Lenovo

XClarity Controller（配备 Intel Xeon SP（第三代）和 AMD EPYC（第二代、第三代））用户指南

注：使用本指南前，请先阅读第 **205** 页附录 **B** “声明”中的一般信息。

第十五版 (2021 年 5 月)

目录

第 1 章　简介

Lenovo XClarity Controller（XCC）取代了基板管理控制器（BMC），是适用于 Lenovo ThinkSystem 服务器的新一代管理控制器。

它是 Integrated Management Module II（IMM2）服务处理器的升级产品，将服务处理器功能、超级 I/O、视频控制器和远程呈现功能整合到服务器主板上的单个芯片中。它提供以下功能：

- 可选择专用或共享以太网连接进行系统管理
- 支持 HTML5
- 支持通过 XClarity Mobile 进行访问
- XClarity Provisioning Manager
- 使用 XClarity Essentials 或 XClarity Controller CLI 进行远程配置
- 应用程序和工具能够本地或远程访问 XClarity Controller
- 增强的远程呈现功能
- 提供针对其他 Web 相关服务和软件应用程序的 REST API（Redfish 架构）支持

  注：XClarity Controller 当前支持 Redfish 可扩展平台管理 API 规范 1.0.2 和架构 2016.2

注：

- 在 XClarity Controller Web 界面中，BMC 用于指代 XCC。
- 专用系统管理网络端口在部分 ThinkSystem 服务器上不一定可用；这些服务器仅可通过与服务器操作系统共享的一个网络端口访问 XClarity Controller。
- 对于 Flex 服务器，Chassis Management Module（CMM）是系统管理功能的主要管理模块。可通过 CMM 上的网络端口访问 XClarity Controller。

本文档说明如何在 ThinkSystem 服务器中使用 XClarity Controller 的功能。XClarity Controller 与 XClarity Provisioning Manager 和 UEFI 共同为 ThinkSystem 服务器提供系统管理功能。

要检查固件更新，请完成以下步骤。

注：首次访问支持门户时，必须选择您的服务器所对应的产品类别、产品系列和型号。下次访问支持门户时，网站会预载您初次选中的产品，并仅显示针对您的产品的链接。要在产品列表中更改或添加内容，请单击**管理我的产品列表**链接。网站定期更改内容。查找固件和文档的过程可能与本文档中的描述稍有不同。

1. 请转至 http://datacentersupport.lenovo.com。
2. 在 Support（**支持**）下选择 Data Center（**数据中心**）。
3. 内容加载完成后，选择 Servers（**服务器**）。
4. 在 Select Series（**选择系列**）下，首先选择特定服务器硬件系列，然后在 Select SubSeries（**选择子系列**）下选择特定服务器产品子系列，最后在 Select Machine Type（**选择机器类型**）下选择特定机器类型。

XClarity Controller Standard、Advanced 和 Enterprise 级别功能

XClarity Controller 提供 **Standard**、**Advanced** 和 **Enterprise** 级别的功能。如需了解您的服务器中安装的 **XClarity Controller** 提供哪些功能级别，请参阅服务器文档。所有级别均提供以下功能：

- 全天候远程访问和管理服务器
- 不限受管服务器状态的远程管理
- 远程控制硬件和操作系统

注：部分功能可能不适用于 **Flex System** 服务器。

以下是 **XClarity Controller Standard** 级别的功能列表：

XClarity Controller Standard 级别功能

以下是 **XClarity Controller Standard** 级别的功能列表：

行业标准管理界面

- **IPMI 2.0** 接口
- **Redfish**
- **CIM-XML**
- **DCMI 1.5**
- **SNMPv3**
- **SNMPv1**（仅陷阱）需要最低 **v2.10** 或 **v2.12 XCC** 固件更新，具体取决于服务器类型。有关详细信息，请参阅 **XCC** 固件更新更改文件。

其他管理界面

- **Web**
- **Legacy CLI**
- 前面板 **USB** - 通过移动设备使用的虚拟操作员面板

电源/重置控制

- 打开电源
- 硬关机/软关机
- 定时电源控制
- 系统重置
- 引导顺序控制

事件日志

- **IPMI SEL**
- 用户可读的日志
- 审核日志

环境监控

- 免代理监控
- 传感器监控
- 风扇控制
- **LED** 控制
- 芯片组错误（**Caterr**、**IERR** 等）
- 系统运行状况指示
- **I/O** 适配器 **OOB** 性能监控
- 清单显示和导出

RAS

- 虚拟 **NMI**
- 自动固件恢复
- 备份固件自动升级
- **POST** 看守程序
- 操作系统装入程序看守程序
- 蓝屏捕获（操作系统故障）
- 嵌入式诊断工具

网络配置

- **IPv4**
- **IPv6**
- **IP** 地址、子网掩码、网关
- **IP** 地址分配模式
- 主机名
- 可编程 **MAC** 地址
- 双 **MAC** 选择（如果服务器硬件支持）
- 网络端口重新分配
- **VLAN** 标记

网络协议

- **DHCP**
- **DNS**
- **DDNS**
- **HTTP/HTTPS**
- **SNMPv3**
- **SNMPv1**（仅陷阱）
- **SSL**
- **SSH**
- **SMTP**

- **LDAP 客户机**
- **NTP**
- **SLP**
- **SSDP**

警报

- **PET 陷阱**
- **CIM 指示**
- **SNMP 陷阱**
- 电子邮件
- **Redfish 事件**

串口重定向

- **IPMI SOL**
- 串口配置

安全性

- **XClarity Controller 可信度量根核（CRTM）**
- 数字签名的固件更新
- 基于角色的访问控制（**RBAC**）
- 本地用户帐户
- **LDAP/AD 用户帐户**
- 固件安全回滚
- 机箱入侵检测（仅在部分服务器型号上可用）
- **UEFI TPM 物理现场授权 XCC 远程生效**
- 配置更改和服务器操作的审核记录
- 公钥（**PK**）认证
- 系统停用/重用

远程呈现

- 远程卡上磁盘（**RDOC**）：通过 **CIFS**、**NFS**、**HTTP**、**HTTPS**、**FTP**、**SFTP** 和 **LOCAL** 对远程 **ISO/IMG** 文件执行虚拟介质装载

电源管理

- 实时功率计量器

许可证管理

- 激活密钥验证和存储库

部署和配置

- 远程配置

- 嵌入式 **XClarity Provisioning Manager** 部署和配置工具以及驱动程序包
- 配置备份与恢复

固件更新

- 免代理更新
- 远程更新

XClarity Controller Advanced 级别功能

以下是 **XClarity Controller Advanced** 级别的功能列表：

所有 **XClarity Controller Standard** 级别功能，外加：

警报

- 系统日志

远程呈现

- 远程 **KVM**

串口重定向

- 通过 **SSH** 串口重定向

安全性

- **Security Key Lifecycle Manager（SKLM）**
- **IP** 地址阻止

电源管理

- 实时功率计图形
- 历史功率计数器
- 温度图形

部署和配置

- 使用具有 **XClarity Controller** 远程 **KVM** 功能的嵌入式 **XClarity Provisioning Manager** 进行远程操作系统部署

XClarity Controller Enterprise 级别功能

以下是 **XClarity Controller Enterprise** 级别功能的列表：

XClarity Controller Standard 和 **Advanced** 级别功能，外加：

RAS

- 引导捕获

远程呈现

- 质量/带宽控制
- 虚拟控制台协作（六个用户）
- 虚拟控制台聊天
- 虚拟介质
  - 通过远程控制台装载远程 ISO/IMG 文件
  - 从网络装载文件：- 将 ISO 或 IMG 映像文件从文件服务器（HTTPS、CIFS、NFS）作为 DVD 或 USB 驱动器装载到主机

电源管理

- 功率上限
- OOB 性能监控 - 系统性能度量值

部署和配置

- 使用 Lenovo XClarity Administrator 进行远程部署。使用 Lenovo XClarity Administrator 进行操作系统部署时，请访问 http://sysmgt.lenovofiles.com/help/index.jsp?topic=%2Fcom.lenovo.lxca.doc%2Fsupported_operating_system_images.html 获取受支持操作系统的详细信息。

升级 XClarity Controller

如果服务器拥有 Standard 级别或 Advanced 级别的 XClarity Controller 固件功能，那么也许能够升级服务器中的 XClarity Controller 功能。有关可用升级级别和如何订购的更多信息，请参阅第 87 页第 8 章 “许可证管理”。

Web 浏览器和操作系统要求

按本主题中的信息查看服务器支持的浏览器、密码套件和操作系统的列表。

XClarity Controller Web 界面需要使用以下 Web 浏览器之一：

- 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 Edge
- Safari 9.0.2 或更高版本（iOS 7 或更高版本和 OS X）

注：移动设备操作系统中的浏览器不支持远程控制台功能。

上面列出的浏览器与 XClarity Controller 固件当前支持的浏览器一致。可能会定期增强 XClarity Controller 固件以包含对其他浏览器的支持。

根据 XClarity Controller 中固件版本的不同，支持的 Web 浏览器可能与本节中所列的浏览器有所不同。要查看 XClarity Controller 上当前固件支持的浏览器列表，请从 XClarity Controller 登录页面中单击**支持的浏览器**菜单列表。

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

- ECDHE-ECDSA-AES256-GCM-SHA384

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

因特网浏览器的高速缓存将存储您所访问的 **Web** 页面的信息，便于以后更快速地载入这些信息。对 **XClarity Controller** 固件进行闪存更新后，浏览器可能继续使用其高速缓存中的信息，而不是从 **XClarity Controller** 进行检索。更新 **XClarity Controller** 固件后，建议您清除浏览器高速缓存，以确保 **XClarity Controller** 提供的 **Web** 页面能正确显示。

多语言支持

按本主题中的信息查看 **XClarity Controller** 支持的语言列表。

默认情况下，**XClarity Controller Web** 界面选中的语言是英语。该界面可以显示多个语言。具体包括如下：

- 法语
- 德语
- 意大利语
- 日语
- 韩语
- 葡萄牙语（巴西）
- 俄语
- 简体中文
- 西班牙语（国际）
- 繁体中文

要选择您的语言首选项，请单击当前所选语言旁边的箭头。该操作将显示一个下拉菜单，让您选择首选的语言。

XClarity Controller 固件生成的文本字符串以浏览器决定的语言进行显示。如果浏览器指定的语言不是上方列出的已翻译语言之一，则文本以英文显示。此外，所有由 **XClarity Controller** 固件显示，但不由 **XClarity Controller** 生成的文本字符串（例如 **UEFI**、**PCIe** 适配器等生成的消息）以英文显示。

当前不支持英语以外的语言特有文本输入，如*非法入侵消息*。仅支持英语输入的文本。

MIB 简介

请参阅本主题中的信息访问管理信息库（MIB）。

可以从 https://support.lenovo.com/ 下载 SNMP MIB（在门户上按机器类型进行搜索）。它包含以下四个 MIB。

- SMI MIB 描述了 Lenovo 数据中心组的管理信息结构。
- 产品 MIB 描述了 Lenovo 产品的对象标识符。
- XCC MIB 提供了 Lenovo XClarity Controller 的清单和监控信息。
- XCC 警报 MIB 定义了 Lenovo XClarity Controller 检测到的警报条件陷阱。

注：这四个 MIB 的导入顺序为 SMI MIB → 产品 MIB → XCC MIB → XCC 警报 MIB。

本文档中使用的注意事项

使用以下信息了解本文档中使用的注意事项。

本文档中使用以下注意事项：

- **注**：这些注意事项提供重要的提示、指导或建议。
- **重要**：这些注意事项提供的信息或建议有可能帮助您避免不便的情况或问题。
- **注意**：这些注意事项指示可能会损坏程序、设备或数据。注意事项放置在可能会发生损坏的说明或情况之前。

第 2 章　打开和使用 XClarity Controller Web 界面

本主题描述登录过程以及可在 **XClarity Controller Web** 界面中执行的操作。

XClarity Controller 将服务处理器功能、视频控制器和远程呈现功能整合到一块芯片中。要使用 **XClarity Controller Web** 界面远程访问 **XClarity Controller**，您必须先登录。本章介绍登录过程以及 **XClarity Controller Web** 界面中可执行的操作。

访问 XClarity Controller Web 界面

本主题中的信息介绍如何访问 **XClarity Controller Web** 界面。

XClarity Controller 支持静态和动态主机配置协议（**DHCP**）**IPv4** 寻址。向 **XClarity Controller** 分配的默认静态 **IPv4** 地址是 **192.168.70.125**。**XClarity Controller** 初始配置为尝试从 **DHCP** 服务器获取地址，如果无法获取地址，它会使用该静态 **IPv4** 地址。

XClarity Controller 也支持 **IPv6**，但其在默认情况下没有固定的静态 **IPv6 IP** 地址。首次在 **IPv6** 环境下访问 **XClarity Controller** 时，可使用 **IPv4 IP** 地址或 **IPv6** 链路本地地址。**XClarity Controller** 将生成一个唯一的链路本地 **IPv6** 地址，该地址为插入两个八位元后的 **IEEE 802 MAC** 地址，其中十六进制值 **0xFF** 和 **0xFE** 位于 **48** 位 **MAC** 中间（如 **RFC4291** 中所述），并从 **MAC** 地址的第一个八位元的右边开始翻转第 **2** 个位。例如，如果 **MAC** 地址是 **08-94-ef-2f-28-af**，则链路本地地址将为：

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

访问 **XClarity Controller** 时，以下 **IPv6** 条件将设置为默认值：

- 启用 **IPv6** 自动地址配置。
- 禁用 **IPv6** 静态 **IP** 地址配置。
- 启用 **DHCPv6**。
- 启用无状态自动配置。

XClarity Controller 可选择使用 *专用* 系统管理网络连接（如果适用），或与服务器 *共享* 的网络连接。机架式安装和立式服务器的默认连接是使用 *专用* 系统管理网络接口。

大多数服务器上的专用系统管理网络连接通过一个单独的 **1Gbit** 网络接口控制器提供。但是，某些系统上的专用系统管理网络连接可能通过在多端口网络接口控制器的某个网络端口中使用网络控制器边带接口（**NCSI**）来提供。在这种情况下，专用系统管理网络连接限制为边带接口的 **10/100** 速度。有关系统上管理端口实现的信息和限制，请参阅系统文档。

注： *专用* 系统管理网络端口在您的服务器上可能不可用。如果您的硬件没有 *专用* 网络端口，*共享* 设置将是唯一可用的 **XClarity Controller** 设置。

通过 XClarity Provisioning Manager 设置 XClarity Controller 的网络连接

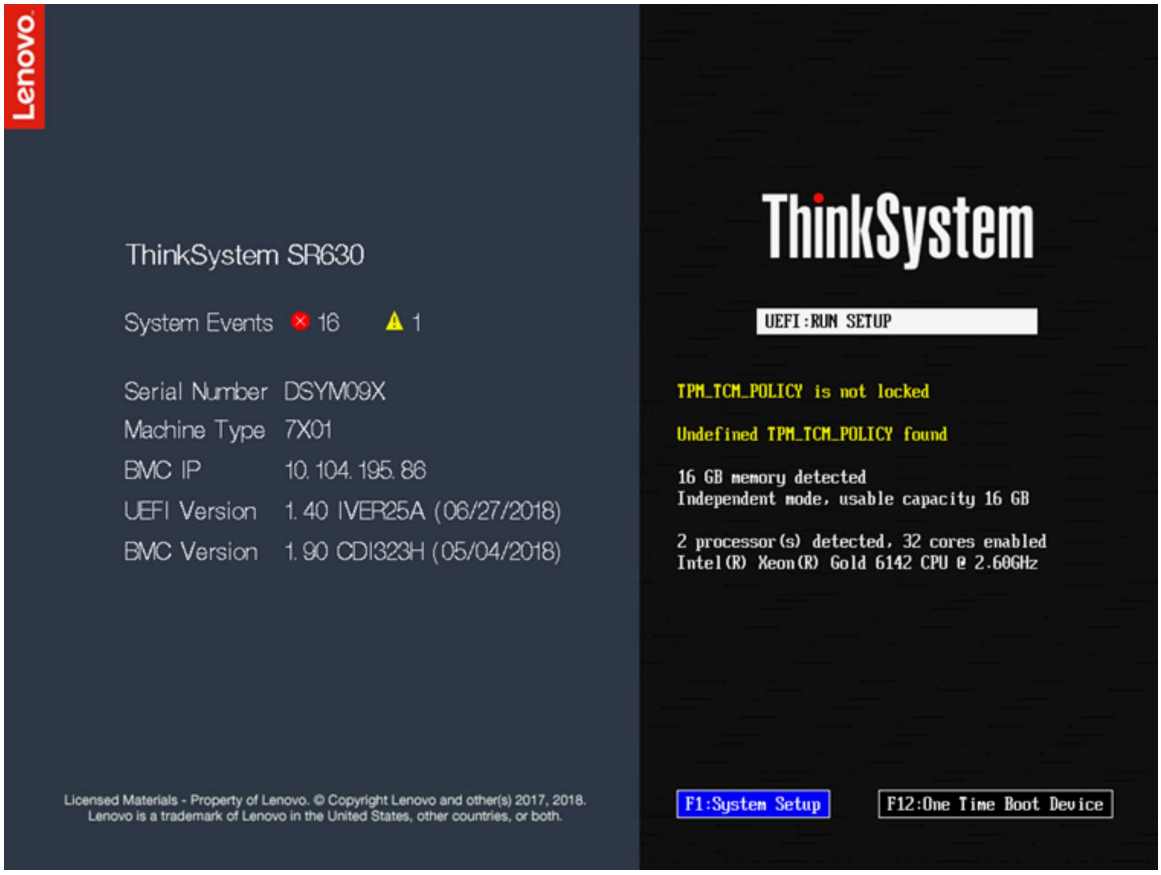
按本主题中的信息通过 **XClarity Provisioning Manager** 设置 **XClarity Controller** 的网络连接。

启动服务器后，可使用 **XClarity Provisioning Manager** 配置 **XClarity Controller** 的网络连接。具有 **XClarity Controller** 的服务器必须连接到 **DHCP** 服务器，或者必须将服务器网络配置为使用

XClarity Controller 静态 IP 地址。要通过 Setup Utility 设置 XClarity Controller 网络连接，请完成以下步骤：

步骤 1. 开启服务器。随后将显示 ThinkSystem 欢迎屏幕。

注：服务器连接到交流电源后最多约 40 秒，电源控制按钮便会激活。



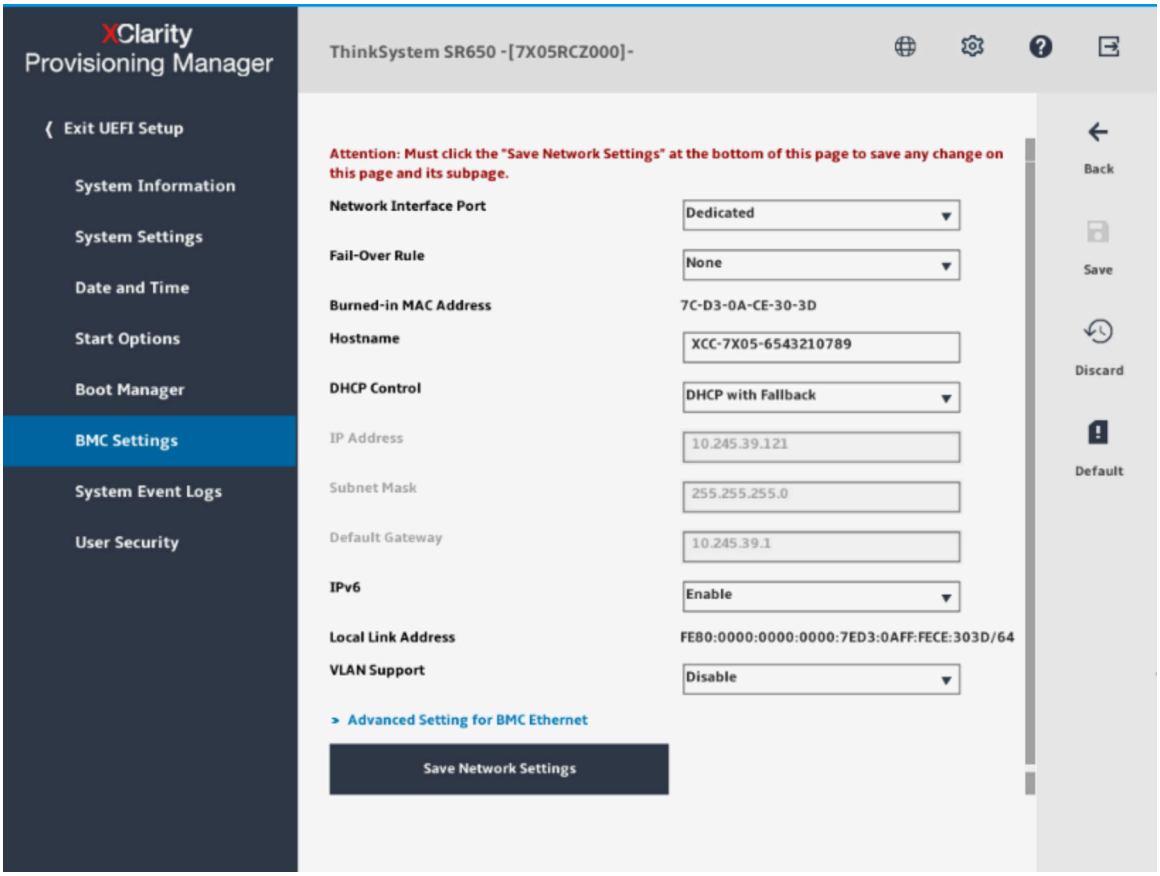
步骤 2. 显示 <F1> System Setup 提示后，按 F1。如果同时设置了开机密码和管理员密码，则必须输入管理员密码才能访问 XClarity Provisioning Manager。

步骤 3. 从 XClarity Provisioning Manager 主菜单中选择 UEFI Setup。

步骤 4. 在下一个屏幕上，选择 BMC Settings；然后，单击 Network Settings。

步骤 5. DHCP Control 字段中有三个 XClarity Controller 网络连接选项：

- Static IP
- DHCP Enabled
- DHCP with Fallback



步骤 6. 选择其中一个网络连接选项。

步骤 7. 如果选择使用静态 IP 地址，那么必须指定 IP 地址、子网掩码和默认网关。

步骤 8. 您也可以使用 Lenovo XClarity Controller Manager 来选择专用网络连接（如果服务器具有专用网络端口）或共享 XClarity Controller 网络连接。

注：

- 专用系统管理网络端口在您的服务器上可能不可用。如果您的硬件没有专用网络端口，***shared*** 设置将是唯一可用的 XClarity Controller 设置。在 Network Configuration 屏幕上的 Network Interface Port 字段中，选择 Dedicated（如果适用）或 Shared。
- 要查找 XClarity Controller 在您服务器上所使用的以太网接口的位置，请参阅服务器随附的文档。

步骤 9. 单击**保存**。

步骤 10. 退出 XClarity Provisioning Manager。

注：

- 您必须等待大约 1 分钟以使更改生效，然后服务器固件才能恢复正常运行。
- 您也可以通过 XClarity Controller Web 界面或命令行界面（CLI）来配置 XClarity Controller 网络连接。在 XClarity Controller Web 界面中，可通过单击导航面板左侧的 **BMC 配置**，然后选择**网络**来配置网络连接。在 XClarity Controller CLI 中，通过使用一些命令来配置网络连接，具体取决于安装的配置。

登录到 XClarity Controller

按本主题中的信息通过 XClarity Controller Web 界面访问 XClarity Controller。

重要： XClarity Controller 初始设置的用户名为 USERID，密码为 PASSWORD（包含数字零，而不是字母 O）。此默认用户设置具有主管访问权限。请在初始配置期间更改此用户名和密码以增强安全性。更改后，不能将 PASSWORD 再次设置为登录密码。

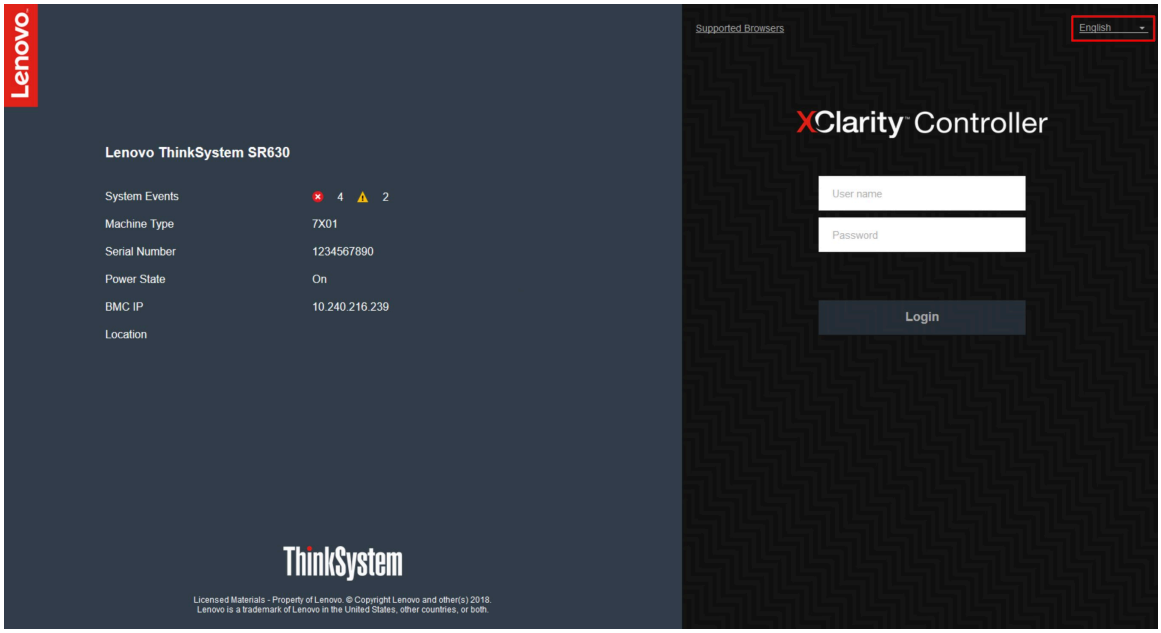
注： 在 Flex System 中，XClarity Controller 用户帐户可由 Flex System Chassis Management Module（CMM）管理，并且可能使用不同于上面所述的 USERID/PASSW0RD 组合。

要通过 XClarity Controller Web 界面访问 XClarity Controller，请完成下列步骤：

步骤 1. 打开 Web 浏览器。在地址或 URL 字段中，输入要连接的 XClarity Controller 的 IP 地址或主机名。

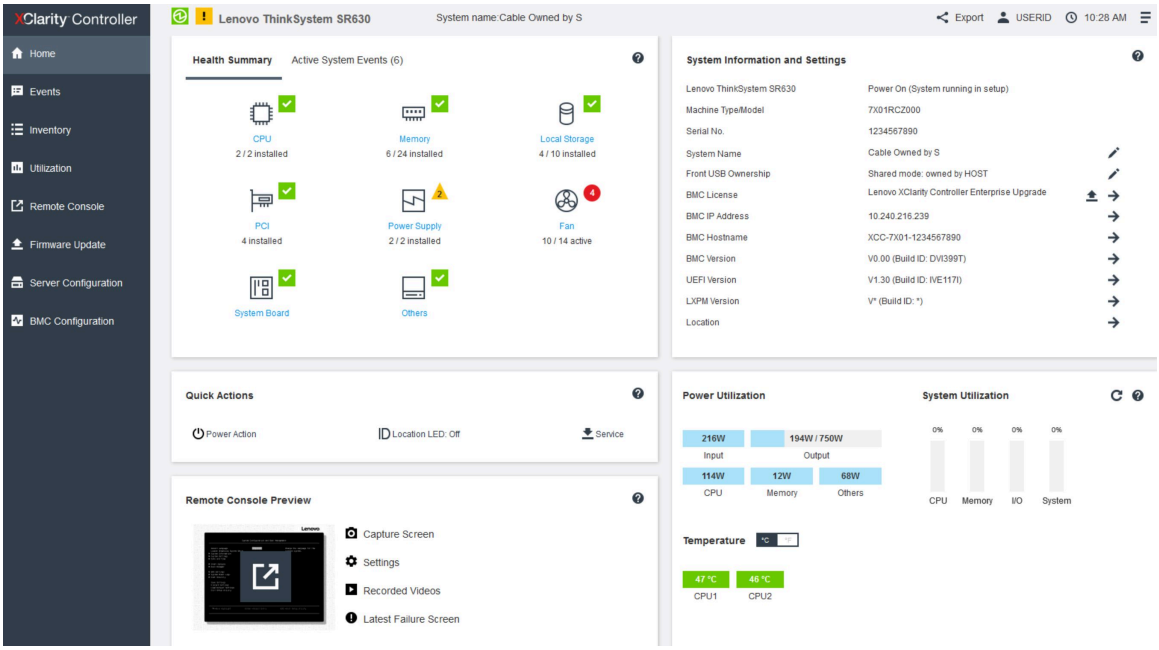
步骤 2. 从语言下拉列表中选择所需的语言。

下图显示了登录窗口。



步骤 3. 在 XClarity Controller 登录窗口中输入您的用户名和密码。如果是首次使用 XClarity Controller，可以从系统管理员处获取用户名和密码。所有登录尝试都会记录到事件日志中。根据系统管理员配置用户 ID 的方式不同，可能登录后需要输入新密码。

步骤 4. 单击**登录**以开始会话。浏览器会打开 XClarity Controller 主页，如下图所示。主页显示 XClarity Controller 所管理的系统的信息，其中图标指示系统当前存在多少紧急错误 1 和多少警告 1。



主页基本上分为两个部分。第一部分是左侧的导航面板，包含一组可执行以下操作的主题：

- 监控服务器状态
- 配置服务器
- 配置 **XClarity Controller** 或 **BMC**
- 更新固件

第二个部分是导航面板右侧提供的图形化信息。模块化的格式方便您快速查看服务器状态及执行某些快捷操作。

Web 界面上的 XClarity Controller 功能描述

下表介绍左侧导航面板中的 **XClarity Controller** 功能。

注：在 **Web** 界面中浏览时，还可以单击问号图标查看联机帮助。

表 1. XClarity Controller 功能

以下三列表格包含可以通过 **XClarity Controller Web** 界面执行的操作的描述。

选项卡	选择	描述
主页	运行状况摘要/活动系统事件	显示系统中主要硬件组件的当前状态。
	系统信息与设置	提供常见系统信息的摘要。
	快捷操作	提供控制服务器电源和位置 **LED** 的快速链接，以及用于下载服务数据的按钮。
	电源利用率/系统利用率/温度	提供当前电源利用率、系统利用率和总体服务器温度的简要概述。
	远程控制台预览	在操作系统级别控制服务器。您可从自己的计算机查看并操作服务器控制台。**XClarity Controller** 主页的远程

表 1. XClarity Controller 功能 （续）

选项卡	选择	描述
		控制台部分显示一个带启动按钮的屏幕图像。右侧工具栏包含以下快捷操作： • 截屏 • 设置 • 录制的视频 • 最近一次故障截屏
事件	事件日志	提供所有硬件和管理事件的历史记录列表。
	审核日志	提供用户操作（如登录到 **Lenovo XClarity Controller**、创建新用户和更改用户密码）的历史记录。可使用审核日志在 **IT** 系统中跟踪和记录认证和控件。
	维护历史记录	显示所有固件更新、配置和硬件更换的历史记录。
	警报接收方	管理系统事件的通知接收方。通过它可配置每个接收方，并管理适用于所有事件接收方的设置。您还可以生成测试事件，以验证通知配置设置。
清单		显示系统中的所有组件及其状态和密钥信息。单击设备可显示其他信息。 **注**：有关解决方案电源状态的更多详细信息，请参阅 **SMM2 Web** 界面。
使用率		以图形或表格的形式显示服务器及其组件的环境/组件温度、电源利用率、电压级别、系统子系统利用率和风扇速度信息。
存储	详细信息	显示存储设备的物理结构和存储配置。
	RAID 设置	查看或修改当前的 **RAID** 配置，包括虚拟磁盘和物理存储设备的信息。
远程控制台		提供访问远程控制台的功能。可使用虚拟介质功能装载系统上或网络位置上（可通过使用 **CIFS**、**NFS**、**HTTPS** 或 **SFTP** 的 **BMC** 进行访问）的 **ISO** 或 **IMG** 文件。已安装的磁盘显示为与服务器连接的 **USB** 磁盘驱动器。
固件更新		• 显示固件级别。 • 更新 **XClarity Controller** 固件和服务器固件。 • 从存储库更新 **XClarity Controller** 固件。
服务器配置	适配器	显示已安装的网络适配器的信息，以及可通过 **XClarity Controller** 配置的设置。
	引导选项	• 选择下次服务器重新启动时一次性引导的引导设备。 • 更改引导模式和引导顺序设置。
	电源策略	• 配置电源模块发生故障期间的电源冗余。 • 配置功率上限策略。 • 配置电源恢复策略。

表 1. XClarity Controller 功能 （续）

选项卡	选择	描述
		注：有关解决方案电源状态的更多详细信息，请参阅 **SMM2 Web** 界面。
	服务器属性	• 监控服务器的各种属性、状态状况和设置。 • 管理服务器启动超时以检测服务器挂起并从中恢复。 • 创建非法侵入消息。您可以创建非法侵入消息以查看用户登录到 **XClarity Controller** 的时间。
BMC 配置	备份与恢复	将 **XClarity Controller** 的配置重置为出厂默认值、备份当前配置或从文件恢复配置。
	许可证	管理可选 **XClarity Controller** 功能的激活密钥。
	网络	配置 **XClarity Controller** 的网络属性、状态和设置。
	安全性	配置 **XClarity Controller** 的安全性属性、状态和设置。
	用户/**LDAP**	• 配置 **XClarity Controller** 登录概要文件和全局登录设置。 • 查看当前登录到 **XClarity Controller** 的用户帐户。 • **LDAP** 选项卡配置用于一个或多个 **LDAP** 服务器的用户认证。您还可通过它启用或禁用 **LDAP** 安全性并管理其证书。
	Call Home	配置 **Call Home** 选项以收集有关系统的信息，并将其发送给 **Lenovo** 以获取服务。

第 3 章　配置 XClarity Controller

请参阅本章中的信息了解 **XClarity Controller** 配置可用的选项。

配置 **XClarity Controller** 时，可使用以下密钥选项：

- 备份与恢复
- 许可证
- 网络
- 安全性
- 用户/**LDAP**

配置用户帐户/LDAP

请参阅本主题中的信息了解如何管理用户帐户。

单击 **BMC 配置**下的**用户/LDAP** 以创建、修改和查看用户帐户并配置 **LDAP** 设置。

本地用户选项卡显示 **XClarity Controller** 中配置的用户帐户以及当前登录到 **XClarity Controller** 的用户帐户。

LDAP 选项卡用于访问保存在 **LDAP** 服务器上的用户帐户的 **LDAP** 配置。

用户认证方法

请参阅本主题中的信息了解 **XClarity Controller** 对登录尝试进行认证可使用的模式。

单击**允许登录**以选择如何对用户的登录尝试进行认证。可以选择以下一种认证方法：

- **仅本地**：通过搜索在 **XClarity Controller** 中配置的本地用户帐户而认证用户。如果没有匹配的用户 **ID** 和密码，则拒绝访问。
- **仅 LDAP**：**XClarity Controller** 尝试使用 **LDAP** 服务器上保存的凭证认证用户。此认证方法*不*搜索 **XClarity Controller** 中的本地用户帐户。
- **本地用户优先，其次 LDAP**：首先尝试进行本地认证。如果本地认证失败，则尝试进行 **LDAP** 认证。
- **LDAP 优先，本地用户其次**：首先尝试进行 **LDAP** 认证。如果 **LDAP** 认证失败，则尝试进行本地认证。

注：

- 仅本地管理的帐户可在 **IPMI** 和 **SNMP** 接口共用。这些接口不支持 **LDAP** 认证。
- 将**允许登录**字段设置为**仅 LDAP** 时，**IPMI** 和 **SNMP** 用户可使用本地管理的帐户进行登录。

创建新角色

按本主题中的信息创建新角色。

创建角色

单击**角色**选项卡，然后单击**创建**以创建自定义角色。

填写以下字段：**角色名称**和**权限级别**。有关权限级别的详细信息，请参阅以下部分。

所创建的角色显示在“用户”部分的角色下拉菜单中。

注：不允许编辑和删除“用户”和“**LDAP**”中所使用的角色名称，但可以修改相应的自定义权限。

权限级别

自定义角色可以支持以下权限的任意组合：

配置 - 网络和 BMC 安全性
用户可以在“**BMC** 安全性”和“网络”页面上修改配置参数。

用户帐户管理
用户可以添加、修改或删除用户，以及更改全局登录设置。

远程控制台访问权限
用户可以访问远程控制台。

远程控制台和远程磁盘访问
用户可以访问远程控制台和虚拟介质功能。

远程服务器电源操作/重新启动
用户可以对远程服务器执行打开电源和重新启动操作。

配置 - 基本
用户可以在服务器属性和事件页面上修改配置参数。

清除事件日志的能力
用户可以清除事件日志。任何人都可以查看事件日志；但是，需要此权限级别才能清除日志。

配置 - 高级（固件更新，重新启动 BMC，还原配置）
用户在配置 **XClarity Controller** 时没有任何限制。此外，用户对 **XClarity Controller** 具有管理访问权限。管理访问权限包括以下高级功能：固件更新、**PXE** 网络引导、恢复 **XClarity Controller** 出厂默认值、通过配置文件修改并恢复 **XClarity Controller** 设置以及重新启动/重置 **XClarity Controller**。

配置 - UEFI 安全性
用户可以修改 **UEFI** 安全设置。

预定义角色

以下为预定义角色，无法进行编辑或删除：

管理员
管理员角色不受任何限制，可以执行所有操作。

只读
只读角色可以查看服务器信息，但不能执行影响系统状态的操作，例如保存、修改、清除、重启、更新固件。

操作员
具有操作员角色的用户拥有以下权限：

- 配置 - 网络和 BMC 安全性
- 远程服务器电源操作/重新启动
- 配置 - 基本
- 清除事件日志的能力
- 配置 - 高级（固件更新，重新启动 BMC，还原配置）

创建新用户帐户

按本主题中的信息创建一个新本地用户。

创建用户

单击**创建**以创建新用户帐户。

填写以下字段：**用户名**、**密码**、**确认密码**，并从下拉菜单中选择**角色**。有关**角色**的更多详细信息，请参阅以下部分。

角色

可以根据用户需要创建新的自定义角色。系统提供以下预定义角色：

管理员
管理员角色不受任何限制，可以执行所有操作。

只读
只读角色可以查看服务器信息，但不能执行影响系统状态的操作，例如保存、修改、清除、重启、更新固件。

操作员
具有操作员角色的用户拥有以下权限：

- 配置 - 网络和 BMC 安全性
- 远程服务器电源操作/重新启动
- 配置 - 基本
- 清除事件日志的能力
- 配置 - 高级（固件更新，重新启动 BMC，还原配置）

SNMPv3 设置

要启用用户的 **SNMPv3** 访问权限，请选中 **SNMPv3 设置**旁边的复选框。下文对以下用户访问选项进行说明：

访问类型
仅支持**获取**操作。**XClarity Controller** 不支持 **SNMPv3 设置**操作。**SNMP3** 只能执行查询操作。

陷阱地址
指定用户的陷阱目标。这可以是 **IP** 地址或主机名。通过使用陷阱，**SNMP** 代理会向管理站通知有关事件（例如，当处理器温度超过限制时）。

认证协议
仅支持 **HMAC SHA** 作为认证协议。**SNMPv3** 安全模型使用该算法进行认证。

隐私协议
可以使用加密来保护 SNMP 客户端和代理之间的数据传输。支持的方法为 CBC-DES 和 AES。

注：即使 SNMPv3 用户使用包含重复字符串的密码，仍将允许访问 XClarity Controller。下面的两个示例供您参考。

- 如果密码设置为“***11111111***”（包含八个 1 的八位数字），并且在输入该密码时输入的 1 意外地超过了八个，用户仍然可以访问 XClarity Controller。例如，如果输入的密码为“***111111111***”（包含十个 1 的十位数字），仍会授予访问权限。将把重复字符串视为具有相同的密钥。
- 如果将密码设置为“***bertbert***”，并且输入该密码时意外地输为了“***bertbertbert***”，用户仍可访问 XClarity Controller。这两个密码被视为具有相同的密钥。

有关更多详细信息，请参阅 RFC 3414 Internet 标准文档（https://tools.ietf.org/html/rfc3414）的第 72 页。

SSH 密钥

XClarity Controller 支持 SSH 公钥认证（RSA 密钥类型）。要向本地用户帐户添加 SSH 密钥，请选中 **SSH 密钥**旁边的复选框。有下列两个选项供选择：

选择密钥文件
从服务器选择要导入到 XClarity Controller 的 SSH 密钥文件。

在文本字段中输入密钥
在文本字段中粘贴或输入 SSH 密钥数据。

注：

- 部分 Lenovo 工具在服务器操作系统上运行时可能会创建一个临时用户帐户以访问 XClarity Controller。该临时帐户不可见，且不占用 12 个本地用户帐户的位置。该帐户使用随机用户名（例如，“20luN4SB”）和密码进行创建。帐户仅用于在内部 Ethernet over USB 接口上访问 XClarity Controller，并且仅限访问 CIM-XML 和 SFTP 接口。创建和删除该临时帐户以及工具通过这些凭证执行的任何操作均将记录在审核日志中。
- 对于 SNMPv3 引擎 ID，XClarity Controller 使用十六进制字符串表示该 ID。这个十六进制字符串是从默认 XClarity Controller 主机名转换而来。请参阅以下示例：

  主机名“XCC 7X06 S4AHJ300”首先转换为 ASCII 格式：**88 67 67 45 55 88 48 54 45 83 52 65 72 74 51 48 48**

  然后使用 ASCII 格式生成十六进制字符串（请忽略中间的空格）：**58 43 43 2d 37 58 30 36 2d 53 34 41 48 4a 33 30 30**

删除用户帐户

按本主题中的信息删除一个本地用户帐户。

要删除本地用户帐户，请单击要删除帐户所在行上的垃圾桶图标。如果拥有权限，您可以删除自己的帐户或其他用户的帐户（即使其当前已登录），除非它是当前剩下的唯一一个有用户帐户管理权限的帐户。删除用户帐户时不会自动终止正在进行的会话。

使用散列密码进行认证

可按本主题中的信息了解如何使用散列密码进行认证。

除了支持使用密码和 **LDAP /AD** 用户帐户，**XClarity Controller** 还支持使用第三方散列密码进行认证。特殊密码使用单向散列 (**SHA256**) 格式，并受 **XClarity Controller Web**、**OneCLI** 和 **CLI** 界面支持。但是请注意，**XCC SNMP**、**IPMI** 和 **CIM** 界面的认证均不支持第三方散列密码。只有 **OneCLI** 工具和 **XCC CLI** 界面可新建带散列密码的帐户，或执行散列密码更新。如果启用了散列密码读取功能，**OneCLI** 工具和 **XClarity Controller CLI** 界面还可通过 **XClarity Controller** 检索散列密码。

通过 XClarity Controller Web 设置散列密码

单击 **BMC 配置**下的**安全性**，然后向下滚动到 **Security Password Manager** 部分启用或禁用第三方密码功能。如果启用，将采用第三方散列密码进行登录认证。也可以启用或禁用从 **XClarity Controller** 检索第三方散列密码。

注：默认情况下，已禁用*第三方密码*和*允许检索第三方密码*功能。

要检查用户密码是*本机*还是*第三方密码*，请单击 **BMC 配置**下的**用户/LDAP** 了解详细信息。信息位于**高级属性**列下方。

注：

- 如果密码是第三方密码，则用户不能进行更改，而**密码**和**确认密码**字段则已灰显。
- 如果第三方密码已到期，用户登录期间将显示警告消息。

通过 OneCLI 功能设置散列密码

- 启用功能

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

- 创建散列密码（无 **Salt**）。以下命令演示如何使用 ***password123*** 密码登录 **XClarity Controller**。

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

- 创建采用散列密码（有 **Salt**）的用户。以下命令演示如何使用 ***password123*** 密码登录 **XClarity Controller**。**Salt=abc**。

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

- 检索散列密码和 **salt**。

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

- 删除散列密码和 **salt**。

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

- 为现有帐户设置散列密码。

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

注：散列密码一经设置，将立即生效。原始标准密码将失效。在本示例中，只有在删除散列密码之后，才能再次使用原始标准密码 ***Passw0rd123abc***。

通过 CLI 功能设置散列密码

- 启用功能

```
> hashpw -sw enabled
```

- 创建散列密码（无 **Salt**）。以下命令演示如何使用 ***password123*** 密码登录 **XClarity Controller**。

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

- 创建采用散列密码（有 **Salt**）的用户。以下命令演示如何使用 ***password123*** 密码登录 **XClarity Controller**。**Salt=abc**。

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

- 检索散列密码和 **salt**。

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

- 删除散列密码和 **salt**。

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

- 为现有帐户设置散列密码。

```
> users -2 -n admin -p Passw0rd123abc -shp 5e884898da28047151d0e56f8dc6292773603d0d6aa-
bbdd62a11ef721d1542d8 -a super
```

注：散列密码一经设置，将立即生效。原始标准密码将失效。在本示例中，只有在删除散列密码之后，才能再次使用原始标准密码 ***Passw0rd123abc***。

设置散列密码之后，务必不要将其用于登录 **XClarity Controller**。登录时，您需要使用纯文本密码。在下面的示例中，纯文本密码为 “**password123**” 。

```
$ pwhash = ‘echo –n password123 | openssl dgst –sha256 | awk '{print $NF}''
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
```

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

配置全局登录设置

按本主题中的信息配置适用于所有用户的登录和密码策略设置。

Web 空闲超时

按本主题中的信息设置 **Web** 空闲会话超时选项。

在 **Web 空闲会话超时**字段中，您可以指定 **XClarity Controller** 断开空闲 **Web** 会话的连接之前等待的时间长度（以分钟为单位）。最长等待时间为 **1440** 分钟。如果设置为 **0**，则 **Web** 会话永不到期。

XClarity Controller 固件最多同时支持六个 **Web** 会话。为释放会话以供他人使用，建议您在结束时注销 **Web** 会话，而不要等待空闲会话超时自动关闭。

注：如果 **XClarity Controller Web** 页面在浏览器中始终保持打开状态且自动刷新，那么您的 **Web** 会话将不会由于在空闲时自动关闭。

帐户安全策略设置

按以下信息了解并设置服务器的帐户安全策略。

注：在 **Flex System** 中，帐户安全策略设置由 **Flex System Chassis Management Module**（**CMM**）来管理，不能通过 **XCC** 进行修改。使用 **CMM** 配置帐户安全策略时，请注意以下事项：

- **CMM** 与 **XCC** 不同，没有*密码到期警告周期（天数）*设置。如果在 **CMM** 中将*密码有效期*配置为超过 **5** 天，**XCC** 将把密码到期警告周期设置为 **5** 天。相反，如果设置为不到 **5** 天，则密码到期警告周期将与*密码有效期*中输入的值相同。
- 对于*最大登录失败次数（次数）*设置，**CMM** 中设置的范围为 **0-100** 次。但是，**XCC** 中定义的范围为 **0-10** 次。因此，如果用户在 **CMM** 中选择的值超过 **10** 次，**XCC** 仍然会将最大登录失败次数设置为 **10** 次。
- 对于*最短密码更改时间间隔（小时数）*设置，**CMM** 中设置的范围为 **0-1440** 小时。但是，**XCC** 中定义的范围为 **0-240** 小时。因此，如果用户在 **CMM** 中选择的值超过 **240** 小时，**XCC** 仍然会将最短密码更改时间间隔设置为 **240** 小时。

以下信息介绍安全设置字段。

首次登录时强制更改密码

设置具有默认密码的新用户后，选中此复选框将强制该用户在首次登录时更改其密码。该字段的默认值是选中该复选框。

需要复杂密码

该选项框默认为选中，复杂密码必须遵循以下规则：

- 仅包含以下字符（不允许空格字符）：**A-Z**、**a-z**、**0-9**、**~‘!@#$%^&*()-+={}[]|:;"’<>,?/._**
- 必须包含至少一个字母
- 必须包含至少一个数字
- 必须至少包含以下任意两种的组合：

  - 至少一个大写字母。
  - 至少一个小写字母。
  - 至少一个特殊字符。
- 不允许使用其他字符（特别是空格或空白字符）
- 密码不能包含两个以上连续相同的字符（即“aaa”）。
- 密码不得在字面上与用户名相同，也不得是用户名的一次或多次重复或用户名字符的反序。
- 密码必须最少包含 **8** 个字符，最多包含 **32** 个字符

如果未选中该选项框，最短密码长度指定的字符数可设置为 **0–32** 个字符。如果最短密码长度设置为 **0**，则帐户密码可能为空。

密码有效期（天）
此字段包含必须更改密码之前允许的最长密码寿命。支持的值为 **0** 到 **30** 天。此字段的默认值为 **14** 天。

密码到期警告周期（天数）
此字段包含警告用户其密码到期之前的天数。如果设置为 **0**，则不发送任何警告。支持的值为 **0** 到 **30** 天。此字段的默认值为 **14** 天。

最短密码长度
此字段包含密码的最小长度。此字段支持 **8** 到 **32** 个字符。此字段的默认值为 **10**。

密码重复使用的最短周期
此字段指定在使用多少个不同的密码后才能复用先前的密码。可以比较最多十个先前密码。选择 **0** 以允许复用所有先前密码。支持的值为 **0** 到 **10**。此字段的默认值为 **5**。

最短密码更改时间间隔（小时数）
此字段包含用户在前后两次密码更改之间必须等待的时间长度。支持的值为 **0** 到 **240** 小时。此字段的默认值为 **1** 小时。

最大登录失败次数（次数）
此字段包含将用户锁定一段时间之前允许的失败登录尝试次数。支持的值为 **0** 到 **10**。此字段的默认值为五次登录失败。

达到最大登录失败次数之后的锁定期（分钟数）
此字段指定达到最大登录失败次数后，**XClarity Controller** 子系统将禁用远程登录尝试的时间长度（以分钟计）。支持的值为 **0** 到 **2880** 分钟。此字段的默认值为 **60** 分钟。

配置 LDAP

按照本主题中的信息查看或更改 **XClarity Controller** 的 **LDAP** 设置。

LDAP 支持包括：

- 支持 **LDAP** 协议版本 **3**（**RFC-2251**）
- 支持标准 **LDAP** 客户机 **API**（**RFC 1823**）
- 支持标准 **LDAP** 搜索过滤器语法（**RFC 2254**）
- 支持适用于传输层安全的轻型目录访问协议（**v3**）扩展（**RFC-2830**）

LDAP 实施支持以下 LDAP 服务器：

- Microsoft Active Directory（Windows 2003、Windows 2008、Windows 2012、Windows 2016、Windows 2019）
- Microsoft Active Directory 应用程序模式（Windows 2003 Server）
- Microsoft 轻型目录服务（Windows 2008、Windows 2012）
- Novell eDirectory Server 版本 8.7、8.8 和 9.4
- OpenLDAP Server 2.1、2.2、2.3 和 2.4

单击 LDAP 选项卡可查看或修改 XClarity Controller 的 LDAP 设置。

XClarity Controller 除使用存储在 XClarity Controller 自身中的本地用户帐户之外（或无需该本地用户帐户），还可通过中央 LDAP 服务器远程认证用户的访问。使用 IBMRBSPermissions 字符串可为每个用户帐户指定权限。除普通用户（密码检查）认证外，您还可以使用 LDAP 服务器向组中分配用户并执行组认证。例如，XClarity Controller 可以与一个或多个组关联，仅当用户属于至少一个与 XClarity Controller 关联的组时，该用户才能通过组认证。

要配置 LDAP 服务器，请完成以下步骤：

1. 在 LDAP **服务器信息**下，有如下选项可用：
   - **使用 LDAP 服务器仅进行认证（和本地授权）**：选择此选项将指示 XClarity Controller 将凭证仅用于向 LDAP 服务器进行认证及检索组成员身份信息。可在 Active Directory 设置部分中配置组名称和权限。
   - **使用 LDAP 服务器进行认证和授权**：选择此选项将指示 XClarity Controller 将凭证既用于向 LDAP 服务器进行认证，也用于识别用户权限。

   注：可手动配置或通过 DNS SRV 记录动态发现用于认证的 LDAP 服务器。

   - **使用预先配置的服务器**：如果启用了 DNS，可通过输入每个服务器的 IP 地址或主机名配置最多四个 LDAP 服务器。每个服务器的端口号是可选的。如果该字段留空，那么为非加密 LDAP 连接使用默认值 389。对于安全连接，默认端口值为 636。您必须至少配置一个 LDAP 服务器。
   - **使用 DNS 查找服务器**：可选择动态发现 LDAP 服务器。RFC2782（用于指定服务位置的 DNS RR）中所述的机制可用于查找 LDAP 服务器。该机制称为 DNS SRV。您需要指定一个完全限定域名（FQDN），以用作 DNS SRV 请求中的域名。
     - **AD 林**：在包含跨域通用组的环境中，必须配置林名称（域集）才能发现所需的全局目录（GC）。在不适用跨域组成员资格的环境中，可以将此字段留空。
     - **AD 域**：您需要指定一个完全限定域名（FQDN），以用作 DNS SRV 请求中的域名。

   如果要启用安全 LDAP，请单击**启用安全 LDAP** 复选框。要支持安全 LDAP，必须具备有效的 SSL 证书，且必须将至少一个 SSL 客户端可信证书导入到 XClarity Controller。您的 LDAP 服务器必须支持传输层安全性（TLS）版本 1.2 以使其与 XClarity Controller 安全 LDAP 客户端兼容。有关证书处理的更多信息，请参阅第 36 页 “SSL 证书处理”。
2. 在**其他参数**下填写信息。以下是参数说明。

   绑定方法

   必须先发送绑定请求，然后才能搜索或查询 LDAP 服务器。该字段控制初始绑定到 LDAP 服务器的执行方式。绑定方法有以下几种：

- **无需凭证**

  使用此方法，可不使用可分辨名称（DN）或密码进行绑定。由于大多数服务器配置为不允许针对特定用户记录的搜索请求，所以非常不推荐使用此方法。

- **使用已配置的凭证**

  使用此方法，可使用已配置的客户端 DN 和密码进行绑定。

- **使用登录凭证**

  使用此方法，可使用在登录过程中提供的凭证进行绑定。用户 ID 可以是 DN、局部 DN、完全限定域名，或是与 XClarity Controller 上配置的“UID 搜索属性”相匹配的用户 ID。如果提供的凭证类似于局部 DN（例如，cn=joe），则会将此局部 DN 添加为已配置的根 DN 的前缀，以尝试创建与用户记录匹配的 DN。如果绑定尝试失败，则将 cn= 添加为登录凭证的前缀，然后将生成的字符串添加为已配置的根 DN 的前缀，以进行最终绑定尝试。

如果初始绑定成功，将执行搜索操作以在 LDAP 服务器上查找属于已登录用户的条目。如果需要，将进行第二次绑定尝试，这次将使用从用户 LDAP 记录中检索到的 DN 以及在登录过程中输入的密码。如果第二次绑定尝试失败，则将拒绝用户访问。仅当使用**无需凭证**或**使用已配置的凭证**绑定方法时，才会执行第二次绑定。

根可分辨名称（DN）

这是 LDAP 服务器上目录树根条目的可分辨名称（DN）（例如，dn=mycompany，dc=com）。此 DN 用作所有搜索请求的基础对象。

UID 搜索属性

当绑定方法设置为**无需凭证**或**使用已配置的凭证**时，在初始绑定到 LDAP 服务器后将跟随一个搜索请求，该请求将检索有关用户的特定信息，其中包括用户的 DN、登录权限和组成员资格。此搜索请求必须指定代表该服务器上用户 ID 的属性名称。此属性名称在该字段中配置。在 Active Directory 服务器上，属性名称通常是 sAMAccountName。在 Novell eDirectory 和 OpenLDAP 服务器上，属性名称是 uid。如果该字段留空，那么默认值是 uid。

组筛选条件

组筛选条件字段用于组认证。用户凭证验证成功后，将尝试进行组认证。如果组认证失败，那么将拒绝用户的登录尝试。配置组筛选条件后，它将用于指定 XClarity Controller 所属的组。这意味着用户必须至少属于一个已配置组认证的组，才能登录成功。如果**组筛选条件**字段留空，那么组认证将自动成功。如果配置了组筛选条件，将尝试将该列表中的至少一个组与用户所属的组进行匹配。如果无匹配项，那么用户将认证失败并被拒绝访问。如果至少有一个匹配项，那么组认证将成功。

该匹配是区分大小写的。筛选条件限制为 511 个字符，并且可以包含一个或多个组名称。必须使用冒号（:）字符对多个组名进行定界。前导空格和尾随空格将被忽略，但任何其他空格将会视为组名称的一部分。

注：通配符（*）将不再视为通配符。为防止安全漏洞，已停止使用通配符概念。组名称可以指定为完整 DN 或只使用 *cn* 部分。例如，可以使用实际 DN 或使用 adminGroup 来指定 DN 为 cn=adminGroup, dc=mycompany, dc=com 的组。

仅在 Active Directory 环境中支持嵌套组成员资格。例如，如果某个用户是 GroupA 和 GroupB 的成员，并且 GroupA 还是 GroupC 的成员，那么也将称该用户为 GroupC 的成员。嵌套搜索将在搜索过 128 个组后停止。系统将先搜索某一级别中的组，然后才搜索较低级别的组。不检测循环。

组搜索属性

在 Active Directory 或 Novell eDirectory 环境中，Group Search Attribute 字段指定用于识别用户所属组的属性名称。在 Active Directory 环境中，属性名称是 memberOf。在 eDirectory 环境中，属性名称是 groupMembership。在 OpenLDAP 服务器环境中，通常将用户分配到 objectClass 等于 PosixGroup 的组中。在此环境中，此字段指定用于识别特定 PosixGroup 成员的属性名称。此属性名称是 memberUid。如果该字段留空，那么过滤器中的属性名称默认设置为 memberOf。

登录权限属性

当用户通过 LDAP 服务器认证成功后，必须检索该用户的登录权限。要检索登录权限，发送到该服务器的搜索筛选条件必须指定与登录权限关联的属性名称。**登录权限属性**字段指定该属性名称。如果该字段留空，那么将为用户分配默认的只读权限（假设用户已通过用户和组认证）。

LDAP 服务器返回的属性值将搜索关键字字符串 IBMRBSPermissions=。该关键字字符串必须紧跟一个二进制位串，该二进制位串输入为 12 个连续的 0 或 1。每一位表示一组功能。这些位根据位置进行编号。最左边的位是位置 0，最右边的位是位置 11。如果某个位置上的值为 1，则表示将启用与该位置关联的功能。如果某个位置上的值为 0，则表示将禁用与该位置相关联的功能。

字符串 IBMRBSPermissions=010000000000 就是一个有效示例。采用“IBMRBSPermissions=关键字”这种形式可方便管理员将其放置在该字段的任意位置。这样一来，LDAP 管理员将能够重复使用现有属性，而不必对 LDAP 模式进行扩展。另一方面，该属性也得以用于其原始用途。您可以在该字段的任意位置添加此关键字字符串。您使用的属性可以允许自由格式的字符串。成功检索到此属性后，可根据下表中的信息对 LDAP 服务器返回的值进行解读。

表 2. 权限位

以下三列表格包含对位置的说明。

位置	功能	说明
0	始终拒绝	用户将始终认证失败。此功能可用于阻止与特定组关联的一个或多个特定用户。
1	管理员访问权限	授予用户管理员权限。用户对每个功能具有读/写访问权限。如果设置此位，那么不必分别设置其他位。
2	只读访问权限	用户具有只读访问权限，并且无法执行任何维护过程（例如，重新启动、远程操作或固件更新）或进行修改（例如，保存、清除或还原功能）。位置 2 和所有其他位互斥，其中位置 2 具有最低优先顺序。当设置了任何其他位时，将忽略此位。
3	联网和安全性	用户可以修改安全性、网络协议、网络接口、端口分配和串口配置。
4	用户帐户管理	用户可以添加、修改或删除用户，并可以在登录概要文件窗口中更改全局登录设置。
5	远程控制台访问权限	用户可以访问远程服务器控制台。
6	远程控制台和远程磁盘访问权限	用户可以访问远程服务器控制台和远程磁盘功能。
7	远程服务器电源操作/重新启动权限	用户可以对远程服务器执行打开电源和重新启动操作。

表 2. 权限位 （续）

位置	功能	说明
8	基本适配器配置	用户可以在系统设置和警报窗口中修改配置参数。
9	清除事件日志的能力	用户可以清除事件日志。 **注：**所有用户都可查看事件日志；但是，用户需要具有此权限级别才能清除日志。
10	高级适配器配置	用户在配置 **XClarity Controller** 时没有任何限制。此外，用户对 **XClarity Controller** 具有管理访问权限。用户可以执行以下高级功能：固件升级、**PXE** 网络引导、恢复 **XClarity Controller** 出厂默认值、根据配置文件修改和恢复适配器配置以及重新启动/重置 **XClarity Controller**。
11	保留	将保留此位置以供将来使用。如果未设置任何位，那么用户具有只读权限。直接从用户记录中检索到的登录权限指定优先级将拥有最高优先级。 如果在用户记录中没有登录权限属性，那么将尝试从用户所属的组中检索权限。此操作在组认证阶段中执行。系统将针对所有组向用户以兼或方式分配所有位。 仅当其他所有位均设置为零时，才会设置“只读访问权限”位（位置 **2**）。如果为任何组设置了“始终拒绝”位（位置 **0**），那么将拒绝用户访问。“始终拒绝”位（位置 **0**）始终优先于其他所有位。

如果未设置任何位，则为用户将默认值设置为**只读**。

请注意，直接从用户记录中检索到的登录权限将拥有最高优先级。如果记录中没有用户的登录权限属性，那么将尝试从用户所属的组中检索权限（如果已配置，则检索与组筛选条件匹配的权限）。在此情况下，系统将针对所有组向用户以兼或方式分配所有位。同样，仅当所有其他位为零时，才会设置**只读访问权限**位。另请注意，如果为任何组设置了**始终拒绝**位，则用户将被拒绝访问。**始终拒绝**位始终优先于其他所有位。

注：如果您向用户授予修改基本适配器配置参数、网络适配器配置参数和/或与安全性相关的适配器配置参数的权限，则应考虑向同一用户授予重新启动 **XClarity Controller**（位置 **10**）的权限。如果没有此权限，用户可能能够更改参数（例如，适配器的 **IP** 地址），但是将无法使参数生效。

3. 在 **Active Directory 设置**下选择是否**针对 Active Directory 用户启用基于角色的增强安全性**（如果是**使用 LDAP 服务器进行认证和授权**模式），或配置**本地授权组**（如果是**使用 LDAP 服务器仅进行认证（和本地授权）**模式）。

   - **启用针对 Active Directory 用户的基于角色的增强安全性支持**

     如果启用基于角色的增强安全性设置，则必须配置自由格式的服务器名称以用作此特定 **XClarity Controller** 的目标名称。目标名称可通过基于角色的安全性（**RBS**）管理单元与 **Active Directory** 服务器上的一个或多个角色相关联。这可以通过以下方式来完成：创建受管目标，向目标提供特定名称，然后将目标与相应角色相关联。如果在此字段中配置一个名称，则它可以为属于同一角色的用户和 **XClarity Controller**（目标）定义特定角色。当用户登录到 **XClarity Controller** 且通过 **Active Directory** 进行认证时，将从该目录中检索用户所属的角色。分配给用户的权限将从符合以下条件的角色中提取：角色包含与此处已配置的服务器名称相匹配的成员目标，或包含与任何 **XClarity Controller** 相匹配的目标。多个 **XClarity Controller** 可以共享同一目标名称。因此，可同时对多个 **XClarity Controller**

进行分组，并作为一个受管目标分配到相同的一个或多个角色。与此相反，每个 **XClarity Controller** 仅有一个唯一名称。

- **本地授权组**

  配置组名称以便为用户组提供本地授权规范。可为每个组名称分配与上表中所述相同的权限（角色）。**LDAP** 服务器将用户关联到一个组名称。用户登录时，将为其分配与其所属组关联的权限。单击“+”图标可配置更多组，单击“**x**”图标可删除组。

配置网络协议

按照本主题中的信息查看或建立 **XClarity Controller** 的网络设置。

配置以太网设置

按本主题中的信息查看或更改 **XClarity Controller** 以太网连接的通信方式。

注：AMD 服务器不支持以太网故障转移功能。

XClarity Controller 使用两个网络控制器。一个网络控制器连接到专用管理端口，另一个网络控制器连接到共享端口。每个网络控制器均分配了独有的固化 **MAC** 地址。如果使用 **DHCP** 为 **XClarity Controller** 分配 **IP** 地址，那么当用户在网络端口之间进行切换，或者故障自专用网络端口转移至共享网络端口时，**DHCP** 服务器可能会为 **XClarity Controller** 分配另一个 **IP** 地址。如果使用 **DHCP**，建议用户使用主机名访问 **XClarity Controller**，而不要使用 **IP** 地址。即使 **XClarity Controller** 的网络端口没有更改，但是在 **DHCP** 租约到期或 **XClarity Controller** 重新启动时，**DHCP** 服务器也有可能为 **XClarity Controller** 分配另一个 **IP** 地址。如果用户需要使用固定不变的 **IP** 地址访问 **XClarity Controller**，那么应对 **XClarity Controller** 配置静态 **IP** 地址，而不是 **DHCP**。

单击 **BMC 配置**下的**网络**以修改 **XClarity Controller** 的以太网设置。

配置 XClarity Controller 主机名

默认 **XClarity Controller** 主机名由字符串“**XCC -**”后接服务器机器类型和服务器序列号组合生成（例如，“**XCC-7X03-1234567890**”）。可在此字段中输入最多 **63** 个字符来更改 **XClarity Controller** 主机名。主机名不得包含句点（.），仅可包含字母、数字、连字符和下划线字符。

以太网端口

此设置控制管理控制器使用的以太网端口（包括共享端口和专用端口）的启用。

禁用之后，不会为任何以太网端口分配任何 **IPv4** 或 **IPv6** 地址，并且阻止对任何以太网配置进行任何进一步的更改。

注：此设置不会影响服务器正面的 **USB LAN** 接口或 **USB** 管理端口。这些接口具有自己的专用启用设置。

配置 IPv4 网络设置

要使用 **IPv4** 以太网连接，请完成以下步骤：

1. 启用 **IPv4** 选项。

   注：禁用以太网接口会阻止从外部网络访问 **XClarity Controller**。

2. 从**方法**字段中选择以下选项之一：

- **从 DHCP 获取 IP**：XClarity Controller 将从 DHCP 服务器获取其 IPv4 地址。
- **使用静态 IP 地址**：XClarity Controller 将使用用户指定值作为其 IPv4 地址。
- **优先尝试 DHCP，再使用静态 IP 地址**：XClarity Controller 将尝试从 DHCP 服务器获取 IPv4 地址，但如果该尝试失败，XClarity Controller 将使用用户指定的 IPv4 地址。

3. 在**静态地址**字段中，输入要分配给 XClarity Controller 的 IP 地址。

   注：IP 地址必须包含以句点分隔的四个整数（从 **0** 到 **255**）且不含空格。如果方法设置为**从 DHCP 获取 IP**，则此字段不可配置。

4. 在**网络掩码**字段中，输入 XClarity Controller 使用的子网掩码。

   注：子网掩码必须包含以句点分隔的四个整数（从 **0** 到 **255**）且不含空格和连续句点。默认设置为 **255.255.255.0**。如果方法设置为**从 DHCP 获取 IP**，则此字段不可配置。

5. 在**默认网关**字段中，输入网络网关路由器。

   注：网关地址必须包含以句点分隔的四个整数（从 **0** 到 **255**）且不含空格和连续句点。如果方法设置为**从 DHCP 获取 IP**，则此字段不可配置。

配置高级以太网设置

单击**高级以太网**选项卡以设置其他以太网设置。

注：在 Flex System 中，VLAN 设置由 Flex System CMM 管理，而无法在 XClarity Controller 上修改。

要启用虚拟 LAN（VLAN）标记，请选择**启用 VLAN** 复选框。启用 VLAN 并配置 VLAN ID 之后，XClarity Controller 仅接受带指定 VLAN ID 的数据包。可以使用 **1** 到 **4094** 之间的数值配置 VLAN ID。

从 **MAC 选择**列表中选择以下选项之一：

- 使用固化 MAC 地址

  固化 MAC 地址选项是制造商向此 XClarity Controller 分配的唯一物理地址。该地址是只读字段。

- 使用自定义 MAC 地址

  如果指定了一个值，那么本地管理地址会覆盖固化 MAC 地址。本地管理地址必须是 000000000000 到 FFFFFFFFFFFF 之间的一个十六进制值。此值格式必须为 *xx:xx:xx:xx:xx:xx*，其中 *x* 为 **0** 到 **9** 或“**a**”到“**f**”之间的十六进制数。XClarity Controller 不支持使用多播地址。多播地址的第一个字节是奇数（最低有效位设置为 **1**）；因此，第一个字节必须是偶数。

在**最大传输单元**字段中，为网络接口指定数据包的最大传输单元（以字节为单位）。最大传输单元的范围是 **60** 到 **1500**。此字段的默认值是 **1500**。

要使用 **IPv6** 以太网连接，请完成以下步骤：

配置 IPv6 网络设置

1. 启用 **IPv6** 选项。
2. 使用以下分配方法之一为接口分配 **IPv6** 地址：
   - 使用无状态地址自动配置

- 使用有状态地址配置（**DHCPv6**）
- 使用静态分配的 **IP** 地址

  注：选择**使用静态分配的 IP 地址**后，将要求您输入以下信息：

  – **IPv6** 地址
  – 前缀长度
  – 网关

配置 DNS

按照本主题中的信息查看或更改 **XClarity Controller** 的域名系统（**DNS**）设置。

注：在 **Flex System** 中，无法在 **XClarity Controller** 上修改 **DNS** 设置。**DNS** 设置由 **CMM** 管理。

单击 **BMC 配置**下的**网络**以查看或修改 **XClarity Controller** 的 **DNS** 设置。

如果单击**使用其他 DNS 地址服务器**复选框，最多可指定您网络上的三个域名系统服务器的 **IP** 地址。每个 **IP** 地址必须包含以句点分隔的四个整数（从 **0** 到 **255**）。这些 **DNS** 服务器地址将添加到搜索列表的顶部，因此首先将在这些服务器上进行主机名搜索，然后才会在 **DHCP** 服务器自动分配的服务器上进行主机名搜索。

配置 DDNS

按本主题中的信息在 **XClarity Controller** 上启用或禁用动态域名系统（**DDNS**）协议。

单击 **BMC 配置**下的**网络**以查看修改 **XClarity Controller** 的 **DDNS** 设置。

单击**启用 DDNS** 复选框以启用 **DDNS**。启用 **DDNS** 后，**XClarity Controller** 会通知域名服务器实时更改 **XClarity Controller** 所配置的主机名、地址或域名服务器中存储的其他信息的活动域名服务器配置。

从项目列表中选择一个选项，以决定要如何选择 **XClarity Controller** 的域名。

- **使用定制域名**：可指定 **XClarity Controller** 所属的域名。
- **使用从 DHCP 服务器获取的域名**：**XClarity Controller** 所属的域名由 **DHCP** 服务器指定。

配置 Ethernet over USB

按本主题中的信息控制 **Ethernet over USB** 接口，用于在服务器和 **XClarity Controller** 之间进行带内通信。

单击 **BMC 配置**下的**网络**以查看或修改 **XClarity Controller** 的 **Ethernet over USB** 设置。

Ethernet over USB 用于与 **XClarity Controller** 进行带内通信。单击此复选框以启用或禁用 **Ethernet over USB** 接口。

重要：如果禁用 **Ethernet over USB**，那么将无法使用 **Linux** 或 **Windows** 闪存实用程序对 **XClarity Controller** 固件或服务器固件执行带内更新。

选择 **XClarity Controller** 分配地址到 **Ethernet over USB** 接口端点的方法。

- **对 Ethernet over USB 使用 IPv6 链路本地地址：** 此方法使用基于分配到 Ethernet over USB 接口端点的 MAC 地址生成的 IPv6 地址。通常情况下，IPv6 链路本地地址使用 MAC 地址生成（RFC 4862），但 Windows 2008 和更高版本的 2016 操作系统在接口主机端不支持静态链路本地 IPv6 地址。相反，默认的 Windows 行为是在运行时重新生成随机的链路本地地址。如果 XClarity Controller 的 Ethernet over USB 接口配置为使用 IPv6 链路本地地址模式，各种使用此接口的功能将无法工作，因为 XClarity Controller 不知道 Windows 分配给接口的地址。如果服务器运行 Windows，请使用其他 Ethernet over USB 地址配置方法，或使用此命令禁用默认 Windows 行为：***netsh interface ipv6 set global randomizeidentifiers=disabled***
- **对 Ethernet over USB 使用 IPv4 链路本地地址：** 分配一个 169.254.0.0/16 范围内的 IP 地址给 XClarity Controller 和网络的服务器端。
- **为 Ethernet over USB 配置 IPv4 设置：** 此方法将指定分配给 XClarity Controller 和 Ethernet over USB 接口服务器端的 IP 地址和网络掩码。

注：

1. 操作系统 IP 配置设置不用于设置 Ethernet Over USB 接口的操作系统 IP 地址，但用于通知 BMC，说明 Ethernet over USB 的操作系统 IP 地址已更改。
2. 配置 Ethernet over USB 的三项 IP 设置时，需要在本地操作系统中配置 Ethernet over USB 接口的操作系统 IP 地址。

通过单击**对 Ethernet over USB 端口转发启用外部以太网**复选框，并填写您希望从管理网络接口到服务器的转发端口的映射信息，可以控制外部以太网端口号到 Ethernet over USB 端口号的映射。

配置 SNMP

按本主题中的信息配置 SNMP 代理。

完成以下步骤以配置 XClarity Controller SNMP 警报设置。

1. 单击 BMC **配置**下的**网络**。
2. 选中相应的复选框以启用 **SNMPv1 陷阱**、**SNMPv2 陷阱**和/或 **SNMPv3 陷阱**。
3. 如果启用 **SNMPv1 陷阱**或 **SNMPv2 陷阱**，请填写以下字段：
   a. 在**团体名称**字段中，输入团体名称；名称不能为空。
   b. 在**主机**字段中，输入主机地址。
4. 如果启用 **SNMPv3 陷阱**，请填写以下字段：
   a. 在**引擎 ID** 字段中，输入引擎 ID。引擎 ID 不能为空。
   b. 在**陷阱接收端口**字段中，输入端口号。默认端口号为 **162**。
5. 如果启用 SNMP 陷阱，请选择以下希望收到警报的事件类型：
   - **紧急**
   - **注意**
   - **系统**

   注：单击每个主要类别，可以进一步选择希望收到警报的子类别事件类型。

启用或禁用 IPMI 网络访问权限

按本主题中的信息控制对 XClarity Controller 的 IPMI 网络访问权限。

单击 **BMC 配置**下的**网络**以查看或修改 **XClarity Controller** 的 **IPMI** 设置。请填写以下字段以查看或修改 **IPMI** 设置：

IPMI over LAN 访问
单击开关以启用或禁用对 **XClarity Controller** 的 **IPMI** 网络访问权限。

重要：

- 如果不在服务器上使用任何通过 **IPMI** 协议来访问 **XClarity Controller** 的工具或应用程序，强烈建议禁用 **IPMI** 网络访问权限以提高安全性。
- 默认情况下，已禁用对 **XClarity Controller** 的 **IPMI over LAN** 访问。

使用 IPMI 命令配置网络设置

按本主题中的信息使用 **IPMI** 命令配置网络设置。

由于每个 **BMC** 网络设置使用单独的 **IPMI** 请求进行配置且无任何特定顺序，因此重新启动 **BMC** 以应用暂挂的网络更改前 **BMC** 无法查看全部网络设置。更改网络设置的请求可能在提出请求时被认为成功，但可能在之后请求进行其他更改时被认为无效。如果重新启动 **BMC** 后，暂挂的网络设置不兼容，则不会应用新设置。重新启动 **BMC** 后，应尝试使用新设置访问 **BMC** 以确保其已按预期被应用。

服务启用与端口分配

按本主题中的信息查看或更改 **XClarity Controller** 上某些服务使用的端口号。

单击 **BMC 配置**下的**网络**以查看或修改 **XClarity Controller** 的端口分配。请填写以下字段以查看或修改端口分配：

Web
端口号为 **80**。此字段用户不可配置。

Web over HTTPS
在此字段中指定 **Web Over HTTPS** 的端口号。默认值为 **443**。

REST over HTTPS
端口号将自动更改为 **Web over HTTPS** 字段中指定的端口号。此字段用户不可配置。

CIM over HTTP
在此字段中指定 **CIM over HTTP** 的端口号。默认值为 **5989**。

注：默认情况下禁用 **CIM**。

远程呈现
在此字段中指定远程呈现的端口号。默认值为 **3900**。

IPMI over LAN
端口号为 **623**。此字段用户不可配置。

注：默认情况下禁用 **IPMI**。

SFTP

在此字段中指定用于 SSH 文件传输协议（SFTP）的端口号。端口号为 115。此字段用户不可配置。

注：针对 OneCLI 带内更新，必须设置 IMM.SFTPPortControl=open。

SLP
在此字段中指定用于 SLP 的端口号。端口号为 427。此字段用户不可配置。

注：XClarity Controller 报告两种服务类型：

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

SSDP
端口号为 1900。此字段用户不可配置。

SSH
在此字段中指定配置用于通过 SSH 协议访问命令行界面的端口号。默认值为 22。

SNMP 代理
在此字段中指定在 XClarity Controller 上运行的 SNMP 代理的端口号。默认值为 161。有效端口号值为 1 到 65535。

SNMP 陷阱
在此字段中指定用于 SNMP 陷阱的端口号。默认值为 162。有效端口号值为 1 到 65535。

配置访问限制

按本主题中的信息查看或更改阻止从 IP 地址或 MAC 地址访问 XClarity Controller 的设置。

单击 BMC 配置下的**网络**以查看或修改 XClarity Controller 的访问控制设置。

阻止列表和时间限制

利用这些选项，可以在特定时间段内阻止特定的 IP/MAC 地址。

- **阻止的 IP 地址列表**
  - 您可输入最多三个不允许访问 XClarity Controller 的 IPv4 地址（或范围）和最多三个 IPv6 地址（或范围），以逗号分隔。请参阅以下 IPv4 示例：
  - 单个 IPv4 地址示例：192.168.1.1
  - 超级网络 IPv4 地址示例：192.168.1.0/24
  - IPv4 范围示例：192.168.1.1–192.168.1.5
- **阻止的 MAC 地址列表**
  - 您可输入最多三个不允许访问 XClarity Controller 的 MAC 地址，以逗号分隔。例如：11:22:33:44:55:66。
- **限制访问（一次性）**
  - 您可设置一个一次性有效的时间间隔，该期间内不允许访问 XClarity Controller。对于指定的时间间隔：
  - 开始日期和时间必须晚于当前 XCC 时间。

– 结束日期和时间必须晚于开始日期和时间。

- **限制访问（日常）**
  - 您可设置一个或多个日常时间间隔，该期间内不允许访问 **XClarity Controller**。对于每个指定的时间间隔：
  - 结束日期和时间必须晚于开始日期和时间。

外部触发的阻止列表

利用这些选项，可以设置自动阻止客户端从特定的 **IP** 地址（**IPv4** 和 **IPv6**）连续尝试使用不同的错误用户名或密码登录到 **XClarity Controller**。

自动阻止功能将动态识别来自特定 **IP** 地址的登录失败次数过多的情形，并在预定义的时间内阻止从该地址访问 **XClarity Controller**。

- **特定 IP 的最大登录失败次数**
  - 该最大次数表示在特定 **IP** 地址被锁定之前，用户可以从该 **IP** 地址使用错误的密码发生登录失败的次数。
  - 如果设置为 **0**，则 **IP** 地址将永远不会由于登录失败而被锁定。
  - 从该 **IP** 地址成功登录后，特定 **IP** 地址的失败登录计数器将重置为零。
- **阻止 IP 的锁定期**
  - 在用户可以尝试从锁定的 **IP** 地址重新登录之前必须经过的最短时间（以分钟为单位）。
  - 如果设置为 **0**，则在管理员显式解锁之前，系统将始终阻止从锁定的 **IP** 地址进行访问。
- **阻止列表**
  - 阻止列表显示了所有锁定的 **IP** 地址。可以从“阻止列表”中解锁一个或所有 **IP** 地址。

配置前面板 USB 端口以进行管理

按本主题中的信息配置 **XClarity Controller** 前面板 **USB** 端口到管理。

在某些服务器上，可切换前面板 **USB** 端口以连接到服务器或 **XClarity Controller**。连接到 **XClarity Controller** 主要用于运行 **Lenovo XClarity** 移动应用程序的移动设备。在移动设备和服务器的前面板之间连接 **USB** 线缆后，设备上正在运行的移动应用程序和 **XClarity Controller** 之间将建立 **Ethernet over USB** 连接。

单击 **BMC 配置**下的**网络**以查看或修改 **XClarity Controller** 的前面板 **USB** 端口到管理设置。

有四种类型的设置可以选择：

主机专用模式
前面板 **USB** 端口始终仅连接到服务器。

BMC 专用模式
前面板 **USB** 端口始终仅连接到 **XClarity Controller**。

共享模式：由 BMC 所有
前面板 **USB** 端口由服务器和 **XClarity Controller** 共享，但该端口切换到 **XClarity Controller**。

共享模式：由主机所有

前面板 USB 端口由服务器和 XClarity Controller 共享，但该端口切换到主机。

有关该 Mobile 应用程序的其他信息，请参阅以下站点：

http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/lxca_usemobileapp.html

注：

- 如果前面板 USB 端口配置为共享模式，则未通电时该端口连接到 XClarity Controller，而通电时连接到服务器。通电后，前面板 USB 端口可在服务器和 XClarity Controller 之间来回切换。在共享模式下，通过按住前面板标识按钮（对于计算节点可能为 USB 管理按钮）3 秒钟以上，该端口也可在主机和 XClarity Controller 之间切换。
- 配置为共享模式且 USB 端口当前连接到服务器时，XClarity Controller 可支持将前面板 USB 端口切换回 XClarity Controller 的请求。执行此请求时，前面板 USB 端口将保持连接到 XClarity Controller，直至到 XClarity Controller 的 USB 无活动时间达到无活动超时指定的时间。

配置安全设置

按本主题中的信息配置安全协议。

注：默认的最低 TLS 版本设置为 TLS 1.2，但如果浏览器或管理应用程序需要，也可配置 XClarity Controller 使用其他 TLS 版本。要了解更多信息，请参阅第 148 页 “tls 命令”。

单击 BMC **配置**下**安全性**以访问和配置 XClarity Controller 的安全性属性、状态和设置。

SSL 概述

本主题概述 SSL 安全协议。

SSL 是一种提供通信隐私的安全协议。SSL 使客户端/服务器应用程序能够以一种防止窃听、篡改和消息伪造的方式进行通信。您可以配置 XClarity Controller 为不同类型的连接使用 SSL 支持，例如安全 Web 服务器（HTTPS）、安全 LDAP 连接（LDAPS）、CIM over HTTPS 和 SSH 服务器，还可以管理 SSL 要求的证书。

SSL 证书处理

本主题介绍对配合 SSL 安全协议使用的证书进行管理的信息。

您可以将 SSL 与自签名证书或由第三方证书颁发机构签名的证书配合使用。虽然使用自签名证书是使用 SSL 的最简单方法，但是该方法会带来一个较小的安全性风险。发生风险的原因是，针对 SSL 客户端和 SSL 服务器之间首次尝试的连接，SSL 客户端无法验证 SSL 服务器的身份。例如，第三方有可能会冒充 XClarity Controller Web 服务器，并拦截真实 XClarity Controller Web 服务器和用户 Web 浏览器之间的数据流。如果在浏览器和 XClarity Controller 之间首次连接时，将自签名证书导入到浏览器的证书库中，那么针对该浏览器的所有后续通信都将是安全的（假设首次连接未遭受攻击）。

要获取更完整的安全性，可以使用证书颁发机构（CA）签名的证书。要获取签名证书，需要选择**生成证书签名请求（CSR）**。选择**下载证书签名请求（CSR）**并将该证书签名请求（CSR）发送到 CA 以获取签名证书。收到签名证书后，选择**导入签名证书**以将其导入 XClarity Controller。

CA 的功能是验证 XClarity Controller 的身份。一个证书包含 CA 和 XClarity Controller 的数字签名。如果某知名 CA 发放了证书，或者 CA 的证书已导入到 Web 浏览器中，那么浏览器可以验证该证书，并明确地识别 XClarity Controller Web 服务器。

XClarity Controller 要求 HTTPS 服务器、CIM over HTTPS 和安全 LDAP 客户端与证书配合使用。此外，安全 LDAP 客户端还要求导入一个或多个可信证书。安全 LDAP 客户端使用可信证书来明确识别 LDAP 服务器。可信证书是由签署 LDAP 服务器证书的 CA 所发出的证书。如果 LDAP 服务器使用自签名证书，那么可信证书可以是 LDAP 服务器本身的证书。如果在您的配置中使用了多个 LDAP 服务器，必须导入其他可信证书。

SSL 证书管理

本主题介绍使用 SSL 安全协议证书进行证书管理时可选择的部分操作。

单击 BMC 配置下的**安全性**以配置 SSL 证书管理。

管理 XClarity Controller 证书时，将显示以下操作：

下载签名证书
使用此链接下载当前安装的证书的副本。证书可以 PEM 或 DER 格式下载。可使用 OpenSSL（www.openssl.org）等第三方工具查看证书内容。使用 OpenSSL 查看证书内容的命令行类似于如下：

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

下载证书签名请求（CSR）
使用此链接下载证书签名请求的副本。CSR 可以 PEM 或 DER 格式下载。

生成签名证书
生成自签名证书。操作完成后，可能会使用新证书启用 SSL。

注：执行**生成签名证书**操作时，“生成 HTTPS 的自签名证书”窗口将打开。您将看到填写必需和可选字段的提示。您*必须*完成必填字段。输入信息完毕后，请单击**生成**以完成任务。

生成证书签名请求（CSR）
生成证书签名请求（CSR）操作完成后，可下载 CSR 文件并将其发送到证书颁发机构（CA）进行签名。

注：执行**生成证书签名请求（CSR）**操作时，“生成 HTTPS 的证书签名请求”窗口将打开。您将看到填写必需和可选字段的提示。您*必须*完成必填字段。输入信息完毕后，请单击**生成**以完成任务。

导入签名证书
使用此操作导入签名证书。要获得签名证书，必须先生成证书签名请求（CSR）并将其发送到证书颁发机构（CA）。

配置安全 Shell 服务器

按本主题中的信息了解并启用 SSH 安全协议。

单击 BMC 配置下的**网络**以配置安全 Shell 服务器。

要使用 SSH 协议，需要先生成一个密钥以启用 SSH 服务器。

注：

- 使用此选项不需要任何证书管理。
- XClarity Controller 将创建一个初始 SSH 服务器密钥。如果要生成新的 SSH 服务器密钥，请单击 BMC 配置下的**网络**，然后单击**重新生成密钥**。
- 完成操作后，必须重新启动 XClarity Controller 以使更改生效。

IPMI over Keyboard Controller Style（KCS）访问

按本主题中的信息可控制通过 IPMI over Keyboard Controller Style（KCS）对 XClarity Controller 进行访问。

XClarity Controller 提供 IPMI 接口，该接口使用 KCS 通道，无需认证。

单击 BMC 配置下的**安全性**以启用或禁用 IPMI over KCS 访问。

注：更改设置后，必须重新启动 XClarity Controller 以使更改生效。

重要：如果不在服务器上运行任何通过 IPMI 协议来访问 XClarity Controller 的工具或应用程序，强烈建议禁用 IPMI KCS 访问以提高安全性。XClarity Essentials 使用 IPMI over KCS 接口访问 XClarity Controller。如果禁用 IPMI over KCS 接口，在服务器上运行 XClarity Essentials 前请重新启用该接口。然后在使用完毕后禁用该接口。

阻止系统固件降级

按本主题中的信息阻止系统固件被更改到较低的固件级别。

此功能可决定是否允许系统固件回退到较低的固件级别。

单击 BMC 配置下的**网络**可阻止系统固件降级。

要启用或禁用该功能，请单击 BMC 配置下的**网络**。所做的任何更改将立即生效，无需重新启动 XClarity Controller。

配置安全密钥管理（SKM）

按本主题中的信息创建和管理安全密钥。

此功能使用集中式密钥管理服务器提供用于解锁存储硬件的密钥，从而访问存储在 ThinkSystem 服务器 SED 上的数据。密钥管理服务器包括 SKLM - IBM SED 密钥管理服务器和 KMIP - Thales/Gemalto SED 密钥管理服务器（KeySecure 和 CipherTrust）。

XClarity Controller 需要利用网络从密钥管理服务器检索密钥，因此 XClarity Controller 必须能够访问密钥管理服务器。XClarity Controller 在密钥管理服务器与发出请求的 ThinkSystem 服务器之间提供通信通道。XClarity Controller 固件尝试与每个已配置的密钥管理服务器连接，并在成功建立连接时停止尝试。

如果满足以下条件，XClarity Controller 即与密钥管理服务器建立通信：

- XClarity Controller 中配置了一个或多个密钥管理服务器主机名/IP 地址。

- **XClarity Controller** 中安装了用于与密钥管理服务器进行通信的两个证书（客户端证书和服务器证书）。

注：为设备配置了至少两个具有相同协议的密钥管理服务器（主要密钥管理服务器和辅助密钥管理服务器）。如果主密钥管理服务器未响应来自 **XClarity Controller** 的连接尝试，则用其他密钥管理服务器发起连接尝试，直到成功建立连接为止。

必须在 **XClarity Controller** 与密钥管理服务器之间建立传输层安全性（**TLS**）连接。**XClarity Controller** 认证密钥管理服务器的方法是对比密钥管理服务器提交的服务器证书与以前导入到 **XClarity Controller** 的信任存储区中的密钥管理服务器证书。密钥管理服务器将认证与其进行通信的每个 **XClarity Controller**，并核准该 **XClarity Controller** 访问密钥管理服务器。实现此认证的方法是对比 **XClarity Controller** 提交的客户端证书与密钥管理服务器上存储的可信证书列表。

至少将连接到一个密钥管理服务器，并将设备组视为可选。需要导入密钥管理服务器证书，同时需要指定客户端证书。默认情况下，使用 **HTTPS** 证书。如果要更换它，可生成新证书。

注：要连接 **KMIP** 服务器（**KeySecure** 和 **CipherTrust**），必须生成证书签名请求（**CSR**），且其公用名必须与 **KMIP** 服务器中定义的用户名匹配；然后，为 **CSR** 导入已由证书颁发机构（**CA**）签名且受 **KMIP** 服务器信任的证书。

配置密钥管理服务器

按本主题中的信息创建密钥管理服务器的主机名或 **IP** 地址以及关联的端口信息。

密钥管理服务器配置部分包含以下字段：

主机名或 IP 地址
在此字段中输入密钥管理服务器的主机名（如果启用并配置了 **DNS**）或 **IP** 地址。最多可添加四个服务器。

端口
在此字段中输入密钥管理服务器的端口号。如果将此字段留空，则使用默认值 **5696**。有效的端口号值为 **1** 至 **65535**。

配置设备组

按本主题中的信息配置 **SKLM** 服务器中使用的设备组。

在 **SKLM** 服务器中，用户可按设备组管理多个服务器上的自加密硬盘（**SED**）密钥。还必须在 **SKLM** 服务器上创建同名的设备组。

“设备组”部分包含以下字段：

设备组
通过设备组，用户可按组管理多个服务器上的 **SED** 密钥。还必须在 **SKLM** 服务器上创建同名的设备组。此字段的默认值为 **IBM_SYSTEM_X_SED**。

建立证书管理

本主题介绍客户端和服务器证书管理。

客户端和服务器证书用于认证 **SKLM** 服务器与位于 **ThinkSystem** 服务器中的 **XClarity Controller** 之间的通信。本节中讨论客户端和服务器证书管理。

客户端证书管理

本主题介绍客户端证书管理。

客户端证书分类如下：

- **XClarity Controller** 自分配证书。
- 从 **XClarity Controller** 证书签名请求（**CSR**）生成并由第三方 **CA**（在外部）签署的证书。

与 **SKLM** 服务器进行通信需要客户端证书。客户端证书包含 **CA** 和 **XClarity Controller** 的数字签名。

注：

- 固件更新后证书保持不变。
- 如果未创建客户端证书以供与 **SKLM** 服务器进行通信，则将使用 **XClarity Controller HTTPS** 服务器证书。
- **CA** 的功能是验证 **XClarity Controller** 的身份。

要创建客户端证书，请单击加号图标（ ），然后选择以下某项：

- 生成新密钥和自签名证书
- 生成新密钥和证书签名请求（**CSR**）

生成新密钥和自签名证书操作项生成新加密密钥和自签名证书。在“生成新密钥和自签名证书”窗口中，输入或选择必填字段以及任何适用于您的配置的可选字段（请参阅下表）中的信息。单击**确定**以生成您的加密密钥和证书。生成自签名证书时将显示进度窗口。成功安装证书时将显示确认窗口。

注：新加密密钥和证书替换任何现有的密钥和证书。

表 3. 生成新密钥和自签名证书

带标题的两列表格，其中记载用于生成新密钥和自签名证书操作的必填和可选字段。最后一行跨两列。

字段	描述
国家/地区[1]	从列表项中，选择 **BMC** 实体所在的国家/地区。
州或省[1]	输入 **BMC** 实体所在的州或省。
城市或地区[1]	输入 **BMC** 实体所在的城市或地区。
组织机构名称[1]	输入拥有 **BMC** 的公司或组织名称。
BMC 主机名[1]	输入在 **Web** 地址栏中显示的 **BMC** 主机名。
联系人	输入负责 **BMC** 的联系人的姓名。
电子邮件地址	输入负责 **BMC** 的联系人的电子邮件地址。
组织单位	输入公司内拥有 **BMC** 的单位。
姓氏	输入负责 **BMC** 的人员的姓氏。此字段最多可包含 **60** 个字符。
名字	输入负责 **BMC** 的人员的名字。此字段最多可包含 **60** 个字符。

表 3. 生成新密钥和自签名证书 （续）

字段	描述
首字母	输入负责 BMC 的人员的姓名首字母缩写。此字段最多可包含 20 个字符。
DN 限定符	输入 BMC 的可分辨名称限定符。此字段最多可包含 60 个字符。
1. 这是必填字段。	

生成客户端证书后，可通过选择**下载证书**操作项，将证书下载并存储到 XClarity Controller 上。

生成新密钥和证书签名请求（CSR）操作项生成新加密密钥和 CSR。在“生成新密钥和证书签名请求”窗口中，输入或选择必填字段以及任何适用于您的配置的可选字段（请参阅下表）中的信息。单击**确定**以生成新加密密钥和 CSR。

生成 CSR 时将显示进度窗口，而成功完成时将显示确认窗口。生成 CSR 后，必须将 CSR 发送到 CA 进行数字签名。选择**下载证书签名请求**（CSR）操作项，然后单击**确定**以将 CSR 保存到您的服务器。然后，可将 CSR 提交到您的 CA 进行签名。

表 4. 生成新密钥和证书签名请求

带标题的两列表格，其中记载用于生成新密钥和证书签名请求操作的必填和可选字段。最后一行跨两列。

字段	描述
国家/地区[1]	从列表项中，选择 BMC 实体所在的国家/地区。
州或省[1]	输入 BMC 实体所在的州或省。
城市或地区[1]	输入 BMC 实体所在的城市或地区。
组织机构名称[1]	输入拥有 BMC 的公司或组织名称。
BMC 主机名[1]	输入在 Web 地址栏中显示的 BMC 主机名。
联系人	输入负责 BMC 的联系人的姓名。
电子邮件地址	输入负责 BMC 的联系人的电子邮件地址。
组织单位	输入公司内拥有 BMC 的单位。
姓氏	输入负责 BMC 的人员的姓氏。此字段最多可包含 60 个字符。
名字	输入负责 BMC 的人员的名字。此字段最多可包含 60 个字符。
首字母	输入负责 BMC 的人员的姓名首字母缩写。此字段最多可包含 20 个字符。
DN 限定符	输入 BMC 的可分辨名称限定符。此字段最多可包含 60 个字符。
提问密码	输入 CSR 的密码。此字段最多可包含 30 个字符。
非结构化名称	输入其他信息，如分配给 BMC 的非结构化名称。此字段最多可包含 60 个字符。
1. 这是必填字段。	

CA 使用用户的证书处理工具（如 *OpenSSL* 或 *Certutil* 命令行工具），以数字方式签署 CSR。使用用户的证书处理工具签署的所有客户端证书具有相同的*基本*证书。还必须将此*基本*证书导入到 SKLM 服务器，以使 SKLM 服务器接受用户以数字方式签署的所有服务器。

在 CA 签署证书后，必须将它导入到 BMC 中。选择**导入签名证书**操作项，选择要作为客户端证书上传的文件，然后单击**确定**。上传 CA 签署的证书时将显示进度窗口。如果上传过程成功，则显示“上传证书”窗口。如果上传过程不成功，则显示“上传证书出错”窗口。

注：

- 要提高安全性，请使用 CA 以数字方式签署的证书。
- 导入到 XClarity Controller 中的证书必须对应于以前生成的 CSR。

将 CA 签署的证书导入到 BMC 中后，选择**下载证书**操作项。选择此操作项时，将从 XClarity Controller 下载 CA 签署的证书以存储在您的系统上。

服务器证书管理

本主题介绍服务器证书管理。

在 SKLM 服务器中生成服务器证书，并且必须将服务器证书导入到 XClarity Controller 中，然后才能使用安全硬盘访问功能。要将认证 SKLM 服务器的证书导入到 BMC，请从“硬盘访问”页面的“服务器证书状态”部分中单击**导入证书**。将文件传输到 XClarity Controller 上的存储时将显示进度指示器。

成功地将服务器证书传输到 XClarity Controller 后，“服务器证书状态”区域将显示以下内容：
A server certificate is installed。

如果要删除可信证书，请单击对应的**删除**按钮。

扩展审核日志

按本主题中的信息控制扩展审核日志。

利用此功能，可以决定是否将来自 LAN 和 KCS 通道的 IPMI set 命令（原始数据）的日志条目包含在审核日志中。

单击 XCC Web 上 BMC **配置**下的**安全性**，以启用/禁用扩展审核日志。

注：如果 IPMI set 命令来自 LAN 通道，则用户名和源 IP 地址将包含在日志消息中。会排除所有带有敏感安全性信息（例如密码）的 IPMI 命令。

加密设置

请参阅本主题中的信息了解不同的加密设置。

高安全模式

- 仅支持新式强密码。
- 符合 NIST。
- 符合 PFS（完美前向保密）。

兼容性模式

- 支持各种密码套件，以实现最大的兼容性。
- 不符合 **PFS** 和 **NIST**。

NIST 合规模式

- 支持各种密码套件，以实现最大的兼容性。
- 符合 **NIST**。
- 符合 **PFS**。

支持的 TLS 版本

- **TLS 1.0** 及更高版本
- **TLS 1.1** 及更高版本
- **TLS 1.2** 及更高版本
- **TLS 1.3**

TLS 加密设置用于限制 **BMC** 服务所支持的 **TLS** 密码套件。

请参考下表了解不同设置下所支持的 **TLS** 密码套件

安全模式	TLS 版本	TLS 密码套件
高安全模式	TLS 1.3 及更低版本	• TLS_AES_256_GCM_SHA384
高安全模式	TLS 1.2 及更低版本	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
NIST 合规模式	TLS 1.3 及更低版本	• TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256
NIST 合规模式	TLS 1.2 及更低版本	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256

安全模式	TLS 版本	TLS 密码套件
兼容性模式	TLS 1.3 及更低版本	• TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256
兼容性模式	TLS 1.2 及更低版本	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256
兼容性模式	TLS 1.1 及更低版本	• TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256

配置 Call Home

按本主题中的信息配置 **Call Home**。

可以创建一个服务转发器，该服务转发器使用 **Call Home** 功能将任何受管设备的服务数据自动发送到 **Lenovo** 支持中心。

Lenovo 致力于提高安全性。启用后，**Call Home** 会自动与 **Lenovo** 联系以开立服务凭单，并在受管设备报告硬件故障时发送从该设备收集的服务数据。当用户将服务数据手动上传到 **Lenovo** 支持中心时，数据会使用 **TLS 1.2** 或更高版本通过 **HTTPS** 自动发送到 **Lenovo** 支持中心，但其中绝对不会包含业务数据。只有授权服务人员才能访问 **Lenovo** 支持中心中的服务数据。

首次进入 Call Home 页面

首次进入 **Call Home** 页面时将显示警告窗口，单击“查看条款和条件”以继续。

注意：您必须接受 **Lenovo 隐私声明**才能将数据传输到 **Lenovo** 支持中心。只需在首次进入该页面时执行一次此操作。

注：可以在页面顶部找到“查看条款和条件”和 **Lenovo 隐私声明**，可以随时进行查看。

配置 Call Home

有九个必填字段：

- 国家/地区
- 联系人姓名
- 电话
- 电子邮件
- 邮政编码
- 公司名称
- 地址
- 城市
- 省/自治区/直辖市

注意：必须填写所有必填字段，否则您将无法应用更改并启用**向 Lenovo 服务报告**。

凭单状态

每个凭单可以具有以下五种状态之一：

- **待处理**：服务信息正在发送或等待响应。
- **处理中**：服务信息已成功发送，当前正在处理该问题。
- **失败**：服务信息未成功发送。
- **已关闭**：该问题已处理并关闭。
- **已取消**：该问题已处理并取消。

测试 Call Home

您可以通过单击“测试 **Call Home**”来测试 **Call Home** 功能，页面顶部将显示一条消息，以指示操作是否成功。您将能够在下面的事件日志中查看测试结果。

- **操作 - 取消**： 当某个凭单的状态为“处理中”时，可以单击“操作”列中的“撤消”图标以取消该凭单。
- **操作 - 注释**：单击“操作”列中的“注释”图标时，系统将提示您为相应的事件留下注释。

  注：必须同时填写标题和消息正文才能成功发送。此功能**仅向服务器发送信息**，而不会保存和显示信息。如果再次单击“注释”，则会显示新的“注释”窗口，提示您留下另一条消息。

注意：要成功地执行 **Call Home**，请确保 **DNS** 设置有效，并且已连接到 **Call Home** 所需的 **Internet** 地址。如果 **XClarity Controller** 通过 **HTTP** 代理访问 **Internet**，请确保将代理服务器配置为使用基本认证并将其设置为非终止代理。

HTTP 代理

HTTP 代理充当两个中介角色，分别是 **HTTP** 客户端和 **HTTP** 服务器，以实现安全性、可管理性和高速缓存功能。**HTTP** 代理将 **HTTP** 客户端请求从 **Web** 浏览器路由到 **Internet**，同时支持 **Internet** 数据高速缓存。

- **代理服务器地址**：需要使用此字段来启用 **HTTP** 代理。它最多只能接受 **63** 个字符，允许用户指定 **IP** 地址或主机名。主机名仅包含字母数字、连字符（-）和下划线（_）字符。
- **端口**：需要使用此字段来指定 **HTTP** 代理的端口。此字段仅允许输入范围为 **1-65535** 的数字。

- **测试代理**：要启用此功能，需要填写正确的代理位置和代理端口以测试当前的 **HTTP** 代理功能是否可用。
- **用户名**：如果选中了**需要认证**选项，则需要填写用户名，它表示代理凭证。此字段允许的最大长度为 **30** 个字符，空格无效。
- **密码**：此字段是可选的，如果选中了“需要认证”选项，则会显示此字段。此字段允许的最大长度为 **15** 个字符，空格无效。

备份和恢复 BMC 配置

本主题中的信息介绍如何恢复或修改 **BMC** 配置。

在 **BMC 配置**下选择**备份与恢复**以执行以下操作：

- 查看管理控制器配置摘要
- 备份或恢复管理控制器配置
- 查看备份或恢复状态
- 将管理控制器配置恢复为其出厂默认设置
- 访问管理控制器初始设置向导

备份 BMC 配置

本主题中的信息介绍如何备份 **BMC** 配置。

在 **BMC 配置**下选择**备份与恢复**。最顶部是**备份 BMC 配置**部分。

如果之前做过备份，您将在**上一次备份**字段中看到详细信息。

要备份当前 **BMC** 配置，请按如下所示的步骤操作：

1. 指定 **BMC** 备份文件的密码。
2. 选择要加密整个文件还是仅加密敏感数据。
3. 单击**开始备份**开始备份过程。在此过程中，不允许执行任何恢复/重置操作。
4. 该过程完毕后，将显示一个按钮让您下载并保存该文件。

注：当用户设置新的 **XClarity Controller** 用户/密码并执行配置备份时，也会包括默认帐户/密码（USERID/PASSWORD）。随后从该备份删除默认帐户/密码将导致系统显示一条消息，通知用户在恢复 **XClarity Controller** 帐户/密码时出错。用户可忽略此消息。

恢复 BMC 配置

本主题中的信息介绍如何恢复 **BMC** 配置。

在 **BMC 配置**下选择**备份与恢复**。**从配置文件恢复 BMC** 部分位于**备份 BMC 配置**下方。

要将 **BMC** 恢复到以前保存的配置，请按如下所示的步骤操作：

1. 浏览以选择备份文件，出现提示时输入密码。
2. 单击**查看内容**以查看详细信息，从而验证该文件。
3. 验证内容后，单击**开始恢复**。

将 BMC 重置为出厂默认值

本主题中的信息介绍如何将 **BMC** 重置为出厂默认设置。

在 **BMC 配置**下选择**备份与恢复**。**将 BMC 重置为出厂默认值**部分位于**从配置文件恢复 BMC** 下方。

要将 **BMC** 重置为出厂默认值，请按照如下所示的步骤操作：

1. 单击**将 BMC 重置为出厂默认值**。

   注：

   - 只有具有主管用户权限级别的人员才能执行此操作。
   - 以太网连接将暂时断开。重置操作完成后，必须再次登录 **XClarity Controller Web** 界面。
   - 一旦单击**开始将 BMC 重置为出厂默认值**，所有以前的配置更改都将丢失。恢复 **BMC** 配置时如果要启用 **LDAP**，需先导入一个可信安全证书。
   - 该过程完成后，**XClarity Controller** 将重新启动。如果是本地服务器，那么 **TCP/IP** 连接将丢失，您可能需要重新配置网络接口才能恢复连接。
   - 将 **BMC** 重置为出厂默认设置不会影响 **UEFI** 设置。

重新启动 XClarity Controller

本主题中的信息介绍如何重新启动 **XClarity Controller**。

有关如何重新启动 **XClarity Controller** 的详细信息，请参阅第 **60** 页 “电源操作”

第 4 章　监控服务器状态

请参阅本主题中的信息了解如何查看并监控所访问的服务器的信息。

登录 **XClarity Controller** 后，将显示一个系统状态页面。从此页面可查看服务器硬件状态、事件和审核日志、系统状态、维护历史记录和警报接收方。

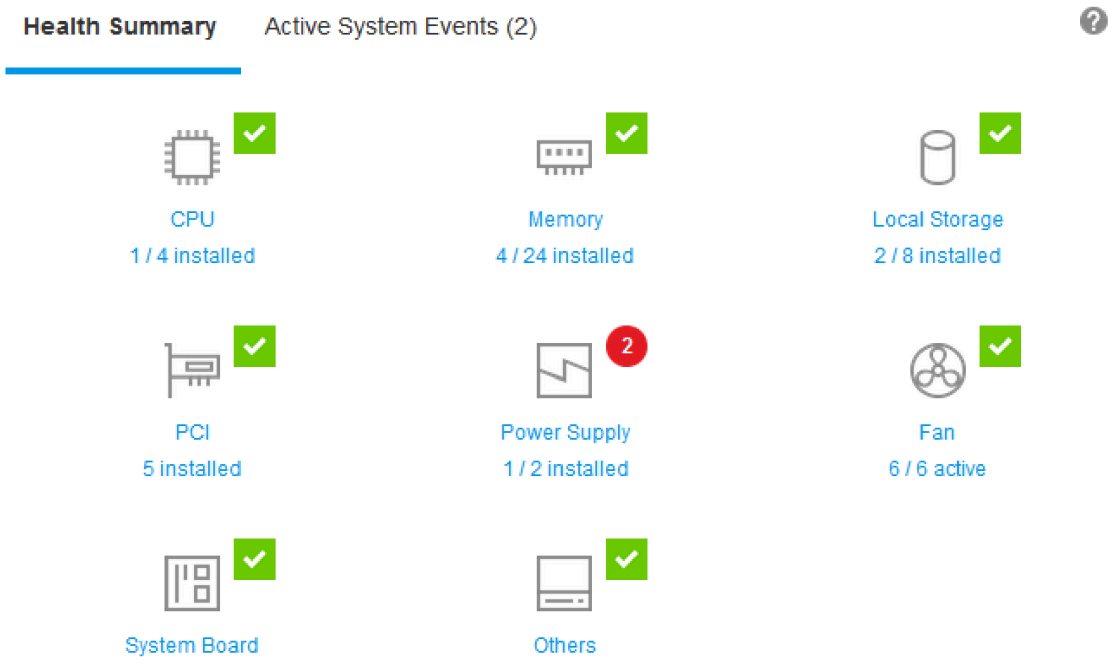
查看运行状况摘要/活动系统事件

按本主题中的信息了解如何查看运行状况摘要/活动系统事件。

访问 **XClarity Controller** 主页时，默认情况下显示**运行状况摘要**。其中采用图形表示形式，显示已安装的硬件组件的数量及其各自的运行状况状态。受监控的硬件组件包括以下各项：

- 处理器（**CPU**）
- 内存
- 本地存储
- **PCI** 适配器
- 电源模块
- 风扇
- 主板
- 其他

注：在配备易插拔背板的系统上，**本地存储**可能会显示“不可用”状态图标。



如果其中任何一个硬件组件未正常运行，它将标有紧急或警告图标。红色圆形图标指示紧急状况，而黄色三角形图标指示警告状况。将鼠标图标悬停在紧急或警告标志上时，最多将显示该组件当前活动的三个事件。

要查看其他事件，请单击**活动系统事件**选项卡。随后将显示一个窗口，其中显示系统中的当前活动事件。单击**查看所有事件日志**查看整个事件历史记录。

如果硬件组件标有绿色复选标记，则表示它在正常运行，并且没有活动的事件。

硬件组件下方的文本说明所安装的组件数。如果单击该文本，则将您定向到**清单**页面。

查看系统信息

本主题说明如何获取通用服务器信息的摘要。

主页左侧的**系统信息和设置**窗格提供常规服务器信息的摘要，其中包括以下各项：

- 机器名称、电源和操作系统状态
- 机器类型/型号
- 序列号

- 系统名称
- 正面 USB 所有权
- BMC 许可证
- BMC IP 地址
- BMC 主机名
- UEFI 版本
- BMC 版本
- LXPM 版本
- 位置

服务器可以是下表中所列的任意一种系统状态。

表 5. 系统状态描述

以下表格（包含两列）描述了服务器的系统状态。

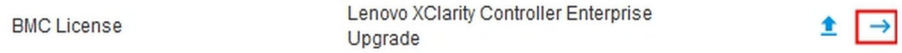
状态	描述
系统电源关闭/状态未知	服务器电源已关闭。
系统开启/正在启动 UEFI	服务器电源已打开，但是 UEFI 未运行。
系统正在 UEFI 中运行	服务器电源已打开，且 UEFI 正在运行。
系统已在 UEFI 中停止	服务器电源已打开；UEFI 检测到问题并已停止运行。
正在引导操作系统或所在的操作系统不受支持	服务器可能由于以下原因之一而处于此状态： • 操作系统装入程序已启动，但操作系统未运行 • BMC Ethernet over USB 接口已禁用。 • 操作系统未加载支持 Ethernet over USB 接口的驱动程序。
操作系统已引导	服务器操作系统正在运行。
暂挂到 RAM	已将服务器置于待机或睡眠状态。
系统正在运行内存测试	服务器电源已打开并且正在运行内存诊断工具。
系统处于设置状态	服务器已打开电源，且系统已引导至 UEFI F1 Setup 菜单或 LXPM 菜单。
系统正在以 LXPM 维护模式运行	服务器已打开电源，且系统已引导至 LXPM 维护模式，在该模式下用户无法浏览 LXPM 菜单。

如果要更改系统名称，请单击铅笔图标。输入要使用的系统名称，然后单击绿色复选标记。

如果要更改正面 USB 所有权，请单击铅笔图标，然后从下拉菜单中选择**正面 USB 所有权**模式。然后，单击绿色复选标记。

如果服务器的许可证不是 XClarity Controller Enterprise 许可证，则您可以购买许可证升级以启用增强功能。要在获取升级许可证后进行安装，请单击向上箭头图标。

要添加、删除或导出许可证，请单击向右箭头图标。



要更改 **BMC IP** 地址、**BMC** 主机名、**UEFI** 版本、**BMC** 版本和位置项的相关设置，请单击向右箭头。

- 对于 **IP** 地址和主机名，系统将导航到**网络**下的**以太网配置**部分。
- 对于 **UEFI** 和 **BMC** 版本等项，系统将导航到**固件更新**页面。
- 对于位置项，系统将导航到**服务器配置**页面上的**服务器属性**部分。

查看系统利用率

通过单击左侧窗格中的**利用率**，可查看提供的常规服务器利用率信息摘要。

系统利用率是根据处理器、内存和 **I/O** 子系统的实时利用率计算得出的复合度量值。利用率数据全部来自 **ME**（节点管理器）侧，包括以下几项：

- **CPU 利用率**
  - 处于 **C** 状态下的总时间
  - 测得时间为每秒已使用的 **C0** 状态时间占最大 **C0** 状态时间的百分比。
- **内存利用率**
  - 所有内存通道的总读取/写入量。
  - 测得带宽为每秒已使用的内存带宽占最大可用内存带宽的百分比。
- **I/O 利用率**
  - **PCIe*** 总线中根端口的总读取/写入量。
  - 测得带宽为每秒已使用的 **I/O** 带宽占最大可用 **I/O** 带宽的百分比。

查看事件日志

事件日志中列出所有硬件和管理事件的历史记录。

在**事件**中选择**事件日志**以显示**事件日志**页面。该日志中的所有事件均使用 **XClarity Controller** 日期和时间设置加入时间戳。如果在**警报接收方**页面上进行了相应配置，某些事件发生时还会生成警报。您可以对事件日志中的事件进行排序和筛选。

以下内容说明在**事件日志**页面中可以执行的操作。

- **定制表**：选择此操作项以选择希望在表中显示的信息类型。多个事件具有相同的时间戳时，可显示序号以帮助确定事件的顺序。

  注：某些序号为内部 **BMC** 进程所用，因此按序号对事件进行排序时，如果出现不连贯的序号是正常现象。
- **清除日志**：选择此操作项以删除事件日志。
- **刷新**：选择此操作项以显示自页面上次刷新后发生的所有事件日志条目。
- **类型**：选择要显示的事件类型。事件类型包括以下几种：

  
  显示日志中的错误条目

  
  显示日志中的警告条目

  
  显示日志中的参考条目

  单击每个图标可关闭或打开要显示的错误类型。连续单击图标可在显示事件和不显示事件之间切换。图标周围的蓝色框指示要显示的事件类型。
- **源类型筛选条件**：从下拉菜单中选择一项以只显示希望显示的事件日志条目类型。
- **时间筛选条件**：选择此操作项以指定时间间隔来查看此期间发生的事件。
- **搜索**：要搜索特定类型的事件或关键字，请单击放大镜图标，然后在**搜索**框中输入要搜索的字。请注意，输入区分大小写。

注：事件日志记录的最大数量为 **1024**。事件日志已满时，新的日志条目将自动覆盖最旧的日志条目。

查看审核日志

审核日志提供用户操作的历史记录，如登录到 **XClarity Controller**、创建新用户和更改用户密码等。

可使用审核日志跟踪和记录认证、更改和系统操作。

事件日志和审核日志支持类似的维护和查看操作。要查看可在“审核日志”页面上执行的显示和筛选操作的描述，请参阅第 52 页 “查看事件日志”。

注：

- 在服务器操作系统上运行 **Lenovo** 工具后，审核日志可能包含您不认识的用户名（例如用户”**20luN4SB**“）执行的操作的记录。部分工具在服务器操作系统上运行时可能会创建一个临时用户帐户以访问 **XClarity Controller**。该帐户使用随机用户名和密码进行创建，并仅用于在内部 **Ethernet over USB** 接口上访问 **XClarity Controller**。该帐户仅可用于访问 **XClarity**

Controller CIM-XML 和 **SFTP** 接口。创建和删除该临时帐户以及工具通过这些凭证执行的任何操作均将记录在审核日志中。

- 审核日志记录的最大数量为 **1024**。审核日志已满时，新的日志条目将自动覆盖最旧的日志条目。

查看维护历史记录

维护历史记录页面包含固件更新、配置和硬件更换历史记录的有关信息。

可筛选维护历史记录的内容以显示特定类型的事件或特定时间段的历史记录。

注：维护历史记录的最大数量为 **250**。维护历史记录日志已满时，新的日志条目将自动覆盖最旧的日志条目。

配置警报接收方

按本主题中的信息添加与修改电子邮件、**Syslog** 通知或 **SNMP** 陷阱接收方。

以下内容介绍在**警报接收方**选项卡中可执行的操作。

可在**电子邮件/Syslog** 接收方部分执行以下操作项。

- **创建**：选择此操作项以创建其他新电子邮件接收方和 **Syslog** 接收方。最多可配置 **12** 个电子邮件和 **Syslog** 接收方。
  - **创建电子邮件接收方**：选择此操作项以创建电子邮件接收方。
    - 输入接收方的姓名和电子邮件地址。
    - 选择启用或禁用事件通知。如果选择禁用，该帐户将保持配置状态，但不会发送电子邮件。
    - 选择通知接收方的事件类型。如果单击“紧急”、“注意”或“系统”类别标签旁边的下拉菜单，可选择或取消选择该类别中特定组件的通知。
    - 可选择是否将事件日志的内容包含在电子邮件警报中。
    - 可通过索引指定具体分配到哪个接收方。
    - 您可以在此处配置接收事件转发的电子邮件服务器，或通过单击此部分顶部的 **SMTP** 服务器操作进行配置。有关配置详细信息，请参阅下方的 **SMTP** 服务器。
  - **创建 Syslog 接收方**：选择此操作项以创建 **Syslog** 接收方。
    - 输入 **Syslog** 服务器的 **IP** 地址或主机名。
    - 选择启用或禁用事件通知。如果选择禁用，该帐户将保持配置状态，但不会发送电子邮件。
    - 可通过索引指定具体分配到哪个接收方。
    - 选择要发送至 **Syslog** 服务器的事件类型。如果单击“紧急”、“注意”或“系统”类别标签旁边的下拉菜单，可选择或取消选择该类别中特定组件的通知。
- **SMTP 服务器**：选择此操作项以配置 **SMTP** 电子邮件服务器的相关设置。仅可配置一个电子邮件服务器。向所有配置的电子邮件接收方发送警报时均将使用同一电子邮件配置。如果目标邮件服务器支持，**BMC** 会自动从安全连接切换到加密连接，以便使用 **STARTTLS** 命令统一通过端口 **587** 进行邮件传输。
  - 输入电子邮件服务器的主机名/**IP** 地址和网络端口号。
  - 如果电子邮件服务器需要认证，请选择**需要认证**复选框，并输入用户名和密码。选择电子邮件服务器要求的认证类型，可以是质询-响应方法（**CRAM-MD5**）或简单凭证（**登录**）。

  - 如果反向路径值不是预期值，某些网络可能会阻止发出的电子邮件。默认情况下，**XClarity Controller** 将使用 **alertmgr@domain**，其中 **domain** 是在 **XClarity Controller Web** 页面的 **DDNS** 部分中指定的域名。可使用自己的发件人信息替换默认发件人信息。
  - 您可以测试与电子邮件服务器的连接，以确保正确配置电子邮件设置。**XClarity Controller** 将显示一条消息，指示连接是否成功。
- **重试和延迟**：选择此操作项以配置重试和延迟选项的相关设置。
  - 重试限制指定 **XClarity Controller** 在首次尝试失败的情况下重新尝试发送警报的次数。
  - 条目之间的延迟指定 **XClarity Controller** 向两个接收方发送警报之间等待的时间。
  - 尝试之间的延迟指定 **XClarity Controller** 在一次尝试失败后到重新尝试发送警报之间等待的时间。
- **协议**：选择此操作项以配置连接协议的相关设置。
  - 可以在 **TCP 协议**和 **UDP 协议**之间进行选择，请注意，此设置将适用于所有 **Syslog** 接收方。
- 如果已创建电子邮件或 **Syslog** 接收方，它们将在本部分中列出。
  - 要编辑电子邮件或 **Syslog** 接收方的设置，请单击操作标题下方要配置的接收方旁边的铅笔图标。
  - 要删除电子邮件或 **Syslog** 接收方，请单击垃圾桶图标。
  - 要向电子邮件或 **Syslog** 接收方发送测试警报，请单击纸飞机图标。

SNMPv3 用户部分中可执行以下操作。

- **创建**：选择此操作项以创建 **SNMPv3** 陷阱接收方。
  - 选择与 **SNMPv3** 陷阱关联的用户帐户。该用户帐户必须为十二个本地用户帐户之一。
  - 指定将接收 **SNMPv3** 陷阱的 **SNMPv3** 管理器的主机名或 **IP** 地址。
  - **XClarity Controller** 使用 **HMAC-SHA** 散列算法向 **SNMPv3** 管理器进行认证。这是唯一受支持的算法。
  - 隐私密码与隐私协议配合使用以对 **SNMP** 数据进行加密。
  - **SNMPv3 全局设置**适用于所有 **SNMPv3** 陷阱接收方。创建 **SNMPv3** 陷阱接收方时即可对此进行配置，或单击 **SNMPv3** 用户部分顶部的 **SNMPv3** 设置操作来进行配置。
    - 选择启用或禁用 **SNMPv3** 陷阱。如果禁用，设置将保持配置状态，但不会发送 **SNMPv3** 陷阱。
    - 必须在服务器属性 **Web** 页面上填写和配置 **BMC** 联系人和位置信息。请参阅第 **78** 页 “设置位置和联系人”，了解更多信息。
    - 选择触发向 **SNMPv3** 管理器发送陷阱的事件类型。如果单击“紧急”、“注意”或“系统”类别标签旁边的下拉菜单，可选择或取消选择该类别中特定组件的通知。

  注：可以使用加密来保护 **SNMP** 客户端和代理之间的数据传输。**隐私协议**支持的方法为 **CBC-DES** 和 **AES**。
- 如果已创建 **SNMPv3** 陷阱接收方，它们将在本部分中列出。
  - 要编辑 **SNMPv3** 接收方的设置，请单击操作标题下方要配置的接收方旁边的铅笔图标。
  - 要删除 **SNMPv3** 接收方，请单击垃圾桶图标。

捕获上次操作系统故障屏幕数据

按本主题中的信息捕获并查看操作系统故障屏幕。

操作系统看守程序发生超时时，将自动捕获操作系统屏幕。如果发生导致操作系统停止运行的事件，将触发操作系统看守程序功能，并捕获屏幕内容。**XClarity Controller** 只能存储一个截屏。操作系统看守程序发生超时时，新的截屏将覆盖以前的截屏。必须启用操作系统看守程序功能才能捕获操作系统故障屏幕。要设置操作系统看守程序时间，请参阅第 **78** 页 “设置服务器超时”获取更多信息。操作系统故障截屏功能仅对 **XClarity Controller Advanced** 或 **Enterprise** 功能级别可用。有关服务器中所安装 **XClarity Controller** 功能级别的信息，请参阅服务器文档。

单击 **XClarity Controller** 主页**远程控制台**部分中的**最近一次故障截屏**操作，可查看操作系统看守程序发生超时时捕获的操作系统显示器图像。也可通过在主页**快捷操作**部分中单击**服务**，然后单击**最近一次故障截屏**来查看该截屏。如果系统因未发生操作系统看守程序超时而未捕获操作系统屏幕，则将显示一条消息，指示尚未创建故障屏幕。

第 5 章　配置服务器

请参阅本章中的信息了解服务器配置可用的选项。

配置服务器时可使用以下选项：

- 适配器
- 引导选项
- 电源策略
- 服务器属性

查看适配器信息和配置设置

按本主题中的信息查看有关服务器中安装的适配器的信息。

在**服务器配置**下单击**适配器**以查看有关服务器中安装的适配器的信息。

注：

- 如果适配器不支持状态监控，则它对于监控或配置不可见。有关所有已安装的 **PCI** 适配器的清单信息，可参阅**清单**页面。

配置系统引导模式和顺序

要配置系统引导模式和顺序，请参阅本主题中的信息。

在**服务器配置**下选择**引导选项**后可配置系统引导模式和顺序。

注：不允许使用未经认证的带内方法来更改与安全性相关的系统设置。例如，不得使用操作系统或 **UEFI shell** 通过未经认证的带内 **API** 来配置安全引导。这包括在带内运行并使用 **IPMI** 获取临时凭证的 **OneCLI**，或任何用于配置安全引导、**TPM**、**UEFI** 设置密码相关设置的工具和 **API**。所有与安全性相关的设置都必须要求具有足够特权的适当认证。

对于系统引导模式，有以下两个选项可用：

UEFI 引导
选择此选项可配置支持 **Unified Extensible Firmware Interface**（**UEFI**）的服务器。如果引导启用了 **UEFI** 的操作系统，此选项可以通过禁用 **legacy** 选项 **ROM** 缩短引导时间。

Legacy 引导
如果要将服务器配置为启动需要 **legacy** (**BIOS**) 固件的操作系统，请选择此选项。如果要引导未启用 **UEFI** 的操作系统，请选择此选项。

要配置系统引导顺序，请从**可用设备**列表中选择一个设备，然后单击向右箭头将该设备添加到引导顺序。要从引导顺序中删除设备，请从引导顺序列表中选择一个设备，然后单击向左箭头将该设备移回到可用设备列表。要更改引导顺序，请选择一个设备并单击向上或向下箭头以上下移动设备的优先级。

更改引导顺序时，必须先选择一个重新启动选项，然后再应用更改。以下选项可用：

- **立即重新启动服务器**：保存引导顺序更改并立即重新启动服务器而不等待操作系统关闭。
- **正常重新启动服务器**：保存引导顺序更改并关闭操作系统，然后再重新启动服务器。
- **稍后手动重新启动**：保存引导顺序更改，但更改将于下一次重新启动服务器时生效。

配置一次性引导

要暂时忽略配置的引导而一次性引导至指定设备，请参阅本主题中的信息。

在**服务器配置**下单击**引导选项**，并选择从下拉菜单中选择一个设备进行配置，下一次服务器重新启动时系统将一次性引导至该设备。有以下选项可供使用：

PXE 网络
将服务器设置为尝试预启动执行环境网络引导。

主要可移动介质
从默认 **USB** 设备引导服务器。

默认 CD/DVD
从默认 **CD/DVD** 光驱引导服务器。

F1 系统设置
将服务器引导至 **Lenovo XClarity Provisioning Manager**。

诊断分区
将服务器引导至 **Lenovo XClarity Provisioning Manager** 的诊断程序部分。

默认硬盘
从默认硬盘引导服务器。

主要远程介质
服务器从装载的虚拟介质引导。

无一次性引导
使用配置的引导顺序。不对配置的引导顺序进行一次性引导覆写。

更改一次性引导设备将执行的引导类型时，您也可以将引导指定为 **legacy** 引导或 **UEFI** 引导。如果希望引导是 **legacy BIOS** 引导，请单击**首选 Legacy 引导**复选框。如果希望是 **UEFI** 引导，则取消勾选此框。选择一次性更改引导顺序时，必须先选择一个重新启动选项，然后再应用更改。

- **立即重新启动服务器**：保存引导顺序更改并立即重新启动服务器而不等待操作系统关闭。
- **正常重新启动服务器**：保存引导顺序更改并关闭操作系统，然后再重新启动服务器。
- **稍后手动重新启动**：保存引导顺序更改，但更改将于下一次重新启动服务器时生效。

管理服务器电源

要查看电源管理信息和执行电源管理功能，请参阅本主题中的信息。

选择**服务器配置**下的**电源策略**选项可查看电源管理信息并执行电源管理功能。

注：包含刀片服务器或高密度服务器节点的机箱中，机箱散热和电源由机箱管理控制器控制，而不由 **XClarity Controller** 控制。

配置电源冗余

要配置电源冗余，请参阅本主题中的信息。

注：目前，用户无法更改 AMD 系统内的电源策略。

当安装两个电源模块单元时，冗余模式设置为“冗余（N+N）”。使用这种两个电源模块单元的配置时，如果其中一个电源模块单元发生故障、交流电源丢失或已被卸下，XCC 事件日志中将报告冗余丢失事件。

如果装运后仅安装了 1 个电源模块单元，冗余模式将自动设置为“非冗余模式”。

电源冗余部分包含如下字段：

- **冗余（N+N）**：此模式下，服务器在发生丢失一个电源模块的事件时将保持运行。
  - **零输出模式**：在冗余配置下启用后，某些 PSU 将在轻负载条件下自动进入待机状态。通过这种方式，剩余的 PSU 可以提供整个电源负载，从而提高效率。
- **冗余（N+1）**：此模式下，在安装了四个电源模块的情况下，服务器在发生丢失一个电源模块的事件时将保持运行。
- **非冗余模式**：此模式下，服务器无法保证在丢失一个电源模块的情况下保持运行。如果某个电源模块尝试保持运行失败，则服务器将调速。

完成配置更改后单击**应用**。

配置功率上限策略

要配置功率上限策略，请参阅本主题中的信息。

注：AMD 处理器服务器不支持用户配置电源上限策略功能。

您可以选择启用或禁用功率上限功能。如果启用了功率上限，则可选择服务器使用的功率上限。如果禁用了功率上限，则服务器使用的最大功率由电源冗余策略决定。要更改该设置，请先单击**重置**。选择首选的设置，然后单击**应用**。

功率上限可通过交流电源功耗测量或直流电源功耗测量启用。从下拉菜单中选择用于确定功率上限的测量的类型。在交流和直流之间切换时，滑块上的数字也将相应地发生变化。

可通过两种方法更改功率上限值：

- **方法 1**： 将滑块标记移至所需的瓦数来设置服务器总功率上限。
- **方法 2**：在输入框中输入值。滑块标记将自动将移至相应的位置。

完成配置更改后单击**应用**。

注：XClarity Controller 位于包含刀片或高密度服务器节点的机箱中时，**电源策略**选项不可用。该电源策略由机箱管理控制器控制，而不是由 **XClarity Controller** 控制。

配置电源恢复策略

要配置服务器断电之后恢复供电时服务器的反应，请参阅本主题中的信息。

配置电源恢复策略时，可使用以下三个选项：

始终关闭
即使恢复供电，服务器仍将保持电源关闭状态。

恢复
发生电源故障时如果服务器已打开电源，则恢复供电后服务器将自动打开电源。否则，恢复供电后服务器电源仍将保持关闭状态。

始终打开
恢复供电后，服务器将自动打开电源。

完成配置更改后单击**应用**。

注：电源策略选项在包含刀片或高密度服务器节点的机箱中不可用。该电源恢复策略由机箱管理控制器控制，而不是由 **XClarity Controller** 控制。

电源操作

请参阅本主题中的信息以了解可对服务器执行的电源操作。

在 **XClarity Controller** 主页中的**快捷操作**部分单击**电源操作**。

下表包含可在服务器上执行的电源操作和重新启动操作的描述。

表 6. 电源操作和描述

包含服务器电源操作和重新启动操作描述的两列表格。

电源操作	**描述**
打开服务器电源	选择此操作项打开服务器电源并引导操作系统。
正常关闭服务器电源	选择此操作项关闭操作系统并关闭服务器电源。
立即关闭服务器电源	选择此操作项在不关闭操作系统的情况下关闭服务器电源。
正常重新启动服务器	选择此操作项关闭操作系统并关闭再打开服务器电源。
立即重新启动服务器	选择此操作项在不关闭操作系统的情况下立即关闭并再打开服务器电源。
将服务器引导至系统设置	选择此项打开服务器电源或重新启动服务器，然后自动引导至系统设置，而无需在引导期间按 **F1**。
触发不可屏蔽中断（**NMI**）	选择此操作项以在“挂起的”系统上强制执行不可屏蔽中断（**NMI**）。通过选择此操作项，平台操作系统可以执行内存转储以用于调试系统挂起情况。**F1** 系统设置菜单中针对 **NMI** 设置的自动重新启动功能决定 **XClarity Controller** 在 **NMI** 后是否会重新启动服务器。
安排电源操作顺序	选择此操作项以为服务器安排每天和每周电源操作和重新启动操作。

表 6. 电源操作和描述 （续）

电源操作	描述
重新启动管理控制器	选择此操作项以重新启动 **XClarity Controller**
关闭再打开服务器交流电源	选择此操作以关闭再打开服务器电源。
注：如果操作系统在尝试关机时处于屏幕保护模式或锁定模式中，则 **XClarity Controller** 可能无法发起正常关机。**XClarity Controller** 将在关闭电源延迟时间间隔结束后执行硬重置或关机，而操作系统可能仍在运行。	

使用 IPMI 命令管理和监控功耗

按本主题中的信息使用 **IPMI** 命令管理和监控功耗。

本主题介绍如何使用智能平台管理接口（**IPMI**）命令通过 **Intel Intelligent Power Node Manager** 和 **Data Center Manageability Interface**（**DCMI**）为服务器提供电源和散热监控以及基于策略的电源管理功能。

对于使用 **Intel Node Manager SPS 3.0** 的服务器，**XClarity Controller** 用户可使用 **Intel Management Engine**（**ME**）提供的 **IPMI** 电源管理命令控制 **Node Manager** 的功能及监控服务器功耗。此外，也可使用 **DCMI** 电源管理命令完成服务器电源管理。本主题提供了 **Node Manager** 和 **DCMI** 电源管理命令的示例。

使用 Node Manager 命令管理服务器电源

按本主题中的信息使用 **Node Manager** 管理服务器电源。

Intel Node Manager 固件没有外部接口；因此，**Node Manager** 命令必须先由 **XClarity Controller** 接收，然后再发送到 **Intel Node Manager**。**XClarity Controller** 使用标准 **IPMI** 桥接充当 **IPMI** 命令的中继和传输设备。

注：使用 **Node Manager IPMI** 命令更改 **Node Manager** 策略可能会与 **XClarity Controller** 电源管理功能发生冲突。默认情况下已禁用 **Node Manager** 命令的桥接以防止发生任何冲突。

对于希望使用 **Node Manager** 而不是 **XClarity Controller** 来管理服务器电源的用户，有由（网络功能：***0x3A***）和（命令：***0xC7***）组成的 **OEM IPMI** 命令可供使用。

要启用本机 **Node Manager IPMI** 命令类型：`ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSWORD> raw 0x3a 0xc7 0x01`

要禁用本机 **Node Manager IPMI** 命令类型：`ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSWORD> raw 0x3a 0xc7 0x00`

以下信息是 **Node Manager** 电源管理命令的示例。

注：

- 通过指定 **IPMI** *通道* ***0*** 和 ***0x2c*** 目标地址，您可使用 **IPMITOOL** 将命令发送至 **Intel Node Manager** 进行处理。请求消息用于发起一个操作，请求方将收到返回的响应消息。
- 由于空间限制，命令显示为以下格式。

使用”获取全局系统电源统计信息“监控电源，（命令代码 0xC8）：请求：ipmitool -H *<$XClarity_Controller_IP>* -U *<USERID>* -P *<PASSWORD>* -b *0x00* -t *0x2c* raw *0x2E 0xC8 0x57 0x01 0x00 0x01 0x00 0x00* 响应：**57 01 00 38 00 04 00 41 00 39 00 ec 56 f7 53 5a 86 00 00 50**

使用”设置 Intel Node Manager 策略“设置功率上限，（命令代码 0xC1）请求：ipmitool -H *<$XClarity_Controller_IP>* -U *<USERID>* -P *<PASSWORD>* -b *0x00* -t *0x2c* raw *0x2e 0xC1 0x57 0x01 0x00 0x10 0x01 0xA0 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00 0x00 0x1e 0x00* 响应：**57 01 00**

使用“设置 Intel Node Manager 策略”进行节能，（命令代码 0xC1）：请求：ipmitool -H *<$XClarity_Controller_IP>* -U *<USERID>* -P *<PASSWORD>* -b *0x00* -t *0x2c* raw *0x2e 0xC1 0x57 0x01 0x00 0x10 0x01 0x00 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00 0x00 0x1e 0x00*

使用“获取 Intel Management Engine Device ID”获取 Device ID 功能：请求：ipmitool -H *<$XClarity_Controller_IP>* -U *<USERID>* -P *<PASSWORD>* -b *0x00* -t *0x2c* raw *0x06 0x01* 响应：**50 01 03 05 02 21 57 01 00 05 0b 03 40 20 01**

有关其他 Intel Node Manager 命令，请参阅 **https://businessportal.intel.com** 上最新版本的 ***Intel Intelligent Power Node Manager External Interface Specification Using IPMI***。

使用 DCMI 命令管理服务器电源

按本主题中的信息使用 DCMI 命令管理服务器电源。

DCMI 提供可通过标准管理软件接口使用的监控和控制功能。此外，也可使用 DCMI 命令完成服务器电源管理功能。

以下信息是常用 DCMI 电源管理功能和命令的示例。请求消息用于发起一个操作，请求方将收到返回的响应消息。

注：由于空间限制，命令显示为以下格式。

获取功率读数：请求：ipmitool -H *<$XClarity_Controller_IP>* -U *<USERID>* -P *<PASSWORD>* raw *0x2c 0x02 0xdc 0x01 0x00 0x00* 响应：dc 39 00 38 00 3b 00 39 00 e3 6f 0a 39 e8 03 00 00 40

设置功率限制：请求：ipmitool -H *<$XClarity_Controller_IP>* -U *<USERID>* -P *PASSWORD* raw *0x2c 0x04 0xdc 0x00 0x00 0x00 0x00 0xA0 0x00 0xe8 0x03 0x00 0x00 0x00 0x00 0xe8 0x03* 响应：dc

获取功率上限：请求：ipmitool -H *<$XClarity_Controller_IP>* -U *<USERID>* -P *<PASSWORD>* raw *0x2c 0x03 0xdc 0x00 0x00* 响应：dc 00 00 00 a0 00 e8 03 00 00 00 00 01 00

激活功率限制：请求：ipmitool -H *<$XClarity_Controller_IP>* -U *<USERID>* -P *<PASSWORD>* raw *0x2c 0x05 0xdc 0x01 0x00 0x00* 响应：dc

停用功率限制：请求：ipmitool -H *<$XClarity_Controller_IP>* -U *<USERID>* -P *<PASSWORD>* raw *0x2c 0x05 0xdc 0x00 0x00 0x00* 响应：dc

注：某些服务器上可能不支持对**设置功率限制**命令的异常操作。例如，可能不支持*硬关闭系统电源和向 **SEL** 发送日志事件*参数。

有关 DCMI 规范支持的命令的完整列表，请参阅 https://www.intel.com/content/dam/www/public/us/en/documents/technical-specifications/dcmi-v1-5-rev-spec.pdf 上最新版本的 ***Data Center Manageability Interface Specification***。

远程控制台功能

请参阅本主题中的信息了解如何远程查看服务器控制台并与之进行交互。

您可以在 XClarity Controller Web 界面中使用远程控制台功能查看服务器控制台并与之交互。您可以在服务器上将磁盘映像（ISO 或 IMG 文件）作为虚拟硬盘分配。远程控制台功能对 XClarity Controller Advanced 和 XClarity Controller Enterprise 功能可用且仅可通过 Web 界面使用。您必须使用具有主管访问权限或远程控制台访问权限的用户 ID 登录到 XClarity Controller，才能使用任何远程控制功能。有关从 XClarity Controller Standard 升级到 XClarity Controller Advanced 或 XClarity Controller Enterprise 的详细信息，请参阅第 6 页 “升级 XClarity Controller”。

使用远程控制台功能执行以下操作：

- 远程查看视频，图形分辨率高达 1280 x 1024（72 或 75 Hz），而与服务器状态无关。
- 使用远程客户端的键盘和鼠标远程访问服务器。
- 将位于本地系统或远程系统上的 ISO 和 IMG 文件作为可供服务器使用的虚拟硬盘装载。
- 将 IMG 或 ISO 映像上传到 XClarity Controller 内存并将其作为虚拟硬盘装载到服务器。可上传最多两个文件（总大小不超过 50 MB）到 XClarity Controller 内存。

注：

- 以多用户模式启动远程控制台功能时（具有 XClarity Controller Enterprise 功能集的 XClarity Controller 最多支持六个并发会话），一次仅限一个会话执行远程磁盘功能。
- 远程控制台仅可显示主板上视频控制器生成的视频。如果安装了独立的视频控制器适配器并代替了系统的视频控制器，那么 XClarity Controller 远程控制台无法显示来自所添加适配器的视频内容。
- 如果网络中有防火墙，则必须打开一个网络端口以支持远程控制台功能。要查看或更改远程控制台功能使用的网络端口号，请参阅第 33 页 “服务启用与端口分配”。
- 远程控制台功能使用 HTML5 在 Web 页面上显示服务器视频。要使用此功能，浏览器必须支持使用 HTML5 元素显示视频内容。
- 如果正在使用自签名证书和 IPv6 地址通过 Internet Explorer 浏览器访问 BMC，则远程控制台会话可能因证书错误而无法启动。要避免此问题，可将自签名证书添加到 Internet Explorer 信任的根证书颁发机构：
  - 在 BMC **配置**下选择**安全性**，然后下载自签名证书。
  - 将证书文件的扩展名更改为 *.crt，然后双击该 Web 证书文件。
  - 清除 IE11 浏览器高速缓存。
  - 单击**安装证书**以按照证书导入向导的步骤将证书安装到证书库。

启用远程控制台功能

本主题介绍远程控制台功能。

如前文所述，XClarity Controller 远程控制台功能仅在 XClarity Controller Advanced 和 XClarity Controller Enterprise 功能中可用。如果没有操作远程控制台的权限，您将看到一个锁图标。

购买并获得 **XClarity Controller Advanced** 升级激活密钥后，请根据第 87 页 “安装激活密钥”中的说明进行安装。

要使用远程控制台功能，请完成以下步骤：

1. 单击 **XClarity Controller** 主页或远程控制台 **Web** 页面“远程控制台”部分中带白色对角箭头的图像。
2. 选择以下模式之一：
   - 以单用户模式启动远程控制台
   - 以多用户模式启动远程控制台

   注：拥有 **XClarity Controller Enterprise** 功能集的 **XClarity Controller** 在多用户模式下最多支持六个同时视频会话。
3. 选择如果有人想使用远程控制台功能而该功能已处于单用户模式，或多用户模式下正在使用远程控制台的用户数量超过最大数量时，是否允许其向远程控制台用户请求发送断开请求。**无响应时间间隔**指定在断开请求未收到响应的情况下，**XClarity Controller** 自动断开该用户的连接之前等待的时间。
4. 选择是否允许记录最近三个服务器引导视频。
5. 选择是否允许记录最近三个服务器崩溃视频。
6. 选择是否允许包含硬件错误的操作系统故障截屏。
7. 单击**启动远程控制台**在另一个选项卡中打开远程控制台页面。如果所有可能的远程控制台会话均正在使用，将弹出一个对话框。用户可从该对话框中向启用了**允许他人请求断开我的远程会话连接**设置的远程控制台用户发送断开请求。用户可接受或拒绝该断开请求。如果用户未在**无响应时间间隔**设置指定的时间间隔内响应，**XClarity Controller** 将自动终止该用户会话。

远程电源控制

本主题介绍如何从远程控制台窗口发送服务器电源和重新启动命令。

您可以从远程控制台窗口发送服务器电源和重新启动命令而不返回到主 **Web** 页面。要通过远程控制台控制服务器电源，请单击**电源**，然后选择以下命令之一：

打开服务器电源
选择此操作项打开服务器电源并引导操作系统。

正常关闭服务器电源
选择此操作项关闭操作系统并关闭服务器电源。

立即关闭服务器电源
选择此操作项在不关闭操作系统的情况下关闭服务器电源。

正常重新启动服务器
选择此操作项关闭操作系统并关闭再打开服务器电源。

立即重新启动服务器
选择此操作项在不关闭操作系统的情况下立即关闭并再打开服务器电源。

将服务器引导至系统设置
选择此项打开服务器电源或重新启动服务器，然后自动引导至系统设置，而无需在引导期间按 **F1**。

远程控制台截屏

请参阅本主题中的信息了解如何使用远程控制台截屏功能。

远程控制台窗口中的截屏功能可捕获服务器的视频显示内容。要捕获并保存屏幕图像，请完成以下步骤：

步骤 1. 在远程控制台窗口中，单击**截屏**。

步骤 2. 在弹出的窗口中，单击**保存文件**，然后按**确定**。该文件将命名为 **rpviewer.png**，并保存到默认下载文件夹中。

注：截屏图像另存为 **PNG** 文件类型。

远程控制台键盘支持

键盘下的远程控制台窗口中提供以下选项：

- 单击**虚拟键盘**以启动虚拟键盘。如果正在使用没有物理键盘的平板设备，此功能将十分有用。以下选项可用于创建可发送到服务器的宏和组合键。您所使用的客户端系统上的操作系统可能会拦截某些键组合（如 **Ctrl+Alt+Del**），而不将其发送到服务器。其他键（如 **F1** 或 **Esc**）则可能会被正在使用的程序或浏览器拦截。宏提供一种机制可将用户可能无法发送的按键发送到服务器。
- 单击**服务器宏**以使用服务器定义的宏。某些服务器宏由 **XClarity Controller** 固件预定义。其他服务器定义的宏可使用 **Lenovo XClarity Essentials** 进行定义并可通过 **XClarity Controller** 下载。这些定义的宏适用于远程控制台功能的所有用户。
- 单击**配置**以添加或删除用户定义的宏。用户定义的宏仅适用于远程控制台的当前用户。用户定义的宏对其他远程控制台用户不可见。
  - 单击“添加宏”图标，然后按下所需的按键序列，然后单击**添加**来添加一个新的宏。
  - 要删除用户定义的宏，请从列表中选择宏，然后单击垃圾桶图标。
  - 要将用户定义的宏发送到服务器，请选择**用户定义的宏**选项，然后单击要发送的宏。

远程控制台鼠标支持

按以下信息了解远程鼠标控制的选项。

远程控制台窗口中提供若干鼠标控制选项，包括绝对鼠标控制、相对鼠标控制（无加速）和鼠标控制（**RHEL**，较旧版本的 **Linux**）。

绝对和相对鼠标控制

按以下信息访问用于控制鼠标的绝对和相对选项。

要访问用于控制鼠标的绝对和相对选项，请完成以下步骤：

步骤 1. 在远程控制台窗口中，单击**鼠标**。

步骤 2. 从下拉菜单中单击**鼠标设置**。

步骤 3. 选择以下**鼠标加速**模式之一：

绝对定位（Windows、Linux 较高版本和 Mac OS X）
客户端将相对于查看区域原点（左上方区域）的鼠标位置消息发送到服务器。

相对定位，无加速
客户机将鼠标位置以与先前鼠标位置的偏移量的形式进行发送。

相对定位（Linux 较低版本）
此模式应用加速因子以在部分 Linux 目标上更好地将鼠标对齐。加速设置已选中以最大化与旧 Linux 发行版的兼容性。

屏幕录像/回放

按照本主题中的信息来录制或回放远程呈现屏幕视频。

XClarity Controller Web 界面提供类似 DVR 的功能，以支持录制和回放远程呈现屏幕视频。此功能仅支持将视频录制到网络文件夹。目前支持 NFS 和 CIFS 协议。以下是使用录制和回放功能的步骤。

1. 在远程控制台 Web 页面上，单击**屏幕录制**打开设置窗口。
2. 在设置窗口中，可能需要指定以下信息。
   - 如果选择了“CIFS”装载类型，请指定**远程文件夹**、**用户名**和**密码**参数。CIFS 远程文件夹的格式为“//<**远程 IP 地址**>/<**文件夹名称**>”。例如：**//xxx.xxx.xxx.xxx/folder**。
   - 如果选择了“NFS”装载类型，请指定**远程文件夹**参数。NFS 远程文件夹的格式为“<**远程 IP 地址**>:/<**文件夹名称**>”。例如：**xxx.xxx.xxx.xxx:/folder**。
   - 如果需要，请指定视频文件名。如果已经提供了文件名，则将显示错误消息框。要覆盖现有文件名，请选择“覆盖文件名”。如果勾选了“自动”复选框，将自动生成视频文件名。
   - “最大文件大小”表示视频录制自动停止之前录制的最大视频文件大小。
   - “最大录制时长”表示录制自动停止之前视频文件的最大录制时长。
3. 单击**开始录制**开始录像。
4. 单击**停止录制**停止录像。随后将显示一个弹出窗口，提示“视频录制已完成”，并显示相关视频录制信息。
5. 将录制的视频从 NFS 或 CIFS 下载到本地文件夹。在 XClarity Controller 主页的“远程控制台预览”部分中，单击**录制的视频**并选择要回放的视频文件。

远程控制台屏幕模式

按本主题中的信息配置远程控制台屏幕模式。

要配置远程控制台屏幕模式，请单击**屏幕模式**。

将提供以下菜单选项：

全屏
此模式使视频显示填满客户端桌面。在此模式下按 Esc 键将退出全屏模式。由于远程控制台菜单在全屏模式下不可见，因此必须退出全屏模式才能使用远程控制台菜单提供的任何功能（如键盘宏）。

适应屏幕
这是远程控制台启动后的默认设置。此设置下，不带滚动条完全显示目标桌面。保留原纵横比。

扩展屏幕
启用缩放后，将调整视频图像使缩放后的完整图像填满控制台窗口。

原始屏幕
视频图像尺寸与服务器端尺寸相同。必要时将显示滚动条，以便查看窗口中无法容纳的视频图像区域。

颜色模式
调整远程控制台窗口的颜色深度。有两种颜色模式可选：

- 颜色：**7**、**9**、**12**、**15** 和 **23** 位
- 灰度：**16**、**32**、**64** 和 **128** 灰度级

注：通常情况下，如果与远程服务器的连接带宽有限并希望降低带宽需求时可调整颜色模式。

介质装载方法

请参阅本主题中的信息了解如何执行介质装载。

有三种机制可将 **ISO** 和 **IMG** 文件作为虚拟硬盘装载。

- 通过单击**介质**，可从远程控制台会话将虚拟硬盘添加到服务器。
- 直接从远程控制台 **Web** 页面操作，无需建立远程控制台会话。
- 独立工具

用户需要**远程控制台和远程磁盘访问权限**才能使用虚拟介质功能。

可从本地系统或远程服务器将文件作为虚拟介质装载，并可通过网络访问或使用 **RDOC** 功能将其上传到 **XClarity Controller** 内存。这些机制的说明如下。

- 本地介质是用于访问 **XClarity Controller** 的系统上的 **ISO** 或 **IMG** 文件。此机制只能通过远程控制台会话使用，而无法直接从远程控制台 **Web** 页面使用，且仅当拥有 **XClarity Controller Enterprise** 功能时才可用。要装载本地介质，请在**装载本地介质**部分中单击**激活**。最多可同时将四个文件装载到服务器。

  注：

  – 使用 **Google Chrome** 浏览器时，另有一个名为**装载文件/文件夹**的装载选项可用，通过它可直接拖放文件/文件夹。
  – 如果正在与 **XClarity Controller** 进行多个并发远程控制台会话，则只有其中一个会话可激活此功能。
- 远程系统上的文件也可作为虚拟介质装载。最多可同时将四个文件作为虚拟硬盘装载。**XClarity Controller** 支持以下文件共享协议：

  – **CIFS - 通用 Internet 文件系统**：
    – 输入在远程系统上定位该文件的 **URL**。
    – 如果要让该文件作为只读虚拟介质提供给服务器，则勾选该复选框。
    – 输入 **XClarity Controller** 用于访问远程系统上的文件的凭证。

      注：**XClarity Controller** 不支持用户名、密码或 **URL** 中包含空格。请确保 **CIFS** 服务器的登录凭证不包含带空格的用户名和密码，且 **URL** 中不含空格。

    – 装载选项为可选，且由 **CIFS** 协议定义。

  - 如果远程服务器属于某个集中处理安全性的服务器集群，请输入该远程服务器所属的域名。
- **NFS - 网络文件系统**：
  - 输入在远程系统上定位该文件的 URL。
  - 如果要让该文件作为只读虚拟介质提供给服务器，则勾选该复选框。
  - 装载选项为可选，且由 NFS 协议定义。支持 NFSv3 和 NFSv4。例如，要使用 NFSv3，需指定选项“nfsvers = 3”。如果 NFS 服务器使用 AUTH_SYS 安全方式来认证 NFS 操作，则需指定选项“sec=sys”。
- **HTTPFS – 基于 HTTP Fuse 的文件系统**：
  - 输入在远程系统上定位该文件的 URL。
  - 如果要让该文件作为只读虚拟介质提供给服务器，则勾选该复选框。

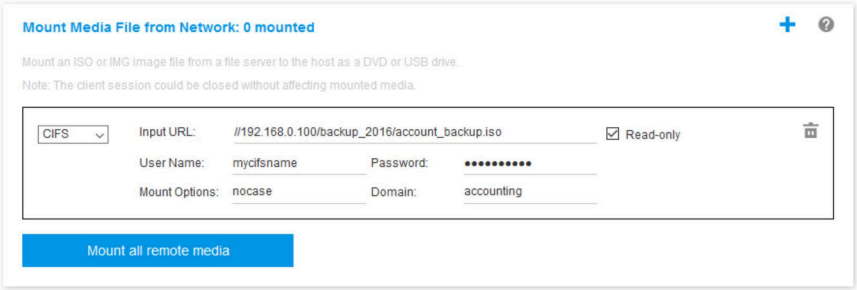
  注：装载 Microsoft IIS 生成的安全证书过程中可能发生错误。如果发生该情况，请参阅第 76 页 “介质装载错误问题”。

单击**挂载所有远程介质**将文件作为虚拟介质装载。要删除虚拟介质，请单击所装载介质右侧的垃圾桶图标。

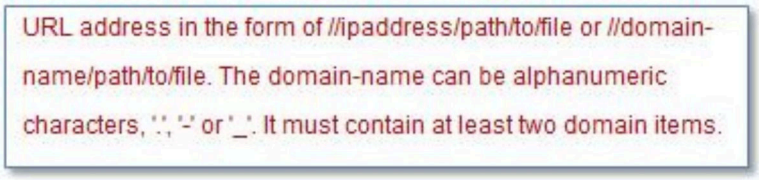
- 最多可向 XClarity Controller 内存上传两个文件，并使用 XClarity Controller RDOC 功能将其作为虚拟介质装载。两个文件的总大小不能超过 50 MB。这些文件在被删除前将一直保留在 XClarity Controller 内存中，即使远程控制台会话已结束。RDOC 功能在上传文件时支持以下机制：
  - **CIFS - 通用 Internet 文件系统**：有关详细信息，请参阅上文描述。

    示例：

    要将 IP 地址为 192.168.0.100 的 CIFS 服务器 backup_2016 目录中名称为 account_backup.iso 的 ISO 文件作为服务器上的只读虚拟硬盘进行装载，需填写下图所示的字段。本示例中，位于 192.168.0.100 的服务器是“accounting”域下服务器集合中的一个。域名可选。如果您的 CIFS 服务器不属于某个域，请将**域**字段留空。本示例中**装载选项**字段指定 CIFS 装载选项为“不区分大小写字母”，指明应忽略对 CIFS 服务器中文件名大写字母/小写字母的检查。**装载选项**字段可选。BMC 未使用用户在该字段输入的信息，并且在发出装载请求时，该信息会直接传递到 CIFS 服务器。请参阅 CIFS 服务器实施文档，来确定您的 CIFS 服务器支持哪些选项。



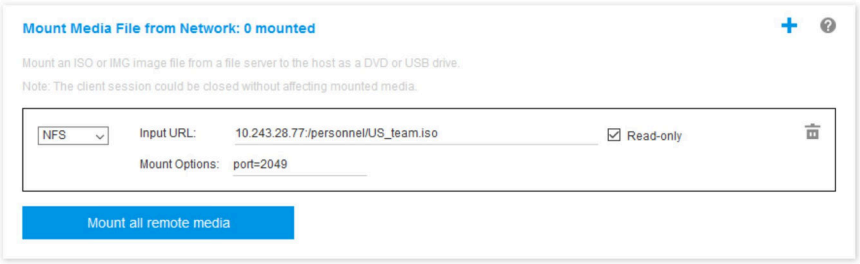
    BMC 会在指定 URL 时提供指导。如果所输入的 URL 无效，“装载”按钮将灰显，URL 字段下方会用红色文本显示 URL 的预期格式。



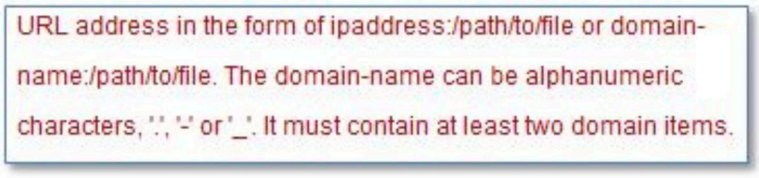
– **NFS - 网络文件系统**：有关详细信息，请参阅上文描述。

  示例：

  要将 IP 地址为 **10.243.28.77** 的 NFS 服务器“**personnel**”目录中名称为 **US_team.iso** 的 ISO 文件作为服务器上的只读虚拟硬盘进行安装，需填写如下图所示字段。**NFS**“端口=**2049**”装载选项指定网络端口 **2049** 应用于传输数据。**装载选项**字段可选。发出装载请求时，用户在该字段中输入的信息将传递到 NFS 服务器。请参阅 NFS 服务器实施文档，来确定您的 NFS 服务器支持哪些选项。



  BMC 会在指定 **URL** 时提供指导。如果所输入的 **URL** 无效，“装载”按钮将灰显，**URL** 字段下方会用红色文本显示 **URL** 的预期格式。

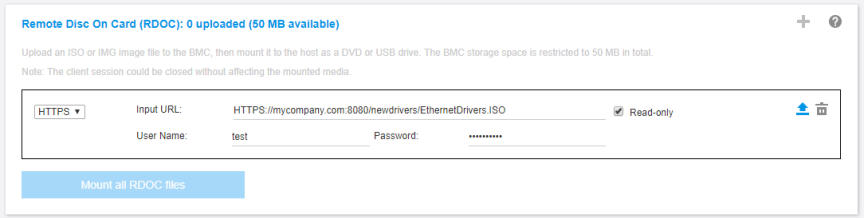


– **HTTPS – 安全超文本传输协议：**
  – 输入在远程系统上定位该文件的 **URL**。
  – 如果要让该文件作为只读虚拟介质提供给服务器，则勾选该复选框。
  – 输入 **XClarity Controller** 用于访问远程系统上的文件的凭证。

  注：

  – 装载 **Microsoft IIS** 生成的安全证书过程中可能发生错误。如果发生该情况，请参阅第 76 页 “介质装载错误问题”。
  – **XClarity Controller** 不支持用户名、密码或 **URL** 中包含空格。请确保 **CIFS** 服务器的登录凭证不包含带空格的用户名和密码，且 **URL** 中不含空格。**示例：**

    要使用网络端口 **8080** 将域名为“**mycompany.com**”的 **HTTPS** 服务器“**newdrivers**”目录中名称为 **EthernetDrivers.ISO** 的 **ISO** 文件作为服务器上的只读虚拟硬盘进行装载，需填写下图所示的字段。



BMC 会在指定 URL 时提供指导。如果所输入的 URL 无效，“装载”按钮将灰显，URL 字段下方会用红色文本显示 URL 的预期格式。

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

- **SFTP - SSH 文件传输协议**
  - 输入在远程系统上定位该文件的 URL。
  - 如果要让该文件作为只读虚拟介质提供给服务器，则勾选该复选框。
  - 输入 XClarity Controller 用于访问远程系统上的文件的凭证。

  注：

  - XClarity Controller 不支持用户名、密码或 URL 中包含空格。请确保 CIFS 服务器的登录凭证不包含带空格的用户名和密码，且 URL 中不含空格。
  - XClarity Controller 连接到 HTTPS 服务器时将弹出一个窗口，显示该 HTTPS 服务器所用的安全证书的信息。XClarity Controller 无法验证安全证书的真实性。
- **本地 - 通用 Internet 文件系统：**
  - 在系统中浏览到要装载的 ISO 或 IMG 文件。
  - 如果要让该文件作为只读虚拟介质提供给服务器，则勾选该复选框。

单击**挂载所有 RDOC 文件**将文件作为虚拟介质装载。要删除虚拟介质，请单击所装载介质右侧的垃圾桶图标。

独立工具

需要使用 XClarity Controller（.iso / .img）安装设备或映像的用户可使用 OneCLI 包的 rdmount 独立代码部分。具体而言，rdmount 将打开 XClarity Controller 的连接，并将设备或映像装载到该主机。

rdmount 采用以下语法：

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

装载 iso 文件的示例：

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

使用 Java 客户端的远程磁盘

本节介绍如何使用 Java 客户端装载本地介质。

您可以使用 Java 客户端向服务器分配一个计算机上的 CD 或 DVD 光驱、软盘驱动器或 USB 闪存驱动器，也可以指定您计算机上的一个磁盘映像供服务器使用。您可将该硬盘用于诸如以下的功能：重新启动（引导）服务器、更新代码、在服务器上安装新软件，以及在服务器上安装或更新操作系统。您可以访问远程磁盘。硬盘和磁盘映像在服务器上显示为 USB 驱动器。

注：远程控制台 Java 支持以下任一 Java 环境，并且只有在 HTML5 客户端未运行时才能打开。

1. Oracle Java Runtime Environment 1.8/Java SE 8 或更高版本。
2. OpenJDK 8。支持 HotSpot JVM 版本的 AdoptOpenJDK。

如果使用 AdoptOpenJDK，则必须在 OSX、Windows 和 Linux 下使用 https://openwebstart.com/。

创建映像文件

要从指定的源文件夹创建新的映像文件，请完成以下步骤：

1. 在虚拟介质 Java 客户端窗口中的**虚拟介质**选项卡下单击**创建映像**选项。随后将显示“从文件夹创建映像”窗口。
2. 单击与**源文件夹**字段关联的**浏览**按钮以选择特定源文件夹。
3. 单击与**新映像文件**字段关联的**浏览**按钮以选择要使用的映像文件。
4. 单击**创建映像**按钮。

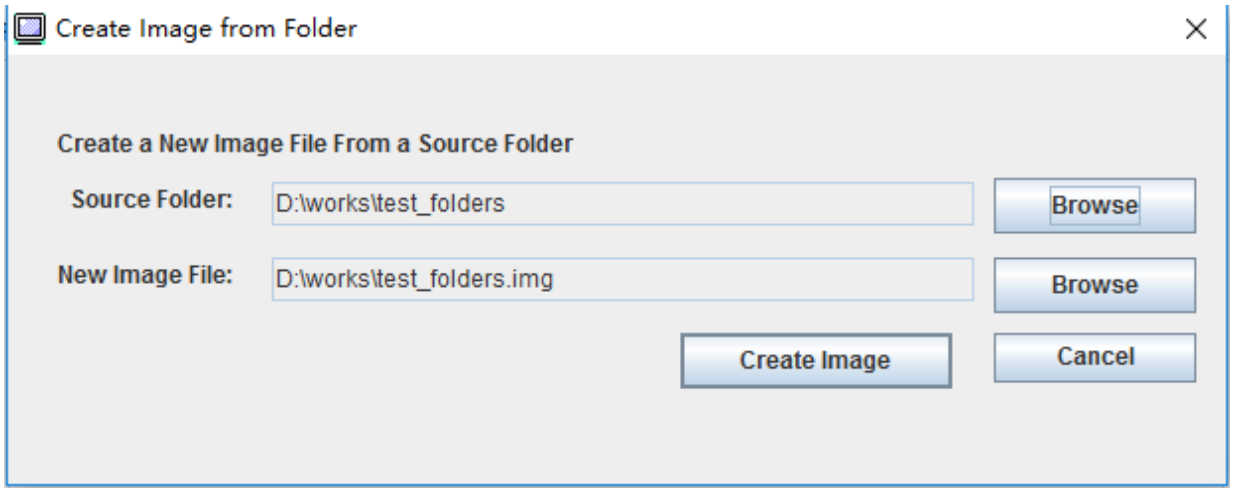


图 1. 创建映像文件

选择要装载的设备

要装载本地映像、文件夹和 CD/DVD/USB 驱动器，请完成以下步骤：

在虚拟介质 Java 客户端窗口中的**虚拟介质**选项卡下单击**选择要装载的设备**选项。随后将显示“选择要装载的设备”窗口。

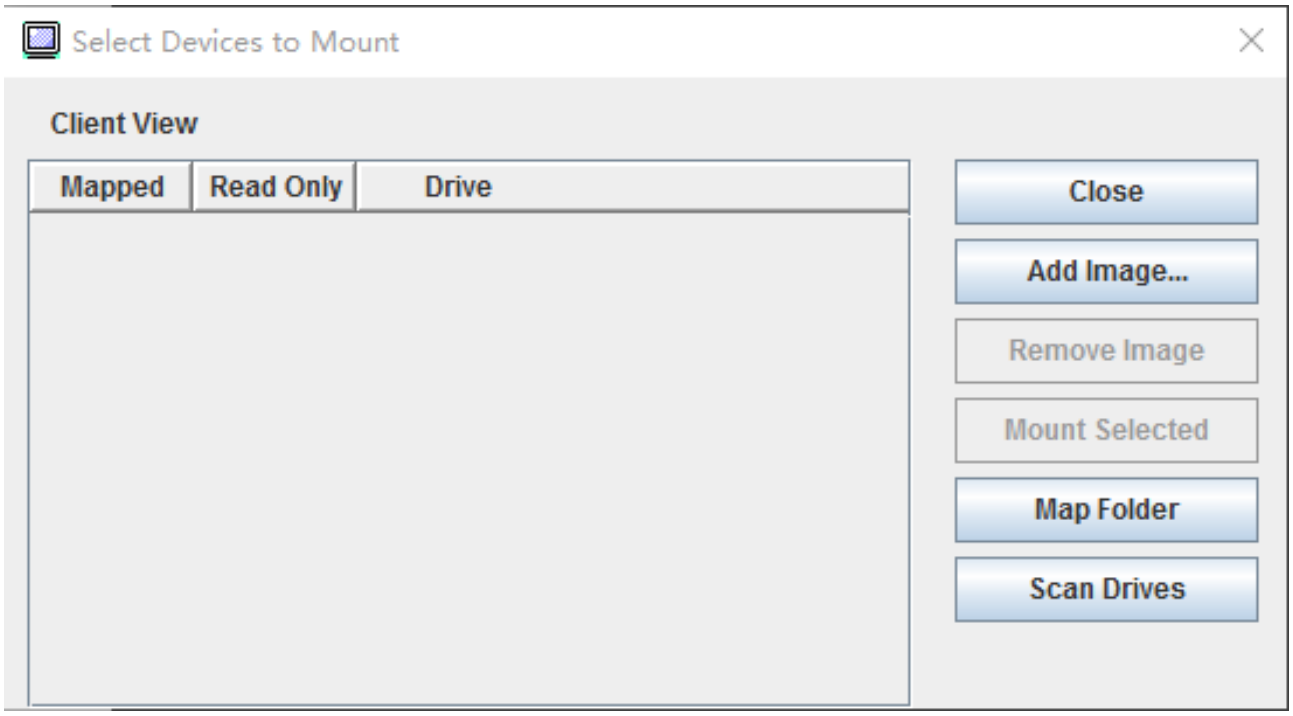


图 2. “选择要装载的设备”窗口

通过执行以下步骤装载本地映像、文件夹和 **CD/DVD/USB** 驱动器：

- **装载本地映像：**
  1. 单击**添加映像**按钮选择要装载的映像。
  2. 检查**已映射**选项。
  3. 检查**只读**选项以启用该功能（如果需要）。
  4. 单击**装载所选**按钮即可成功装载本地映像。

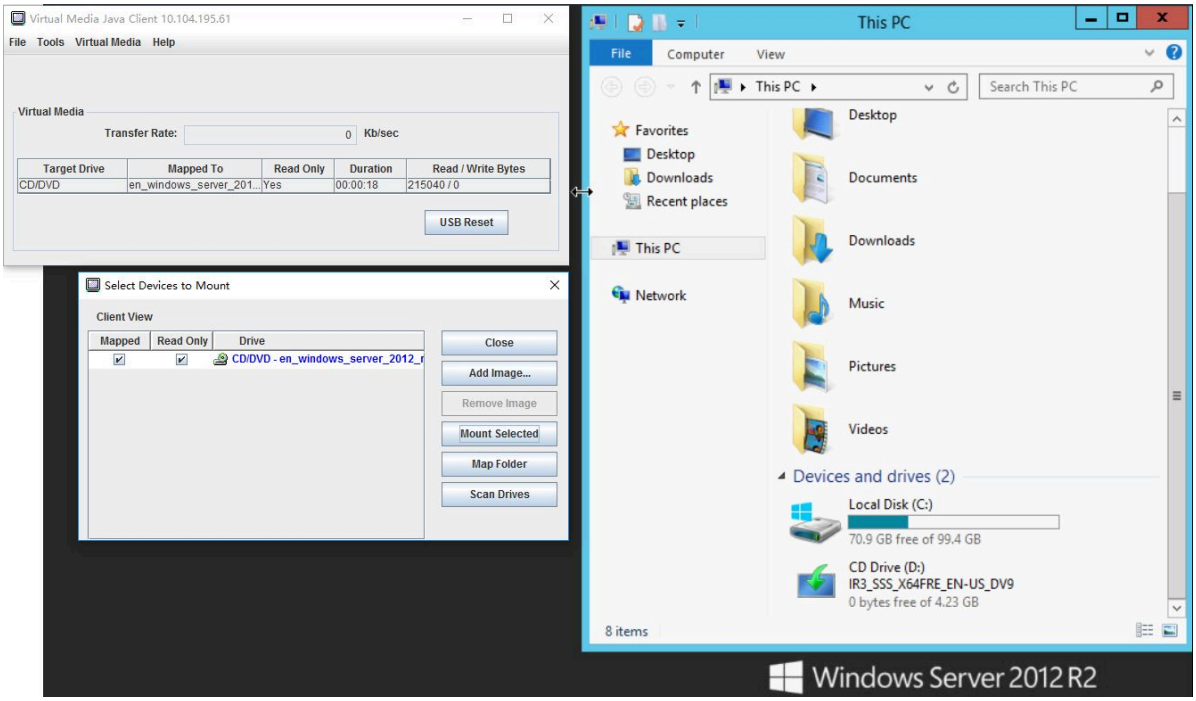


图 3. 装载本地映像

- **装载本地文件夹：**
  1. 单击**映射文件夹**按钮选择要装载的本地文件夹。
  2. 单击**装载所选**按钮即可成功装载本地文件夹。

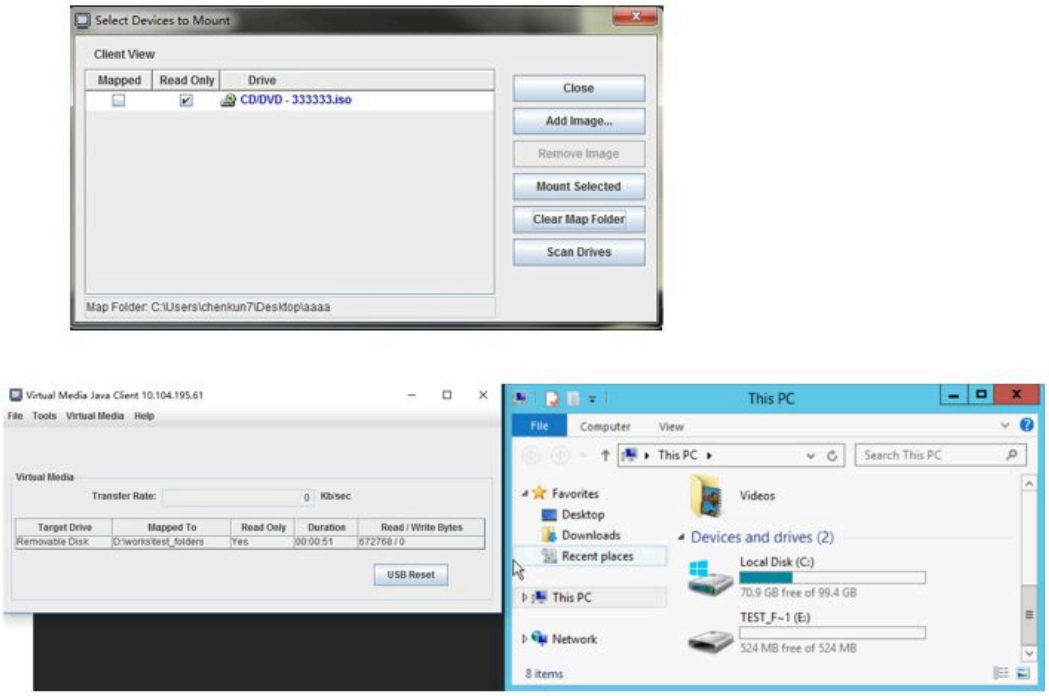


图 4. 装载本地文件夹

- **装载 CD/DVD 或 USB 驱动器:**
  1. 单击**扫描硬盘**按钮以检测插入的 CD/DVD 或 USB 硬盘。
  2. 检查**已映射**选项。
  3. 检查**只读**选项以启用该功能（如果需要）。
  4. 单击**装载所选**按钮即可成功装载本地映像。

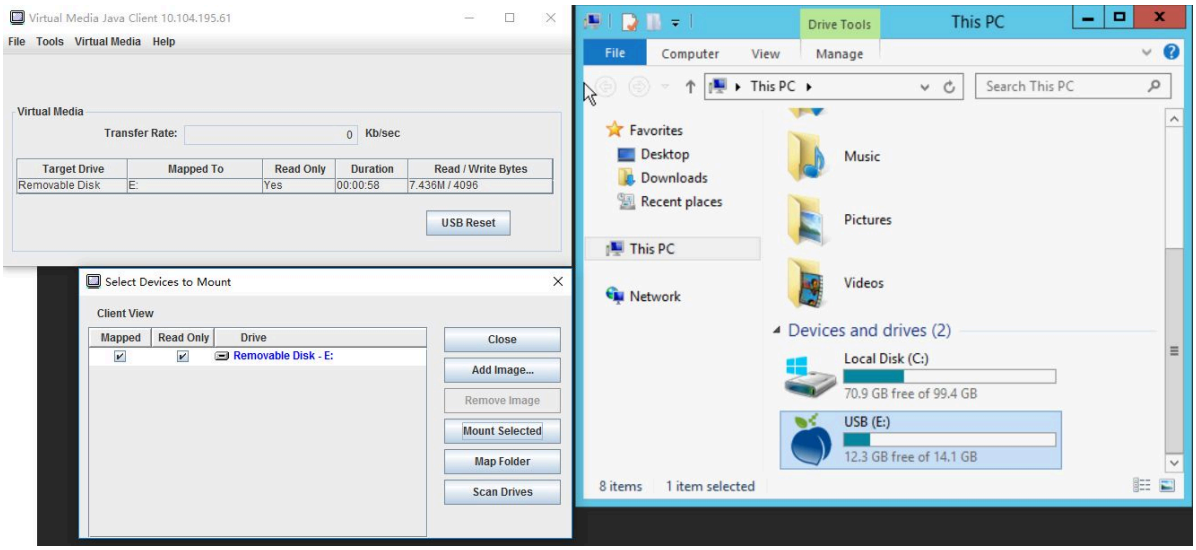


图 5. 装载 CD/DVD 或 USB 驱动器

“选择要装载的设备”窗口包含当前可装载的本地设备的列表。此窗口包含以下字段和按钮：

- **已映射**字段包含允许您选择要安装或映射的设备的复选框。
- **只读**字段包含一个复选框，该复选框允许您选择在主机服务器上*只读*的已映射或装载的设备。
- **硬盘**字段包含本地计算机上的设备路径。
- 单击**关闭**按钮关闭“选择要装载的设备”窗口。
- 单击**添加映像**按钮在本地文件系统中浏览要添加到设备列表中的软盘映像和 ISO 映像文件。
- 单击**删除映像**按钮删除已添加到设备列表中的映像。
- 单击**装载所选**按钮以装载或映射在**已映射**字段中勾选的要装载或映射的所有设备。

  注：文件夹将作为只读文件夹装载。
- 单击**扫描硬盘**按钮刷新本地设备列表。

选择要卸载的设备

要卸载主机服务器设备，请完成以下步骤：

1. 在虚拟介质 Java 客户端窗口中的**虚拟介质**选项卡下单击**卸载全部**选项。
2. 选择**卸载全部**选项后，将显示“卸载全部”确认窗口。如果接受，则服务器上的*所有*主机服务器设备将卸载。

   注：不能单个卸载硬盘。

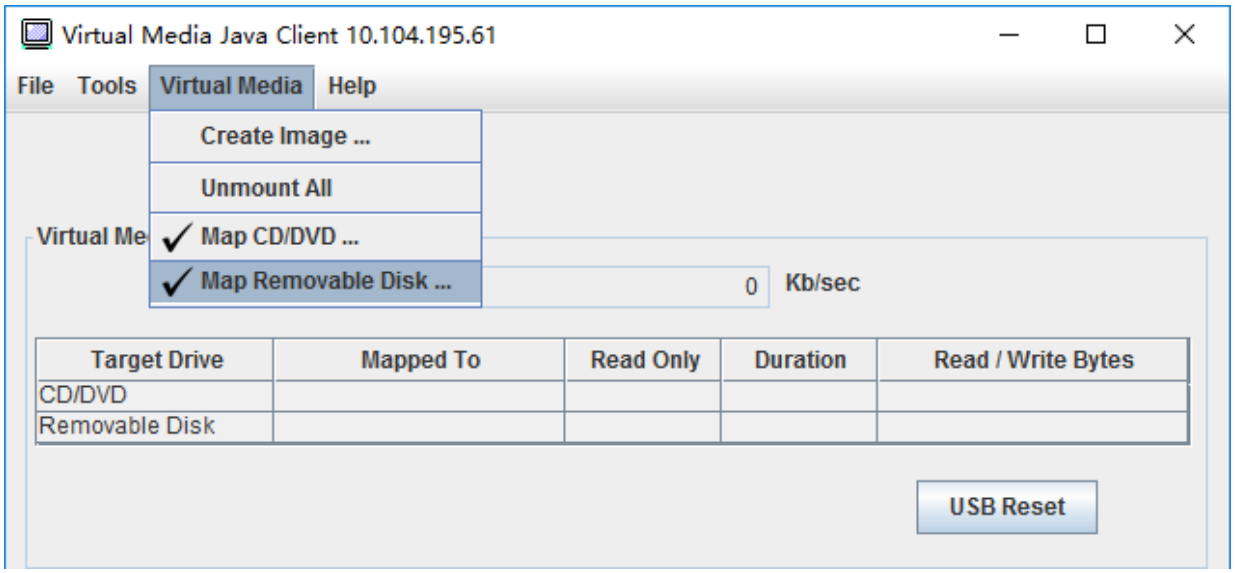


图 6. 卸载全部

介质装载错误问题

按本主题中的信息解决介质装载错误问题。

使用 **Microsoft IIS** 生成的安全证书时，装载过程中可能发生错误。如果发生该情况，请将该安全证书替换为由 **openssl** 新生成的安全证书。尤其需注意将新生成的 **pfx** 文件加载到 **Microsoft IIS** 服务器。

以下是显示如何在 **Linux** 操作系统中通过 **openssl** 生成新安全证书的示例。

```
$ openssl
OpenSSL>

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

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

Please enter the following 'extra' attributes
to be sent with your certificate request
```

```
A challenge password []:
An optional company name []:LNV

$ ls
server.csr  server.key

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

$ ls
server.crt  server.csr  server.key

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

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

退出远程控制台会话

本主题介绍如何结束远程控制台会话。

要退出远程控制台会话，请关闭远程控制台和虚拟介质会话窗口。

下载服务数据

按本主题中的信息收集服务器的服务信息。正常情况下此过程仅在服务人员请求您协助解决服务器问题时进行。

在 **XClarity Controller** 主页中，单击**快捷操作**部分中的**服务**，然后选择**下载服务数据**。单击**确定**以下载服务数据。

服务和支持数据收集过程需耗时数分钟以生成服务数据。该文件将保存到您的默认下载文件夹中。服务数据文件的命名约定遵循以下规约：<machine type and model>_<serial number>_xcc_<date>-<time>.tgz

例如：**7X2106Z01A_2345678_xcc_170511-175656.tgz**。

除了 **tgz** 格式，还可以使用 **tzz** 格式下载服务数据。**Tzz** 使用另一种压缩算法，并且可以使用“**lzop**”之类实用程序解压缩。

服务器属性

按本主题中的信息更改或查看相关的服务器属性。

设置位置和联系人

按本主题中的信息设置各种参数以帮助操作人员和支持人员识别系统。

在**服务器配置**下选择**服务器属性**以配置**位置和联系人**信息。

联系人
允许您指定系统发生问题的情况下应联系的人员的姓名和电话号码。

注：此字段与 **SNMPv3** 配置中的“联系人”字段相同，且必须启用 **SNMPv3**。

机架名称
通过指定其所在的机架以便您更容易地找到此服务器。

注：该字段为可选，但在 **Flex** 节点中不可配置。

房号
通过指定其所在的房间以便您更容易地找到此服务器。

构建
通过指定其所在的机房以便您更容易地找到此服务器。

最低 U
通过指定其在机架中的位置以便您更容易地找到此服务器。

注：该字段为可选，但在 **Flex** 节点中不可配置。

地址
允许您指定服务器所在位置的完整邮寄地址。

注：输入相关信息后，这些信息将在 **SNMPv3** 部分的**位置**字段和 **XClarity Controller** 主页中以单独一行显示。

设置服务器超时

按本主题中的信息设置服务器超时。

这些超时用于恢复已挂起服务器的操作。

在**服务器配置**下选择**服务器属性**以配置服务器超时。提供的服务器超时选择如下：

操作系统看守程序
操作系统看守程序用于监控操作系统以确保其未挂起。要使用此功能，必须启用 **Ethernet over USB** 接口。有关详细信息，请参阅第 31 页 “配置 Ethernet over USB”。**XClarity Controller** 按照**操作系统看守程序时间**选择中配置的时间间隔联系操作系统。如果操作系统在下一次检查前未响应，则 **XClarity Controller** 认为操作系统发生挂起。**XClarity Controller** 将捕获服务器显示器的内容，然后重新启动服务器以尝试恢复操作。**XClarity Controller** 只能重新启动服

务器一次。如果重新启动后操作系统仍然挂起，则将让服务器保持挂起状态而不继续重新启动服务器，以便调查问题并解决问题。要重置启用操作系统看守程序，请关闭服务器电源，然后再打开。要启用操作系统看守程序，请从操作系统看守程序时间下拉列表中选择一个时间间隔，然后单击**应用**。要禁用操作系统看守程序，请在操作系统看守程序时间下拉菜单上选择**无**。

装入程序看守程序

装入程序看守程序监控从 **POST** 完成到操作系统开始运行之间的时间间隔。要使用此功能，必须启用 **Ethernet over USB** 接口。有关详细信息，请参阅第 31 页 “配置 Ethernet over USB”。**POST** 完成后，**XClarity Controller** 开始计时，然后开始联系操作系统。如果操作系统在装入程序看守程序选择中配置的时间内未响应，则 **XClarity Controller** 认为操作系统引导发生挂起。**XClarity Controller** 将再重新启动服务器以尝试恢复操作。**XClarity Controller** 只能重新启动服务器一次。如果重新启动后操作系统引导仍然挂起，则将让服务器保持挂起状态而不继续重新启动服务器，以便调查问题并解决问题。关闭并重新打开服务器或将服务器成功引导至操作系统时将重置装入程序看守程序。要启用装入程序看守程序，请从装入程序看守程序下拉列表中选择一个时间间隔，然后单击**应用**。要禁用装入程序看守程序，请在装入程序看守程序时间下拉列表上选择**无**。

启用关闭电源延迟

使用“关闭电源延迟”字段可指定 **XClarity Controller** 子系统在强制关闭电源之前将等待操作系统关闭的分钟数。要设置关闭电源延迟超过值，请从下拉列表中选择一个时间间隔，然后单击**应用**。要禁用 **XClarity Controller** 强制关闭电源，请从下拉列表选择中选择**无**。

非法侵入消息

要创建在用户登录到 **XClarity Controller** 时显示的消息，请参阅本主题中的信息。

在**服务器配置**下选择**服务器属性**。使用**非法入侵消息**选项来配置您希望向用户显示的消息。完成后，单击 **应用**。

当用户登录时，在 **XClarity Controller** 登录页面的消息区域中将显示该消息文本。

设置 XClarity Controller 的日期和时间

按本主题中的信息了解 **XClarity Controller** 的日期和时间设置。可根据提供的说明配置 **XClarity Controller** 的日期和时间。**XClarity Controller** 的日期和时间用于对事件日志中记录的所有事件及发送的警报加盖时间戳记。

在 **XClarity Controller** 主页中，单击右上角的时钟图标可查看或更改 **XClarity Controller** 的日期和时间。**XClarity Controller** 没有其自己的实时时钟。可配置 **XClarity Controller** 与网络时间协议服务器或服务器上的实时时钟硬件进行时间和日期同步。

与 NTP 同步

完成以下步骤以将 **XClarity Controller** 时钟与 **NTP** 服务器进行同步：

- 选择**与 NTP 同步时间**并指定 **NTP** 服务器地址。
- 通过单击“+”图标可指定其他 **NTP** 服务器。
- 指定希望 **XClarity Controller** 与 **NTP** 服务器进行同步的频率。
- 从 **NTP** 服务器获得的时间格式为协调世界时（**UTC**）格式。

  - 如果希望 **XClarity Controller** 调整为本地区域的时间和日期，请从下拉菜单中选择所在区域的时区偏移量。
  - 如果所在位置采用夏令时，请勾选**针对夏令时（DST）自动调整**复选框。
- 完成配置更改后，单击**应用**。

与主机同步

服务器实时时钟硬件中保留的时间可能为协调世界时格式，也可能已经过调整并存储为本地时间格式。部分操作系统将实时时钟存储为 **UTC** 格式，而其他操作系统则将时间存储为本地时间。服务器实时时钟不指示时间格式。因此，将 **XClarity Controller** 配置为与主机的实时时钟同步时，用户可选择 **XClarity Controller** 如何使用从实时时钟获取的时间和日期。

- 本地（例如：**Windows**）：此模式下，**XClarity Controller** 认为从实时时钟获取的时间和日期为已应用适用时区和 **DST** 偏移量的本地时间。
- **UTC**（例如：**Linux**）：此模式下，**XClarity Controller** 认为从实时时钟获取的时间和日期为未应用时区和 **DST** 偏移量的协调世界时。此模式下，通过从下拉菜单中选择所在区域的时区偏移量，可选择将时间和日期调整为本地区域的时间和日期。如果所在位置采用夏令时，也可勾选**针对夏令时（DST）自动调整**复选框。
- 完成配置更改后，单击**应用**。

注：

- 发生夏令时调整时，任何计划在时钟拨快的间隔中发生的 **XClarity Controller** 操作将不予执行。例如，如果美国夏令时开始时间为 **3** 月 **12** 日凌晨 **2:00**，而某个电源操作计划于 **3**月 **12** 日凌晨 **2:10** 执行，则该操作将不会发生。因为时间一旦到达凌晨 **2:00**，**XClarity Controller** 将把时间读取为凌晨 **3:00**。
- 在 **Flex System** 中，无法修改 **XClarity Controller** 的日期和时间设置。

第 6 章　配置存储

请参阅本章中的信息了解存储配置可用的选项。

配置存储时可使用以下选项：

- 详细信息
- **RAID** 设置

RAID 详细信息

要使用 **RAID** 详细功能，请参阅本主题中的信息。

此功能显示存储设备的物理结构和存储配置以及详细信息，例如其位置、制造商、产品名称、状态、容量、接口、介质、外形规格和其他信息。

RAID 设置

要执行 **RAID** 设置功能，请参阅本主题中的信息。

按本主题中的信息查看和配置 **RAID** 适配器的存储池、关联的虚拟磁盘和硬盘。如果系统电源已关闭，请打开电源后再查看 **RAID** 信息。

查看和配置虚拟硬盘

按本主题中的信息查看和配置虚拟硬盘。

选择**服务器配置**下的 **RAID 设置**后，默认情况下将选中**阵列配置**选项卡并显示现有的虚拟磁盘。逻辑硬盘按磁盘阵列和控制器进行排序。有关虚拟磁盘的详细信息（例如虚拟磁盘条带大小和可引导信息）将显示出来。

要配置 **RAID** 设置，请单击**启用编辑模式**。

编辑模式下，可单击控制器操作菜单，查看当前的 **RAID** 虚拟磁盘并创建新的 **RAID** 虚拟磁盘。

从“控制器操作”菜单可执行以下操作：

清除 RAID 配置
清除所选控制器上的所有配置和数据。

管理外部配置
导入任何检测到的外部硬盘。外部硬盘是从其他 **RAID** 配置移至当前 **RAID** 控制器的硬盘

注：如果未检测到任何外部硬盘，您将收到通知。

特定控制器的当前 **RAID** 虚拟磁盘信息显示为单独的“虚拟磁盘卡”。每张卡显示虚拟磁盘的名称、状态、容量和操作等信息。通过铅笔图标可编辑信息，通过垃圾桶图标可删除“虚拟磁盘卡”。

注：容量和 **RAID** 级别无法更改。

单击虚拟磁盘名称将显示虚拟磁盘属性窗口。

要创建新的 **RAID** 虚拟磁盘，请执行以下步骤：

注： 如果无剩余存储容量，将无法创建新的虚拟磁盘。

1. **选择有可用存储容量的硬盘或磁盘阵列**
   a. 在新磁盘阵列中创建虚拟磁盘时，需要指定 **RAID** 级别。如果在可选硬盘不足的情况下单击**下一步**，该 **RAID** 级别字段下将显示一条错误消息。

      对于某些 **RAID** 级别，必需使用磁盘簇。磁盘簇中必须存在一定数量的硬盘。

      1) 对于这些情况，**Web** 界面默认情况下将显示**磁盘簇 1**。

      2) 选择硬盘，然后单击**添加成员**以将硬盘添加到**磁盘簇 1**。**磁盘簇 1** 中没有足够硬盘时，禁用**添加磁盘簇**链接。

      3) 单击**添加磁盘簇**以添加**磁盘簇 2**。选择硬盘，然后单击**添加成员**以将硬盘添加到**磁盘簇 2**。

      4) 单击**添加成员**将硬盘添加到最后一个磁盘簇。如果要再次将硬盘添加到**磁盘簇 1**，需单击磁盘簇 **1**，然后选择要添加到**磁盘簇 1** 的硬盘。

      5) 如果磁盘簇数量达到最大限制，禁用**添加磁盘簇**。

   b. 要在现有磁盘阵列中创建虚拟磁盘，必须选择有剩余容量的磁盘阵列。

2. **创建虚拟磁盘**
   a. 默认情况下，将创建一个使用全部存储容量的虚拟磁盘。无存储可用时将禁用**添加**图标。可单击铅笔图标以更改容量或其他属性。

   b. 编辑第一个虚拟磁盘来使用部分存储容量时，**添加**图标将会启用。单击该图标以显示**添加虚拟磁盘**窗口。

   c. 如果虚拟磁盘数量超过一个，将启用**删除**图标。仅有一个虚拟磁盘时不显示此图标。单击**删除**图标后将立即删除所选的行。此时不会显示任何确认窗口，因为尚未创建该虚拟磁盘。

   d. 单击**开始创建虚拟磁盘**以启动该过程。

注：如果不支持该控制器，将显示一条消息。

查看和配置存储清单

按本主题中的信息查看和配置存储清单。

在**存储清单**选项卡下，您可以查看并配置 **RAID** 控制器的磁盘阵列、关联的虚拟硬盘和硬盘。

- **对于支持 RAID 配置的存储设备：**
  1. 如果控制器包含已配置的磁盘阵列，则将根据磁盘阵列显示安装的硬盘。以下是对窗口显示项目的说明。
     - **表格标题：**显示磁盘阵列标识、**RAID** 级别和硬盘总数。
     - **表格内容：**列出基本属性 - 硬盘名、**RAID** 状态、类型、序列号、部件号、**FRU** 编号和操作。您可以转至**清单**页面来查看 **XClarity Controller** 可检测到的所有属性。
     - **操作：**可执行的操作项如下所示。部分操作在硬盘处于不同状态时不可用。
       - **分配热备用：**指定作为全局热备用或专用热备用的硬盘。
       - **删除热备用：**将硬盘从热备用中删除。
       - **将硬盘设置为脱机：**将硬盘设置为脱机。
       - **将硬盘设置为联机：**将硬盘设置为联机。

- **将硬盘设置为可重用**： 将硬盘设置为可重用。
- **将硬盘设置为缺失**：将硬盘设置为缺失。
- **将硬盘设置为对 JBOD 完好**：将硬盘添加到 JBOD 磁盘排列。
- **将硬盘设置为未配置的完好硬盘**：将硬盘设置为可供配置阵列，或可用作紧急热备用。
- **将硬盘设置为未配置的故障硬盘**：将硬盘标记为不正常，使其无法在阵列中使用或作为紧急热备用。
- **将硬盘设置为准备卸下**：将硬盘设置为准备卸下。

2. 如果控制器包含尚未配置的硬盘，则将显示在**非 RAID 硬盘**表格中。通过单击**将 JBOD 转换为配置就绪**选项将打开一个窗口，其中显示支持此操作项的所有硬盘。您可以选择一个或多个硬盘进行转换。

对于不支持 RAID 配置的存储设备：XClarity Controller 可能无法检测到部分硬盘的属性。

第 7 章　更新服务器固件

按本主题中的信息更新服务器固件。

概述

关于更新服务器固件的一般信息。

导航面板上的**固件更新**选项具有 **4** 个功能：

- **系统固件**：系统固件状态和版本概述。并执行系统固件更新。
- **自动将主 XCC 提升为备用 XCC**：启用后，暂挂的备用存储体固件将在主存储体通过映像稳定性指标（ISM）衡量后从主存储体同步。
- **适配器固件**：已安装的适配器固件概述，它们的状态和版本。并执行适配器固件更新。
- **PSU 固件**：电源模块单元固件版本概述。并执行 **PSU** 固件更新。
- **从存储库更新**：将服务器固件与远程 **CIFS/NFS** 存储库同步进行批量更新。

将显示 **BMC**、**UEFI**、**LXPM**、**LXPM** 驱动程序和适配器固件的当前状态和版本，包括 **BMC** 主版本和备份版本。固件状态有四种类别：

- **活动**：固件处于活动状态。
- **非活动**：固件处于非活动状态。
- **等待**：固件正在等待变为活动状态。
- **不适用**：该组件未安装任何固件。

注意：

- 在更新 **UEFI** 之前，必须将 **XCC** 和 **IMM** 更新到最新版本。以不同的顺序更新可能会导致异常或错误的行为。
- 安装错误的固件更新可能会导致服务器发生故障。在安装固件或设备驱动程序更新之前，请阅读所下载的更新随附的任何自述文件和变更历史记录文件。这些文件中包含有关此更新和安装更新过程的重要信息，包括从旧固件或设备驱动程序版本更新至最新版本的任何特殊过程。由于 **Web** 浏览器可能包含 **XCC** 高速缓存数据，因此建议在 **XCC** 固件升级后重新加载 **Web** 页面。
- 除 **SATA M.2** 适配器外，**AMD** 处理器服务器不支持带外适配器固件更新。
- 某些固件更新需要重启系统，以执行固件激活或内部更新。此过程在系统引导中称为“系统维护模式”，在此过程中暂时不允许用户执行电源操作。在固件更新过程中也会启用该模式。当系统进入维护模式时，用户不应断开交流电源。

系统、适配器和 PSU 固件更新

更新系统固件、适配器固件和 **PSU** 固件的步骤。

要手动更新**系统固件**、**适配器固件**和 **PSU 固件**，请完成以下步骤：

1. 在每个功能中单击**更新固件**。随后会显示“更新服务器固件”窗口。
2. 单击**浏览**选择要使用的固件更新文件。

3. 浏览至要选择的文件，然后单击**打开**。您将返回到“更新服务器固件”窗口，此窗口中会显示所选的文件。
4. 单击**下一步** > 以开始上传并验证所选文件上的进程。上传并验证文件时，将会显示进度条。您可以查看此状态窗口，以验证选定要更新的文件是否是正确的文件。对于**系统固件**，状态窗口将包含有关要更新的固件文件类型（如 **BMC**、**UEFI** 或 **LXPM**）的信息。固件文件上传并验证成功后，单击**下一步**选择要更新的设备。
5. 单击**更新**开始固件更新。进度条将显示更新进度。固件更新成功完成后，单击**完成**。如果更新需要重新启动 **XClarity Controller** 才能生效，将会显示一条警告消息。有关如何重新启动 **XClarity Controller** 的详细信息，请参阅第 **60** 页 “电源操作”。

从远程存储库更新

从远程存储库更新服务器固件的步骤

通过**从存储库更新**，用户可以配置 **XCC** 以便将服务器固件与远程 **CIFS/NFS** 固件存储库同步。固件存储库应包含 **SUP** 包，包括二进制和元数据 **XML** 文件，或 **UXSP** 元数据 **XML** 和相应的二进制文件。**XCC** 解析元数据 **XML** 文件，挑选出支持对此特定系统硬件进行 **OOB** 更新的固件包，然后开始批量更新。

有五种更新状态：

- **绿色复选标记** ：固件升级成功完成。
- **红色 X 标记** ：固件升级失败。
- **更新中**：固件正在升级过程中。
- **取消**：固件升级被取消。
- **等待中**：固件升级正在等待部署。

当用户单击**停止更新**时，将在当前安装包更新完成后，取消队列中的升级。

要从存储库更新，请完成以下步骤：

1. 输入远程存储库信息后，单击**连接**以连接至远程存储库。
2. 单击**更新**开始批量更新。
3. 单击**查看详情**查看更新状态，如上所述，有 **5** 种状态。
4. 单击**停止更新**时，将在当前安装包更新完成后，取消队列中的升级。
5. 单击**断开连接**以断开与远程存储库的连接。
6. 如果更新需要重新启动 **XClarity Controller** 才能生效，将会显示一条警告消息。有关如何重新启动 **XClarity Controller** 的详细信息，请参阅第 **60** 页 “电源操作”。

第 8 章　许可证管理

Lenovo XClarity Controller 许可证管理可安装并管理可选服务器和系统管理功能。

有多个级别的 **XClarity Controller** 固件功能和功能部件可用于您的服务器。安装在服务器上的固件功能的级别根据硬件类型而异。

您可以通过购买并安装激活密钥来升级 **XClarity Controller** 的功能。

要订购激活密钥，请联系您的销售代表或业务合作伙伴。

使用 **XClarity Controller Web** 界面或 **XClarity Controller CLI** 可手动安装激活密钥，通过该激活密钥可使用已购买的可选功能。激活密钥前：

- 激活密钥必须位于用于登录到 **XClarity Controller** 的系统上。
- 您必须已订购许可证密钥，并通过信件或电子邮件接收到其授权代码。

有关使用 **XClarity Controller Web** 界面管理激活密钥的信息，请参阅第 **87** 页 “安装激活密钥”、第 **88** 页 “删除激活密钥”或第 **88** 页 “导出激活密钥”。有关使用 **XClarity Controller CLI** 管理激活密钥的信息，请参阅第 **124** 页 “**keycfg** 命令”。

要注册一个标识以管理 **XClarity Controller** 许可证，请单击以下链接：
http://thinksystem.lenovofiles.com/help/index.jsp

以下 **Lenovo Press** 网站提供有关 **Lenovo** 服务器许可证管理的其他信息：

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

注意：不能从 **XClarity Controller Standard** 级别直接升级到 **Enterprise** 级别。必须先升级到 **Advanced** 级别，然后才能激活 **Enterprise** 级别功能。

安装激活密钥

按本主题中的信息向服务器添加可选功能。

要安装激活密钥，请完成以下步骤：

步骤 **1.** 单击 **BMC 配置**下的**许可证**。

步骤 **2.** 单击**升级许可证**。

步骤 **3.** 在**添加新许可证**窗口中，单击**浏览**；在“文件上传”窗口中选择要添加的激活密钥文件，然后单击**打开**以添加文件，或单击**取消**以停止安装。要完成添加密钥，请在“添加激活密钥”窗口中单击**确定**，或者单击**取消**以停止安装。

成功窗口指示已安装激活密钥。

注：

- 如果激活密钥无效，那么将显示一个错误窗口。

步骤 4. 单击**确定**以关闭成功窗口。

删除激活密钥

按本主题中的信息从服务器删除可选功能。

要删除激活密钥，请完成以下步骤：

步骤 1. 单击 **BMC 配置**下的**许可证**。

步骤 2. 选择要删除的激活密钥，然后单击**删除**。

步骤 3. 在确认删除激活密钥窗口中，单击**确定**以确认删除激活密钥或者单击**取消**以保留密钥文件。
所选激活密钥将从服务器中删除，并且不再出现在“许可证管理”页面中。

导出激活密钥

按本主题中的信息从服务器导出可选功能。

要导出激活密钥，请完成以下步骤：

步骤 1. 单击 **BMC 配置**下的**许可证**。

步骤 2. 从“许可证管理”页面中，选择要导出的激活密钥，然后单击**导出**。

步骤 3. 在**导出所选许可证**窗口中，单击**导出**以确认激活密钥导出，或单击**取消**以取消密钥导出请求。

步骤 4. 选择用于保存文件的目录。
随后从服务器导出所选的激活密钥。

第 9 章　Lenovo XClarity Controller Redfish REST API

Lenovo XClarity Controller 提供一组与 Redfish 兼容且简单易用的 REST API，可用于从 Lenovo XClarity Controller 框架以外运行的应用程序访问 Lenovo XClarity Controller 数据和服务。

这样可轻松地将 Lenovo XClarity Controller 功能集成到其他软件中，无论该软件在与 Lenovo XClarity Controller 服务器相同的系统上运行，还是在同一网络中的远程系统上运行。这些 API 基于行业标准 Redfish REST API，可通过 HTTPS 协议访问。

《XClarity Controller Redfish REST API 用户指南》位于以下网站：https://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.restapi.doc/xcc_restapi_book.pdf。

Lenovo 提供开源示例 Redfish 脚本，开发与 Lenovo Redfish REST API 通信的软件时可以用作参考。这些示例脚本可在此找到：

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

与 Redfish API 相关的 DMTF 规范位于：https://redfish.dmtf.org/。此网站提供 Redfish REST API 的一般规范和其他参考资料。

第 10 章　命令行界面

按本主题中的信息输入管理和监控 **XClarity Controller** 的命令，而无需使用 **XClarity Controller Web** 界面。

使用 **XClarity Controller** 命令行界面（**CLI**）可访问 **XClarity Controller** 而不必使用 **Web** 界面。它提供了 **Web** 界面提供的一部分管理功能。

您可以通过 **SSH** 会话访问 **CLI**。您必须先通过 **XClarity Controller** 认证，然后才能发出 **CLI** 命令。

访问命令行界面

按本主题中的信息访问 **CLI**。

要访问 **CLI**，请向 **XClarity Controller** 的 **IP** 地址启动 **SSH** 会话（有关更多信息，请参阅第 **91** 页 “配置 **serial-to-SSH** 重定向”）。

登录到命令行会话

按本主题中的信息登录到命令行会话。

要登录到命令行，请完成以下步骤：

步骤 **1.** 建立与 **XClarity Controller** 的连接。

步骤 **2.** 在用户名提示符处，输入用户 **ID**。

步骤 **3.** 在密码提示符处，输入用于登录到 **XClarity Controller** 的密码。

您已登录到命令行。随后将显示命令行提示符 `system>`。命令行会话继续，直至您在命令行上输入 `exit`。您已注销并且会话已结束。

配置 serial-to-SSH 重定向

本主题提供将 **XClarity Controller** 用作串行终端服务器的有关信息。

通过 **serial-to-SSH** 重定向，系统管理员可以将 **XClarity Controller** 用作串行终端服务器。启用了串口重定向时，可以通过 **SSH** 连接访问服务器串口。

注：CLI console 1 命令用于通过 **COM** 端口启动串口重定向会话。

示例会话

```
$ ssh USERID@10.240.1.12
Password:

system>
```

所有来自 **SSH** 会话的流量都路由到 **COM2**。

```
ESC (
```

输入退出按键序列以返回到 **CLI**。在此示例中，按 **Esc** 键，然后输入左圆括号。将显示 **CLI** 提示符，以指示返回到 **IMM CLI**。

```
system>
```

命令语法

查看本主题中的准则以了解如何在 **CLI** 中输入命令。

开始用命令前，请阅读以下准则：

- 每个命令都具有以下格式：
  command [*arguments*] [-*options*]
- 命令语法区分大小写。
- 命令名全部为小写。
- 所有参数都必须紧跟在命令后面。选项紧跟在参数后面。
- 每个选项的前面始终带有连字符（-）。选项可以是短选项（单个字母），也可以是长选项（多个字母）。
- 如果某个选项具有参数，那么必须参数为必填，例如：
  ifconfig eth0 -i 192.168.70.34 -g 192.168.70.29 -s 255.255.255.0
  其中，**ifconfig** 是命令，**eth0** 参数，**-i**、**-g** 和 **-s** 是选项。在此示例中，所有三个选项都具有参数。
- 方括号指示参数或选项是可选的。方括号不属于输入的命令。

功能和限制

本主题介绍 **CLI** 的功能和限制。

CLI 具有以下功能和限制：

- 允许通过 **SSH** 进行多个并发 **CLI** 会话。
- 每行允许一个命令（限制为 **1024** 个字符，包括空格）。
- 长命令没有连续字符。唯一的编辑功能是使用退格键擦除您刚输入的字符。
- 向上方向键和向下方向键可用于浏览最近八个命令。**history** 命令显示最近八个命令的列表，可用作执行某个命令的快捷方式，如以下示例中所示：

```
system > history
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
system > !0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n XClarity ControllerA00096B9E003A
-r auto
```

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

- 在 **CLI** 中，输出缓冲区限制为 **2 KB**。不进行缓冲。单个命令的输出不能超过 **2048** 个字符。此限制不适用于串口重定向模式（在串口重定向期间会缓冲数据）。
- 简单文本消息用于表示命令执行状态，如以下示例中所示：
```
system> power on
ok
system> power state
Power: On
State: System power off/State unknown
system>
```
- 命令语法区分大小写。
- 在选项及其参数之间至少应有一个空格。例如， `ifconfig eth0 -i192.168.70.133` 是不正确的语法。正确的语法是 `ifconfig eth0 -i 192.168.70.133`。
- 所有命令都具有 `-h`, `-help` 和 `?` 选项，它们可提供语法帮助。以下所有示例均提供相同结果：
```
system> power -h
system> power -help
system> power ?
```
- 以下各节中描述的某些命令在您的系统配置中可能不可用。要查看您的配置所支持的命令的列表，请使用 `help` 或 `?` 选项，如以下示例中所示：
```
system> help
system> ?
```
- 在 **Flex System** 中，一些设置由 **CMM** 管理，而无法在 **XClarity Controller** 上修改。

按字母顺序排列的命令列表

本主题包含按字母顺序排列的 **CLI** 命令列表。每个命令均提供了主题链接。每个命令主题提供有关该命令及其功能、语法和用法的信息。

以下是所有 **XClarity Controller CLI** 命令的完整列表（按字母顺序排列）：

实用程序命令

本主题按字母顺序提供实用程序 CLI 命令的列表。

当前有 3 条实用程序命令：

exit 命令

使用命令可注销 CLI 会话。

使用 exit 命令可注销并结束 CLI 会话。

help 命令

该命令显示所有命令的列表。

使用 help 命令可显示所有命令的列表，以及每个命令的简短描述。您也可以在命令提示符处输入 ?。

history 命令

该命令提供以前发出的命令的列表。

使用 **history** 命令可显示带索引的历史记录列表，提供最近发出的八个命令。然后，可使用索引作为快捷方式（前面带有 !），以重新发出此历史记录列表中的命令。

示例：

```
system> history
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
HISTORY-g 0.0.0.0
-s 255.255.255.0
-n XCCA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system>
```

监控命令

本主题按字母顺序提供监控 **CLI** 命令的列表。

当前有 **11** 条监控命令：

clearlog 命令

此命令用于清除 **IMM** 事件日志。

使用 **clearlog** 命令可清除 **IMM** 的事件日志。您必须具有清除事件日志的权限才能使用此命令。

注：此命令仅供支持人员使用。

下表显示选项的参数。

表 7. clearlog 命令

下表是一个单行两列的表格，由选项和选项描述组成。

选项	描述
-t <all | platform | audit>	事件类型，选择要清除的事件类型。如果未指定此项，则将选择所有事件类型。

事件类型描述

- **all：**所有事件类型，包括平台事件和审核事件。

- **platform**：平台事件类型。
- **audit**：审核事件类型。

示例：

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

fans 命令

此命令用于显示服务器风扇的速度。

使用 **fans** 命令可显示每个服务器风扇的速度。

示例：

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

ffdc 命令

此命令用于生成新的服务数据文件。

使用最初故障数据捕获（**ffdc**）命令生成服务数据并将其传送到支持机构。

以下列表由要与 **ffdc** 命令配合使用的命令组成：

- **generate**，创建新服务数据文件
- **status**，检查服务数据文件的状态
- **copy**，复制现有服务数据
- **delete**，删除现有服务数据

下表显示选项的参数。

表 8. ffdc 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-t	类型编号	**1**（处理器转储）和 **4**（服务数据）。处理器转储包含所有可用日志文件和文件。服务数据仅包含一部分日志和文件。默认值为 **1**。
-f [1]	远程文件名或 **sftp** 目标目录。	对于 **sftp**，请使用完整路径或在目录名称上使用尾随 **/**（**~/** 或 **/tmp/**）。默认值是系统生成的名称。
-ip [1]	**tftp/sftp** 服务器的地址	

表 8. ffdc 命令 （续）

选项	描述	值
-pn [1]	**tftp/sftp** 服务器的端口号	默认值为 **69/22**。
-u [1]	**sftp** 服务器的用户名	
-pw [1]	**sftp** 服务器的密码	
1. generate 和 **copy** 命令的附加参数		

语法：

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

示例：

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


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

hreport 命令

使用此命令可显示嵌入式运行状况报告。

下表显示 **hreport** 命令。

表 9. hreport 命令

下表是一个多行两列的表格，由此不同 **hreport** 命令的描述组成。

表 9. hreport 命令 （续）

选项	描述
生成	创建新运行状况报告
状态	检查状态
copy	拷贝现有运行状况报告
删除	删除现有运行状况报告

下表显示 **generate** 和 **copy** 选项的参数。

表 10. generate 和 copy 命令

下表是一个多行两列的表格，由 **generate** 和 **copy** 命令选项以及选项描述组成。

选项	描述
-f	远程文件名或 **sftp** 目标目录（默认值是系统生成的名称（（对于 **sftp**，使用完整路径或在目录名称后加 **/**（**~/** 或 **/tmp/**））
-ip	**tftp/sftp** 服务器的地址
-pn	**tftp/sftp** 服务器的端口号（默认值是 **69/22**）
-u	**sftp** 服务器的用户名
-pw	**sftp** 服务器的密码

mhlog 命令

使用此命令可显示维护历史记录活动日志条目。

下表显示选项的参数。

表 11. mhlog 命令

下表是一个多行两列的表格，由选项和选项描述组成。

选项	描述
-c <count>	显示“**count**”条目（**1-250**）
-i <index>	显示从索引（**1-250**）处开始的条目
-f	远程日志文件的文件名
-ip	**tftp/sftp** 服务器的地址
-pn	**tftp/sftp** 服务器的端口号（默认值是 **69/22**）
-u	**sftp** 服务器的用户名
-pw	**sftp** 服务器的密码

示例

显示内容将如下所示：

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

led 命令

使用此命令可显示和设置 **LED** 状态。

led 命令可显示和设置服务器 **LED** 的状态。

- 运行不带任何选项的 **led** 命令将显示前面板 **LED** 的状态。
- **led -d** 命令选项必须与 **led -identify on** 命令选项结合使用。

下表显示选项的参数。

表 12. led 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-l	获取所有系统及系统子组件的 **LED** 状态	
-chklog	关闭检查日志 **LED**	关
-identify	更改机柜标识 **LED** 的状态	**off**、**on** 和 **blink**
-d	在指定时间段打开标识 **LED**	时间段（秒）

语法：

```
led [options]
option:
 -l
 -chklog off
 -identify state
  -d time
```

示例：

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

system> led -l
Label          Location          State     Color
Battery         Planar           Off
BMC Heartbeat      Planar            Blink     Green
BRD            Lightpath Card       Off
Channel A        Planar            Off
Channel B        Planar            Off
Channel C        Planar            Off
```

```
Channel D        Planar            Off
Channel E        Planar            Off
Chklog          Front Panel         Off
CNFG           Lightpath Card       Off
CPU            Lightpath Card       Off
CPU 1           Planar            Off
CPU 2           Planar            Off
DASD           Lightpath Card       Off
DIMM           Lightpath Card       Off
DIMM 1          Planar            Off
DIMM 10         Planar            Off
DIMM 11         Planar            Off
DIMM 12         Planar            Off
DIMM 13         Planar            Off
DIMM 14         Planar            Off
DIMM 15         Planar            Off
DIMM 16         Planar            Off
DIMM 2          Planar            Off
DIMM 3          Planar            Off
DIMM 4          Planar            Off
DIMM 5          Planar            Off
DIMM 6          Planar            Off
DIMM 7          Planar            Off
DIMM 8          Planar            Off
DIMM 9          Planar            Off
FAN            Lightpath Card       Off
FAN 1           Planar            Off
FAN 2           Planar            Off
FAN 3           Planar            Off
Fault           Front Panel (+)      Off
Identify         Front Panel (+)       On       Blue
LINK           Lightpath Card       Off
LOG            Lightpath Card       Off
NMI            Lightpath Card       Off
OVER SPEC        Lightpath Card       Off
PCI 1           FRU              Off
PCI 2           FRU              Off
PCI 3           FRU              Off
PCI 4           FRU              Off
Planar          Planar            Off
Power           Front Panel (+)      Off
PS             Lightpath Card       Off
RAID           Lightpath Card       Off
Riser 1         Planar            Off
Riser 2         Planar            Off
SAS ERR          FRU              Off
SAS MISSING       Planar            Off
SP             Lightpath Card       Off
TEMP           Lightpath Card       Off
VRM            Lightpath Card       Off
system>
```

readlog 命令

此命令显示 **IMM** 事件日志。

使用 **readlog** 命令可显示 **IMM** 事件日志条目。一次可显示五个事件日志。条目按从最新到最旧的顺序显示。

readlog 可显示事件日志中的前五个条目，第一次执行该命令时从最新条目开始显示，以后每次调用时显示接下来的五条。

readlog -a 可显示事件日志中的所有条目，从最新条目开始显示。

readlog -f 可重置计数器并显示事件日志中的前 **5** 个条目，从最新条目开始显示。

readlog -date *date* 可显示以 **mm/dd/yy** 格式指定的指定日期的事件日志条目。可以是以竖线（|）分隔的日期列表。

readlog -sev *severity* 可显示指定严重性级别（**E**、**W** 和 **I**）的事件日志条目。它可以是以竖线（|）分隔的严重性级别列表。

readlog -i *ip_address* 可设置用于保存事件日志的 **TFTP** 或 **SFTP** 服务器的 **IPv4** 或 **IPv6 IP** 地址。**-i** 和 **-l** 命令选项共同用于指定位置。

readlog -l *filename* 可设置事件日志文件的文件名。**-i** 和 **-l** 命令选项共同用于指定位置。

readlog -pn *port_number* 可显示或设置 **TFTP** 或 **SFTP** 服务器的端口号（默认值为 **69/22**）。

readlog -u *username* 可指定 **SFTP** 服务器的用户名。

readlog -pw *password* 可指定 **SFTP** 服务器的密码。

语法：

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

示例：

```
system> readlog -f
1 I 2017-06-17T09:31:59.217 Remote Login Successful. Login ID: USERID
from SSH at IP address 10.134.78.180
2 I 2017-06-17T07:23:04.685 Remote Login Successful. Login ID: USERID
from webguis at IP address 10.134.78.180.
3 I 2017-06-16T11:00:35.581 Login ID: USERID from webguis at IP address 10.134.78.180 has logged off.
4 I 2017-06-16T11:00:15.174 Login ID: USERID from webguis at IP address 10.104.209.144 has logged off.
5 I 2017-06-16T10:40:14.352 Login ID: USERID from webguis at IP address 10.104.209.144 has logged off.
system> readlog
6 E SERVPROC 12/18/03 10:09:31 Fan 2 Fault. Multiple fan failures
7 E SERVPROC 12/18/03 10:09:31 Fan 1 Fault. Single fan failure
8 I SERVPROC 12/18/03 10:09:25 Ethernet[0] Link Established at 100Mb, Full Duplex.
9 I SERVPROC 12/18/03 10:09:24 Ethernet[0] configured to do Auto Speed/Auto Duplex.
10 I SERVPROC 12/18/03 10:09:24 Ethernet[0] MAC Address currently
being used: 0x00-09-6B-CA-0C-80
system>
```

syshealth 命令

此命令提供运行状况或活动事件的摘要。

使用 **syshealth** 命令可显示服务器的运行状况或活动事件的摘要。显示内容包括：电源状态、系统状态、硬件状态（包括风扇、电源模块、存储、处理器、内存）、重新启动次数和 **IMM** 软件状态。

语法：

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

示例：

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

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

temps 命令

此命令显示所有温度和温度阈值信息。

使用 **temps** 命令可显示所有温度和温度阈值。显示的一组温度与 **Web** 界面中相同。

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

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

注：

1. 输出具有以下列标题：
   - **WR**：警告重置（正向阈值滞后值）
   - **W**：警告（非临界阈值上限）
   - **T**：温度（当前值）
   - **SS**：软关机（临界阈值上限）
   - **HS**：硬关机（不可恢复阈值上限）
2. 所有温度值都以华氏度/摄氏度为单位。
3. **N/A** 表示不适用。

volts 命令

使用此命令显示服务器电压信息。

使用 **volts** 命令可显示所有电压和电压阈值。显示的一组电压与 **Web** 界面中相同。

```
Example:
system> volts

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

注：输出具有以下列标题：

HSL：硬关机下限（不可恢复阈值下限）

SSL：软关机下限（临界阈值下限）

WL：警告下限（非临界阈值下限）

WRL：警告重置下限（负向阈值滞后值）

V：电压（当前值）

WRH：警告重置上限（正向阈值滞后值）

WH：警告上限（非临界阈值上限）

SSH：软关机上限（临界阈值上限）

HSH：硬关机上限（不可恢复阈值上限）

vpd 命令

此命令显示与服务器硬件和软件关联的配置和参考数据（重要产品数据）。

使用 **vpd** 命令可显示系统（**sys**）、**IMM**（**bmc**）、服务器 **BIOS**（**uefi**）、**Lenovo XClarity Provisioning Manager**（**lxpm**）、服务器固件（**fw**）、服务器组件（**comp**）和 **PCIe** 设备（**pcie**）的重要产品数据。显示的信息与 **Web** 界面中相同。

语法：

```
vpd sys  - displays Vital Product Data for the system
vpd bmc  - displays Vital Product Data for the management controller
vpd uefi - displays Vital Product Data for system BIOS
vpd lxpm  - displays Vital Product Data for system LXPM
vpd fw  - displays Vital Product Data for the system firmware
vpd comp - displays Vital Product Data for the system components
vpd pmem - displays Vital Product Data for Intel Optane PMem
vpd pcie - displays Vital Product Data for PCIe devices
```

示例：

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

```
system>
```

服务器电源和重新启动控制命令

本主题按字母顺序提供电源和重新启动 **CLI** 命令的列表。

当前有 **4** 条服务器电源和重新启动命令：

power 命令

此命令描述如何控制服务器电源。

使用 **power** 命令来控制服务器电源。要发出 **power** 命令，您必须具有远程服务器电源操作/重新启动访问权限级别。

下表包含可与 **power** 命令结合使用的一部分命令。

表 13. power 命令

下表是一个多行三列表格，包含 **power** 命令、命令描述以及与命令关联值的信息。

命令	描述	值
打开电源	使用此命令可开启服务器电源。	**on** 和 **off**
关机	使用此命令可关闭服务器电源。 **注：-s** 选项先关闭操作系统，然后关闭服务器。	**on** 和 **off**
power cycle	使用此命令可关闭然后再打开服务器电源。 **注：-s** 选项先关闭操作系统，然后关闭服务器。	
power enterS3	使用此命令可将操作系统置于 **S3**（睡眠）模式。 **注：**只有当操作系统开启时才能使用此命令。并非所有服务器上都支持 **S3** 模式。	
power rp	使用此选项可指定主机电源恢复策略。	**alwayson|alwaysoff|restore**
power S3resume	使用此命令可将操作系统从 **S3**（睡眠）模式中唤醒。 **注：**只有当操作系统开启时才能使用此命令。并非所有服务器上都支持 **S3** 模式。	
power state	使用此命令可显示服务器电源状态以及服务器的当前状态。	**on** 和 **off**

下表包含 **power on**、**power off** 和 **power cycle** 命令的选项。

表 14. power 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

表 14. power 命令 （续）

选项	描述	值
-s	使用此选项可先关闭操作系统，然后关闭服务器。 **注**：对 **power off** 和 **power cycle** 命令使用 **-every** 选项时暗含 **-s** 选项。	
-every	此选项与 **power on**、**power off** 和 **power cycle** 命令配合使用可控制服务器电源。您可以设置打开、关闭服务器电源或关闭再打开服务器电源的日期、时间和频率（每日或每周）。	**注**：由于空间限制，此选项的值显示为单独几行。 **Sun|Mon|Tue|Wed|Thu|** **Fri|Sat|Day|clear**
-t	使用此选项可指定打开服务器电源、关闭操作系统、关闭服务器电源以及重新启动服务器的时间（单位：小时和分钟）。	使用以下格式：**hh:mm**
-d	使用此选项可指定打开服务器电源的日期。这是 **power on** 命令的补充选项。 **注**：不能对同一个命令同时使用 **-d** 和 **-every** 选项。	使用以下格式：**mm/dd/yyyy**
-clear	使用此选项可清除安排的打开电源日期。这是 **power on** 命令的补充选项。	

语法：

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

以下信息是 **power** 命令的示例。

要在每周日 **1:30** 关闭操作系统和关闭服务器，请输入以下命令：

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

要在每天 **1:30** 关闭操作系统并重新启动服务器，请输入以下命令：

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

要在每周一 **1:30** 打开服务器电源，请输入以下命令：

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

要在 **2013** 年 **12** 月 **31** 日下午 **11:30** 打开服务器电源，请输入以下命令：

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

要清除每周关闭再打开电源操作，请输入以下命令：

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

reset 命令

此命令描述如何重置服务器电源。

使用 **reset** 命令来重新启动服务器。要使用此命令，您必须拥有电源和重新启动访问权限。

下表显示选项的参数。

表 15. reset 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-s	重置服务器前，关闭操作系统。	
-d	将重置的执行延迟给定的秒数。	**0 - 120**
-nmi	在服务器上生成不可屏蔽的中断（NMI）。	

语法：

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

fuelg 命令

此命令显示有关服务器电源的信息。

使用 **fuelg** 命令显示有关服务器电源使用情况的信息以及配置服务器电源管理。此命令还配置应对失去电源冗余的策略。下表显示选项的参数。

表 16. fuelg 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-pme	在服务器上启用或禁用电源管理和功率上限。	**on** 和 **off**
-pcap-mode	设置服务器的功率上限模式。	**input** 和 **output**
-pcap	对目标运行没有任何选项的 **fuelg** 命令时显示的一个在功率上限值范围内的数值。	瓦数值
-history	显示功耗或性能历史记录	**pc** 和 **perf**
-period	显示历史记录的数值（**1**、**6**、**12**、**24** 小时）	以小时为单位的数值
-pm	设置应对失去冗余电源的策略模式。	• **bt** - 基本含调速 • **rt** - 冗余含调速（默认） • **ort** - **N_1** 冗余含调速
-zm	启用或禁用零输出模式。仅当策略模式设置为冗余含调速时，才能配置此设置。	**on** 和 **off**

表 16. fuelg 命令 （续）

选项	描述	值
-perf	显示当前计算利用率，包括系统、微处理器和 I/O。	百分比
-pc	显示当前功耗	• **output** - 显示当前直流功耗。对于机架和塔式服务器，它将包括系统、CPU、内存和其他组件的功耗；对于 ITE 刀片服务器，它将仅包含系统功耗。 • **input** - 显示当前输入功耗，包括系统功耗。

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

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

pxeboot 命令

此命令可显示并设置预启动执行环境的条件。

在无任何选项的情况下运行 **pxeboot** 将返回当前预启动执行环境设置。下表显示选项的参数。

表 17. pxeboot 命令

下表是一个单行三列表格，包含选项、选项描述和关联值的信息。

选项	描述	值
-en	设置下次系统重新启动时的预启动执行环境条件。	**enabled**、**disabled**

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

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

串口重定向命令

本主题包含串口重定向命令。

仅有一条串口重定向命令：第 109 页 “console 命令”。

console 命令

此命令用于启动串口重定向控制台会话。

使用 **console** 命令可对 **IMM** 指定的串口启动串口重定向控制台会话。

语法：

```
console 1
```

配置命令

本主题按字母顺序提供配置 **CLI** 命令的列表。

当前有 **41** 条配置命令：

accseccfg 命令

使用此命令可显示并配置帐户安全设置。

在无任何选项的情况下运行 **accseccfg** 命令将显示所有帐户安全信息。下表显示选项的参数。

表 18. accseccfg 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-am	设置用户认证方法。	**local**、**ldap**、**localldap** 和 **ldaplocal**
-lp	达到最大登录失败次数之后的锁定期（分钟数）。	介于 **0** 和 **2880** 之间，**0** = 锁定期不会到期
-pe	密码到期时间段（天数）。	介于 **0** 和 **365** 之间，**0** = 永不到期
-pew	密码到期警告时间段 **注**：密码到期警告时间段必须短于密码到期时间段。	介于 **0** 和 **30** 之间，**0** = 永不警告
-pc	密码复杂性规则启用状态。	**on** 和 **off**
-pl	密码长度。	如果启用了密码复杂性规则，则密码长度介于 **8** 和 **32** 之间。否则，密码长度介于 **0** 和 **32** 之间。
-ci	最短密码更改时间间隔（小时数）。	介于 **0** 和 **240** 之间，**0** = 立即更改
-lf	登录失败最大次数。	介于 **0** 和 **10** 之间，**0** = 永不锁定
-chgnew	首次登录后更改新用户密码。	**on** 和 **off**

表 18. accseccfg 命令 （续）

选项	描述	值
-rc	密码重新使用周期。	介于 **0** 和 **10** 之间，**0** = 立即重用
-wt	**Web** 和 **Secure Shell** 非活动会话超时（分钟）。	介于 **0** 和 **1440** 之间

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

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

alertcfg 命令

使用此命令可显示并配置 **IMM** 全局远程警报参数。

在无任何选项的情况下运行 **alertcfg** 命令将显示所有全局远程警报参数。下表显示选项的参数。

表 19. alertcfg 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

表 19. alertcfg 命令 （续）

选项	描述	值
-dr	设置 **IMM** 重新发送警报之前两次重试之间的等待时间。	**0** 到 **4.0** 分钟，按 **0.5** 分钟递增
-da	设置 **IMM** 向列表中的下一接收方发送警报之前的等待时间。	**0** 到 **4.0** 分钟，按 **0.5** 分钟递增
-rl	设置在先前尝试未成功的情况下，**IMM** 额外尝试发送警报的次数。	**0** 到 **8**

语法：

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

示例：

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

asu 命令

此命令用于配置 **UEFI** 设置。

Advanced Settings Utility 命令（**ASU**）用于配置 **UEFI** 设置。必须重新启动主机系统，任何 **UEFI** 设置更改才能生效。

下表包含可与 **asu** 命令结合使用的一部分命令。

表 20. asu 命令

下表是一个多行三列的表格，由可与 **asu** 命令结合使用的一部分命令组成。其中提供这些命令的描述性信息和关联的值。

命令	描述	值
delete	使用此命令删除设置的实例或记录。该设置必须是允许删除的实例，例如 **iSCSI.AttemptName.1**。	*设置实例*
帮助	使用此命令显示一个或多个设置的帮助信息。	*设置*

表 20. asu 命令 （续）

命令	描述	值
set	使用此命令更改设置的值。将 **UEFI** 设置设为所输入的值。 **注：** • 设置一个或多个设置/值对。 • 如果设置扩展为单一设置，则它可包含通配符。 • 如果值包含空格，则必须用引号引起该值。 • 有序列表值以等号（=）进行分隔。例如，**set B*.Bootorder "CD/DVD Rom=Hard Disk 0=PXE Network"**。	*设置值*
showgroups	使用此命令显示可用的设置组。此命令显示已知组的名称。组名称可能因所安装的设备而异。	*设置*
show	使用此命令显示一个或多个设置当前的值。	*设置*
showvalues	使用此命令显示一个或多个设置所有可取的值。 **注：** • 此命令将显示有关允许设置使用的值的信息。 • 其中显示允许设置使用的最小和最大实例数。 • 如有默认值，则将显示默认值。 • 用左右尖括号（< 和 >）括起默认值。 • 文本值显示最小和最大长度以及正则表达式。	*设置*
注： • 在命令语法中，*设置* 为要查看或更改的设置的名称，*值* 为赋给该设置的值。 • *设置* 可以是多个名称，但使用 **set** 命令时除外。 • *设置* 可包含通配符，例如，星号（*）或问号（?）。 • *设置* 可以是组、设置名称或 **all**。		

以下列表中举出 **asu** 命令语法的示例：

- 要显示所有 **asu** 命令选项，请输入 `asu --help`。
- 要显示所有命令的详细帮助，请输入 `asu -v --help`。
- 要显示一个命令的详细帮助，请输入 `asu -v set --help`。
- 要更改值，请输入 `asu set setting value`。
- 要显示当前的值，请输入 `asu show setting`。
- 要以长批处理格式显示设置，请输入 `asu show -l -b all`
- 要显示某个设置可取的所有值，请输入 `asu showvalues setting`。**show values** 命令示例：

```
system> asu showvalues S*.POST*
SystemRecovery.POSTWatchdogTimer==<Disable>=Enable
SystemRecovery.POSTWatchdogTimerValue=numeric min=5 max=20 step=1 default=5
system>
```

下表显示选项的参数。

表 21. asu 选项

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-b	以批处理格式显示。	
--help[1]	显示命令用法和选项。**--help** 选项置于命令前，例如 **asu --help show**。	
--help[1]	显示命令的帮助。**--help** 选项置于命令后，例如 **asu show --help**。	
-l	长格式设置名称（包括配置集）。	
-m	混合格式设置名称（使用配置标识）。	
-v[2]	详细输出。	

1. **--help** 选项可与任何命令结合使用。
2. 仅在 **asu** 与命令之间使用 **-v** 选项。

语法：

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

注：有关更多命令选项，请参阅个别命令。

使用 **asu** 事务命令设置多个 **UEFI** 设置以及创建和执行批处理模式命令。使用 **tropen** 和 **trset** 命令创建一个事务文件，其中包含多个要应用的设置。使用 **tropen** 命令打开具有给定标识的事务。使用 **trset** 命令将设置添加到集合。使用 **trcommit** 命令提交已完成的事务。事务执行完毕时，可使用 **trrm** 命令删除它。

注：恢复 **UEFI** 设置的操作将产生一个事务，其标识使用随机的三位数。

下表包含可与 **asu** 命令结合使用的事务命令。

表 22. asu 事务命令

下表是一个多行三列的表格，由事务命令、命令描述以及与命令关联的值组成。

命令	描述	值
tropen ***id***	此命令创建一个新事务文件，其中包含要设置的若干设置。	***id*** 为 **1** 至 **3** 个字母数字字符的标识字符串。
trset ***id***	此命令将一个或多个设置或值对添加到事务。	***id*** 为 **1** 至 **3** 个字母数字字符的标识字符串。

表 22. asu 事务命令 （续）

命令	描述	值
trlist *id*	此命令首先显示事务文件的内容。在 **CLI shell** 中创建事务文件时，这一点可能很有用。	*id* 为 **1** 至 **3** 个字母数字字符的标识字符串。
trcommit *id*	此命令提交并执行事务文件的内容。随后将显示执行结果和任何错误。	*id* 为 **1** 至 **3** 个字母数字字符的标识字符串。
trrm *id*	此命令在提交事务文件后删除它。	*id* 为 **1** 至 **3** 个字母数字字符的标识字符串。

建立多个 **UEFI** 设置的示例：

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

backup 命令

使用此命令可生成包含当前系统安全设置的备份文件。

下表显示选项的参数。

表 23. backup 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-f	备份文件名	有效文件名
-pp	用于加密备份文件内密码的密码或口令	有效密码或以引号分隔的口令
-ip	**TFTP/SFTP** 服务器的 **IP** 地址	有效的 **IP** 地址
-pn	**TFTP/SFTP** 服务器的端口号	有效端口号（默认值为 **69/22**）
-u	**SFTP** 服务器的用户名	有效用户名
-pw	**SFTP** 服务器的密码	有效密码
-fd	备份 **CLI** 命令的 **XML** 描述的文件名	有效文件名

语法：

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

示例：

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

dhcpinfo 命令

使用此命令查看 DHCP 服务器 为 **eth0** 分配的 IP 配置。

使用 **dhcpinfo** 命令可查看 DHCP 服务器为 **eth0** 分配的 IP 配置（如果该接口由 DHCP 服务器自动配置）。您可使用 **ifconfig** 命令来启用或禁用 DHCP。

语法：

```
dhcpinfo eth0
```

Example:

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

下表描述了该示例的输出。

表 24. dhcpinfo 命令

下表是一个多行两列表格，描述以上示例中使用的选项。

选项	描述
-server	分配配置的 DHCP 服务器
-n	分配的主机名
-i	分配的 IPv4 地址

表 24. dhcpinfo 命令 （续）

选项	描述
-g	分配的网关地址
-s	分配的子网掩码
-d	分配的域名
-dns1	主 **IPv4 DNS** 服务器 **IP** 地址
-dns2	辅助 **IPv4 DNS IP** 地址
-dns3	第三 **IPv4 DNS** 服务器 **IP** 地址
-i6	**IPv6** 地址
-d6	**IPv6** 域名
-dns61	主 **IPv6 DNS** 服务器 **IP** 地址
-dns62	辅助 **IPv6 DNS IP** 地址
-dns63	第三 **IPv6 DNS** 服务器 **IP** 地址

dns 命令

使用此命令可查看并设置 **IMM** 的 **DNS** 配置。

注：在 **Flex System** 中，无法在 **IMM** 上修改 **DNS** 设置。**DNS** 设置由 **CMM** 管理。

在无任何选项的情况下运行 **dns** 命令将显示所有 **DNS** 配置信息。下表显示选项的参数。

表 25. dns 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-state	**DNS** 状态	**on** 和 **off**
-ddns	**DDNS** 状态	**enabled**、**disabled**
-i1	主 **IPv4 DNS** 服务器 **IP** 地址	采用点分十进制 **IP** 地址格式的 **IP** 地址。
-i2	辅助 **IPv4 DNS IP** 地址	采用点分十进制 **IP** 地址格式的 **IP** 地址。
-i3	第三 **IPv4 DNS** 服务器 **IP** 地址	采用点分十进制 **IP** 地址格式的 **IP** 地址。
-i61	主 **IPv6 DNS** 服务器 **IP** 地址	采用 **IPv6** 格式的 **IP** 地址。
-i62	辅助 **IPv6 DNS IP** 地址	采用 **IPv6** 格式的 **IP** 地址。
-i63	第三 **IPv6 DNS** 服务器 **IP** 地址	采用 **IPv6** 格式的 **IP** 地址。
-p	**IPv4/IPv6** 优先级	**ipv4** 或 **ipv6**

语法：

```
dns [options]
option:
 -state state
 -ddns state
```

-i1 *first_ipv4_ip_address*
-i2 *second_ipv4_ip_address*
-i3 *third_ipv4_ip_address*
-i61 *first_ipv6_ip_address*
-i62 *second_ipv6_ip_address*
-i63 *third_ipv6_ip_address*
-p *priority*

注：以下示例显示了禁用 DNS 时的 IMM 配置。

示例：

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

system>
```

下表描述以上示例中使用的选项。

表 26. dns 命令输出

下表是一个多行两列表格，描述以上示例中使用的选项。

选项	描述
-state	DNS 状态（on 或 off）
-i1	主 IPv4 DNS 服务器 IP 地址
-i2	辅助 IPv4 DNS IP 地址
-i3	第三 IPv4 DNS 服务器 IP 地址
-i61	主 IPv6 DNS 服务器 IP 地址
-i62	辅助 IPv6 DNS IP 地址
-i63	第三 IPv6 DNS 服务器 IP 地址
-ddns	DDNS 状态（enabled 或 disabled）
-dnsrc	首选 DDNS 域名（dhcp 或 manual）
-ddn	手动指定的 DDN
-ddncur	当前 DDN（只读）
-p	首选 DNS 服务器（ipv4 或 ipv6）

encaps 命令

使用此命令可让 BMC 退出 Encapsulation 模式。

下表显示选项的参数。

表 27. encaps 命令

下表是一个单行两列的表格，由选项和选项描述组成。

选项	描述
lite off	让 **BMC** 退出 **Encapsulation** 模式并打开对所有用户的全局访问权限

ethtousb 命令

使用 **ethtousb** 命令可显示并配置 **Ethernet - Ethernet over USB** 端口映射。

该命令允许您将外部以太网端口号映射到不同的 **Ethernet-over-USB** 端口号。

在无任何选项的情况下运行 **ethtousb** 命令将显示 **Ethernet-over-USB** 信息。下表显示选项的参数。

表 28. ethtousb 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-en	**Ethernet-over-USB** 状态	**enabled**、**disabled**
-m*x*	配置索引 ***x*** 的端口映射	以英文冒号（:）分隔的端口对，格式为 ***port1*:*port2*** 其中： • 端口索引号 ***x*** 在命令选项中指定为 **1** 到 **10** 之间的整数。 • 端口对的 ***port1*** 是外部以太网端口号。 • 端口对的 ***port2*** 是 **Ethernet-over-USB** 端口号。
-rm	删除指定索引的端口映射	**1** 到 **10** 通过在无任何选项的情况下使用 **ethtousb** 命令可显示端口映射索引。

语法：

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

示例：

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

firewall 命令

使用此命令可将防火墙配置为限制来自某些地址的访问，并可以选择限制访问时间范围。如果未指定任何选项，将显示当前设置。

下表显示选项的参数。

表 29. firewall 命令

下表是一个多行三列表，包含选项和选项描述。

选项	描述	值
-bips	阻止 **1-3** 个 **IP** 地址（以逗号分隔、**CIDR** 或范围）	有效的 **IP** 地址 **注：IPv4** 和 **IPv6** 地址可以使用 **CIDR** 格式来阻止一系列地址。
-bmacs	阻止 **1-3** 个 **MAC** 地址（以逗号分隔）	有效的 **MAC** 地址 **注：MAC** 地址筛选仅适用于特定的地址。
-bbd	阻止开始日期	格式为 **<YYYY-MM-DD>** 的日期
-bed	阻止结束日期	格式为 **<YYYY-MM-DD>** 的日期
-bbt	阻止开始时间	格式为 **<HH:MM>** 的时间
-bet	阻止结束时间	格式为 **<HH:MM>** 的时间
-bti	阻止 **1-3** 个时间间隔（以逗号分隔） 例如，***firewall - bti 01:00–02:00,05:05–10:30*** 每天都会在 **01:00-02:00** 和 **05:05-10:30** 期间阻止访问	格式为 **<HH:MM-HH:MM>** 的时间范围
-clr	清除给定类型的防火墙规则	**ip**、**mac**、**datetime**、**interval**、**all**
以下选项用于 **IP** 地址阻止		
-iplp	**IP** 地址锁定期（以分钟为单位）。	介于 **0** 和 **2880** 之间的数值，**0** = 永不到期
-iplf	**IP** 地址被锁定之前的最大登录失败次数。 **注：**如果此值不为 **0**，那么它必须大于或等于通过 ***<accseccfg -lf>*** 设置的 **<最大登录失败次数>**	介于 **0** 和 **32** 之间的数值，**0** = 永不锁定
-ipbl	显示/配置被锁定的 **IP** 地址列表。	**del**、**clrall**、**show** • **-del：**从阻止列表中删除 **IPv4** 或 **IPv6** 地址 • **-clrall：**清除所有阻止 **IP** • **-show：**显示所有阻止 **IP**

示例：

· “firewall”: Show all options’ value and IP addresses blocking list.
· “firewall -bips 192.168.1.1,192.168.1.0/24,192.168.1.1-192.168.1.5”: Block the access from multi IPs
· “firewall -bti 01:00-02:00,05:05-10:30,14:15-20:00”: Block all access during 01:00-02:00,05:05-10:30,14:15-20:00 every day.

· “firewall –clr all”: Clear all rules of “Block List and Time Restriction”.
· “firewall -iplp 60”:Set IP address lockout period to 60 minutes.
· “firewall -iplf 5”:Set maximum number of login failures to 5 timesi.
· “firewall -ipbl -del 192.168.100.1”:Delete 192.168.100.1 from IP address blocking list.
· “firewall –ipbl -del 3fcc:1234::2”:Delete 3fcc:1234::2 from IP address blocking list.
· “firewall –ipbl –clrall”: Delete all blocking IP addresses.
· “firewall –ipbl –show”: Show all blocking IP addresses.

gprofile 命令

使用此命令可显示和配置 **IMM** 的组概要文件。

下表显示选项的参数。

表 30. gprofile 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-clear	删除组	**enabled**、**disabled**
-n	该组的名称	***group_name*** 字符串，最长为 **63** 个字符。 ***group_name*** 必须唯一。
-a	基于角色的权限级别	**supervisor**、**operator**、**rbs** <角色列表>: **nsc**|**am**|**rca**|**rcvma**|**pr**|**bc**|**cel**|**ac** 使用竖线分隔的值列表指定角色列表值。
-h	显示命令用法和选项	

语法：

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

hashpw 命令

将此命令与 **-sw** 选项一起使用可启用/禁用第三方密码功能，或者与**-re** 选项一起使用可启用/禁用允许检索第三方密码的功能。

下表显示选项的参数。

表 31. hashpw 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

表 31. hashpw 命令 （续）

选项	描述	值
-sw	第三方密码开关状态	**enabled、disabled**
-re	第三方密码读取状态 **注：**如果启用了开关，则可以设置读取。	**enabled、disabled**

示例：

```
system> hashpw -sw enabled -re enabled
system> users -5 -n guest5 -shp ef92b778bafe771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f - r Administrator
system> users -5 ghp
ef92b778bafe771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f
system> users
Account    Login ID    Advanced Attribute         Role       Password Expires
-------    --------    ------------------       ------       ----------------
  1       USERID          Native           Administrator    Password doesn't expire
5       guest5   Third-party Password        Administrator          90 day(s)
```

ifconfig 命令

使用此命令可配置以太网接口。

输入 ifconfig eth0 可显示当前以太网接口配置。要更改以太网接口配置，请输入选项，其后跟值。要更改接口配置，您必须至少具有适配器网络和安全性配置权限。

注：在 **Flex System** 中，**VLAN** 设置由 **Flex System CMM** 管理，而无法在 **IMM** 上修改。

下表显示选项的参数。

表 32. ifconfig 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-b	固化 **MAC** 地址（只读且不可配置）	
-state	接口状态	**disabled** 和 **enabled**
-c	配置方法	**dhcp**、**static** 和 **dthens**（**dthens** 与 **Web** 界面上的 **try dhcp server, if it fails use static config** 选项对应）
-i	静态 **IP** 地址	有效格式的地址。
-g	网关地址	有效格式的地址。
-s	子网掩码	有效格式的地址。
-n	主机名	最多包含 **63** 个字符的字符串。该字符串可以包括字母、数字、句点、下划线和连字符。
-r	数据速率	**10**、**100** 和 **auto**
-d	双工方式	**full**、**half** 和 **auto**

表 32. ifconfig 命令 （续）

选项	描述	值
-m	**MTU**	**60** 和 **1500** 之间的数字。
-l	**LAA**	**MAC** 地址格式。不允许多播地址（第一个字节必须是偶数）。
-dn	域名	有效格式的域名。
-auto	自动协商设置，它决定数据速率和双工网络设置是否可配置。	**true** 和 **false**
-ghn	从 **DHCP** 获取主机名	**disabled** 和 **enabled**
-nic	切换 **NIC** 模式[1]	**shared**、**dedicated** 和 **shared:nixX**[2]
-failover[2]	故障转移模式	**none**、**shared** 和 **shared:nicX**
-nssync[3]	网络设置同步	**enabled**、**disabled**
-address_table	自动生成的 **IPv6** 地址及其前缀长度的表 **注**：仅当启用 **IPv6** 和无状态自动配置时，此选项才可见。	此值为只读且不可配置。
-ipv6	**IPv6** 状态	**disabled** 和 **enabled**
-lla	链路本地地址 **注**：仅当启用 **IPv6** 时，才会显示链路本地地址。	链路本地地址由 **IMM** 确定。此值为只读且不可配置。
-ipv6static	静态 **IPv6** 状态	**disabled** 和 **enabled**
-i6	静态 **IP** 地址	以太网通道 **0** 的静态 **IP** 地址（**IPv6** 格式）。
-p6	地址前缀长度	**1** 到 **128** 之间的数值。
-g6	网关或默认路由	以太网通道 **0** 的网关或默认路由的 **IP** 地址（**IPv6** 格式）。
-dhcp6	**DHCPv6** 状态	**enabled**、**disabled**
-sa6	**IPv6** 无状态自动配置状态	**enabled**、**disabled**
-vlan	启用或禁用 **VLAN** 标记	**enabled**、**disabled**
-vlanid	**IMM** 的网络数据包标识标记	**1** 到 **4094** 之间的数值。

注：

1. **-nic** 还将显示 **nic** 的状态。**[active]** 指示当前正在使用哪个 **nic XCC**

   例如：

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

   指示 **nic3** 在插槽 **5** 上处于共享模式，**nic2** 位于插槽 **3** 上，**nic1** 是 **XCC** 专用端口，**XCC** 正在使用 **nic3**。
2. 可在安装了可选夹层网卡的服务器上使用 **shared:nicX** 值。**IMM** 可使用此夹层网卡。
3. 如果将 **IMM** 配置为使用专用管理网络端口，那么 **-failover** 选项将指示 **IMM** 在专用端口断开连接的情况下切换到共享网络端口。
4. 如果启用了故障转移模式，那么 **-nssync** 选项将指示 **IMM** 对共享网络端口使用在专用管理网络端口上使用的相同网络设置。

语法：

```
ifconfig eth0 [options]
options:

 -state interface_state
 -c config_method
 -i static_ipv4_ip_address
 -g ipv4_gateway_address
 -s subnet_mask
 -n hostname
 -r data_rate
 -d duplex_mode
 -m max_transmission_unit
 -l locally_administered_MAC
 -b burned_in_MAC_address
 -dn domain_name
 -auto state
 -nic state
 -failover mode
 -nssync state
 -address_table
 -lla ipv6_link_local_addr
 -dhcp6 state
 -ipv6 state
 -ipv6static state
 -sa6 state
 -i6 static_ipv6_ip_address
 -g6 ipv6_gateway_address
 -p6 length
 -vlan state
  -vlanid VLAN ID
```

示例：

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

```
   nic3: ext card slot #5 [active]
-address_table   :

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

keycfg 命令

使用此命令可显示、添加或删除激活密钥。

激活密钥控制对可选 **IMM** 功能的访问权限。

注：

- 运行不带任何选项的 **keycfg** 命令时，将会显示已安装的激活密钥列表。显示的密钥信息包括每个激活密钥的索引号、激活密钥的类型、密钥的有效期、剩余使用次数、密钥状态和密钥描述。
- 通过文件传输添加新激活密钥。
- 通过指定密钥数或密钥类型删除旧密钥。按类型删除密钥时，仅会删除给定类型的第一个密钥。

下表显示选项的参数。

表 33. keycfg 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-add	添加激活密钥	**-ip**、**-pn**、**-u**、**-pw** 和 **-f** 命令选项的值
-ip	具有要添加的激活密钥的 **TFTP** 服务器的 **IP** 地址	**TFTP** 服务器的有效 **IP** 地址
-pn	具有要添加的激活密钥的 **TFTP/SFTP** 服务器的端口号	**TFTP/SFTP** 服务器的有效端口号（默认值 **69/22**）
-u	具有要添加的激活密钥的 **SFTP** 服务器的用户名	**SFTP** 服务器的有效用户名
-pw	具有要添加的激活密钥的 **SFTP** 服务器的密码	**SFTP** 服务器的有效密码
-f	要添加的激活密钥的文件名	激活密钥文件的有效文件名
-del	按索引号删除激活密钥	**keycfg** 列表中的有效激活密钥索引号
-deltype	按密钥类型删除激活密钥	有效密钥类型值

语法：

```
keycfg [options]
option:
 -add
   -ip tftp/sftp server ip address
   -pn pn port number of tftp/sftp server (default 69/22)
   -u  username for sftp server
   -pw password for sftp server
```

```
  -f filename
  -del  n ( where n is a valid ID number from listing)
  -deltype x ( where x is a Type value)
```

示例：

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

注：标识号 **3** 的**描述**字段因空间限制显示为单独几行。

ldap 命令

使用此命令可显示并配置 **LDAP** 协议配置参数。

下表显示选项的参数。

表 34. ldap 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-a	用户认证方法	**local only**、**LDAP only**、**local first then LDAP** 和 **LDAP first then local**
-aom	仅认证模式	**enabled**、**disabled**
-b	绑定方法	**anonymous**、**bind with ClientDN and password** 和 **bind with Login Credential**
-c	客户端可分辨名称	针对 ***client_dn*** 的字符串，最多包含 **127** 个字符
-d	搜索域	针对 ***search_domain*** 的字符串，最多包含 **63** 个字符
-f	组筛选条件	针对 ***group_filter*** 的字符串，最多包含 **127** 个字符
-fn	林名称	针对 **Active Directory** 环境。最多包含 **127** 个字符的字符串。
-g	组搜索属性	针对 ***group_search_attr*** 的字符串，最多包含 **63** 个字符
-l	登录权限属性	针对 ***string*** 的字符串，最多包含 **63** 个字符
-p	客户机密码	针对 ***client_pw*** 的字符串，最多包含 **15** 个字符
-pc	确认客户端密码	针对 ***confirm_pw*** 的字符串，最多包含 **15** 个字符 命令用法为：**ldap -p** ***client_pw*** **-pc** ***confirm_pw*** 当您更改客户端密码时，此选项是必需的。该选项将 ***confirm_pw*** 参数与 ***client_pw*** 参数进行比较。如果这两个参数不匹配，该命令将失败。
-ep	加密密码	备份/恢复密码（仅限内部使用）
-r	根条目可分辨名称（**DN**）	针对 ***root_dn*** 的字符串，最多包含 **127** 个字符
-rbs	**Active Directory** 用户基于角色的增强型安全性	**enabled**、**disabled**

表 34. ldap 命令 （续）

选项	描述	值
-s1ip	服务器 **1** 主机名/IP 地址	针对 ***host name/ip_addr*** 的字符串，最多包含 **127** 个字符
-s2ip	服务器 **2** 主机名/IP 地址	针对 ***host name/ip_addr*** 的字符串，最多包含 **127** 个字符
-s3ip	服务器 **3** 主机名/IP 地址	针对 ***host name/ip_addr*** 的字符串，最多包含 **127** 个字符
-s4ip	服务器 **4** 主机名/IP 地址	针对 ***host name/ip_addr*** 的字符串，最多包含 **127** 个字符
-s1pn	服务器 **1** 端口号	针对 ***port_number*** 的数字端口号，最多包含 **5** 位数
-s2pn	服务器 **2** 端口号	针对 ***port_number*** 的数字端口号，最多包含 **5** 位数
-s3pn	服务器 **3** 端口号	针对 ***port_number*** 的数字端口号，最多包含 **5** 位数
-s4pn	服务器 **4** 端口号	针对 ***port_number*** 的数字端口号，最多包含 **5** 位数
-t	服务器目标名称	启用 **rbs** 选项后，此字段指定可通过基于角色的安全性（**RBS**）管理单元与 **Active Directory** 服务器上的一个或多个角色相关联的目标名称。
-u	**UID** 搜索属性	针对 ***search_attrib*** 的字符串，最多包含 **63** 个字符
-v	通过 **DNS** 获取 **LDAP** 服务器地址	**off** 或 **on**
-h	显示命令用法和选项	

语法：

```
ldap [options]
options:
  -a loc|ldap|locld|ldloc
  -aom enable/disabled
  -b anon|client|login
  -c client_dn
  -d search_domain
  -f group_filter
  -fn forest_name
  -g group_search_attr
  -l string
  -p client_pw
  -pc confirm_pw
  -ep encrypted_pw
  -r root_dn
  -rbs enable|disabled
  -s1ip host name/ip_addr
  -s2ip host name/ip_addr
  -s3ip host name/ip_addr
  -s4ip host name/ip_addr
  -s1pn port_number
  -s2pn port_number
  -s3pn port_number
  -s4pn port_number
  -t name
  -u search_attrib
  -v off|on
   -h
```

ntp 命令

使用此命令可显示并配置网络时间协议（NTP）。

下表显示选项的参数。

表 35. ntp 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-en	启用或禁用网络时间协议。	**enabled**、**disabled**
-i[1]	网络时间协议服务器的名称或 IP 地址。这是网络时间协议服务器的索引号。	要用于时钟同步的 NTP 服务器的名称。NTP 服务器的索引号范围是 **-i1** 到 **-i4**。
-f	IMM 时钟与网络时间协议服务器同步的频率（以分钟为单位）。	**3** 到 **1440** 分钟
-synch	请求立即与网络时间协议服务器同步。	没有与此参数配合使用的值。
1. -i 与 **i1** 相同。		

语法：

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

示例：

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

portcfg 命令

使用此命令可针对串口重定向功能配置 IMM。

必须将 IMM 配置为与服务器内部串口设置相匹配。要更改串口配置，请输入选项，其后跟值。要更改串口配置，您必须至少具有适配器网络和安全性配置权限。

注：服务器外部串口只能由 IMM 用于 IPMI 功能。不通过串口支持 CLI。不支持在 Remote Supervisor Adapter II CLI 中出现的 **serred** 和 **cliauth** 选项。

在无任何选项的情况下运行 **portcfg** 命令将显示串口配置。下表显示选项的参数。

注：数据位数（**8**）是在硬件中设置的，不能更改。

表 36. portcfg 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

表 36. portcfg 命令 （续）

选项	描述	值
-b	波特率	**9600, 19200, 38400, 57600, 115200**
-p	奇偶校验	**none**、**odd** 和 **even**
-s	停止位	**1, 2**
-climode	**CLI** 方式	**0, 1, 2** 其中： • **0 = none**：禁用 **CLI** • **1 = cliems**：启用 **CLI**，使用与 **EMS** 兼容的按键序列 • **2 = cliuser**：启用 **CLI**，使用用户定义的按键序列

语法：

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

示例：

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

portcontrol 命令

使用此命令开启或关闭网络服务端口。

当前，此命令仅支持控制 **IPMI** 协议的端口。输入 **portcontrol** 以显示 **IPMI** 端口状态。要启用或禁用 **IPMI** 网络端口，请输入 **-ipmi** 选项后接 **on** 或 **off** 值。

表 37. portcontrol 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-all	启用或禁用所有接口和发现协议	**on** 和 **off**
-cim	启用或禁用 **CIM** 发现	**on** 和 **off**
-ipmi	启用或禁用通过 **LAN** 进行的 **IPMI** 访问	**on** 和 **off**
-ipmi-kcs	启用或禁用从服务器进行的 **IPMI** 访问	**on** 和 **off**

表 37. portcontrol 命令 （续）

选项	描述	值
-rest	启用或禁用 **REST** 发现	**on** 和 **off**
-slp	启用或禁用 **SLP** 发现	**on** 和 **off**
-snmp	启用或禁用 **SNMP** 发现	**on** 和 **off**
-ssdp	启用或禁用 **SSDP** 发现	**on** 和 **off**
-cli	启用或禁用 **CLI** 发现	**on** 和 **off**
-web	启用或禁用 **WEB** 发现	**on** 和 **off**

语法：

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

示例：

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

ports 命令

使用此命令可显示和配置 **IMM** 端口。

运行不带任何选项的 **ports** 命令将显示所有 **IMM** 端口的信息。下表显示选项的参数。

表 38. ports 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-open	显示打开的端口	
-reset	将端口重置为默认设置	
-httpp	**HTTP** 端口号	默认端口号：**80**
-httpsp	**HTTPS** 端口号	默认端口号：**443**
-sshp	**SSH legacy CLI** 端口号	默认端口号：**22**
-snmpap	**SNMP** 代理端口号	默认端口号：**161**
-snmptp	**SNMP** 陷阱端口号	默认端口号：**162**
-rpp	远程呈现端口号	默认端口号：**3900**

表 38. ports 命令 （续）

选项	描述	值
-cimhp	**CIM over HTTP 端口号**	默认端口号：**5988**
-cimhsp	**CIM over HTTPS 端口号**	默认端口号：**5989**

语法：

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

示例：

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

rdmount 命令

使用此命令可装载远程磁盘映像或网络共享

下表显示选项的参数。

表 39. rdmount 命令

下表是一个多行两列的表格，由选项和选项描述组成。

注：

- 最多可向 **XClarity Controller** 内存上传两个文件，并使用 **XClarity Controller RDOC** 功能将其作为虚拟介质装载。两个文件的总大小不能超过 **50 MB**。除非使用 **–rw** 选项，否则上传的映像为只读。
- 使用 **HTTP**、**SFTP** 或 **FTP** 协议装载或映射映像时，所有映像的总大小不得超过 **50 MB**。如果使用 **NFS** 或 **SAMBA** 协议，则不限制大小。

表 39. rdmount 命令 （续）

选项	描述
-r	**rdoc** 操作（如果使用，则必须为第一个选项） **-r -map**：装载 **RDOC** 映像 **-r -unmap**<文件名>：卸载装载的 **RDOC** 映像 **-r -maplist**：显示通过 **XClarity Controller Web** 浏览器和 **CLI** 界面装载的 **RDOC** 映像
-map	**-t <samba|nfs|http|sftp|ftp>** 文件系统类型 **-ro** 只读 **-rw** 读写 **-u** 用户 **-p password** **-l** 文件位置（**URL** 格式） **-o** 选项（**samba** 和 **nfs** 装载的额外选项字符串） **-d** 域（**samba** 装载的域）
-maplist	显示映射的映像
-unmap <id|fname>	对网络映像使用 **id**，对 **rdoc** 则使用文件名
-mount	装载映射的映像
-unmount	卸载装载的映像

restore 命令

使用此命令从备份文件中恢复系统设置。

下表显示选项的参数。

表 40. restore 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-f	备份文件名	有效文件名
-pp	用于加密备份文件内密码的密码或口令	有效密码或以引号分隔的口令
-ip	**TFTP/SFTP** 服务器的 **IP** 地址	有效的 **IP** 地址
-pn	**TFTP/SFTP** 服务器的端口号	有效端口号（默认值为 **69/22**）
-u	**SFTP** 服务器的用户名	有效用户名
-pw	**SFTP** 服务器的密码	有效密码

语法：
```
restore [options]
option:
 -f filename
 -pp password
 -ip ip_address
 -pn port_number
 -u username
  -pw password
```

示例：
```
system> restore f xcc-back.cli pp xxxxxx ip 192.168.70.200
ok
system>
```

restoredefaults 命令

使用此命令可将所有 IMM 设置恢复为出厂默认值。

- **restoredefaults** 命令没有选项。
- 在继续执行之前，将要求您确认该命令。

语法：
```
restoredefaults
```

示例：
```
system> restoredefaults

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

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

Proceed? (y/n)
Y
Restoring defaults
```

roles 命令

使用此命令可显示或配置角色。

下表显示选项的参数。

表 41. roles 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

表 41. roles 命令 （续）

选项	描述	值
-n	要配置的角色	限制为 **32** 个字符
-p	设置权限	定制：**am**|**rca**|**rcvma**|**pr**|**cel**|**bc**|**nsc**|**ac**|**us** • **am**：用户帐户管理访问 • **rca**：远程控制台访问权限 • **rcvma**：远程控制台和远程磁盘（虚拟介质）访问 • **pr**：远程服务器电源/重新启动访问 • **cel**：清空事件日志的能力 • **bc**：适配器配置（基本） • **nsc**：适配器配置（网络和安全性） • **ac**：适配器配置（高级） • **us**：**UEFI** 安全性 **注**：能够以任意组合使用以上定制权限标志
d	删除行	

语法

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

示例

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



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

seccfg 命令

使用此命令可执行固件回滚。

下表显示选项的参数。

表 42. seccfg 命令

下表是一个多行两列的表格，由选项和选项描述组成。

选项	描述	值
-fwrb	允许固件回滚到以前的版本	**yes**、**no**
-aubp	启用或禁用“自动将备用 **XCC** 提升为主 **XCC**”功能	**enabled**、**disabled**

set 命令

使用此命令可更改部分 **IMM** 设置。

- 可以使用简单的 **set** 命令来更改某些 **IMM** 设置。
- 其中一些设置（例如，环境变量）由 **CLI** 使用。

下表显示选项的参数。

表 43. set 命令

下表是一个单行三列表格，包含命令描述和关联的信息。

选项	描述	值
值	设置指定路径或设置的值	针对指定路径或设置的适当值。

语法：

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

smtp 命令

使用此命令可显示并配置 **SMTP** 接口的设置。

在无任何选项的情况下运行 **smtp** 命令将显示所有 **SMTP** 接口信息。下表显示选项的参数。

表 44. smtp 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-auth	**SMTP** 认证支持	**enabled**、**disabled**
-authepw	**SMTP** 认证已加密的密码	有效密码字符串

表 44. smtp 命令 （续）

选项	描述	值
-authmd	**SMTP** 认证方法	**CRAM-MD5** 或 **LOGIN**
-authn	**SMTP** 认证用户名	字符串（限制为 **256** 个字符）
-authpw	**SMTP** 认证密码	字符串（限制为 **256** 个字符）
-pn	**SMTP** 端口号	有效端口号
-s	**SMTP** 服务器 **IP** 地址或主机名	有效的 **IP** 地址或主机名（限制为 **63** 个字符）

语法：

```
smtp [options]
option:
 -auth enabled|disabled
 -authepw password
 -authmd CRAM-MD5|LOGIN
 -authn username
 -authpw password
 -s ip_address_or_hostname
  -pn port_number
```

示例：

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

snmp 命令

使用此命令可显示和配置 **SNMP** 接口信息。

运行不带任何选项的 **snmp** 命令将显示所有 **SNMP** 接口信息。下表显示选项的参数。

表 45. snmp 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-a3	**SNMPv3** 代理	**on** 和 **off** **注：**要启用 **SNMPv3** 代理，必须满足以下条件： • 使用 **-cn** 命令选项指定 **IMM** 联系人。 • 使用 **-l** 命令选项指定 **IMM** 位置。
-t1	**SNMPv1** 陷阱	**on** 和 **off**
-t2	**SNMPv2** 陷阱	**on** 和 **off**
-t	**SNMPv3** 陷阱	**on** 和 **off**

表 45. snmp 命令 （续）

选项	描述	值
-l	**IMM** 位置	字符串（限制为 **47** 个字符）。 **注：** • 包含空格的自变量必须用引号引起来。自变量中不允许出现任何前导空格或尾部空格。 • 通过不指定任何参数或者指定空字符串作为参数（如“”）来清除 **IMM** 位置。
-cn	**IMM** 联系人姓名	字符串（限制为 **47** 个字符）。 **注：** • 包含空格的自变量必须用引号引起来。自变量中不允许出现任何前导空格或尾部空格。 • 通过不指定任何参数或者指定空字符串作为参数（如“”）来清除 **IMM** 联系人姓名。
-c	**SNMP** 团体名称	字符串（限制为 **15** 个字符）。 **注：** • 包含空格的自变量必须用引号引起来。自变量中不允许出现任何前导空格或尾部空格。 • 通过不指定任何参数或者指定空字符串作为参数（如 “”）来清除 **SNMP** 团体名称。
-ct	**SNMPv2** 陷阱团体名称	字符串（限制为 **15** 个字符）。 **注：** • 包含空格的自变量必须用引号引起来。自变量中不允许出现任何前导空格或尾部空格。 • 通过不指定任何参数或者指定空字符串作为参数（如 ""）来清除 **IMM** 联系人姓名。
-ci	**SNMP** 团体 **IP** 地址/主机名	有效 **IP** 地址或主机名（限制为 **63** 个字符）。 **注：** • **IP** 地址或主机名只能包含点、下划线、减号、字母和数字。不允许任何嵌入式空格或连续句点。 • 通过不指定任何参数来清除 **SNMP** 团体 **IP** 地址或主机名。
-cti	**SNMPv2** 陷阱团体 **IP** 地址/主机名	有效 **IP** 地址或主机名（限制为 **63** 个字符）。 **注：** • **IP** 地址或主机名只能包含点、下划线、减号、字母和数字。不允许任何嵌入式空格或连续句点。 • 通过不指定任何参数来清除 **SNMP** 团体 **IP** 地址或主机名。
-eid	**SNMP** 引擎 **ID**	字符串（限制为 **1** 到 **27** 个字符）

语法：

```
snmp [options]
option:
 -a3 state
 -t state
 -l location
 -cn contact_name
```

-t1 *state*
-c *community name*
-ci *community IP address/hostname*
-t2 *state*
-ct *community name*
-cti *community IP address/hostname*
-eid *engine id*

示例：

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

snmpalerts 命令

使用此命令可管理通过 **SNMP** 发送的警报。

运行不带任何选项的 **snmpalerts** 将显示所有 **SNMP** 警报设置。下表显示选项的参数。

表 46. snmpalerts 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-status	**SNMP** 警报状态	**on** 和 **off**
-crt	设置发送警报的紧急事件	**all**、**none**、**custom:te|vo|po|di|fa|cp|me|in|re|ot** 定制紧急警报设置使用竖线分隔的值列表指定，格式为 **snmpalerts -crt custom:te|vo**，其中 **custom** 值为： • **te**：超过临界温度阈值 • **vo**：超过临界电压阈值 • **po**：紧急电源故障 • **di**：硬盘故障 • **fa**：风扇故障 • **cp**：微处理器故障 • **me**：内存故障 • **in**：硬件不兼容 • **re**：电源冗余故障 • **ot**：所有其他紧急事件
-crten	发送紧急事件警报	**enabled**、**disabled**

表 46. snmpalerts 命令 （续）

选项	描述	值
-wrn	设置发送警报的警告事件	**all**、**none**、**custom:rp|te|vo|po|fa|cp|me|ot** 定制警告警报设置使用竖线分隔的值列表指定，格式为 **snmpalerts -wrn custom:rp|te**，其中 **custom** 值为： • **rp**：电源冗余警告 • **te**：超过警告温度阈值 • **vo**：超过警告电压阈值 • **po**：超过警告功率阈值 • **fa**：非紧急风扇事件 • **cp**：微处理器处于降级状态 • **me**：内存警告 • **ot**：所有其他警告事件
-wrnen	发送警告事件警报	**enabled**、**disabled**
-sys	设置发送警报的常规事件	**all**、**none**、**custom:lo|tio|ot|po|bf|til|pf|el|ne** 定制常规警报设置使用竖线分隔的值列表指定，格式为 **snmpalerts -sys custom:lo|tio**，其中 **custom** 值为： • **lo**：成功的远程登录 • **tio**：操作系统超时 • **ot**：所有其他参考和系统事件 • **po**：系统打开/关闭电源 • **bf**：操作系统引导失败 • **til**：操作系统装入程序看守程序超时 • **pf**：预测故障（**PFA**） • **el**：事件日志 **75%** 已满 • **ne**：网络更改
-sysen	发送常规事件警报	**enabled**、**disabled**

语法：

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

srcfg 命令

使用此命令可指示通过串口重定向模式进入 **CLI** 的按键序列。

要更改串口重定向配置，请输入选项，其后跟值。要更改串口重定向配置，您必须至少具有适配器网络和安全性配置权限。

注：IMM 硬件未提供串口-串口通过功能。因此，不支持在 Remote Supervisor Adapter II CLI 中出现的 -passthru 和 entercliseq 选项。

在无任何选项的情况下运行 srcfg 命令将显示当前串口重定向按键序列。下表显示了 srcfg -entercliseq 命令选项的参数。

表 47. srcfg 命令

下表是一个单行三列表格，包含选项、选项描述和选项值的信息。

选项	描述	值
-entercliseq	进入 CLI 按键序列	用户定义的用于进入 CLI 的按键序列。 **注：**此序列必须具有最少一个字符最多 **15** 个字符。插入标记符号（^）在此序列中具有特殊含义。它代表映射到 **Ctrl** 序列的按键中的 **Ctrl**（例如，**^[** 表示 **Esc** 键，而 **^M** 表示回车符）。所有出现的 ^ 都将解释为 **Ctrl** 序列的一部分。请参阅 **ASCII-键转换表**，以了解 **Ctrl** 序列的完整列表。此字段的默认值是“^[(”，即 **Esc** 后跟 (。

语法：

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

示例：

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

sshcfg 命令

使用此命令可显示并配置 SSH 参数。

在无任何选项的情况下运行 sshcfg 命令将显示所有 SSH 参数。下表显示选项的参数。

表 48. sshcfg 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-cstatus	SSH CLI 的状态	**enabled**、**disabled**
-hk gen	生成 SSH 服务器私钥	
-hk rsa	显示服务器 RSA 公钥	

语法：

```
sshcfg [options]
option:
 -cstatus state
 -hk gen
 -hk rsa
```

示例：

```
system> sshcfg
-cstatus enabled
CLI SSH port 22
ssh-rsa 2048 bit fingerprint: b4:a3:5d:df:0f:87:0a:95:f4:d4:7d:c1:8c:27:51:61
1 SSH public keys installed
system>
```

ssl 命令

使用此命令可显示并配置 **SSL** 参数。

要启用 **SSL** 客户端，必须先安装客户端证书。在无任何选项的情况下运行 **ssl** 命令将显示 **SSL** 参数。下表显示选项的参数。

表 49. ssl 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-ce	启用或禁用 **SSL** 客户端	**on** 和 **off**
-se	启用或禁用 **SSL** 服务器	**on** 和 **off**
-cime	在 **SSL** 服务器上启用或禁用 **CIM over HTTPS**	**on** 和 **off**

语法：

```
portcfg [options]
 options:
  -ce state
  -se state
   -cime state
```

参数：以下参数会出现在 **ssl** 命令的选项状态显示中，并且仅从 **CLI** 输出：

Server secure transport enable
此状态显示为只读，不能直接设置。

Server Web/CMD key status
此状态显示为只读，不能直接设置。可能的命令行输出值如下所示：

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

SSL server CSR key status
此状态显示为只读，不能直接设置。可能的命令行输出值如下所示：

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

SSL client LDAP key status
此状态显示为只读，不能直接设置。可能的命令行输出值如下所示：

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

SSL client CSR key status
此状态显示为只读，不能直接设置。可能的命令行输出值如下所示：

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

sslcfg 命令

使用此命令可显示并配置 IMM 的 SSL，并管理证书。

在无任何选项的情况下运行 **sslcfg** 命令将显示所有 SSL 配置信息。**sslcfg** 命令用于生成新加密密钥和自签名证书/证书签名请求（CSR）。下表显示选项的参数。

表 50. sslcfg 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-server	SSL 服务器状态	**enabled**、**disabled** **注**：仅当安装了有效的证书时，才能启用 SSL 服务器。
-client	SSL 客户端状态	**enabled**、**disabled** **注**：仅当安装了有效的服务器或客户端证书时，才能启用 SSL 客户端。
-cim	CIM over HTTPS 状态	**enabled**、**disabled** **注**：仅当安装了有效的服务器或客户端证书时，才能启用 CIM over HTTPS。
-cert	生成自签名证书	**server**、**client**、**sysdir**、**storekey** **注**： • 生成自签名证书时，**-c**、**-sp**、**-cl**、**-on** 和 **-hn** 命令选项的值是必需的。 • 生成自签名证书时，**-cp**、**-ea**、**-ou**、**-s**、**-gn**、**-in** 和 **-dq** 命令选项的值是可选的。

表 50. sslcfg 命令 （续）

选项	描述	值
-csr	生成 **CSR**	**server**、**client**、**sysdir**、**storekey** **注：** • 生成 **CSR** 时，**-c**、**-sp**、**-cl**、**-on** 和 **-hn** 命令选项的值是必需的。 • 生成 **CSR** 时，**-cp**、**-ea**、**-ou**、**-s**、**-gn**、**-in**、**-dq**、**-cpwd** 和 **-un** 命令选项的值是可选的。
-i	**TFTP/SFTP** 服务器的 **IP** 地址	有效的 **IP** 地址 **注：**上传证书或者下载证书/**CSR** 时，必须指定 **TFTP** 或 **SFTP** 服务器的 **IP** 地址。
-pn	**TFTP/SFTP** 服务器的端口号	有效端口号（默认值为 **69/22**）
-u	**SFTP** 服务器的用户名	有效用户名
-pw	**SFTP** 服务器的密码	有效密码
-l	证书文件名	有效文件名 **注：**下载或者上传证书/**CSR** 时，文件名是必需的。如果下载时未指定文件名，将对文件使用并显示默认名称。
-dnld	下载证书文件	此选项不带参数；但是，也必须为 **-cert** 或 **-csr** 命令选项指定值（取决于所下载的证书类型）。此选项不带参数；但是，也必须为 **-i** 命令选项和 **-l**（可选）命令选项指定值。
-upld	导入证书文件	此选项不带参数；但是，也必须为 **-cert**、**-i** 和 **-l** 命令选项指定值。
-tc*x*	**SSL** 客户端的可信证书 ***x***	**import**、**download** 或 **remove** **注：**可信证书号 ***x*** 在命令选项中指定为 **1** 到 **3** 之间的整数。
-c	国家/地区	国家/地区代码（**2** 个字母） **注：**生成自签名证书或 **CSR** 时必填。
-sp	省/自治区/直辖市	引号分隔的字符串（最多 **60** 个字符） **注：**生成自签名证书或 **CSR** 时必填。
-cl	市/县/区或地点	引号分隔的字符串（最多 **50** 个字符） **注：**生成自签名证书或 **CSR** 时必填。
-on	组织机构名称	引号分隔的字符串（最多 **60** 个字符） **注：**生成自签名证书或 **CSR** 时必填。
-hn	**IMM** 主机名	字符串（最多 **60** 个字符） **注：**生成自签名证书或 **CSR** 时必填。
-cp	联系人	引号分隔的字符串（最多 **60** 个字符） **注：**生成自签名证书或 **CSR** 时可选填。
-ea	联系人电子邮件地址	有效电子邮件地址（最多 **60** 个字符） **注：**生成自签名证书或 **CSR** 时可选填。
-ou	组织机构单位	引号分隔的字符串（最多 **60** 个字符） **注：**生成自签名证书或 **CSR** 时可选填。
-s	姓氏	引号分隔的字符串（最多 **60** 个字符） **注：**生成自签名证书或 **CSR** 时可选填。

表 50. sslcfg 命令 （续）

选项	描述	值
-gn	名字	引号分隔的字符串（最多 **60** 个字符） **注**：生成自签名证书或 **CSR** 时可选填。
-in	首字母	引号分隔的字符串（最多 **20** 个字符） **注**：生成自签名证书或 **CSR** 时可选填。
-dq	域名限定词	引号分隔的字符串（最多 **60** 个字符） **注**：生成自签名证书或 **CSR** 时可选填。
-cpwd	提问密码	字符串（最少 **6** 个字符，最多 **30** 个字符） **注**：生成 **CSR** 时可选填。
-un	非结构化名称	引号分隔的字符串（最多 **60** 个字符） **注**：生成 **CSR** 时可选填。

语法：

```
sslcfg [options]
option:
 -server state
 -client state
 -cim state
 -cert certificate_type
 -csr certificate_type
 -i ip_address
 -pn port_number
 -u username
 -pw password
 -l filename
 -dnld
 -upld
 -tc xaction
 -c country_code
 -sp state_or_province
 -cl city_or_locality
 -on organization_name
 -hn bmc_hostname
 -cp contact_person
 -ea email_address
 -ou organizational_unit
 -s surname
 -gn given_name
 -in initials
 -dq dn_qualifier
 -cpwd challenge_password
  -un unstructured_name
```

示例：

```
system> sslcfg
-server enabled
-client disabled
-sysdir enabled
SSL Server Certificate status:
 A self-signed certificate is installed
SSL Client Certificate status:
 A self-signed certificate is installed
SSL CIM Certificate status:
```

```
A self-signed certificate is installed
SSL Client Trusted Certificate status:
 Trusted Certificate 1: Not available
 Trusted Certificate 2: Not available
 Trusted Certificate 3: Not available
 Trusted Certificate 4: Not available
```

客户端证书示例：

- 要生成存储密钥的 CSR，请输入以下命令：
  ```
  system> sslcfg
  -csr storekey -c US -sp NC -cl rtp -on Lenovo -hn XCC-5cf3fc6e0c9d
  -cp Contact -ea "" -ou""
  ok
  ```
  以上示例由于空间限制显示为多行。
- 要将证书从 IMM 下载到另一台服务器上，请输入以下命令：
  ```
  system> sslcfg
  -csr storekey -dnld -i 192.168.70.230 -l storekey.csr
  ok
  ```
- 要上传经证书颁发机构（CA）处理的证书，请输入以下命令：
  ```
  system> sslcfg
  -cert storekey -upld -i 192.168.70.230 -l tklm.der
  ```
- 要生成自签名证书，请输入以下命令：
  ```
  system> sslcfg
  -cert storekey -c US -sp NC -cl rtp -on Lenovo -hn XCC-5cf3fc6e0c9d
  -cp Contact -ea "" -ou "
  ok
  ```
  以上示例由于空间限制显示为多行。

SKLM 服务器证书示例：

- 要导入 SKLM 服务器证书，请输入以下命令：
  ```
  system> storekeycfg
  -add -ip 192.168.70.200 -f tklm-server.der
  ok
  ```

storekeycfg 命令

使用此命令可配置 SKLM 服务器的主机名或 IP 地址以及网络端口。

最多可配置四个 SKLM 服务器目标。storekeycfg 命令还用于安装和删除 IMM 用于向 SKLM 服务器进行认证的证书。

下表显示选项的参数。

表 51. storekeycfg 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

表 51. storekeycfg 命令 （续）

选项	描述	值
-add	添加激活密钥	值为 **-ip**、**-pn**、**-u**、**-pw** 和 **-f** 命令选项
-ip	**TFTP/SFTP** 服务器的主机名或 **IP** 地址	**TFTP/SFTP** 服务器的有效主机名或 **IP** 地址
-pn	**TFTP** 或 **SFTP** 服务器的端口号	**TFTP/SFTP** 服务器的有效端口号（默认值为 **69/22**）
-u	**SFTP** 服务器的用户名	**SFTP** 服务器的有效用户名
-pw	**SFTP** 服务器的密码	**SFTP** 服务器的有效密码
-f	激活密钥的文件名	激活密钥文件名的有效文件名
-del	使用此命令按索引号删除激活密钥	**keycfg** 列表中的有效激活密钥索引号
-dgrp	添加设备组	设备组名称
-sxip	添加 **SKLM** 服务器的主机名或 **IP** 地址	**SKLM** 服务器的有效主机名或 **IP** 地址。数值 **1**、**2**、**3** 或 **4**。
-sxpn	添加 **SKLM** 服务器的端口号	**SKLM** 服务器的有效端口号。数值 **1**、**2**、**3** 或 **4**。
-testx	测试配置以及与 **SKLM** 服务器的连接	数值 **1**、**2**、**3** 或 **4**
-h	显示命令用法和选项	

语法：

```
storekeycfg [options]
 options:
  -add state
  -ip ip_address
  -pn port_number
  -u username
  -pw password
  -f filename
  -del key_index
  -dgrp device_group_name
  -sxip ip_address
  -sxpn port_number
  -testx numeric value of SKLM server
  -h
```

示例：

要导入 **SKLM** 服务器证书，请输入以下命令：

```
system> storekeycfg
add -ip 192.168.70.200 -f tklm-server.der
system> ok
```

要配置 **SKLM** 服务器地址和端口号，请输入以下命令：

```
system> storekeycfg
-s1ip 192.168.70.249
```

```
system> ok
```

要设置设备组名称，请输入以下命令：

```
system> storekeycfg
-dgrp IBM_SYSTEM_X_SED
system> ok
```

syncrep 命令

使用此命令可从远程存储库启动固件同步。

下表显示选项的参数。

表 52. syncrep 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-t	用于连接存储库的协议	**samba**、**nfs**
-l	远程存储库的位置	采用 **URL** 格式
-u	用户	
-p	密码	
-o	选项	**samba** 和 **nfs** 装载的额外选项字符串
-d	域	**samba** 装载的域
-q	查询当前更新状态	
-c	取消同步过程	

语法

```
syncrep [options]  Launch firmware sync from remote repository
 options:
   -t <samba|nfs> protocol to connect repository
   -l location of remote repository (URL format)
   -u User
   -p Password
   -o option (extra option string for samba and nfs mounts)
   -d domain (domain for samba mount)
   -q query current update status
   -c cancel the sync process
```

示例

```
(1) start sync with repository
system> syncrep -t samba -l url -u user -p password
(2) query current update status
system> syncrep -q
(3)cancel the sync process
system> syncrep -c
```

thermal 命令

使用此命令可显示并配置主机系统的散热模式策略。

在无任何选项的情况下运行 **thermal** 命令将显示散热模式策略。下表显示选项的参数。

表 53. thermal 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-mode	温度模式选择	**normal**、**performance**、**minimal**、**efficiency**、**custom**
-table	供应商、设备标识（ID）和备用散热表	

语法：

```
thermal [options]
option:
 -mode thermal_mode
 -table vendorID_devicetable_number
```

示例：

```
system> thermal
-mode normal
-table 80860126 1 10DE0DFA 3
system>
```

timeouts 命令

使用此命令可显示或更改超时值。

- 要显示超时，请输入 timeouts。
- 要更改超时值，请输入选项，其后跟值。
- 要更改超时值，您必须至少具有适配器配置权限。

下表显示了超时值的参数。这些值与 **Web** 界面上服务器超时的分度标下拉选项一致。

表 54. timeouts 命令

下表是一个多行四列表格，包含选项、选项描述和选项关联值的信息。

选项	超时	单位	值
-f	关闭电源延迟	分钟	**disabled**、**0.5**、**1**、**2**、 **3**、**4**、**5**、**7.5**、**10**、**15**、 **20**、**30**、**60** 或 **120**
-l	装入程序超时	分钟	**disabled**、**0.5**、**1**、**1.5**、 **2**、**2.5**、**3**、**3.5**、**4**、 **4.5**、**5**、**7.5**、**10**、**15**、 **20**、**30**、**60** 和 **120**

表 54. timeouts 命令 （续）

选项	超时	单位	值
-o	操作系统超时	分钟	**disabled**、**2.5**、**3**、**3.5** 和 **4**
-s	包含硬件错误的操作系统故障截屏	/	**disabled** 和 **enabled**

语法：

```
timeouts [options]
options:
-f power_off_delay_watchdog_option
-o OS_watchdog_option
-l loader_watchdog_option
-s OS failure screen capture with HW error
```

示例：

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

tls 命令

使用此命令设置最低 **TLS** 级别。

下表显示选项的参数。

表 55. tls 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-min	选择最低 **TLS** 级别	**1.1**, **1.2**[1], **1.3**
-h	列出用法和选项	
注： **1.** 将加密模式设置为“**NIST-800-131A** 合规性模式”时，必须将 **TLS** 版本设置为 **1.2**。		

用法：

```
tls [-options] - configures the minimum TLS level
  -min <1.1 | 1.2 | 1.3> - Selects the minimum TLS level
  -h - Lists usage and options
```

示例：

要了解 **tls** 命令的用法，请发出以下命令：

```
system> tls
-h
system>
```

要获取当前 **tls** 版本，请发出以下命令：

```
system> tls
-min 1.2
system>
```

要将当前 **tls** 版本更改为 **1.2**，请发出以下命令：

```
system> tls
-min 1.2
ok
system>
```

trespass 命令

使用此命令可配置和显示非法侵入消息。

trespass 命令可用于配置和显示非法侵入消息。非法侵入消息将显示给通过 **Web** 或 **CLI** 界面登录的任何用户。

下表显示选项的参数。

表 56. uefipw 命令

下表是一个多行两列的表格，由选项和选项描述组成。

选项	描述
-s	配置非法侵入消息
-h	列出用法和选项

语法：

```
usage:
  trespass display the trespass message
  -s <trespass message> configure trespass message
  -h - Lists usage and options
```

示例：

注：非法侵入消息不包含任何空格。

```
system> trespass -s testingmessage
ok
system> trespass
testingmessage

The trespass message contains spaces:
system> trespass -s "testing message"
ok
system> trespass
testing message
```

uefipw 命令

使用此命令可配置 **UEFI** 管理员密码。密码是只写的。

uefipw 命令可与“**-p**”选项一起使用来配置 **UEFI** 管理员密码（对于 **XCC**），或者可与“**-ep**”选项一起使用来通过 **CLI** 界面配置 **UEFI** 管理员密码（对于 **LXCA**）。密码是只写的。

下表显示选项的参数。

表 57. uefipw 命令

下表是一个多行两列的表格，由选项和选项描述组成。

选项	描述
-cp	当前密码（限制为 **20** 个字符）
-p	新密码（限制为 **20** 个字符）
-cep	加密的当前密码
-ep	加密的新密码

语法：

```
usage:
  uefipw [-options] - Configure the UEFI admin password
options:
  -cp    - current password (limited to 20 characters)
  -p     - new password (limited to 20 characters)
  -cep   - current password encrypted
  -ep    - new password encrypted
```

usbeth 命令

使用此命令可启用或禁用带内 **LAN over USB** 接口。

语法：

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

示例：

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

usbfp 命令

使用此命令可控制 **BMC** 使用前面板 **USB** 端口的方式

下表显示选项的参数。

表 58. usbfp 命令

下表是一个多行两列的表格，由选项和选项描述组成。

选项	描述
-mode <bmc | server | shared>	将使用模式设置为 **BMC**、服务器或共享
-it <minutes>	以分钟为单位的空闲超时（共享模式）
-btn <on | off>	允许使用标识按钮切换所有者（共享模式）
-own <bmc | server >	将使用者设置为 **BMC** 或服务器（共享模式）

users 命令

使用此命令可访问所有用户帐户及其权限级别。

users 命令还可用于创建新用户帐户和修改现有帐户。在无任何选项的情况下运行 **users** 命令将显示用户的列表和某些基本用户信息。下表显示选项的参数。

表 59. users 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-user_index	用户帐户索引号	**1** 到 **12**（含二者）或 all 表示所有用户。
-n	用户帐户名称	仅包含数字、字母、句点和下划线的唯一字符串。最少 **4** 个字符，最多 **16** 个字符。
-p	用户帐户密码	至少包含一个字母字符和一个非字母字符的字符串。最少 **6** 个字符，最多 **20** 个字符。该字符串为空时将创建一个不带密码的帐户，用户必须在首次登录时设置密码。
-r	角色名称	如第 **132** 页 “**roles** 命令”中所列
-ep	加密密码（用于备份/恢复）	有效密码
-clear	擦除指定用户帐户 如果拥有权限，您可以删除自己的帐户或其他用户的帐户（即使其当前已登录），除非它是当前剩下的唯一一个有用户帐户管理权限的帐户。删除用户帐户时不会自动终止正在进行的会话。	必须指定要擦除的用户帐户索引号，并遵循以下格式： users -clear -*user_index*
-curr	显示当前登录的用户	
-sauth	**SNMPv3** 认证协议	**HMAC-SHA**、**none**
-spriv	**SNMPv3** 隐私协议	**CBC-DES**、**AES** 或 **none**
-spw	**SNMPv3** 隐私密码	有效密码

表 59. users 命令 （续）

选项	描述	值
-sepw	**SNMPv3** 隐私密码（已加密）	有效密码
-sacc	**SNMPv3** 访问类型	**get** 或 **set**
-strap	**SNMPv3** 陷阱主机名	有效主机名
-pk	显示用户的 **SSH** 公钥	用户帐户索引号。 **注：** • 将显示向该用户分配的每个 **SSH** 密钥，并带有标识密钥索引号。 • 使用 **SSH** 公钥选项时，必须在用户索引（*-userindex* 选项）后使用 -pk 选项，格式为：users -2 -pk。 • 所有密钥均采用 **OpenSSH** 格式。 • 对于 **Flex** 节点，用户命令仅限用于本地 **IPMI** 和 **SNMP** 帐户。**Flex** 系统不支持 -pk 选项。
-e	以 **OpenSSH** 格式显示整个 **SSH** 密钥 *（**SSH** 公钥选项）*	此选项不带参数，并且不得与所有其他 users -pk 选项按共用。 **注：**使用 **SSH** 公钥选项时，必须在用户索引（*-userindex* 选项）后使用 -pk 选项，格式为：users -2 -pk -e。
-remove	从用户中除去 **SSH** 公用密钥 *（**SSH** 公钥选项）*	必须将要删除的公钥索引号指定为一个特定 *-key_index* 或 -all（表示向用户分配的所有密钥）。 **注：** • 使用 **SSH** 公钥选项时，必须在用户索引（*-userindex* 选项）后使用 -pk 选项，格式为：users -2 -pk -remove -1。 • 对于 **Flex** 节点，用户命令仅限用于本地 **IPMI** 和 **SNMP** 帐户。**Flex** 系统不支持 -remove 选项。
-add	为用户添加 **SSH** 公钥 *（**SSH** 公钥选项）*	以引号分隔的密钥，采用 **OpenSSH** 格式 **注：** • -add 选项不得与所有其他 users -pk 命令选项共用。 • 使用 **SSH** 公钥选项时，必须在用户索引（*-userindex* 选项）后使用 -pk 选项，格式为：users -2 -pk -add "AAAAB3NzC1yc2EAAAABIwAAAQEAvfn-TUzRF7pdBuaBy4dO/aIFasa/Gtc+o/wlZnuC4aDHMA1Um-nMyLOCiIaNOy4OOICEKCqjKEhrYymtAoVtfKApvY39Gp-nSGRC/qcLGWLM4cmirKL5kxHNOqIcwbT1NPceoKH j46X7E+mqlfWnAhhjDpcVFjagM3Ek2y7w/tBGrwGgN7DP HJU1tzcJy68mEAnIrzjUoR98Q3/B9cJD77ydGKe8rPdI2 hIEpXR5dNUiupA1Yd8PSSMgdukASKEd3eRRZTBl3SAtMu cUsTkYjlXcqex1OQz4+N5OR6MbNcwlsx+mTEAvvcpJhug a7OUNPGhLJMl6k7jeJiQ8Xd2p XbOZQ==" • 对于 **Flex** 节点，用户命令仅限用于本地 **IPMI** 和 **SNMP** 帐户。**Flex** 系统不支持 -add 选项。

表 59. users 命令 （续）

选项	描述	值
-upld	上传 **SSH** 公钥 *（**SSH** 公钥选项）*	需要 -i 和 -l 选项来指定密钥位置。 **注：** • -upld 选项不得与所有其他 users -pk 命令选项共用（-i 和 -l 除外）。 • 要将一个密钥替换为新密钥，必须指定 -*key_index*。如果要向当前密钥列表的末尾添加一个密钥，请勿指定密钥索引。 • 使用 **SSH** 公钥选项时，必须在用户索引（-*userindex* 选项）后使用 -pk 选项，格式为：users -2 -pk -upld -i tftp://9.72.216.40/ -l file.key。 • 对于 **Flex** 节点，用户命令仅限用于本地 **IPMI** 和 **SNMP** 帐户。**Flex** 系统不支持 -upld 选项。
-dnld	下载指定的 **SSH** 公钥 *（**SSH** 公钥选项）*	需要 -*key_index* 来指定要下载的密钥，并且需要 -i 和 -l 选项来指定在另一运行 **TFTP** 服务器的计算机上的下载位置。 **注：** • -dnld 选项不得与所有其他 users -pk 命令选项共用（-i、-l 和 -*key_index* 除外）。 • 使用 **SSH** 公钥选项时，必须在用户索引（-*userindex* 选项）后使用 -pk 选项，格式为：users -2 -pk -dnld -1 -i tftp://9.72.216.40/ -l file.key。
-i	用于上传或下载密钥文件的 **TFTP/SFTP** 服务器的 **IP** 地址。 *（**SSH** 公钥选项）*	有效的 **IP** 地址 **注：**users -pk -upld 和 users -pk -dnld 命令选项需要 -i 选项。
-pn	**TFTP/SFTP** 服务器的端口号 *（**SSH** 公钥选项）*	有效端口号（默认值为 **69/22**） **注：**users -pk -upld 和 users -pk -dnld 命令选项的可选参数。
-u	**SFTP** 服务器的用户名 *（**SSH** 公钥选项）*	有效用户名 **注：**users -pk -upld 和 users -pk -dnld 命令选项的可选参数。
-pw	**SFTP** 服务器的密码 *（**SSH** 公钥选项）*	有效密码 **注：**users -pk -upld 和 users -pk -dnld 命令选项的可选参数。
-l	通过 **TFTP** 或 **SFTP** 上传或下载密钥文件的文件名 *（**SSH** 公钥选项）*	有效文件名 **注：**users -pk -upld 和 users -pk -dnld 命令选项需要 -l 选项。
-af	接受来自主机的连接 *（**SSH** 公钥选项）*	以逗号分隔的主机名和 **IP** 地址的列表，限制为 **511** 个字符。有效字符包括：字母数字、逗号、星号、问号、惊叹号、句点、连词符、冒号和百分号。
-cm	注释 *（**SSH** 公钥选项）*	以引号分隔的字符串，最多 **255** 个字符。 **注：**使用 **SSH** 公钥选项时，必须在用户索引（-*userindex* 选项）后使用 -pk 选项，格式为：users -2 -pk -cm "This is my comment."。

语法：

```
users [-options] - display/configure user accounts
options:
```

```
  -[1-12]  - user account number
  -l     - display password expiration days
  -n     - username (limited to 16 characters)
  -p     - password (limited to 32 characters)
  -shp    - set hashpassword (total 64 characters)
  -ssalt   - set salt (limited to 64 characters)
  -ghp    - get hashpassword
  -gsalt   - get salt
  -ep     - encrypted password (used with backup/restore )
  -r     - role name as listed in roles command
  -clear   - clear user account
  -curr   - display current users
  -sauth  (none|HMAC-SHA)       - snmpv3 authentication protocol
  -spriv  (none|CBC-DES|AES)     - snmpv3 privacy protocol
  -spw   password           - snmpv3 privacy password
  -sepw   encryptedpassword      - snmpv3 privacy password (encrypted)
  -sacc   (Get)          - snmpv3 Access type
  -strap  hostname           - snmpv3 trap hostname

  -pk    - SSH public keys options:
    -e     - Displays the entire key in OpenSSH format
    -remove  - Removes the specified key for the specified user
    -add    - Adds a public key for the specified user
    -upld   - Used to upload a public key in OpenSSH/RFC4716 format
    -dnld   - Used to download the specified public key to a TFTP/SFTP server
    -i     - IP address of the TFTP/SFTP
    -pn     - port number of tftp/sftp server (default 69/22)
    -u     - username for sftp server
    -pw     - password for sftp server
    -l     - Filename of the key file when uploading or downloading via TFTP/SFTP
    -af     - accept connections from host, in the format: from="<list>", where
          <list> is a comma-separated list of hostnames and IP addresses
          (limited to 511 characters)
    -cm     - comment (limited to 255 characters, must be quote-delimited)
```

示例：

```
system> users
 Account    Login ID    Advanced Attribute        Role       Password Expires
 -------    --------    ------------------       ------      ----------------
   1       USERID           Native          Administrator           89 day(s)
system> users -2 -n sptest -p Passw0rd12 -r Administrator
The user is required to change the password when the user logs in to the management server for the first time
ok
system> users
 Account    Login ID    Advanced Attribute       Role        Password Expires
 -------    --------    ------------------      ------       ----------------
   1       USERID           Native       Administrator           90 day(s)
2       sptest           Native          Administrator       Password expired
system> hashpw -sw enabled -re enabled
system> users -5 -n guest5 -shp 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee -ssalt abc -r Administrator
system> users -5 ghp
292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
system> users -5 gsalt
abc
```

IMM 控制命令

本主题按字母顺序提供 **IMM 控制 CLI** 命令的列表。

当前有 **7** 条 **IMM** 控制命令：

alertentries 命令

使用此命令可管理警报接收方。

- 不带有任何选项的 **alertentries** 将显示所有警报条目设置。
- **alertentries -number -test** 可向给定的接收方索引号生成测试警报。
- **alertentries -number**（其中 **number** 为 **0** 到 **12**）可显示指定接收方索引号的警报条目设置或允许您修改该接收方的警报设置。

下表显示选项的参数。

表 60. alertentries 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-number	要显示、添加、修改或删除的警报接收方索引号	**1** 到 **12**
-status	警报接收方状态	**on** 和 **off**
-type	警报类型	**email** 或 **syslog**
-log	在警报电子邮件中包括事件日志	**on** 和 **off**
-n	警报接收方名称	字符串
-e	警报接收方电子邮件地址	有效的电子邮件地址
-ip	**Syslog IP** 地址或主机名	有效的 **IP** 地址或主机名
-pn	**Syslog** 端口号	有效端口号
-del	删除指定的接收方索引号	
-test	向指定的接收方索引号生成测试警报	
-crt	设置发送警报的紧急事件	**all**、**none**、**custom:te|vo|po|di|fa|cp|me|in|re|ot** 定制紧急警报设置通过使用以竖线分隔的值列表来指定，格式为：**alertentries -crt custom:te|vo**，其中 **custom** 值包括： • **te**：超过临界温度阈值 • **vo**：超过临界电压阈值 • **po**：紧急电源故障 • **di**：硬盘故障 • **fa**：风扇故障 • **cp**：微处理器故障 • **me**：内存故障 • **in**：硬件不兼容 • **re**：电源冗余故障 • **ot**：所有其他紧急事件

表 60. alertentries 命令 （续）

选项	描述	值
-crten	发送紧急事件警报	**enabled**、**disabled**
-wrn	设置发送警报的警告事件	**all**、**none**、**custom:rp**|**te**|**vo**|**po**|**fa**|**cp**|**me**|**ot** 定制警告警报设置通过使用以竖线分隔的值列表来指定，格式为：**alertentries -wrn custom:rp**|**te**，其中 **custom** 值包括： • **rp**：电源冗余警告 • **te**：超过警告温度阈值 • **vo**：超过警告电压阈值 • **po**：超过警告功率阈值 • **fa**：非紧急风扇事件 • **cp**：微处理器处于降级状态 • **me**：内存警告 • **ot**：所有其他警告事件
-wrnen	发送警告事件警报	**enabled**、**disabled**
-sys	设置发送警报的常规事件	**all**、**none**、**custom:lo**|**tio**|**ot**|**po**|**bf**|**til**|**pf**|**el**|**ne** 定制常规警报设置通过使用以竖线分隔的值列表来指定，格式为：**alertentries -sys custom:lo**|**tio**，其中 **custom** 值包括： • **lo**：成功的远程登录 • **tio**：操作系统超时 • **ot**：所有其他参考和系统事件 • **po**：系统打开/关闭电源 • **bf**：操作系统引导失败 • **til**：操作系统装入程序看守程序超时 • **pf**：预测故障（**PFA**） • **el**：事件日志 **75%** 已满 • **ne**：网络更改
-sysen	发送常规事件警报	**enabled**、**disabled**

语法：

```
alertentries [options]
  options:
  -number recipient_number
    -status status
    -type alert_type
    -log include_log_state
    -n recipient_name
    -e email_address
    -ip ip_addr_or_hostname
    -pn port_number
    -del
    -test
    -crt event_type
    -crten state
    -wrn event_type
    -wrnen state
```

-sys *event_type*
-sysen *state*

示例：

```
system> alertentries
1. test
2. <not used>
3. <not used>
4. <not used>
5. <not used>
6. <not used>
7. <not used>
8. <not used>
9. <not used>
10. <not used>
11. <not used>
12. <not used>

system> alertentries -1
-status off
-log off
-n test
-e test@mytest.com
-crt all
-wrn all
-sys none
system>
```

batch 命令

使用此命令可执行文件中包含的一个或多个 **CLI** 命令。

- 批处理文件中的注释行以“#”开头。
- 当运行批处理文件时，失败的命令将随故障返回码一起返回。
- 包含不可识别的命令选项的批处理文件命令可能生成警告。

下表显示选项的参数。

表 61. batch 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-f	批处理文件名	有效文件名
-ip	**TFTP/SFTP** 服务器的 **IP** 地址	有效的 **IP** 地址
-pn	**TFTP/SFTP** 服务器的端口号	有效端口号（默认值为 **69/22**）
-u	**SFTP** 服务器的用户名	有效用户名
-pw	**SFTP** 服务器的密码	有效密码

语法：

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

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

示例：
```
system> batch -f sslcfg.cli -ip 192.168.70.200
1 : sslcfg client dnld ip 192.168.70.20
Command total/errors/warnings: 8 / 1 / 0
system>
```

clearcfg 命令

使用此命令可将 **IMM** 配置设置为其出厂默认值。

您至少应具有高级适配器配置权限才能发出此命令。清除 **IMM** 的配置后，**IMM** 将重新启动。

clock 命令

使用此命令显示当前日期和时间。您可以设置 **UTC** 偏移量和夏令时设置

BMC 从主机服务器或 **NTP** 服务器获取时间。

从主机获得的时间可能是本地时间或 **UTC** 时间。如果未使用 **NTP** 且主机使用 **UTC** 格式，则主机选项应设置为 **UTC**。**UTC** 偏移量可以采用 **+0200**、**+2:00**、**+2** 或 **2** 格式表示正偏移量，采用 **-0500**、**-5:00** 或 **-5** 格式表示负偏移量。**UTC** 偏移量和夏令时用于 **NTP** 或主机模式是 **UTC** 的情况。

如果 **UTC** 偏移量为 **+2**、**-7**、**-6**、**-5**、**-4** 和 **-3**，那么需要特殊夏令时设置。

- 如果为 **+2**，那么夏令时选项如下：**off**、**ee**（东欧）、**tky**（土耳其）、**bei**（贝鲁特）、**amm**（安曼）和 **jem**（耶路撒冷）。
- 如果为 **-7**，那么夏令时设置如下：**off**、**mtn**（芒廷）和 **maz**（马萨特兰）。
- 如果为 **-6**，那么夏令时设置如下：**off**、**mex**（墨西哥）和 **cna**（北美中部）。
- 如果为 **-5**，那么夏令时设置如下：**off**、**cub**（古巴）和 **ena**（北美东部）。
- 如果为 **-4**，那么夏令时设置如下：**off**、**asu**（亚松森）、**cui**（库亚巴）、**san**（圣地亚哥）和 **cat**（加拿大-大西洋）。
- 如果为 **-3**，那么夏令时设置如下：**off**、**gtb**（戈特霍布）和 **bre**（巴西-东部）。

语法：
```
clock [options]
options:
-u UTC offset
-dst on/off/special case
-host - local | utc , format of time obtained from host (default: utc)
Windows systems use local, Linux uses utc
```

示例：
```
system> clock
12/12/2011 13:15:23 GMT-5:00 dst on
```

identify 命令

使用此命令可使机箱识别 **LED** 点亮或熄灭，或使其闪烁。

-d 选项可与 **-s on** 选项配合使用，使 **LED** 仅在 **-d** 选项指定的秒数内点亮。在经过该秒数后，**LED** 将熄灭。

语法：

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

示例：

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

info 命令

使用此命令可显示和配置有关 **IMM** 的信息。

运行不带任何选项的 **info** 命令会显示所有 **IMM** 位置和联系信息。下表显示选项的参数。

表 62. info 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-name	**IMM** 名称	字符串
-contact	**IMM** 联系人的姓名	字符串
-location	**IMM** 位置	字符串
-room[1]	**IMM** 房间标识	字符串
-rack[1]	**IMM** 机架标识	字符串
-rup[1]	**IMM** 在机架中的位置	字符串
-ruh	机架单元高度	只读
-bbay	刀片插槽位置	只读
1. 如果 **IMM** 位于 **Flex System** 中，那么值为只读且无法重置。		

语法：

```
info [options]
option:
 -name xcc_name
 -contact contact_name
 -location xcc_location
 -room room_id
 -rack rack_id
 -rup rack_unit_position
 -ruh rack_unit_height
```

-bbay *blade_bay*

spreset 命令

使用此命令可重新启动 IMM。

您至少应具有高级适配器配置权限才能发出此命令。

Service Advisor 命令

本主题按字母顺序提供 Service Advisor CLI 命令的列表。

当前有 3 条 Service Advisor 命令：

chconfig 命令

使用此命令显示和配置 Service Advisor 设置。

- 配置任何其他参数前，必须使用 chconfig -li 命令选项接受 Service Advisor 条款和条件。
- 需要先填写所有联系信息字段以及**服务支持中心**字段（使用 chconfig -sc 命令选项），然后才可以启用对 Service Advisor 的支持。
- 如果需要 HTTP 代理，则必须设置所有 HTTP 代理字段。

下表显示选项的参数。

表 63. chconfig 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-li	查看或接受 Service Advisor 条款和条件 **注**：必须接受这些条款和条件，然后才能配置任何其他参数。	view、accept
-sa	Service Advisor 的支持状态 **注**：要启用 Service Advisor，必须满足以下条件： • 国家/地区代码是必需的。 • “Service Advisor 联系信息”中的所有选项都是必需的。	enabled、disabled
-sc	服务支持中心的国家/地区代码	两个字符的 ISO 国家/地区代码
Service Advisor 联系信息选项：		
-cn	主要联系人的姓名	引号分隔的字符串（最多 30 个字符）
-cph	主要联系人的电话号码	引号分隔的字符串（5 到 30 个字符）

表 63. chconfig 命令 （续）

选项	描述	值
-ce	主要联系人的电子邮件地址 **注**：可以使用字母数字字符“.”、“-”或“_”作为用户 **ID** 或主机名。电子邮件地址必须至少包含两个域项，并且最后一个域项应包含 **2–4** 个字母字符。	格式为 userid@hostname 的有效电子邮件地址（最多 **30** 个字符）
-co	主要联系人的组织或公司名称	引号分隔的字符串（最多 **30** 个字符）
-ca	机器位置的地址	引号分隔的字符串（最多 **30** 个字符）
-cci	机器位置所在的城市	引号分隔的字符串（最多 **30** 个字符）
-cs	机器位置所在的省/直辖市/自治区	引号分隔的字符串（最多 **30** 个字符）
-cz	机器位置的邮政编码	引号分隔的字符串（最多 **9** 个字符）
备用 **Service Advisor** 联系信息选项：		
-an	备用联系人的姓名	引号分隔的字符串（最多 **30** 个字符）
-aph	备用联系人的电话号码	引号分隔的字符串（**5** 到 **30** 个字符）
-ae	备用联系人的电子邮件地址 **注**：可以使用字母数字字符“.”、“-”或“_”作为用户 **ID** 或主机名。电子邮件地址必须至少包含两个域项，并且最后一个域项应包含 **2–4** 个字母字符。	格式为 userid@hostname 的有效电子邮件地址（最多 **30** 个字符）
-ao	备用联系人的组织或公司名称	引号分隔的字符串（最多 **30** 个字符）
-aa	备用机器位置的地址	引号分隔的字符串（最多 **30** 个字符）
-aci	备用机器位置所在的城市	引号分隔的字符串（最多 **30** 个字符）
-as	备用机器位置所在的省/直辖市/自治区	引号分隔的字符串（最多 **30** 个字符）
-az	备用机器位置的邮政编码	引号分隔的字符串（最多 **9** 个字符）
HTTP 代理设置选项：		
-loc	**HTTP** 代理位置	**HTTP** 代理的标准主机名或 **IP** 地址（最多 **63** 个字符）
-po	**HTTP** 代理端口	有效端口号（**1** 到 **65535**）
-ps	**HTTP** 代理状态	**enabled**、**disabled**
-pw	**HTTP** 代理密码	引号分隔的有效密码（最多 **15** 个字符）
-epw	**HTTP** 代理加密密码	引号分隔的有效密码（最多 **15** 个字符）
-u	**HTTP** 代理用户名	引号分隔的有效用户名（最多 **30** 个字符）
-test	测试 **HTTP** 代理	

语法：

```
chconfig [options]
option:
 -li view|accept
 -sa enable|disable
```

-sc *service_country_code*
-ce *contact_email*
-cn *contact_name*
-co *company_name*
-cph *contact_phone*
-cpx *contact_extension_phone*
-an *alternate_contact_name*
-ae *alternate_contact_email*
-aph *alternate_contact_phone*
-apx *alternate_contact_extension_phone*
-mp *machine_phone_number*
-loc *hostname/ip_address*
-po *proxy_port*
-ps *proxy_status*
-pw *proxy_pw*
-ccl *machine_country_code*
-u *proxy_user_name*

chmanual 命令

使用此命令可生成手动 **Call Home** 请求。

注：使用 **chconfig** 命令配置 **Call Home** 消息接收方。

- **chmanual -test** 命令将生成 **Call Home** 测试消息。

下表显示选项的参数。

表 64. chmanual 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-test	为 **Call Home** 接收方生成测试消息	

语法：

```
chmanual [options]
Generates a manual Call Home or a Test Call Home
 -test: Generate a test Call Home.
```

chlog 命令

使用此命令可显示最近五个 **Call Home** 事件并通过案例编号取消与这些事件相关联的案例。

chlog 命令显示服务器或用户生成的 **Call Home** 活动日志中的最近五个条目。最先显示最近的 **Call Home** 条目。服务器将不发送重复事件（如果这些事件在活动日志中未确认为已更正）。

下表显示选项的参数。

表 65. chconfig 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

表 65. chconfig 命令 （续）

选项	描述	值
-c	通过案例编号取消与事件相关联的案例	

语法：

```
chlog[-options]
   Displays the last five call home events that were generated either by
   the system or the user (most recent call home entry first.)

   -c: cancel the case associated with the event by caseNumber
```

无代理命令

本主题按字母顺序提供无代理命令的列表。

当前有 **3** 条无代理命令：

storage 命令

使用此命令可显示和配置（如果平台支持）有关受 **IMM** 管理的服务器存储设备的信息。

下表显示选项的参数。

表 66. storage 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-list	列出受 **IMM** 管理的存储目标。	***controllers*/*pools*/*volumes*/*drives*** 其中，***target*** 为： • ***controllers*：** 列出支持的 **RAID** 控制器[1] • ***pools*：** 列出与 **RAID** 控制器关联的存储池[1] • ***volumes*：** 列出与 **RAID** 控制器关联的存储卷[1] • ***drives*：** 列出与 **RAID** 控制器关联的存储硬盘[1]
-list -target *target_id*	根据 ***target_id*** 列出受 **IMM** 管理的存储*目标*。	***pools*/*volumes*/*drives ctrl[x]*/*pool[x]*** 其中，***target*** 和 ***target_id*** 为： • ***pools ctrl[x]*：** 根据 **target_id** 列出与 **RAID** 控制器关联的存储池[1] • ***volumes ctrl[x]*/*pool[x]*：** 根据 **target_id** 列出与 **RAID** 控制器关联的存储卷[1] • ***drives ctrl[x]*/*pool[x]*：** 根据 **target_id** 列出与 **RAID** 控制器关联的存储驱动器[1]
-list flashdimms	列出受 **IMM** 管理的 **Flash DIMM**。	

表 66. storage 命令 （续）

选项	描述	值
-list devices	显示受 IMM 管理的所有磁盘和 Flash DIMM 的状态。	
-show ***target_id***	显示受 IMM 管理的所选目标的信息。	其中，***target_id*** 为： ***ctrl[x]/vol[x]/disk[x]/pool[x]*** ***/flashdimm[x]*** 3
-show ***target_id*** **info**	显示受 IMM 管理的所选目标的详细信息。	其中，***target_id*** 为： ***ctrl[x]/vol[x]/disk[x]/pool[x]*** ***/flashdimm[x]*** 3
-show ***target_id*** ***firmware***[3]	显示受 IMM 管理的所选目标的固件信息。	其中，***target_id*** 为： ***ctrl[x]/disk[x]/flashdimm[x]***[2]
-showlog ***target_id<m:n|all>***[3]	显示受 IMM 管理的所选目标的事件日志。	其中，***target_id*** 为：***ctrl[x]***[4] ***m:n|all*** 其中，***m:n*** 为一到事件日志的最大数量 其中，***all*** 为所有事件日志
-config ctrl -scanforgn -target ***target_id***[8]	检测外部 RAID 配置。	其中，***target_id*** 为：***ctrl[x]***[5]
-config ctrl -imptforgn -target ***target_id***[8]	导入外部 RAID 配置。	其中，***target_id*** 为：***ctrl[x]***[5]
-config ctrl -clrforgn -target ***target_id***[8]	清除外部 RAID 配置。	其中，***target_id*** 为：***ctrl[x]***[5]
-config ctrl -clrcfg -target ***target_id***[8]	清除 RAID 配置。	其中，***target_id*** 为：***ctrl[x]***[5]
-config drv -mkoffline -target ***target_id***[8]	将硬盘状态从联机更改为脱机。	其中，***target_id*** 为：***disk[x]***[5]
-config drv -mkonline -target ***target_id***[8]	将硬盘状态从脱机更改为联机。	其中，***target_id*** 为：***disk[x]***[5]
-config drv -mkmissing -target ***target_id***[8]	将脱机硬盘标为未配置的完好硬盘。	其中，***target_id*** 为：***disk[x]***[5]
-config drv -prprm -target ***target_id***[8]	准备未配置的完好硬盘以供删除。	其中，***target_id*** 为：***disk[x]***[5]
-config drv -undoprprm -target ***target_id***[8]	取消准备未配置的完好硬盘以供删除的操作。	其中，***target_id*** 为：***disk[x]***[5]
-config drv -mkbad -target ***target_id***[8]	将未配置的完好硬盘更改为未配置的故障硬盘。	其中，***target_id*** 为：***disk[x]***[5]

表 66. storage 命令 （续）

选项	描述	值
-config drv -mkgood -target *target_id*[8]	将未配置的故障硬盘更改为未配置的完好硬盘。 或 将简单磁盘捆绑（JBOD）硬盘转换为未配置的完好硬盘。	其中，***target_id*** 为：***disk[x]***[5]
-config drv -addhsp -*[dedicated pools]* -target *target_id*[8]	将所选硬盘作为热备件分配给一个控制器或现有存储池。	其中，***target_id*** 为：***disk[x]***[5]
-config drv -rmhsp -target *target_id*[8]	删除该热备件。	其中，***target_id*** 为：***disk[x]***[5]
-config vol -remove -target *target_id*[8]	删除一个卷。	其中，***target_id*** 为：***vol[x]***[5]
-config vol -set [-N] [-w] [-r] [-i] [-a] [-d] [-b] -target *target_id*[8]	修改一个卷的属性。	• **[-N *volume_name*]** 为该卷的名称 • **[-w *<0/1/2>*]** 为高速缓存写入策略： – 类型 ***0*** 表示直写策略 – 类型 ***1*** 表示回写策略 – 类型 ***2*** 表示备用电池单元（BBU）写入策略 • **[-r *<0/1/2>*]** 为高速缓存读取策略： – 类型 ***0*** 表示不预读策略 – 类型 ***1*** 表示预读策略 – 类型 ***2*** 表示自适应预读策略 • **[-i *<0/1>*]** 为高速缓存 I/O 策略： – 类型 ***0*** 表示直接 I/O 策略 – 类型 ***1*** 表示缓存 I/O 策略 • **[-a *<0/2/3>*]** 为访问策略： – 类型 ***0*** 表示读写策略 – 类型 ***2*** 表示只读策略 – 类型 ***3*** 表示已阻止策略 • **[-d *<0/1/2>*]** 为磁盘高速缓存策略： – 如果未更改策略，则为类型 ***0*** – 类型 ***1*** 表示启用策略[6] – 类型 ***2*** 表示禁用策略 • **[-b *<0/1>*]** 为后台初始化： – 类型 ***0*** 表示启用初始化 – 类型 ***1*** 表示禁用初始化 • ***-target_id*** 为 ***vol[x]***[5]

表 66. storage 命令 （续）

选项	描述	值
-config vol -add<[-R] [-D disk] [-H disk] [-1 hole]> [-N] [-w] [-r][3],[7]	当目标为控制器时，为新存储池创建一个卷。 或 当目标为存储池时，用现有存储池创建一个卷。	• **[-R *<0/1/5/1E/6/10/50/60/00/1ERLQ-0/1E0RLQ0>*]** 此选项定义 **RAID** 级别，仅用于新存储池 • **[-D disk *[id11]:disk[id12]:..disk[id21]:disk[id22]:..*]**此选项定义硬盘组（包括范围），仅用于新存储池 • **[-H disk *[id1]:disk[id2]:..*]**此选项定义热备件组，仅用于新存储池 • **[-1 hole]** 此选项定义现有存储池的可用孔空间的索引号 • **[-N *volume_name*]** 为该卷的名称 • **[-w *<0/1/2>*]** 为高速缓存写入策略： – 类型 ***0*** 表示直写策略 – 类型 ***1*** 表示回写策略 – 类型 ***2*** 表示备用电池单元（**BBU**）写入策略 • **[-r *<0/1/2>*]** 为高速缓存读取策略： – 类型 ***0*** 表示不预读策略 – 类型 ***1*** 表示预读策略 – 类型 ***2*** 表示自适应预读策略
-config vol -add[-i] [-a] [-d] [-f] [-S] [-P] -target *target_id*[8]	当目标为控制器时，为新存储池创建一个卷。 或 当目标为存储池时，用现有存储池创建一个卷。	• **[-i *<0/1>*]** 为高速缓存 **I/O** 策略： – 类型 ***0*** 表示直接 **I/O** 策略 – 类型 ***1*** 表示缓存 **I/O** 策略 • **[-a *<0/2/3>*]** 为访问策略： – 类型 ***0*** 表示读写策略 – 类型 ***2*** 表示只读策略 – 类型 ***3*** 表示已阻止策略 • **[-d *<0/1/2>*]** 为磁盘高速缓存策略： – 如果策略保持不变，则为类型 ***0*** – 类型 ***1*** 表示启用策略[6] – 类型 ***2*** 表示禁用策略 • **[-f *<0/1/2>*]** 为初始化的类型： – 类型 ***0*** 表示不初始化 – 类型 ***1*** 表示快速初始化 – 类型 ***2*** 表示全面初始化 • **[-S *volume_size*]** 为新卷的大小（以 **MB** 计） • **[-P *strip_size*]** 为卷的条带大小，例如，**128K** 或 **1M** • **-target *target_id*** 为：

表 66. storage 命令 （续）

选项	描述	值
		– ***ctrl[x]***（新存储池）[5] – ***pool[x]***（现有存储池）[5]
-config vol -getfreecap[-R] [-D disk] [-H disk] -target *target_id*[6]	获取硬盘组的可用容量。	• **[-R *<0/1/5/1E/6/10/50/60/00/1ERLQ-0/1E0RLQ0>*]** 此选项定义 **RAID** 级别，仅用于新存储池 • **[-D disk *[id11]:[id12]:..[id21]:[id22]:..*]**此选项定义硬盘组（包括范围），仅用于新存储池 • **[-H disk *[id1]:[id2]:..*]**此选项定义热备件组，仅用于新存储池 • **-target *target_id*** 为： – ***ctrl[x]***[5]
-help	显示命令用法和选项	

注：

1. 只有在 **IMM** 可访问 **RAID** 控制器的服务器上支持此命令。
2. 仅显示关联的控制器、磁盘和 **Flash DIMM** 的固件信息。而不显示关联的池和卷的固件信息。
3. 因空间有限，信息显示在多行上。
4. 只有在支持 **RAID** 日志的服务器上支持此命令。
5. 只有在支持 **RAID** 配置的服务器上支持此命令。
6. ***Enable*** 值不支持 **RAID** 级别 **1** 配置。
7. 此处列出一部分可用选项的列表。以下行中列出 **storage -config vol -add** 命令的其余选项。

语法：

```
storage [options]
option:
 -config ctrl/drv/vol -option [-options] -target target_id
 -list controllers/pools/volumes/drives
 -list pools -target ctrl[x]
 -list volumes -target ctrl[x]/pool[x]
 -list drives -target ctrl[x]/pool[x]
 -list devices
 -list flashdimms
 -show target_id
 -show {ctrl[x]/pool[x]/disk[x]/vol[x]/flashdimm[x]} info
 -show {ctrl[x]/disk[x]/flashdimm[x]}firmware
 -showlog ctrl[x]m:n/all
  -h help
```

示例：

```
system> storage
-config ctrl -clrcfg -target ctrl[0]
ok
system>
system> storage
-config ctrl -clrforgn -target ctrl[0]
ok
system>
system> storage
-config ctrl -imptforgn -target ctrl[0]
ok
```

```
system>
system> storage
-config ctrl -scanforgn -target ctrl[0]
Detect 1 foreign configuration(s) on controller ctrl[0]
system>
system> storage
-config drv -addhsp -dedicated pool[0-1] -target disk[0-0]
ok
system>
system> storage
-config drv -addhsp -target disk[0-0]
ok
system>
system> storage
-config drv -mkbad -target disk[0-0]
ok
system>
system> storage
-config drv -mkgood -target disk[0-0]
ok
system>
system> storage
-config drv -mkmissing -target disk[0-0]
ok
system>
system> storage
-config drv -mkoffline -target disk[0-0]
ok
system>
system> storage
-config drv -mkonline -target disk[0-0]
ok
system>
system> storage
-config drv -prprm -target disk[0-0]
ok
system>
system> storage
-config drv -rmhsp -target disk[0-0]
ok
system>
system> storage
-config drv -undoprprm -target disk[0-0]
ok
system>
system> storage
-config vol -add -1 1 -target pool[0-1]
ok
system>
system> storage
-config vol -add -R 1 -D disk[0-0]:disk[0-1] -w 1 -r 2 -i 0 -a 0 -d 0 -f 0
-N LD_volume -S 100000 -P 64K -H disk[0-2] -target ctrl[0]
ok
system>
system> storage
-config vol -getfreecap -R 1 -D disk[0-0]:disk[0-1] -H disk[0-2] -target ctrl[0]
The drive group configuration is good with free capacity 500000MB
system>
system> storage
-config vol -remove -target vol[0-1]
ok
```

```
system>
system> storage
-config vol -set -N LD_volume -w 0 -target vol[0-0]
ok
system>
system> storage
-list controllers
ctrl[0]   ServerRAID M5110e(Slot No. 0)
ctrl[1]   ServerRAID M5110f(Slot No. 1)
system>
system> storage
-list drives
disk[0-0]   Drive 0
disk[0-1]   Drive 1
disk[0-2]   Drive 2
system>
system> storage
-list flashdimms
flashdimm[1]   Flash DIMM 1
flashdimm[4]   Flash DIMM 4
flashdimm[9]   Flash DIMM 9
system>
system> storage
-list pools
pool[0-0]   Storage Pool 0
pool[0-1]   Storage Pool 1
system>
system> storage
-list volumes
system>storage -list volumes
vol[0-0]   Volume 0
vol[0-1]   Volume 1
Vol[0-2]   Volume 2
system>
system> storage
-list drives -target ctrl[0]
disk[0-0]   Drive 0
disk[0-1]   Drive 1
disk[0-2]   Drive 2
system>
system> storage
-list drives -target pool[0-0]
disk[0-0]   Drive 0
disk[0-1]   Drive 1
system>
system> storage
-list pools -target ctrl[0]
pool[0-0]   Storage Pool 0
system>
system> storage
-list volumes -target ctrl[0]
vol[0-0]   Volume 0
vol[0-1]   Volume 1
system>
system> storage
-list volumes -target pool[0-0]
vol[0-0]   Volume 0
vol[0-1]   Volume 1
system>
system> storage
-show ctrl[0] firmware
```

```
Total Firmware number: 2
Name: RAID Firmware1
Description: RAID Firmware
Manfacture: IBM
Version: 4.01(3)T
Release Date: 01/05/2013
Name: RAID Firmware2
Description: RAID Firmware
system>
system> storage
-show ctrl[0] info
Product Name: ServerRAID M5110e
Firmware Package Version: 23.7.0.1.2
Battery Backup: Installed
Manufacture: IBM
UUID: 1234567890123456
Model Type / Model: 1234AHH
Serial No.: 1234567890
FRU No.: 5005076049CC4
Part No.: LSI2004
Cache Model Status: Unknown
Cache Model Memory Size: 300MB
Cache Model Serial No.: PBKUD0XTA0P04Y
PCI Slot Number: 0
PCI Bus Number: 2
PCI Device Number: 2
PCI Function Number: 10
PCI Device ID: 0x1000
PCI Subsystem Device ID: 0x1413
Ports: 2
Port 1: 12345678901234
Port 2: 12345678901235
Storage Pools: 2
pool[0-0] Storage Pool 0
pool[0-1] Storage Pool 1
Drives: 3
disk[0-0]  Drive 0
disk[0-1]  Drive 1
disk[0-2]  Drive 2
system>
system> storage
-show disk[0-0] firmware
Total Firmware number: 1
Name: Drive
Description:
Manufacture:
Version: BE24
Release Date:
system>
system> storage
-show disk[0-0] info
Product Name: ST98394893
State: Online
Slot No.: 0
Disk Type: SATA
Media Type: HHD
Health Status: Normal
Capacity: 100.000GB
Speed: 6.0Gb/s
Current Temperature: 33C
Manufacture: ATA
```

```
Device ID: 5
Enclusure ID: 0x00FC
Machine Type:
Model:
Serial No.: 9XKJKL
FRU No.:
Part No.:
system>
system> storage
-show flashdimm[15]
Name: CPU1 DIMM 15
Health Status: Normal
Operational Status: Online
Capacity(GB): 400GB
Model Type: DDR3
Part Number: 93E40400GGM101PAT
FRU S/N: 44000000
Manuf ID: Diablo Technologies
Temperature: 0C
Warranty Writes: 100%
Write Endurance: 100%
F/W Level: A201.0.0.49152
system>
system> storage
-show pool[0-0]
RAID State: RAID 0
RAID Capacity: 67.000GB (0.000GB free)
Drives: 2
disk[0-0]   Drive 0
disk[0-1]   Drive 1
Volumes: 2
vol[0-0]   Volume 0
vol[0-1]   Volume 1
system>
system> storage
-show pool[0-1] info
RAID State: RAID 1
RAID Capacity: 231.898GB (200.000GB free)
Holes: 2
#1 Free Capacity: 100.000GB
#2 Free Capacity: 100.000GB

Drives: 2
disk[0-1]   Drive 1
disk[0-2]   Drive 2

Volume: 1
vol[0-1]   LD_volume
system>
system> storage
-show vol[0-0]
Name: Volume 0
Stripe Size: 64KB
Status: Offline
Capacity: 100.000GB
system>
system> storage
-show vol[0-0] info
Name: LD_volume
Status: Optimal
Stripe Size: 64KB
```

```
Bootable: Not Bootable
Capacity: 231.898GB
Read Policy: No Read Ahead
Write Policy: Write Through
I/O Policy: Direct I/O
Access Policy: Read Write
Disk Cache Policy: Unchanged
Background Initialization: Enable
system>
```

adapter 命令

此命令用于显示 **PCIe** 适配器清单信息。

如果不支持 **adapter** 命令，则服务器在发出该命令时用以下消息进行响应：
Your platform does not support this command.
如果卸下、更换或配置任何适配器，则必须重新启动服务器（至少一次）才能查看更新后的适配器信息。

下表显示选项的参数。

表 67. adapter 命令

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

选项	描述	值
-list	列出服务器中的所有 **PCIe** 适配器	
-show ***target_id***	显示目标 **PCIe** 适配器的详细信息	***target_id [info|firmware|ports|chips]*** 其中： • ***info***：显示适配器的硬件信息 • ***firmware***：显示适配器的所有固件信息 • ***ports***：显示适配器的所有以太网端口信息 • ***chips***：显示适配器的所有 **GPU** 芯片信息
-h	显示命令用法和选项	

语法：

```
adapter [options]
option:
 -list
 -show target_id [info|firmware|ports|chips]
  -h help
```

示例：

```
system> adapter
list
ob-1   Flex System CN4054 10Gbps Virtual Fabric Adapter
ob-2   GPU Card 1
slot-1  Raid Controller 1
```

```
slot-2  Adapter 01:02:03

system> adapter
show ob-1 info
Product Name: Flex System CN4054 10Gbps Virtual Fabric Adapter
Card Interface: PCIe x 16
Function Count: 2

Function Name: xxx Emulx xx component1
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1
Class Code: 2
Sub Vendor: 334
Sub Device: 223
Slot Description: a slot
Slot Type: 23
Slot Data Bus Width: 0
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
Model: 345
Function Sku: 221
Fod Uid: 2355
Required Daughter: 0
Max Data Width: 0
Connector Layout: pci x

Package Type: dici
Function Name: xxx nVidia xx component2
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1
Class Code: 2
Sub Vendor: 334
Sub Device: 223
Slot Description: a slot
Slot Type: 23
Slot Data Bus Width: 0
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
Model: 345
Function Sku: 221
Fod Uid: 2355
```

```
Required Daughter: 0
Max Data Width: 0
Connector Layout: pci x
Package Type: dici
```

mvstor 命令

使用此命令可获得与 **M.2** 相关的清单信息并管理虚拟卷。

下表显示选项的参数。

表 68. mvstor 命令

下表是一个多行两列的表格，由选项和选项描述组成。

选项	描述
-h/?	打印此命令的帮助信息
-version	显示控制器固件信息
-disks	显示介质磁盘信息
-volumes	显示虚拟卷信息
-create	创建一个虚拟卷，可以指定 **VD_Name**，**RaidLevel** 和 **StripeSize**
-delete	删除虚拟卷
-import	导入一个外部虚拟卷。导入该虚拟卷后，系统重新启动将自动重建该虚拟卷。

用法

```
 mvstor [-options] - raid configuration for SATA/NVMe RAID boot solution.
options:
  -version            - displays controller firmware version.
  -disks             - displays information of media disks.
  -volumes            - displays information of virtual disks
  -create -slot <slot_no> -name <vd name> -level <0|1> -stripe <32|64|128|256|512> - create virtual volume.
    Marvell SATA RAID: stripe size can only be 32k or 64k
    Marvell NVMe RAID: vd name is unapplicable. The name will always be VD_0.
  -delete -slot <slot_no> -id <0|1>      - delete the virtual volume
  -import -slot <slot_no> -id <0|1>      - import a foreign virtual volume
```

示例

```
system> mvstor -version
  Controller Slot    Device Name                          Version
1          ThinkSystem M.2 SATA 2-Bay RAID Enablement Kit     2.3.20.1203


system> mvstor -disks
 Controller Slot 1   M.2 Bay0     128GB M.2 SATA SSD   LEN
 Controller Slot 1   M.2 Bay1     128GB M.2 SATA SSD   LEN

system> mvstor -volumes
Controller Slot 1:
  VD_ID:     0
  VD_Name:    VD_Test
  PD_Member:   0,1
  RaidLevel:   1
```

```
  StripSize:  64k
  VD_Capacity: 117 GB
  VD_Status:  Optimal
    1        64k       29 GB       Optimal

system> mvstor -delete –slot 1 -id 0
VD_ID 0 is deleted

system> mvstor -create –slot 1 -name M2RAID -level 1 -strip 64
New volume is created

system> mvstor -import –slot 1 -id 0
VD_ID 0 is imported
```

支持命令

本主题按字母顺序提供支持命令的列表。

仅有一条支持命令：第 175 页 “dbgshimm 命令”。

dbgshimm 命令

使用此命令可解锁网络访问权限以安全调试 **shell**。

注：此命令仅供支持人员使用。

下表显示选项的参数。

表 69. dbgshimm 命令

下表是一个多行两列的表格，由选项和选项描述组成。

选项	描述
状态	显示状态
启用	允许调试访问（未指定任何选项时的默认值）
禁用	禁用调试访问

第 11 章　IPMI 接口

本章介绍 XClarity Controller 支持的 IPMI 接口。

有关标准 IPMI 命令的详细信息，请参阅《智能平台管理接口（IPMI）规范》文档（2.0 或更高版本）。本文档提供与 XClarity Controller 固件支持的标准 IPMI 和 OEM IPMI 命令一起使用的 OEM 参数的说明。

使用 IPMI 管理 XClarity Controller

按本主题中的信息使用智能平台管理接口（IPMI）管理 XClarity Controller。

XClarity Controller 的初始用户 ID 设置为用户名为 USERID，密码为 PASSW0RD（包含数字零而不是字母 O）。此用户具有主管访问权限。

重要：请在初始配置期间更改此用户名和密码以增强安全性。

在 Flex System 中，用户可配置 Flex System CMM 集中管理 XClarity Controller IPMI 用户帐户。此情况下，CMM 完成 IPMI 用户 ID 配置前您可能无法使用 IPMI 访问 XClarity Controller。

注：CMM 配置的用户 ID 凭证可能与上述 USERID/PASSW0RD 组合不同。如果 CMM 未配置 IPMI 用户 ID，则与 IPMI 协议关联的网络端口将关闭。

XClarity Controller 还提供以下 IPMI 远程服务器管理能力：

IPMI 命令行界面
IPMI 命令行界面使您可通过 IPMI 2.0 协议直接访问服务器管理功能。您可以使用 IPMItool 发出命令以控制服务器电源、查看服务器信息和识别服务器。有关 IPMItool 的更多信息，请参阅第 177 页 “使用 IPMItool”。

Serial over LAN
要从远程位置管理服务器，请使用 IPMItool 建立 Serial over LAN（SOL）连接。有关 IPMItool 的更多信息，请参阅第 177 页 “使用 IPMItool”。

使用 IPMItool

按本主题中的信息访问关于 IPMItool 的信息。

IPMItool 提供各种可用于管理和配置 IPMI 系统的工具。可以使用带内或带外 IPMItool 来管理和配置 XClarity Controller。

有关 IPMItool 的更多信息或要下载 IPMItool，请转至 https://github.com/ipmitool/ipmitool。

IPMI 命令和 OEM 参数

获取/设置 LAN 配置参数

为反映 XCC 为某些网络设置提供的功能，部分参数数据的值如下定义。

DHCP

除了获取 IP 地址的常用方法外，XCC 还提供了一种模式：在该模式下，XCC 会在给定的时间段内尝试从 DHCP 服务器获取 IP 地址，如果不成功，则将故障转移到使用静态 IP 地址。

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

参数	#	参数数据
IP 地址源	4	数据 1 [7:4] – 已保留 [3:0] – 地址源 0h = 未指定 1h = 静态地址（手动配置） 2h = XCC 运行 DHCP 获得的地址 3h = BIOS 或系统软件获得的地址 4h = XCC 运行其他地址分配协议获得的地址。 XCC 使用值 4h 指示故障转移到静态地址的 DHCP 地址模式。

以太网接口选择

XCC 硬件包含带有 RMII 接口的双 10/100 以太网 MAC。XCC 硬件还包含带有 RGMII 接口的双 1Gbps 以太网 MAC。其中一个 MAC 通常连接到共享服务器 NIC，另一个 MAC 用作专用系统管理端口。在给定时间，服务器上只有一个以太网端口处于活动状态。两个端口不会同时启用。

在某些服务器上，系统设计者可以选择仅连接系统平板上这些以太网接口中的一个或另一个。在这些系统中，XCC 仅支持在平面上连接的以太网接口。使用未连接端口的请求将返回 CCh 完成代码。

所有可选网卡的包 IDS 编号如下：

- 可选卡 #1，包标识 = 03h（eth2），
- 可选卡 #2，包标识 = 04h（eth3），

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

参数	#	参数数据
OEM 参数 XCC 使用此参数号指示应使用哪个可用的以太网端口（逻辑包）。 “获取/设置 LAN 配置参数”命令中的此参数不使用组选择	C0h	数据 1 00h = eth0 01h = eth1 02h = eth2 以此类推...

参数	#	参数数据
器或不需要块选择器，因此这些字段应设置为 **00h**。 响应数据将返回 **3** 个字节，如果设备在 **NCSI** 包中，则返回 **4** 个字节（可选）。 字节 **1** = 完成代码 字节 **2** = 修订 字节 **3** = **00h**（对于 **eth0**）或 **01h**（对于 **eth1**），以此类推… 字节 **4** =（可选）通道号（如果设备是 **NCSI** 包）		**FFh** = 禁用所有外部网络端口 **XCC** 还支持一个可选数据字节，以指定使用包中的哪个通道 数据 **2** **00h** = 通道 **0** **01h** = 通道 **1** 以此类推... 如果请求中未指定数据 **2**，则假定为通道 **0**

数据 **1** 字节用于指定逻辑包。它可能是专用系统管理 **NIC** 或与服务器共享的 **NIC** 中的 **NCSI** 接口。

如果包是 **NCSI** 设备，则数据 **2** 字节用于指定逻辑包的通道。如果请求中未指定数据 **2** 并且逻辑包是 **NCSI** 设备，则假定为通道 **0**。如果请求中未指定数据 **2**，但逻辑包不是 **NCSI** 设备，则忽略通道信息。

示例：

附录 **A.** 如果要将平面上的共享 **NIC** 的通道 **2**（包标识 = **0**，**eth0**）用作管理端口，则输入数据为：**0xC0 0x00 0x02**

附录 **B**：如果要使用第一个网络夹层卡的第一个通道，则输入为：**0xC0 0x02 0x0**

启用/禁用 Ethernet over USB

以下参数用于启用或禁用 **XCC** 带内接口。

下表是一个多行三列表格，包含选项、选项描述和选项关联值的信息。

参数	#	参数数据
OEM 参数 （**XCC** 使用此参数号来启用或禁用 **Ethernet over USB** 接口。） “获取 **LAN** 配置参数”命令中的此参数不使用组选择器或不需要块选择器，因此这些字段应设置为 **00h**。 响应数据将返回 **3** 个字节：	**C1h**	数据 **1** **0x00** = 已禁用 **0x01** = 已启用

参数	#	参数数据
字节 **1** = 完成代码 字节 **2** = 修订 字节 **3** = **00h**（已禁用）或 **01h**（已启用）		

数据 **1** 字节用于指定逻辑包。它可能是专用系统管理 **NIC** 或与服务器共享的 **NIC** 中的 **NCSI** 接口。

如果包是 **NCSI** 设备，则数据 **2** 字节用于指定逻辑包的通道。如果请求中未指定数据 **2** 并且逻辑包是 **NCSI** 设备，则假定为通道 **0**。如果请求中未指定数据 **2**，但逻辑包不是 **NCSI** 设备，则忽略通道信息。

示例：

附录 **A.** 如果要将平面上的共享 **NIC** 的通道 **2**（包标识 = **0**，**eth0**）用作管理端口，则输入数据为：**0xC0 0x00 0x02**

附录 **B**：如果要使用第一个网络夹层卡的第一个通道，则输入为：**0xC0 0x02 0x0**

用于获取 DUID-LLT 的 IPMI 选项

需要通过 **IPMI** 公开的另一个只读值是 **DUID**。根据 **RFC3315**，此格式的 **DUID** 基于链路层地址加时间。

参数	#	参数数据
OEM 参数 （**XCC** 使用此参数号来启用或禁用 **Ethernet over USB** 接口。） “获取 **LAN** 配置参数”命令中的此参数不使用组选择器或不需要块选择器，因此这些字段应设置为 **00h**。 响应数据将返回 **3** 个字节： 字节 **1** = 完成代码 字节 **2** = 参数修订（如 **IPMI** 规范） 字节 **3** = 后续数据字节的长度（当前为 **16** 个字节） 字节 **4-n DUID_LLT**	**C2h**	

以太网配置参数

以下参数可用于配置特定以太网设置。

参数	#	参数数据
OEM 参数 （XCC 使用此参数号来启用或禁用以太网接口的自动协商设置。） 响应数据将返回 3 个字节： 字节 1 = 完成代码 字节 2 = 修订 字节 3 = 00h（已禁用）或 01h（已启用）	C3h	数据 1 0x00 = 已禁用 0x01 = 已启用 注：在 Flex 和 Stark 系统上，自动协商设置不可更改，因为它可能会破坏通过 CMM 和 SMM 的网络通信路径。
OEM 参数 （XCC 使用此参数号来获取或设置以太网接口的数据速率。） 响应数据将返回 3 个字节： 字节 1 = 完成代码 字节 2 = 修订 字节 3 = 00h（10Mb）或 01h（100Mb）	C4h	数据 1 0x00 = 10 Mb 0x01 = 100 Mb
OEM 参数 （XCC 使用此参数号来获取或设置以太网接口的双工设置。） 响应数据将返回 3 个字节： 字节 1 = 完成代码 字节 2 = 修订 字节 3 = 00h（半双工）或 01h（全双工）	C5h	数据 1 0x00 = 半双工 0x01 = 全双工
OEM 参数 （XCC 使用此参数号来获取或设置以太网接口的 MTU。） 响应数据将返回 3 个字节： 字节 1 = 完成代码 字节 2 = 修订 字节 3-4 = MTU 的大小	C6h	数据 1 MTU 的大小
OEM 参数	C7h	数据 1 - 6

参数	#	参数数据
（XCC 使用此参数号来获取或设置本地管理的 MAC 地址。） 响应数据将返回 3 个字节： 字节 1 = 完成代码 字节 2 = 修订 字节 3 – 8 = Mac 地址		MAC 地址

IPMI 选项用于获取链路本地地址

此为只读参数，用于检索 IPV6 链路本地地址。

参数	#	参数数据
OEM 参数 此参数用于获取 XCC 的链路本地地址： 响应数据将返回以下内容： 字节 1 = 完成代码 字节 2 = 参数修订（如 IPMI 规范） 字节 3 = IPV6 地址前缀长度 字节 4-19 链路本地地址（二进制格式）	C8h	

用于启用/禁用 IPv6 的 IPMI 选项

此为用于在 XCC 中启用/禁用 IPV6 的读/写参数。

参数	#	参数数据
OEM 参数 此参数用于在 XCC 中启用/禁用 IPv6 响应数据将返回以下内容： 字节 1 = 完成代码 字节 2 = 参数修订（如 IPMI 规范） 字节 3 = 00h（已禁用）或 01h（已启用）	C9h	数据 1 0x00 = 已禁用 0x01 = 已启用

Ethernet-over-USB 直通外部网络

以下参数用于将 Ethernet-over-USB 配置为外部以太网直通。

参数	#	参数数据
OEM 参数 “获取/设置 LAN 配置参数”命令中的此参数不使用组选择器或不需要块选择器，因此这些字段应设置为 00h。 获取响应数据将返回以下内容： 字节 1 = 完成代码 字节 2 = 修订 字节 3 = 已保留（00h） 字节 4：5 = Ethernet-over-USB 端口号（最低有效字节在前） 字节 6:7 = 外部以太网端口号（最低有效字节在前） 接下来的字节数根据寻址模式而有所不同（1、4、16 字节）： • 字节 8 = 预定义模式： 00h = 已禁用直通 01h = 使用了 CMM IP 地址 字节 8:11 = 二进制形式的 IPv4 外部网络 IP 地址 字节 8:23 = 二进制形式的 IPv6 外部网络 IP 地址 完成代码： 00h – 成功 80h – 不支持该参数 C1h – 不支持该命令 C7h – 请求数据长度无效	CAh	设置 LAN 配置参数： 数据 1 已保留（= 00h） 数据 2:3 Ethernet over USB 端口号，最低有效字节在前 数据 4:5 外部以太网端口号，最低有效字节在前 接下来的字节数根据寻址模式而有所不同（1、4、16 字节）： 数据 6 00h = 禁用直通 01h = 使用 CMM IP 地址 数据 6:9 二进制形式的 IPv4 外部网络 IP 地址 数据 6:21 二进制形式的 IPv6 外部网络 IP 地址
OEM 参数 此参数用于设置和获取 XCC 的 lan over usb IP 地址和网络掩码： 响应数据将返回以下内容： 字节 1 = 完成代码	CBh	数据 1:4 XCC 侧 lan over usb 接口的 IP 地址。 数据 5:8 XCC 侧 lan over usb 接口的网络掩码

参数	#	参数数据
字节 **2** = 参数修订（如 **IPMI** 规范） 字节 **3:10** = **IP** 地址和网络掩码值（最高有效字节在前）		
OEM 参数 此参数用于设置和获取主机操作系统的 **lan over usb IP** 地址： 响应数据将返回以下内容： 字节 **1** = 完成代码 字节 **2** = 参数修订（如 **IPMI** 规范） 字节 **3:6** = **IP** 地址（最高有效字节在前）	**CCh**	数据 **1:4** 主机侧 **lan over usb** 接口的 **IP** 地址。

查询逻辑包清单

以下参数用于查询 **NCSI** 包清单。

参数	#	参数数据
OEM 参数 “获取/设置 **LAN** 配置参数”命令中的此参数不使用组选择器或不需要块选择器，因此这些字段应设置为 **00h**。 查询包清单操作 通过发出带有 **D3h** 参数号和两个 **0x00** 数据字节的请求来执行查询包信息操作。 查询包清单： **--> 0x0C 0x02 0x00 0xD3 0x00 0x00** 对于每个存在的包，**XCC** 响应包含一个信息字节： 位 **7:4** = 包中 **NCSI** 通道的数量 位 **3:0** = 逻辑包编号 响应	**D3h**	获取/设置 **LAN** 配置参数：

参数	#	参数数据
--> 0x00 0x00 0x40 0x01 0x32 指示存在 **3** 个逻辑包： 包 **0** 具有 **4** 个 **NCSI** 通道 包 **1** 不是 **NCSI NIC**，因此不支持 **NCSI** 通道 包 **2** 具有 **3** 个 **NCSI** 通道		

获取/设置逻辑包数据

以下参数用于读取和设置分配给每个包的优先级。

参数	#	参数数据
OEM 参数 “获取/设置 **LAN** 配置参数”命令中的此参数不使用组选择器或不需要块选择器，因此这些字段应设置为 **00h**。 该命令支持 **2** 个操作： • 读取包优先级 • 设置包优先级 读取包优先级操作 通过发出带有 **D4h** 参数号和两个 **0x00** 数据字节的请求来执行读取包优先级操作。 读取包优先级： **--> 0x0C 0x02 0x01 0xD4 0x00 0x00** 响应 **--> 0x00 0x00 0x00 0x12 0x23** 逻辑包 **0** = 优先级 **0** 逻辑包 **2** = 优先级 **1** 逻辑包 **3** = 优先级 **2** 设置包优先级操作 通过发出带有 **D4h** 参数号和一个或更多参数的请求来执行设置包优先级操作。	**D4**	获取/设置 **LAN** 配置参数： 位 **[7-4]** = 逻辑包的优先级（**1** = 最高，**15** = 最低） 位 **[3-0]** = 逻辑包编号

参数	#	参数数据
设置包优先级： **--> 0x0C 0x01 0x01 0xD4 0x00 0x12 0x23** 设置逻辑包 **0** = 优先级 **0** 设置逻辑包 **2** = 优先级 **1** 设置逻辑包 **3** = 优先级 **2** 响应： 仅完成代码，没有其他数据		

获取/设置 XCC 网络同步状态

参数	#	参数数据
OEM 参数 该字节用于配置以在专用和共享 **nic** 模式之间同步网络设置 “获取 **LAN** 配置参数”命令中的此参数不使用组选择器或不需要块选择器，因此这些字段应设置为 **00h**。 响应数据将返回 **3** 个字节： 字节 **1** = 完成代码 字节 **2** = 修订 字节 **3** = **00h**（已启用）或 **01h**（已禁用）	**D5h**	数据 **1** **0x00** = 同步 **0x01** = 独立

该字节用于配置以在专用和共享 **nic** 模式之间同步网络设置，此处的默认值为 **0h**，这意味着 **XCC** 将自动更新模式更改之间的网络设置，并使用共享 **nic**（板载）作为主要参考。如果设置为 **1h**，每个网络设置在此处均为独立，即可以在模式之间配置不同的网络设置，例如在专用模式中设置 **VLAN** 启用以及在共享 **NIC**模式中的设置 **VLAN** 禁用。

获取/设置 XCC 网络模式

参数	#	参数数据
OEM 参数 此参数用于获取/设置 XCC 管理 NIC 的网络模式。 响应数据将返回 4 个字节： 字节 1 = 完成代码 字节 2 = 修订 字节 3 = 已应用/指定的网络模式 字节 4 = 应用的网络模式的包标识 字节 5 = 应用的网络模式的通道标识	D6h	设置 LAN 配置参数： 数据 1 要设置的网络模式 获取 LAN 配置参数： 数据 1 要获取的网络模式，此为可选数据，默认为查询当前的网络模式

OEM IPMI 命令

XCC 支持以下 IPMI OEM 命令。每个命令需要不同的权限级别，如下所示。

代码	Netfn 0x2E 命令	权限
0xCC	将 XCC 重置为默认设置	PRIV_USR

代码	Netfn 0x3A 命令	权限
0x00	查询固件版本	PRIV_USR
0x0D	板信息	PRIV_USR
0x1E	机箱电源恢复延迟选项	PRIV_USR
0x38	NMI 和重置	PRIV_USR
0x49	发起数据收集	PRIV_USR
0x4A	推送文件	PRIV_USR
0x4D	数据收集状态	PRIV_USR
0x50	获取 Build 信息	PRIV_USR
0x55	获取/设置主机名	PRIV_USR
0x6B	查询 FPGA 固件修订级别	PRIV_USR
0x6C	查询板硬件修订级别	PRIV_USR
0x6D	查询 PSoC 固件修订级别	PRIV_USR

代码	Netfn 0x3A 命令	权限
0x98	前面板 USB 端口控制	PRIV_USR
0xC7	本机 NM IPMI 交换机	PRIV_ADM

将 XCC 重置为默认设置命令

此命令将 XCC 配置设置重置为默认值。

网络功能 = 0x2E			
代码	命令	请求、响应数据	描述
0xCC	将 XCC 重置为默认设置	**请求:** 字节 1 – 0x5E 字节 2 – 0x2B 字节 3 – 0x00 字节 4 – 0x0A 字节 5 – 0x01 字节 6 – 0xFF 字节 7 – 0x00 字节 8 – 0x00 字节 9 – 0x00 **响应:** 字节 1 – 完成代码 字节 2 – 0x5E 字节 3 – 0x2B 字节 4 – 0x00 字节 5 – 0x0A 字节 6 – 0x01 字节 7 – 响应数据 0 = 成功 非 0 = 失败	此命令将 XCC 配置设置重置为默认值。

板/固件信息命令

本节列出了用于查询板和固件信息的命令。

网格功能 = 0x3A			
代码	**命令**	**请求、响应数据**	**描述**
0x00	查询固件版本	**请求：** 无请求的数据 **响应：** 字节 **1** – 完成代码 字节 **2** – 主要版本 字节 **3** – 次要版本	此命令返回固件的主要和次要版本号。如果使用可选的 **1** 字节请求数据发出命令，则 **XCC** 响应还会返回版本的第三个字段（修订号）。 （主要.次要.修订）
0x0D	查询板信息	**请求**：不适用 **响应：** 字节 **1** – 系统标识 字节 **2** – 板修订号	此命令返回板标识和平板修订号。
0x50	查询 **Build** 信息	**请求**：不适用 **响应：** 字节 **1** – 完成代码。 字节 **2:10** – **ASCIIZ Build** 名称 字节 **11:23** – **ASCIIZ Build** 日期 字节 **24:31** – **ASCII Build** 时间	此命令返回 **Build** 名称，**Build** 日期和 **Build** 时间。**Build** 名称和 **Build** 日期字符串以零终止。 **Build** 日期格式为 **YYYY-MM-DD**。 例如，“**ZUBT99A**” “**2005-03-07**” “**23:59:59**”
0x6B	查询 **FPGA** 固件修订级别	**请求：** 字节 **1** – **FPGA** 设备类型* **FPGA** 设备类型 **0** = 本地（活动级别） **1** = **CPU** 卡 **1**（活动级别） **2** = **CPU** 卡 **2**（活动级别） **3** = **CPU** 卡 **3**（活动级别） **4** = **CPU** 卡 **4**（活动级别） **5** = 本地主要 **ROM** **6** = 本地恢复 **ROM**	此命令返回 **FPGA** 固件的修订级别。 如果省略字节 **1**，则将选择本地（活动级别）

网格功能 = 0x3A			
代码	**命令**	**请求、响应数据**	**描述**
		响应： 字节 **1** – 完成代码 字节 **2** – 主要修订级别 字节 **3** – 次要修订级别 字节 **4** – 次要子修订级别 （**XCC** 平台上的测试字节）	
0x6C	查询板硬件修订级别	**请求：** 无数据。 **响应：** 字节 **1** – 完成代码 字节 **2** – 修订级别	此命令返回 **FPGA** 所在板硬件的修订级别。
0x6D	查询 **PSoC** 固件修订级别	**请求：** 无 **响应：** 字节 **1** – 完成代码 字节 **2** – **bin#** 字节 **3** – **APID** 字节 **4** – 修订号 字节 **5-6** – **FRU** 标识 字节 **6**：**N** – 对每个检测到的 **PSoC** 重复字节 **2-6**	此命令返回所有检测到的 **PSoC** 设备的修订级别。 注：**bin#** 代表物理位置。有关详细信息，请查阅系统规格。

系统控制命令

IPMI 规格提供基本电源和重置控制。**Lenovo** 增加了其他控制功能。

<table>
<tr><th colspan="4">网络功能 = 0x2E</th></tr>
<tr><th>代码</th><th>命令</th><th>请求、响应数据</th><th>描述</th></tr>
<tr><td>0x1E</td><td>机箱电源恢复延迟选项</td><td>请求：<table><tr><td>字节 1</td><td>请求类型：

0x00 = 设置延迟选项

0x01 = 查询延迟选项</td></tr><tr><td>字节 2</td><td>（如果字节 1= 0x00）

0x00 = 已禁用（默认）

0x01 = 随机

0x02 - 0xFF 已保留</td></tr></table>响应：

字节 1 – 完成代码

字节 2 – 延迟选项（仅适用于查询请求）</td><td>如果机箱电源恢复策略设置为交流电源通电/电源恢复时始终打开电源或恢复为打开电源（如果之前打开了电源），则使用此设置。有 2 个选择：已禁用（默认设置，打开电源时无延迟）和随机。随机延迟设置提供在交流电源通电/电源恢复以及服务器自动开机时发生 1 到 15 秒之间的随机延迟。

XCC 仅在机架服务器上支持该命令。</td></tr>
<tr><td>0x38</td><td>NMI 和重置</td><td>请求：

字节 1 – 秒数
0 = 仅限 NMI

字节 2 – 重置类型
0 = 软重置
1 = 关闭再打开电源

响应：

字节 1 – 完成代码</td><td>此命令用于执行系统 NMI。（可选）可以在 NMI 之后重置系统（重新引导）或关闭再打开电源。

如果“秒数”字段不为 0，则系统将在指定的秒数过后重置或关闭再打开电源。

请求的字节 2 为可选。如果未提供字节 2，或者字节 2 的值为 0x00，则将执行软重置。如果字节 2 为 0x01，则将关闭再打开系统电源。</td></tr>
</table>

其他命令

本节收录了其他各节不适用的命令。

<table>
<tr><th colspan="4">网格功能 = 0x3A</th></tr>
<tr><th>代码</th><th>命令</th><th>请求、响应数据</th><th>描述</th></tr>
<tr><td>0x55</td><td>获取/设置主机名</td><td>请求长度 = 0：

空请求数据

响应：

<table><tr><td>字节 1</td><td>完成代码</td></tr><tr><td>字节 2-65</td><td>当前主机名。

ASCIIZ，以 Null 终止的字符串。</td></tr></table>
请求长度 1-64：

<table><tr><td>字节 1-64</td><td>DHCP 主机名

ASCIIZ 以 00h 终止</td></tr></table></td><td>使用此命令获取/设置主机名。

设置主机名时，所需的值必须以 00h 终止。主机名限制为 63 个字符（包括 null 在内）。</td></tr>
<tr><td>0x98</td><td>前面板 USB 端口控制</td><td>请求：

字节 1

<table><tr><td>01h：</td><td>获取前面板 USB 端口的当前所有者</td></tr></table>
响应：

字节 1 – 完成代码

字节 2

<table><tr><td>00h：</td><td>由主机所有</td></tr><tr><td>01h：</td><td>由 BMC 所有</td></tr></table>
请求：

字节 1

<table><tr><td>02h：</td><td>获取前面板 USB 端口的配置</td></tr></table>
响应：</td><td>此命令用于查询前面板 USB 端口的状态/配置，配置前面板 USB 端口的模式/超时以及在主机和 BMC 之间切换 USB 端口所有者

在配置中，前面板 USB 可以有 3 种模式 – 主机专用、BMC 独占或允许所有者在主机和 BMC 之间切换的共享模式。

如果启用了共享模式，则关闭服务器电源时，USB 端口将连接到 BMC；打开服务器电源时，USB 端口将连接到服务器。

启用共享模式并打开服务器电源后，如果发生了配置中的空闲超时，BMC 会将 USB 端口返回给服务器。

如果服务器具有标识按钮，则用户可以通过长按标识按钮 3 秒钟以上来启用/禁用标识按钮以切换前面板 USB 端口的所有者。</td></tr>
</table>

<table>
<tr><th colspan="4">网格功能 = 0x3A</th></tr>
<tr><th>代码</th><th>命令</th><th>请求、响应数据</th><th>描述</th></tr>
<tr><td></td><td></td><td>字节 1 – 完成代码

字节 2

<table><tr><td>00h:</td><td>主机专用</td></tr><tr><td>01h:</td><td>BMC 专用</td></tr><tr><td>02h:</td><td>共享模式</td></tr></table>
字节 3:4 – 空闲超时，以分钟为单位（最高有效字节在前）

字节 5 – 启用标识按钮

<table><tr><td>00h:</td><td>已禁用</td></tr><tr><td>01h:</td><td>已启用</td></tr></table>
字节 6 – 滞后（可选），以秒为单位

请求：

字节 1

03h：设置前面板 USB 端口的配置

字节 2

<table><tr><td>00h:</td><td>主机专用</td></tr><tr><td>01h:</td><td>BMC 专用</td></tr><tr><td>02h:</td><td>共享模式</td></tr></table>
字节 3:4 – 空闲超时，以分钟为单位（最高有效字节在前）

字节 5 – 启用标识按钮

<table><tr><td>00h:</td><td>已禁用</td></tr><tr><td>01h:</td><td>已启用</td></tr></table>
字节 6 – 滞后（可选），以秒为单位

响应：</td><td>在关闭再打开电源期间自动切换端口时，会设置以秒为单位的滞后。此为可选参数。

SD530 服务器

在 SD530 平台上，该端口是可选的，并且如果存在，则直接连接到 XCC，并且仅连接到 XCC。无法将端口切换到主机。

• 当发出的命令中字节 1 = 1 时，XCC 始终响应该端口由 BMC 所有。
• 当发出的命令中字节 1 = 2 时，XCC 始终响应该端口由 BMC 专用。
• 当发出的命令中字节 1 = 3 或字节 1 = 4 时，XCC 响应完成代码 D6h。

非 SD530 服务器

在非 SD530 平台上，可以通过切换到“主机专用”模式来禁用 XCC 对前面板 USB 端口的使用。

当发出的命令中字节 1 = 5 或字节 1 = 6 时，XCC 响应完成代码 D6h。</td></tr>
</table>

<table>
<tr><th colspan="4">网格功能 = 0x3A</th></tr>
<tr><th>代码</th><th>命令</th><th>请求、响应数据</th><th>描述</th></tr>
<tr><td></td><td></td><td>字节 1 – 完成代码 字节 2
<table><tr><td>00h:</td><td>切换到主机</td></tr><tr><td>01h:</td><td>切换到 BMC</td></tr></table>
响应:
字节 1 – 完成代码
字节 1
<table><tr><td>05h:</td><td>启用/禁用前面板 USB 端口</td></tr></table>
字节 2
<table><tr><td>00h:</td><td>禁用</td></tr><tr><td>01h:</td><td>启用</td></tr></table>
响应:
字节 1 – 完成代码
请求:
字节 1
<table><tr><td>06h:</td><td>读取前面板 USB 端口的启用/禁用状态</td></tr></table>
响应:
字节 1 - 完成代码
字节 2</td><td></td></tr>
<tr><td>0xC7</td><td>本机 NM IPMI 交换机</td><td>请求长度 = 0:
空请求数据
响应:</td><td>此命令用于为本机 Intel IPMI 命令启用/禁用 XCC 的桥接功能。</td></tr>
</table>

<table>
<tr><th colspan="4">网格功能 = 0x3A</th></tr>
<tr><th>代码</th><th>命令</th><th>请求、响应数据</th><th>描述</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>字节 1</td><td>完成代码</td></tr>
<tr><td>字节 2</td><td>当前启用/禁用状态</td></tr>
</table>
请求长度 = 1:
<table>
<tr><td>字节 1</td><td>本机 NM IPMI 接口启用/禁用属性

00h – 禁用

01h – 启用</td></tr>
</table>
响应:
<table>
<tr><td>字节 1</td><td>完成代码</td></tr>
</table>
</td><td></td></tr>
</table>

第 12 章　Edge 服务器

本主题描述 **Edge** 服务器的特定功能。

注：

1. 首次登录时，系统会要求您更改 **XCC** 密码。
2. 默认情况下，**IPMI-over-LAN** 已禁用。
3. 默认情况下，**IPMI-over-KCS** 已禁用。

系统锁定模式

系统锁定模式处于活动状态时，表示系统处于锁定模式。您可以激活系统并对其进行解锁，否则将不允许引导主机系统。

单击 **BMC 配置**下的**安全性**，然后滚动到**系统锁定模式**。

系统锁定模式

要激活系统并退出**系统锁定模式**，请完成以下步骤。

1. 单击**非活动**按钮，随后将弹出一个 **Key Vault激活**窗口以显示**质询文本**。
2. 与您的 **IT** 管理员联系并提供**质询文本**。
3. 从您的 **IT** 管理员处获得**质询响应**，然后在 **Key Vault 激活**窗口中输入.
4. 单击**确定**按钮，然后单击**应用**。
5. 如果所有设置均正常运行，您将看到**系统锁定模式**更改为**非活动**。

注：系统锁定模式处于活动状态时，对系统机密的任何访问都将被**拒绝**，例如 **SED** 密钥。

要强制系统进入系统锁定模式，请完成以下步骤。

1. 单击**活动**按钮。
2. 单击**确定**按钮，然后单击**应用**。

运动检测

您可以启用此功能以检测服务器的任何物理移动，从而保护服务器。
如果启用了运动检测，可以根据自己的偏好和配置设置以下项目。

- **灵敏度级别：**根据偏好从**低**、**中**、**高**中选择灵敏度级别
- **方向：**从**立式桌面**、**壁挂式（水平）**、**壁挂式（垂直）**、**书架式**和**吊装**中选择您的配置。

注：系统进入锁定模式时，运动检测将自动禁用。

机箱入侵检测

您可以启用此功能以检测顶盖的任何物理移动，从而保护服务器。

其他配置

如果安装了支持无线的 **LOM** 封装，则对于检测到的篡改事件可以选择三种设置。
在某些特殊情况下，**质询文本**可能无法通过 **ThinkShield Key Vault Portal** 进行验证，此时在 **IT** 管理员的要求下激活设备之前可能需要重置设备内部计数器。

SED 认证密钥（AK）管理器

对于安装了 SED（自加密硬盘）的系统，此功能控制 BMC 以部署 SED 密钥。您可以使用 SED 密钥对引导和数据硬盘进行加密，且无需手动干预即可引导系统。

注：系统未激活（系统锁定模式生效）或当前用户无权管理 SED 密钥时，不允许执行此操作。

单击 BMC **配置**下的**安全性**，然后滚动到 **SED 认证密钥（AK）管理器**。

更改 SED AK

根据口令生成 SED AK：设置密码并重新输入密码进行确认。单击**重新生成**以获取新的 SED AK。

生成随机 SED AK：单击**重新生成**以获取随机 SED AK。

备份 SED AK：设置密码并重新输入密码进行确认。单击**开始备份**以备份 SED AK；然后，下载 SED AK 文件并将其存储在安全的地方以备将来使用。

注：如果使用备份 SED AK 文件来恢复配置，系统将询问此处设置的密码。

恢复 SED AK：仅在 SED 无法正常工作时才能执行此任务。可通过两种方法恢复 SED AK：

- **使用口令恢复 SED AK：**使用**根据口令生成** SED AK 模式中设置的密码来恢复 SED AK。
- **从备份文件中恢复 SED AK：**上传**备份** SED AK 模式中生成的备份文件，并输入相应的备份文件密码以恢复 SED AK。

Edge 网络

仅在安装支持无线的 LOM 封装时支持此功能页面。

有关网络拓扑预设表，请参阅 https://thinksystem.lenovofiles.com/help/topic/SE350/pdf_files.html 了解更多细节。

Wi-Fi 连接

单击**已启用**，然后即可根据自己的 Wi-Fi 配置来配置设置。

LTE 连接

这允许您控制 Edge 网卡的 LTE 连接。

Edge 网卡地址

IPv4 或 IPv6 状态	DHCP 服务器状态	方法
已禁用	已禁用	从 DHCP 获取 IP
已启用	已启用	使用静态 IP 地址
已启用	已禁用	从 DHCP 获取 IP 或使用静态 IP 地址，具体取决于您的使用场景。

BMC 网桥

您可以通过选择**下行链路端口**、**Wi-Fi 端口**、**上行链路端口**或**无**来访问 BMC。

注：选择**无**表示此功能已禁用。

Edge 网卡故障诊断

立即重新启动：可以通过此按钮重新启动网卡。

重置为出厂默认值：可以通过此按钮将网卡重置为默认设置。

附录 A　获取帮助和技术协助

如果您需要帮助、服务或技术协助，或者只是希望获取关于 Lenovo 产品的更多信息，那么将会发现 Lenovo 提供了的多种资源来协助您。

万维网上的以下位置提供有关 Lenovo 系统、可选设备、服务和支持的最新信息：

http://datacentersupport.lenovo.com

注：本节包含对 IBM 网站的引用以及关于如何获取服务的信息。IBM 是 Lenovo 对于 ThinkSystem 的首选服务提供商。

致电之前

在致电之前，可执行几个步骤以尝试自行解决问题。如果您确定自己确实需要致电寻求帮助，请提前收集技术服务人员所需的信息以便更快解决您的问题。

尝试自行解决问题

通过执行 Lenovo 在联机帮助或 Lenovo 产品文档中提供的故障诊断过程，您可以在没有外部帮助的情况下解决许多问题。Lenovo 产品文档还介绍了多种可执行的诊断测试。大多数系统、操作系统和程序的文档均包含故障诊断步骤以及对错误消息和错误代码的说明。如果怀疑软件有问题，请参阅操作系统或程序的文档。

可在以下位置找到 ThinkSystem 产品的产品文档：

http://thinksystem.lenovofiles.com/help/index.jsp

可执行以下步骤以尝试自行解决问题：

- 确认所有线缆均已连接。
- 确认系统和所有可选设备的电源开关均已开启。
- 检查是否有经过更新的软件、固件和操作系统设备驱动程序适用于您的 Lenovo 产品。Lenovo 保修条款和条件声明 Lenovo 产品的所有者负责维护和更新产品的所有软件和固件（除非另有维护合同涵盖此项）。如果软件升级中记载了问题的解决方案，则技术服务人员将要求您升级软件和固件。
- 如果您在自己的环境中安装了新硬件或软件，请查看 http://www.lenovo.com/serverproven/ 以确保您的产品支持该硬件和软件。
- 访问 http://datacentersupport.lenovo.com 并检查是否有可帮助您解决问题的信息。
  - 查看 Lenovo 论坛（https://forums.lenovo.com/t5/Datacenter-Systems/ct-p/sv_eg）以了解是否其他人遇到过类似问题。

通过执行 Lenovo 在联机帮助或 Lenovo 产品文档中提供的故障诊断过程，您可以在没有外部帮助的情况下解决许多问题。Lenovo 产品文档还介绍了多种可执行的诊断测试。大多数系统、操作系统和程序的文档均包含故障诊断步骤以及对错误消息和错误代码的说明。如果怀疑软件有问题，请参阅操作系统或程序的文档。

收集致电支持机构时所需的信息

如果您认为您的 Lenovo 产品需要保修服务，那么请在致电之前做好准备，这样技术服务人员将能够更高效地为您提供帮助。您还可以查看 http://datacentersupport.lenovo.com/warrantylookup 了解关于产品保修的详细信息。

收集以下信息以提供给技术服务人员。这些信息有助于技术服务人员快速提供问题解决方案，确保您享受到合同约定的服务水准。

- 硬件和软件维护协议合同编号（如果适用）
- 机器类型编号（Lenovo 四位数机器标识）
- 型号
- 序列号
- 当前系统 UEFI 和固件级别
- 其他相关信息，如错误消息和日志

除了致电 Lenovo 支持机构，您还可以访问 https://www-947.ibm.com/support/servicerequest/Home.action 提交电子服务请求。通过提交电子服务请求，技术服务人员将能够获知问题相关信息，从而启动问题解决流程。在您完成并提交“电子服务请求”后，Lenovo 技术服务人员将立即为您寻求问题解决方案。

收集服务数据

为了明确识别服务器问题的根本原因或响应 Lenovo 支持机构的请求，您可能需要收集可用于进一步分析的服务数据。服务数据包括事件日志和硬件清单等信息。

可通过以下工具收集服务数据：

- **Lenovo XClarity Controller**

  可使用 Lenovo XClarity Controller Web 界面或 CLI 来收集服务器的服务数据。可保存文件并将其发送到 Lenovo 支持机构。

  - 有关使用 Web 界面收集服务数据的更多信息，请参阅 http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/NN1ia_c_servicesandsupport.html。
  - 有关使用 CLI 收集服务数据的更多信息，请参阅 http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/nn1ia_r_ffdccommand.html。

- **Lenovo XClarity Administrator**

  可设置 Lenovo XClarity Administrator，使其在 Lenovo XClarity Administrator 和受管端点中发生某些可维护事件时自动收集诊断文件并发送到 Lenovo 支持机构。可选择将诊断文件使用 Call Home 发送到 Lenovo 支持机构或使用 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。

  可在以下网址找到有关 Lenovo XClarity Administrator 内设置自动问题通知的更多信息：http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/admin_setupcallhome.html。

- **Lenovo XClarity Provisioning Manager**

  使用 Lenovo XClarity Provisioning Manager 的“收集服务数据”功能可收集系统服务数据。可收集现有系统日志数据，也可运行新诊断程序以收集新数据。

- **Lenovo XClarity Essentials**

可通过操作系统在带内运行 **Lenovo XClarity Essentials**。除了硬件服务数据，**Lenovo XClarity Essentials** 还可收集有关操作系统的信息，如操作系统事件日志。

要获取服务数据，可运行 `getinfor` 命令。有关运行 `getinfor` 的更多信息，请参阅 **http://sysmgt.lenovofiles.com/help/topic/toolsctr_cli_lenovo/onecli_r_getinfor_command.html**。

联系支持机构

可联系支持以获取问题帮助。

可通过 **Lenovo** 授权服务提供商获取硬件服务。要查找 **Lenovo** 授权提供保修服务的服务提供商，请访问 **https://datacentersupport.lenovo.com/us/en/serviceprovider**，然后使用筛选功能搜索不同国家/地区的支持信息。要查看 **Lenovo** 支持电话号码，请参阅 **https://datacentersupport.lenovo.com/us/en/supportphonelist** 了解所在区域的支持详细信息。

附录 B 声明

Lenovo 可能不会在全部国家/地区都提供本文档中讨论的产品、服务或功能特性。有关您当前所在区域的产品和服务的信息，请向您当地的 **Lenovo** 代表咨询。

任何对 **Lenovo** 产品、程序或服务的引用并非意在明示或暗示只能使用该 **Lenovo** 产品、程序或服务。只要不侵犯 **Lenovo** 的知识产权，任何同等功能的产品、程序或服务，都可以代替 **Lenovo** 产品、程序或服务。但是，用户需自行负责评估和验证任何其他产品、程序或服务的运行。

Lenovo 公司可能已拥有或正在申请与本文档中所描述内容有关的各项专利。提供本文档并非要约，因此本文档不提供任何专利或专利申请下的许可证。您可以用书面方式将查询寄往以下地址：

Lenovo (United States), Inc.
1009 Think Place
Morrisville, NC 27560
U.S.A.
Attention: Lenovo VP of Intellectual Property

LENOVO“按现状”提供本出版物，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的有关非侵权、适销性和特定用途适用性的保证。某些管辖区域在某些交易中不允许免除明示或暗含的保修，因此本条款可能不适用于您。

本信息中可能包含技术方面不够准确的地方或印刷错误。此处的信息将定期更改；这些更改将编入本资料的新版本中。**Lenovo** 可以随时对本出版物中描述的产品和/或程序进行改进和/或更改，而不另行通知。

本文档中描述的产品不应该用于移植或其他生命支持应用（其中的故障可能导致人身伤害或死亡）。本文档中包含的信息不影响或更改 **Lenovo** 产品规格或保修。根据 **Lenovo** 或第三方的知识产权，本文档中的任何内容都不能充当明示或暗含的许可或保障。本文档中所含的全部信息均在特定环境中获得，并且作为演示提供。在其他操作环境中获得的结果可能不同。

Lenovo 可以按它认为适当的任何方式使用或分发您所提供的任何信息而无须对您承担任何责任。

在本出版物中对非 **Lenovo** 网站的任何引用都只是为了方便起见才提供的，不以任何方式充当对那些网站的保修。那些网站中的资料不是此 **Lenovo** 产品资料的一部分，使用那些网站带来的风险将由您自行承担。

此处包含的任何性能数据都是在受控环境下测得的。因此，在其他操作环境中获得的数据可能会有明显的不同。有些测量可能是在开发级系统上进行的，因此不保证与一般可用系统上进行的测量结果相同。此外，有些测量可能是通过推算估计出的。实际结果可能会有差异。本文档的用户应验证其特定环境的适用数据。

商标

Lenovo、**Lenovo** 徽标、**ThinkSystem**、**Flex System**、**System x**、**NeXtScale System** 和 **x Architecture** 是 **Lenovo** 在美国和/或其他国家或地区的商标。

Intel 和 **Intel Xeon** 是 **Intel Corporation** 在美国和/或其他国家或地区的商标。

Internet Explorer、**Microsoft** 和 **Windows** 是 **Microsoft** 企业集团的商标。

Linux 是 **Linus Torvalds** 的注册商标。

其他公司、产品或服务名称可能是其他公司的商标或服务标记。

重要注意事项

处理器速度指示微处理器的内部时钟速度；其他因素也会影响应用程序性能。

CD 或 **DVD** 光驱速度是可变读取速率。实际速度各有不同，经常小于可达到的最大值。

当指代处理器存储、真实和虚拟存储或通道容量时，**KB** 代表 **1024** 字节，**MB** 代表 **1048576** 字节，**GB** 代表 **1073741824** 字节。

当指代硬盘容量或通信容量时，**MB** 代表 **1000000** 字节，**GB** 代表 **1000000000** 字节。用户可访问的总容量可因操作环境而异。

内置硬盘的最大容量假定更换任何标准硬盘，并在所有硬盘插槽中装入可从 **Lenovo** 购得的当前支持的最大容量硬盘。

达到最大内存可能需要将标准内存更换为可选内存条。

每个固态存储单元的写入循环次数是单元必然会达到的一个固有、有限的数字。因此，固态设备具有一个可达到的最大写入循环次数，称为 total bytes written (**TBW**)。超过此限制的设备可能无法响应系统发出的命令或可能无法向其写入数据。**Lenovo** 不负责更换超出其最大担保编程/擦除循环次数（如设备的正式发表的规范所记载）的设备。

Lenovo 对于非 **Lenovo** 产品不作任何陈述或保证。对于非 **Lenovo** 产品的支持（如果有）由第三方提供，而非 **Lenovo**。

某些软件可能与其零售版本（如果存在）不同，并且可能不包含用户手册或所有程序功能。

颗粒污染物

注意：如果空气中悬浮的颗粒（包括金属屑或微粒）与活性气体单独发生反应，或与其他环境因素（如湿度或温度）发生组合反应，可能会对本文档中所述的设备构成威胁。

颗粒水平过高或有害气体聚集所引发的风险包括设备故障或设备完全损坏。为避免此类风险，本规格中对颗粒和气体进行了限制。不得将这些限制视为或用作决定性的限制，因为有大量其他因素（如空气的温度或含水量）会影响微粒或环境腐蚀物的作用程度以及气体污染物的转移。如果不使用本文档中所规定的特定限制，您必须采取必要措施，使颗粒和气体级别保持在能够保护人员健康和安全的水平。如果 **Lenovo** 判断您所处环境中的颗粒或气体水平已对设备造成损害，则 **Lenovo** 可在实施适当的补救措施时决定维修或更换设备或部件以减轻此类环境污染。此类补救措施的实施由客户负责。

表 70. 颗粒和气体的限制

污染物	限制
颗粒	• 根据 **ASHRAE Standard 52.2**[1]，必须持续以 **40%** 的大气尘比色效率（**MERV 9**）过滤室内空气。 • 必须使用符合 **MIL-STD-282** 标准的高效微粒空气（**HEPA**）过滤器，将进入数据中心的空气过滤到 **99.97%** 或更高的效率。 • 颗粒污染物的潮解相对湿度必须大于 **60%**[2]。 • 室内不能存在导电污染物，如锌晶须。
气体	• 铜：**G1** 类，依据 **ANSI/ISA 71.04-1985**[3] • 银：**30** 天内腐蚀率小于 **300** Å

[1] **ASHRAE 52.2-2008 -** *按颗粒大小测试常规通风空气净化设备除尘效率的方法*。亚特兰大：美国采暖、制冷与空调工程师学会（**American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.**）。

[2] 颗粒污染物的潮解相对湿度是指使尘埃吸收足够的水分后变湿并成为离子导电物的相对湿度。

[3] **ANSI/ISA-71.04-1985**。*流程测量和控件系统的环境条件：空气污染物*。美国北卡罗莱纳州三角研究园美国仪器学会（**Instrument Society of America**）。

电信监管声明

本产品在您的国家/地区可能尚未通过以任何方式连接到远程通信网络的认证。在进行任何此类连接之前，可能需要获得进一步的认证。如有任何疑问，请联系 **Lenovo** 代表或经销商。

电子辐射声明

在将显示器连接到设备时，必须使用显示器随附的专用显示器线缆和任何抑制干扰设备

有关其他电子辐射声明，请访问：

http://thinksystem.lenovofiles.com/help/index.jsp

台湾 BSMI RoHS 声明

單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛Lead (Pb)	汞Mercury (Hg)	鎘Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr^{+6})	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
機架	○	○	○	○	○	○
外部蓋板	○	○	○	○	○	○
機械組合件	–	○	○	○	○	○
空氣傳動設備	–	○	○	○	○	○
冷卻組合件	–	○	○	○	○	○
內存模塊	–	○	○	○	○	○
處理器模塊	–	○	○	○	○	○
鍵盤	–	○	○	○	○	○
調製解調器	–	○	○	○	○	○
監視器	–	○	○	○	○	○
滑鼠	–	○	○	○	○	○
電纜組合件	–	○	○	○	○	○
電源	–	○	○	○	○	○
儲備設備	–	○	○	○	○	○
電池匣組合件	–	○	○	○	○	○
有mech的電路卡	–	○	○	○	○	○
無mech的電路卡	–	○	○	○	○	○
雷射器	–	○	○	○	○	○

備考1. 〝超出0.1 wt %〞及〝超出0.01 wt %〞係指限用物質之百分比含量超出百分比含量基準值。

Note1 : “exceeding 0.1wt%” and “exceeding 0.01 wt%” indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.

備考2. 〝○〞係指該項限用物質之百分比含量未超出百分比含量基準值。

Note2 : “○”indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.

備考3. 〝-〞係指該項限用物質為排除項目。

Note3 : The “-“ indicates that the restricted substance corresponds to the exemption.

台湾进口和出口联系信息

提供台湾进口和出口联系信息。

委製商/進口商名稱: 台灣聯想環球科技股份有限公司
進口商地址: 台北市南港區三重路 66 號 8 樓
進口商電話: 0800-000-702

索引

h

i

k

l

m

n

o

p

r

s

入

刀

力

卩

口

口

士

士

夕

子

宀

寸

尸

系

组

网

耳

自

获

西

见

许

车

辶

酉

里

阝

佳

青

非

页

高

黑

鼠

Lenovo

部件号：**SP47A30085**

Printed in China

(**1P**) **P/N: SP47A30085**