



集成管理模块 II 用户指南





集成管理模块 II 用户指南

目录

表	vii
-------------	-----

第 1 章 简介 1

IMM2 基本级、标准级和高级功能	2
IMM2 Basic 级别功能部件	2
IMM2 Standard 级别功能部件	2
IMM2 Advanced 级别功能部件	3
IMM2 功能部件改进	3
升级 IMM2	3
将 IMM2 与 BladeCenter 高级管理模块配合使用	3
Web 浏览器和操作系统需求	4
本书中使用的声明	6

第 2 章 打开并使用 IMM2 Web 界面 . . . 7

访问 IMM2 Web 界面	7
通过 IBM System x 服务器固件 Setup Utility 设置	
IMM2 网络连接	7
登录到 IMM2	10
IMM2 操作描述	11

第 3 章 IMM2 Web 用户界面概述 . . . 17

Web 会话设置	17
Page Auto Refresh	17
Trespass Message	18
注销	19
System Status 选项卡	20
Events 选项卡	26
Event log	26
Event Recipients	28
Service and Support 选项卡	31
Problems 选项	31
Settings 选项	34
Download Service Data 选项	37
Server Management 选项卡	38
Server Firmware	38
远程控制	43
Server Properties	48
Server Power Actions	52
Cooling Devices	52
Power Modules	53
Disks	54
Memory	54
Processors	56
Server Timeout	57
PXE 网络引导	57
Latest OS Failure Screen	57
IMM Management 选项卡	58

第 4 章 配置 IMM2 59

设置服务器超时	62
更改 IMM2 固件自动升级设置	63

设置 IMM2 日期和时间	64
配置串口设置	66
配置用户帐户	67
用户帐户	67
组概要文件	71
配置全局登录设置	72
常规设置	72
帐户安全策略设置	73
配置网络协议	76
配置以太网设置	76
配置 SNMP 警报设置	78
配置 DNS	80
配置 DDNS	80
配置 SMTP	81
配置 LDAP	81
配置 Telnet	85
配置 USB	86
配置端口分配	87
配置安全性设置	88
配置 HTTPS 协议	88
配置 CIM over HTTPS 协议	89
配置 LDAP 客户机协议	90
配置 Secure Shell 服务器	92
SSL 概述	93
SSL 证书处理	93
SSL 证书管理	93
配置 Cryptography Management	94
复原和修改 IMM 配置	96
重新启动 IMM2	96
将 IMM2 重置为出厂缺省值	97
激活管理密钥	98

第 5 章 监控服务器状态 99

查看系统状态	99
查看系统信息	101
查看服务器运行状况	102
查看硬件运行状况	103

第 6 章 执行 IMM2 任务 107

控制服务器的电源状态	108
远程感知和远程控制功能	109
更新 IMM2 固件和 Java 或 ActiveX applet	109
启用远程感知功能	110
远程控制截屏	110
远程控制 Video Viewer 方式	111
远程控制视频颜色方式	111
远程控制键盘支持	112
远程控制鼠标支持	114
远程电源控制	115
查看性能统计信息	115
启动远程桌面协议	115

Knock-knock 功能部件描述	116
远程磁盘	119
设置 PXE 网络引导	120
更新服务器固件	121
管理系统事件	126
管理事件日志	126
系统事件通知	128
收集服务和支持信息	134
捕获最新操作系统故障屏幕数据	135
管理服务器电源	136
控制电源和总系统电源	137
显示当前已安装的电源	139
显示电源容量	139
显示电源历史记录	139

第 7 章 Features on Demand 141

安装激活密钥	141
除去激活密钥	144
导出激活密钥	145

第 8 章 命令行界面 147

通过 IPMI 管理 IMM2	147
使用 IPMItool	147
访问命令行界面	147
登录到命令行会话	148
配置 serial-to-Telnet 或 SSH 重定向	148
命令语法	148
功能和限制	149
按字母顺序排列的命令列表	150
实用程序命令	152
exit 命令	152
help 命令	152
history 命令	152
监控命令	152
clearlog 命令	153
fans 命令	153
ffdc 命令	153
led 命令	154
readlog 命令	155
syshealth 命令	156
temps 命令	157
volts 命令	157
vpd 命令	158
服务器电源和重新启动控制命令	158
fuelg 命令	158
power 命令	159
pxeboot 命令	161
reset 命令	161
串行重定向命令	162
console 命令	162
配置命令	162
accseccfg 命令	163
alertcfg 命令	164
asu 命令	165
autopromo 命令	168
backup 命令	168

cryptomode 命令	169
dhcpcinfo 命令	169
dns 命令	170
ethtousb 命令	172
gprofile 命令	172
ifconfig 命令	173
keycfg 命令	175
ldap 命令	176
ntp 命令	177
passwordcfg 命令	178
ports 命令	179
portcfg 命令	180
portcontrol 命令	180
restore 命令	181
restoredefaults 命令	182
set 命令	182
smtp 命令	182
snmp 命令	183
snmpalerts 命令	185
srcfg 命令	186
sshcfg 命令	187
ssl 命令	188
sslcfg 命令	189
telnetcfg 命令	191
tls 命令	192
thermal 命令	192
timeouts 命令	192
usbeth 命令	193
users 命令	193
IMM2 控制命令	197
alertentries 命令	197
batch 命令	200
clearcfg 命令	201
clock 命令	201
identify 命令	201
info 命令	202
resetsp 命令	202
spreset 命令	202
Service Advisor 命令	203
autoftp 命令	203
chconfig 命令	203
chlog 命令	205
chmanual 命令	205
events 命令	206
sdemail 命令	206

附录 A. 获取帮助和技术协助 207

在致电请求服务之前	207
使用文档	208
从万维网获取帮助和信息	208
如何向 IBM 发送 DSA 数据	208
创建个性化支持 Web 页面	208
软件服务和支持	208
硬件服务和支持	209
IBM 台湾产品服务	209

附录 B. 声明	211
商标	211
重要声明	212
颗粒污染物	212
文档格式	213
电信规章声明	214
电子辐射声明	214
联邦通信委员会 (FCC) 声明	214
加拿大工业部 A 级辐射规范符合声明	214
Avis de conformité à la réglementation d'Industrie	
Canada.	214

澳大利亚和新西兰 A 级声明	214
欧盟 EMC 指令一致性声明	214
德国 A 级声明	215
日本 VCCI A 级声明	216
韩国通信委员会 (KCC) 声明	216
俄罗斯电磁干扰 (EMI) A 级声明	216
中华人民共和国 A 级电子辐射声明	216
台湾甲类规范符合声明	217
索引	219

表

1. IMM2 操作	11	6. 电源操作和描述	108
2. 服务器电源和运行状态	22	7. Power 命令	159
3. 安全性设置策略值	74	8. ASU 命令	165
4. 许可权位	84	9. 事务命令	167
5. 系统状态描述	100	10. 颗粒和气体的限制	213

第 1 章 简介

集成管理模块 II (IMM2) 服务处理器是第二代集成管理模块 (IMM) 服务处理器，它将服务处理器功能、Super I/O、视频控制器和远程感知功能整合到服务器主板上的一块芯片中。与 IMM 相似，IMM2 对键盘管理控制器 (BMC) 和 Remote Supervisor Adapter II 的组合功能提供了一些改进，其中包括以下功能：

- 可选择专用或共享以太网连接进行系统管理。
- 针对智能平台管理接口 (IPMI) 和服务处理器接口的一个 IP 地址。该功能不适用于 IBM® BladeCenter 刀片服务器。
- Embedded Dynamic System Analysis (DSA)。
- 使用 Advanced Settings Utility (ASU) 进行远程配置。该功能不适用于 IBM BladeCenter 刀片服务器。
- 应用程序和工具能够在频带内或频带外访问 IMM2。在 IBM BladeCenter 刀片服务器上仅支持频带内 IMM2 连接。
- 增强型远程感知功能。该功能不适用于 IBM BladeCenter 刀片服务器。

备注：

- 在 IBM BladeCenter 刀片服务器和某些 System x 服务器上不提供专用系统管理网络端口；对于这些服务器，仅提供 *shared* 设置。
- 对于 IBM BladeCenter 刀片服务器，IBM BladeCenter 高级管理模块是用于系统管理功能和键盘/显示器/鼠标 (KVM) 多路复用的主要管理模块。

IBM System x® Server Firmware 是 IBM 实施的统一扩展固件接口 (UEFI)。它替代了 IBM System X 服务器和 IBM BladeCenter 刀片服务器中的基本输入/输出系统 (BIOS)。BIOS 是控制基本硬件操作（例如，与软盘驱动器、硬盘驱动器和键盘的交互）的标准固件代码。IBM System x Server Firmware 提供了 BIOS 没有的一些功能，包括 UEFI 2.3 合规性、iSCSI 兼容性、Active Energy Manager 技术，以及增强的可靠性和服务功能。Setup Utility 提供服务器信息、服务器设置和定制兼容性，并确定引导设备顺序。

备注：

- 在本文档中，IBM System x Server Firmware 通常称为服务器固件，有时称为 UEFI。
- IBM System x Server Firmware 与非 UEFI 操作系统完全兼容。
- 有关使用 IBM System x Server Firmware 的更多信息，请参阅您的 IBM 服务器随附的文档。

本文档说明如何在 IBM 服务器中使用 IMM2 的功能。IMM2 与 IBM System x Server Firmware 协作，为 System x、BladeCenter 和 IBM Flex System 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 IBM Support Portal 时，必须选择您的存储子系统所对应的产品类别、产品系列和型号。下次访问 IBM Support Portal 时，Web 站点会预先装入您初始选中的产品，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。

IBM Web 站点会定期进行更改。查找固件和文档的过程可能与本文档中描述的过程略有不同。

1. 请转至 <http://www.ibm.com/support/entry/portal>。
2. 在选择产品下，选择浏览产品并展开硬件。
3. 根据您的服务器的类型，单击系统 > **System x** 或系统 > **BladeCenter**，然后选中一个或多个服务器所对应的框。
4. 在选择任务下，单击下载。
5. 在查看结果下，单击查看页面。
6. 在“Flash 和警报”框中，单击适当的下载链接，或单击更多结果以查看其他链接。

IMM2 基本级、标准级和高级功能

对于 IMM2，提供了基本级、标准级和高级 IMM2 功能。请参阅针对您服务器的文档，以获取有关在您的 IBM 服务器中安装的 IMM2 级别的更多信息。所有级别均提供以下功能：

- 全天候远程访问和管理您的服务器
- 远程管理与受管服务器的状态无关
- 远程控制硬件和操作系统

此外，标准级和高级可通过标准 Web 浏览器支持基于 Web 的管理。

注：某些功能可能不适用于 IBM BladeCenter 刀片服务器。

以下是 IMM2 基本级功能的列表：

IMM2 Basic 级别功能部件

以下是 IMM2 Basic 级别功能部件的列表：

- IPMI 2.0 接口
- 温度监控
- 风扇控制
- 指示灯管理
- 服务器电源/重置控制
- 传感器监控
- IPMI 平台事件陷阱警报
- IPMI Serial over LAN

IMM2 Standard 级别功能部件

以下是 IMM2 Standard 级别功能部件的列表：

- 所有 IMM2 Basic 级别功能部件
- 使用标准 Web 浏览器进行基于 Web 的管理
- SNMPv1 和 SNMPv3 接口
- Telnet 和 SSH CLI
- 安排的服务器电源/重置控制

- 可读的事件和审计日志记录
- 系统运行状况指示
- 操作系统装入程序和操作系统看守程序
- LDAP 认证和授权
- SNMP 陷阱、电子邮件、系统日志和 CIM 指示警报
- NTP 时钟同步
- 通过 Telnet/SSH 进行串行控制台重定向

IMM2 Advanced 级别功能部件

以下是 IMM2 Advanced 级别功能部件的列表：

- 所有 IMM2 Basic 和 Standard 级别功能部件
- 远程感知 Java 和 ActivX 客户机：
 - 远程键盘、显示器和鼠标支持
 - 远程介质
 - 卡上的远程磁盘
- 针对操作系统挂起的故障截屏

IMM2 功能部件改进

以下是相对于 IMM，IMM2 功能部件的改进列表：

- 安全性（可信服务处理器）：
 - 安全引导
 - 签名更新
 - IMM2 信任度量核心根
 - 可信平台模块
- 在整个 IBM System x 平台中都一致的权新 Web GUI 设计
- 提高了远程感知视频分辨率和色深
- ActiveX 远程感知客户机
- Ethernet-over-USB 接口升级到 USB 2.0
- 系统日志警报
- 配置更改后无需重置 IMM2

升级 IMM2

如果您的 IBM 服务器随附 Basic 级别或 Standard 级别 IMM2 固件功能，那么您或许能够升级服务器中的 IMM2 功能。有关可用升级级别和如何订购的更多信息，请参阅第 141 页的第 7 章，『Features on Demand』。

将 IMM2 与 BladeCenter 高级管理模块配合使用

BladeCenter 高级管理模块是 IBM BladeCenter 产品中的标准系统管理接口。虽然目前在某些 IBM BladeCenter 刀片服务器中包括了 IMM2，但是针对包括 IBM 刀片服务器的 IBM BladeCenter 产品，该高级管理模块仍然是用于系统管理功能和 KVM 多路复用的管理模块。

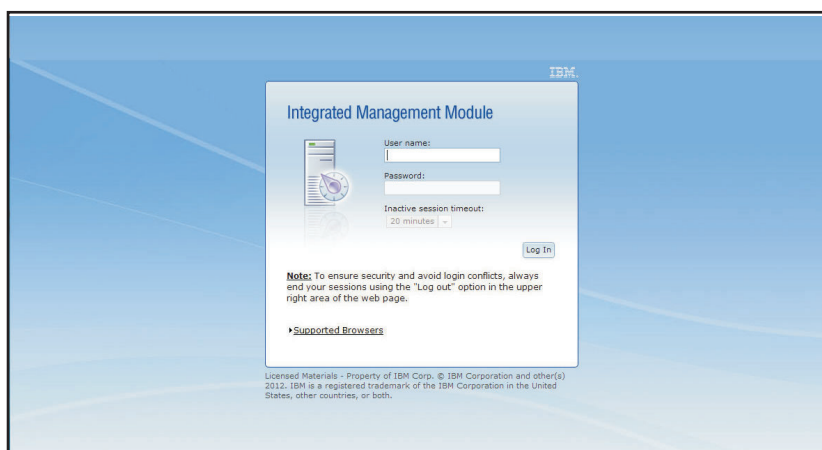
无法通过外部网络访问 IBM BladeCenter 刀片服务器上的 IMM2，必须使用高级管理模块对 IBM BladeCenter 刀片服务器进行远程管理。IMM2 代替了过去在 IBM 刀片服务器产品中提供的 BMC 以及并行键盘、显示器和鼠标 (cKVM) 选件卡的功能。

Web 浏览器和操作系统需求

IMM2 Web 界面需要 Java™ 插件 V1.5 或更高版本（用于远程感知功能），以及以下一个 Web 浏览器：

- Microsoft Internet Explorer V8 到 V10
- Mozilla Firefox V3.6 到 V20
- Chrome V13 到 V26

如果使用较新版本的 Microsoft Internet Explorer，那么建议您使用 Internet Explorer 中的“兼容性视图”来显示 IMM2 Web 页面。上面列出的浏览器与 IMM2 固件当前支持的浏览器匹配。可能会定期增强 IMM2 固件以包含对其他浏览器的支持。下图显示 IMM2 登录屏幕。



根据 IMM2 上固件的版本，支持的 Web 浏览器可能与本部分中所列的浏览器有所不同。要查看当前位于 IMM2 上的固件的受支持浏览器的列表，请单击 IMM2 登录页面中的 **Supported Browsers** 菜单列表（如下图所示）。

Integrated Management Module



User name:

Password:

Inactive session timeout:

20 minutes ▼

Log In

Note: To ensure security and avoid login conflicts, always end your sessions using the "Log out" option in the upper right area of the web page.

▼Supported Browsers

The Firefox browser is recommended for JAWs users.
The IMM2 web interface works with these browsers:

- Internet Explorer 8-10
- Firefox 3.6-20
- Chrome 13-26

The IMM2 Remote Control function works with these client operating systems:

- SLES11
- RHEL5, RHEL6
- Windows XP
- Windows Vista
- Windows 2008
- Windows 7, 8
- Windows 2012

为了提高安全性，现在使用 https 时仅支持高强度密码。使用 https 时，您的客户机操作系统和浏览器的组合必须支持以下密码套件之一：

- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-SHA256
- DHE-RSA-AES256-SHA
- DHE-RSA-CAMELLIA256-SHA
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA
- DHE-RSA-SEED-SHA
- DHE-RSA-CAMELLIA128-SHA
- AES256-GCM-SHA384
- AES256-SHA256
- AES256-SHA
- AES128-GCM-SHA256
- AES128-SHA256

- AES128-SHA
- CAMELLIA256-SHA
- CAMELLIA128-SHA
- EDH-RSA-DES-CBC3-SHA
- DES-CBC3-SHA
- SEED-SHA
- RC4-SHA

IMM2 远程控制功能可用于以下客户机操作系统：

- SUSE Linux Enterprise Server 11 (SLES11)
- Red Hat Enterprise Linux Enterprise 5 (RHEL5)
- Red Hat Enterprise Linux Enterprise 6 (RHEL6)
- Microsoft Windows XP
- Microsoft Windows Vista
- Microsoft Windows 2008
- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 2012

因特网浏览器的高速缓存用于存储您所访问的 Web 页面的信息，便于以后更快速地装入这些信息。对 IMM2 固件进行快速更新后，浏览器可能继续使用其高速缓存中的信息，而不是从 IMM2 进行检索。更新 IMM2 固件后，建议您清除浏览器高速缓存，以确保 IMM2 提供的 Web 页面正确显示。

本书中使用的声明

本文档中使用以下声明：

- 注：这些注意事项提供重要的提示、指导或建议。
- 要点：这些注意事项提供的信息或建议可帮助您避免不便的情况或问题。
- 注意：这些注意事项指出可能对程序、设备或数据造成的损坏。注意事项在可能会发生损坏的说明或情况之前列出。

第 2 章 打开并使用 IMM2 Web 界面

要点：本节不适用于 IBM BladeCenter 和 IBM 刀片服务器。虽然 IMM2 在某些 IBM BladeCenter 产品和 IBM 刀片服务器中是标配，但是针对包括 IBM 刀片服务器的 IBM BladeCenter 产品，IBM BladeCenter 高级管理模块是用于系统管理功能和键盘/显示器/鼠标 (KVM) 多路复用的主要管理模块。希望在刀片服务器上配置 IMM2 设置的用户应该使用刀片服务器上的 Advanced Settings Utility (ASU) 来执行这些操作。

IMM2 将服务处理器功能、视频控制器和远程感知功能（在安装了可选 Virtual Media Key 的情况下）整合在一块芯片中。要使用 IMM2 Web 界面远程访问 IMM2，您必须先登录。本章描述登录过程以及可在 IMM2 Web 界面中执行的操作。

访问 IMM2 Web 界面

IMM2 支持静态和动态主机配置协议 (DHCP) IPv4 寻址。向 IMM2 分配的缺省静态 IPv4 地址是 192.168.70.125。IMM2 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。

IMM2 也支持 IPv6，但是在缺省情况下，IMM2 没有固定的静态 IPv6 IP 地址。在 IPv6 环境中初始访问 IMM2 时，可以使用 IPv4 IP 地址或 IPv6 链路本地地址。IMM2 会生成唯一链路本地 IPv6 地址，该地址显示在 IMM2 Web 界面的 Network Interfaces 页面上。该链路本地 IPv6 地址具有与以下示例相同的格式。

```
fe80::21a:64ff:fee6:4d5
```

当访问 IMM2 时，将以下 IPv6 条件设置为缺省值：

- 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。

IMM2 提供了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的选项。机架安装式和塔式服务器的缺省连接是使用专用系统管理网络接口。

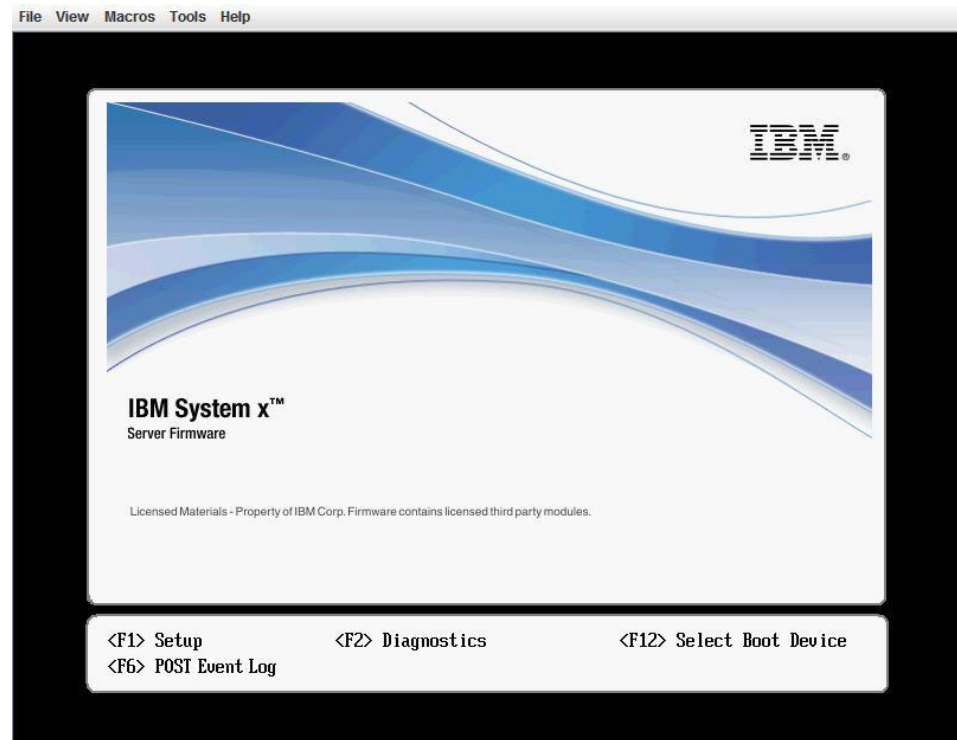
注：专用的系统管理网络端口在您的服务器上可能不可用。如果您的硬件不具有专用网络端口，那么可用的唯一 IMM2 设置是共享设置。

通过 IBM System x 服务器固件 Setup Utility 设置 IMM2 网络连接

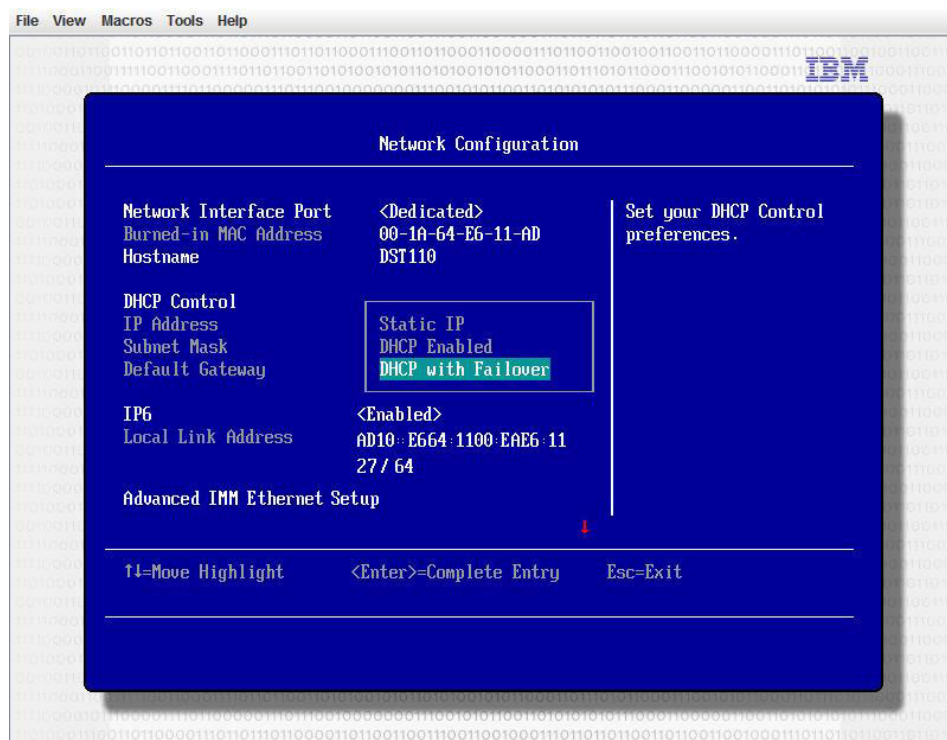
启动服务器后，您可以使用 Setup Utility 来选择 IMM2 网络连接。具有 IMM2 硬件的服务器必须连接到 DHCP 服务器，或者必须将服务器网络配置为使用 IMM2 静态 IP 地址。要通过 Setup Utility 设置 IMM2 网络连接，请完成以下步骤：

1. 开启服务器。此时会显示 IBM System x 服务器固件欢迎屏幕。

注：服务器连接到交流电源大约 90 秒后，电源控制按钮便会激活。



2. 当显示提示 <F1> Setup 时，请按 F1 键。如果您设置了开机密码和管理员密码，那么必须输入管理员密码才能访问完整的 Setup Utility 菜单。
3. 从 Setup Utility 主菜单中，选择 **System Settings**。
4. 在下一个屏幕中，选择 **Integrated Management Module**。
5. 在下一个屏幕中，选择 **Network Configuration**。
6. 突出显示 **DHCP Control**。DHCP Control 字段中有三个 IMM2 网络连接选项：
 - Static IP
 - DHCP Enabled
 - DHCP with Failover (缺省值)



7. 选择其中一个网络连接选项。
8. 如果选择使用静态 IP 地址，那么必须指定 IP 地址、子网掩码和缺省网关。
9. 您也可以使用 Setup Utility 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 IMM2 网络连接。

备注：

- 专用的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 IMM2 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 IMM2 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。

10. 向下滚动并选择 **Save Network Settings**。
11. 退出 Setup Utility。

备注：

- 您必须等待大约 1 分钟以使更改生效，然后服务器固件才再次可运作。
- 您也可以通过 IMM2 Web 界面或命令行界面 (CLI) 来配置 IMM2 网络连接。在 IMM2 Web 界面中，网络接口在 **Network Protocol Properties** 页面（从 **IMM Management** 菜单中选择 **Network**）上进行配置。在 IMM2 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。

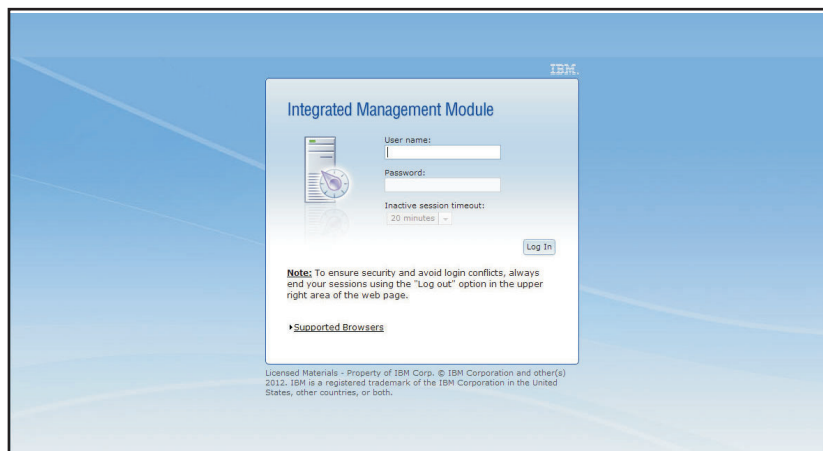
登录到 IMM2

要点：最初设置的 IMM2 用户名为 USERID，密码为 PASSWORD（包含数字零而不是字母 O）。此缺省用户设置具有 Supervisor 访问权。请在初始配置期间更改此用户名和密码以增强安全性。

要通过 IMM2 Web 界面访问 IMM2，请完成以下步骤：

1. 打开 Web 浏览器。在地址或 URL 字段中，输入要连接到的 IMM2 的 IP 地址或主机名。
2. 在 IMM2 Login 窗口中输入您的用户名和密码。如果您是首次使用 IMM2，那么可以从系统管理员处获取用户名和密码。所有登录尝试都记录在事件日志中。根据系统管理员配置用户标识的方式，可能需要输入新密码。

下图中显示了 Login 窗口。

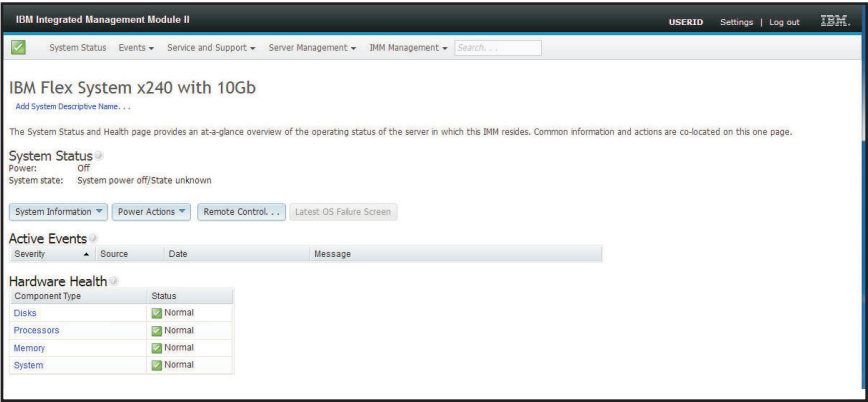


3. 单击 **Log In** 以启动会话。浏览器会打开 **System Status** 页面，如下图所示。通过该页面可以快速查看服务器状态和服务器运行状况摘要。

注：如果在 IMM2 GUI 中时引导至操作系统并且在 **System Status** → **System State** 下显示消息“Booting OS or in unsupported OS”，请禁用 Windows 2008 防火墙或者在 Windows 2008 控制台中输入以下命令。这可能还影响蓝屏捕获功能。

```
netsh firewall set icmpsetting type=8 mode=ENABLE
```

缺省情况下，Windows 防火墙会阻止 icmp 包。当您在 Web 和 CLI 界面中按照上面所指示更改设置后，IMM2 GUI 将更改为“OS booted”状态。



有关可以通过 IMM2 Web 界面顶部选项卡执行的操作的描述，请参阅『IMM2 操作描述』。

IMM2 操作描述

浏览至 IMM2 窗口顶部，以通过 IMM2 执行活动。标题栏标识已登录的用户名。通过标题栏，可以针对状态屏幕刷新率和定制入侵消息配置 **Settings**，并对 IMM2 Web 界面执行 **Log out**，如下图所示。标题栏下方是可用于访问各种 IMM2 功能的选项卡，如表 1 中所列。

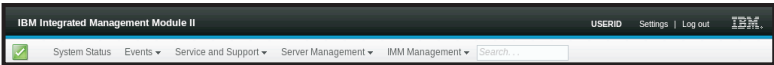


表 1. IMM2 操作

选项卡	选择	描述
System Status		通过 System Status 页面，可以查看系统状态、活动系统事件和硬件运行状况信息。它提供 Server Management 选项卡的 System Information、Server Power Actions 和 Remote Control 功能的快速链接，并使您能够查看最近操作系统故障截屏的图像。请参阅第 20 页的『System Status 选项卡』和第 99 页的『查看系统状态』，以获取其他信息。

表 1. IMM2 操作 (续)

选项卡	选择	描述
Events	Event Log	Event Log 页面显示 IMM2 事件日志中当前存储的条目。该日志包含所报告的系统事件的文本描述，其中包括有关所有远程访问尝试和配置更改的信息。日志中的所有事件都使用 IMM2 日期和时间设置添加了时间戳记。某些事件还生成警报（如果它们的配置如此）。您可以排序和过滤事件日志中的事件，并将其导出至文本文件。请参阅第 26 页的『Events 选项卡』和第 126 页的『管理事件日志』，以获取其他信息。
	Event Recipients	通过 Event Recipients 页面，可以管理将收到系统事件通知的人员。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，以验证通知功能操作。请参阅第 28 页的『Event Recipients』和第 128 页的『系统事件通知』，以获取其他信息。
Service and Support	Problems	Problems 页面允许您查看当前未解决而 Support Center 可维护的问题。您还可以查看与其解决办法相关的每个问题的状态。请参阅第 31 页的『Problems 选项』，以获取其他信息。
	Settings	Settings 页面配置您的服务器以监控和报告服务事件。请参阅第 34 页的『Settings 选项』，以获取其他信息。
	Download Service Data	Download Service Data 页面用于创建信息的压缩文件，IBM 支持人员可使用该文件为您提供帮助。请参阅第 37 页的『Download Service Data 选项』和第 134 页的『收集服务和支持信息』，以获取其他信息。

表 1. IMM2 操作 (续)

选项卡	选择	描述
Server Management	Server Firmware	Server Firmware 页面显示固件级别，并允许您更新 IMM2 固件、服务器固件和 DSA 固件。请参阅第 38 页的『Server Firmware』和第 121 页的『更新服务器固件』，以获取其他信息。
	Remote Control	通过 Remote Control 页面，可以在操作系统级别控制服务器。可通过该页面访问“远程磁盘”和“远程控制台”功能。您可以通过计算机查看和操作服务器控制台，并且可以将某个计算机驱动器（如 CD-ROM 驱动器或软盘驱动器）安装在服务器上。当您安装了磁盘后，您可以使用该磁盘来重新启动服务器并更新服务器上的固件。已安装的盘显示为连接到服务器的 USB 盘驱动器。请参阅第 43 页的『远程控制』和第 109 页的『远程感知和远程控制功能』，以获取其他信息。
	Server Properties	Server Properties 页面提供对服务器的各种属性、状况和设置的访问。Server Properties 页面提供以下选项： • General Settings 选项卡显示操作和支持人员用于识别系统的信息。 • LEDs 选项卡显示所有系统指示灯的状态。通过它还可更改位置指示灯的状态。 • Hardware Information 选项卡显示服务器重要产品数据 (VPD)。IMM2 将收集服务器信息、服务器组件信息和网络硬件信息。 • Environmentals 选项卡显示服务器及其组件的电压和温度信息。 • Hardware Activity 选项卡显示已向系统中添加或从中除去的现场可更换部件 (FRU) 组件的历史记录。 请参阅第 48 页的『Server Properties』，以获取其他信息。
	Cooling Devices	Cooling Devices 页面显示服务器中散热风扇的当前速度和状态。请参阅第 52 页的『Cooling Devices』，以获取其他信息。
	Power Modules	Power Modules 页面显示系统中的电源模块以及状态和额定功率。请参阅第 53 页的『Power Modules』，以获取其他信息。
	Server Power Actions	Server Power Actions 页面通过开机、关机和重新启动操作提供对服务器的完全远程电源控制。请参阅第 52 页的『Server Power Actions』和第 108 页的『控制服务器的电源状态』，以获取其他信息。
	Disks	Hard Disks 页面显示服务器中硬盘驱动器的状态。您可以单击驱动器名称，以显示该硬盘驱动器的活动事件。请参阅第 54 页的『Disks』，以获取其他信息。
	Memory	Memory 页面显示系统中可用的内存条及其状态、类型和容量。您可以单击内存条名称，以显示其事件和其他硬件信息。如果卸下或更换双列直插式内存条 (DIMM)，那么在卸下或更换后服务器至少要开机一次，以显示正确的内存信息。请参阅第 54 页的『Memory』，以获取其他信息。

表 1. IMM2 操作 (续)

选项卡	选择	描述
Server Management (续)	Processors	CPU _s 页面显示系统中的微处理器及其状态和时钟速度。您可以单击微处理器名称，以显示该微处理器的事件和其他硬件信息。请参阅第 56 页的『Processors』，以获取其他信息。
	Server Timeouts	通过 Server Timeouts 页面，可以管理服务器启动超时，以检测发生的服务器挂起事件并从中恢复。请参阅第 57 页的『Server Timeout』和第 62 页的『设置服务器超时』，以获取其他信息。
	PXE Network Boot	通过 PXE Network Boot 页面，可以更改下次重新启动时的主机服务器启动（引导）顺序，以尝试预引导执行环境 (PXE)/动态主机配置协议 (DHCP) 网络启动。仅当主机未处于特权访问保护 (PAP) 之下时，主机启动顺序才会更改。请参阅第 57 页的『PXE 网络引导』和第 120 页的『设置 PXE 网络引导』，以获取其他信息。
	Latest OS Failure Screen	Latest OS Failure Screen 页面显示服务器上最新操作系统故障的屏幕图像（可用时）。为了使 IMM2 能够捕获操作系统故障屏幕，必须启用操作系统看守程序。请参阅第 57 页的『Latest OS Failure Screen』和第 135 页的『捕获最新操作系统故障屏幕数据』，以获取其他信息。
	Power Management	Server Power Management 页面允许您管理与电源相关的策略和硬件，并包含服务器使用的电量的历史记录。请参阅第 136 页的『管理服务器电源』，以获取其他信息。
IMM Management (在下一页继续)	IMM Properties	IMM Properties 页面提供对 IMM2 的各种属性和设置的访问。IMM Properties 页面提供以下选项： • Firmware 选项卡提供指向 Server Management 的 Server Firmware 部分的链接。您还可以通过此选项卡对 IMM2 备份固件启用自动升级。 • 通过 IMM Date and Time Settings 选项卡，可以查看和配置 IMM2 的日期和时间设置。 • Serial Port 选项卡用于配置 IMM2 串口设置。这些设置包括串口重定向功能所使用的串口波特率，以及用于在串行重定向和 CLI 方式之间切换的键序列。 请参阅第 59 页的第 4 章，『配置 IMM2』，以获取其他信息。
	Users	Users 页面用于配置 IMM2 登录概要文件和全局登录设置。您还可以查看当前登录到 IMM2 的用户帐户。全局登录设置包括启用轻量级目录访问协议 (LDAP) 服务器认证、设置 Web 不活动超时，以及定制帐户安全设置。请参阅第 67 页的『配置用户帐户』，以获取其他信息。

表 1. IMM2 操作 (续)

选项卡	选择	描述
IMM Management (续)	Network	Network Protocol Properties 页面提供对 IMM2 的联网属性、状态和设置的访问： • Ethernet 选项卡管理 IMM2 使用以太网进行通信的方式。 • SNMP 选项卡用于配置 SNMPv1 和 SNMPv3 代理。 • DNS 选项卡配置与 IMM2 交互的 DNS 服务器。 • DDNS 选项卡启用或禁用以及配置 IMM2 的动态 DNS。 • SMTP 选项卡配置用于通过电子邮件发送的警报的 SMTP 服务器信息。 • LDAP 选项卡配置用于一个或多个 LDAP 服务器的用户认证。 • Telnet 选项卡管理对 IMM2 的 Telnet 访问。 • USB 选项卡控制用于在服务器和 IMM2 之间进行频带内通信的 USB 接口。这些设置不影响 USB 远程控制功能（键盘、鼠标和海量存储器）。 • 通过 Port Assignments 选项卡，可以更改 IMM2 上某些服务使用的端口号。 请参阅第 76 页的『配置网络协议』，以获取其他信息。
	Security	IMM Security 页面提供对 IMM2 的安全性属性、状态和设置的访问： • 通过 HTTPS Server 选项卡，可以启用或禁用 HTTPS 服务器并管理其证书。 • 通过 CIM Over HTTPS 选项卡，可以启用或禁用 CIM over HTTPS 并管理其证书。 • 通过 LDAP Client 选项卡，可以启用或禁用 LDAP 安全性并管理其证书。 • 通过 SSH Server 选项卡，可以启用或禁用 SSH 服务器并管理其证书。 请参阅第 88 页的『配置安全性设置』，以获取其他信息。
	IMM Configuration	IMM Configuration 页面显示当前 IMM2 配置设置的摘要。请参阅第 96 页的『复原和修改 IMM 配置』，以获取其他信息。
	Restart IMM	通过 Restart IMM 页面，可以重置 IMM2。请参阅第 96 页的『重新启动 IMM2』，以获取其他信息。
	Reset IMM to factory defaults...	通过 Reset IMM to factory defaults... 页面，可以将 IMM2 的配置重置为出厂缺省值。请参阅第 97 页的『将 IMM2 重置为出厂缺省值』，以获取其他信息。 警告： 单击 Reset IMM to factory defaults... 时，对 IMM2 进行的所有修改都会丢失。
	Activation Key Management	通过 Activation Key Management 页面，可以管理可选 IMM2 或服务器 Features on Demand (FoD) 功能部件的激活密钥。请参阅第 98 页的『激活管理密钥』，以获取其他信息。

第 3 章 IMM2 Web 用户界面概述

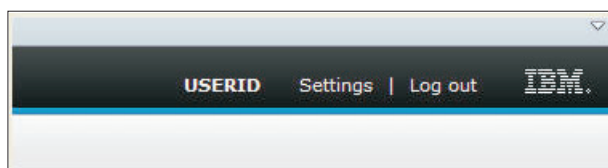
本章提供如何使用 IMM2 Web 用户界面功能部件的概述。

要点：本节不适用于 IBM BladeCenter 和 IBM 刀片服务器。虽然 IMM2 在某些 IBM BladeCenter 产品和 IBM 刀片服务器中是标配，但是 IBM BladeCenter 高级管理模块是用于系统管理功能的主要管理模块。希望在刀片服务器上配置 IMM2 设置的用户应该使用刀片服务器上的 Advanced Settings Utility (ASU) 来执行这些操作。

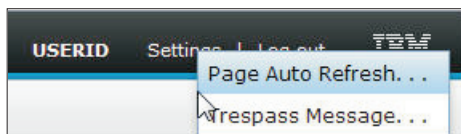
Web 会话设置

此部分提供有关 Web 界面会话主页的设置的信息。

IMM2 主页在 Web 页面的右上方显示菜单选项。通过这些菜单项，可以配置 Web 页面刷新行为以及在用户输入其凭证以登录时向用户显示的消息。下图显示 Web 页面右上方的菜单选项。

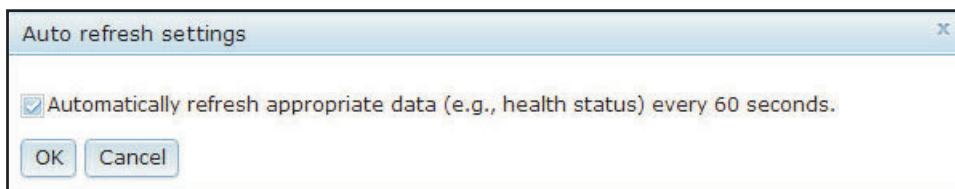


单击 **Settings** 项，然后将显示以下菜单选项：



Page Auto Refresh

使用 Web 会话页面右上方 Settings 菜单项下的 **Page Auto Refresh** 选项，以将页面内容设置为每 60 秒自动刷新一次。要将页面内容设置为每 60 秒刷新一次，请选中 **Automatically refresh appropriate data...** 复选框，然后按 **OK**。要禁用自动页面刷新，请取消选中该复选框，然后按 **OK**。下图显示 Auto refresh settings 窗口。



即使未选中自动刷新复选框，也会自动刷新一些 IMM2 Web 页面。自动刷新的 IMM2 Web 页面如下：

- **System Status：**

系统和电源状态每三秒自动刷新一次。

- **Server Power Actions：**（位于 Server Management 选项卡下）：

电源状态每三秒自动刷新一次。

- **Remote Control：**（位于 Server Management 选项卡下）：

Start remote control... 按钮每秒自动刷新一次。Session List 表每 60 秒刷新一次。

备注：

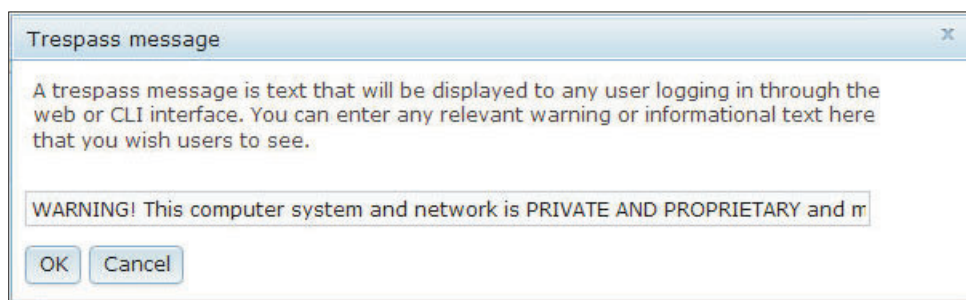
- 如果从 Web 浏览器浏览至自动刷新的 Web 页面，那么不活动超时将自动结束 Web 会话。
- 如果使用 Server Management 下的 Remote Control 选项页面向远程控制用户发送请求，那么无论在从远程控制用户收到响应或者远程控制用户超时之前浏览至哪个 Web 页面，Web 会话都不会超时。当来自远程控制用户的请求完成处理时，不活动超时功能将恢复。

注：前述备注适用于所有 Web 页面。

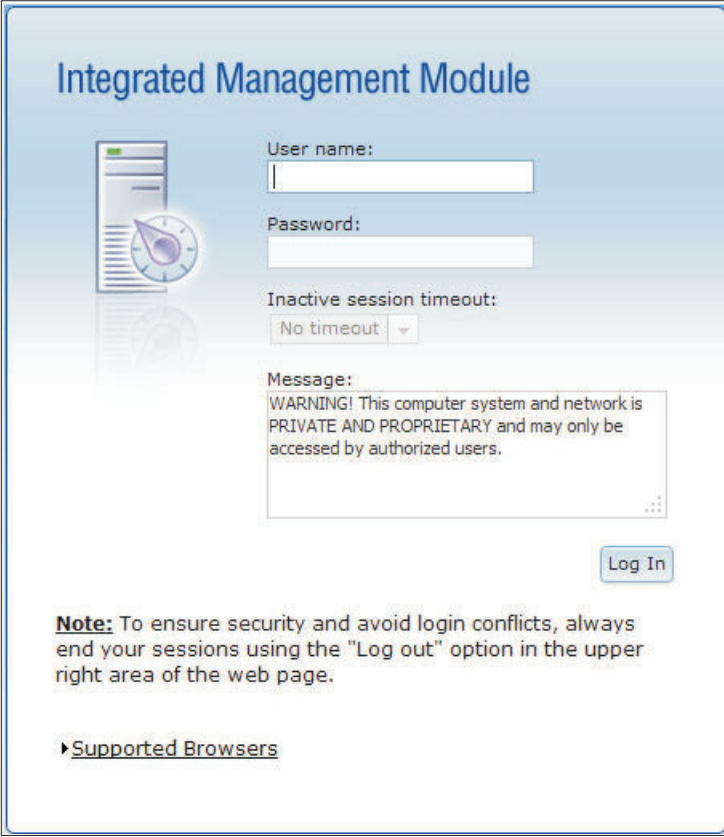
- IMM2 固件最多支持六个同时 Web 会话。要为用户释放会话，请在完成时注销 Web 会话，而不是等待不活动超时以自动关闭会话。如果在处于自动刷新的 IMM2 Web 页面上时退出浏览器，那么 Web 会话将不会由于不活动而自动关闭。

Trespass Message

使用 Web 会话页面右上方 Settings 菜单项下的 **Trespass Message** 选项，以设置您希望用户登录到 IMM2 服务器时显示的消息。当选择 Trespass Message 选项时，会显示以下屏幕。在提供的字段中输入您希望向用户显示的消息文本，然后按 **OK**。



当用户登录时，在 IMM2 登录页面的 Message 区域中将显示消息文本，如下图中所示。



Integrated Management Module

User name:

Password:

Inactive session timeout:
No timeout ▼

Message:
WARNING! This computer system and network is PRIVATE AND PROPRIETARY and may only be accessed by authorized users.

Log In

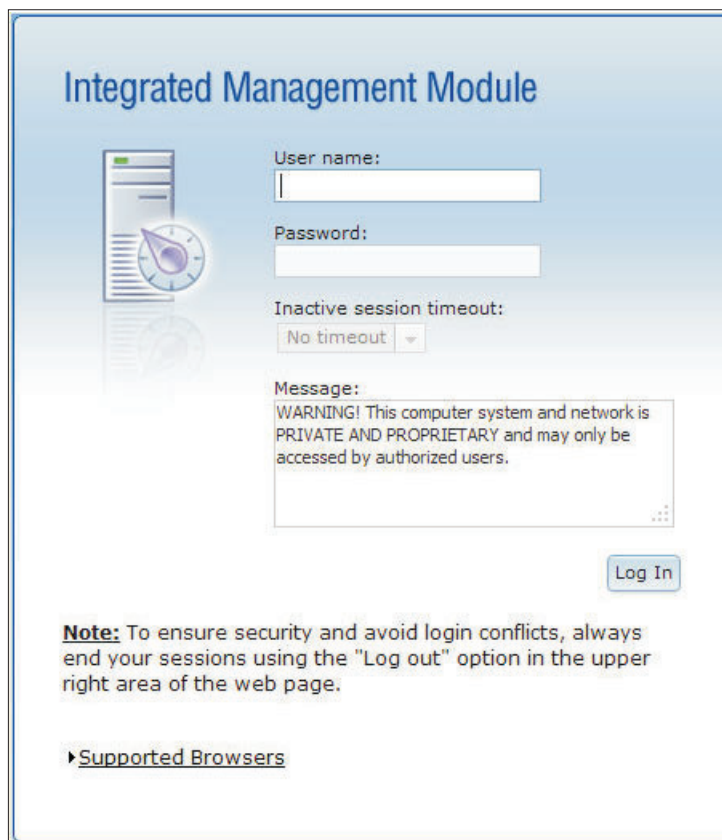
Note: To ensure security and avoid login conflicts, always end your sessions using the "Log out" option in the upper right area of the web page.

► [Supported Browsers](#)

注销

为确保安全性，请在完成时注销 IMM2 Web 会话，并手动关闭可能打开的任何其他 IMM2 Web 浏览器窗口。

要注销 Web 会话，请单击 Web 页面右上方区域中的 **Log out**。将显示 Login 窗口。



Integrated Management Module



User name:

Password:

Inactive session timeout:
No timeout ▼

Message:
WARNING! This computer system and network is PRIVATE AND PROPRIETARY and may only be accessed by authorized users.

[Log In](#)

Note: To ensure security and avoid login conflicts, always end your sessions using the "Log out" option in the upper right area of the web page.

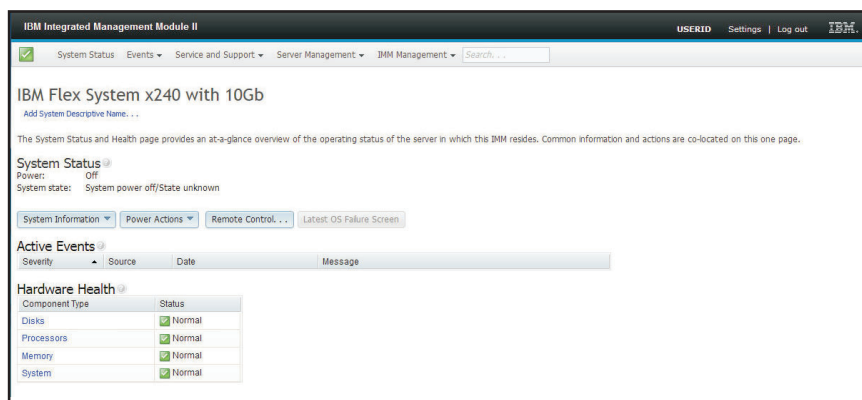
► [Supported Browsers](#)

注：IMM2 固件最多支持六个同时 Web 会话。要为用户释放会话，请在完成时注销 Web 会话，而不是等待不活动超时以自动关闭会话。如果在处于自动刷新的 IMM2 Web 页面上时退出浏览器，那么 Web 会话将不会由于不活动而自动关闭。

System Status 选项卡

此部分提供有关使用 IMM2 Web 用户界面上 System Status 选项卡下选项的信息。

在您登录到 IMM2 Web 用户界面后或单击 **System Status** 选项卡时，会显示 System Status 页面。在 System Status 页面中，可以查看系统状态、活动系统事件和硬件运行状况信息。单击 System Status 选项卡或登录到 IMM2 Web 界面时，将打开以下窗口。



IBM Integrated Management Module II

USERID Settings Log out IBM

System Status Events Service and Support Server Management IMM Management Search...

IBM Flex System x240 with 10Gb

Add System Descriptive Name...

The System Status and Health page provides an at-a-glance overview of the operating status of the server in which the IMM resides. Common information and actions are co-located on this one page.

System Status

Power: Off
System state: System power off/State unknown

System Information Power Actions Remote Control... Latest OS Failure Screen

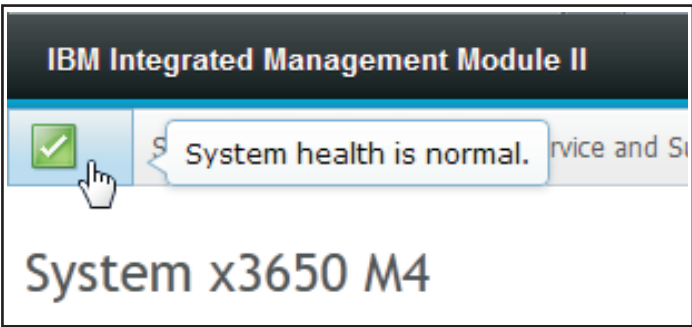
Active Events

Severity	Source	Date	Message

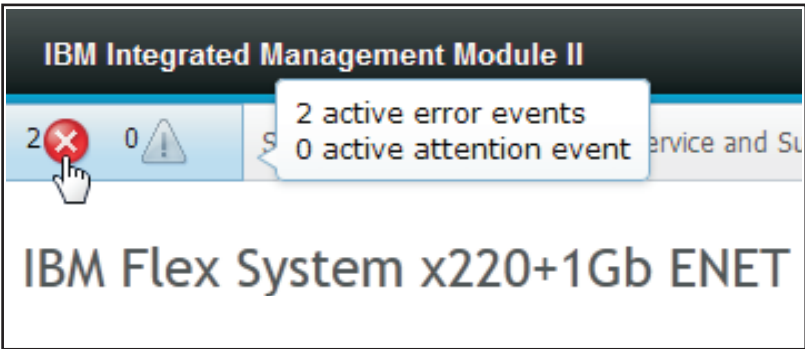
Hardware Health

Component Type	Status
Disks	Normal
Processors	Normal
Memory	Normal
System	Normal

您可以单击页面左上角的绿色图标（带有复选标记），以获取服务器运行状况的快速摘要。复选标记指示服务器在正常运行。



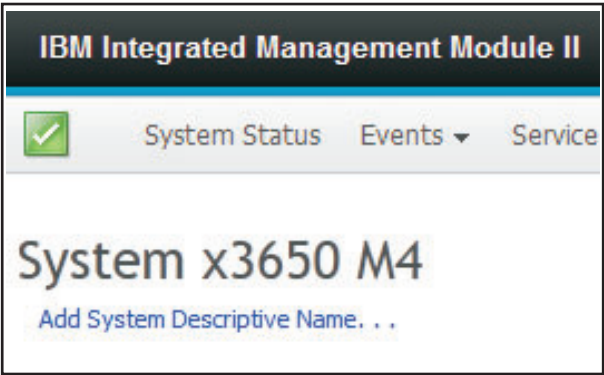
如果显示了红色圆形或黄色三角形图标，表明存在错误或警告情况，如下图中所示。



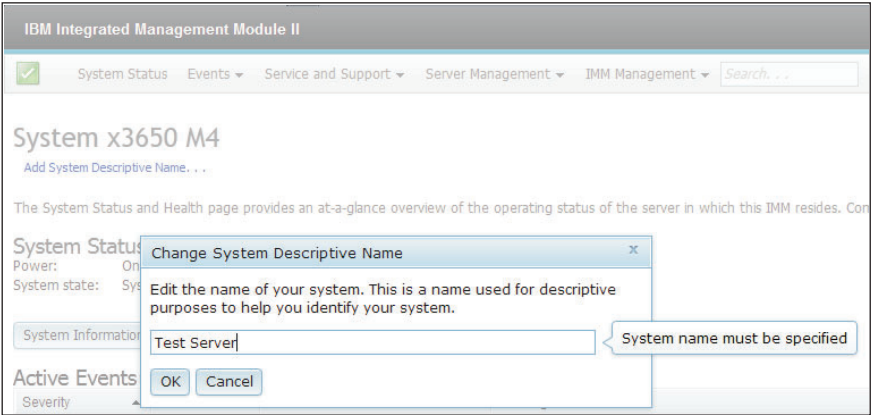
红色圆形图标指示服务器上存在错误情况。黄色三角形图标指示存在警告情况。当显示了红色圆形或黄色三角形图标时，在 System Status 页面上的 Active Events 部分下会列出与该情况关联的事件，如下图中所示。

Active Events			
Severity	Source	Date	Message
Error	System	16 Jul 2012 01:00:28.000 PM	Sensor Mezz Exp 2 Fault has transitioned to critical from a less severe state.
Error	System	16 Jul 2012 01:00:29.000 PM	Sensor Mezz Exp 2 Fault has transitioned to critical from a less severe state.

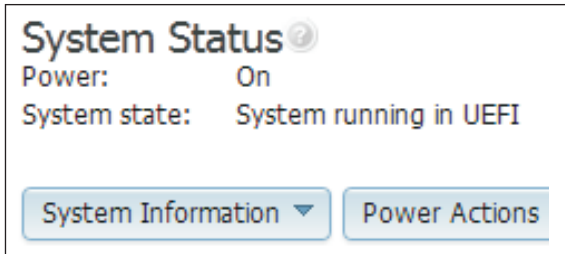
您可以向 IMM2 服务器中添加描述性名称来帮助区分 IMM2 服务器。要向 IMM2 服务器指定描述性名称，请单击位于服务器产品名称下方的 **Add System Descriptive Name...** 链接。



单击 **Add System Descriptive Name...** 链接时，将打开以下窗口，以使您指定要与 IMM2 服务器关联的名称。您可以随时更改系统描述性名称。



System Status 页面上的 **System Status** 部分提供服务器电源状态和服务器的运行状态。所显示的状态是 System Status 页面打开时的服务器状态（如下图中所示）。



服务器可以是下表中所描述的其中一种状态：

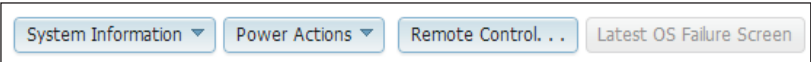
表 2. 服务器电源和运行状态

服务器状态	描述
系统电源关闭/状态未知	服务器已关闭。
系统开启/正在启动 UEFI	服务器已开机，但 UEFI 未在运行。
系统正在 UEFI 中运行	服务器已开机，并且 UEFI 正在运行。

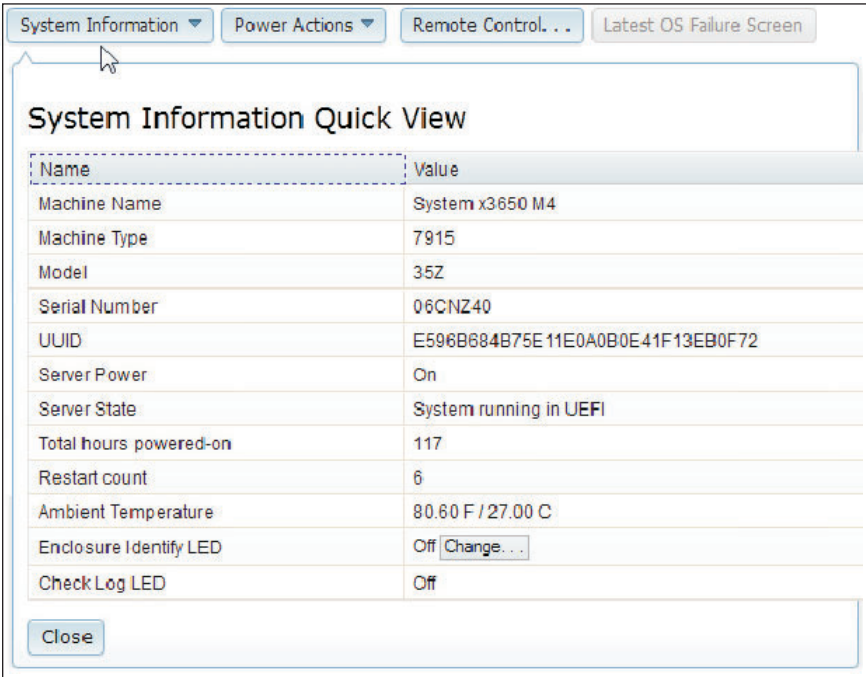
表 2. 服务器电源和运行状态 (续)

服务器状态	描述
系统在 UEFI 中已停止	服务器已开机；UEFI 检测到问题并已停止运行。
正在引导操作系统或处于不受支持的操作系统中	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，但操作系统尚未在运行。 • IMM2 Ethernet over USB 接口已禁用。 • 操作系统未装入支持 Ethernet over USB 接口的驱动程序。 • 操作系统可能正在运行防火墙；因此，阻止与 IMM2 的通信。
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。

System Status 页面还为 **System Information**、**Power Actions**、**Remote Control** 和 **Latest OS Failure Screen** 提供选项卡。



单击 **System Information** 选项卡以查看有关服务器的信息



单击 **Power Actions** 选项卡以查看可执行的操作，从而通过开机、关机和重新启动操作来获取对服务器的完全远程电源控制。请参阅第 108 页的『控制服务器的电源状态』以获取有关如何远程控制服务器电源的详细信息。

单击 **Remote Control** 选项卡以获取有关如何在操作系统级别控制服务器的信息。请参阅第 109 页的『远程感知和远程控制功能』以获取有关远程控制功能的详细信息。

单击 **Latest OS Failure Screen** 选项卡以获取有关如何捕获最新操作系统故障屏幕数据的信息。请参阅第 135 页的『捕获最新操作系统故障屏幕数据』以获取有关 Latest OS Failure Screen 的详细信息。

System Status 页面的 **Hardware Health** 部分下是一个表，其中列出了受监控的硬件组件及其运行状态。针对组件显示的状态可能反映该表中 Component Type 列中组件的最关键状态。例如，服务器可能安装有若干电源模块，并且除一个电源模块外，所有其他电源模块都在正常运行。由于这一个电源模块，该表中 Power Modules 组件的状态将是 Critical（如下图所示）。

Hardware Health ?	
Component Type	Status
Cooling Devices	✓ Normal
Power Modules	✗ Critical
Disks	✓ Normal
Processors	✓ Normal
Memory	✓ Normal
System	✓ Normal

每个组件类型都是可单击以获取更详细信息的链接。单击组件类型时，会显示一个表，其中列出了每个个别组件的状态（如下图所示）。

Memory			
Display the memory modules available on the server. Clicking on a module displays a Properties pop-up window with 2 tabs: Eve			
FRU Name	Status	Type	Capacity (GB)
DIMM 4	✓ Normal	DDR3	4
DIMM 9	✓ Normal	DDR3	4
DIMM 16	✓ Normal	DDR3	4
DIMM 21	✓ Normal	DDR3	4

您可以单击表的 FRU Name 列中的组件，以获取该组件的其他信息。将显示该组件的所有活动事件。

Properties for DIMM 4

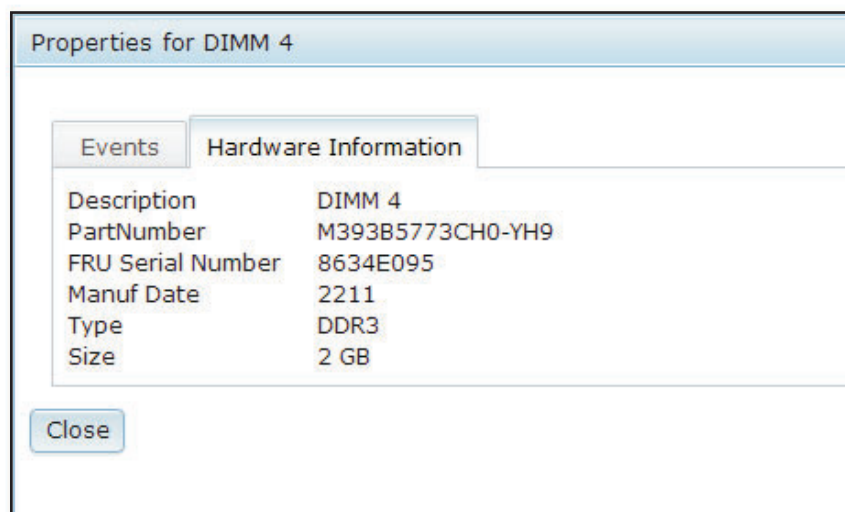
Events

Hardware Information

There are no active events for this device

Close

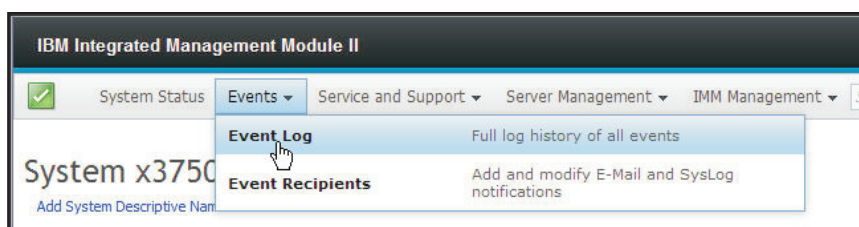
单击 **Hardware Information** 选项卡以获取有关组件的详细信息。



Events 选项卡

此部分提供有关使用 IMM2 Web 用户界面上 Events 选项卡下选项的信息。

通过 **Events** 选项卡下的选项，可以管理 Event Log 历史记录以及电子邮件和系统日志通知的 Event Recipients。下图显示 IMM2 Web 页面上 Events 选项卡下的选项。



Event log

选择 Events 选项卡下的 **Event Log** 以显示 Event Log 页面。Event Log 页面显示由 IMM2 报告的事件的严重性，以及有关所有远程访问尝试和配置更改的信息。日志中的所有事件都使用 IMM2 日期和时间设置添加了时间戳记。某些事件还会生成警报（如果在 Event Recipients 页面上对其进行了该配置）。您可以对事件日志中的事件进行排序和过滤。以下是 Event Log 页面的插图。

Event Log
This page displays the contents of the IMM event log, and allows you to sort and filter the log. By default the log entries are displayed in reverse chronological order (most recent log entry first displayed along with a timestamp, source and a text mess. . . more. . .

Filters: [Icons] Time: All Dates Search Events Go

Severity	Source	Date	Event ID	Message
0 of 51 items filtered 0 items selected Clear filter Applied filters: Events [Error Warning Information Audit]				
Informational	System	31 1 2013 09:02:42.771 AM	0x4000000e00000000	Remote Login Successful. Login ID: USERID from webguis at IP address 9.111.29.57.
Informational	System	31 1 2013 09:01:00.297 AM	0x4000001600000000	ENETICIM ep1 DHCP+HSTN=IMM2-5cae8b4e83cd DN=cn.ibm.com IP@=9.186.166.78 SN=255.255.255.128. GVI@=9.186.166.1 DNS1@=9.0.148.50
Informational	System	31 1 2013 09:00:58.957 AM	0x4000001900000000	LAN: Ethernet(BM.ep2) interface is now active.
Informational	System	31 1 2013 09:00:55.004 AM	0x4000001700000000	ENETICIM ep2 IP-Cfg.HstName=IMM2-5cae8b4e83cd IP@=100.254.95.119 NetMask=255.255.0.0 GVI@=0.0.0.0
Informational	System	31 1 2013 09:00:53.403 AM	0x4000003700000000	ENETICIM ep1 IPv6-LinkLocal-HstName=IMM2-5cae8b4e83cd IP@fe80: 6eae 80ff fe4e 83cd Pref=54
Informational	System	31 1 2013 09:00:51.592 AM	0x4000001900000000	LAN: Ethernet(BM.ep1) interface is now active.
Informational	System	31 1 2013 09:00:47.068 AM	0x4000001000000000	Management Controller SN# 05K3KL9 Network Initialization Complete.
Informational	System	31 1 2013 09:00:02.874 AM	0x800801282101fff	Device Low Security Jump has been added.
Informational	Power	31 1 2013 09:00:02.304 AM	0x800800091301fff	Host Power has been turned off.
Informational	System	31 1 2013 08:55:11.252 AM	0x4000001500000000	Management Controller SN# 05K3KL9 reset was initiated by user USERID.
Informational	System	31 1 2013 08:47:59.118 AM	0x4000002300000000	Flash of SN# 05K3KL9 from (SN# 9.186.166.119) succeeded for user USERID.
Informational	System	31 1 2013 08:43:15.666 AM	0x4000000e00000000	Remote Login Successful. Login ID: USERID from webguis at IP address 9.186.166.119.
Informational	System	31 1 2013 08:43:15.666 AM	0x4000000e00000000	Remote Login Successful. Login ID: USERID from webguis at IP address 9.111.29.57.

要对事件日志中的事件进行排序和过滤，请选择列标题（如下图所示）。

Severity	Source	Date	Event ID	Message
0 of 52 items filtered 0 items selected Clear filter Applied filters: Events [Error Warning Information Audit]				
Informational	System	31 Jan 2013 09:11:04.024 AM	0x4000000e00000000	Remote Login Successful. Login ID: USERID from webguis at IP address 9.186.166.119.
Informational	System	31 Jan 2013 09:02:42.771 AM	0x4000000e00000000	Remote Login Successful. Login ID: USERID from webguis at IP address 9.111.29.57.

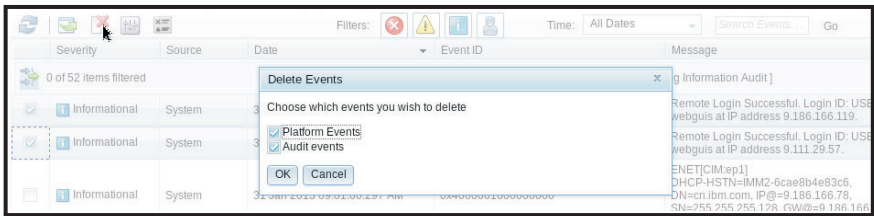
您可以使用 **Export** 按钮将事件日志中的所有事件或选定事件保存到文件。要选择特定事件，请在 Event Log 主页面上选择一个或多个事件并左键单击 **Export** 按钮（如下图所示）。

Event Log
This page displays the contents of the IMM event log, and allows you to sort and filter the log. By default the log entries are displayed in reverse chronological order (most recent log entry first). For each log entry, the severity of the event is displayed.

Export Event Logs

Severity	Source	Date
0 of 52 items filtered 2 items selected		
☒	Informational	System 31 Jan 2013 09:11:04.024 AM
☒	Informational	System 31 Jan 2013 09:02:42.771 AM

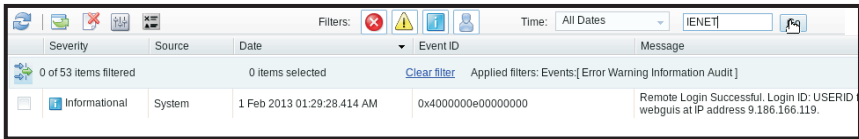
使用 **Delete Events** 按钮选择要删除事件的类型（如下图所示）。



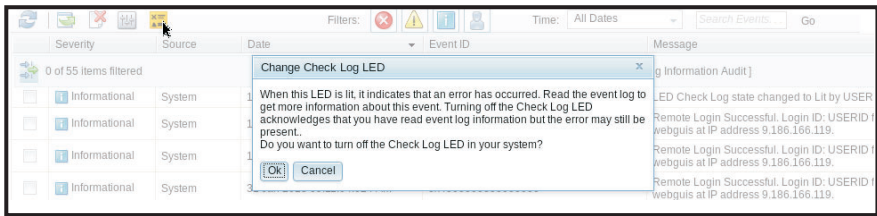
要选择希望显示的事件日志条目的类型，请单击相应按钮（如下图所示）。



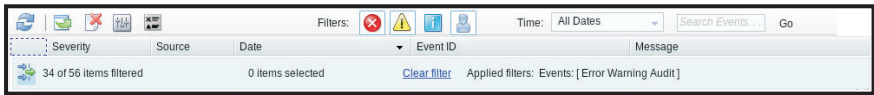
要搜索特定类型的事件或关键字，请在 **Search Events** 框中输入事件或关键字的类型；然后，单击 **Go**（如下图所示）。



要在检查日志指示灯点亮且已选择相关事件日志时关闭检查日志指示灯，请单击 **Check Log LED Status** 按钮（如下图所示）。

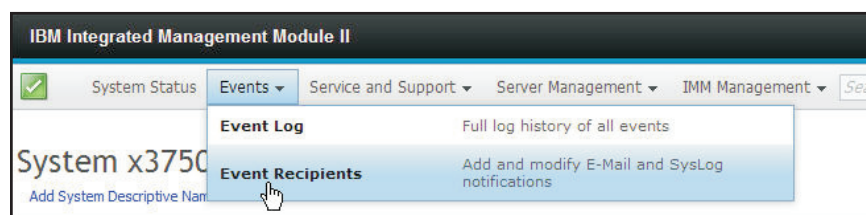


在 Event Log 工具栏上，可以单击任何 **Filter Events** 按钮以选择要显示的事件。要清除过滤器并显示所有类型的事件，请单击下图所示的 **Clear Filter** 链接。



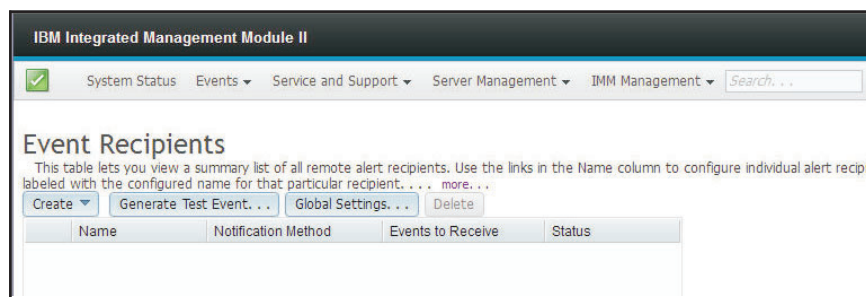
Event Recipients

使用 Events 选项卡下的 **Events Recipients** 选项，以添加和修改电子邮件和系统日志通知。

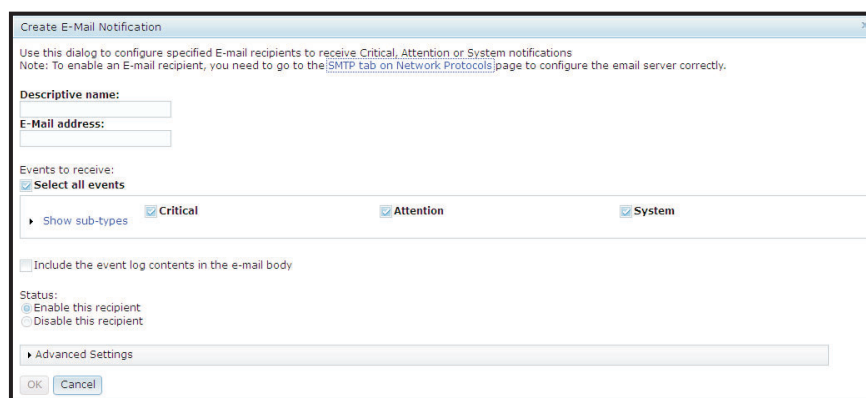


通过 Event Recipients 选项，可以管理将收到系统事件通知的人员。您可以配置每个接收方，并管理适用于所有事件接收方的设置。您还可以生成测试事件，以验证通知功能。

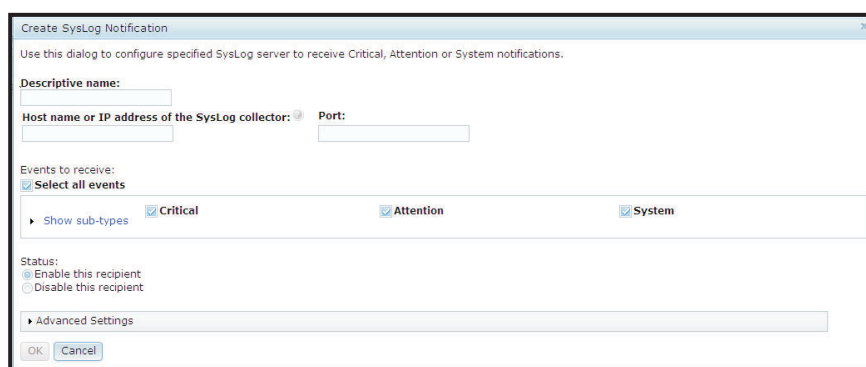
单击 **Create** 按钮以创建电子邮件和系统日志通知。下图显示 Event Recipients 窗口。



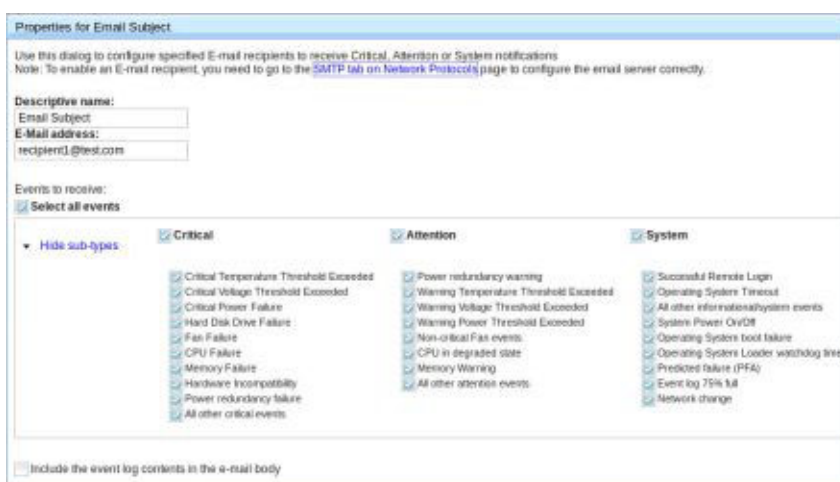
选择 **Create E-mail Notification** 选项以设置目标电子邮件地址，并且选择您希望收到通知的事件类型。此外，还可以单击 **Advanced Settings** 以选择起始索引号。要在电子邮件中包含事件日志，请选中 **Include the event log contents in the e-mail body** 复选框。以下是 Create E-mail Notification 窗口的插图。



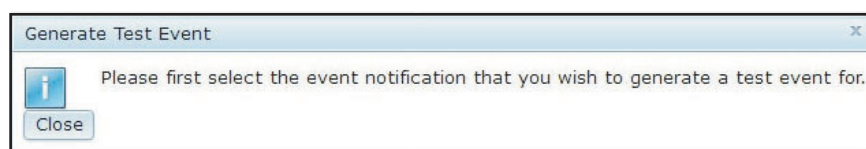
选择 **Create SysLog Notification** 选项以设置系统日志收集器的主机名和 IP 地址，并且选择您希望收到通知的事件类型。此外，还可以单击 **Advanced Settings** 以选择起始索引号。您还可以指定要用于此通知类型的端口。以下是 Create SysLog Notification 窗口的插图。



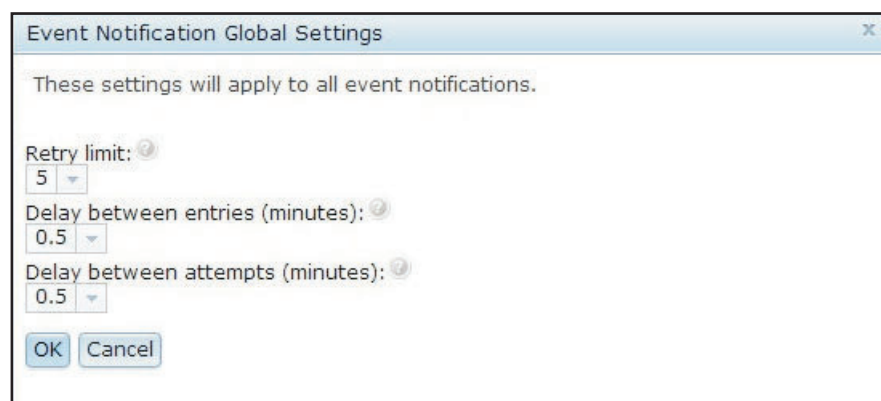
要配置现有的电子邮件通知或系统通知目标，请单击目标名称。以下是用于配置现有电子邮件通知和系统通知目标的 Properties for Email Subject 窗口的插图。



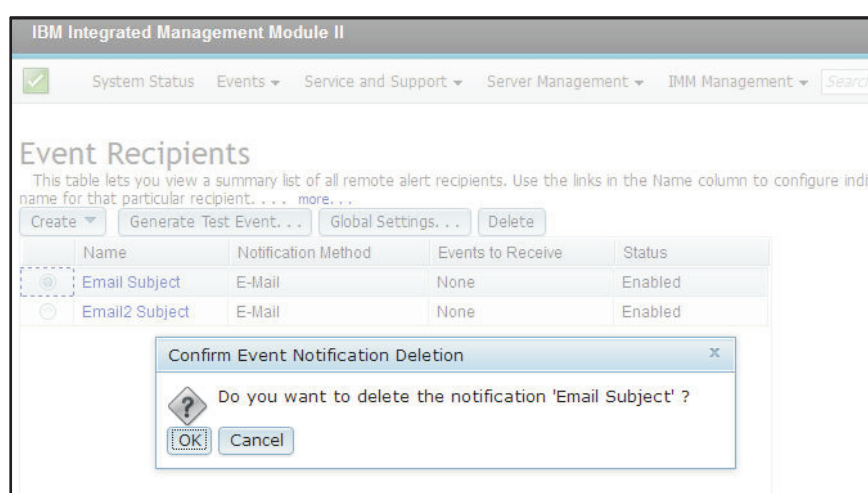
选择 **Generate Test Event** 按钮，以将测试电子邮件发送到所选电子邮件目标（如下图中所示）。



选择 **Global Settings** 按钮，以设置事件通知重试限制、事件通知条目之间的延迟（以分钟为单位）和尝试之间的延迟（以分钟为单位）（如下图中所示）。

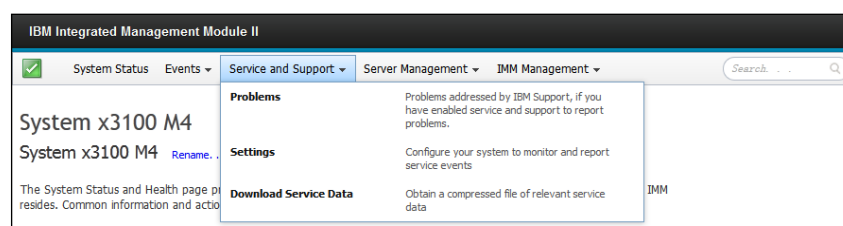


如果要除去电子邮件或系统日志通知目标，请选择 **Delete** 按钮。将打开以下窗口：



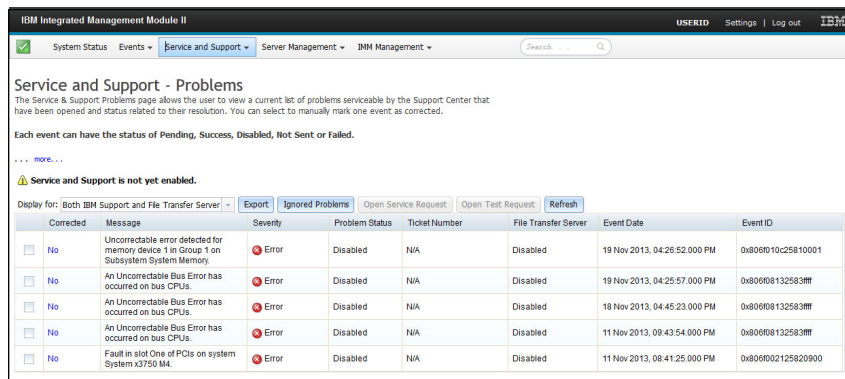
Service and Support 选项卡

此部分提供有关使用 IMM2 Web 用户界面页面上 Service and Support 选项卡下选项的信息（如下图所示）。



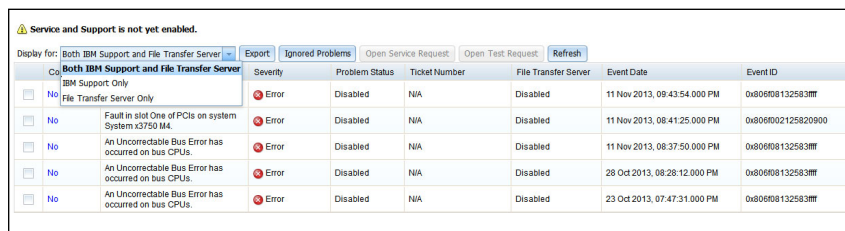
Problems 选项

使用 Service and Support 选项卡下的 **Problems** 选项查看 Support Center 可维护的未解决问题的列表（如下图所示）。您可以在 Problem Status 列中查看每个问题的状态，在问题得到解决后，在 Corrected 列中手动将事件标记为已更正。事件可以具有 Problem Status 值 Pending、Success、Disable、Not Sent 或 Failed。

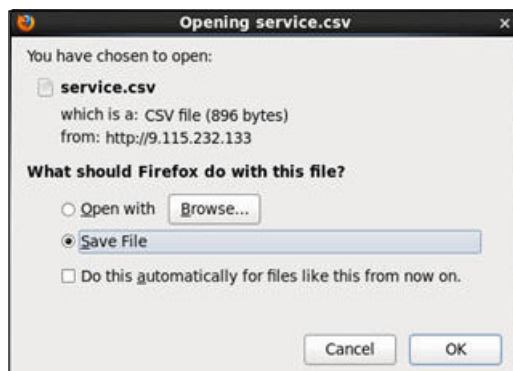


Display for: 字段显示以下方式之一（如下图所示）：

- Both IBM Support and File Transfer Server
- IBM Support Only
- File Transfer Server Only

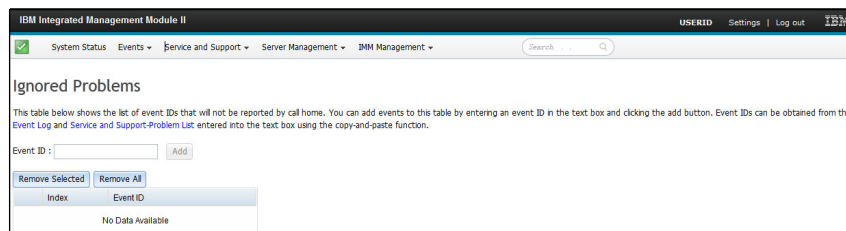


单击 **Export** 选项卡以下载 service.csv 文件。此时将显示以下窗口。

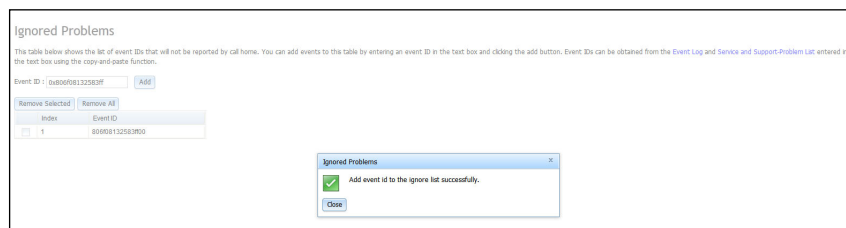


单击 **Ignore Problems** 选项卡以显示回拨功能将不报告的事件标识的列表。您可以通过在 **Event ID** 字段中输入事件标识并单击 **Add** 按钮来将事件标识添加到此列表（如下图所示）。

注：从事件日志中或者从 Service and Support Problem List 内的 Event ID 列中获取事件标识。使用复制和粘贴功能将事件标识添加到文本框中。



在输入有效的事件标识并单击 **Add** 按钮之后，将显示一个确认窗口，指示事件标识已成功添加。

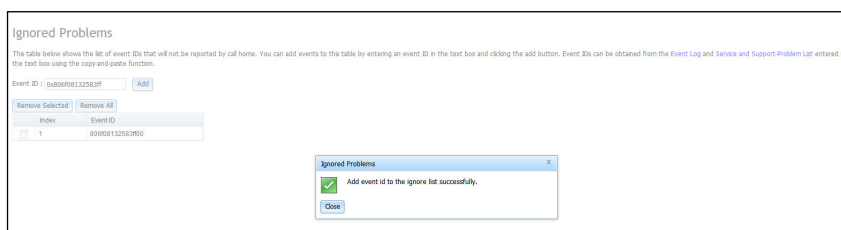


要从 Ignored Problems 列表中除去事件标识，请完成以下步骤：

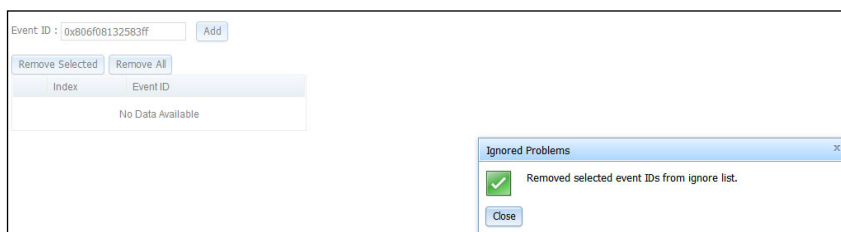
1. 选中要除去的事件标识的 **Index** 复选框。

注：要除去多个事件标识，请选中所有适用的 **Index** 复选框。

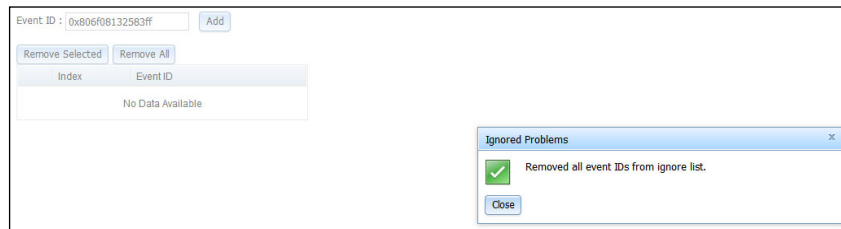
2. 单击 **Remove Selected** 按钮（如下图所示）。



将删除所选事件并显示一个确认窗口。



要从列表中除去所有事件标识，请选择 **Remove All** 按钮。此时将显示以下窗口。



单击 **Open Service Request** 选项卡以通过指示问题区域并输入问题的文本描述来手动提交服务请求。

单击 **Open Test Request** 选项卡以生成测试回拨（致电 IBM 支持）请求，加快完成此功能的正确配置或测试其正确操作。

单击 **Refresh** 选项卡以使用当前状态更新问题列表（如下图所示）。

Service and Support is not yet enabled.

Display for: Both IBM Support and File Transfer Server | **Export** | **Ignored Problems** | Open Service Request | Open Test Request | **Refresh**

Corrected	Message	Severity	Problem Status	Ticket Number	File Transfer Server	Event Date	Event ID
☐ No	An Unrecoverable Bus Error has occurred on bus CPUs.	Error	Disabled	N/A	Disabled	11 Nov 2013, 09:43:54.000 PM	0x80608132583fff
☐ No	Fault in slot One of PCIs on system System x3750-M4.	Error	Disabled	N/A	Disabled	11 Nov 2013, 08:41:25.000 PM	0x806002125820900
☐ No	An Unrecoverable Bus Error has occurred on bus CPUs.	Error	Disabled	N/A	Disabled	11 Nov 2013, 08:37:50.000 PM	0x80608132583fff
☐ Yes	An Unrecoverable Bus Error has occurred on bus CPUs.	Error	Disabled	N/A	Disabled	28 Oct 2013, 08:28:12.000 PM	0x80608132583fff
☐ No	An Unrecoverable Bus Error has occurred on bus CPUs.	Error	Disabled	N/A	Disabled	23 Oct 2013, 07:47:31.000 PM	0x80608132583fff

Settings 选项

使用 Service and Support 选项卡下的 **Settings** 选项查看、添加或更改服务和支持设置（如下图所示）。

备注：

- 要成功回拨（致电 IBM 支持），请确保域名系统（DNS）设置有效。
- 需要服务中心和联系信息来获取 IBM 支持。
- 要启用文件传输服务器，必须正确填写服务器信息。

IBM Integrated Management Module II USERID Settings Log out IBM

System Status Events Service and Support Server Management IBM Management Search

Service and Support - Settings

Use this page to view or change current service and support settings. To successfully Call home (IBM support), make sure DNS settings are valid. The service center and contact information is required to enable IBM support. To enable file transfer server, to input the server information correctly.

... more ...

Service and Support is not yet enabled.

IBM Support File Transfer Server HTTP Proxy

Enable IBM Support

To successfully Call home (IBM support), make sure DNS settings are valid. The service center and contact information is required to enable IBM support.

☐ **Enable IBM Support.** Automatically send the service information to IBM.

IBM Service Center

Country code:

Contact Information

The information here will be used by IBM Support for any follow-up inquires and shipment.

Primary Contact

Company name:

Contact name:

Telephone number: Extension:

Alternate Contact (Optional)

Contact name:

Telephone number: Extension:

Contact Email address:

要允许服务处理器将服务信息自动发送到 IBM，请完成以下步骤（如下图所示）：

1. 单击 **IBM Support** 选项卡。
2. 单击 **Enable IBM Support** 复选框。
3. 从 **IBM Service Center** 列表中，选择 IBM Service Center 位置。
4. 在以下字段中输入 **Primary Contact** 信息：
 - Company name
 - Contact name
 - Telephone number
 - Extension (如果适用)
 - Contact Email address
 - Address
 - City
 - State/Province
 - Postal code
5. 单击 **Apply IBM Support Settings** 按钮。

IBM Support | File Transfer Server | HTTP Proxy

Enable IBM Support

To successfully Call home (IBM support), make sure DNS settings are valid. The service center and contact information is required to enable IBM support.

☒ **Enable IBM Support.** Automatically send the service information to IBM.

IBM Service Center

Country code:

Contact Information

The information here will be used by IBM Support for any follow-up inquiries and shipment.

Primary Contact Company name: Company Contact name: Contact Telephone number: 000000 Extension: Contact Email address: test@test.com Address: Address City: City State/Province: Sta Postal code: 000	Alternate Contact (Optional) Contact name: Telephone number: Extension: Contact Email address: Machine Location Phone:
--	---

要允许服务处理器将硬件服务性事件和数据发送到指定的文件传输服务器站点，请完成以下步骤（如下图所示）：

1. 单击 **File Transfer Server** 选项卡。
2. 选中 **Enable File Transfer Server** 复选框。
3. 单击 **Apply File Transfer Server Settings** 按钮。

IBM Support File Transfer Server HTTP Proxy

Use this feature to send hardware serviceable events and data to the File Transfer Server site you specify. If an approved service provider is providing your hardware warranty, you should specify the File Transfer Server site provided by your service provider. Information contained in the service data will assist your service provider in correcting the hardware issue.

☒ **Enable File Transfer Server**

Protocol:
FTP

IP address or host name: 9.115.232.123 Port: 21

User name:
USERID

Password:

Apply File Transfer Server Settings Reset

要建立用于连接到因特网的方法，请完成以下步骤（如下图所示）：

1. 单击 **HTTP Proxy** 选项卡。
2. 单击以下方法之一来访问因特网：
 - 管理服务器可以在没有代理服务器的情况下访问因特网
 - 管理服务器将需要代理服务器才能访问因特网

IBM Support File Transfer Server HTTP Proxy

Select the method to connect internet

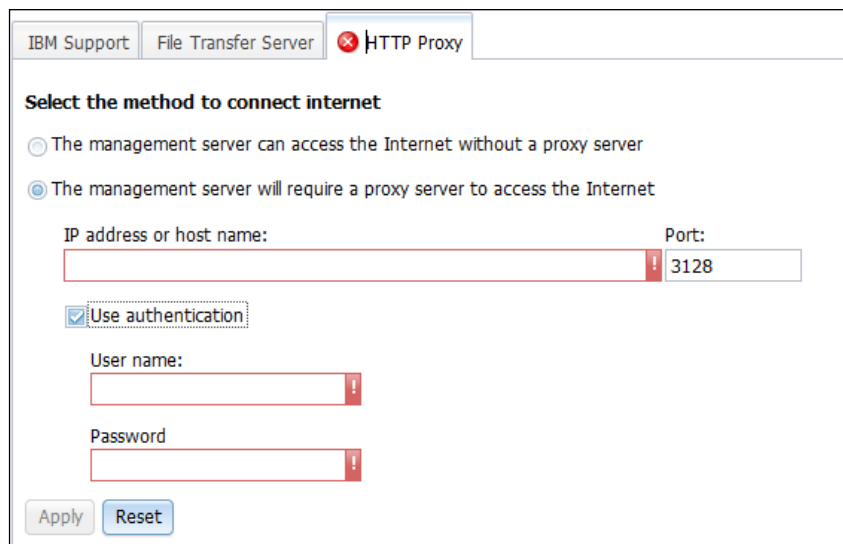
☒ The management server can access the Internet without a proxy server

☐ The management server will require a proxy server to access the Internet

Apply Reset

3. 如果访问因特网必需代理服务器，请完成以下步骤（如下图所示）；否则，请继续第 37 页的 4 步。
 - a. 在 **IP address or host name** 字段中，输入代理服务器的 IP 地址或主机名。
 - b. 在 **Port** 字段中，输入代理服务器的端口。

注：**Use authentication** 复选框是可选选项。

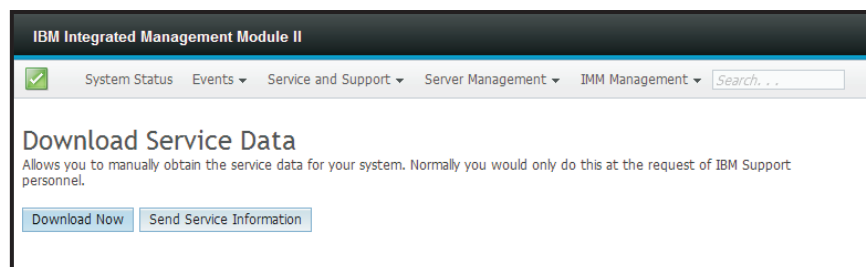


4. 单击 **Apply** 按钮。

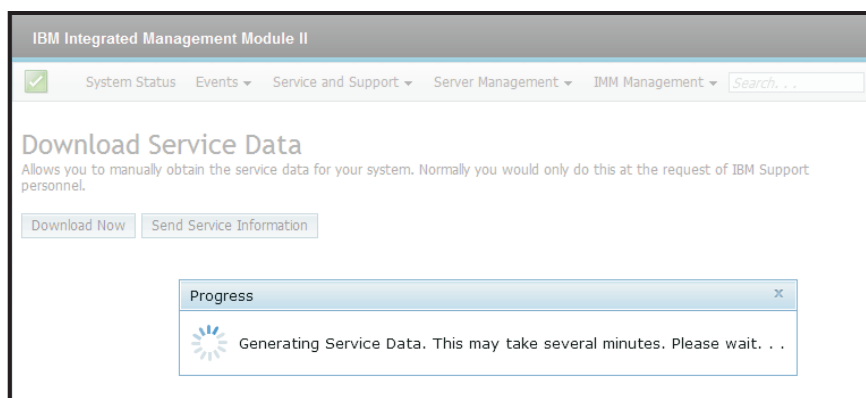
Download Service Data 选项

使用 Service and Support 选项卡下的 **Download Service Data** 选项收集信息并创建服务器相关压缩文件。您可以将该文件发送给 IBM 支持人员以帮助确定问题。

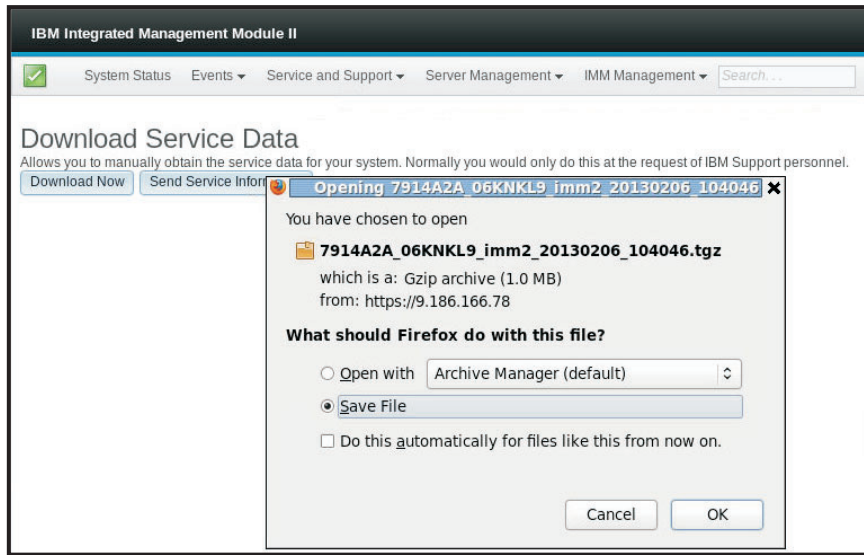
单击 **Download Now** 按钮以下载服务和支持数据（如下图中所示）。



这样将启动收集数据的过程。该过程需要几分钟时间来生成之后可保存到文件的服务数据。将会显示进度窗口，指示正在生成数据。



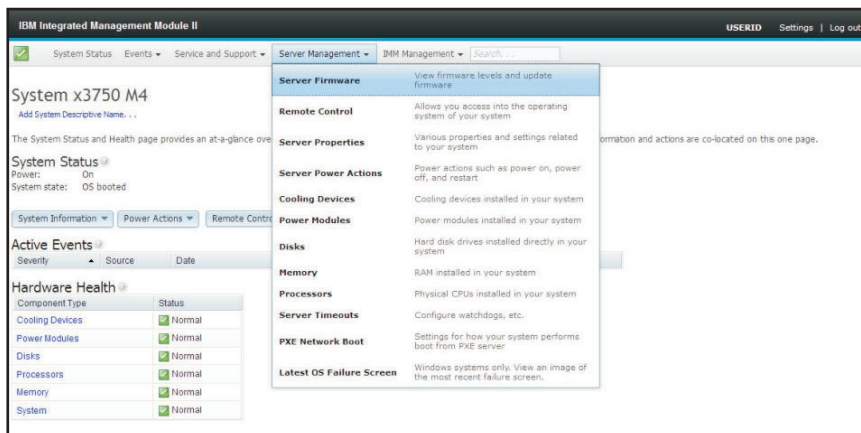
当该过程完成时，会显示以下窗口，提示您输入要保存所生成文件的位置。



Server Management 选项卡

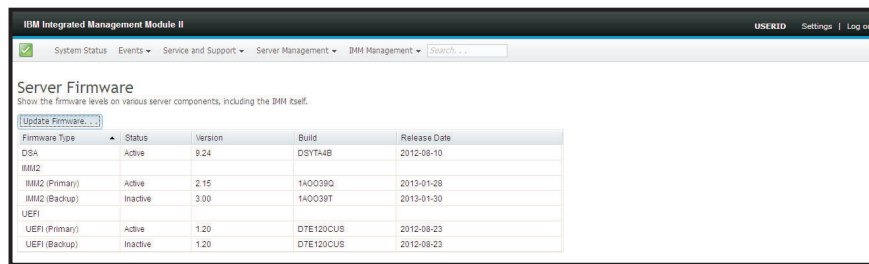
此部分提供有关 IMM2 Web 用户界面主页上 Server Management 选项卡下选项的信息。

通过 Server Management 选项卡下的选项，可以查看有关服务器固件状态和控制、远程控制访问、服务器属性状态和控制、服务器电源操作、散热设备、电源模块、磁盘、内存、处理器、服务器超时、PXE 网络引导和最新操作系统故障屏幕的信息（如下图所示）。



Server Firmware

选择 Server Management 选项卡下的 **Server Firmware** 选项以查看服务器上安装的固件的级别以及应用固件更新。下图显示服务器固件级别，并允许您更新 DSA、IMM2 和 UEFI 固件。



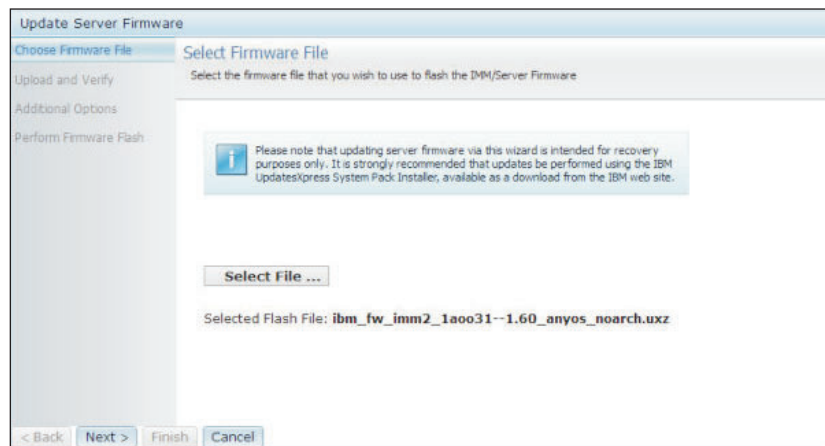
将显示 IMM2、UEFI 和 DSA 固件的当前状态和版本，包括 Primary 和 Backup 版本。固件状态有三种类别：

- **Active**：固件处于活动状态。
- **Inactive**：固件处于非活动状态。
- **Pending**：固件正在等待变为活动状态。

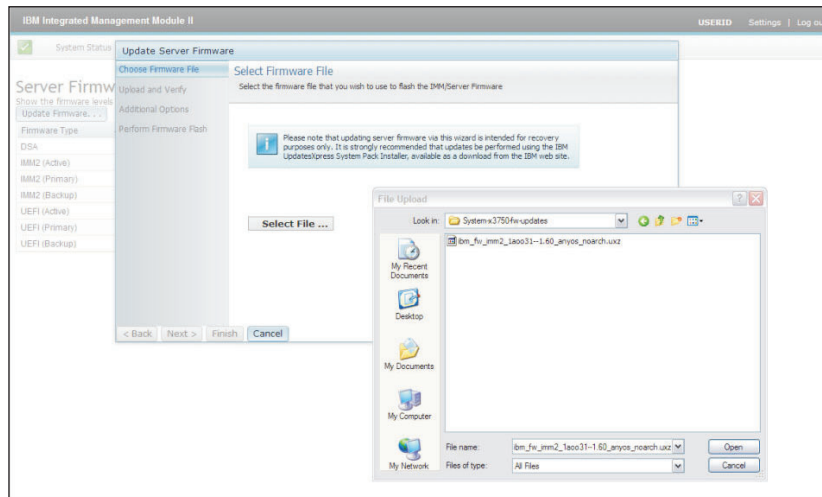
注意：安装错误的固件更新可能会导致服务器发生故障。在安装固件或设备驱动程序更新之前，请阅读所下载更新随附的任何自述文件和变更历史记录文件。这些文件包含有关更新的重要信息和安装更新的过程，包括从早期固件或设备驱动程序版本更新到最新版本的任何特殊过程。

要更新固件，请选择 **Update Firmware...** 按钮。这样会显示 Update Server Firmware 窗口（如下图所示）。您可以单击 **Cancel** 并返回到上一个 Server Firmware 窗口，或者单击 **Select File...** 按钮以选择要用于更新服务器固件的固件文件。

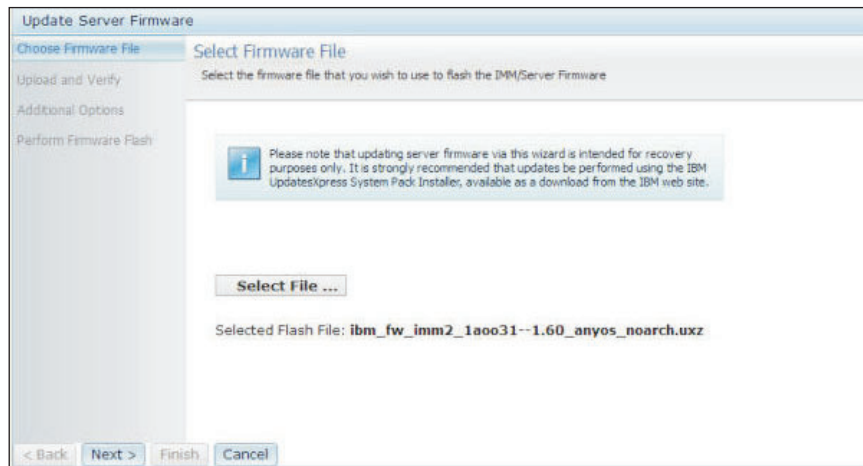
注：单击 **Select File...** 按钮之前，请阅读窗口提示中显示的警告，然后再继续。



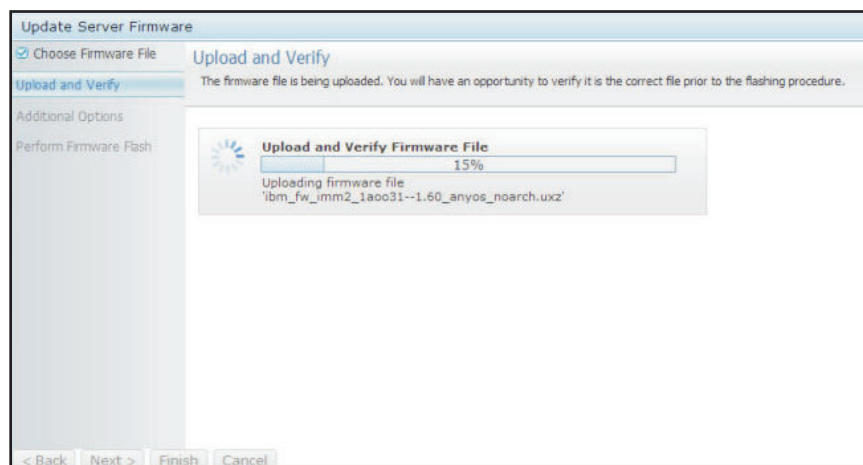
单击 **Select File...** 按钮时，会显示 File Upload 窗口，通过该窗口可浏览至所需文件。



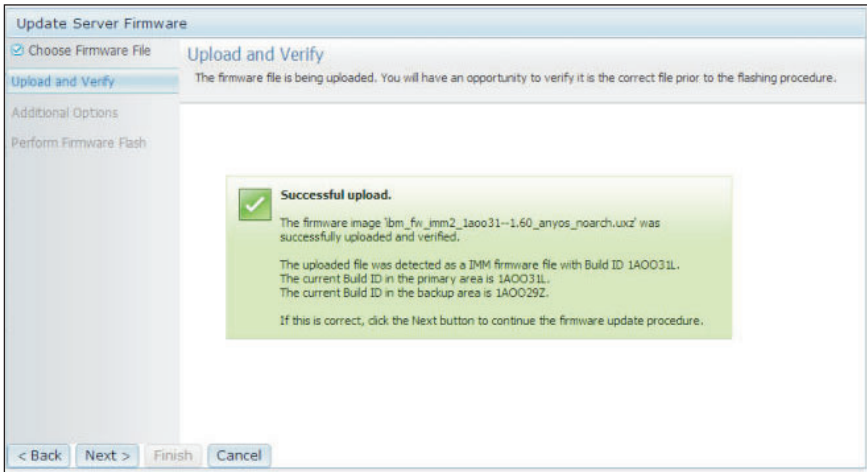
浏览至要选择的文件后，单击 **Open** 按钮，您将返回到显示了所选文件的 Update Server Firmware 窗口（如下图所示）。



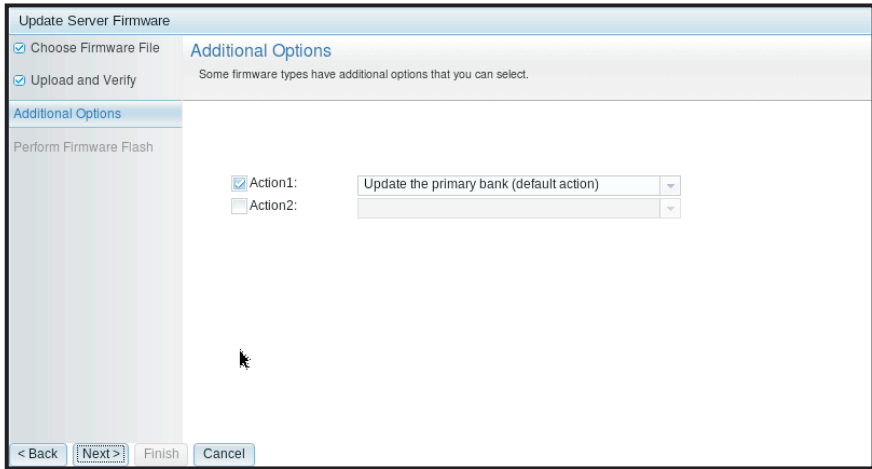
单击 **Next >** 按钮以开始上传并验证有关所选文件的进程（如下图所示）。上传并验证文件时，将会显示进度计量表。



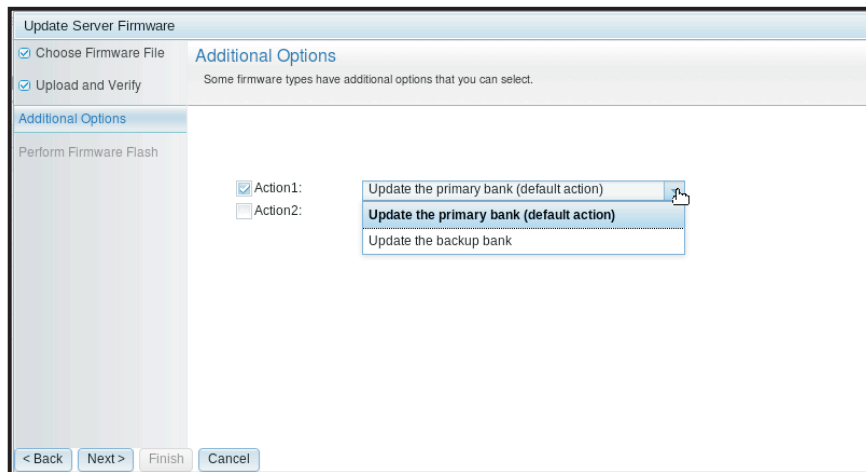
将打开状态窗口（如下图所示），以使您能够验证选定要更新的文件是否是正确的文件。该窗口将包含有关要更新的固件文件类型（如 DSA、IMM2 或 UEFI）的信息。如果信息正确，请单击 **Next >** 按钮。如果要重做任何选择，请单击 **< Back** 按钮。



当单击 **Next >** 按钮时，会显示一组其他选项，如下图所示。



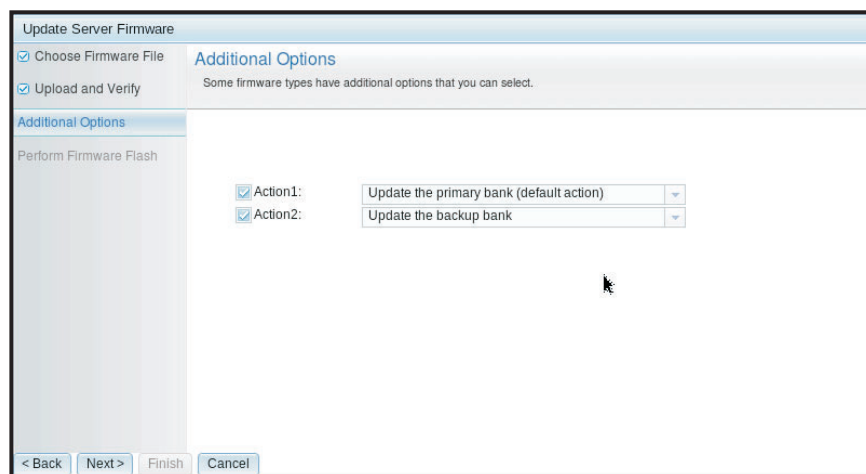
通过 **Action 1** 旁的下拉菜单（如下图所示），可以选择 **Update the primary bank (default action)** 或 **Update the backup bank**。



选择操作后，您将返回到上一个窗口，通过单击 **Action 2** 复选框可选择其他操作。

装入操作后，会显示所选操作和新的 **Action 2** 下拉菜单（如下图所示）。

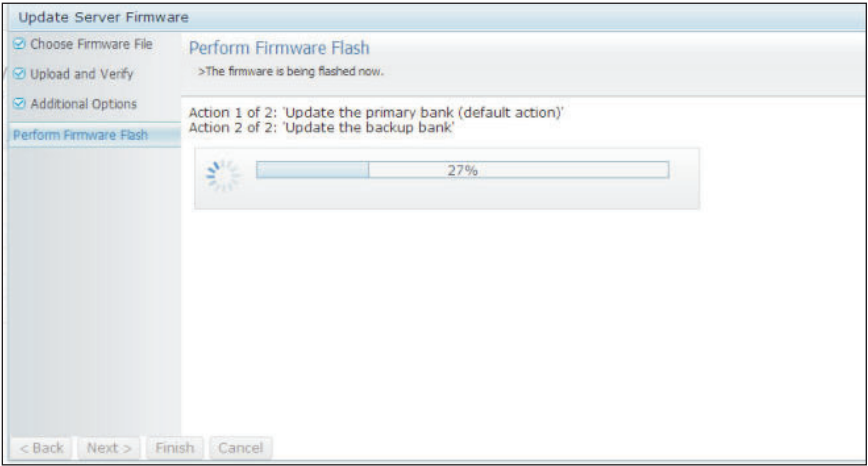
注：要禁用操作，请单击相关操作旁的复选框。



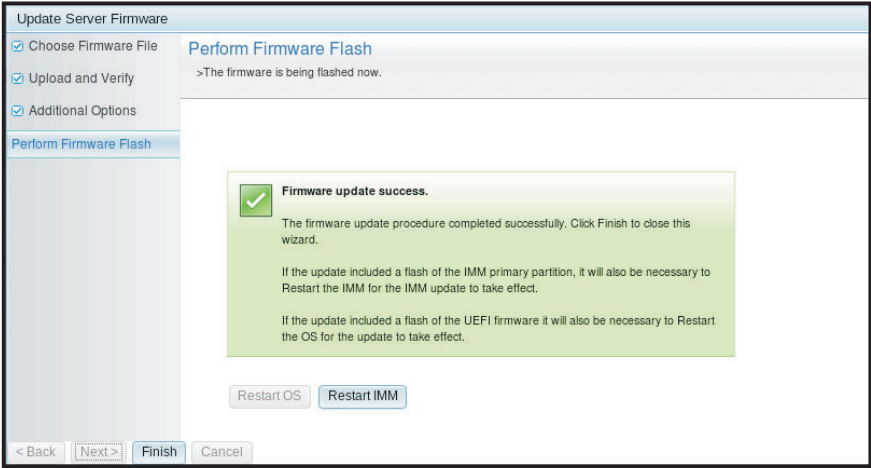
上一个屏幕显示了对于 Action 1，选择要更新主内存区。您还可以在 Action 2 下选择更新备份内存区（如上一窗口中所示）。单击 **Next >** 时，将同时更新主内存区和备份内存区。

注：Action 1 必须不同于 Action 2。

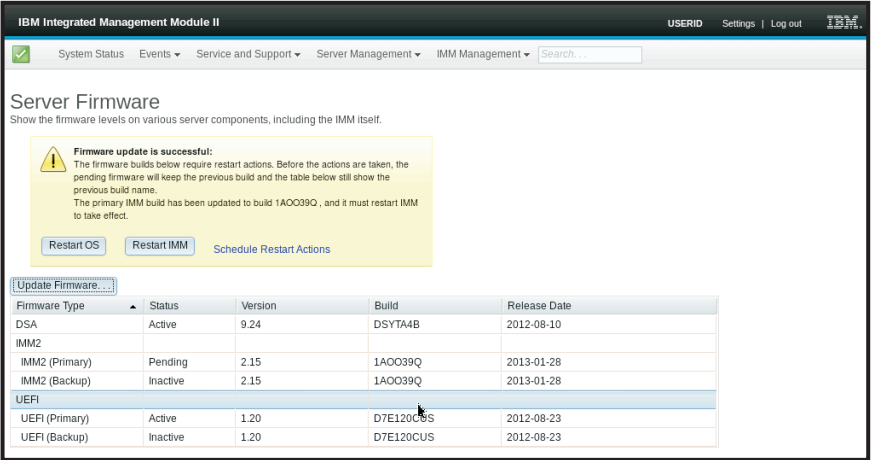
将显示进度计量表，其中会显示固件更新的进度（如下图所示）。



成功完成固件更新后，会打开以下窗口。根据显示的内容选择相关操作，以完成更新过程。



如果主要的固件更新未完成，那么会打开以下窗口。



远程控制

本节提供有关远程控制功能部件的信息。

ActiveX 客户机和 Java 客户机是图形远程控制台，可用于通过客户机键盘和鼠标来远程查看服务器视频显示并与其交互。

备注：

- ActiveX 客户机只能用于 Internet Explorer 浏览器。
- 要使用 Java 客户机，需要 Java Plug-in 1.5 或更高发行版。
- Java 客户机与 IBM Java 6 SR9 FP2 或更高发行版兼容。

远程控制功能部件包括两个单独的窗口：

- **Video Viewer**

Video Viewer 窗口使用远程控制台进行远程系统管理。远程控制台是服务器的交互式图形用户界面 (GUI) 显示，可以在计算机上查看。您显示器上显示的内容与服务器控制台上的内容完全相同，并且您使用键盘和鼠标对控制台进行控制。

注：视频查看器能够仅显示主板上视频控制器生成的视频。如果安装独立的视频控制器适配器并代替系统的视频控制器，那么 IMM2 无法在远程视频查看器上显示来自所添加适配器的视频内容。

- **Virtual Media Session**

Virtual Media Session 窗口列出了客户机上所有可映射为远程驱动器的驱动器，并且可用于将 ISO 和软盘映像文件映射为虚拟驱动器。每个映射的各驱动器可标记为只读。CD 驱动器、DVD 驱动器以及 ISO 映像始终为只读。可通过 Video Viewer 窗口的 Tools 菜单栏访问 Virtual Media Session 窗口。

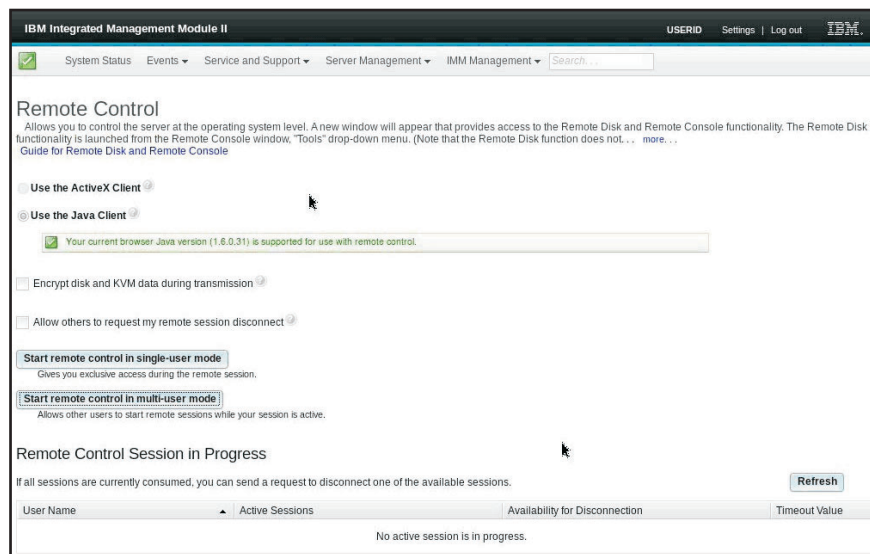
备注：

- Virtual Media Session 每次只能由一个远程控制会话客户机使用。
- 如果使用 ActiveX 客户机，将打开一个父窗口，必须使该窗口始终保持打开状态，直到远程会话完成为止。

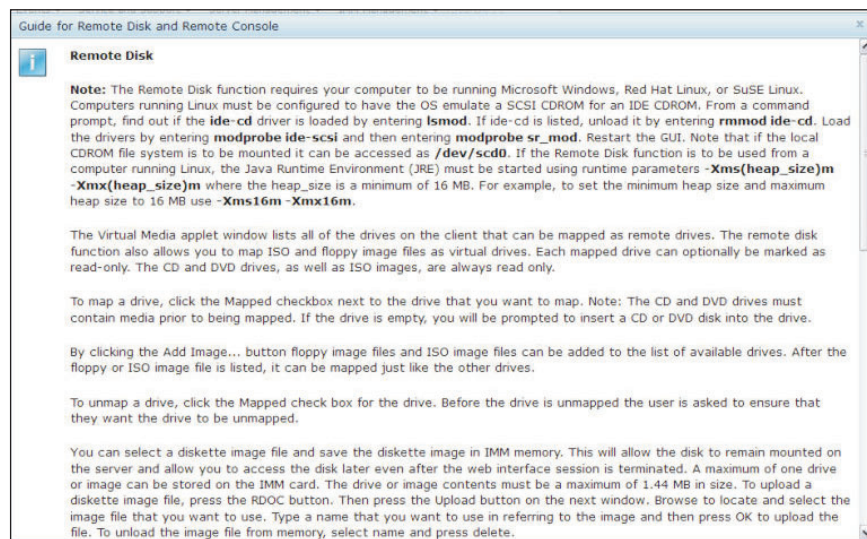
要远程访问服务器控制台，请完成以下步骤：

1. 登录到 IMM2（请参阅第 10 页的『登录到 IMM2』，以获取更多信息）。
2. 通过选择以下一个菜单选项访问 Remote Control 页面：
 - 从 Server Management 选项卡中选择 **Remote Control** 选项。
 - 单击 System Status 页面上的 **Remote Control...**。

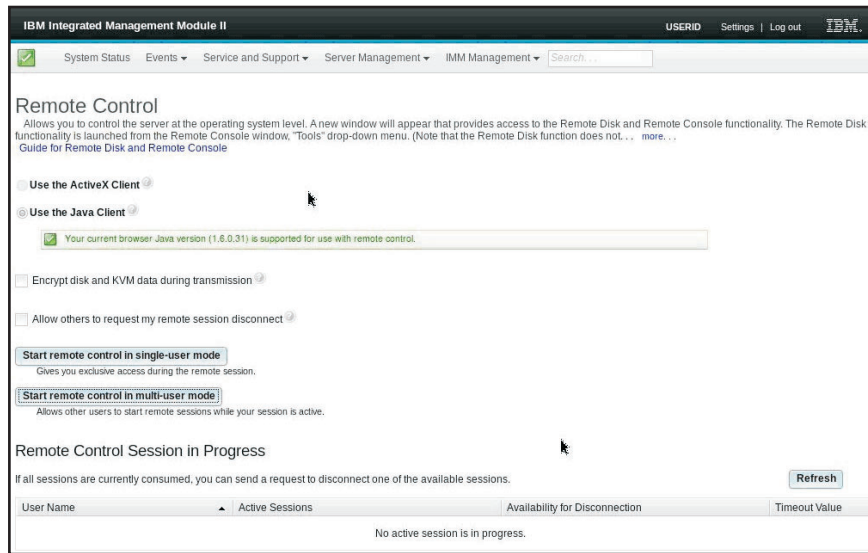
此时将打开 Remote Control 页面，如下图所示。



3. 可以单击 **Guide for Remote Disk and Remote Console** 链接以访问更多信息。
下图显示了 Guide for Remote Disk and Remote Console 窗口。



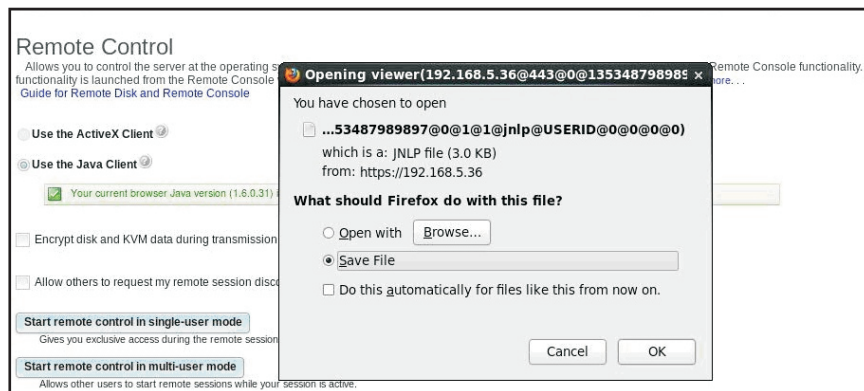
- a. 单击 **Close** 以退出 Guide for Remote Disk and Remote Console 窗口。
4. 选择以下一项图形远程控制台选项：
 - 要使用 Internet Explorer 作为浏览器，请选择 **Use the ActiveX Client**。
 - 要使用 Java 客户机，请选择 **Use the Java Client**，如下图所示。



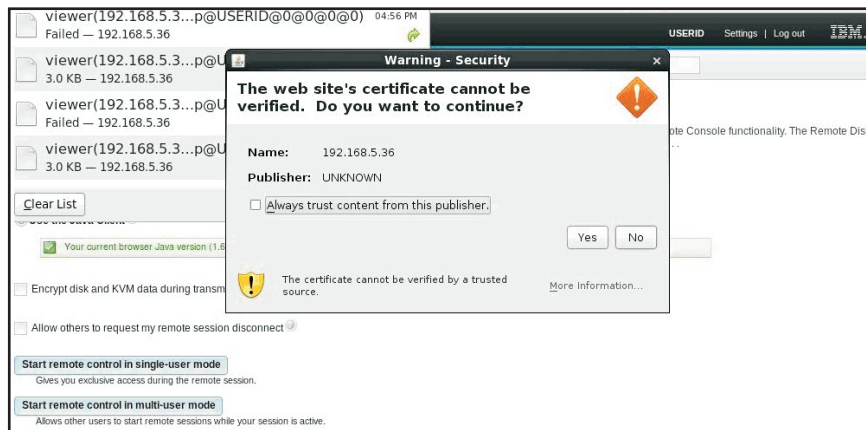
备注：

- 如果您未使用 Internet Explorer 浏览器，那么只能选择 Java 客户机。
- ActiveX 和 Java 客户机具有相同的功能。
- 将显示状态行，指示客户机是否受支持。

此时将打开以下窗口。该窗口显示浏览器（例如，Firefox 浏览器）将用于打开 Viewer 文件的信息。



5. 浏览器下载并打开 Viewer 文件后，将打开一个确认窗口，其中显示有关 Web 站点证书验证的警告（如下图所示）。单击 **Yes** 以接受证书。

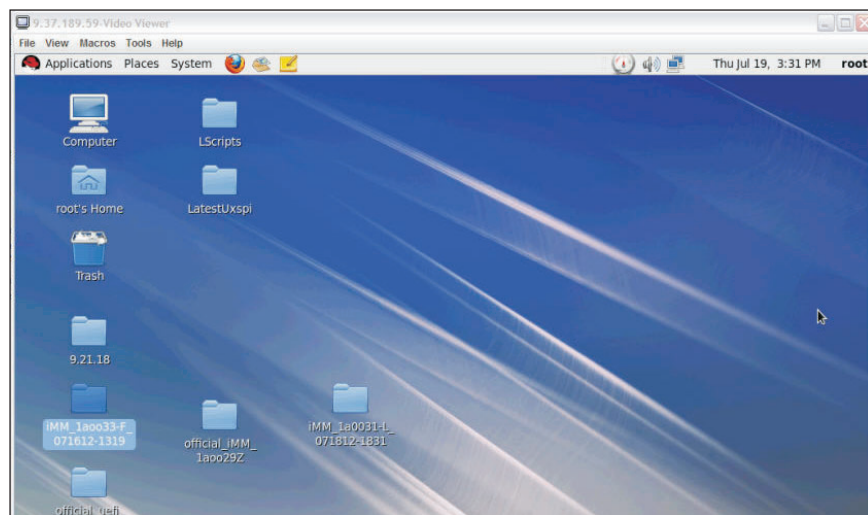


6. 要远程控制服务器，请选择以下一个菜单选项：

- 要在会话期间具有独占远程访问权，请单击 **Start remote control in single User mode**。
- 要允许其他人在您会话期间具有远程控制台访问权，请单击 **Start remote control in multi user mode**。

注：如果在 Video Viewer 窗口打开前选中了 **Encrypt disk and KVM data during transmission** 复选框，那么在会话期间将通过 ADES 加密来加密磁盘数据。

此时将打开 Video Viewer 窗口（如下图所示）。此窗口可用于访问远程控制台功能。



7. 完成使用远程控制功能时，请关闭 Video Viewer 和 Virtual Media Session 窗口。

备注：

- Video Viewer 将自动关闭 Virtual Media Session 窗口。
- 如果当前映射了远程磁盘，请勿关闭 Virtual Media Session 窗口。请参阅第 119 页的『远程磁盘』以获取有关关闭和取消映射远程磁盘的指示信息。
- 如果在使用远程控制功能时出现鼠标或键盘问题，请参阅 Web 界面中的 Remote Control 页面上提供的帮助。

- 如果使用远程控制来更改 Setup Utility 程序中 IMM2 的设置，那么服务器可能会重新启动 IMM2。您将丢失远程控制台和登录会话。短暂延迟后，您可以使用新会话再次登录到 IMM2，再次启动远程控制台，以及退出 Setup Utility 程序。

要点：IMM2 使用 Java applet 或 ActiveX applet 来执行远程感知功能。当 IMM2 更新为最新固件级别时，Java applet 和 ActiveX applet 也会更新为最新级别。缺省情况下，Java 对先前使用的 applet 进行高速缓存（本地存储）。对 IMM2 固件进行快速更新后，服务器使用的 Java applet 可能不是最新级别。

要更正此问题，请关闭高速缓存。所使用的方法应根据平台和 Java 版本而不同。以下步骤适用于 Windows 上的 Oracle Java 1.5：

1. 单击开始 → 设置 → 控制面板。
2. 双击 **Java Plug-in 1.5**。此时会打开 Java Plug-in 控制面板窗口。
3. 单击 **Cache** 选项卡。
4. 选择以下选项之一：
 - 清除 **Enable Caching** 复选框，以便始终禁用 Java 高速缓存。
 - 单击 **Clear Caching**。如果选择此选项，那么在各 IMM2 固件更新后必须单击 **Clear Caching**。

有关更新 IMM2 固件的更多信息，请参阅第 121 页的『更新服务器固件』。

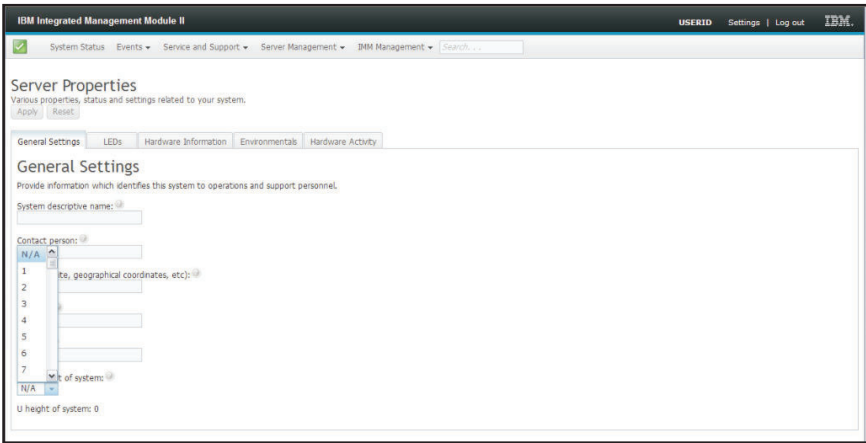
有关远程控制功能部件的更多信息，请参阅第 109 页的『远程感知和远程控制功能』。

Server Properties

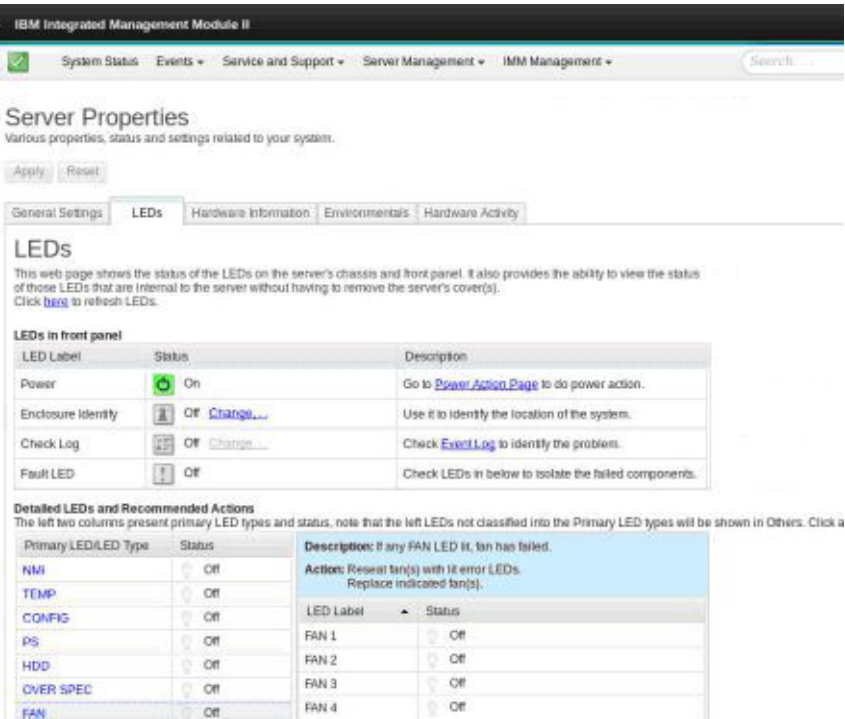
选择 Server Management 选项卡下的 **Server Properties** 选项，以设置各种参数帮助识别系统。您可以指定 **System descriptive name**、**Contact person**、**Location** 及其他信息，如下图所示。在这些字段中输入的信息将在您单击 **Apply** 时生效。要清除自从上次应用更改以来在字段中输入的信息，请单击 **Reset**。

The screenshot shows the 'Server Properties' configuration page in the IMM2 interface. The 'General Settings' tab is active, displaying various fields for system identification. The fields include 'System descriptive name', 'Contact person', 'Location (site, geographical coordinates, etc.)', 'Room ID', 'Rack ID', 'Lowest unit of system' (with a dropdown menu showing 'N/A'), and 'U height of systems'.

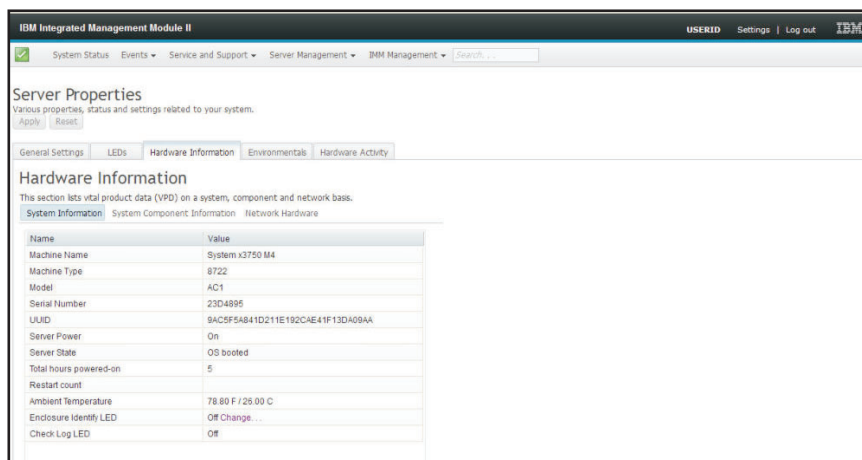
在下图中，可以指定 **Lowest unit of the system**。**Lowest unit of the system** 字段需要与管理模块（例如高级管理模块或机箱管理模块）连接。



要查看系统中的指示灯，请单击 **LED** 选项卡。此时将打开以下窗口。

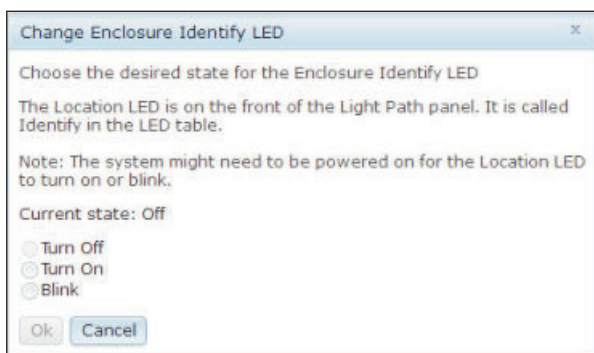


要查看系统信息、系统组件信息和网络硬件信息，请单击 **Hardware Information** 选项卡。选择 **Hardware Information** 选项卡内的相应选项卡以查看各种重要产品数据 (VPD) 信息。**System Information** 选项卡提供诸如机器名称、序列号和型号之类的信息。下图显示 **System Information** 窗口。

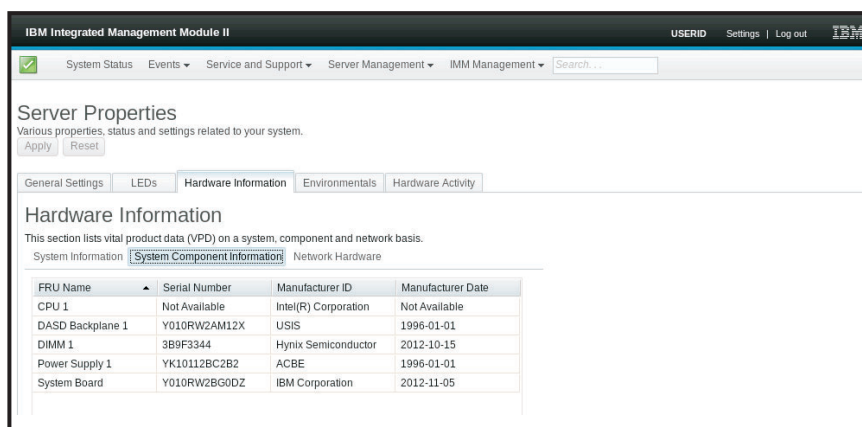


可以从 System Information 窗口查看和更改 **Enclosure Identify LED** 的状态。要更改 **Enclosure Identify LED**，请单击 **Change..** 链接。此时将打开以下窗口。

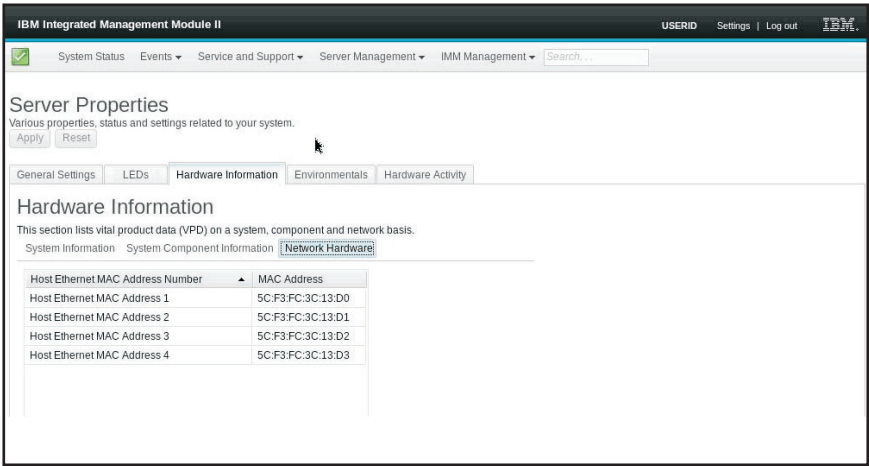
注：机柜身份指示灯位于光通路面板的正面。



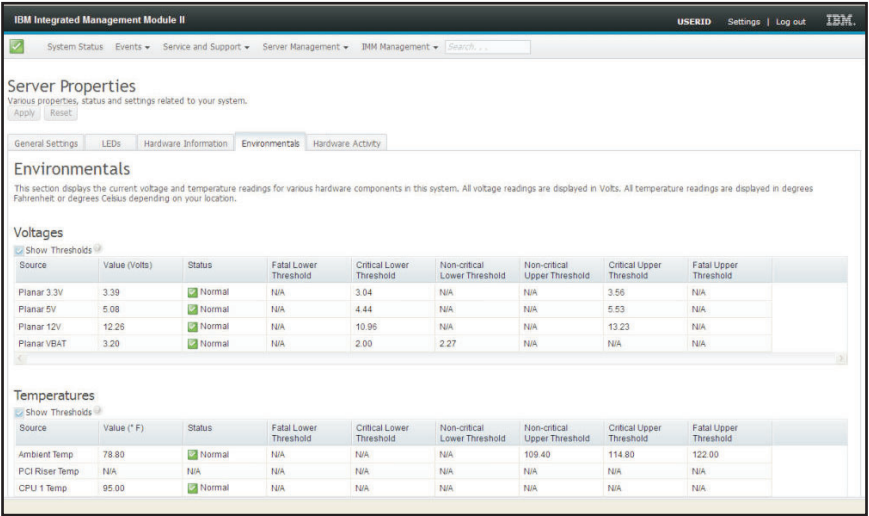
选择 **System Component Information** 选项卡以查看组件信息。组件信息包括 FRU Name、Serial Number、Manufacturer ID 和 Manufacturer Date。下图显示单击 **System Component Information** 选项卡时您将看到的信息。



选择 **Network Hardware** 选项卡以查看网络硬件信息。网络硬件信息包括 Host Ethernet MAC Address Number 和 MAC Address。下图显示单击 **Network Hardware** 选项卡时您将看到的信息。



选择 Server Properties 页面上的 **Environmentals** 选项卡以查看系统中硬件组件的电压和温度。此时将打开以下窗口。表中的 **Status** 列显示服务器中的正常活动或问题区域。



Server Properties 页面上的 **Hardware Activity** 选项卡提供已添加或从系统中除去的硬件的历史记录。下图显示单击 **Hardware Activity** 选项卡时您将看到的信息。

FRU Name	Serial Number	Manufacturer ID	Action	Time of Action
CPU/IMM Tray	Y135B61C000R	CLCH	Added	19 Jul 2012 09:12 AM
Power Supply 1	K10511BE006	Delta	Added	19 Jul 2012 09:12 AM
Power Supply 2	K10511BE00F	Delta	Added	19 Jul 2012 09:12 AM
SAS Backplane 1	Y011U515G98C	MDLX	Added	19 Jul 2012 09:12 AM
CPU 1	Not Available	Intel(R) Corporation	Added	19 Jul 2012 09:12 AM
CPU 2	Not Available	Intel(R) Corporation	Added	19 Jul 2012 09:12 AM
CPU 3	Not Available	Intel(R) Corporation	Added	19 Jul 2012 09:12 AM
CPU 4	Not Available	Intel(R) Corporation	Added	19 Jul 2012 09:12 AM

Server Power Actions

此部分提供有关 IMM2 Web 界面主页上 Server Management 选项卡下 Server Power Actions 选项的信息。

选择 Server Management 选项卡下的 **Server Power Actions** 选项以查看可用于控制系统电源的操作的列表。下图是 Server Power Actions 窗口示例。

Actions
Power On Server Immediately
Power On Server at Specified Date and Time
Power Off Server Immediately
Shut down OS and then Power Off Server
Shut down OS and then Restart Server
Restart the Server Immediately
Restart the Server with Non-volatile Internet (NMI)
Schedule Daily/Weekly Power and Restart Actions

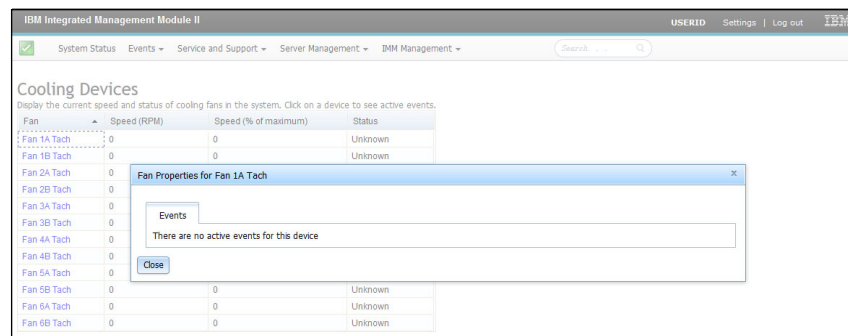
您可以选择立即使服务器开机，或者在安排的时间使服务器开机。您也可以选择关机，然后重新启动操作系统。有关控制服务器电源的更多信息，请参阅第 108 页的『控制服务器的电源状态』。

Cooling Devices

选择 Server Management 选项卡下的 **Cooling Devices** 选项，以查看服务器中散热风扇的当前速度和状态（如下图所示）。

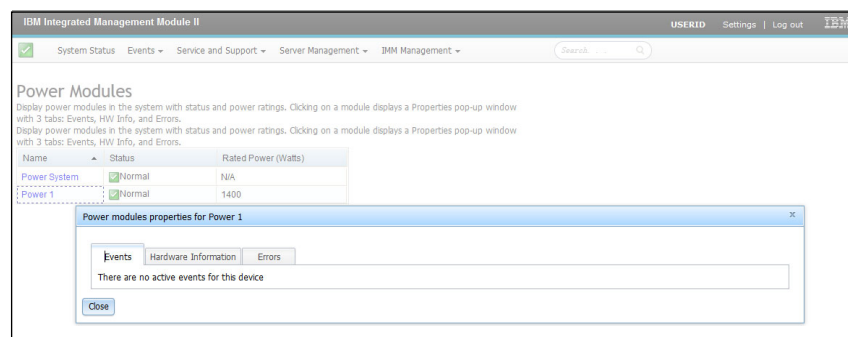
Fan	Speed (RPM)	Speed (% of maximum)	Status
Fan 1A Tach	0	0	Unknown
Fan 1B Tach	0	0	Unknown
Fan 2A Tach	0	0	Unknown
Fan 2B Tach	0	0	Unknown
Fan 3A Tach	0	0	Unknown
Fan 3B Tach	0	0	Unknown
Fan 4A Tach	0	0	Unknown
Fan 4B Tach	0	0	Unknown
Fan 5A Tach	0	0	Unknown
Fan 5B Tach	0	0	Unknown
Fan 6A Tach	0	0	Unknown
Fan 6B Tach	0	0	Unknown

单击表中的散热设备（Fan 链接）以查看设备的任何活动事件（如以下屏幕所示）。

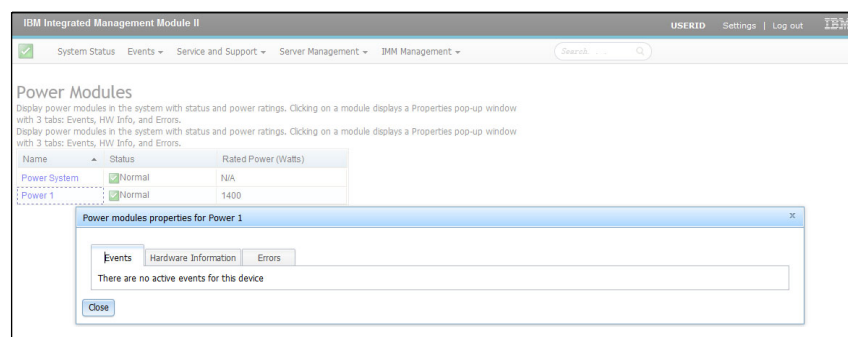


Power Modules

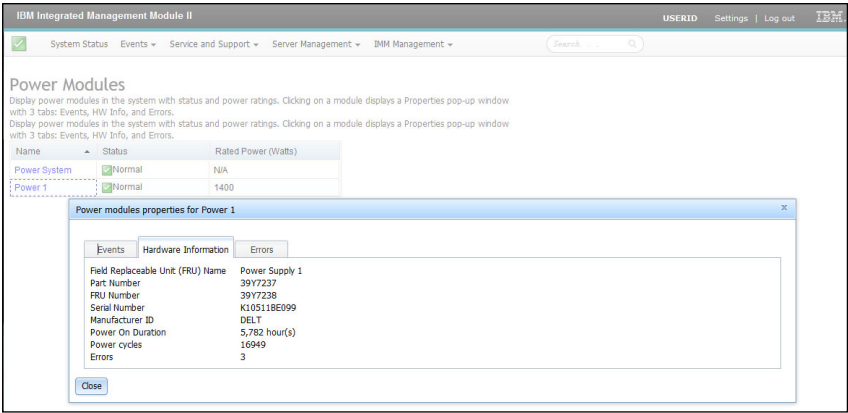
选择 **Server Management** 选项卡下的 **Power Modules** 选项，以查看系统中的电源模块以及状态和额定功率。单击表中的电源链接以查看与电源模块关联的活动事件、硬件信息和错误（如下图所示）。



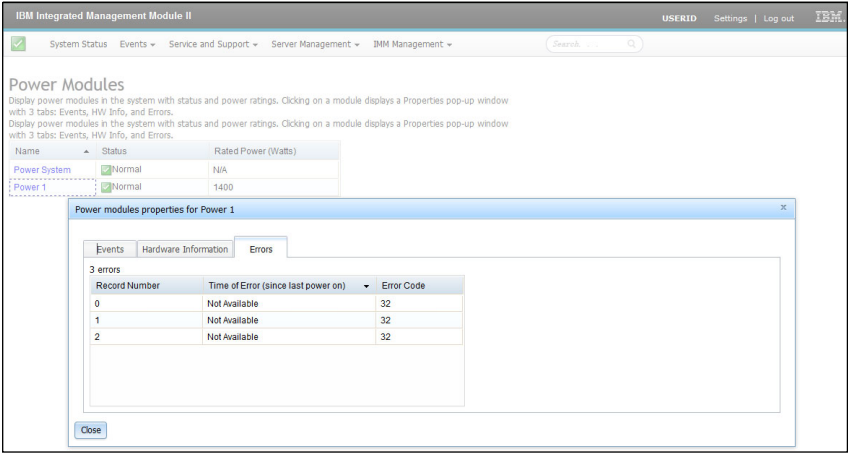
Events 选项卡将显示活动事件（如果有）（如以下屏幕所示）。



单击 **Hardware Information** 选项卡以查看有关组件的详细信息，如 FRU 名称和制造商标识（如下图所示）。

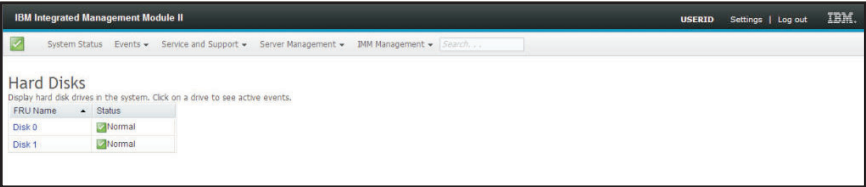


单击 **Errors** 选项卡以查看有关电源模块错误的详细信息（如下图所示）。



Disks

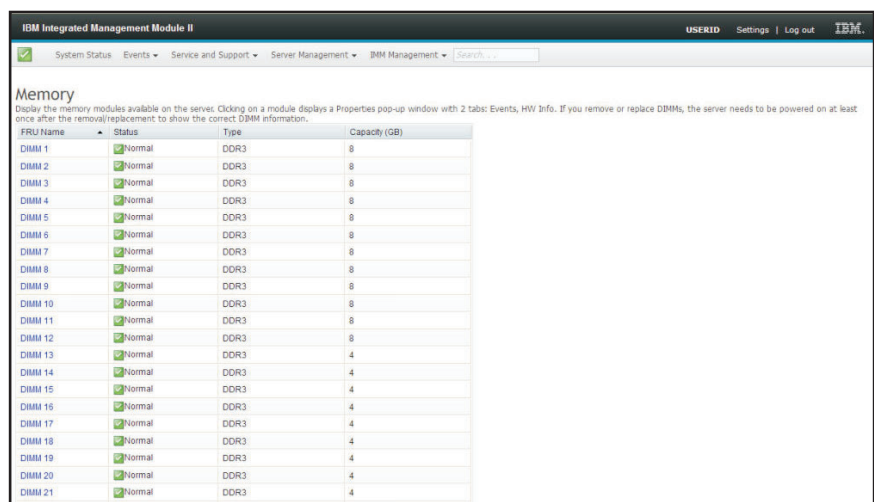
选择 **Server Management** 选项卡下的 **Disks** 选项，以查看系统中的硬盘驱动器（如下图所示）。单击硬盘驱动器，以查看与该硬盘驱动器关联的事件。



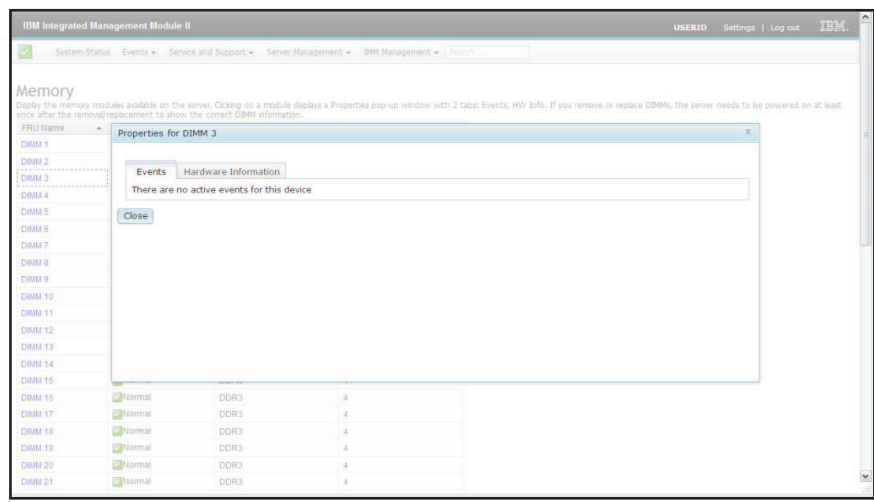
Memory

选择 **Server Management** 选项卡下的 **Memory** 选项，以查看有关系统中安装的内存条的信息。此时将打开以下窗口。每个内存条在表中都显示为链接，可以单击链接以获取有关内存条的更详细信息。该表还显示 DIMM 状态、DIMM 类型和 DIMM 容量。

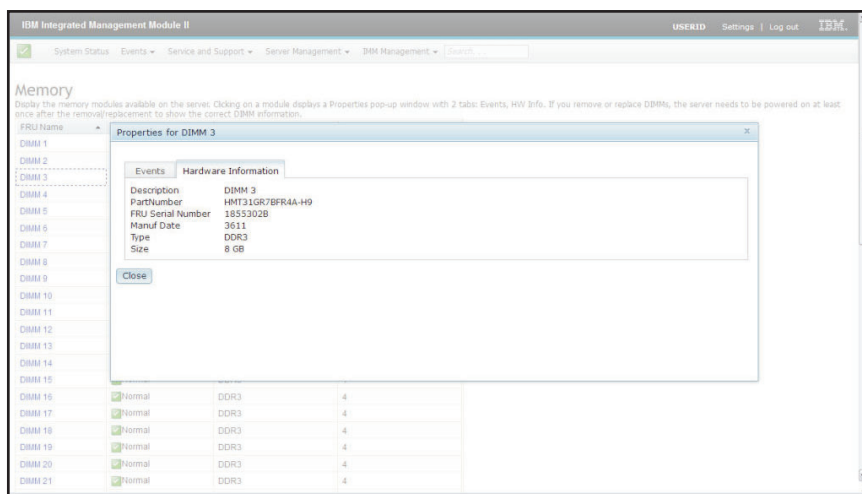
注：如果卸下或更换 DIMM，那么必须重新启动系统来查看已更新的 DIMM 信息，从而了解对系统 DIMM 进行的更改。



单击表中的 **DIMM** 链接，以查看任何活动事件以及有关组件的更多信息（如以下屏幕中所示）。

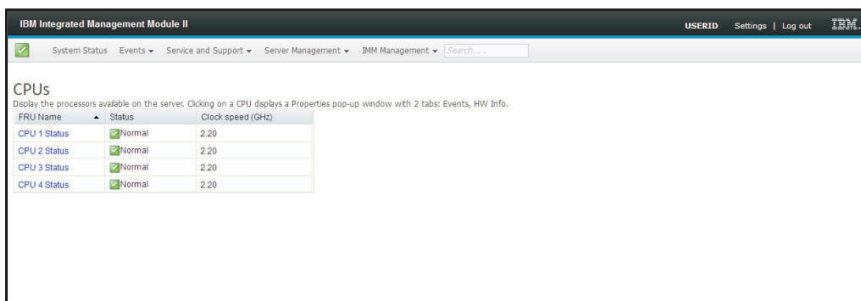


单击 **Hardware Information** 选项卡以查看有关组件的详细信息，如描述、部件号、FRU 序列号、制造日期（周/年）、类型（例如 DDR3）和以千兆字节为单位的大小（如下图所示）。

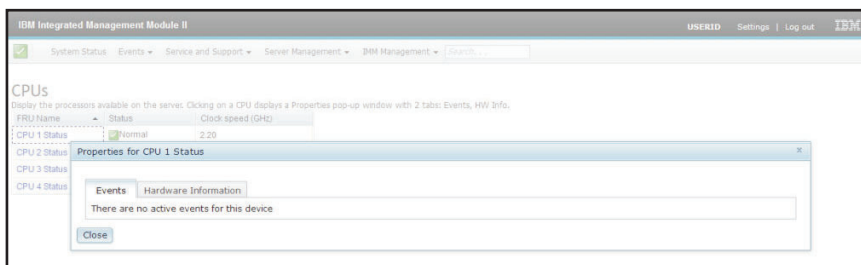


Processors

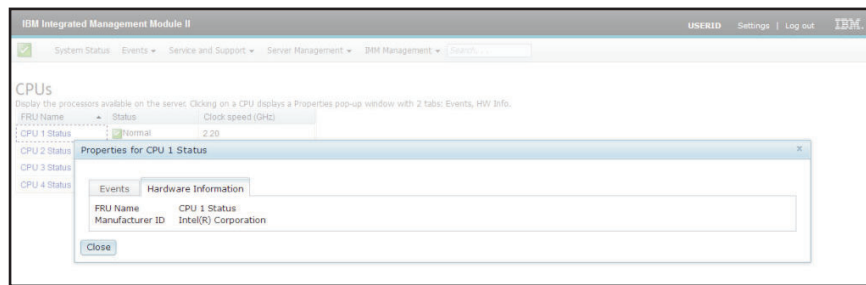
选择 **Server Management** 选项卡下的 **Processors** 选项以查看有关系统中安装的微处理器的信息。此时将打开以下窗口。



单击表中的 **CPU** 链接以查看任何活动事件以及有关组件的更多信息（如下图所示）。



单击 **Hardware Information** 选项卡以查看有关组件的详细信息，如 FRU 名称和制造商标识（如下图所示）。

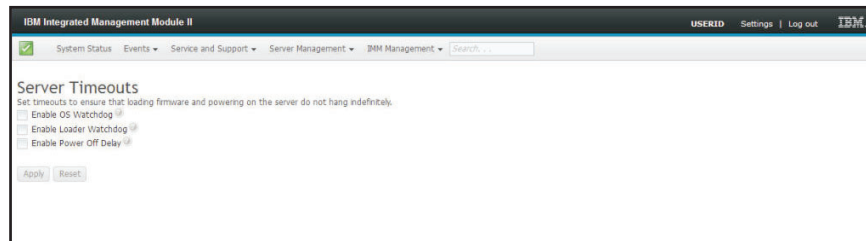


Server Timeout

选择 **Server Management** 选项卡下的 **Server Timeouts** 选项以设置超时，确保在固件更新和开启服务器期间，服务器不会无限期地挂起。您可以通过设置选项值来启用此功能。

注：服务器超时要求启用频带内 USB 接口或 LAN over USB 以使用命令。有关配置 USB 接口的更多信息，请参阅第 86 页的『配置 USB』。

下图显示 **Server Timeouts** 窗口。



有关服务器超时的其他信息，请参阅第 62 页的『设置服务器超时』。

PXE 网络引导

选择 **Server Management** 选项卡下方的 **PXE Network Boot** 选项可将服务器设置为在下次服务器重新启动时尝试进行 PXE 网络引导。有关设置 PXE 网络引导的更多信息，请参阅第 120 页的『设置 PXE 网络引导』。

Latest OS Failure Screen

选择 **Server Management** 选项卡下的 **Latest OS Failure Screen** 选项，以查看或清除 IMM2 已保存的最近操作系统故障屏幕数据。IMM2 仅存储最近的错误事件信息，从而在发生新错误事件时覆盖较早的操作系统故障屏幕数据。

下图是操作系统故障屏幕的示例。

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

The end-user manually generated the crashdump.

If this is the first time you've seen this stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup options, and then
select Safe Mode.

Technical information:

*** STOP: 0x000000E2 (0x0000000000000000,0x0000000000000000,0x0000000000000000,0
x0000000000000000)

Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk: 100
Physical memory dump complete.
Contact your system admin or technical support group for further assistance.
```

有关 Latest OS Failure Screen 选项的更多信息，请参阅第 135 页的『捕获最新操作系统故障屏幕数据』。

IMM Management 选项卡

此部分提供有关 IMM2 Web 用户界面主页上 IMM Management 选项卡下选项的信息。

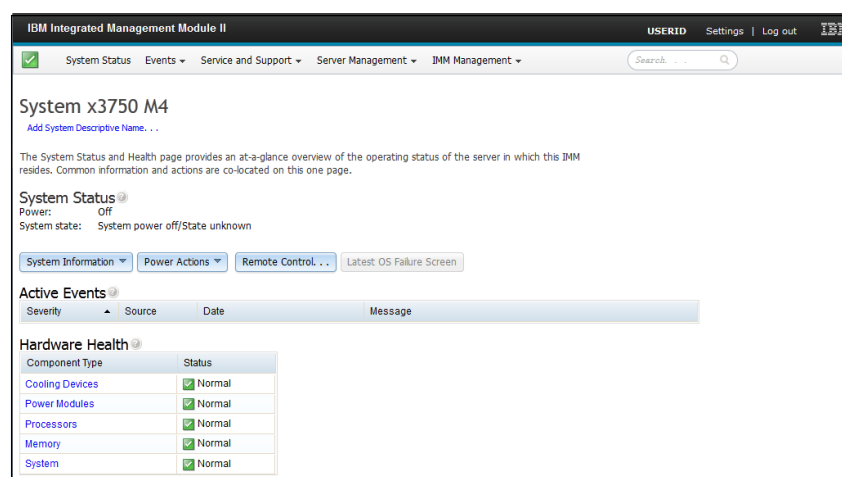
通过 IMM Management 选项卡下的选项，可以查看和修改 IMM2 设置。有关选项列表以及如何使用选项来配置 IMM2 的详细信息，请参阅第 59 页的第 4 章，『配置 IMM2』。

第 4 章 配置 IMM2

IMM Management 选项卡包含用于配置 IMM2 的选项。使用 IMM Management 选项卡以查看和更改 IMM2 设置。在 IMM Management 选项卡下列出了以下选项（如下图所示）。

- IMM Properties
- Users
- Network
- Security
- IMM Configuration
- Restart IMM
- Reset IMM to factory defaults
- Activation Key Management

注：在 IBM Flex System 中，一些设置由 IBM Flex System Chassis Management Module (CMM) 管理，而无法在 IMM2 上修改。



在 Integrated Management Module (IMM) Properties 页面中，可以执行以下功能：

- 访问服务器固件信息
- 设置日期和时间：
 - 选择 IMM2 时间设置方法：手动或 NTP
 - 针对手动设置方法设置 IMM2 日期和时间
 - 针对 NTP 设置方法设置 NTP 信息
 - 设置 IMM2 时区信息
- 访问 IMM2 串口信息：
 - 配置 IMM2 串口
 - 设置 IMM2 命令行界面 (CLI) 键序列

在 User Accounts 页面中，可以执行以下功能：

- 管理 IMM2 用户帐户：
 - 创建用户帐户
 - 单击用户名以编辑该用户的属性：
 - 编辑用户名
 - 设置用户密码
 - 为用户配置 SNMPv3 设置
 - 为用户管理安全 Shell (SSH) 公用认证密钥
 - 删除用户帐户
- 配置全局用户登录设置：
 - 设置用户认证方法
 - 设置 Web 不活动超时
 - 配置可用于 IMM2 的用户帐户安全性级别
- 查看当前连接到 IMM2 的用户

在 Network Protocol Properties 页面中，可以执行以下功能：

- 配置以太网设置：
 - 以太网设置：
 - 主机名
 - IPv4 和 IPv6 支持与地址设置
 - 高级以太网设置：
 - 自动协商支持
 - MAC 地址管理
 - 设置最大传输单元
 - 虚拟 LAN (VLAN) 支持
- 配置 SNMP 设置：
 - SNMPv1 支持和配置：
 - 设置联系人信息
 - 社区管理
 - SNMPv3 支持和配置：
 - 设置联系人信息
 - 用户帐户配置
 - SNMP 陷阱支持和配置
 - 在 Traps 选项卡中配置已发出警报的事件
- 配置 DNS 设置：
 - 设置 DNS 寻址首选项 (IPv4 或 IPv6)
 - 其他 DNS 服务器寻址支持和配置
- 配置 DDNS 设置：
 - DDNS 支持
 - 选择域名源 (定制或 DHCP 服务器)

- 为手动指定的定制源设置定制域名
- 查看 DHCP 服务器指定的域名
- 配置 SMTP 设置：
 - 设置 SMTP 服务器 IP 地址或主机名
 - 设置 SMTP 服务器端口号
 - 测试 SMTP 连接
- 配置 LDAP 设置：
 - 设置 LDAP 服务器配置（DNS 或预配置）：
 - 如果 DNS 指定了 LDAP 服务器配置，请设置搜索域：
 - 从登录标识抽取搜索域
 - 手动指定的搜索域和服务名称
 - 尝试从登录标识抽取搜索域，然后使用手动指定的搜索域和服务名称
 - 如果使用预配置 LDAP 服务器：
 - 设置 LDAP 服务器主机名或 IP 地址
 - 设置 LDAP 服务器端口号
 - 设置 LDAP 服务器根专有名称
 - 设置 UID 搜索属性
 - 选择绑定方法（匿名、使用已配置的凭证和使用登录凭证）：
 - 对于已配置的凭证，请设置客户机专有名称和密码
 - 针对 Active Directory 用户的基于角色的增强安全性支持：
 - 如果已禁用：
 - 设置组过滤器
 - 设置组搜索属性
 - 设置登录许可权属性
 - 如果已启用，请设置服务器目标名称
- 配置 Telnet 设置：
 - Telnet 访问支持
 - 设置最大 Telnet 会话数
- 配置 USB 设置：
 - Ethernet over USB 支持
 - 从外部以太网到 Ethernet over USB 的端口转发支持和管理
- 配置端口分配：
 - 查看打开的端口号
 - 设置由 IMM2 服务使用的端口号：
 - HTTP
 - HTTPS
 - Telnet CLI
 - SSH CLI
 - SNMP 代理
 - SNMP Traps

- Remote Control
- CIM over HTTPS
- CIM over HTTP

在 Security 页面中，可以执行以下功能：

- HTTPS 服务器支持和证书管理
- CIM over HTTPS 支持和证书管理
- LDAP 安全性选择和证书管理
- SSH 服务器支持和证书管理

在 IMM Configuration 页面中，可以执行以下功能：

- 查看 IMM2 配置摘要
- 备份或复原 IMM2 配置
- 查看备份或复原状态
- 将 IMM2 配置重置为其出厂缺省设置
- 访问 IMM2 初始设置向导

在 Restart IMM 页面中，可以重置 IMM2。

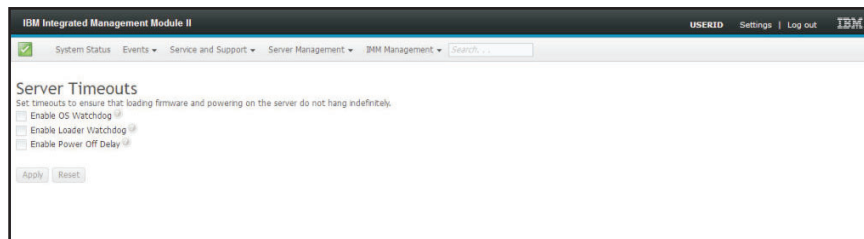
在 Reset IMM2 to factory defaults.. 页面中，可以将 IMM2 配置重置为其出厂缺省设置。

在 Activation Key Management 页面中，可以管理可选 IMM2 和服务器 Features on Demand (FoD) 的激活密钥。请参阅第 141 页的第 7 章, 『Features on Demand』，以获取有关管理 FoD 激活密钥的信息。

设置服务器超时

使用 Server Timeouts 选项可设置超时，以确保服务器不会在固件更新或服务器开机期间无限期挂起。您可以通过为此选项设置值来启用该功能，如下图所示。

注：服务器超时要求启用频带内 USB 接口或 LAN over USB 以使用命令。有关启用和禁用 USB 接口的更多信息，请参阅第 86 页的『配置 USB』。



要设置服务器超时值，请完成以下步骤：

1. 登录到要为其设置服务器超时的 IMM2。（请参阅第 10 页的『登录到 IMM2』）。
2. 单击 **Server Management**；然后，选择 **Server Timeouts**。

您可以将 IMM2 设置为自动对以下事件进行响应：

- 操作系统暂停
 - 装入操作系统失败
3. 启用与您希望 IMM2 自动响应的事件相对应的服务器超时。请参阅“Server timeout selections”，以获取关于每个选项的描述。
 4. 单击 **Apply**。

注：有一个 **Reset** 按钮，您可使用此按钮来同时清除所有超时。

服务器超时选择

Enable OS Watchdog

使用 **Enable OS Watchdog** 字段可指定 IMM2 在两次检查操作系统之间间隔的分钟数。如果操作系统未能对其中一次检查进行响应，那么 IMM2 将生成 OS 超时警报并重新启动服务器。重新启动服务器后，会禁用操作系统看守程序，直至关闭操作系统关闭并且再打开服务器电源为止。要设置 OS 看守程序值，请选择 **Enable OS Watchdog** 并从菜单中选择一个时间间隔。要关闭此看守程序，请取消选择 **Enable OS Watchdog**。要捕获操作系统故障屏幕，必须在 **Enable OS Watchdog** 字段中启用看守程序。

Enable Loader Watchdog

使用 **Enable Loader Watchdog** 字段可指定 IMM2 在 POST 完成和操作系统启动之间等待的分钟数。如果超过此时间间隔，那么 IMM2 将生成装入程序超时警报并自动重新启动服务器。重新启动服务器后，会自动禁用装入程序超时，直至关闭操作系统关闭并且再打开服务器电源（或者直至操作系统启动且软件成功装入）为止。要设置装入程序超时值，请选择 IMM2 等待操作系统启动完成的时间限制。要关闭此看守程序，请从菜单中取消选择 **Enable Loader Watchdog**。

Enable Power Off Delay

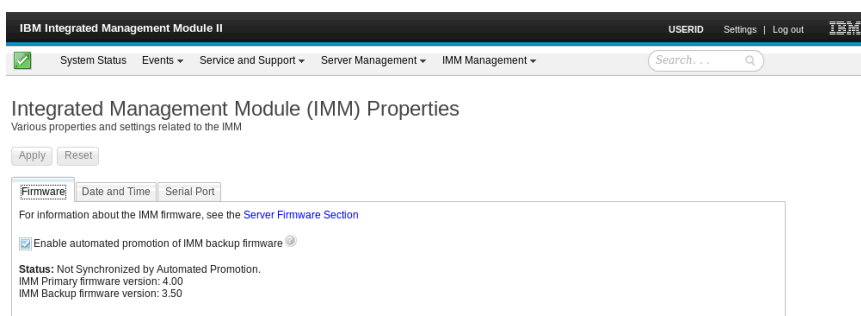
使用 **Enable Power Off Delay** 字段可指定 IMM2 子系统在关闭服务器电源之前等待操作系统关闭的分钟数。要设置断电延迟超时值，请选择操作系统关闭后 IMM2 等待的时间限制。要关闭此看守程序，请从菜单中取消选择 **Enable Loader Watchdog**。

更改 IMM2 固件自动升级设置

选择 **Firmware** 选项卡以查看或更改 IMM2 备份固件的固件自动升级设置。如果已启用自动升级功能，那么当 IMM2 固件在主区域中成功运行一段时间之后，自动升级功能会自动将该固件从主区域复制到备份区域中。此活动将使主区域和备份区域具有相同的固件版本。如果希望在主区域和备份区域中保留不同版本的 IMM2 固件，那么不应选中 **Enable automated promotion of IMM backup firmware** 复选框。

IMM2 固件会使用各种度量（如运行时量和固件活动）来验证主区域中固件的稳定性，之后才会将固件复制到备份区域中。执行自动升级之前的最小时间间隔为两周；但实际时间间隔可能会更长，这取决于该时间间隔期间发生的 IMM2 活动。

下图显示了已选中 **Enable automated promotion of IMM backup firmware** 复选框的 **Firmware** 选项卡。



设置 IMM2 日期和时间

注：无法在 IBM Flex System 中修改 IMM2 Date and Time 设置。

选择 **Date and Time** 选项卡以查看或更改 IMM2 日期和时间。IMM2 使用自己的实时时钟来为事件日志中记录的所有事件添加时间戳记。通过电子邮件和简单网络管理协议 (SNMP) 发送的警报使用实时时钟设置来为警报添加时间戳记。时钟设置支持格林威治标准时间 (GMT) 偏移和夏令时，从而为通过不同时区远程管理系统的管理员增强易用性。即使关闭或禁用服务器，也可以远程访问事件日志。

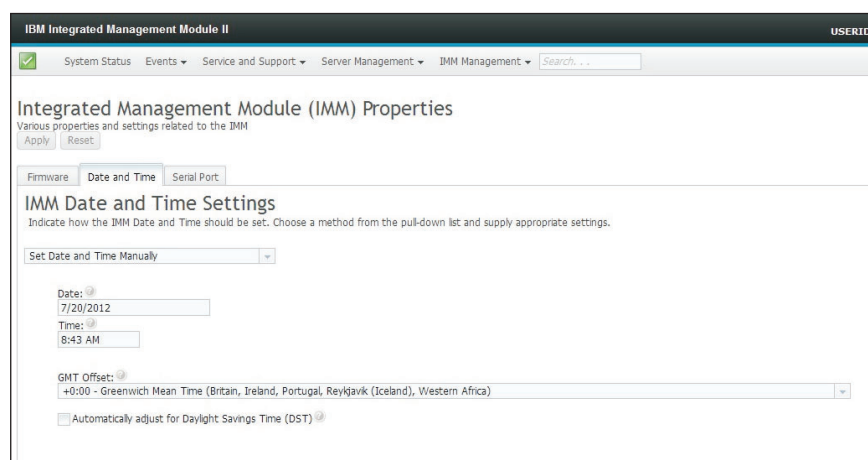
IMM2 日期和时间设置仅影响 IMM2 时钟而不影响服务器时钟。IMM2 实时时钟和服务器的时钟是分离的单独时钟，可以设置为不同的时间。

更改时间和日期设置（手动方式）

完成以下步骤以手动更改时间和日期设置：

1. 在 **Indicate how the IMM date and time should be set** 菜单列表中，单击 **Set Date and Time Manually**。
2. 在 **Date** 字段中，输入当前的年月日。
3. 在 **Time** 字段中，输入对应于当前小时和分钟的数字。
 - 小时必须是 1- 12 的数字，以 12 小时时钟表示。
 - 分钟必须是 00 - 59 的数字。
 - 选择 **AM** 或 **PM**。
4. 在 **GMT Offset** 字段中，选择用于指定与 GMT 之间的偏移（以小时为单位）的数字。此数字必须与服务器所在的时区对应。
5. 选中或取消选中 **Automatically adjust for Daylight Saving Time (DST)** 复选框，以指定当本地时间在标准时间和夏令时之间更改时 IMM2 时钟是否自动调整。

下图显示手动设置日期和时间时的 IMM Date and Time 选项卡。

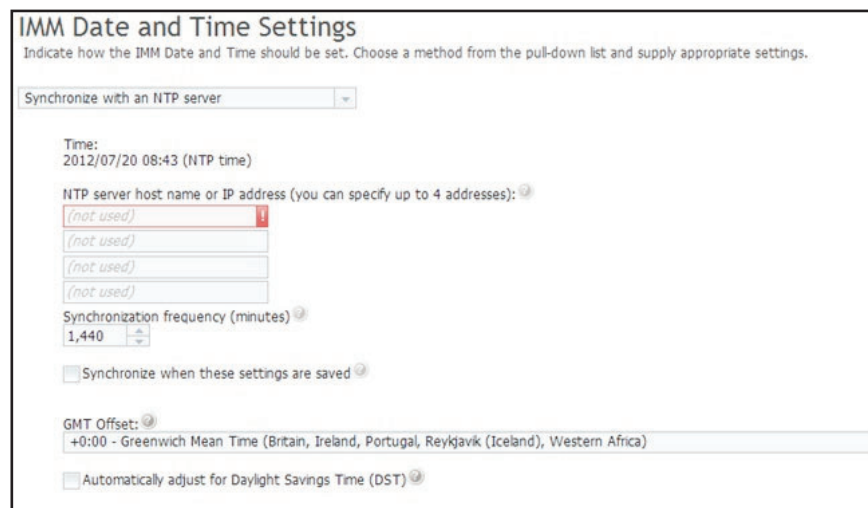


更改时间和日期设置（NTP 服务器方式）

完成以下步骤以将 IMM2 时钟与服务器时钟同步：

1. 在 **Indicate how the IMM date and time should be set** 菜单列表中，单击 **Synchronize with an NTP server**。
2. 在 **NTP server host name or IP address** 字段中，指定要用于时钟同步的 NTP 服务器的名称。
3. 在 **Synchronization frequency (in minutes)** 字段中，指定同步请求之间的大致时间间隔。输入 3 - 1440 分钟之间的值。
4. 选中 **Synchronize when these settings are saved** 复选框，以请求立即同步（当单击 **Apply** 时）而不是等待间隔时间流逝。
5. 在 **GMT Offset** 字段中，选择用于指定与 GMT 之间的偏移（以小时为单位）的数字，对应于服务器所在的时区。
6. 选中或取消选中 **Automatically adjust for Daylight Saving Time (DST)** 复选框，以指定当本地时间在标准时间和夏令时之间更改时 IMM2 时钟是否自动调整。

下图显示与服务器时钟同步时的 IMM Date and Time 选项卡。



配置串口设置

选择 **Serial Port** 选项卡可指定主机的串口重定向。IMM2 提供两个用于串行重定向的串口：

串口 1 (COM1)

System x 服务器上的串口 1 (COM1) 用于智能平台管理接口 (IPMI) Serial over LAN (SOL)。只能通过 IPMI 界面配置 COM1。

串口 2 (COM2)

在刀片服务器上，串口 2 (COM2) 用于 SOL。在 System x 机架服务器和 IBM Flex System 上，COM2 用于通过 Telnet 或 SSH 进行串行重定向。COM2 不可通过 IPMI 界面进行配置。在机架式安装和塔式服务器上，COM2 是不提供外部访问机制的内部 COM 端口。

请填写以下串口重定向字段：

Baud Rate

在此字段中指定串口连接的数据传输率。要设置波特率，请在 9600 和 115200 之间选择与串口连接相对应的数据传输率。

Parity 在此字段中指定串口连接的奇偶位。可用选项包括 None、Odd 或 Even。

Stop Bits

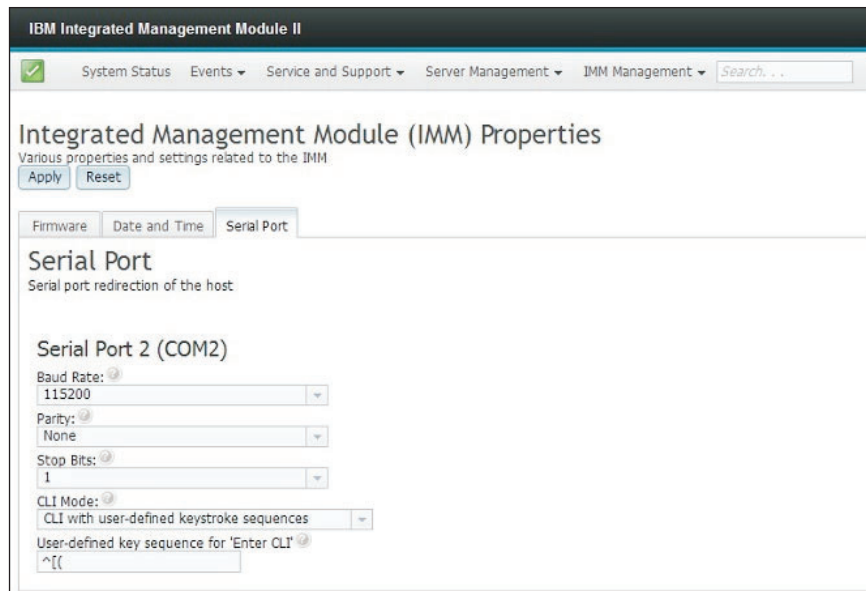
在此字段中指定串口连接的停止位的数目。可用选项包括 1 或 2。

CLI Mode

在此字段中，请选择 **CLI with IMM2 compatible keystroke sequences**；或者，如果您要使用自己的键序列，请选择 **CLI with user defined keystroke sequences**。如果选择 **CLI with user defined keystroke sequences**，那么必须在 **User-defined key sequence for 'Enter CLI'** 字段中定义键序列。

在串行重定向启动后，它会持续运行，直到您输入退出键序列为止。输入退出键序列后，串行重定向将停止，并且您将返回到 Telnet 或 SSH 会话中的命令方式。使用 **User-defined key sequence for 'Enter CLI'** 字段可指定退出键序列。

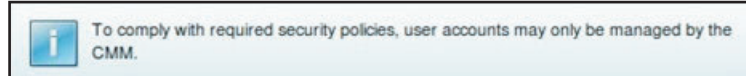
下图显示了 Serial Port 选项卡。



配置用户帐户

选择 IMM Management 选项卡下的 **Users** 选项，以创建和修改 IMM2 的用户帐户并查看组概要文件。您将看到以下参考消息。

注：在 IBM Flex System 中，IMM2 用户帐户由 CMM 管理。

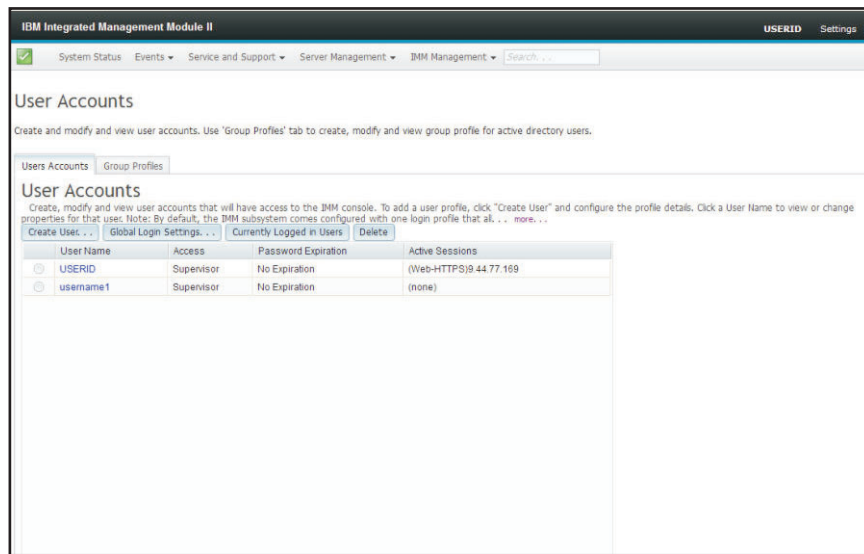


在 IBM Flex System 中，只有在 IMM2 设置中配置的用户帐户才能使用 IPMI 和 SNMPv3 协议对 IMM2 的访问权进行认证。如果用户已配置 CMM 集中管理 IMM2 上的 IPMI 和 SNMPv3 用户帐户，那么您将无法直接在 IMM2 自身上配置帐户。使用 CMM 已配置 IMM2 使用的 LDAP 服务器上的帐户凭证对其他 IMM2 界面（如 Web 和 CLI）的访问权进行认证。

用户帐户

选择 **Users Accounts** 选项卡可创建、修改和查看用户帐户，如下图所示。

注：IMM2 子系统附带了一个登录概要文件。



创建用户

单击 **Create User...** 选项卡可创建新用户帐户。请填写以下字段：**User name**、**Password** 和 **Confirm Password**（如下图所示）。

用户属性

单击 **User Properties** 选项卡可修改现有用户帐户（如下图所示）。

用户权限

单击 **Authority** 选项卡可设置用户权限级别。将提供以下用户权限级别：

Supervisor

Supervisor 用户权限级别没有任何限制。

Read only

Read only 用户权限级别具有只读访问权，并且无法执行诸如文件传输、电源和重新启动操作或远程感知功能之类的操作。

Custom

Custom 用户权限级别通过对允许用户执行的操作进行设置，来允许针对用户权限对概要文件进行更大程度定制。

选择以下一个或多个 Custom 用户权限级别：

User Account Management

用户可以添加、修改或删除用户，以及更改全局登录设置。

Remote Console Access

用户可以访问远程控制台。

Remote Console and Virtual Media Access

用户可以访问远程控制台和虚拟介质功能部件。

Remote Server Power/Restart Access

用户可以执行远程服务器的开机和重新启动功能。

Ability to Clear Event Logs

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

Adapter Configuration - Basic

用户可以在 **Server Properties** 和 **Events** 页面上修改配置参数。

Adapter Configuration - Networking & Security

用户可以在 Security、Network 和 Serial Port 页面上修改配置参数。

Adapter Configuration - Advanced

用户在配置 IMM2 时没有任何限制。此外，用户对 IMM2 具有管理访问权。管理访问权包括以下高级功能：固件更新、PXE 网络引导、复原 IMM2 出厂缺省值、通过配置文件修改并复原 IMM2 设置以及重新启动/重置 IMM2。

当用户设置 IMM2 登录标识的权限级别时，会根据以下优先级来设置对应 IPMI 用户标识的所产生的 IPMI 特权级别：

- 如果用户将 IMM2 登录标识权限级别设置为 **Supervisor**，那么 IPMI 特权级别会设置为 Administrator。
- 如果用户将 IMM2 登录标识权限级别设置为 **Read Only**，那么 IPMI 特权级别会设置为 User。
- 如果用户将 IMM2 登录标识权限级别设置为以下任何类型的访问权，那么 IPMI 特权级别会设置为 Administrator：
 - User Account Management Access
 - Remote Console Access
 - Remote Console and Remote Disk Access
 - Adapter Configuration - Networking & Security
 - Adapter Configuration - Advanced
- 如果用户将 IMM2 登录标识权限级别设置为 **Remote Server Power/Restart Access** 或 **Ability to Clear Event Logs**，那么 IPMI 特权级别会设置为 Operator。
- 如果用户将 IMM2 登录标识权限级别设置为 **Adapter Configuration - Basic**，那么 IPMI 特权级别会设置为 User。

SNMP 访问权

单击 **SNMPv3** 选项卡可设置帐户的 SNMP 访问权。将提供以下用户访问选项：

Authentication protocol

指定 **HMAC-MD5** 或 **HMAC-SHA** 作为认证协议。这些是供 SNMPv3 安全模型用于认证的算法。如果未启用 **Authentication Protocol**，将不使用任何认证协议。

Privacy protocol

可以使用加密来保护 SNMP 客户机和代理之间的数据传输。支持的方法为 **DES** 和 **AES**。仅当认证协议设置为 **HMAC-MD5** 或 **HMAC-SHA** 时，隐私协议才有效。

Privacy password

在此字段中指定加密密码。

Confirm privacy password

再次指定加密密码用于确认。

Access type

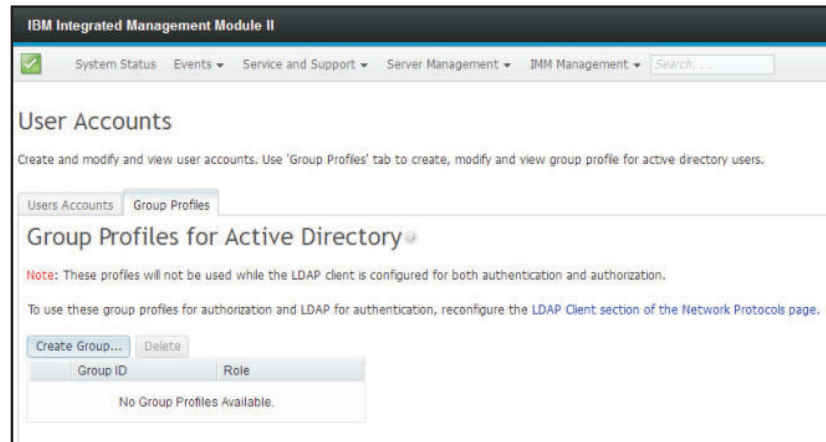
指定 **Get** 或 **Set** 作为访问类型。以 **Get** 作为访问类型的 SNMPv3 用户只能执行查询操作。以 **Set** 作为访问类型的 SNMPv3 用户可以执行查询操作并修改设置（例如，为用户设置密码）。

Hostname/IP address for traps

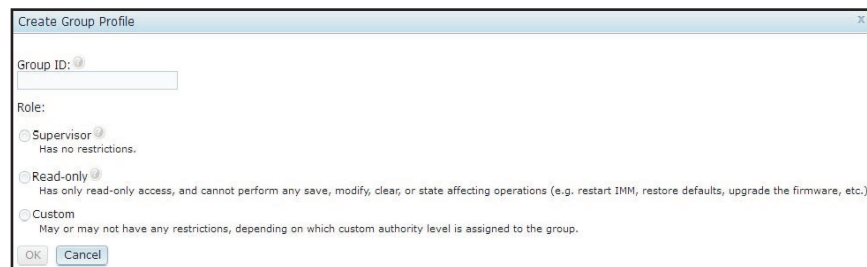
为用户指定陷阱目标。这可以是 IP 地址或主机名。通过使用陷阱，SNMP 代理会通知管理站有关事件的信息（例如，当处理器温度超过限制时）。

组概要文件

选择 **Group Profiles** 选项卡以创建、修改和查看组概要文件（如下图中所示）。

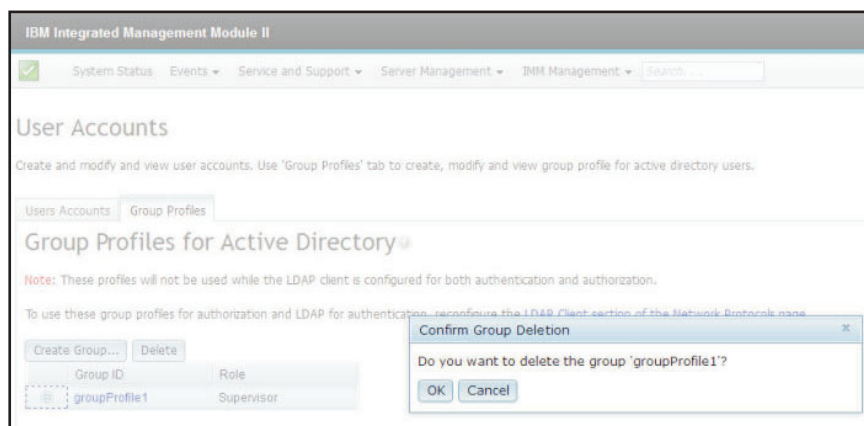


单击 **Create Group** 以创建新用户组。下图显示 Create Group Profile 窗口。



输入 **Group ID** 并选择 **Role**（请参阅第 69 页的『用户权限』，以获取有关用户权限级别的信息）。

如果需要删除组，请单击 **Delete**。下图显示 Confirm Group Deletion 窗口。



配置全局登录设置

使用 Global login settings 选项卡可配置适用于所有用户的登录设置。

常规设置

单击 **General** 选项卡可选择如何认证用户登录尝试，并指定在 IMM2 断开不活动 Web 会话的连接之前等待的时间长度（以分钟为单位）。在 **User authentication method** 字段中，您可以指定应如何认证尝试登录的用户。可以选择以下一种认证方法：

- **Local only**：通过搜索在 IMM2 上配置的本地使用帐户来认证用户。如果没有匹配的用户标识和密码，将拒绝访问。
- **LDAP only**：IMM2 尝试通过使用 LDAP 服务器来认证用户。对于此认证方法，不会搜索 IMM2 上的本地用户帐户。
- **Local first, then LDAP**：首先尝试本地认证。如果本地认证失败；那么将尝试进行 LDAP 认证。
- **LDAP first, then Local**：首先尝试 LDAP 认证。如果 LDAP 认证失败；那么将尝试进行本地认证。

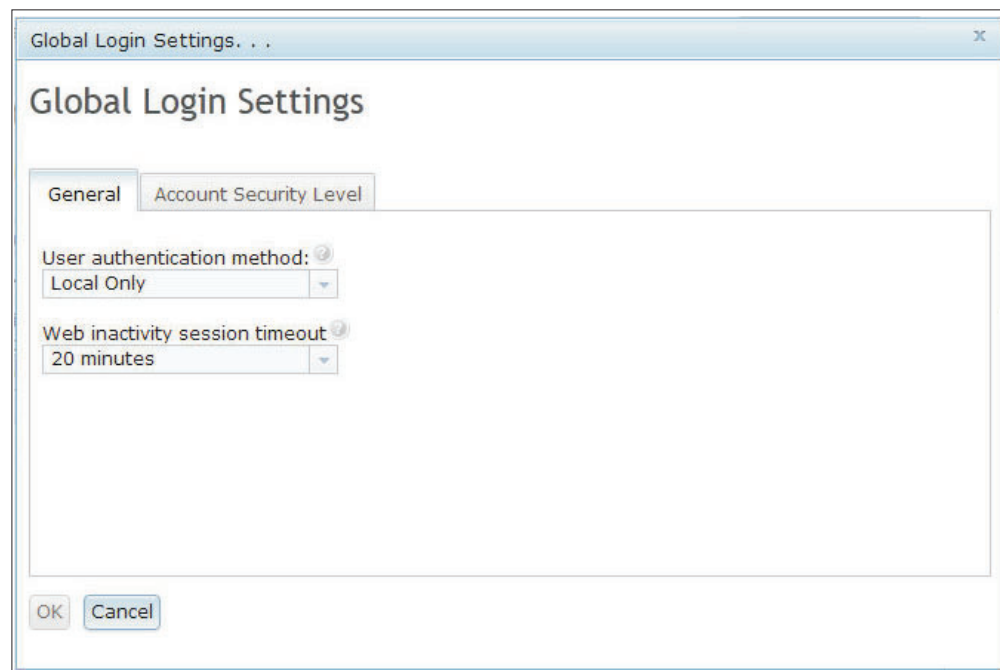
备注：

- 仅与 IPMI 和 SNMP 界面共享在本地管理的帐户。这些界面不支持 LDAP 认证。
- 当 **User authentication method** 字段设置为 **LDAP only** 时，IPMI 和 SNMP 用户可以通过使用在本地管理的帐户进行登录。

在 **Web inactivity session timeout** 字段中，您可以指定在 IMM2 断开不活动 Web 会话的连接之前等待的时间长度（以分钟为单位）。选择 **No timeout** 以禁用此功能。选择 **User picks timeout** 可选择在登录过程中的超时期。

不活动超时仅适用于不自动刷新的 Web 页面。当用户浏览某个自动刷新的 Web 页面时，如果 Web 浏览器持续请求 Web 页面更新，那么不活动超时将不会自动结束用户会话。用户可以选择是否使 Web 页面内容每 60 秒自动刷新。请参阅第 17 页的『Page Auto Refresh』，以获取描述自动刷新设置的更多信息。

下图显示了 General 选项卡。



有一些 IMM2 Web 页面即使未选择自动刷新设置时也会自动刷新。自动刷新的 IMM2 Web 页面如下：

- **System Status**：系统和电源状态将每 3 秒自动刷新。
- **Server Power Actions**：电源状态将每 3 秒自动刷新。
- **Remote Control**：Start 远程控制按钮将每 1 秒自动刷新。Session List 表将每 1 分钟自动刷新。

IMM2 固件最多同时支持 6 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，而不要依赖于不活动超时来自动关闭您的会话。

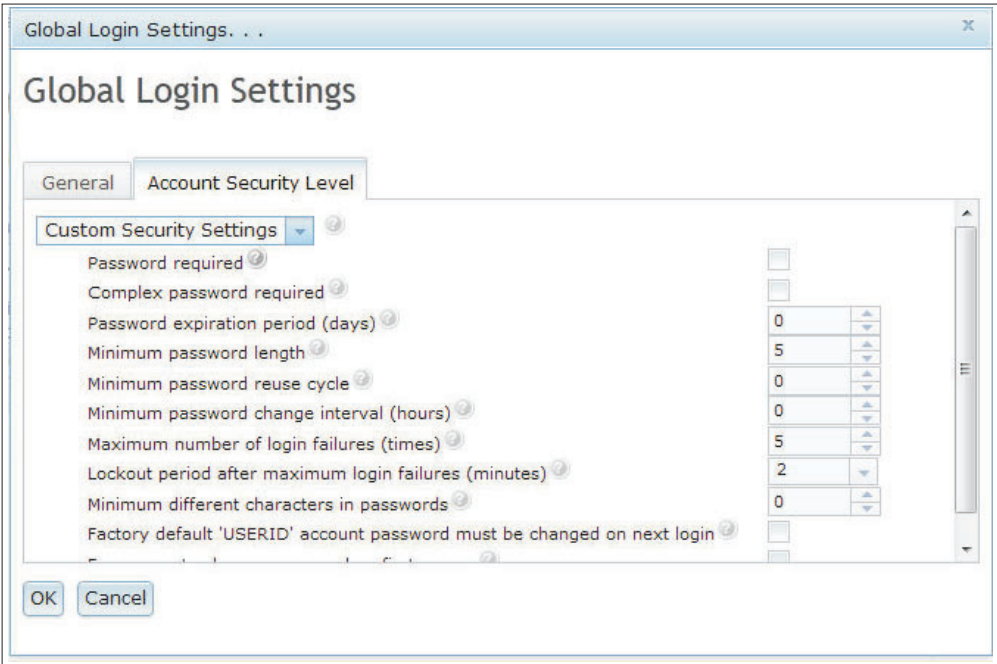
注：如果您使浏览器保持打开某个自动刷新的 IMM2 Web 页面，那么您的 Web 会话将不会由于不活动而自动关闭。

帐户安全策略设置

单击 **Account Security Level** 选项卡以选择帐户安全策略设置。帐户安全策略设置有三种级别：

- Legacy Security Settings
- High Security Settings
- Custom Security Settings

下图中显示了 Account Security Level 选项卡。



从 Security Settings 项目列表中选择帐户安全策略设置。

备注：

- Legacy Security Settings 和 High Security Settings 预先定义了策略设置值且无法更改。
- Custom Security Settings 允许用户根据需要定制安全策略。

下表显示每个安全性设置级别的值。

表 3. 安全性设置策略值

策略设置/字段	Legacy Security Settings	High Security Settings	Custom Security Settings
Password required	否	是	是或否
Complex password required	否	是	是或否
Password expiration period (days)	无	90	0 - 365
Minimum password length	无	8	5 - 20
Minimum password reuse cycle	无	5	0 - 5
Minimum password change interval (hours)	无	24	0 - 240
Maximum number of login failures (times)	5	5	0 - 10
Lockout period after maximum login failures (minutes)	2	60	0 - 240

表 3. 安全性设置策略值 (续)

策略设置/字段	Legacy Security Settings	High Security Settings	Custom Security Settings
Minimum different characters in passwords	无	2	0 - 19
Factory default 'USERID' account password must be changed on next login	否	是	是或否
Force user to change password on first access	否	是	是或否

以下信息是安全性设置字段的描述。

Password required

此字段指示是否允许创建无密码的登录标识。如果选中 **Password required** 复选框，那么用户下次登录时将要求任何无密码的现有登录标识定义密码。

Complex password required

如果需要复杂密码，那么密码必须遵守以下规则：

- 密码最小长度必须为 8 个字符。
- 密码至少应包含以下四个类别中的三个：
 - 至少一个小写字母字符。
 - 至少一个大写字母字符。
 - 至少一个数字字符。
 - 至少一个特殊字符。
- 不允许空格或空格字符。
- 密码不能包含三个以上连续使用的同一字符（例如 aaa）。
- 密码不得是关联用户标识的重复或反向拼写。

如果无需复杂密码，那么密码：

- 最小长度必须为 5 个字符（或者是 **Minimum password length** 字段中指定的数字）。
- 不能包含任何空格或空格字符。
- 至少应包含一个数字字符。
- 可以为空白（仅在禁用 **Password Required** 复选框的情况下）。

Password expiration period (days)

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 365 天。此字段的缺省值为 0（已禁用）。

Minimum password length

此字段包含密码的最小长度。针对此字段，支持 5 到 20 个字符。如果选中 **Complex password required** 复选框，那么最小密码长度至少应为 8 个字符。

Minimum password reuse cycle

此字段包含无法复用的先前密码数。可以比较最多五个先前密码。选择 0 以允许复用所有先前密码。此字段的缺省值为 0（已禁用）。

Minimum password change interval (hours)

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。此字段的缺省值为 0（已禁用）。

Maximum number of login failures (times)

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。此字段的缺省值为 0（已禁用）。

登录失败最大次数后的锁定期（分钟）

此字段指定 IMM2 子系统在检测到来自任何用户的五次以上连续登录失败后，将禁止所有用户进行远程登录尝试的时间长度（以分钟为单位）。

Minimum different characters in passwords

此字段指定新密码和先前密码之间必须不同的字符数。支持的值为 0 到 19。

Factory default 'USERID' account password must be changed on next login

提供了制造选项以在第一次成功登录后重置缺省 USERID 概要文件。启用此复选框时，必须更改缺省密码，然后才能使用该帐户。新密码遵守所有活动密码实施规则。

Force user to change password on first access

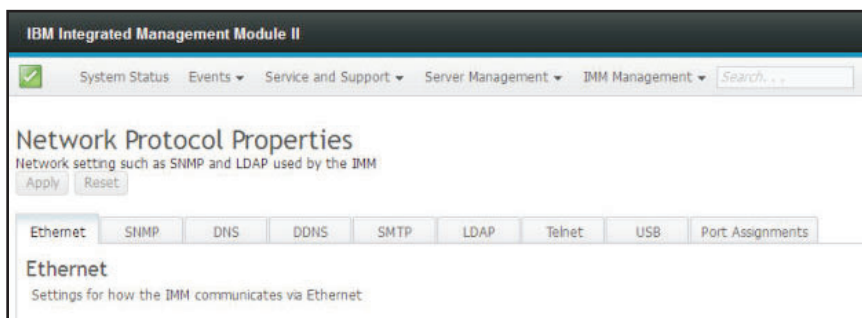
在设置具有缺省密码的新用户后，选中此复选框将强制该用户在首次登录时更改其密码。

配置网络协议

单击 IMM Management 选项卡下的 **Network** 选项可查看并设置网络设置。

配置以太网设置

单击 **Ethernet** 选项卡以查看或修改 IMM2 以太网设置（如下图中所示）。



要使用 IPv4 以太网连接，请完成以下步骤：

1. 选择 **IPv4** 选项；然后，选择对应的复选框。

注：禁用以太网接口会防止从外部网络访问 IMM2。

2. 从 **Configure IP address settings** 列表中，选择以下选项之一：

- Obtain an IP address from a DHCP server

- Use static IP address
3. 如果您希望 IMM2 在无法联系 DHCP 服务器的情况下缺省使用静态 IP 地址，请选择对应的复选框。
 4. 在 **Static address** 字段中，输入 IMM2 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。

5. 在 **Subnet mask** 字段中，输入 IMM2 所使用的子网掩码。

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。缺省设置为 255.255.255.0。

6. 在 **Default Gateway** 字段中，输入网关路由器。

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。

下图显示 Ethernet 选项卡。

The screenshot shows the 'Ethernet' configuration window with the 'Advanced Ethernet' tab selected. The 'Host name' field contains 'IMM2-e41f13d90631'. Below this, the 'IPv4' tab is active, and the 'Enable IPv4' checkbox is checked. A section titled 'Currently assigned IPv4 address information' displays a table of network parameters. Below this, the 'Configure IP address settings' section shows a dropdown menu with 'Obtain IP address from DHCP server' selected, and 'Use static IP address' is also visible. At the bottom, fields for 'Static address', 'Subnet mask', and 'Default gateway' are shown with values 192.168.70.125, 255.255.255.0, and 0.0.0.0 respectively.

	Address
Host name	IMM2-e41f13d90631
IP address	9.37.189.59
Subnet mask	255.255.240.0
Gateway address	9.37.176.1
Domain name	raleigh.ibm.com
Primary DNS Server	9.0.128.50
Second DNS Server	9.0.130.50
Tertiary DNS Server	0.0.0.0

Static address:	192.168.70.125
Subnet mask:	255.255.255.0
Default gateway:	0.0.0.0

配置高级以太网设置

单击 **Advanced Ethernet** 选项卡以设置其他以太网设置。

要启用虚拟 LAN (VLAN) 标记，请选择 **Enable VLAN** 复选框。启用 VLAN 并配置 VLAN ID 之后，IMM2 仅接受具有所指定 VLAN ID 的包。可以使用 1 到 4094 之间的数字值配置 VLAN ID。

从 **MAC selection** 列表中选择以下选项之一：

- Used burned in MAC address

- 烧录 MAC 地址选项是制造商向此 IMM2 分配的唯一物理地址。该地址是只读字段。
- Used locally administered MAC address
 - 如果指定了一个值，那么局部管理地址会覆盖烧录 MAC 地址。局部管理地址必须是从 000000000000 到 FFFFFFFF 的十六进制值。该值的格式必须为 xx:xx:xx:xx:xx:xx，其中 x 是从 0 到 9 的数字。IMM2 不支持使用多点广播地址。多点广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 **Maximum transmission unit** 字段中，为您的网络接口指定包的最大传输单元（以字节为单位）。最大传输单元范围从 60 到 1500。此字段的缺省值为 1500。

下图显示 Advanced Ethernet 选项卡和关联字段。

The screenshot shows the 'Network Protocol Properties' page for the IBM Integrated Management Module II. The 'Ethernet' tab is selected, and the 'Advanced Ethernet' sub-tab is active. The page displays settings for how the IMM communicates via Ethernet. Key settings include: 'Use Autonegotiation' (checked), 'Enable VLAN' (checked) with a value of 4094, 'MAC selection' set to 'Use burned-in MAC address' with a burned-in MAC address of 6cae:8b:4b:3d:ed, and 'Maximum transmission unit (bytes)' set to 1,500. There are 'Apply' and 'Reset' buttons at the top of the settings area.

配置 SNMP 警报设置

请完成以下步骤以配置 IMM2 SNMP 设置。

1. 单击 **SNMP** 选项卡（如下图所示）。

The screenshot shows the 'Network Protocol Properties' page for the IBM Integrated Management Module II, with the 'SNMP' tab selected. The page displays settings for the Simple Network Management Protocol (SNMP). Key settings include: 'Enable SNMPv1 Agent' (unchecked), 'Enable SNMPv3 Agent' (unchecked), and 'Enable SNMP Traps' (unchecked). There are 'Apply' and 'Reset' buttons at the top of the settings area.

2. 选中相应的复选框以启用 SNMPv1 代理程序、SNMPv3 代理程序或 SNMP 陷阱。
3. 如果启用 SNMPv1 代理程序，请继续执行步骤 4。如果启用 SNMPv3 代理程序，请继续执行步骤 5。如果启用 SNMP 陷阱，请继续执行步骤 6
4. 如果启用 SNMPv1 代理程序，请填写以下字段：
 - a. 单击 **Contact** 选项卡。在 **Contact person** 字段中，输入联系人的姓名。在 **Location** 字段中，输入位置（地理坐标）。
 - b. 单击 **Communities** 选项卡来设置社区，以定义 SNMP 代理和 SNMP 管理器之间的管理关系。必须定义至少一个社区。

备注：

- 如果显示错误消息窗口，请对错误窗口中列出的字段进行必要的调整；然后，滚动到页面顶部并单击 **Apply** 以保存已更正的信息。
- 必须配置至少一个社区才能启用此 SNMP 代理。

填写以下字段：

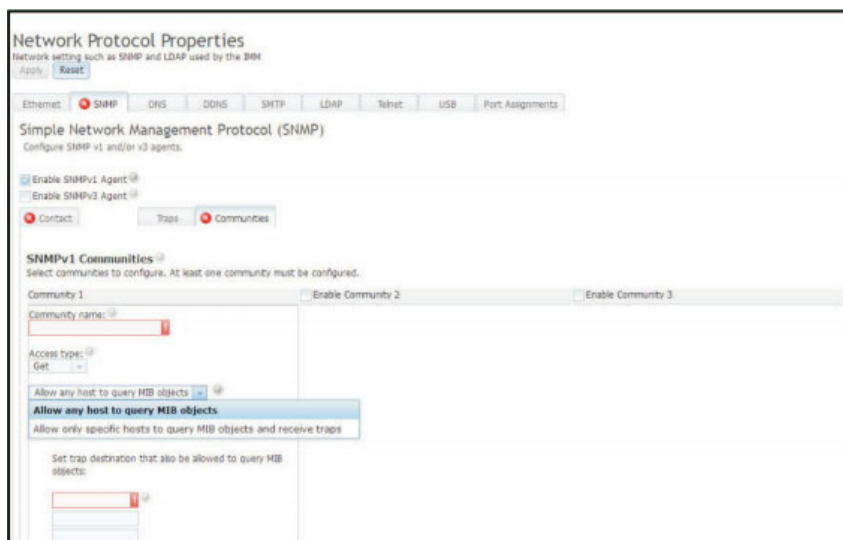
- 1) 在 **Community Name** 字段中，输入名称或认证字符串以指定社区。
 - 2) 在 **Access type** 字段中，选择访问类型。
 - 选择 **Trap** 以允许社区中的所有主机接收陷阱。
 - 选择 **Get** 以允许社区中的所有主机接收陷阱并查询管理信息基础 (MIB) 对象。
 - 选择 **Set** 以允许社区中的所有主机接收陷阱、查询并设置 MIB 对象。
 - c. 在 **Host Name** 或 **IP Address** 字段中，输入每个社区管理器的主机名或 IP 地址。
 - d. 单击 **Apply** 以应用所作更改。
5. 如果启用 SNMPv3 代理程序，请填写以下字段：
 - a. 单击 **Contact** 选项卡。在 **Contact person** 字段中，输入联系人的姓名。在 **Location** 字段中，输入位置（地理坐标）。
 - b. 单击 **Users** 选项卡以显示控制台的本地用户帐户的列表。

注：此列表与 Users 选项中的列表相同。您必须为将需要 SNMPv3 访问权的每个用户帐户配置 SNMPv3。

- c. 单击 **Apply** 以应用所作更改。
6. 如果启用 SNMP 陷阱，请配置 **Traps** 选项卡中已发出警报的事件。

注：配置 SNMP 时，如果必填字段未填写或者具有不正确的值，将以红色 X 突出显示，这可用于协助您填写必填字段。

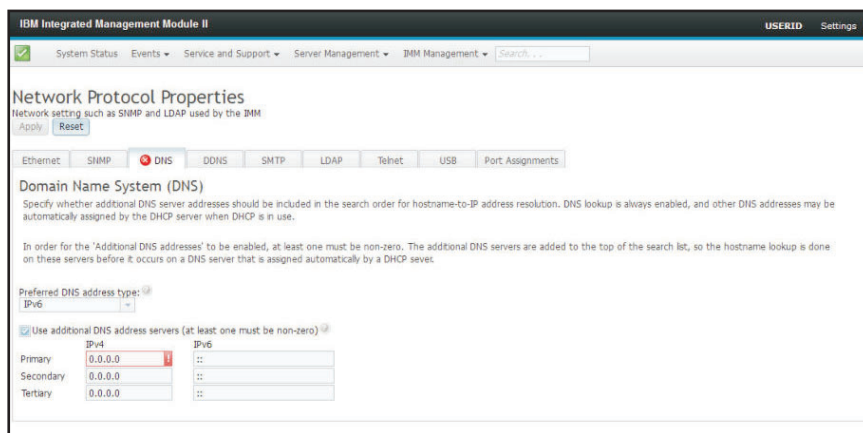
下图显示了配置 SNMPv1 代理程序时的 SNMP 选项卡。



配置 DNS

注：在 IBM Flex System 中，无法在 IMM2 上修改 DNS 设置。DNS 设置由 CMM 管理。

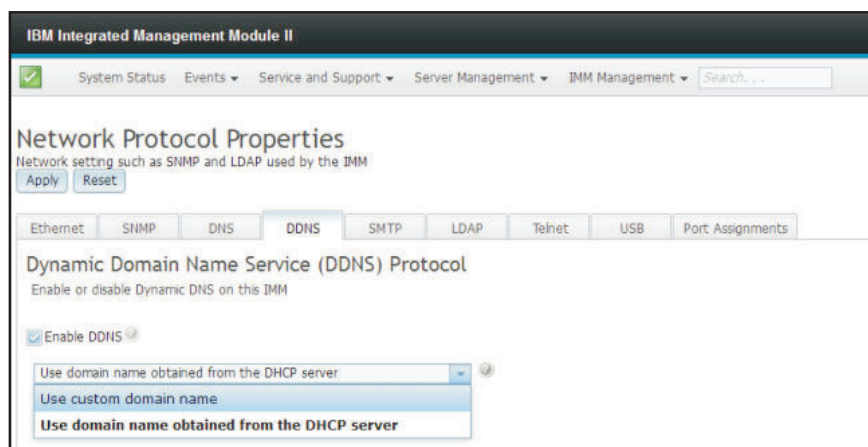
单击 **DNS** 选项卡可查看或修改 IMM2 域名系统设置。如果单击 **Use additional DNS address servers** 复选框，最多可指定您网络上的三个域名系统服务器的 IP 地址。每个 IP 地址都必须包含以句点分隔的 0 到 255 之间的整数（如下图所示）。



配置 DDNS

单击 **DDNS** 选项卡以查看或修改 IMM2 动态域名系统设置。单击 **Enable DDNS** 复选框以启用 DDNS。当启用了 DDNS 时，IMM2 会通知域名服务器实时更改其所配置的主机名、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，以选取要如何选择 IMM2 的域名（如下图所示）。



配置 SMTP

单击 **SMTP** 选项卡可查看或修改 IMM2 SMTP 设置。请填写以下字段以查看或修改 SMTP 设置：

IP 地址或主机名

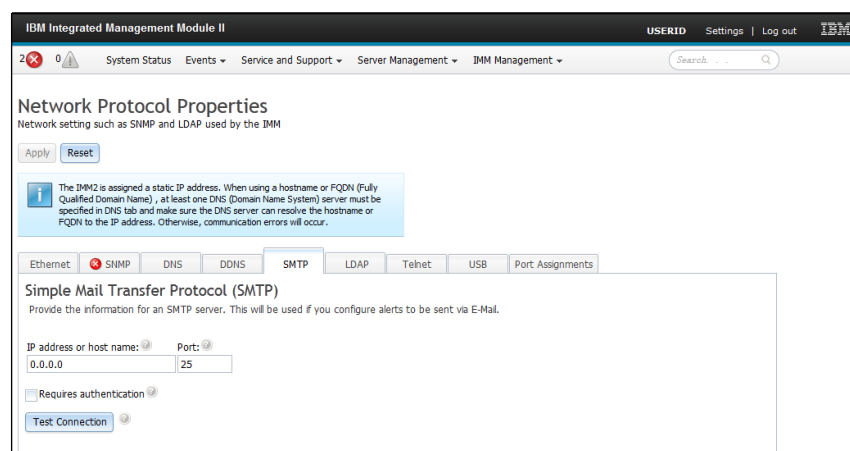
输入 SMTP 服务器的主机名。使用此字段来指定 SMTP 服务器的 IP 地址或主机名（如果启用并配置了 DNS）。

Port 指定 SMTP 服务器的端口号。缺省值为 25。

Test connection

单击 **Test Connection**，将发送一封测试电子邮件以验证您的 SMTP 设置是否正确。

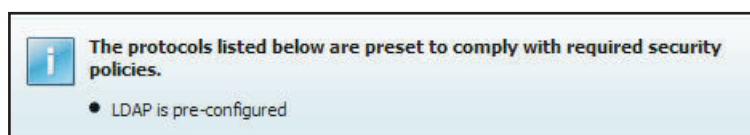
下图显示了 SMTP 选项卡。



配置 LDAP

单击 **LDAP** 选项卡可查看或修改 IMM2 LDAP 客户机设置。

注：在 IBM Flex System 中，IMM2 设置为使用在 CMM 上运行的 LDAP 服务器。您将看到一条参考消息，提醒您无法更改 LDAP 设置（如下图所示）。



IMM2 可以使用 LDAP 服务器，通过查询或搜索 LDAP 服务器上的 LDAP 目录（而不是检查其本地用户数据库）对用户进行认证。IMM2 可以通过中央 LDAP 服务器来远程认证任何用户访问。您可以根据在 LDAP 服务器上找到的信息来分配权限级别。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和 IMM2 并执行组认证。例如，IMM2 可以与一个或多个组关联，仅当用户属于至少一个与 IMM2 关联的组时，该用户才会传递组认证。

下图显示了 LDAP 选项卡。

A screenshot of the IBM Integrated Management Module II (IMM2) web interface. The title bar says "IBM Integrated Management Module II" and "USER1". The main menu includes "System Status", "Events", "Service and Support", "Server Management", and "IMM Management". The "Network Protocol Properties" section is active, showing "Network setting such as SNMP and LDAP used by the IMM". Below this are tabs for "Ethernet", "SNMP", "DNS", "DDNS", "SMTP", "LDAP", "Telnet", "USB", and "Port Assignments". The "LDAP" tab is selected, showing the "Lightweight Directory Access Protocol (LDAP) Client" configuration. It includes a description of the client, a dropdown for "Use LDAP Servers for: Authentication and Authorization", and "Active Directory Settings" with a checkbox for "Enable enhanced role-based security for Active Directory Users". Below this is a section for "Use Pre-configured LDAP servers" with a table of "Host name or IP address" and "Port". The table has one row with "0.0.0.0" and "389". There are also "Miscellaneous Settings" including "Root distinguished name", "UID search attribute" (set to "sAMAccountName"), "Binding method" (set to "Anonymously"), "Group Filter", "Group Search Attribute" (set to "memberOf"), and "Login Permission Attribute".

要使用预先配置的 LDAP 服务器，请填写以下字段：

LDAP server configuration item list

从项目列表中选择 **Use Pre-Configured LDAP Server**。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 连接使用缺省值 389。对于加密连接，缺省值是 636。必须至少配置一个 LDAP 服务器。

Root distinguished name

这是 LDAP 服务器上的目录树根条目的专有名称（DN）（例如，dn=mycompany,dc=com）。此 DN 用作所有搜索的基础对象。

UID search attribute

当绑定方法设置为 **Anonymously** 或 **With Configured Credentials** 时，在初始绑定到 LDAP 服务器后，将后跟一个搜索请求，该请求将检索有关用户的

特定信息，其中包括用户的 DN、登录许可权和组成员资格。此搜索请求必须指定代表该服务器上用户标识的属性名称。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，那么缺省值是 **uid**。

Binding method

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。将提供以下绑定方法：

- Anonymously
 - 使用此方法可不使用 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，所以强烈建议不要使用该方法。
- With Configured Credentials
 - 使用此方法可使用已配置的客户机 DN 和密码进行绑定。
- With Login Credentials
 - 使用此方法可使用在登录过程中提供的凭证进行绑定。可以通过 DN、标准域名或者用户标识（与 IMM2 上配置的 **UID Search Attribute** 相匹配）来提供用户标识。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。如果此次尝试失败，将拒绝用户访问。仅当使用 **Anonymous** 或 **With Configured Credentials** 绑定方法时，才会执行第二次绑定。

Group Filter

Group Filter 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。配置组过滤器后，它将用于指定服务处理器所属的组。这意味着用户必须至少属于一个已配置的组，组认证才能成功。如果 **Group Filter** 字段留空，那么组认证将自动成功。如果配置了组过滤器，将尝试将该列表中的至少一个组与用户所属的组相匹配。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。

比较是区分大小写的。过滤器限制为 511 个字符，并且可以包含一个或多个组名。必须使用冒号 (:) 字符对多个组名进行定界。将忽略前导空格和尾随空格，但会将任何其他空格视为组名的一部分。提供了允许或禁止在组名中使用通配符的选项。过滤器可以是特定组名（例如，IMMWest）、星号 (*)（用作可匹配任何内容的通配符），或者带有前缀的通配符（例如，IMM*）。缺省过滤器是 IMM*。如果您安装中的安全策略禁止使用通配符，那么可以选择不允许使用通配符。然后，通配符 (*) 将处理为一般字符而非通配符。可以将组名指定为完整 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，才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，那么还会将该用户称为 GroupC 的成员。嵌套搜索将在搜索过 128 个组后停止。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。

Group Search Attribute

在 Active Directory 或 Novell eDirectory 环境中，**Group Search Attribute**

字段指定用于标识用户所属的组的属性名称。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，该字段指定用于标识特定 PosixGroup 的成员的属性名称。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缺省设置为 **memberOf**。

Login Permission Attribute

当用户通过某个 LDAP 服务器认证成功后，必须检索该用户的登录许可权。要检索登录许可权，发送到该服务器的搜索过滤器必须指定与登录许可权相关联的属性名称。**Login Permission Attribute** 字段指定该属性名称。如果该字段留空，那么将为用户分配缺省的只读许可权（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。这些位根据它们的位置进行编号。左边第一位是位置 0 位，右边第一位是位置 11 位。当某个位置位的值为 1 时，将启用与该位置位相关联的功能。当某个位置位的值为 0 时，将禁用与该位置位相关联的功能。

字符串 **IBMRBSPermissions=010000000000** 就是一个有效示例。**IBMRBSPermissions=** 关键字用于允许将其放置在该字段的任意位置。这使 LDAP 管理员能够复用现有属性；因此，禁止对 LDAP 模式进行扩展。这还使该属性用于其原始用途。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，将根据下表中的信息对 LDAP 服务器返回的值进行解释。

表 4. 许可权位

位位置	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	Supervisor 访问权	授予用户管理员特权。用户对每个功能具有读/写访问权。如果设置此位，那么不必分别设置其他位。
2	Read Only 访问权	用户具有只读访问权，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）。位位置 2 和所有其他位互斥，其中位位置 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 Security、Network Protocols、Network Interface、Port Assignments 和 Serial Port 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 Login Profiles 窗口中更改 Global Login Settings。
5	远程控制台访问	用户可以访问远程服务器控制台。

表 4. 许可权位 (续)

位位置	功能	说明
6	远程控制台和远程磁盘访问	用户可以访问远程服务器的远程服务器控制台和远程磁盘功能。
7	远程服务器电源/重新启动访问	用户可以访问远程服务器的开机和重新启动功能。
8	基本适配器配置	用户可以在 System Settings 和 Alerts 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，用户需要具有此许可权级别才能清除日志。
10	高级适配器配置	用户在配置 IMM2 时没有任何限制。此外，用户对 IMM2 具有管理访问权。用户可以执行以下高级功能：固件升级、PXE 网络引导、复原 IMM2 出厂缺省值、通过配置文件修改并复原适配器配置以及重新启动/重置 IMM2。
11	保留	此位置位保留供将来使用。如果未设置任何位，那么用户具有只读权限。将向直接从用户记录中检索到的登录许可权指定优先级。 如果在用户记录中没有登录许可权属性，那么将尝试从用户所属的组中检索许可权。此操作在组认证阶段中执行。将向用户分配对所有组的所有位按包含性 OR 方式计算所得的结果。 仅当其他所有位均设置为零时，才会设置“只读访问”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。

配置 Telnet

选择 **Telnet** 选项卡可查看或修改 IMM2 Telnet 设置。请填写以下字段以查看或修改 Telnet 设置：

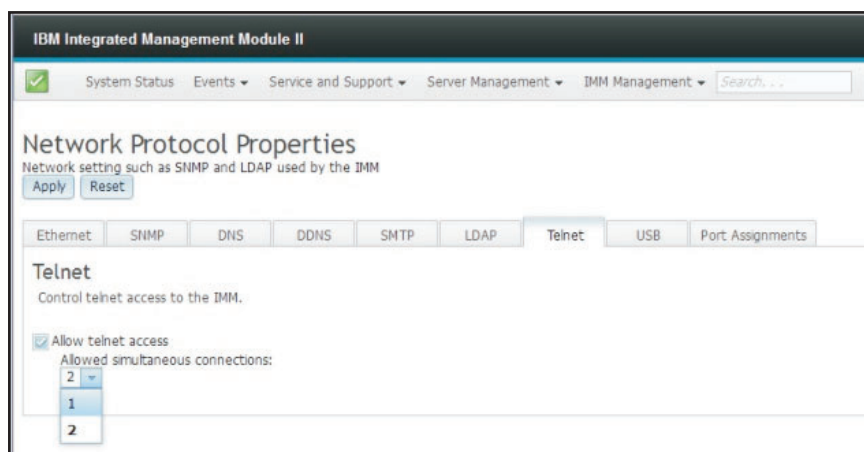
Allow telnet access

在复选框中单击以选择您是否希望 IMM2 允许 Telnet 访问。

Allowed simultaneous connections

使用 **Allowed simultaneous connections** 列表以选择在相同时间允许的 Telnet 连接数。

下图显示了 Telnet 选项卡。

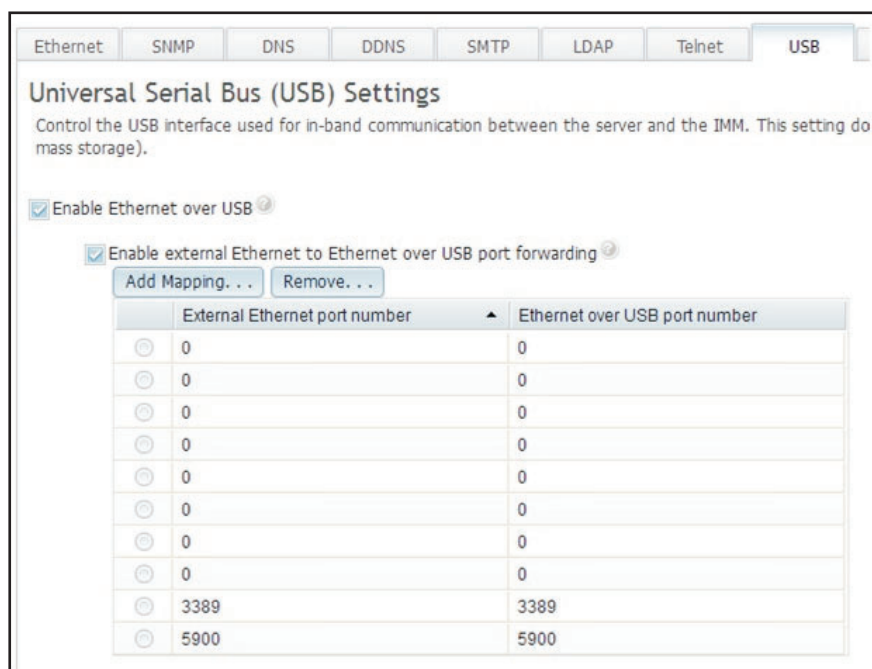


配置 USB

选择 **USB** 选项卡以查看或修改 IMM2 USB 设置。USB 频带内接口或 LAN over USB 用于与 IMM2 的频带内通信。单击 **Enable Ethernet over USB** 复选框，以启用或禁用 IMM2 LAN over USB 接口。

要点：如果禁用 USB 频带内接口，那么将无法使用 Linux 或 Windows 闪存实用程序对 IMM2 固件、服务器固件和 DSA 固件执行频带内更新。如果禁用了 USB 频带内接口，请使用 Server Management 选项卡下的 Firmware Server 选项来更新固件。如果禁用 USB 频带内接口，请同时禁用看守程序超时，以防止服务器意外重新启动。

下图显示 USB 选项卡。



通过单击 **Enable external Ethernet to Ethernet over USB port forwarding** 复选框，并完成您希望已转发的端口的映射信息，可以控制外部以太网端口号到 Ethernet over USB 端口号的映射。

配置端口分配

选择 **Port Assignments** 选项卡可查看或修改 IMM2 端口分配。请填写以下字段以查看或修改端口分配：

HTTP 在此字段中指定 IMM2 的 HTTP Server 的端口号。缺省值为 80。有效端口号值为 1 到 V65535。

HTTPS

在此字段中指定用于 Web 界面 HTTPS 安全套接字层 (SSL) 流量的端口号。缺省值为 443。有效端口号值为 1 到 V65535。

Telnet CLI

在此字段中指定 Legacy CLI 通过 Telnet 服务进行登录的端口号。缺省值为 23。有效端口号值为 1 到 V65535。

SSH Legacy CLI

在此字段中指定为 Legacy CLI 通过 SSH 协议进行登录而配置的端口号。缺省值为 22。

SNMP Agent

在此字段中指定在 IMM2 上运行的 SNMP 代理的端口号。缺省值为 161。有效端口号值为 1 到 V65535。

SNMP Traps

在此字段中指定用于 SNMP 陷阱的端口号。缺省值为 162。有效端口号值为 1 到 V65535。

Remote Control

在此字段中指定远程控制功能部件用于查看服务器控制台并与其进行交互的端口号。对于机架式安装和塔式服务器，缺省值为 3900。

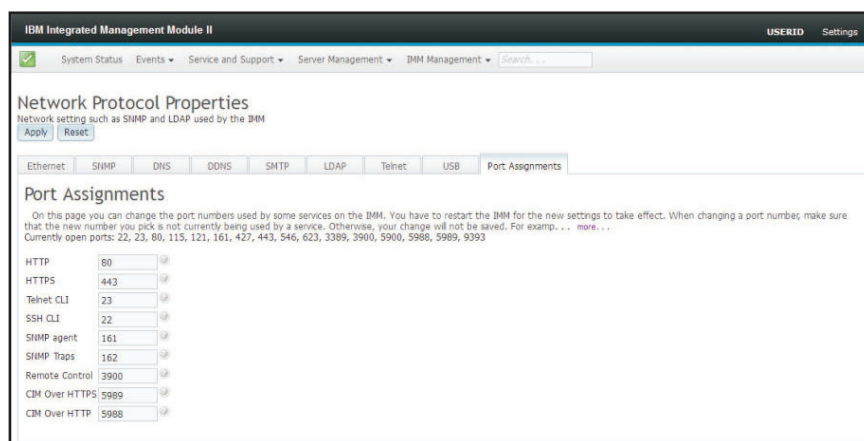
CIM over HTTP

在此字段中指定 CIM over HTTP 的端口号。缺省值为 5988。

CIM over HTTPS

在此字段中指定 CIM over HTTPS 的端口号。缺省值为 5989。

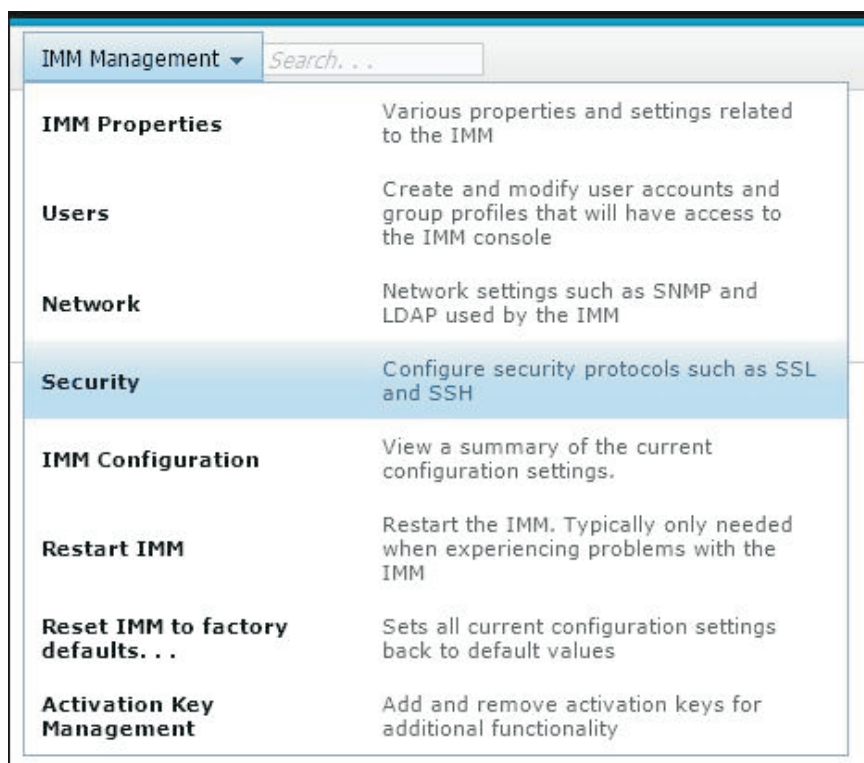
下图显示了 Port Assignments 选项卡。



配置安全性设置

（如下图所示）单击 IMM Management 选项卡下的 **Security** 选项可访问并配置 IMM2 的安全性属性、状态和设置。

要应用任何所作更改，必须单击 IMM Security 窗口左上角的 **Apply** 按钮。要重置所作任何更改，必须单击 **Reset Values** 按钮。



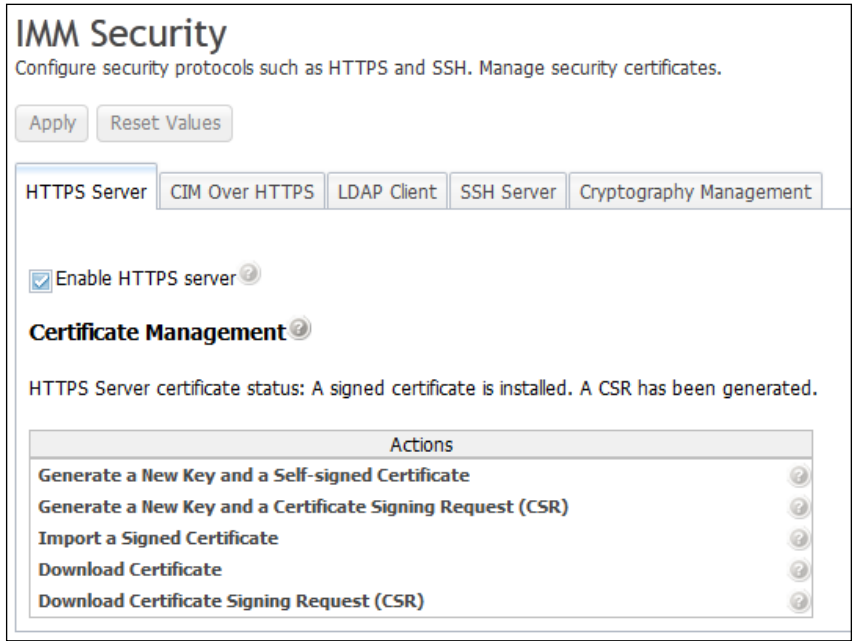
配置 HTTPS 协议

单击 **HTTPS Server** 选项卡可将 IMM2 Web 界面配置为使用更安全的 HTTPS 协议，而不使用缺省 HTTP 协议。

备注：

- 每次只能启用一个协议。
- 启用此选项需要对 SSL 证书进行其他配置。
- 更改协议时，必须重新启动 IMM2 Web 服务器。

有关 SSL 的更多信息，请参阅第 93 页的『SSL 概述』。下图显示了 HTTPS Server 选项卡。



注：在某些服务器上，IMM2 安全性级别可能受其他管理系统控制。在此类环境中，可以在 IMM2 Web 界面上禁用上述操作。

HTTPS 证书处理

使用 Actions 菜单中的选项可进行 HTTPS 证书处理。如果禁用了某个选项，那么可能需要先执行其他操作来将其启用。当处理 HTTPS 证书时，应禁用 HTTPS 服务器。有关证书处理的更多信息，请参阅第 93 页的『SSL 证书处理』。

注：在设置了证书处理后，必须重新启动 IMM2 以使更改生效。

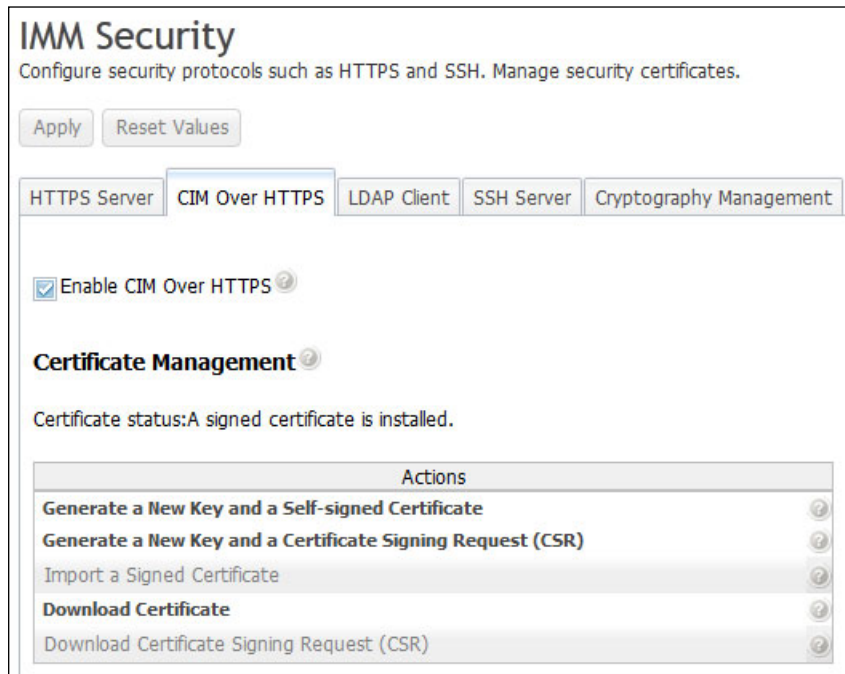
配置 CIM over HTTPS 协议

单击 **CIM over HTTPS** 选项卡，以将 IMM2 Web 界面配置为使用更安全的 CIM over HTTPS 协议，而不是缺省的 CIM over HTTP 协议。

备注：

- 一次只能启用一个协议。
- 启用此选项需要对 SSL 证书进行其他配置。
- 更改协议时，必须重新启动 IMM2 Web 服务器。

有关 SSL 的更多信息，请参阅第 93 页的『SSL 概述』。下图显示 CIM over HTTPS 选项卡。



CIM over HTTPS 证书处理

使用 Actions 菜单下的选项进行 CIM over HTTPS 证书处理。如果禁用了某个选项，那么可能要先执行其他操作来将其启用。有关证书处理的更多信息，请参阅第 93 页的『SSL 证书处理』。

注：在设置了证书处理后，必须重新启动 IMM2 以使更改生效。

配置 LDAP 客户机协议

单击 **LDAP Client** 选项，以使用更安全的 LDAP over SSL 协议而不是缺省 LDAP 协议。

注：启用此选项需要对 SSL 证书进行其他配置。
有关 SSL 的更多信息，请参阅第 93 页的『SSL 概述』。

下图显示 LDAP Client 选项卡。

IMM Security

Configure security protocols such as HTTPS and SSH. Manage security certificates.

Apply
Reset Values

HTTPS Server
CIM Over HTTPS
LDAP Client
SSH Server
Cryptography Management

LDAP security:

LDAP security: ?

Disable secure LDAP

Certificate Management ?

Signed Certificate status: No certificate is installed.

Trusted certificates: No trusted certificates are installed

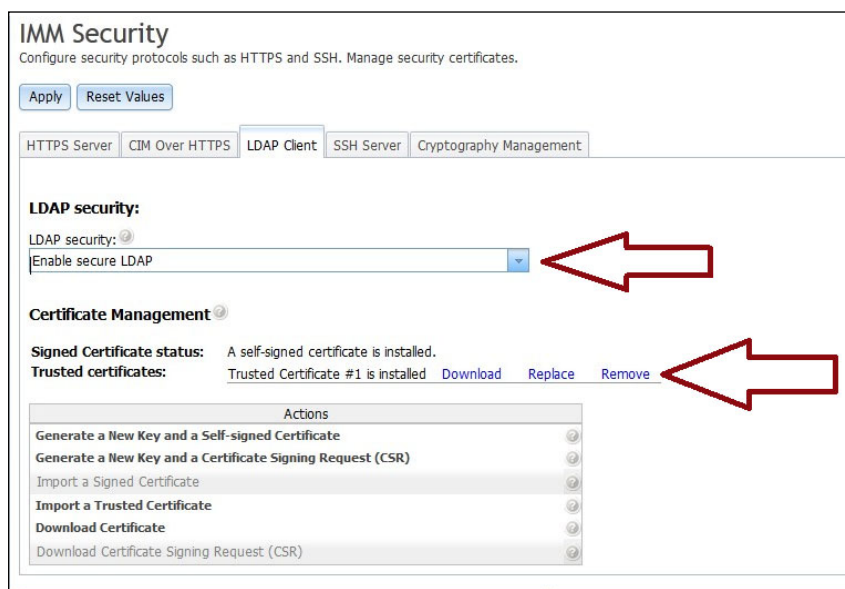
Actions
Generate a New Key and a Self-signed Certificate ?
Generate a New Key and a Certificate Signing Request (CSR) ?
Import a Signed Certificate ?
Import a Trusted Certificate ?
Download Certificate ?
Download Certificate Signing Request (CSR) ?

安全 LDAP 客户机证书处理

使用 Actions 菜单下的选项进行 LDAP over SSL 证书处理。如果禁用了某个选项，那么可能要先执行其他操作来将其启用。处理 HTTPS 证书时，应禁用 HTTPS 服务器。有关证书处理的更多信息，请参阅第 93 页的『SSL 证书处理』。一旦您安装了可信证书，即可启用 LDAP over SSL，如下图中所示。

备注：

- 对 IMM2 的更改将立即生效。
- 您的 LDAP 服务器必须支持安全套接字层 3 (SSL3) 或传输层安全性 (TLS)，以便与 IMM2 安全 LDAP 客户机兼容。



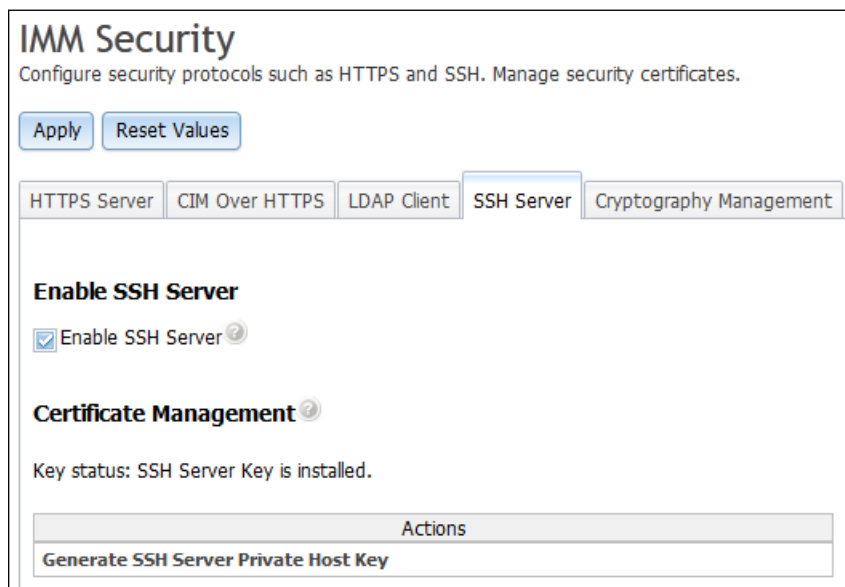
配置 Secure Shell 服务器

单击 **SSH Server** 选项卡可将 IMM2 Web 界面配置为使用更安全的 SSH 协议，而不使用缺省 Telnet 协议。

注：

- 使用此选项不需要任何证书管理。
- IMM2 起初将创建一个 SSH Server 密钥。如果您希望生成一个新的 SSH Server 密钥，请单击 Actions 菜单中的 **Generate SSH Server Private Host Key**。
- 在完成该操作后，必须重新启动 IMM2 以使您所作更改生效。

下图中显示了 SSH Server 选项卡。



SSL 概述

SSL 是一种用于确保通信隐私的安全协议。SSL 使客户机/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。您可以将 IMM2 配置为使用 SSL 支持进行不同类型的连接，例如，安全 Web 服务器 (HTTPS)、安全 LDAP 连接 (LDAPS)、CIM over HTTPS 和 SSH 服务器。您可以通过 IMM Management 选项卡中的 Security 选项查看或更改 SSL 设置。您还可以启用或禁用 SSL 并管理 SSL 所需的证书。

SSL 证书处理

您可以将 SSL 与自签名证书或由第三方认证中心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，但是该方法会带来较小的安全性风险。发生风险的原因是，针对 SSL 客户机和 SSL 服务器之间首次尝试的连接，客户机无法验证服务器的身份。例如，第三方有可能会冒充 IMM2 Web 服务器，并拦截真实 IMM2 Web 服务器和用户 Web 浏览器之间的数据流。如果在浏览器和 IMM2 之间最初连接时，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（假设初始连接未遭受攻击）。

要获取更完整的安全性，可以使用认证中心 (CA) 签名的证书。要获取签名证书，请单击 Actions 菜单中的 **Generate a New Key and a Certificate Signing Request (CSR)**。然后，必须将该证书签名请求 (CSR) 发送至 CA 并进行相应安排以获取最终的证书。接收到最终证书后，单击 Actions 菜单中的 **Import a Signed Certificate** 将其导入到 IMM2。

CA 的功能是验证 IMM2 的身份。证书包含 CA 和 IMM2 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 IMM2 Web 服务器。

IMM2 要求 HTTPS Server、CIM over HTTPS 和安全 LDAP 客户机与证书配合使用。此外，安全 LDAP 客户机还要求导入一个或多个可信证书。安全 LDAP 客户机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。

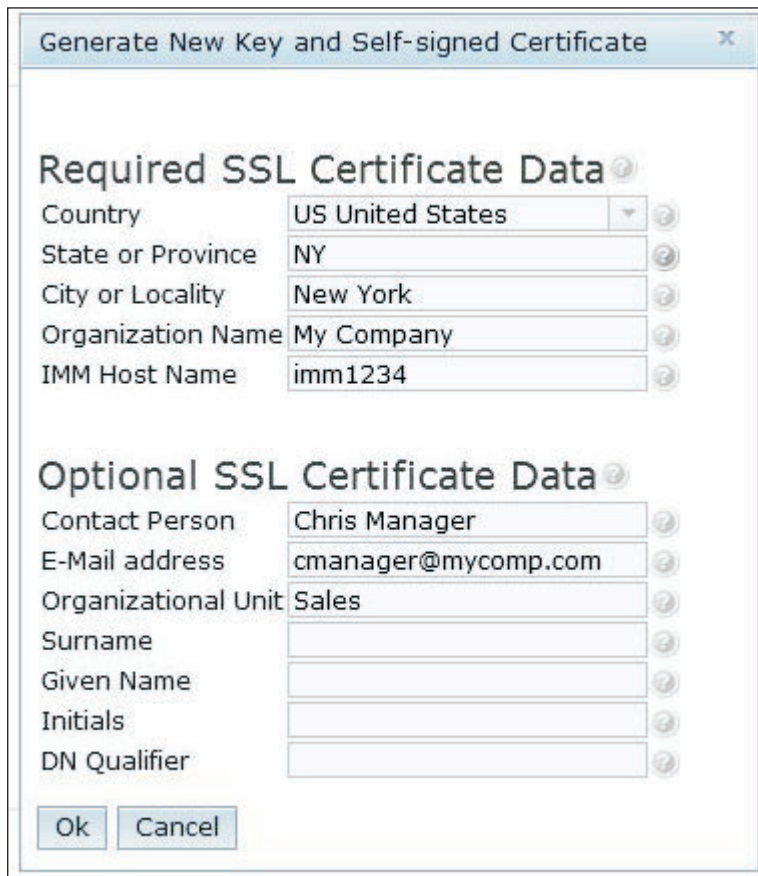
SSL 证书管理

管理 IMM2 证书时，会为您提供操作列表或操作子集（如下图所示）。



如果当前安装了证书，那么您将能够使用 Actions 菜单中的 **Download Certificate** 操作来下载当前已安装的证书或 CSR。灰显的证书表明当前未安装。安全 LDAP 客户机需要用户导入可信证书。单击 Actions 菜单中的 **Import a Trusted Certificate**。生成 CSR 后，单击 Actions 菜单中的 **Import a Signed Certificate**。

在执行其中一项“Generate”操作时，会打开 Generate New Key and Self-signed Certificate 窗口（如下图所示）。



Generate New Key and Self-signed Certificate

Required SSL Certificate Data

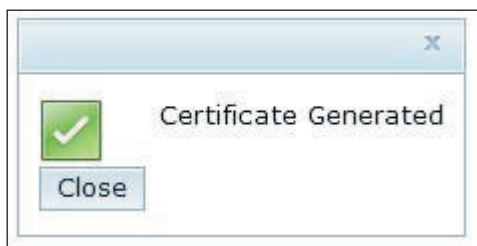
Country: US United States
State or Province: NY
City or Locality: New York
Organization Name: My Company
IMM Host Name: imm1234

Optional SSL Certificate Data

Contact Person: Chris Manager
E-Mail address: cmanager@mycomp.com
Organizational Unit: Sales
Surname:
Given Name:
Initials:
DN Qualifier:

Ok Cancel

Generate New Key and Self-signed Certificate 窗口将提示您完成必填和可选字段。您必须完成必填字段。一旦您输入信息，即可单击 **Ok** 来完成任务。这样会打开 Certificate Generated 窗口（如下图所示）。



配置 Cryptography Management

单击 **Cryptography Management** 选项卡以配置 IMM2 固件，使其遵守 SP 800-131A 的要求。

Cryptography Management 选项卡包含两个选项：

- Basic Compatibility Mode
- NIST SP 800-131A Compliance Mode

Basic Compatibility Mode 与较旧的固件版本以及不使用 NIST SP 800-131A Compliance Mode 的浏览器和其他网络客户机兼容。

下图中显示了已选择 **Basic Compatibility Mode** 的 Cryptography Management 选项卡。

IMM Security

Configure security protocols such as HTTPS and SSH. Manage security certificates.

Apply

Reset Values

HTTPS Server

CIM Over HTTPS

LDAP Client

SSH Server

Cryptography Management

☒ Basic Compatibility Mode

- This mode is compatible with older firmware versions and with browsers and other network clients that do not implement the stricter security requirements of the compliance mode below.

☐ NIST SP 800-131A Compliance Mode

- Select this mode to have the IMM2 firmware comply with the requirements of SP 800-131A.

- **Note:** To prevent loss of access to the IMM2, this mode should only be selected if you are sure that your browser and other network clients also work with the required SP 800-131A encryption modes.

NIST SP 800-131A Compliance Mode 提供严格的安全性要求。使用 **NIST SP 800-131A Compliance Mode** 时，IMM2 固件将遵守 SP 800-131A 的要求。

备注：

- 为防止丢失 IMM2 的访问权，只有当您确保自己的浏览器和其他网络客户机可以使用 SP 800-131A 加密方式时，才使用 **NIST SP 800-131A Compliance Mode**。
- 使用 **NIST SP 800-131A Compliance Mode** 时，您可以允许 SNMPv3 帐户不遵守该方式设置的限制。

下图中显示了已选择 **NIST SP 800-131A Compliance Mode** 的 Cryptography Management 选项卡。

IMM Security

Configure security protocols such as HTTPS and SSH. Manage security certificates.

Apply

Reset Values

HTTPS Server

CIM Over HTTPS

LDAP Client

SSH Server

Cryptography Management

☐ Basic Compatibility Mode

- This mode is compatible with older firmware versions and with browsers and other network clients that do not implement the stricter security requirements of the compliance mode below.

☒ NIST SP 800-131A Compliance Mode

- Select this mode to have the IMM2 firmware comply with the requirements of SP 800-131A.

- **Note:** To prevent loss of access to the IMM2, this mode should only be selected if you are sure that your browser and other network clients also work with the required SP 800-131A encryption modes.

Select the settings below to override a strict compliance.

☒ Allow SNMPv3 accounts that don't comply.

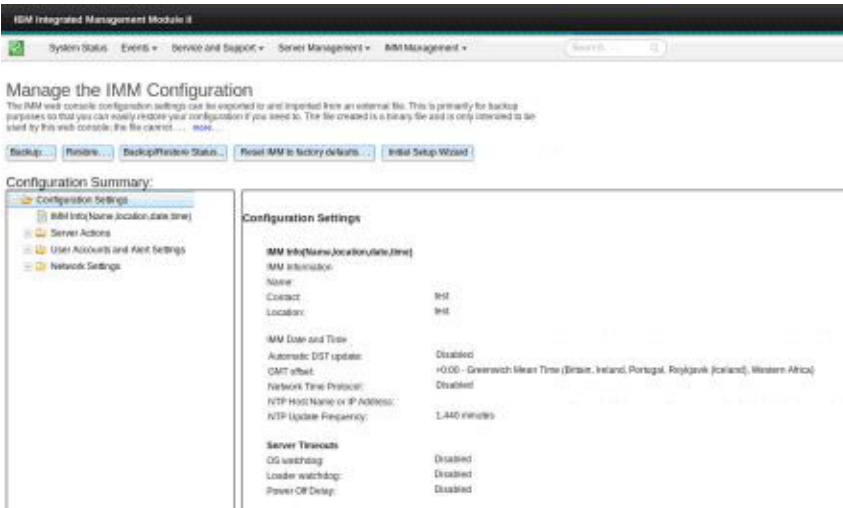
第 4 章 配置 IMM2 95

复原和修改 IMM 配置

从 IMM Management 选项卡中选择 **IMM Configuration** 选项，以选择用于执行以下操作的选项：

- 查看 IMM2 配置摘要
- 备份或复原 IMM2 配置
- 查看备份或恢复状态
- 将 IMM2 配置重置为其出厂缺省设置
- 访问 IMM2 初始设置向导

下图显示“Manage the IMM Configuration”窗口。

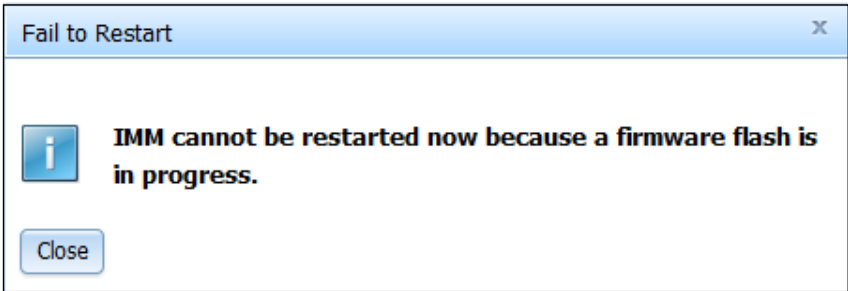


重新启动 IMM2

选择 IMM Management 选项卡中的 **Restart IMM** 选项以重新启动 IMM2。

备注：

- 只有具有 Supervisor 用户权限级别的人员才能执行此功能。
- 当以太网连接暂时断开时，您必须登录到 IMM2 才能访问 IMM2 Web 界面。
- 当任何其他用户更新服务器固件时，将无法执行 Restart IMM（如下图所示）。

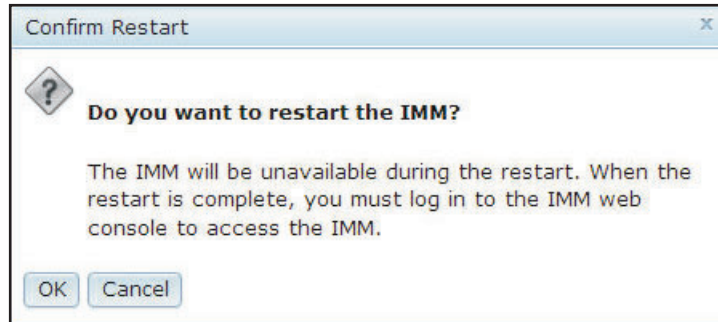


要重新启动 IMM2，请完成以下步骤：

1. 登录到 IMM2。有关更多信息，请参阅第 10 页的『登录到 IMM2』。

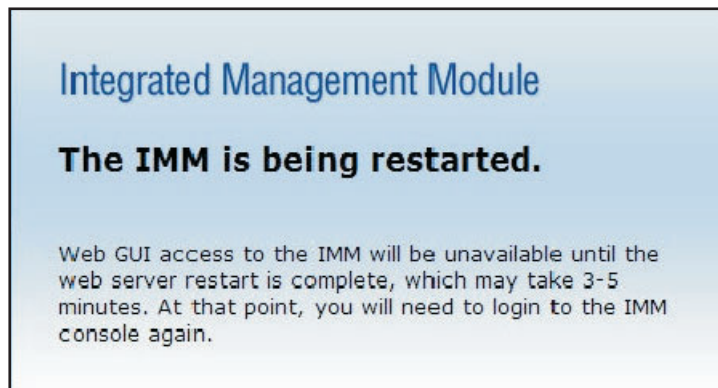
2. 单击 **IMM Management** 选项卡；然后，单击 **Restart IMM**。
3. 单击 Confirm Restart 窗口上的 **OK** 按钮。这样将重新启动 IMM2。

下图显示 Confirm Restart 窗口。



重新启动 IMM2 时，TCP/IP 或调制解调器连接会中断。

下图显示重新启动 IMM2 时您将看到的通知窗口。



4. 再次登录以使用 IMM2 Web 界面（请参阅第 10 页的『登录到 IMM2』以获取指示信息）。

将 IMM2 重置为出厂缺省值

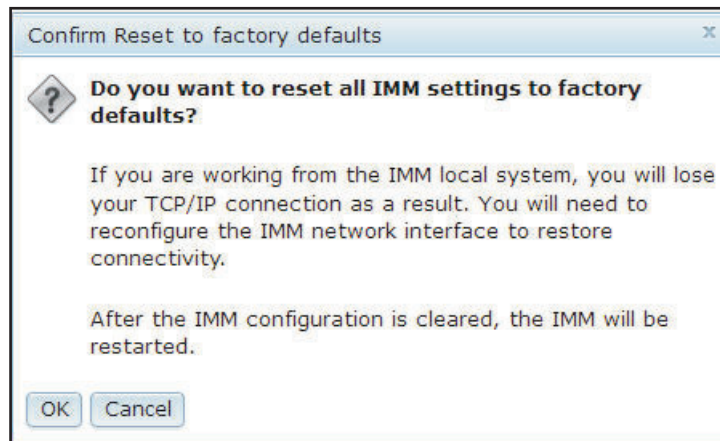
从 IMM Management 选项卡中选择 **Reset IMM to factory defaults...** 选项，以将 IMM2 复原为出厂缺省设置。

备注：

- 只有具有 Supervisor 用户权限级别的人员才能执行此功能。
- 当以太网连接暂时断开时，您必须登录到 IMM2 才能访问 IMM2 Web 界面。
- 使用 Reset IMM to factory defaults 选项时，您将丢失对 IMM2 进行的所有修改。

要复原 IMM2 出厂缺省值，请完成以下步骤：

1. 登录到 IMM2。有关更多信息，请参阅第 10 页的『登录到 IMM2』。
2. 单击 **IMM Management** 选项卡；然后，单击 **IMM Reset to factory defaults...**。
3. 单击 Confirm Reset to factory defaults 窗口上的 **OK** 按钮（如下图中所示）。



注：IMM2 配置完成后，将重新启动 IMM2。如果这是本地服务器，那么 TCP/IP 连接将中断，您必须重新配置网络接口才能复原连接。

4. 再次登录到 IMM2，以使用 IMM2 Web 界面（请参阅第 10 页的『登录到 IMM2』以获取指示信息）。
5. 重新配置网络接口以复原连接。

激活管理密钥

单击 IMM Management 选项卡中的 **Activation Key Management** 选项，以管理可选 IMM2 和服务端 Features on Demand (FoD) 功能部件的激活密钥。请参阅第 141 页的第 7 章，『Features on Demand』，以获取有关管理 FoD 激活密钥的信息。

第 5 章 监控服务器状态

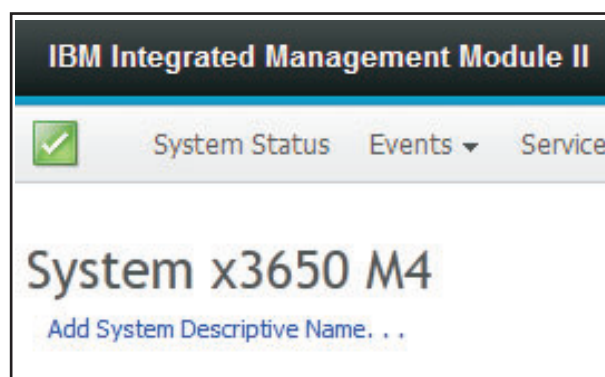
本章提供的信息包括如何查看并监控所访问的服务器的信息。

查看系统状态

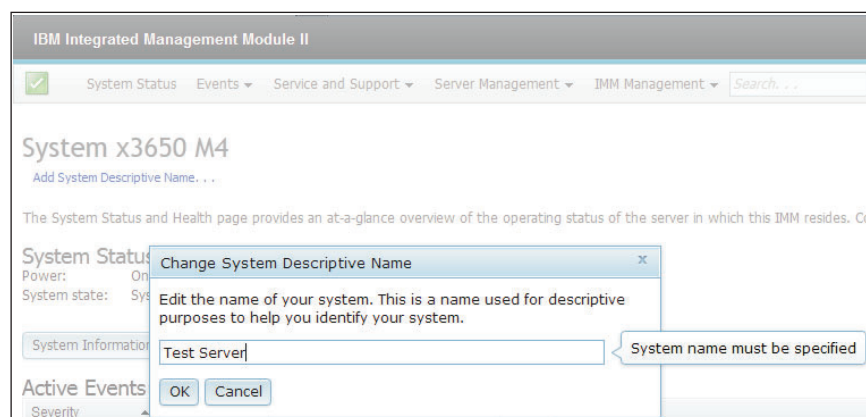
System Status 页面提供 IMM2 服务器运行状态的概述。此页面还显示服务器的硬件运行状况以及在服务器上发生的任何活动事件。

注：如果您通过 System Status 页面访问另一页面，那么可以通过单击该页面顶部菜单项中的 **System Status** 来返回到 System Status 页面。

可以向 IMM2 添加描述性名称以帮助将某个 IMM2 与其他 IMM2 区分开。单击位于服务器产品名下方的 **Add System Descriptive Name...** 链接可指定一个与 IMM2 相关联的名称（如下图所示）。

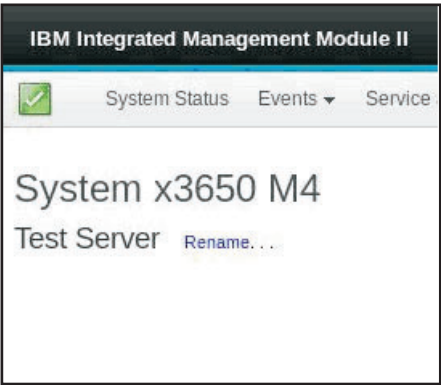


在 Change System Descriptive Name 窗口中，指定一个与 IMM2 相关联的名称（如下图所示）。



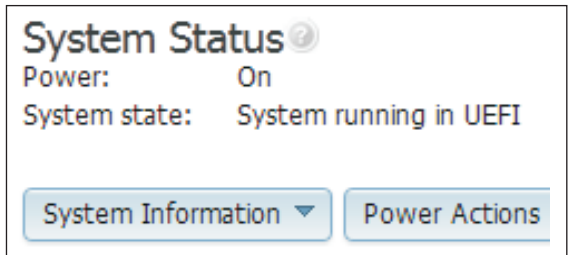
可以通过单击位于 System Descriptive 名称旁边的 **Rename...** 链接来重命名 System Descriptive Name。

下图显示了 Rename 链接。



System Status 页面显示服务器电源状态和运行状态。所显示的状态是 System Status 页面打开时的服务器状态。

下图显示了 **Power** 和 **System state** 字段。



服务器可以是下表中所列的其中一种系统状态。

表 5. 系统状态描述

State	描述
系统电源关闭/状态未知	服务器已关闭。
系统开启/正在启动 UEFI	服务器已开启；但是，UEFI 未运行。
系统正在 UEFI 中运行	服务器已开启并且 UEFI 正在运行。
系统已在 UEFI 中停止	服务器已开启；已检测到 UEFI 有问题并且已停止运行。
正在引导操作系统或处于不受支持的操作系统中	服务器可能由于以下一种原因而处于此状态： • 操作系统 (OS) 装入程序已启动；但是操作系统未运行 • IMM2 Ethernet over USB 接口已禁用。 • 操作系统未装入可支持 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	服务器已置于待机或睡眠状态。

System Status 页面上的以下菜单选项可提供更多服务器信息以及可针对服务器执行的操作。

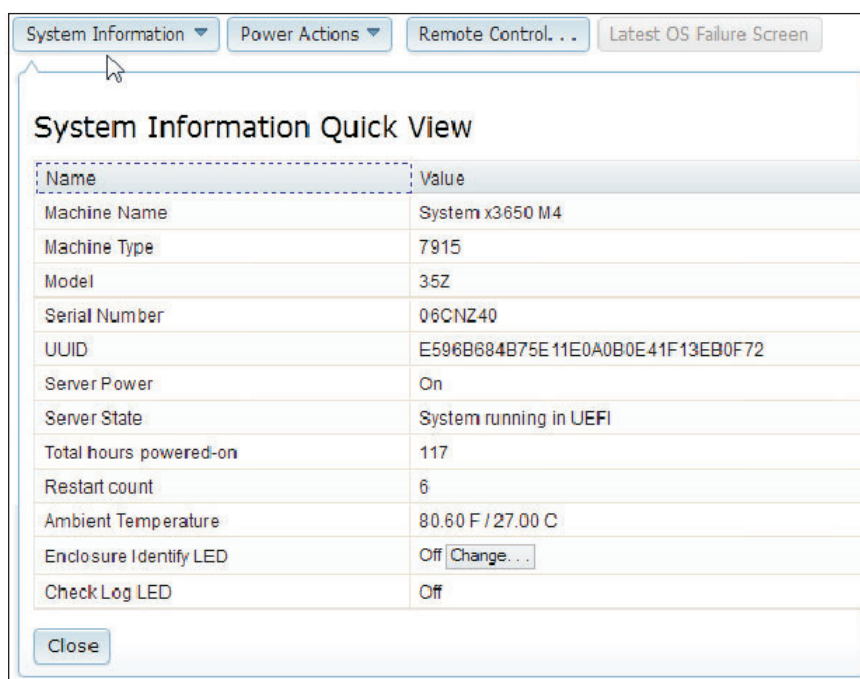
- System Information
- Power Actions
- Remote Control (请参阅第 109 页的『远程感知和远程控制功能』, 以获取更多信息)。
- Latest OS Failure 屏幕 (请参阅第 135 页的『捕获最新操作系统故障屏幕数据』, 以获取更多信息)。

查看系统信息

System Information 菜单提供常规服务器信息的摘要。在 System Status 页面上单击 **System Information** 选项卡可查看以下信息：

- 机器名
- 机器类型
- 型号
- 序列号
- 通用唯一标识 (UUID)
- 服务器电源
- 服务器状态
- 总开机时数
- Restart count
- 环境温度
- 机柜身份指示灯
- 检查日志指示灯

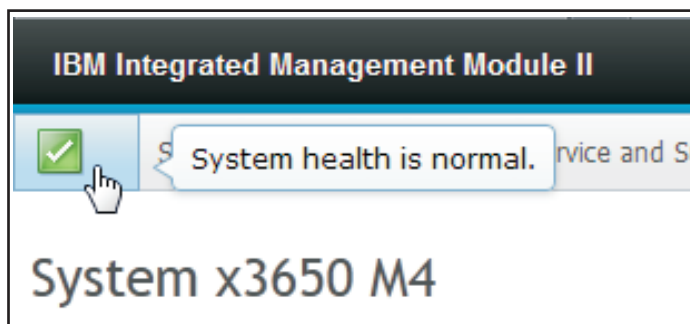
下图显示了 System Information 窗口。



查看服务器运行状况

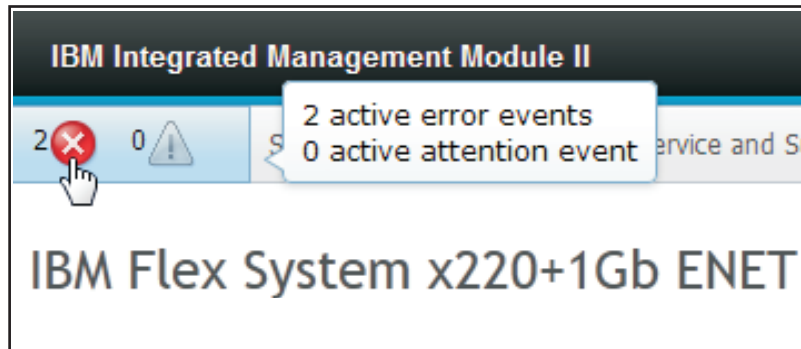
服务器运行状况显示在 System Status 页面左上角的标题栏下，并通过图标指定。绿色复选标记指示服务器硬件在正常运行。将光标移至绿色复选标记上，可获取服务器运行状况的快速指示。

下图是处于正常运行方式的服务器的示例。



黄色三角形图标指示存在警告情况。红色圆形图标指示存在错误情况。

下图是包含活动错误事件的服务器的示例。



如果显示警告图标（黄色三角形）或错误图标（红色圆形），请单击该图标以在 System Status 页面的 Active Events 部分中显示对应事件。

下图是包含错误情况的 Active Events 部分的示例。

Active Events			
Severity	Source	Date	Message
Error	System	16 Jul 2012 01:00:28.000 PM	Sensor Mezz Exp 2 Fault has transitioned to critical from a less severe state.
Error	System	16 Jul 2012 01:00:29.000 PM	Sensor Mezz Exp 2 Fault has transitioned to critical from a less severe state.

查看硬件运行状况

System Status 页面的 Hardware Health 部分列出了服务器硬件组件，并显示由 IMM2 监控的每个组件的运行状态。针对组件显示的运行状态可能反映某个组件类型的所有个别组件的最关键状态。例如，服务器可能安装有若干电源模块，并且除一个电源模块外，所有其他电源模块都在正常运行。Power Modules 组件的状态将由于该电源模块未在正常运行而指示 Critical。

下图显示 System Status 页面的 Hardware Health 部分。

Hardware Health	
Component Type	Status
Cooling Devices	✓ Normal
Power Modules	✗ Critical
Disks	✓ Normal
Processors	✓ Normal
Memory	✓ Normal
System	✓ Normal

每个组件类型都显示为可单击以获取更详细信息的链接。选择要查看的组件类型时，会显示一个表，其中列出该组件类型的所有组件的状态。

下图显示 Memory 组件类型的组件。

Memory
Display the memory modules available on the server. Clicking on a module displays a Properties pop-up window with 2 tabs: Events and Hardware Information.

FRU Name	Status	Type	Capacity (GB)
DIMM 4	✓ Normal	DDR3	4
DIMM 9	✓ Normal	DDR3	4
DIMM 16	✓ Normal	DDR3	4
DIMM 21	✓ Normal	DDR3	4

您可以单击表中的个别现场可更换部件 (FRU) 链接，以获取该组件的其他信息。然后，Events 选项卡中会显示该组件的所有活动事件。

下图显示 DIMM 4 的 Events 选项卡。



如果适用，那么在 Hardware Information 选项卡中可能会提供该组件的其他信息。

下图显示 DIMM 4 的 Hardware Information 选项卡。

Properties for DIMM 4

Events

Hardware Information

Description	DIMM 4
PartNumber	M393B5773CH0-YH9
FRU Serial Number	8634E095
Manuf Date	2211
Type	DDR3
Size	2 GB

Close

第 6 章 执行 IMM2 任务

您可以使用本节和第 17 页的第 3 章,『IMM2 Web 用户界面概述』中的信息来执行以下 IMM2 控制任务。

在 System Status 选项卡上,您可以执行以下任务:

- 查看服务器运行状况
- 查看服务器信息,例如,机器名称、类型以及序列号
- 查看服务器电源和重新启动活动
- 远程控制服务器的电源状态
- 远程访问服务器控制台
- 远程将磁盘或磁盘映像连接到服务器
- 查看活动事件
- 查看服务器组件的硬件运行状况

注:在登录到 IMM2 后,将显示 System Status 页面。常用信息和操作都位于此页面上。

在 Events 选项卡上,您可以执行以下任务:

- 管理事件日志历史记录
- 管理电子邮件通知的事件接收方
- 管理系统日志通知的事件接收方

在 Services and Support 选项卡上,您可以执行以下任务:

- 手动获取您服务器的服务数据

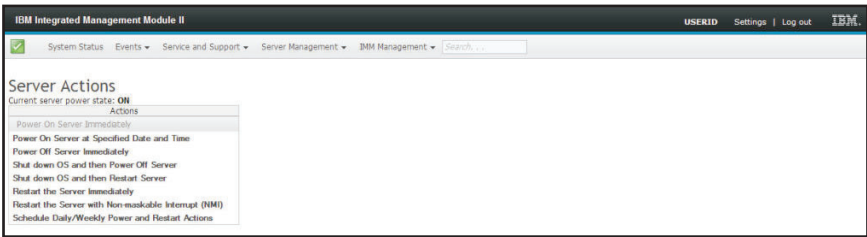
在 Server Management 选项卡上,您可以选择选项来执行以下任务:

- 通过 Server Firmware 选项,查看并更新服务器组件的固件级别。
- 通过 Remote Control 选项,远程查看服务器控制台并与其交互:
 - 远程控制服务器的电源状态
 - 远程访问服务器控制台
 - 远程将 CD 驱动器、DVD 驱动器、软盘驱动器、USB 闪存驱动器或磁盘映像附加到服务器。
- 通过 Server Properties 选项,可以设置用于帮助标识服务器的参数。
- 通过 Server Power Actions 选项,可以执行例如开机、关机和重新启动等操作。
- 通过 Disks 选项,可以查看硬盘驱动器以及与服务器中安装的硬盘驱动器相关联的事件。
- 通过 Memory 选项,可以查看服务器中安装的内存条的有关信息。
- 通过 Processor 选项,可以查看服务器中安装的微处理器的有关信息。
- 通过 Server Timeouts 选项,可以设置超时,以确保服务器不会在固件更新或服务器开机期间无限期挂起。

- 通过 PXE Network Boot 选项，可以设置对预引导服务器执行环境的尝试。
- 通过 Latest OS Failure Screen 选项，可以捕获 OS 故障屏幕数据并进行存储。
- 通过 Power Management 选项，可以查看系统电源使用情况和电源容量，并设置系统电源使用情况的参数。

控制服务器的电源状态

Power Actions 选项包含可用来控制服务器电源的操作的列表（如下图中所示）。您可以选择立即使服务器开机，或者在安排的时间使服务器开机。您也可以选择关机，然后重新启动操作系统。



完成以下步骤以执行服务器电源和重新启动操作：

1. 通过执行以下步骤之一来访问 Power Actions 菜单：
 - 单击 System Status 页面上的 **Power Actions** 选项卡。
 - 单击 Server Management 选项卡中的 **Server Power Actions**。
2. 从 Actions 菜单列表中选择服务器操作。

下表包含可在服务器上执行的电源和重新启动操作的描述。

表 6. 电源操作和描述

电源操作	描述
Power on server immediately	选择此操作项以使服务器开机并引导操作系统。
Power on server at specified date and time	选择此操作项以将服务器安排为在特定日期和时间自动开机。
Power off server immediately	选择此操作项以使服务器关机而不关闭操作系统。
Shut down operating system and then power off server ¹	选择此操作项以关闭操作系统并使服务器关机。
Shut down operating system and then restart server ¹	选择此操作项以重新引导操作系统。
Restart the server immediately	选择此操作项以使服务器立即关闭并再打开电源而不关闭操作系统。
Restart the server with non-maskable interrupt (NMI)	选择此操作项以在“挂起”系统上强制执行 NMI。通过选择此操作项，平台操作系统可以执行内存转储，这可用于系统挂起条件的调试目的。IMM2 固件通过 Setup 菜单中的 UEFI F1 使用 NMI 设置上的自动重新引导来确定是否需要在 NMI 后重新引导。

表 6. 电源操作和描述 (续)

电源操作	描述
Schedule daily/weekly power and restart actions	选择此操作项以便为服务器安排每天和每周电源和重新启动操作。
Enter Sleep Mode	当平台操作系统支持 S3 (睡眠方式) 功能并且已启用 S3 功能时, 将显示此操作项。当操作系统开启时, 选择此操作项以将操作系统置于睡眠方式。
Exit Sleep Mode	当平台操作系统支持 S3 (睡眠方式) 功能并且已启用 S3 功能时, 将显示此操作项。选择此操作项以将操作系统从睡眠方式中唤醒。
1. 如果在尝试“关机”请求时操作系统处于屏幕保护程序或锁定方式中, 那么 IMM2 可能无法启动正常关机。IMM2 将在关机延迟时间间隔到期后执行硬重置或关机, 而操作系统可能仍在运行。	

远程感知和远程控制功能

您可以在 IMM2 Web 界面中使用 IMM2 远程控制功能部件或远程感知功能, 以查看服务器控制台并与之交互。您可以向服务器分配一个您计算机上的 CD 或 DVD 驱动器、软盘驱动器、USB 闪存驱动器或磁盘映像。远程感知功能可用于 IMM2 Premium 功能部件, 并且仅通过 IMM2 Web 界面提供。您必须使用具有监管员访问权的用户标识登录到 IMM2, 才能使用任何远程控制功能部件。有关从 IMM2 Basic 或 IMM2 Standard 升级到 IMM2 Premium 的更多信息, 请参阅第 3 页的『升级 IMM2』。请参阅服务器随附的文档, 以获取有关服务器中所安装 IMM2 的级别的信息。

使用远程控制功能部件执行以下操作:

- 远程查看视频, 图形分辨率高达 1600 x 1200 (75 Hz), 而与服务器状态无关。
- 使用远程客户机的键盘和鼠标远程访问服务器。
- 映射远程客户机上的 CD 或 DVD 驱动器、软盘驱动器和 USB 闪存驱动器, 并将 ISO 和软盘映像文件映射为可供服务器使用的虚拟驱动器。
- 将软盘映像上载到 IMM2 内存, 并将其作为虚拟驱动器映射到服务器。

备注:

- 在多用户方式下启动远程控制功能时, IMM2 最多支持六个同时发生的会话。一次只能由一个会话使用远程磁盘功能。
- 视频查看器能够仅显示主板上视频控制器生成的视频。如果安装独立的视频控制器适配器并代替系统的视频控制器, 那么 IMM2 无法在远程视频查看器上显示来自所添加适配器的视频内容。

更新 IMM2 固件和 Java 或 ActiveX applet

本节提供有关更新固件以及 Java 和 ActiveX applet 的信息。

要点: IMM2 使用 Java applet 或 ActiveX applet 来执行远程感知功能。当 IMM2 更新为最新固件级别时, Java applet 和 ActiveX applet 也会更新为最新级别。缺省情况下, Java 对先前使用的 applet 进行高速缓存 (本地存储)。对 IMM2 固件进行快速更新后, 服务器使用的 Java applet 可能不是最新级别。

要更正此问题，请关闭高速缓存。所使用的方法应根据平台和 Java 版本而不同。以下步骤适用于 Windows 上的 Oracle Java 1.5：

1. 单击开始 → 设置 → 控制面板。
2. 双击 **Java Plug-in 1.5**。此时会打开 Java Plug-in 控制面板窗口。
3. 单击 **Cache** 选项卡。
4. 选择以下选项之一：
 - 清除 **Enable Caching** 复选框，以便始终禁用 Java 高速缓存。
 - 单击 **Clear Caching**。如果选择此选项，那么在各 IMM2 固件更新后必须单击 **Clear Caching**。

有关更新 IMM2 固件的更多信息，请参阅第 121 页的『更新服务器固件』。

启用远程感知功能

仅在 IMM2 Premium 中提供 IMM2 远程感知功能。有关从 IMM Standard 升级到 IMM Premium 的更多信息，请参阅第 3 页的『升级 IMM2』。

购买并获取用于 IMM Premium 升级的激活密钥之后，安装该激活密钥，请参阅第 141 页的『安装激活密钥』。

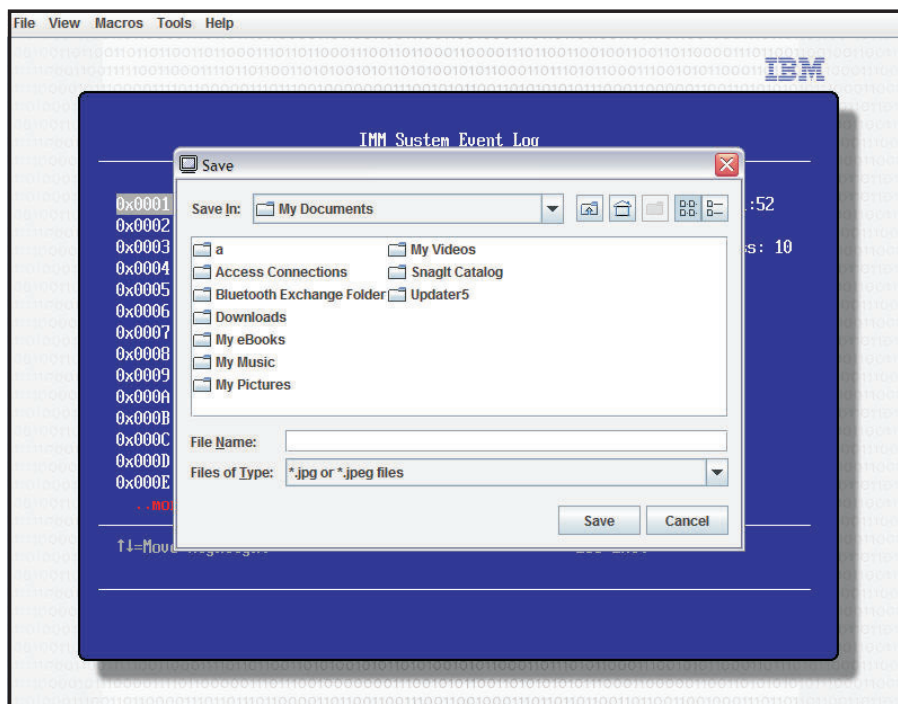
远程控制截屏

Video Viewer 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：

1. 在 Video Viewer 窗口中，单击 **File**。
2. 从菜单中选择 **Capture to File**。
3. 当显示提示时，为图像文件输入名称并将该其保存到您在本地客户机上选择的位置。

注：Java 客户机将截屏图像另存为 JPG 文件类型。ActiveX 客户机将截屏图像另存为 BMP 文件类型。

下图显示了用于指定图像文件的位置并输入图像文件名称的窗口。



远程控制 Video Viewer 方式

要更改 Video Viewer 窗口的视图，请单击 **View**。将提供以下菜单选项：

Hide Status Bar

隐藏用于显示大写锁定、数字锁定和滚动锁定键的状态的状态栏。仅当状态栏显示时，此选项才可用。

Show Status Bar

显示用于显示大写锁定、数字锁定和滚动锁定键的状态的状态栏。仅当状态栏隐藏时，此选项才可用。

Refresh

Video Viewer 使用服务器中的视频数据重新绘制视频显示。

Full Screen

Video Viewer 使视频显示填满客户机桌面。仅当 Video Viewer 未处于全屏方式时，此选项才可用。

Windowed

Video Viewer 从全屏方式中退出到窗口方式。仅当 Video Viewer 处于全屏方式时，此选项才可用。

Fit

Video Viewer 对大小进行调整，以完全显示目标桌面且没有外加边框和滚动条。这需要客户机桌面足够大以显示已调整大小的窗口。

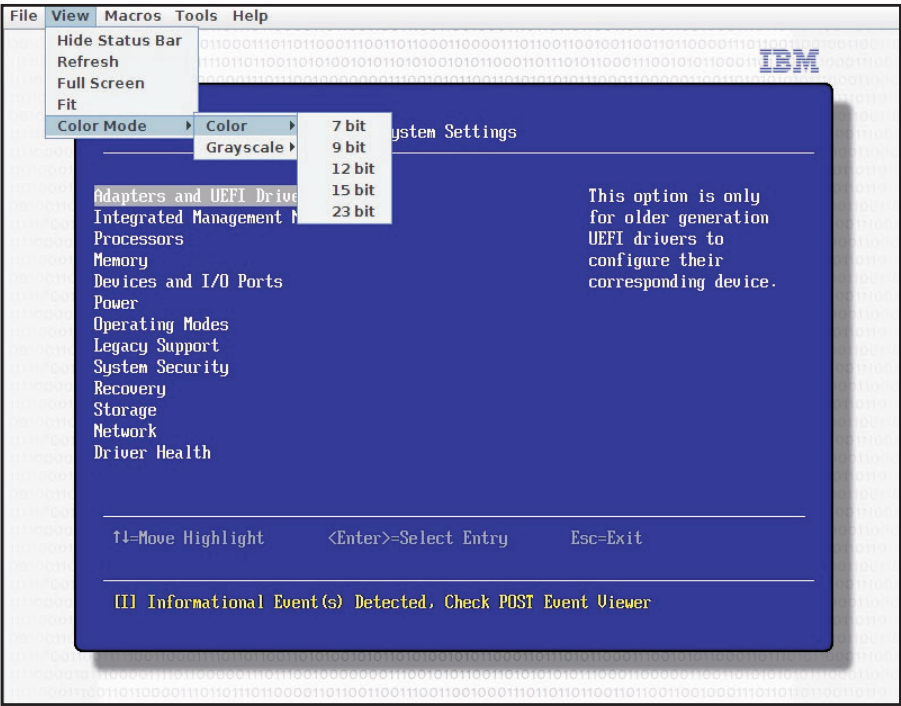
远程控制视频颜色方式

如果您与远程服务器的连接的带宽有限，那么可以通过在 Video Viewer 窗口中调整颜色设置来降低 Video Viewer 的带宽需求。

注：IMM2 包含一个菜单项，可调整色深以减少在低带宽情况下传输的数据。此菜单项代替了在 Remote Supervisor Adapter II 界面中使用的带宽滑块。

要更改视频颜色方式，请完成以下步骤：

1. 在 Video Viewer 窗口中，单击 **View**。
2. 单击 **Color Mode**。提供两个颜色方式选项（如下图所示）：
 - 颜色：7、9、15 和 23 位
 - 灰度：16、32、64 和 128 灰度级



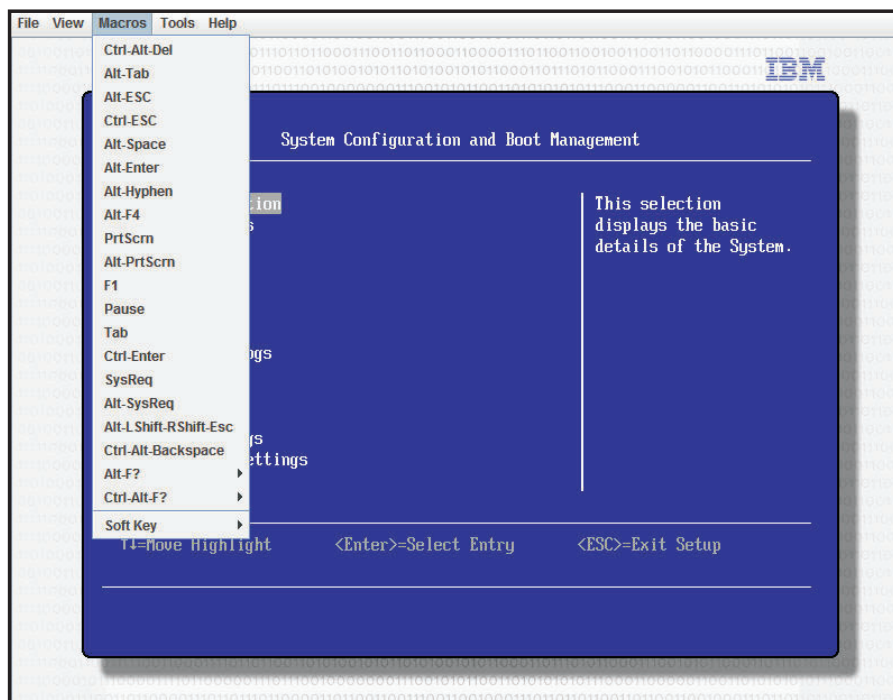
3. 选择颜色或灰度设置。

远程控制键盘支持

您正在使用的客户机服务器上的操作系统会对某些键组合（如在 Microsoft Windows 中为 Ctrl+Alt+Del）设置陷阱，而不是将其传输到服务器。其他键（如 F1）可能会在您的计算机以及服务器上导致操作。

要使用会影响远程服务器而不是本地客户机的键组合，请完成以下步骤：

1. 在 Video Viewer 窗口中，单击 **Macros**。
2. 从菜单中选择其中一种预定义键组合，或者选择 **Soft Key** 以选择或添加用户定义的键组合（如下图所示）。



使用 Video Viewer **Macros** 菜单项创建和编辑可用于向服务器发送击键的定制按钮。

要创建和编辑定制按钮，请完成以下步骤：

1. 在 Video Viewer 窗口中，单击 **Macros**。
2. 选择 **Soft Key**，然后选择 **Add**。此时将打开一个新窗口。
3. 单击 **New** 以添加新键组合，或者选择某个键组合并单击 **Delete** 以除去现有键组合。
4. 如果要添加新组合，请在选择 **New** 后，在打开的窗口中输入要定义的键组合；然后，单击 **OK**。
5. 完成定义或除去键组合时，单击 **OK**。

国际键盘支持

Video Viewer 使用特定于平台的本机代码来截取键事件以直接访问物理键信息。客户机检测到物理键事件，然后将其传递到服务器。服务器检测到客户机遇到的相同物理击键并支持所有标准键盘布局，唯一的限制是目标和客户机使用相同键盘布局。如果远程用户具有与服务器不同的键盘布局，那么用户可以在远程访问服务器布局时将其切换，然后重新切换回来。

键盘通过方式

键盘通过方式禁止在客户机上处理大多数特殊组合键，以便可以将其直接传递到服务器。这提供了使用宏的备选方法。

某些操作系统将特定击键定义不受应用程序的控制，因此，通过机制的行为独立于服务器进行操作。例如，在 Linux X 会话中，Ctrl+Alt+F2 组合键切换到虚拟控制台 2。没有机制来截获此击键顺序，因此，客户机无法将这些击键直接传递到目标。在此情况下，唯一选项是使用为此目的定义的键盘宏。

要启用或禁用键盘通过方式，请完成以下步骤：

1. 在 Video Viewer 窗口中，单击 **Tools**。
2. 从菜单选择 **Session Options**。
3. Session Options 窗口打开后，单击 **General** 选项卡。
4. 选中 **Pass all keystrokes to target** 复选框以启用或禁用键盘通过方式。
5. 单击 **OK** 以保存选项。

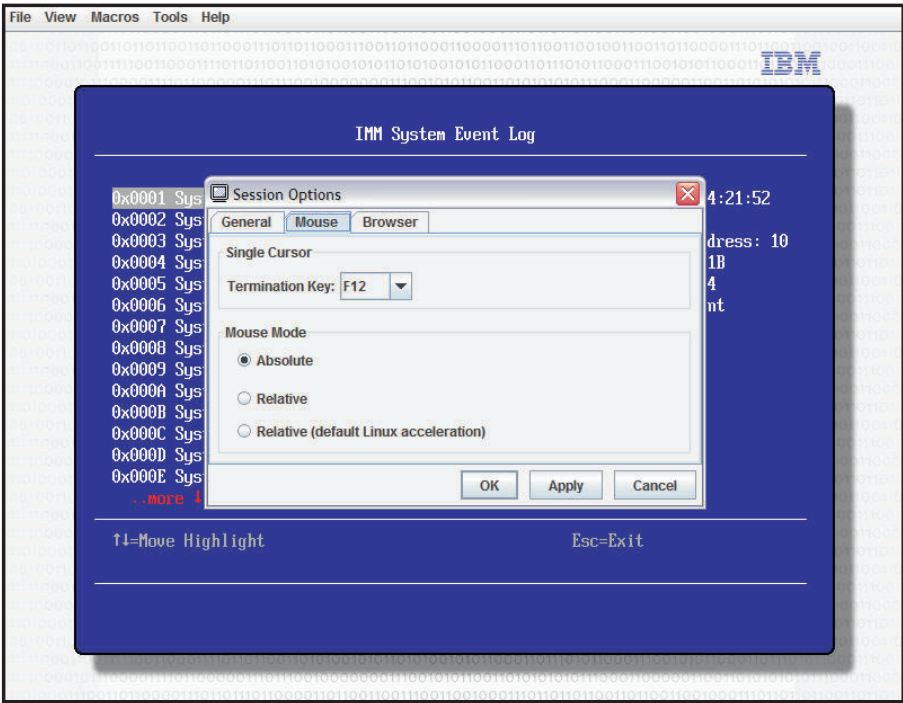
远程控制鼠标支持

Video Viewer 窗口提供了一些鼠标控制选项，包括绝对鼠标控制、相对鼠标控制和单光标方式。

绝对和相对鼠标控制

要访问用于控制鼠标的绝对和相对选项，请完成以下步骤：

1. 在 Remote Control 窗口中，单击 **Tools**。
2. 从菜单中选择 **Session Options**。
3. Session Options 窗口打开后，单击 **Mouse** 选项卡（如下图所示）。



4. 选择以下一种鼠标方式：

Absolute

客户机将鼠标位置消息发送到总是相对于查看区域的原点（左上方区域）的服务器。

Relative

客户机将鼠标位置作为与先前位置的偏移量进行发送。

Relative (default Linux acceleration)

客户机应用加速因子以在 Linux 目标上更好地将鼠标对齐。已选择加速设置来最大化与 Linux 分发版的兼容性。

单光标方式

某些操作系统不会将本地光标与远程光标对齐，这会导致在本地鼠标光标和远程鼠标光标之间出现偏移。单光标方式会在鼠标位于 Video Viewer 窗口中时隐藏本地客户机光标。激活单光标方式后，您仅会看到远程光标。要启用单光标方式，在 Video Viewer 窗口中单击 **Tools > Single Cursor**。

注：当 Video Viewer 处于单光标方式下时，不能使用鼠标切换到其他窗口或在 KVM 客户机窗口外单击，因为没有本地光标。

要禁用单光标方式，请单击 **Defined Termination** 键。要查看定义的终止键或更改终止键，请单击 **Tools > Session Options > Mouse**。

远程电源控制

您可以从 Video Viewer 窗口发送服务器电源和重新启动命令而不返回到 Web 浏览器。要通过 Video Viewer 来控制服务器电源，请完成以下步骤：

1. 在 Video Viewer 窗口中，单击 **Tools**。
2. 单击 **Power**。选择以下一个命令：

On 开启服务器电源。

Off 关闭服务器电源。

Reboot
重新启动服务器。

Cycle 关闭服务器电源，然后重新开启。

查看性能统计信息

要在 Video Viewer 窗口中查看 Video Viewer 性能统计信息，请单击 **Tools**；然后，单击 **Stats**。下列信息将显示：

Frame Rate

客户机每秒解码的帧数的运行平均数。

Bandwidth

客户机每秒收到的千字节总数的运行平均数。

Compression

由于视频压缩，带宽减少的运行平均数。该值通常显示为 100.0%。将其四舍五入为 10% 的倍数。

Packet Rate

每秒收到的视频包数的运行平均数。

启动远程桌面协议

如果安装了基于 Windows 的远程桌面协议 (RDP) 客户机，您可以改用 RDP 客户机来替换 KVM 客户机。远程服务器必须配置为接收 RDP 连接。

Knock-knock 功能部件描述

当所有可能的远程控制会话都被占用时（单用户方式选项中的一个会话或多用户方式选项中的六个会话），另一个 Web 用户可以向已启用 Knock-knock 功能部件的远程控制用户发送断开连接请求。只有当启用 Knock-knock 功能部件的用户未处理来自其他 Web 用户的断开连接请求时，才可能出现此情况。

如果已启用 Knock-knock 功能部件的远程控制用户接受请求或在超时值指示的时间内未回复请求，那么远程控制会话将终止，并将为发送请求的 Web 用户保留。如果发送断开连接请求的 Web 用户在五分钟内不启动带有保留远程控制会话的 Java 或 ActiveX 远程控制会话，那么将不再为 Web 用户保留远程控制会话。

要启用 Knock-knock 功能部件，请完成以下步骤：

1. 通过选择以下一个菜单选项访问 Remote Control 页面：
 - 单击 Server Management 选项卡中的 **Remote Control**。
 - 单击 System Status 页面上的 **Remote Control...**。
2. 单击 **Allow others to request my remote session disconnect** 复选框。

注：必须存在一个或多个当使用远程控制功能部件时会选中 **Allow others to request my remote session disconnect** 复选框的其他用户。

3. 从 **No response time interval** 字段中选择时间间隔。
4. 通过选择用户方式来启动远程控制会话。选择以下方式之一：
 - 以单用户方式启动远程控制
 - 以多用户方式启动远程控制

备注：

- 在多用户方式下，IMM2 最多支持六个同时发生的视频会话。
- 将会自动启用 Knock-knock 功能部件。

下图显示步骤 2 到 4 中描述的字段。

要请求远程会话，请完成以下步骤：

1. 单击 **Refresh** 以显示正在进行中的远程控制会话。

下图显示 Remote Control Session in Progress 窗口。

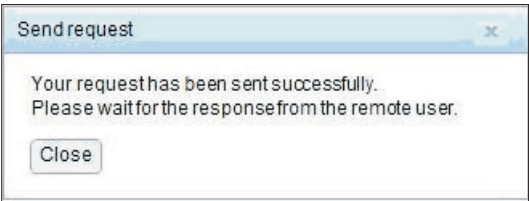
Remote Control Session in Progress			
If all sessions are currently consumed, you can send a request to disconnect one of the available sessions.			
Refresh			
User Name	Active Sessions	Availability for Disconnection	Timeout Value
USERID	192.168.5.11	Request to connect	1 hour

您将在 **Availability for Disconnection** 字段中看到以下响应之一：

- **Request to connect:** 当远程控制用户启用 Knock-knock 功能部件且未在处理来自另一 Web 用户的断开连接请求时，会显示此文本。当前 Web 用户尚未向远程控制用户发送断开连接请求。
- **Waiting for response:** 当远程控制用户正在处理来自当前 Web 用户的断开连接请求时，会显示此文本。当前 Web 用户可以通过单击 **Cancel** 按钮来向远程控制用户发送取消请求。
- **Other request is pending:** 针对以下情况之一会显示此文本：
 - 远程控制用户正在处理来自另一 Web 用户的断开连接请求。
 - 远程控制用户已启用 Knock-knock 功能部件，并且当前 Web 用户正在等待来自另一远程控制用户的断开连接请求的响应。
- **Not available:** 在以下一种情况下会显示此文本：
 - 所有远程控制会话都未被占用。远程控制用户是否已启用 Knock-knock 功能部件对此情况没有影响。
 - 所有远程控制会话都被占用，并且远程控制用户尚未启用 Knock-knock 功能部件。
 - 此远程控制连接为另一用户保留五分钟。

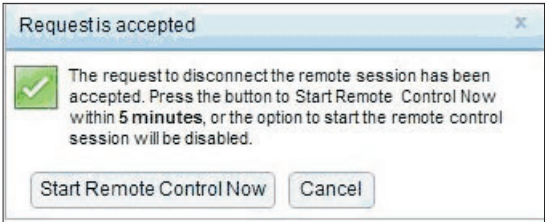
2. 单击 **Request to connect** 以向远程控制用户发送断开连接请求。

下图显示成功发送请求时所显示的窗口。

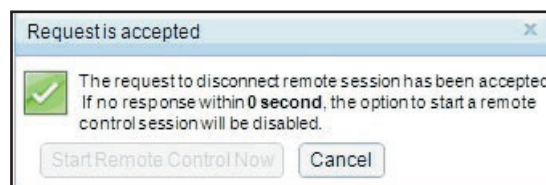


如果远程控制用户接受断开连接请求，那么 Web 用户在五分钟内必须启动远程控制会话。如果 Web 用户在五分钟内未启动会话，那么将不保留该会话。

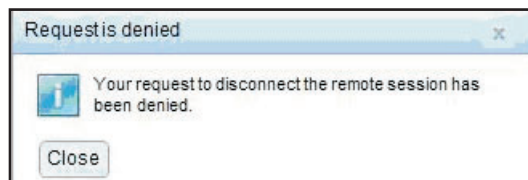
下图显示接受断开连接请求并且请求处于保留状态时所显示的信息。



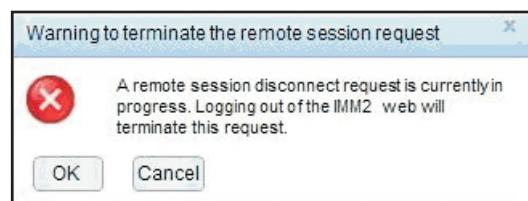
下图显示接受断开连接请求并且请求处于未保留状态时所显示的信息。



如果远程控制用户拒绝断开连接请求，那么提交断开连接请求的用户将接收表明拒绝请求的信息（如下图所示）。

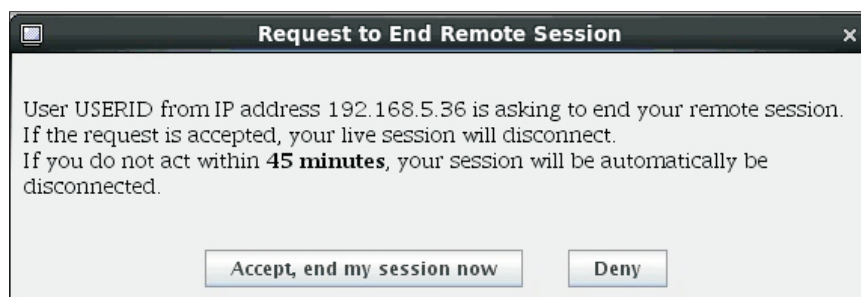


如果 Web 用户尝试在接收有关其请求的消息之前注销 IMM2，那么 Web 用户将接收一条消息（如下图所示）。

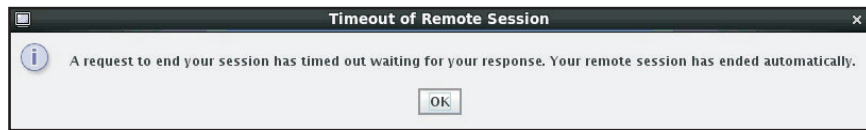


远程控制用户接收请求后，用户必须确定在启动远程控制会话之前是否在选定的间隔时间内释远程会话。将会显示 Request to End Remote Session 窗口，以提示远程控制用户剩余的任何时间。

下图中显示了 Request to End Remote Session 窗口。



如果远程控制用户选择 **Accept, end my session now**，那么远程查看器将自动关闭。如果远程控制用户选择 **Deny**，那么远程控制用户将继续保留远程会话。结束 Request to End Remote Session 后，将自动释远程会话并会打开以下窗口。



远程磁盘

在 Virtual Media Session 窗口中，可以向服务器分配一个您计算机上的 CD 或 DVD 驱动器、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。您可将该驱动器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。驱动器和磁盘映像在服务器上显示为 USB 驱动器。

备注：

- USB 支持是远程磁盘功能所必需的。以下服务器操作系统具有 USB 支持：
 - Microsoft Windows Server 2003 : Web、Std、Ent、DC (SP2、R2、SBS)
 - Microsoft Windows Server 2008 SP2 : Std、SBS、EBS
 - Microsoft Windows Server 2008 R2
 - SUSE Linux Enterprise Server V10 SP3 : x86_64
 - SUSE Linux Enterprise Server V11 : x86、_64
 - Red Hat Enterprise Linux Enterprise Servers V3.7 : x86、x86_64
 - Red Hat Enterprise Linux Enterprise Servers V4.8 : x86、x86_64
 - Red Hat Enterprise Linux Enterprise Servers V5.5 : x86、x86_64
 - Red Hat Enterprise Linux Enterprise Servers V6.0 : x86、x86_64
 - ESX 4.5 : 4.0 U1
- 客户机服务器需要 Java 1.5 插件或更高版本。
- 客户机服务器必须具有 Intel Pentium III 微处理器或更高版本（运行速度为 700 MHz 或更快），或者与其相当的微处理器。

访问远程控制

要开始远程控制会话并访问远程磁盘，请完成以下步骤：

1. 在 Video Viewer 窗口中，单击 **Tools**。
2. 单击 **Launch Virtual Media**。此时会打开 Video Viewer 窗口。

注：如果在打开 Video Viewer 窗口之前选中了 **Encrypt disk and KVM data during transmission** 复选框，那么会通过 ADES 加密来加密磁盘数据。

Virtual Media Session 窗口独立于 Video Viewer 窗口。Virtual Media Session 窗口列出了客户机上所有可映射为远程驱动器的驱动器。通过 Virtual Media Session 窗口，还可以将 ISO 和软盘映像文件映射为虚拟驱动器。每个映射的各驱动器可标记为只读。CD 和 DVD 驱动器以及 ISO 映像始终为只读。

映射和取消映射驱动器

要映射驱动器，请选中要映射的驱动器旁边的 **Select** 复选框。

注：CD 或 DVD 驱动器在映射之前必须包含介质。如果驱动器为空，那么系统会提示您将 CD 或 DVD 插入驱动器。

单击 **Mount Selected** 按钮以安装并映射一个或多个所选驱动器。如果单击 **Add Image**，那么可以将软盘映像文件和 ISO 映像文件添加到可用驱动器列表。在 Virtual Media Session 窗口中列出软盘或 ISO 映像文件后，可以对其进行映射，就如同其他驱动器一样。要取消映射驱动器，请单击 **Unmount All** 按钮。取消映射驱动器之前，必须确认要取消映射这些驱动器。

注：确认要取消映射驱动器之后，将会卸载所有驱动器。不能分别卸载驱动器。

将映像添加列表后并且 **Map** 复选框处于选中状态时，（如果映像适合装入 IMM2 内存以用于卡上的远程磁盘 (RDOC) 功能）将打开一个窗口。该窗口用于选择是否将该映像传输到服务器。如果选择 **Yes**，请为该映像输入名称。

注：请勿在名称中输入特殊字符，例如“&”字符或空格。

将映像装入 IMM2 内存可使磁盘能够保持安装在服务器上，以便您可以稍后访问磁盘，即使在 IMM2 Web 界面会话结束后也如此。虽然可以将多个映像存储在 IMM2 上；但是，所使用的总空间不能超过 50 Mb。要卸载存储器中的映像文件，请在 RDOC Setup 窗口中选择名称，然后单击 **Delete**。

退出远程控制

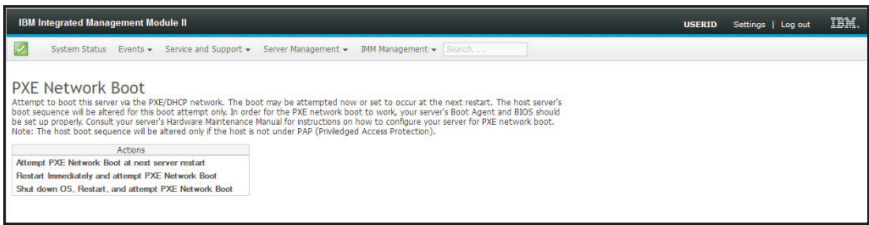
完成使用远程控制功能时，关闭 Video Viewer 和 Virtual Media Session 窗口。

设置 PXE 网络引导

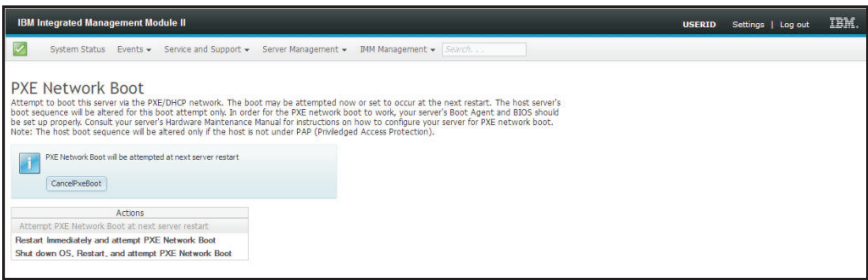
使用 PXE Network Boot 选项可设置对预引导服务器执行环境的尝试。请执行以下步骤，以将服务器设置为在下次服务器重新启动时尝试预引导执行环境网络引导。

1. 登录到 IMM2。有关更多信息，请参阅第 10 页的『登录到 IMM2』以获取更多信息。
2. 单击 **Server Management**；然后，选择 **PXE Network Boot**。

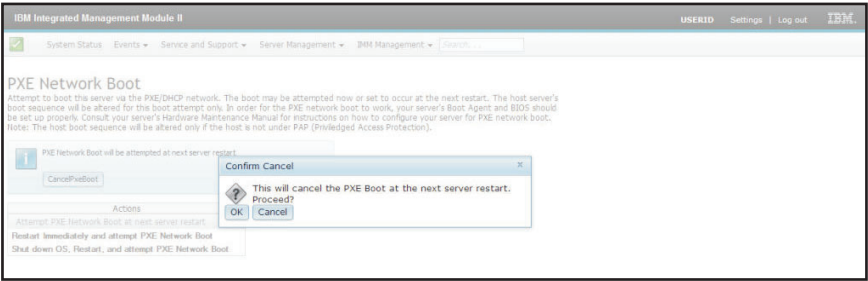
此时将打开以下窗口。



3. 从 Action 选项中选择 **Attempt PXE Network Boot at next server restart**。此时将打开以下窗口。



如果您希望取消选择，请单击 **CancelPxeBoot**。这样会打开以下 Confirm Cancel 窗口。



更新服务器固件

Server Firmware 选项显示固件级别，并允许您更新 DSA、IMM2 和 UEFI 固件。将会显示 IMM2、UEFI 和 DSA 固件的当前版本。这包括 Active、Primary 和 Backup 版本。

下图显示 Server Firmware 页面。

Firmware Type	Status	Version	Build	Release Date
DSA	Active	9.24	DSVT44B	2012-06-10
IMM2				
IMM2 (Primary)	Active	2.15	140039Q	2013-01-28
IMM2 (Backup)	Inactive	3.00	140039T	2013-01-30
UEFI				
UEFI (Primary)	Active	1.20	D7E120CUB	2012-09-23
UEFI (Backup)	Inactive	1.20	D7E120CUB	2012-09-23

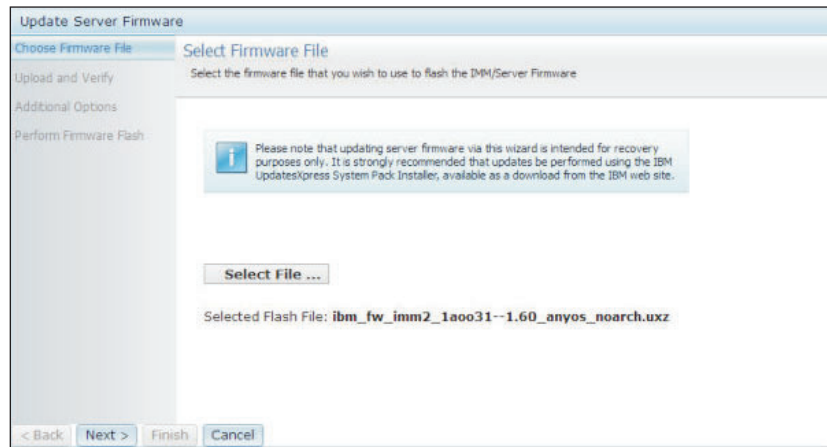
将显示 IMM2、UEFI 和 DSA 固件的当前状态和版本，包括 Primary 和 Backup 版本。固件状态有三种类别：

- **Active**：固件处于活动状态。
- **Inactive**：固件处于非活动状态。
- **Pending**：固件正在等待变为活动状态。

注意：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，请阅读所下载更新随附的任何自述文件和变更历史记录文件。这些文件包含有关更新的重要信息和安装更新的过程，包括从早期固件或设备驱动程序版本更新到最新版本的任何特殊过程。

要更新服务器固件，请完成以下步骤：

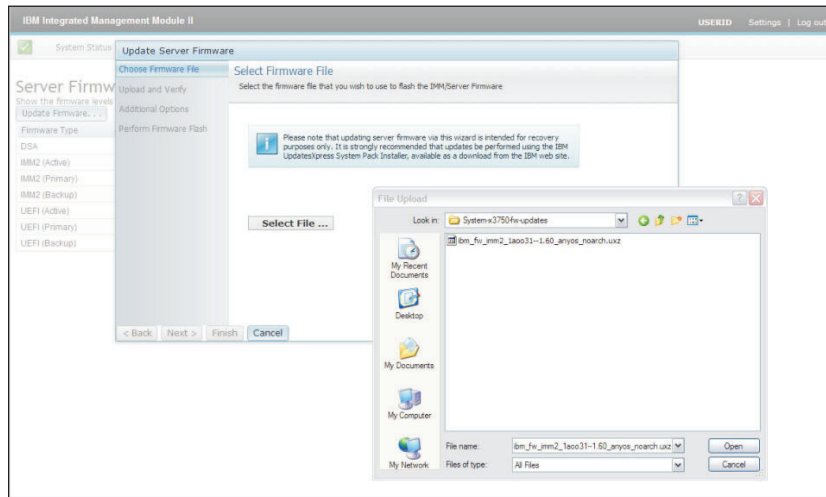
1. 单击 **Server Management** 菜单列表中的 **Server Firmware**。
2. 单击 **Update Firmware**。这样会打开 **Update Server Firmware** 窗口（如下图所示）。



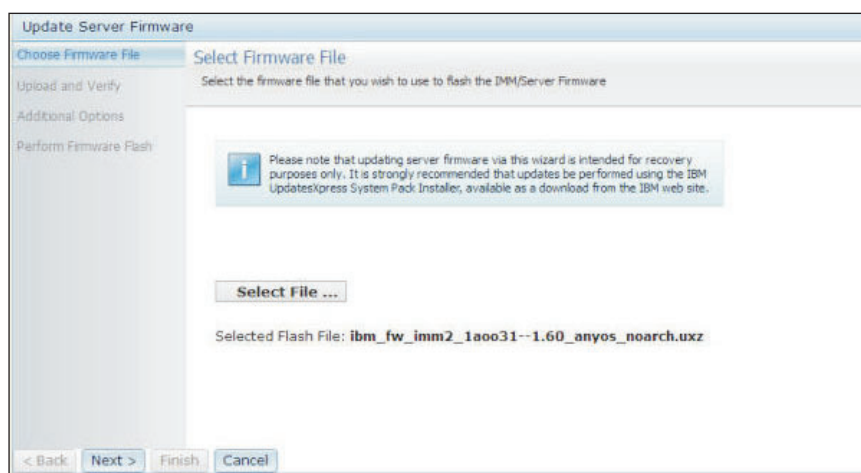
3. 请先阅读警告声明，然后再继续下一步。
4. 执行以下步骤之一：
 - 单击 **Cancel** 并返回到先前的 **Server Firmware** 窗口。
 - 单击 **Select File...** 以选择要用于更新服务器固件的固件文件。

注：Update Server Firmware 窗口最初打开时，所有其他选项都会灰显。

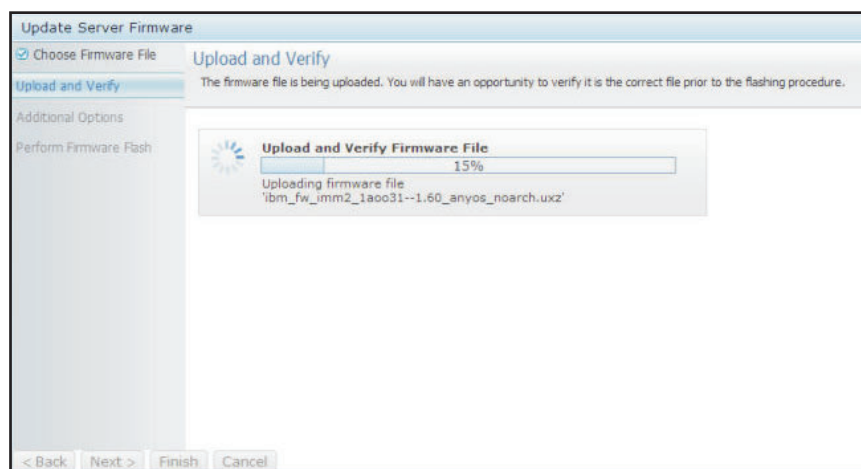
单击 **Select File...** 时，会打开 **File Upload** 窗口（如下图所示）。通过此窗口，可以浏览至所需文件。



5. 浏览至要选择的文件，然后单击 **Open**。您将返回到显示了所选文件的 **Update Server Firmware** 窗口（如下图所示）。

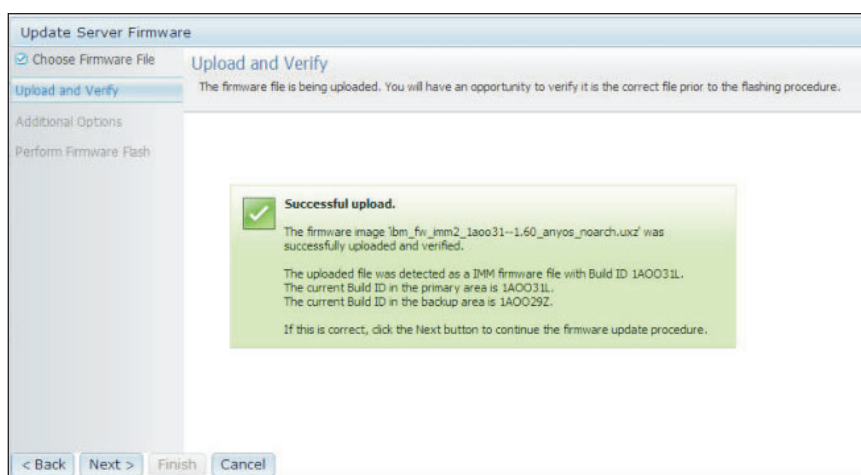


- 单击 **Next >** 以开始上载并验证所选文件上的进程。上载并验证文件时，将会显示进度计量表（如下图所示）。



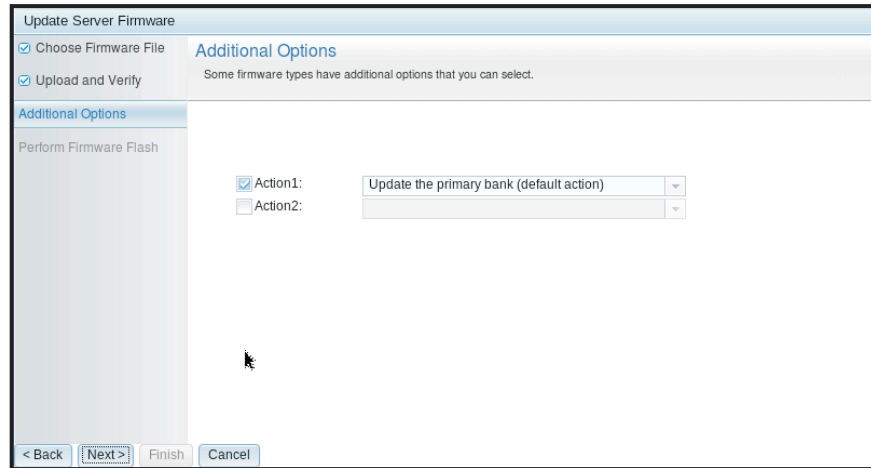
您可以查看此状态窗口，以验证选定要更新的文件是否是正确的文件。状态窗口将包含有关要更新的固件文件类型（如 DSA、IMM 或 UEFI）的信息。

成功上载并验证固件文件后，会打开 Successful upload 窗口（如下图所示）。

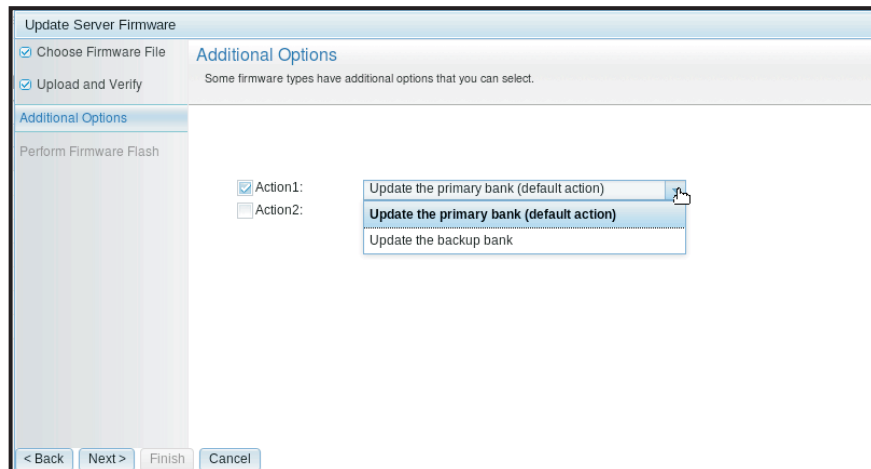


7. 如果信息正确，请单击 **Next >**。如果要重做任何选择，请单击 **< Back**。

如果单击 **Next >**，那么会显示一组其他选项（如下图所示）。



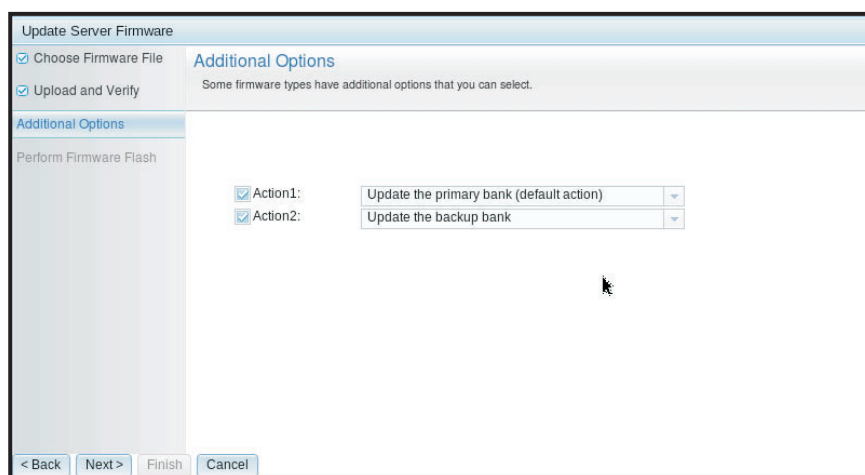
8. 通过 **Action 1** 字段旁的下拉菜单，可以选择 **Update the primary bank (default action)** 或 **Update the backup bank**（如下图所示）。



选择操作后，您将返回到显示了所请求的其他操作的先前屏幕。

装入所选操作后，会显示该操作和新的 **Action 2** 下拉菜单（如下图所示）。

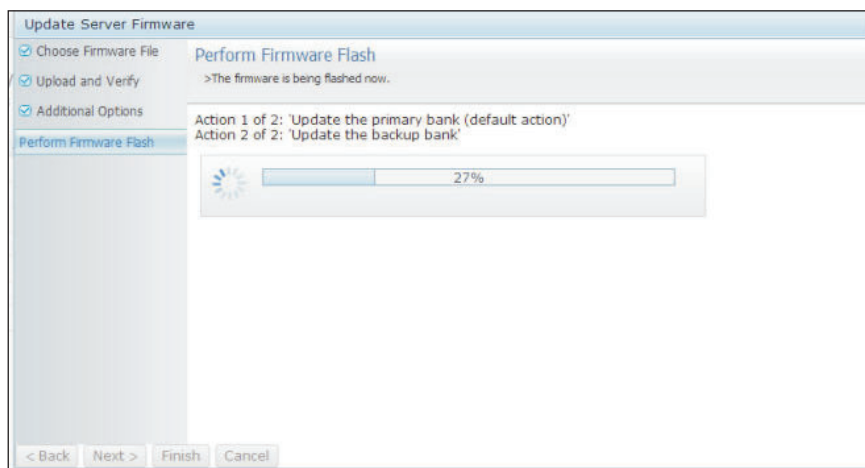
注：要禁用操作并再次启动其他选项过程，请单击相关操作旁的复选框。



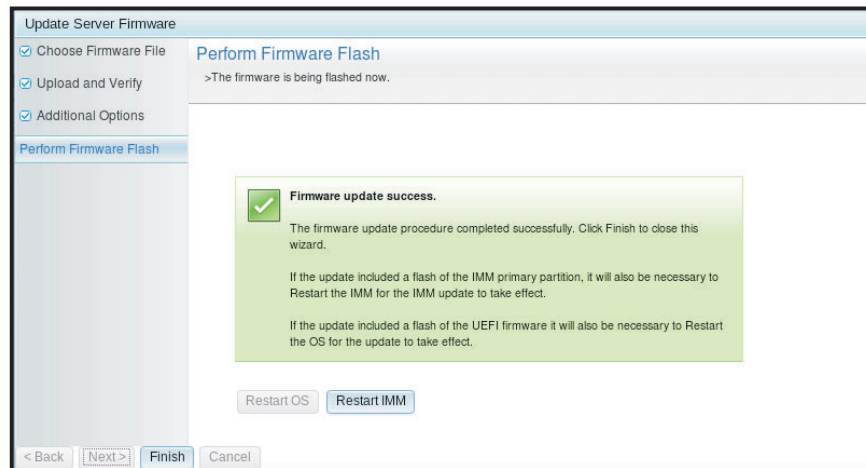
上一个屏幕显示了对 Action 1，选择要更新主内存区。您还可以在 Action 2 下选择更新备份内存区（如上一个屏幕所示）。单击 **Next >** 时，将同时更新主内存区和备份内存区。

注：Action 1 必须不同于 Action 2。

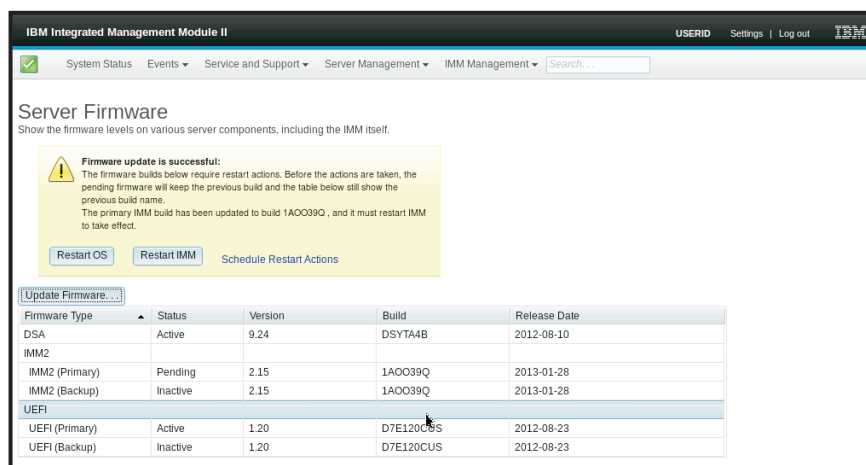
进度计量表显示主内存区和备份内存区的更新进度（如下图所示）。



成功完成固件更新后，会打开以下窗口。根据显示的内容选择相关操作，以完成更新过程。



如果主要的固件更新未完成，那么当显示 Server Firmware 屏幕时会打开以下窗口。



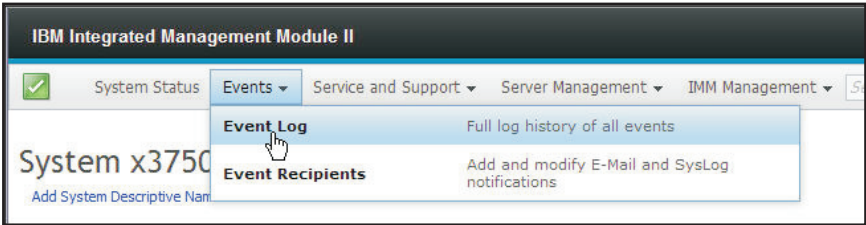
管理系统事件

通过 Events 菜单，可以管理 Event Log 历史记录以及电子邮件和系统日志通知的 Event Recipients。

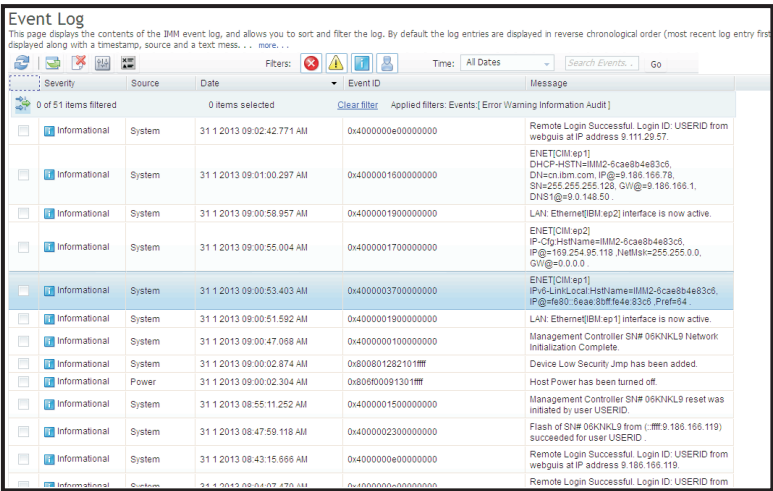
管理事件日志

单击 **Event Log** 选项以显示 Event Log 窗口。Event Log 窗口包含由 IMM2 报告的事件的描述，以及有关所有远程访问尝试和配置更改的信息。日志中的所有事件都使用 IMM2 日期和时间设置添加了时间戳记。某些事件会生成警报（如果在 Event Recipients 窗口上对其进行了该配置）。您还可以对事件日志中的事件进行排序和过滤。IMM2 日志的容量可以容纳大约 1024 条事件记录和 1024 条审计记录。实际记录数取决于每个日志的记录内容的大小。

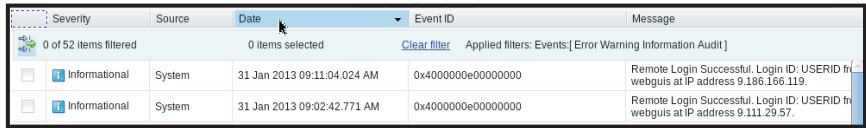
单击 **Event Log** 选项。此时将打开以下窗口。



选择 Event Log 选项后，将打开以下窗口。



要对事件日志中的事件进行排序和过滤，请选择列标题（如下图所示）。

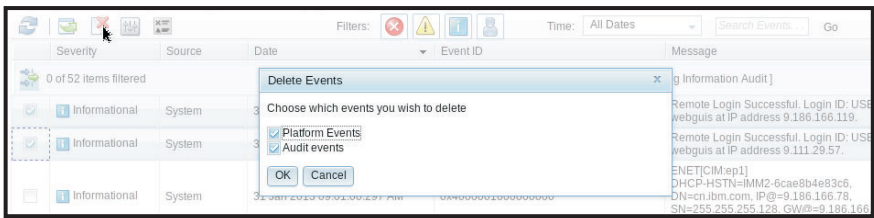


您可以使用 **Export** 按钮将事件日志中的所有事件或选定事件保存到文件。要选择特定事件，请在 Event Log 主页面上选择一个或多个事件并左键单击 **Export** 按钮（如下图所示）。

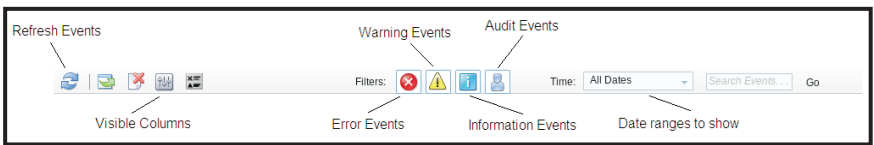


要选择希望删除的事件的类型，请单击 **Delete Events**。必须选择希望删除的事件的类别。

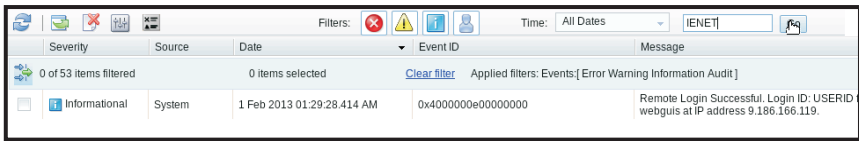
下图显示 Delete Events 窗口。



要选择希望显示的事件日志条目的类型，请单击相应按钮（如下图中所示）。



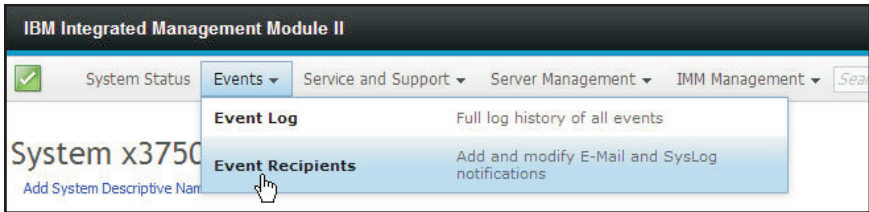
要搜索特定类型的事件或关键字，请在 **Search Events** 字段中输入事件或关键字的类型，然后单击 **Go**（如下图中所示）。



系统事件通知

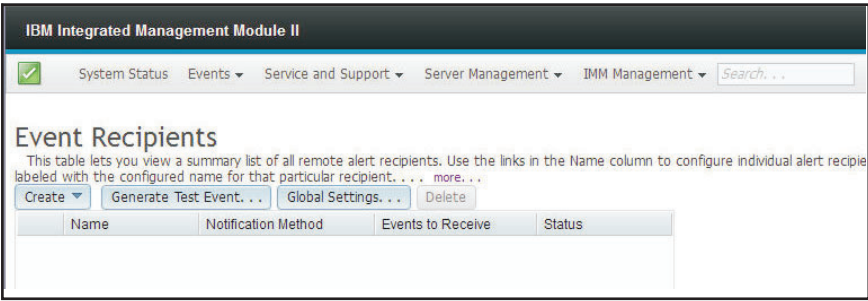
选择 **Event Recipients** 选项以添加和修改电子邮件和系统日志通知。

下图显示 Event Recipients 选项的选择。

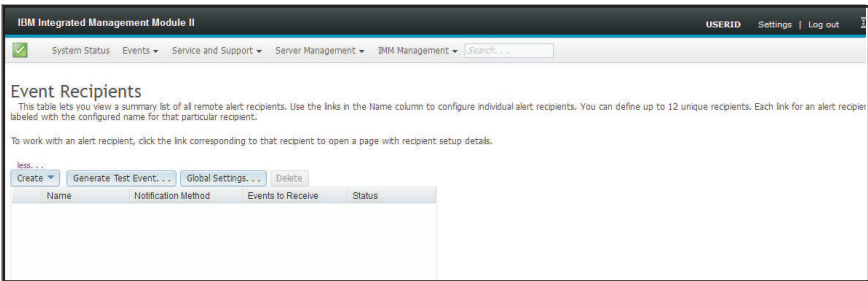


通过 Event Recipients 选项，可以管理将收到系统事件通知的人员。您可以配置每个接收方，并管理适用于所有事件接收方的设置。您还可以生成测试事件，以验证通知功能操作。

下图显示 Event Recipients 页面。



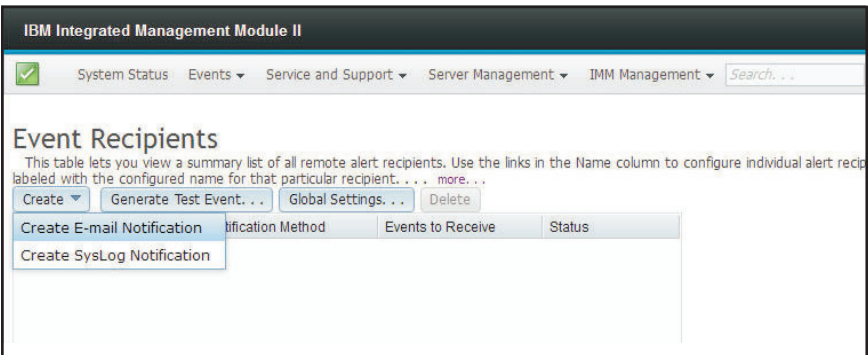
下图显示单击 Event Recipients 页面上的 **more** 链接时所显示的其他信息。



创建电子邮件和系统日志通知

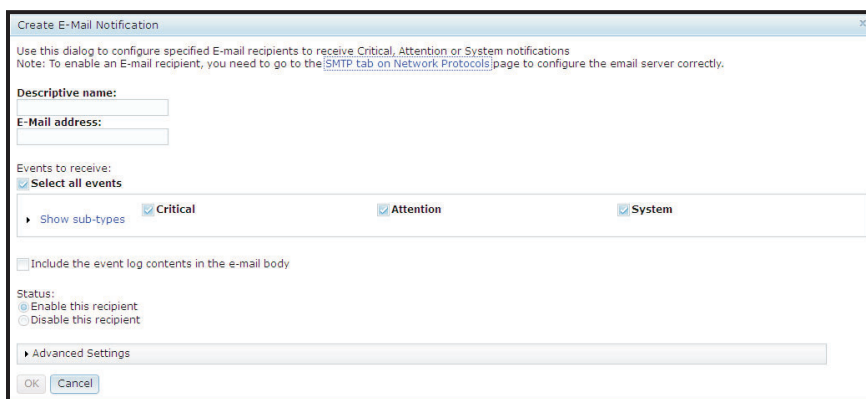
选择 **Create** 选项卡以创建电子邮件和系统日志通知。

下图显示 Create 菜单中可用的选项。

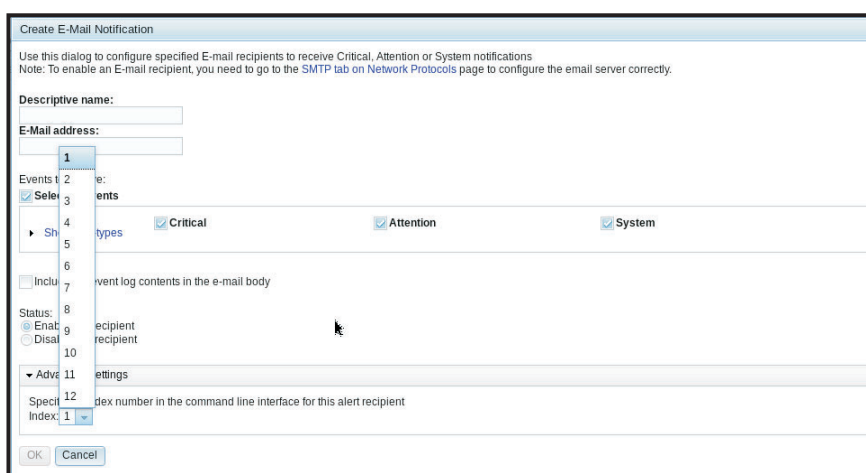


在 **Create E-mail Notification** 选项中，可以设置目标电子邮件地址，并选择您希望收到通知的事件类型。此外，可以单击 **Advanced Settings** 以选择起始索引号。要在电子邮件中包含事件日志，请选中 **Include the event log contents in the e-mail body** 复选框。

下图显示 Create E-mail Notification 屏幕。

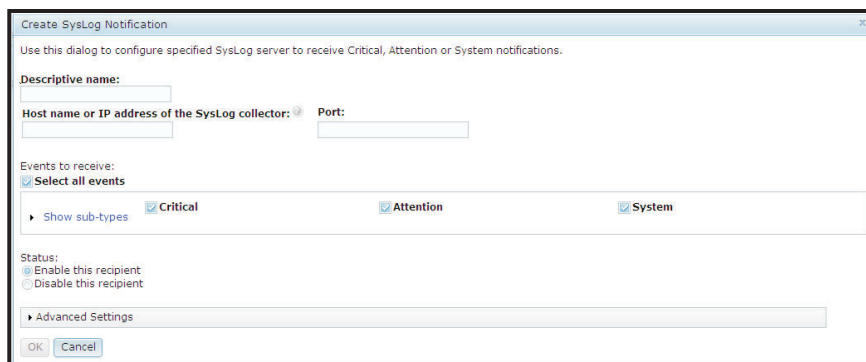


下图显示 Advanced Settings 窗格中的选项。



在 **Create Syslog Notification** 选项中，可以设置系统日志收集器的主机名和 IP 地址，并且选择您希望收到通知的事件类型。您可以单击 **Advanced Settings** 以选择起始索引号。您还可以指定要用于此通知类型的端口。

下图显示 Create Syslog Notification 屏幕。



下图显示 Advanced Settings 窗格中的选项。

Create SysLog Notification

Use this dialog to configure specified SysLog server to receive Critical, Attention or System notifications.

Descriptive name:

Host no:

Address of the SysLog collector: Port:

Events to receive:

☒ Critical ☒ Attention ☒ System

Status: ☒ Enabled ☐ Disabled

Special Index:

OK Cancel

生成测试事件

使用 **Generate Test Event...** 选项卡，以将测试电子邮件发送到所选电子邮件目标。选择事件通知后，单击 **OK** 以生成测试事件。测试事件将发送给接收方，并通知这是一次测试。

下图显示 **Generate Test Event** 窗口。

IBM Integrated Management Module II

USERID Settings Log out

System Status Events Service and Support Server Management IBM Management Search...

Event Recipients

The table lets you view a summary list of all remote alert recipients. Use the links in the Name column to configure individual alert recipients. You can define up to 12 unique recipients. Each link for an alert recipient is labeled with the configured name for that particular recipient. ... more ...

Create Generate Test Event... Global Settings... Delete

Name	Notification Method	Events to Receive	Status
Target User	E-Mail	None	Enabled

Generate Test Event

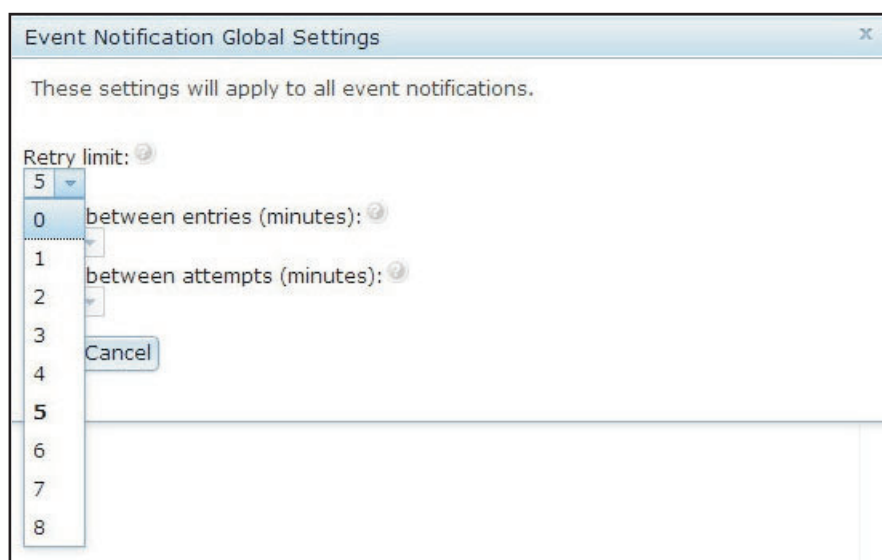
This will generate a test event and will be broadcast to the recipient 'Target User' indicating that it is just a test. Do you wish to proceed?

OK Cancel

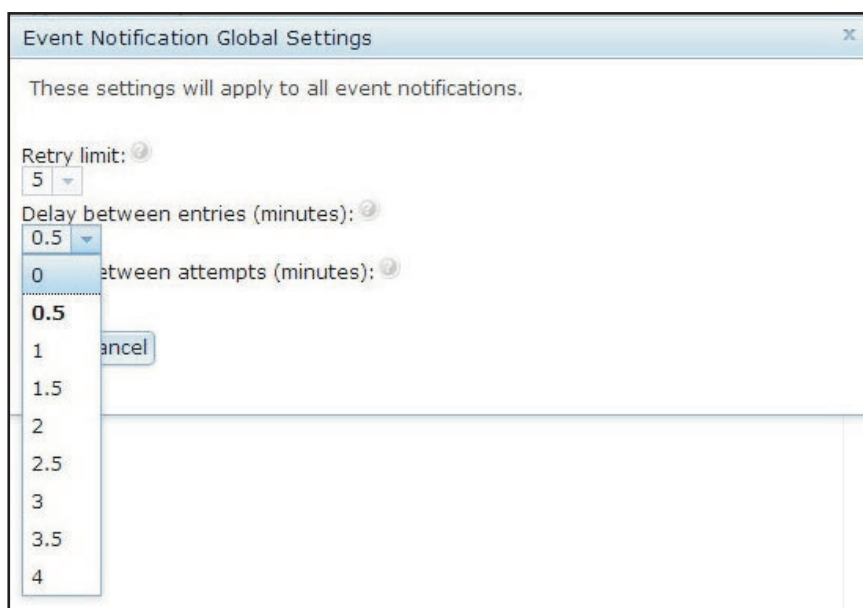
设置通知重试限制

使用 **Global Settings...** 选项卡以设置重试事件通知、重试事件通知条目之间的延迟（以分钟为单位）和重试尝试之间的延迟（以分钟为单位）所受的限制。

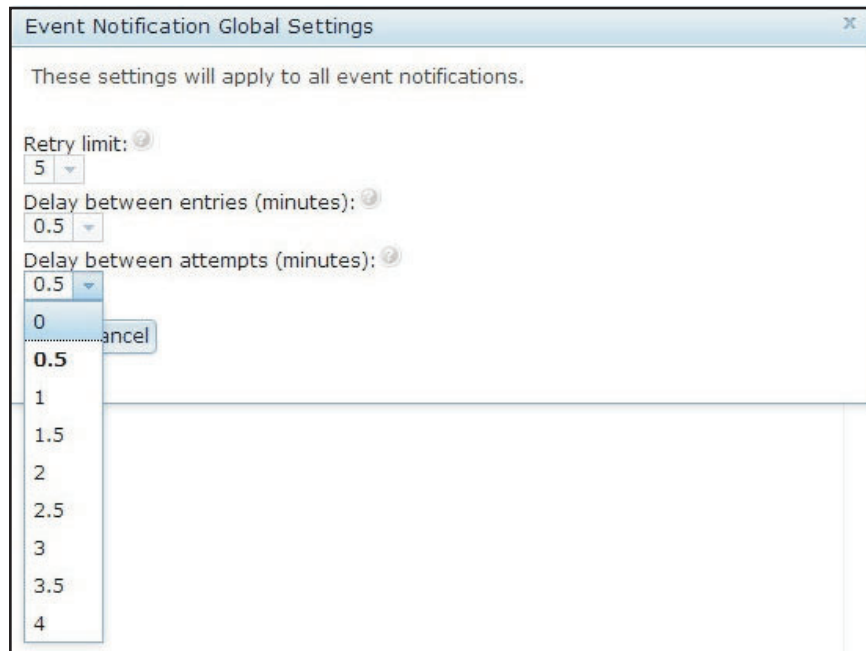
下图显示 **Retry limit** 选项的设置。



下图显示 Delay between entries (minutes) 选项的设置。



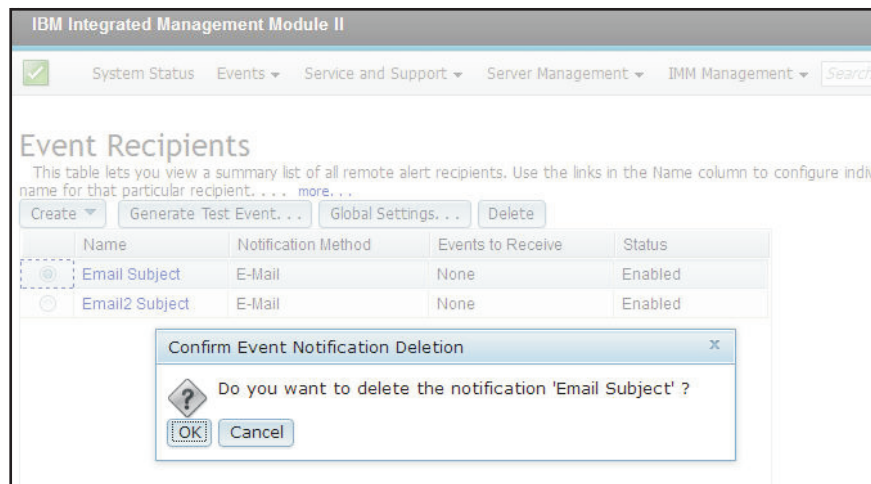
下图显示 Delay between attempts (minutes) 选项的设置。



删除电子邮件或系统日志通知

使用 **Delete** 选项卡以除去电子邮件或系统日志通知目标。

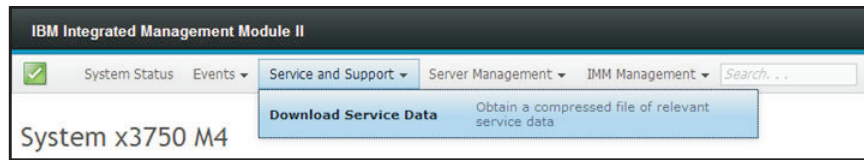
下图显示 Confirm Event Notification Deletion 窗口。



收集服务和支持信息

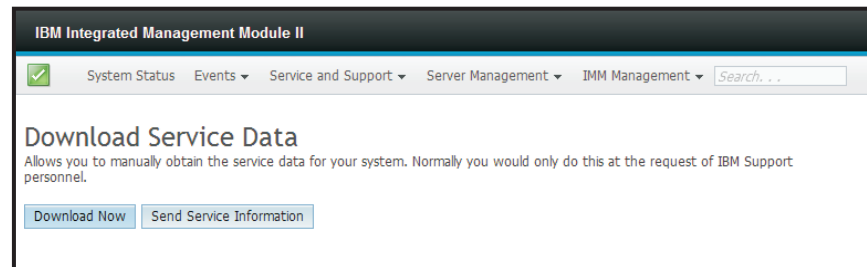
单击 **Service and Support** 菜单下的 **Download Service Data** 选项，以收集有关服务器的信息，IBM 支持人员可使用该信息来帮助您解决问题。

下图显示 **Service and Support** 菜单。



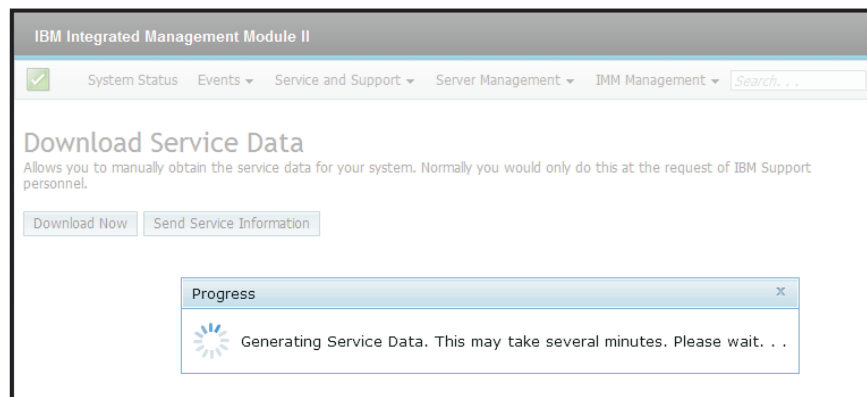
如果要下载服务和支持数据，请单击 **Download Now** 按钮。

下图显示 **Download Service Data** 窗口。

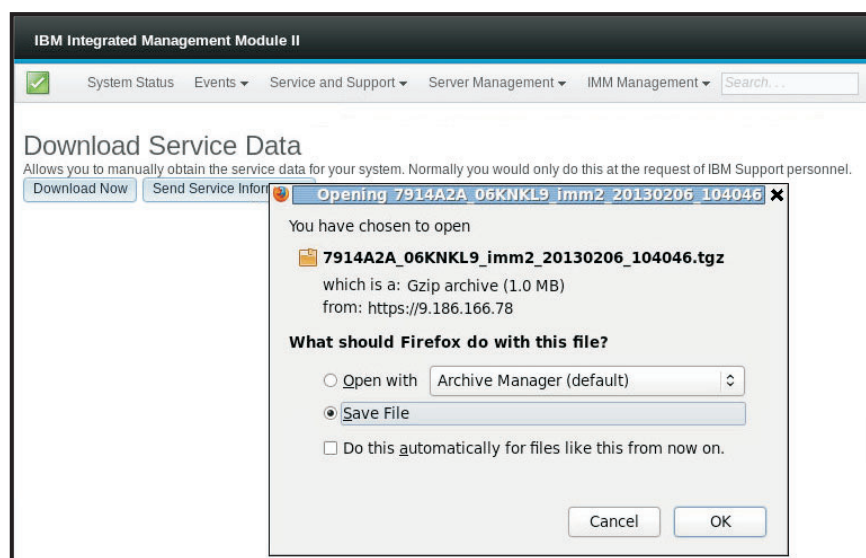


这样将启动收集服务和支持数据的过程。该过程需要几分钟时间来生成可保存到文件的服务数据。

生成服务数据时，将看到以下 **Progress** 窗口。



当该过程完成时，将提示您输入要保存文件的位置。请参阅下图以获取示例。



捕获最新操作系统故障屏幕数据

使用 Latest OS Failure Screen 选项以捕获操作系统故障屏幕数据并存储数据。IMM2 仅存储最近的错误事件信息，从而在发生新错误事件时覆盖较早的操作系统故障屏幕数据。必须启用操作系统看守程序功能部件才能捕获操作系统故障屏幕。如果发生导致操作系统停止运行的事件，那么会触发操作系统看守程序功能部件。只能通过 IMM2 Advanced 级别功能来使用操作系统故障截屏。请参阅服务器文档，以获取有关服务器中所安装 IMM2 的级别的信息。

要远程显示操作系统故障屏幕图像，请选择以下菜单选项之一：

- Server Management 选项卡中的 **Latest OS Failure Screen**
- System Status 页面上的 **Latest OS Failure Screen** 选项卡

注：如果尚未捕获操作系统故障屏幕，那么 System Status 页面上的 Latest OS Failure Screen 选项卡将灰显且无法选择。

下图显示操作系统故障屏幕。

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

The end-user manually generated the crashdump.

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup options, and then
select Safe Mode.

Technical information:

*** STOP: 0x000000E2 (0x0000000000000000,0x0000000000000000,0x0000000000000000,0
x0000000000000000)

Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk: 100
Physical memory dump complete.
Contact your system admin or technical support group for further assistance.
```

管理服务器电源

使用 Power Management 选项卡可执行以下任务：

- 显示有关已安装电源的信息。
- 控制管理电源的方式。
- 控制总系统电源。
- 显示有关已安装电源和当前电源容量的信息。
- 显示已使用电量的历史记录。

选择 Server Management 选项卡下的 **Power Management** 选项，可查看电源管理信息并执行电源管理功能（如下图所示）。

Server Management ▾	IMM Management ▾	Search
Server Firmware	View firmware levels and update firmware	
Remote Control	Allows you access into the operating system of your system	
Server Properties	Various properties and settings related to your system	
Server Power Actions	Power actions such as power on, power off, and restart	
Cooling Devices	Cooling devices installed in your system	
Power Modules	Power modules installed in your system	
Disks	Hard disk drives installed directly in your system	
Memory	RAM installed in your system	
Processors	Physical CPUs installed in your system	
Server Timeouts	Configure watchdogs, etc.	
PXE Network Boot	Settings for how your system performs boot from PXE server	
Latest OS Failure Screen	Windows systems only. View an image of the most recent failure screen.	
Power Management	Power devices, policies, and consumption	

控制电源和总系统电源

单击 **Policies** 选项卡可控制电源的管理方式，并可选择通过在 Active Energy Manager 中设置上限策略来控制总系统电源（如下图所示）。

注：在 IBM Flex System 中未提供 **Policies** 选项卡。

Server Power Management

Manage power related policies and hardware

Policies

Power Modules

Power Allocation

Power History

Power Policies

Redundant with Throttling

Set policies for how or if you wish to protect your system in the case of potential power module failure.

Current Policy: **Power Module Redundancy with Throttling Allowed** [Change](#)

Power Limiting/Capping Policy

Set policies for how or if you wish to limit the total amount of power that the system overall is allowed to consume.

Current Policy: **No Power Limiting** [Change](#)

要选择当潜在电源模块发生故障时用于保护服务器的策略，请单击 Power Policies 窗口中 Redundant with Throttling 选项的当前策略 **Change** 按钮。

注：通过选择电源策略，可以在冗余与可用电源之间进行权衡。

电源策略选择如下：

Redundant without Throttling

如果保证服务器在经历电源丢失后仍继续运行而不调速，那么允许服务器引导。

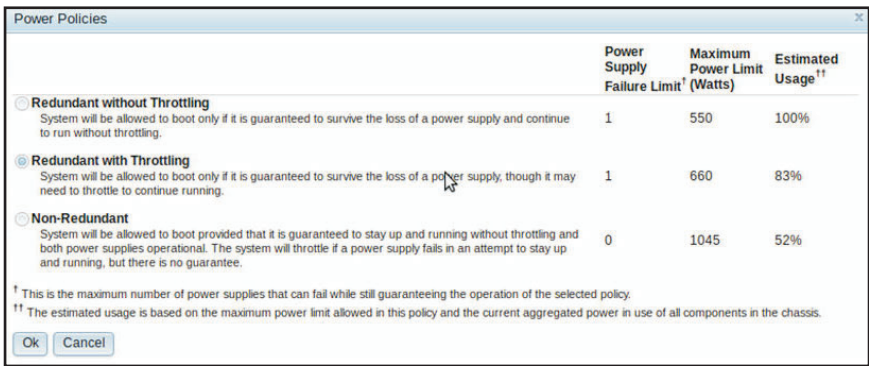
Redundant with Throttling

如果保证服务器在经历电源丢失后仍继续运行，但需要进行调速，那么允许服务器引导。

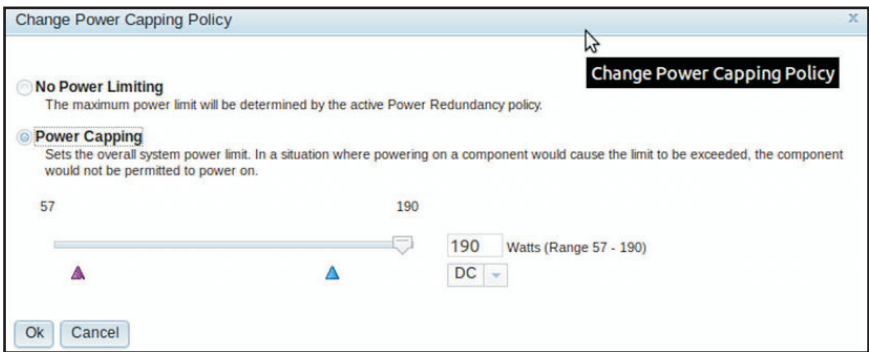
Non-Redundant

如果保证服务器继续运行而不调速并且两个电源都可运行，那么允许服务器引导。如果电源尝试继续保持运行失败，那么服务器将调速；但没有保证。

当选择 Redundant with Throttling 选项的 **Change** 按钮时，将打开以下窗口。



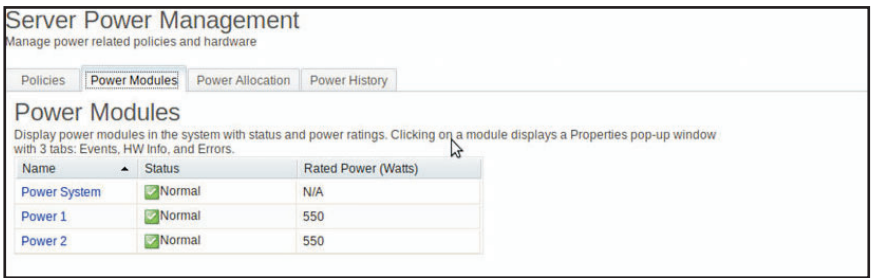
通过 Active Energy Manager，可以限制允许服务器使用的总电量。要设置服务器用电量限制，请单击 Power Policies 窗口中 Power Limiting/Capping Policy 选项的当前策略 **Change** 按钮。这样会打开 Change Power Capping Policy 窗口（如下图所示）。



选择 **Power Capping** 按钮，将滑块标记移至所需的瓦数。滑块标记下的右侧箭头指示 Active Energy Manager 可以保证的最小设置。滑块标记下的左侧箭头指示过去 24 小时内的最大系统用电量。这两个箭头可指导您设置电源上限。

显示当前已安装的电源

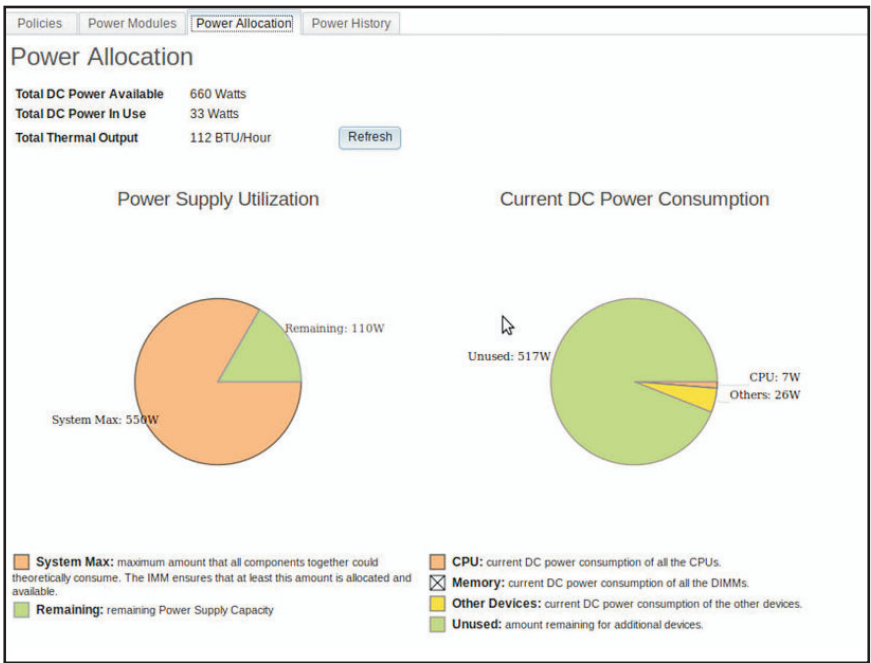
单击 **Power Modules** 选项卡可显示有关当前已安装电源的信息（如下图所示）。



显示服务器中各个电源模块的名称，以及各个电源模块的状态和额定功率。要显示电源模块的其他信息，请单击电源模块名称。这样会打开 Properties 窗口，其中包含三个选项卡：该特定电源模块的 Events、HW Info 和 Errors。

显示电源容量

单击 **Power Allocation** 选项卡可显示正在使用的电源容量以及服务器的当前直流电源耗电量（如下图所示）。



显示电源历史记录

单击 **Power History** 选项卡可显示系统在所选时间段内使用的电量。从 Power History 页面上的 **Chart** 选项卡，可以选择时间段，还有用于查看交流或直流电源的选项。显示了平均、最小和最大用电量（如下图所示）。



第 7 章 Features on Demand

通过 IMM2 Features on Demand (FoD) , 可以安装并管理可选服务器和系统管理功能部件。

有多个级别可用于您服务器的 IMM2 固件功能和功能部件。安装在您的服务器上的 IMM2 固件功能部件的级别根据硬件类型而异。有关您的服务器中 IMM2 硬件和功能部件类型的信息, 请参阅服务器随附的文档。

您可以通过购买并安装 FoD 激活密钥来升级 IMM2 功能。有关 FoD 的其他详细信息, 请参阅位于以下地址的 *Features on Demand User's Guide* : <http://www.ibm.com/systems/x/fod/>。

注: IBM Integrated Management Module Standard Upgrade 是在具有 IMM2 Basic 级别功能的服务器上安装 IBM Integrated Management Module Advanced Upgrade 功能的先决条件。

要订购 FoD 激活密钥, 请联系 IBM 代表或业务合作伙伴, 或者转至 <http://www.ibm.com/systems/x/fod/>。

使用 IMM2 Web 界面或 IMM2 命令行界面 (CLI) 手动安装 FoD 激活密钥, 通过该激活密钥可使用已购买的可选功能部件。在激活密钥之前:

- FoD 激活密钥必须位于用于登录到 IMM2 的系统上。
- 您必须已订购 FoD 选项, 并通过信件或电子邮件接收到其授权代码。

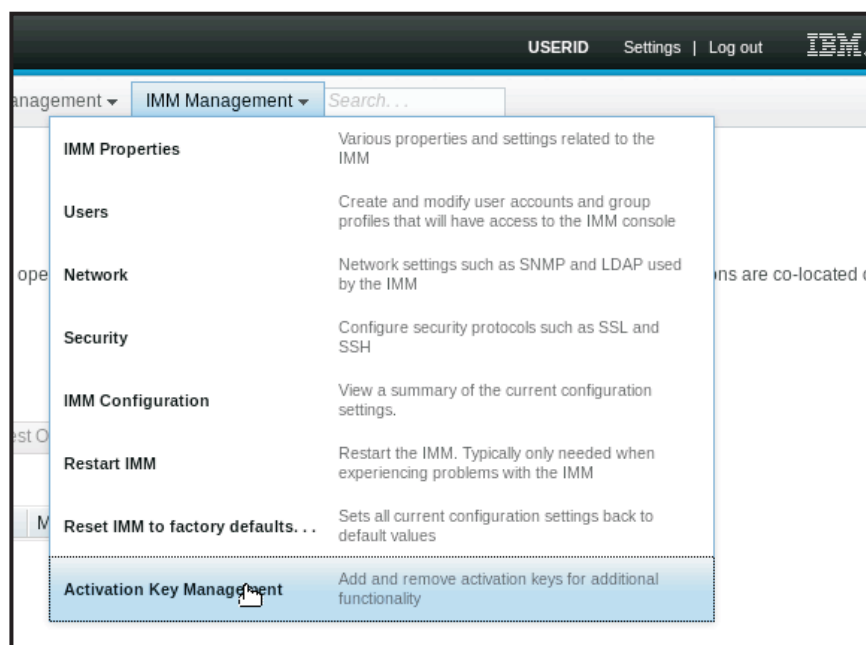
请参阅『安装激活密钥』、第 144 页的『除去激活密钥』或第 145 页的『导出激活密钥』, 以获取有关使用 IMM2 Web 界面管理 FoD 激活密钥的信息。请参阅第 175 页的『keycfg 命令』, 以获取有关使用 IMM2 CLI 管理 FoD 激活密钥的信息。

安装激活密钥

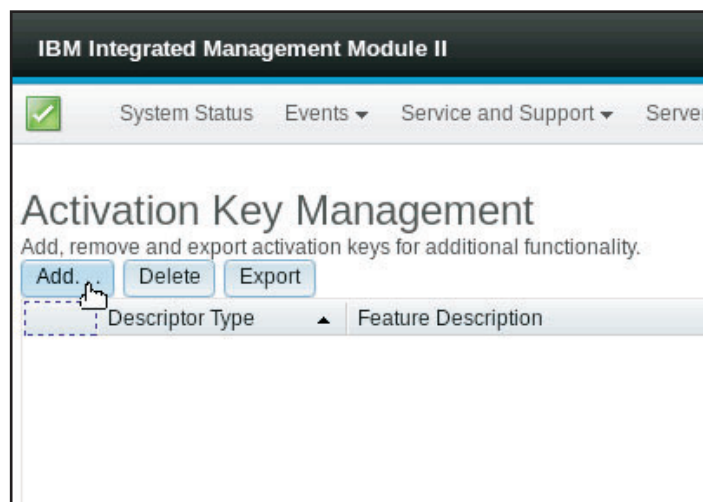
安装 FoD 激活密钥以向服务器添加可选功能部件。

要安装 FoD 激活密钥, 请完成以下步骤:

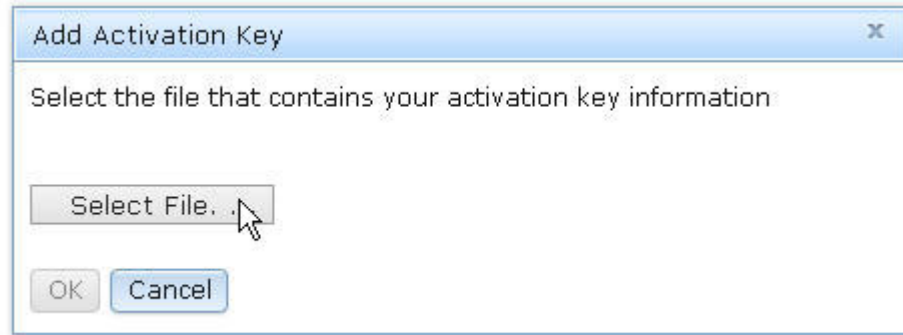
1. 登录到 IMM2。有关更多信息, 请参阅第 10 页的『登录到 IMM2』。
2. 在 IMM2 Web 界面中, 单击 **IMM Management** 选项卡; 然后, 单击 **Activation Key Management**。



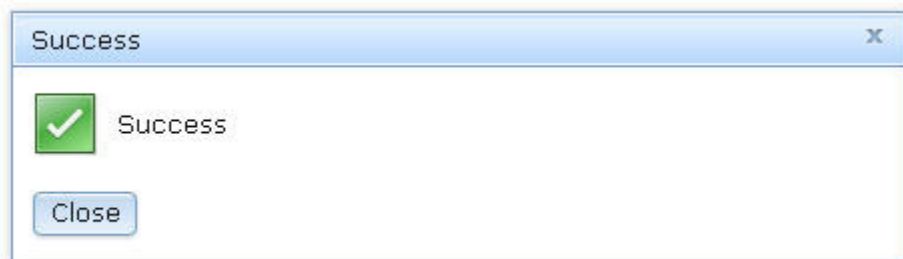
3. 在 Activation Key Management 页面中，单击 **Add...**。



4. 在 Add Activation Key 窗口中，单击 **Select File...**；然后，在 File Upload 窗口中选择要添加的激活密钥文件，并且单击 **Open** 以添加文件或者单击 **Cancel** 以停止安装。要完成添加密钥，请单击 Add Activation Key 窗口中的 **OK**，或者单击 **Cancel** 以停止安装。

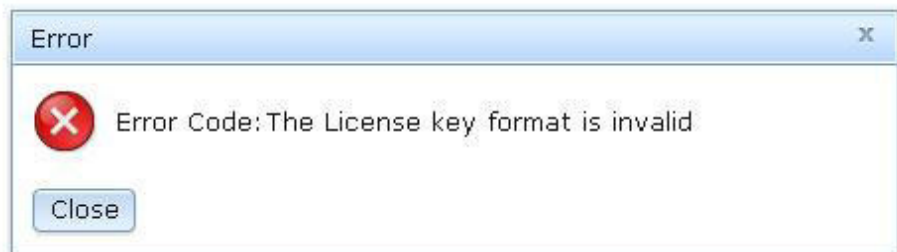


Success 窗口指示已安装激活密钥。

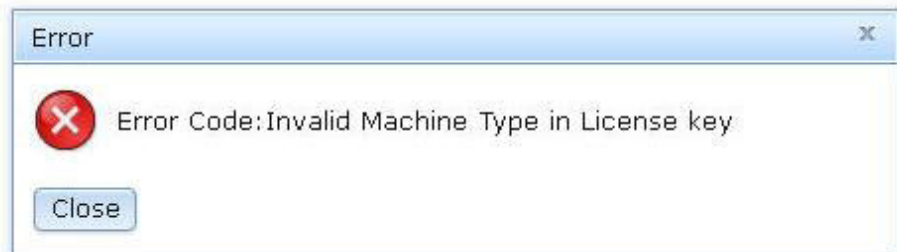


注：

- 如果激活密钥无效，那么将显示以下错误窗口。

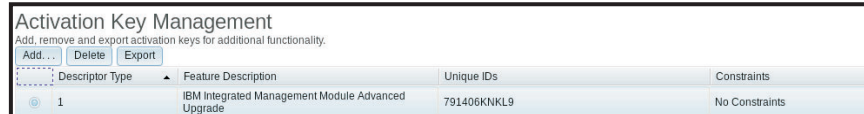


- 如果是尝试在不支持 FoD 功能部件的机器类型上安装激活密钥，那么将显示以下错误窗口。



5. 单击 **OK** 以关闭 Success 窗口。

所选激活密钥已添加到服务器，并出现在 Activation Key Management 页面中。

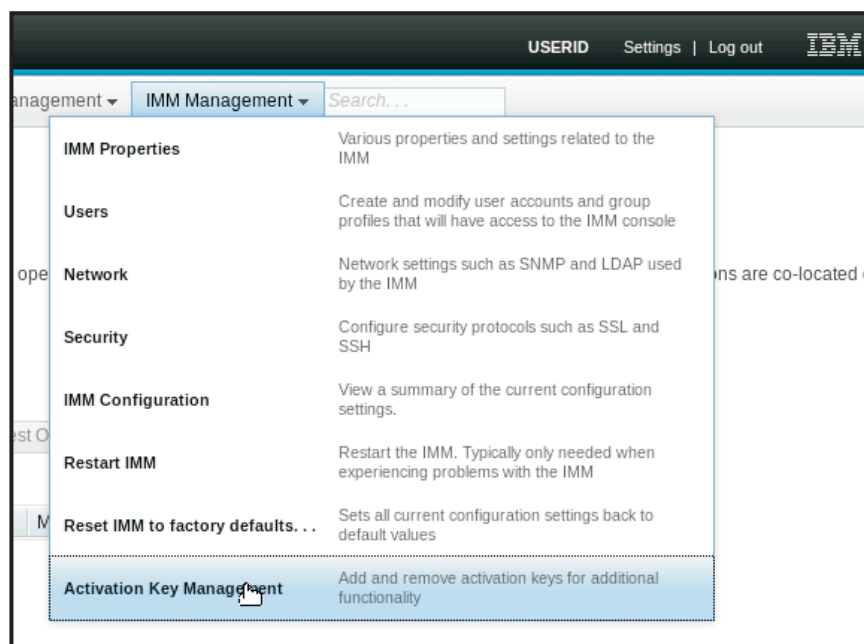


除去激活密钥

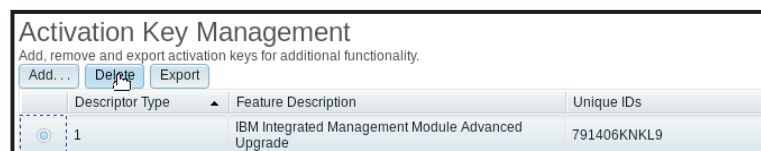
除去 FoD 激活密钥以从服务器中删除可选功能部件。

要除去 FoD 激活密钥，请完成以下步骤：

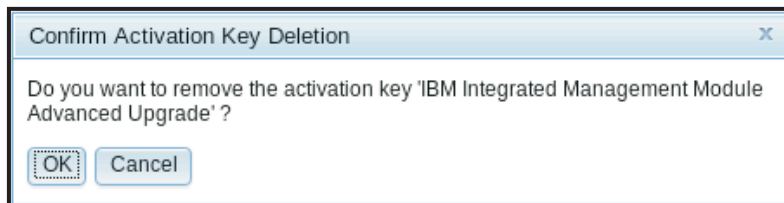
1. 登录到 IMM2。有关更多信息，请参阅第 10 页的『登录到 IMM2』。
2. 在 IMM2 Web 界面中，单击 **IMM Management** 选项卡；然后，单击 **Activation Key Management**。



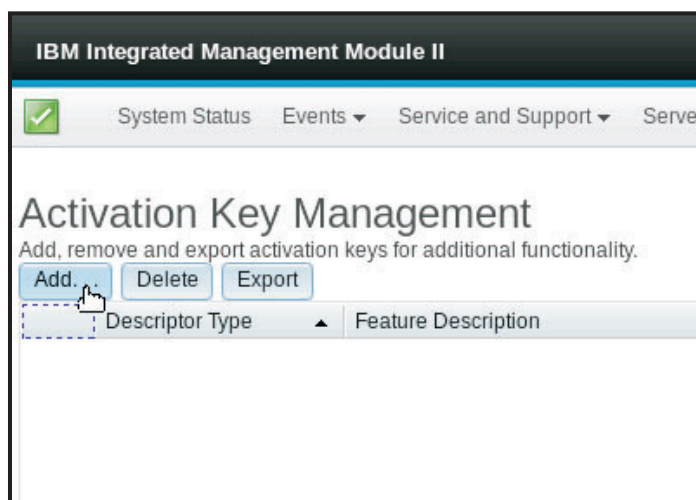
3. 在 Activation Key Management 页面中，选择要除去的激活密钥；然后，单击 **Delete**。



4. 在 Confirm Activation Key Deletion 窗口中，单击 **OK** 以确认激活密钥删除或者单击 **Cancel** 以保留密钥文件。



所选激活密钥已从服务器中除去，并且不再出现在 Activation Key Management 页面中。

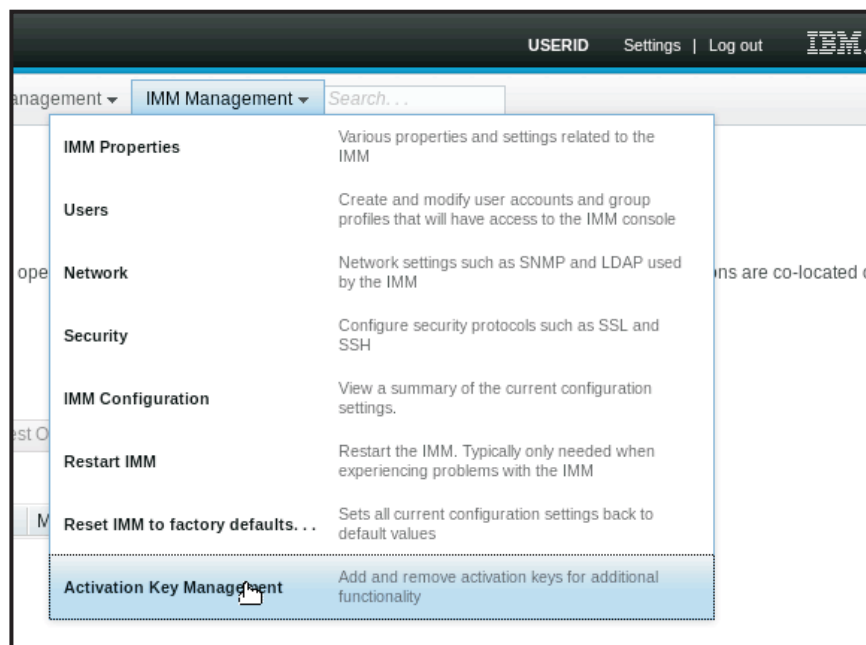


导出激活密钥

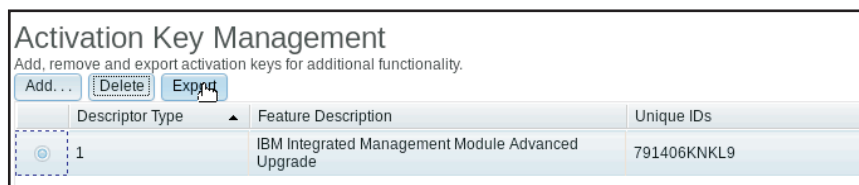
导出 FoD 激活密钥以从服务器导出可选功能部件。

要导出 FoD 激活密钥，请完成以下步骤：

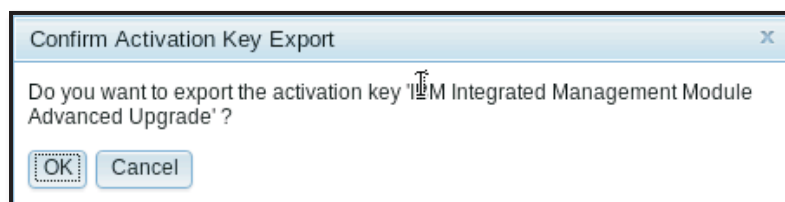
1. 登录到 IMM2。有关更多信息，请参阅第 10 页的『登录到 IMM2』。
2. 在 IMM2 Web 界面中，单击 **IMM Management** 选项卡；然后，单击 **Activation Key Management**。



3. 在 Activation Key Management 页面中，选择要导出的激活密钥；然后，单击 **Export**。



4. 在 Confirm Activation Key Export 窗口中，单击 **OK** 以确认激活密钥导出或者单击 **Cancel** 以取消密钥导出请求。



5. 选择用于保存文件的目录。 所选的激活密钥已从服务器导出。

第 8 章 命令行界面

使用 IMM2 命令行界面 (CLI) 可访问 IMM2 而不必使用 Web 界面。它提供了 Web 界面提供的其中一部分管理功能。

您可以通过 Telnet 或 SSH 会话访问 CLI。您必须先经过 IMM2 认证，然后才能发出任何 CLI 命令。

通过 IPMI 管理 IMM2

IMM2 最初将 User ID 1 设置成用户名为 USERID，密码为 PASSWORD（包含数字零而不是字母 O）。此用户具有 Supervisor 访问权。

要点：请在初始配置期间更改此用户名和密码以增强安全性。

在 IBM Flex System 中，用户可以配置 IBM Flex System Chassis Management Module (CMM) 以集中管理 IMM2 智能平台管理接口 (IPMI) 用户帐户。在此情况下，您可能无法使用 IPMI 访问 IMM2，直至 CMM 配置 IPMI 用户标识。CMM 配置的用户标识凭证可能与上述 USERID/PASSWORD 组合不同。

IMM2 还提供以下 IPMI 远程服务器管理能力：

命令行界面

CLI 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『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『使用 IPMITool』。

使用 IPMITool

IPMITool 提供各种可用于管理和配置 IPMI 系统的工具。可以使用频带内或频带外 IPMITool 来管理和配置 IMM2。

有关 IPMITool 的更多信息或要下载 IPMITool，请转至 <http://sourceforge.net/>。

访问命令行界面

要访问 CLI，请启动到 IMM2 IP 地址的 Telnet 或 SSH 会话（请参阅第 148 页的『配置 serial-to-Telnet 或 SSH 重定向』以获取更多信息）。

登录到命令行会话

要登录到命令行，请完成以下步骤：

1. 与 IMM2 建立连接。
2. 在用户名提示符处，输入用户标识。
3. 在密码提示符处，输入用于登录到 IMM2 的密码。

您已登录到命令行。命令行提示符为 `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-Telnet 或 SSH 重定向

通过 Serial-to-Telnet 或 SSH 重定向，系统管理员可以将 IMM2 用作串行终端服务器。当启用了串行重定向时，可以从 Telnet 或 SSH 连接来访问服务器串口。

备注：

1. IMM2 允许打开最多两个 Telnet 会话。Telnet 会话可以独立访问串口，以便多个用户可具有已重定向串口的并发视图。
2. CLI **console 1** 命令用于通过 COM 端口启动串行重定向会话。

示例会话

```
telnet 192.168.70.125 (Press Enter.)
Connecting to 192.168.70.125...
username: USERID (Press Enter.)
password: ***** (Press Enter.)
system> console 1 (Press Enter.)
```

所有来自 COM2 的流量现在都重定向到 Telnet 会话。所有来自 Telnet 或 SSH 会话的流量都路由到 COM2。

ESC (

输入出口键序列以返回到 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 IMM2 CLI。

```
system>
```

命令语法

在开始用命令之前，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。
- 所有自变量都必须紧跟在命令后面。选项紧跟在自变量后面。
- 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）。
- 如果某个选项具有自变量，那么该自变量是必需的，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 是自变量，-i、-g 和 -s 是选项。在此示例中，所有这三个选项都具有自变量。

- 方括号指示自变量或选项是可选的。方括号不属于您输入的命令。

功能和限制

CLI 具有以下功能和限制：

- 通过不同访问方法（Telnet 或 SSH）允许多个并发 CLI 会话。在任何时间，最多可激活两个 Telnet 命令行会话。

注：Telnet 会话数是可配置的；有效值包括 0、1 和 2。值 0 意味着禁用 Telnet 接口。

- 每行允许一个命令（限制为 160 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 Backspace 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，您可将该列表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 IMM2A00096B9E003A
-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。此限制不适用于串行重定向方式（在串行重定向期间会缓冲数据）。
- 在命令完成执行后，命令的输出会显示在屏幕上。这使命令无法报告实时执行状态。例如，在 **flashing** 命令的详细方式下，不会实时显示闪存进度。在命令完成执行后才会显示。
- 使用简单文本消息来表示命令执行状态，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。
- 在选项及其自变量之间至少应有一个空格。例如，`ifconfig eth0 -i192.168.70.133` 是语法错误。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。要查看所用配置支持的命令的列表，请使用 `help` 或 `?` 选项，如下示例中所示：

```
system> help
system> ?
```

- 在 IBM Flex System 中，一些设置由 CMM 管理，而无法在 IMM2 上修改。

按字母顺序排列的命令列表

所有 IMM2 CLI 命令的完整列表（按字母顺序排列）如下：

- 第 163 页的 『accseccfg 命令』
- 第 164 页的 『alertcfg 命令』
- 第 197 页的 『alertentries 命令』
- 第 165 页的 『asu 命令』
- 第 203 页的 『autoftp 命令』
- 第 168 页的 『autopromo 命令』
- 第 168 页的 『backup 命令』
- 第 200 页的 『batch 命令』
- 第 203 页的 『chconfig 命令』
- 第 205 页的 『chlog 命令』
- 第 205 页的 『chmanual 命令』
- 第 201 页的 『clearcfg 命令』
- 第 153 页的 『clearlog 命令』
- 第 201 页的 『clock 命令』
- 第 162 页的 『console 命令』
- 第 169 页的 『cryptomode 命令』
- 第 169 页的 『dhcpinfo 命令』
- 第 170 页的 『dns 命令』
- 第 172 页的 『ethtousb 命令』
- 第 206 页的 『events 命令』
- 第 152 页的 『exit 命令』
- 第 153 页的 『fans 命令』
- 第 153 页的 『ffdc 命令』
- 第 158 页的 『fuelg 命令』
- 第 172 页的 『gprofile 命令』
- 第 152 页的 『help 命令』
- 第 152 页的 『history 命令』
- 第 201 页的 『identify 命令』
- 第 173 页的 『ifconfig 命令』
- 第 202 页的 『info 命令』

- 第 175 页的 『keycfg 命令』
- 第 176 页的 『ldap 命令』
- 第 154 页的 『led 命令』
- 第 177 页的 『ntp 命令』
- 第 178 页的 『passwordcfg 命令』
- 第 179 页的 『ports 命令』
- 第 180 页的 『portcfg 命令』
- 第 180 页的 『portcontrol 命令』
- 第 159 页的 『power 命令』
- 第 161 页的 『pxeboot 命令』
- 第 155 页的 『readlog 命令』
- 第 161 页的 『reset 命令』
- 第 202 页的 『resetsp 命令』
- 第 181 页的 『restore 命令』
- 第 182 页的 『restoredefaults 命令』
- 第 206 页的 『sdemail 命令』
- 第 182 页的 『set 命令』
- 第 182 页的 『smtp 命令』
- 第 183 页的 『snmp 命令』
- 第 185 页的 『snmpalerts 命令』
- 第 202 页的 『spreset 命令』
- 第 186 页的 『srcfg 命令』
- 第 187 页的 『sshcfg 命令』
- 第 188 页的 『ssl 命令』
- 第 189 页的 『sslcfg 命令』
- 第 156 页的 『syshealth 命令』
- 第 191 页的 『telnetcfg 命令』
- 第 157 页的 『temps 命令』
- 第 192 页的 『thermal 命令』
- 第 192 页的 『timeouts 命令』
- 第 192 页的 『tls 命令』
- 第 193 页的 『usbeth 命令』
- 第 193 页的 『users 命令』
- 第 157 页的 『volts 命令』
- 第 158 页的 『vpd 命令』

实用程序命令

实用程序命令如下所示：

- 『exit 命令』
- 『help 命令』
- 『history 命令』

exit 命令

使用 **exit** 命令可注销并结束 CLI 会话。

help 命令

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。您还可以在命令提示符处输入 ?。

history 命令

使用 **history** 命令可显示最近发出的八个命令的带索引历史记录列表。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
-g 0.0.0.0
-s 255.255.255.0
-n IMM2A00096B9E003A
-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

监控命令如下所示：

- 第 153 页的 『clearlog 命令』
- 第 153 页的 『fans 命令』
- 第 153 页的 『ffdc 命令』
- 第 154 页的 『led 命令』
- 第 155 页的 『readlog 命令』
- 第 156 页的 『syshealth 命令』
- 第 157 页的 『temps 命令』
- 第 157 页的 『volts 命令』

- 第 158 页的『vpd 命令』

clearlog 命令

使用 **clearlog** 命令可清除 IMM2 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。

fans 命令

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

使用 **ffdc**（最初故障数据捕获）命令可生成服务数据并将其传送给 IBM 支持人员。

以下列表包含与 **ffdc** 命令配合使用的命令：

- **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

下表显示选项的自变量。

选项	描述	值
-t	类型编号	1（处理器转储）和 4（服务数据）。缺省值为 1。
-f ¹	远程文件名或 sftp 目标目录。	对于 sftp，请对目录名称使用标准路径或尾随“/”（~/ 或 /tmp/）。缺省值是系统生成的名称。
--ip ¹	tftp/sftp 服务器的地址	
-pn ¹	tftp/sftp 服务器的端口号	缺省值为 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 命令的其他自变量		

语法：

```
ffdc [options]
option:
  -t 1 或 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_imm2_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_imm2_120926-105320.tgz
system>
```

led 命令

- 使用 **led** 命令可显示和设置指示灯状态。
- 运行不带任何选项的 **led** 命令会显示前面板指示灯的状态。
 - **led -d** 命令选项必须与 **led -identify on** 命令选项结合使用。

下表显示选项的自变量。

选项	描述	值
-l	获取系统及其子组件上所有指示灯的状态	
-chklog	关闭检查日志指示灯	off
-identify	更改机柜标识指示灯的状态	off、on 和 blink
-d	在指定时间段打开标识指示灯	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

使用 **readlog** 命令可显示 IMM2 事件日志条目，每次 5 条。将按从最新到最旧的顺序显示条目。

readlog 可显示事件日志中的前 5 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 5 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。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 **-I** 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 (缺省值为 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 SERVPROC 12/18/03 10:18:58 Remote Login Successful.  
Login ID: 'USERID' CLI authenticated from 192.168.70.231 (Telnet).'  
2 I SERVPROC 12/18/03 10:12:22 Remote Login successful.  
Login ID: 'USERID' from web browser at IP=192.168.70.231'  
3 E SERVPROC 12/18/03 10:10:37 Failure reading I2C device.  
4 E SERVPROC 12/18/03 10:10:37 Environmental monitor not responding.  
5 E SERVPROC 12/18/03 10:10:37 Failure reading I2C device.  
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

使用 **syshealth** 命令可显示服务器运行状况的摘要。将显示电源状态、系统状态、重新启动计数和 IMM2 软件状态。

示例：

```
system> syshealth
Power On
State System on/starting UEFI
Restarts 71
system>
```

temps 命令

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

示例：

```
system> temps
Temperatures are displayed in degrees Fahrenheit/Celsius
      WR      W      T      SS      HS
-----
CPU1  65/18  72/22  80/27  85/29  90/32
CPU2  58/14  72/22  80/27  85/29  90/32
DASD1 66/19  73/23  82/28  88/31  92/33
Amb   59/15  70/21  83/28  90/32  95/35
system>
```

备注：

- 1. 输出具有以下列标题：
WR：警告重置
W：警告
T：温度（当前值）
SS：软关机
HS：硬关机
- 2. 所有温度值都以华氏度/摄氏度为单位。

volts 命令

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

示例：

```
system> volts
      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：硬关机低
- SSL：软关机低
- WL：警告低
- WRL：警告重置低
- V：电压（当前值）
- WRH：警告重置高

- WH：警告高
- SSH：软关机高
- HSH：硬关机高

vpd 命令

使用 **vpd** 命令可显示系统的重要产品数据 (sys)、IMM2 (imm)、服务器 BIOS (uefi)、服务器 Dynamic System Analysis Preboot (dsa)、服务器固件 (fw) 和服务器组件 (comp)。将显示与 Web 界面中相同的信息。

语法：

```
vpd [options]
option:
  -sys
  -imm
  -uefi
  -dsa
  -fw
  -comp
```

使用 vpd 命令可显示服务器不同部分的重要产品数据。

选项	描述
-sys	显示系统的重要产品数据
-imm	显示 IMM2 控制器的重要产品数据
-uefi	显示 BIOS 的重要产品数据
-dsa	显示 Diag 的重要产品数据
-fw	显示系统固件的重要产品数据
-comp	显示系统组件的重要产品数据

示例：

```
system> vpd -dsa
Type      Version      Build      ReleaseDate
-----
DSA       9,25           DSYTA5A    2012/07/31
system>
```

服务器电源和重新启动控制命令

服务器电源和重新启动命令如下所示：

- 『fuelg 命令』
- 第 159 页的 『power 命令』
- 第 161 页的 『pxeboot 命令』
- 第 161 页的 『reset 命令』

fuelg 命令

使用 **fuelg** 命令可显示和配置服务器电源管理。

使用 **fuelg** 命令可显示有关服务器电源使用情况的信息，并且可配置服务器电源管理。此命令还将针对电源冗余丢失配置策略。下表显示了选项的自变量。

选项	描述	值
-pme	在服务器上启用或禁用电源管理和上限	on 或 off
-pcapmode	为服务器设置功率封顶方式	ac 或 dc
-pcap	对目标运行不带任何选项的 fuelg 命令时显示的功率封顶值范围内的数字值。	数字瓦特值
如果不支持电源冗余，那么将支持以下选项：		
-pm	为冗余电源丢失设置策略方式	基本含调速（缺省）、冗余不含调速或冗余含调速
如果支持电源冗余，那么将支持以下选项：		
-mpc	为服务器设置最大耗电量预算	当前配置或所有热插拔组件
-at	允许调速以将服务器保持在电源预算内	on 或 off
-r	针对服务器允许电源冗余	on 或 off
-nn	N+N 冗余配置的值	冗余配置值

语法：

```
fuelg [options]
option:
  -pme on|off
  -pcapmode dc|ac
  -pcap
  -pm bt|r|rt
  -mpc cc|ahp
  -at on|off
  -r on|off
  -nn
```

示例：

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

power 命令

使用 **power** 命令来控制服务器电源。要发出 **power** 命令，您必须具有 Remote Server Power/Restart Access 权限级别。

下表包含可与 **power** 命令结合使用的一部分命令。

表 7. Power 命令

命令	描述	值
power on	使用此命令可开启服务器电源。	on 或 off
power off	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 或 off

表 7. Power 命令 (续)

命令	描述	值
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）方式。 注：只有当操作系统开启时才能使用此命令。并非在所有服务器上支持 S3 方式。	
power S3resume	使用此命令可将操作系统从 S3（睡眠）方式中唤醒。 注：只有当操作系统开启时才能使用此命令。并非在所有服务器上支持 S3 方式。	
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 或 off

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

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	将此选项与 power on 、 power off 和 power cycle 命令一起使用来控制服务器电源。您可以设置开启服务器、关闭服务器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，将在不同的行上提供此选项的值。 Sun Mon Tue Wed Thu Fri Sat Day clear
-t	使用此选项可指定开启服务器、关闭操作系统以及关闭或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
-rp	使用此选项可指定主机电源复原策略。	alwayson alwaysoff restore
-d	使用此选项可指定开启服务器的日期。这是 power on 命令的另一个选项。 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开启日期。这是 power on 命令的另一个选项。	

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：

```
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：

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

要在每周一 1:30 开启服务器，请输入以下命令：

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

要在 2013 年 12 月 31 日下午 11:30 开启服务器，请输入以下命令：

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

要清除每周关闭再打开电源，请输入以下命令：

```
power cycle -every clear
```

pxeboot 命令

使用 **pxeboot** 命令可显示并设置预引导执行环境的条件。

在无任何选项的情况下运行 **pxeboot** 可返回当前预引导执行环境设置。下表显示了选项的自变量。

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

语法：

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

示例：

```
system> pxeboot
-en disabled
system>
```

reset 命令

使用 **reset** 命令来重新启动服务器。要使用此命令，您必须具有电源和重新启动访问权限。 **-s** 选项先关闭操作系统，然后重新启动服务器。

语法：

reset [选项]

选项：

-s

串行重定向命令

存在一个串行重定向命令：『console 命令』。

console 命令

使用 **console** 命令可启动针对 IMM2 指定串口的串行重定向控制台会话。

语法：

console 1

配置命令

配置命令如下所示：

- 第 163 页的 『accseccfg 命令』
- 第 164 页的 『alertcfg 命令』
- 第 165 页的 『asu 命令』
- 第 168 页的 『autopromo 命令』
- 第 168 页的 『backup 命令』
- 第 169 页的 『cryptomode 命令』
- 第 169 页的 『dhcinfo 命令』
- 第 170 页的 『dns 命令』
- 第 172 页的 『ethtousb 命令』
- 第 172 页的 『gprofile 命令』
- 第 173 页的 『ifconfig 命令』
- 第 175 页的 『keycfg 命令』
- 第 176 页的 『ldap 命令』
- 第 177 页的 『ntp 命令』
- 第 178 页的 『passwordcfg 命令』
- 第 179 页的 『ports 命令』
- 第 180 页的 『portcfg 命令』
- 第 180 页的 『portcontrol 命令』
- 第 181 页的 『restore 命令』
- 第 182 页的 『restoredefaults 命令』
- 第 182 页的 『set 命令』
- 第 182 页的 『smtp 命令』
- 第 183 页的 『snmp 命令』
- 第 185 页的 『snmpalerts 命令』
- 第 186 页的 『srcfg 命令』

- 第 187 页的『sshcfg 命令』
- 第 188 页的『ssl 命令』
- 第 189 页的『sslcfg 命令』
- 第 191 页的『telnetcfg 命令』
- 第 192 页的『thermal 命令』
- 第 192 页的『timeouts 命令』
- 第 192 页的『tls 命令』
- 第 193 页的『usbeth 命令』
- 第 193 页的『users 命令』

accseccfg 命令

使用 **accseccfg** 命令可显示并配置帐户安全性设置。

在无任何选项的情况下运行 **accseccfg** 命令可显示所有帐户安全性信息。下表显示了选项的自变量。

选项	描述	值
-legacy	将帐户安全性设置为预定义的遗留缺省值集	
-high	将帐户安全性设置为预定义的高缺省值集	
-custom	将帐户安全性设置为用户定义的值	
-am	设置用户认证方法	local、ldap、localldap 和 ldaplocal
-lp	登录失败最大次数后的锁定期（分钟）	0、1、2、5、10、15、20、30、60、120、180 或 240 分钟。如果启用了“High Security”，缺省值是 60；如果启用了“Legacy Security”，缺省值是 2。零值将禁用该功能。
-pe	密码到期时间段（天）	0 到 365 天
-pr	需要密码	on 或 off
-pc	密码复杂性规则	on 或 off
-pd	密码中不同字符的最少个数	0 到 19 个字符
-pl	密码长度	1 到 20 个字符
-ci	最短密码更改时间间隔（小时）	0 到 240 小时
-lf	登录失败的最大次数	0 到 10
-chgdf	在首次登录后更改缺省密码	on 或 off
-chgnew	在首次登录后更改新用户密码	on 或 off
-rc	密码重用周期	0 到 5
-wt	Web 不活动会话超时（分钟）	1、5、10、15、20、none 或 user

语法：

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

示例：

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

alertcfg 命令

使用 **alertcfg** 命令可显示并配置 IMM2 全局远程警报参数。

在无任何选项的情况下运行 **alertcfg** 命令可显示所有全局远程警报参数。下表显示了选项的自变量。

选项	描述	值
-dr	设置在 IMM2 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	设置在 IMM2 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，IMM2 额外尝试发送警报的次数	0 到 8

语法：

```
alertcfg [选项]
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

Advanced Settings Utility 命令用于设置 UEFI 设置。必须重新引导主机系统，才能使任何 UEFI 设置更改生效。

下表包含可与 **asu** 命令结合使用的一部分命令。

表 8. ASU 命令

命令	描述	值
delete	使用此命令可删除设置的实例或记录。设置必须是允许删除的实例，例如 iSCSI.AttemptName.1。	<i>setting_instance</i>
help	使用此命令可显示一个或多个设置的帮助信息。	<i>setting</i>
set	使用此命令可更改设置的值。将 UEFI 设置设为输入值。 备注： • 设置一个或多个设置/值对。 • 如果设置扩展为单一设置，那么它可以包含通配符。 • 如果值包含空格，那么必须用引号将其引起来。 • 已排序列表值以等号 (=) 分隔。例如，set B*.Bootorder "CD/DVD Rom=Hard Disk 0=PXE Network"。	<i>setting value</i>
showgroups	使用此命令可显示可用设置组。此命令显示已知组的名称。组名可能根据已安装的设备而异。	<i>setting</i>
show	使用此命令可显示一个或多个设置的当前值。	<i>setting</i>

表 8. ASU 命令 (续)

命令	描述	值
showvalues	使用此命令可显示一个或多个设置的所有可能值。 备注： • 此命令将显示有关设置的允许值的信息。 • 将显示针对设置允许的最小和最大实例数。 • 将显示缺省值（如果可用）。 • 缺省值用左尖括号和右尖括号（< 和 >）括起来。 • 文本值显示最小和最大长度以及正则表达式。	setting
备注： • 在命令语法中，<i>setting</i> 是要查看或更改的设置的名称，<i>value</i> 是赋给该设置的值。 • <i>Setting</i> 可以是多个名称（使用 set 命令时除外）。 • <i>Setting</i> 可以包含通配符，例如星号（*）或问号（?）。 • <i>Setting</i> 可以是组、设置名称或 all。		

以下列表中提供了 **asu** 命令的语法示例：

- 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`。
- 要显示设置的所有可能值，请输入 `asu showvalues setting`。

示例 **show values** 命令：

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

下表显示选项的自变量。

选项	描述	值
-b ¹	以批处理格式显示。	
--help ³	显示命令用法和选项。--help 选项置于命令前，例如 asu --help show 。	
--help ³	显示命令的帮助。--help 选项置于命令后，例如 asu show --help 。	

选项	描述	值
-l ¹	长格式设置名称（包括配置集）。	
-m ¹	混合格式设置名称（使用配置标识）。	
-v ²	详细输出。	
1. -v 选项仅在 asu 和命令之间使用。 2. --help 选项可与任何命令结合使用。		

语法：

```
asu [options] command [cmdopts]
options:
    -v 详细输出
    --help 显示主要帮助
cmdopts:
    --help 命令的帮助
```

注：请参阅个别命令以获取更多命令选项。

使用 **asu** 事务命令以设置多个 UEFI 设置，并创建和执行批处理方式命令。使用 **tropen** 和 **trset** 命令，以创建包含要应用的多个设置的事务文件。使用 **tropen** 命令可打开具有给定标识的事务。使用 **trset** 命令可向集合中添加设置。使用 **trcommit** 命令可落实已完成的事务。完成事务时，可以使用 **trrm** 命令将其删除。

注：UEFI 设置复原操作将使用随机三位数创建具有标识的事务。

下表包含可与 **asu** 命令结合使用的事务命令。

表 9. 事务命令

命令	描述	值
tropen <i>id</i>	此命令创建包含要设置的若干设置的新事务文件。	<i>Id</i> 是标识字符串，1 - 3 个字母数字字符。
trset <i>id</i>	此命令向事务中添加一个或多个设置或值对。	<i>Id</i> 是标识字符串，1 - 3 个字母数字字符。
trlist <i>id</i>	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，这会很有用。	<i>Id</i> 是标识字符串，1 - 3 个字母数字字符。
trcommit <i>id</i>	此命令落实并执行事务文件的内容。将显示执行结果和任何错误。	<i>Id</i> 是标识字符串，1 - 3 个字母数字字符。
trrm <i>id</i>	此命令会在事务文件落实后将其除去。	<i>Id</i> 是标识字符串，1 - 3 个字母数字字符。

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
```

autopromo 命令

使用 **autopromo** 命令显示和配置用于自动升级 IMM2 备份固件的设置。如果已启用自动升级功能，那么当 IMM2 固件在主区域中成功运行一段时间之后，自动升级功能会自动将该固件从主区域复制到备份区域中。

运行不带任何选项的 **autopromo** 命令可显示自动升级参数和状态信息。下表显示了选项的自变量。

选项	描述	值
-en	对 IMM2 备份固件启用或禁用自动升级。	enabled、disabled

语法：

```
autopromo [options]
options:
    -en enabled/disabled
```

示例：

```
system>autopromo -en enabled
ok
system>autopromo
-en: enabled
Status: Not Synced
Primary bank version: 4.00
Backup bank version: 2.60
```

backup 命令

使用 **backup** 命令可生成包含当前系统安全性设置的备份文件。

下表显示了选项的自变量。

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	有效密码或以引号定界的口令
-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（缺省值为 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 imm-back.cli -pp xxxxxx -ip 192.168.70.200
ok
system>
```

cryptomode 命令

使用 **cryptomode** 命令显示和配置存在加密异常的合规性方式。下表显示了选项的自变量。

选项	描述	值
-set	选择合规性方式	basic、NIST
-esnmpv3	通过 NIST 合规性方式，允许或禁止 SNMPv3 帐户以非合规方式操作	enable 或 disable
-h	列出用法和选项	

语法：

```
cryptomode [options]
options:
  -set basic|nist
  -esnmpv3 enabled|disabled
  -h usage_options
```

示例：

```
system> cryptomode
Basic Compatibility
system>
```

dhcpinfo 命令

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
```

示例：

```
system> dhcpinfo eth0

-server : 192.168.70.29
-n      : IMM2A-00096B9E003A
-i      : 192.168.70.202
-g      : 192.168.70.29
-s      : 255.255.255.0
```

```
-d      : linux-sp.raleigh.ibm.com
-dns1   : 192.168.70.29
-dns2   : 0.0.0.0
-dns3   : 0.0.0.0
-i6     : 0::0
-d6     : *
-dns61  : 0::0
-dns62  : 0::0
-dns63  : 0::0
system>
```

下表描述了该示例的输出。

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
-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 **dns** 命令可查看并设置 IMM2 的 DNS 配置。

注：在 IBM Flex System 中，无法在 IMM2 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** 命令可显示所有 DNS 配置信息。下表显示了选项的自变量。

选项	描述	值
-state	DNS 状态	on 或 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。

选项	描述	值
-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：以下示例显示了启用 DNS 的 IMM2 配置。

示例：

```
system> dns
-state : enabled
-i1    : 192.168.70.202
-i2    : 192.168.70.208
-i3    : 192.168.70.212
-i61   : fe80::21a:64ff:fee6:4d5
-i62   : fe80::21a:64ff:fee6:4d6
-i63   : fe80::21a:64ff:fee6:4d7
-ddns  : enabled
-ddn   : ibm.com
-ddncur : ibm.com
-dnsrc : dhcp
-p     : ipv6
system>
```

下表描述了该示例的输出。

选项	描述
-state	DNS 的状态 (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 的状态 (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)

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** 命令可显示 Ethernet-over-USB 信息。下表显示了选项的自变量。

选项	描述	值
-en	Ethernet-over-USB 状态	enabled、disabled
-mx	配置索引 <i>x</i> 的端口映射	以冒号 (:) 分隔的端口对，格式为 <i>port1:port2</i> 其中： - 端口索引号 <i>x</i> 在命令选项中指定为 1 到 10 之间的整数。 - 端口对的 <i>port1</i> 是外部以太网端口号。 - 端口对的 <i>port2</i> 是 Ethernet-over-USB 端口号。
-rm	除去指定索引的端口映射	1 到 10 通过在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
  -mx port_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>
```

gprofile 命令

使用 **gprofile** 命令来显示和配置 IMM2 的组概要文件。

下表显示了选项的自变量。

选项	描述	值
-clear	删除组	enabled、disabled
-n	组的名称	对于 <i>group_name</i> ，最多为 63 个字符的字符串。 <i>group_name</i> 必须唯一。
-a	基于角色的权限级别	supervisor、operator、rbs <role list>: nslclamrlcalrcvmaipribclcellac 使用竖线分隔的值列表来指定角色列表值。

选项	描述	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
```

ifconfig 命令

使用 **ifconfig** 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，后跟值。要更改接口配置，您至少应具有 Adapter Networking and Security Configuration 权限。

下表显示了选项的自变量。

选项	描述	值
-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	数据率	10、100 和 auto
-d	双工方式	full、half 和 auto
-m	MTU	60 和 1500 之间的数字
-l	LAA	MAC 地址格式。不允许多点广播地址 (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，可确定 Data Rate 和 Duplex 网络设置是否可配置。	true 和 false
-nic	NIC 访问	shared 或 dedicated

选项	描述	值
-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。	此值是只读的，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 IMM2 确定。此值是只读的，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 之间的数字值
-g6	网关或缺省路径	以太网通道 0 的网关或缺省路径的 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	IMM2 的网络包标识标记	1 到 4094 之间的数字值

语法：

```
ifconfig eth0 [options]
```

选项：

```
-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
-dn domain_name
-auto state
-nic state
-address_table
-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
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n IMM2A00096B9E003A
-r auto
```

```
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system> ifconfig eth0 -c static -i 192.168.70.133
These configuration changes will become active after the next reset of the IMM2.
system>
```

注：ifconfig 显示中的 **-b** 选项用于烧录 MAC 地址。烧录 MAC 地址是只读的，不可配置。

keycfg 命令

使用 **keycfg** 命令可显示、添加或删除激活密钥。这些密钥控制对可选 IMM2 Features on Demand (FoD) 功能部件的访问。

- 运行不带任何选项的 **keycfg** 时，将会显示已安装的激活密钥的列表。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、密钥的有效日期、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。

下表显示选项的自变量。

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（缺省值 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 ip_address
    -pn port_number
    -u username
```

```

        -pw password
        -f filename
    -del key_index
    -deltype key_type

```

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"
system>

```

Idap 命令

使用 **Idap** 命令可显示并配置 LDAP 协议配置参数。

下表显示了选项的自变量。

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	仅认证方式	enabled、disabled
-b	绑定方法	anonymous、bind with ClientDN and password 和 bind with Login Credential
-c	客户机专有名称	针对 <i>client_dn</i> 的字符串，最多包含 127 个字符
-d	搜索域	针对 <i>search_domain</i> 的字符串，最多包含 63 个字符
-f	组过滤器	针对 <i>group_filter</i> 的字符串，最多包含 127 个字符
-fn	森林名称	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 <i>group_search_attr</i> 的字符串，最多包含 63 个字符
-l	登录许可权属性	针对 <i>string</i> 的字符串，最多包含 63 个字符
-p	客户机密码	针对 <i>client_pw</i> 的字符串，最多包含 15 个字符
-pc	确认客户机密码	针对 <i>confirm_pw</i> 的字符串，最多包含 15 个字符 命令用法为：ldap -p <i>client_pw</i> -pc <i>confirm_pw</i> 当您更改客户机密码时，此选项是必需的。该选项将 <i>confirm_pw</i> 参数与 <i>client_pw</i> 参数进行比较。如果这两个参数不匹配，该命令将失败。
-r	根条目专有名称 (DN)	针对 <i>root_dn</i> 的字符串，最多包含 127 个字符
-rbs	Active Directory 用户的增强型基于角色的安全性	enabled、disabled
-s1ip	服务器 1 主机名/IP 地址	针对 <i>host name/ip_addr</i> 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 <i>host name/ip_addr</i> 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 <i>host name/ip_addr</i> 的字符串，最多包含 127 个字符

选项	描述	值
-s4ip	服务器 4 主机名/IP 地址	针对 <i>host_name/ip_addr</i> 的字符串，最多包含 127 个字符
-s1pn	服务器 1 端口号	针对 <i>port_number</i> 的数字端口号，最多包含 5 位数
-s2pn	服务器 2 端口号	针对 <i>port_number</i> 的数字端口号，最多包含 5 位数
-s3pn	服务器 3 端口号	针对 <i>port_number</i> 的数字端口号，最多包含 5 位数
-s4pn	服务器 4 端口号	针对 <i>port_number</i> 的数字端口号，最多包含 5 位数
-t	服务器目标名称	启用 -rbs 选项时，此字段指定可通过 Role-Based Based Security (RBS) Snap-In 工具与 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 <i>search_attr</i> 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]
选项：
-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
-r root_dn
-rbs enable|disabled
-slip 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_attr
-v off/on
-h
```

ntp 命令

使用 **ntp** 命令可显示并配置网络时间协议 (NTP)。

下表显示了选项的自变量。

选项	描述	值
-en	启用或禁用网络时间协议	enabled、disabled

选项	描述	值
-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	IMM2 时钟与网络时间协议服务器同步的频率（以分钟为单位）	3 分钟到 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
```

passwordcfg 命令

使用 **passwordcfg** 命令可显示并配置密码参数。

选项	描述
-legacy	将帐户安全性设置为预定义的遗留缺省值集
-high	将帐户安全性设置为预定义的高缺省值集
-exp	最长密码寿命（0 到 365 天）。设置为 0 表示不会过期。
-cnt	在使用多少个不同的密码后才能复用先前的密码（0 到 5）
-nul	允许帐户无密码（yes no）
-h	显示命令用法和选项

语法：

```
passwordcfg [options]
options: {-high}|{-legacy}|{-exp|-cnt|-nul}
-legacy
-high
-exp:
-cnt:
-nul:
-h
```

示例：

```
system> passwordcfg
Security Level: Legacy
system> passwordcfg -exp 365
ok
```

```
system> passwordcfg -nul yes
ok
system> passwordcfg -cnt 5
ok
system> passwordcfg
Security Level: Customize
-exp: 365
-cnt: 5
-nul: allowed
```

ports 命令

使用 **ports** 命令可显示和配置 IMM2 端口。

运行不带任何选项的 **ports** 命令会显示所有 IMM2 端口的信息。下表显示选项的自变量。

选项	描述	值
-open	显示打开的端口	
-reset	将端口重置为缺省设置	
-http	HTTP 端口号	缺省端口号：80
-https	HTTPS 端口号	缺省端口号：443
-telnet	Telnet 遗留 CLI 端口号	缺省端口号：23
-ssh	SSH 遗留 CLI 端口号	缺省端口号：22
-snmp	SNMP 代理端口号	缺省端口号：161
-snmptrap	SNMP 陷阱端口号	缺省端口号：162
-rpp	远程感知端口号	缺省端口号：3900
-cimhttp	CIM over HTTP 端口号	缺省端口号：5988
-cimhttps	CIM over HTTPS 端口号	缺省端口号：5989

语法：

```
ports [options]
option:
  -open
  -reset
  -http port_number
  -https port_number
  -telnet port_number
  -ssh port_number
  -snmp port_number
  -snmptrap port_number
  -rpp port_number
  -cimhttp port_number
  -cimhttps port_number
```

示例：

```
system> ports
-http 80
-https 443
-rpp 3900
-snmp 161
-snmptrap 162
-ssh 22
```

```
-telnetp 23
-cimhp 5988
-cimhsp 5989
system>
```

portcfg 命令

使用 **portcfg** 命令可针对串行重定向功能配置 IMM2。

必须将 IMM2 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，后跟值。要更改串口配置，您至少应具有 Adapter Networking and Security Configuration 权限。

注：服务器外部串口只能由 IMM2 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** 命令可显示串口配置。下表显示了选项的自变量。

注：数据位数 (8) 是在硬件中设置的，不能更改。

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

语法：

portcfg [*options*]

选项：

```
-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 **portcontrol** 命令开启或关闭网络服务端口。

当前该命令仅对 IPMI 协议支持端口控制。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** 选项后跟 **on** 或 **off** 值。

选项	描述	值
-ipmi	启用或禁用 ipmi 服务器 623 端口	on 或 off
-h		

语法：

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

示例：

```
system> portcontrol
-ipmi : on
system>
```

restore 命令

使用 **restore** 命令从备份文件中恢复系统设置。

下表显示了选项的自变量。

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	有效密码或以引号定界的口令
-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（缺省值为 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 imm-back.cli -pp xxxxxx -ip 192.168.70.200
ok
system>
```

restoredefaults 命令

使用 **restoredefaults** 命令可将所有 IMM2 设置恢复为出厂缺省值。

- **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...

set 命令

使用 **set** 命令可更改 IMM2 设置。

- 可以使用简单的 **set** 命令来更改某些 IMM2 设置。
- 其中一些设置（例如，环境变量）由 CLI 使用。

下表显示了选项的自变量。

选项	描述	值
<i>value</i>	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 **smtp** 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** 命令可显示所有 SMTP 接口信息。下表显示了选项的自变量。

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

选项	描述	值
-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
  -authpw 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 **snmp** 命令可显示和配置 SNMP 接口信息。

运行不带任何选项的 **snmp** 命令会显示所有 SNMP 接口信息。下表显示选项的自变量。

选项	描述	值
-a	SNMPv1 代理	on 和 off 注：要启用 SNMPv1 代理，必须满足以下条件： - 使用 -cn 命令选项指定 IMM2 联系人。 - 使用 -l 命令选项指定 IMM2 位置。 - 使用 -cx 命令选项之一指定至少一个 SNMP 社区名称。 - 使用 -xiy 命令选项之一为每个 SNMP 社区指定至少一个有效 IP 地址。
-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 IMM2 联系人。 - 使用 -l 命令选项指定 IMM2 位置。
-t	SNMP 陷阱	on 和 off
-l	IMM2 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。 - 通过不指定任何自变量或者指定空字符串作为自变量（如 ""）来清除 IMM2 位置。

选项	描述	值
-cn	IMM2 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。 - 通过不指定任何自变量或者指定空字符串作为自变量（如 ""）来清除 IMM2 联系人姓名。
-cx	SNMP 社区 <i>x</i> 名称	字符串（限制为 15 个字符）。 注： - 在命令选项中，<i>x</i> 指定为 1、2 或 3，以指示社区号。 - 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。 - 通过不指定任何自变量或者指定空字符串作为自变量（如 ""）来清除 SNMP 社区名称。
-cxiy	SNMP 社区 <i>x</i> IP 地址或主机名 <i>y</i>	有效 IP 地址或主机名（限制为 63 个字符）。 注： - 在命令选项中，<i>x</i> 指定为 1、2 或 3，以指示社区号。 - 在命令选项中，<i>y</i> 指定为 1、2 或 3，以指示 IP 地址或主机名编号。 - 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。 - 通过不指定任何自变量来清除 SNMP 社区 IP 地址或主机名。
-cax	SNMPv3 社区 <i>x</i> 访问类型	get、set 和 trap 注：在命令选项中， <i>x</i> 指定为 1、2 或 3，以指示社区号。

语法：

```
snmp [options]
option:
  -a state
  -a3 state
  -t state
  -l location
  -cn contact_name
  -c1 snmp_community_1_name
  -c2 snmp_community_2_name
  -c3 snmp_community_3_name
  -cli1 community_1_ip_address_or_hostname_1
  -cli2 community_1_ip_address_or_hostname_2
  -cli3 community_1_ip_address_or_hostname_3
  -c2i1 community_2_ip_address_or_hostname_1
  -c2i2 community_2_ip_address_or_hostname_2
  -c2i3 community_2_ip_address_or_hostname_3
  -c3i1 community_3_ip_address_or_hostname_1
  -c3i2 community_3_ip_address_or_hostname_2
  -c3i3 community_3_ip_address_or_hostname_3
  -ca1 community_1_access_type
  -ca2 community_2_access_type
  -ca3 community_3_access_type
```

示例：

```
system> snmp
-a Enabled
-a3 Enabled
-t Enabled
-l RTC,NC
-cn Snmp Test
-cl public
-cl1 192.44.146.244
-cl2 192.44.146.181
-cl3 192.44.143.16
-ca1 set
-ch1 specific
-c2 private
-c2i1 192.42.236.4
-c2i2
-c2i3
-ca2 get
-ch2 specific
-c3
-c3i1
-c3i2
-c3i3
-ca3 get
-ch3 ipv4only
system>
```

snmpalerts 命令

使用 **snmpalerts** 命令可管理通过 SNMP 发送的警报。

运行不带任何选项的 **snmpalerts** 会显示所有 SNMP 警报设置。下表显示选项的自变量。

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 和 custom:telvolpoldilfalcplmelinlrelot 定制紧急警报设置使用格式为 snmpalerts -crt custom:telvo 的管道符分隔的值列表指定，其中 custom 值为： - te：超过了临界温度阈值 - vo：超过了临界电压阈值 - po：紧急电源故障 - di：硬盘驱动器故障 - 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

选项	描述	值
-wrn	设置发送警报的警告事件	all、none 和 custom:rpltelvolpolfalcpmlot 定制警告警报设置使用格式为 snmpalerts -wrn custom:rplte 的管道符分隔的值列表指定，其中 custom 值为： • rp：电源冗余警告 • te：超过了警告温度阈值 • vo：超过了警告电压阈值 • po：超过了警告电源阈值 • fa：非紧急风扇事件 • cp：微处理器处于已降级状态 • 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	设置发送警报的例行事件	all、none 和 custom:loltiolotlpolbftillpfellne 定制例行警报设置使用格式为 snmpalerts -sys custom:loltio 的管道符分隔的值列表指定，其中 custom 值为： • lo：成功远程登录 • tio：操作系统超时 • ot：所有其他参考事件和系统事件 • po：系统开机/关机 • 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：预测性故障（PFA） • el：事件日志 75% 已满 • ne：网络更改
-sysen	发送例行事件警报	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 **srcfg** 命令可指示用于通过串行重定向方式进入 CLI 的键序列。要更改串行重定向配置，请输入选项，后跟值。要更改串行重定向配置，您至少应具有 Adapter Networking and Security Configuration 权限。

注：IMM2 硬件未提供串口-串口通过功能。因此，在 Remote Supervisor Adapter II CLI 中出现的 -passthru 和 entercliseq 选项不受支持。

在无任何选项的情况下运行 **srcfg** 命令可显示当前串行重定向击键序列。下表显示了 srcfg -entercliseq 命令选项的参数。

选项	描述	值
-entercliseq	进入 CLI 击键序列	用户定义的用于进入 CLI 的击键序列。 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。它代表映射为 Ctrl 序列的击键中的 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。此字段的缺省值是“^[_”，即 Esc 后跟 (。

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

```
示例：
system> srcfg
-entercliseq ^[_Q
system>
```

sshcfg 命令

使用 **sshcfg** 命令可显示并配置 SSH 参数。

在无任何选项的情况下运行 **sshcfg** 命令可显示所有 SSH 参数。下表显示了选项的自变量。

选项	描述	值
-cstatus	SSH CLI 的状态	enabled、disabled
-hk gen	生成 SSH 服务器专用密钥	
-hk rsa	显示服务器 RSA 公用密钥	

```
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 **ssl** 命令可显示并配置 SSL 参数。

注：必须先安装客户机证书，然后才能启用 SSL 客户机。

在无任何选项的情况下运行 **ssl** 命令可显示 SSL 参数。下表显示了选项的自变量。

选项	描述	值
-ce	启用或禁用 SSL 客户机	on 或 off
-se	启用或禁用 SSL 服务器	on 或 off
-cime	在 SSL 服务器上启用或禁用 CIM over HTTPS	on 或 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 **sslcfg** 命令可显示并配置 IMM2 的 SSL，并管理证书。

在无任何选项的情况下运行 **sslcfg** 命令可显示所有 SSL 配置信息。下表显示了选项的自变量。

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 客户机状态	enabled、disabled 注：仅当安装了有效的服务器或客户机证书时，才能启用 SSL 客户机。
-cim	CIM over HTTPS 状态	enabled、disabled 注：仅当安装了有效的服务器或客户机证书时，才能启用 CIM over HTTPS。
-cert	生成自签名证书	server、client 或 sysdir 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。
-csr	生成 CSR	server、client 或 sysdir 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：当上载证书时，或者下载证书或 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（缺省值为 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：当下载或者上载证书或 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缺省名称。

选项	描述	值
-dnld	下载证书文件	此选项不带自变量；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）。此选项不带自变量；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	此选项不带自变量；但是，也必须为 -cert 、 -i 和 -l 命令选项指定值。
-tcx	SSL 客户机的可信证书 <i>x</i>	import、download 或 remove 注：可信证书号 <i>x</i> 在命令选项中指定为 1 到 3 之间的整数。
-c	Country	国家或地区代码（2 个字母） 注：生成自签名证书或 CSR 时必选。
-sp	省/自治区/直辖市	引号定界的字符串（最多 60 个字符） 注：生成自签名证书或 CSR 时必选。
-cl	市/县/区或地点	引号定界的字符串（最多 50 个字符） 注：生成自签名证书或 CSR 时必选。
-on	组织机构名称	引号定界的字符串（最多 60 个字符） 注：生成自签名证书或 CSR 时必选。
-hn	IMM2 主机名	字符串（最多 60 个字符） 注：生成自签名证书或 CSR 时必选。
-cp	联系人	引号定界的字符串（最多 60 个字符） 注：生成自签名证书或 CSR 时可选。
-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。
-ou	组织机构单位	引号定界的字符串（最多 60 个字符） 注：生成自签名证书或 CSR 时可选。
-s	Surname	引号定界的字符串（最多 60 个字符） 注：生成自签名证书或 CSR 时可选。
-gn	指定名字	引号定界的字符串（最多 60 个字符） 注：生成自签名证书或 CSR 时可选。
-in	Initials	引号定界的字符串（最多 20 个字符） 注：生成自签名证书或 CSR 时可选。
-dq	域名限定词	引号定界的字符串（最多 60 个字符） 注：生成自签名证书或 CSR 时可选。
-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。
-un	非结构化名称	引号定界的字符串（最多 60 个字符） 注：生成 CSR 时可选。

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
-tcx action
-c country_code
-sp state_or_province
-cl city_or_locality
-on organization_name
-hn imm_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
system>
```

telnetcfg 命令

使用 **telnetcfg** 命令可显示并配置 Telnet 设置。

在无任何选项的情况下运行 **telnetcfg** 命令可显示 Telnet 状态。下表显示了选项的自变量。

选项	描述	值
-en	Telnet 状态	disabled、1 或 2 注：如果未禁用，Telnet 将针对一个或两个用户启用。

语法：

```
0telnetcfg [选项]
option:
  -en state
```

示例：

```
system> telnetcfg
-en 1
system>
```

tls 命令

使用 **tls** 命令可设置最小 TLS 级别。下表显示了选项的自变量。

选项	描述	值
-min	选择最小 TLS 级别	1.0、1.1 或 1.2
-h	列出用法和选项	

语法：

```
tls [options]
option:
  -min 1.0|1.1|1.2
```

示例：

```
system> tls
-min 1.0
system>
```

thermal 命令

使用 **thermal** 命令可显示并配置主机系统的温度方式策略。

在任何选项的情况下运行 **thermal** 命令可显示温度方式策略。下表显示了选项的自变量。

选项	描述	值
-mode	温度方式选择	normal 或 performance

语法：

```
thermal [options]
option:
  -mode thermal_mode
```

示例：

```
system> thermal
-mode normal
system>
```

timeouts 命令

使用 **timeouts** 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，后跟值。要更改超时值，您至少应具有适配器配置权限。

下表显示了超时值的自变量。这些值与 Web 界面上服务器超时的分度标下拉选项匹配。

选项	超时	单位	值
-f	断电延迟	分钟	disabled、0.5、1、2、3、4、5、7.5、10、15、20、30、60 或 120

选项	超时	单位	值
-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
-o	操作系统超时	分钟	disabled、2.5、3、3.5 和 4

语法：

```
timeouts [options]
options:
-f power_off_delay_watchdog_option
-o OS_watchdog_option
-l loader_watchdog_option
```

示例：

```
system> timeouts
-o disabled
-l 3.5
system> timeouts -o 2.5
ok
system> timeouts
-o 2.5
-l 3.5
```

usbeth 命令

使用 **usbeth** 命令可启用或禁用频带内 LAN over USB 接口。

语法：

```
usbeth [options]
选项：
-en <enabled|disabled>
```

示例：

```
system>usbeth
-en : disabled
system>usbeth -en enabled
ok
system>usbeth
-en : disabled
```

users 命令

使用 **users** 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** 命令可显示用户的列表和某些基本用户信息。下表显示了选项的自变量。

选项	描述	值
-user_index	用户帐户索引号	1 到 12 (包括) 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。

选项	描述	值
-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，用户必须在其首次登录时设置密码。
-a	用户权限级别	super、ro 或 custom 其中： • super（超级） • ro（只读） • custom 后跟冒号和由竖线 () 分隔的值列表，格式为：custom:am rca。可以任意组合使用这些值。 am（用户帐户管理访问） rca（远程控制台访问） rcvma（远程控制台和虚拟介质访问） 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 and 安全性） ac（适配器配置 - 高级）
-ep	加密密码（用于备份/恢复）	有效密码
-clear	擦除指定的用户帐户	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-MD5、HMAC-SHA 或 none
-spriv	SNMPv3 隐私协议	CBC-DES、AES 或 none
-spw	SNMPv3 隐私密码	有效密码
-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 公用密钥	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。 • 当使用 SSH 公用密钥选项时，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。

选项	描述	值
-e	以 OpenSSH 格式显示整个 SSH 密钥 (SSH 公用密钥选项)	此选项不带有自变量，并且必须与所有其他 users -pk 选项按独占方式使用。 注：当使用 SSH 公用密钥选项时，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 公用密钥选项)	必须将要除去的公用密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：当使用 SSH 公用密钥选项时，必须在用户索引 (-userindex 选项) 后使用 -pk 选项，格式为：users -2 -pk -remove -1。
-add	为用户添加 SSH 公用密钥 (SSH 公用密钥选项)	以引号定界的密钥，采用 OpenSSH 格式 注： -add 选项与所有其他 users -pk 命令选项按独占方式使用。 - 当使用 SSH 公用密钥选项时，必须在用户索引 (-userindex 选项) 后使用 -pk 选项，格式为： <pre>users -2 -pk -add "AAAAB3NzC1yc2EAAAABIwAAAQEA vfnTUzRF7pdBuaBy4d0/aIFasa/Gtc+o/wlZnuC4aD HMA1UmnMyLOciIaN0y400ICEKcjqKEhrYymtAoVtFKApv Y39GpnSGRC/qcLGWLM4cmirKL5kxHNOqIcwbT1NPceoKH j46X7E+mqlfWnAhhjDpcVFjagM3Ek2y7w/tBGrwGgN7DP HJU1tzCjy68mEAnIrzjUoR98Q3/B9cJD77ydGKe8rPdI2 hIEpXR5dNUiupA1Yd8PSSMgdukASKEd3eRRZTB13SA tMucUsTkYjlXcqex10Qz4+N50R6MbNcwlsx+mTEAvvc pJhuga70UNPghLJM16k7jeJiQ8Xd2p Xb0ZQ=="</pre>
-upld	上载 SSH 公用密钥 (SSH 公用密钥选项)	需要 -i 和 -l 选项来指定密钥位置。 注： -upld 选项与所有其他 users -pk 命令选项按独占方式使用 (-i 和 -l 除外)。 - 要将一个密钥替换为新密钥，必须指定 -key_index。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。 - 当使用 SSH 公用密钥选项时，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。
-dnld	下载指定的 SSH 公用密钥 (SSH 公用密钥选项)	需要 -key_index 来指定要下载的密钥，并且需要 -i 和 -l 选项来指定在运行 TFTP 服务器的其他计算机上的下载位置。 注： -dnld 选项与所有其他 users -pk 命令选项按独占方式使用 (-i、-l 和 -key_index 除外)。 - 当使用 SSH 公用密钥选项时，必须在用户索引 (-userindex 选项) 后使用 -pk 选项，格式为：users -2 -pk -dnld -l -i tftp://9.72.216.40/ -l file.key。

选项	描述	值
-i	用于上载或下载密钥文件的 TFTP/SFTP 服务器的 IP 地址。 (SSH 公用密钥选项)	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 公用密钥选项)	有效端口号（缺省值为 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 公用密钥选项)	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 公用密钥选项)	有效密码 注：users -pk -upld 和 users -pk -dnld 命令选项的可选参数。
-l	用于通过 TFTP 或 SFTP 上载或下载密钥文件的文件名 (SSH 公用密钥选项)	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 公用密钥选项)	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 公用密钥选项)	以引号定界的字符串，最多 255 个字符。 注：当使用 SSH 公用密钥选项时，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*]

选项：

```

-user_index
-n username
-p password
-a authority_level
-ep encryption_password
-clear
-curr
-sauth protocol
-spriv protocol
-spw password
-sepw password
-sacc state
-strap hostname

```

users -pk [*选项*]

选项：

```

-e
-remove index
-add key
-upld
-dnld
-i ip_address
-pn port_number
-u username

```

```
-pw password
-l filename
-af list
-cm comment
```

示例：

```
system> users
1. USERID Read/Write
Password Expires: no expiration
2. manu Read Only
Password Expires: no expiration
3. eliflippen Read Only
Password Expires: no expiration
4. <not used>
5. jacobyackenovic custom:cel|ac
Password Expires: no expiration
system> users -7 -n sptest -p PASSWORD -a custom:am|rca|cel|nsc|ac
ok
system> users
1. USERID Read/Write
Password Expires: no expiration
2. test Read/Write
Password Expires: no expiration
3. test2 Read/Write
Password Expires: no expiration
4. <not used>
5. jacobyackenovic custom:cel|ac
Password Expires: no expiration
6. <not used>
7. sptest custom:am|rca|cel|nsc|ac
Password Expires: no expiration
8. <not used>
9. <not used>
10. <not used>
11. <not used>
12. <not used>
system>
```

IMM2 控制命令

IMM2 控制命令如下：

- 『alertentries 命令』
- 第 200 页的 『batch 命令』
- 第 201 页的 『clearcfg 命令』
- 第 201 页的 『clock 命令』
- 第 201 页的 『identify 命令』
- 第 202 页的 『info 命令』
- 第 202 页的 『resetsp 命令』
- 第 202 页的 『spreset 命令』

alertentries 命令

使用 **alertentries** 命令可管理警报接收方。

- 不带有任何选项的 **alertentries** 可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。

下表显示了选项的自变量。

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 或 off
-type	报警类型	email 或 syslog
-log	在警报电子邮件中包括事件日志	on 或 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:telvolpoldilfalcpmlinlrelot 定制紧急警报设置是通过使用以竖线分隔的值列表来指定的，格式为： alertentries -crt custom:telvo ，其中定制值包括： • te：超过临界温度阈值 • vo：超过临界电压阈值 • po：关键电源故障 • di：硬盘驱动器故障 • 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

选项	描述	值
-wrn	设置发送警报的警告事件	all、none、custom:rpitelvolpolfalcpmlmelot 定制警告警报设置是通过使用以竖线分隔的值列表来指定的，格式为： alertentries -wrn custom:rpitel ，其中定制值包括： • 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：超过警告电源阈值 • 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:loltiolotlpolbftilpfllelne 定制常规警报设置是通过使用以竖线分隔的值列表来指定的，格式为： alertentries -sys custom:loltio ，其中定制值包括： • lo：成功的远程登录 • tio：操作系统超时 • ot：所有其他信息和系统事件 • po：系统供电/断电 • 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：预测的故障（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 -l
-status off
-log off
-n test
-e test@mytest.com
-crt all
-wrn all
-sys none
system>
```

batch 命令

使用 **batch** 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。

下表显示了选项的自变量。

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（缺省值为 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 **clearcfg** 命令可将 IMM2 配置设置为其出厂缺省值。您至少应具有高级适配器配置权限才能发出此命令。在清除 IMM2 的配置后，IMM2 将重新启动。

clock 命令

使用 **clock** 命令可根据 IMM2 时钟和 GMT 偏移量显示当前日期和时间。您可以设置日期、时间、GMT 偏移量和夏令时设置。

请注意以下信息：

- 如果 GMT 偏移量为 +2、-7、-6、-5、-4 或 -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）、mik（明斯克）、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）、moo（蒙得维的亚）和 bre（巴西-东部）。
- 年份必须为 2000 到 2089（包括 2000 和 2089）。
- 月份、日期、小时、分钟和秒钟可以是单位数值（例如，9:50:25 可代替 09:50:25）。
- GMT 偏移量可以采用 +2:00、+2 或 2 格式表示正偏移量，采用 -5:00 或 -5 格式表示负偏移量。

语法：

```
clock [options]
选项：
-d mm/dd/yyyy
-t hh:mm:ss
-g gmt offset
-dst on/off/special case
```

示例：

```
system> clock
12/12/2011 13:15:23 GMT-5:00 dst on
system> clock -d 12/31/2011
ok
system> clock
12/31/2011 13:15:30 GMT-5:00 dst on
```

identify 命令

使用 **identify** 命令可使机箱识别指示灯点亮或熄灭，或使其闪烁。-d 选项可与 -s on 配合使用，使指示灯仅在以 -d 参数指定的秒数内点亮。在经过该秒数后，指示灯将熄灭。

语法：

```
identify [options]
选项：
-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 **info** 命令可显示和配置有关 IMM2 的信息。

运行不带任何选项的 **info** 命令会显示所有 IMM2 位置和联系人信息。下表显示选项的自变量。

选项	描述	值
-name	IMM2 名称	字符串
-contact	IMM2 联系人的姓名	字符串
-location	IMM2 位置	字符串
-room ¹	IMM2 槽标识	字符串
-rack ¹	IMM2 机架标识	字符串
-rup ¹	IMM2 在机架中的位置	字符串
-ruh	机架单元高度	只读
-bbay	刀片托架位置	只读
1. 如果 IMM2 驻留在 IBM Flex System 中，那么值为只读且无法重置。		

语法：

```
info [options]
option:
-name imm_name
-contact contact_name
-location imm_location
-room room_id
-rack rack_id
-rup rack_unit_position
-ruh rack_unit_height
-bbay blade_bay
```

resetsp 命令

使用 **resetsp** 命令可重新启动 IMM2。您至少应具有高级适配器配置权限才能发出此命令。

spreset 命令

使用 **spreset** 命令可重新启动 IMM2。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

Service Advisor 命令如下：

- 『autoftp 命令』
- 『chconfig 命令』
- 第 205 页的 『chlog 命令』
- 第 205 页的 『chmanual 命令』
- 第 206 页的 『events 命令』
- 第 206 页的 『sdemail 命令』

autoftp 命令

使用 **autoftp** 命令显示和配置 IMM2 的 FTP/TFTP/SFTP 服务器设置。服务器将不发送重复事件（如果这些事件在活动日志中保留为未确认）。

下表显示了选项的自变量。

选项	描述	值
-m	自动化问题报告方式	ftp、sftp、tftp、disabled 备注： • 对于 ftp 方式，必须设置所有字段。 • 对于 tftp 方式，只需要 -i 和 -p 选项。
-i	自动化问题报告的 FTP、SFTP 或 TFTP 服务器 IP 地址或主机名	有效的 IP 地址或主机名
-p	自动化问题报告的 FTP、SFTP 或 TFTP 传输端口	有效端口号（1 到 65535）
-u	自动化问题报告的 FTP、SFTP 或 TFTP 用户名	引号定界的字符串（最多 63 个字符）
-pw	自动化问题报告的 FTP 密码	引号定界的字符串（最多 63 个字符）

语法：

```
autoftp [options]
option:
  -m mode
  -i ip_address_or_hostname
  -p port_number
  -u user_name
  -pw password
```

chconfig 命令

使用 **chconfig** 命令显示和配置 Service Advisor 设置。

备注：

- 在配置任何其他参数之前，必须使用 **chconfig -li** 命令选项接受 Service Advisor 条款和条件。

- 需要填写所有联系信息字段以及 IBM Service Support Center 字段，然后才可以启用对 Service Advisor 的 IBM 支持。
- 必须设置所有 HTTP 代理字段（如果需要 HTTP 代理）。

下表显示了选项的自变量。

选项	描述	值
-li	查看或接受 Service Advisor 条款和条件	view、accept
-sa	Service Advisor 的 IBM 支持状态	enabled、disabled
-sc	IBM Service Support Center 的国家或地区代码	两个字符的 ISO 国家或地区代码
Service Advisor 联系信息选项：		
-ce	主要联系人的电子邮件地址	格式为 userid@hostname 的有效电子邮件地址（最多 30 个字符）
-cn	主要联系人的姓名	引号定界的字符串（最多 30 个字符）
-co	主要联系人的组织或公司名称	引号定界的字符串（最多 30 个字符）
-cph	主要联系人的电话号码	引号定界的字符串（5 到 30 个字符）
-cpx	主要联系人的电话分机	引号定界的联系人电话分机（1 到 5 个字符）
备用 Service Advisor 联系信息选项：		
-ae	备用联系人的电子邮件地址	格式为 userid@hostname 的有效电子邮件地址（最多 30 个字符）
-an	备用联系人的姓名	引号定界的字符串（最多 30 个字符）
-aph	备用联系人的电话号码	引号定界的字符串（5 到 30 个字符）
-apx	备用联系人的电话分机	引号定界的字符串（1 到 5 个字符）
系统位置信息选项：		
-mp	机器位置的电话号码	引号定界的字符串（5 到 30 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	引号定界的有效密码（最多 15 个字符）
-u	HTTP 代理用户名	引号定界的有效用户名（最多 30 个字符）

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
```

chlog 命令

使用 **chlog** 命令显示 Service Advisor 活动日志条目。**chlog** 命令显示服务器或用户生成的回拨活动日志中的最后五个条目。最先显示最近回拨条目。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）。

下表显示选项的自变量。

选项	描述	值
-index	使用来自活动日志的索引来指定回拨条目	事件索引号。可以使用 chlog 命令查看索引号。
-ack	确认或未确认，已更正回拨事件。	yes、no 注： -event_index 命令选项指定确认或未确认的事件。
-s	显示回拨活动日志中的最后五个 IBM 支持条目	
-f	显示回拨活动日志中的最后五个 FTP/TFTP 服务器条目	

语法：

```
chlog [options]
option:
  -index
  -ack state
  -s
  -f
```

chmanual 命令

使用 **chmanual** 命令生成人工回拨请求或测试回拨事件。

注：使用 **chconfig** 命令配置回拨消息接收方。

- **chmanual -test** 命令将生成回拨测试消息。
- **chmanual -desc** 命令将生成人工回拨消息。

下表显示了选项的自变量。

选项	描述	值
-test	为回拨接收方生成测试消息	
-desc	将用户生成的消息发送至回拨接收方	引号定界的问题描述字符串（最多 100 个字符）

语法：

```
chmanual [options]
option:
  -test
  -desc message
```

events 命令

注：在使用 **events** 命令之前必须先接受 Service Advisor 条款和条件。

使用 **events** 命令查看和编辑回拨事件配置。IMM2 生成的每种类型的事件都具有唯一的事件标识。您可以通过将特定事件添加到回拨事件排除列表来阻止其生成回拨消息。下表显示了选项的自变量。

选项	描述	值
-add	将回拨事件添加到回拨排除列表中	格式为 0xhhhhhhhhhhhhhhhh 的事件标识。
-rm	从回拨排除列表中除去回拨事件	格式为 0xhhhhhhhhhhhhhhhh 的事件标识或者所有事件。

语法：

```
events -che [options]
option:
  -add event_id
  -rm event_id
```

sdemail 命令

使用 **sdemail** 命令以通过电子邮件发送服务信息。**sdemail** 命令将电子邮件发送给指定的收件人，并将 IMM2 服务日志作为附件。

下表显示了选项的自变量。

选项	描述	值
-to	收件人信息（必需选项）	收件人的电子邮件地址： - 使用逗号分隔多个地址（最多 119 个字符），格式为：userid1@hostname1,userid2@hostname2。 - 用户标识可以是字母数字字符、“.”、“-”或“_”；但是必须以字母数字字符开头和结束。 - 主机名可以是字母数字字符、“.”、“-”或“_”。必须包含两个域项。每个域项应该以字母数字字符开头和结束。最后一个域项应该是 2 到 20 个字母字符
-subj	电子邮件主题	引号定界的字符串（最多 119 个字符）

语法：

```
sdemail [options]
option:
  -to recipient_info
  -subj subject
```

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，或者只是希望了解有关 IBM 产品的更多信息，您可以从 IBM 找到各种有用的资源来帮助您。

使用此信息可获取有关 IBM 和 IBM 产品的其他信息，确定 IBM 系统或可选设备出现问题时要采取哪些措施，以及确定在必要时向谁请求服务。

在致电请求服务之前

在致电请求服务之前，请确保已执行以下步骤来尝试自行解决问题。

如果您认为需要 IBM 对您的 IBM 产品执行保修服务，那么在致电请求服务之前您应做好准备，这样 IBM 技术服务人员将可以更有效地向您提供帮助。

- 检查所有电缆以确保它们都已连接。
- 检查电源开关以确保系统和任何可选设备已经开启。
- 检查所用 IBM 产品已更新的软件、固件和操作系统设备驱动程序。IBM 保修条款和条件规定，由 IBM 产品所有者负责维护和更新产品的所有软件和固件（除非其他维护合同另行声明）。如果软件升级中已记录问题的解决方案，那么 IBM 技术服务人员将请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，请检查<http://www.ibm.com/systems/info/x86servers/serverproven/compat/us>以确保您的 IBM 产品支持该硬件和软件。
- 转至<http://www.ibm.com/supportportal>以查看用于帮助您解决问题的信息。
- 收集以下信息以提供给 IBM 支持人员。此数据将帮助 IBM 服务人员快速提供问题解决方案，并确保您享受合同规定的服务级别。
 - 硬件和软件维护协议合同编号（如果适用）
 - 机器类型编号（IBM 4 位数字机器标识）
 - 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
- 转至http://www.ibm.com/support/entry/portal/Open_service_request以提交电子服务请求。提交“电子服务请求”即是向 IBM 服务人员快速有效地提供相关信息，从而启动确定问题解决方案的过程。完成并提交电子服务请求后，IBM 技术服务人员会立即开始处理您的解决方案。

按照 IBM 在联机帮助或 IBM 产品随附的文档中所提供的故障诊断过程，您无需外界帮助即可解决许多问题。IBM 系统随附的文档还描述了您可以执行的诊断测试。大多数系统、操作系统和程序都随附包含故障诊断过程及错误消息和错误代码说明的文档。如果您怀疑软件有问题，请参阅操作系统或程序的文档。

使用文档

有关 IBM 系统和预安装软件（如果有）或可选设备的信息可从产品随附的文档中获得。该文档可包含印刷文档、联机文档、自述文件和帮助文件。

有关使用诊断程序的指示信息，请参阅您的系统文档中的故障诊断信息。故障诊断信息或诊断程序可能会告诉您需要其他或更新的设备驱动程序或其他软件。IBM 对您可以获取最新的技术信息并下载设备驱动程序及更新的万维网页面进行维护。要访问这些页面，请转至 <http://www.ibm.com/supportportal>。

从万维网获取帮助和信息

万维网上提供了 IBM 产品和支持相关的最新信息。

在万维网上以下地址处提供关于 IBM 系统、可选设备、服务和支持的最新信息：<http://www.ibm.com/supportportal>。IBM System x 信息位于 <http://www.ibm.com/systems/x>。IBM BladeCenter 信息位于 <http://www.ibm.com/systems/bladecenter>。IBM IntelliStation 信息位于 <http://www.ibm.com/systems/intellistation>。

如何向 IBM 发送 DSA 数据

使用 IBM Enhanced Customer Data Repository 向 IBM 发送诊断数据。

在向 IBM 发送诊断数据前，请先阅读以下地址中的使用条款：<http://www.ibm.com/de/support/ecurep/terms.html>。

您可以使用以下任意方法向 IBM 发送诊断数据：

- 标准上载：http://www.ibm.com/de/support/ecurep/send_http.html
- 带系统序列号的标准上载：http://www.ecurep.ibm.com/app/upload_hw
- 安全上载：http://www.ibm.com/de/support/ecurep/send_http.html#secure
- 带系统序列号的安全上载：https://www.ecurep.ibm.com/app/upload_hw

创建个性化支持 Web 页面

您可以通过识别感兴趣的 IBM 产品来创建个性化支持 Web 页面。

要创建个性化支持 Web 页面，请转至 <http://www.ibm.com/support/mynotifications>。从此个性化页面中，您可以预订有关新技术文档的每周电子邮件通知，搜索信息和下载以及访问各种管理服务。

软件服务和支持

通过 IBM 支持热线，您可以获取付费电话协助，内容涉及 IBM 产品的使用、配置和软件问题。

有关支持热线和其他 IBM 服务的更多信息，请访问 <http://www.ibm.com/services> 或请访问 <http://www.ibm.com/planetwide> 以了解支持电话号码。在中国，请拨打免费咨询热线 800-810-1818 转 5300 或 010-84981188 转 5300 查询相关信息。

硬件服务和支持

您可以通过 IBM 经销商或者 IBM 服务中心获得硬件服务。

要查找由 IBM 授权提供保修服务的经销商，请转至 <http://www.ibm.com/partnerworld>，然后单击 **Business Partner Locator**。要获取 IBM 支持电话号码，请访问 <http://www.ibm.com/planetwide>。在中国，请拨打免费咨询热线 800-810-1818 转 5300 或 010-84981188 转 5300 查询相关信息。

在美国和加拿大，每天 24 小时，每周 7 天都可获得硬件服务和支持。在英国，周一至周五的上午九点至下午六点可获取这些服务。

IBM 台湾产品服务

使用本信息来联系 IBM 台湾产品服务。

台灣 IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路 7 號 3 樓
電話：0800-016-888

IBM 台湾产品服务联系信息：

IBM Taiwan Corporation
3F, No 7, Song Ren Rd.
Taipei, Taiwan
电话：0800-016-888

附录 B. 声明

本信息是为在美国提供的产品和服务编写的。

IBM 可能在其他国家或地区不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 IBM 代表咨询。任何对 IBM 产品、程序或服务的引用，并非意在明示或暗示只能使用 IBM 的产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，均可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务的运行，则由用户自行负责。

IBM 公司可能已拥有或正在申请与本文档内容有关的各项专利。提供本文档并未授予用户使用这些专利的任何许可。您可以用书面方式将许可查询寄往：

*IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.*

International Business Machines Corporation“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、适销和适用于某种特定用途的保证。某些国家或地区在某些交易中不允许免除明示或暗含的保证。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。IBM 可以随时对本资料中描述的产品和/或程序进行改进和/或更改，而不另行通知。

本信息中对非 IBM Web 站点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 Web 站点的保证。那些 Web 站点中的资料不是本 IBM 产品资料的一部分，使用那些 Web 站点带来的风险将由您自行承担。

IBM 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需对您承担任何责任。

商标

IBM、IBM 徽标和 [ibm.com](http://www.ibm.com) 是 International Business Machines Corp. 在全球许多国家或地区注册的商标。其他产品和服务名称可能是 IBM 或其他公司的商标。

Web 站点 <http://www.ibm.com/legal/us/en/copytrade.shtml> 上包含了 IBM 商标的最新列表。

Adobe 和 PostScript 是 Adobe Systems Incorporated 在美国和/或其他国家或地区的注册商标或商标。

Cell Broadband Engine 是 Sony Computer Entertainment, Inc. 在美国和/或其他国家或地区的商标，并且根据相应许可进行使用。

Intel、Intel Xeon、Itanium 和 Pentium 是 Intel Corporation 或其分公司在美国和/或其他国家或地区的商标或注册商标。

Java 和所有基于 Java 的商标和徽标是 Oracle 和/或其下属公司的商标或注册商标。

Linux 是 Linus Torvalds 在美国和/或其他国家或地区的注册商标。

Microsoft、Windows 和 Windows NT 是 Microsoft Corporation 在美国和/或其他国家或地区的商标。

UNIX 是 The Open Group 在美国和其他国家或地区的注册商标。

重要声明

处理器速度代表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 驱动器速度是可变的读取速度。实际速度会发生变化，并且经常会小于可能达到的最大速度。

当提到处理器存储量、实际和虚拟存储量或通道量时，KB 代表 1024 字节，MB 代表 1048576 字节，而 GB 代表 1073741824 字节。

当提到硬盘驱动器容量或通信量时，MB 代表 1000000 字节，GB 代表 1000000000 字节。用户可访问的总容量可随操作环境而变化。

内置硬盘驱动器的最大容量是指用 IBM 提供的当前支持的最大容量驱动器来替换任何标准硬盘驱动器，并装满所有硬盘驱动器托架时的容量。

最大内存的实现可能需要使用可选内存条来替换标准内存。

各固态内存单元具有单元可引发的内在有限数量的写循环。因此，固态设备具有其受制的最大写循环数，以总写入字节数 (TBW) 表示。超过此限制的设备可能无法对系统生成的命令进行响应，或者不能进行写入。如设备的正式发布规范中所记载，IBM 不负责更换超过其最大保证程序/擦除循环数的设备。

IBM 对于符合 ServerProven[®] 认证的非 IBM 的产品或服务不作任何陈述或保证，包括但不限于对适销和适用于某种特定用途的暗含保证。这些产品由第三方提供和单独保证。

IBM 对于非 IBM 产品不作任何陈述或保证。对于非 IBM 产品的支持（如有）由第三方提供，而非 IBM。

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：空气浮尘（包括金属屑或微粒）和化学性质活泼的气体单独反应或其他环境因素（如湿度或温度）发生组合反应可能会对本文档中描述的设备造成风险。

由于颗粒级别过量或者有害气体聚集造成的风险包括可能导致设备故障或者完全损坏。本规范规定了针对颗粒和气体的限制，旨在避免此类损害。这些限制不可视为或

用作绝对限制，因为大量其他因素（如温度或空气的湿度）都可能对颗粒或环境腐蚀性以及气态污染物流动的后果造成影响。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 IBM 确定您的环境中的颗粒或气体级别对设备造成了损害，那么在实施相应的补救措施以减轻此类环境污染时，IBM 可能会酌情调整修复或更换设备或部件的服务。实施此类补救措施由客户负责。

表 10. 颗粒和气体的限制

污染物	限制
颗粒	• 依据 ASHRAE 标准 52.2¹，必须采用 40% 大气尘比色效率（MERV 9）连续不断地过滤房间内的空气。 • 必须使用符合 MIL-STD-282 的高效率空气颗粒（HEPA）过滤器对进入数据中心的空气进行过滤，以使其达到 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。 • 房间内不能存在导电污染物，如锌晶须。
气态	• 铜：G1 类，按照 ANSI/ISA 71.04-1985³ • 银：30 天内腐蚀率小于 300 Å

¹ ASHRAE 52.2-2008 - *Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size*。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。 *Environmental conditions for process measurement and control systems: Airborne contaminants*。美国北卡罗莱纳州三角研究园美国仪器学会（Instrument Society of America）。

文档格式

此产品的出版物采用 Adobe 可移植文档格式（PDF），符合辅助功能选项标准。如果您在使用 PDF 文件时遇到困难，并且希望获得基于 Web 格式或可访问的 PDF 文档格式的出版物，请将邮件寄往以下地址：

Information Development
IBM Corporation
205/A015
3039 E. Cornwallis Road
P.O. Box 12195
Research Triangle Park, North Carolina 27709-2195
U.S.A.

在请求中，请确保包含出版物的部件号和标题。

当您发送信息给 IBM 后，即授予 IBM 非专有权，IBM 对于您所提供的任何信息，有权利以任何它认为适当的方式使用或分发，而不必对您负任何责任。

电信规章声明

在您所在国家或地区，本产品可能未获得以任何一种方式连接到公共远程通信网络接口的认证。在进行任何此类连接前，可能需要依法进行进一步认证。如有任何疑问，请联系 IBM 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电缆和任何抑制干扰设备

联邦通信委员会 (FCC) 声明

注：依据 FCC 规则的第 15 部分，本设备经过测试，符合 A 级数字设备的限制。这些限制旨在为运行于商业环境中的设备提供合理保护，使其免受有害干扰。本设备生成、使用并可辐射射频能量，并且如果不按照说明手册进行安装和使用，可能会对无线电通信产生有害干扰。在居民区运行本设备很可能产生有害干扰，在这种情况下将由用户自行承担消除干扰的费用。

必须使用正确屏蔽并接地的电缆和连接器，以符合 FCC 辐射限制。因使用非推荐的电缆或连接器，或者对此设备进行未经授权的更改或修改而导致的任何无线电或电视干扰，IBM 概不负责。未经授权的更改或改动可能会使用户操作本设备的权限无效。

本设备符合 FCC 规则第 15 部分的规定。操作该设备应符合以下两个条件：(1) 此设备应不会导致有害干扰，并且 (2) 此设备必须能承受接收到的任何干扰，包括可能导致非期望操作的干扰。

加拿大工业部 A 级辐射规范符合声明

本 A 级数字设备符合加拿大 ICES-003 标准。

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

澳大利亚和新西兰 A 级声明

警告：本产品为 A 级产品。在家用环境中，本产品可能引起射频干扰，此时用户可能需要采取适当的措施。

欧盟 EMC 指令一致性声明

依据各成员国有关电磁兼容性的相近法律，本产品符合欧盟委员会指令 2004/108/EC 中的保护要求。IBM 对任何因擅自改动本产品（包括安装非 IBM 选件卡）而导致无法满足保护要求所产生的任何后果概不负责。

警告：本产品为 EN 55022 A 级产品。在家用环境中，本产品可能引起射频干扰，此时用户可能需要采取适当的措施。

制造商：

International Business Machines Corp.
New Orchard Road Armonk, New York 10504
914-499-1900

欧盟联系方式：

IBM Deutschland GmbH
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Germany
Telephone: +49 7032 15 2941
Email: lugi@de.ibm.com

德国 A 级声明

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/ eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:
Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen.

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG). Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:

International Business Machines Corp.
New Orchard Road Armonk, New York 10504
914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland GmbH
Technical Regulations, Abteilung M372
IBM-Allee 1, 71139 Ehningen, Germany
Telephone: +49 7032 15 29411
Email: lugi@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

日本 VCCI A 级声明

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用する
と電波妨害を引き起こすことがあります。この場合には使用者が適切な対策
を講ずるよう要求されることがあります。
VCCI-A

这是基于电磁干扰控制委员会 (VCCI) 标准的 A 级产品。如果在家用环境中使用本设备，可能引起射频干扰，此时用户可能需要采取纠正措施。

韩国通信委员会 (KCC) 声明

이 기기는 업무용(A급)으로 전자파적합기기로서
판매자 또는 사용자는 이 점을 주의하시기
바라며, 가정외의 지역에서 사용하는 것을 목
적으로 합니다.

本产品为商用电磁波兼容设备 (A 级)。卖方和用户需要注意。本产品针对非家用的其他所有领域。

俄罗斯电磁干扰 (EMI) A 级声明

ВНИМАНИЕ! Настоящее изделие относится к классу A.
В жилых помещениях оно может создавать радиопомехи, для
снижения которых необходимы дополнительные меры

中华人民共和国 A 级电子辐射声明

中华人民共和国“A类”警告声明

声 明

此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

台湾甲类规范符合声明

警告使用者：
這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。

索引

[A]

安全性

- 配置 62
- CIM over HTTPS 62, 188, 189
- CIM over HTTPS 协议 89
- cryptography management 94
- HTTPS 服务器 62, 188, 189
- HTTPS 协议 88
- LDAP 62, 188, 189
- LDAP 客户机 90
- SSH 服务器 62, 187
- ssh 服务器 92
- ssl 概述 93
- ssl 证书处理 93
- SSL 证书管理 93

安装

- 激活密钥 141, 175

安装功能部件

- Features on Demand 141, 175
- FoD 141, 175

按字母顺序排列的命令列表 150

澳大利亚 A 级声明 214

[B]

帮助

- 从万维网 208
- 向 IBM 发送诊断数据 208
- 源 207

绑定方法

- LDAP 服务器 61, 176

备份配置

- IMM2 62

备份状态视图

- IMM2 62

[C]

操作系统故障屏幕数据

- 捕获 135

操作系统截屏 110

操作系统需求 4

测试

- SMTP 61

测试事件

- 生成 128

查看

- 系统运行状况 102
- 系统状态 99
- 硬件运行状况 103

查看备份状态

- IMM 62

查看打开的端口 61, 179

查看当前

- 用户 60
- users 193

查看复原状态

- IMM2 62

查看固件信息

- 服务器 59, 158

查看配置

- IMM2 62

产品服务, IBM 台湾 209

重新启动

- IMM 202

重要注意事项 212

重置

- IMM2 62

重置配置

- IMM 182
- IMM2 62

除去

- 激活密钥 144, 175

除去功能部件

- Features on Demand 144, 175
- FoD 144, 175

串行重定向命令 162

串口

- 配置 59, 66, 180

创建

- 电子邮件通知 128
- 系统日志通知 128
- 用户帐户 60, 193

创建个性化支持 Web 页面 208

磁盘, 远程 119

[D]

单光标方式 115

刀片服务器 1, 3, 7

导出

- 激活密钥 145

导出功能部件

- Features on Demand 145
- FoD 145

德国 A 级声明 215

登录到 IMM2 10

登录许可权属性

- LDAP 61, 176

电话号码 208, 209

电信规章声明 214

电源

- 容量 139

电源管理

- Active Energy Manager 137
- chart 选项卡 139
- policies 选项卡 137
- power allocation 选项卡 139
- power history 选项卡 139
- power modules 选项卡 139

电子辐射 A 级声明 214

电子邮件接收方

- 设置 28

定制支持 Web 页面 208

端口

- 查看打开的 61

- 配置 61

- 设置端口号 61

端口号

- 设置 61, 179
- LDAP 服务器 61, 176
- SMTP 服务器 61, 182

端口转发

- Ethernet over USB 172

[E]

俄罗斯 A 级电子辐射声明 216

[F]

访问

- 远程控制 119
- Telnet 61, 191

服务和支持

- 软件 208
- 硬件 209
- 在致电请求服务之前 207

服务和支持数据

- 收集 134
- 下载 134

服务器超时

- 选择 62

服务器电源

- 控制 108

服务器电源和重新启动

- 命令 158

服务器固件

- 更新 121

服务器管理

- 操作系统故障屏幕数据 135
- 服务器超时, 设置 62

服务器管理 (续)
 服务器固件 121
 PXE 网络引导 120
 PXE 网络引导选项 57

服务器目标名称
 LDAP 61, 176

服务器寻址
 DNS 60, 170

服务器状态
 监控 99

复原配置
 IMM2 62

复原状态视图
 IMM2 62

[G]

概述
 download service data 37
 ssl 93

高级管理模块 1, 3, 7

高级以太网
 设置 76

根专有名称
 LDAP 服务器 61

更新
 ActiveX applet 109
 Java applet 109

更新固件 109

工具
 IPMItool 147

功能部件
 卡上的远程磁盘 119
 knock knock 116

固件
 查看服务器 59, 158

固件自动升级, IMM2
 设置 63

固件, 服务器
 更新 121

管理
 激活密钥 62, 175
 用户 60, 193
 DDNS 60, 170
 Features on Demand 62, 175
 FoD 62, 175
 MAC 地址 60, 173
 SNMPv1 社区 60, 183

[H]

韩国 A 级电子辐射声明 216

恢复配置
 IMM2 181

会话数, 最大
 Telnet 61, 191

[J]

激活密钥
 安装 141, 175
 除去 144, 175
 导出 145
 管理 62, 175

基于角色的安全性, 增强
 LDAP 193

基于角色的级别
 操作员 172
 超级用户 172
 rbs 172

加拿大 A 级电子辐射声明 214

监控服务器状态 99

监控命令 152

静态 IP 地址, 缺省 7

绝对鼠标控制 114

[K]

卡上的远程磁盘 119

颗粒污染物 212

可访问的文档 213

客户机专有名称
 LDAP 服务器 61, 176

控制电源状态
 服务器的 108

[L]

蓝屏捕获 110

联机出版物
 错误代码信息 1
 固件更新信息 1
 文档更新信息 1

浏览器需求 4

[M]

美国 FCC A 级声明 214

密码
 用户 60, 193
 LDAP 服务器 61, 176

命令
 电源 159
 accseccfg 163
 alertcfg 164
 alertentries 197
 asu 165
 autoftp 203
 autopromo 168

命令 (续)
 backup 168
 batch 200
 chconfig 203
 chlog 205
 chmanual 205
 clearcfg 201
 clearlog 153
 clock 201
 console 162
 cryptomode 169
 dhcpinfo 169
 dns 170
 ethtousb 172
 events 206
 exit 152
 fans 153
 ffdc 153
 fuelg 158
 gprofile 172
 help 152
 history 152
 identify 201
 ifconfig 173
 info 202
 keycfg 175
 ldap 176
 led 154
 ntp 177
 passwordcfg 178
 portcfg 180
 portcontrol 180
 ports 179
 pxeboot 161
 readlog 155
 reset 161
 resetsp 202
 restore 181
 restoreddefaults 182
 sdemail 206
 set 182
 smtp 182
 snmp 183
 snmpalerts 185
 spreset 202
 srcfg 186
 sshcfg 187
 ssl 188
 sslcfg 189
 syshealth 156
 telnetcfg 191
 temps 157
 thermal 192
 timeouts 192
 TLS 192
 usbeth 193

命令 (续)

- users 193
- volts 157
- vpd 158

命令行界面 (CLI)

- 登录 148
- 访问 147
- 功能和限制 149
- 描述 147
- 命令语法 148

命令, 按字母顺序排列的列表 150

命令, 类型

- 串行重定向 162
- 服务器电源和重新启动 158
- 配置 162
- 显示器 152
- IMM2 控制 197
- Service Advisor 203
- utility 152

目标名称, 服务器

- LDAP 61, 176

[O]

欧盟 EMC 指令一致性声明 214

[P]

配置

- 安全性 62
- 安全性设置 88
- 串口 59, 66, 180
- 端口 61
- 端口分配 87
- 全局登录设置 72
- 网络服务端口 180
- 网络协议 76
- 以太网 60, 173
- 以太网设置 76
- 用户帐户安全性级别 60, 163
- CIM over HTTPS 协议 89
- cryptography management 94
- DDNS 60, 170
- DDNS 设置 80
- DNS 60, 170
- DNS 设置 80
- Ethernet over USB 61, 172
- HTTPS 协议 88
- IMM2 62
- IPv4 60, 173
- IPv6 60, 173
- LDAP 61, 176
- LDAP 服务器 61, 176
- LDAP 客户机协议 90
- LDAP 设置 81

配置 (续)

- ports 179
- serial-to-SSH 重定向 148
- serial-to-Telnet 重定向 148
- SMTP 61, 182
- SMTP 设置 81
- SNMP 警报设置 78
- SNMPv1 60, 183
- SNMPv1 陷阱 60, 183
- SNMPv3 用户帐户 60, 193
- ssh 服务器 92
- Telnet 191
- Telnet 设置 61, 85
- USB 61, 172
- USB 设置 86

配置备份

- IMM2 62

配置复原

- IMM2 62

配置恢复

- IMM2 181

配置命令

配置视图

- IMM2 62

配置摘要, 查看 11

配置 IMM2

- 用于配置的选项

- IMM2 59

[Q]

启动顺序, 更改 11

气态污染物 212

驱动器

- 取消映射 119

- 映射 119

取消映射驱动器 119

全局登录

- 设置 72

全局登录设置

- 常规选项卡 72

- account security level 选项卡 73

缺省静态 IP 地址 7

缺省配置

- IMM 182

- IMM2 62

[R]

日本 A 级电子辐射声明 216

日期

- 设置 59, 201

日期和时间, IMM2

- 设置 64

软件服务和支 持电话号码 208

[S]

删除

- 电子邮件通知 128

- 系统日志通知 128

- 用户 60, 193

删除组

- 启用, 禁用 172

商标 211

设置

- 安全性 88

- 端口分配 87

- 高级 76

- 警报接收方 28

- 全局登录 72

- 常规选项卡 72

- account security level 选项卡 73

- 日期 59, 201

- 时间 59, 201

- 以太网 76

- 用户认证方法 60, 163

- 远程控制端口 62, 179

- 主机名 60, 173

- 自动协商 60

- 最大传输单元 60, 173

- autonegotiation (自动协商) 173

- CIM over HTTP 端口 62, 179

- CIM over HTTPS 89

- CIM over HTTPS 端口 62, 179

- CLI 键序列 59, 180

- cryptography management 94

- DDNS 80

- DNS 80

- HTTP 端口 61, 179

- HTTPS 88

- HTTPS 端口 61, 179

- IMM2 固件自动升级 63

- IMM2 日期和时间 64

- LDAP 81

- LDAP 服务器端口 61, 176

- LDAP 客户机协议 90

- MTU 60, 173

- services and support 选项卡 31

- SMTP 81

- SNMP 代理端口 61, 179

- SNMP 警报 78

- SNMP 陷阱端口 61, 179

- SNMPv1 联系人 60, 183

- SNMPv3 联系人 60, 183

- ssh 服务器 92

- SSH CLI 端口 61, 179

- Telnet 85

- Telnet CLI 端口 61, 179

- USB 86

- VLAN 支持 60

- Web 不活动超时 60, 163

- 设置 (续)
 - Web 会话 17
- 设置端口号 61, 179
- 设置服务器超时 62
- 设置向导
 - IMM2 62
- 声明 211
 - 电子辐射 214
 - FCC, A 级 214
- 时间
 - 设置 59, 201
- 实用程序命令 152
- 使用
 - 事件日志中的事件 26
 - 远程感知功能 109
 - 远程控制功能部件 109
 - ActiveX 客户机 43
 - Java 客户机 43
- 事件
 - 日志 126
- 事件标识
 - 问题列表 31
- 事件接收方 28
- 事件日志 26
 - 管理 126
- 事件通知 28
- 收集服务和支持数据 134
- 鼠标控制
 - 绝对 114
 - 相对 114
 - 与缺省 Linux 加速相对 114
- 搜索域
 - LDAP 服务器 61, 176

[T]

- 台湾甲类电子辐射声明 217

[W]

- 网络服务端口
 - 配置 180
- 网络连接 7
 - 静态 IP 地址, 缺省 7
 - 缺省静态 IP 地址 7
 - IP 地址, 缺省静态 7
- 网络协议属性
 - 端口分配 87
 - 以太网设置 76
 - DDNS 80
 - DNS 80
 - LDAP 81
 - SMTP 81
 - SNMP 警报设置 78
 - Telnet 85

- 网络协议属性 (续)
 - USB 86
- 文档
 - 格式 213
 - 使用 208
- 问题列表
 - 事件标识 31
- 污染物, 颗粒和气态 212

[X]

- 系统事件
 - 重试通知 128
 - 通知 128
- 系统事件通知 28
- 系统信息 101
 - 查看 101
- 系统运行状况 102
- 系统状态 99
- 相对鼠标控制 114
- 向 IBM 发送诊断数据 208
- 协助, 获取 207
- 新西兰 A 级声明 214
- 信息中心 208
- 虚拟光通路 11
- 需求
 - 操作系统 4
 - Web 浏览器 4
- 选项
 - IMM management 选项卡 58
 - server management 选项卡 38

[Y]

- 已安装的电源
 - 电源管理 139
 - power modules 选项卡 139
- 以太网
 - 配置 60, 173
- 硬件服务和支持电话号码 209
- 硬件运行状况 103
- 映射驱动器 119
- 用户
 - 查看当前 60
 - 管理 60, 193
 - 密码 60, 193
 - 删除 60, 193
 - SNMPv3 设置 60, 193
 - SSH 密钥 60, 193
- 用户认证方法
 - 设置 60, 163
- 用户帐户
 - 创建 60, 193
 - 管理 67
 - 配置 67
- 用户帐户 (续)
 - 组概要文件 71
- 用户帐户安全性级别
 - 配置 60, 163
- 域名源
 - DDNS 60, 170
- 域名, 定制
 - DDNS 61, 170
- 域名, DHCP 服务器指定
 - DDNS 170
- 域名, DHCP 服务器指定的
 - DDNS 61
- 预配置
 - LDAP 服务器 61, 176
- 远程磁盘 119
- 远程电源控制 115
- 远程访问 2
- 远程感知功能 109
 - 启用 110
- 远程控制
 - 单光标方式 115
 - 电源和重新启动命令 115
 - 访问 119
 - 国际键盘支持 113
 - 键盘通过方式 113
 - 键盘支持 112
 - 截屏 110
 - 绝对鼠标控制 114
 - 视频查看器 109
 - 鼠标支持 114
 - 退出 120
 - 相对鼠标控制 114
 - 性能统计信息 115
 - 虚拟介质会话 109
 - Linux 相对鼠标控制 (缺省 Linux 加速) 114
 - Video Viewer 111
 - Virtual Media Session 119
- 远程控制端口
 - 设置 62, 179
- 远程控制功能部件 43, 109
- 远程控制鼠标支持 114
- 远程控制中的国际键盘支持 113
- 远程控制中的键盘通过方式 113
- 远程控制中的键盘支持 112
- 远程控制中的视频颜色方式 111
- 远程控制中的视图方式 111
- 远程控制中的鼠标支持 114
- 远程控制, 窗口
 - 视频查看器 43
 - 虚拟介质会话 43
- 远程引导 119
- 远程桌面协议 (RDP)
 - 启动 115

[Z]

增强基于角色的安全性

LDAP 193

证书处理

安全 LDAP 客户机 90

CIM over HTTPS 89

证书管理

CIM over HTTPS 62, 188, 189

HTTPS 服务器 62, 188, 189

LDAP 62, 188, 189

SSH 服务器 62, 187

支持 Web 页面, 定制 208

执行

IMM2 任务 107

中国 A 级电子辐射声明 216

中华人民共和国 A 级电子辐射声明 216

主机服务器启动顺序, 更改 11

主机名

设置 60, 173

LDAP 服务器 61, 176

SMTP 服务器 61, 182

注销 IMM2 会话 19

注意事项和声明 6

注意事项, 重要 212

专有名称, 根

LDAP 服务器 61

专有名称, 客户机

LDAP 服务器 61, 176

专有名称, root 用户

LDAP 服务器 176

自动协商

设置 60

组概要文件

管理 71

组过滤器

LDAP 61, 176

组搜索属性

LDAP 61, 176

最大传输单元

设置 60, 173

最大会话数

Telnet 61, 191

最小, 级别

TLS 192

A

A 级电子辐射声明 214

accsecfg 命令 163

Active Directory 用户

LDAP 61, 193

Active Energy Manager

policies 选项卡 137

ActiveX applet

更新 109

advanced 级别功能部件 3

Advanced Settings Utility (ASU) 1

alertcfg 命令 164

alertentries 命令 197

asu 命令 165

autoftp 命令 203

autonegotiation

设置 173

autopromo 命令 168

B

backup 命令 168

basic 级别功能部件 2

batch 命令 200

BIOS (基本输入/输出系统) 1

BladeCenter 1, 3, 7

BMC 控制器 1

C

chconfig 命令 203

chlog 命令 205

chmanual 命令 205

CIM over HTTP 端口

设置 62, 179

CIM over HTTPS

安全性 62, 188, 189

证书管理 62, 188, 189

CIM over HTTPS 端口

设置 62, 179

clearcfg 命令 201

clearlog 命令 153

CLI 键序列

设置 59, 180

clock 命令 201

console 命令 162

cooling devices 选项

Server Management 选项卡下 52

cryptomode 命令 169

D

DDNS

定制域名 61, 170

管理 60, 170

配置 60, 170

域名源 60, 170

DHCP 服务器指定的域名 61, 170

dhcpinfo 命令 169

disks 选项

Server Management 选项卡下 54

DNS

服务器寻址 60, 170

配置 60, 170

DNS (续)

IPv4 寻址 60, 170

IPv6 寻址 60, 170

LDAP 服务器 61, 176

dns 命令 170

download service data

选项, 概述 37

services and support 选项卡 31

DSA, 向 IBM 发送数据 208

E

enhanced role-based security

LDAP 61

Ethernet over USB

端口转发 61, 172

配置 61, 172

ethtousb 命令 172

event 选项卡

日志 26

event recipients

管理 126

events

recipients 128

events 菜单 126

events 命令 206

events 选项卡

概述 26

exit 命令 152

F

fans 命令 153

FCC A 级声明 214

Features on Demand 141

安装功能部件 141, 175

除去功能部件 144, 175

导出功能部件 145

管理 62, 175

ffdc 命令 153

FoD 141

安装功能部件 141, 175

除去功能部件 144, 175

导出功能部件 145

管理 62, 175

fuelg 命令 158

G

gprofile 命令 172

H

help 命令 152

history 命令 152

- HTTP 端口
 - 设置 61, 179
- HTTPS 端口
 - 设置 61, 179
- HTTPS 服务器
 - 安全性 62, 188, 189
 - 证书管理 62, 188, 189

I

- IBM 刀片服务器 1, 3, 7
- IBM 台湾产品服务 209
- IBM BladeCenter 1, 3, 7
- IBM System X 服务器固件
 - Setup Utility 7
- IBM System x Server Firmware
 - 描述 1
- identify 命令 201
- ifconfig 命令 173
- IMM
 - 重新启动 202
 - 重置配置 182
 - 恢复配置 181
 - 配置 62
 - 缺省配置 182
 - reset 202
 - sreset 202
- IMM 管理
 - 安全性设置 88
 - 配置网络协议 76
 - 用户
 - 帐户 67
 - IMM 配置
 - 恢复和修改 IMM 配置 96
 - IMM 属性
 - 串口设置 66
- IMM management
 - 重新启动 IMM2 96
 - 激活管理密钥 98
 - 配置用户帐户 67
 - 用户
 - 组概要文件 71
- IMM management 选项卡 58
- IMM2
 - 备份配置 62
 - 备份状态视图 62
 - 操作描述 11
 - 查看备份状态 62
 - 查看复原状态 62
 - 查看配置 62
 - 重新启动 96
 - 重置 62
 - 重置配置 62
 - 串行重定向 148
 - 复原配置 62
 - 复原状态视图 62

- IMM2 (续)
 - 功能部件 2
 - 激活管理密钥 98
 - 描述 1
 - 配置备份 62
 - 配置复原 62
 - 配置恢复 181
 - 配置视图 62
 - 配置选项 59
 - 缺省配置 62
 - 设置向导 62
 - 网络连接 7
 - 新功能 1
 - IMM2 标准级 2
 - IMM2 高级 2
 - IMM2 基本级 2
 - reset 97
 - restart 62
 - Web 界面 7
 - Web 用户界面概述 17
- IMM2 的功能 2
- IMM2 功能部件
 - advanced 级别 3
 - basic 级别 2
- IMM2 功能部件standard 级别功能部件
 - standard 级别 2
- IMM2 控制命令 197
- IMM2 任务 107
- IMM2 management
 - 重置 IMM2 97
 - IMM 属性
 - 固件自动升级 63
 - IMM properties
 - date and time 64
- IMM2 Web 会话
 - 注销 19
- IMM2 Web 用户界面
 - 概述 17
 - events 选项卡
 - 选项概述 26
 - service and support 选项卡
 - 选项概述 31
 - system status 选项卡
 - 概述 20
- info 命令 202
- IP 地址
 - 配置 7
 - IPv4 7
 - IPv6 7
 - LDAP 服务器 61, 176
 - SMTP 服务器 61, 182
- IP 地址, 缺省静态 7
- IPMI
 - 远程服务器管理 147
- IPMItool 147

- IPv4
 - 配置 60, 173
- IPv4 寻址
 - DNS 60, 170
- IPv6 7
 - 配置 60, 173
- IPv6 寻址
 - DNS 60, 170

J

- Java 4, 119
- Java applet
 - 更新 109

K

- keycfg 命令 175
- knock knock 功能部件
 - 启用 116
 - 请求远程会话 116
 - 用户方式
 - 单 116
 - 多 116

L

- latest OS failure screen 选项
 - Server Management 选项卡下 57
- LDAP
 - 安全性 62, 188, 189
 - 登录许可权属性 61, 176
 - 服务器目标名称 61, 176
 - 基于角色的安全性, 增强 193
 - 配置 61, 176
 - 增强基于角色的安全性 193
 - 证书管理 62, 188, 189
 - 组过滤器 61, 176
 - 组搜索属性 61, 176
 - Active Directory 用户 61, 193
 - enhanced role-based security 61
 - role-based security, enhanced 61
- LDAP 服务器
 - 绑定方法 61, 176
 - 端口号 61, 176
 - 根专有名称 61
 - 客户机专有名称 61, 176
 - 密码 61, 176
 - 配置 61, 176
 - 搜索域 61, 176
 - 预配置 61, 176
 - 主机名 61, 176
 - DNS 61, 176
 - IP 地址 61, 176
 - root 用户专有名称 176

LDAP 服务器 (续)
 UID 搜索属性 61, 176
LDAP 服务器端口
 设置 61, 176
ldap 命令 176
led 命令 154
Linux 相对鼠标控制 (缺省 Linux 加速)
 114

M

MAC 地址
 管理 60, 173
memory 选项
 Server Management 选项卡下 54
MTU
 设置 60, 173

N

ntp 命令 177

P

page auto refresh 选项 17
passwordcfg 命令 178
port forwarding
 Ethernet over USB 61
portcfg 命令 180
portcontrol 命令 180
ports
 查看打开的 179
 配置 179
 设置端口号 179
ports 命令 179
power 命令 159
power actions 108
power allocation 选项卡
 电源 139
 电源管理 139
power management 选项
 Server Management 选项卡下
 电源策略 136
 电源设备 136
 耗电量 136
power modules 选项
 Server Management 选项卡下 53
problems
 services and support 选项卡 31
problems, 选项
 services and support 31
processors 选项
 Server Management 选项卡下 56
PXE 网络引导
 设置 120

PXE 网络引导选项
 在 Server Management 选项卡下方 57
PXE Boot Agent 11
pxeboot 命令 161

R

RDOC 119
readlog 命令 155
Remote Supervisor Adapter II 1
reset
 IMM 202
reset 命令 161
resetsp 命令 202
restart
 IMM2 62
restore 命令 181
restoredefaults 命令 182
role-based security, enhanced
 LDAP 61
root 用户专有名称
 LDAP 服务器 176

S

sdemail 命令 206
Serial over LAN 147
serial-to-SSH 重定向 148
serial-to-Telnet 重定向 148
server firmware 选项
 Server Management 选项卡下 38
Server Management
 服务器 cooling devices 选项 52
 disks 选项 54
 latest OS failure screen 选项 57
 memory 选项 54
 power modules 选项 53
 processors 选项 56
 server firmware 选项 38
 server power actions 选项 52
 server properties 选项 48
 server timeouts 选项 57
server management 选项卡 38
server power actions 选项
 Server Management 选项卡下 52
server properties
 environmentals 选项卡 48
 general settings 选项卡 48
 hardware activity 选项卡 48
 hardware information 选项卡
 network hardware 选项卡 48
 system component information 选项卡 48
 system information 选项卡 48
LED 选项卡 48

server properties 选项
 Server Management 选项卡下 48
server timeouts 选项
 Server Management 选项卡下 57
Service Advisor 的命令 203
service and support 选项卡
 概述 31
services and support
 选项, problems 31
 选项, settings 34
services and support 选项卡
 设置 31
 download service data 31
 problems 31
set 命令 182
settings, 选项
 services and support 34
SMTP
 测试 61
 服务器端口号 61, 182
 服务器主机名 61, 182
 服务器 IP 地址 61, 182
 配置 61, 182
smtp 命令 182
SNMP 代理端口
 设置 61, 179
snmp 命令 183
SNMP 陷阱端口
 设置 61, 179
snmpalerts 命令 185
SNMPv1
 配置 60, 183
SNMPv1 联系人
 设置 60, 183
SNMPv1 社区
 管理 60, 183
SNMPv1 陷阱
 配置 60, 183
SNMPv3 联系人
 设置 60, 183
SNMPv3 设置
 用户 60, 193
SNMPv3 用户帐户
 配置 60, 193
spreset 命令 202
srcfg 命令 186
SSH 服务器
 安全性 62, 187
 证书管理 62, 187
SSH 密钥
 用户 60, 193
SSH CLI 端口
 设置 61, 179
sshcfg 命令 187
SSL
 证书处理 93

SSL (续)
 证书管理 93
ssl 命令 188
sslcfg 命令 189
syshealth 命令 156
system status 选项卡
 概述 20
system status 页面, 概述 20

T

Telnet
 访问 61, 191
 配置 191
 最大会话数 61, 191
Telnet 设置
 配置 61
Telnet CLI 端口
 设置 61, 179
telnetcfg 命令 191
temps 命令 157
thermal 命令 192
timeouts 命令 192
TLS
 最小级别 192
TLS 命令 192
trespass message 选项 18

U

UID 搜索属性
 LDAP 服务器 61, 176
USB
 配置 61, 172
usbeth 命令 193
users
 查看当前 193
users 命令 193

V

Video Viewer
 单光标方式 115
 电源和重新启动命令 115
 国际键盘支持 113
 键盘通过方式 113
 截屏 110
 绝对鼠标控制 114
 视频颜色方式 111, 112
 视图方式 111
 鼠标支持 114
 退出 120
 相对鼠标控制 114
 性能统计信息 115

Video Viewer (续)
 Linux 相对鼠标控制 (缺省 Linux 加速) 114
Virtual Media Session
 启动 119
 取消映射驱动器 119
 退出 120
 映射驱动器 119
 远程磁盘 119
VLAN 支持
 设置 60
volts 命令 157
vpd 命令 158

W

Web 不活动超时
 设置 60, 163
Web 会话设置 17
Web 界面
 登录到 Web 界面 10
Web 界面, 打开并使用 7
Web 浏览器需求 4



部件号： 00FH274

Printed in China

(1P) P/N: 00FH274

