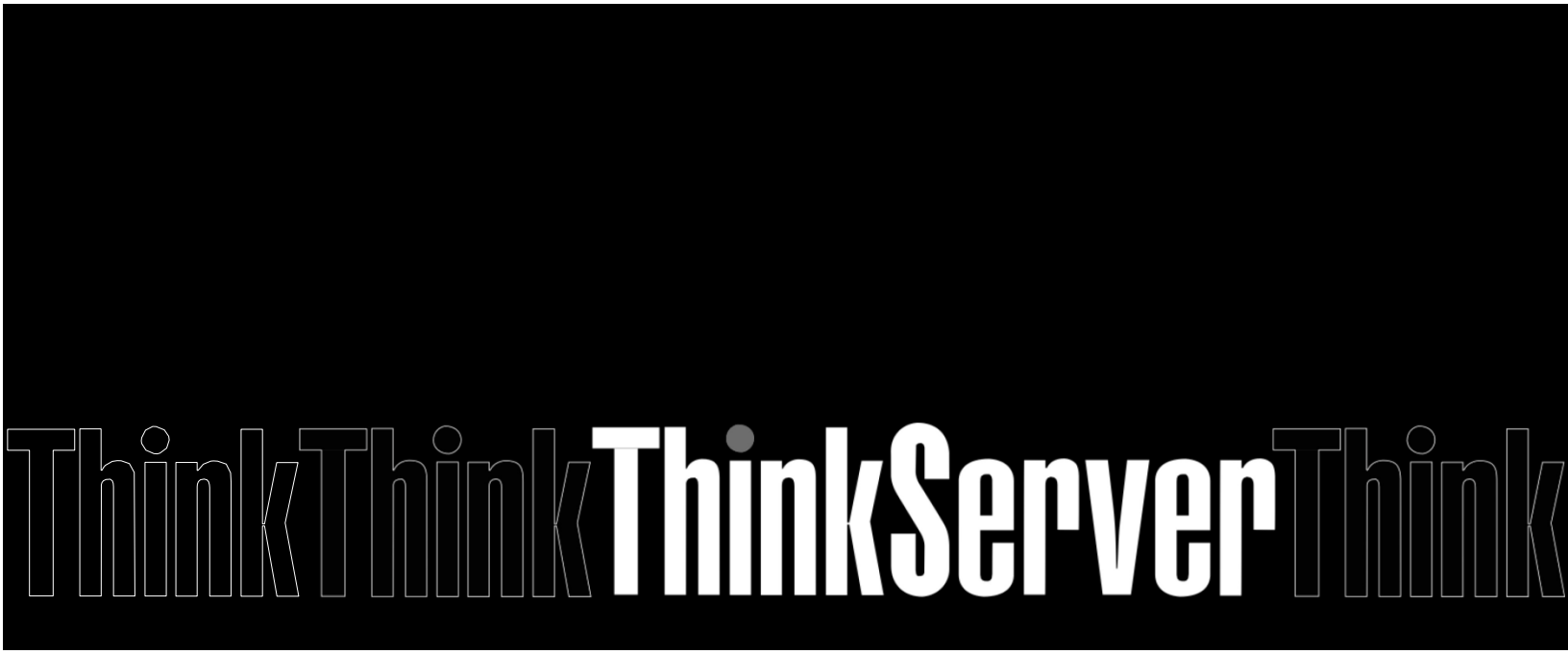
Lenovo

# ThinkServer 管理模块
# 用户指南



**注意：**在使用信息和产品之前，请务必阅读和理解“附录 A 通知”。

**初版（2016 年 6 月）**

| 日期 | 版本 | 说明 |
| --- | --- | --- |
| *06-08-2016* | *v0.1* | *初稿* |
| *07-01-2016* | *v0.2* | *1. 修改标志*<br>*2. 修改“目录”、第4、5 章* |
| *07-15-2016* | *v0.3* | *1. 修改第5 章* |
| *07-26-2016* | *v0.4* | *1. 修改第5 章*<br>*2. 增加第6 章* |
| *08-04-2016* | *v0.5* | *1. 修改第5 章* |
| *08-25-2016* | *v0.6* | *1. 修改第5 章* |
| *09-22-2016* | *v0.7* | *1. 修改第5 章* |
| *10-06-2016* | *v0.8* | *1. 修改第5 章* |
| *10-20-2016* | *v0.9* | *1. 修改第5 章*<br>*2. 修改第6 章* |
| *10-27-2016* | *v1.0* | *1. 修改第5 章* |
| *11-04-2016* | *v1.1* | *1. 修改第5 章* |
| *11-11-2016* | *v1.2* | *1. 修改第5 章* |
| *11-17-2016* | *v1.3* | *1. 修改第5 章* |

# 目录

# 第 1 章 简介

欢迎使用《Lenovo ThinkServer 管理模块（TMM）用户指南》。简便起见，在下面的章节中我们用“TMM”代替“Lenovo ThinkServer 管理模块”。

本用户指南介绍如何使用 RS160 上的 TMM，概述模块功能及如何设置和操作模块。

本用户指南针对负责 TMM 配置、升级和维护的系统管理员。对于那些已经熟悉用户指南的系统管理员，可以在紧急情况下从任何地方远程访问 TMM。如果需要进一步帮助，请前往 Lenovo 支持网站。

本文档中有些截图可能与 TMM 实际用户界面不一致，仅作参考。

## 术语

下表列举本文档所用的术语及对应说明。

| 简写 | 定义 |
|---|---|
| AD | 活动目录 |
| BIOS | 基本输入/输出系统 |
| BMC | 基板管理控制器 |
| CPLD | 复杂可编程逻辑设备 |
| DCMI | 数据中心管理接口 |
| DHCP | 动态主机配置协议 |
| DIMM | 双列直插式内存模块 |
| DNS | 域名服务 |
| FRU | 现场可更换设备 |
| FQDN | 完全限定的域名 |
| IP | Internet 协议 |
| IPMI | 智能平台管理接口 |
| KVM | 键盘、视频和鼠标 |
| LAN | 局域网 |
| LDAP | 轻量目录访问协议 |
| MAC | 介质访问控制器 |

| | |
|---|---|
| ME/NM | 节点管理器 |
| NCSI | 网络通讯服务接口 |
| NFS | 网络文件系统 |
| NIC | 网络接口控制器 |
| Nsupdate | 直接动态 DNS |
| NTP | 网络时间协议 |
| PEF | 平台事件过滤器 |
| POST | 加电自检 |
| PSU | 电源 |
| RAID | 独立磁盘冗余阵列 |
| RADIUS | 远程拨入用户身份验证服务 |
| SEL | 系统事件日志 |
| SMASH | 服务器硬件系统管理架构 |
| SMTP | 简单邮件传输协议 |
| SNMP | 简单网络管理协议 |
| SOL | 串口网络重定向 |
| SSH | 安全外壳 |
| SSL | 安全套接字层 |
| TCP/IP | 传输控制协议/Internet 协议 |
| TDM | ThinkServer 部署管理器 |
| TMM | ThinkServer 管理模块 |
| TSIG | 交易签名 |
| USB | 通用串行总线 |
| VLAN | 虚拟局域网 |

# 安全信息

**警告**

在阅读本指南或其他文档时，必须首先特别注意安全信息，然后再操作 ThinkServer。为确保完全遵守现有的认证和许可，必须遵守本指南规定的安装说明。

开关机：电源按钮不会停止 TMM 电源。要禁用 TMM，必须将交流电源线从插头拔出。当打开机柜安装或拆卸部件时，确保已断开电源线。

# 第 2 章 Lenovo TMM 概述

本章节介绍 TMM 的功能。TMM 在 ThinkServer 内集成了嵌入式操作系统。该嵌入式操作系统独立于服务器的操作系统，可提供完整、稳定而高效的服务器解决方案。作为系统管理员，可以通过网络远程管理，查看系统事件日志消息。

## TMM 功能

TMM 可通过网络连接访问，如果安装了远程 KVM，用户甚至可以远程连接到内置远程访问的操作系统和相关控制软件。

TMM 主要功能如下：

- 嵌入式网页用户界面：远程开关机、系统健康、系统信息、报警通知和事件日志。
- 安全：开源 SSL
- 兼容 IPMI V2.0
- KVM：允许在 POST 和 BIOS 设置程序中远程查看和配置
- 支持平台部署管理
- 同时支持使用 IPv4 和 IPv6 SNMP。
- 支持 NTP 客户端。
- 支持 USB 重定向、远程媒介（虚拟媒介）。
- 支持扩展 SEL。
- 支持 LDAP 和 LDAPS。
- 支持通过 SMTP 邮件通知报警。
- 支持 TMM 和 BIOS。
- 支持 SMASH

# 第 3 章 配置 TMM

本章节介绍如何使用服务器配置实用程序配置 TMM。第一次安装后，TMM 默认会搜索网络上 DHCP 服务器，自动分配 IP 地址、子网掩码和网关。建议用户在 BIOS 中手动设置固定 IP 地址。

要设置 IP 地址，请按下列操作：

1. 在出现 Lenovo 标志画面时立即按下 F1。
2. 从 BIOS 设置菜单，选择 Server management（服务器管理） →Network Settings（网络设置） → Configuration Address Source（配置地址源）。
3. 从 Configuration（配置）选项，选择静态或 DHCP 设置 IP 地址。
4. 完成配置后，保存设置。

*表 1 IPMI 2.0 配置子菜单*

| | | |
|---|---|---|
| **Configuration Address Source（配置地址源）** | **Static（静态）** | 静态 IP 配置。可手动配置 IP 和子网掩码 |
| | **DHCP** | Dynamic IP configuration（动态 IP 配置）。系统自动获取 IP |

## 系统需求

**支持的浏览器：**

- Chrome，版本 48.0.2564.109 或更高
- Firefox，版本 44.0.2 或更高
- Internet Explorer，版本 11.0.9600.18097

如果要使用虚拟控制器，必须正确安装 Java Run-Time Environment (JRE)，包括所选浏览器的 Java 插件。根据所安装 JRE 版本不同，可能需要降低 Java 安全性才可运行虚拟控制台。

**注意：**

使用 Chrome 时远程控制台预览窗口是空白的，因为 Chrome 已不再支持 NPAPI（Java applet 所用的技术），请参阅下面链接了解详情。

https://www.java.com/en/download/faq/chrome.xml

**支持的 Java：**

- Java 1.8.0_77 KVM/VM

# 第 4 章 TMM 快速入门

## 连接 TMM

TMM 内嵌网页服务器和应用，带多个标准接口。本章节介绍这些接口及用途。可以使用 TCP/IP 协议访问这些接口。

如需深入了解初始设置，请参阅第 7 页第 3 章“配置 TMM”。默认用户名和密码如下：

- 用户名 = lenovo
- 密码 = len0vO

可使用标准支持 Java 的网页浏览器通过 HTTPS 访问，因为是通过 HTTPS 协议访问 TMM，浏览器会提示信任和安装安全数字证书。请根据提示导入和确认证书。

## 登录

要登录 TMM，请按下面操作：

1. 在网页浏览器中输入分配给 TMM 的 IP 地址。
   例如：
   http://10.99.87.131/
   如果要安全连接，可参阅下列网址： https://10.99.87.131/
   浏览器会打开 TMM 的登录页面。
2. 在 TMM 的登录页面，输入用户名和密码。例如：
   - 用户名 = lenovo
   - 密码 = len0vO
3. 单击 **Sign in（登录）**访问 TMM 的主页。

## 导航

成功登录到 TMM 后，可看到 TMM 仪表板。可以选择左右箭头在仪表板上导航。每一仪表板上的信息和任务见下表。

*表 2：TMM 仪表板属性*

| | **评论** |
|---|---|
| Dashboard（仪表板） | 该仪表板包含以下信息：<br>• **Device Information（设备信息）**<br>• **Network Information（网络信息）**<br>• **Location LED status（位置 LED 状态）**<br>• **Remote Control Preview Box（远程控制器预览框）**<br>• **Sensor Monitoring（传感器监控）**<br>• **Event Log summary（事件日志汇总）** |

**Refresh（刷新）**
可以随时点击“Refresh（刷新）”重新加载当前页面。
**Print（打印）**
可以随时点击“Print（打印）”打印当前页面。
**Logout（注销）**
可以随时点击“Logout（注销）”退出当前页面。
**Help（帮助）**
可以随时点击“Help（帮助）”查看帮助页面。

# 第 5 章 TMM 网页控制台选项

本章节介绍 TMM 网页控制台。可以检查 ThinkServer 的传感器状态、查看安装的硬件原件、授权其他用户和配置 TMM 设置。本章节介绍所有的功能及每一功能可能的操作。

## 登录和访问控制

如要登录 TMM，必须输入有效的用户名和密码，两个字段都必须正确填写，如果字段无效，则无法登录 TMM.

TMM 支持本地用户以及活动目录和 LDAP。可以询问系统管理员获取登录凭证。

**注意：**如要登录 TMM 网页，必须提供有效的用户名和密码。两个字段都必须正确填写。如果尝试失败三次，帐户就会锁定 30 分钟。对于活动目录和 LDAP 服务，用户名字段中用户名前不需要输入域名（例如，domainABC\userXYZ）。

默认 TMM 会尝试按下列顺序进行身份认证：

1. 本地
2. LDAP（如果启用）
3. 活动目录（如果启用）

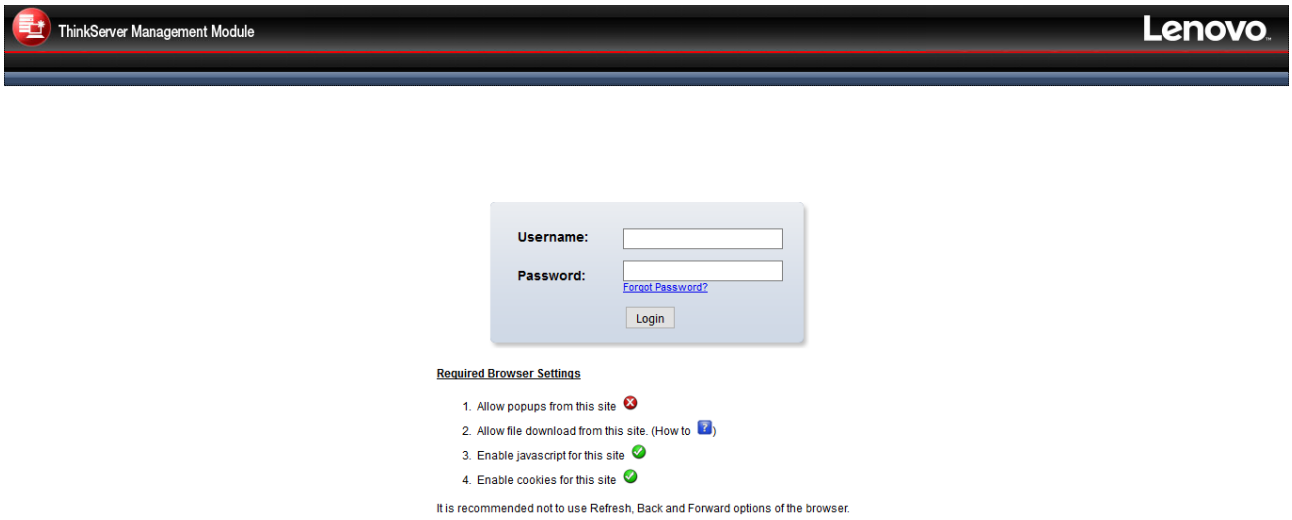



*图 1：登录页面*

## Forgot password（忘记密码）

可使用该链接“Forgot password（忘记密码）”生成新的密码，输入用户名，然后点击“Forgot password（忘记密码）”。会向该用户关联的电子邮件发送新生成的密码。

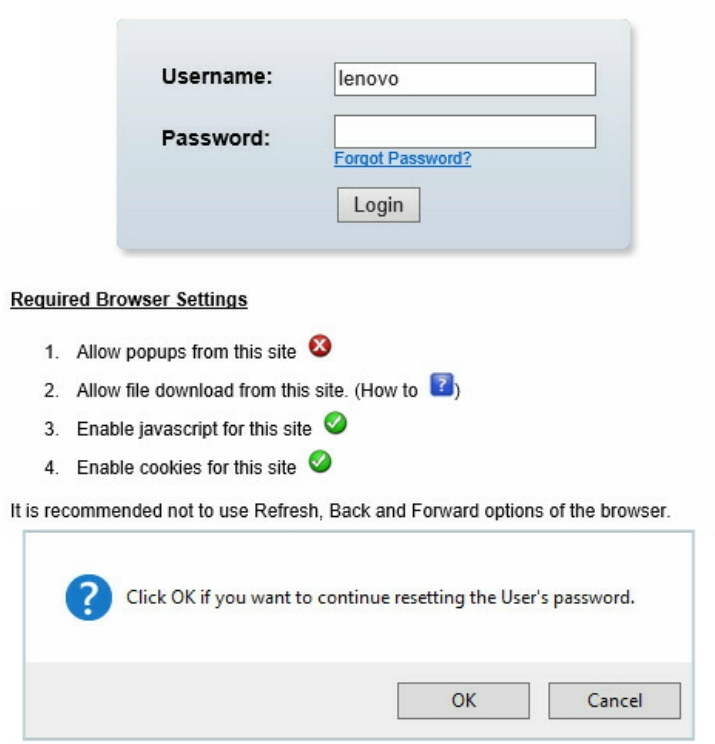



*图2：忘记密码对话框*

## Required Browser Settings（所需浏览器设置）

**Allow pop-ups from this site（允许本网站的弹出窗口）：** 图标标识浏览器是否允许本网站弹出窗口。
**Allow file download from this site（允许下载本网站文件）：** 对于 Internet Explorer，选择工具 ->Internet 选项 ->安全选项卡，根据设备设置，选择 Internet、本地 Internet、受信任的网站和受限制的网站。单击自定义级别... 打开安全设置 - 区域，在设置下，找到下载选项，启用文件下载选项。单击确定关闭对话框。
对于所有其他浏览器，在提示时接受文件下载。
**Enable javascript for this site（启用本网站 javascript）：** 图标表示浏览器是否启用 javascript。
**Enable cookies for this site（启用本网站 cookies）：** 图标表示浏览器是否启用 cookies。
**注意：**必须启用 cookies 才可访问网站。

## Dashboard（仪表板）

仪表板显示设备状态的整体信息。从本页面启动远程控制台重定向窗口。如要启动，必须具有管理员权限或 KVM 权限。
登录后，TMM 显示仪表板页面，显示所有服务器状态。

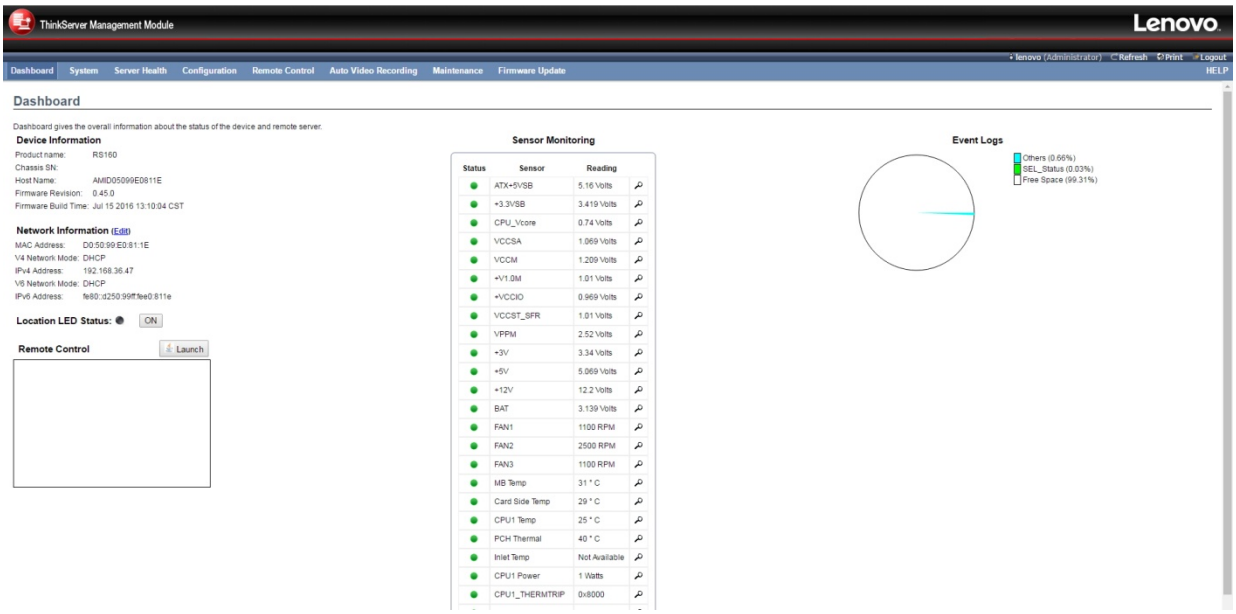



*图3：仪表板*

下面简要介绍仪表板页面。

## Device Information（设备信息）

显示固件版本和固件构建时间（日期和时间）。

## Network Information（网络信息）

显示设备的网络设置。单击链接编辑查看网络设置页面。

## Location LED Status（位置 LED 状态）

显示位置 LED 的当前状态。单击 ON/OFF（开/关）按钮控制位置 LED。

## Remote Control（远程控制）

从该页启动控制台，启用主机远程重定向。单击“Remote Control（远程控制）”的“Launch（启动）”按钮，下载 jviewer.jnlp 文件。文件下载并启动后，会显示 Java 重定向窗口。

## Remote Control Screenshot（远程控制截图）

使用 Java 应用程序显示远程服务器的截图。单击“Refresh（刷新）”按钮重新加载截图。

## Sensor Monitoring（传感器监控）

罗列设备上的所有传感器并标注如状态、名称、读数和状态图标信息，以及到该传感器页面的链接。显示模拟传感器的当前读数，在读数字段显示离散传感器的事件状态。
一个传感器会有 3 种状态：

- 绿点表示正常状态。
- 黄色感叹号表示警告状态。
- 红色 x 表示重要状态。

放大镜可用于查看该传感器的详细信息。

## Event Logs（事件日志）

图形显示所有各个传感器检测到的事件，以及日志占用和可用空间。如果单击图列中彩色长方形，只能看到一列这些特定事件。

**注意：**如果日志不属于设备 SDR，那么就被归为“其他”组。可以在“剩余空间”组找到事件日志的可用空间。

## Menu Bar（菜单栏）

菜单栏显示下列内容。

- Dashboard（仪表板）
- System（系统）
- Server Health（服务器健康）
- Configuration（配置）
- Remote Control（远程控制）
- Auto Video Recording（自动视频录制）
- Maintenance（维护）
- Firmware Update（固件更新）

菜单栏截图如下。

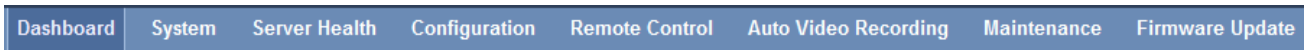



*图4：菜单栏*

## System（系统）

系统组显示以下信息：

- Inventory（库存）
- FRU information（FRU 信息）

“系统”菜单项截图如下。

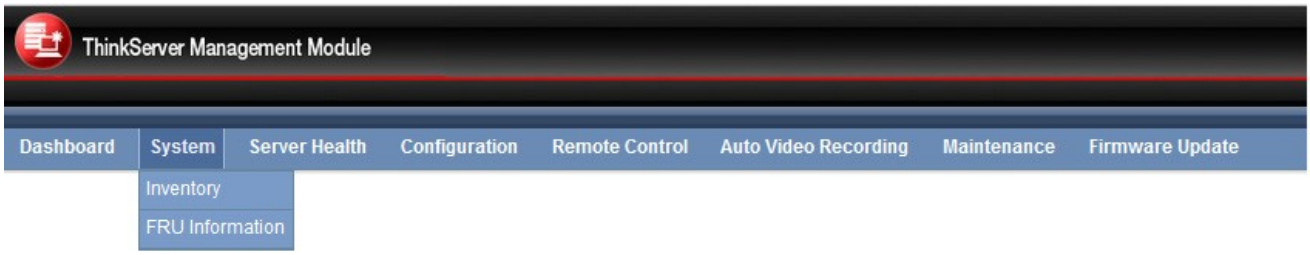



*图5：系统-菜单*

## Inventory（库存）

该页显示设备清单信息。

- **BIOS 信息：**显示 BIOS 信息。
  - BIOS Vendor（BIOS 供应商）
  - BIOS Version（BIOS 版本）
  - BIOS Build Date（BIOS 构建日期）
- **CPU 信息：**显示 CPU 信息。
  - CPU Model（CPU 型号）
  - CPU Signature（CPU 签名）
  - CPU Core Count（CPU 内核数）

- CPU Thread Count（CPU 线程数）
- Base CPU Speed（基本 CPU 速度）
- Max CPU Speed（最大 CPU 速度）
- Min CPU Speed（最小 CPU 速度）
- L1 iCache
- L1 dCache
- L2 Cache（L2 缓存）
- L3 Cache（L3 缓存）

- **Memory Information（内存信息）**：显示内存信息。
  - 总内存
  - 内存选择
  - DDR4 插槽
  - 容量
  - 类型
  - 类型细节
  - 等级
  - 配置速度
  - 电压
  - 制造商
  - 部件号
  - 序列号
- **存储信息**：显示存储信息。
  - HDD 端口
  - 端口速度
  - 设备型号
  - 设备版本
  - 序列号
- **网络信息**：显示板载网络信息。
  - 端口数
  - 端口选择
  - MAC 地址

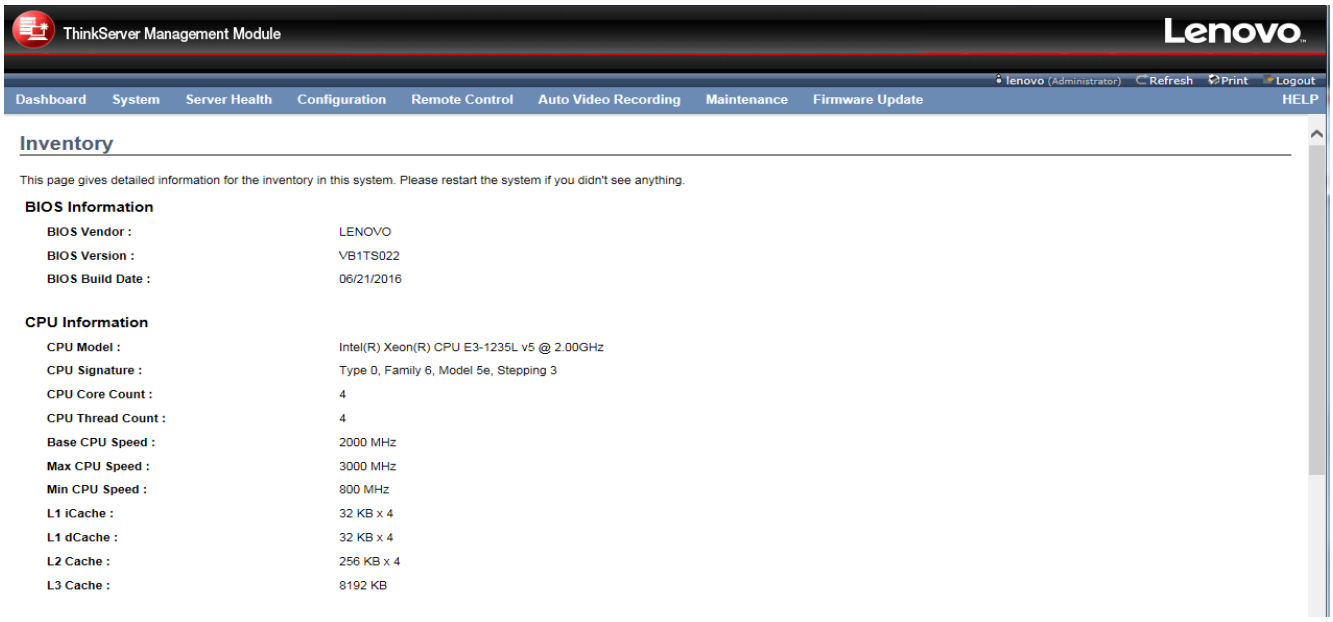



*图6：库存*

## FRU Information（FRU 信息）

该页显示 BMC FRU 文件信息。选择任何特定 FRU 设备 ID 后就会显示对应的 FRU 信息。

如要打开 FRU 信息页，可单击菜单栏中的 **FRU Information（FRU 信息）**。从基本信息区选择 FRU 设备 ID，然后查看所选设备的详细信息。FRU 信息屏幕截图如下。

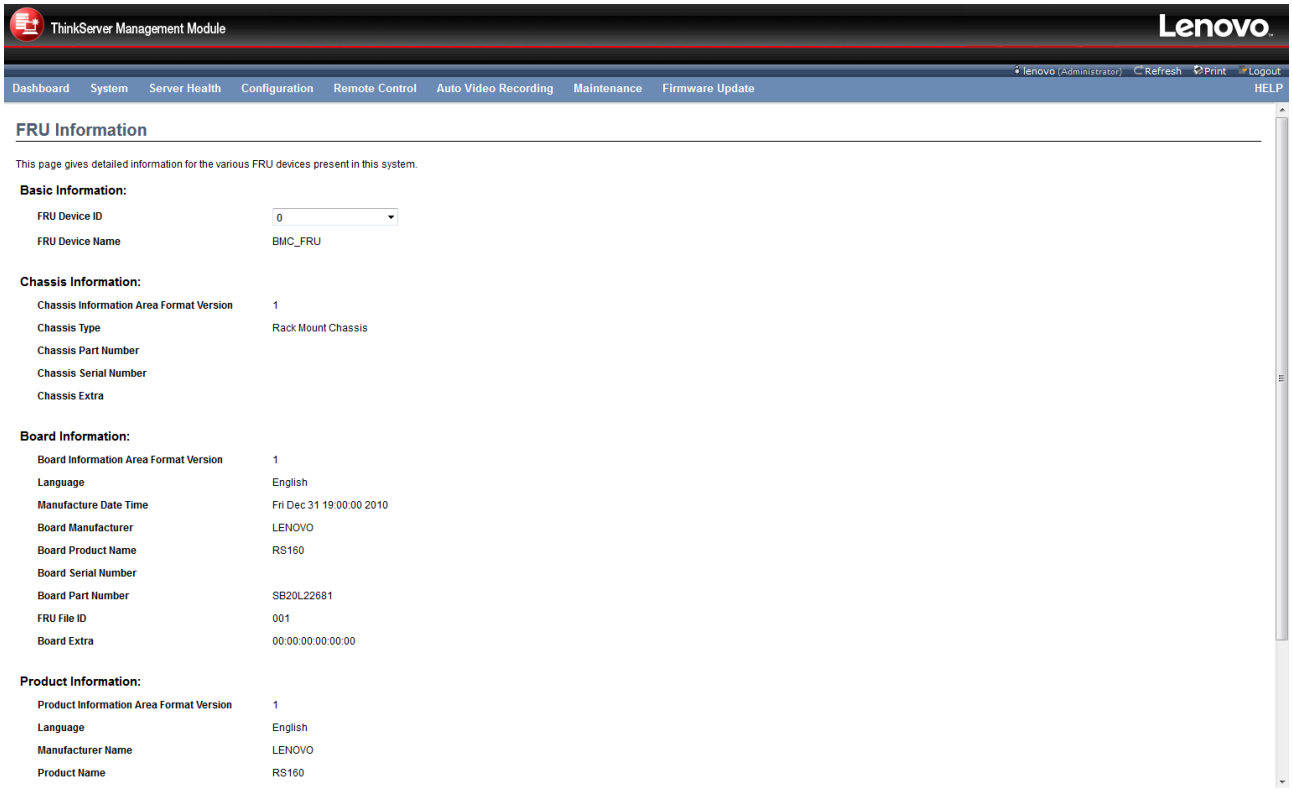



*图7：FRU 信息*

- **Basic Information（基本信息）：**显示所选 FRU 设备 ID 对应的 FRU 设备名称。该页面显示每一字段内所列项目的机架、主板、产品详细信息（如有）。
- **Chassis Information（机架信息）：**显示 FRU 机架区域。
  - 机架信息区域格式版本
  - 机架类型
  - 机架部件号
  - 机架序列号
  - 机架其他信息
- **Board Information（主板信息）：**显示 FRU 主板区域。
  - 主板信息区域格式版本
  - 语言
  - 制造日期和时间
  - 主板制造商
  - 主板产品名称
  - 主板序列号
  - 主板部件号
  - FRU 文件 ID
  - 主板其他信息
- **Product Information（产品信息）：**显示 FRU 产品区域。
  - 产品信息区域格式版本
  - 语言
  - 制造商名称
  - 产品名称
  - 产品部件号
  - 产品版本
  - 产品序列号
  - 资产标签
  - FRU 文件 ID
  - UUID

**注意：**如通过 ipmitool 获取 FRU 数据，UUID 将显示在产品其他信息内，数据可能无法正常显示，因为其定义为十六进制数据（FRU 数据在 ipmitool 里按 ASCII 显示）。

## Server Health Group（服务器健康组）

服务器健康组显示以下信息。

- Sensor Readings（传感器读数）
- Event Log（事件日志）
- BSOD Screen（BSOD 屏幕）

“服务器健康”菜单项截图如下。

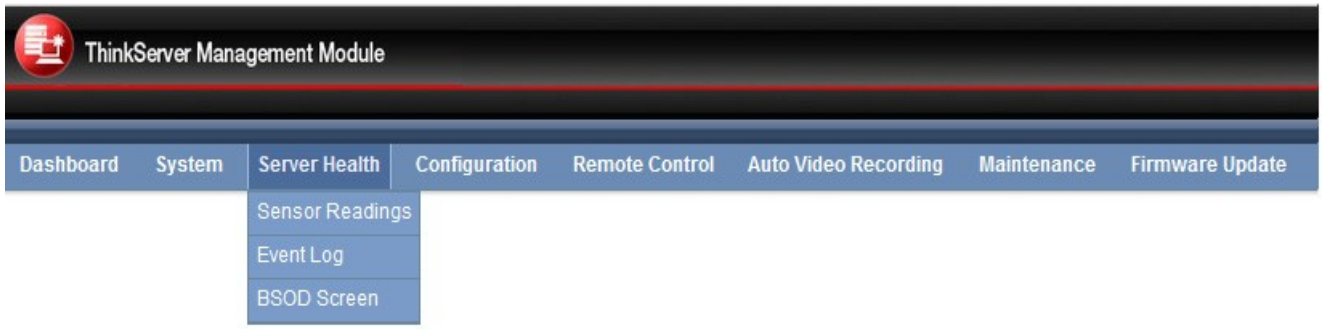



*图8：服务器健康 - 菜单*

下面详细介绍服务器健康组

## Sensor Readings（传感器读数）

在此显示一列传感器读数。显示模拟传感器的当前读数，显示离散传感器的事件状态。单击记录显示该传感器的更多信息，包括阈值和图形显示所有相关的已发生的事件。双击记录开关该传感器的活动小部件。

**注意：**N/A 代表不可用。

如要打开传感器读数页面，请从菜单单击 Server **Health （服务器健康）> Sensor Readings（传感器读数）**。单击任何传感器显示该传感器的更多信息，包括阈值和图形显示所有相关事件。

传感器读数屏幕截图如下。

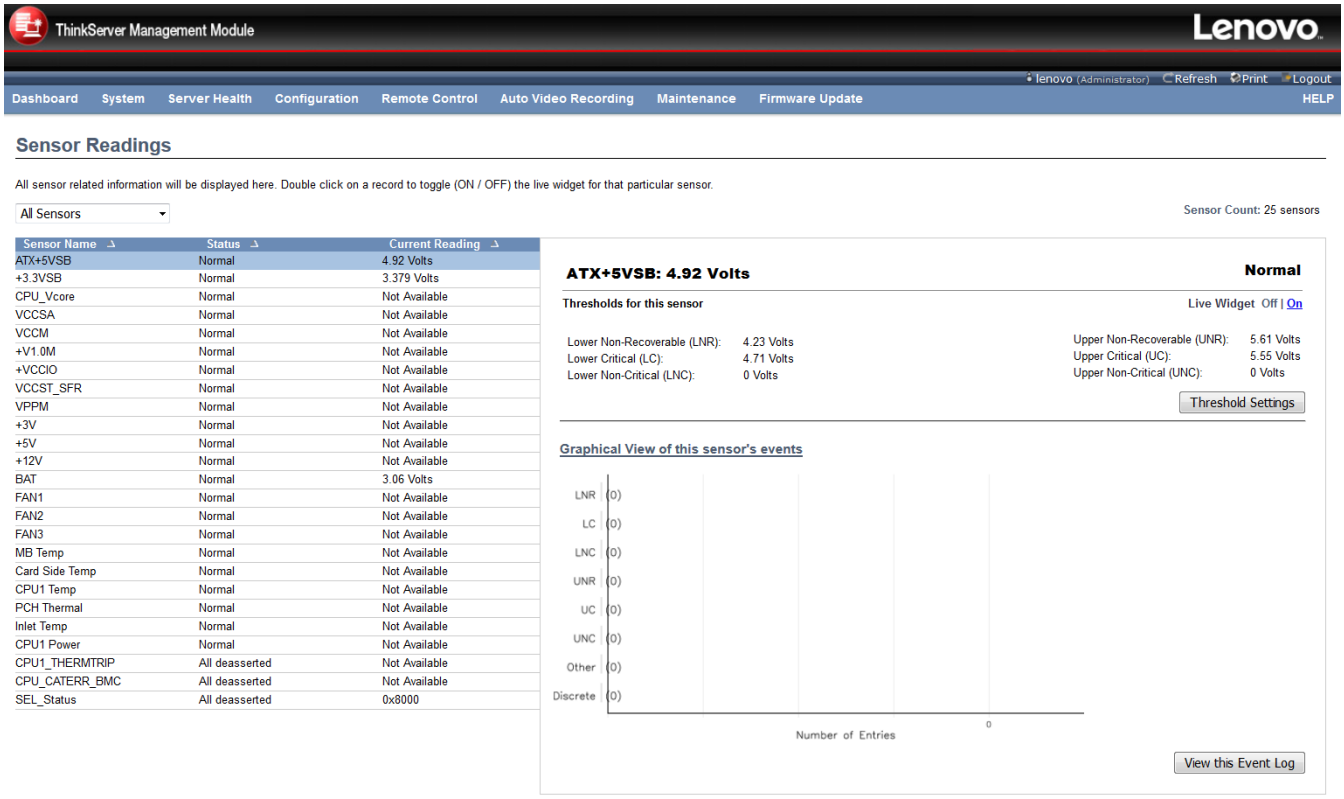



*图9：传感器读数页面*

- **Threshold Settings（阈值设置）：**单击选项配置阈值设置。选项包括
  - 不可恢复下限（LNR）
  - 关键下限（LC）

- 非关键下限（LNC)
- 不可恢复上限（UNR）
- 关键上限（UC）
- 非关键上限（UNC）

- **Live Widget（活动小部件）：**打开或关闭该传感器的活动小部件。该小部件可动态显示传感器的读数。
- **View this Event Log（查看事件日志）：**单击按钮查看所选传感器的事件日志页。

**Sensor Type (drop down ment)（传感器类型（下拉菜单））**

该下拉菜单可选择传感器类型。如果选择所有传感器，所有传感器的详细信息都会显示，如传感器名称、状态和当前读数，否则只选择要显示的传感器类型。比如温度传感器、风扇传感器、看门狗传感器和电压传感器等。

**Live Widget（活动小部件）**

对于所选传感器，可以单击 ON 或 OFF 启用或关闭小部件。该小部件可动态显示传感器的读数。也可双击记录开关该传感器的活动小部件。下面是小部件开启后的截图示例。

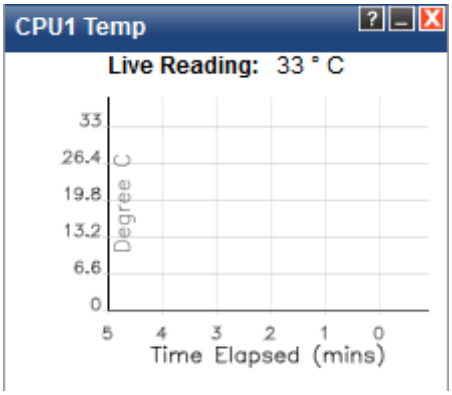



*图 10：活动小部件*

小部件是一些小的构件，可实时提供某个传感器的信息。用户可定期持续跟踪传感器的行为。结果在小部件中以线形图显示。

因为小部件需要实时数据，只要小部件打开着，会话就不会结束。

- **Minimize/Restore（最小化、恢复）：**最小化按钮可隐藏图形，但会继续显示实时读数。请注意恢复时图形依然保持更新。恢复可以将小部件回到正常大小。
- **Close（关闭）：**用户可以随时关闭小部件。客户端会丢失截至目前的传感器历史，但是所有事件依然会写入服务器。

**Threshold Settings（阈值设置）**

可单击此按钮配置阈值设置。示例截图如下。

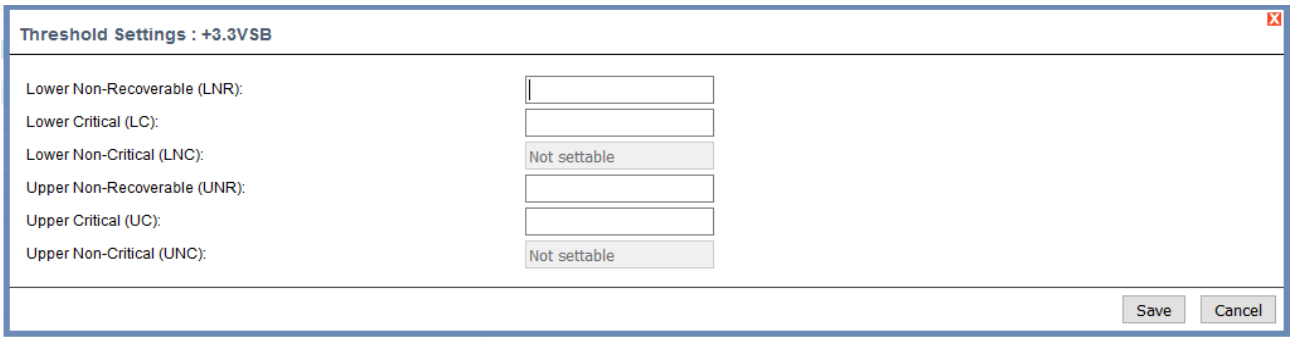



*图 11：阈值设置*

使用该页面配置阈值设置。

- **Lower Non-Recoverable (LNR)（不可恢复下限（LNR））：**设置不可恢复下限阈值。
- **Lower Critical (LC)（关键下限（LC））：**设置关键下限阈值。
- **Lower Non-Critical (LNC)（非关键下限（LNC））：**设置非关键下限阈值。
- **Upper Non-Recoverable (UNR)（不可恢复上限（UNR））：**设置不可恢复上限阈值。
- **Upper Critical (UC)（关键上限（UC））：**设置关键上限阈值。
- **Uppdr Non-Critical (UNC)（非关键上限（UNC））：**设置非关键上限阈值。
- **Save（保存）：**保存设置。文本框内所有数据会转换成 IPMI 数据类型，如需了解更多信息，请参阅 IPMI 规范 2.0（第 36 章“传感器类型和数据转换”）。
- **Cancel（取消）：**取消所做的变更。

### View this Event Log（查看事件日志）

可以单击“**View this Event Log（查看事件日志）**”查看所选传感器事件日志。

**注意：**有些传感器类型是 **OEM define（OEM 定义）**，通过 ipmitool 获取传感器状态时会看到“Unknown”。如“Unknown CPU_CATERR_BMC”

## Event Log（事件日志）

该页面显示该设备不同传感器捕获的事件。双击记录查看该条目详细信息。还可单击任何列头对条目列表排序。

如要打开事件日志页面，请从菜单单击 **Server Health （服务器健康）> Event Log（事件日志）**。事件日志页面截图示例如下。

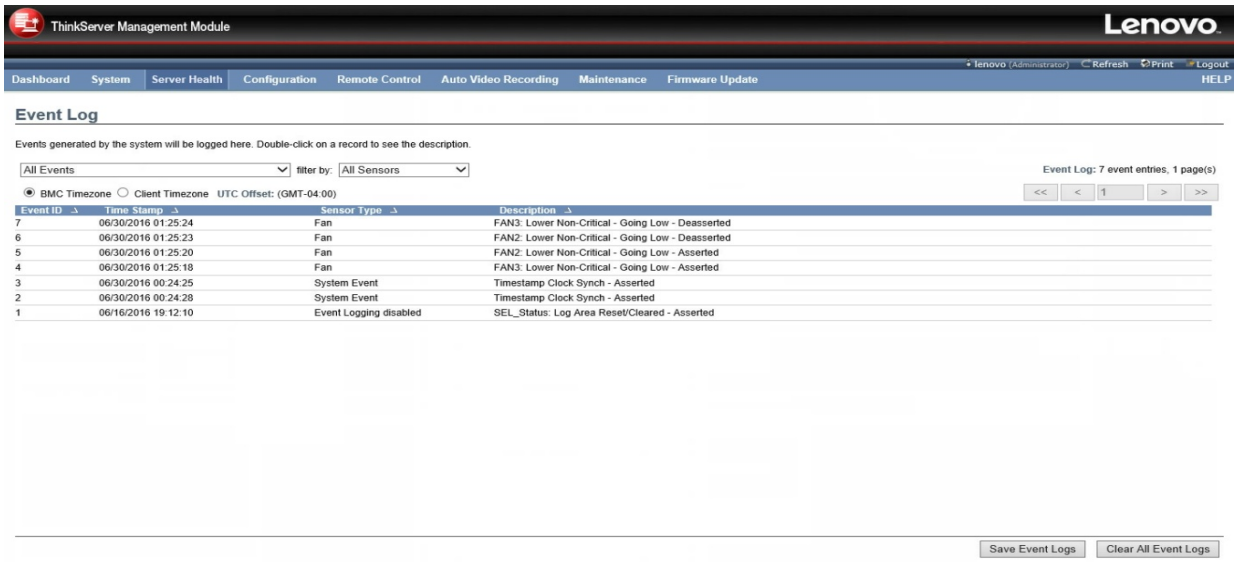



*图12：事件日志页面*

可以使用传感器类型或传感器名称过滤选项查看该设备记录的特定事件。

- **Event log Category（事件日志类别）：**传感器类型组，可以根据传感器类型过滤事件日志。

所有事件、系统事件记录、OEM 事件记录、BIOS 生成事件、SMI 句柄事件、系统管理软件事件、系统软件-OEM 事件、远程控制台软件事件、终端模式远程控制台软件事件，可参阅下表了解更多。

| 事件 | 记录类型 | Generator ID1（生成 ID1） | |
|---|---|---|---|
| | | [7:1] | [0] |
| BIOS 生成事件 | 0x00 – 0xBF | 0x00 – 0x0F | 1b |
| SMI 句柄事件 | | 0x10 – 0x1F | |
| 系统管理软件事件 | | 0x20 – 0x2F | |
| 系统软件-OEM 事件 | | 0x30 – 0x3F | |
| 远程控制台软件事件 | | 0x40 – 0x46 | |
| 终端模式远程控制台软件事件 | | 0x47 | |
| 系统事件记录 | | 其它 | |
| OEM 事件记录 | 0xC0 – 0xFF | | |

**注意：**关于“Record Type（记录类型）”和“Generator ID（生成 ID）”，可以参阅 IPMI 2.0 规范了解详情。

- **Filter By（过滤条件）：**传感器名称组，可以根据传感器名称过滤事件日志。
- **BMC Time zone（BMC 时区）：**选中该选项，按 BMC 时区显示记录的事件日志。
- **Client Time zone（客户端时区）：**选中该选项，按客户端（用户）时区显示记录的事件日志。
- **UTC Offset（UTC 偏移）：**根据事件要更新的时间戳显示当前 UTC 偏移值。
  使用导航箭头可选择性访问事件日志各个页面。
- **Event ID（事件 ID）：**显示事件的 ID 号。
- **Time Stamp（时间戳）：**显示事件的时间戳。
- **Sensor Type（传感器类型）：**显示传感器事件类型。
- **Description（说明）：**显示更多信息，包括生成该事件的传感器名称。
- **Clear All Event Logs（清除所有事件日志）：**清除所有事件日志选项可删除所有传感器的现有的所有记录。
  **注意：**有些事件日志“Bugcheck 代码 OEM 事件记录”是在系统 BSOD 后操作系统生成。
- **Save Event Logs（保存事件日志）：**单击此按钮弹出保存对话框，保存所有记录。

## BSOD 屏幕

该页面显示系统崩溃时捕获的蓝屏快照。

如要打开 BSOD 屏幕页面，请从菜单单击 **Server Health （服务器健康）> BSOD Screen（BSOD 屏幕）**。BSOD 屏幕截图示例如下。

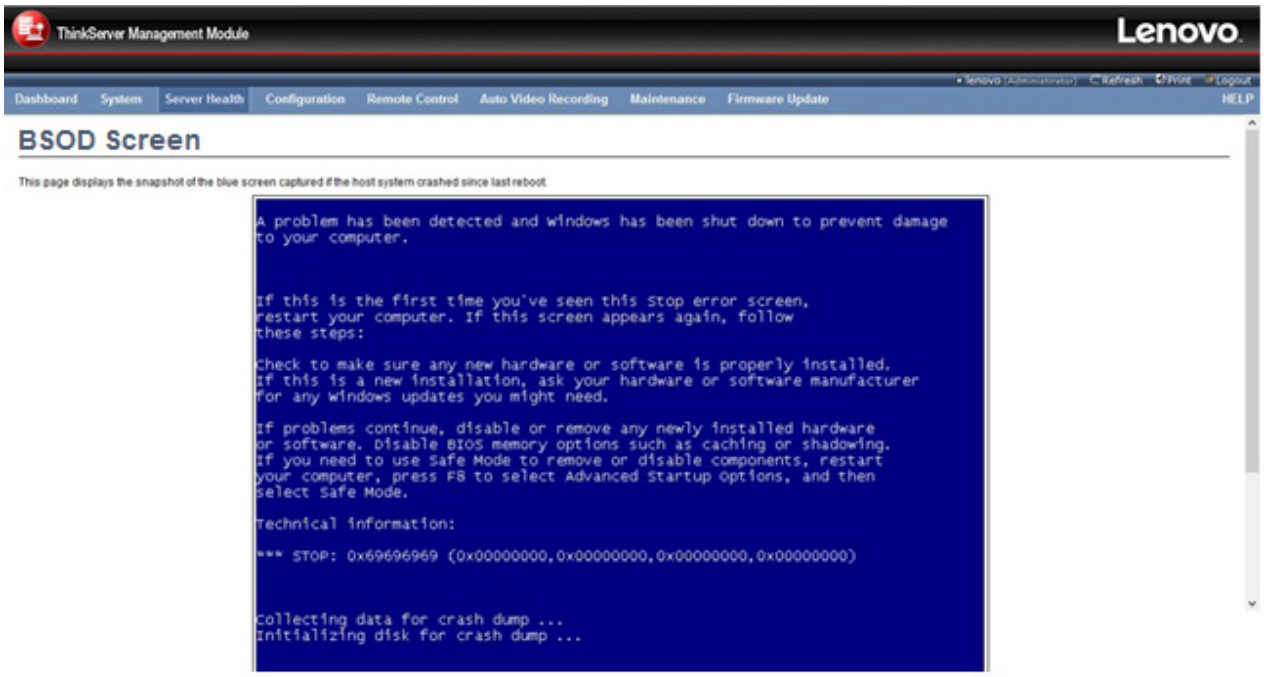



*图 13：BSOD 屏幕*

**注意：**

- 需要启用 KVM 服务才可显示 BSOD 屏幕。KVM 服务可在 Configuration（配置）-> Services（服务）->KVM 下配置。

## Configuration Group（配置组）

该组页面可访问不同的配置设置。配置组菜单截图如下。

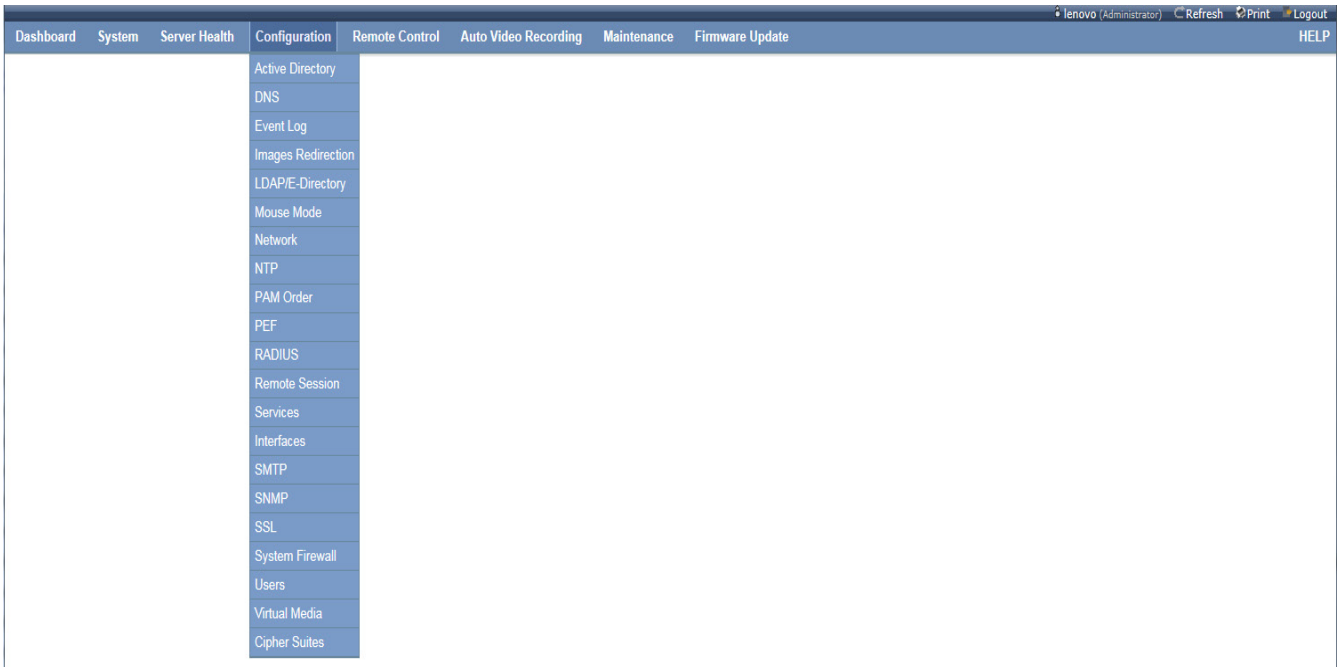



*图 14：配置组菜单*

下面详细介绍配置菜单。

## Active Directory（活动目录）

所列表格显示全部配置角色组和可用的插槽。可以在此修改、添加或删除角色组。组域可以是 AD 域或受信任的域。组名称应与实际 AD 组一致。要查看该页面，必须至少具有用户权限。如要修改或添加组，必须是管理员（或 OEM 专用）。

**注意：**空闲插槽在所有列中用“~”表示。

活动目录是指 Microsoft windows 计算机和服务器所用的目录结构，用于存储关于网络和域的信息和数据。活动目录（有时称为 AD）具有许多功能，包括提供对象信息。还可帮助组织这些对象，方便检索和访问，允许终端用户和管理员访问，允许管理员设置目录安全。

活动目录设置页面，从菜单栏单击 **Configuration（配置）> Active Directory（活动目录）**。活动目录页面截图示例如下。

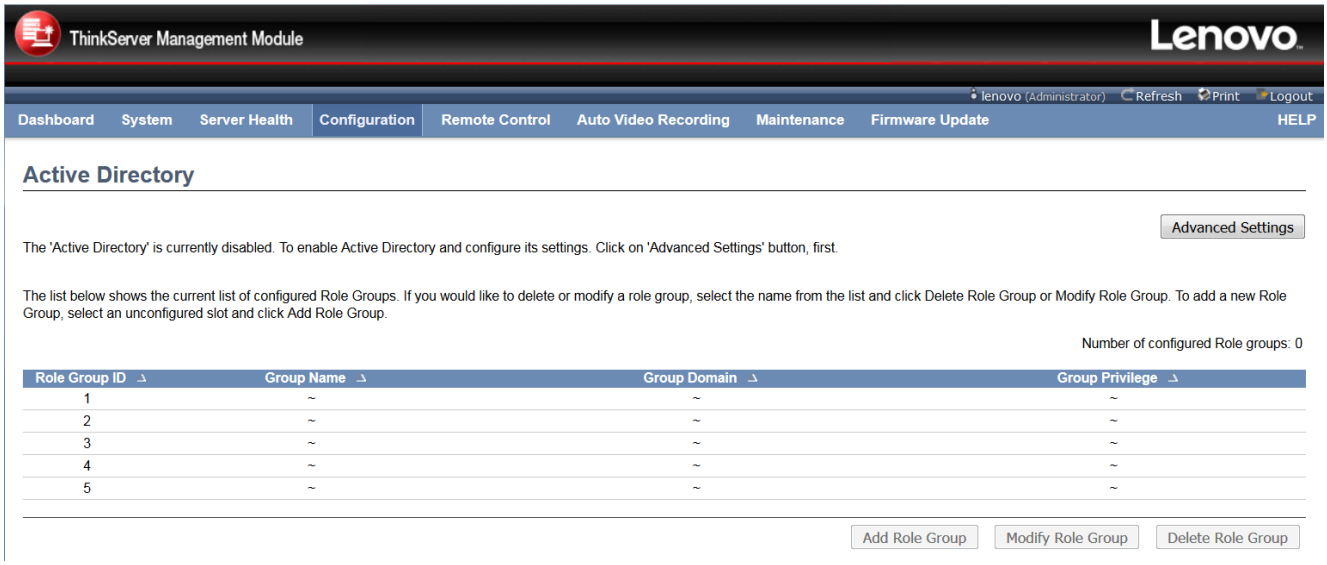



*图 15：活动目录设置*

- **Advanced Settings（高级设置）：**单击选项配置活动目录设置。选项包括活动目录身份验证、用户域名、超时和 3 个域控制器发射器地址。
- **Add Role Group（添加角色组）：**选择空闲插槽，单击“Add Role Group（添加角色组）”给设备添加新的角色组。还可双击空闲插槽添加角色组。
- **Modify Role Group（修改角色组）：**选择配置的插槽，单击“Modify Role Group（修改角色组）”修改角色组。还可双击配置的插槽。
- **Delete Role Group（删除角色组）：**选择要删除的角色组，单击“Delete Role Group（删除角色组）”。
- **Role Group ID（角色组 ID）：**角色组的编号。
- **Group Name（组名称）：**输入角色组名称。该名称用于标识活动目录中的角色组。
- **Group Domain（组域）：**这是角色组所在的域。
- **Group Privilege（组权限）：**这是分配给角色组的权限水平。

**Advanced Setting（高级设置）**

该页面用于配置活动目录高级设置，同时支持受信任的域。

活动目录设置页面，从菜单栏单击 **Configuration（配置）> Active Directory（活动目录）> Advanced Settings（高级设置）**。

活动目录页面截图示例如下。

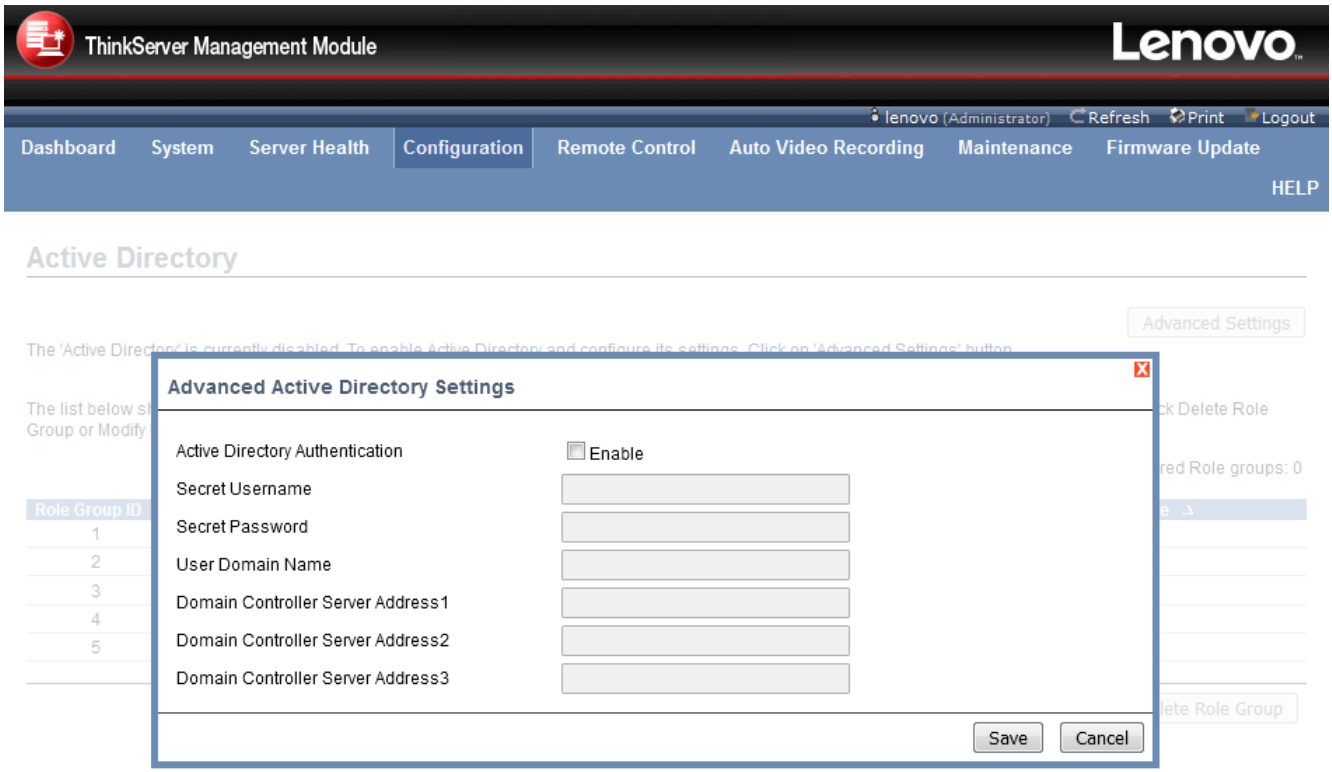



*图 16：高级活动目录设置*

- **Active Directory Authentication（活动目录身份验证）：**如要启用或禁止活动目录，可分别勾选或取消“Active Directory Authentication（活动目录身份验证）”复选框。
  如果启用了活动目录身份验证，那么可以输入所需的信息，访问活动目录服务器。
- **Secret Username（秘密用户）：**指定活动目录服务器的用户名。
  - 用户名是一串 1-64 数字字符。

- 第一个必须是字母字符。
- 并区分大小写。
- 不允许特殊字符，如逗号、句号、分号、冒号、斜杠、反斜杠、方括号、尖括号、竖线、等号、加号、星号、问号、双引号、空格。

**注意：**如果不需要秘密用户和密码，两个字段都留空。

- **Secret Password（秘密口令）：**指定活动目录服务器的密码。
  - 密码至少必须有 6 个字符。
  - 不允许空格。

  **注意：**该字段不能超过 127 个字符。
- **User Domain Name（用户域名）：**指定用户域名，如 MyDomain.com
- **Domain Controller Server Address1, Domain Controller Server Address2 & Domain Controller Server Address3（域控制器服务器地址 1，域控制器服务器地址 2 和域控制器服务器地址 3）：**输入活动目录服务器的 IP 地址。至少需要配置一个域控制器服务器地址。
  - IP 地址 4 组数字组成，由点分隔，如“xxx.xxx.xxx.xxx”。
  - 每一数字范围从 0 到 255。
  - 第一个数字不能为 0。

  域控制器服务器地址支持：
  - IPv4 地址格式。
  - IPv6 地址格式。
- **Save（保存）：**单击“Save（保存）”保存设置。
- **Cancel（取消）：**单击“取消”取消修改，返回到活动目录页面。

## DNS

该页面用于配置主机名和域名服务器。

**域名系统（DNS）**用于为连接到 Internet 或私有网络的计算机、服务器或任何资源分布式分层命名系统。它将网络成员与域名关联起来。最重要的是，它将人类可以识别的域名转换成网络设备数字（二进制）标识符，用于这些设备全球定位和寻址。DNS 服务器设置页面可用于管理设备的 DNS 设置。

DNS 服务器设置页面，从菜单栏单击 **Configuration（配置） > DNS**。DNS 服务器设置页面截图示例如下。

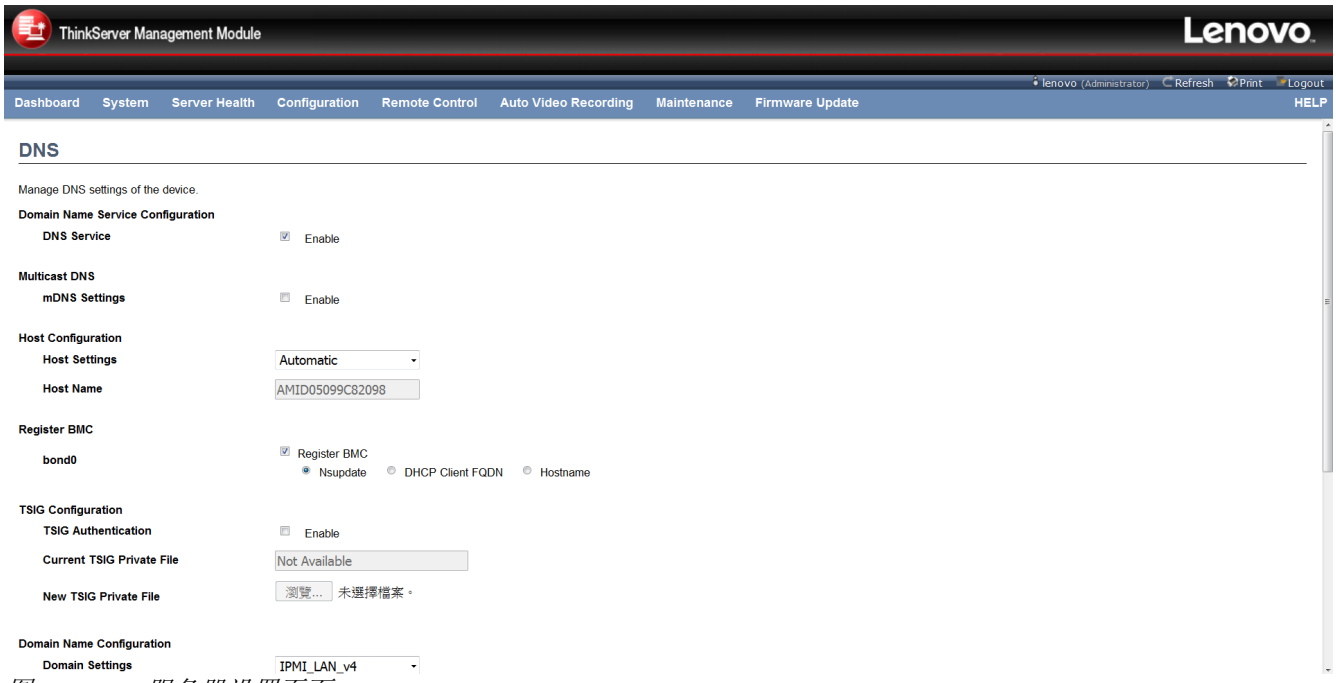



*图 17：DNS 服务器设置页面*

**Domain Name Service Configuration（域名服务配置）**

- **DNS Service（DNS 服务）：**选中启用所有 DNS 服务配置。

**Multicast DNS（组播 DNS）**

- **mDNS Settings（DNS 设置）：**选中启用或禁止 mDNS 支持配置。

**Host configuration（主机配置）**

- **Host Settings（主机设置）：**选择自动或手动设置。
- **Host Name（主机名）：**如果上面选择自动，显示设备主机名。如果主机设置选为手动，就需要手动设置设备主机名。
  - 值范围为 1 到 63 个数字字符。
  - 允许特殊字符“-”（连字符）和“_”（下划线）。
  - 首位不能使用“-”（连字符）。

  **注意：**如果主机名任何部分包含下划线（_），IE 浏览器无法正常工作。

**Register BMC（注册 BMC）**

选择 BMC 网络端口注册 DNS 设置。选中“Register BMC（注册 BMC）”注册 DNS 设置。

- **Nsupdate：**选择选项“Nsupdate”使用 nsupdate 应用注册 DNS 服务器。
- **DHCP Client FQDN（DHCP 客户端 FQDN）：**选择选项“DHCP Client FQDN（DHCP 客户端 FQDN）”，使用 DHCP 选项 81 注册 DNS 服务器。
- **Hostname（主机名）：**选择选项“DHostname（主机名）”，使用 DHCP 选项 12 注册 DNS 服务器。

  **注意：**如果 DHCP 服务器不支持 DHCP 客户端 FQDN 选项，请选择主机选项。

**TSIG Configuration（TSIG 配置）**

- **TSIG Authentication（TSIG 身份认证）：**勾选该选项，在通过 Nsupdate 注册 DNS 时启用 TSIG 身份验证。
- **Current TSIG Private File（当前 TSIG 私有文件）：**显示当前 TSIG 私有信息和更新的日期时间（只读）。
- **New TSIG Private File（新 TSIG 私有文件）：**浏览导航到 TSIG 私有文件。
  - TSIG 文件应为私有类型

**Domain Name Configuration（域务配置）**

- **Domain Settings（域名设置）：**列举域名接口选项，multiLAN 通道手动、v4 或 v6。
- **Domain Name（域名）：**如果上面选择自动，显示设备域名。如果域设置选为手动，就需要手动设置设备域名。

**Domain Name Server Configuration（域名服务器配置）**

- **DNS Server Settings（DNS 服务器设置）：**列举 DNS 接口、手动和可用的 LAN 接口选项。
- **IP Priority（IP 优先级）：**如果 IP 优先级是 IPv4，它就会有两个 IPv4 DNS 服务器和一个 IPv6 DNS 服务器。如果 IP 优先级是 IPv6，它就会有两个 IPv6 DNS 服务器和一个 IPv4 DNS 服务器。
  注意：手动配置不适用。
- **DNS Server 1, 2 & 3（DNS 服务器 1、2 和 3）：**指定要配置给 BMC 的 DNS（域名系统）服务器地址。
  - IPv4 地址由 4 组数字组成，由点分隔，如“xxx.xxx.xxx.xxx”。
  - 每一数字范围从 0 到 255。
  - 第一个数字不能为 0。

  DNS 服务器地址支持：
  - IPv4 地址格式。
  - IPv6 地址格式。

  **注意：**只允许全球 IPv6 地址。
- **Save（保存）：**单击“Save（保存）”保存所做的更改。会从当前界面会话注销，然后再次登录。
- **Reset（重置）：**重置所做的变更。

## Event Log（事件日志）

该页面用于配置系统事件日志行为。线性 SEL 类型可线性保存系统事件日志，直到达到 SEL 存储器大小，占满后 SEL 就会整个被丢弃。循环 SEL 类型可线性保存系统事件日志，直到达到 SEL 存储器大小，占满后 SEL 就会开始覆盖。

如要打开系统事件日志页面，请从菜单单击 **Configuration（配置）> Event Log（事件日志）**。系统事件日志页面截图示例如下。

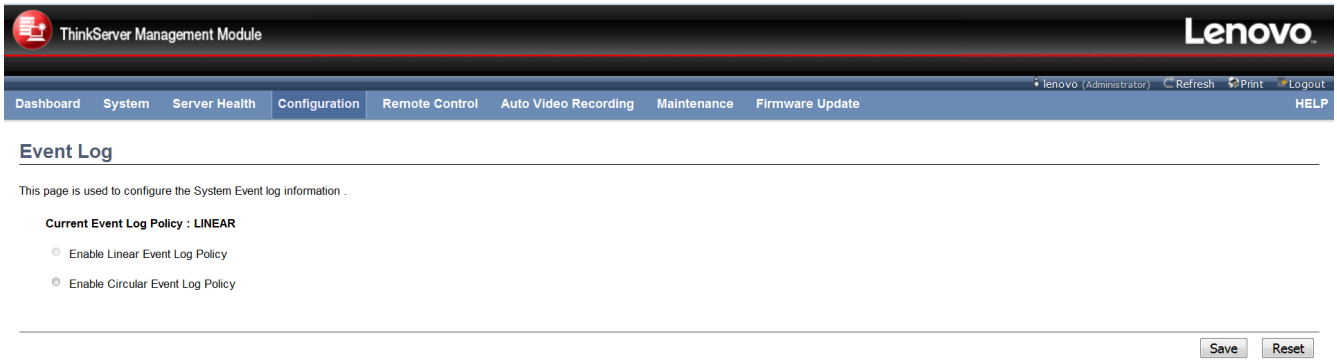



*图 18：系统事件日志页面*

- **Current Event Log Policy（当前事件日志策略）：** 显示配置事件日志策略。
- **Linear Event Log Policy（线性事件日志策略）：** 选中该选项启用事件日志的线性系统事件日志策略。
- **Circular Event Log Policy（循环事件日志策略）：** 选中该选项启用事件日志的循环系统事件日志策略。
- **Save（保存）：** 单击“Save（保存）”保存配置设置。
- **Reset（重置）：** 单击 “Reset（重置）”重置修改。

## Images Redirection（镜像重定向）

下表显示 BMC 上配置的镜像。启用或停止重定向或删除从这里到远程媒介的镜像。
每一镜像类型下可配置任何数量的镜像。
要配置镜像，使用“Advanced Settings（高级设置）”启用远程媒介支持。
要启用或停止重定向或删除镜像，必须具有管理员权限。
**注意：**空闲插槽使用“~”表示。
要打开镜像重定向页面，从菜单栏单击 **Configuration （配置）> Images Redirection（镜像重定向）**。镜像重定向页面示例如下。

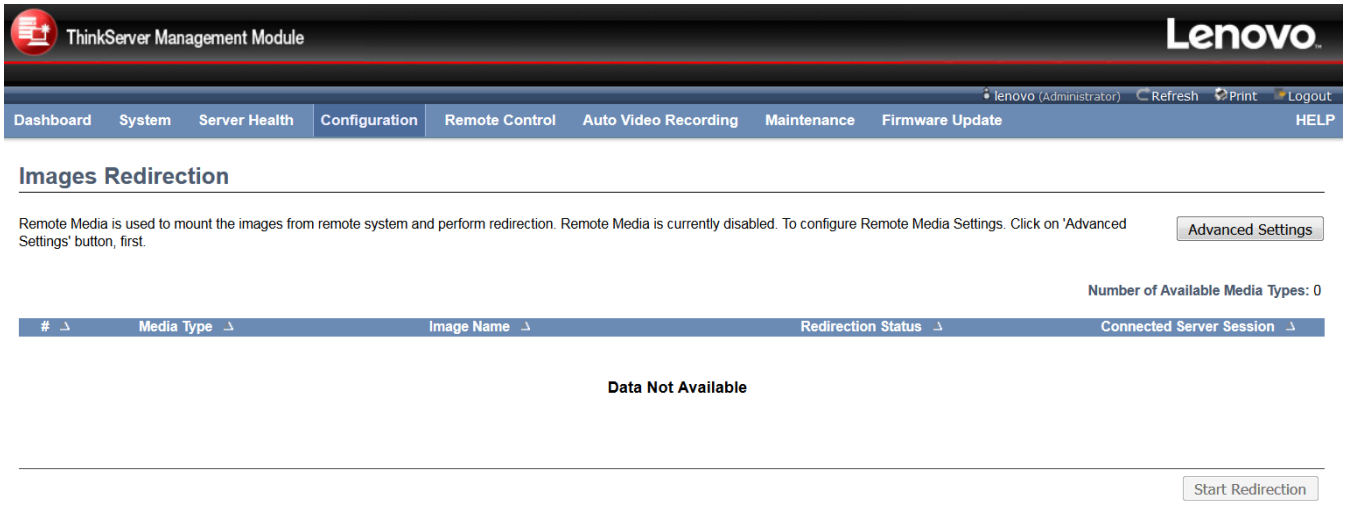



*图 19：镜像重定向页面*

- **Advanced Settings（高级设置）：** 单击选项配置远程媒介设置。可启用或禁止远程媒介支持、服务器地址、源路径、共享类型、用户名、密码和域名。
- **#:** 序列号。
- **Media Type（媒介类型）：** 显示支持的媒介类型。
- **Image Name（镜像名称）：** 显示镜像名称。
- **Redirection Status（重定向状态）：** 显示重定向状态。
- **Connected Server Session（连接的服务器会话）：** 显示已连接的服务器会话。
- **Start/Stop Redirection（开始 / 停止重定向）：** 选择配置的插槽，单击“Start Redirection（开始重定向）”开始启用远程媒介重定向。开关按钮。如果镜像被成功重定向，然后单击“Stop Redirection（停止重定向）”按钮停止远程媒介重定向。

### Advanced Setting（高级设置）

该页面用于配置高级媒介设置。

如要打开高级媒介设置页面，单击 **Configuration（配置） > Images Redirection（镜像重定向） > Advanced Settings（高级设置）**。

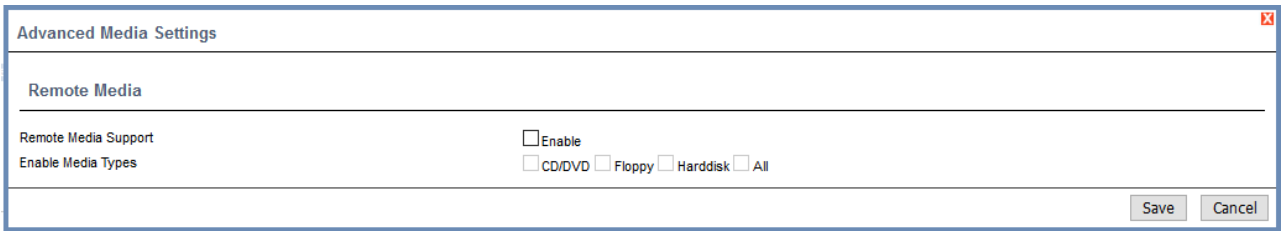



*图 20：高级媒介设置页面*

- **Remote Media Support（远程媒介支持）：** 如要启用或禁止远程媒介支持，可分别勾选或取消“Enable（启用）”。如果启用或禁止远程媒介支持，下列远程媒介类型会被启用或禁止。
- **Enable Media Types（启用媒介类型）：** 选择远程媒介类型。
- **CD/DVD, Floppy, Harddisk, All（CD/DVD、软盘、硬盘、全部）：** 下列字段根据所选远程媒介类型不同而可见。如果选择了 **All（全部）**选项，输入的全部配置会应用于所有的远程媒介类型。选择每个远程媒介类型会出现三个配置行。用户可以启用对应的媒介类型，给每一远程媒介类型配置不同设置。如果选择了 **All（全部）**，那么只会更新输入的媒介类型，配置同其他远程媒介类型。
- **Server Address（服务器地址）：** 存储远程媒介镜像的服务器地址。
- **Source Path（源路径）：** 到远程媒介镜像的源路径。
- **Share Type（共享类型）：** 远程媒介服务器的共享类型可以是 NFS 或 Samba（CIFS）。
- **Username, Password and Domain Name（用户名、密码和域名）：** 如果共享类型是 Samba（CIFS），那么请输入用户凭证完成服务器身份认证。
  **注意：**域名字段是可选字段。
- **Save（保存）：** 单击“Save（保存）”保存设置。
- **Cancel（取消）：** 单击“取消”取消修改，返回到活镜像列表。

## LDAP/E-Directory

**轻量目录访问协议（LDAP）/E-Directory 设置**是 Internet 协议（IP）网络中目录服务查询和修改数据的应用协议。

在 TMM 图形界面上，LDAP 是一种 Internet 协议，TMM 可用于验证用户身份。如果网络中配置了 LDAP 服务器，可以使用它方便地添加、管理和验证 TMM 用户。将登录请求发送给 LDAP 服务器实现。意味着使用 TMM 时无需定义其他验证机制。因为 LDAP 服务器进行集中验证，这样就可以始终知道谁在访问网络资源，可轻松定义用户或用户组策略或控制访问。

如要打开 LDAP/E-DIRECTORY 设置页面，从菜单栏单击 **Configuration（配置） > LDAP/E-Directory**。

LDAP/E-Directory 页面截图示例如下。

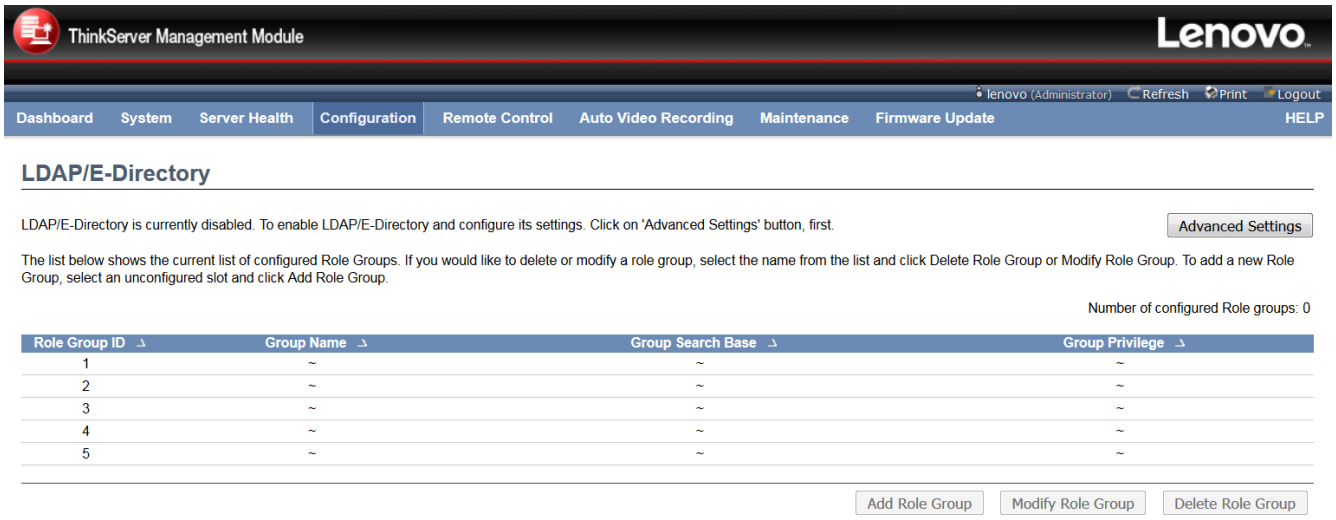



*图 21：LDAP/E-Directory 设置页面*

所列表格显示全部配置角色组和可用的插槽。可以在此修改、添加或删除角色组。
组搜索条件可以是组所在位置到基础域名的路径。组名称应与实际 LDAP/E-Directory 组一致。要查看该页面，必须至少具有用户权限。
如要修改或添加组，必须是管理员（或 OEM 专用）。
**注意：**空闲插槽在所有列中用“~”表示。

LDAP/E-Directory 页面字段说明如下。

- **Advanced Settings（高级设置）：**单击选项配置 LDAP/E-Directory 高级设置。启用 LDAP/E-Directory 身份认证、IP 地址、端口、绑定域名、密码和搜索条件的选项。
- **Add Role Group（添加角色组）：**选择空闲插槽，单击“Add Role Group（添加角色组）”给设备添加新的角色组。还可双击空闲插槽添加角色组。
- **Modify Role Group（修改角色组）：**选择配置的插槽，单击“Modify Role Group（修改角色组）”修改角色组。还可双击配置的插槽。
- **Delete Role Group（删除角色组）：**选择要删除的角色组，单击“Delete Role Group（删除角色组）”。

## Advanced Setting（高级设置）

使用该页面配置高级 LDAP/E-Directory 设置。
在 LDAP/E-Directory 设置页面，单击高级设置。
高级 LDAP/E-Directory 设置页面截图示例如下。


*图 22：高级 LDAP/E-Directory 设置页面*

- **LDAP/E-Directory Authentication（LDAP/E-Directory 身份验证）：** 勾选下面的框启用 LDAP/E-Directory 身份验证。
- **Encrypted Type（加密类型）：** 选择 LDAP/E-Directory 加密类型。
  **注意：** 启用 SSL 时，配置正确的端口号。
- **Server Address（服务器地址）：** LDAP/E-Directory 服务器 IP 地址
  - IP 地址 4 组数字组成，由点分隔，如“xxx.xxx.xxx.xxx”。
  - 每一数字范围从 0 到 255。
  - 第一个数字不能为 0。
  LDAP/E-Directory 服务器地址支持：
  - IPv4 地址格式。
  - IPv6 地址格式。
  **注意：** 使用 FQDN 下 StartTLS 时，请配置 FQDN 地址。
- **Port（端口）：** 指定 LDAP/E-Directory 端口。
  - 默认端口 389。
  - 对于 SSL 连接，默认端口是 636。
  - 端口数值范围从 1 到 65535。
- **Bind DN（绑定域名）：** 绑定域名用于绑定操作，进行客户端认证。
  -绑定域名是一串 4-63 数字字符。
  -第一个必须是字母字符。
  -允许特殊符号，如点（.)、逗号（,）、连接符（-）、下划线(_)、等号（=）。
  - 例如：cn=manager, ou=login, dc=domain, dc=com
- **Password（密码）：** 绑定密码用于绑定操作，进行客户端认证。
  -密码至少必须 1 个字符长。
  -不允许空格。
  **注意：** 该字段不能超过 48 个字符。
- **Search Base（搜索条件）：** 搜索条件告诉 LDAP/E-Directory 服务器要搜索哪部分外部目录树。搜索条件可以是外部目录组织、组。
  -搜索条件是一串 4-64 数字字符。
  -第一个必须是字母字符。
  -允许特殊符号，如点（.)、逗号（,）、连接符（-）、下划线(_)、等号（=）。
  - 例如：ou=login, dc=domain, dc=com
- **Attribute of User Login（用户登录属性）：** 用户登录字段属性告诉 LDAP/E-Directory 服务器应使用那些属性来确定用户[1]。
  - 仅支持 cn 或 uid
  **注意：** 启用 StartTLS 时需要所有 3 个文件。
- **Save（保存）：** 保存设置。
- **Cancel（取消）：** 取消所做的变更。

## Mouse Mode（鼠标模式）

重定向控制台使用三种方式之一，实现本地窗口到远程屏幕的鼠标仿真。只有“Administrator（管理员）”有权限配置该选项。

- 相对鼠标模式
- 绝对鼠标模式
- 其他鼠标模式

如要打开鼠标模式页面，从菜单栏单击 **Configuration（配置） > Mouse Mode（鼠标模式）**。鼠标模式设置截图示例如下。

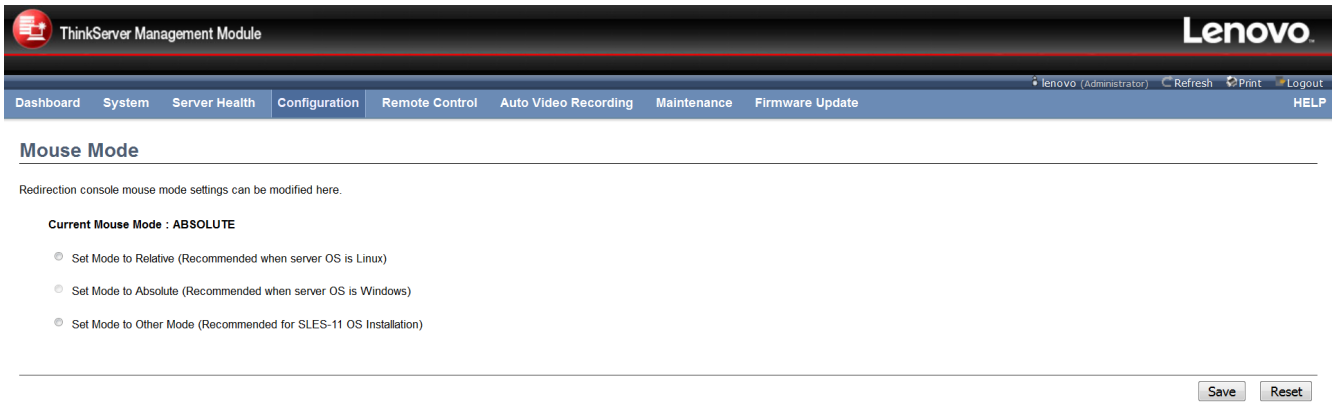



*图 23：鼠标模式设置页面*

鼠标模式设置页面字段说明如下。

- **Relative Mouse mode（相对鼠标模式）：**相对模式发送鼠标相对偏移计算值给服务器。如要选择该模式，请选择“Set mode to Relative（设置相对模式）”选项。
- **Absolute Mouse mode（绝对鼠标模式）：**发送本地鼠标绝对位置给服务器。如要选择该模式，请选择“Set mode to Absolute（设置绝对模式）”选项。建议 Windows 或高版本 Linux。
- **Other Mouse mode（其他鼠标模式）：**选择其他模式将本地鼠标离中心位置的偏移计算值发送给服务器。使用该模式安装 SLES 11 Linux OS。
- **Save（保存）：**单击“Save（保存）”保存所做的更改。
- **Reset（重置）：**单击 “Reset（重置）”重置修改。

## Network（网络）

该页面用于配置可用 LAN 通道的网络设置。

如要打开网络设置页面，从菜单栏单击 **Configuration（配置）> Network（网络）**。网络设置页面截图示例如下。

**建议：**

使用访问控制列表（ACL）或隔离网络限制对ThinkServer RS160 IPMI管理接口的访问。

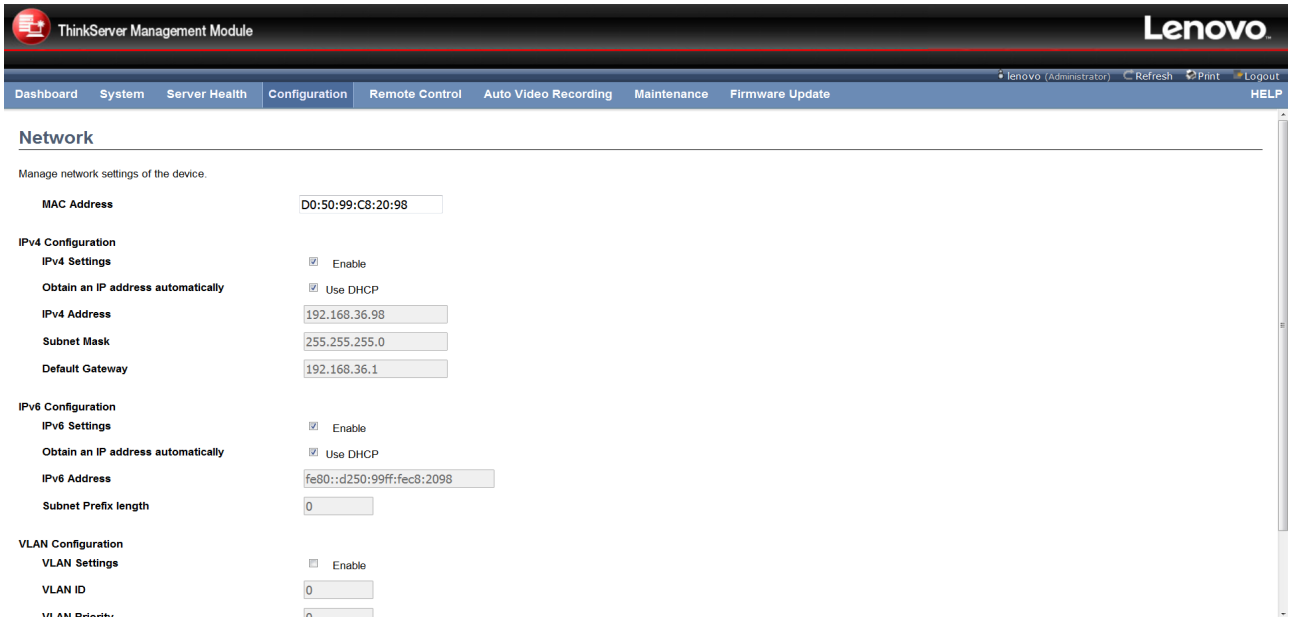



*图 24：网络设置页面*

网络设置页面字段说明如下。

- **MAC Address（MAC 地址）：**该字段显示所选接口（只读）的 MAC 地址。
- **IPv4 Configuration（IPv4 配置）：**它列出 IPv4 配置设置。
- **IPv4 Settings（IPv4 设置）：**勾选为所选接口启用 IPv4 支持。
- **Obtain an IP Address automatically（自动获取 IP 地址）：**启用“使用 DHCP”，使动态主机配置协议（DHCP）动态配置 IPv4 地址。
- **Ipv4 Address, Subnet Maslk, Default Gateway（IPv4 地址、子网掩码和默认网关）：**如果禁用 DHCP，请为所选接口指定静态 IPv4 地址、子网掩码和默认网关。
  - IP 地址由 4 组数字组成，由点分隔，如“xxx.xxx.xxx.xxx”。
  - 每一组范围从 0 到 255。
  - 第一个数字不能为 0。
- **IPv6 Configuration（IPv6 配置）：**它列出 IPv6 配置设置。
- **IPv6 Settings（IPv6 设置）：**勾选为所选接口启用 IPv6 支持。
- **Obtain an IPv6 address automatically（自动获取 IPv6 地址）：**启用“使用 DHCP”，使用动态主机配置 v6 协议（DHCPv6）动态配置 IPv6 地址。
- **IPv6 Address（IPv6 地址）**: 为所选接口指定静态 IPv6 地址。
- **Subnet Prefix length（子网前缀长度）：**指定 IPv6 的子网前缀长度。
  - 值范围为 0 到 128。
- **VLAN Configuration（VLAN 配置）：**它列出 VLAN 配置设置。
- **VLAN Settings（VLAN 设置）：**勾选为所选接口启用 VLAN 支持。
- **VLAN ID：**指定 VLAN 配置标识符。
  - 值范围为 2 到 4094。

  **注意：**未重设 VLAN 配置不能更改 VLAN ID。VLAN ID 0、1、4095 位保留 VLAN ID。
- **VLAN Priority（VLAN 优先级）：**指定 VLAN 配置优先级。
  - 值范围为 0 到 7。

  **注意：**7 是 VLAN 最高优先级。
- **Save（保存）：**单击“Save（保存）”保存所做的更改。提示从当前用户界面会话注销，然后从新 IP 地址登录。
- **Reset（重置）：**单击 “Reset（重置）”重置修改。

## NTP

该页面显示设备的当前日期和时间设置。可用于配置设备的日期和时间或 NTP（网络事件协议）服务器设置。

**Network Time Protocol(NTP)（网络时间协议（NTP））**协议用于同步数据包交换、可变延迟数据网络内的计算机系统时钟。使用抖动缓存器可有效消除不同延迟的影响。

如要打开 NTP 设置页面，从菜单栏单击 **Configuration（配置） > NTP**。NTP 设置页面截图示例如下。

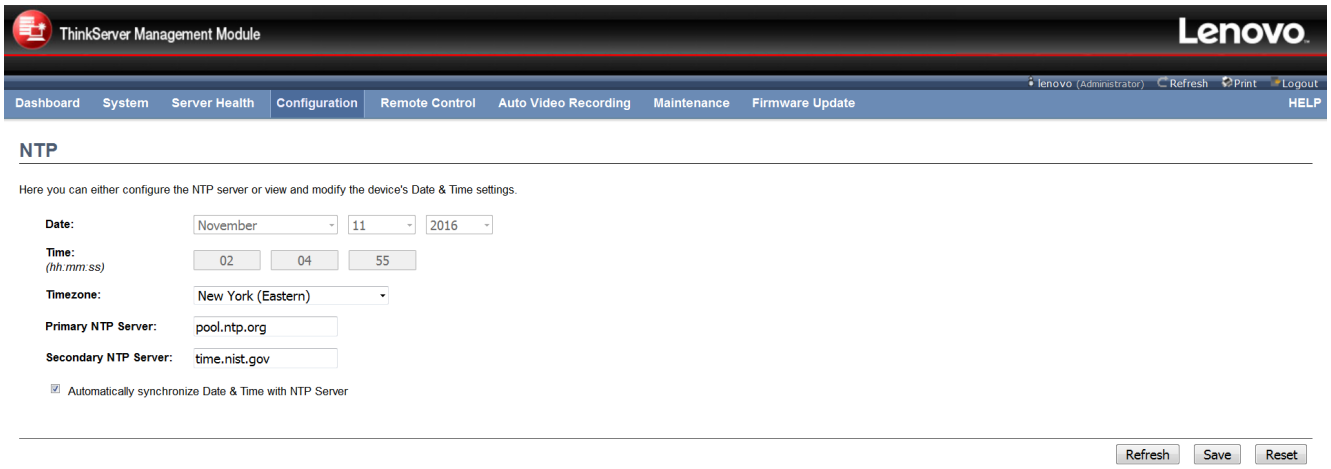



*图 25：NTP 设置页面*

NTP 配置字段说明如下。

- **Date（日期）**：指定设备日期。
- **Time（时间）**：指定设备时间。
  **注意：**因为存在 2038 年问题，可接受的日期范围是 01-01-2005 到 01-18-2038。
- **Primary NTP Server & Secondary NTP Server（主要 NTP 服务器和辅助 NTP 服务器）**：指定设备的 NTP 服务器。NTP 服务器字段支持：
  - IP 地址（IPv4 和 IPv6 格式）。
  - FQDN（完全限定域名）格式。
  - FQDN 值范围为 1 到 128 个数字字符。

  **注意：**辅助 NTP 服务器是可选字段。如果主 NTP 服务器不工作，辅助 NTP 服务器就会尝试继续。
- **Timezone（时区）**：时区列表包含 NTP 服务器的 UTC 偏移、位置、手动 UTC 偏移，可用于精确显示本地时间。
- **Automatically synchronize（自动同步）**: 勾选自动与 NTP 服务器每 12 小时同步日期和时间。
  **注意**：重启系统时，BIOS 会检查 BMC 时间。如果 BIOS 和 BMC 时差大于 2 秒，BIOS 回更新 BMC 时间。
- **Refresh（刷新）**：单击“Refresh（刷新）”重新加载当前日期和时间设置。
- **Save（保存）**：单击“Save（保存）”保存所做的更改。
- **Reset（重置）**：单击 “Reset（重置）”重置修改。

**注意**：如果用户取消“Automatically synchronize Date & Time with NTP Server（自动与 NTP 服务器同步日期和时间）”，则可以手动修改时间和时区。当用户修改时区时，不会自动修改当前时间。

## PAM Order（PAM 订购）

该页面可用于配置 BMC 用户身份验证 PAM 订购。

如要打开 PAM 订购页面，从菜单栏单击 **Configuration （配置）> PAM Order（PAM 订购）**。PAM 订购页面示例如下。

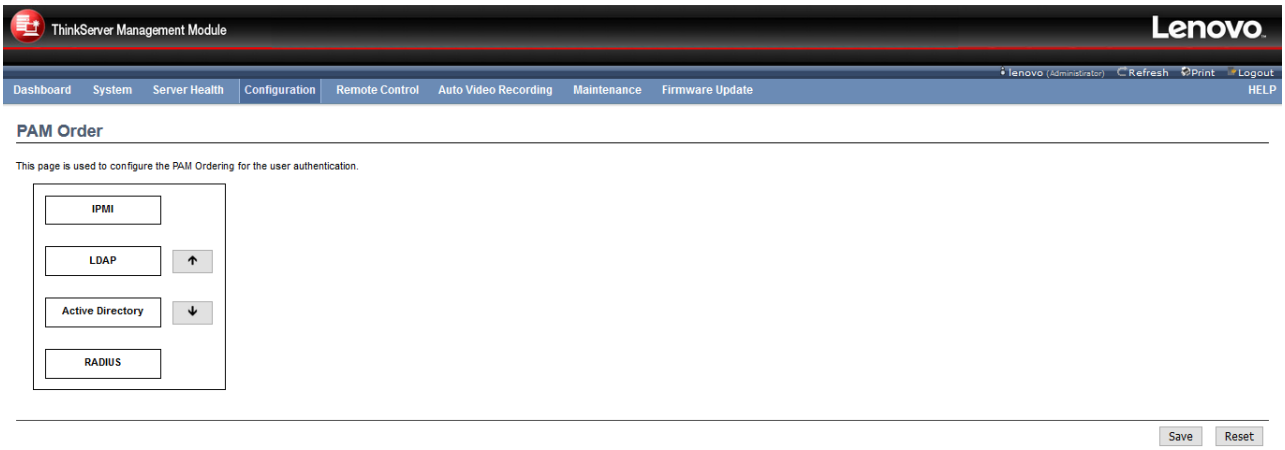



*图 26：PAM 订购页面*

- **PAM Module（PAM 模块）：** 显示 BMC 支持的 PAM 模块列表。
- **IPMI：** IPMI 的 PAM 模块。
- **LDAP：** LDAP 的 PAM 模块。
- **Active Directory（活动目录）：** 活动目录的 PAM 模块。
- **RADIUS：** RADIUS 的 PAM 模块。
- **Move Up（上移）：** 单击所需的 PAM 模块选中。单击“Move Up（上移）”将所选的 PAM 模块在现有 PAM 模块上移动一步。
- **Move down（下移）：** 单击所需的 PAM 模块选中。单击“Move Down（下移）”将所选的 PAM 模块在现有 PAM 模块下移动一步。
- **Save（保存）：** 单击“Save（保存）”保存所做的更改。
  **注意：** 一旦配置有修改，网页服务器就会自动重启。登录的会话都会注销。
- **Reset（重置）：** 单击 “Reset（重置）”重置修改。

## PEF

该页面用于配置事件过滤器、报警策略和报警的 LAN 目的地。要查看该页面，必须至少具有操作员权限。如要修改或添加 PEF，用户必须是管理员（或 OEM 专用）。
**注意：** 空闲插槽在特别列中用“~”表示。
如需了解更多信息，请参阅 IPMI 规范“平台事件过滤（PEF）”章节。
如要打开 PEF 管理设置页面，从菜单栏单击 **Configuration（配置）> PEF**。每一选项卡解释如下。

- **Event Filter（事件过滤）：** 单击事件过滤选项卡显示所有已配置的事件过滤器和可用的插槽。可以在此修改、添加新事件过滤条目。默认下，一共 40 个插槽中会配置 15 个事件过滤条目。
  - PEF ID：显示配置的 PEF 的 ID。
  - Filter Configuration（过滤配置）：显示 PEF 设置是否启用或禁止。
  - Event Filter Action（事件过滤动作）：这是必填字段，默认勾选。可启用 PEF 报警动作。
  - 事件严重性：显示事件严重性的 PEF 设置。
  - Sensor Name（传感器名称）：显示传感器名称的 PEF 设置。
- **Alert Policy（报警策略）：** 单击报警策略选项卡显示所有已配置的报警策略和可用的插槽。可以在此修改、添加新报警策略。最多可用 60 个插槽。
  - Policy Entry #（策略条目#）：显示策略编号。
  - Policy Number（策略编号）：显示事件过滤表中配置的策略编号。
  - Policy Configuration（策略配置）：显示策略设置是否启用或禁止。

- Policy Set（策略集）：显示策略集数值。
- Channel Number（通道编号）：显示通道编号的策略设置。
- Destination Selector（目的地选择器）：显示目的地选择器的策略设置。

- **LAN Destination（LAN 目的地）：**单击 LAN 目的地选项卡显示所有已配置的 LAN 目的地和可用的插槽。可以在此修改、添加新 LAN 目的地。最多可用 15 个插槽。
  - LAN Destination（LAN 目的地）：显示 LAN 目的地编号。
  - Destination Type（目的地类型）：显示目的地类型。
  - Destination Address（目的地地址）：显示目的地地址。

## Event Filter（事件过滤）

这些事件中其中一些应预先配置于常见系统故障事件，如过高温、电源系统故障、风扇故障事件等。剩余条目可用于系统管理软件配置的事件。注意每个条目都可标记预留给系统使用，所以在需要时，预先配置的条目和运行时可配置条目的比例可重新分配。事件过滤页面截图示例如下。

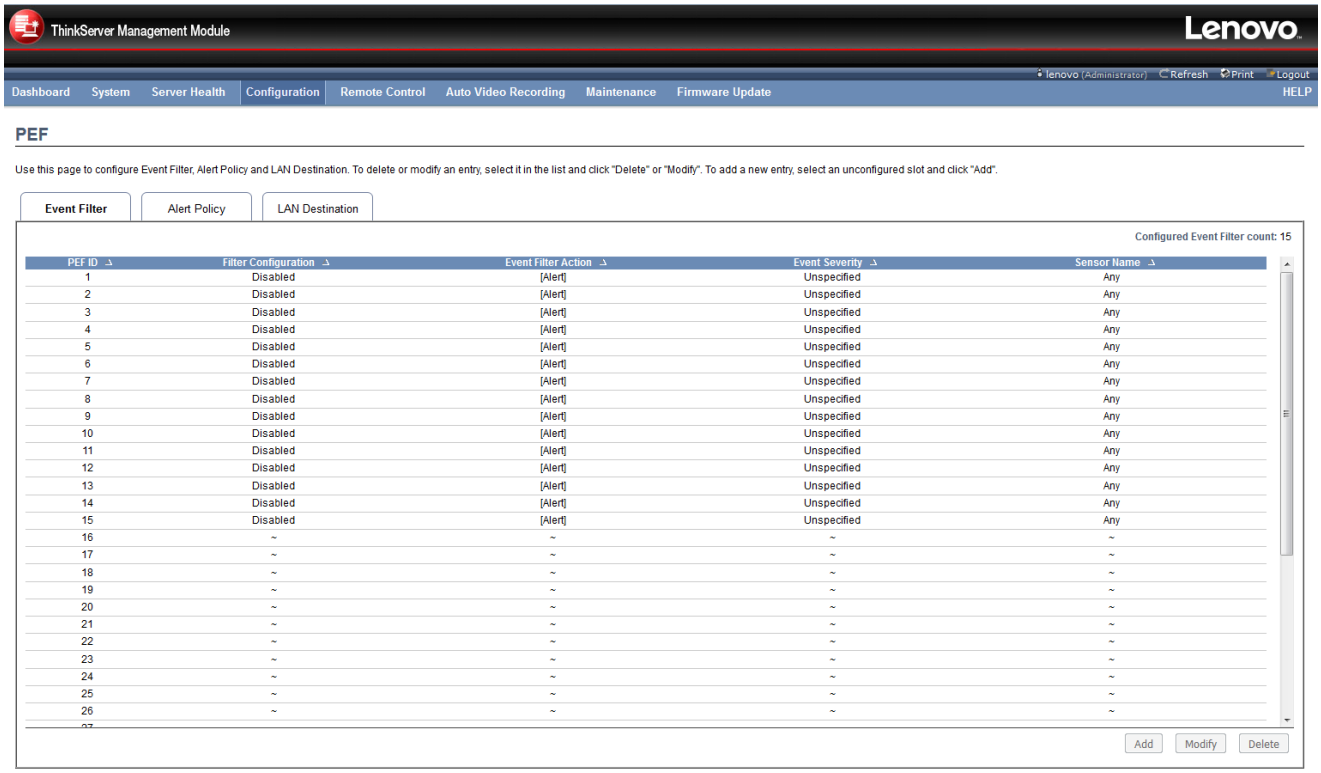



*图 27：PEF 管理：事件过滤页面*

PEF 管理字段：事件过滤选项卡解释如下。该页面包含一列配置的 PEF

- **Add（添加）：**选择空闲插槽，单击“Add（添加）”给设备添加新条目。还可双击空闲的插槽。
- **Modify（修改）：**选择配置的插槽，单击“Modify（修改）”修改所选条目。还可双击配置的插槽。
- **Delete（删除）：**选择要删除的插槽，然后单击“Delete（删除）”。

**Modify Event Filter Entry（修改事件过滤条目）：**

本表单用于修改现有的事件过滤条目。如需了解更多信息，请参阅 IPMI 规范“平台事件过滤（PEF）”章节。

- 单击 **Event Filter（事件过滤）**选项卡，在可用的插槽内配置事件过滤。
- 如要修改所选的条目，请选择已配置的插槽，单击 **Modify（修改）**或双击已配置的插槽，打开修改事件过滤条目页面。修改事件过滤页面截图示例如下。

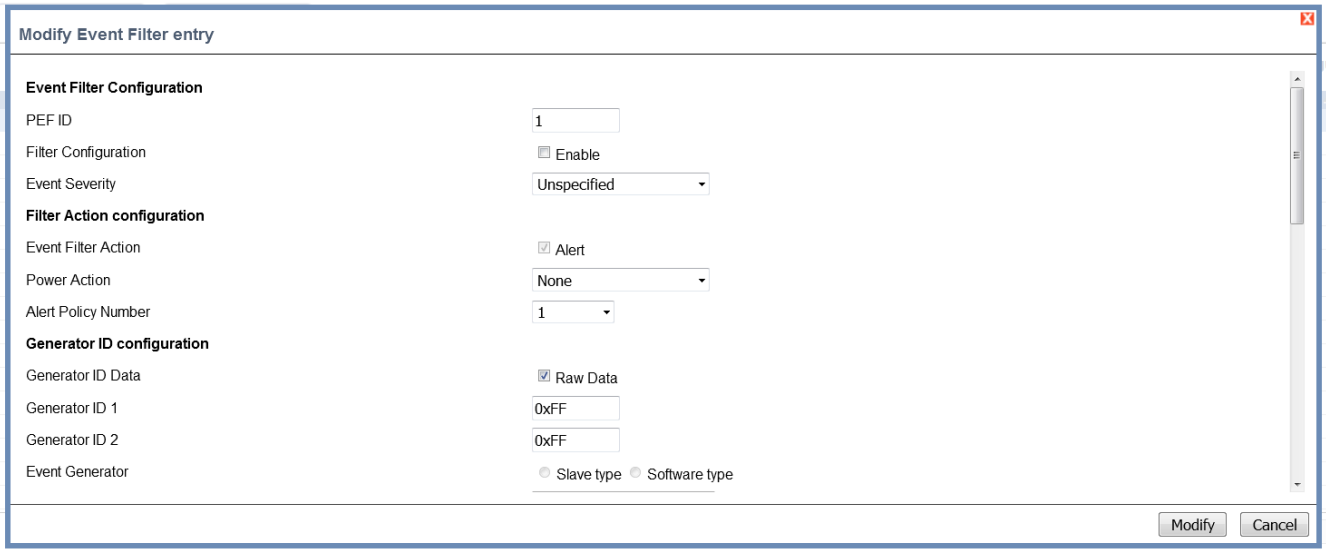



*图 28：PEF 管理：修改事件过滤页面*

**Event Filter Configuration（事件过滤配置）**

- **PEF ID：**显示配置的 PEF 的 ID（只读）。
- **Filter configuration（过滤配置）：**勾选“Enable（启用）”启用 PEF 设置。
- **Event Severity（事件严重性）：**从下拉列表中选择其中一种事件严重性。

**Filter Action configuration（过滤动作配置）**

- **Event Filter Action（事件过滤动作）：**这是必填字段，默认勾选。可启用 PEF 报警动作（只读）。
- **Power Action（电源动作）：**选择电源动作，从下拉列表中选择去电、复位或电源循环。
- **Alert Policy Number（报警策略编号）：**从下拉列表中选择已配置的报警策略编号。
  **注意：**报警策略可在 Configuration（配置）->PEF->Alert Policy（报警策略）下配置。

**Generator ID configuration（生成 ID 配置）**

- **Generator ID Data（生成 ID 数据）：**启用该选项进入原始数据生成 ID。
- **Generator ID 1（生成 ID 1）：**进入原始生成 ID1 数据。
- **Generator ID 2（生成 ID 2）：**进入原始生成 ID2 数据。
  **注意：**在 RAW 数据字段，使用“0x”指定十六进制前缀。
- **Event Generator（事件生成器）：**如果事件从 IPMB 生成，将事件生成器选为从地址，如果从系统软件生成，这选择系统软件 ID。
- **Slave Address/Software ID（从地址、软件 ID）：**指定对应的 $I^2C$ 从地址或系统软件 ID。
- **Channel Number（通道编号）：**选择接收事件消息的通道的编号。如果事件消息通过系统接口、主 IPMB 接收或由 BMC 内部生成，则选择“0”。
- **IPMB Device LUN（IPMB 设备 LUN）：**如果事件由 IPMB 生成，则选择对应的 IPMB 设备 LUN。

**Sensor configuration（传感器配置）**

- **Sensor Type（传感器类型）：**触发事件过滤动作的传感器类型。
- **Sensor Name（传感器名称）：**从传感器列表中选择特定传感器。

- **Event Options（事件选项）：**选择全部事件或传感器特定事件。
- **Sensor Events（传感器事件）：**所选传感器所有可能的事件列表。

**Event Data configuration（事件数据配置）**

- **Event Trigger（事件触发器）：**该字段用于赋予事件、读数类型数值。
  - 值范围为 1 到 255
- **Event Data 1 AND Mask（事件数据 1 和掩码）：**该字段用于表示通配或比较位。
  - 值范围为 0 到 255。
- **Event Data 1 Compare 1 & Event Data 1 Compare 2（事件数据 1 比较 1 和事件数据 1 比较 2）：**该字段用于表示每一位位置比较是否是精确比较。
  - 值范围为 0 到 255。

**Event Data 2 configuration（事件数据 2 配置）**

- **Event Data 2 AND Mask（事件数据 2 和掩码）：**该字段类似事件数据 1 和掩码。
- **Event Data 2 Compare 1 & Event Data 2 Compare 2（事件数据 2 比较 1 和事件数据 2 比较 2）：**这些字段分别类似事件数据 1 比较 1 和事件数据 1 比较 2。

**Event Data 3configuration（事件数据 3 配置）**

- **Event Data 3 AND Mask（事件数据 3 和掩码）：**该字段类似事件数据 1 和掩码。
- **Event Data 3 Compare 1 & Event Data 3 Compare 2（事件数据 3 比较 1 和事件数据 3 比较 2）：**这些字段分别类似事件数据 1 比较 1 和事件数据 1 比较 2。

- **Modify（修改）：**单击“Modify（修改）”接受修改，返回到事件过滤列表。
- **Delete（删除）：**单击“Cancel（取消）”取消修改，返回到事件过滤列表。

### Add Event Filter（添加事件过）：

使用该表单添加新事件过滤条目。如需了解更多信息，请参阅 IPMI 规范“平台事件过滤（PEF）”章节。

- 单击 **Event Filter（事件过滤）**选项卡，在可用的插槽内配置事件过滤。
- 如要添加事件过滤条目，请选择空闲插槽，单击 **Add（添加）**或双击空白插槽，打开添加事件过滤条目页面。

添加事件过滤页面截图示例如下。

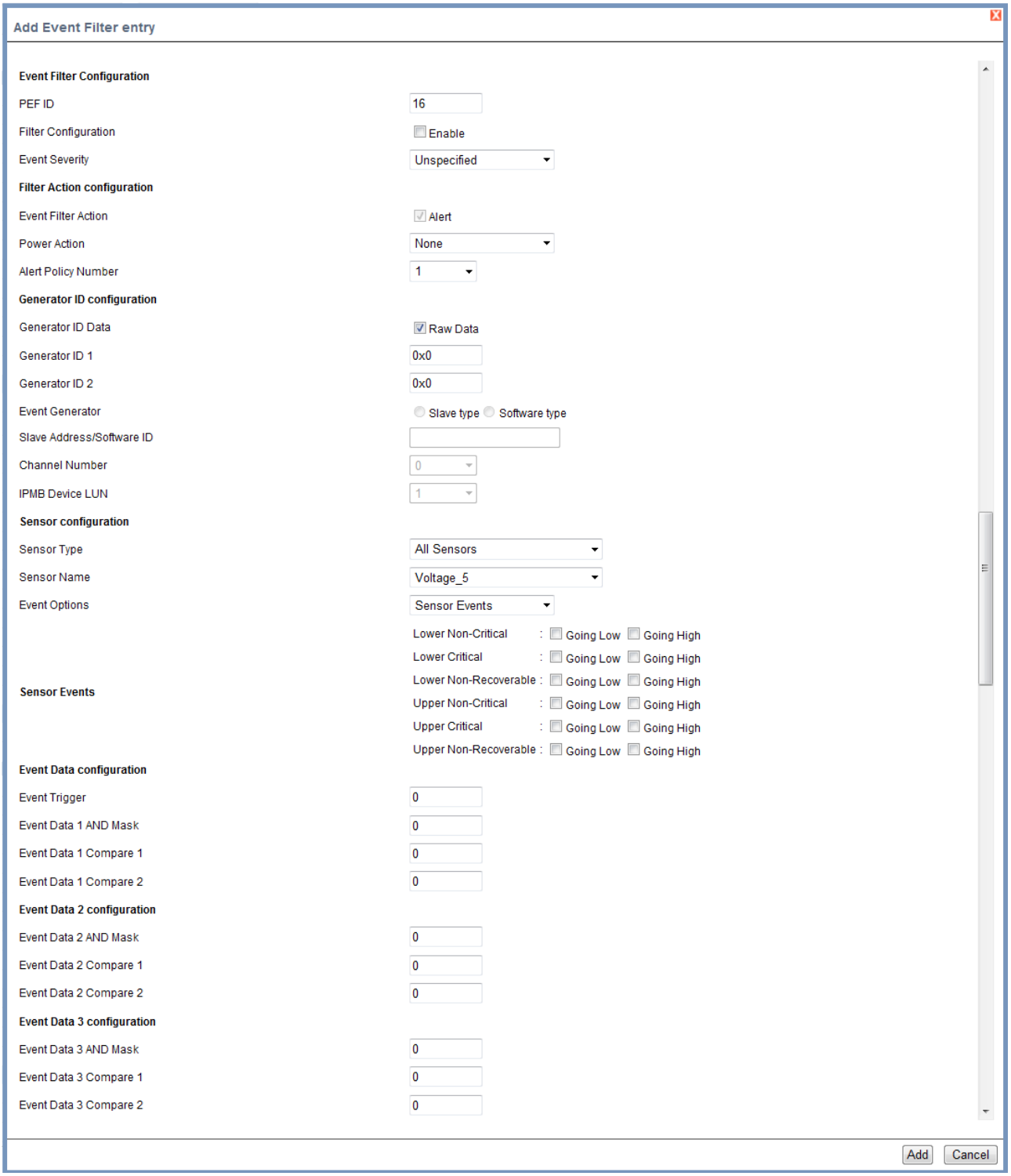



*图 29：PEF 管理：添加事件过滤条目页面*

**Event Filter Configuration（事件过滤配置）**

- **PEF ID：**显示新配置的 PEF 的 ID（只读）。
- **Filter configuration（过滤配置）：**勾选“Enable（启用）”启用 PEF 设置。
- **Event Severity（事件严重性）：**从下拉列表中选择其中一种事件严重性。

**Filter Action configuration（过滤动作配置）**

- **Event Filter Action（事件过滤动作）：**这是必填字段，默认勾选。可启用 PEF 报警动作（只读）。
- **Power Action（电源动作）：**选择电源动作，从下拉列表中选择去电、复位或电源循环。
- **Alert Policy Number（报警策略编号）：**从下拉列表中选择已配置的报警策略编号。
  **注意：**报警策略可在 Configuration（配置）->PEF->Alert Policy（报警策略）下配置。

**Generator ID configuration（生成 ID 配置）**

- **Generator ID Data（生成 ID 数据）：**启用该选项进入原始数据生成 ID。
- **Generator ID 1（生成 ID 1）：**进入原始生成 ID1 数据。
- **Generator ID 2（生成 ID 2）：**进入原始生成 ID2 数据。
  **注意：**在 RAW 数据字段，使用“0x”指定十六进制前缀。
- **Event Generator（事件生成器）：**如果事件从 IPMB 生成，将事件生成器选为从地址，如果从系统软件生成，这选择系统软件 ID。
- **Slave Address/Software ID（从地址、软件 ID）：**指定对应的 $I^2C$ 从地址或系统软件 ID。
- **Channel Number（通道编号）：**选择接收事件消息的通道的编号。如果事件消息通过系统接口、主 IPMB 接收或由 BMC 内部生成，则选择“0”。
- **IPMB Device LUN（IPMB 设备 LUN）：**如果事件由 IPMB 生成，则选择对应的 IPMB 设备 LUN。

**Sensor configuration（传感器配置）**

- **Sensor Type（传感器类型）：**触发事件过滤动作的传感器类型。
- **Sensor Name（传感器名称）：**从传感器列表中选择特定传感器。
- **Event Options（事件选项）：**选择全部事件或传感器特定事件。
- **Sensor Events（传感器事件）：**所选传感器所有可能的事件列表。

**Event Data configuration（事件数据配置）**

- **Event Trigger（事件触发器）：**该字段用于赋予事件、读数类型数值。
  - 值范围为 1 到 255
- **Event Data 1 AND Mask（事件数据 1 和掩码）：**该字段用于表示通配或比较位。
  - 值范围为 0 到 255。
- **Event Data 1 Compare 1 & Event Data 1 Compare 2（事件数据 1 比较 1 和事件数据 1 比较 2）：**该字段用于表示每一位位置比较是否是精确比较。
  - 值范围为 0 到 255。

**Event Data 2 configuration（事件数据 2 配置）**

- **Event Data 2 AND Mask（事件数据 2 和掩码）：**该字段类似事件数据 1 和掩码。
- **Event Data 2 Compare 1 & Event Data 2 Compare 2（事件数据 2 比较 1 和事件数据 2 比较 2）：**这些字段分别类似事件数据 1 比较 1 和事件数据 1 比较 2。

**Event Data 3configuration（事件数据 3 配置）**

- **Event Data 3 AND Mask（事件数据 3 和掩码）：**该字段类似事件数据 1 和掩码。
- **Event Data 3 Compare 1 & Event Data 3 Compare 2（事件数据 3 比较 1 和事件数据 3 比较 2）：**这些字段分别类似事件数据 1 比较 1 和事件数据 1 比较 2。

- **Add（添加）：**单击“Add（添加）”保存新事件过滤条目，并返回到事件过滤列表。
- **Cancel（取消）：**单击“Cancel（取消）”取消修改，返回到事件过滤列表。

### Alert Policy（报警策略）

该页面用于配置 PEF 配置的报警策略。可以添加、删除或修改该页面内任何条目。报警策略页面截图示例如下。

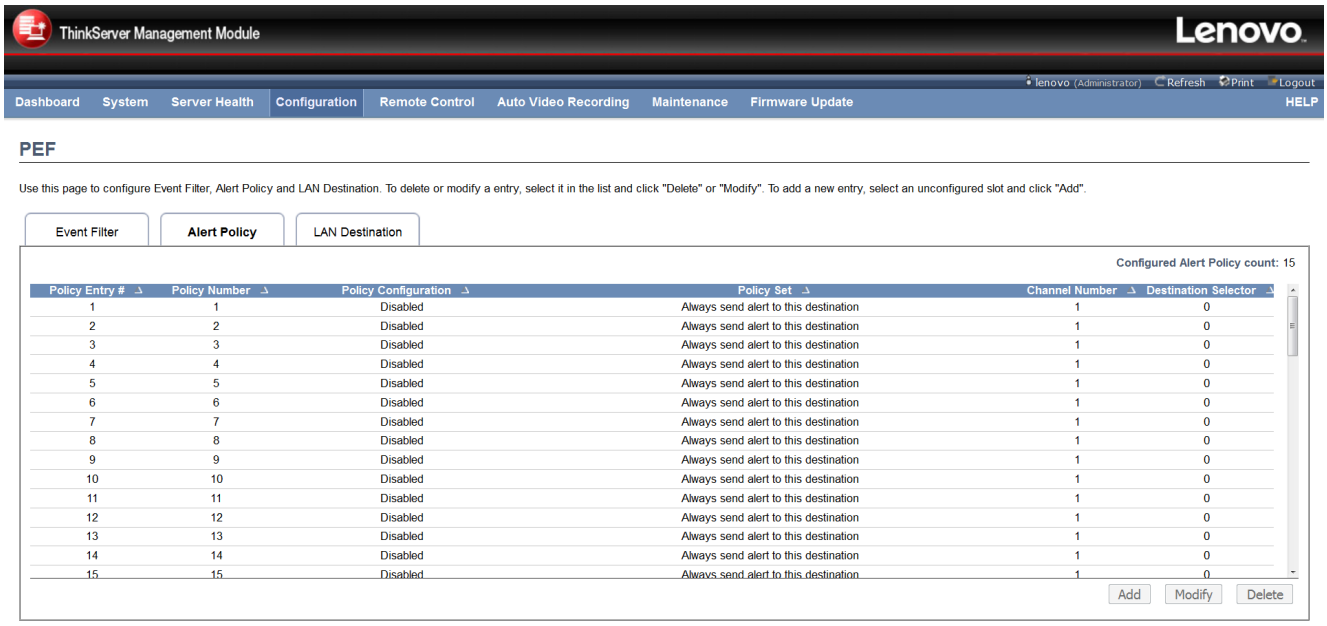



*图 30：PEF 管理：报警策略页面*

PEF 管理字段：报警策略选项卡解释如下。

- **Add（添加）：**选择空闲插槽，单击“Add（添加）”给设备添加新条目。还可双击空闲的插槽。
- **Modify（修改）：**选择配置的插槽，单击“Modify（修改）”修改所选条目。还可双击配置的插槽。
- **Delete（删除）：**选择要删除的插槽，然后单击“Delete（删除）”。

**Modify Alert Policy Entry（修改报警策略条目）：**

本表单用于修改现有的报警策略。如需了解更多信息，请参阅 IPMI 规范“平台事件过滤（PEF）”章节。

- 在报警策略选项卡，选择要配置报警策略的插槽。也就是说，在 **Event Filter Entry Page（事件过滤条目页面）**，如果报警策略编号已经选为 4，就可以在报警策略选项卡中配置第 4 个插槽（策略编号为 4 的插槽）。
- 选择插槽，单击 **Modify（修改）**或双击已配置的插槽，打开如下所示的 **Modify Alert Policy Entry Page（修改报警策略条目页面）**。

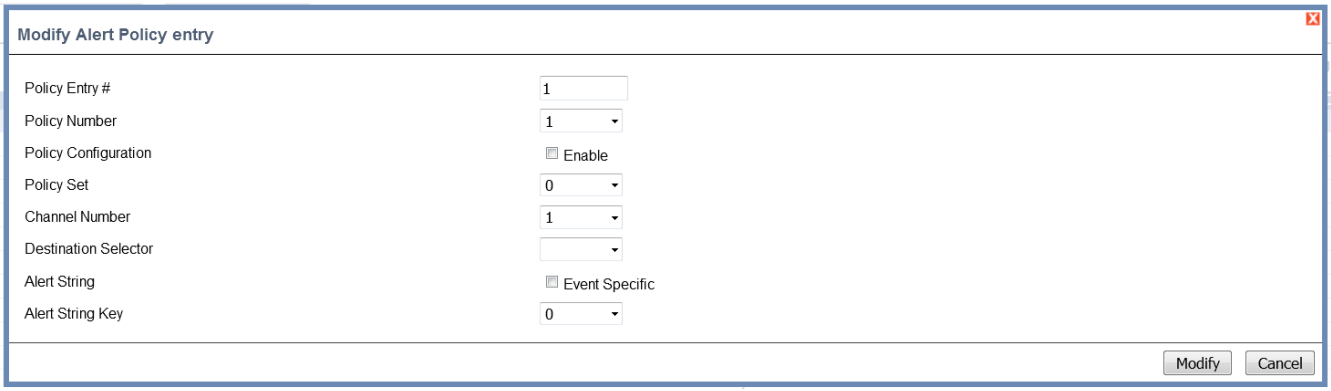



*图 31：PEF 管理：修改报警策略页面*

- **Policy Entry #（策略条目#）：**该字段显示所选插槽的策略编号（只读）。
- **Policy Number（策略编号）：**选择事件过滤表中配置的策略编号。
- **Policy Configuration（策略配置）：**勾选“Enable（启用）”启用策略设置。

- **Policy Set（策略集）：**从列表中选择任一策略集。
  0 - 始终发送报警到该目的地。
  1 - 如果到前一目的地的报警已成功，请勿发送报警给这个目的地。继续策略集中下一条。
  2 - 如果到前一目的地的报警已成功，请勿发送报警给这个目的地。请勿继续处理策略集中其他策略。
  3 - 如果到前一目的地的报警已成功，请勿发送报警给这个目的地。继续策略集中分配给其他通道的下一条。
  4 - 如果到前一目的地的报警已成功，请勿发送报警给这个目的地。继续策略集中分配给其他目的地类型的下一条。
- **Channel Number（通道编号）：**从可用的通道列表中选择所需的通道。
- **Destination Selector（目的地选择器）：**从配置的目的地列表中选择所需的目的地。
  **注意：**需要在 Configuration（配置）->PEF->LAN Destination（LAN 目的地）配置 LAN 目的地。
- **Alert String（报警字符串）：**勾选指定事件相关的报警字符串。
- **Alert String Key（报警字符串键）：**从一组数字中选择，全部链接到 PEF 配置参数中的字符串，指定该报警策略要发送的字符串。
- **Modify（修改）：**单击“Modify（修改）”接受修改，返回到报警过滤列表。
- **Cancel（取消）：**单击“Cancel（取消）”取消修改，返回到报警过滤列表。

### Add Alert Policy Entry（添加报警策略条目）：

本表单用于添加新报警策略。如需了解更多信息，请参阅 IPMI 规范“平台事件过滤（PEF）”章节。

- 在报警策略选项卡，选择要配置报警策略的插槽。也就是说，在 **Event Filter Entry Page（事件过滤条目页面）**，如果报警策略编号已经选为 4，就可以在报警策略选项卡中配置第 4 个插槽（策略编号为 4 的插槽）。
- 选择插槽，单击 **Add（添加）**或双击空闲的插槽，打开如下所示的 **Add Alert Policy Entry Page（添加报警策略条目页面）**。

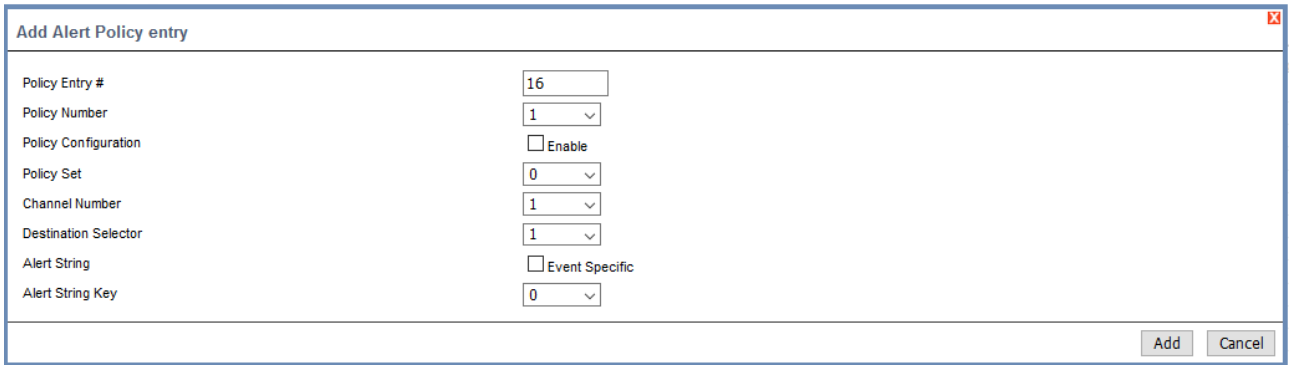



*图 32：PEF 管理：添加报警策略条目页面*

- **Policy Entry #（策略条目#）：**该字段显示所选插槽的策略编号（只读）。
- **Policy Number（策略编号）：**选择事件过滤表中配置的策略编号。
- **Policy Configuration（策略配置）：**勾选“Enable（启用）”启用策略设置。
- **Policy Set（策略集）：**从列表中选择任一策略集。
  0 - 始终发送报警到该目的地。
  1 - 如果到前一目的地的报警已成功，请勿发送报警给这个目的地。继续策略集中下一条。
  2 - 如果到前一目的地的报警已成功，请勿发送报警给这个目的地。请勿继续处理策略集中其他策略。
  3 - 如果到前一目的地的报警已成功，请勿发送报警给这个目的地。继续策略集中分配给其他通道

的下一条。

4 - 如果到前一目的地的报警已成功，请勿发送报警给这个目的地。继续策略集中分配给其他目的地类型的下一条。

- **Channel Number（通道编号）：**从可用的通道列表中选择所需的通道。
- **Destination Selector（目的地选择器）：**从配置的目的地列表中选择所需的目的地。
  **注意：**需要在 Configuration（配置）->PEF->LAN Destination（LAN 目的地）配置 LAN 目的地。
- **Alert String（报警字符串）：**勾选指定事件相关的报警字符串。
- **Alert String Key（报警字符串键）：**从一组数字中选择，全部链接到 PEF 配置参数中的字符串，指定该报警策略要发送的字符串。
- **Add（添加）：**单击“Add（添加）”保存新报警过滤条目，并返回到报警策略列表。
- **Cancel（取消）：**单击“Cancel（取消）”取消修改，返回到报警过滤列表。

## LAN Destination（LAN 目的地）

该页面用于配置 PEF 配置的 LAN 目的地。LAN 目的地页面截图示例如下。

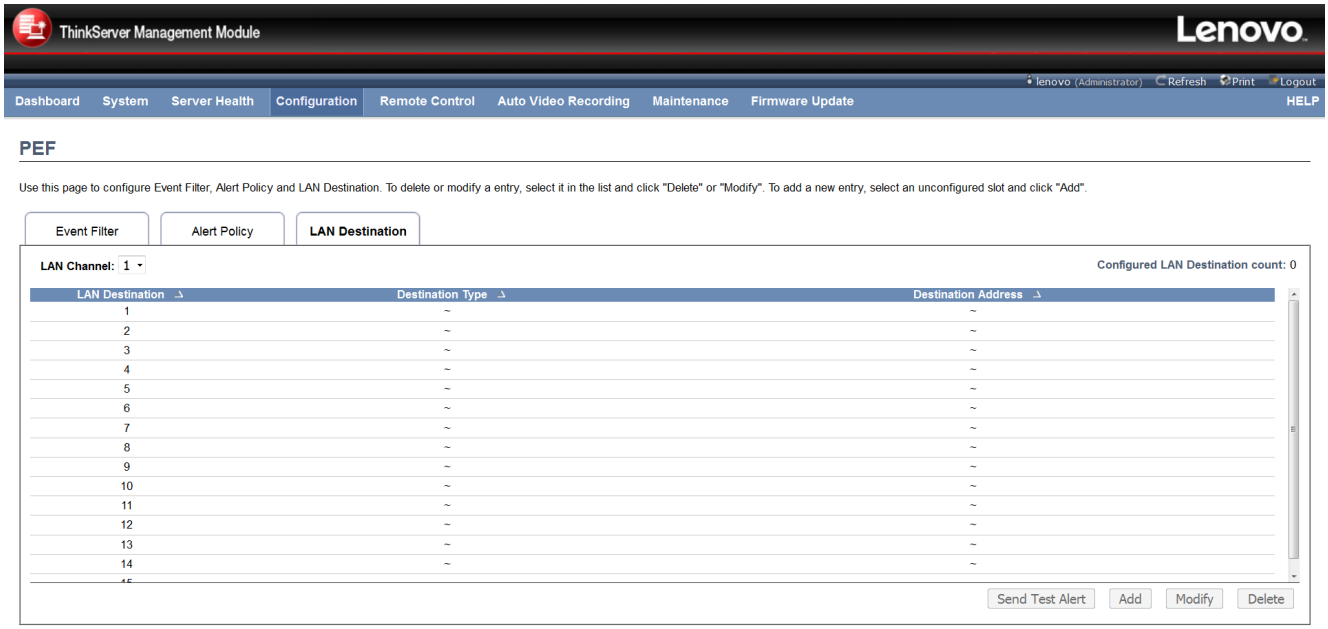



*图 33：PEF 管理：LAN 目的地页面*

PEF 管理字段：LAN 目的地选项卡解释如下。

- **LAN Channel（LAN 通道）：**请从下面列表选择要配置的 LAN 通道。
- **Send Test Alert（发送测试报警）：**在 LAN 目的地选项卡中选择已配置的插槽，单击“Send Test Alert（发送测试报警）”，将示例报警发送到已配置的目的地。
  **注意：**只有配置好 SMTP 后才可发送测试报警。可在 Configuration（配置）->SMTP 下启用 SMTP 支持。确保 SMTP 服务器地址和端口号都被正确配置。
- **Add（添加）：**选择空闲插槽，单击“Add（添加）”给设备添加新条目。还可双击空闲的插槽。
- **Modify（修改）：**选择配置的插槽，单击“Modify（修改）”修改所选条目。还可双击配置的插槽。
- **Delete（删除）：**选择要删除的插槽，然后单击“Delete（删除）”。

**Modify LAN Destination entry（修改 LAN 目的地）：**

本表单用于修改现有的 LAN 目的地。

- 在 **LAN Destination Tab（LAN 目的地选项卡）**，选择要配置的插槽。应跟在报警策略中：目的地选择器字段所选的插槽一致。如果在报警策略选项卡的报警策略页面的目的地选择器中选择了 4，那么就要在 LAN 目的地页面选择第 4 个插槽。
- 选择插槽，然后单击 **Modify（修改）**或双击已配置的插槽。打开 **Modify LAN Destination entry（修改 LAN 目的地）**。

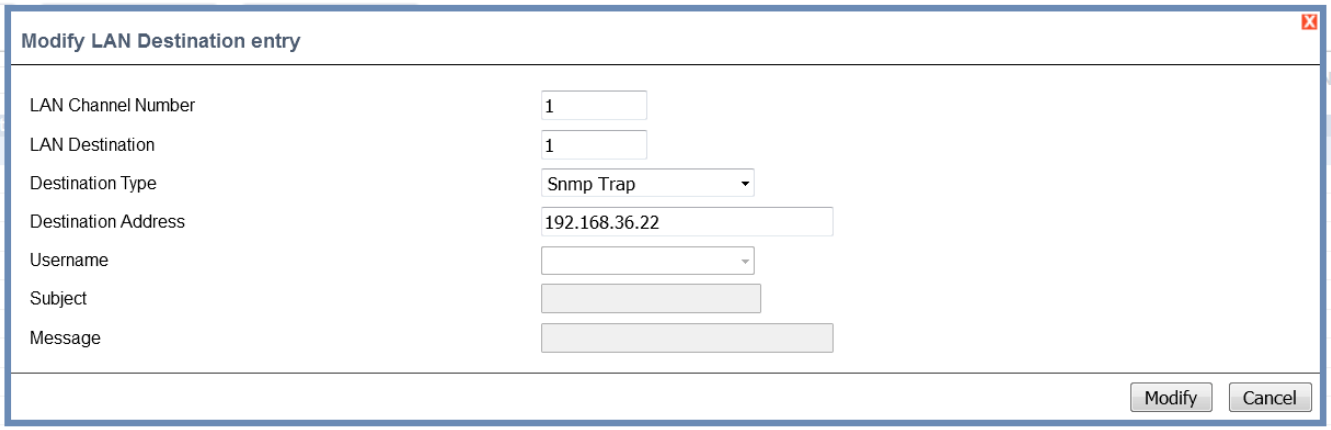



*图 34：PEF 管理：修改 LAN 目的地页面*

- **LAN Channel Number（LAN 通道编号）：**显示所选插槽的 LAN 通道编号（只读）。
- **LAN Destination（LAN 目的地）：**显示所选插槽的目的地编号（只读）。
- **Destination Type（目的地类型）：**目的地类型可以是 SNMP 陷阱或电子邮件通知。如果是 SNMP 陷阱，需要填写目的地 IP 地址。如果是电子邮件通知，需要填写 3 个字段，用户名、邮件主题和正文。还要在 **Configuration（配置）->SMTP** 下配置 SMTP 服务器信息。
- **Destination Address（目的地地址）：**如果目的地类型是 SNMP 陷阱，这填写接收报警的系统 IP 地址。目的地地址支持：
  - IPv4 地址格式。
  - IPv6 地址格式。
- **Username（用户名）：**如果目的地类型是电子邮件通知，那么可选择电子邮件通知要发送到的用户。
  **注意：**可在 Configuration（配置）->Users（用户）下配置用户电子邮件地址。
- **Subject & Message（主题和消息）：**如果目的地类型选择电子邮件通知，这这些字段必须配置。如果发生任何严重等级的事件，就会给用户电子邮件地址发送一封电子邮件，主题由“主题”字段定义，邮件正文包含字段内容。
  **注意：**这些字段不可用于“AMI-格式”电子邮件用户。
- **Modify（修改）：**单击“Modify（修改）”接受修改，返回到 LAN 目的地列表。
- **Cancel（取消）：**单击“Cancel（取消）”取消修改，返回到 LAN 目的地列表。

**Add LAN Destination entry（添加 LAN 目的地）：**

使用该表单添加新 LAN 目的地。

- 在 **LAN Destination Tab（LAN 目的地选项卡）**，选择要配置的插槽。应跟在报警策略中：目的地选择器字段所选的插槽一致。如果在报警策略选项卡的报警策略页面的目的地选择器中选择了 4，那么就要在 LAN 目的地页面选择第 4 个插槽。
- 选择插槽，然后单击 **Add（添加）**或双击空闲的插槽。打开 **Add LAN Destination entry（添加 LAN**

目的地）。

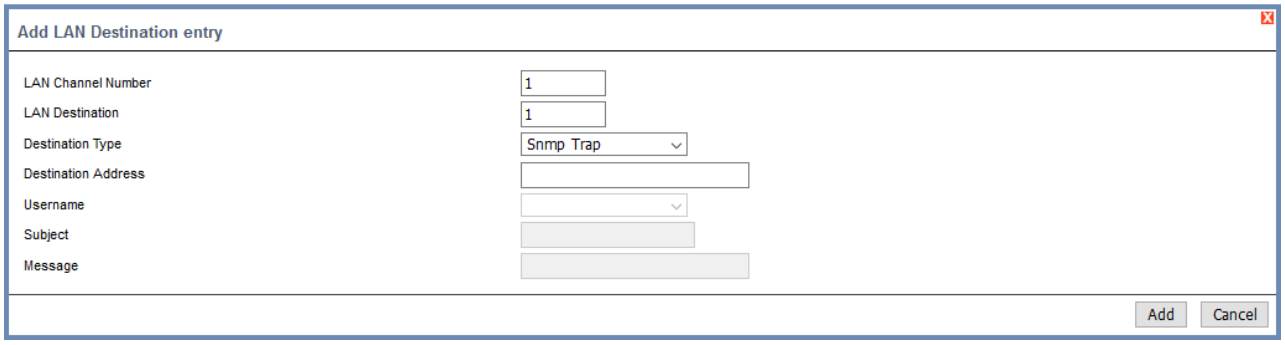



*图 35：PEF 管理：添加 LAN 目的地页面*

- **LAN Channel Number（LAN 通道编号）：** 显示所选插槽的 LAN 通道编号（只读）。
- **LAN Destination（LAN 目的地）：** 显示所选插槽的目的地编号（只读）。
- **Destination Type（目的地类型）：** 目的地类型可以是 SNMP 陷阱或电子邮件通知。如果是 SNMP 陷阱，需要填写目的地 IP 地址。如果是电子邮件通知，需要填写 3 个字段，用户名、邮件主题和正文。还要在 Configuration（配置）->SMTP 下配置 SMTP 服务器信息。
- **Destination Address（目的地地址）：** 如果目的地类型是 SNMP 陷阱，这填写接收报警的系统 IP 地址。目的地地址支持：
  - IPv4 地址格式。
  - IPv6 地址格式。
- **Username（用户名）：** 如果目的地类型是电子邮件通知，那么可选择电子邮件通知要发送到的用户。
  **注意：** 可在 Configuration（配置）->Users（用户）下配置用户电子邮件地址。
- **Subject & Message（主题和消息）：** 如果目的地类型选择电子邮件通知，这这些字段必须配置。如果发生任何严重等级的事件，就会给用户电子邮件地址发送一封电子邮件，主题由“主题”字段定义，邮件正文包含字段内容。
  **注意：** 这些字段不可用于“AMI-格式”电子邮件用户。
- **Add（添加）：** 单击“Add（添加）”保存新 LAN 目的地，并返回到 LAN 目的地列表。
- **Cancel（取消）：** 单击“Cancel（取消）”取消修改，返回到 LAN 目的地列表。

## RADIUS

如要启用或禁止 RADIUS，可以分别选中或取消 RADIUS 身份验证启用复选框。
**注意：** 仅支持常规免费 RADIUS。
RADIUS 是一套模块化、高性能、多功能 RADIUS 套件，包括服务器、客户端、开发库及许多其他 RADIUS 相关工具，打开 RADIUS 设置页面，单击菜单栏 **Configuration（配置） > RADIUS**。RADIUS 设置页面截图示例如下。

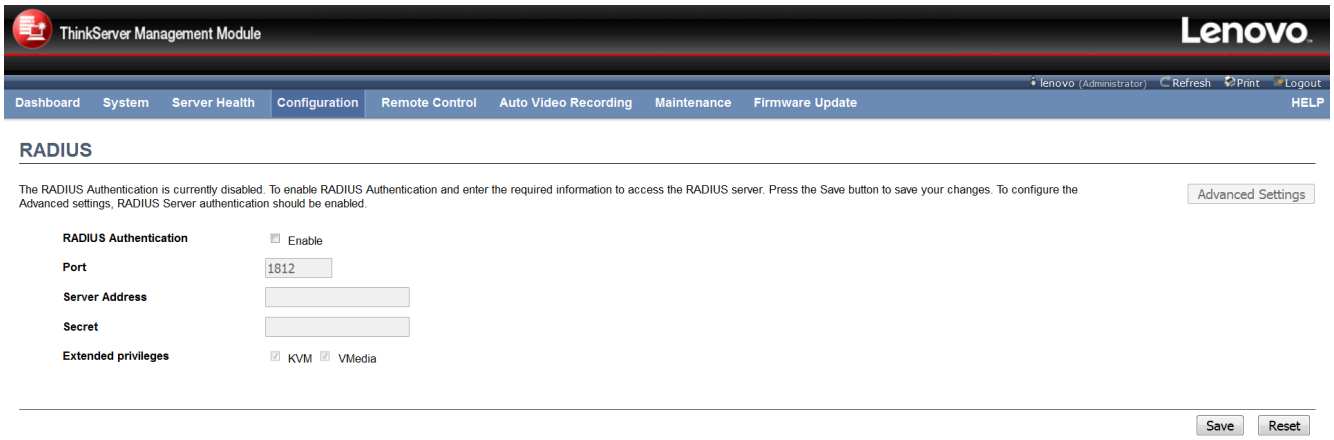



*图 36：RADIUS 设置页面*

RADIUS 设置页面字段说明如下。

- **RADIUS Authentication（RADIUS 身份验证）**：勾选“Enable（启用）”启用 RADIUS 设置。
- **Port（端口）**：指定 RADIUS 端口。
  - 默认端口 1812。
  - 端口数值范围从 1 到 65535。
- **Server Address（服务器地址）**：启用 RADIUS 服务器的“服务器地址”。服务器地址支持：
  - IP 地址（IPv4 和 IPv6 格式）。
  - FQDN（完全限定域名）格式。
- **Secret（密钥）**：输入 RADIUS 服务器的“身份验证密钥”。
  - 密钥至少必须有 4 个字符。
  - 不允许空格。

  **注意：**该字段不能超过 31 个字符。
- **Extended Privileges（扩展权限）**：该字段用于给用户分配 KVM 和 VMedia 权限。

  **注意：**如果用户权限是管理员（其他）时，KVM 和 VMedia 权限会自动启用（禁止）。
- **Advanced Settings（高级设置）**：单击“Advanced Settings（高级设置）”Radius 用户授权。
- **Save（保存）**：单击“Save（保存）”保存设置。
- **Reset（重置）**：单击 “Reset（重置）”重置修改。

## Advanced Settings（高级设置）

使用该页面配置高级 Radius 授权设置。

- 选择 **RADIUS Authentication（RADIUS 身份验证）**复选框，验证 RADIUS。
- 单击 **Advanced Settings（高级设置）**，打开如下 Radius 授权窗口。

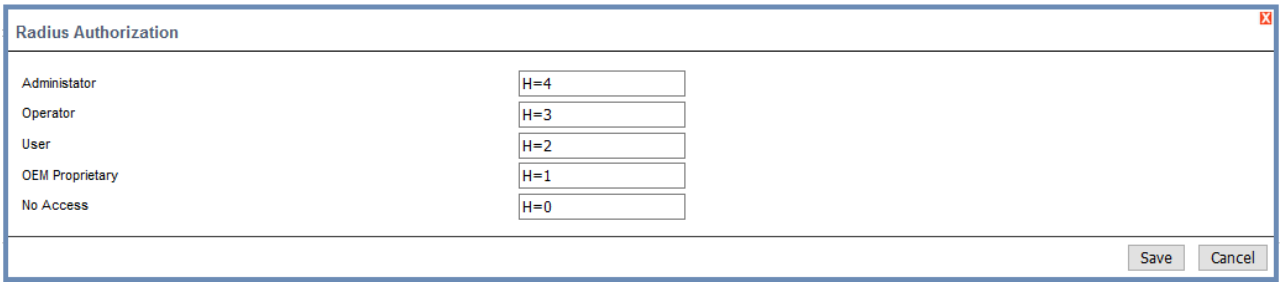



*图 37：RADIUS 授权页面*

- **Radius User Authorization（Radius 用户授权）**：因为授权原因，应在服务器端按供应商的属性配置

Radius 用户。

- **Vendor Specific Attribute in Server side（服务器端供应商属性）：** 需要在 Radius 服务器上配置 VSA。
  - 示例：1
    testadmin Auth-Type:=PAP, Cleartext- Password:='admin', Auth-Type:=PAP, Vendor- Specific='H=4'
  - 示例：2
  - testoperator Auth-Type:=PAP, Cleartext- Password:='operator', Auth-Type:=PAP, Vendor- Specific='H=3'

  如果更改供应商属性，就需要在该页面更改相同的值。
- **Administrator（管理员）：** 服务器端给管理员设置供应商属性。
- **Operator（操作员）：** 服务器端给操作员设置供应商属性。
- **User（用户）：** 服务器端给用户设置供应商属性。
- **OEM Proprietary（OEM 专用）：** 服务器端给 OEM 专用设置供应商属性。
- **No Access（无访问）：** 服务器端给无访问设置供应商属性。
  **注意：** 该字段不能超过 127 个字符。不允许“#”。
- **Save（保存）：** 单击“Save（保存）”保存设置。
- **Cancel（取消）：** 单击“Cancel（取消）”重置修改。

## Remote Session（远程会话）

该页面用于给下一重定向会话配置虚拟媒介设置。默认启用“单端口应用”。如果默认禁用“单端口应用”KVM 和媒介加密，请打开远程会话页面，从菜单栏单击 **Configuration（配置）> Remote Session（远程会话）**。远程会话页面截图示例如下。

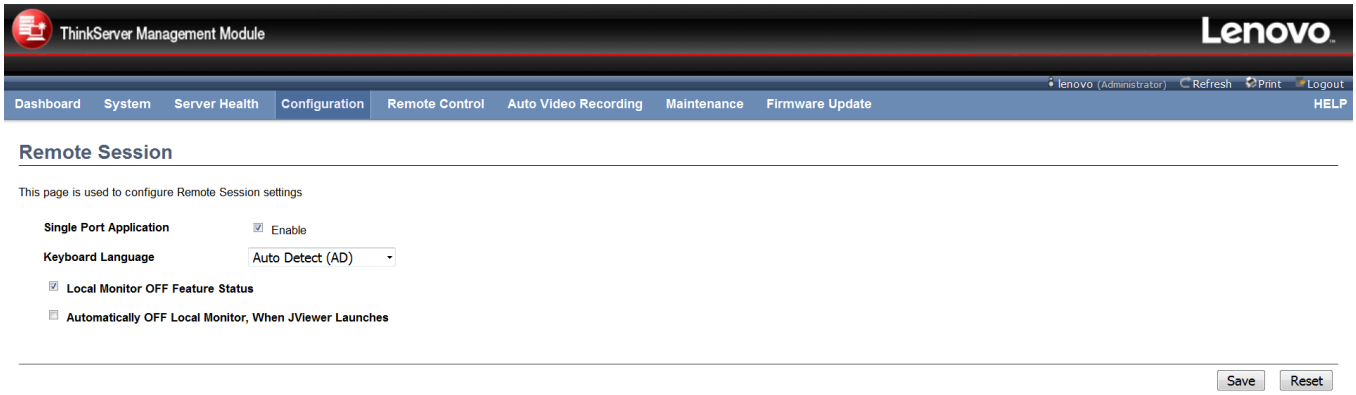



*图 38：远程会话页面*

配置远程会话页面字段说明如下。

- **Single Port Application（单端口应用）：** 选择该框，可在运行时启用单端口应用支持。
- **KVM Encryption（KVM 加密）：** 为下一重定向会话启用、禁止 KVM 数据加密。
  **注意：** 它会自动关闭现有的远程重定向，可以是 KVM 或虚拟媒介会话。
- **Keyboard Languages（键盘语言）：** 选择该框，选择键盘支持的语言。
- **Local Monitor OFF Feature Status（本地监控关闭功能状态）：** 选择该框启用本地监控开关命令。
- **Automatically OFF local Monitor, When Jviewer Launches（当 JViewer 启动时，自动关闭本地监视器）：** 选择该框，当 JViewer 启动时自动锁定本地监视器。
- **Save（保存）：** 单击“Save（保存）”保存当前变更。
- **Reset（重置）：** 单击 “Reset（重置）”重置修改。

## Services（服务）

该页面显示 BMC 运行服务的基本信息。如要修改服务，用户必须是管理员（或 OEM 专用）。打开服务页面，从菜单栏单击 **Configuration（配置）> Services（服务）**。服务截图示例如下。

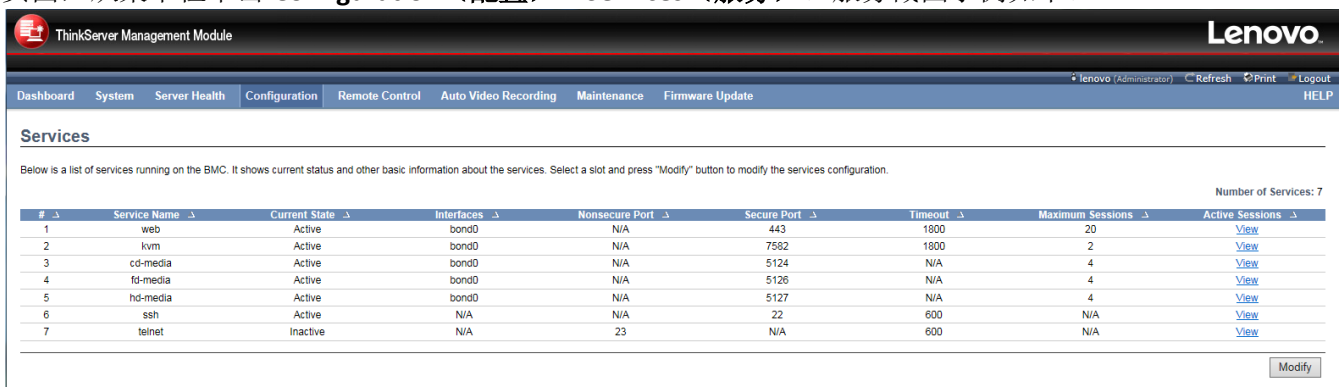



*图 39：服务页面*

服务页面字段说明如下。

- **Service Name（服务名称）**：显示所选插槽的服务名称（只读）。
- **Current State（当前状态）**：显示服务的当前状态，活动还是停止。
- **Interfaces（接口）**：显示服务运行的接口。
- **Nonsecure Port（不安全的端口）**：该端口用于配置不安全的服务端口号。
- **Secure Port（安全端口）**：用于配置安全的服务端口号。
- **Timeout（超时）**：显示服务的会话超时数值。对于网页、SSH 和 telnet 服务，用户可以配置会话超时数值。
- **Maximum Sessions（最大会话数）**：显示服务允许的最大会话数。
- **Active Sessions（活动会话）**：查看服务的当前活动会话。
- **Modify（修改）**：选择一个插槽，单击“Modify（修改）”修改服务配置。还可双击插槽。
  **注意：**一旦配置有修改，服务器就会自动重启。只有当用户关闭已打开的会话，才可变更。

### Active Sessions（活动会话）：

该页面显示 BMC 中各种服务的活动会话的基本信息。如要终止会话，用户必须是管理员（或 OEM 专用）。

- 单击 **View（查看）**查看服务活动会话的详细信息。
- 打开 **Active Session（活动会话）**屏幕（例如：网页服务屏幕），截图如下所示。

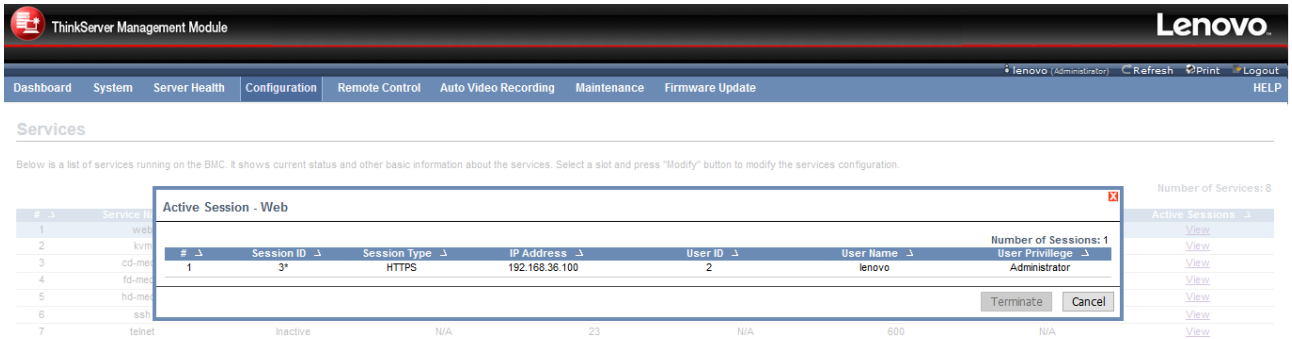



*图 40：活动会话页面*

- **#:** 序列号。
- **Session ID（会话 ID）：** 显示活动会话的 ID 号。
- **Session Type（会话类型）：** 显示活动会话的类型。
- **IP Address（IP 地址）：** 显示活动会话已配置的 IP 地址。
- **User ID（用户 ID）：** 显示用户的 ID 号。
- **User Name（用户名）：** 显示用户名称。
- **User Privilege（用户权限）：** 显示用户的访问权限。
- **Terminate（终止）：** 选择一个插槽，单击“Terminate（终止）”某个服务配置。
- **Cancel（取消）：** 单击“Cancel（取消）”取消修改，返回服务列表。

  **注意：** 各个 PAM 模块用户的默认用户 ID 是，
  - 活动目录用户是 30
  - LDAP/E-Directory 用户是 20
  - RADIUS 用户是 40

**Modify Service（修改服务）：**

使用该表单修改 BMC 中运行的服务的配置。

- 选择一个插槽，单击 **Modify（修改）**修改服务配置。还可双击插槽。
- 打开 **Modify Service（修改服务）**屏幕，截图如下所示。

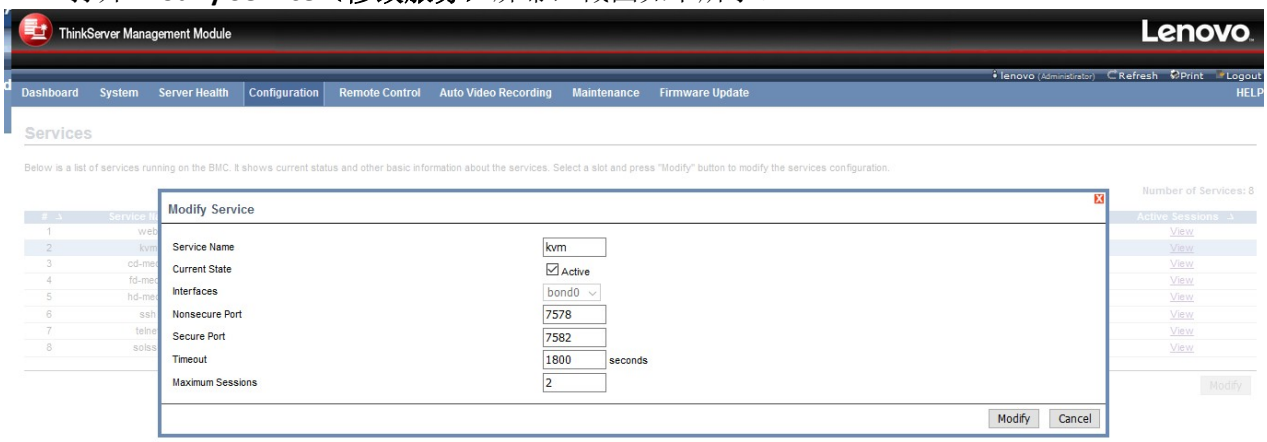



*图 41：修改服务页面*

- **Service Name（服务名称）：** 显示所选插槽的服务名称（只读）。
- **Current State（当前状态）：** 显示服务的当前状态，活动还是停止。选择该框启动停止的服务。
- **Interface（接口）：** 显示服务运行的接口。用户可选择任一可用的接口。

  **注意：**
  - 无法将服务映射到禁止的接口。接口状态可以在 Configuration（配置） -> Network（网络） -> LAN Settings（LAN 设置）下选中或启用。
  - 当启用单端口时，KVM 和媒介接口都是只读。
- **Nonsecure Port（不安全的端口）：** 该端口用于配置不安全的服务端口号。
  - Telnet 默认端口 23。
  - 端口数值范围从 1 到 65535。

  **注意：** 网页/KVM/CD/FD/HD/SSH 服务不支持不安全的端口。
- **Secure Port（安全端口）：** 用于配置安全的服务端口号。
  - 网页默认端口 443。
  - KVM 默认端口 7582。

- CD 媒介默认端口 5124。
- FD 媒介默认端口 5126。
- HD 媒介默认端口 5127。
- SSH 默认端口 22。
- 端口数值范围从 1 到 65535。

**注意：**Telnet 服务不支持安全端口。

- **Timeout（超时）：**显示服务的会话超时数值。对于网页、SSH 和 telnet 服务，用户可以配置会话超时数值。
  - 网页和 KVM 超时数值范围从 300 到 1800 秒。
  - 如果存在任何活动 KVM 会话，就会忽略网页超时。
  - SSH 和 Telnet 超时数值范围从 60 到 1800 秒。
  - SSH 和 Telnet 超时数值是 60 的倍数。

  **注意：**SSH 和 Telnet 服务使用相同的超时数值。如果用户配置 SSH 超时数值，就会同时应用于 telnet 服务，反之亦然。
- **Maximum Sessions（最大会话数）：**显示服务允许的最大会话数。
- **Active Sessions（活动会话）：**查看服务的当前活动会话数。
- **Modify（修改）：**单击“Modify（修改）”保存服务的配置，并返回到服务列表。

  **注意：**会影响已经打开的服务会话，服务会重启。
- **Cancel（取消）：**单击“Cancel（取消）”取消修改，返回服务列表。

## Interfaces（接口）

使用该页面配置接口设置。接口设置页面截图示例如下。

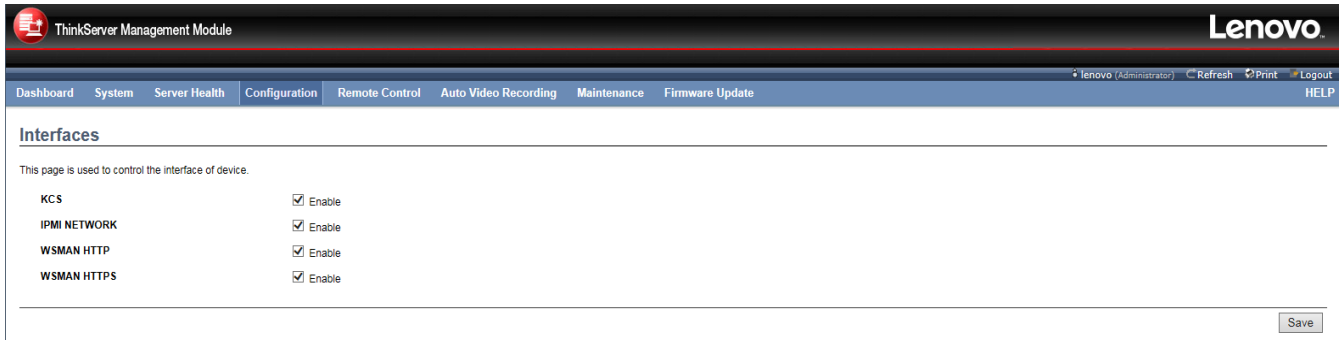



*图 42：接口页面*

接口设置字段说明如下。

- **KCS：**勾选“Enable（启用）”启用 KCS。
- **IPMI NETWORK（IPMI 网络）：**勾选“Enable（启用）”启用 IPMI 网络。

  **注意：**如果启用该选项，设备会自动设置防火墙，意味着可以在“系统防火墙”页面找到 IPMI 网络设置的端口。
- **WSMAN HTTP：**勾选“Enable（启用）”启用 WSMAN HTTP。

  **注意：**如果启用该选项，设备会自动设置防火墙，意味着可以在“系统防火墙”页面找到 WSMAN HTTP 设置的端口。
- **WSMAN HTTPS：**勾选“Enable（启用）”启用 WSMAN HTTPS。

  **注意：**如果启用该选项，设备会自动设置防火墙，意味着可以在“系统防火墙”页面找到 WSMAN HTTP 设置的端口。
- **Save（保存）：**单击“Save（保存）”保存所做的更改。

## SMTP

该页面用于配置 SMTP 设置。

**Simple Mail Transfer Protocol (SMTP)（简单邮件传输协议（SMTP））**是电子邮件在 Internet 协议（IP）网络上传输的 Internet 标准。

如要打开 SMTP 设置页面，从菜单栏单击 **Configuration（配置）> SMTP**。

SMTP 设置页面截图示例如下。

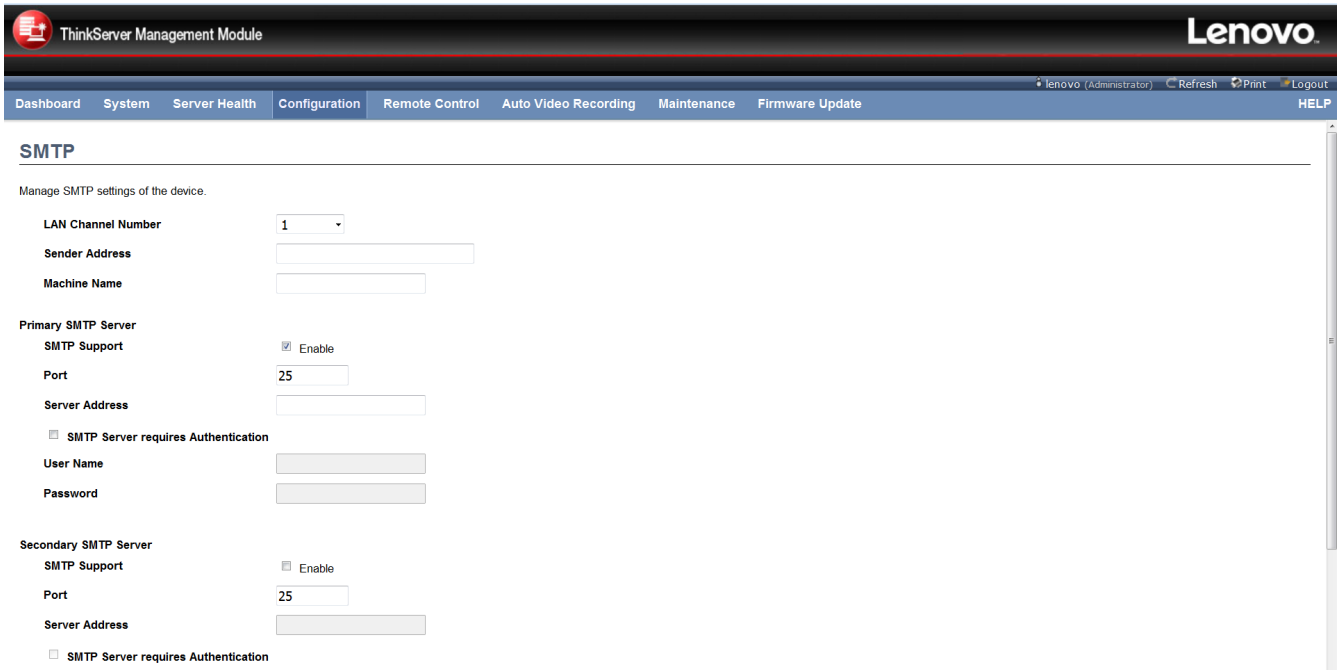



*图 43：SMTP 页面*

SMTP 设置字段说明如下。

- **LAN Channel Number（LAN 通道编号）：** 请选择要配置 SMTP 信息的 LAN 通道。
- **Sender Address（发件人地址）：** 在 SMTP 服务器上输入有效的“发件人地址”。
- **Machine Name（机器名称）：** 输入 SMTP 服务器的“机器名称”。
  - 机器名称是一串 15 个数字字母长的字符串。
  - 不允许空格、特殊字符。
- **Primary SMTP Server（主 SMTP 服务器）：** 列举主 SMTP 服务器配置。
- **SMTP Support（SMTP 支持）：** 勾选启用 BMC SMTP 支持。
- **Port（端口）：** 指定 SMTP 端口。
  - 默认端口 25。
  - 端口数值范围从 1 到 65535。
- **Server Address（服务器地址）：** 输入 SMTP 服务器的“IP 地址”。必填字段。
  - IP 地址 4 组数字组成，由点分隔，如“xxx.xxx.xxx.xxx”。
  - 每一数字范围从 0 到 255。
  - 第一个数字不能为 0。

  服务器地址支持：
  - IPv4 地址格式。
  - IPv6 地址格式。

- **SMTP Server requires Authentication（SMTP 服务器需要身份验证）：** 勾选“Enable（启用）”启用 SMTP 设置。
  **注意：**SMTP 服务器支持的身份验证类型有：
  - CRAM-MD5
  - 登录
  - PLAIN

  如果 SMTP 服务器不支持以上任何一种身份验证类型，用户收到错误消息，显示*“身份验证类型不受 SMTP 服务器支持。”*
- **Username（用户名）：** 输入访问 SMTP 账户的用户名。
  - 用户名可以是 4 到 64 个数字字符、点（.）、破折号（-）和下划线（_）。
  - 第一个必须是字母。
  - 不允许使用特殊字符。
- **Password（密码）：** 输入 SMTP 用户帐户的密码。
  - 密码至少必须有 4 个字符长。
  - 不允许空格。

  **注意：**该字段不能超过 64 个字符。
- **Secondary SMTP Server（次 SMTP 服务器）：** 列举次 SMTP 服务器配置。可选字段。
  如果主 SMTP 服务器不工作，那么会尝试次 SMTP 服务器。
- **Save（保存）：** 单击“Save（保存）”保存新的 SMTP 服务器配置。
- **Reset（重置）：** 单击 “Reset（重置）”重置修改。

## SNMP

使用该页面配置 SNMP 设置。

**Simple Network Management Protocol (SNMP)（简单网络管理协议（SNMP））**是 Internet 标准协议，用于收集、组织和修改 IP 网络管理信息，并更改设备行为。

如要打开 SNMP 设置页面，从菜单栏单击 **Configuration（配置）> SNMP**。SNMP 设置页面截图示例如下。

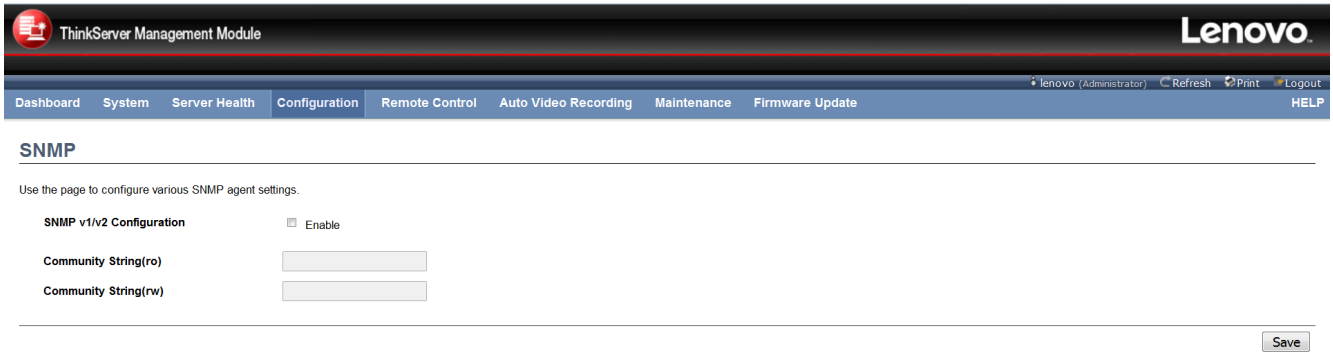



*图 44：SNMP 页面*

SNMP 设置字段说明如下。

- **SNMP：** 勾选“Enable（启用）”启用 SNMP。
- **SNMP v1/v2 Configuration（SNMP v1/v2 配置）：** 勾选“Enable（启用）”启用 SNMPv1 和 SNMPv2c 功能。
- **Community String（社区字符串）：** 社区字符串在 SNMPv1 和 SNMPv2c 两者一致。可选字段。
- **Save（保存）：** 单击“Save（保存）”保存 SNMP 配置。

## SSL

**Secure Socket Layer（安全套接字层）**协议由 Netscape 创造，用于确保网页服务器和浏览器之间安全传输。协议使用第三方认证授权（CA）标识交易的一方或双方。
如要打开 SSL 证书设置页面，从菜单栏单击 **Configuration（配置）> SSL**。该页面共有 3 个选项卡。
**注意：**该页面介绍生成 SSL 证书的简单方法，它并不是受信任的认证授权，如果需要，可以自己上传一个受信任的证书。

- **Upload SSL（上传 SSL）**可用于向 BMC 上传证书和私钥文件。
- **Generate SSL（生成 SSL）**可用于根据配置详细信息生成 SSL 证书。
- **View SSL（查看 SSL）**可按可读格式查看上传的 SSL 证书。

### Upload SSL Tab（上传 SSL 选项卡）

该页面用于上传新 SSL 证书和私钥。
**注意：**在上传 SSL 证书时，请在“Configuration（配置）”菜单检查 NTP 上当前 BMC 时间。
SSL 证书配置：上传 SSL 截图示例页面如下。

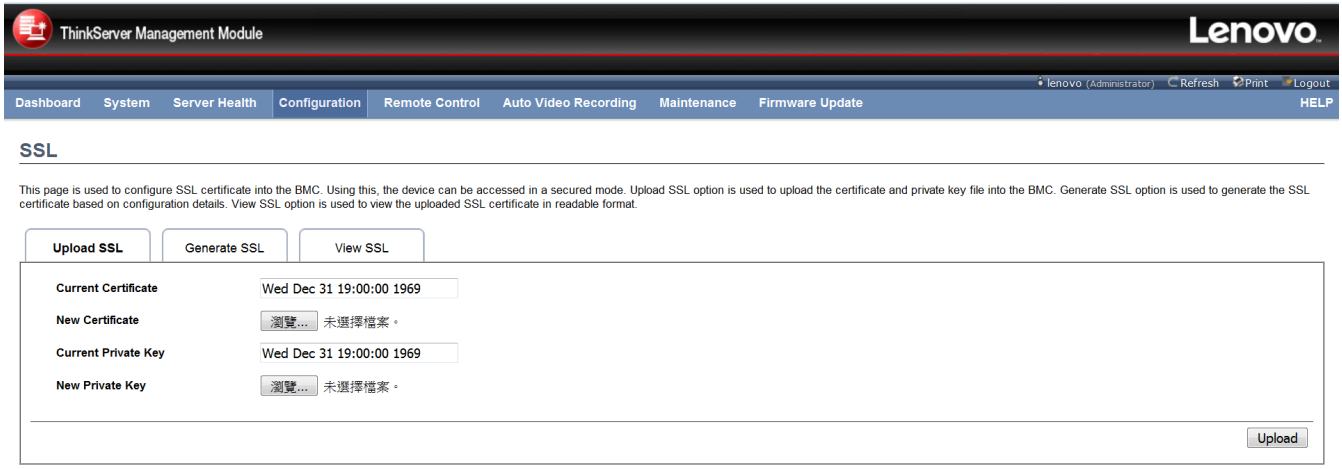



*图 45：SSL 证书配置：上传 SSL 页面*

SSL 证书配置：上传 SSL 选项卡字段说明如下。

- **Current Certificate（当前证书）：**显示当前证书信息和上传的日期时间（只读）。
- **New Certificate（新证书）：**浏览导航到证书文件。
  - 证书文件应为 PEM 类型
- **Current Privacy Key（当前私钥）：**显示当前私钥信息和上传的日期时间（只读）。
- **New Privacy Key（新私钥）：**浏览导航到私钥文件。
  - 私钥文件应是 PEM 类型
- **Upload（上传）：**单击“upload（上传）”向 BMC 上传 SSL 证书和私钥。
  **注意：**成功上传后，HTTPS 服务会重启，使用新上传的 SSL 证书。

### Generate SSL Tab（生成 SSL 选项卡）

该选项卡用于根据配置生成 SSL 证书。
SSL 证书配置：生成 SSL 截图示例页面如下。

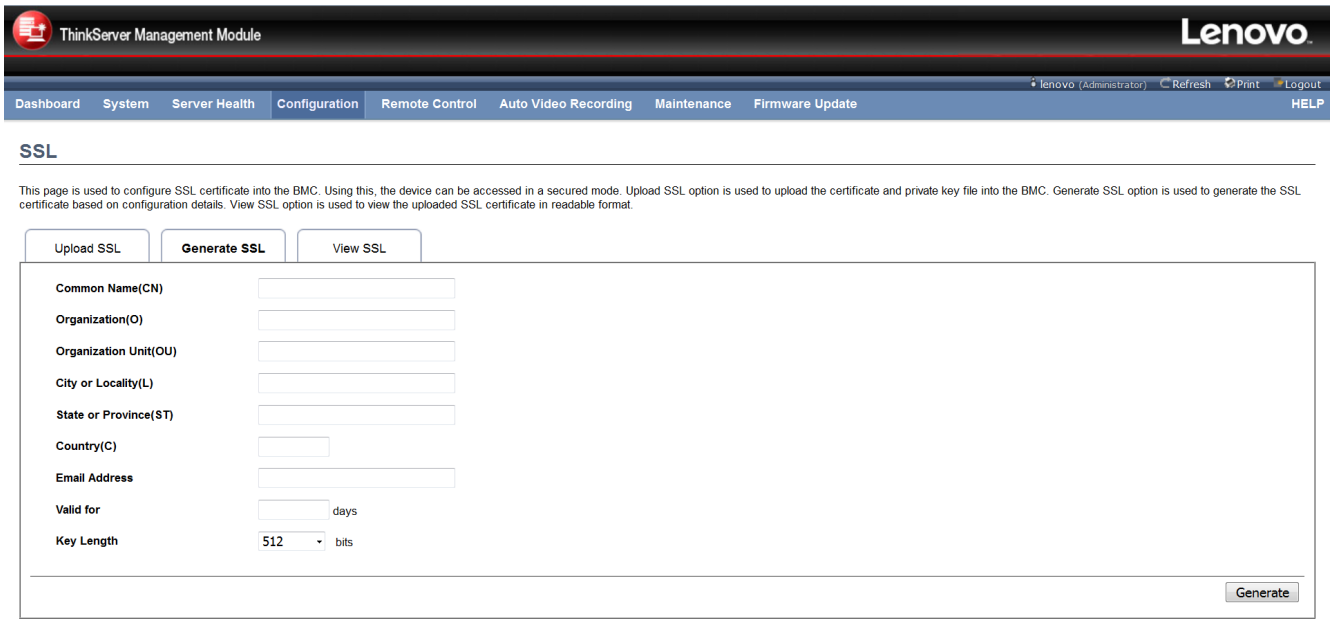



*图 46：SSL 证书配置：生成 SSL 页面*

SSL 证书配置：生成 SSL 选项卡字段说明如下。

- **Common Name(CN)（通用名称（CN））：**生成证书所用的通用名称。
  - 最长 64 个字符。
  - 是一串数字字符。
  - 不允许使用特殊字符“#”和“$”。
- **Organization(O)（组织（O））：**生成证书所用的组织名称。
  - 最长 64 个字符。
  - 是一串数字字符。
  - 不允许使用特殊字符“#”和“$”。
- **Organization Unit(OU)（组织单位（OU））：**生成证书所用的所有组织单元名称。
  - 最长 64 个字符。
  - 是一串数字字符。
  - 不允许使用特殊字符“#”和“$”。
- **City or Locality(L)（城市或地方（L））：**确定城市或地方。
  - 最长 64 个字符。
  - 是一串数字字符。
  - 不允许使用特殊字符“#”和“$”。
- **State or Province(ST)（州或省（ST））：**确定州或省。
  - 最长 64 个字符。
  - 是一串数字字符。
  - 不允许使用特殊字符“#”和“$”。
- **Country(C)（国家（C））：**确定国家代码。
  - 仅允许两个字符。
  - 不允许使用特殊字符。
- **Email Address（电子邮件地址）：**确定组织的电子邮件地址。
- **Valid for（有效期）：**证书有效的天数。
  - 值范围为 1 到 3650。

- **Key Length（密钥长度）：** 选择证书的密钥长度位值。
- **Generate（生成）：** 单击生成新的 SSL 证书。

  **注意：**
  - 成功上传后，HTTPS 服务会重启，使用新上传的 SSL 证书。
  - HTTPS 会话在某些 512 位 RSA 密钥的浏览器中无法工作，请访问浏览器官方网站了解详细信息。

### View SSL Tab（查看 SSL 选项卡）

该选项卡可按用户可读格式查看上传的 SSL 证书。

SSL 证书配置：查看 SSL 截图示例页面如下。

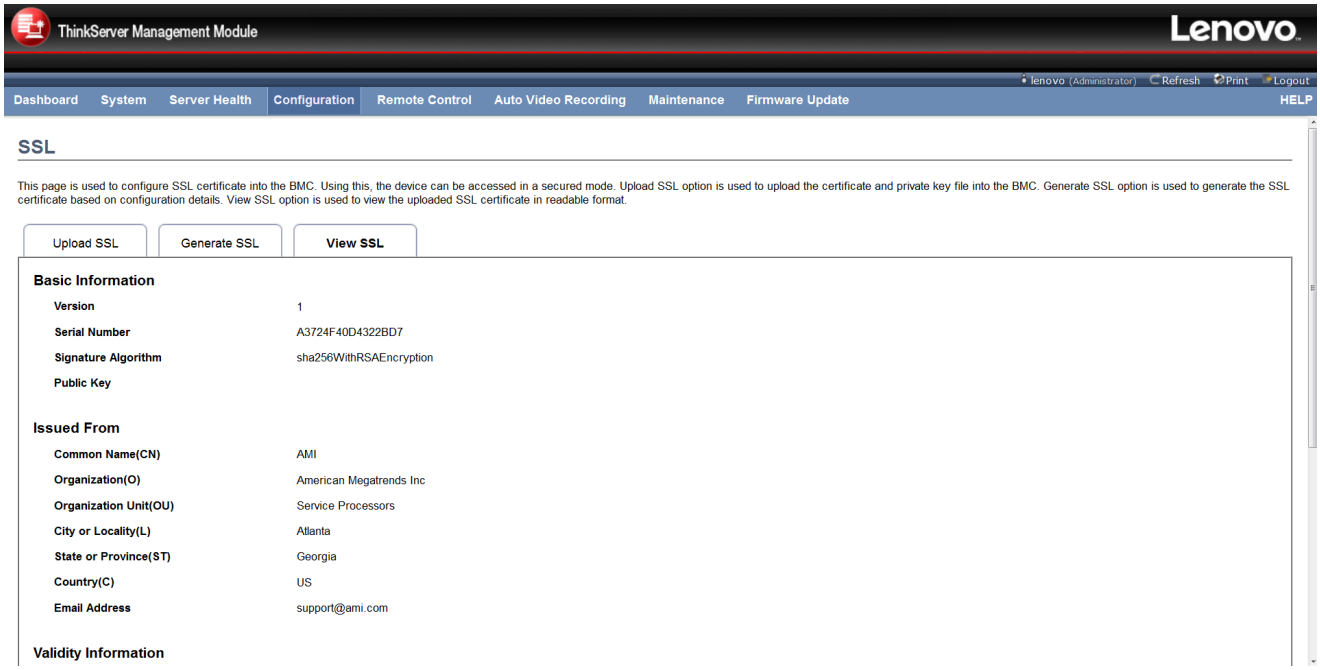



*图 47：证书配置：查看 SSL 页面*

SSL 证书配置：查看 SSL 选项卡字段说明如下。

- **Basic Information（基本信息）：** 显示上传的 SSL 证书的基本信息。显示下列字段。
  - 版本
  - 序列号
  - 签名算法
  - 公钥
- **Issued From（发行单位）：** 包含证书发行方的信息。
  - Common Name(CN)（通用名称（CN））
  - Organization(O)（组织（O））
  - Organization Unit(OU)（组织单位（OU））
  - City or Locality(L)（城市或地方（L））
  - State or Province(ST)（州或省（ST））
  - Country(C)（国家（C））
  - Email Address（电子邮件地址）
- **Validity Information（有效期信息）：** 显示上传的证书的有效期。
  - Valid From（有效期开始）
  - Valid To（有效期结束）

- **Issued To（发行给）：** 显示证书接收方的信息。
  - Common Name(CN)（通用名称（CN））
  - Organization(O)（组织（O））
  - Organization Unit(OU)（组织单位（OU））
  - City or Locality(L)（城市或地方（L））
  - State or Province(ST)（州或省（ST））
  - Country(C)（国家（C））
  - Email Address（电子邮件地址）

## System Firewall（系统防火墙）

该页面用于配置系统防火墙支持。要查看该页面，必须至少具有操作员权限。
如要添加或删除防火墙，用户必须是管理员（或 OEM 专用）。
防火墙规则可以用一个 IP 地址或一段 IP 地址，或端口号。打开系统防火墙页面，从菜单栏单击 **Configuration（配置）> System Firewall（系统防火墙）**。

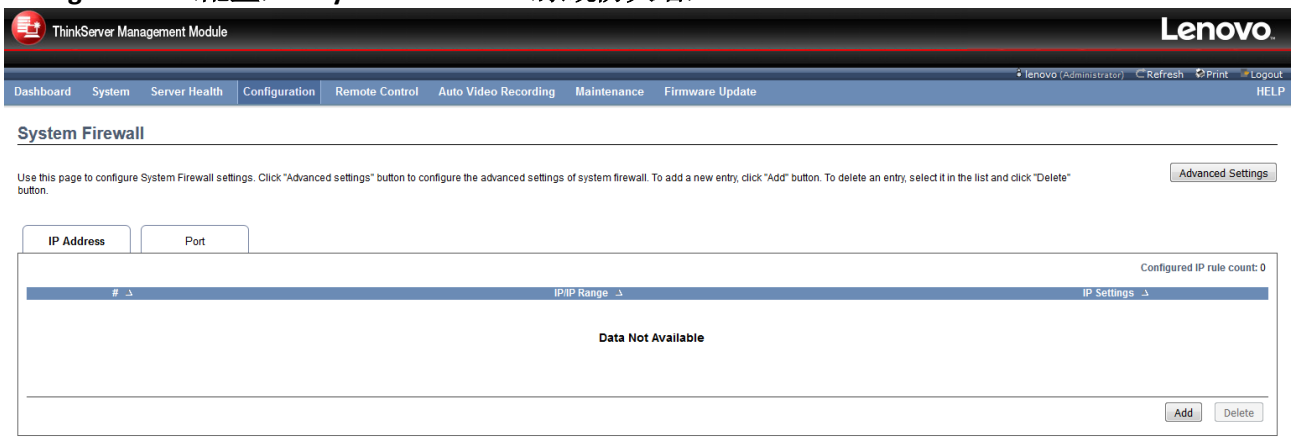



*图 48：系统防火墙页面*

- **Advanced Settings（高级设置）：** 单击该选项配置高级防火墙设置。可以选择阻止全部或清除全部。
- **#：** 序列号。
- **IP/IP Address Range（IP/IP 地址范围）：** 该字段用于显示已配置的 IP 地址或访问。
- **IP Settings（IP 设置）：** 该列说明所列 IP 地址或 IP 地址段的当前规则设置（允许或阻止）。
- **Add（添加）：** 单击“Add（添加）”添加新规则到防火墙规则列表。
- **Delete（删除）：** 选择要删除的插槽，然后单击“Delete（删除）”。

### Advanced Settings（高级设置）

该表单用于配置高级系统防火墙设置。

- 单击 **Advanced Settings（高级设置）**按钮。打开如下高级防火墙设置窗口。

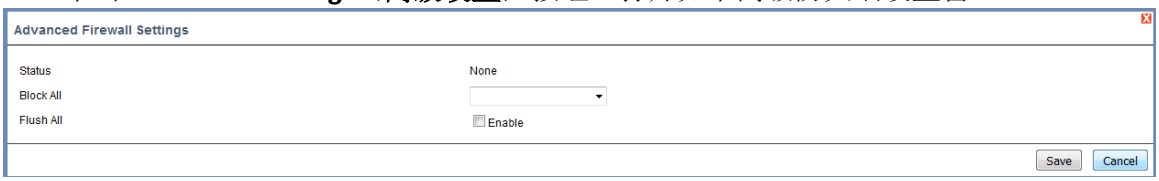



*图 49：高级防火墙页面*

- **Block All（阻止全部）：** 可阻止所有入站 IP 和端口。
- **Flush All（清除全部）：** 用于清除所有系统防火墙规则。
- **Save（保存）：** 单击“Save（保存）”保存配置好的规则。
- **Cancel（取消）：** 单击“Cancel（取消）”取消对现有设置的修改。

**Set system firewall for an IP or a range of IP Addresses（为 IP 或 IP 地址段设置系统防火墙）：**
该表单用于添加新的 IP 地址或 IP 地址段规则设置。
如下单击“Add（添加）”按钮。

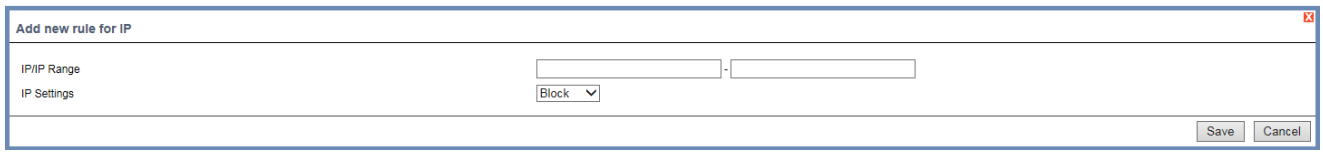



*图 50：添加新 IP 地址段规则。*

- **IP/IP Range（IP/IP 地址段）：** 该字段用于显示配置 IP 地址或 IP 地址段。
  IP 地址支持 IPv4 和 IPv6 地址格式：
  - IPv4 地址由 4 组数字组成，由点分隔，如“xxx.xxx.xxx.xxx”。
  - 每一数字范围从 0 到 255。
  - 第一个数字不能为 0。
  - IPv6 地址有 8 组 4 位十六进制数字组成，冒号分隔，如 xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx。
  - 十六进制数字使用小写字母。
- **IP Settings（IP 设置）：** IP 地址用于确定规则，是否阻止或允许配置的 IP 或 IP 范围。
- **Save（保存）：** 单击“Save（保存）”保存配置好的规则
- **Cancel（取消）：** 单击“Cancel（取消）”取消对现有设置的修改。

**To set system firewall for a single port or range of Port numbers（设置单端口或端口段系统防火墙）：**
该页面用于配置系统防火墙支持。如要查看该页，用于必须是操作员。
要添加或删除防火墙，用户必须是管理员（或 OEM 专用）。
单击 Port（端口） 选项卡。端口选项卡截图示例如下。

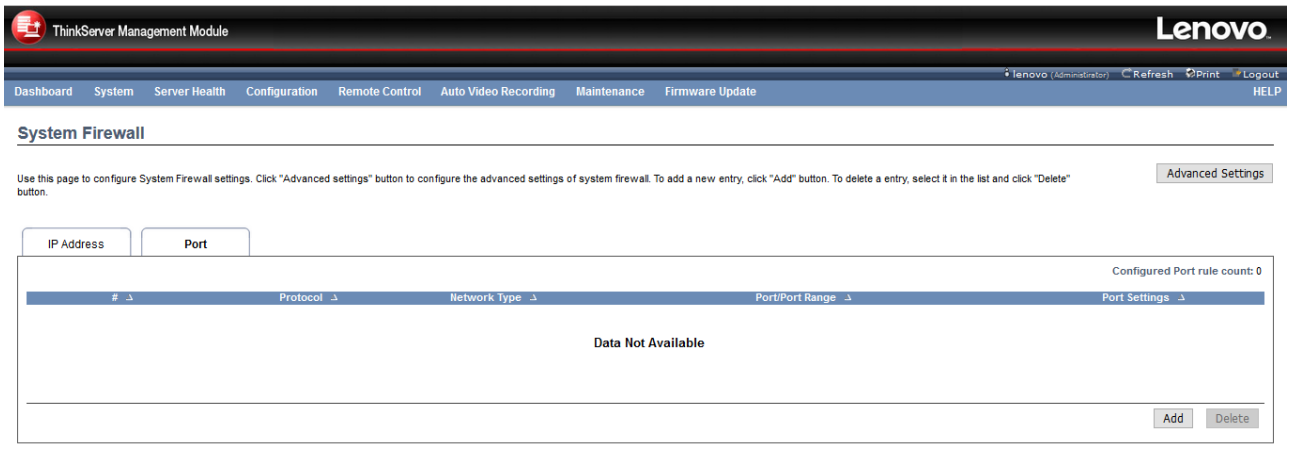



*图 51：系统防火墙页面*

系统防火墙：**Port（端口）**选项卡字段解释如下。

- **Advanced Settings（高级设置）：**单击该选项配置高级防火墙设置。可以选择阻止全部或清除全部。
- **#：**序列号。
- **Protocol（协议）：**该字段指定端口或端口段影响的协议。
- **Network Type（网络类型）：**该字段指定端口或端口段影响的网络类型。
- **Port/Port Range（端口/端口段）：**该字段用于显示已配置的端口或端口段。
- **Port Settings（端口设置）**: 该列说明所列端口或端口段的当前规则设置（允许或阻止）。
- **Add（添加）：**单击“Add（添加）”添加新规则到防火墙规则列表。
- **Delete（删除）：**选择要删除的插槽，然后单击“Delete（删除）”。

**Add New Rule for Port（添加新端口规则）：**

该表单用于添加新的端口或端口段规则设置。

如下单击“Add（添加）”按钮。

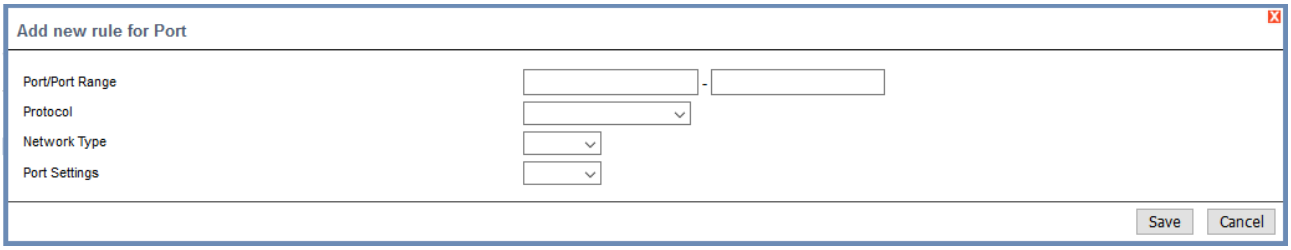



*图 52：添加新的端口段规则页面*

- **Port/Port Range（端口/端口段）：**该字段用于配置端口或端口段址段。
  - 端口数值范围从 1 到 65535。
- **Protocol（协议）：**该字段用于选择协议。可能是 TCP、UDP 或两者。
- **Network Type（网络类型）：**该字段用于选择网络类型。可能是 IPv4、IPv6 或两者。
- **Port Settings（端口设置）:** 端口设置用于确定规则，是否阻止或允许配置的端口或端口范围。
- **Save（保存）：**单击“Save（保存）”保存配置好的规则。
- **Cancel（取消）：**单击“Cancel（取消）”取消对现有设置的修改。

## Users（用户）

所列表格显示全部已配置的用户和可用的插槽。可以在此修改或添加新用户。

最多提供 10 个插槽，包括管理员默认插槽。要查看该页面，必须具有操作员权限。如要修改或添加用户，必须具有管理员权限。

**注意：**空闲插槽在所有列中用“~”表示。

打开用户管理页面，从菜单栏单击 **Configuration（配置） > Users（用户）**。用户管理截图示例如下。

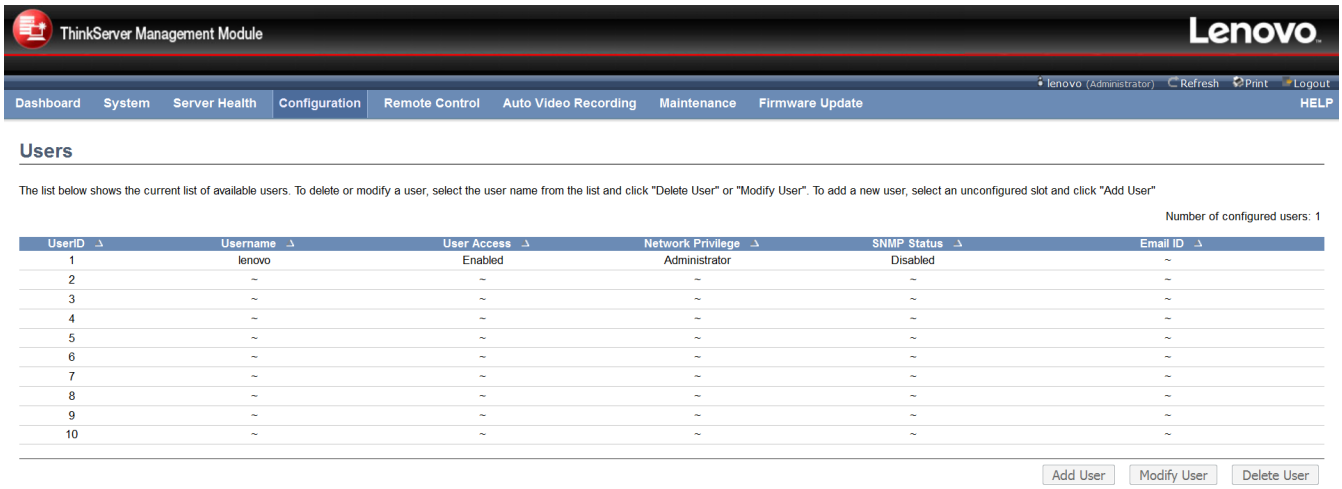



*图 53：用户管理页面*

用户管理页面字段说明如下。

- **Add User（添加用户）：**选择空闲插槽，单击“Add User（添加用户）”给设备添加新用户。还可双击空闲插槽添加用户。
- **Modify User（修改用户）：**选择已配置的插槽，单击“Modify User（修改用户）”修改所选条目。还可双击配置的插槽。
- **Delete User（删除用户）：**选择要删除的用户，然后单击“Delete User（删除用户）”。

**Add a new user（添加新用户）：**

使用该表单添加新用户。

- 如要添加新用户，选择空闲插槽，然后单击 **Add User（添加用户）**或双击空闲的插槽。打开 Add User（添加用户）画面，截图如下所示。

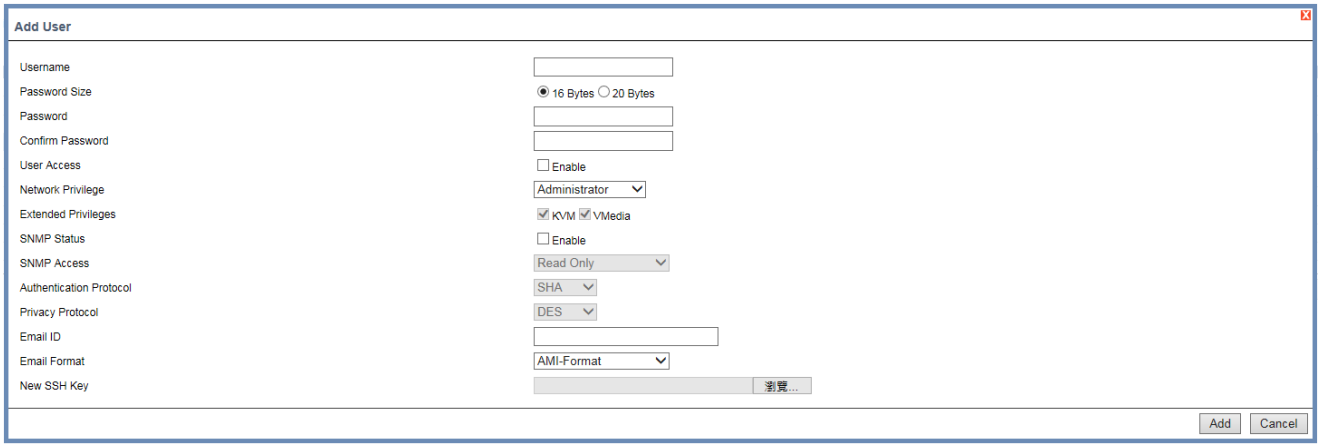



*图 54：添加新用户页面*

- **User Name（用户名）：**输入新用户的用户名。
  - 用户名是一串 1-16 数字字符。
  - 第一个必须是字母字符。
  - 并区分大小写。
  - 允许特殊字符“-”（连字符）和“_”（下划线）、“@”（at 符号）。

- **Password Size（密码长度）：**可选择 16 字节或 20 字节长度密码。默认是 16 字节。
  如果选择了“16 字节”，密码最大长度是 16 个字符。如果选择了“20 字节”，密码最大长度是 20 个字符。
  **注意：**对于 20 字节密码，无法创建 Ian 会话。
- **Password, Confirm Password（密码，确认密码）：**在此输入和确认密码。
  - 密码至少必须有 1 个字符。
  - 不允许空格。

  **注意：**该字段不能超过 16/20 个字符（具体视密码长度字段值）。
- **User Access（用户访问）：**选择用户访问复选框会内部分配 IPMI 消息权限给用户。
  **注意：**建议通过 IPMI 创建用户时，启用用户 IPMI 消息权限，启用 **User Access（用户访问）**选项。
- **Network Privilege（网络权限）：**选择要分配给用户的网络权限等级。共有 5 个等级。管理员、操作员、用户、OEM 专用和无访问。
- **Extended Privileges（扩展权限）：**该字段用于显示分配给用户的 KVM 和 VMedia 权限。
  **注意：**如果用户网络权限是管理员（其他）时，KVM 和 VMedia 权限会自动启用（禁止）。
- **SNMP Status（SNMP 状态）：**选择复选框，给用户启用 SNMP 访问。
  **注意 1：**请在“SNMP”页面启用 SNMP。
  **注意 2：**当 SNMP 状态启用后，密码字段是必填，至少 8 个字符长。
  对于“匿名”用户，这禁止 SNMP 访问，用户名和密码长度为空。
- **SNMP Access（SNMP 访问）：**选择用户的 SNMP 访问等级。可以是只读或读写。
- **Authentication Protocol（身份验证协议）：**选择 SNMP 设置身份验证协议。
  **注意：**如果更改了身份验证协议，密码字段为必填。
- **Privacy protocol（隐私协议）：**选择 SNMP 设置的加密算法。
- **Email ID（电子邮件 ID）：**输入用户的电子邮件 ID。如果用户忘记密码，新密码会发送到配置的电子邮件 ID。
  **注意：**必须配置 SMTP 服务器才可发送电子邮件。
- **Email Format（电子邮件格式）：**指定电子邮件的格式。发送电子邮件时会使用该格式。共有两种格式：
  - AMI 格式：该电子邮件格式下的主题是“Alert from (your Hostname)（（来自主机的）通知）”。电子邮件内容显示传感器信息，如：传感器类型和说明。
  - 固定主题格式：该格式根据用户设置显示消息。必须设置电子邮件通知的主题和消息。
- **New SSH Key（新 SSH 密钥）：**使用“Browse（浏览）”按钮导航到 SSH 公钥文件。
  - SSH 密钥文件应是公钥类型。
- **Add（添加）：**单击“Add（添加）”保存新用户，并返回到用户列表。
- **Cancel（取消）：**单击“Cancel（取消）”取消修改，并返回到用户列表。

### Modify an existing User(修改现有用户)

使用该表单修改现有用户密码和权限。

- 从列表选择一位现有用户，然后单击 **Modify User（修改用户）**或双击已配置的插槽。打开 Modify User（修改用户）画面，截图如下所示。

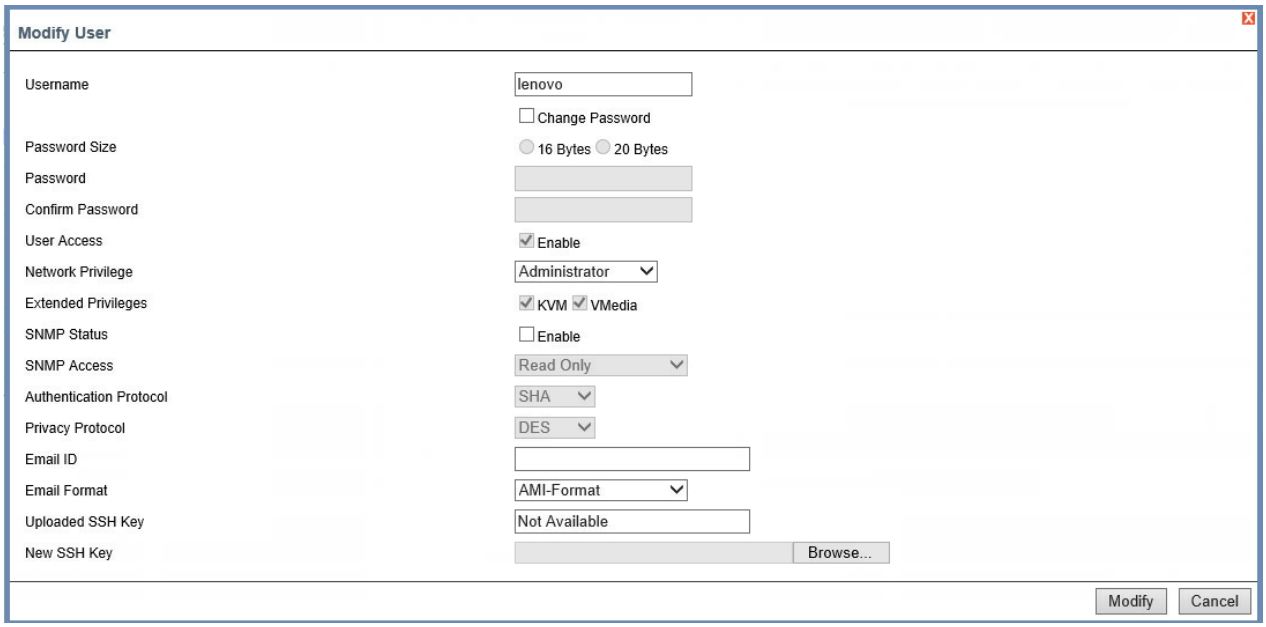



*图 55：修改用户页面*

- **User Name（用户名）：**修改现有用户。
  - 用户名是一串 1-16 数字字符。
  - 第一个必须是字母字符。
  - 并区分大小写。
  - 允许特殊字符“-”（连字符）和“_”（下划线）、“@”（at 符号）。
- **Password Size（密码长度）：**可选择 16 字节或 20 字节长度密码。默认是 16 字节。
  如果选择了“16 字节”，密码最大长度是 16 个字符。如果选择了“20 字节”，密码最大长度是 20 个字符。
  **注意：**对于 20 字节密码，无法创建 lan 会话。
- **Password, Confirm Password（密码，确认密码）：**在此输入和确认密码。
  - 密码至少必须有 1 个字符。
  - 不允许空格。
  **注意：**该字段不能超过 16/20 个字符（具体视密码长度字段值）。
- **User Access（用户访问）：**选择用户访问复选框会内部分配 IPMI 消息权限给用户。
  **注意：**建议通过 IPMI 创建用户时，启用用户 IPMI 消息权限，启用 **User Access（用户访问）**选项。
- **Network Privilege（网络权限）：**选择要分配给用户的网络权限等级。共有 5 个等级。管理员、操作员、用户、OEM 专用和无访问。
- **Extended Privileges（扩展权限）：**该字段用于显示分配给用户的 KVM 和 VMedia 权限。
  **注意：**如果用户网络权限是管理员（其他）时，KVM 和 VMedia 权限会自动启用（禁止）。
- **SNMP Status（SNMP 状态）：**选择复选框，给用户启用 SNMP 访问。
  **注意 1：**请在“SNMP”页面启用 SNMP。
  **注意 2：**当 SNMP 状态启用后，密码字段是必填，至少 8 个字符长。
  对于“匿名”用户，这禁止 SNMP 访问，用户名和密码长度为空。
- **SNMP Access（SNMP 访问）：**选择用户的 SNMP 访问等级。可以是只读或读写。
- **Authentication Protocol（身份验证协议）：**选择 SNMP 设置身份验证协议。
  **注意：**如果更改了身份验证协议，密码字段为必填。
- **Privacy protocol（隐私协议）：**选择 SNMP 设置的加密算法。

- **Email ID（电子邮件 ID）：**输入用户的电子邮件 ID。如果用户忘记密码，新密码会发送到配置的电子邮件 ID。
  **注意：**必须配置 SMTP 服务器才可发送电子邮件。
- **Email Format（电子邮件格式）：**指定电子邮件的格式。发送电子邮件时会使用该格式。共有两种格式：
  - AMI 格式：该电子邮件格式下的主题是“Alert from (your Hostname)（（来自主机的）通知）”。电子邮件内容显示传感器信息，如：传感器类型和说明。
  - 固定主题格式：该格式根据用户设置显示消息。必须设置电子邮件通知的主题和消息。
- **Uploaded SSH Key（上传的 SSH 密钥）：**显示上传的 SSH 密钥信息（只读）。
- **New SSH Key（新 SSH 密钥）：**使用“Browse（浏览）”按钮导航到 SSH 公钥文件。
  - SSH 密钥文件应是公钥类型。
- **Modify（修改）：**单击“Modify（修改）”接受修改，返回到用户列表。
- **Cancel（取消）：**单击“Cancel（取消）”取消修改，并返回到用户列表。

## Virtual Media（虚拟媒介）

使用该页面配置虚拟媒介设备设置。如果在该页面更改了虚拟媒介配置，会在 JViewer Vmedia 向导显示正确的设备。例如，如果在 Configure（配置） -> Virtual Media（虚拟媒介）->Jviewer -> VMedia 选择两个软盘设备，可以查看这两个软盘进行重定向，打开虚拟媒介页面，从菜单栏单击 **Configuration（配置） > Virtual Media（虚拟媒介）**。虚拟媒介页面截图示例如下。

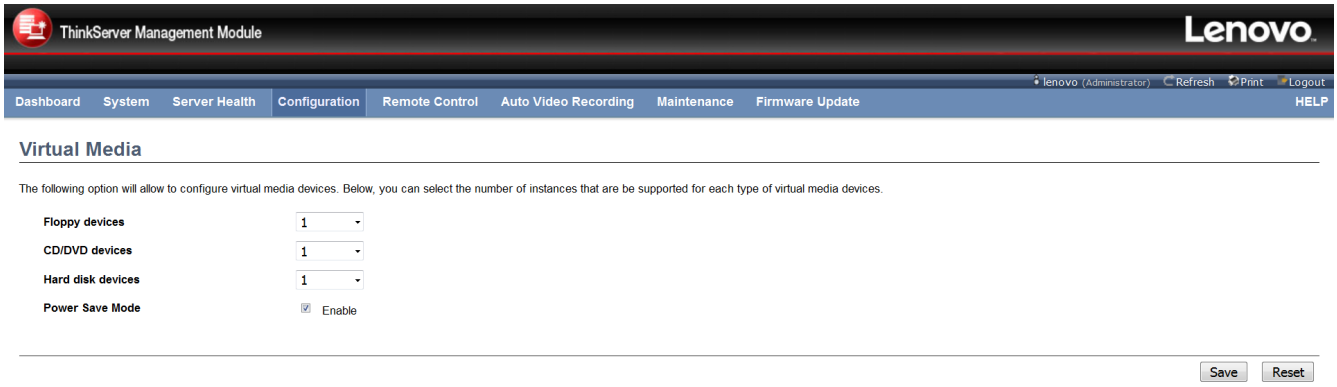



*图 56：虚拟媒介页面*

该页面会显示如下字段。

- **Floppy devices（软盘）：**选择虚拟媒介重定向需要支持的软盘数。
- **CD/DVD devices（CD/DVD 设备）：**选择虚拟媒介重定向需要支持的 CD/DVD 数。
- **Hard disk devices（硬盘驱动器）：**选择虚拟媒介重定向需要支持的硬盘数。
- **Power Save Mode（节能模式）：**启用或禁止虚拟 USB 设备在主机上是否可见。
- **Save（保存）：**单击“Save（保存）”保存配置设置。
- **Reset（重置）：**单击 “Reset（重置）”先前保存的数值。

## Cipher Suites（加密算法）

使用该页面配置加密算法。

如要打开加密算法设置页面，从菜单栏单击 **Configuration（配置） > Cipher Suites（加密算法）**。加密算法页面截图示例如下。

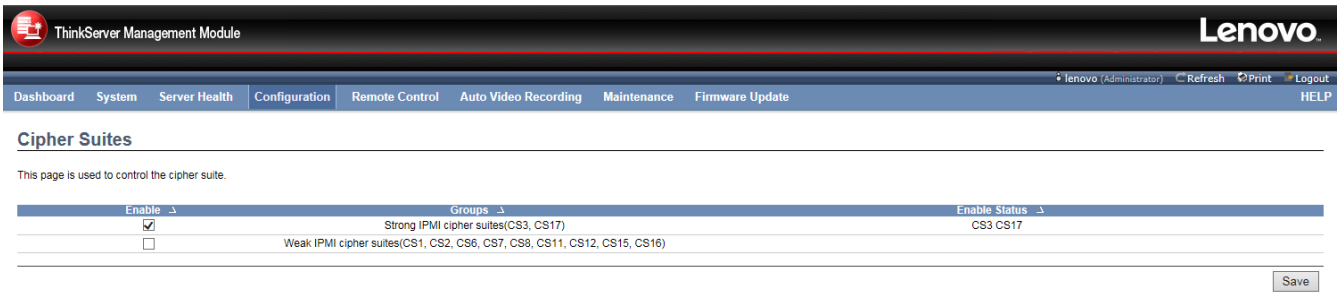



*图 57：加密算法页面*

加密算法字段说明如下。

- **Enable（启用）：** 选择启用群组。
- **Groups（群组）：** 显示群组详细信息。
- **Enable Status（显示状态）：** 显示群组状态。
- **Save（保存）：** 单击“Save（保存）”保存配置。

## Remote Control（远程控制）

远程控制包含下列菜单项。

- Console Redirection（控制台重定向）
- Server Power Control（服务器电源控制）
- Java SOL

远程控制截图示例如下。

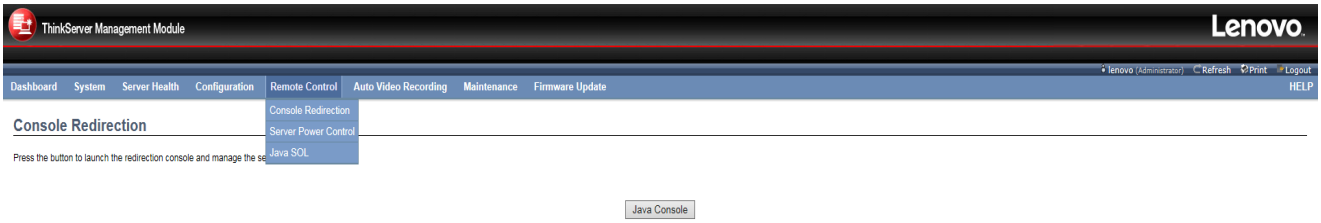



*图 58：远程控制页面*

下面详细介绍菜单。

## Console Redirection（控制台重定向）

从本页面启动远程控制台重定向窗口。如要启动，必须具有管理员权限或 KVM 权限。

**注意：**启动 JNLP 文件之前必须安装兼容的 JRE。

打开控制台重定向页面，从菜单栏单击 **Remote Control（远程控制）> Console Redirection（控制台重定向）**。控制台重定向页面截图示例如下。

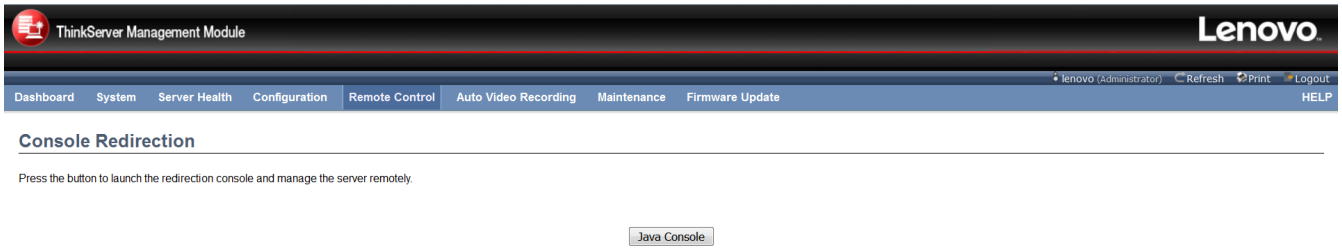



*图 59：控制台重定向页面*

- **Java Console（Java 控制台）：**单击“Java Console（Java 控制台）”开始下载 jviewer.jnlp 文件。文件下载并启动后，会显示 Java 重定向窗口。

## Browser Settings（浏览器设置）

要启动 KVM，需要禁用弹出阻止。在 Internet explorer 上，在设置中启用文件下载。

## Java Console（Java 控制台）

这是独立于系统的插件，可用于安装有 JRE 的 Windows、Linux。JRE 应安装在客户端系统。可以使用下列链接安装 JRE。*http://www.java.com/en/download/manual.jsp*

在 TMM 用户界面，可用两种方式启动控制台。

1. 打开 **Dashboard（仪表板）**页面，在远程控制区单击启动 Java 控制台。
2. 打开 **Remote Control（远程控制）>Console Redirection（控制台重定向）**页面，单击 Java 控制台。

从 BMC 下载.jnlp 文件。如要打开.jnlp 文件，请使用正确的 JRE 版本（Javaws）。当下载完成时，它会打开控制台重定向窗口。

控制台重定向菜单栏包含下列菜单项。

### 小窍门：清除 Java 缓存。

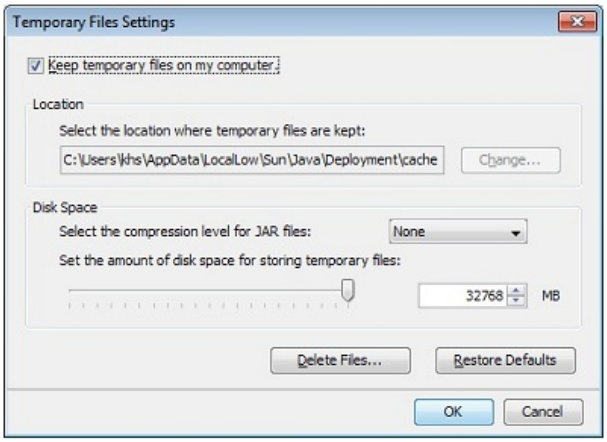
清除 Java 插件缓存会强制浏览器重新加载网页和程序。

通过 Java 控制台面板删除临时文件清除 Java 缓存，可以使用下列链接了解更多详细信息。

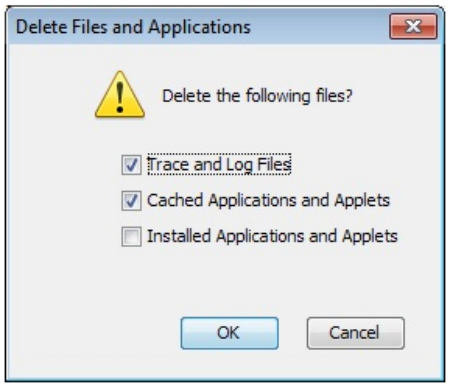
*https://www.java.com/en/download/help/plugin_cache.xml*

文章适用于：

- **平台：**Windows 8、Windows 7、Vista、Windows XP、Windows 10
- **Java 版本：**7.0, 8.0
- **通过 Java 控制台面板删除临时文件：**
  1. 在 Java 控制面板 **General（常规）**选项卡下，单击临时 Internet 文件的 **Settings（设置）**。弹出 **Temporary Files Settings（临时文件设置）**对话框。




  2. 在临时文件设置对话框上单击 **Delete Files（删除文件）**。弹出 **Delete Files and Applications（删除文件和应用）**对话框。




3. 单击 **Delete Files and Applications（删除文件和应用）** 对话框上的 **OK（确定）**。删除缓存内所有下载的应用程序和小程序。
4. 在 **Temporary Files Settings（临时文件设置）**单击 **OK（确定）**。如果希望删除缓存中的某个应用程序或小程序，请分别单击“View Application（查看应用程序）”和“View Applet（查看小程序）”。

## Video（视频）

菜单包含下列子菜单。

- **Pause redirection（暂停重定向）**：可暂停控制台重定向。
- **Resume Redirection（恢复重定向）**：当会话暂停时，可用于恢复控制台重定向。
- **Refresh Video（刷新视频）**：可用于更新控制台重定向窗口显示。
- **Capture Screen（捕捉屏幕）**：帮助捕捉主机屏幕，并保存到客户端系统。
- **Compression Mode（压缩模式）**：按某种模式压缩视频数据。可以选择以下某一模式：
  - YUV 420
  - YUV 444
  - YUV 444 + 2 colors VQ
  - YUV 444 + 4 colors VQ
- **DTC Quantization Table（DTC 量化表）**：帮助选择视频质量。可以选择以下某一模式：
  - 0 最佳
  - 1
  - 2
  - 3
  - 4
  - 5
  - 6
  - 7 最差
- **Turn ON Host Display（开启主机显示）**：如果禁止，服务器显示空白，但可以在控制台重定向中查看屏幕。如果启用，会重新显示服务器屏幕。
- **Turn OFF Host Display/Host Video Output（关闭主机显示/主机视频输出）**：如果启用，服务器显示空白，但可以在控制台重定向中查看屏幕。如果禁止，会重新显示服务器屏幕。
- **Full Screen（全屏）**：可用于全屏模式（最大）查看控制台重定向。只有当客户端和主机分辨率一致才可启用。
- **Exit（退出）**：可退出控制台重定向屏幕。

## Keyboard（键盘）

菜单包含下列子菜单。

- **Hold Right Ctrl Key（长按右 Ctrl 键）：**在控制台重定向下，该菜单可用于充当右<CTRL>键。
- **Hold Right Alt Key（长按右 Alt 键）：**在控制台重定向下，该菜单可用于充当右<ALT>键。
- **Hold Left Ctrl Key（长按左 Ctrl 键）：**在控制台重定向下，该菜单可用于充当左<CTRL>键。
- **Hold Left Alt Key（长按左 Alt 键）：**在控制台重定向下，该菜单可用于充当左<ALT>键。
- **Left Windows Key（左 Windows 键）：**在控制台重定向下，该菜单可用于充当左<WIN>键。还可决定如何按下该键：长按或按下放开。
- **Right Windows Key（右 Windows 键）：**在控制台重定向下，该菜单可用于充当右<WIN>键。还可决定如何按下该键：长按或按下放开。
- **Ctrl+Alt+Del：**该菜单可用于充当同时在重定向的服务器上按下<CTRL>、<ALT> 和<DEL>。
- **Context menu（上下文菜单）：**在控制台重定向下，该菜单可用于充当上下文菜单键。
- **Hot Keys（热键）：**该菜单可用于为主机添加用户可配快捷键。配置的快捷键保存在 BMC 中。
- **Full Keyboard Support（全键盘支持）：**可提供全键盘支持。可直接在物理键盘上直接触发主机上的 Ctrl 和 Alt 键。

## Mouse（鼠标）

- **Show Cursor（显示光标）：**该菜单可用于在远程客户端系统上显示或隐藏本地鼠标光标。
- **Mouse Calibration（鼠标校准）：**只有当鼠标模式设为相对时，才可使用该菜单。

在这一步可发现远程服务器上的鼠标阈值。本地鼠标光标以红色显示，远程光标成为远程视频屏幕一部分。两个光标会在开始时同步。使用“+”或“-”更改阈值，直到光标不同步为止。请记下第一个光标不同步的读数。记下后，使用“ALT-T”保存阈值。

- **Mouse Mode（鼠标模式）：**重定向控制台使用两种方式之一，实现本地窗口到远程屏幕的鼠标仿真。只有“Administrator（管理员）”有权限配置该选项。
  - **Absolute Mouse mode（绝对鼠标模式）：**如果选择该选项，会发送本地鼠标绝对位置给服务器。
  - **Relative Mouse mode（相对鼠标模式）：**如果选择该选项，会相对模式发送鼠标相对偏移计算值给服务器。
  - **Other Mouse mode（其他鼠标模式）：**该鼠标模式在客户端系统中设置客户端光标，并将偏差发送给主机。该鼠标模式仅用于 SUSE Linux。

## Options（选项）

- **Band width (Except Hornet)（带宽（除了 Hornet））：**带宽使用可调节带宽。可以选择以下某一模式：
  - **Auto Detect（自动检测）：**可自动检测 BMC 网络带宽使用情况。
  - 256 Kbps
  - 512 Kbps
  - 1 Mbps
  - 10 Mbps
  - 100 Mbps
- **Keyboard/Mouse Encryption（键盘、鼠标加密）：**允许加密彼此发送的键盘输入和鼠标动作。
- **Zoom（缩放）**
  - **Zoom In（放大）：**增加屏幕尺寸。在 100%到 150%按 10%递增缩小。
  - **Zoom Out（缩小）：**缩小屏幕尺寸。在 100%到 50%按 10%递增缩小。
  - **Actual Size（实际尺寸）：**默认选择该选项。

- **Fit to Client Resolution（适配客户端分辨率）：** 如果主机屏幕分辨率大于客户端屏幕分辨率，请选择该选项适配主机屏幕和客户端屏幕。主机视频会在 KVM 控制台缩小和渲染。此时主机鼠标光标看起来会比客户端鼠标光标小。客户端和主机鼠标光标可能无法完美同步。
- **Fit to Host Resolution（适配主机分辨率）：** 如果主机屏幕分辨率小于客户端屏幕分辨率，请选择该选项缩放 JViewer 适配主机屏幕。

- **Send IPMI Command（发送 IPMI 命令）：** 该选项可打开 IPMI 命令对话框。在十六进制字段按十六进制值输入原始 IPMI 命令，并单击“Send（发送）”。显示如下截图的响应。

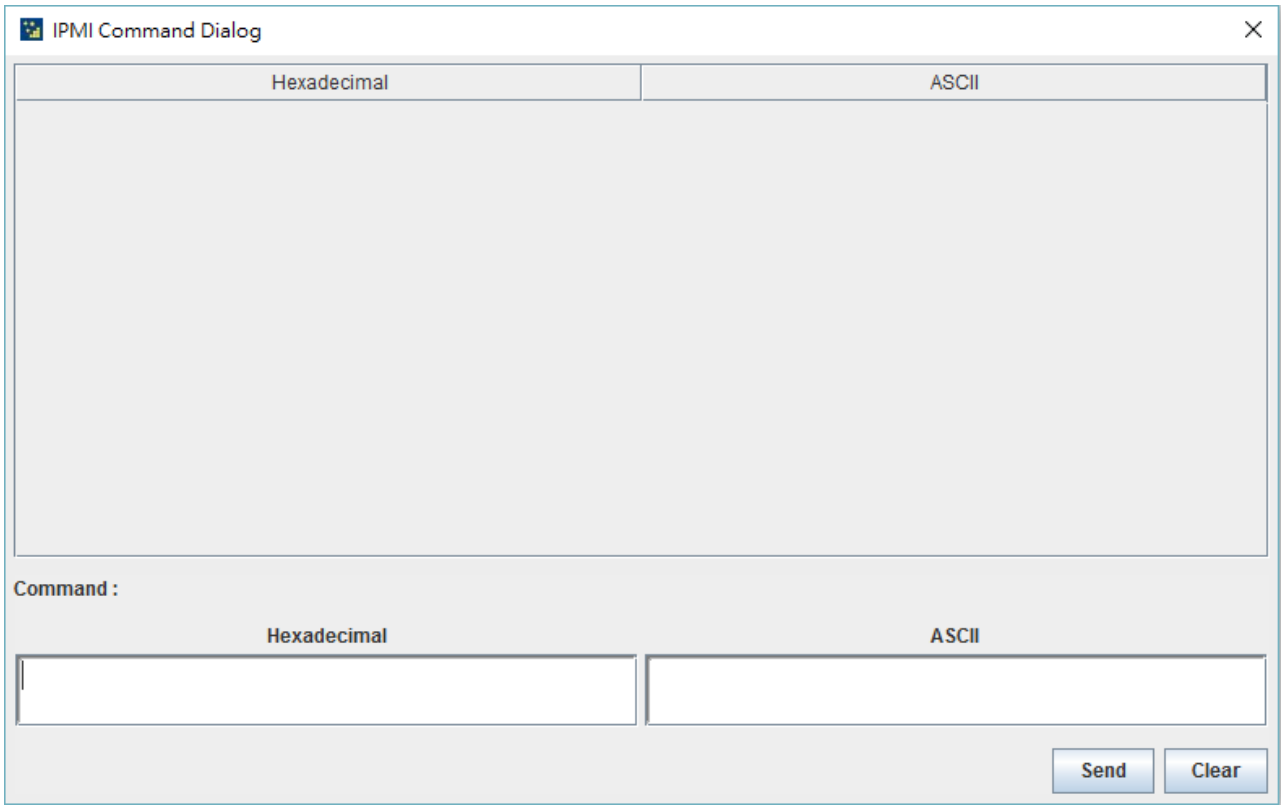



*图 60：IPMI 命令对话框*

- **GUI Languages（图像用户界面语言）：** 选择所需的图形用户界面语言。

## Media（媒介）

- **Virtual Media Wizard（虚拟媒介向导）**

  如要添加或修改媒介，选择单击 **Virtual Media Wizard（虚拟媒介向导）**按钮，弹出 **Virtual Media（虚拟媒介）**框，在上面配置媒介。虚拟媒介屏幕截图示例如下。

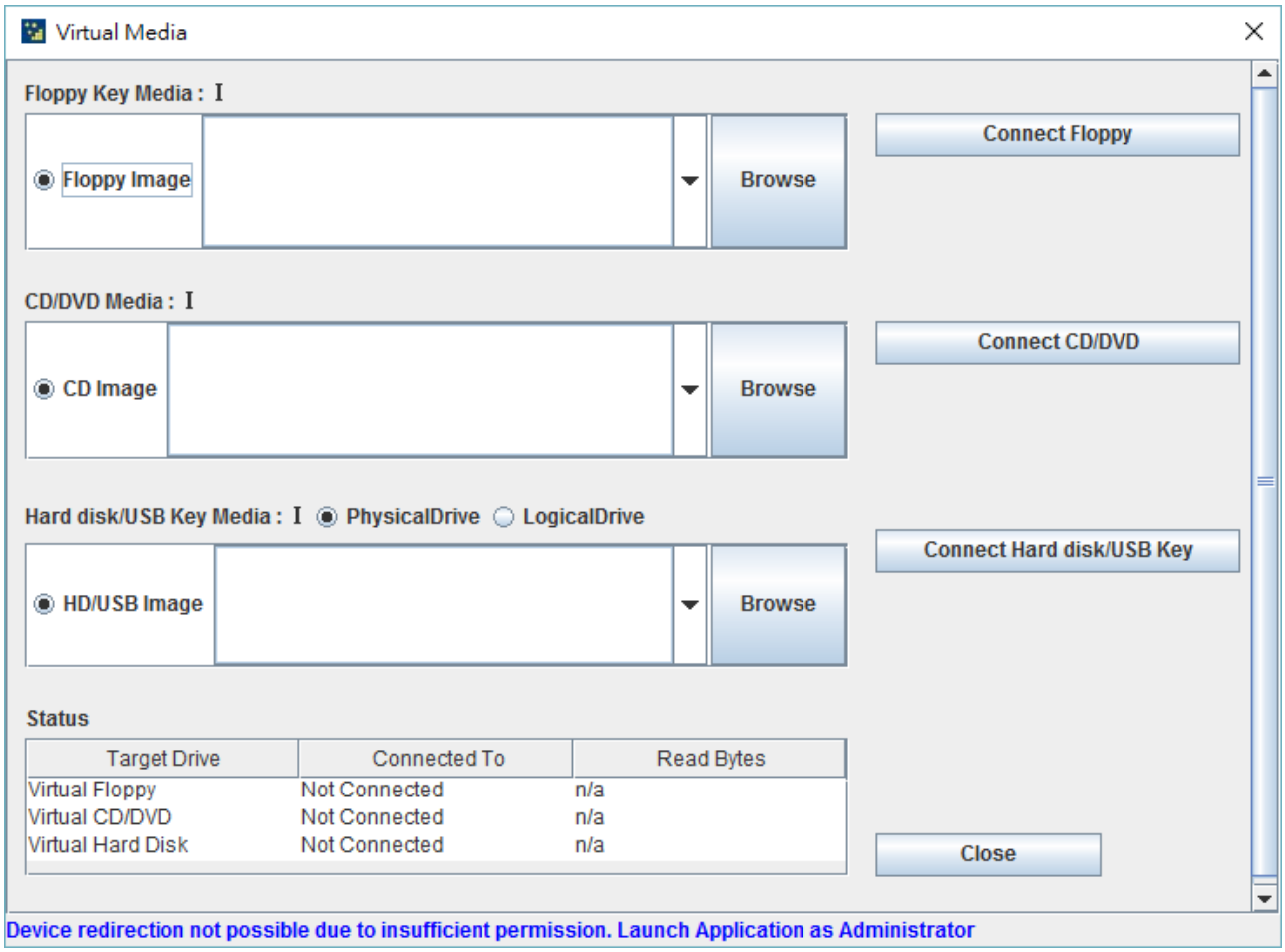



*图 61：虚拟媒介*

- **Floppy Key Media（软盘媒介）：**该菜单可用于启动或停止物理软盘重定向，软盘镜像类型如 img。
- **CD/DVD Media（CD/DVD 媒介）：**该菜单可用于启动或停止 DVD/CD-ROM 重定向，CD 镜像类型如 iso。
- **Hard disk/USB Key Media（硬盘/USB 闪存媒介）：**该菜单可用于启动或停止硬盘/USB 闪存重定向，USB 闪存镜像类型如 img。

## Keyboard Layout（键盘布局）

- **Auto Detect（自动检测）：**用于自动检测键盘布局。如果客户端和主机键盘布局一致，对于所有支持的物理键盘布局，必须选择该选项避免输入错误。如果主机和客户端语言不同，用户可以在菜单选择主机语言布局，然后直接使用物理键盘。
- **Host Physical Keyboard（主机物理键盘）：**该功能完全兼容键盘语言布局相同的主机和客户端。如果客户端和主机语言布局不一致，有些特殊字符可能不兼容。
  - **Host Platform（主机平台）：**该功能包含两种选择，Windows 和 Linux。当在 Windows 主机下工作，请选择 Windows。当在 Linux 主机下工作，请选择 Linux。应根据物理键盘布局正确选择该选项，才可正常工作。默认选择 Windows。

  列举 TMM JViewer 支持的所有软物理键盘语言。
  - 英语 - 美国
  - 英语 - 英国
  - 法语

- 法语（比利时）
- 德语（德国）
- 德语（瑞士）
- 日语
- 西班牙语
- 意大利语
- 丹麦语
- 芬兰语
- 挪威语（挪威）
- 葡萄牙语（葡萄牙）
- 瑞典语
- 荷兰语（荷兰）
- 荷兰语（比利时）
- 土耳其语-F
- 土耳其语-Q

- **Soft Keyboard（软键盘）：** 允许选择键盘布局。显示类似 Windows 屏幕键盘的对话框。如果客户端和主机语言不同，可以从 JViewer 列表中选择与主机键盘布局一致的软键盘，避免使用时输入错误。列举 TMM JViewer 支持的所有软物理键盘语言。
  - 英语 - 美国
  - 英语 - 英国
  - 西班牙语
  - 法语
  - 德语（德国）
  - 意大利语
  - 丹麦语
  - 芬兰语
  - 德语（瑞士）
  - 挪威语（挪威）
  - 葡萄牙语（葡萄牙）
  - 瑞典语
  - 希伯来语
  - 法语（比利时）
  - 荷兰语（荷兰）
  - 荷兰语（比利时）
  - 俄语（俄罗斯）
  - 日语（QWERTY）
  - 日语（平假名）
  - 日语（片假名）
  - 土耳其语-F
  - 土耳其语-Q

## Video Record（视频录制）

- **Start Record（开始录制）：** 可开始录制屏幕。
- **Stop Record（停止录制）：** 可停止录制。
- **Settings（设置）：** 如要设置视频录制，

1. 单击 **Video Record（视频录制） > Settings（设置）**打开如下所示设置页面。

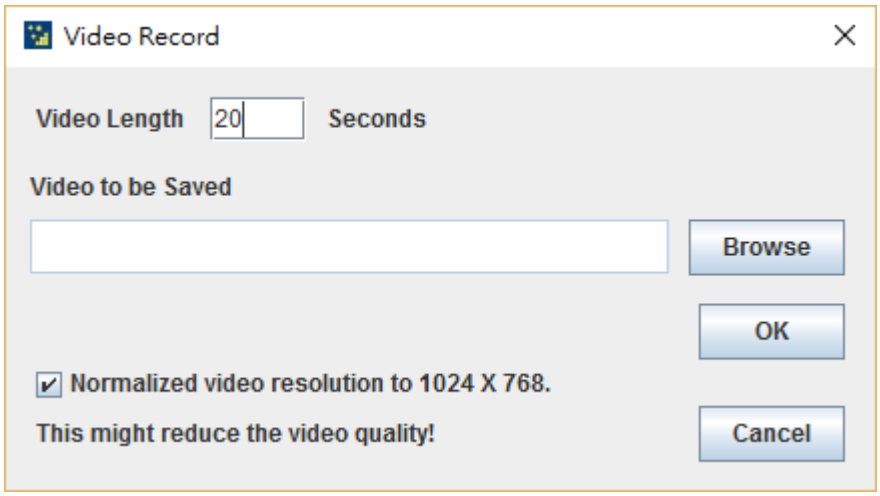



*图 62：视频录制设置页面*

2. 输入 **Video Length（视频长度）**秒数。
3. 浏览和输入保存视频的位置。
4. 启用“标准化”视频分辨率到 1024 X 768。
5. 单击 **OK（确定）**保存，并返回到控制台重定向屏幕。
6. 如果不希望保存，则单击 **Cancel（取消）**。
7. 在控制台重定向窗口，单击 **Video Record（视频录制） > Start Record（开始录制）**。
8. 录制过程。
9. 如要停止录制，单击 **Video Record（视频录制） > Stop Record（停止录制）**。

## Power（电源）

电源选项可用于执行任何电源周期操作。单击所需的选项执行下列操作。

- **Reset Server（重设服务器）：**不关机重启系统（热重启）。
- **Immediate Shutdown（立即关机）：**立即断掉服务器电源。
- **Orderly Shutdown（有序关机）：**在断开电源前开始关闭操作系统。
- **Power On Server（开机）：**开后服务器。
- **Power Cycle Server（服务器电源周期）：**首先关闭电源，然后重启系统（冷重启）。

## Active Users（活动用户）

单击选项显示活动用户和系统 IP 地址。

## Help（帮助）

Jviewer：显示版权和版本信息。

## Quick Buttons（快捷按钮）

控制台重定向窗口右下方显示所有快速按钮。这些快速按钮可一键执行这些功能。

| 快捷按钮 | 说明 |
| --- | --- |
|  | 该按键用于播放暂停后的控制台重定向。 |
|  | 该按键可暂停控制台重定向。 |
|  | 可用于全屏模式查看控制台重定向。<br><br>**注意：** *将客户端系统分辨率设为主机系统分辨率一致，这样全屏查看服务器。* |
|  | 这 3 个快捷按钮可弹出虚拟媒介，用于配置媒介。 |
|  | 用于在远程客户端系统上显示或隐藏鼠标光标的快捷按钮。 |
|  | 用于显示或隐藏软键盘的快捷按钮。 |
|  | 用于录制视频的快捷按钮。 |
|  | 显示可用热键的快捷按钮。 |
|  | 拖动缩放。 |
|  | 活动用户 |
|  | 用过锁定或解锁本地主机显示的快捷按钮。 |
|  | 该快捷按钮如同开关，图标绿色，服务器状态是 **power on（开机）**，如果图标显示红色，服务器状态为 **power off（关机）**，单击这个按钮会触发 **immediate shutdown（立即关机）**动作。单击按钮 **power on（开机）**。 |

## Server Power Control（服务器电源控制）

该页面用于查看或执行任何主机电源周期操作。打开电源控制和状态页面，从菜单栏单击 **Remote Control （远程控制）> Server Power Control（服务器电源控制）**。

电源控制和状态页面截图示例如下。

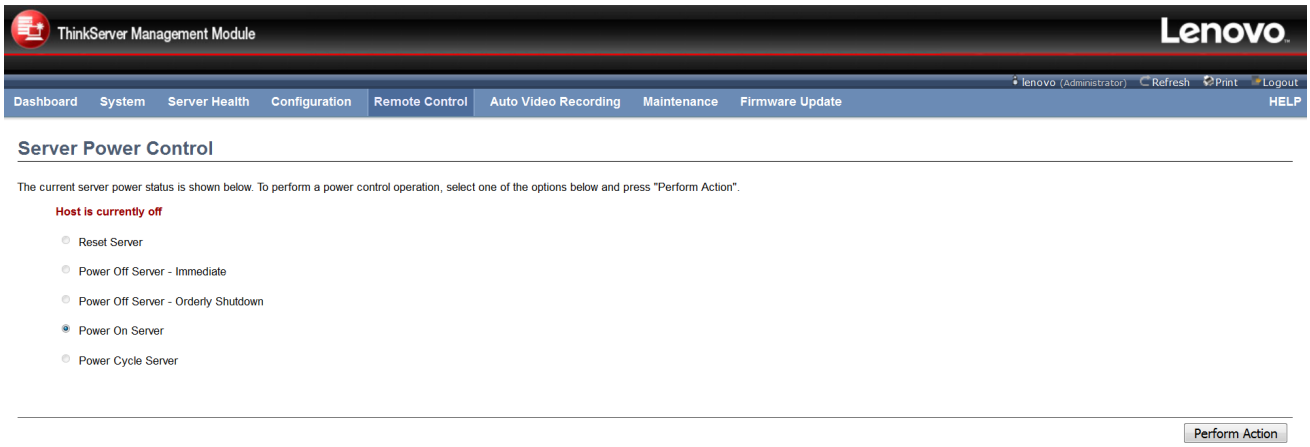



*图 63：电源控制和状态页面*

不同电源控制选项如下所示。

- **Reset Server（重设服务器）：**选择不关机重启系统（热重启）。
- **Power Off Server – Immediate（关机-立即）：**选择该选项立即断掉服务器电源。
- **Power Off Server – Orderly Shutdown（关机-有序关闭）：**如果选择该选项，在断开电源前开始关闭操作系统。
- **Power On Server（开机）：**开启服务器电源。
- **Power Cycle Server（服务器电源周期）：**首先关闭电源，然后重启系统（冷重启）。
- **Perform Action（执行动作）：**单击“Perform Action（执行动作）”执行所选选项。

## Java SOL

该页面允许启动 Java SOL。Java SOL 用于查看使用 SQL 重定向的主机屏幕，打开 Java SQL 页面，从菜单栏单击 **Remote Control（远程控制） > Java SOL**。Java SOL 页面截图示例如下。

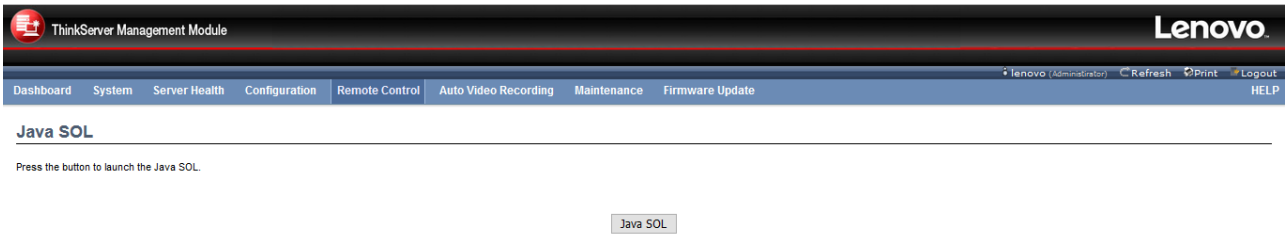



*图 64：Java SOL 页面*

- 

如要启动 Java SOL，必须具有管理员权限或 KVM 权限。

**注意：**启动 JNLP 文件之前必须安装兼容的 JRE。

1. 单击 Java SOL 按钮打开 Java SOL 窗口。

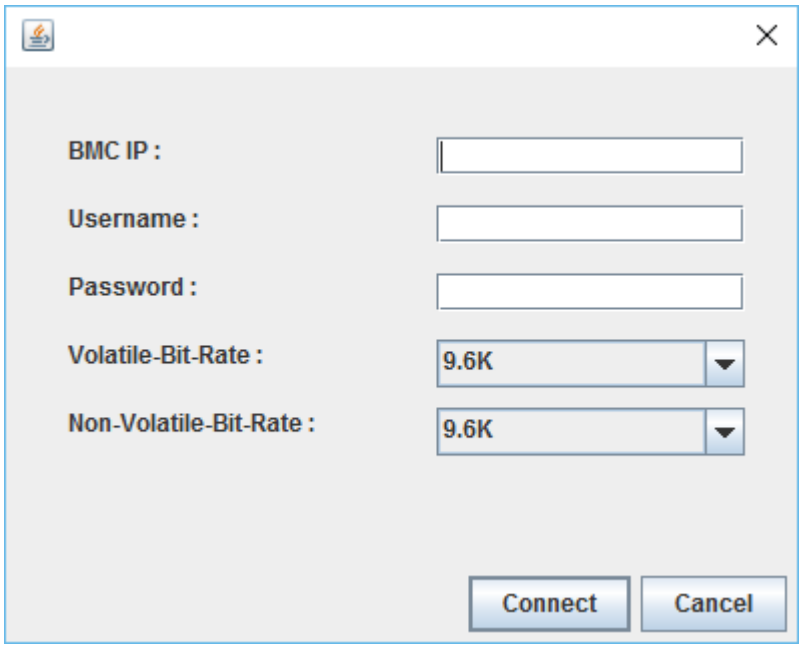



*图 65：Java SOL 页面*

2. 在各个字段输入 BMC IP 地址、用户名称和密码。
3. 从下拉列表选择易失比特率和非易失比特率。
4. 单击 **Connect（连接）**打开 SOL 重定向。

**注意：**

- 打开 SOL 之前，请首先启用 BIOS 设置的 SOL。
- 用户名/密码同网页用户。

## Auto Video Recording（自动视频录制）

TMM 支持触发视频录制。自动视频录制菜单截图如下所示，包括触发配置设置。

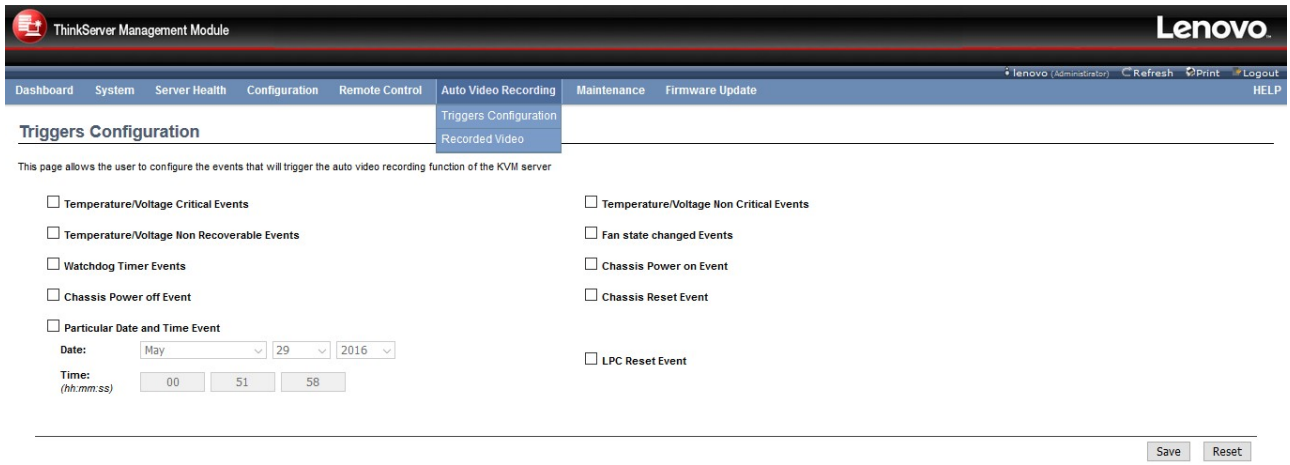



*图 66：自动视频录制菜单*

## Triggers Configuration（触发配置）

配置页面上哪个事件会触发启动自动视频录制。

如要打开触发配置页面，从菜单栏单击 **Auto Video Recording（自动视频录制） > Triggers Configuration（触发配置）**。触发配置页面截图示例如下。

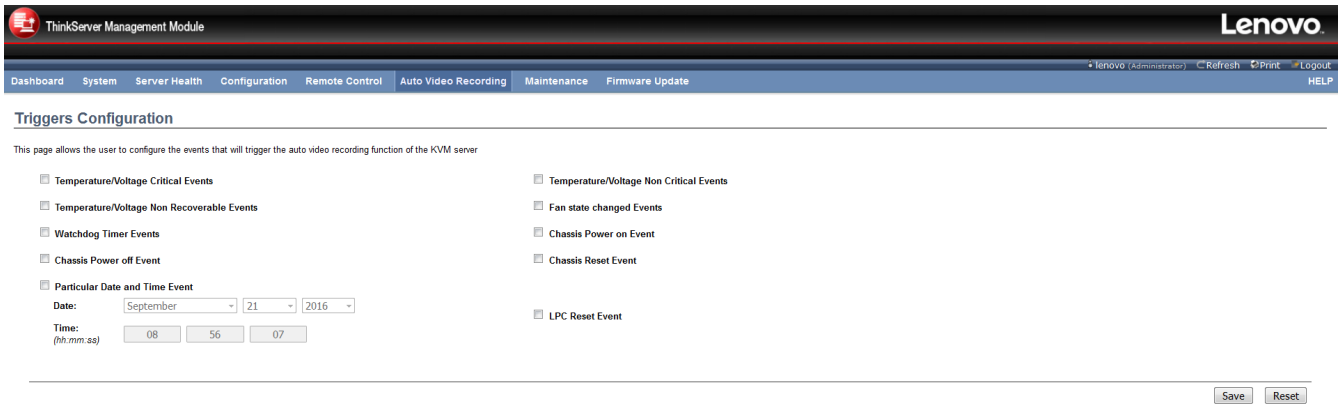



*图 67：触发配置页面*

- **Event List（事件列表）：** 可以选择或取消选择该框添加或删除系统触发。
- **Save（保存）：** 单击“Save（保存）”保存所做的更改。
  **注意：** 需要启用 KVM 服务（“Configuration（配置） -> Services（服务）”下）才可进行自动视频录制。日期和时间应先于系统日期和时间。
- **Reset（重置）：** 单击 “Reset（重置）”重置修改。

## Recorded Video（录制的视频）

该页面显示一列已录制的视频文件。录制的视频的不同字段如下所示：
#: 序列号。
File Name（文件名）：视频文件名。
Video Type（视频类型）：视频类型，前期事件或后期事件。
File Information（文件信息）：视频上传天、日期和时间。
**注意：** 如果启用远程视频支持，可以录制 3 个前期事件视频和最多的后期事件视频。如果禁用远程视频支持，可以录制 1 个前期事件视频和 2 个后期事件视频。
如果远程共享加载失败，视频文件会存储在 BMC 的本地路径下。
如要打开视频录制页面，从菜单栏单击 **Auto Video Recording（自动视频录制） > Recorded Video（录制的视频）**。已录制视频页面截图示例如下。

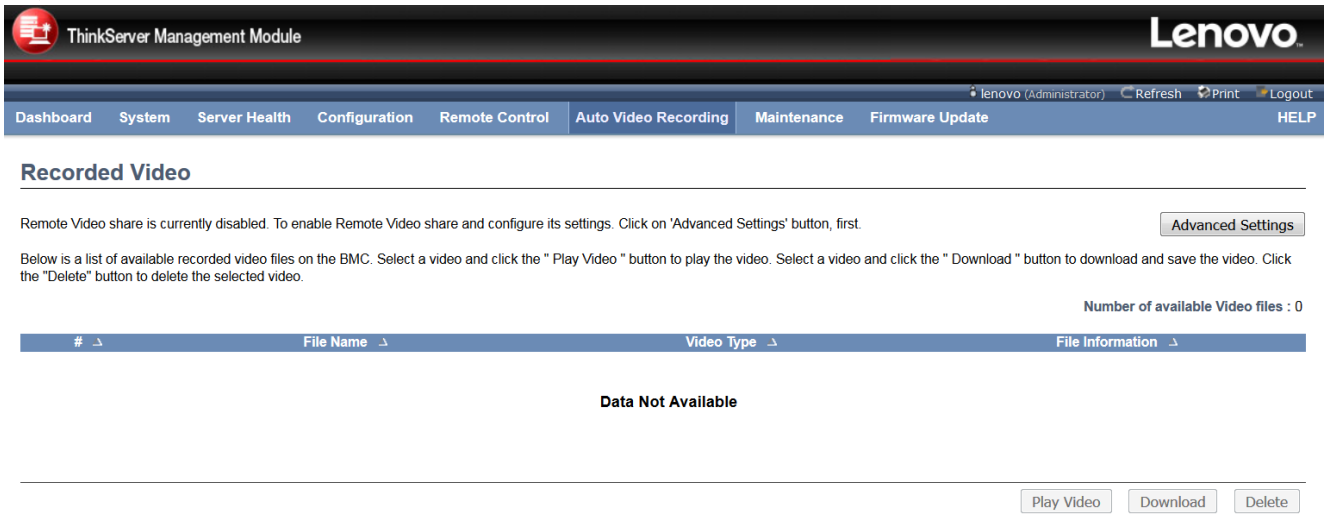



*图 68：录制视频*

- **Advanced Settings（高级设置）：**单击选项配置远程视频设置。可启用或禁止远程视频支持、服务器地址、源路径、共享类型、用户名、密码和域名。
- **Play Video（播放视频）：**选择一个视频，单击“Play Video（播放视频）”按钮，在 Java 应用程序中播放视频。
- **Download（下载）：**选择视频，单击“Download（下载）”按钮开始下载，并保存视频文件到客户端机器。视频按（.avi）格式下载。
- **Delete（删除）：**单击“Delete（删除）”按钮删除已选择的视频文件。

**Procedure for Auto Recorded Video（自动录制视频步骤）：**

该页面用于配置远程视频高级设置。支持所有受信任的域。

**注意：**已配置的设置会在下次视频录制时生效。

如要打开高级远程视频设置页面，请单击 **Advanced Settings（高级设置）**。

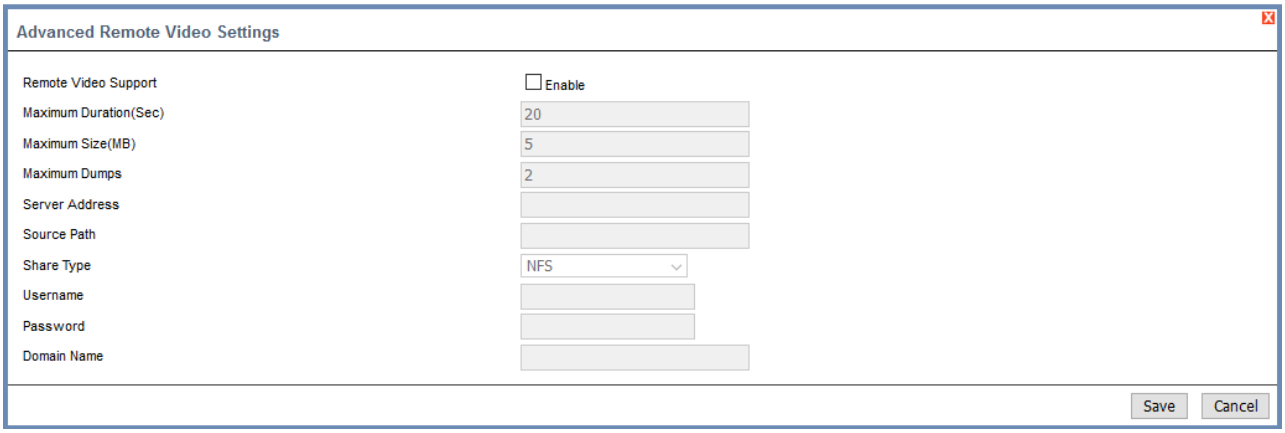



*图 69：高级远程视频设置*

- **Remote Video Support（远程视频支持）：**如要启用或禁止远程视频支持，可分别勾选或取消“Enable（启用）”。

  **注意：**默认下视频文件会存储在 BMC 的本地路径下。如果启用了远程视频支持，视频文件将仅保存在远程路径下，而不是 BMC 内。
- **Maximum Duration (Sec)（最长持续时间（秒））：**最长持续时间范围是 1 到 3600 秒。
- **Maximum Size (MB)（最大大小 (MB)）：**最长大小范围是 1 到 500 MB。
- **Maximum Dumps（最多转储）：**最多转储次数范围是 1 到 100。
- **Server Address（服务器地址）：**存储远程视频的服务器的地址。服务器地址支持：
  - IP 地址（IPv4 和 IPv6 格式）。
  - FQDN（完全限定域名）格式。
- **Source Path（源路径）：**存储远程视频的源路径目录。
  - 不允许特殊字符“<”（小于）、“>”（大于）、“:”（冒号）、“*”（星号）、“|”（竖线）、“.”（点）、“?”（问号）。
- **Share Type（共享类型）：**远程视频服务器的共享类型可以是 NFS 或 Samba（CIFS）。
- **Username, Password and Domain Name（用户名、密码和域名）：**如果共享类型是 Samba（CIFS），请输入服务器认证用户凭证。

  **注意：**域名字段是可选字段。

## Maintenance Group（维护组）

该组页面可完成设备的维护工作。菜单包含以下内容：

- 保留配置
- 恢复配置

## Preserve Configuration（保留配置）

该页面可选择在“恢复配置”、“不保留配置固件更新”下要保留的特定配置。打开保有配置页面，从菜单单击 **Maintenance Group（维护组） > Preserve Configuration（保留配置）**。保留配置页面截图示例如下。

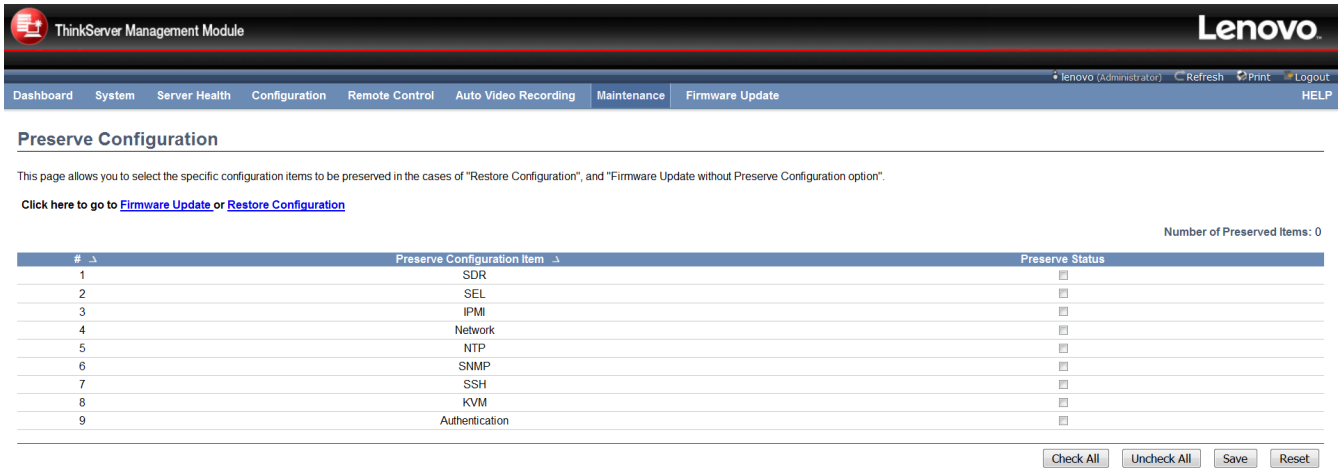



*图 70：保留配置*

选择在恢复配置时要保留的配置。

- **#:** 序列号。
- **Configuration list（配置列表）：** 可以选择或取消选择该框保留或删除系统配置。
- **Check All（选择全部）：** 单击该按钮选择所有配置列表。
- **Uncheck All（取消选择全部）：** 单击该按钮取消选择所有配置列表。
- **Save（保存）：** 单击“Save（保存）”保存所做的更改。
  **注意：** 该配置用于恢复配置过程。在选择“SEL”或“NTP”作为依赖配置时，请同时请启用“IPMI”。
- **Reset（重置）：** 单击 “Reset（重置）”重置修改。

### Files Preserved（保留的文件）

- **SDR：** 该文件包含 IPMI 所用的传感器数据录制信息。
- **SEL：** 该文件包含 IPMI 记录的系统事件日志。
- **IPMI：** 该文件包含 IPMI 配置，如 SEL 库/SDR 库大小、接口、启用/禁用、主/次、IPMB 总线数等。
- **Network（网络）：** 该文件包含网络配置， 如主机名、接口、PHY 配置、NCSI 配置等。
- **NTP：** 此文件包含 NTP 配置。
- **SNMP:** 此文件包含 SNMP 配置。
- **SSH:** 此文件包含 SSH 配置。
- **KVM:** 此文件包含 KVM 配置。
- **Authentication（验证）：** 此文件包含身份认证配置。

## Restore Configuration（恢复配置）

该页面帮助恢复设备的配置。请注意一旦进入恢复配置、部件和其他网页，服务就会停止。所有打开的小部件会自动关闭。设备会在几分钟内重置和重启。

打开恢复出厂默认页面，单击菜单栏 **Maintenance（维护） > Restore Configuration（恢复配置）**。出厂默认页面截图示例如下。

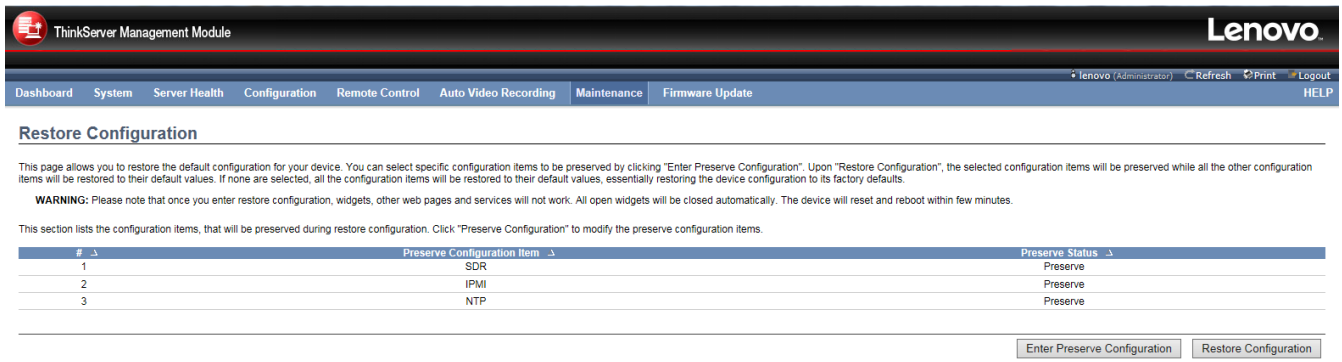



*图 71：恢复配置*

- **#:** 序列号。
- **Preserve Configuration（保留配置）：** 单击此处跳转到保留配置页面，保留某些配置，不会被默认值覆盖。
- **Restore Configuration（恢复配置）：** 单击此处使用默认配置恢复固件。

## Firmware Update（固件更新）

该组页面可完成如下工作。菜单包含以下内容：

- Firmware Update（固件更新）
- BIOS Update（BIOS 更新）
- Protocol Configuration（协议配置）

详细说明如下：

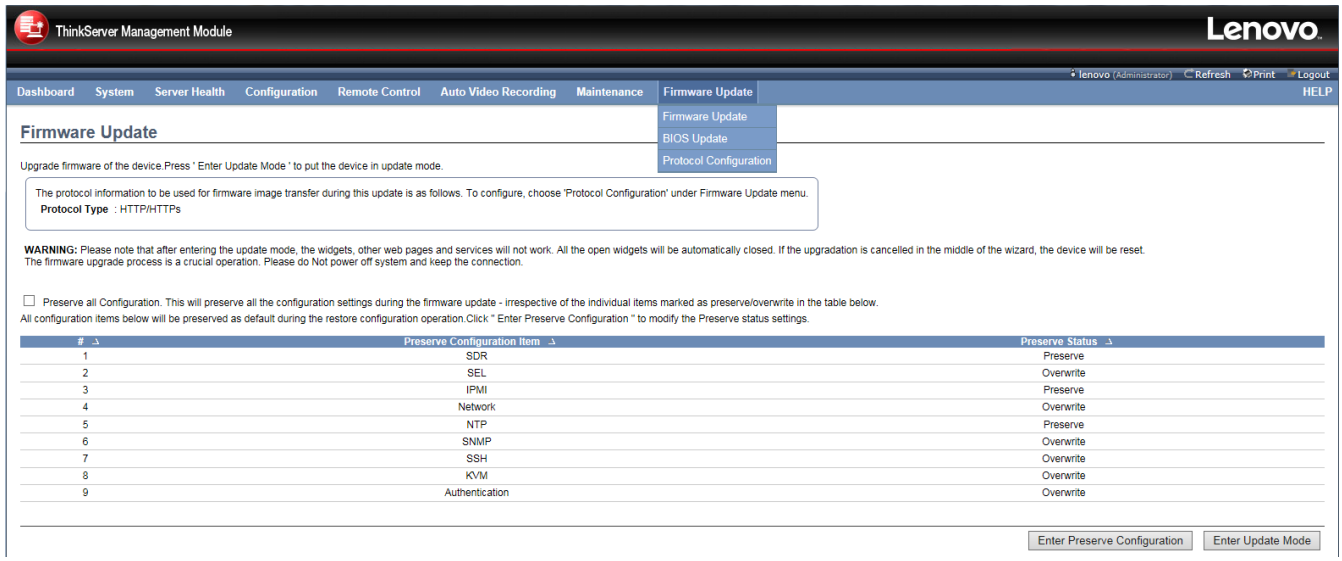



*图 72：固件更新菜单*

## Firmware Update（固件更新）

该向导包含固件升级整个过程。升级完成或取消后，自动会出现一个复位可选框。出现是否保留配置选项。要在升级时保留配置，可启用该选项，打开固件更新页面，从菜单栏单击 **Firmware Update（固件更新）> Firmware Update（固件更新）**。固件更新截图示例如下。

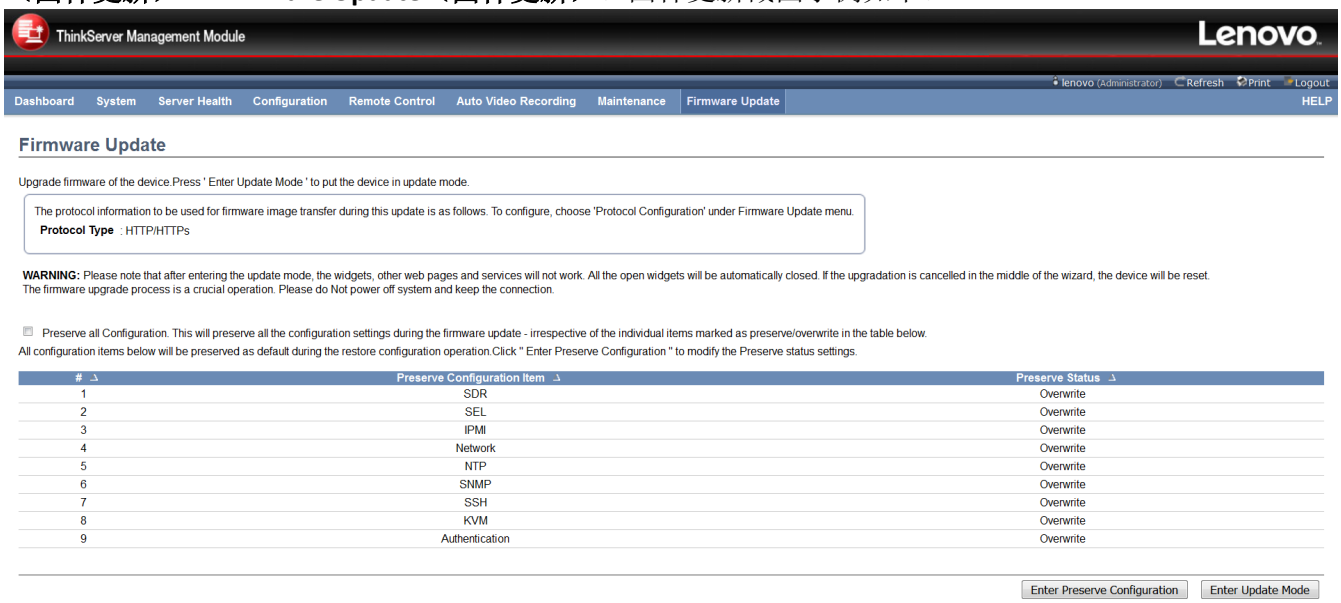



*图 73：固件更新*

各个字段显示如下。

- **#:** 序列号。
- **Enter Preserve Configuration（进入保留配置）：** 单击该按钮进入保留配置页面，可以选择不让默认配置覆盖。
- **Enter Update Mode（进入更新模式）：** 单击“Enter Update Mode（进入更新模式）”升级当前设备固件。

### Procedure（流程）

1. 单击 **Enter Update Mode（进入更新模式）**升级当前设备固件，按以下步骤，
2. 关闭所有活动的客户端请求。

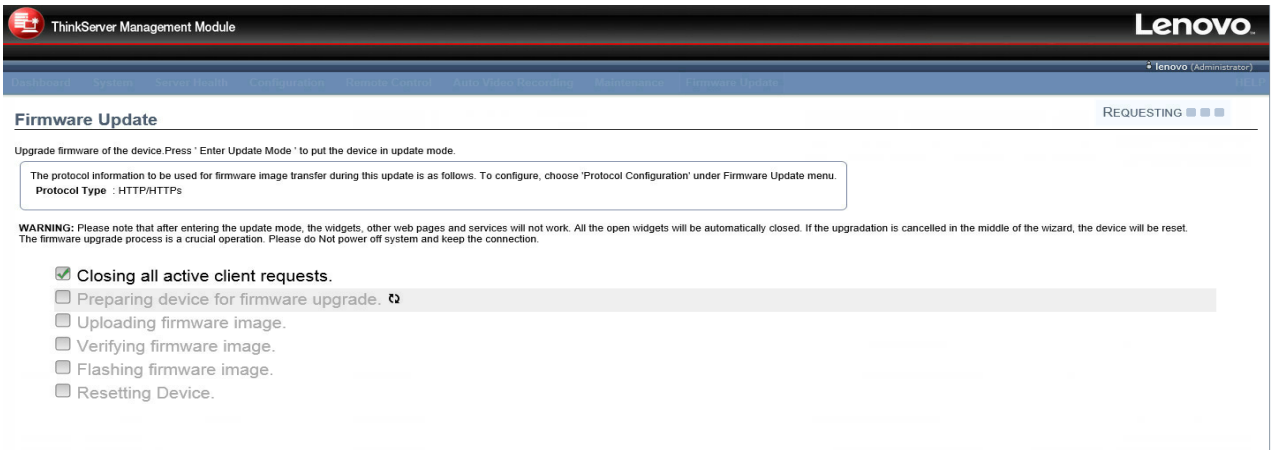
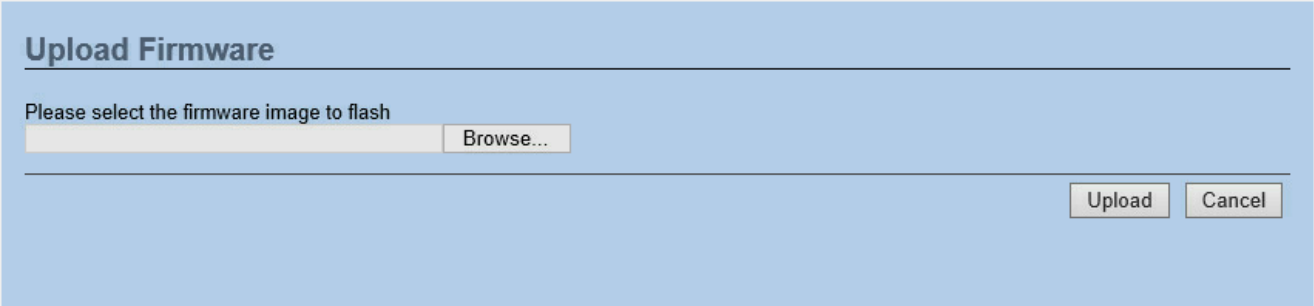



*图 74：固件更新过程*

3. 准备设备固件升级。
4. 上传固件镜像。
5. 浏览和选择要写入的固件镜像，单击 **Upload（上传）**。




6. 验证固件镜像。
7. 刷写固件镜像。
8. 重置设备。

## BIOS Update（BIOS 更新）

该向导包含 BIOS 升级整个过程。升级完成或取消后，自动会出现一个复位可选框。出现是否保留配置选项。要在升级时保留配置，可启用该选项，打开固件更新页面，从菜单栏单击 **Firmware Update（固件更新）> BIOS Update（BIOS 更新）**。BIOS 更新截图示例如下。

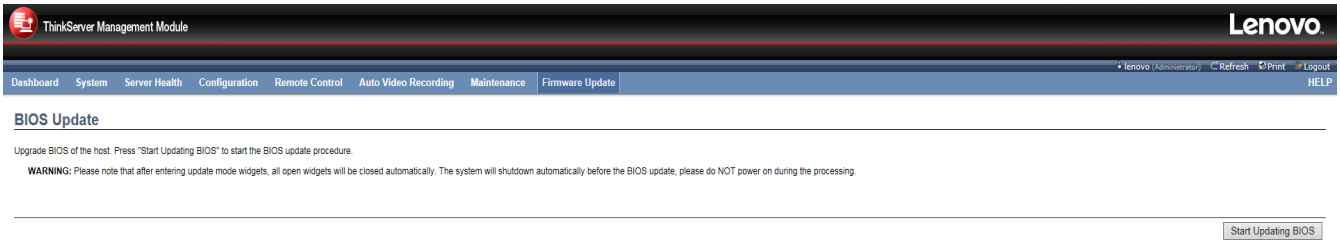



*图 75：BIOS 更新*

- **Start Updating BIOS（开始更新 BIOS）：**单击“Start Updating BIOS（开始更新 BIOS）”升级当前设备 BIOS。

1. 单击“Start Updating BIOS（开始更新 BIOS）”，出现如下截图所示页面。

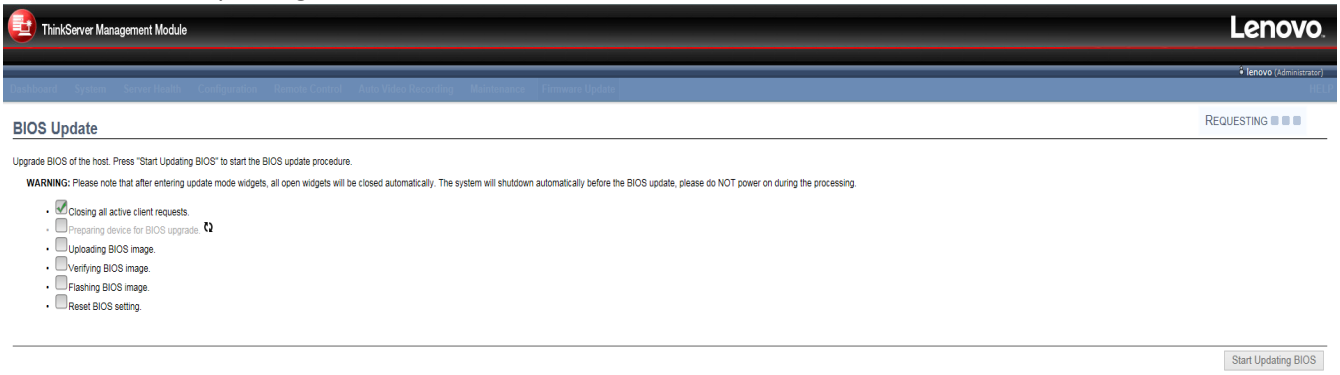



*图 76：开始更新 BIOS 页面*

2. 关闭所有活动的客户端请求。

3. 准备设备固件升级。
4. 上传固件镜像。
5. 浏览和选择要写入的固件镜像，单击 **Upload（上传）**。

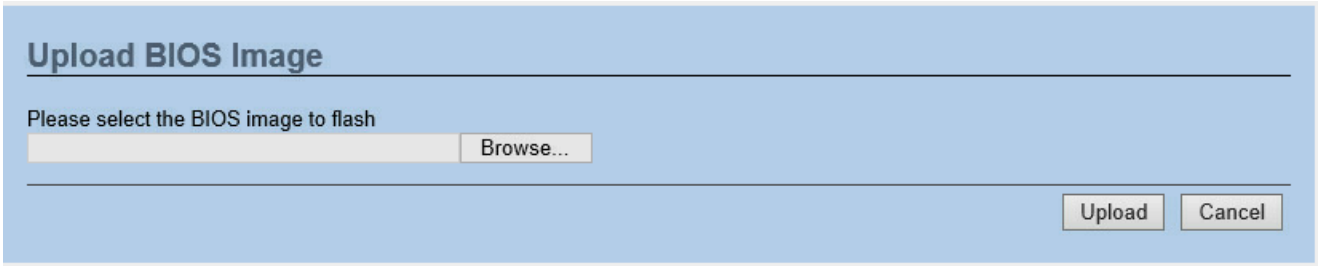



*图 77：上传 BIOS 镜像页面*

6. 验证固件镜像
7. 刷写固件镜像
8. 重置设备

## Protocol Configuration（协议配置）

该页面可用于配置固件镜像协议信息。

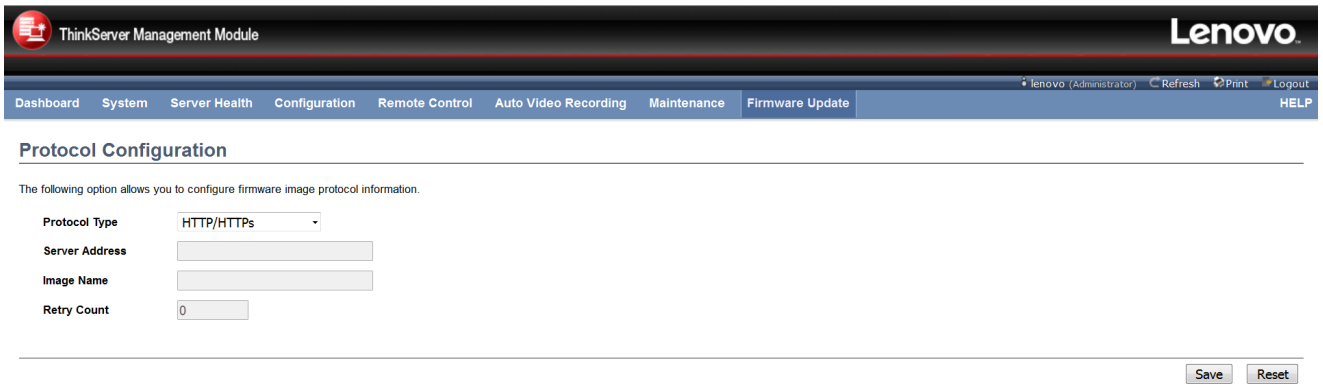



*图 78：图像传输协议*

- **Protocol Type（协议类型）：** 传输固件镜像到 BMC 所用的协议。
- **Server Address（服务器地址）：** 存储固件镜像的服务器地址。它支持 IPv4 和 IPv6。
  - IPv4 地址由 4 组数字组成，由点分隔，如“xxx.xxx.xxx.xxx”。
  - 每一数字范围从 0 到 255。
  - 第一个数字不能为 0。
  - IPv6 地址有 8 组 4 位十六进制数字组成，冒号分隔，如“xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx”。
  - 十六进制数字使用小写字母。
- **Image Name（镜像名称）：** TFTP 服务器上的镜像文件名。
- **Retry Count（重试次数）：** 传输失败发生时重试次数。重试次数范围从 0 到 255。
- **Save（保存）：** 单击“Save（保存）”保存配置设置。
- **Reset（重置）：** 单击 “Reset（重置）”重置修改。

1. 注意组的成员属性应为“成员”。

# 第 6 章 用户权限

本章节介绍 TMM 网页界面的访问权限。

| | | 访问 | 运行 |
|---|---|---|---|
| 仪表板 | | A,O,U,OEM | A |
| 系统 | 库存 | A,O,U,OEM | A,O,U,OEM |
| | FRU 信息 | A,O,U,OEM | A,O,U,OEM |
| 服务器健康 | 传感器读数 | A,O,U,OEM | A,O,OEM |
| | 事件日志 | A,O,U,OEM | A,OEM |
| | BSOD 屏幕 | A,OEM | A,OEM |
| 配置 | 活动目录 | A,O,U,OEM | A,OEM |
| | DNS | A,O,OEM | A,OEM |
| | 事件日志 | A,O,U,OEM | A,OEM |
| | 镜像重定向 | A,O,U,OEM | A,OEM |
| | LDAP/E-Directory | A,O,U,OEM | A,OEM |
| | 鼠标模式 | A,O,U,OEM | A,OEM |
| | 网络 | A,O,OEM | A,OEM |
| | NTP | A,O,U,OEM | A,OEM |
| | PAM 订购 | A,O,U,OEM | A,OEM |
| | PEF | A,O,OEM | A,OEM |
| | RADIUS | A,O,U,OEM | A,OEM |
| | 远程会话 | A,O,U,OEM | A,OEM |
| | 服务 | A,O,U,OEM | A,OEM |
| | 接口 | A,O,OEM | A,OEM |
| | SMTP | A,O,OEM | A,OEM |
| | SNMP | A,O,U,OEM | A,OEM |
| | SSL | A,O,U,OEM | A,OEM |
| | 系统防火墙 | A,O,OEM | A,OEM |
| | 用户 | A,O,OEM | A,OEM |
| | 虚拟媒介 | A,O,U,OEM | A,OEM |
| | 加密算法 | A,O,OEM | A,OEM |
| 远程控制 | 控制台重定向 | A,O,U,OEM | A |
| | 服务器电源控制 | A,O,U,OEM | A,OEM |
| | Java SOL | A,O,U,OEM | A |
| 自动视频录制 | 触发配置 | A,O,OEM | A,OEM |
| | 录制的视频 | A,O,U,OEM | A,OEM |
| 维护 | 保留配置 | A,O,U,OEM | A,OEM |
| | 恢复配置 | A,OEM | A,OEM |
| 固件更新 | 固件更新 | A,OEM | A,OEM |
| | BIOS 更新 | A,OEM | A,OEM |
| | 协议配置 | A,OEM | A,OEM |

A：Administrator（管理员）

O：Operator（操作员）

U：User（用户）

OEM：OEM Proprietary（OEM 专用）

N：No Access（无访问）

# 附录 A：通知

Lenovo 可能无法为所有国家提供本文档中介绍的产品、服务或功能。请咨询当地 Lenovo 代表，了解所在地区产品和服务信息。对 Lenovo 产品、程序或服务的任何引用并不表明或暗示 Lenovo 产品、程序或服务可用。可能会使用任何功能相似不侵犯 Lenovo 的知识产权的产品、程序或服务。但是，用户负责评估和验证任何其他产品、程序或服务。

本文档中谈及的内容 Lenovo 可能拥有专利或正在申请中的专利。提供本文档并不代表将这些专利许可给您。可以发送许可查询，致信给：

*Lenovo (United States), Inc. 1009*
*Think Place - Building One Morrisville, NC 27560 U.S.A.*
*Attention: Lenovo Director of Licensing*

LENOVO 按“原样”提供本出版物，不承担任何明示或默示担保，包括但不限于以任何特殊目的默示担保无侵权、适销性或适当性。
某些司法管辖区不允许在某些交易中免除明示或默示的保证，因此，本声明可能不适用于您。

此信息可能包括技术不准确或印刷错误。定期对这些信息进行更改; 这些变更将纳入新出版的版本中。Lenovo 可能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，恕不另行通知。

本文档中描述的产品不适用于移植或其他生命支持应用，由此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改变 Lenovo 产品规格或保修条款。本文档中的任何内容均不得作为 Lenovo 或第三方知识产权下的明示或默示许可或者赔偿。本文档中包含的所有信息均在特定环境中获取，只用作说明。在其他操作环境中获得的结果可能会有所不同。

Lenovo 可以使用或分发任何您认为适当的信息，而不会对您承担任何义务。

本出版物中对非 Lenovo 网站的任何引用仅为方便起见提供，不以任何方式作为这些网站的认可。这些网站上的资料不属于 Lenovo 产品的材料，使用这些网站将自行承担风险。

此处包含的任何性能数据均在受控环境中确定。因此，在其他操作环境中获得的结果可能会有很大差异。一些测量可能是在开发级系统上进行，并不能保证这些测量在正式系统上是相同的。
此外，可能通过外推估计某些测量。实际结果可能不同。本文档的用户应对其特定环境的适用数据进行验证。

# 商标

Lenovo、Lenovo 徽标和 ThinkServer 是 Lenovo 在美国和/或其他国家或地区的商标。
Windows 是 Microsoft®集团公司的商标。

其他公司、产品或服务名称可能是其他公司各自的商标或服务标记。