户角色，用户才能与 ThinkSystem SR635 和 SR655 服务器进行通信。
  - 管理控制器固件不支持与服务器本地用户具有相同用户名的 LDAP 用户。

- 对于 ThinkServer 和 System x M4 服务器，不使用 XClarity Administrator 认证服务器。而是在设备上创建以“LXCA_”为前缀并后接随机字符串的 IPMI 帐户。（不会禁用现有的本地 IPMI 用户帐户。）终止管理 ThinkServer 服务器时，将禁用该“LXCA_”用户帐户，并将前缀“LXCA_”替换为前缀“DISABLED_”。为了确定 ThinkServer 服务器是否受另一实例管理，XClarity Administrator 检查是否存在以“LXCA_”为前缀的 IPMI 帐户。如果决定强制管理某个受管的 ThinkServer 服务器，则将禁用并重命名该设备上所有以“LXCA_”为前缀的 IPMI 帐户。请考虑手动清除不再使用的 IPMI 帐户。

  如果您使用手动输入的凭证，XClarity Administrator 将会自动创建存储的凭证，并使用该存储的凭证来管理设备。

  注：如果为设备启用了受管认证，则不能使用 XClarity Administrator 编辑该设备的存储的凭证。

  - 每次使用手动输入的凭证管理设备时，将为该设备新建一个存储的凭证，即使在之前的管理过程中已为该设备创建过存储的凭证。
  - 终止管理设备时，XClarity Administrator 不会删除管理过程中自动为该设备创建的存储的凭证。

恢复用户帐户

如果指定了恢复密码，XClarity Administrator 将禁用本地 CMM 或管理控制器用户帐户，并在设备上创建一个新的恢复用户帐户（RECOVERY_ID），以待将来用于认证。如果管理软件发生故障，则可使用 RECOVERY_ID 帐户登录到该设备，执行恢复操作以恢复设备上的帐户管理功能，直至恢复或替换管理节点为止。

如果终止管理具有 RECOVERY_ID 用户帐户的设备，则将启用所有本地用户帐户并删除 RECOVERY_ID 帐户。

- 如果更改已禁用的本地用户帐户（例如更改密码），则这些更改对该 RECOVERY_ID 帐户无任何影响。在受管认证模式下，RECOVERY_ID 帐户是唯一一个激活且可操作的用户帐户。

- 只有在紧急情况下，例如管理软件发生故障，或网络问题使得设备无法与 **XClarity Administrator** 通信以对用户进行认证，才能使用 RECOVERY_ID 帐户。
- 发现设备时，将指定 RECOVERY_ID密码。请务必记录密码以备将来使用。

有关恢复管理设备的信息，请参阅 **XClarity Administrator** 在线文档中的在发生管理软件故障后用 CMM 恢复 管理机箱和在发生管理软件故障后恢复管理 机架或立式服务器。

用户帐户和角色组

用户帐户 用于登录和管理 **Lenovo XClarity Administrator** 以及所有受管机箱和服务器。**XClarity Administrator** 用户帐户涉及两个相互依赖的过程：认证和授权。

认证 是用以验证用户凭证的安全机制。认证过程使用存储在所配置的认证服务器中的用户凭证。它还会阻止未经授权的管理软件或恶意受管系统应用程序访问资源。通过认证后，用户可以访问 **XClarity Administrator**。但是，要访问特定资源或执行特定任务，用户还必须有合适的授权。

授权 检查通过认证的用户的权限，并根据用户在角色组中的成员资格控制其对资源的访问。*角色组* 用于将特定角色分配给在认证服务器中定义和管理的一组用户帐户。例如，如果用户是具有“主管”权限的角色组的成员，则该用户可以在 **XClarity Administrator** 中创建、编辑和删除用户帐户。如果用户具有“操作员”权限，则该用户只能查看用户帐户信息。

有关用户帐户和角色组的更多信息，请参阅 **XClarity Administrator** 在线文档中的管理用户帐户。

用户帐户安全

用户帐户设置控制着密码复杂度、帐户锁定以及 **Web** 会话不活动超时。可更改帐户安全设置的值。

有关帐户安全设置的更多信息，请参阅 **Lenovo XClarity Administrator** 在线文档中的更改用户帐户安全设置。

高可用性注意事项

要为 **Lenovo XClarity Administrator** 设置高可用性，请使用主机操作系统或容器环境中提供的高可用性功能。

Docker

可以使用 **Docker Datacenter** 为 **Docker** 引擎中运行的 **XClarity Administrator** 容器设置高可用性环境。有关 **Docker Datacenter** 高可用性的详细信息，请参阅“使用 **Docker Datacenter** 实现高可用性架构 和应用程序”网页。

Citrix

可使用为 **Citrix** 环境提供的高可用性功能。有关详细信息，请参阅 **XClarity Administrator** 在线文档中的实现高可用性（**Citrix**）。

KVM（CentOS、RedHat 和 Ubuntu）

可使用 **OpenStack**；如果已经具有高可用性环境，还可以继续使用内部过程。有关 **OpenStack** 高可用性的详细信息，请参阅 **XClarity Administrator** 在线文档中的实现高可用性（**KVM**）。

Microsoft Hyper-V

可使用为 **ESXi** 环境提供的高可用性功能。有关信息，请参阅 **XClarity Administrator** 在线文档中的**实现高可用性（Microsoft Hyper-V）**。

Nutanix AHV

可使用为 **Nutanix AHV** 环境提供的虚拟机高可用性功能。有关详细信息，请参阅 **XClarity Administrator** 在线文档中的**实现高可用性（Nutanix）**。

VMware ESXi

在 **VMware High Availability** 环境中，将多个主机配置为一个集群。共享存储用于制作对集群中主机可用的虚拟机（虚拟机）的磁盘映像。一次仅在一个主机上运行虚拟机。当虚拟机有问题时，将在备用主机上启动该虚拟机的另一实例。

VMware High Availability 需要以下组件：

- 最少两个装有 **ESXi** 的主机。这些主机将成为 **VMware** 集群的一部分。
- 另外一个装有 **VMware vCenter** 的主机。

  提示：确保所安装的 **VMware vCenter** 版本与要在集群中所用主机上安装的 **ESXi** 版本兼容。

  VMware vCenter 可安装在集群中所用的某个主机上。但是，如果该主机已关闭电源或不可用，则您也将无法访问 **VMware vCenter** 界面。
- 集群中所有主机均可访问的共享存储（数据存储）。可使用 **VMware** 支持的任何类型的共享存储。**VMware** 使用数据存储决定虚拟机是否应故障转移到其他主机（检测信号）。

有关设置 **VMware High Availability** 集群的详细信息，请参阅 **XClarity Administrator** 在线文档中的**实现高可用性 (VMware ESXi)**。

Features on Demand

Features on Demand 可激活某些功能而无需安装硬件或购买新设备。为完成此激活过程，需获取和安装相应的 **Features on Demand** 密钥。

要使用 **Lenovo XClarity Administrator** 中的远程控制和操作系统部署操作，必须对默认情况下未激活这些功能的服务器启用 **XClarity Controller Enterprise** 级别或 **MM** 高级升级。这些操作还要求 **ThinkSystem**、**Converged** 和 **System x** 服务器上装有用于远程呈现的 **Features on Demand** 密钥。可从“服务器”页面确定是否已在服务器上启用、禁用或安装远程呈现（请参阅查看受管服务器的状态（在 **XClarity Administrator** 在线文档中））。

使用 **Features on Demand** 密钥会激活某些高级服务器功能。如果功能具有在 **UEFI** 设置期间显示的可配置设置，则可使用 **Configuration Patterns** 来配置设置；但是，产生的配置要在安装相应的 **Features on Demand** 密钥后才会激活。

注：无法从 **XClarity Administrator** 中安装或管理 **Features on Demand** 密钥，但可查看受管服务器上当前安装的 **Features on Demand** 密钥的列表。有关查看所安装的 **Features on Demand** 密钥的详细信息，请参阅 **XClarity Administrator** 在线文档中的**查看 Feature on Demand 密钥**。

要获取和安装 **Features on Demand** 密钥，请执行以下操作：

1. 按相应的部件号购买 **Features on Demand** 升级。

   可从 **Feature on Demand 门户网站**购买密钥。购买完毕后，您将通过电子邮件收到授权代码。

2. 在 **Feature on Demand** 门户网站上，输入所收到的授权代码以及要升级的服务器的唯一系统标识。
3. 下载 **.KEY** 文件形式的激活密钥。
4. 将激活密钥上传到服务器的管理控制器。
5. 重新启动服务器。重新启动完毕后，即激活功能。

有关 **Features on Demand** 密钥的详细信息，请参阅使用 **Lenovo Features on Demand**。

第 3 章　在 Docker、CentOS、Citrix、Red Hat KVM、Rocky、Ubuntu、VMware ESXi 或 Windows Hyper-V 环境中安装 Lenovo XClarity Administrator

可通过几种方法将可管理的设备连接到网络，并设置 Lenovo XClarity Administrator 虚拟设备来管理这些设备。请按照本节中的信息设置可管理的设备并在 Docker、CentOS、Citrix、Red Hat KVM、Ubuntu、VMware ESXi 或 Windows Hyper-V 环境中安装 XClarity Administrator

本节介绍如何设置几种常用拓扑。本节不一一介绍所有可能的网络拓扑，

注意：要管理设备，XClarity Administrator 必须有权访问管理网络。

了解更多：
- 在 VMware vCenter 上安装 Lenovo XClarity Administrator
- 在 VMware vSphere 上安装 Lenovo XClarity Administrator
- 在 Windows Hyper-V 上安装 Lenovo XClarity Administrator
- 在 Red Hat KVM 上安装 Lenovo XClarity Administrator

单一数据和管理网络

在这种网络拓扑中，数据网络和管理网络是同一网络。

开始之前

确保已启用所有相应端口，包括 XClarity Administrator 需要的端口（请参阅端口可用性）。

确保要使用 XClarity Administrator 管理的每个设备上都至少装有所需的最低版本固件。可在“XClarity Administrator 支持 – 兼容性” Web 页面 中单击 Compatibility（兼容性）选项卡，然后单击相应设备类型的链接，找到所需的最低固件级别。

重要：配置设备和组件时尽量少更改 IP 地址。考虑使用静态 IP 地址代替动态主机配置协议（DHCP）。如果使用 DHCP，则务必尽量少更改 IP 地址。

关于本任务

对于虚拟设备，XClarity Administrator 与网络之间的所有通信是通过主机上的 eth0 网络接口进行的。对于容器，可以使用自定义名称；但是，此方案中使用 eth0。

重要：实现共享数据和管理网络可能会导致流量中断，如丢弃数据包或管理网络连接问题，具体取决于网络配置（例如，来自服务器的流量具有高优先级，而来自管理控制器的流量具有低优先级）。除 TCP 之外，管理网络还使用 UDP 流量。当网络流量较高时，UDP 流量可能具有较低的优先级。

下图显示在数据网络和管理网络为同一网络时设置所处环境的一种方法。图中的数字对应于以下各节中的编号步骤。

注：此图并未完整显示您的环境可能需要的线缆连接选项。而是仅显示机架服务器、机架交换机、Flex 交换机和 CMM 的线缆连接选项要求，因为这些要求与设置单一数据/管理网络相关。

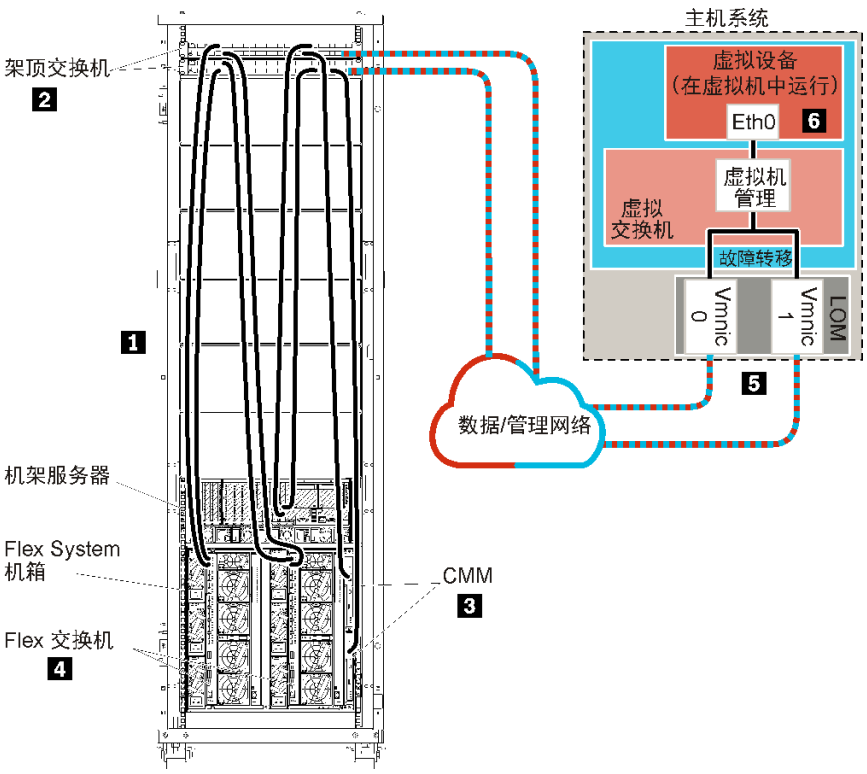


图 8. 虚拟设备单一数据和管理网络拓扑示例

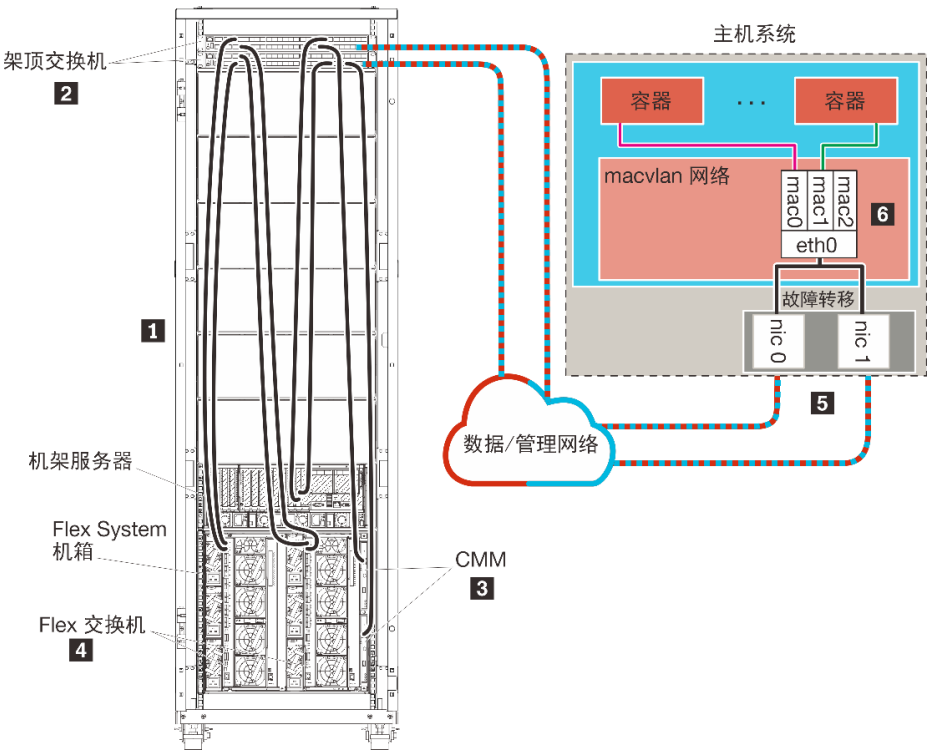


图 9. 容器单一数据和管理网络拓扑示例

重要：可在包括受管服务器在内的任何满足 **XClarity Administrator** 要求的系统上设置 **XClarity Administrator**。如果将受管服务器用于 **XClarity Administrator** 主机，则：

- 必须实现虚拟隔离的数据和管理网络拓扑或单一数据和管理网络拓扑。
- 不得使用 **XClarity Administrator** 将固件更新应用于该受管服务器。即便仅有某些固件在应用时立即激活，**XClarity Administrator** 仍强制目标服务器重新启动，而这还将重新启动 **XClarity Administrator**。在应用固件但延迟激活时，重新启动 **XClarity Administrator** 主机后仅应用某些固件。
- 如果使用 **Flex System** 机箱中的服务器，请确保该服务器设置为自动开机。可从 **CMM Web** 界面中设置此选项，具体方法是单击**机箱管理 → 计算节点**，选择该服务器，然后对**自动开机模式**选择**自动开机**。

如果要安装 **XClarity Administrator** 以管理已配置的现有机箱和机架服务器，请继续执行步骤 5：安装和配置主机。

有关规划此拓扑的其他信息（包括有关网络设置以及 **Eth1** 和 **Eth0** 配置的信息），请参阅单一数据和管理网络。

步骤 1：用线缆将机箱、机架服务器和 Lenovo XClarity Administrator 主机连接到架顶交换机

用线缆将机箱、机架服务器和 **XClarity Administrator** 主机连接到架顶交换机以使设备与您的网络之间可进行通信。

过程

用线缆将每个机箱中的每个 **Flex** 交换机和 **CMM**、每个机架服务器和 **XClarity Administrator** 主机连接到架顶交换机。可选择该架顶交换机中的任何端口。

下图是一个示例，其中显示用线缆将机箱（**Flex** 交换机和 **CMM**）、机架服务器和 **XClarity Administrator** 主机连接到架顶交换机。

注：此图并未完整显示您的环境可能需要的线缆连接选项。而是仅显示机架服务器、机架交换机、**Flex** 交换机和 **CMM** 的线缆连接选项要求，因为这些要求与设置单一数据/管理网络相关。

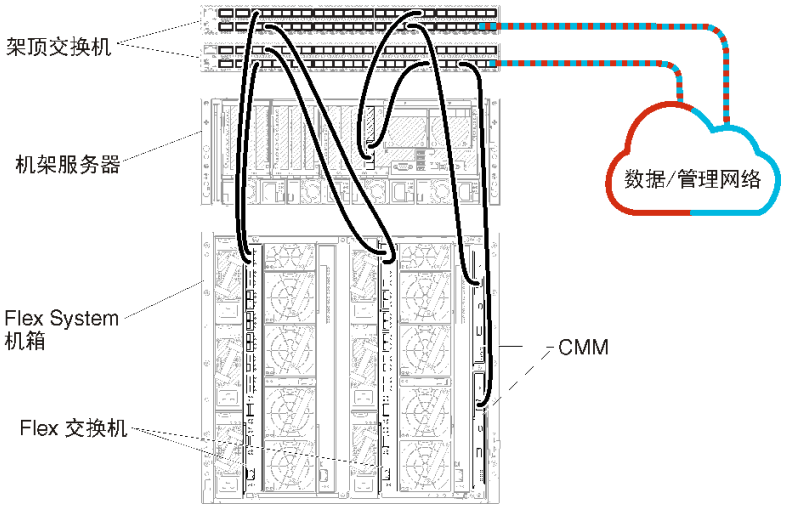


图 10. 单一数据和管理网络的示例线缆连接

步骤 2：配置架顶交换机

配置架顶交换机。

开始之前

除满足架顶交换机的典型配置要求外，还应确保已启用所有相应端口，包括 **Flex** 交换机、机架服务器和网络的外部端口以及 **CMM**、机架服务器和网络的内部端口。

过程

配置步骤可能因所安装的机架交换机类型而异。

有关配置 **Lenovo** 架顶交换机的信息，请参阅**System x** 在线文档中的“机架交换机”。如果装有其他架顶交换机，请参阅该交换机随附的文档。

步骤 3：配置 Chassis Management Module（CMM）

配置机箱中的主 **Chassis Management Module**（**CMM**）以管理机箱中的所有设备。

关于本任务

有关配置 **CMM** 的详细信息，请参阅**Flex System** 在线文档中的 “配置机箱组件”。

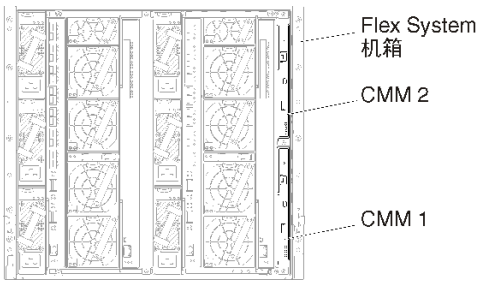
另请参阅机箱随附的说明书中的步骤 **4.1 - 4.5**。

过程

完成以下步骤以配置 **CMM**。

如果装有两个 **CMM**，则仅配置*主* **CMM**，而后自动与备用 **CMM** 同步配置。

步骤 **1.** 将一条以太网线缆从插槽 **1** 中的 **CMM** 连接到客户端工作站以建立一个直接连接。



首次连接到 CMM 时，可能需要更改客户端工作站上的 Internet 协议属性。

重要：确保客户端工作站子网与 CMM 子网相同。（默认 CMM 子网为 **255.255.255.0**）。为客户端工作站选择的 IP 地址必须与 CMM 在同一网络上（例如，**192.168.70.0 - 192.168.70.24**）。

步骤 2. 要启动 CMM 管理界面，在客户端工作站上打开 Web 浏览器，然后访问 CMM IP 地址。

注：

- 确保使用安全连接并在 URL 中加入 **https**（例如，**https://192.168.70.100**）。如果不加入 **https**，则将发生“未找到页面”错误。
- 如果使用默认 IP 地址 **192.168.70.100**，则可能数分钟后才会显示 CMM 管理界面。发生这一延迟的原因是，CMM 先花两分钟时间尝试获取 DHCP 地址，之后才回退到默认静态地址。

步骤 3. 使用默认用户标识 USERID 和密码 PASSWORD 登录到 CMM 管理界面。登录后，必须更改默认密码。

步骤 4. 完成 CMM 初始安装向导以指定所处环境的详细信息。初始安装向导包括以下选项：

- 查看机箱清单和运行状况。
- 从现有配置文件导入配置。
- 配置常规 CMM 设置。
- 配置 CMM 日期和时间。

  提示：在安装 XClarity Administrator 时，您需要配置 XClarity Administrator 以及受 XClarity Administrator 管理的所有机箱以使用 NTP 服务器。
- 配置 CMM IP 信息。
- 配置 CMM 安全策略。
- 配置域名系统（DNS）。
- 配置事件转发器。

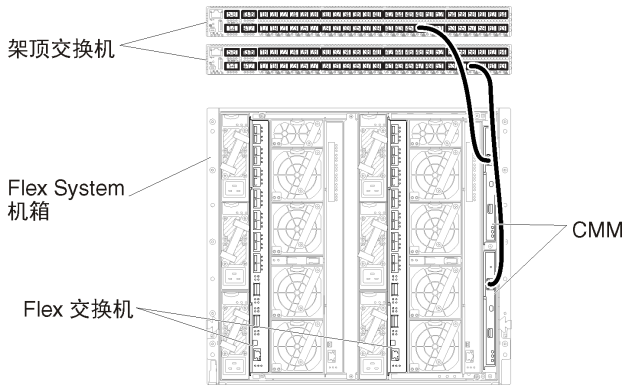
步骤 5. 保存安装向导设置并应用更改后，为机箱中的所有组件配置 IP 地址。

请参阅随机箱提供的说明书的步骤 **4.6**。

注：必须重置每个计算节点的系统管理处理器并重新启动 Flex 交换机才能显示新 IP 地址。

步骤 6. 使用 CMM 管理界面重新启动 CMM。

步骤 7. 当 CMM 重新启动时，将一条线缆从 CMM 上的以太网端口连接到网络。



步骤 8. 使用新 IP 地址登录到 CMM 管理界面。

完成之后

还可配置 CMM 以支持冗余。使用 CMM 帮助系统详细了解以下每个页面上可用的字段。

- 为 CMM 配置故障转移，以防主 CMM 出现硬件故障。从 CMM 管理界面中，单击**管理模块的管理 → 属性 → 高级故障转移**。
- 配置发生网络问题时的故障转移（上行链路）。从 CMM 管理界面中，依次单击**管理模块的管理 → 网络**、**以太网**选项卡、**高级以太网**。至少务必选中**在失去物理网络链路时进行故障转移**。

步骤 4：配置 Flex 交换机

在每个机箱中配置 Flex 交换机（I/O 模块）。

开始之前

确保已启用所有相应端口，包括从 Flex 交换机到架顶交换机的外部端口以及 CMM 的内部端口。

如果将 Flex 交换机设置为通过 DHCP 获取动态网络设置（IP 地址、网络掩码、网关和 DNS 地址），则确保 Flex 交换机的设置一致（例如，确保 IP 地址与 CMM 在同一子网中）。

重要：对于每个 Flex System 机箱，确保机箱中每个服务器内扩展卡的构造类型与同一机箱中所有 Flex 交换机的构造类型兼容。例如，如果机箱中装有以太网交换机，则该机箱中的所有服务器必须通过板载网卡接口或以太网扩展卡建立以太网连接。有关配置 Flex 交换机的详细信息，请参阅 Flex System 在线文档中的 “配置 I/O 模块”。

过程

配置步骤可能因所安装的 Flex 交换机类型而异。有关每个支持的 Flex 交换机的详细信息，请参阅 Flex System 在线文档中的 “Flex System 网络交换机”。

通常，必须配置 Flex 交换机插槽 1 和 2 中的 Flex 交换机。

提示：在查看机箱背面时，Flex 交换机插槽 2 是第三个模块插槽。

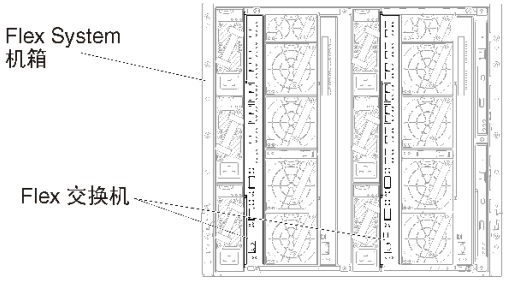


图 11. 机箱中的 Flex 交换机位置

步骤 5: 安装和配置主机

可在任何满足 **Lenovo XClarity Administrator** 要求的服务器上安装 **Docker**。

开始之前

可以使用 **Docker Datacenter** 为 **Docker** 引擎中运行的 **XClarity Administrator** 容器设置高可用性环境。有关 **Docker Datacenter** 高可用性的详细信息，请参阅“使用 **Docker Datacenter** 实现高可用性架构 和应用程序”网页。

确保主机满足 **XClarity Administrator** 在线文档中的硬件和软件先决条件。

确保主机系统与要管理的设备在同一网络上。

重要：可在包括受管服务器在内的任何满足 **XClarity Administrator** 要求的系统上设置 **XClarity Administrator**。如果将受管服务器用于 **XClarity Administrator** 主机，则：

- 必须实现虚拟隔离的数据和管理网络拓扑或单一数据和管理网络拓扑。
- 不得使用 **XClarity Administrator** 将固件更新应用于该受管服务器。即便仅有某些固件在应用时立即激活，**XClarity Administrator** 仍强制目标服务器重新启动，而这还将重新启动 **XClarity Administrator**。在应用固件但延迟激活时，重新启动 **XClarity Administrator** 主机后仅应用某些固件。
- 如果使用 **Flex System** 机箱中的服务器，请确保该服务器设置为自动开机。可从 **CMM Web** 界面中设置此选项，具体方法是单击**机箱管理 → 计算节点**，选择该服务器，然后对**自动开机模式**选择**自动开机**。

过程

按 **Docker** 发行版提供的说明在主机上安装并配置 **Docker**。

步骤 6. 安装和配置 XClarity Administrator

在刚刚安装的 **Docker** 主机上安装和配置 **Lenovo XClarity Administrator** 容器。

开始之前

确保主机系统满足最低的硬件和软件要求（请参阅硬件和软件先决条件）。

确保已启用所有相应端口，包括 **XClarity Administrator** 需要的端口（请参阅端口可用性）。

确保主机系统与要管理的设备在同一网络上。

确保主机操作系统和 **XClarity Administrator** 使用相同的 **NTP** 服务器。

XClarity Administrator 允许对用于数据管理、硬件管理和操作系统部署的网络使用自定义名称（请参阅网络配置）。以下过程中的相应示例使用的是 **eth0**。

确保在主机系统上的内核中加载了 **macvlan** 网络。要检查是否已加载该网络，请使用 **lsmod | grep macvlan** 命令。要将 **macvlan** 加载到内核中，请运行 **modprobe macvlan** 命令。

在同一主机上运行多个 **XClarity Administrator** 容器时，确保为每个容器使用唯一的名称和 **IP** 地址。

如果要管理 **ThinkServer** 和其他 **Legacy** 设备，请确保启用 **Docker** 以支持 **IPv6**。

1. 编辑 **/etc/docker/daemon.json** 文件，将 **ipv6** 键设为 **true**，并将 **fixed-cidr-v6** 键设为您的 **IPv6** 子网。以下是一个示例 **daemon** 文件。
```
{
  "ipv6": true,
  "fixed-cidr-v6": "2001:db8:1::/64",
  "experimental": true,
  "ip6tables": true
}
```
2. 运行以下命令重新加载 **Docker** 配置文件。
```
systemctl reload docker
```

注：XClarity Administrator *不是* 作为特权容器运行。

过程

要使用 **Docker compose** 安装 **XClarity Administrator** 容器，请完成以下步骤。

步骤 **1.** 从 **XClarity Administrator 下载 Web 页面** 将 **XClarity Administrator** 虚拟设备映像、环境文件和 **YAML** 文件下载到客户端工作站。登录到该网站，然后使用提供给您的访问密钥下载该映像。

步骤 **2.** 通过运行以下命令将 **XClarity Administrator** 容器镜像导入 **Docker** 主机。
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

步骤 **3.** 编辑 docker_compose.env 文件，更新以下环境变量。

- **CONTAINER_NAME**。唯一的容器名称，用于为每个 **XClarity Administrator** 实例创建 **Docker** 卷（例如，CONTAINER_NAME=LXCA-203）
- **ADDRESS**。容器的静态 **IPv4** 地址（例如，ADDRESS=192.0.2.0）
- **BACKUP_MOUNT**。（可选）可用于存储 **XClarity Administrator** 备份的远程共享路径。必须为 /mnt/backup_share。
- **FIRMWARE_MOUNT**。（可选）可用作固件更新远程存储库的远程共享路径。必须为 /mnt/fw_share。

以下是一个示例环境文件。
```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

步骤 4. 编辑 docker_compose.yml，更新以下属性。

- 将 **image** 属性设置为步骤 2 中使用的安装映像文件的名称。

  注：可使用 `docker tag` 命令更改映像文件名（例如，更改为“**latest**”）。
- 如果要使用远程共享作为远程固件存储库并存储 **XClarity Administrator** 备份，请在 **volumes** 属性中为每个远程共享设置主机装载点。
- 将 **dns** 属性设为 **DNS** 服务器的 **IP** 地址。
- 容器会共享主机可用的处理器和内存资源池。（可选）通过设置 **cpus** 和 **memory** 属性来定义资源使用限制。
- 将 **parent** 属性设置为主机系统上的网络接口名称以用作容器中 **macvlan** 接口的父接口。此接口必须可以直接访问分配给容器的子网。
- 根据您的网络拓扑设置 **subnet** 和 **gateway**。通常，子网和网关用于 **${ADDRESS}** 所属的管理网络。
- 如果要支持 **IPv6**，请将 **enable_ipv6** 属性设为 **true**，将 **ipv6_address** 属性设为 **IPv6** 地址，并根据您的网络拓扑再添加一组 **subnet** 和 **gateway** 属性（通常针对该 **IPv6** 地址所属的管理网络）。

注：XClarity Administrator 使用 **macvlan** 配置容器网络。有关详细信息，请参阅“使用 **macvlan** 网络” **Web** 页面。

下面是启用了 **IPv6** 的 **YML** 文件示例。

```
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"
```

步骤 5. 通过运行以下命令在 Docker 中部署映像，其中 *<ENV_FILENAME>* 是在步骤 2 中创建的环境变量文件的名称。

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

完成之后

登录并配置 XClarity Administrator（请参阅首次访问 Lenovo XClarity Administrator Web 界面和配置 Lenovo XClarity Administrator）。

物理隔离的数据和管理网络

在此拓扑中，数据网络和管理网络是物理隔离的网络。通过主机上的 Eth0 网络接口进行 Lenovo XClarity Administrator 与网络之间的管理通信。通过 Eth1 网络接口进行数据通信。

开始之前

确保已启用所有相应端口，包括 XClarity Administrator 需要的端口（请参阅端口可用性）。

确保要使用 XClarity Administrator 管理的每个设备上都至少装有所需的最低版本固件。可在“XClarity Administrator 支持 – 兼容性” Web 页面 中单击 Compatibility（兼容性）选项卡，然后单击相应设备类型的链接，找到所需的最低固件级别。

重要：配置设备和组件时尽量少更改 IP 地址。考虑使用静态 IP 地址代替动态主机配置协议（DHCP）。如果使用 DHCP，则务必尽量少更改 IP 地址。

关于本任务

下图显示在数据网络和管理网络是物理隔离的网络时设置所处环境的一种方法。图中的数字对应于以下各节中的编号步骤。

注：此图并未完整显示您的环境可能需要的线缆连接选项。而是仅显示 Flex 交换机、CMM 和机架服务器的线缆连接选项要求，因为这些要求与设置物理隔离的数据和管理网络相关。

提示：除了设置每个网络连接两个物理交换机以实现冗余（总共四个交换机），还可设置每个网络仅连接单个物理交换机（总共两个交换机）。在这种情况下，每台交换机将与两个网络相连，并且将实现两个 VLAN：一个用于数据网络，另一个用于管理网络，以便分开数据流量。

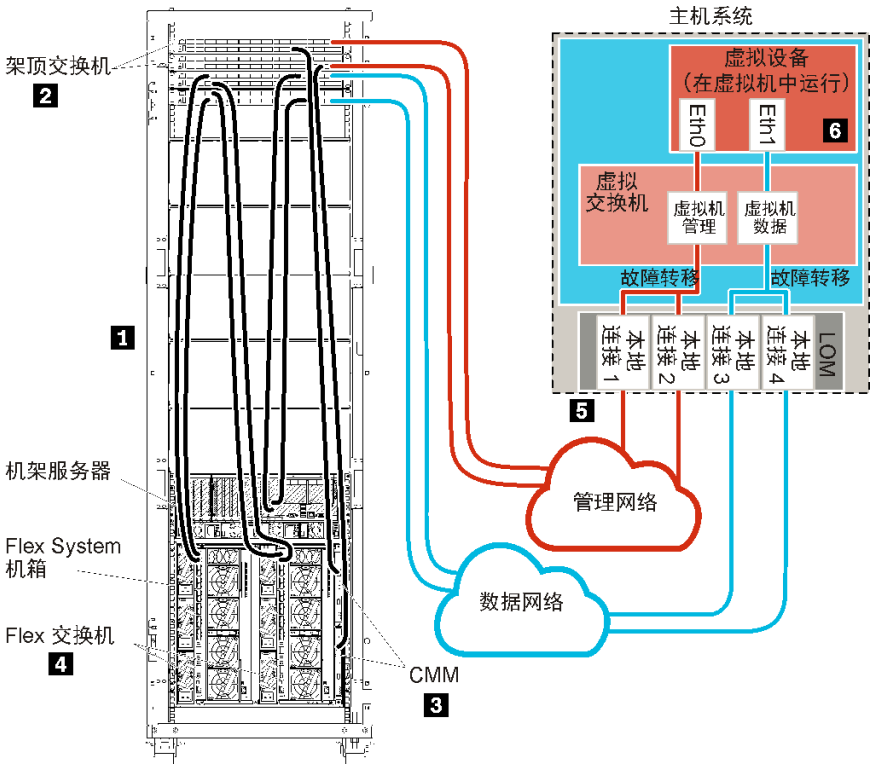


图 12. 虚拟设备物理隔离的数据和管理网络拓扑示例

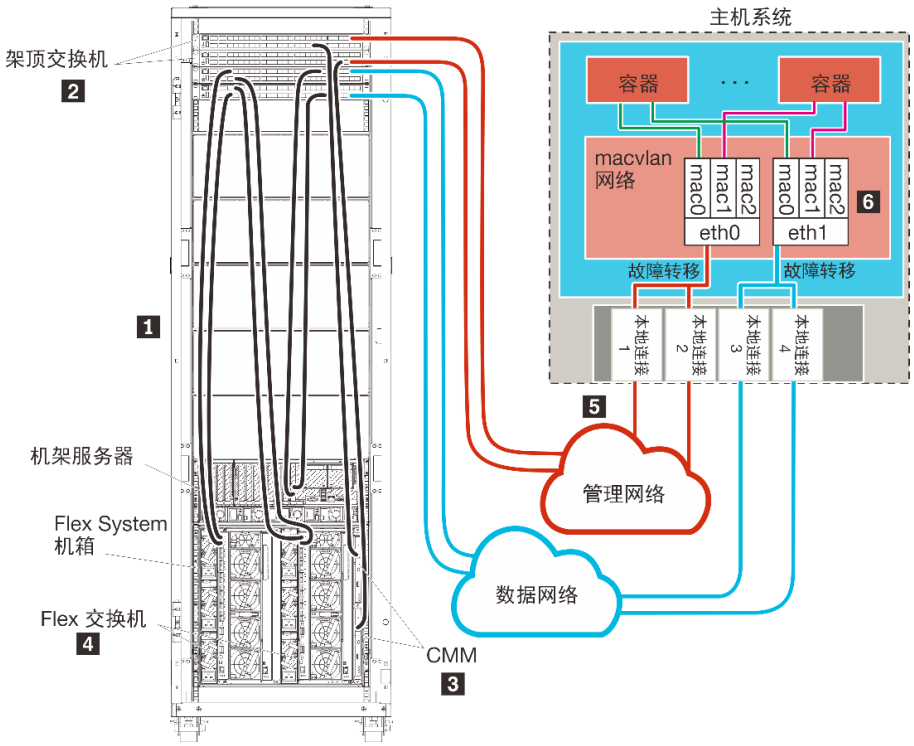


图 13. 容器物理隔离的数据和管理网络拓扑示例

如果要安装 **XClarity Administrator** 以管理已配置的现有机箱和机架服务器，请继续执行步骤 5：安装和配置主机。

有关规划此拓扑的其他信息（包括有关网络设置以及 **Eth1** 和 **Eth0** 配置的信息），请参阅物理隔离的数据和管理网络。

步骤 1：用线缆将机箱、机架服务器和 Lenovo XClarity Administrator 主机连接到架顶交换机

用线缆将机箱、机架服务器和 **XClarity Administrator** 主机连接到架顶交换机以使设备与您的网络之间可进行通信。

过程

用线缆将每个机箱中的每个 **Flex** 交换机和 **CMM**、每个机架服务器和 **XClarity Administrator** 主机连接到架顶交换机。可选择该架顶交换机中的任何端口。

下图是一个示例，其中显示用线缆将机箱（**Flex** 交换机和 **CMM**）、机架服务器和 **XClarity Administrator** 主机连接到架顶交换机。

注：此图并未完整显示您的环境可能需要的线缆连接选项。而是仅显示 **Flex** 交换机、**CMM** 和机架服务器的线缆连接选项要求，因为这些要求与设置物理隔离的数据和管理网络相关。

提示：除了设置每个网络连接两个物理交换机以实现冗余（总共四个交换机），还可设置每个网络仅连接单个物理交换机（总共两个交换机）。在这种情况下，每台交换机将与两个网络相连，并且将实现两个 VLAN：一个用于数据网络，另一个用于管理网络，以便分开数据流量。

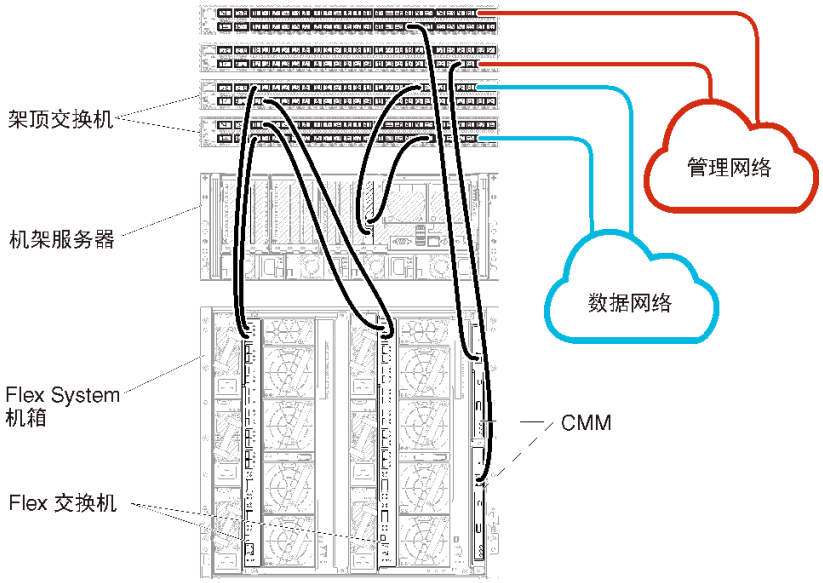


图 14. 物理隔离的数据和管理网络的示例线缆连接

步骤 2：配置架顶交换机

配置架顶交换机。

开始之前

除满足架顶交换机的典型配置要求外，还应确保已启用所有相应端口，包括 Flex 交换机、机架服务器和网络的外部端口以及 CMM、机架服务器和网络的内部端口。

过程

配置步骤可能因所安装的机架交换机类型而异。

有关配置 Lenovo 架顶交换机的信息，请参阅System x 在线文档中的“机架交换机”。如果装有其他架顶交换机，请参阅该交换机随附的文档。

步骤 3：配置 Chassis Management Module（CMM）

配置机箱中的主 Chassis Management Module（CMM）以管理机箱中的所有设备。

关于本任务

有关配置 CMM 的详细信息，请参阅Flex System 在线文档中的 “配置机箱组件”。

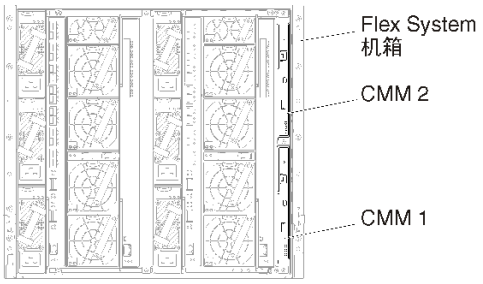
另请参阅机箱随附的说明书中的步骤 4.1 - 4.5。

过程

完成以下步骤以配置 CMM。

如果装有两个 CMM，则仅配置*主* CMM，而后自动与备用 CMM 同步配置。

步骤 1. 将一条以太网线缆从插槽 1 中的 CMM 连接到客户端工作站以建立一个直接连接。



首次连接到 CMM 时，可能需要更改客户端工作站上的 Internet 协议属性。

重要：确保客户端工作站子网与 CMM 子网相同。（默认 CMM 子网为 **255.255.255.0**）。为客户端工作站选择的 IP 地址必须与 CMM 在同一网络上（例如，**192.168.70.0 - 192.168.70.24**）。

步骤 2. 要启动 CMM 管理界面，在客户端工作站上打开 Web 浏览器，然后访问 CMM IP 地址。

注：

- 确保使用安全连接并在 URL 中加入 **https**（例如，**https://192.168.70.100**）。如果不加入 **https**，则将发生“未找到页面”错误。
- 如果使用默认 IP 地址 **192.168.70.100**，则可能数分钟后才会显示 CMM 管理界面。发生这一延迟的原因是，CMM 先花两分钟时间尝试获取 DHCP 地址，之后才回退到默认静态地址。

步骤 3. 使用默认用户标识 USERID 和密码 PASSWORD 登录到 CMM 管理界面。登录后，必须更改默认密码。

步骤 4. 完成 CMM 初始安装向导以指定所处环境的详细信息。初始安装向导包括以下选项：

- 查看机箱清单和运行状况。
- 从现有配置文件导入配置。
- 配置常规 CMM 设置。
- 配置 CMM 日期和时间。

  提示：在安装 XClarity Administrator 时，您需要配置 XClarity Administrator 以及受 XClarity Administrator 管理的所有机箱以使用 NTP 服务器。
- 配置 CMM IP 信息。
- 配置 CMM 安全策略。
- 配置域名系统（DNS）。
- 配置事件转发器。

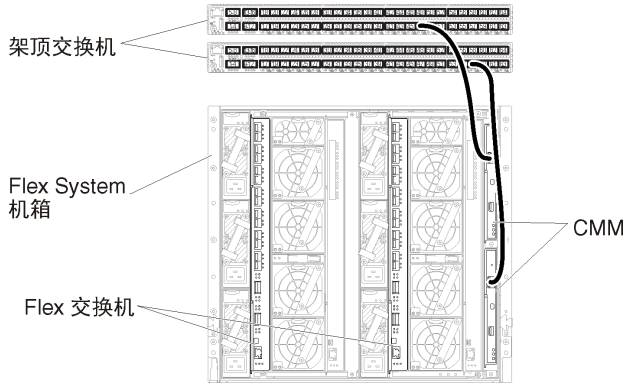
步骤 5. 保存安装向导设置并应用更改后，为机箱中的所有组件配置 IP 地址。

请参阅随机箱提供的说明书的步骤 **4.6**。

注：必须重置每个计算节点的系统管理处理器并重新启动 **Flex** 交换机才能显示新 **IP** 地址。

步骤 **6.** 使用 **CMM** 管理界面重新启动 **CMM**。

步骤 **7.** 当 **CMM** 重新启动时，将一条线缆从 **CMM** 上的以太网端口连接到网络。



步骤 **8.** 使用新 **IP** 地址登录到 **CMM** 管理界面。

完成之后

还可配置 **CMM** 以支持冗余。使用 **CMM** 帮助系统详细了解以下每个页面上可用的字段。

- 为 **CMM** 配置故障转移，以防主 **CMM** 出现硬件故障。从 **CMM** 管理界面中，单击**管理模块的管理 → 属性 → 高级故障转移**。
- 配置发生网络问题时的故障转移（上行链路）。从 **CMM** 管理界面中，依次单击**管理模块的管理 → 网络**、**以太网**选项卡、**高级以太网**。至少务必选中**在失去物理网络链路时进行故障转移**。

步骤 4：配置 Flex 交换机

配置每个机箱中的 **Flex** 交换机。

开始之前

确保已启用所有相应端口，包括从 **Flex** 交换机到架顶交换机的外部端口以及 **CMM** 的内部端口。

如果将 **Flex** 交换机设置为通过 **DHCP** 获取动态网络设置（**IP** 地址、网络掩码、网关和 **DNS** 地址），则确保 **Flex** 交换机的设置一致（例如，确保 **IP** 地址与 **CMM** 在同一子网中）。

重要：对于每个 **Flex System** 机箱，确保机箱中每个服务器内扩展卡的构造类型与同一机箱中所有 **Flex** 交换机的构造类型兼容。例如，如果机箱中装有以太网交换机，则该机箱中的所有服务器必须通过板载网卡接口或以太网扩展卡建立以太网连接。有关配置 **Flex** 交换机的详细信息，请参阅 **Flex System** 在线文档中的 “配置 **I/O** 模块”。

过程

配置步骤可能因所安装的 **Flex** 交换机类型而异。有关每个支持的 **Flex** 交换机的详细信息，请参阅 **Flex System** 在线文档中的 “**Flex System** 网络交换机”。

通常，必须配置 **Flex** 交换机插槽 **1** 和 **2** 中的 **Flex** 交换机。

提示：在查看机箱背面时，**Flex** 交换机插槽 **2** 是第三个模块插槽。

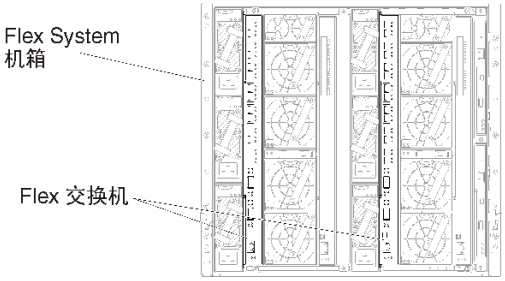


图 15. 机箱中的 Flex 交换机位置

步骤 5：安装和配置主机

可在任何满足 **Lenovo XClarity Administrator** 要求的服务器上安装 **Docker**。

开始之前

可以使用 **Docker Datacenter** 为 **Docker** 引擎中运行的 **XClarity Administrator** 容器设置高可用性环境。有关 **Docker Datacenter** 高可用性的详细信息，请参阅“使用 **Docker Datacenter** 实现高可用性架构 和应用程序”网页。

确保主机满足 **XClarity Administrator** 在线文档中的硬件和软件先决条件。

确保主机系统与要管理的设备在同一网络上。

重要：可在包括受管服务器在内的任何满足 **XClarity Administrator** 要求的系统上设置 **XClarity Administrator**。如果将受管服务器用于 **XClarity Administrator** 主机，则：

- 必须实现虚拟隔离的数据和管理网络拓扑或单一数据和管理网络拓扑。
- 不得使用 **XClarity Administrator** 将固件更新应用于该受管服务器。即便仅有某些固件在应用时立即激活，**XClarity Administrator** 仍强制目标服务器重新启动，而这还将重新启动 **XClarity Administrator**。在应用固件但延迟激活时，重新启动 **XClarity Administrator** 主机后仅应用某些固件。
- 如果使用 **Flex System** 机箱中的服务器，请确保该服务器设置为自动开机。可从 **CMM Web** 界面中设置此选项，具体方法是单击**机箱管理 → 计算节点**，选择该服务器，然后对**自动开机模式**选择**自动开机**。

过程

按 **Docker** 发行版提供的说明在主机上安装并配置 **Docker**。

步骤 6. 安装和配置 XClarity Administrator

在刚刚安装的 **Docker** 主机上安装和配置 **Lenovo XClarity Administrator** 容器。

开始之前

确保主机系统满足最低的硬件和软件要求（请参阅硬件和软件先决条件）。

确保已启用所有相应端口，包括 **XClarity Administrator** 需要的端口（请参阅端口可用性）。

确保主机系统与要管理的设备在同一网络上。

确保主机操作系统和 **XClarity Administrator** 使用相同的 **NTP** 服务器。

XClarity Administrator 允许对用于数据管理、硬件管理和操作系统部署的网络使用自定义名称（请参阅网络配置）。以下过程中的相应示例使用的是 **eth0**。

XClarity Administrator 允许对用于数据和硬件管理的网络和用于操作系统部署的网络使用自定义名称（请参阅网络配置）。以下过程中的相应示例分别使用 **eth0** 和 **eth1**。

确保在主机系统上的内核中加载了 **macvlan** 网络。要检查是否已加载该网络，请使用 **lsmod | grep macvlan** 命令。要将 **macvlan** 加载到内核中，请运行 **modprobe macvlan** 命令。

在同一主机上运行多个 **XClarity Administrator** 容器时，确保为每个容器使用唯一的名称和 **IP** 地址。

如果要管理 **ThinkServer** 和其他 **Legacy** 设备，请确保启用 **Docker** 以支持 **IPv6**。

1. 编辑 **/etc/docker/daemon.json** 文件，将 **ipv6** 键设为 **true**，并将 **fixed-cidr-v6** 键设为您的 **IPv6** 子网。以下是一个示例 **daemon** 文件。
```
{
  "ipv6": true,
  "fixed-cidr-v6": "2001:db8:1::/64",
  "experimental": true,
  "ip6tables": true
}
```
2. 运行以下命令重新加载 **Docker** 配置文件。
```
systemctl reload docker
```

注：XClarity Administrator *不是* 作为特权容器运行。

过程

要使用 **Docker compose** 安装 **XClarity Administrator** 容器，请完成以下步骤。

步骤 **1.** 从 **XClarity Administrator** 下载 **Web** 页面 将 **XClarity Administrator** 虚拟设备映像、环境文件和 **YAML** 文件下载到客户端工作站。登录到该网站，然后使用提供给您的访问密钥下载该映像。

步骤 **2.** 通过运行以下命令将 **XClarity Administrator** 容器镜像导入 **Docker** 主机。
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

步骤 **3.** 编辑 `docker_compose.env` 文件，更新以下环境变量。

- **CONTAINER_NAME**。唯一的容器名称，用于为每个 **XClarity Administrator** 实例创建 **Docker** 卷（例如，`CONTAINER_NAME=LXCA-203`）
- **ADDRESS**。容器的静态 **IPv4** 地址（例如，`ADDRESS=192.0.2.0`）
- **BACKUP_MOUNT**。（可选）可用于存储 **XClarity Administrator** 备份的远程共享路径。必须为 `/mnt/backup_share`。
- **FIRMWARE_MOUNT**。（可选）可用作固件更新远程存储库的远程共享路径。必须为 `/mnt/fw_share`。

以下是一个示例环境文件。

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

步骤 4. 编辑 docker_compose.yml，更新以下属性。

- 将 **image** 属性设置为步骤 **2** 中使用的安装映像文件的名称。

  注：可使用 `docker tag` 命令更改映像文件名（例如，更改为“**latest**”）。
- 如果要使用远程共享作为远程固件存储库并存储 **XClarity Administrator** 备份，请在 **volumes** 属性中为每个远程共享设置主机装载点。
- 将 **dns** 属性设为 **DNS** 服务器的 **IP** 地址。
- 容器会共享主机可用的处理器和内存资源池。（可选）通过设置 **cpus** 和 **memory** 属性来定义资源使用限制。
- 将 **parent** 属性设置为主机系统上的网络接口名称以用作容器中 **macvlan** 接口的父接口。此接口必须可以直接访问分配给容器的子网。
- 根据您的网络拓扑设置 **subnet** 和 **gateway**。通常，子网和网关用于 **${ADDRESS}** 所属的管理网络。
- 如果要支持 **IPv6**，请将 **enable_ipv6** 属性设为 **true**，将 **ipv6_address** 属性设为 **IPv6** 地址，并根据您的网络拓扑再添加一组 **subnet** 和 **gateway** 属性（通常针对该 **IPv6** 地址所属的管理网络）。

下面是启用了 **IPv6** 的 **YML** 文件示例。

```
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"
```

步骤 5. 通过运行以下命令在 Docker 中部署映像，其中 *<ENV_FILENAME>* 是在步骤 2 中创建的环境变量文件的名称。

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

完成之后

登录并配置 XClarity Administrator（请参阅首次访问 Lenovo XClarity Administrator Web 界面和配置 Lenovo XClarity Administrator）。

虚拟隔离的数据和管理网络拓扑

在此拓扑中，虚拟地将数据网络与管理网络隔离。通过同一物理连接发送来自数据网络的数据包和来自管理网络的数据包。对所有管理网络数据包使用 VLAN 标记以隔离两个网络之间的流量。

开始之前

确保已启用所有相应端口，包括 XClarity Administrator 需要的端口（请参阅端口可用性）。

确保要使用 XClarity Administrator 管理的每个设备上都至少装有所需的最低版本固件。可在“XClarity Administrator 支持 – 兼容性” Web 页面 中单击 Compatibility（兼容性）选项卡，然后单击相应设备类型的链接，找到所需的最低固件级别。

确保已为数据网络和管理网络设置 VLAN ID。（可选）如果从 Flex 交换机中实现 VLAN 标记，则从 Flex 交换机中启用标记；如果从架顶交换机中实现标记，则从架顶交换机中启用。

确保将 CMM 连接到的端口定义为属于管理 VLAN。

重要：配置设备和组件时尽量少更改 IP 地址。考虑使用静态 IP 地址代替动态主机配置协议（DHCP）。如果使用 DHCP，则务必尽量少更改 IP 地址。

关于本任务

下图显示一种方法，用于设置所处环境，以使管理网络与虚拟网络隔离。图中的数字对应于以下各节中的编号步骤。

注：此图并未完整显示您的环境可能需要的线缆连接选项。而是仅显示 Flex 交换机、CMM 和机架服务器的线缆连接选项要求，因为这些要求与设置虚拟隔离的数据和管理网络相关。

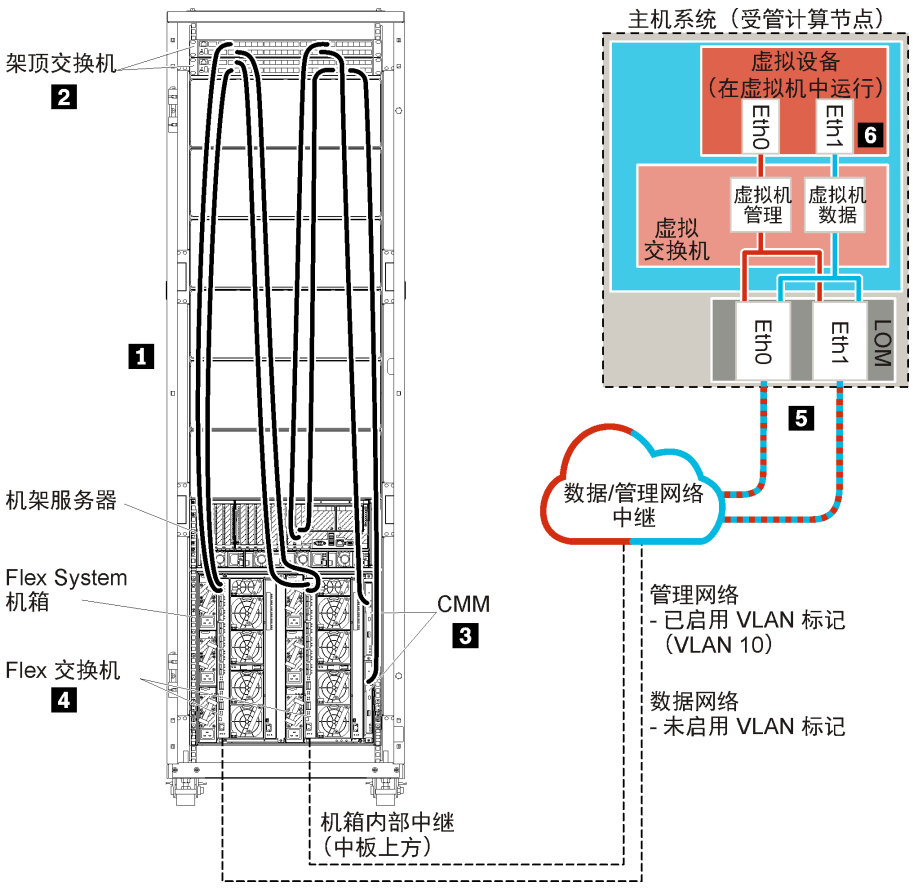


图 16. 虚拟设备的虚拟隔离的数据和管理网络拓扑示例

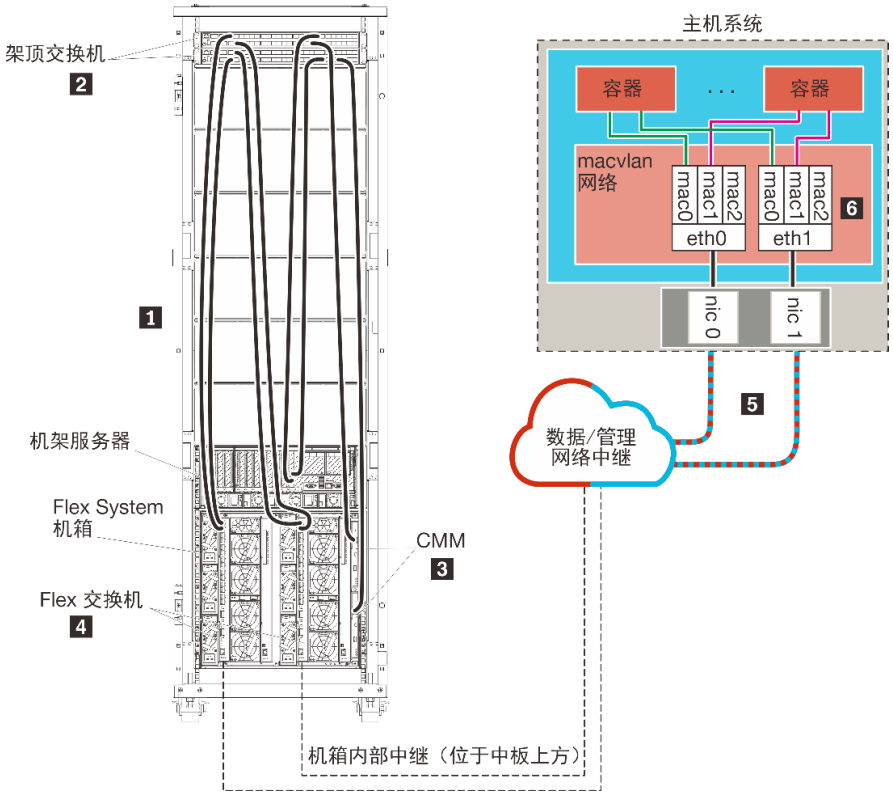


图 17. 容器的虚拟隔离的数据和管理网络拓扑示例

在这种情况下，**XClarity Administrator** 安装在受 **XClarity Administrator** 管理的 **Flex System** 机箱中的服务器上。

重要：可在包括受管服务器在内的任何满足 **XClarity Administrator** 要求的系统上设置 **XClarity Administrator**。如果将受管服务器用于 **XClarity Administrator** 主机，则：

- 必须实现虚拟隔离的数据和管理网络拓扑或单一数据和管理网络拓扑。
- 不得使用 **XClarity Administrator** 将固件更新应用于该受管服务器。即便仅有某些固件在应用时立即激活，**XClarity Administrator** 仍强制目标服务器重新启动，而这还将重新启动 **XClarity Administrator**。在应用固件但延迟激活时，重新启动 **XClarity Administrator** 主机后仅应用某些固件。
- 如果使用 **Flex System** 机箱中的服务器，请确保该服务器设置为自动开机。可从 **CMM Web** 界面中设置此选项，具体方法是单击**机箱管理 → 计算节点**，选择该服务器，然后对**自动开机模式**选择**自动开机**。

此外，在这种情况下，通过相同物理连接发送所有数据。管理网络与数据网络的分离是通过 **VLAN** 标记实现的，其中，与管理网络相对应的特定标记将附加到传入数据包，以确保数据包路由到相应接口。这些标记将从传出数据包移除。

可在以下设备之一上启用 **VLAN** 标记：

- **架顶交换机**。与管理网络相对应的 **VLAN** 标记在数据包进入架顶交换机时添加到数据包上，通过**Flex** 交换机进行传递，一直传递到 **Flex System** 机箱中的服务器。回程中在将数据包从架顶交换机发送到管理控制器时删除 **VLAN** 标记。

- **Flex 交换机**。在数据包进入Flex 交换机时向这些数据包添加与管理网络对应的 VLAN 标记，然后这些标记传递到 Flex System 机箱中的服务器。回程中，服务器添加 VLAN 标记并将其传递到Flex 交换机，后者在转发到管理控制器时删除这些标记。

是否实现 VLAN 标记是根据环境的需要与复杂性选择的。

如果要安装 XClarity Administrator 以管理已配置的现有机箱和机架服务器，请继续执行步骤 5: 安装和配置主机。

有关规划此拓扑的其他信息（包括有关网络设置以及 Eth1 和 Eth0 配置的信息），请参阅虚拟隔离的数据和管理网络。

步骤 1: 用线缆将机箱和机架服务器连接到架顶交换机

用线缆将机箱和机架服务器连接到同一架顶交换机以使设备之间可进行通信。

过程

用线缆将每个机箱中的每个 Flex 交换机和 CMM 以及每个机架服务器连接到两个架顶交换机。您可以选择该架顶交换机上的任何端口。

下图是一个示例，其中显示机箱中装有 Lenovo XClarity Administrator 的服务器将受 XClarity Administrator 管理时，从机箱（Flex 交换机和 CMM）和机架服务器到架顶交换机的线缆连接。

注：此图并未完整显示您的环境可能需要的线缆连接选项。而是仅显示 Flex 交换机、CMM 和机架服务器的线缆连接选项要求，因为这些要求与设置虚拟隔离的数据和管理网络相关。

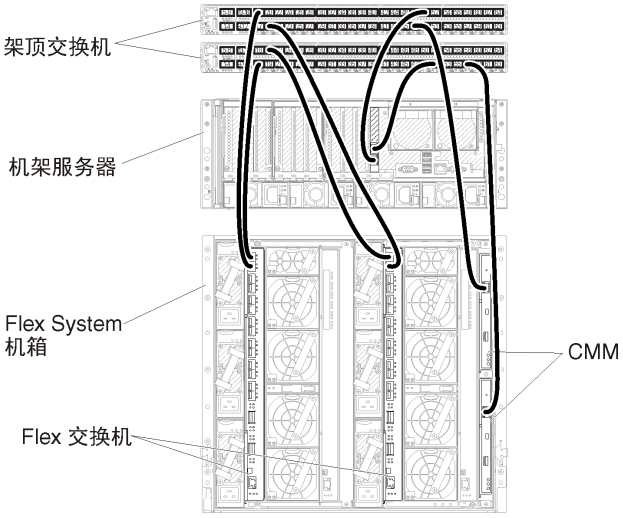


图 18. 虚拟隔离的数据和管理网络的示例线缆连接

步骤 2: 配置架顶交换机

配置架顶交换机。

开始之前

除满足架顶交换机的典型配置要求外，还应确保已启用所有相应端口，包括 **Flex** 交换机、机架服务器和网络的外部端口以及 **CMM**、机架服务器和网络的内部端口。

可根据环境的需要和复杂程度，在 **Flex** 交换机或架顶交换机中实现 **VLAN** 标记。如果从架顶交换机中实现标记，则从架顶交换机中启用 **VLAN** 标记。

确保已为管理网络和数据网络设置 **VLAN ID**。

过程

配置步骤可能因所安装的机架交换机类型而异。

下图是一个示例方案，其中显示在架顶交换机中实现但仅在管理网络上启用的 **VLAN** 标记。管理 **VLAN** 已设置为 **VLAN 10**。

在这种情况下，必须将 **CMM** 连接到的端口定义为属于管理 **VLAN**。

注：也可在数据网络上启用 **VLAN** 标记以配置数据 **VLAN**。

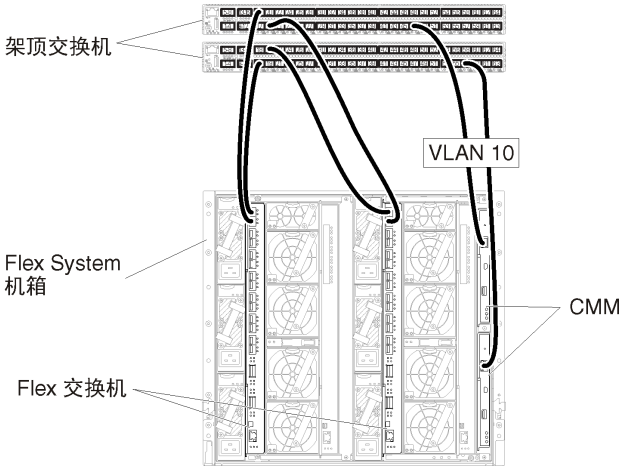


图 19. 在管理网络上启用 VLAN 标记的虚拟隔离的数据和管理网络（VMware ESXi）上 Flex 交换机的示例配置

有关配置 **Lenovo** 架顶交换机的信息，请参阅**System x** 在线文档中的“机架交换机”。如果装有其他架顶交换机，请参阅该交换机随附的文档。

步骤 3：配置 Chassis Management Module（CMM）

配置机箱中的主 **Chassis Management Module**（**CMM**）以管理机箱中的所有设备。

关于本任务

有关配置 **CMM** 的详细信息，请参阅**Flex System** 在线文档中的 “配置机箱组件”。

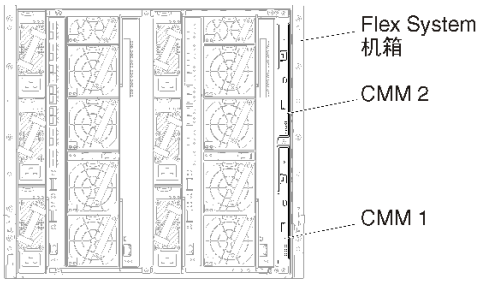
另请参阅机箱随附的说明书中的步骤 **4.1 - 4.5**。

过程

完成以下步骤以配置 CMM。

如果装有两个 CMM，则仅配置*主* CMM，而后自动与备用 CMM 同步配置。

步骤 1. 将一条以太网线缆从插槽 1 中的 CMM 连接到客户端工作站以建立一个直接连接。



首次连接到 CMM 时，可能需要更改客户端工作站上的 Internet 协议属性。

重要：确保客户端工作站子网与 CMM 子网相同。（默认 CMM 子网为 **255.255.255.0**）。为客户端工作站选择的 IP 地址必须与 CMM 在同一网络上（例如，**192.168.70.0 - 192.168.70.24**）。

步骤 2. 要启动 CMM 管理界面，在客户端工作站上打开 Web 浏览器，然后访问 CMM IP 地址。

注：

- 确保使用安全连接并在 URL 中加入 **https**（例如，**https://192.168.70.100**）。如果不加入 **https**，则将发生“未找到页面”错误。
- 如果使用默认 IP 地址 **192.168.70.100**，则可能数分钟后才会显示 CMM 管理界面。发生这一延迟的原因是，CMM 先花两分钟时间尝试获取 DHCP 地址，之后才回退到默认静态地址。

步骤 3. 使用默认用户标识 USERID 和密码 PASSWORD 登录到 CMM 管理界面。登录后，必须更改默认密码。

步骤 4. 完成 CMM 初始安装向导以指定所处环境的详细信息。初始安装向导包括以下选项：

- 查看机箱清单和运行状况。
- 从现有配置文件导入配置。
- 配置常规 CMM 设置。
- 配置 CMM 日期和时间。

  提示：在安装 **XClarity Administrator** 时，您需要配置 **XClarity Administrator** 以及受 **XClarity Administrator** 管理的所有机箱以使用 **NTP** 服务器。
- 配置 CMM IP 信息。
- 配置 CMM 安全策略。
- 配置域名系统（DNS）。
- 配置事件转发器。

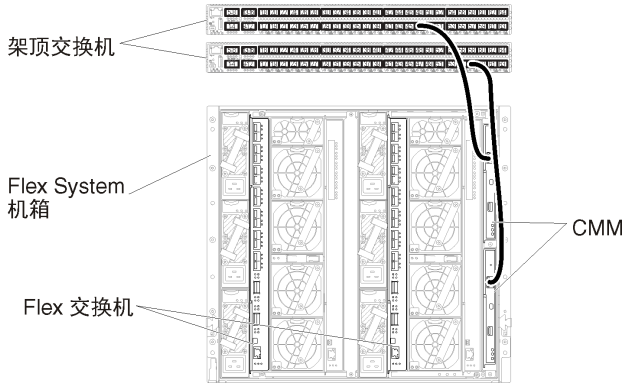
步骤 5. 保存安装向导设置并应用更改后，为机箱中的所有组件配置 IP 地址。

请参阅随机箱提供的说明书的步骤 **4.6**。

注：必须重置每个计算节点的系统管理处理器并重新启动 **Flex** 交换机才能显示新 **IP** 地址。

步骤 **6.** 使用 **CMM** 管理界面重新启动 **CMM**。

步骤 **7.** 当 **CMM** 重新启动时，将一条线缆从 **CMM** 上的以太网端口连接到网络。



步骤 **8.** 使用新 **IP** 地址登录到 **CMM** 管理界面。

完成之后

还可配置 **CMM** 以支持冗余。使用 **CMM** 帮助系统详细了解以下每个页面上可用的字段。

- 为 **CMM** 配置故障转移，以防主 **CMM** 出现硬件故障。从 **CMM** 管理界面中，单击**管理模块的管理 → 属性 → 高级故障转移**。
- 配置发生网络问题时的故障转移（上行链路）。从 **CMM** 管理界面中，依次单击**管理模块的管理 → 网络**、**以太网**选项卡、**高级以太网**。至少务必选中**在失去物理网络链路时进行故障转移**。

步骤 4：配置 Flex 交换机

配置每个机箱中的 **Flex** 交换机。

开始之前

确保已启用所有相应端口，包括从 **Flex** 交换机到架顶交换机的外部端口以及 **CMM** 的内部端口。

可根据环境的需要和复杂程度，在 **Flex** 交换机或架顶交换机中实现 **VLAN** 标记。如果从 **Flex** 交换机中实现标记，则从 **Flex** 交换机中启用 **VLAN** 标记。

确保已为管理网络和数据网络设置 **VLAN ID**。

重要：对于每个 **Flex System** 机箱，确保机箱中每个服务器内扩展卡的构造类型与同一机箱中所有 **Flex** 交换机的构造类型兼容。例如，如果机箱中装有以太网交换机，则该机箱中的所有服务器必须通过板载网卡接口或以太网扩展卡建立以太网连接。有关配置 **Flex** 交换机的详细信息，请参阅 **Flex System** 在线文档中的 **“配置 I/O 模块”**。

过程

配置步骤可能因所安装的 **Flex** 交换机类型而异。有关每个支持的 **Flex** 交换机的详细信息，请参阅 **Flex System** 在线文档中的 **“Flex System 网络交换机”**。

下图是一个示例方案，其中显示在 **Flex** 交换机中实现但仅在管理网络上启用的 **VLAN** 标记。管理 **VLAN** 已设置为 **VLAN 10**。

注：可通过在数据网络上启用 **VLAN** 标记，配置数据 **VLAN**。

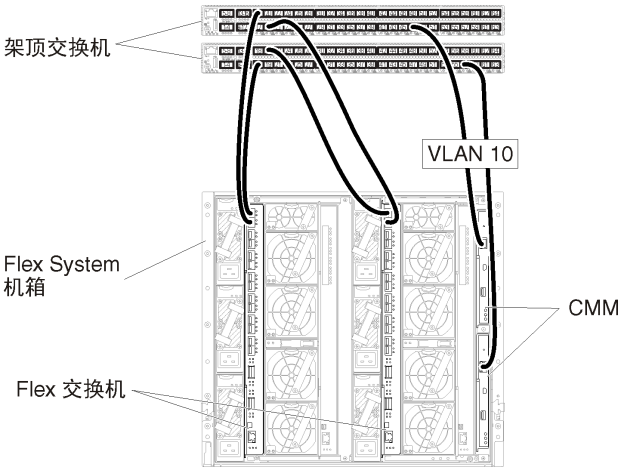


图 20. 在管理网络上启用 VLAN 标记的虚拟隔离的数据和管理网络（VMware ESXi）上 Flex 交换机的示例配置

完成以下步骤以配置此方案的 **Flex** 交换机：

步骤 **1.** 配置 **Flex** 交换机插槽 **1** 中的 **Flex** 交换机：

- **a.** 定义管理 **VLAN**（在本示例中，我们选择了 **VLAN 10**）以包含用于将线缆连接到架顶管理交换机的外部端口（**Ext1**）。
- **b.** 将一个内部端口定义为 **VLAN 10**（管理 **VLAN**）的一部分。务必在该端口上启用 **VLAN** 中继。

步骤 **2.** 配置 **Flex** 交换机插槽 **2** 中的 **Flex** 交换机：

提示：如果从机箱的背面看，**Flex** 交换机插槽 **2** 实际上是第三个模块插槽：

- **a.** 定义管理 **VLAN**（在本示例中，我们选择了 **VLAN 10**）以包含用于将线缆连接到架顶管理交换机的外部端口。
- **b.** 将一个内部端口定义为 **VLAN 10**（管理 **VLAN**）的一部分。务必在该端口上启用 **VLAN** 中继。

步骤 5：安装和配置主机

您可在任何满足 **Lenovo XClarity Administrator** 要求的系统上安装 **Docker**。

开始之前

可以使用 **Docker Datacenter** 为 **Docker** 引擎中运行的 **XClarity Administrator** 容器设置高可用性环境。有关 **Docker Datacenter** 高可用性的详细信息，请参阅“使用 **Docker Datacenter** 实现高可用性架构 和应用程序”网页。

确保主机满足 **XClarity Administrator** 在线文档中的硬件和软件先决条件。

确保主机系统与要管理的设备在同一网络上。

重要：可在包括受管服务器在内的任何满足 XClarity Administrator 要求的系统上设置 XClarity Administrator。如果将受管服务器用于 XClarity Administrator 主机，则：

- 必须实现虚拟隔离的数据和管理网络拓扑或单一数据和管理网络拓扑。
- 不得使用 XClarity Administrator 将固件更新应用于该受管服务器。即便仅有某些固件在应用时立即激活，XClarity Administrator 仍强制目标服务器重新启动，而这还将重新启动 XClarity Administrator。在应用固件但延迟激活时，重新启动 XClarity Administrator 主机后仅应用某些固件。
- 如果使用 Flex System 机箱中的服务器，请确保该服务器设置为自动开机。可从 CMM Web 界面中设置此选项，具体方法是单击**机箱管理 → 计算节点**，选择该服务器，然后对**自动开机模式**选择**自动开机**。

过程

按 Docker 发行版提供的说明在主机上安装并配置 Docker。

步骤 6. 安装和配置 XClarity Administrator

在刚刚安装的 Docker 主机上安装和配置 Lenovo XClarity Administrator 容器。

开始之前

确保主机系统满足最低的硬件和软件要求（请参阅硬件和软件先决条件）。

确保已启用所有相应端口，包括 XClarity Administrator 需要的端口（请参阅端口可用性）。

确保主机系统与要管理的设备在同一网络上。

确保主机操作系统和 XClarity Administrator 使用相同的 NTP 服务器。

XClarity Administrator 允许对用于数据管理、硬件管理和操作系统部署的网络使用自定义名称（请参阅网络配置）。以下过程中的相应示例使用的是 **eth0**。

XClarity Administrator 允许对用于数据和硬件管理的网络和用于操作系统部署的网络使用自定义名称（请参阅网络配置）。以下过程中的相应示例分别使用 **eth0** 和 **eth1**。

确保在主机系统上的内核中加载了 **macvlan** 网络。要检查是否已加载该网络，请使用 **lsmod | grep macvlan** 命令。要将 **macvlan** 加载到内核中，请运行 **modprobe macvlan** 命令。

在同一主机上运行多个 XClarity Administrator 容器时，确保为每个容器使用唯一的名称和 IP 地址。

如果要管理 ThinkServer 和其他 Legacy 设备，请确保启用 Docker 以支持 IPv6。

1. 编辑 **/etc/docker/daemon.json** 文件，将 **ipv6** 键设为 **true**，并将 **fixed-cidr-v6** 键设为您的 IPv6 子网。以下是一个示例 **daemon** 文件。

```
{
  "ipv6": true,
  "fixed-cidr-v6": "2001:db8:1::/64",
  "experimental": true,
```

```
  "ip6tables": true
}
```

2. 运行以下命令重新加载 **Docker** 配置文件。
```
systemctl reload docker
```

注：XClarity Administrator *不是* 作为特权容器运行。

过程

要使用 **Docker compose** 安装 **XClarity Administrator** 容器，请完成以下步骤。

步骤 1. 从 **XClarity Administrator 下载 Web 页面** 将 **XClarity Administrator** 虚拟设备映像、环境文件和 **YAML** 文件下载到客户端工作站。登录到该网站，然后使用提供给您的访问密钥下载该映像。

步骤 2. 通过运行以下命令将 **XClarity Administrator** 容器镜像导入 **Docker** 主机。
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

步骤 3. 编辑 `docker_compose.env` 文件，更新以下环境变量。

- **CONTAINER_NAME**。唯一的容器名称，用于为每个 **XClarity Administrator** 实例创建 **Docker** 卷（例如，`CONTAINER_NAME=LXCA-203`）
- **ADDRESS**。容器的静态 **IPv4** 地址（例如，`ADDRESS=192.0.2.0`）
- **BACKUP_MOUNT**。（可选）可用于存储 **XClarity Administrator** 备份的远程共享路径。必须为 `/mnt/backup_share`。
- **FIRMWARE_MOUNT**。（可选）可用作固件更新远程存储库的远程共享路径。必须为 `/mnt/fw_share`。

以下是一个示例环境文件。
```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

步骤 4. 编辑 `docker_compose.yml`，更新以下属性。

- 将 **image** 属性设置为步骤 2 中使用的安装映像文件的名称。

  注：可使用 `docker tag` 命令更改映像文件名（例如，更改为“**latest**”）。
- 如果要使用远程共享作为远程固件存储库并存储 **XClarity Administrator** 备份，请在 **volumes** 属性中为每个远程共享设置主机装载点。
- 将 **dns** 属性设为 **DNS** 服务器的 **IP** 地址。
- 容器会共享主机可用的处理器和内存资源池。（可选）通过设置 **cpus** 和 **memory** 属性来定义资源使用限制。
- 将 **parent** 属性设置为主机系统上的网络接口名称以用作容器中 **macvlan** 接口的父接口。此接口必须可以直接访问分配给容器的子网。
- 根据您的网络拓扑设置 **subnet** 和 **gateway**。通常，子网和网关用于 **${ADDRESS}** 所属的管理网络。
- 如果要支持 **IPv6**，请将 **enable_ipv6** 属性设为 **true**，将 **ipv6_address** 属性设为 **IPv6** 地址，并根据您的网络拓扑再添加一组 **subnet** 和 **gateway** 属性（通常针对该 **IPv6** 地址所属的管理网络）。

下面是启用了 **IPv6** 的 **YML** 文件示例。

```
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"
```

步骤 5. 通过运行以下命令在 Docker 中部署映像，其中 *<ENV_FILENAME>* 是在步骤 2 中创建的环境变量文件的名称。

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

完成之后

登录并配置 XClarity Administrator（请参阅首次访问 Lenovo XClarity Administrator Web 界面和配置 Lenovo XClarity Administrator）。

仅限于管理的网络拓扑

在此拓扑中，Lenovo XClarity Administrator 仅有管理网络。而没有数据网络。

开始之前

确保已启用所有相应端口，包括：

- XClarity Administrator 需要的端口（请参阅 XClarity Administrator 在线文档中的端口可用性）
- 网络的外部端口
- CMM 的内部端口

确保要使用 XClarity Administrator 管理的每个设备上都至少装有所需的最低版本固件。可在“XClarity Administrator 支持 – 兼容性” Web 页面 中单击 Compatibility（兼容性）选项卡，然后单击相应设备类型的链接，找到所需的最低固件级别。

重要：配置设备和组件时尽量少更改 IP 地址。考虑使用静态 IP 地址代替动态主机配置协议（DHCP）。如果使用 DHCP，则务必尽量少更改 IP 地址。

关于本任务

下图显示 **Lenovo XClarity Administrator** 只有管理网络（而无数据网络）时设置所处环境的一种方法。图中的数字对应于以下各节中的编号步骤。

注：此图并未完整显示您的环境可能需要的线缆连接选项。而是仅显示 **Flex** 交换机、**CMM** 和机架服务器的线缆连接选项要求，因为这些要求与设置仅限于管理的网络相关。

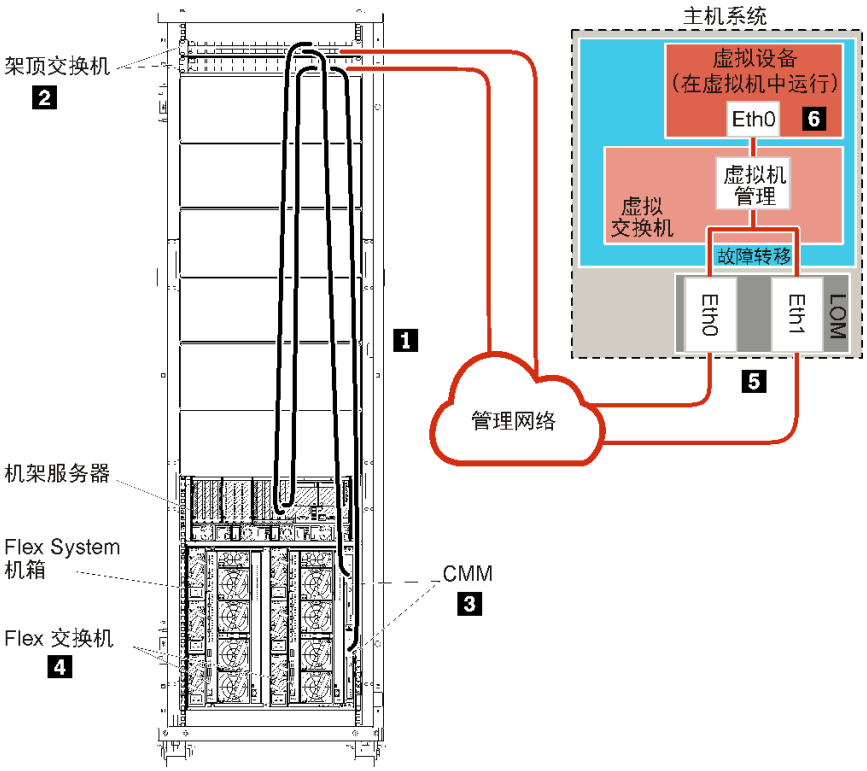


图 21. 虚拟设备仅限于管理的网络拓扑示例

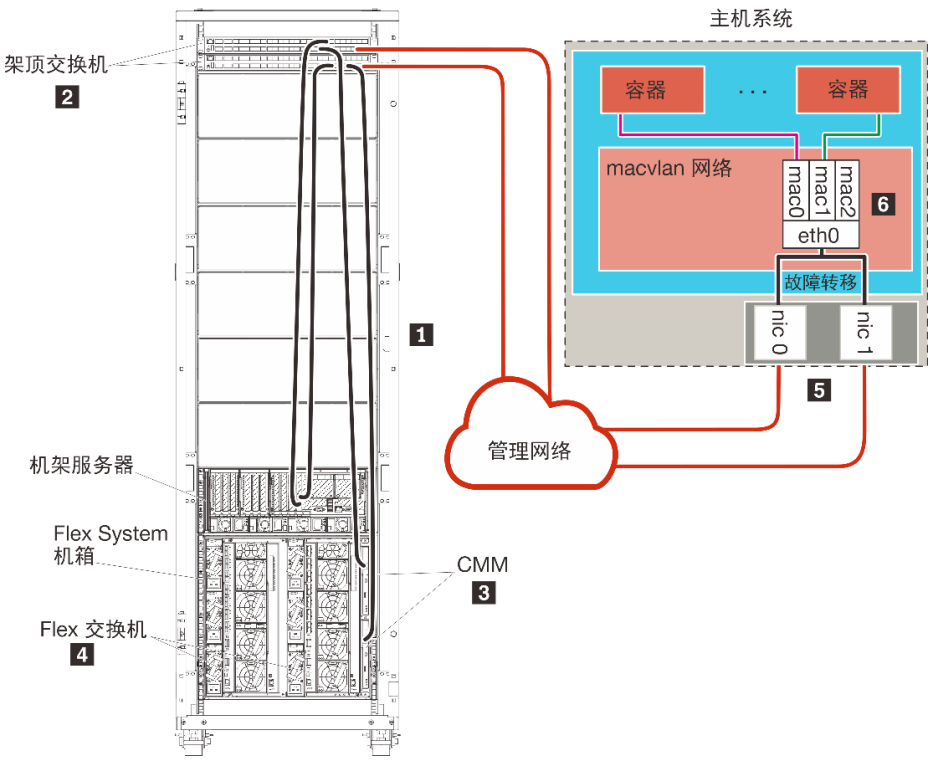


图 22. 容器仅限于管理的网络拓扑示例

如果要安装 **XClarity Administrator** 以管理已配置的现有机箱和机架服务器，请继续执行步骤 5：安装和配置主机。

有关规划此拓扑的其他信息（包括有关网络设置以及 **Eth1** 和 **Eth0** 配置的信息），请参阅仅限于管理的网络。

步骤 1：用线缆将机箱、机架服务器和 Lenovo XClarity Administrator 主机连接到架顶交换机

用线缆将机箱、机架服务器和 **XClarity Administrator** 主机连接到架顶交换机以使设备与您的网络之间可进行通信。

过程

用线缆将每个机箱中的每个 **Flex** 交换机和 **CMM**、每个机架服务器和 **XClarity Administrator** 主机连接到架顶交换机。可选择该架顶交换机中的任何端口。

下图是一个示例，其中显示用线缆将机箱（**Flex** 交换机和 **CMM**）、机架服务器和 **XClarity Administrator** 主机连接到架顶交换机。

注：此图并未完整显示您的环境可能需要的线缆连接选项。而是仅显示 **Flex** 交换机、**CMM** 和机架服务器的线缆连接选项要求，因为这些要求与设置仅限于管理的网络相关。

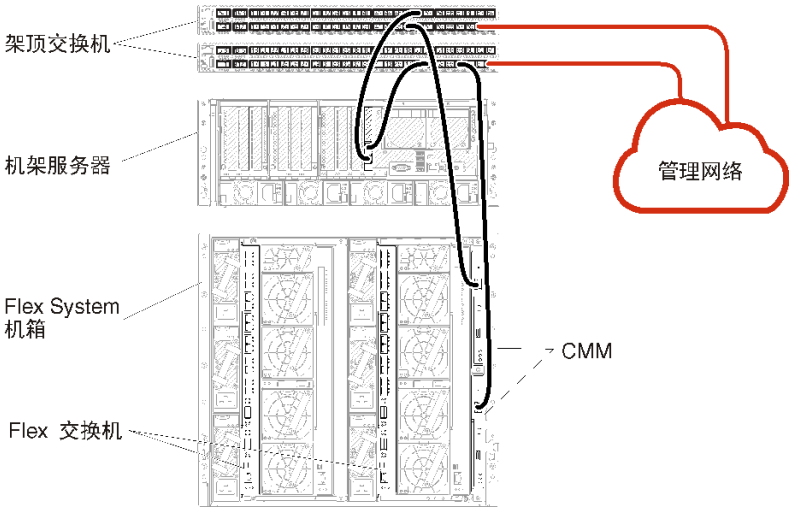


图 23. 仅限于管理的网络的示例线缆连接

步骤 2：配置架顶交换机

配置架顶交换机。

开始之前

除满足架顶交换机的典型配置要求外，还应确保已启用所有相应端口，包括 **Flex** 交换机、机架服务器和网络的外部端口以及 **CMM**、机架服务器和网络的内部端口。

过程

配置步骤可能因所安装的机架交换机类型而异。

有关配置 **Lenovo** 架顶交换机的信息，请参阅**System x** 在线文档中的“机架交换机”。如果装有其他架顶交换机，请参阅该交换机随附的文档。

步骤 3：配置 Chassis Management Module（CMM）

配置机箱中的主 **Chassis Management Module**（**CMM**）以管理机箱中的所有设备。

关于本任务

有关配置 **CMM** 的详细信息，请参阅**Flex System** 在线文档中的 “配置机箱组件”。

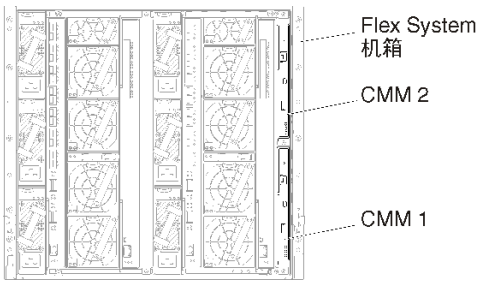
另请参阅机箱随附的说明书中的步骤 **4.1 - 4.5**。

过程

完成以下步骤以配置 **CMM**。

如果装有两个 **CMM**，则仅配置*主* **CMM**，而后自动与备用 **CMM** 同步配置。

步骤 **1**. 将一条以太网线缆从插槽 **1** 中的 **CMM** 连接到客户端工作站以建立一个直接连接。



首次连接到 CMM 时，可能需要更改客户端工作站上的 Internet 协议属性。

重要：确保客户端工作站子网与 CMM 子网相同。（默认 CMM 子网为 255.255.255.0）。为客户端工作站选择的 IP 地址必须与 CMM 在同一网络上（例如，192.168.70.0 - 192.168.70.24）。

步骤 2. 要启动 CMM 管理界面，在客户端工作站上打开 Web 浏览器，然后访问 CMM IP 地址。

注：

- 确保使用安全连接并在 URL 中加入 https（例如，https://192.168.70.100）。如果不加入 https，则将发生“未找到页面”错误。
- 如果使用默认 IP 地址 192.168.70.100，则可能数分钟后才会显示 CMM 管理界面。发生这一延迟的原因是，CMM 先花两分钟时间尝试获取 DHCP 地址，之后才回退到默认静态地址。

步骤 3. 使用默认用户标识 USERID 和密码 PASSWORD 登录到 CMM 管理界面。登录后，必须更改默认密码。

步骤 4. 完成 CMM 初始安装向导以指定所处环境的详细信息。初始安装向导包括以下选项：

- 查看机箱清单和运行状况。
- 从现有配置文件导入配置。
- 配置常规 CMM 设置。
- 配置 CMM 日期和时间。

  提示：在安装 XClarity Administrator 时，您需要配置 XClarity Administrator 以及受 XClarity Administrator 管理的所有机箱以使用 NTP 服务器。
- 配置 CMM IP 信息。
- 配置 CMM 安全策略。
- 配置域名系统（DNS）。
- 配置事件转发器。

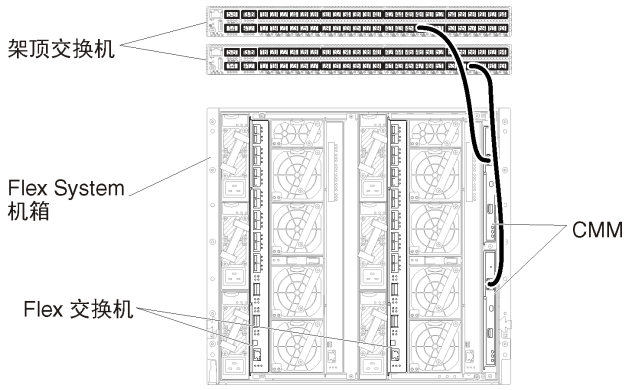
步骤 5. 保存安装向导设置并应用更改后，为机箱中的所有组件配置 IP 地址。

请参阅随机箱提供的说明书的步骤 4.6。

注：必须重置每个计算节点的系统管理处理器并重新启动 Flex 交换机才能显示新 IP 地址。

步骤 6. 使用 CMM 管理界面重新启动 CMM。

步骤 7. 当 CMM 重新启动时，将一条线缆从 CMM 上的以太网端口连接到网络。



步骤 8. 使用新 IP 地址登录到 CMM 管理界面。

完成之后

还可配置 CMM 以支持冗余。使用 CMM 帮助系统详细了解以下每个页面上可用的字段。

- 为 CMM 配置故障转移，以防主 CMM 出现硬件故障。从 CMM 管理界面中，单击**管理模块的管理 → 属性 → 高级故障转移**。
- 配置发生网络问题时的故障转移（上行链路）。从 CMM 管理界面中，依次单击**管理模块的管理 → 网络**、**以太网**选项卡、**高级以太网**。至少务必选中**在失去物理网络链路时进行故障转移**。

步骤 4：配置 Flex 交换机

配置每个机箱中的 Flex 交换机。

开始之前

确保已启用所有相应端口，包括从 Flex 交换机到架顶交换机的外部端口以及 CMM 的内部端口。

如果将 Flex 交换机设置为通过 DHCP 获取动态网络设置（IP 地址、网络掩码、网关和 DNS 地址），则确保 Flex 交换机的设置一致（例如，确保 IP 地址与 CMM 在同一子网中）。

重要：对于每个 Flex System 机箱，确保机箱中每个服务器内扩展卡的构造类型与同一机箱中所有 Flex 交换机的构造类型兼容。例如，如果机箱中装有以太网交换机，则该机箱中的所有服务器必须通过板载网卡接口或以太网扩展卡建立以太网连接。有关配置 Flex 交换机的详细信息，请参阅 Flex System 在线文档中的 “配置 I/O 模块”。

过程

配置步骤可能因所安装的 Flex 交换机类型而异。有关每个支持的 Flex 交换机的详细信息，请参阅 Flex System 在线文档中的 “Flex System 网络交换机”。

通常，必须配置 Flex 交换机插槽 1 和 2 中的 Flex 交换机。

提示：在查看机箱背面时，Flex 交换机插槽 2 是第三个模块插槽。

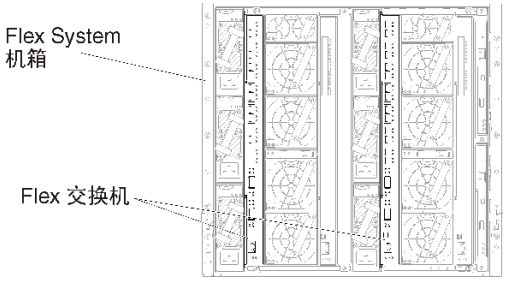


图 24. 机箱中的 Flex 交换机位置

步骤 5: 安装和配置主机

您可在任何满足 **Lenovo XClarity Administrator** 要求的系统上安装 **Docker**。

开始之前

可以使用 **Docker Datacenter** 为 **Docker** 引擎中运行的 **XClarity Administrator** 容器设置高可用性环境。有关 **Docker Datacenter** 高可用性的详细信息，请参阅“使用 **Docker Datacenter** 实现高可用性架构 和应用程序”网页。

确保主机满足 **XClarity Administrator** 在线文档中的硬件和软件先决条件。

确保主机系统与要管理的设备在同一网络上。

重要：可在包括受管服务器在内的任何满足 **XClarity Administrator** 要求的系统上设置 **XClarity Administrator**。如果将受管服务器用于 **XClarity Administrator** 主机，则：

- 必须实现虚拟隔离的数据和管理网络拓扑或单一数据和管理网络拓扑。
- 不得使用 **XClarity Administrator** 将固件更新应用于该受管服务器。即便仅有某些固件在应用时立即激活，**XClarity Administrator** 仍强制目标服务器重新启动，而这还将重新启动 **XClarity Administrator**。在应用固件但延迟激活时，重新启动 **XClarity Administrator** 主机后仅应用某些固件。
- 如果使用 **Flex System** 机箱中的服务器，请确保该服务器设置为自动开机。可从 **CMM Web** 界面中设置此选项，具体方法是单击**机箱管理 → 计算节点**，选择该服务器，然后对**自动开机模式**选择**自动开机**。

过程

按 **Docker** 发行版提供的说明在主机上安装并配置 **Docker**。

步骤 6. 安装和配置 XClarity Administrator

在刚刚安装的 **Docker** 主机上安装和配置 **Lenovo XClarity Administrator** 容器。

开始之前

确保主机系统满足最低的硬件和软件要求（请参阅硬件和软件先决条件）。

确保已启用所有相应端口，包括 **XClarity Administrator** 需要的端口（请参阅端口可用性）。

确保主机系统与要管理的设备在同一网络上。

确保主机操作系统和 XClarity Administrator 使用相同的 NTP 服务器。

XClarity Administrator 允许对用于数据管理、硬件管理和操作系统部署的网络使用自定义名称（请参阅网络配置）。以下过程中的相应示例使用的是 eth0。

XClarity Administrator 允许对用于数据和硬件管理的网络使用自定义名称（请参阅网络配置）。以下过程中的相应示例使用的是 eth0。

确保在主机系统上的内核中加载了 macvlan 网络。要检查是否已加载该网络，请使用 lsmod | grep macvlan 命令。要将 macvlan 加载到内核中，请运行 modprobe macvlan 命令。

在同一主机上运行多个 XClarity Administrator 容器时，确保为每个容器使用唯一的名称和 IP 地址。

如果要管理 ThinkServer 和其他 Legacy 设备，请确保启用 Docker 以支持 IPv6。

1. 编辑 /etc/docker/daemon.json 文件，将 ipv6 键设为 true，并将 fixed-cidr-v6 键设为您的 IPv6 子网。以下是一个示例 daemon 文件。
```
{
  "ipv6": true,
  "fixed-cidr-v6": "2001:db8:1::/64",
  "experimental": true,
  "ip6tables": true
}
```
2. 运行以下命令重新加载 Docker 配置文件。
```
systemctl reload docker
```

注：XClarity Administrator *不是* 作为特权容器运行。

过程

要使用 Docker compose 安装 XClarity Administrator 容器，请完成以下步骤。

步骤 1. 从 XClarity Administrator 下载 Web 页面 将 XClarity Administrator 虚拟设备映像、环境文件和 YAML 文件下载到客户端工作站。登录到该网站，然后使用提供给您的访问密钥下载该映像。

步骤 2. 通过运行以下命令将 XClarity Administrator 容器镜像导入 Docker 主机。
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

步骤 3. 编辑 docker_compose.env 文件，更新以下环境变量。

- CONTAINER_NAME。唯一的容器名称，用于为每个 XClarity Administrator 实例创建 Docker 卷（例如，CONTAINER_NAME=LXCA-203）
- ADDRESS。容器的静态 IPv4 地址（例如，ADDRESS=192.0.2.0）
- BACKUP_MOUNT。（可选）可用于存储 XClarity Administrator 备份的远程共享路径。必须为 /mnt/backup_share。
- FIRMWARE_MOUNT。（可选）可用作固件更新远程存储库的远程共享路径。必须为 /mnt/fw_share。

以下是一个示例环境文件。
```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
```

```
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

步骤 4. 编辑 docker_compose.yml，更新以下属性。

- 将 **image** 属性设置为步骤 **2** 中使用的安装映像文件的名称。

  注：可使用 `docker tag` 命令更改映像文件名（例如，更改为“**latest**”）。
- 如果要使用远程共享作为远程固件存储库并存储 **XClarity Administrator** 备份，请在 **volumes** 属性中为每个远程共享设置主机装载点。
- 将 **dns** 属性设为 **DNS** 服务器的 **IP** 地址。
- 容器会共享主机可用的处理器和内存资源池。（可选）通过设置 **cpus** 和 **memory** 属性来定义资源使用限制。
- 将 **parent** 属性设置为主机系统上的网络接口名称以用作容器中 **macvlan** 接口的父接口。此接口必须可以直接访问分配给容器的子网。
- 根据您的网络拓扑设置 **subnet** 和 **gateway**。通常，子网和网关用于 **${ADDRESS}** 所属的管理网络。
- 如果要支持 **IPv6**，请将 **enable_ipv6** 属性设为 **true**，将 **ipv6_address** 属性设为 **IPv6** 地址，并根据您的网络拓扑再添加一组 **subnet** 和 **gateway** 属性（通常针对该 **IPv6** 地址所属的管理网络）。

下面是启用了 **IPv6** 的 **YML** 文件示例。

```
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"
```

步骤 5. 通过运行以下命令在 Docker 中部署映像，其中 *<ENV_FILENAME>* 是在步骤 2 中创建的环境变量文件的名称。

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

完成之后

登录并配置 XClarity Administrator（请参阅首次访问 Lenovo XClarity Administrator Web 界面和配置 Lenovo XClarity Administrator）。

实现高可用性

可以使用 Docker Datacenter 为 Docker 引擎中运行的 Lenovo XClarity Administrator 容器设置高可用性环境。

有关 Docker Datacenter 高可用性的详细信息，请参阅“使用 Docker Datacenter 实现高可用性架构 和应用程序”网页。

第 4 章　配置 Lenovo XClarity Administrator

首次访问 Lenovo XClarity Administrator 时，必须完成几个步骤才能初始设置 XClarity Administrator。

了解更多： XClarity Administrator：首次配置

过程

完成以下步骤以首次设置 XClarity Administrator。

步骤 1. 访问 XClarity Administrator Web 界面。

步骤 2. 阅读并接受许可协议。

步骤 3. 创建具有主管权限的用户帐户。

提示：请考虑至少创建两个具有主管权限的用户帐户以备不时之需。

步骤 4. 配置网络访问权限，包括数据网络和管理网络的 IP 地址。

步骤 5. 配置日期和时间。

步骤 6. 配置服务和支持设置，包括隐私声明、使用情况和硬件数据、Lenovo 支持中心（Call Home）、Lenovo 上传设施和产品保修。

步骤 7. 配置安全设置，包括认证服务器、用户组、服务器证书和加密模式。

步骤 8. 管理机箱、服务器、交换机和存储设备。

首次访问 Lenovo XClarity Administrator Web 界面

可从任何与 XClarity Administrator 虚拟机具有网络连接的计算机中启动 XClarity Administrator Web 界面。

开始之前

务必使用以下某种支持的 Web 浏览器：

- Chrome™ 48.0 或更高版本（对于远程控制台，使用 55.0 或更高版本）
- Firefox® ESR 38.6.0 或更高版本
- Microsoft® Internet Explorer® 11
- Microsoft Edge
- Safari® 9.0.2 或更高版本（iOS7 或更高版本和 OS X）

注：不支持使用 Safari Web 浏览器从 XClarity Administrator 中启动管理控制器界面。

务必从与 XClarity Administrator 管理节点具有网络连接的系统中登录到 XClarity Administrator Web 界面。

过程

完成以下步骤以对 **XClarity Administrator Web** 界面进行首次访问。

步骤 **1.** 用浏览器访问 **XClarity Administrator** 的 **IP** 地址。

提示：通过安全连接访问 **Web** 界面。务必使用 **https**。

- **对于容器**，使用为 **${ADDRESS}** 变量指定的 **IPv4** 地址通过以下 **URL** 访问 **XClarity Administrator:**
  https://*<IPv4_address>*/ui/login.html

  例如：
  https://192.0.2.10/ui/login.html
- **对于虚拟设备**，要使用的 **IP** 地址取决于环境设置。

  如果 **Eth0** 和 **Eth1** 网络在不同的子网上，并且这两个子网上均使用 **DHCP**，则在访问 **Web** 界面进行初始设置时，请使用 ***Eth1*** **IP** 地址。首次启动 **XClarity Administrator** 时，**Eth0** 和 **Eth1** 均获取由 **DHCP** 分配的 **IP** 地址，并将 **XClarity Administrator** 默认网关设置为 ***Eth1*** 由 **DHCP** 分配的网关。

  使用静态 IPv4 地址

  如果在 **eth0_config** 中指定了 **IPv4** 地址，则使用该 **IPv4** 地址通过以下 **URL** 访问：**XClarity Administrator**
  https://*<IPv4_address>*/ui/login.html

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

  使用与 XClarity Administrator 位于同一个广播域中的 DHCP 服务器

  如果在与 **XClarity Administrator** 相同的广播域中设置了 **DHCP** 服务器，则使用在 **XClarity Administrator** 虚拟机控制台中显示的 **IPv4** 地址通过以下 **URL** 访问：**XClarity Administrator**
  https://*<IPv4_address>*/ui/login.html

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

  使用与 XClarity Administrator 位于不同广播域中的 DHCP 服务器

  如果*未*在同一广播域中设置 **DHCP** 服务器，则使用 **XClarity Administrator** 虚拟机控制台中为 **eEth0**（管理网络）显示的 **IPv6 Link-Local** 地址（**LLA**）访问 **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
 ... ...
```

提示：IPv6 Link-Local 地址（LLA）从接口的 MAC 地址派生而来。

注意：如果远程配置 XClarity Administrator，则必须与同一第 2 层网络建立连接。在完成初始设置之前，必须从非路由地址访问该网络。因此，请考虑从另一可连接到 XClarity Administrator 的虚拟机访问 XClarity Administrator。例如，可从装有 XClarity Administrator 的主机上的另一虚拟机访问 XClarity Administrator。

– **Firefox：**

  要从 **Firefox** 浏览器中访问 **XClarity Administrator Web** 界面，请使用以下 **URL** 登录。注：输入 **IPv6** 地址时需要使用括号。

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

  例如，根据所显示的前一 **Eth0** 示例，在 **Web** 浏览器中输入以下 **URL：**

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

– **Internet Explorer：**

  要从 **Internet Explorer** 浏览器中访问 **XClarity Administrator Web** 界面，请使用以下 **URL** 登录。注：输入 **IPv6** 地址时需要使用括号。

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

  其中 ***<zone_index>*** 是从启动 **Web** 浏览器的计算机连接到管理网络的以太网适配器的标识符。如果在 **Windows** 中使用浏览器，则使用 `ipconfig` 命令查找区域索引，它显示在适配器的**链路本地 IPv6 地址**字段中的百分号（**%**）之后。在以下示例中，区域索引为“**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 . . . . . .:
  ```

  如果使用 **Linux** 中的浏览器，则使用 `ifconfig` 命令查找该区域索引。还可使用适配器的名称（通常为 **Eth0**）作为区域索引。

  例如，根据所显示的 **Eth0** 和区域索引示例，在 **Web** 浏览器中输入以下 **URL：**

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

步骤 **2.** 首次访问 **Lenovo XClarity Administrator** 时可能会收到安全或证书警告。可忽略这些警告。

结果

随后将显示初始设置页面。

完成之后

完成初始设置步骤以配置 XClarity Administrator（请参阅配置 Lenovo XClarity Administrator）。

创建用户帐户

用户帐户用于管理对 Lenovo XClarity Administrator 和受到受管认证的设备的授权和访问。

关于本任务

所创建的第一个用户帐户必须具有主管角色，并且必须激活（启用）它。

为提高安全性，至少要创建两个具有主管角色的用户帐户。务必记录并妥善保管这些用户帐户的密码，在必须恢复 Lenovo XClarity Administrator 时要用到这些密码。

过程

要创建用户帐户，请完成以下步骤。

步骤 1. 填写“新建主管用户”对话框中的以下信息。

- 输入该用户的用户名和描述。
- 输入并确认新密码。密码的规则基于当前的帐户安全设置。

- 选择一个或多个角色组以授权用户执行相应任务。

  有关角色组和如何创建定制角色组的详细信息，请参阅创建角色组（位于 **XClarity Administrator** 在线文档中）。
- （可选）如果要强制用户在首次登录到 **XClarity Administrator** 时更改密码，则将**首次访问时更改密码**设置为 `Yes`。

步骤 **2.** 单击**创建**。

步骤 **3.** 单击**创建**图标（  ）并重复上述步骤以创建更多用户。

步骤 **4.** 单击**返回初始设置**。

配置网络访问权限

配置网络访问权限时，配置最多两个网络接口、**Lenovo XClarity Administrator** 的主机名，以及要使用的 **DNS** 服务器。

关于本任务

XClarity Administrator 有两个单独的网络接口可为所处环境定义，具体取决于所实现的网络拓扑。对于虚拟设备，这些网络命名为 **eth0** 和 **eth1**。对于容器，可以选择自定义名称。

- 仅存在一个网络接口（**eth0**）时：
  - 必须配置接口以支持设备发现和管理（如服务器配置和固件更新）。它必须可与每个受管机箱中的 **CMM** 和 **Flex** 交换机、每个受管服务器中的主板管理控制器，以及每个 **RackSwitch** 交换机通信。
  - 如果要使用 **XClarity Administrator** 获取固件和操作系统设备驱动程序更新，则必须有至少一个网络接口连接到 **Internet**，且最好通过防火墙。否则，必须将更新导入到存储库中。
  - 如果要收集服务数据或使用自动问题通知（包括 **Call Home** 和 **Lenovo** 上传设施），至少一个网络接口必须连接到 **Internet**，且最好通过防火墙。
  - 如果要部署操作系统映像并更新操作系统设备驱动程序，则此接口必须通过 **IP** 网络连接到用于访问主机操作系统的服务器网络接口。

    注：如果已实现一个单独的网络用于部署操作系统和更新操作系统设备驱动程序，则可将第二个网络接口配置为连接到该网络而非数据网络。但是，如果每个服务器上的操作系统均无权访问数据网络，则在服务器上另外配置一个接口以从主机操作系统连接到用于操作系统部署和操作系统设备驱动程序更新的数据网络（如果需要）
- 存在两个网络接口（**eth0** 和 **eth1**）时：
  - 第一个网络接口（通常是 **Eth0** 接口）必须连接到管理网络并配置为支持设备发现和管理（包括服务器配置和固件更新）。它必须可与每个受管机箱中的 **CMM** 和 **Flex** 交换机、每个受管服务器中的管理控制器，以及每个 **RackSwitch** 交换机通信。
  - 第二个网络接口（通常是 **eth1** 接口）可配置为与内部数据网络和/或公共数据网络进行通信。
  - 如果要使用 **XClarity Administrator** 获取固件和操作系统设备驱动程序更新，则必须有至少一个网络接口连接到 **Internet**，且最好通过防火墙。否则，必须将更新导入到存储库中。
  - 如果要收集服务数据或使用自动问题通知（包括 **Call Home** 和 **Lenovo** 上传设施），至少一个网络接口必须连接到 **Internet**，且最好通过防火墙。
  - 如果要部署操作系统映像并更新设备驱动程序，可选择使用 **eth1** 或 **eth0** 接口。但是，使用的接口必须通过 **IP** 网络连接到用于访问主机操作系统的服务器网络接口。

注：如果已实现一个单独的网络用于部署操作系统和更新操作系统设备驱动程序，则可将第二个网络接口配置为连接到该网络而非数据网络。但是，如果每个服务器上的操作系统均无权访问数据网络，则在服务器上另外配置一个接口以从主机操作系统连接到用于操作系统部署和操作系统设备驱动程序更新的数据网络（如果需要）

下表根据已在所处环境中实现的网络拓扑类型，显示 **XClarity Administrator** 网络接口可采用的配置。根据此表决定如何定义各网络接口。

表 3. 各网络接口的角色（基于网络拓扑）

网络拓扑	接口 1（eth0）的角色	接口 2（eth1）的角色
聚合网络（支持操作系统部署和操作系统设备驱动程序更新的管理和数据网络）	管理网络 • 发现和管理 • 服务器配置 • 固件更新 • 服务数据集合 • 自动通知问题（如 **Call Home** 和 **Lenovo** 更新设施） • 保修数据检索 • 操作系统部署 • 操作系统设备驱动程序更新	无
数据网络和支持操作系统部署和操作系统设备驱动程序更新的单独管理网络	管理网络 • 发现和管理 • 服务器配置 • 固件更新 • 服务数据集合 • 自动通知问题（如 **Call Home** 和 **Lenovo** 更新设施） • 保修数据检索 • 操作系统部署 • 操作系统设备驱动程序更新	数据网络 • 无
单独的管理网络和支持操作系统部署和操作系统设备驱动程序更新的数据网络	管理网络 • 发现和管理 • 服务器配置 • 固件更新 • 服务数据集合 • 自动通知问题（如 **Call Home** 和 **Lenovo** 更新设施） • 保修数据检索	数据网络 • 操作系统部署 • 操作系统设备驱动程序更新
单独的管理网络和不支持操作系统部署和操作系统设备驱动程序更新的数据网络	管理网络 • 发现和管理 • 服务器配置 • 固件更新 • 服务数据集合 • 自动通知问题（如 **Call Home** 和 **Lenovo** 更新设施） • 保修数据检索	数据网络 • 无
仅管理网络（不支持操作系统部署和操作系统设备驱动程序更新）	管理网络 • 发现和管理 • 服务器配置 • 固件更新 • 服务数据集合	无

表 3. 各网络接口的角色（基于网络拓扑）（续）

网络拓扑	接口 1（eth0）的角色	接口 2（eth1）的角色
	• 自动通知问题（如 Call Home 和 Lenovo 更新设施） • 保修数据检索	

有关 XClarity Administrator 网络接口的详细信息，请参阅 XClarity Administrator 在线文档中的网络注意事项。

过程

要配置网络访问权限，请完成以下步骤。

步骤 1. 从“初始设置”页面中，单击**配置网络访问权限**。随后将显示编辑网络访问权限页面。

步骤 2. 如果希望使用 XClarity Administrator 部署操作系统并更新操作系统设备驱动程序，请选择要用于管理操作系统的网络接口。

- 如果仅为 XClarity Administrator 定义了一个接口，请选择该接口是仅用于发现和管理硬件，还是也用于管理操作系统。
- 如果为 XClarity Administrator 定义了两个接口（**Eth0** 和 **Eth1**），请确定将哪个接口用于管理操作系统。如果选择“无”，则*无法* 从 XClarity Administrator 将操作系统映像部署到受管服务器，或将操作系统设备驱动程序更新到受管服务器。

步骤 3. 指定 IP 设置。

a. 对于第一个接口，请指定 IPv4 地址、IPv6 地址或两者。

- **IPv4**。必须为该接口分配一个 IPv4 地址。可决定使用静态分配的 IP 地址或从 DHCP 服务器获取 IP 地址。
- **IPv6**。您可以选择使用以下分配方法中的一种为接口分配 IPv6 地址：
  – 使用静态分配的 IP 地址

- 使用有状态的地址配置（**DHCPv6**）
- 使用无状态地址自动配置

注：有关 **IPv6** 地址限制的信息，请参阅IP 配置限制。

b. 如果第二个接口可用，请指定 **IPv4** 地址和/或 **IPv6** 地址。

注：分配给此接口的 **IP** 地址必须与分配给第一个接口的 **IP** 地址位于不同子网中。如果决定使用 **DHCP** 向这两个接口（**Eth0** 和 **Eth1**）分配 **IP** 地址，则 **DHCP** 服务器不得为这两个接口的 **IP** 地址分配同一子网。

- **IPv4**。可决定使用静态分配的 **IP** 地址或从 **DHCP** 服务器获取 **IP** 地址。
- **IPv6**。您可以选择使用以下分配方法中的一种为接口分配 **IPv6** 地址：
  - 使用静态分配的 **IP** 地址
  - 使用有状态的地址配置（**DHCPv6**）
  - 使用无状态地址自动配置

c. 指定默认网关。

指定默认网关时，必须使用有效的 **IP** 地址，并且必须使用与其中一个网络接口（**Eth0** 或 **Eth1**）的 **IP** 地址相同的网络掩码（同一子网）。如果只使用一个接口，默认网关必须与网络接口在同一子网上。

如果任何一个接口使用 **DHCP** 获取 **IP** 地址，则默认网关也使用 **DHCP**。要手动输入默认网关地址，从而覆盖从 **DHCP** 服务器收到的地址，请选中**覆盖网关**复选框。

提示：

- 请确保该网关与其中一个网络接口的子网匹配。默认网关会通过该网络接口自动设置。
- 要恢复使用 **DHCP** 提供的网关，请清除**覆盖网关**复选框。

警告：
如果选择覆盖网关，请注意输入正确的网关地址；否则，此管理软件将无法访问，并且无法远程登录进行纠正。

d. 单击**保存 IP 设置**。

步骤 **4.** 可选：**可选：**配置高级设置。

a. 单击**高级路由**选项卡。

b. 在**高级路由设置**表中指定要供此接口使用的一个或多个路由条目。

要定义一个或多个路由条目，请完成以下步骤。

1. 选择接口。

2. 指定路由类型，可以是到另一主机或网络的路由。
3. 指定将路由定向到的目标主机或网络地址。
4. 指定目标地址的子网掩码。
5. 指定数据包要寻址的网关地址。

c. 单击**保存高级路由**。

步骤 5. （可选）修改 DNS 和代理设置。

a. 单击 **DNS 和代理**选项卡。

b. 指定要用于 XClarity Administrator 的主机名和域名。

c. 选择 DNS 操作方式。可以是**静态**或 DHCP。

注意：更改 DNS 运行模式时，必须重新启动管理软件。

注：如果选择使用 DHCP 服务器获取 IP 地址，则下次 XClarity Administrator 续订 DHCP 租约时将覆盖对 DNS **服务器**字段作出的任何更改。

d. 指定要使用的一个或多个域名系统（DNS）服务器的 IP 地址，以及每个服务器的优先级顺序。

e. 指定使用直接连接还是 HTTP 代理访问 Internet（如果 XClarity Administrator 接入 Internet）。

注：如果使用 HTTP 代理，请确保满足以下要求。

- 确保代理服务器设置为使用基本认证。

- 务必将代理服务器设置为非终止代理。
- 务必将代理服务器设置为转发代理。
- 确保负载均衡器配置为保持与一个代理服务器之间的会话而不在二者之间切换。

如果选择使用 **HTTP** 代理，请完成必填字段：

1. 指定代理服务器主机名和端口。
2. 选择是否使用认证，并指定用户名和密码（如果需要）。
3. 指定代理测试 **URL**。
4. 单击**测试代理**以确认代理设置已正确配置且正常工作。

f. 单击**保存 DNS 和代理**。

g. 将 **XClarity Administrator** 管理软件完全限定域名（**FQDN**）和 **DNS** 信息推送给配备 **IMM2**、**XCC** 和 **XCC2** 的受管服务器，以便受管服务器可以使用这些信息找到管理软件。

1. 单击**将 FQDN/DNS 推送到 BMC**。
2. 选择如何处理主板管理控制器中的现有 **DNS** 条目。
   - 保留现有的 **DNS** 条目，并将管理软件 **DNS** 条目附加到下一个可用槽位中。
   - 将所有现有 **DNS** 条目替换为管理软件 **DNS** 条目。
3. 在编辑字段中输入 **YES**。
4. 单击**应用**。

随即会创建一个作业以执行此操作。可以从**监控 → 作业**卡监控该作业的进度。如果作业未成功完成，请单击作业链接以显示有关作业的详细信息（请参阅 **XClarity Administrator** 在线文档中的“使用作业”）。

还可以单击**从 BMC 中删除 FQDN/DNS**，从配备 **IMM2**、**XCC** 和 **XCC2** 的受管服务器中删除管理软件的 **FQDN** 和 **DNS** 信息。可以选择保留其他现有的 **DNS** 条目、删除所有 **DNS** 条目或仅删除与管理软件信息匹配的条目。

步骤 **6.** 单击**返回**。

步骤 **7.** 单击**测试连接**以验证网络设置。

配置日期和时间

虽然可手动设置 **Lenovo XClarity Administrator** 的日期和时间，但更好的方法是设置可用于在 **XClarity Administrator** 与所有受管设备之间同步时间戳的网络时间协议（**NTP**）服务器。

开始之前

必须使用至少一个（最多四个）网络时间协议（**NTP**）服务器将从受管设备收到的所有事件的时间戳与 **XClarity Administrator** 进行同步。

提示：必须可通过管理网络（通常为 **Eth0** 接口）访问 **NTP** 服务器。请考虑在运行 **XClarity Administrator** 的主机上设置该 **NTP** 服务器。

如果更改 **NTP** 服务器上的时间，则 **XClarity Administrator** 可能需要一段时间才能与新时间同步。

注意：必须将 **XClarity Administrator** 虚拟设备及其主机设置为同步到同一个时间源，以防止 **XClarity Administrator** 及其主机之间意外失去同步。通常情况下，主机配置为使其虚拟设备与

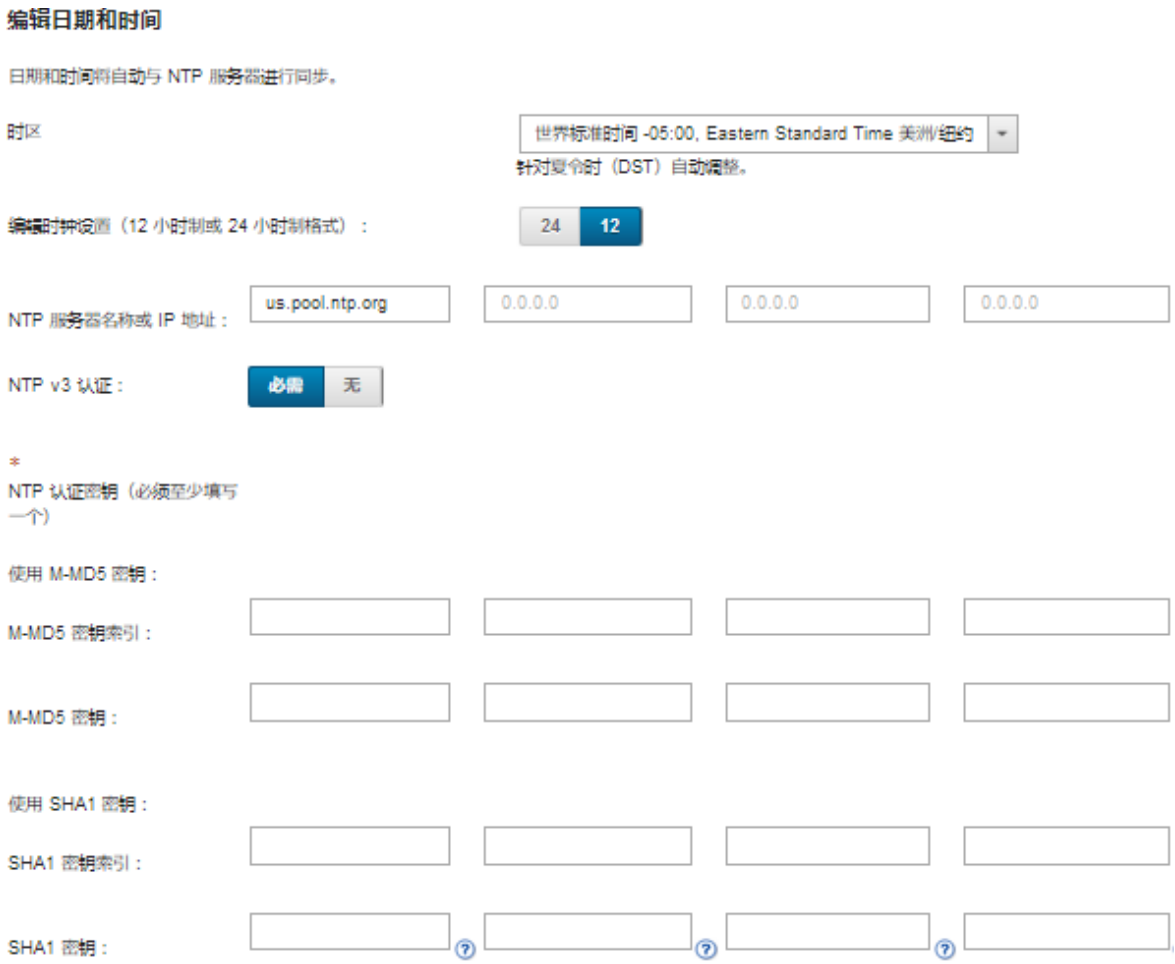
其进行时间同步。如果 XClarity Administrator 设置为同步到其主机之外的其他源，则必须禁用 XClarity Administrator 虚拟设备及其主机之间的主机时间同步。

- 对于 ESXi，请按照“VMware – 禁用时间同步” Web 页面上的说明进行操作。
- 对于 Hyper-V，在 Hyper-V 管理器中右键单击 XClarity Administrator 虚拟机，然后单击**设置**。在对话框中，单击导航窗格中的**管理 > 集成服务**，然后清除**时间同步**。

过程

要设置 XClarity Administrator 的 NTP 服务器，请完成以下步骤。

步骤 1. 从“初始设置”页面中，单击**配置日期和时间首选项**。随后显示编辑日期和时间页面。



步骤 2. 填写日期和时间对话框。

1. 选择 XClarity Administrator 主机所在的时区。

   如果所选时区采用夏令时（DST），则针对 DST 自动调整时间。
2. 选择使用 12 小时制或 24 小时制时钟。
3. 指定网络中每个 NTP 服务器的主机名或 IP 地址。最多可定义四个 NTP 服务器。
4. 选择**必需**以在 XClarity Administrator 与网络中的 NTP 服务器之间启用 NTP v3 认证，或选择**无**以使用 NTP v1 认证。

如果受管 **Flex System CMM** 和主板管理控制器有固件需要 **v3** 认证，而且 **XClarity Administrator** 与网络中的一个或多个 **NTP** 服务器之间需要 **NTP v3** 认证，则可使用 **v3** 认证。

5. 如果启用了 **NTP v3** 认证，请为每个适用的 **NTP** 服务器设置认证密钥和索引。可指定 **M-MD5** 密钥和/或 **SHA1** 密钥。如果同时指定 **M-MD5** 和 **SHA1** 密钥，**XClarity Administrator** 会将 **M-MD5** 或 **SHA1** 密钥推送到支持相应密钥的受管 **Flex System CMM** 和管理控制器。**XClarity Administrator** 使用该密钥向 **NTP** 服务器进行认证
   - 对 **M-MD5** 密钥指定的 **ASCII** 字符串应仅包含大小写字母（**a-z**、**A-Z**）、数字（**0–9**）和以下特殊字符 **@#**。
   - 对于 **SHA1** 密钥，指定一个 **40** 字符 **ASCII** 字符串，其中仅包含 **0 - 9** 和 **a - f**。
   - 指定的密钥索引和认证密钥必须与在 **NTP** 服务器上设置的密钥标识和密码值匹配。例如，如果在 **NTP** 服务器上输入的 **SHA1** 密钥的密钥索引为 **5**，则指定的 **XClarity Administrator SHA1** 密钥的密钥索引也应为 **5**。有关设置密钥标识和密码的详细信息，请参阅 **NTP** 服务器文档。
   - 必须为使用 **v3** 认证的每个 **NTP** 服务器指定此密钥，即使两个或更多 **NTP** 服务器使用同一个密钥也不例外。
   - 如果启用 **v3** 认证，但不为 **NTP** 服务器提供认证密钥和索引，默认情况下将使用 **v1** 认证。
   - 如果指定了多个 **NTP** 服务器，则 **NTP** 服务器必须全部采用 **v3** 认证或全部采用 **v1** 认证。不支持混合使用 **v3** 认证的 **NTP** 服务器和 **v1** 认证的 **NTP** 服务器。
   - 如果指定了多个采用 **v3** 认证的 **NTP** 服务器，并且密钥不同，则密钥索引必须唯一。例如，如果 **NTP** 服务器 **1** 和 **2** 中的 **SHA1** 密钥不同，则 **NTP** 服务器 **1** 和 **2** 的 **SHA1** 密钥索引不能为 **1**。必须将其中一个 **NTP** 服务器重新配置为接受密钥索引与另一个 **NTP** 服务器不同的密钥；否则，将为具有相同密钥索引的所有 **NTP** 服务器配置与密钥索引关联的最后一个定义的密钥。

步骤 **3**. 单击**保存**。

配置服务和支持

可配置服务和支持设置，包括使用数据、**Lenovo** 支持机构（**Call Home**）、**Lenovo** 上传设施和产品保修。

过程

完成以下步骤以配置安全性。

步骤 **1**. 从“初始设置”页面中，单击**配置服务与支持设置**。随后将显示服务与支持页面。

步骤 2. 阅读并接受 Lenovo 隐私声明。

注：如果不先接受 Lenovo 隐私声明，则不能收集数据并发送给 Lenovo。如果选择拒绝隐私声明，以后可以从**服务与支持** → **Call Home 配置**页面查看和接受隐私声明。

步骤 3. （可选）选择允许 **Lenovo XClarity Administrator** 收集使用情况信息和硬件信息，然后单击**应用**。

可以收集以下类型的数据并发送给 **Lenovo**。

- **使用情况数据**

  在您同意向 **Lenovo** 发送使用情况数据之后，将收集以下数据并每周一次发送。此数据*匿名*。不收集或向 **Lenovo** 发送隐私数据（包括序列号、**UUID**、主机名、**IP** 地址和用户名）。
  - 所执行操作的日志
  - 引发的事件的列表，以及引发时的时间戳
  - 引发的审核事件的列表，以及引发时的时间戳
  - 运行的作业的列表，以及各作业的成功或失败信息
  - **XClarity Administrator** 度量值，包括内存使用情况、处理器使用情况和磁盘空间
  - 有关所有受管设备的有限清单数据
- **硬件数据**

  在您同意向 **Lenovo** 发送硬件数据之后，将收集以下数据并定期发送。此数据*不匿名*。硬件数据包括属性，例如 **UUID** 和序列号。不包括 **IP** 地址或主机名。
  - **每天硬件数据**。包含每次清单更改的以下数据。

- 清单更改事件（**FQXHMDM0001I**）
- 对与该事件关联的设备的清单数据更改

– **每周硬件数据**。包含所有受管设备的清单数据。

向 Lenovo 发送使用情况数据和硬件数据时，将在审核日志中记录事件。

随时可以更改此设置，并使用链接下载最近收集并发送给 Lenovo 的存档，方法是单击**管理 → 服务与支持**，然后单击**定期上传数据**选项卡。

步骤 4. 可选择单击 **Call Home 配置**以设置自动向 Lenovo 支持机构（Call Home）发送问题通知。然后，单击**应用并启用**以创建默认 Call Home 服务转发器，或单击**仅应用**以保存联系信息。

有关设置自动向 Lenovo 支持机构发送问题通知的详细信息，请参阅设置 Call Home（位于 XClarity Administrator 在线文档中）。

步骤 5. （可选）单击 **Lenovo 上传设施**以设置自动将问题通知发送给 Lenovo 上传设施。然后，单击**应用并启用**以创建默认 Lenovo 上传设施服务转发器，或单击**仅应用**以保存设置信息。

有关设置自动向 Lenovo 上传设施发送问题通知的详细信息，请参阅设置自动向 Lenovo 上传设施 通知问题（位于 XClarity Administrator 在线文档中）。

步骤 6. （可选）单击**保修**以启用收集受管设备保修信息所需的外部连接。

有关查看受管设备保修状态（包括延长保修）的详细信息，请参阅查看保修信息（位于 XClarity Administrator 在线文档中）。

步骤 7. （可选）单击 **Lenovo 公告服务**以允许 Lenovo 将服务公告发送到 XClarity Administrator，然后单击**应用**。

有关 Lenovo 发送的服务公告类型的更多信息，请参阅 XClarity Administrator 在线文档中的“从 Lenovo 获取公告”。

步骤 8. 指定当 XClarity Administrator 失去响应且无法恢复时，可用于收集和下载服务数据和日志的服务恢复密码。

有关服务恢复密码的详细信息，请参阅 XClarity Administrator 在线文档中的更改服务恢复密码。

步骤 9. 单击**返回初始设置**。

配置安全性

可配置安全性，包括角色组、认证服务器、用户帐户安全设置、加密和证书。

过程

完成以下步骤以配置安全性。

步骤 1. 从“初始设置”页面中，单击**配置其他安全设置**。随后将显示安全性页面。

步骤 2. 创建定制角色组以管理对资源的授权和访问权限（请参阅 XClarity Administrator 在线文档中的创建角色组）。

角色组 是一个或多个角色的集合，用于将这些角色分配给多个用户。您为角色组配置的角色决定了授予该角色组每位成员用户的访问权级别。每个 **XClarity Administrator** 用户都必须是至少一个角色组的成员。

步骤 **3.** 配置认证服务器（请参阅 **XClarity Administrator** 在线文档中的管理认证服务器）。

认证服务器 是用于认证用户凭证的 **Microsoft Active Directory**（**LDAP**）服务器。**XClarity Administrator** 使用单个认证服务器集中对所有受管设备（**Flex** 交换机除外）进行用户管理。当设备受 **XClarity Administrator** 管理时，受管设备及其安装的组件（**Flex** 交换机除外）被配置为使用 **XClarity Administrator** 认证服务器。认证服务器中定义的用户帐户用于登录到 **XClarity Administrator**、**CMM** 和主板管理控制器。

可使用外部认证服务器代替管理节点上的本地认证服务器。

步骤 **4.** 配置用户帐户安全设置，这些设置控制密码复杂程度、帐户封锁和 **Web** 会话非活动超时（请参阅 **XClarity Administrator** 在线文档中的更改用户帐户安全设置）。

步骤 **5.** 配置加密设置，该设置用于定义控制 **XClarity Administrator** 与受管设备之间安全通信处理模式的通信模式和协议（请参阅 **XClarity Administrator** 在线文档中的设置加密模式和通信 协议）

步骤 **6.** 如果要使用本地认证而不是 **XClarity Administrator** 受管认证管理机架服务器，请创建一个或多个存储的凭证，并且这些凭证与设备上或 **Active Directory** 中可用于在管理过程中登录设备的活动用户帐户对应。有关存储的凭证的详细信息，请参阅管理存储的凭证（位于 **XClarity Administrator** 在线文档中）。

步骤 **7.** 如果打算使用包括您自己的信息的定制服务器证书或使用外部签署的证书，则生成并部署新证书，然后再开始管理系统。有关生成您自己的安全证书的信息，请参阅 **XClarity Administrator** 在线文档中的使用安全证书。

步骤 **8.** 从“安全性”页面上的垂直菜单中，单击**返回初始设置**。

管理设备

Lenovo XClarity Administrator 可管理多种类型的系统，包括 **Flex System** 机箱、机架和立式服务器、**RackSwitch** 交换机和存储设备。可使用批量导入文件导入设备的相关信息轻松发现和管理环境中的大量设备。

开始之前

重要:

- 一次最多可管理 **300** 台设备。批量导入文件中包含的设备不能超过 **300** 个。
- 启动设备管理操作后，请等待整个管理作业完成后再启动其他设备管理操作。

在管理包含机箱组件（如 **CMM**、计算节点、交换机和存储设备）的机箱时，将自动发现和管理这些机箱组件。脱离机箱即无法发现和管理机箱组件。

某些端口必须可用，以便与机箱中的 **CMM** 和服务器中的主板管理控制器进行通信。请确保这些端口可用，然后再尝试管理系统。有关端口的详细信息，请参阅 **XClarity Administrator** 在线文档中的端口可用性。

确保要使用 **XClarity Administrator** 管理的每个系统上都至少装有所需的最低版本固件。可在“**XClarity Administrator** 支持 – 兼容性” **Web** 页面 中单击 **Compatibility**（**兼容性**）选项卡，然后单击相应设备类型的链接，找到所需的最低固件级别。

确保至少设置三个 TCP Command 模式会话以便与 CMM 进行带外通信。有关设置会话数的详细信息，请参阅CMM 在线文档中的 tcpcmdmode 命令。

考虑为受 XClarity Administrator 管理的所有 CMM 和 Flex 交换机实现 IPv4 *或* IPv6 地址。如果为某些 CMM 和 Flex 交换机实现 IPv4，为其他交换机实现 IPv6，则可能无法在审核日志中（或作为审核陷阱）收到某些事件。

确保在机架顶部交换机以及所处环境的路由器上启用了多播 SLP 转发。要确定是否启用了多播 SLP 转发，如果禁用，要查找启用它的过程，请参阅特定交换机或路由器随附的文档。

重要：

- 根据 RackSwitch 交换机的固件版本，可能需要使用以下命令在每个 RackSwitch 交换机上手动启用多播 SLP 转发和 SSH，然后才可以由 XClarity Administrator 发现并管理该交换机。有关详细信息，请参阅System x 在线文档中的“机架交换机”。
- 必须先在每个存储设备上启用多播 SLP 转发，XClarity Administrator 才能发现该设备。
- 如果打算使用包括您自己的信息的定制服务器证书或使用外部签署的证书，则生成并部署新证书，然后再开始管理系统。有关生成您自己的安全证书的信息，请参阅 XClarity Administrator 在线文档中的使用安全证书。
- 如果除了 Lenovo XClarity Administrator 还要使用其他管理软件监控机箱，并且该管理软件使用 SNMPv3 通信，则必须先创建配置了相应 SNMPv3 信息的本地 CMM 用户标识，然后再使用该用户标识登录到 CMM 并更改密码。有关详细信息，请参阅 XClarity Administrator 在线文档中的管理注意事项。
- 服务发现协议（例如 SLP 和 SSDP）使 XClarity Administrator 能够自动发现即将受管的设备类型，然后使用适当的机制来管理设备。某些设备类型不支持服务发现协议；某些环境中还会有意关闭服务发现协议。无论哪种情况，都必须选择适当的设备类型来完成管理过程。必须明确识别以下设备类型。
  - Lenovo ThinkSystem DB 系列交换机
  - NVIDIA Mellanox 交换机

关于本任务

XClarity Administrator 可通过探测与 XClarity Administrator 在同一 IP 子网上的可管理设备、使用指定的 IP 地址或 IP 地址范围或从电子表格导入信息，发现所处环境中的系统。

默认情况下，设备的管理方式是使用 XClarity Administrator 受管认证登录。管理机架服务器和 Lenovo 机箱时，可选择使用本地认证或受管认证登录设备。

- 对机架服务器、Lenovo 机箱及 Lenovo 机架交换机使用*本地认证* 时，XClarity Administrator 使用存储的凭证对设备进行认证。*存储的凭证* 可以是设备上的活动用户帐户或 Active Directory 服务器中的用户帐户。

  使用本地认证管理设备之前必须在 XClarity Administrator 中创建中存储的凭证，且凭证须匹配设备上的活动用户帐户或者 Active Directory 服务器中的用户帐户（请参阅 XClarity Administrator 在线文档中的管理存储的凭证）。

  注：

  - RackSwitch 设备仅支持使用存储的凭证进行认证。XClarity Administrator 用户凭证不受支持。

- 借助*受管认证*，可使用 **XClarity Administrator** 认证服务器中的凭证（而非本地凭证）来管理和监控多个设备。对设备（而不是 **ThinkServer** 服务器、**System x M4** 服务器和交换机）使用受管认证时，**XClarity Administrator** 将设备及其安装的组件配置为使用 **XClarity Administrator** 认证服务器进行集中管理。
  - 启用受管认证后，可使用手动输入的凭证或存储的凭证管理设备（请参阅 **XClarity Administrator** 在线文档中的管理用户帐户以及管理存储的凭证）。

    仅当 **XClarity Administrator** 在设备上配置了 **LDAP** 设置，才会使用存储的凭证。此后，存储的凭证发生的任何更改都不会影响该设备的管理或监控。

    注：如果为设备启用了受管认证，则不能使用 **XClarity Administrator** 编辑该设备的存储的凭证。
  - 如果使用本地或外部 **LDAP** 服务器作为 **XClarity Administrator** 认证服务器，则应使用在该认证服务器中定义的用户帐户登录到 **XClarity Administrator** 域中的 **XClarity Administrator**、**CMM** 和主板管理控制器。而本地 **CMM** 和管理控制器用户帐户被禁用。
  - 如果使用 **SAML 2.0** 身份供应商作为 **XClarity Administrator** 认证服务器，则 **SAML** 帐户无法访问受管设备。但是，当 **SAML** 身份供应商与 **LDAP** 服务器一起使用时，如果该身份供应商使用存在于 **LDAP** 服务器中的 **LDAP** 帐户，则可使用 **LDAP** 用户帐户登录受管设备，而 **SAML 2.0** 提供的更高级认证方法（例如多重认证和单点登录）可用于登录 **XClarity Administrator**。
  - 借助单点登录功能，已登录 **XClarity Administrator** 的用户将可以自动登录到主板管理控制器。默认情况下，将 **ThinkSystem** 或 **ThinkAgile** 服务器设置为受 **XClarity Administrator** 管理的服务器后，即可启用单点登录（使用 **CyberArk** 密码管理服务器的情况除外）。可以通过配置全局设置来对所有受管 **ThinkSystem** 和 **ThinkAgile** 服务器启用或禁用单点登录。对特定 **ThinkSystem** 和 **ThinkAgile** 服务器启用单点登录会覆盖适用于所有 **ThinkSystem** 和 **ThinkAgile** 服务器的全局设置（请参阅 **XClarity Administrator** 在线文档中的“管理服务器”）。

    注：使用 **CyberArk** 标识管理系统进行认证时会自动禁用单点登录。
  - 为 **ThinkSystem SR635** 和 **SR655** 服务器启用受管认证时：
    - 主板管理控制器固件最多支持五个 **LDAP** 用户角色。**XClarity Administrator** 在管理期间将这些 **LDAP** 用户角色添加到服务器中：**lxc-supervisor**、**lxc-sysmgr**、**lxc-admin**、**lxc-fw-admin** 和 **lxc-os-admin**。

      必须至少为用户分配一个指定的 **LDAP** 用户角色，用户才能与 **ThinkSystem SR635** 和 **SR655** 服务器进行通信。
    - 管理控制器固件不支持与服务器本地用户具有相同用户名的 **LDAP** 用户。
  - 对于 **ThinkServer** 和 **System x M4** 服务器，不使用 **XClarity Administrator** 认证服务器。而是在设备上创建以“**LXCA_**”为前缀并后接随机字符串的 **IPMI** 帐户。（不会禁用现有的本地 **IPMI** 用户帐户。）终止管理 **ThinkServer** 服务器时，将禁用该“**LXCA_**”用户帐户，并将前缀“**LXCA_**”替换为前缀“**DISABLED_**”。为了确定 **ThinkServer** 服务器是否受另一实例管理，**XClarity Administrator** 检查是否存在以“**LXCA_**”为前缀的 **IPMI** 帐户。如果决定强制管理某个受管的 **ThinkServer** 服务器，则将禁用并重命名该设备上所有以“**LXCA_**”为前缀的 **IPMI** 帐户。请考虑手动清除不再使用的 **IPMI** 帐户。

    如果您使用手动输入的凭证，**XClarity Administrator** 将会自动创建存储的凭证，并使用该存储的凭证来管理设备。

    注：如果为设备启用了受管认证，则不能使用 **XClarity Administrator** 编辑该设备的存储的凭证。

- 每次使用手动输入的凭证管理设备时，将为该设备新建一个存储的凭证，即使在之前的管理过程中已为该设备创建过存储的凭证。
- 终止管理设备时，**XClarity Administrator** 不会删除管理过程中自动为该设备创建的存储的凭证。

在系统受 **XClarity Administrator** 管理后，**XClarity Administrator** 将定期轮询每个受管系统以收集系统清单、重要产品数据和状态等信息。可查看和监控每个受管系统并执行管理操作（如配置系统设置、部署操作系统映像以及打开和关闭电源）。

一个系统同时只能受一个 **XClarity Administrator** 管理。不支持受多个管理器管理。如果系统已受一个 **XClarity Administrator** 管理，而您要用另一 **XClarity Administrator** 管理它，则必须先在当前 **XClarity Administrator** 上终止管理该系统。然后，才能用另一 **XClarity Administrator** 管理该系统。有关终止管理系统的信息，请参阅 **XClarity Administrator** 在线文档中的取消管理机箱、终止管理服务器、终止管理 **RackSwitch** 交换机和终止管理 **Lenovo Storage** 存储系统。

注：XClarity Administrator 在管理过程中不修改安全设置或加密设置（加密模式和用于安全通信的模式）。可在系统受管理后修改加密设置（请参阅 **XClarity Administrator** 在线文档中的设置加密模式和通信 协议）。

注：XClarity Administrator 可预先插入模拟真实硬件的演示机箱（包括 **CMM**、计算节点和交换机）和演示机架或立式服务器的硬件清单。**Web** 界面页面中填充了演示设备，可用于演示管理操作；但是管理操作将失败。例如，可创建 **Configuration Pattern** 并将该 **pattern** 部署到演示服务器，但部署将失败。可通过终止管理演示设备来将其删除（请参阅 **XClarity Administrator** 在线文档中的取消管理机箱和终止管理服务器）。删除演示设备后将无法再次管理它们。

过程

要使用批量导入文件发现和管理 **XClarity Administrator** 中的系统，请完成以下步骤。

注：使用批量导入管理交换机时，交换机上启用 **HTTPS**，且交换机上的 **NTP** 客户端会配置为使用管理软件的 **NTP** 设置。要更改这些设置，必须手动管理交换机。

1. 从 **XClarity Administrator** 菜单栏中，单击**硬件 → 发现和管理新设备**。随后将显示发现和管理页面。
2. 在管理过程中单击**在所有未来受管设备上启用 Encapsulation** 复选框以更改所有设备上的防火墙规则，从而仅接受来自 **XClarity Administrator** 的传入请求。

   注：

   - 交换机、存储设备以及非 **Lenovo** 机箱和服务器不支持 **Encapsulation**。
   - 配置管理网络接口以使用动态主机配置协议（**DHCP**）并启用了 **Encapsulation** 时，管理机架服务器可能需要很长时间。

   管理特定设备后，可在这些设备上启用或禁用 **Encapsulation**。

   注意：如果启用了 **Encapsulation**，但 **XClarity Administrator** 在终止管理设备之前变为不可用状态，则必须采取必要步骤来禁用 **Encapsulation** 以便建立与设备的通信。有关恢复过程，请参阅 **XClarity Administrator** 在线文档中的在发生管理软件故障后用 **CMM** 恢复 管理机箱和在发生管理软件故障后恢复管理 机架或立式服务器。
3. 单击**批量导入**。随后将显示“批量导入”向导。

4. 单击“导入数据文件”页面上的 **Excel 格式**或 **CSV 格式**链接下载 **Excel** 或 **CSV** 格式的模板批量导入文件。

   重要：该模板文件可能会从一个发行版更改为下一个发行版。确保始终使用最新的模板。

5. 填写模板文件中的 **data** 工作表，然后将文件保存为 ***comma-delimited*** **CSV** 格式。

   提示：Excel 模板文件包括一个 **Data** 工作表和一个 **Readme** 工作表。使用 **Data** 工作表填写设备数据。**Readme** 工作表提供有关如何填写 **Data** 工作表上每个字段的信息（包括哪些字段为必填）以及示例数据。

   重要：

   - 按照批量导入文件中列出的顺序管理设备。
   - 设备受管时，**XClarity Administrator** 使用设备配置中定义的机架分配信息。如果在 **XClarity Administrator** 中更改了机架分配，**XClarity Administrator** 将更新设备配置。如果设备受管后更新了设备配置，**XClarity Administrator** 中将反映相关更改。
   - 建议（并非必需）在向设备分配机架前在工作表中显式创建一个机架。如果没有在 **XClarity Administrator** 中显示定义机架且其中先前不存在该机架，为设备指定的机架分配信息将使用 **52U** 的默认高度创建机架。

     如果想要对机架使用其他高度，必须在将机架分配给设备前在工作表中显示定义一个。

   要在批量导入文件中定义设备，请完成以下列。

   - （**A - C** 列）要进行基本发现，必须对设备指定设备类型以及当前的 **IP** 地址或序列号。支持以下类型：
     - **填充件**。终止管理设备的占位装置。在机架视图中，此设备显示为通用填充件图。请参阅 **Excel** 模板中的 **Readme** 工作表，了解其他填充件类型。
     - **flexchassis**。**10U Flex System** 机箱
     - **server**。**XClarity Administrator** 支持的机架和立式服务器
     - **rack**。**6U**、**12U**、**18U**、**25U**、**37U**、**42U**、**45U**、**46U**、**48U**、**50U** 和 **52U** 机架。不支持其他机架高度。默认情况下使用 **52U**。
     - **storage**。存储设备
     - **switch**。**RackSwitch** 交换机

     注：Flex System 计算节点、交换机和存储设备视为机箱发现和管理过程的组成部分。
   - （**D - H** 列）如果选择使用手动输入的凭证而不是存储的凭证（**Z** 列）或标识（**AF – AJ** 列），请指定当前的用户名和密码。如果某些设备的凭证不同，则可以选择手动输入的凭证。如果未在批量导入文件中指定一个或多个设备的凭证，则将改用在批量导入对话框中指

定的全局凭证。有关手动输入用户和受管认证的详细信息，请参阅 **XClarity Administrator** 在线文档中的管理用户帐户。

注：

- 要使用手动输入的凭证，必须选择 **XClarity Administrator** 受管认证。
- 某些字段不适用于某些设备。
- （对于机箱）如果选择受管认证（在 **AA** 列或“批量导入”对话框中），则必须在批量导入文件的 **G** 列或“批量导入”对话框中指定 RECOVERY_ID 密码。如果选择本地认证，则不允许使用恢复密码；请勿在批量导入文件的 **G** 列或“批量导入”对话框中指定恢复密码。
- （对于机架服务器）如果选择受管认证（在 **AA** 列或“批量导入”对话框中），则可选择在批量导入文件的 **G** 列或“批量导入”对话框中指定恢复密码。如果选择本地认证，则不允许使用恢复密码；请勿在批量导入文件的 **G** 列或“批量导入”对话框中指定恢复密码。
- （适用于机架交换机）**RackSwitch** 设备仅支持使用存储的凭证（位于 **Z** 列）向交换机进行认证。不支持手动输入用户凭证。

- （**I - U** 列）如果要在成功管理时将更改应用于设备，则可提供其他信息。

  注：某些字段不适用于某些设备。这些字段不适用于 **RackSwitch** 交换机。

- （**V - Z** 列）（可选）可提供用于创建和分配机架的信息，包括机架名称、位置、机室、最低机架单元值和高度。

  注：

  - 创建机架时，必须指定机架名称和机架高度。支持以下机架高度：**6U**、**12U**、**18U**、**25U**、**37U**、**42U**、**45U**、**46U**、**48U**、**50U** 和 **52U**。不支持其他机架高度。
  - 创建通用填充件时，必须指定机架名称和填充件高度。支持以下填充件高度：**1U**、**2U** 和 **4U**。
  - 创建特定填充件时会忽略填充件高度。**XClarity Administrator** 可识别每个特定填充件的高度。有关填充件类型和高度，请参阅模板电子表格。
  - 将设备分配到机架时会忽略设备高度。将从设备清单检索设备高度。

- （**AA** 列）如果管理因以下一种错误情况而未能成功，请使用强制管理选项重复上述过程。
  - 管理 **XClarity Administrator** 失败且无法恢复。

    注：如果更换的 **XClarity Administrator** 实例和发生故障的 **XClarity Administrator** 使用相同的 **IP** 地址，则可以使用 **RECOVERY_ID** 帐户和密码（如适用）以及强制管理选项再次管理设备。
  - 终止管理设备之前，管理 **XClarity Administrator** 是否已关闭。
  - 是否未能成功终止管理设备。

  设备同时只能受一个 **XClarity Administrator** 实例管理。不支持受多个 **XClarity Administrator** 实例管理。如果设备已受一个 **XClarity Administrator** 管理，而您要用另一 **XClarity Administrator** 管理它，则必须先在原始 **XClarity Administrator** 上终止管理该设备，然后用新的 **XClarity Administrator** 来管理它。

  重要：如果在服务器受 **XClarity Administrator** 管理之后更改此服务器的 **IP** 地址，**XClarity Administrator** 将识别新 **IP** 地址并继续管理此服务器。但是，**XClarity Administrator** 无法识别某些服务器的 **IP** 地址变化。如果 **XClarity Administrator** 显示服务器在 **IP** 地址更改之后处于脱机状态，请使用强制管理选项重新管理该服务器。

- （AB 列）如果选择使用存储的凭证而不是手动输入的凭证（D – H 列）或标识（AF – AJ 列），请指定存储的凭证 ID。可通过在“存储的凭证”页面上单击 XClarity Administrator 菜单中的**管理 → 安全性**，然后单击左侧导航区域中的**存储的凭证**，找到存储的凭证标识。有关存储的凭证和本地认证的详细信息，请参阅 XClarity Administrator 在线文档中的管理存储的凭证。

  注：

  – RackSwtich 设备仅支持使用存储的凭证进行认证。不支持手动输入用户凭证（位于 D 列）。

  – 使用存储的凭证管理设备并启用受管认证时，无法编辑这些存储的凭证。
- （AC 列）如果选择对机箱和机架服务器使用受管认证，则必须在批量导入文件中的 G 列或“批量导入”对话框中指定 RECOVERY_ID 密码。如果选择本地认证，则不允许使用恢复密码；请勿在批量导入文件的 G 列或“批量导入”对话框中指定恢复密码。
- （AD 列）对于机架服务器，可选择通过在该列中指定 FALSE 以使用本地认证，而不是 XClarity Administrator 受管认证。有关受管认证和本地认证的详细信息，请参阅 XClarity Administrator 在线文档中的管理认证服务器。
- （AE 列）（可选）可指定允许查看和管理设备的角色组列表。可仅指定当前用于所在的角色组。

  注：向受管机箱添加设备后，新设备将和机箱属于相同的角色组。
- （AF – AJ 列）如果选择使用标识管理系统而不是手动输入的凭证（D – H 列）或存储的凭证（AB 列），请指定受管服务器的 IP 地址或主机名、用户名，还可以选择指定应用程序 ID、安全位置和文件夹。

  如果指定了应用程序标识，则还必须指定安全位置和文件夹（如果适用）。

  如果未指定应用程序 ID，XClarity Administrator 会使用设置 CyberArk 时定义的路径来标识 CyberArk 中的已注册帐户。

  注：仅支持 ThinkSystem 或 ThinkAgile 服务器。必须在 XClarity Administrator 配置标识管理系统，并且针对受管 ThinkSystem 或 ThinkAgile 服务器的 Lenovo XClarity Controller 必须与 CyberArk 进行集成。

下图显示一个示例批量导入文件：

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	P67X30EL																	
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. 从批量导入向导中，输入 CSV 文件的名称以上传该文件供处理。可单击**浏览**以帮助查找文件。
7. 单击**上传**以上传并验证文件。
8. 单击**下一步**以显示包含要管理的设备列表的“输入摘要”页面。

9. 查看要管理的设备的摘要。

   选择**仅显示存在潜在问题的行**以列出包含不完整数据的行。修复批量导入文件中的任何问题，然后单击**后退**以上传正确的 CSV 文件。

   注：

   - 如果没有在批量导入文件中提供必需数据，则不会管理关联的设备。
   - 输入摘要页面会标出不包含凭证信息的行。如果未在批量导入文件中指定凭证，则将改用在批量导入向导中指定的全局凭证。
10. 单击**下一步**以显示“设备凭证”页面。

11. **可选**：单击每个选项卡并（可选）指定供某特定类型的所有设备使用的全局设置和凭证。每个选项卡右侧会列出将使用上述全局设置和凭证的设备。

    如果决定使用全局凭证，对于没有在批量导入文件中输入凭证的特定设备类型，同一类型内的所有设备必须使用相同的凭证。例如，对于所有机箱，CMM 凭证必须相同，而对于所有存储设备，存储管理凭证必须相同。如果这些凭证不同，则必须在批量导入文件中输入凭证。

    - **机箱**。指定认证模式和凭证类型。指定当前用于登录批量导入文件中定义的所有机箱的凭证。如果当前 CMM 凭证已到期，请指定要使用的新密码。

      如果要强制管理机箱，请对设备凭证指定 RECOVERY_ID 帐户和密码。
    - **服务器**。指定认证模式和凭证类型。指定当前用于登录批量导入文件中定义的所有机架和立式服务器的凭证。如果当前的主板管理控制器凭证已到期，请指定要使用的新密码。

      如果要强制管理服务器，请对设备凭证指定 RECOVERY_ID 帐户和密码。
    - **交换机**。指定用于登录批量导入文件中定义的所有 RackSwitch 交换机的存储的凭证。如果设置此凭证，请同时指定用于进入交换机 Privileged Exec 模式的“enable”密码。
    - **存储**。指定当前用于登录批量导入文件中定义的所有存储设备的凭证。
    - **恢复**。指定用于登录批量导入文件中定义的所有服务器和机箱的恢复密码。

      可以选择使用本地用户帐户或存储的恢复凭证。无论哪种情况，用户名始终为 RECOVERY_ID。

      指定密码后，将在设备上创建 RECOVERY_ID 帐户，并禁用所有本地用户帐户。

      – 对于机箱，则需要恢复密码。

- 对于服务器，如果选择使用受管认证，则恢复密码可选，如果选择使用本地认证，则不允许使用恢复密码。
- 确保密码遵循设备的安全策略和密码策略。安全策略和密码策略可能不尽相同。
- 请务必记录恢复密码以备将来使用。
- **ThinkServer** 和 **System x M4** 服务器不支持恢复帐户。

在批量导入文件中指定的信息将覆盖在设备凭证页面上指定的类似信息。

出现以下情况时，可选择强制管理每种类型的设备：

- 如果设备当前受另一管理系统（如另一 **XClarity Administrator** 实例或 **IBM Flex System Manager**）管理
- **XClarity Administrator** 关闭，但在关闭之前未终止管理设备
- 未正确地终止管理设备，并且未清除 **CIM** 订阅

注：如果设备受另一 **XClarity Administrator** 实例管理，则在发生强制管理之后，设备似乎在一段时间内受原始实例管理。可终止管理设备以将其从原始 **XClarity Administrator** 实例中删除。

12. 单击**管理**。将显示“监控结果”页面，其中包含与批量导入文件中每个设备的管理状态有关的信息。

    为管理过程创建一个作业。关闭批量导入向导后，管理过程将在后台继续运行。可从作业日志中监控管理过程的状态。有关作业日志的信息，请参阅 **XClarity Administrator** 在线文档中的监控作业。

    如果 **XClarity Administrator** 无法使用在批量导入文件中指定的凭证或在对话框中指定的全局凭证登录到设备，则管理该设备失败，而 **XClarity Administrator** 继续管理批量导入文件中的下一设备。

    注：如果管理因以下一种错误情况而未能成功，请使用**强制管理**选项重复上述过程。

    - 管理 **XClarity Administrator** 失败且无法恢复。

      注：如果更换的 **XClarity Administrator** 实例和发生故障的 **XClarity Administrator** 使用相同的 **IP** 地址，可使用 **RECOVERY_ID** 帐户和密码（如适用）以及**强制管理**选项再次管理设备。
    - 终止管理设备之前，管理 **XClarity Administrator** 是否已关闭。
    - 是否未能成功终止管理设备。

    注意：设备同时只能受一个 **XClarity Administrator** 实例管理。不支持受多个 **XClarity Administrator** 实例管理。如果设备已受一个 **XClarity Administrator** 管理，而您要用另一 **XClarity Administrator** 管理它，则必须先在原始 **XClarity Administrator** 上终止管理该设备，然后用新的 **XClarity Administrator** 来管理它。
13. 如果批量导入文件包括新机箱，则确认并更改整个机箱（包括计算节点和 **Flex** 交换机）的管理网络设置，并通过创建并部署 **Server Pattern**，配置计算节点信息、本地存储、**I/O** 适配器、引导目标和固件设置。有关详细信息，请参阅 **XClarity Administrator** 在线文档中的修改机箱的管理 **IP** 设置和使用 **XClarity Administrator** 配置服务器。

完成之后

管理系统后，可执行以下操作：

- 发现和管理其他系统（请参阅 **Lenovo XClarity Administrator** 在线文档中的管理机箱、管理机架、管理服务器、管理存储设备和管理交换机）。
- 通过创建和部署 **Server Pattern**，配置系统信息、本地存储、**I/O** 适配器、引导设置和固件设置（请参阅 **Lenovo XClarity Administrator** 在线文档中的使用 **XClarity Administrator** 配置服务器）。
- 将操作系统映像部署到尚未安装操作系统的服务器（请参阅 **XClarity Administrator** 在线文档中的部署操作系统映像）。
- 更新不符合当前策略的设备上的固件（请参阅 **XClarity Administrator** 在线文档中的更新受管设备上的固件）。
- 将新近管理的系统添加到相应机架以反映物理环境（请参阅 **XClarity Administrator** 在线文档中的管理机架）。
- 监控硬件状态和详细信息（请参阅 **XClarity Administrator** 在线文档中的查看受管服务器的状态）。
- 监控事件和警报（请参阅 **XClarity Administrator** 在线文档中的使用事件和使用警报）。
- 对受管 **ThinkSystem** 和 **ThinkAgile** 服务器禁用或启用单点登录。
  - 要对所有受管 **ThinkSystem** 和 **ThinkAgile** 服务器（全局）启用或禁用单点登录，请单击 **XClarity Administrator** 菜单栏中的**管理 → 安全性**，然后单击**活动会话**，再启用或禁用**单点登录**。
  - 要对特定 **ThinkSystem** 和 **ThinkAgile** 服务器执行该操作，请单击 **XClarity Administrator** 菜单栏中的**硬件 → 服务器**，然后单击**所有操作 → 安全性 → 启用单点登录**或者单击**所有操作 → 安全性 → 禁用单点登录**。

  注：借助单点登录功能，已登录 **XClarity Administrator** 的用户将可以自动登录到主板管理控制器。默认情况下，将 **ThinkSystem** 或 **ThinkAgile** 服务器设置为受 **XClarity Administrator** 管理的服务器后，即可启用单点登录（使用 **CyberArk** 密码管理服务器的情况除外）。可以通过配置全局设置来对所有受管 **ThinkSystem** 和 **ThinkAgile** 服务器启用或禁用单点登录。对特定 **ThinkSystem** 和 **ThinkAgile** 服务器启用单点登录会覆盖适用于所有 **ThinkSystem** 和 **ThinkAgile** 服务器的全局设置。

第 5 章　注册 XClarity Administrator

注册 **Lenovo XClarity Administrator** 实例后，您将可以使用基本功能，而不会再收到有关试用期到期和许可证不合规的警告。注册后不再显示不合规警告；但是，在您根据受管设备的数量购买和安装许可证之前，所有需要许可证的功能都将保持禁用状态。

关于本任务

注册 **XClarity Administrator** 实例不需要共享您的联系信息。**Lenovo** 不会与其他外部实体共享您提供的信息。

如果已经安装了高级功能许可证，则无需注册 **XClarity Administrator** 实例。有关许可证和高级功能的更多信息，请参阅安装启用全功能的许可证。

过程

要注册 **XClarity Administrator**，请完成以下步骤。

- 如果 **XClarity Administrator** 连接到 **Internet**，则
  1. 从 **Lenovo XClarity Administrator** 菜单栏中，单击**管理 → 注册**以显示“注册”页面。
  2. 单击**注册**即可注册新的 **XClarity Administrator** 实例。
  3. 填写公司名称、即将由 **XClarity Administrator** 管理的设备数量以及 **XClarity Administrator** 所在的国家/地区。
  4. 单击**提交**。
- 如果 **XClarity Administrator** 未连接到 **Internet**，则
  1. 注册 **XClarity Administrator**。
     a. 在 **Web** 浏览器中，打开**Lenovo XClarity** 注册门户网站。
     b. 填写公司名称、即将由 **XClarity Administrator** 管理的设备数量以及 **XClarity Administrator** 所在的国家/地区。
     c. 单击**提交**以接收注册令牌。
  2. 从 **Lenovo XClarity Administrator** 菜单栏中，单击**管理 → 注册**以显示“注册”页面。
  3. 单击**导入**以导入注册令牌。
  4. 填写在步骤 **1** 中收到的注册令牌。
  5. 单击**提交**。

第 6 章　安装启用全功能的许可证

90 天的免费试用过期后，您必须为支持高级功能的所有受管设备购买和安装 **Lenovo XClarity Pro** 许可证，才能继续使用 **Lenovo XClarity Administrator** 中的操作系统部署和设备配置功能。您必须拥有*所有*受管设备的 **Lenovo XClarity Pro** 许可证，才能获得 **XClarity Administrator** 服务和支持。

了解更多：  **XClarity Administrator：安装许可证**

开始之前

请查看以下许可证注意事项。

- 许可证*未*与特定设备绑定。
- 一个机箱许可证可以为 **14** 个设备提供许可证。
- 对于 **System x3850 X6**（**6241**）可扩展机器群服务器，无论分区如何，每个服务器都需要一个单独的许可证。
- 对于 **System x3950 X6**（**6241**）可扩展机器群服务器，如果未分区，则每个服务器需要一个单独的许可证。如果分区，则每个分区需要一个单独的许可证。
- 以下设备*不支持*高级功能，因此*不需要*为这些功能提供许可证；但是，必须为每个设备购买许可证才能获得 **XClarity Administrator** 服务和支持。
  - **ThinkServer** 服务器
  - **System x M4** 服务器
  - **System x X5** 服务器
  - **System x3850 X6** 和 **x3950 X6**（**3837**）服务器
  - 存储设备
  - 交换机

必须具有 **lxc-supervisor** 或 **lxc-security-admin** 权限才能安装许可证。

关于本任务

XClarity Administrator 支持以下许可证。

- **Lenovo XClarity Pro**。每个许可证为一台设备提供以下权利。
  - **Lenovo XClarity Integrator** 服务与支持
  - **XClarity Administrator** 服务与支持
  - **XClarity Administrator** 的高级功能：
    - 使用 **Configuration Patterns** 配置服务器
    - 部署操作系统
    - 使用 **Call Home** 报告 **XClarity Administrator** 问题（用于硬件警报的 **Call Home** 不受影响。）

许可证的激活周期从购买许可证并创建授权代码时开始。

许可证的合规性由支持高级功能的受管设备数量来决定。受管设备数量不得超过所有有效许可证密钥中的许可证总数。如果 **XClarity Administrator** 不符合已安装的许可证（例如，许可证过期

或管理的其他设备数量超出有效许可证总数），您将有 **90** 天的宽限期来安装合适的许可证。只要 **XClarity Administrator** 不合规，宽限期都将恢复为 **90** 天。如果宽限期（包括免费试用）在许可证合规之前结束，则将禁用所有设备的高级功能。

例如，如果在现有 **XClarity Administrator** 实例中管理另外 **100** 台 **ThinkSystem** 服务器和 **20** 个机架交换机，则在用户界面中禁用高级功能之前（针对所有设备），您有 **90** 天的时间购买和安装另外 **100** 个许可证。不需要 **20** 个机架交换机的许可证即可使用高级功能，但是，如果您需要服务和支持，则需要这些许可证。如果禁用高级功能，则在安装足够的许可证以恢复合规性后，将重新启用高级功能。

如果您使用的是免费试用许可证，或者您有合规宽限期，而您升级到更高版本的 **XClarity Administrator**，则试用许可证或宽限期将恢复为 **90** 天。

注：

- 宽限期过后，服务器配置和操作系统部署功能会被禁用。
- 许可证不合规时，会禁用针对 **XClarity Administrator** 问题的 **Call Home**（软件 **Call Home** 功能）。该功能没有宽限期。但是，用于硬件警报的 **Call Home** 不受影响。

如果已安装许可证，那么在升级到 **XClarity Administrator** 新版本时*不*需要新许可证。

可通过单击 **XClarity Administrator** 标题栏中的用户操作菜单（ 

），然后单击**关于**，确定许可证状态，包括试用许可证还剩多少天。

获取帮助

- 如果遇到了问题并使用了业务合作伙伴，请联系业务合作伙伴以验证交易和权利。
- 如果没有收到电子权利证明、授权代码或激活密钥或者电子邮件发送有误，请根据所处的地理位置联系区域代表。
  - **ESDNA@lenovo.com**（北美国家/地区）
  - **ESDAP@lenovo.com**（亚太国家/地区）
  - **ESDEMEA@lenovo.com**（欧洲、中东和亚洲国家/地区）
  - **ESDLA@lenovo.com**（拉丁美洲国家/地区）
  - **ESDChina@Lenovo.com**（中国）
- 如果有关权利的信息有误，请发送电子邮件到 **SW_override@lenovo.com** 联系 **Lenovo** 支持中心并在其中包含以下信息：
  - 订单号
  - 联系信息，包括电子邮件地址。
  - 物理地址
  - 您要做的更改
- 如果您对下载许可证有任何疑问或问题，请发送电子邮件到 **-eSupport_-_Ops@lenovo.com** 联系 **Lenovo** 支持中心。

使用 XClarity Administrator Web 界面安装启用完整功能的许可证

如果 **XClarity Administrator** 可访问 **Internet**，则可以使用 **XClarity Administrator Web** 界面兑换和检索现有授权的许可证，然后导入并安装兑换的许可证。

开始之前

要根据要启用的功能和要管理的设备数量购买 **Lenovo XClarity Pro** 许可证，请与 **Lenovo** 代表或授权业务合作伙伴联系。购买许可证后，您将通过*电子权利证明*电子邮件收到授权代码。授权代码是一个 **22** 个字符的字母数字字符串，用于兑换和安装许可证。如果您从业务合作伙伴处购买许可证且没有收到该电子邮件，请联系业务合作伙伴以请求授权代码。

还可以单击**检索授权代码**，从 **Feature on Demand** 门户网站检索授权代码。

过程

要在管理软件中安装 **Lenovo XClarity Pro** 许可证，请完成以下过程之一。

- **兑换并安装单个授权代码中的全部或部分剩余许可证**

  您可以兑换单个授权代码中全部或部分的可用许可证以创建许可证激活密钥；该密钥是一个包含已兑换许可证的所有信息的文件。然后，可使用该许可证激活密钥文件安装已兑换的许可证。

  1. 从 **XClarity Administrator** 菜单栏中，单击**管理 → 许可证**以显示“许可证管理”页面。

  2. 单击**申请激活密钥**图标（ ）以显示“申请激活密钥”对话框。
  3. 单击**单个授权代码**。
  4. 输入 **22** 个字符的授权代码，然后单击**搜索**，从 **Features on Demand** 网站获取该指定授权代码的已购许可证的相关信息。

     如果您收到的授权代码未被接受，请联系 **Lenovo** 支持机构。
  5. 在 **Lenovo 客户编号**字段中输入 **10** 位数的 **Lenovo** 客户编号。
  6. 在**兑换数量**字段中输入要兑换的许可证数量，然后单击**继续**。

     要兑换授权代码中的所有可用许可证，请在**可用许可证**字段中输入匹配的数字。

     如果兑换一部分可用许可证，则可以稍后使用同一个授权代码兑换剩余许可证。

     提示：每个 **XClarity Administrator** 最多支持 **1000** 个受管设备。因此，可在一个 **XClarity Administrator** 实例中安装的单个许可证激活密钥的许可证数量不能超过 **1000**。
  7. 检查联系信息的准确性，并在需要时进行修改。
  8. 单击**提交请求**以兑换许可证并创建许可证激活密钥。

9. 选择包含要安装的许可证的许可证激活密钥。
10. 单击**安装**，在管理软件中安装许可证。
11. 单击**关闭**。

- **兑换并安装多个授权代码中的所有剩余许可证**

  您可以兑换多个授权代码的所有剩余许可证。每个授权代码都会对应创建一个许可证激活密钥。然后，可使用许可证激活密钥安装已兑换的许可证。必须使用提供的模板在 CSV 格式的文件中提供授权代码。

  1. 从 XClarity Administrator 菜单栏中，单击**管理 → 许可证**以显示“许可证管理”页面。
  2. 单击**申请激活密钥**图标（  ）以显示“申请激活密钥”对话框。
  3. 单击**多个授权代码**。
  4. 单击**下载模板**链接，此时会打开一个 Excel 文件。将每个授权代码添加到文件中，然后将文件以 CSV 格式保存到本地系统。
  5. 单击**浏览**以找到并选择授权代码 CSV 文件，然后单击**搜索**，从 Lenovo 支持网站获取有关授权代码的信息。
  6. 查看与每个授权代码关联的已购许可证以及可用许可证激活密钥的相关信息。
  7. 在 **Lenovo 客户编号**字段中输入 10 位数的 Lenovo 客户编号。
  8. 检查联系信息的准确性，并在需要时进行修改。然后，单击**继续**。
  9. 选择**是的，我想兑换所有有效的授权代码**，然后单击**提交请求**以生成许可证激活密钥。
  10. 选择要安装的许可证激活密钥。
  11. 单击**安装**，在管理软件中安装许可证激活密钥。
  12. 单击**关闭**。

- **检索并安装已兑换的许可证**

  可从能够访问 Feature on Demand 门户网站的 XClarity Administrator 实例将许可证激活密钥下载到本地系统，然后将这些许可证激活密钥导入并安装到另一个 XClarity Administrator 实例中。当需要在无法访问 Internet 的 XClarity Administrator 实例上安装许可证时，或重新安装了 XClarity Administrator 并需要恢复已安装的许可证时，这种方法很有用。

  1. 从 XClarity Administrator 菜单栏中，单击**管理 → 许可证**以显示“许可证管理”页面。
  2. 单击**检索历史记录**图标（  ）以显示“检索历史记录”对话框。
  3. 输入您的 Lenovo 客户编号或 22 个字符的授权代码。
  4. 单击**搜索**以检索有关可用许可证和已兑换的许可证的信息。

     如果您收到的授权代码未被接受，请联系 Lenovo 支持机构。
  5. 选择要安装的许可证密钥文件。
  6. 单击**安装**，在 XClarity Administrator 中安装许可证激活密钥。
  7. 单击**关闭**。

- **在另一个 XClarity Administrator 实例上导入并安装已兑换的许可证**

  如果已在一个 XClarity Administrator 实例上兑换许可证，并希望在另一个 XClarity Administrator 实例上安装这些许可证，或者如果发生错误情况而需要恢复已安装的许可证，则可以将许可证密钥文件从本地系统导入到另一个 XClarity Administrator 实例。

1. 在一个可访问 Feature on Demand 门户网站的 XClarity Administrator 实例上，从 Feature on Demand 门户网站中检索许可证激活密钥，然后将许可证激活密钥以文件的形式保存到本地系统上。
   a. 从 XClarity Administrator 菜单栏中，单击**管理** → **许可证**以显示“许可证管理”页面。
   b. 单击**检索历史记录**图标（）以显示“检索历史记录”对话框。
   c. 输入 22 个字符的授权代码。
   d. 单击**搜索**以检索该授权代码的可用许可证和已兑换许可证的相关信息。
      如果您收到的授权代码未被接受，请联系 Lenovo 支持机构。
   e. 选择要安装的许可证激活密钥文件。
   f. 单击**下载**，将许可证密钥文件保存到本地系统。
2. 在要安装许可证激活密钥的 XClarity Administrator 实例上：
   a. 从 XClarity Administrator 菜单栏中，单击**管理** → **许可证**以显示“许可证管理”页面。
   b. 单击**导入并应用**图标（）以导入并安装许可证。
   c. 单击**浏览**，然后选择要安装的许可证的许可证激活密钥。

      要导入多个许可证激活密钥，先将 .KEY 文件压缩为 ZIP 文件，然后选择该 ZIP 文件进行导入。
   d. 单击**接受许可证**以导入并应用许可证。
      安装完成后，表中将列出许可证激活密钥，以及所安装许可证数量和激活周期（开始日期和到期日期）。

完成之后

可从许可证页面执行以下操作。

- 单击**导出**图标（），将一个或多个特定许可证激活密钥下载到本地系统。

  注：导出多个许可证激活密钥时，文件将下载为单个 ZIP 文件。
- 单击**删除**图标（）删除特定的许可证激活密钥。
- 单击页面顶部的**编辑**按钮配置许可证警告周期。许可证警告周期是从 XClarity Administrator 触发警告到许可证到期之间的天数。

获取帮助

- 如果遇到了问题并使用了业务合作伙伴，请联系业务合作伙伴以验证交易和权利。
- 如果没有收到电子权利证明、授权代码或激活密钥或者电子邮件发送有误，请根据所处的地理位置联系区域代表。
  - ESDNA@lenovo.com（北美国家/地区）
  - ESDAP@lenovo.com（亚太国家/地区）
  - ESDEMEA@lenovo.com（欧洲、中东和亚洲国家/地区）
  - ESDLA@lenovo.com（拉丁美洲国家/地区）
  - ESDChina@Lenovo.com（中国）
- 如果有关权利的信息有误，请发送电子邮件到 SW_override@lenovo.com 联系 Lenovo 支持中心并在其中包含以下信息：
  - 订单号
  - 联系信息，包括电子邮件地址。

  - 物理地址
  - 您要做的更改
- 如果您对下载许可证有任何疑问或问题，请发送电子邮件到 -eSupport_-_Ops@lenovo.com 联系 Lenovo 支持中心。

使用 Features on Demand 门户网站安装启用完整功能的许可证

如果 XClarity Administrator *不能* 访问 Internet，则可从另一个可通过网络访问 XClarity Administrator 的系统，使用 Feature on Demand 门户网站来兑换和检索现有授权代码的许可证。然后，可使用 XClarity Administrator Web 界面导入并安装已兑换的许可证。

过程

要在管理软件中安装 Lenovo XClarity Pro 许可证，请完成以下步骤。

步骤 1. 为每个受管设备购买一个 Lenovo XClarity Pro 许可证。

要根据要启用的功能和要管理的设备数量购买 Lenovo XClarity Pro 许可证，请与 Lenovo 代表或授权业务合作伙伴联系。购买许可证后，您将通过*电子权利证明*电子邮件收到授权代码。授权代码是一个 22 个字符的字母数字字符串，用于兑换和安装许可证。如果您从业务合作伙伴处购买许可证且没有收到该电子邮件，请联系业务合作伙伴以请求授权代码。

还可以单击**检索授权代码**，从 Feature on Demand 门户网站检索授权代码。

步骤 2. 使用授权代码兑换全部或部分许可证。兑换许可证时会生成一个许可证激活密钥文件。

1. 从 Web 浏览器中打开 Feature on Demand 门户网站，并使用电子邮件地址作为用户标识登录门户网站。
2. 单击**申请激活密钥**。
3. 选择**输入单个授权代码**。
4. 输入 22 个字符的授权代码，然后单击**继续**。
5. 在 Lenovo **客户编号**字段中输入 Lenovo 客户编号。
6. 在**兑换数量**字段中输入要兑换的许可证数量，然后单击**继续**。

   要兑换此授权代码中的所有可用许可证，请在**可用许可证**字段中输入匹配的数字。

   如果兑换一部分可用许可证，则可以使用同一个授权代码在另一个许可证激活密钥中兑换其余许可证。

   提示：每个 XClarity Administrator 最多支持 **1000** 个受管设备。因此，在一个 XClarity Administrator 实例中安装的单个许可证激活密钥的许可证数量不应超过 **1000**。
7. 按照提示输入产品详细信息和联系信息，然后单击**继续**以生成许可证激活密钥。
8. （可选）指定其他收件人以接收许可证激活密钥。
9. 单击**提交**以发送许可证激活密钥。

   分配到该采购订单的客户和其他收件人将收到一封包含许可证激活密钥的电子邮件。密钥是一个 .KEY 格式的文件。

   注：还可以从 Feature on Demand 门户网站下载许可证激活密钥（单独或批量下载），方法是单击**检索历史记录**，使用 Lenovo 客户编号查找许可证激活密钥，然后下载全

部或部分密钥。接着，单击**电子邮件**通过电子邮件将密钥发送给您，或单击**下载**将密钥下载到本地系统。

步骤 3. 在 XClarity Administrator 中导入并安装许可证。

1. 从 XClarity Administrator 菜单栏中，单击**管理 → 许可证**以显示“许可证管理”页面。
2. 单击**导入并应用**图标（  ）以安装许可证。
3. 单击**浏览**，然后选择要安装的许可证的许可证激活密钥文件。

   提示：要导入多个许可证激活密钥，先将 .KEY 文件压缩为 ZIP 文件，然后选择该 ZIP 文件进行导入。
4. 单击**接受许可证**以导入并应用许可证。

   安装完成后，表中将列出许可证激活密钥，以及所安装许可证数量和激活周期（开始日期和到期日期）。

完成之后

可从许可证页面执行以下操作。

- 单击**导出**图标（  ），将一个或多个特定许可证激活密钥下载到本地系统。

  注：导出多个许可证激活密钥时，文件将下载为单个 ZIP 文件。
- 单击**删除**图标（  ）删除特定的许可证激活密钥。
- 单击页面顶部的**编辑**按钮配置许可证警告周期。许可证警告周期是从 XClarity Administrator 触发警告到许可证到期之间的天数。

获取帮助

- 如果遇到了问题并使用了业务合作伙伴，请联系业务合作伙伴以验证交易和权利。
- 如果没有收到电子权利证明、授权代码或激活密钥或者电子邮件发送有误，请根据所处的地理位置联系区域代表。
  - ESDNA@lenovo.com（北美国家/地区）
  - ESDAP@lenovo.com（亚太国家/地区）
  - ESDEMEA@lenovo.com（欧洲、中东和亚洲国家/地区）
  - ESDLA@lenovo.com（拉丁美洲国家/地区）
  - ESDChina@Lenovo.com（中国）
- 如果有关权利的信息有误，请发送电子邮件到 SW_override@lenovo.com 联系 Lenovo 支持中心并在其中包含以下信息：
  - 订单号
  - 联系信息，包括电子邮件地址。
  - 物理地址
  - 您要做的更改
- 如果您对下载许可证有任何疑问或问题，请发送电子邮件到 -eSupport_-_Ops@lenovo.com 联系 Lenovo 支持中心。

第 7 章　将 XClarity Administrator 作为进行更新

将 **Lenovo XClarity Administrator** 作为容器运行，请按照此更新过程将最新软件安装为新容器，并将原始容器的卷绑定到新容器。

开始之前

只能从 **XClarity Administrator v3.0** 或更高版本的实例更新到 **XClarity Administrator v4.0** 或更高版本。如果使用的 **XClarity Administrator** 版本低于 **v3.0**，则必须先升级到 **v3.0** 或更高版本，然后才能升级到 **v4.0**。

要使用 **Lenovo XClarity Orchestrator** 管理 **XClarity Administrator v4.0** 或更高版本的实例，需要安装 **XClarity Orchestrator v2.0** 或更高版本。如果要将 **XClarity Administrator** 更新到 **v4.0** 或更高版本，请确保 **XClarity Orchestrator** 的版本不低于 **v2.0**。

关于本任务

`docker-compose.yml` 文件使用以下环境变量，这些变量由您在安装*原始*容器的过程中进行设置。新容器也使用这些环境变量。

- **CONTAINER_NAME**。唯一的容器名称，用于为每个 **XClarity Administrator** 实例创建 **Docker** 卷（例如，`CONTAINER_NAME=LXCA-203`）

  XClarity Administrator 使用容器名称为容器创建卷。如果对新容器使用相同的容器名称，则新的 **XClarity Administrator** 实例将使用相同的卷，因此可以访问与原始 **XClarity Administrator** 实例（容器）相同的系统数据和设置。

  如果更改容器名称，则会为容器创建新卷，并且新的 **XClarity Administrator** 实例不能访问与原始 **XClarity Administrator** 实例（容器）相同的系统数据和设置。如果需要更改容器名称或 **IP** 地址，请在安装新容器之前备份原始 **XClarity Administrator** 实例的系统数据和设置，然后使用该备份在新容器中恢复系统数据和设置。

- **ADDRESS**。容器的静态 **IPv4** 或 **IPv6** 地址（例如，`ADDRESS=192.0.2.0`）

  如果管理设备后再更改 **XClarity Administrator** 的 **IP** 地址，可能会使设备在 **XClarity Administrator** 中处于脱机状态。确保更改 **IP** 地址前先终止管理所有设备。

- **BACKUP_MOUNT** 和 **FIRMWARE_MOUNT**。（可选）可用于存储 **XClarity Administrator** 备份或用作固件更新的远程存储库的远程共享路径。路径必须分别为 `/mnt/backup_share` 和 `/mnt/fw_share`。

注：XClarity Administrator *不是* 作为特权容器运行。

过程

要更新 **XClarity Administrator** 容器，请完成以下步骤。

步骤 **1.** 从 **XClarity Administrator** 下载 **Web** 页面将 **XClarity Administrator** 容器镜像下载到客户端工作站。登录到该网站，然后使用提供给您的访问密钥下载该映像。

步骤 **2.** 通过运行以下命令将 **XClarity Administrator** 容器镜像导入 **Docker** 主机。
```
docker load -i lnvgy_sw_lxca_110-3.5.0_anyos_noarch
```

步骤 **3.** 编辑用于原始容器的 `docker-compose.yml`。更新文件顶部的映像属性，使其指向步骤 **2** 中的新 **Docker** 映像。可使用 `docker tag` 命令更改映像标记。

下面是启用了 **IPv6** 的 **yml** 文件示例。

```
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"
```

步骤 4. 通过运行以下命令来关闭*原始*容器。

```
docker-compose -p ${CONTAINER_NAME} down
```

步骤 5. 通过运行以下命令在 **Docker** 中部署*新*映像，其中 ***<ENV_FILENAME>*** 是环境变量文件的名称。

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

第 8 章　卸载 XClarity Administrator

完成以下步骤以卸载 **Lenovo XClarity Administrator** 虚拟设备或容器。

过程

要卸载 **XClarity Administrator** 虚拟设备，请完成以下步骤。

步骤 **1.** 终止管理当前受 **XClarity Administrator** 管理的所有设备。请参阅 管理机箱、管理服务器 和 管理交换机（位于 **XClarity Administrator** 在线文档）。

步骤 **2.** 根据操作系统卸载 **XClarity Administrator:**

- **Docker-compose**运行以下命令以停止容器并删除网络和卷。
  ```
  docker-compose down -v
  ```
- **CentOS、Red Hat、Rocky 和 Ubuntu**
  1. 使用虚拟机管理器连接到主机。
  2. 右键单击虚拟机，然后单击**关闭 → 强制关闭**。
  3. 再次右键单击虚拟机，然后单击**删除**。随后将显示“确认删除”对话框。
  4. 选中所有复选框，然后单击**删除**。
- **ESXi**
  1. 通过 **VMware vSphere Client** 连接到主机。
  2. 右键单击虚拟机，然后单击**电源 → 关机**。
  3. 再次右键单击虚拟机，然后单击**从磁盘中删除**。
- **Hyper-V**
  1. 从服务器管理器仪表板中，单击 **Hyper-V**。
  2. 右键单击服务器，然后单击 **Hyper-V 管理器**。
  3. 右键单击虚拟机，然后单击**关闭**。
  4. 再次右键单击虚拟机，然后单击**删除**。