IBM

集成管理模块 I
用户指南

IBM

集成管理模块 I
用户指南

第七版（**2013** 年 **11** 月）

目录

表

第 1 章 简介

集成管理模块 (IMM) 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。在 IBM® System x 服务器中，IMM 替换了 BMC 控制器和 Remote Supervisor Adapter II。

在 IBM 服务器中使用 IMM 之前，BMC 控制器和基本输入/输出系统 (BIOS) 是标准的系统管理硬件和固件。System x 服务器使用 BMC 服务处理器来管理系统管理软件和平台硬件之间的接口。Remote Supervisor Adapter II 和 Remote Supervisor Adapter II Slimline 是用于频带外服务器管理的可选控制器。

要点：虽然 IMM 在某些 IBM BladeCenter 产品和 IBM 刀片服务器中是标配，但是针对 BladeCenter 和刀片服务器，BladeCenter 高级管理模块仍然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。与 IMM Web 界面和命令行界面相关的内容不适用于 IBM BladeCenter 和刀片服务器。希望在刀片服务器上配置 IMM 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。

IMM 对 BMC 和 Remote Supervisor Adapter II 的组合功能提供了一些改进：

- 专用或共享以太网连接选项。专用以太网连接在刀片服务器或某些 System x 服务器上不可用。

  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 IMM 设置。
- 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。该功能不适用于刀片服务器。
- Embedded Dynamic System Analysis (DSA)。
- 能够在本地或远程更新其他实体，无需重新启动服务器即可启动更新过程。
- 使用 Advanced Settings Utility (ASU) 进行远程配置。该功能不适用于刀片服务器。
- 应用程序和工具能够在频带内或频带外访问 IMM。在刀片服务器上，仅支持频带内 IMM 连接。
- 增强型远程感知功能。该功能不适用于刀片服务器。

IBM System x® 服务器固件是 IBM 实施的统一扩展固件接口 (UEFI)。它在 System x 服务器和 IBM 刀片服务器中替代了 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 服务器固件提供了 BIOS 没有的一些功能，包括 UEFI 2.1 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 服务器固件通常称为服务器固件，有时称为 UEFI。
- IBM System x 服务器固件与非 UEFI 操作系统完全兼容。
- 有关使用 IBM System x 服务器固件的更多信息，请参阅您的服务器随附的文档。

本文档说明如何在 IBM 服务器中使用 IMM 的功能。IMM 与 IBM System x 服务器固件协作，为 System x 和 BladeCenter 服务器提供系统管理能力。

本文档不包含有关错误或消息的说明。在您的服务器随附的《*问题确定与维护指南*》中，对 IMM 错误和消息进行了描述。要在 IBM® Support Portal 上找到本文档或 IBM 白皮书 *Transitioning to UEFI and IMM* 的最新版本，请完成以下步骤：

注：首次访问 IBM Support Portal 时，必须选择您的服务器所对应的产品类别、产品系列和型号。下次访问 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，单击文档。
5. 在查看结果下，单击查看页面。
6. 在“文档”框中，单击更多结果。
7. 在“类别”框中，选中集成管理模块 **(IMM)** 复选框。这样会显示指向 IMM 和 UEFI 文档的链接。

如果有固件更新，您可从 IBM Web 站点进行下载。IMM 可能具有文档中未描述的功能，该文档可能会不定期更新，以包含有关这些功能的信息，也可能通过技术更新的形式提供 IMM 文档中未包含的其他信息。

要检查固件更新，请完成以下步骤。

注：首次访问 IBM Support Portal 时，必须选择您的服务器所对应的产品类别、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。

IMM 功能

IMM 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
- 使用标准 Web 浏览器基于 Web 进行管理

IMM 提供两种类型的 IMM 功能：IMM Standard 功能和 IMM Premium 功能。有关您的服务器中的 IMM 硬件类型的信息，请参阅服务器随附的文档。

IMM Standard 功能

注：以下某些功能不适用于刀片服务器。

- 访问关键服务器设置
- 访问服务器重要产品数据 (VPD)
- 高级 Predictive Failure Analysis (PFA) 支持
- 自动通知和警报
- 持续的运行状况监控和控制
- 专用或共享以太网连接选项（如果适用）。

  注：专用的系统管理网络端口在您的服务器上可能不可用。
- 域名系统 (DNS) 服务器支持
- 动态主机配置协议 (DHCP) 支持
- 电子邮件警报
- Embedded Dynamic System Analysis (DSA)
- 增强的用户权限级别
- 使用 LAN over USB 与 IMM 进行频带内通信
- 事件日志具有时间戳记、保存在 IMM 上，并且可以附加到电子邮件警报
- 业界标准接口和协议
- 操作系统看守程序
- 通过 Advanced Settings Utility (ASU) 进行远程配置
- 远程固件更新
- 远程电源控制
- 图形无缝远程加速
- 安全 Web 服务器用户接口
- Serial over LAN
- 服务器控制台重定向
- 简单网络管理协议 (SNMP) 支持
- 使用与轻量级目录访问协议 (LDAP) 服务器的安全连接进行用户认证

IMM Premium 功能

注：以下某些功能不适用于刀片服务器。

- 访问关键服务器设置
- 访问服务器重要产品数据 (VPD)
- 高级 Predictive Failure Analysis (PFA) 支持
- 自动通知和警报
- 持续的运行状况监控和控制
- 专用或共享以太网连接选项（如果适用）。

  注：专用的系统管理网络端口在您的服务器上可能不可用。
- 域名系统 (DNS) 服务器支持
- 动态主机配置协议 (DHCP) 支持
- 电子邮件警报
- Embedded Dynamic System Analysis (DSA)
- 增强的用户权限级别
- 使用 LAN over USB 与 IMM 进行频带内通信
- 事件日志具有时间戳记、保存在 IMM 上，并且可以附加到电子邮件警报
- 业界标准接口和协议
- 操作系统看守程序
- 通过 Advanced Settings Utility (ASU) 进行远程配置
- 远程固件更新
- 远程电源控制
- 图形无缝远程加速
- 安全 Web 服务器用户接口
- Serial over LAN
- 服务器控制台重定向
- 简单网络管理协议 (SNMP) 支持
- 使用与轻量级目录访问协议 (LDAP) 服务器的安全连接进行用户认证
- 远程感知，包括远程控制服务器
- 操作系统故障屏幕捕获以及通过 Web 界面显示
- 远程磁盘，可以将软盘驱动器、CD/DVD 驱动器、USB 闪存驱动器或磁盘映像连接到服务器

注：IMM 中不包括 Remote Supervisor Adapter II 的以下功能：
- 显示服务器 MAC 地址
- 多个 NTP 服务器项

从 **IMM Standard** 升级至 **IMM Premium**

如果您的服务器具有 IMM Standard 功能，那么可以通过购买 Virtual Media Key 并将其安装在服务器主板上来升级至 IMM Premium。无需任何新固件。

要订购 Virtual Media Key，请转至 http://www.ibm.com/systems/x/newgeneration。

注：有关安装 Virtual Media Key 的信息，请参阅您的服务器随附的文档。

如果在订购方面需要帮助，请拨打零售部件页面上列出的免费电话号码，或与当地的 IBM 代表联系以获取帮助。

比较 System x 服务器中的 IMM 和其他系统管理硬件

下表对 System x 服务器中的 IMM 功能与 BMC 和 Remote Supervisor Adapter II 功能进行了比较。

注：与 BMC 相似，IMM 使用标准 IPMI 规范。

表 1. 比较 System x 服务器中的 IMM 功能与 BMC 和 Remote Supervisor Adapter II 组合功能

描述	**BMC 及 Remote Supervisor Adapter II**	**IMM**
网络连接	BMC 使用与服务器共享的网络连接，并且所用 IP 地址与 Remote Supervisor Adapter II IP 地址不同。 Remote Supervisor Adapter II 使用专用系统管理网络连接，并且所用 IP 地址与 BMC IP 地址不同。	IMM 通过同一网络连接提供 BMC 和 Remote Supervisor Adapter II 功能。同一 IP 地址用于这两种用途。如果您的服务器具有专用系统管理网络端口，那么可以选择专用或共享网络连接。 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 IMM 设置。
更新功能	每个服务器都需要针对 BMC 和 Remote Supervisor Adapter II 的唯一更新。 BIOS 和诊断工具可在频带内更新。	一个 IMM 固件映像可以用于所有适用的服务器。 IMM 固件、System x 服务器固件和 Dynamic System Analysis (DSA) 固件可在频带内和频带外更新。 IMM 可在本地或远程对自身、服务器固件和 DSA 固件进行更新，无需重新启动服务器即可启动更新过程。
配置功能	只能在频带内使用 ASU 进行配置更改。对于 BMC、Remote Supervisor Adapter II 和 BIOS，系统需要不同的配置。	ASU 可以在频带内或频带外运行，并且可配置 IMM 和服务器固件。通过 ASU，您还可以修改引导顺序、iSCSI 和 VPD（机器类型、序列号、UUID 和资产标识）。 服务器固件配置设置由 IMM 保存。因此，您可以在服务器关闭期间或操作系统运行期间进行服务器固件配置更改，这些更改会在服务器下次启动时生效。 可以通过以下 IMM 用户界面在频带内或频带外配置 IMM 配置设置： • Web 界面 • 命令行界面 • IBM Systems Director 界面 • SNMP

表 1. 比较 System x 服务器中的 IMM 功能与 BMC 和 Remote Supervisor Adapter II 组合功能 (续)

描述	**BMC 及 Remote Supervisor Adapter II**	**IMM**
操作系统截屏	当发生操作系统故障时，Remote Supervisor Adapter II 会执行屏幕捕获。屏幕捕获的显示需要 Java applet。	只有 IMM Premium 才提供此功能。有关从 IMM Standard 升级到 IMM Premium 的信息，请参阅第 4 页的『从 IMM Standard 升级至 IMM Premium』。 屏幕捕获由 Web 浏览器直接显示，不需要 Java applet。
错误日志记录	BMC 提供 BMC 系统事件日志（IPMI 事件日志）。 Remote Supervisor Adapter II 提供基于文本的日志，包括由 BMC 报告的事件的描述。该日志还包含由 Remote Supervisor Adapter II 本身检测到的任何信息或事件。	IMM 有两个事件日志： 1. 系统事件日志通过 IPMI 界面提供。 2. 机箱事件日志通过其他 IMM 界面提供。机箱事件日志显示使用“分布式管理任务组织”规范 DSP0244 和 DSP8007 生成的文本消息。 注：有关特定事件或消息的说明，请参阅您的服务器随附的《*问题确定与维护指南*》。
监控	BMC 及 Remote Supervisor Adapter II 具有以下监控功能： • 监控服务器和电池电压、服务器温度、风扇、电源，以及处理器和 DIMM 状态 • 风扇速度控制 • Predictive Failure Analysis (PFA) 支持 • 系统诊断指示灯控制（电源、硬盘驱动器、活动、警报和脉动信号） • 服务器自动重启 (ASR) • BIOS 自动恢复 (ABR)	IMM 提供与 BMC 和 Remote Supervisor Adapter II 相同的监控功能。当在 RAID 配置中使用时，IMM 支持扩展硬盘驱动器状态，包括磁盘驱动器 PFA。

表 1. 比较 System x 服务器中的 IMM 功能与 BMC 和 Remote Supervisor Adapter II 组合功能 (续)

描述	**BMC 及 Remote Supervisor Adapter II**	**IMM**
远程感知	BMC 及 Remote Supervisor Adapter II 具有以下远程感知功能： • 基于 LAN 的图形控制台重定向 • 远程虚拟软盘和 CD-ROM • PCI 显示器、键盘和鼠标的高速远程重定向 • 支持最高 1024 x 768 (70 Hz) 视频分辨率 • 数据加密	只有 IMM Premium 才提供此功能。有关从 IMM Standard 升级到 IMM Premium 的信息，请参阅第 4 页的『从 IMM Standard 升级至 IMM Premium』。 除 Remote Supervisor Adapter II 远程感知功能外，IMM 还具有以下功能： 注：IMM 需要 Java 运行时环境 V1.5 或更高版本或者 ActiveX（如果在 Windows 中使用 Internet Explorer）。 • 支持最高 1280 x 1024 (75 Hz) 视频分辨率 • 用于虚拟键盘、鼠标和海量存储设备的 USB 2.0 支持 • 15 位色深 • 绝对或相对鼠标方式选项 • USB 闪存驱动器支持 • 在 Remote Control 窗口上控制服务器电源操作和复位操作 • Remote Control 窗口上的视频可保存在文件中 IMM 提供两个单独的客户机窗口。一个用于显示器、键盘和鼠标交互，另一个用于虚拟介质。 IMM Web 界面包含一个菜单项，可调整色深以减少在低带宽情况下传输的数据。Remote Supervisor Adapter II 界面有一个带宽滑块。
安全性	Remote Supervisor Adapter II 具有高级安全性功能，包括安全套接字层 (SSL) 和加密。	IMM 具有与 Remote Supervisor Adapter II 相同的安全性功能。

表 1. 比较 System x 服务器中的 IMM 功能与 BMC 和 Remote Supervisor Adapter II 组合功能 (续)

描述	**BMC 及 Remote Supervisor Adapter II**	**IMM**
串行重定向	IPMI Serial over LAN (SOL) 功能是 BMC 的标准功能。 Remote Supervisor Adapter II 能够将服务器串行数据重定向到 Telnet 或 SSH 会话。 注：此功能在某些服务器上不可用。	COM1 端口用于 System x 服务器上的 SOL。只能通过 IPMI 界面配置 COM1。 COM2 端口用于通过 Telnet 或 SSH 进行串行重定向。可通过除 IPMI 界面外的所有 IMM 界面来配置 COM2。COM2 端口用于刀片服务器上的 SOL。 两种 COM 端口配置都限制为 8 个数据位、无奇偶性和 1 个停止位，并且波特率选项为 9600、19200、38400、57600、115200 或 230400。 在刀片服务器上，COM2 端口是不提供外部访问机制的内部 COM 端口。在刀片服务器上无法共享 IPMI 串口。 在机架安装式和塔式服务器上，IMM COM2 端口是不提供外部访问机制的内部 COM 端口。
SNMP	SNMP 支持仅限于 SNMPv1。	IMM 支持 SNMPv1 和 SNMPv3。

将 IMM 与 BladeCenter 高级管理模块配合使用

BladeCenter 高级管理模块是 IBM BladeCenter 和 IBM 刀片服务器中的标准系统管理接口。虽然目前在某些 IBM BladeCenter 和 IBM 刀片服务器中包括了 IMM，但是针对 BladeCenter 和刀片服务器，该高级管理模块仍然是用于系统管理功能以及键盘、显示器和鼠标 (KVM) 多路复用的管理模块。BladeCenter 中未提供连接 IMM 的外部网络接口。

在刀片服务器上，不能通过外部网络访问 IMM。必须使用高级管理模块对刀片服务器进行远程管理。IMM 代替了过去刀片服务器产品中的 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

IMM 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 V6.0、V7.0 或 V8.0，具有最新的 Service Pack。高于 8.0 的版本不受支持。
- Mozilla Firefox V1.5 或更高版本

以下服务器操作系统具有远程感知功能所需的 USB 支持：

- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008
- Microsoft Windows Server 2003
- Red Hat Enterprise Linux V4.0 和 V5.0

- SUSE Linux V10.0
- Novell NetWare 6.5

注：IMM Web 界面不支持双字节字符集 (DBCS) 语言。

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 IMM Web 界面

IMM 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 IMM Web 界面远程访问 IMM，您必须先登录。本章描述登录过程以及可在 IMM Web 界面中执行的操作。

访问 IMM Web 界面

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

IMM 也支持 IPv6，但是在缺省情况下，IMM 没有固定的静态 IPv6 IP 地址。要在 IPv6 环境中初始访问 IMM，可以使用 IPv4 IP 地址或 IPv6 链路本地地址。IMM 会生成唯一链路本地 IPv6 地址，该地址显示在 IMM 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 IMM 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。

IMM 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。

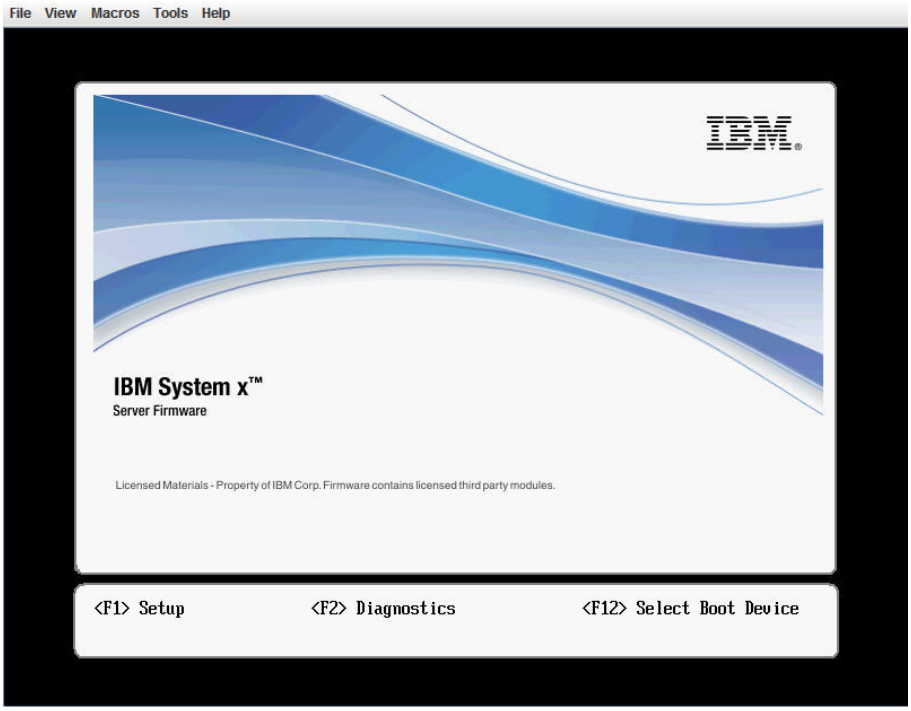
注：专用的系统管理网络端口在您的服务器上可能不可用。如果您的硬件没有专用网络端口，*shared* 设置将是唯一可用的 IMM 设置。

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

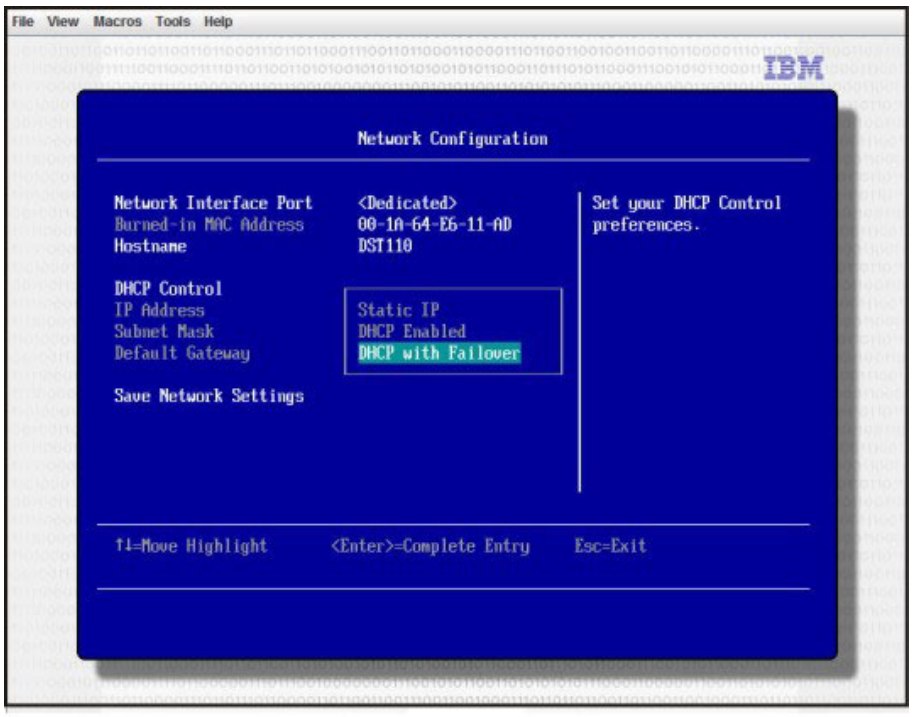
启动服务器后，您可以使用 Setup Utility 来选择 IMM 网络连接。具有 IMM 硬件的服务器必须连接到动态主机配置协议 (DHCP) 服务器，或者必须将服务器网络配置为使用 IMM 静态 IP 地址。要通过 Setup Utility 设置 IMM 网络连接，请完成以下步骤：

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 2 分钟后，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 IMM 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 IMM 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 IMM 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 IMM 所使用的服务器上以太网接口的位置，请参阅服务器随附的文档。
10. 选择 **Save Network Settings**。
11. 退出 Setup Utility。

备注：

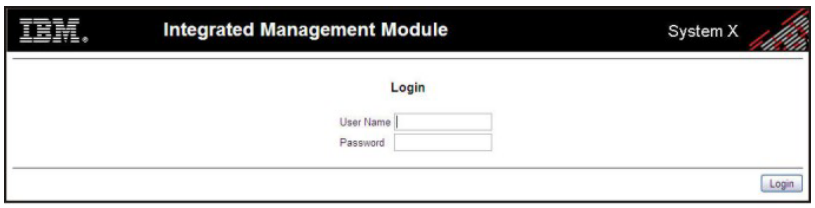
- 您必须等待大约 1 分钟以使更改生效，然后服务器固件才再次可运作。
- 您也可以通过 IMM Web 界面来配置 IMM 网络连接。有关更多信息，请参阅第 33 页的『配置网络接口』。

登录到 IMM

要点：最初设置的 IMM 用户名为USERID，密码为 PASSW0RD（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缺省密码以增强安全性。

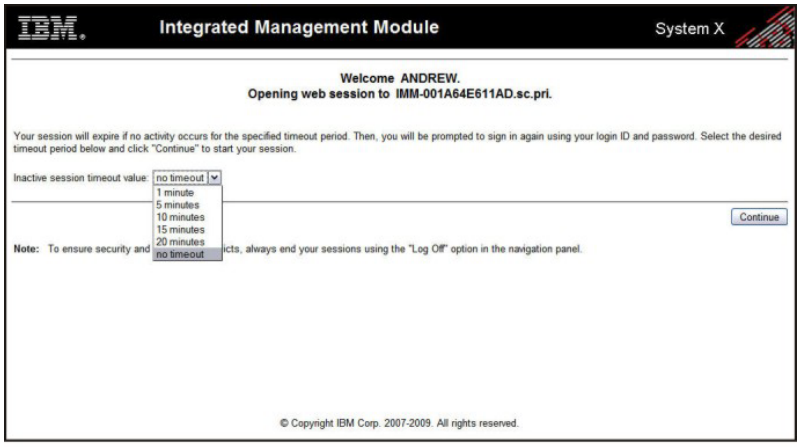
要通过 IMM Web 界面访问 IMM，请完成以下步骤：

1. 打开 Web 浏览器。在地址或 URL 字段中，输入要连接到的 IMM 服务器的 IP 地址或主机名。

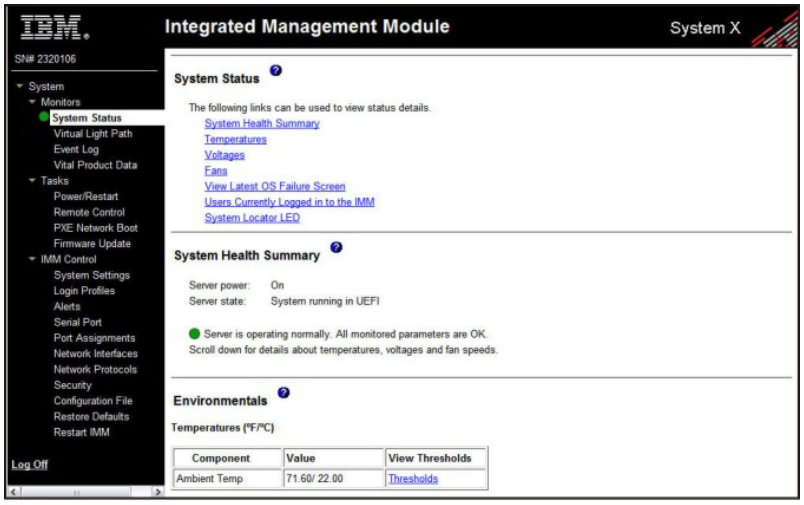


2. 在 IMM Login 窗口中输入用户名和密码。如果您是首次使用 IMM，那么可以从系统管理员处获取用户名和密码。所有登录尝试都记录在事件日志中。根据系统管理员配置用户标识的方式，可能需要输入新密码。
3. 在 Welcome Web 页面上，从提供的字段内的下拉列表中选择超时值。如果浏览器在该分钟数内不活动，那么 IMM 会将您从 Web 界面中注销。

   注：根据系统管理员配置全局登录设置的方式，超时值可能是固定值。



4. 单击 **Continue** 以启动会话。浏览器会打开 System Status 页面，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。



有关可以通过 IMM Web 界面左导航窗格中的链接执行的操作的描述，请参阅『IMM 操作描述』。然后，转至第 17 页的第 3 章，『配置 IMM』。

IMM 操作描述

表 2 列示了您登录到 IMM 后的可用操作。

表 2. IMM 操作

链接	操作	描述
System Status	查看服务器的系统运行状况，查看操作系统故障屏幕捕获，并查看 IMM 中的已登录用户。	您可以在 System Health 页面上监控服务器电源和运行状况状态，以及服务器的温度、电压和风扇状态。您还可以查看最新操作系统故障屏幕捕获的图像和 IMM 中的已登录用户。
Virtual Light Path	查看服务器光通路上每个指示灯的名称、颜色和状态	Virtual Light Path 页面显示服务器上指示灯的当前状态。
Event Log	查看远程服务器的事件日志	Event Log 页面包含机箱事件日志中当前存储的条目。该日志包括由 BMC 报告的事件的文本描述，以及有关所有远程访问尝试和配置更改的信息。该日志中的所有事件都带有使用 IMM 日期和时间设置的时间戳记。某些事件还会生成警报（如果它们在 Alerts 页面上的配置如此）。您可以对事件日志中的事件进行排序和过滤。
Vital Product Data	查看服务器重要产品数据 (VPD)	IMM 收集服务器信息、服务器固件信息和服务器组件 VPD。此数据在 Vital Product Data 页面上提供。
Power/Restart	远程开启或重新启动服务器	通过开机、关机和重新启动操作，IMM 通过您的服务器提供完全远程电源控制。此外，还会捕获并显示开机和重新启动统计信息以显示服务器硬件可用性。
Remote Control	重定向服务器视频控制台，并将您计算机的磁盘驱动器或磁盘映像作为服务器上的驱动器使用	在 Remote Control 页面中，您可以启动远程控制功能部件。通过远程控制，您可以通过自己的计算机查看服务器控制台，并且可以将您计算机上的一个磁盘驱动器（例如，CD-ROM 驱动器或软盘驱动器）安装在服务器上。您可以使用自己的鼠标和键盘与服务器交互并控制服务器。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。已安装的磁盘显示为与服务器连接的 USB 磁盘驱动器。
PXE Network Boot	将主机服务器下次重新启动的启动（引导）顺序更改为尝试预引导执行环境 (PXE)/动态主机配置协议 (DHCP) 网络启动	如果您的服务器固件和 PXE 引导代理实用程序定义正确，那么您可在 PXE Network Boot 页面中将主机服务器下次重新启动的启动（引导）顺序更改为尝试 PXE/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。在下次重新启动时，将取消选中 PXE Network Boot 页面上的复选框。
Firmware Update	更新 IMM 上的固件	使用 Firmware Update 页面上的选项可更新 IMM 固件、服务器固件和 DSA 固件。
System Settings	查看及更改 IMM 服务器设置	在 System Settings 页面中，您可以配置服务器位置和常规信息，例如，IMM 的名称、服务器超时设置和 IMM 的联系信息。
	设置 IMM 时钟	您可以设置用于为事件日志中的条目创建时间戳记的 IMM 时钟。
	启用或禁用 USB 频带内接口	您可以启用或禁用 USB 频带内（或 LAN over USB）接口

表 2. IMM 操作 (续)

链接	操作	描述
Login Profiles	配置 IMM 登录概要文件和全局登录设置	您可以定义最多 12 个用于启用 IMM 访问权的登录概要文件。您还可以定义适用于所有登录概要文件的全局登录设置，包括启用轻量级目录访问协议 (LDAP) 服务器认证和定制帐户安全性级别。
Alerts	配置远程警报和远程警报接收方	您可以将 IMM 配置为针对不同事件生成警报并转发警报。在 Alerts 页面上，您可以配置受监控的警报和不通知的接收方。
	配置简单网络管理协议 (SNMP) 事件	您可以设置将针对其发送 SNMP 陷阱的事件类别。
	配置警报设置	您可以建立适用于所有远程警报接收方的全局设置，例如，警报重试次数和重试之间的延迟。
Serial Port	配置 IMM 串口设置	在 Serial Port 页面中，您可以配置串行重定向功能使用的串口波特率。您还可以配置用于在串行重定向和命令行界面 (CLI) 方式之间切换的键序列。
Port assignments	更改 IMM 协议的端口号	在 Port Assignments 页面中，您可以查看并更改向 IMM 协议（例如，HTTP、HTTPS、Telnet 和 SNMP）分配的端口号。
Network Interfaces	配置 IMM 的网络接口	在 Network Interfaces 页面中，您可以为 IMM 上的以太网连接配置网络访问设置。
Network Protocols	配置 IMM 的网络协议	在 Network Protocols 页面上，您可以配置 IMM 使用的简单网络管理协议 (SNMP)、域名系统 (DNS) 和简单电子邮件传输协议 (SMTP) 设置。您还可以配置 LDAP参数.
Security	配置安全套接字层 (SSL)	您可以启用或禁用 SSL 并管理所使用的 SSL 证书。您还可以启用或禁用用于与 LDAP 服务器连接的 SSL 连接。
	启用 Secure Shell (SSH) 访问权	您可以启用对 IMM 的 SSH 访问。
Configuration File	备份及恢复 IMM 配置	在 Configuration File 页面中，您可以备份、修改和恢复 IMM 的配置并查看配置摘要。
Restore Default Settings	恢复 IMM 缺省设置	警告： 当单击 **Restore Defaults** 时，您对 IMM 所作的所有修改都将丢失。 您可以将 IMM 的配置重置为出厂缺省值。
Restart IMM	重新启动 IMM	您可以重新启动 IMM。
Scalable Partitioning	将服务器配置为可扩展复合体中的一个分区。	如果在可扩展复合体中配置服务器，那么 IMM 允许您控制复合体中的系统。如果服务器扩展有问题，IMM 将报告错误。
Service Advisor	将服务性事件代码转发给 IBM 支持人员	启用后，Service Advisor 将允许 IMM 将服务性事件代码转发给 IBM 支持人员，以进一步进行故障诊断。 注：请参阅服务器的文档以查看您的服务器是否支持此功能部件。
Log off	注销 IMM	您可以注销 IMM 连接。

您可以单击 **View Configuration Summary** 链接（此链接在大部分页面上位于右上角），以快速查看 IMM 的配置。

第 3 章 配置 IMM

使用导航窗格中 **IMM Control** 下方的链接来配置 IMM。

在 System Settings 页面中，可执行以下操作：
- 设置服务器信息
- 设置服务器超时
- 设置 IMM 日期和时间
- 启用或禁用针对 USB 接口的命令

在 Login Profiles 页面中，可执行以下操作：
- 设置登录概要文件，以控制对 IMM 的访问权
- 配置全局登录设置，例如多次登录尝试失败后的锁定期
- 配置帐户安全性级别

在 Alerts 页面中，可执行以下操作：
- 配置远程警报接收方
- 设置远程警报尝试次数
- 选择警报之间的延迟
- 选择要发送的警报及其转发方式

在 Serial Port 页面中，可执行以下操作：
- 为串行重定向配置串口 2 (COM2) 的波特率
- 指定用于在串行重定向和命令行界面 (CLI) 之间切换的击键序列

在 Port Assignments 页面中，您可以更改 IMM 服务的端口号。

在 Network Interfaces 页面中，您可以为 IMM 设置以太网连接。

在 Network Protocols 页面中，可以配置以下方面：
- SNMP 设置
- DNS 设置
- Telnet 协议
- SMTP 设置
- LDAP 设置
- 服务位置协议

在 Security 页面中，您可以安装和配置安全套接字层 (SSL) 设置。

在 Configuration File 页面中，您可以备份、修改和恢复 IMM 的配置。

在 Restore Defaults 页面中，您可以将 IMM 配置重置为出厂缺省值。

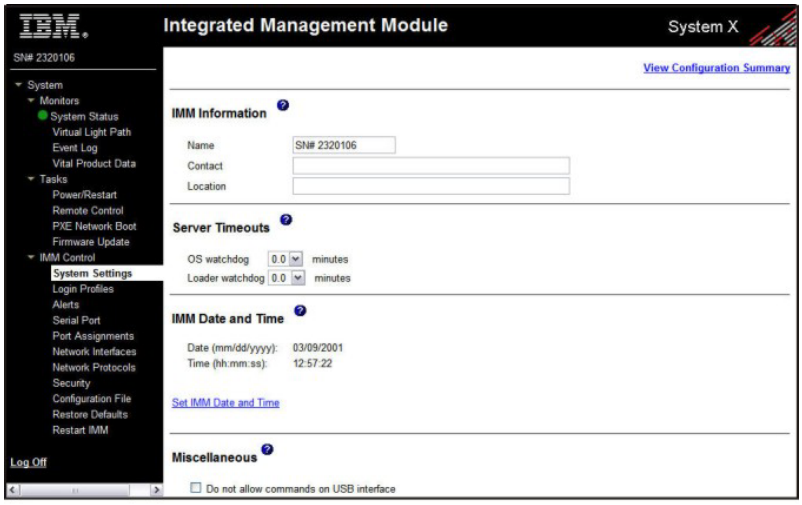
在 Restart IMM 页面中，您可以重新启动 IMM。

设置系统信息

要设置 IMM 系统信息，请完成以下步骤：

1. 登录到要在其之上设置系统信息的 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **System Settings**。此时会显示一个类似于下图中的页面。

   注：System Settings 页面中的可用字段由受访问的远程服务器确定。



3. 在 **IMM Information** 区域内的 **Name** 字段中，输入 IMM 的名称。使用 **Name** 字段为此服务器中的 IMM 指定名称。名称随附于电子邮件和 SNMP 警报通知，以识别警报源。

   注：您的 IMM 名称（在 **Name** 字段中）和 IMM 的 IP 主机名（在 Network Interfaces 页面上的 **Hostname** 字段中）不自动共享同一名称，因为 **Name** 字段限制为 16 个字符。**Hostname** 字段可以包含最多 63 个字符。要尽量减少混淆，请将 **Name** 字段设置为 IP 主机名的非限定部分。非限定 IP 主机名由标准 IP 主机名的第一个句点前的内容组成。例如，对于标准 IP 主机名 imm1.us.company.com，非限定 IP 主机名为 imm1。有关主机名的信息，请参阅第 33 页的『配置网络接口』。
4. 在 **Contact** 字段中，输入联系人信息。例如，可以指定此服务器发生问题情况下要联系的个人的姓名和电话号码。可以在此字段中输入最多 47 个字符。
5. 在 **Location** 字段中，输入服务器的位置。请在此字段中包含足够的详细信息，以快速找到用于维护或其他用途的服务器。可以在此字段中输入最多 47 个字符。
6. 滚动到页面底部并单击 **Save**。

设置服务器超时

注：服务器超时要求启用频带内 USB 接口（或 LAN over USB）以允许使用命令。有关为 USB 接口启用和禁用命令的更多信息，请参阅第 21 页的『禁用 USB 频带内接口』。有关必需设备驱动程序的安装的信息，请参阅第 114 页的『安装设备驱动程序』。

要设置服务器超时值，请完成以下步骤：

1. 登录到要在其之上设置服务器超时的 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **System Settings** 并向下滚动到 **Server Timeouts** 区域。

   您可以设置 IMM 以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 IMM 自动响应的事件对应的服务器超时。

   操作系统看守程序

   使用 **OS watchdog** 字段指定由 IMM 执行的操作系统检查之间间隔的分钟数。如果操作系统未能响应这些检查之一，那么 IMM 将生成操作系统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。

   要设置操作系统看守程序值，请从菜单中选择一个时间间隔。要关闭此看守程序，请从菜单中选择 **0.0**。要捕获操作系统故障屏幕，必须在 **OS watchdog** 字段中启用看守程序。

   装入程序看守程序

   使用 **Loader watchdog** 字段指定 IMM 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 IMM 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 IMM 等待操作系统启动完成的时间限制。要关闭此看守程序，请从菜单中选择 **0.0**。

   关机延迟

   使用 **Power off delay** 字段指定 IMM 在关闭服务器电源（如果操作系统本身未关闭电源）之前等待操作系统关机的分钟数。如果设置关机延迟，那么可以确保操作系统在服务器电源关闭之前有足够时间进行正常关机。要确定服务器的关机延迟，请关闭服务器并观察其关机所用的时间量。向该值添加时间缓冲并使用生成的数字作为关机延迟设置。

   要设置关机延迟值，请从菜单中选择所需时间值。值为 X'0' 意味着由操作系统而不是 IMM 关闭服务器电源。
4. 滚动到页面底部并单击 **Save**。

设置 IMM 日期和时间

IMM 使用其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。

注：IMM 日期和时间设置仅影响 IMM 时钟而不影响服务器时钟。IMM 实时时钟和服务器时钟是分离的单独时钟，并且可以设置为不同时间。要将 IMM 时钟与服务器时钟同步，请转至页面的 **Network Time Protocol** 区域，然后将 NTP 服务器主机名或 IP 地址设置为用于设置服务器时钟的同一服务器主机名或 IP 地址。有关更多信息，请参阅第 20 页的『同步网络中的时钟』。

电子邮件和 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 (DST)，从而为在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。

要验证 IMM 的日期和时间设置，请完成以下步骤：

1. 登录到要在其之上设置 IMM 日期和时间值的 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **System Settings** 并向下滚动到 **IMM Date and Time** 区域，这会显示生成 Web 页面时的日期和时间。
3. 要覆盖日期和时间设置以及启用夏令时 (DST) 和格林威治标准时间 (GMT) 偏移，请单击 **Set IMM Date and Time**。此时会显示一个类似于下图中的页面。

4. 在 **Date** 字段中，输入当前月、日和年的数字。
5. 在 **Time** 字段中，输入与适用输入字段中的当前小时、分钟和秒对应的数字。小时 (hh) 必须是按照 24 小时时钟所表示的 00 - 23 之间的数字。分钟 (mm) 和秒 (ss) 必须是 00 - 59 之间的数字。
6. 在 **GMT offset** 字段中，选择用于指定从格林威治标准时间 (GMT) 的偏移（以小时为单位），对应于服务器所在的时区。
7. 选中或清除 **Automatically adjust for daylight saving changes** 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 IMM 时钟是否自动调整。
8. 单击 **Save**。

同步网络中的时钟

网络时间协议 (NTP) 提供通过计算机网络来同步时钟的方法，从而使任何 NTP 客户机都可从 NTP 服务器获取正确的时间。

IMM NTP 功能提供将 IMM 实时时钟与 NTP 服务器所提供的时间同步的方法。您可以指定要使用的 NTP 服务器，指定与 IMM 同步的频率，启用或禁用 NTP 功能以及请求立即时间同步。

NTP 功能不提供通过 NTP V3 和 NTP V4 中的加密算法来提供的扩展安全性和认证。IMM NTP 功能仅支持不带认证的简单网络时间协议 (SNTP)。

要设置 IMM NTP 功能设置，请完成以下步骤：

1. 登录到要在其之上同步网络中的时钟的 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **System Settings** 并向下滚动到 **IMM Date and Time** 区域。
3. 单击 **Set IMM Date and Time**。此时会显示一个类似于下图中的页面。

4. 在 **Network Time Protocol (NTP)** 下，可从以下设置中进行选择：

   NTP auto-synchronization service
   使用此选项以启用或禁用 IMM 时钟与 NTP 服务器的自动同步。

   NTP server host name or IP address
   使用此字段以指定要用于时钟同步的 NTP 服务器的名称。

   NTP update frequency
   使用此字段以指定同步请求之间的大致时间间隔（以分钟为单位）。输入 3 - 1440 分钟之间的值。

   Synchronize Clock Now
   单击此按钮以请求立即同步而不是等待时间间隔过去。

5. 单击 **Save**。

禁用 USB 频带内接口

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 IMM 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 IMM Web 界面上的 Firmware Update 选项来更新固件。有关更多信息，请参阅第 109 页的『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。有关更多信息，请参阅第 18 页的『设置服务器超时』。

USB 频带内接口或 LAN over USB 用于与 IMM 的频带内通信。要防止在服务器上运行的任何应用程序请求 IMM 执行任务，必须禁用 USB 频带内接口。有关 LAN over USB 的更多信息，请参阅第 113 页的第 6 章，『LAN over USB』。

要禁用 USB 频带内接口，请完成以下步骤：

1. 登录到要在其之上禁用 USB 设备驱动程序接口的 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **System Settings** 并向下滚动到 **Miscellaneous** 区域。此时会显示一个类似于下图中的页面。

3. 要禁用 USB 频带内接口，请从 **Allow commands on the USB interface** 列表中选择 **Disabled**。选择该选项不会对 USB 远程存在功能（例如键盘、鼠标和大容量存储器）产生影响。禁用 USB 频带内接口时，频带内系统管理应用程序（如 Advanced Settings Utility (ASU) 和固件更新包实用程序）可能不工作。

   注：如果安装了 IPMI 设备驱动程序，ASU 可以在禁用 USB 频带内接口的情况下使用。
   如果在禁用频带内接口时尝试使用系统管理应用程序，那么这些应用程序可能不会运行。
4. 单击 **Save**。

要在禁用 USB 设备驱动程序接口后将其启用，请清除 **Do not allow commands on USB interface** 复选框并单击 **Save**。

注：

1. USB 频带内接口也称为“LAN over USB”，并且在第 113 页的第 6 章，『LAN over USB』中进行了更详细的描述。
2. 尝试对一些 Linux 分发版进行网络安装时，如果启用了 IMM USB 频带内接口，那么安装可能会失败。有关更多信息，请访问 http://rhn.redhat.com/errata/RHBA-2009-0127.html。
3. 如果执行的网络安装不包含先前备注 2 中描述的 Red Hat Web 站点上的更新，那么在执行安装之前必须禁用 USB 频带内接口，并且在安装完成后将其启用。
4. 有关 LAN over USB 接口的配置的信息，请参阅第 114 页的『手动配置 LAN over USB 接口』。

创建登录概要文件

使用 Login Profiles 表查看、配置或更改个别登录概要文件。使用 Login ID 列中的链接以配置个别登录概要文件。您可以定义最多 12 个唯一概要文件。Login ID 列中的各链接以所配置的关联概要文件登录标识进行标示。

某些登录概要文件与 IPMI 用户标识进行共享，从而提供一组适用于所有 IMM 用户界面（包括 IPMI）的本地用户帐户（用户名/密码）。以下列表中描述了与这些共享登录概要文件有关的规则：

- IPMI 用户标识 1 始终是空用户。
- IPMI 用户标识 2 映射到登录标识 1，IPMI 用户标识 3 映射到登录标识 2，依此类推。
- 对于 IPMI 用户标识 2 和登录标识 1，IMM 缺省用户设置为 `USERID` 和 `PASSW0RD`（包含数字 0 而不是字母 O）。

例如，如果通过 IPMI 命令添加用户，那么该用户信息也可用于通过 Web、Telnet、SSH 和其他界面进行认证。相反，如果在 Web 或其他界面上添加用户，那么该用户信息可用于启动 IPMI 会话。

由于用户帐户与 IPMI 进行共享，因此会实施某些限制以在使用这些帐户的界面之间提供共同之处。以下列表描述了 IMM 和 IPMI 登录概要文件限制：

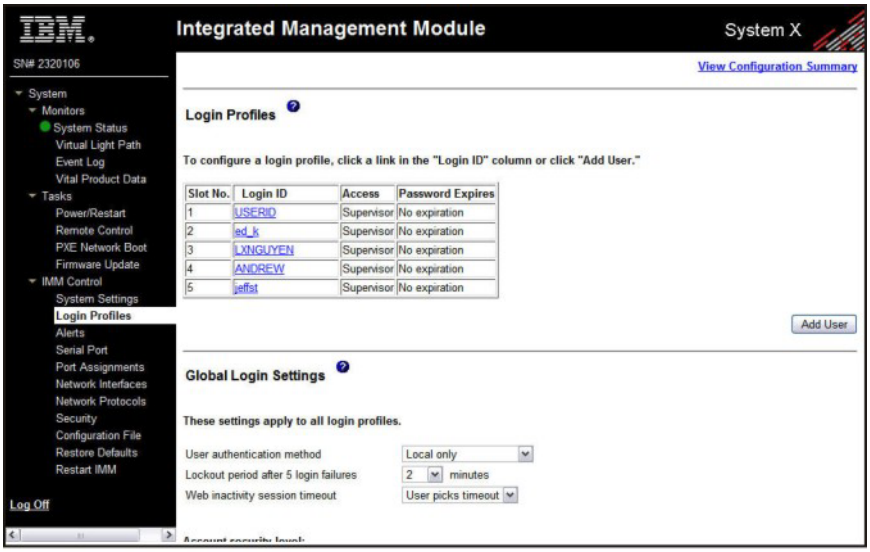
- IPMI 允许最多 64 个用户标识。IMM IPMI 实施仅允许 12 个用户帐户。
- IPMI 允许匿名登录（空用户名和空密码），但 IMM 不允许。

- IPMI 允许多个具有相同用户名的用户标识，但 IMM 不允许。
- 要求将用户名从当前名称更改为同一当前名称的 IPMI 请求会返回 `invalid parameter` 完成代码，因为所请求的用户名已在使用中。
- IMM 的最大 IPMI 密码长度为 16 字节。
- 以下字受限制且不可用作本地 IMM 用户名：
  - immroot
  - nobody
  - ldap
  - lighttpd
  - sshd
  - daemon
  - immftp

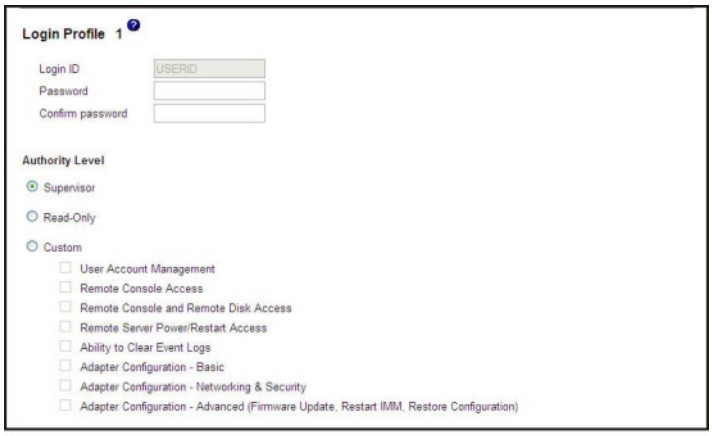
要配置登录概要文件，请完成以下步骤：

1. 登录到要在其之上创建登录概要文件的 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **Login Profiles**。

   注：如果您尚未配置概要文件，那么它不会出现在 Login Profiles 表中。
   Login Profiles 页面显示了各登录标识、登录访问级别和密码到期信息，如下图所示。



   要点：缺省情况下，IMM 使用一个登录概要文件进行了配置，该概要文件使用登录用户标识 `USERID` 和密码 `PASSWORD` 启用远程访问（0 表示零，而不是字母 O）。要避免潜在安全漏洞，请在 IMM 的初始设置期间更改此缺省登录概要文件。
3. 单击 **Add User**。此时会显示一个类似于下图的个别概要文件页面。



4. 在 **Login ID** 字段中，输入概要文件的名称。可以在 **Login ID** 字段中输入最多 16 个字符。有效字符为大写和小写字母、数字、句点和下划线。

   注：此登录标识用于授予对 IMM 的远程访问权。

5. 在 **Password** 字段中，向登录标识分配密码。密码必须包含最少五个字符，其中一个必须是非字母字符。接受空密码。

   注：此密码与登录标识结合使用以授予对 IMM 的远程访问权。

6. 在 **Confirm password** 字段中，再次输入该密码。
7. 在 **Authority Level** 区域中，选择以下选项之一来为此登录标识设置访问权：

   Supervisor

   用户没有任何限制。

   Read Only

   用户仅具有只读访问权，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

   如果选择 Custom 选项，那么必须选择以下一个或多个定制权限级别：

   - **User Account Management:** 用户可以添加、修改或删除用户并在 Login Profiles 页面中更改全局登录设置。
   - **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:** 用户可以访问远程服务器的开机和重新启动功能。这些功能在 Power/Restart 页面中可用。
   - **Ability to Clear Event Logs:** 用户可以清除事件日志。每个人都可查看事件日志，但是必需具有此特定许可权才能清除日志。
   - **Adapter Configuration - Basic:** 用户可以在 System Settings 和 Alerts 页面中修改配置参数。
   - **Adapter Configuration - Networking & Security:** 用户可以在 Security、Network Protocols、Network Interface、Port Assignments 和 Serial Port 页面中修改配置参数。

- **Adapter Configuration - Advanced:** 用户在配置 IMM 时没有任何限制。此外，用户被假定对 IMM 具有管理访问权，意味着用户还可执行以下高级功能：固件更新、PXE 网络引导、复原 IMM 出厂缺省值、根据配置文件修改和复原 IMM 配置以及重新启动和重置 IMM。

当用户设置 IMM 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 IMM 登录标识授权级别设置为 Supervisor，那么 IPMI 特权级别会设置为 Administrator。
- 如果用户将 IMM 登录标识授权级别设置为 Read Only，那么 IPMI 特权级别会设置为 User
- 如果用户将 IMM 登录标识授权级别设置为具有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 IMM 登录标识授权级别设置为具有 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 IMM 登录标识授权级别设置为具有 Adapter Configuration (Basic)，那么 IPMI 特权级别会设置为 User。

注：要将登录概要文件返回到出厂缺省值，请单击 **Clear Login Profiles**。

8. 在 **Configure SNMPv3 User** 区域中，如果用户应通过 SNMPv3 协议对 IMM 具有访问权，请选中该复选框。单击该复选框后，会出现一个类似于下图中的页面区域。

使用以下字段来为用户概要文件配置 SNMPv3 设置：

Authentication Protocol

使用此字段以指定 **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散列算法。Linux 帐户的密码将用于认证。如果选择 **None**，那么不会使用认证协议。

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

使用此字段以指定加密密码。

Confirm Privacy Password

使用此字段以确认加密密码。

Access Type

使用此字段以指定 **Get** 或 **Set** 作为访问类型。具有访问类型 Get 的 SNMPv3 用户只能执行查询操作。通过访问类型 Set，SNMPv3 用户可执行查询操作和修改设置（例如，为用户设置密码）。

Hostname/IP address for traps

使用此字段来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）。

9. 单击 **Save** 以保存登录标识设置。

删除登录概要文件

要删除登录概要文件，请完成以下步骤：

1. 登录到要为其创建登录概要文件的 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **Login Profiles**。Login Profiles 页面显示了各登录标识、登录访问级别和密码到期信息。
3. 单击要删除的登录概要文件。此时会显示该用户的 Login Profile 页面。
4. 单击 **Clear Login Profile**。

配置全局登录设置

完成以下步骤以设置适用于 IMM 的所有登录概要文件的条件：

1. 登录到要为其设置全局登录设置的 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **Login Profiles**。
3. 向下滚动到 **Global Login Settings** 区域。此时会显示一个类似于下图中的页面。

4. 在 **User authentication method** 字段中，指定如何认证尝试登录的用户。选择以下认证方法之一：
   - **Local only:** 通过搜索 IMM 的本地表来认证用户。如果没有匹配的用户标识和密码，那么会拒绝访问。将向已成功认证的用户分配第 22 页的『创建登录概要文件』中配置的权限级别。
   - **LDAP only:** IMM 尝试通过使用 LDAP 服务器来认证用户。通过此认证方法，绝不会搜索 IMM 上的本地用户表。
   - **Local first, then LDAP:** 首先尝试本地认证。如果本地认证失败，那么会尝试 LDAP 认证。
   - **LDAP first, then Local:** 首先尝试 LDAP 认证。如果 LDAP 认证失败，那么会尝试本地认证。

   注：

   a. 仅与 IPMI 界面共享本地管理的帐户，因为 IPMI 不支持 LDAP 认证。

   b. 即使 **User authentication method** 字段设置为 **LDAP only**，用户也可通过使用本地管理的帐户登录到 IPMI 界面。
5. 在 **Lockout period after 5 login failures** 字段中，指定在检测到连续五次远程登录失败的情况下 IMM 禁止远程登录尝试的时间长度（以分钟为单位）。锁定一个用户无法阻止其他用户登录。
6. 在 **Web inactivity session timeout** 字段中，指定 IMM 在断开与不活动 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。如果用户将在登录过程中选择超时期，请选择 **User picks timeout**。
7. （可选）在 **Account security level** 区域中，选择密码安全性级别。**Legacy security settings** 和 **High security settings** 按需求列表中所指示来设置缺省值。
8. 要定制安全性设置，请选择 **Custom security settings** 以查看和更改帐户安全性管理配置。

   User login password required

   使用此字段以指示是否允许使用没有密码的登录标识。

   Number of previous passwords that cannot be used

   使用此字段以指示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。

Maximum Password Age

使用此字段以指示必须更改密码之前允许的最长密码寿命。支持范围在 0 - 365 天内的值。选择 **0** 以禁用密码到期检查。

9. 单击 **Save**。

配置远程警报设置

您可以通过导航窗格中的 **Alerts** 链接来配置远程警报接收方、警报尝试次数、触发远程警报的事件，以及本地警报。

在您配置远程警报接收方之后，当发生从 Monitored Alerts 组中选择的任何事件时，IMM 都会通过网络连接向该接收方发送警报。该警报包含有关事件性质、事件的时间和日期，以及生成该警报的系统名称的信息。

注：如果 **SNMP Agent** 或 **SNMP Traps** 字段未设置为 **Enabled**，那么不会发送 SNMP 陷阱。有关这些字段的信息，请参阅第 38 页的『配置 SNMP』。

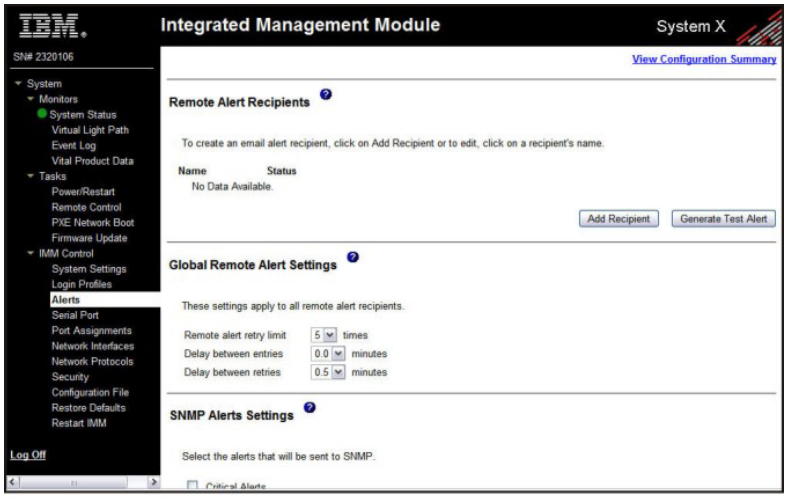
配置远程警报接收方

您可以定义最多 12 个唯一远程警报接收方。警报接收方的各链接以接收方名称和警报状态进行标示。

注：如果您尚未配置警报接收方概要文件，那么该概要文件不会出现在远程警报接收方列表上。

要配置远程警报接收方，请完成以下步骤：

1. 登录到要为其配置远程警报设置的 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **Alerts**。此时会显示 Remote Alert Recipients 页面。您可以查看各接收方的通知方法和警报状态（如果已设置）。



3. 单击其中一个远程警报接收方链接或者单击 **Add Recipient**。此时会显示一个单独的类似于下图的接收方窗口。

4. 在 **Status** 字段中，单击 **Enabled** 以激活远程警报接收方。
5. 在 **Name** 字段中，输入接收方的名称或其他标识。您输入的名称在 Alerts 页面上显示为接收方的链接。
6. 在 **E-mail address** 字段中，输入警报接收方的电子邮件地址。
7. 使用复选框以包含带有电子邮件警报的事件日志。
8. 在 **Monitored Alerts** 字段中，选择发送到警报接收方的警报类型。远程警报按以下严重性级别分类：

   紧急警报
   对于表明服务器组件不再运作的事件会生成紧急警报。

   警告警报
   对于可能进展到严重级别的事件会生成警告警报。

   系统警报
   对于由于系统错误或配置更改而发生的事件会生成系统警报。

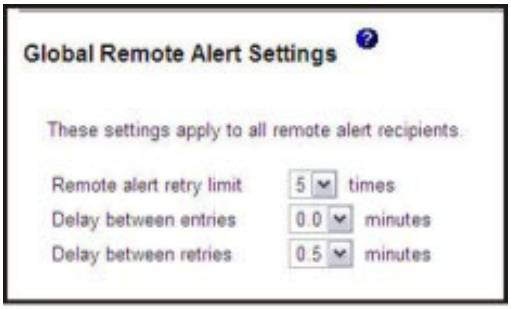
   所有警报都存储在事件日志中并会发送到所有已配置的远程警报接收方。
9. 单击 **Save**。

配置全局远程警报设置

全局远程警报设置仅适用于已转发的警报。

完成以下步骤以设置 IMM 尝试发送警报的次数：

1. 登录到要在其之上设置远程警报尝试次数的 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **Alerts** 并向下滚动到 **Global Remote Alert Settings** 区域。



使用这些设置定义远程警报尝试次数和尝试间隔的时间长度。这些设置仅适用于所有已配置的远程警报接收方。

Remote alert retry limit

使用 **Remote alert retry limit** 字段指定 IMM 尝试向接收方发送警报的附加次数。IMM 不发送多个警报；仅在 IMM 尝试发送初始警报时发生故障的情况下，才会进行其他警报尝试。

注：此警报设置不适用于 SNMP 警报。

Delay between entries

使用 **Delay between entries** 字段指定 IMM 在向列表中的下一个接收方发送警报之前等待的时间间隔（以分钟为单位）。

Delay between retries

使用 **Delay between retries** 字段指定 IMM 在前后两次重试向接收方发送警报期间等待的时间间隔（以分钟为单位）。

3. 滚动到页面底部并单击 **Save**。

配置 SNMP 警报设置

SNMP 代理通过 SNMP 陷阱来通知 IMM 有关事件的信息。您可以将 SNMP 配置为根据事件类型来过滤事件。可供过滤的事件类别为 Critical、Warning 和 System。SNMP 警报设置对于所有 SNMP 陷阱而言为全局设置。

注：

1. IMM 提供两个管理信息库 (MIB) 文件以用于 SNMP 应用程序。MIB 文件包含在 IMM 固件更新包中。
2. IMM 支持 SNMPv1 和 SNMPv3 标准。

完成以下步骤以选择发送到 SNMP 的一个或多个警报类型：

1. 登录到要在其之上设置远程警报尝试次数的 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **Alerts** 并向下滚动到 **SNMP Alerts Settings** 区域。
3. 选择一个或多个警报类型。远程警报按以下严重性级别分类：
   - 临界
   - 警告
   - 系统
4. 滚动到页面底部并单击 **Save**。

配置串口设置

IMM 提供两个用于串行重定向的串口。

System x 服务器上的串口 1 (COM1) 用于 IPMI Serial over LAN (SOL)。只能通过 IPMI 界面配置 COM1。

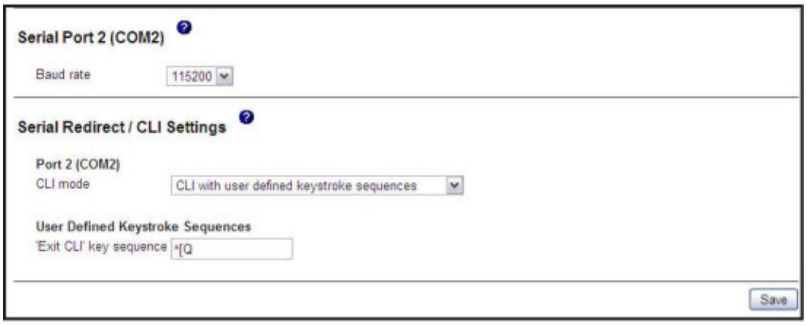
在刀片服务器上，串口 2 (COM2) 用于 SOL。在 System x 服务器上，COM2 用于通过 Telnet 或 SSH 进行串行重定向。COM2 不可通过 IPMI 界面进行配置。在机架式安装和塔式服务器上，COM2 是不提供外部访问机制的内部 COM 端口。

这两个串口均使用 8 个数据位、空奇偶性校验和 1 个停止位。可以选择波特率为 9600、19200、38400、57600、115200 和 230400。

您可以为 IMM 中的 COM2 端口配置串行重定向和命令行界面。

要配置串行数据传输率和重定向，请完成以下步骤：

1. 登录到要在其之上配置串口的 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **Serial Port**。此时会显示一个类似于下图中的页面。



3. 在 **Baud rate** 字段中，选择与要用于串行重定向的服务器 COM 端口的速率匹配的数据传输率。使用 **Baud rate** 字段指定串口连接的数据传输率。要设置波特率，请选择与串口连接对应的数据传输率（位/秒）。
4. 在 **Serial Redirect/CLI Settings** 区域中的 **CLI mode** 字段内，如果您要使用 Microsoft Windows Server 2003 Emergency Management Services (EMS) 兼容键序列来退出串行重定向操作，请选择 **CLI with EMS compatible keystroke sequences**；如果您要使用自己的键序列，请选择 **CLI with user defined keystroke sequences**。

   注：如果选择 **CLI with user defined keystroke sequences**，那么必须定义键序列。

   在串行重定向启动后，它会继续运行直至用户输入出口键序列为止。当输入了出口键序列时，串行重定向停止，并且用户会返回到 Telnet 或 SSH 会话中的命令方式。使用此字段以指定出口键序列。
5. 单击 **Save**。

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 IMM 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. IMM 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. 命令行界面 **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 Q
```

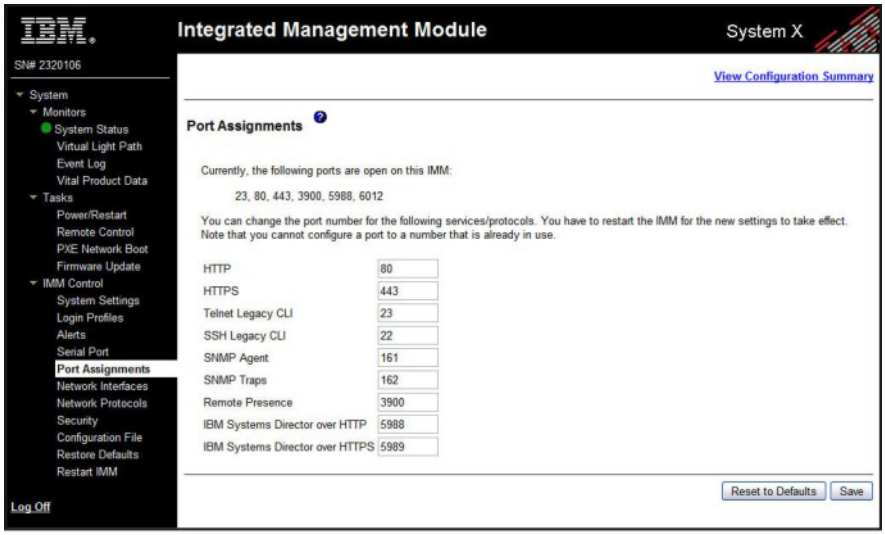
输入出口键序列以返回到命令行界面。在此示例中，按 Esc 键，然后输入 q。

```
Back to LegacyCLI console....
```

配置端口分配

要更改 IMM 服务的端口号，请完成以下步骤：

1. 登录到要在其之上配置端口分配的 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **Port Assignments**。此时会显示一个类似于下图中的页面。



3. 使用以下信息为字段赋值：

HTTP 这是 IMM 的 HTTP Server 的端口号。缺省端口号为 80。其他有效值在范围 1 - 65535 内。如果更改此端口号，那么必须在 Web 地址末尾添加此端口号，前置冒号。例如，如果 HTTP 端口更改为 8500，请输入 `http://hostname:8500/` 以打开 IMM Web 界面。请注意，必须在 IP 地址和端口号之前输入前缀 `http://`。

HTTPS

这是用于 Web 界面 HTTPS (SSL) 流量的端口号。缺省值为 443。其他有效值在范围 1 - 65535 内。

Telnet Legacy CLI

这是供 Legacy CLI 通过 Telnet 服务进行登录的端口号。缺省值为 23。其他有效值在范围 1 - 65535 内。

SSH Legacy CLI
这是为 Legacy CLI 配置以通过 SSH 进行登录的端口号。缺省值为 22。

SNMP Agent
这是在 IMM 上运行的 SNMP 代理的端口号。缺省值为 161。其他有效值在范围 1 - 65535 内。

SNMP Traps
这是用于 SNMP 陷阱的端口号。缺省值为 162。其他有效值在范围 1 - 65535 内。

Remote Presence
这是远程控制功能部件用于查看服务器控制台并与其交互的端口号。对于机架式安装和塔式服务器，缺省值为 3900。

注：BladeCenter 上的并发键盘、视频和鼠标 (Concurrent Keyboard, Video, and Mouse, cKVM) 功能部件要求端口号为 2068。请勿在刀片服务器上更改此端口号。

IBM Systems Director over HTTP
这是 IBM Systems Director 用于与服务器控制台交互的端口号。缺省值为 5988。

IBM Systems Director over HTTPS
这是 IBM Systems Director 用于通过 SSL 与服务器控制台交互的端口号。缺省值为 5989。

以下端口号已保留且只能用于对应的服务。

表 3. 保留端口号

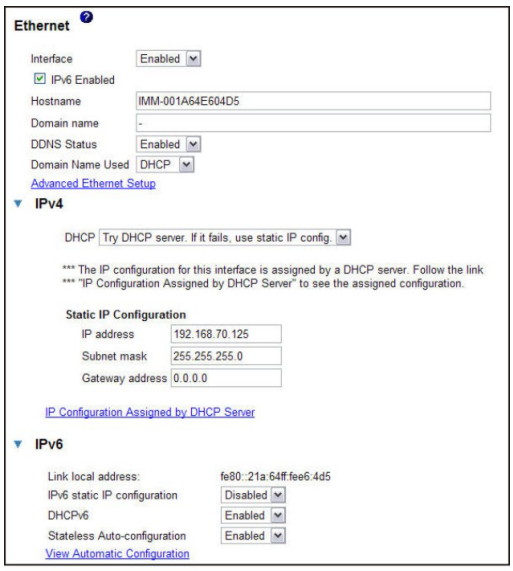
端口号	服务用于
427	SLP
7070 到 7077	分区管理

4. 单击 **Save**。

配置网络接口

在 Network Interfaces 页面上，您可以通过配置与 IMM 的以太网连接来设置对 IMM 的访问。要为 IMM 配置以太网设置，请在必要情况下修改 Network Interfaces 页面中的 Ethernet、IPv4 或 IPv6 区域中的设置。以下部分中描述了各区域中的设置。

注：以下图像中的值为示例。您的设置将会不同。



要查看所有当前配置设置的摘要，请单击 Network Interfaces 页面上的 **View Configuration Summary**。在 Network Interfaces 页面上配置设置之前，请复审以下部分中的信息。

注：您也可以通过 Setup Utility 来配置 IMM 网络连接。有关更多信息，请参阅第 11 页的『通过 IBM System x 服务器固件 Setup Utility 设置 IMM 网络连接』。

配置以太网设置

在 Network Interfaces 页面的 Ethernet 区域中，可以修改以下设置。

Interface

使用此字段可启用或禁用此网络接口。要允许通过此网络接口进行网络连接，请选择 **Enabled**。

IPv6 Enabled

使用此复选框可在 IMM 上启用或禁用 IPv6 支持。

注：如果您取消选中 **IPv6 Enabled** 复选框，那么会显示 **Hide all IPv6 configuration fields when IPv6 is disabled** 复选框。如果选中该新复选框，Web 界面上会隐藏 Network Interfaces 页面上的 IPv6 区域。

Hostname

使用此字段可为 IMM 子系统定义唯一主机名。您最多可以在此字段中输入 63 个字符。主机名只能由字母数字字符、连字符和下划线组成。

注：缺省情况下，主机名为 IMM-，后跟烧录 MAC 地址。

Domain name

使用此字段可定义 DNS 域名。

DDNS Status

使用此字段可启用或禁用动态 DNS (DDNS)。DDNS 使 IMM 能够通知 DNS

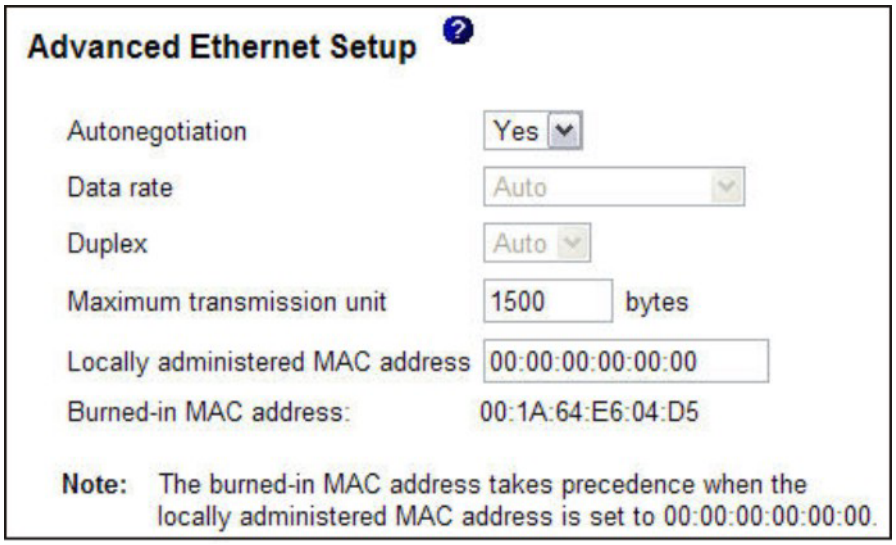
服务器实时更改其所配置的主机名、地址或 DNS 中存储的其他信息的活动 DNS 配置。启用 DDNS 后，IMM 会通知 DNS 服务器通过 DHCP 服务器或通过自身配置接收到的 IP 地址。

Domain Name Used

使用此字段可选择在启用了 DDNS 的情况下，要将 DHCP 分配的域名还是将手动分配的域名发送至 DNS。该值将设置为 DHCP 或 Manual。

Advanced Interface Setup

单击此链接可打开 Advanced Interface Setup 页面，该页面与下图相似。



在此页面中，您可以查看和更改接口的其他设置。下表描述了 Advanced Ethernet Setup 页面上的设置。

表 4. Advanced Ethernet Setup 页面上的设置

设置	功能
Autonegotiate	使用此设置可选择 Data Rate 和 Duplex 网络设置是否可配置。如果 Autonegotiate 设置为 **Yes**，那么 Data Rate 和 Duplex 设置将设置为 **Auto**，并且不可配置。如果 Autonegotiate 设置为 **No**，那么用户可以配置 Data Rate 和 Duplex 设置。
Data Rate	使用此字段可指定每秒通过 LAN 连接传输的数据量。要设置数据率，请选择与您的网络能力对应的以兆位 (Mb) 为单位的数据传输率。要自动检测数据传输率，请选择 **Auto**。
Duplex	使用此字段可指定在您的网络中使用的通信信道的类型。要设置双工方式，请选择 **Full** 或 **Half**。全双工允许数据同时以两个方向传输。半双工通道允许数据以其中一个或另一个方向传输，但不能同时双向传输。要自动检测双工类型，请选择 **Auto**。

表 4. Advanced Ethernet Setup 页面上的设置 (续)

设置	功能
Maximum transmission unit (MTU)	使用此字段可指定针对您的网络接口的最大包大小（以字节为单位）。要设置 MTU 值，请在文本字段中输入所需数字。对于以太网，有效的 MTU 范围是 68 到 1500。
Locally administered MAC address	使用此字段可为此 IMM 子系统指定物理地址。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 000000000000 到 FFFFFFFFFFFF 之间的十六进制值。此值的格式必须为 *XX:XX:XX:XX:XX:XX*，其中，*X* 是 0 到 9 和 A 到 F 之间的值。 IMM 不允许使用多点广播地址。多点广播地址将第一个字节的最低有效位设置为 1。因此，第一个字节必须是偶数。
Burned-in MAC address	烧录 MAC 地址是制造商向 IMM 分配的唯一物理地址。

配置 IPv4 设置

在 Network Interfaces 页面的 IPv4 区域中，可以修改以下设置。

DHCP 使用此字段可指定是否要通过网络上的动态主机配置协议 (DHCP) 服务器来设置 IMM 子系统的以太网端口 TCP/IP 设置。要使用 DHCP 配置，请选择 **Enabled - Obtain IP config. from DHCP server**。要手动配置您的 TCP/IP 设置，请选择 **Disabled - Use static IP configuration**。如果要尝试使用 DHCP 服务器，并且在无法访问 DHCP 服务器的情况下恢复为静态 IP 配置，请选择 **Try DHCP server. If it fails, use static IP config**。

如果 IP 配置是由 DHCP 服务器分配的，请单击链接 **IP Configuration Assigned by DHCP server** 以查看配置详细信息。

注：

1. 如果选择 **Enabled - Obtain IP config. from DHCP server** 选项，那么网络上必须存在可访问且已配置的活动 DHCP 服务器。
2. DHCP 服务器分配的配置将覆盖任何静态 IP 设置。
3. **Try DHCP server. If it fails, use static IP config.** 选项并非在所有 IMM 上均受支持。

Static IP Configuration

以下字段包含此接口的静态 IP 配置。仅当禁用 DHCP 时，才使用这些设置。如果启用了 DHCP，那么 DHCP 服务器分配的动态 IP 配置将覆盖这些静态设置。

- **IP address**：使用此字段可定义通过此网络接口访问的 IMM 子系统的 IP 地址。要设置 IP 地址，请在文本框中输入地址。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。

  注：此字段的缺省值是 192.168.70.125。

- **Subnet mask**：使用此字段可定义 IMM 子系统将使用的子网掩码。要设置子网掩码，请在文本框中输入位掩码。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。从最左侧的位开始连续设置位。例如，0.255.0.0 不是有效的子网掩码。不能将此字段设置为 0.0.0.0 或 255.255.255.255。

  注：此字段的缺省值是 255.255.255.0。

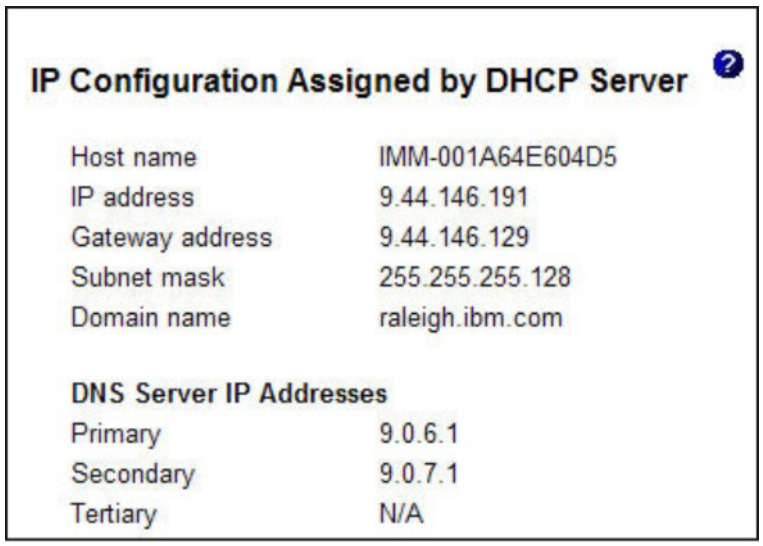
- **Gateway address**：使用此字段可标识您的缺省网关的 IP 地址。要设置网关地址，请在文本框中输入地址。网关地址必须包含以句点分隔的四个整数（从 0 到 255），且不含空格和连续句点。

  注：此字段的缺省值是 0.0.0.0。

IP Configuration Assigned by DHCP Server

单击此链接可查看 DHCP 服务器分配的 IP 配置。这样会显示 IP Configuration Assigned by DHCP Server 页面（与下图相似）。

注：仅当启用 DHCP 时，此选项才可用。



配置 IPv6 设置

在 Network Interfaces 页面的 IPv6 区域中，可以修改以下设置。

注：至少应启用本节中描述的一个 IPv6 配置选项（IPv6 Static Configuration、DHCPv6 或 Stateless Auto-configuration）。

Link local address

链路本地地址是向 IMM 分配的 IPv6 地址。链路本地地址的格式与以下示例相似：

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

IPv6 Static Configuration

使用此字段可启用或禁用 IPv6 的静态配置设置。选中 **IPv6 Static Configuration** 复选框时，以下选项将可用：

- **IP address**：使用此字段可定义通过此网络接口访问的 IMM 的 IPv6 地址。要设置 IP 地址，请在文本框中输入 IPv6 地址。此字段中的值必须是有效的 IPv6 地址。

  注：此字段的缺省值是 0::0。
- **Address prefix length (1 - 128)**：使用此字段可为静态 IPv6 地址设置前缀长度。
- **Default route**：使用此字段可设置您的缺省路径的 IPv6 地址。要设置缺省路径，请在相应的框中输入 IPv6 地址。此字段中的值必须是有效的 IPv6 地址。

  注：此字段的缺省值是 0::0。

  .

DHCPv6

使用此字段可在 IMM 上启用或禁用 DHCPv6 分配的配置。

Stateless Auto-configuration

使用此字段可在 IMM 上启用或禁用无状态自动配置。

View Automatic Configuration (link)

要查看 DHCP 服务器分配的 IPv6 配置，请单击此链接。这样会显示 IPv6 Automatic Configuration 页面。

配置网络协议

在 Network Protocols 页面上，您可以执行以下功能：

- 配置简单网络管理协议 (SNMP)
- 配置域名系统 (DNS)
- 配置 Telnet 协议
- 配置简单电子邮件传输协议 (SMTP)
- 配置轻量级目录访问协议 (LDAP)
- 配置服务位置协议 (SLP)

对网络协议设置的更改要求重新启动 IMM 才能使更改生效。如果您更改的是多个协议，那么可以等待直至所有协议都已进行更改并保存，然后再重新启动 IMM。

配置 SNMP

您可以使用 SNMP 代理来收集信息和控制服务器。IMM 也可配置为向已配置的主机名或 IP 地址发送 SNMP 警报。

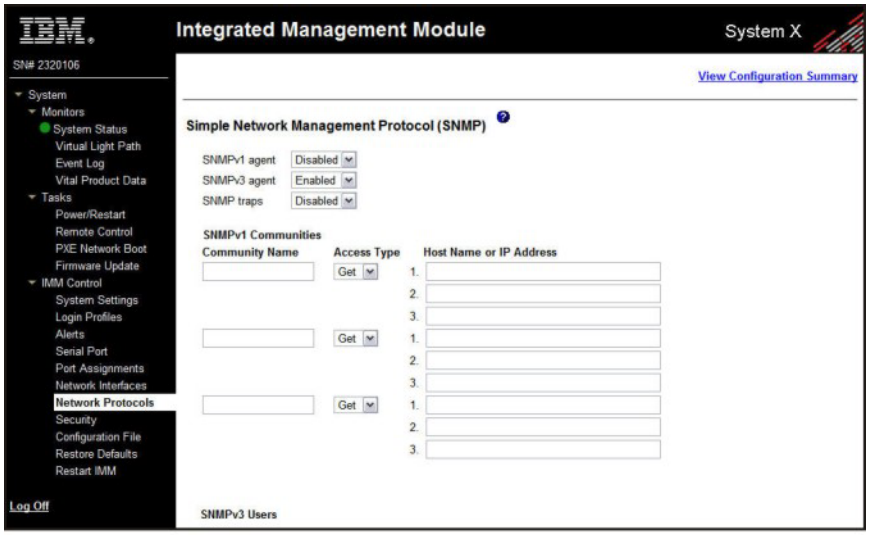
注：

1. IMM 提供两个管理信息库 (MIB) 文件以用于 SNMP 应用程序。MIB 文件包含在 IMM 固件更新包中。
2. IMM 支持 SNMPv1 和 SNMPv3 标准。

要配置 SNMP，请完成以下步骤：

1. 登录到要在其之上配置 SNMP 的 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。

2. 在导航窗格中，单击 **Network Protocols**。此时会显示一个类似于下图中的页面。



3. 在 **SNMPv1 agent** 或 **SNMPv3 agent** 字段中选择 **Enabled**。

   注： 如果您启用了 SNMPv3 代理，那么必须为活动登录概要文件配置 SNMPv3 设置以使 SNMPv3 管理器和 SNMPv3 代理之间的交互正常工作。可以在 Login Profiles 页面上的个别登录概要文件设置的底部配置这些设置（请参阅第 22 页的『创建登录概要文件』以获取更多信息）。单击要配置的登录概要文件的链接，滚动到页面底部，然后单击 **Configure SNMPv3 User** 复选框。

4. 在 **SNMP traps** 字段中选择 **Enabled** 以将警报转发到网络上的 SNMP 社区。要启用 SNMP 代理，必须满足以下条件：
   - 必须在 System Settings 页面上指定系统联系人。有关 System Settings 页面设置的信息，请参阅第 18 页的『设置系统信息』。
   - 必须在 System Settings 页面上指定系统位置。
   - 必须指定至少一个社区名称。
   - 必须为该社区指定至少一个有效的 IP 地址或主机名（如果启用了 DNS）。

   注：除非 **SNMPv1 agent** 或 **SNMPv3 agent** 和 **SNMP traps** 字段设置为 **Enabled**，否则其通知方法为 SNMP 的警报接收方无法接收警报。

5. 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。每个社区定义由以下参数组成：
   - 社区名称
   - 访问类型
   - IP 地址

   如果其中任何参数不正确，那么不会授予 SNMP 管理访问权。

   注：如果打开了错误消息窗口，请对错误窗口中列出的字段进行必要的调整。然后，滚动到页面底部并单击 **Save** 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。

6. 在 **Community Name** 字段中，输入名称或认证字符串以指定社区。

7. 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和查询 MIB 对象；选择 **Set** 以允许社区中的所有主机接收陷阱、查询和设置 MIB 对象。
8. 在对应的 **Host Name or IP Address** 字段中，输入各社区管理器的主机名或 IP 地址。
9. 滚动到页面底部并单击 **Save**。
10. 在导航窗格中，单击 **Restart IMM** 以激活更改。

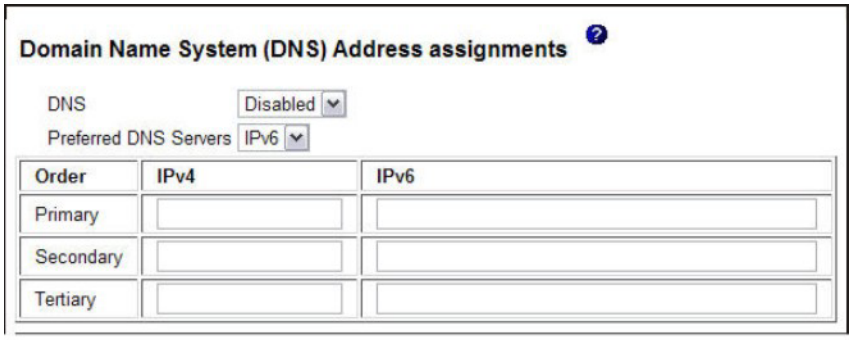
配置 DNS

您可以配置域名系统 (DNS) 设置，以指定是否应在搜索顺序中包含其他 DNS 服务器地址来进行主机名到 IP 地址解析。DNS 查找始终处于已启用状态，当启用了 DHCP 功能时，其他 DNS 地址可能由 DHCP 服务器自动分配。

为启用其他 DNS 地址，至少其中一个地址的值必须大于零。其他 DNS 服务器会添加到搜索列表的顶部，以便在这些服务器上进行主机名查找，然后再在由 DHCP 服务器自动分配的 DNS 服务器上进行该查找。

要配置 DNS，请完成以下步骤：

1. 登录到要在其之上配置 DNS 的 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **Network Protocols** 并向下滚动到页面的 **Domain Name System (DNS) Address assignments** 区域。此时会显示一个类似于下图中的页面部分。



3. 如果一台或多台 DNS 服务器在网络上可用，请在 **DNS** 字段中选择 **Enabled**。**DNS** 字段指定是否在网络上使用 DNS 服务器来将主机名转换为 IP 地址。
4. 如果您具有 IPv4 和 IPv6 DNS 服务器地址，请在 **Preferred DNS Servers** 列表中选择 **IPv4** 或 **IPv6** 以指定首选哪些服务器地址。
5. 如果已启用 DNS，请使用 Primary, Secondary, and Tertiary 文本字段指定网络上最多六台 DNS 服务器的 IP 地址。要设置三个 IPv4 或三个 IPv6 DNS 服务器地址，请在适用文本字段中输入地址。确保 IPv4 或 IPv6 地址为有效格式。
6. 滚动到页面底部并单击 **Save**。
7. 在导航窗格中，单击 **Restart IMM** 以激活更改。

配置 Telnet

要配置 Telnet，请完成以下步骤：

1. 登录到要在其之上配置 Telnet 的 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **Network Protocols** 并向下滚动到页面的 **Telnet Protocol** 区域。您可以设置最大并发 Telnet 用户数，也可以禁用 Telnet 访问。
3. 滚动到页面底部并单击 **Save**。
4. 在导航窗格中，单击 **Restart IMM** 以激活更改。

配置 SMTP

要指定简单电子邮件传输协议 (SMTP) 服务器的 IP 地址或主机名，请完成以下步骤。

1. 登录到要在其之上配置 SMTP 的 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **Network Protocols** 并向下滚动到页面的 **SMTP** 区域。
3. 在 **SMTP Server Host Name or IP address** 字段中，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）。
4. 滚动到页面底部并单击 **Save**。
5. 在导航窗格中，单击 **Restart IMM** 以激活更改。

配置 LDAP

使用轻量级目录访问协议 (LDAP) 服务器，IMM 可以通过查询或搜索 LDAP 服务器上的 LDAP 目录（而不是搜索其本地用户数据库）来对用户进行认证。然后，IMM 可以通过中央 LDAP 服务器来远程认证任何用户访问。这需要 IMM 上的 LDAP 客户机支持。此外，也可以根据在 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 向组中分配用户和 IMM 并执行组认证。例如，IMM 可以与一个或多个组关联，仅当用户属于至少一个与 IMM 关联的组时，该用户才会传递组认证。

此部分中提供了有关配置以下两个 LDAP 服务器的信息：

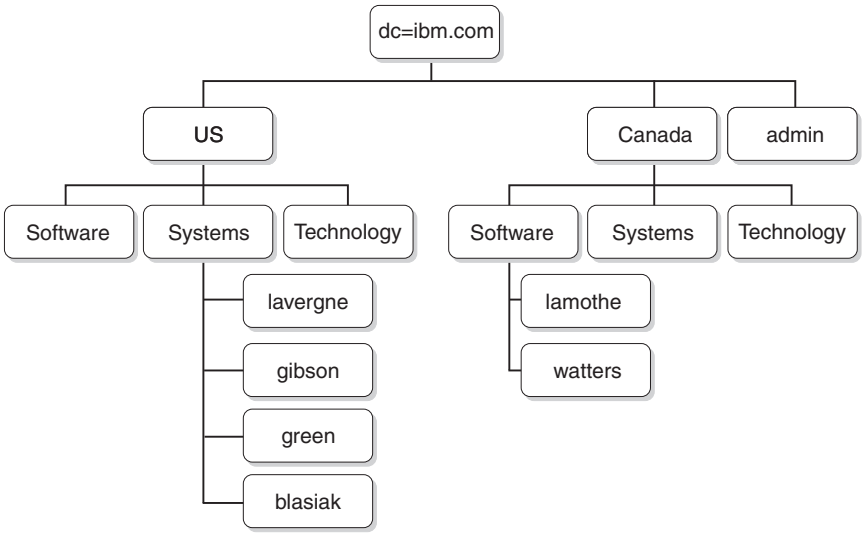
- Novell eDirectory V8.7.1
- Microsoft Windows Server 2003 Active Directory

用户模式示例

本节描述了一个简单的用户模式示例。本模式示例将在整篇文档中使用，用于说明 LDAP 客户机和 LDAP 服务器上的配置。

用户模式示例的根是称为 ibm.com 的域组件。即，该树中的每个对象都具有等于 dc=ibm,dc=com 的根专有名称。现在，假设该树代表一家公司，该公司要根据用户和用户组所属国家或地区和组织对其进行分类。层次结构为：根 → 国家或地区 → 组织 → 人员。

下图显示了本文档中所使用模式的简化视图。请注意，在根下方直接使用了一个用户帐户 (userid=admin)。这是管理员。



下图显示了如何添加用户组。在第一级定义并添加了六个用户组，并且在国家或地区为 Canada 的 Software 组织中添加了另一个用户组。

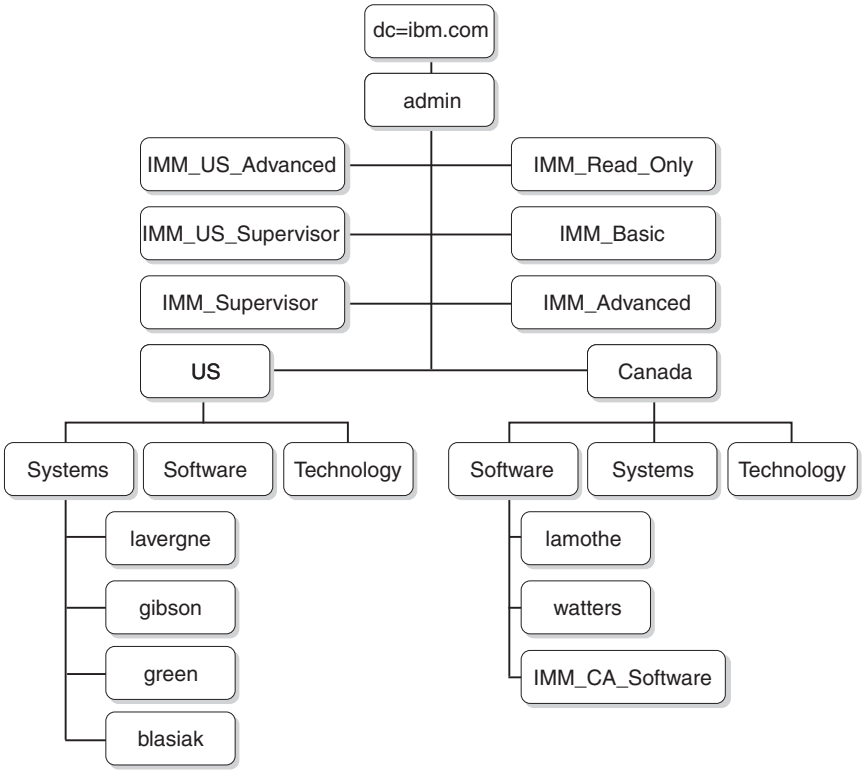


表 5 中的用户和关联的用户组用于完成模式。

表 5. 用户到组的映射

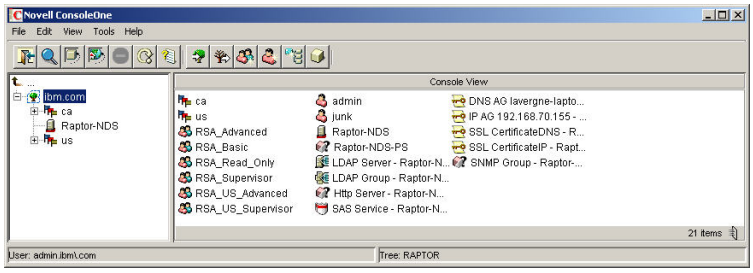
用户专有名称	组成员资格
cn=lavergne, o=Systems, c=us, dc=ibm.com	cn=IMM_Supervisor, dc=ibm.com cn=IMM_US_Supervisor, dc=ibm.com
cn=blasiak, o=Systems, c=us, dc=ibm.com	cn=IMM_US_Advanced, dc=ibm.com

表 5. 用户到组的映射 (续)

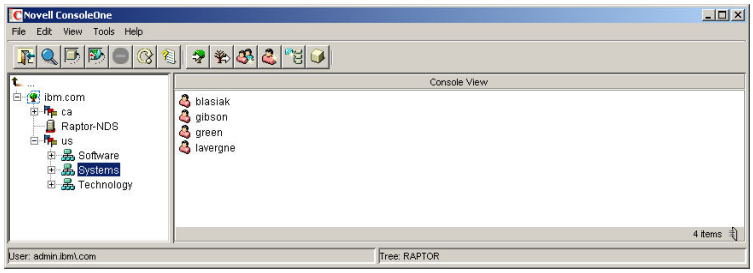
用户专有名称	组成员资格
cn=gibson, o=Systems, c=us, dc=ibm.com	cn=IMM_Basic, dc=ibm.com
cn=green, o=Systems, c=us, dc=ibm.com	cn=IMM_Read_Only, dc=ibm.com
cn=watters, o=Systems, c=ca, dc=ibm.com	cn=IMM_CA_Software, o=Software, c=ca, dc=ibm.com
cn=lamothe, o=Systems, c=ca, dc=ibm.com	cn=IMM_CA_Software, o=Software, c=ca, dc=ibm.com

Novell eDirectory 模式视图

通过使用 Novell ConsoleOne 工具，将第 41 页的『用户模式示例』中描述的模式拉取到 Novell eDirectory 中。下图显示了通过 ConsoleOne 工具看到的顶级模式视图。



下图捕获了 o=Systems, c=us, dc=ibm.com 下的用户。



组成员资格

Novell eDirectory 使用名为 **GroupMembership** 的属性来标识用户作为其成员的组。具体而言，User 对象类会使用此属性。在查询用户所属的组时，LDAP 客户机会在它针对 LDAP 服务器的搜索请求中使用缺省值 **memberOf**。

您可以使用以下一种方法来配置 LDAP 客户机以查询成员资格：

- 在 LDAP 客户机上，配置 **Group Search Attribute** 字段中的值 **GroupMembership**。
- 在 Novell eDirectory LDAP 服务器上，在 **GroupMembership** 和 **memberOf** 之间创建属性映射。

完成以下步骤，以在 LDAP 客户机上配置缺省属性：

1. 在 IMM Web 界面中，单击左侧导航窗格中的 **Network Protocols**。
2. 滚动到 **LDAP Search Attributes** 区域。
3. 在 **Group Search Attribute** 字段中，输入所需的缺省属性。

如果 **Group Search Attribute** 字段为空，它将缺省为 **memberOf**，并且您必须配置 Novell eDirectory 服务器，以将属性 **GroupMembership** 映射到 **memberOf**。完成以下 Novell eDirectory 服务器配置步骤，以将属性 **GroupMembership** 映射到 **memberOf**。

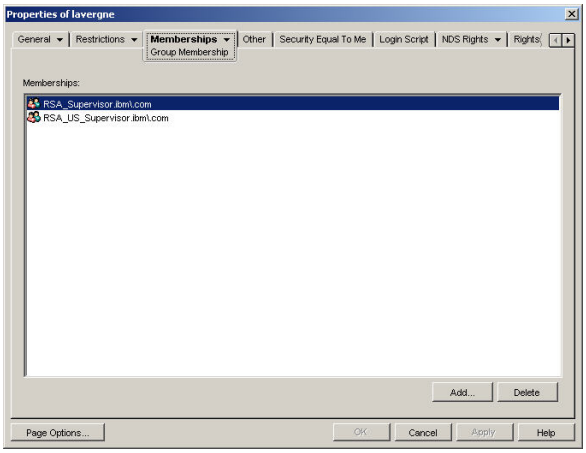
1. 使用 ConsoleOne 工具，右键单击 **LDAP Group** 图标，并单击 **Properties**。这样会打开 Properties of LDAP Group 窗口。
2. 单击 **Attribute Mappings** 选项卡。
3. 单击 **Add**，然后在 **Group Membership** 和 **memberOf** 之间创建映射。
4. 单击 **OK**。这样会打开显示 LDAP 组属性的页面。

向用户组添加用户

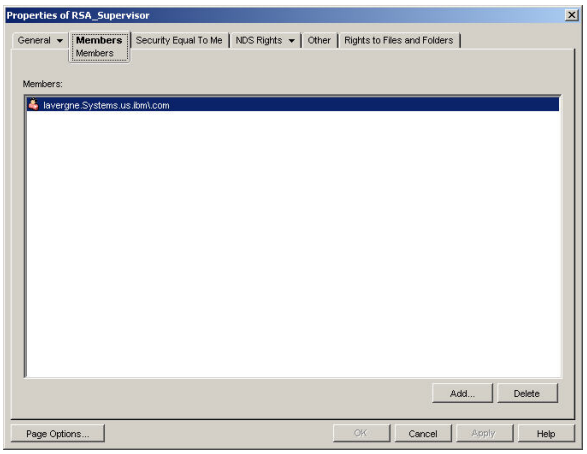
您可以通过向用户的概要文件添加组或者向组的概要文件添加用户来向相应的用户组添加用户。最终结果相同。

例如，在先前用户模式示例中，用户 lavergne 同时是 IMM_US_Supervisor 和 IMM_Supervisor 的成员。通过使用诸如 Novell ConsoleOne 之类的浏览器工具，可以验证模式（双击 **user lavergne** 并选择 **Memberships** 选项卡）。

此时会打开一个类似于下图中的页面。



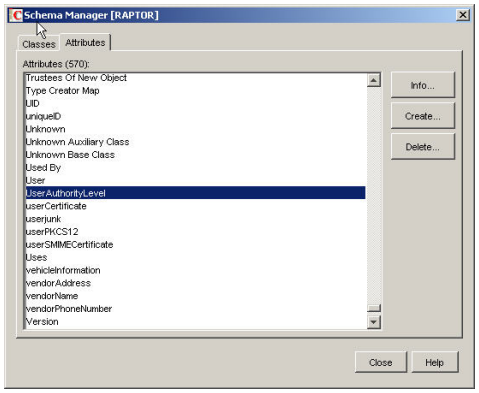
同样，如果显示了 IMM_Supervisor 组的属性，并且选择 **Members** 选项卡，那么会打开一个类似于下图中的页面。



权限级别

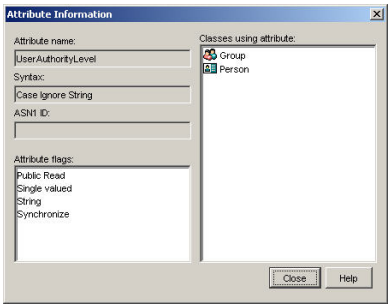
要使用权限级别功能，请使用 ConsoleOne 在 Novell eDirectory 上创建一个标示为 `UserAuthorityLevel` 的新属性。此新属性将用于支持权限级别。

1. 在 Novell ConsoleOne 工具中，单击 **Tools** > **Schema Manager**。
2. 单击 **Attributes** 选项卡，然后单击 **Create**。
3. 标示属性 **UserAuthorityLevel**。将 **ASN1 ID** 保留为空白或者咨询 LDAP 管理员以确定要使用的值。单击下一步。
4. 将语法设置为 **Case Ignore String**。单击下一步。
5. 在适用情况下设置标志。咨询 LDAP 管理员以确保正确设置这些标志。单击 **Public Read** 复选框；然后单击 **Next**。
6. 单击 **Finish**。此时会打开一个类似于下图中的页面。



7. 返回到 Schema Manager 窗口，然后单击 **Classes** 选项卡。
8. 单击 **Person** 类，然后单击 **Add**。请注意，您可以改用 User 对象类。
9. 向下滚动到 **UserAuthorityLevel** 属性，将其选定，然后将其添加到此类的属性。单击 **OK**。
10. 单击 **Group** 类，然后单击 **Add**。
11. 向下滚动到 **UserAuthorityLevel** 属性，将其选定，然后将其添加到此类的属性。单击 **OK**。
12. 要验证是否已将该属性成功添加到类，请在 Schema Manager 窗口中，选择 **Attributes** 类。

13. 滚动到 **UserAuthorityLevel** 属性；然后单击 **Info**。此时会打开一个类似于下图中的页面。



设置权限级别

此部分说明如何解释和使用 UserAuthorityLevel 属性。赋给 UserAuthorityLevel 属性的值确定成功认证后向用户分配的许可权（或权限级别）。

UserAuthorityLevel 属性读取为二进制位串或 0 和 1。位从左到右进行编号。第一个位表示位位置 0。第二个位表示位位置 1，依此类推。

下表提供每个位位置的说明。

表 6. 许可权位

位位置	功能	说明
0	始终拒绝	如果设置，那么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	如果设置，那么会给予用户管理员特权。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	如果设置，那么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）。无法使用保存、清除或复原功能修改任何内容。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。如果设置了任何其他位，那么将忽略此位。
3	联网和安全性	如果设置，那么用户可以在 Security、Network Protocols、Network Interface、Port Assignments 和 Serial Port 面板中修改配置。
4	用户帐户管理	如果设置，那么用户可以添加、修改或删除用户并可以在 Login Profiles 面板中更改 Global Login Settings。
5	远程控制台访问	如果设置，那么用户可以访问远程服务器控制台，并且可以在 Serial Port 面板中修改配置。

表 6. 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	如果设置，那么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。用户还可在 Serial Port 面板中修改配置。
7	远程服务器电源/重新启动访问	如果设置，那么用户可以访问远程服务器的开机、重新启动和服务器超时功能。
8	基本适配器配置	如果设置，那么用户可以在 System Settings 和 Alerts 面板中修改配置参数（Contact、Location 和 Server Timeout 参数除外）。
9	清除事件日志的能力	如果设置，那么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	如果设置，那么用户在配置适配器时没有任何限制，并且用户对 IMM 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、复原适配器出厂缺省值、根据配置文件修改和复原适配器配置以及重新启动/重置适配器。不包括服务器电源/重新启动和超时功能。
11	保留	此位位置保留供将来使用（当前已忽略）。
备注： • 如果未使用位，那么缺省值将针对用户设置为 Read Only。 • 向直接从用户记录中检索到的登录许可权指定优先级。如果用户记录在 **Login Permission Attribute** 字段中不包含名称，那么将尝试从用户所属的组中检索与组过滤器匹配的许可权。在此情况下，会为用户分配所有组的所有位的包含 OR。 • 如果为任何组设置了“始终拒绝”（位位置为 0）位，那么用户将被拒绝访问。“始终拒绝”位优先于所有位。 • 如果用户能够修改基本、联网或安全性相关适配器配置参数，那么应考虑为该用户提供重新启动 IMM（位位置为 10）的能力。如果没有此能力，那么用户可能可以更改参数；但是，参数将不会生效。		

下表包含示例及其描述：

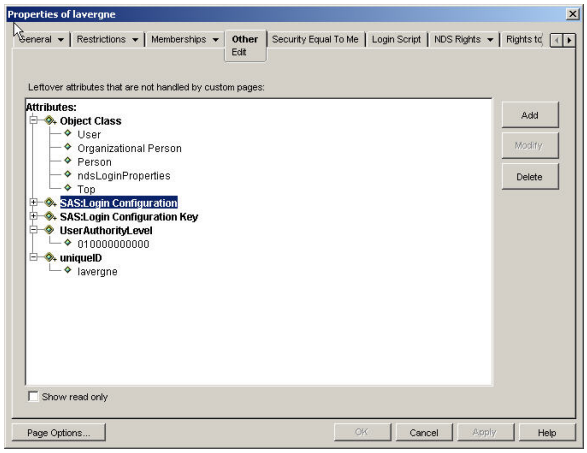
表 7. 示例 UserLevelAuthority 属性和描述

UserLevelAuthority 属性示例	描述
IBMRBSPermissions=010000000000	Supervisor 访问权（设置了位位置 1）
IBMRBSPermissions=001000000000	Read-Only 只读访问权（设置了位位置 2）
IBMRBSPermissions=100000000000	无访问权（设置了位位置 0）
IBMRBSPermissions=000011111100	全部权限（高级适配器配置除外）
IBMRBSPermissions=000011011110	全部权限（对虚拟介质的访问权除外）

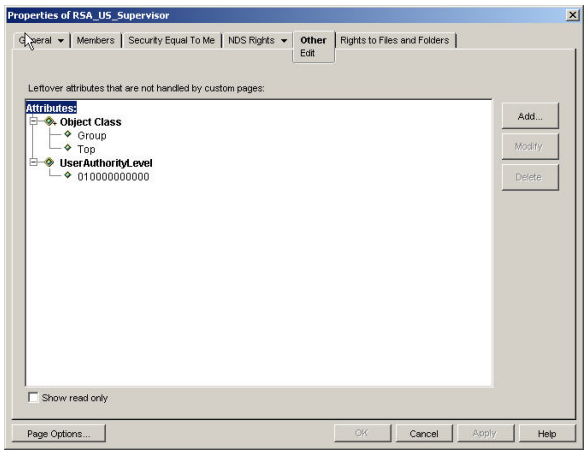
完成以下步骤以向用户 *lavergne* 以及各用户组添加 UserAuthorityLevel 属性：

1. 右键单击用户 **lavergne**，然后单击 **Properties**。
2. 单击 **Other** 选项卡。单击 **Add**。
3. 向下滚动到 **UserAuthorityAttribute**，然后单击 **OK**。
4. 填写要为属性授予的值。例如，如果要分配 Supervisor 访问权，请将属性设置为 **IBMRBSPermissions=010000000000**。单击 **OK**。
5. 针对各用户组重复步骤 1 到 4，并且根据情况设置 **UserAuthorityLevel**。

下图显示了用户 *lavergne* 的属性。



下图显示了 IMM_US_Supervisor 的属性。



下表显示了向用户模式示例中各用户组分配的 **UserAuthorityLevel**。

表 8. 向用户组进行的 UserAuthorityLevel 分配

用户组	**UserAuthorityLevel**	转换
IMM_Basic	IBMRBSPermissions=000100000000	联网和安全性

表 8. 向用户组进行的 UserAuthorityLevel 分配 (续)

用户组	**UserAuthorityLevel**	转换
IMM_CA_Software	IBMRBSPermissions=000101111010	联网和安全性 远程控制台和虚拟介质访问权；远程服务器电源和重新启动访问权 基本适配器配置 高级适配器配置
IMM_Advanced	IBMRBSPermissions=000110111100	联网和安全性 远程控制台和虚拟介质访问权；远程服务器电源和重新启动访问权 基本适配器配置 高级适配器配置 清除事件日志的能力
IMM_Supervisor	IBMRBSPermissions=010000000000	Supervisor 访问权
IMM_Read_Only	IBMRBSPermissions=001000000000	Read-Only 访问权
IMM_US_Advanced	IBMRBSPermissions=000110111100	联网和安全性 用户帐户管理 远程控制台和虚拟介质访问权；远程服务器电源和重新启动访问权 基本适配器配置 清除事件日志的能力
IMM_US_Supervisor	IBMRBSPermissions=010000000000	Supervisor 访问权

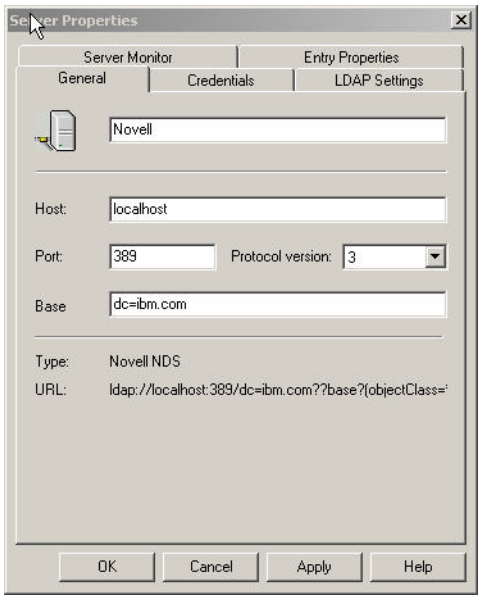
浏览 **LDAP** 服务器

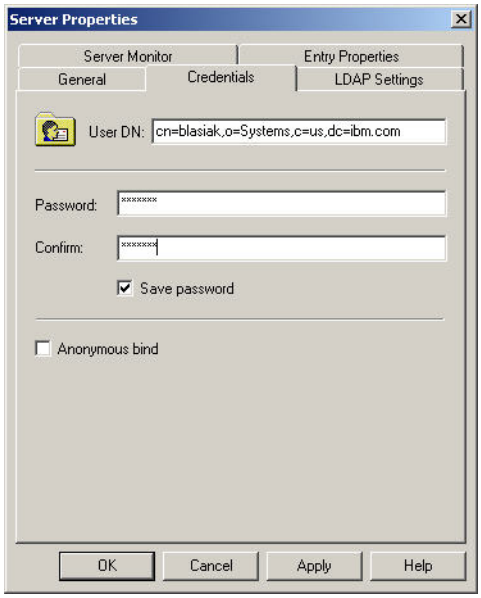
在尝试从 IMM 上的 LDAP 客户机连接到您的 LDAP 服务器之前，请先使用所选的第三方 LDAP 浏览器连接到 LDAP 服务器。例如，在 http://www.ldapbrowser.com 中提供了一个目录浏览工具。

在尝试使用 IMM LDAP 客户机之前使用 LDAP 浏览器有以下益处：

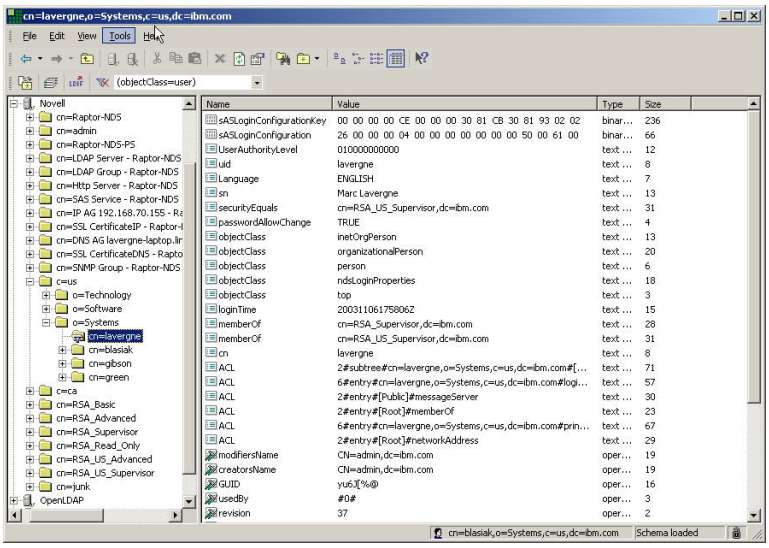
- 能够使用不同凭证绑定到服务器。这将显示 LDAP 服务器上的用户帐户是否设置正确。如果您可以使用浏览器绑定到服务器，但是无法使用 IMM LDAP 客户机绑定到服务器，那么未正确配置 LDAP 客户机。如果无法使用浏览器进行绑定，那么也无法使用 IMM 上的 LDAP 客户机进行绑定。
- 在成功绑定到服务器后，您可以浏览 LDAP 服务器数据库并快速发出搜索查询。这将确认关于对各种对象的访问权，是否按您所需的方式配置了 LDAP 服务器。例如，您可能发现无法查看特定属性，或者可能看不到预期在特定搜索请求下会看到的所有对象。这指示未正确配置向对象分配的许可权（例如，哪些公开可见或者哪些隐藏）。请联系 LDAP 服务器管理员以更正问题。请务必注意，您用于绑定的凭证决定了您将在服务器上具有的特权。
- 验证所有用户的组成员资格。验证向用户和用户组分配的 **UserAuthorityLevel** 属性。

下图显示向使用第 41 页的『用户模式示例』配置的 Novell eDirectory 服务器进行各种查询和搜索的结果。在此情况下，使用 Softerra LDAP 浏览器工具。使用该图中所示的属性和凭证进行了与服务器的初始绑定。

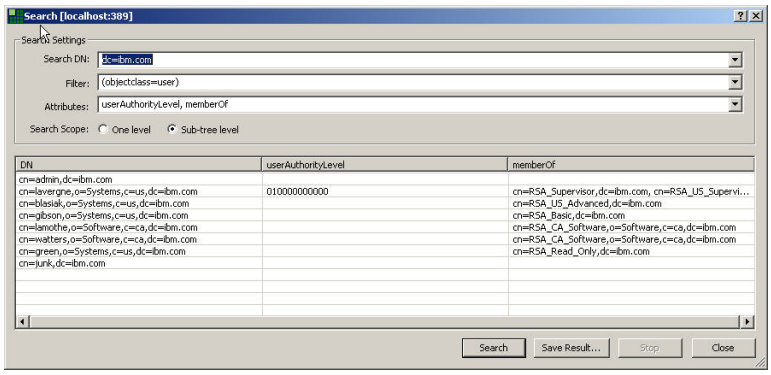




在初始绑定成功后，会显示 Novell eDirectory 上模式的以下视图。



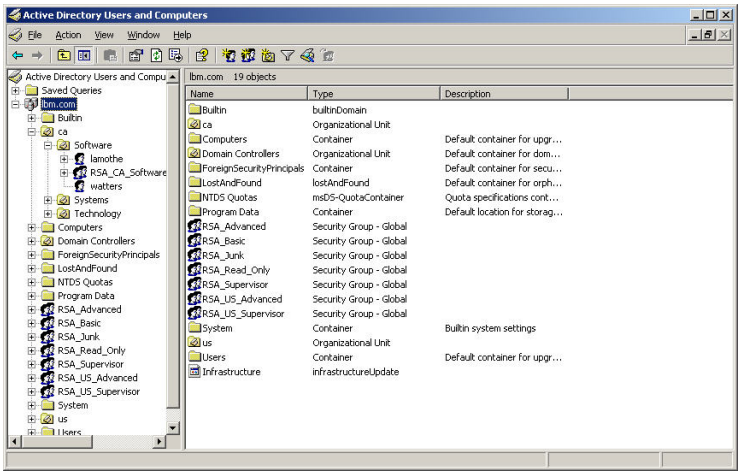
下图显示了通过请求检索 **userAuthorityLevel** 和 **memberOf** 属性对所有用户的查询。



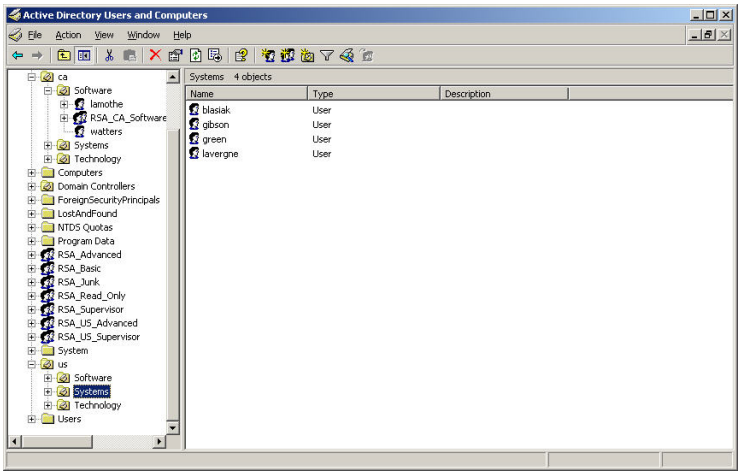
Microsoft Windows Server 2003 Active Directory 模式视图

本节描述与在 Microsoft Windows Server 2003 Active Directory 上捕获第 41 页的『用户模式示例』中的信息相关的一些配置方面。

下图显示了通过“Active Directory 用户和计算机”管理工具看到的顶级模式视图。



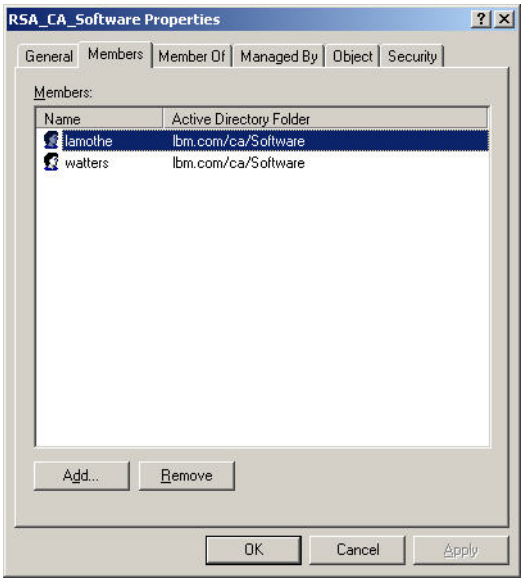
下图显示了 ou=Systems，ou=us，dc=ibm，dc=com 下的用户。



向用户组添加用户

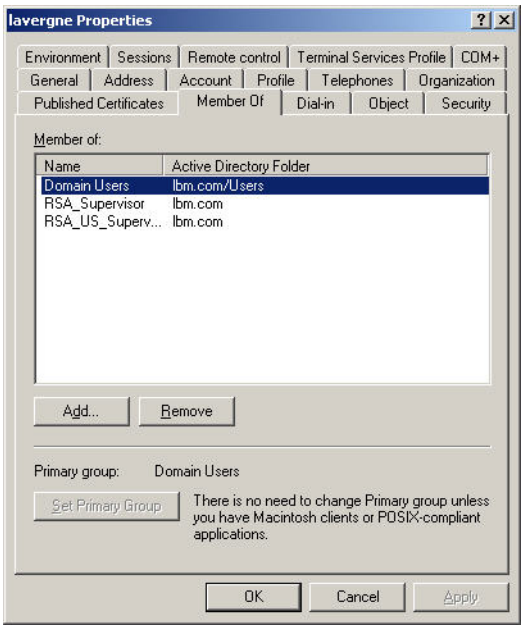
在 Active Directory 中，您可以将组添加到特定用户，也可以将用户添加到特定组。右键单击用户或用户组对象，然后，单击属性。

如果您选择了用户组，然后单击成员选项卡，打开的页面将与下图中的页面相似。



要在用户组中添加或删除用户，请单击添加或除去。

如果您选择了用户，然后单击成员属于选项卡，打开的页面将与下图中的页面相似。

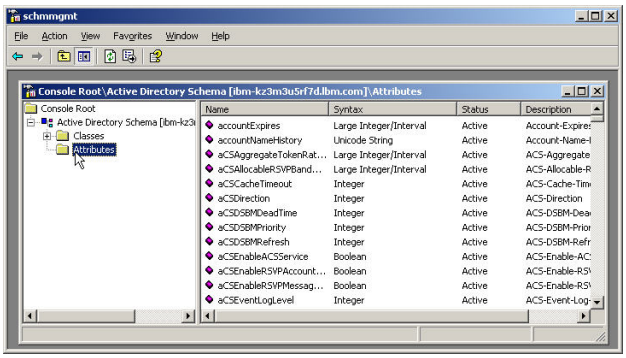


要在用户组中添加或删除用户，请单击添加或除去。

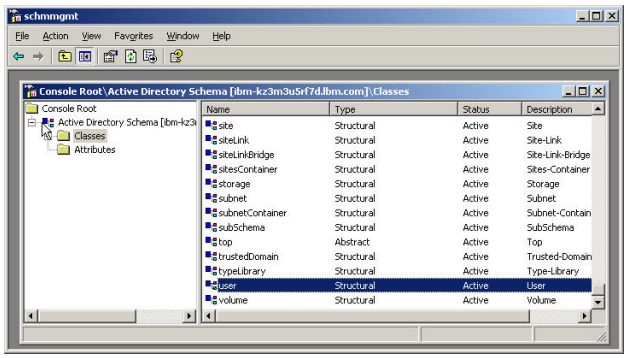
权限级别

第 45 页的『权限级别』部分描述如何通过 Novell eDirectory 服务器创建新属性以支持权限级别的概念，以及如何从 IMM 将这些权限级别分配给向 LDAP 服务器认证的用户。创建的属性称为 **UserAuthorityLevel**。在此部分中，将在 Active Directory 上创建此属性。

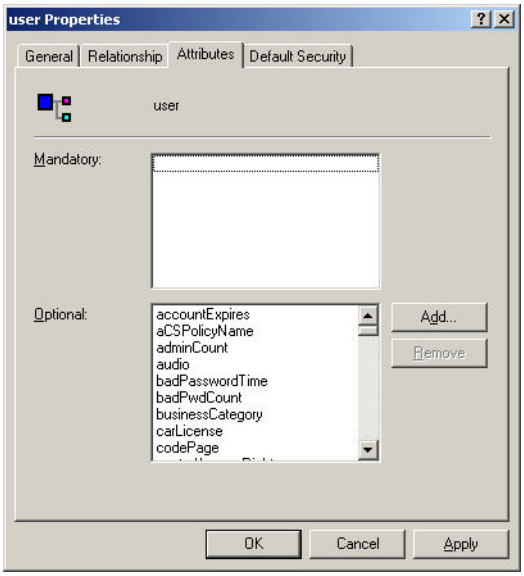
1. 安装“Active Directory 模式管理单元”工具。有关更多信息，请参阅 Active Directory 随附的文档。
2. 启动“Active Directory 模式”。
3. 单击操作 > 创建属性。填写以下字段：
   a. 将“通用名称”设置为 **UserAuthorityLevel**
   b. 将“语法”设置为不区分大小写的字符串
   c. 将“最大值”和“最大值”设置为 **12**
4. 联系系统管理员以分配新 X.500 OID。如果您不希望定义新 X.500 OID，请使用现有属性而不是为权限级别创建新属性。



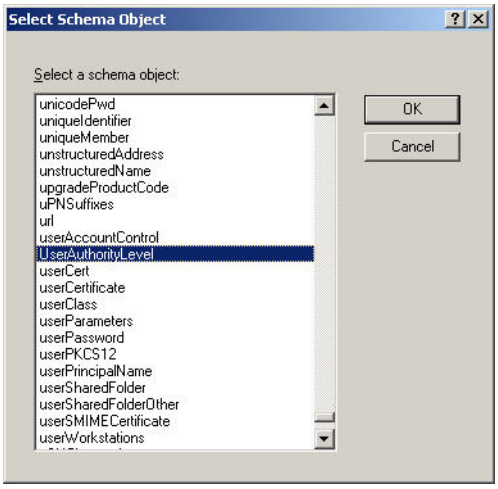
5. 保存属性后，选择类文件夹。



6. 双击类用户。此时会打开用户“特性”窗口。

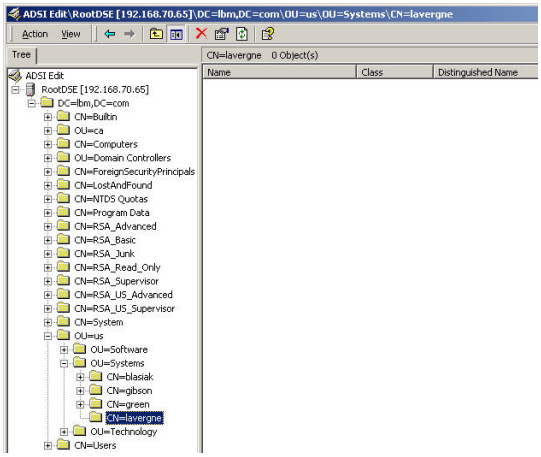


7. 选择属性选项卡，然后单击添加。此时会打开“选择模式对象”窗口。

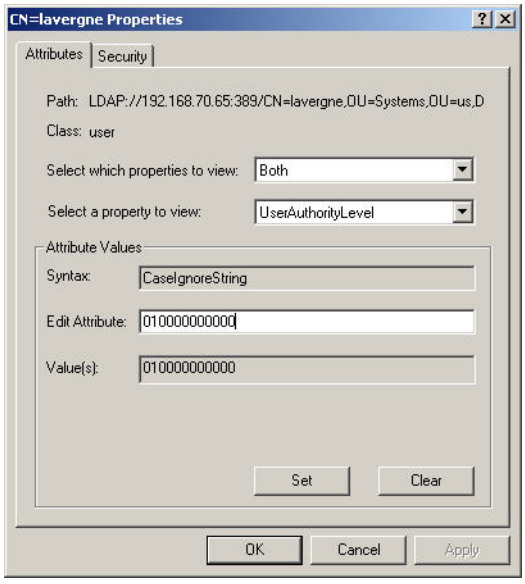


8. 向下滚动到 **UserAuthorityLevel** 并单击确定。此属性现在将出现在用户对象类的可选属性列表中。
9. 针对类组重复步骤 6 到步骤 8。这使 **UserAuthorityLevel** 属性能够分配到用户或用户组。这些是仅有的两个需要使用此新属性的对象类。

10. 将 **UserAuthorityLevel** 属性分配到相应的用户和用户组。要匹配 Novell eDirectory 服务器下定义的模式，请使用与 第 46 页的『设置权限级别』中相同的值。可以使用 ADSI Edit 工具执行此操作。Microsoft ADSI Edit 支持工具是一个 Microsoft Management Console (MMC) 管理单元，用于查看目录中的所有对象（包括模式和配置信息），修改对象以及设置有关对象的访问控制表。
11. 对于此示例，假设要向用户 lavergne 添加 **UserAuthorityLevel** 属性。使用 ADSI Edit 执行此操作。必须提供相应的凭证以连接到 Active Directory；否则，您可能不具有适当的用户特权来修改服务器上的对象。下图显示连接到服务器后 ADSI 所看到的模式。



12. 右键单击 **lavergne**，然后单击特性。此时会打开一个类似于下图中的窗口。



13. 在选择要查看的特性字段中，选择 **UserAuthorityLevel**。
14. 在编辑属性字段中，输入 `IBMRBSPermissions=010000000000`，它转换为 Supervisor 访问权。单击设置。
15. 单击确定。
16. 您可以通过针对要修改的用户组对象遵循相同步骤来将此属性添加到用户组。

检查 Active Directory 配置

在您尝试将 LDAP 客户机连接到 Active Directory（以认证用户）之前，请使用 LDAP 浏览器浏览 Active Directory 模式。请至少发出下表中列示的查询，以检查权限级别和组成员资格。

表 9. 检查权限级别和组成员资格

搜索专有名称	过滤器	属性
DC=ibm, DC=com	(objectclass=user)	memberOf, userAuthorityLevel
DC=ibm, DC=com	(objectclass=group)	member, userAuthorityLevel

配置 LDAP 客户机

您可以将 LDAP 配置为认证管理模块用户。IMM 支持本地和远程用户认证。本地认证使用 Login Profiles 页面中提供的信息来认证用户。管理模块可以使用 LDAP 服务器，通过查询或搜索远程 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。

使用任意类型的远程认证时，您可以选择对每个已成功认证的用户在本地授予许可权，或根据 LDAP 服务器上存储的用于远程认证的信息对这些用户授予许可权。向用户授予的许可权指定了每个用户在登录 IMM 时可执行的操作。以下主题中描述了远程认证方法：

- Active Directory 认证和本地授权
- 基于 Active Directory 角色的认证和授权
- 遗留 LDAP 认证和授权

具有本地授权的 Active Directory 认证

您可以使用 Active Directory 认证为具有本地用户授权的用户设置远程 LDAP 认证。

注：具有本地授权的 Active Directory 认证只适用于在 Active Directory 环境中使用的服务器。

将 Active Directory 认证与本地授权结合使用时，Active Directory 服务器只用于认证用户（验证用户的凭证）。在 Active Directory 服务器上没有存储给定用户的授权信息；必须使用授权信息来配置 IMM 存储的组概要文件。可通过检索 Active Directory 服务器中用户的成员资格信息，获取用于配置组概要文件的授权信息。此成员资格信息给出用户所属的组的列表（支持嵌套组）。然后将在 Active Directory 服务器上指定的组与在 IMM 上本地配置的组名相比较。对于用户所属的每个组，向该用户分配来自该组的许可权。对于在 IMM 上本地配置的每个组名，存在也为该组配置的相应授权概要文件。

IMM 最多支持 16 个本地配置的组名。每个组名的长度限制为 63 个字符。必须将以下属性之一配置为组名，以便与从 Active Directory 服务器检索的组成员资格信息匹配：

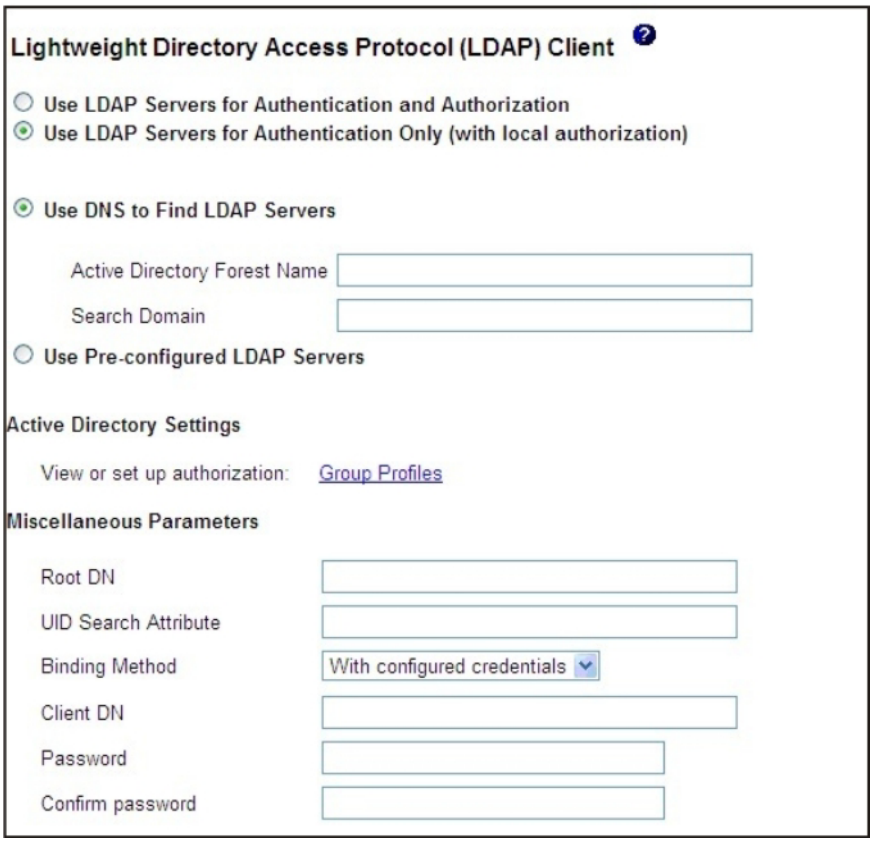
- 专有名称 (DN)
- “cn”属性
- “name”属性
- “sAMAccountName”属性

要为 IMM 配置具有本地授权的 Active Directory 认证，请完成以下步骤：

1. 在导航窗格中，单击 **Network Protocols**。
2. 向下滚动到 **Lightweight Directory Access Protocol (LDAP) Client** 部分。
3. 选择 **Use LDAP Servers for Authentication Only (with local authorization)**。
4. 选择以下选项之一以手动配置或动态发现域控制器：
   - 选择 **Use DNS to find LDAP Servers** 以基于 DNS SVR 记录动态发现域控制器。
   - 选择 **Use Pre-Configured LDAP Servers**（缺省选择）以手动配置域控制器。
5. 如果您在使用 DNS 来动态发现域控制器，请配置以下设置，然后继续执行步骤 第 58 页的 7。

   注：如果您在使用 DNS 来动态发现域控制器，您必须指定域控制器的标准域名。
   - 搜索域
     - 在 **Search Domain** 字段中输入域控制器的域名。
   - Active Directory Forest Name
     - 此可选字段用于发现全局目录。属于跨域中通用组的用户需要使用全局目录。在跨域组成员资格不适用的环境中，可以将该字段留空。

   以下插图显示使用 DNS 来动态发现域控制器时的“LDAP Client”窗口。



6. 如果手动配置域控制器和全局目录，请使用 **Use Pre-Configured LDAP Servers**（缺省值）选项；然后，配置 **LDAP Server Host Name or IP Address** 和 **Port** 字段。

使用 IP 地址或标准主机名最多可以配置四个域控制器。使用端口号 3268 或 3269 来标识全局目录服务器。使用其他任何端口号将指示正在配置域控制器。

7. 如果您在使用组授权概要文件，请单击“Active Directory Settings”部分中的 **Group Profiles** 以查看或配置它们，（请参阅第 59 页的『Active Directory 用户的组概要文件』以了解其他信息）。
8. 返回到“Network Protocols”页面。单击“Group Profiles for Active Directory Users”页面上的**“Network Protocols”**页面的**“LDAP Client”**部分链接，然后滚动到 **Lightweight Directory Access Protocol (LDAP) Client** 部分。
9. 配置 IMM 的其他参数。请参阅下表以了解关于参数的信息。

表 10. 其他参数

字段	描述	选项
Root DN	IMM 将 DN 格式的 **Root DN** 字段用作目录树的根条目。此 DN 将用作所有搜索的基础对象。示例可能类 似 `dc=mycompany,dc=com`。	

表 10. 其他参数 (续)

字段	描述	选项
Binding method	**Binding Method** 字段用于到域控制器服务器的初始绑定，选择一个选项。	• With configured credentials： 输入要用于初始绑定的客户机 DN 和密码。如果该绑定失败，那么认证过程也将失败。如果该绑定成功，那么搜索将尝试查找匹配在 **Client DN** 字段中输入的客户机 DN 的用户记录。该搜索一般查找匹配在登录过程中呈现的用户标识的通用属性。这些属性包括 displayName、sAMAccountName 和 userPrincipalName。如果已配置 **UID search attribute** 字段，那么搜索还将包含该属性。 如果搜索成功，那么尝试第二次绑定，这次使用用户 DN（从搜索中检索）以及在登录过程中呈现的密码。如果第二次绑定尝试成功，那么认证部分便成功，并且将针对 IMM 上本地配置的组检索和匹配该用户的组成员资格信息。匹配的组将定义分配给用户的授权许可权。 • With login credentials： 使用在登录过程中呈现的凭证来进行到域控制器服务器的初始绑定。如果该绑定失败，那么认证过程也将失败。如果该绑定成功，那么搜索将尝试查找用户记录。一旦找到，将针对 IMM 上本地配置的组检索和匹配该用户的组成员资格信息。匹配的组将定义分配给用户的授权许可权。 • Anonymously： 在不使用 DN 或密码的情况下，初始绑定到域控制器服务器。由于大多数服务器配置为不允许对特定用户记录的搜索请求，所以不鼓励使用该选项。

Active Directory 用户的组概要文件

配置组概要文件以便为用户组提供本地授权规范。每个组概要文件包含表示为权限级别（角色）的权限（与登录概要文件中完全相同）。要配置组概要文件，用户必须具有用户帐户管理权限。要将用户与组概要文件关联，需要 LDAP 认证服务器。

组概要文件列表

通过单击 **IMM Control** > **Login Profiles** 来访问组概要文件列表。为每个组概要文件显示组标识和角色摘要（和登录概要文件一样）。从该列表，可以添加新组，可以选择现有组来进行编辑或删除。

以下插图显示“Group Profiles for Active Directory Users”窗口。

要编辑组概要文件，请单击 **Edit**。为该组打开“Group Profile”页面。要删除组概要文件，请单击 **Delete**。要求您确认删除组概要文件。要添加新组概要文件，请单击添加组链接。将为您打开“Group Profile”页面以输入新的组概要文件的信息。最多可以添加 16 个组概要文件。组概要文件名称无需是唯一的。

下表描述“Group Profile”页面上的字段。

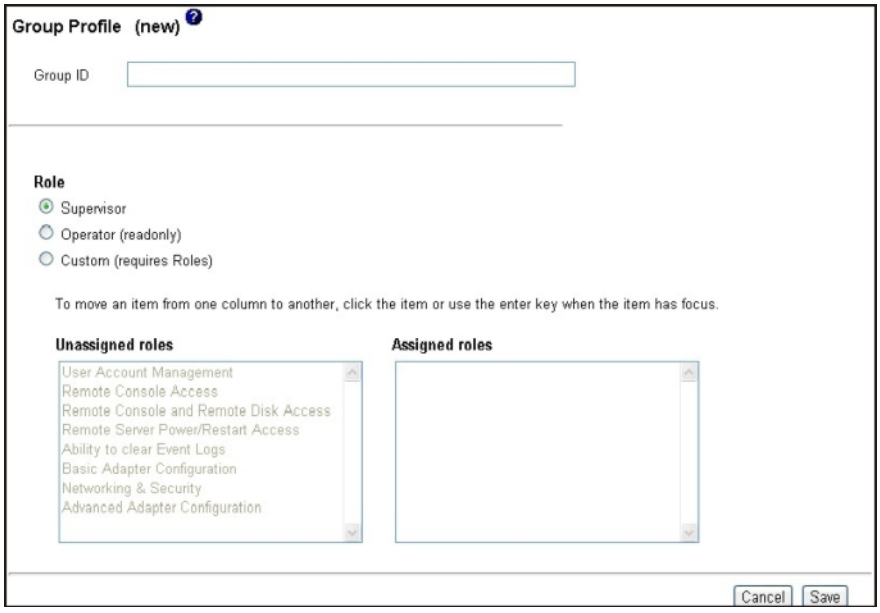
表 11. 组概要文件信息

字段	选项	描述
Group ID		该字段用于指定组概要文件的组标识。您最多可以输入 63 个字符。组标识必须与其在 LDAP 服务器上的对应部分相同。组名的示例为 IMM Admin Group 和 IMM/Robert。
Role		选择与此登录标识关联的角色（权限级别），然后将其传输到 **Assigned roles** 框。 Enter 键或鼠标单击可以用于将所选项从一个框传递到其他框。
	Supervisor	该用户没有限制，除了分配的作用域。
	Operator	用户只有只读访问许可权，且无法执行任何更改，例如：保存、修改和清除。这还包括影响操作（重新启动 IMM、恢复缺省值和升级固件）的状态。
Role	Custom	用户不一定具有任何限制，这取决于分配给用户的定制权限级别。如果您选择“Custom”选项，那么必须选择一个或多个以下客户权限级别： • 联网和安全性 – 用户可以在 Security、Network Protocols、Network Interface、Port Assignments 和 Serial Port 面板中修改配置。 • 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 面板中更改 Global Login 设置。 • 远程控制台访问 – 用户可以访问远程服务器控制台。 • 远程控制台和远程磁盘访问 – 用户可以访问远程服务器控制台以及远程服务器的远程磁盘功能。 • 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、重新启动和服务器超时功能。

表 11. 组概要文件信息 (续)

字段	选项	描述
		• 基本适配器配置 – 用户可以在 System Settings 面板和 Alerts 面板中修改配置参数（Contact、Location 和 Server Timeout 参数除外）。 • 清除事件日志的能力 – 用户可以清除事件日志。 注：每个人都可以查看事件日志；但是，需要该许可权才能清除日志。 • 高级适配器配置 – 用户在配置适配器时没有任何限制，并且用户对 IMM 具有管理访问权。用户可以执行以下高级功能：固件升级、预引导执行环境 (PXE) 网络引导、恢复适配器出厂缺省值、从配置文件修改和恢复适配器配置以及重新启动/重置适配器。 注：此权限级别排除服务器电源/重新启动控制和超时功能。
注：要防止出现没有用户具有读/写访问权的情况，必须至少使用修改登录概要文件的能力来设置首个登录概要文件。必须给予该用户 Supervisor 访问权或“用户帐户管理”访问权。这保证至少一个用户可以执行操作、进行配置更改以及将用户添加到也可以执行操作或进行配置更改的登录概要文件中。		

以下插图显示“Group Profile”窗口。



基于 **Active Directory** 角色的认证和授权

您可以使用 Active Directory 为用户设置远程 LDAP 认证和授权。

备注：

- 基于 Active Directory 角色的认证和授权只适用于在 Active Directory 环境中使用的服务器。
- 基于 Active Directory 角色的认证和授权需要增强的基于角色的安全插入工具。

基于 Active Directory 角色的认证和授权使用在 Active Directory 服务器上存储的配置信息来认证某个用户，然后将许可权与该用户关联。启用基于 Active Directory 角色的认证和授权之前，请使用增强型基于角色的安全管理单元工具将配置信息存储在用于将许可权与用户相关联的 Active Directory 服务器上。该工具可在任何 Microsoft Windows 客户机上运行，可以从 http://www.ibm.com/systems/support/ 下载。

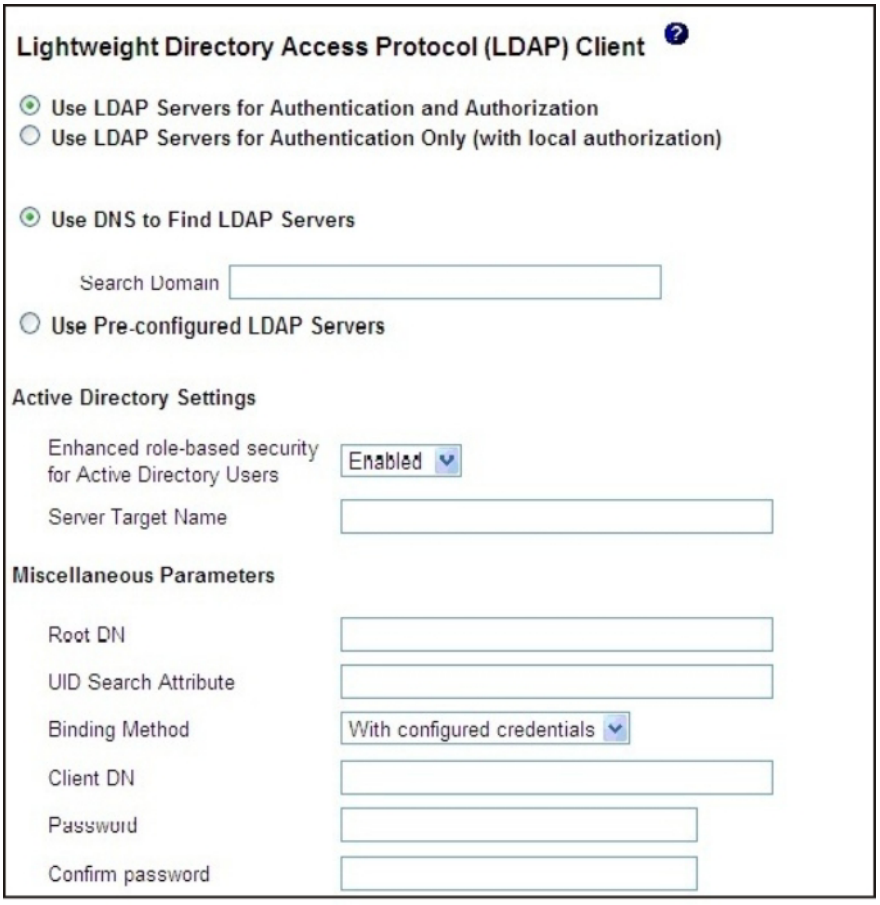
增强型基于角色的安全管理单元工具允许您在 Active Directory 服务器上配置角色以及将 IMM、用户和组关联到这些角色。请参阅增强型基于角色的安全管理单元工具的文档以了解信息和指令。角色标识分配给用户和组的许可权并标识将角色连接到的命令目标，例如 IMM 或刀片服务器。在启用基于 Active Directory 角色的认证和授权之前，应在 Active Directory 服务器上对角色进行配置。

在 **Server Target Name** 字段中配置的可选名称标识特定 IMM，并且可以通过基于角色的安全管理单元工具在 Active Directory 服务器上与一个或多个角色相关联。这是通过创建受管目标、给予目标特定名称，然后将目标与相应角色相关联来完成的。如果配置了服务器目标名称，那么它可以为属于同一角色的用户和 IMM 目标定义特定角色。用户登录到 IMM 且通过 Active Directory 进行了认证时，从该目录检索该用户的角色。从以下角色中抽取分配给用户的许可权：这些角色具有作为成员（其名称匹配该 IMM）的目标或者匹配任何 IMM 的目标。可以给予该 IMM 唯一的名称或者多个 IMM 可以共享同一目标名称。将多个 IMM 分配到同一目标名称，将其一起分组，然后将其分配给同一角色。

要为 IMM 配置基于 Active Directory 角色的认证和授权，请完成以下步骤：

1. 在导航窗格中，单击 **Network Protocols**。
2. 向下滚动至 **Lightweight Directory Access Protocol (LDAP) Client** 部分。
3. 选择 **Use LDAP Servers for Authentication and Authorization**。
4. 为 **Enhanced role-based security for Active Directory Users** 字段选择 **Enabled**。
5. 选择以下选项之一以动态发现或手动配置域控制器：
   - 选择 **Use DNS to find LDAP Servers** 以基于 DNS SVR 记录动态发现域控制器。
   - 选择 **Use Pre-Configured LDAP Servers**（缺省选择）以手动配置域控制器。
6. 如果您使用 DNS 来动态发现域控制器，请配置域控制器的域名；然后继续执行步骤 第 64 页的 8。您必须指定域控制器的标准域名。在 **Search Domain** 字段中输入域控制器的域名。

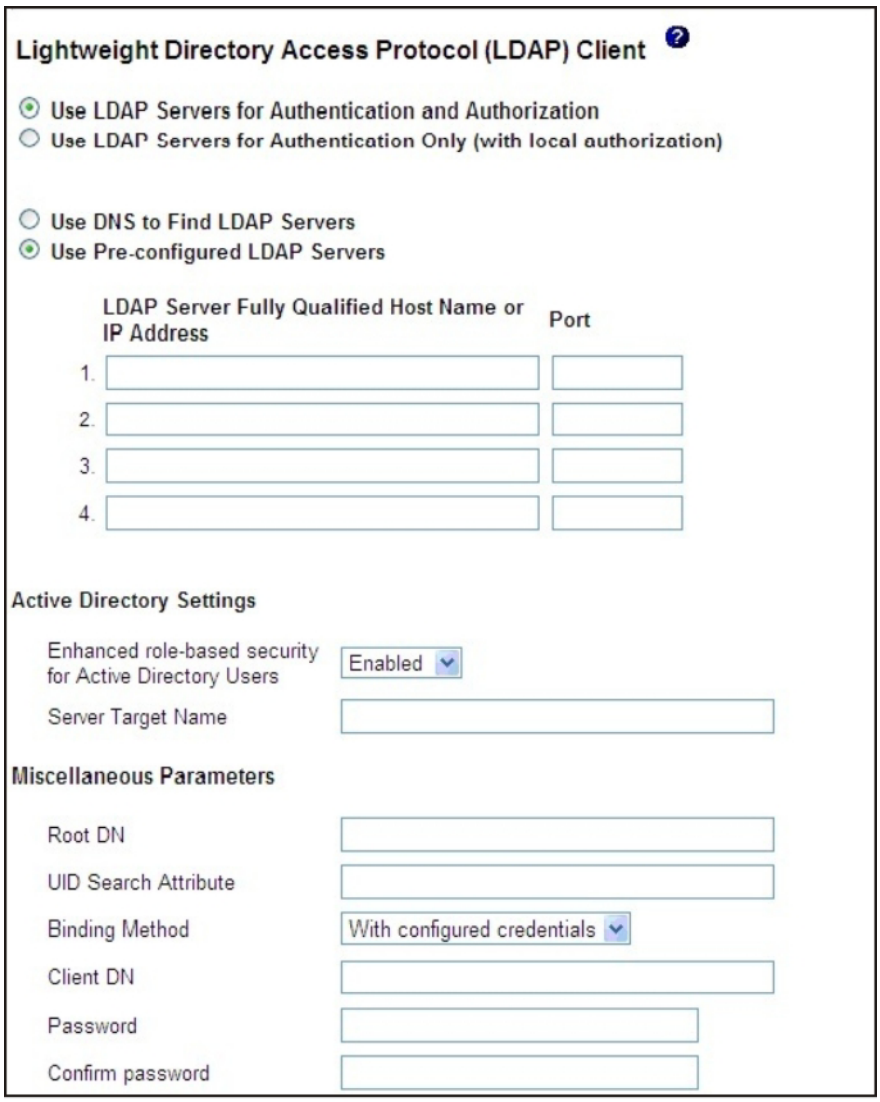
在使用 DNS 来动态发现域控制器时，以下窗口显示“LDAP Client”窗口。



7. 如果您手动配置域控制器，请配置 **LDAP Server Host Name or IP Address** 和 **Port** 字段。

   注：使用 IP 地址或标准主机名最多可以配置四个域控制器。

以下插图显示手动配置域控制器时的“LDAP Client”窗口。



8. 通过从 **Enhanced role-based security for Active Directory Users** 菜单选择 **Enabled** 来配置 Active Directory 设置。
9. 配置其他参数。请参阅下表以了解关于参数的信息。

表 12. 其他参数

字段	描述	选项
Root DN	IMM 将 DN 格式的 **Root DN** 字段用作目录树的根条目。此 DN 将用作所有搜索的基础对象。示例可能类 似 `dc=mycompany,dc=com`。	

表 12. 其他参数 (续)

字段	描述	选项
Binding method	**Binding Method** 字段用于到域控制器服务器的初始绑定，选择一个选项。	• Anonymously： 在不使用 DN 或密码的情况下，初始绑定到域控制器服务器。由于大多数服务器配置为不允许对特定用户记录的搜索请求，所以不鼓励使用该选项。 • With configured credentials： 输入要用于初始绑定的客户机 DN 和密码。 • With login credentials： 使用在登录过程中呈现的凭证来进行到域控制器服务器的初始绑定。可以使用 DN、部分 DN、标准域名或者通过用户标识（与 IMM 上配置的 **UID Search Attribute** 字段相匹配）来提供用户标识。 如果凭证类似部分 DN（例如，cn=joe），那么将此部分 DN 作为前缀添加到配置的根 DN 以尝试创建与用户记录匹配的 DN。如果绑定尝试失败，那么通过将前缀 cn= 添加到登录凭证，然后将字符串的结果添加到配置的根 DN 来进行最终绑定尝试。

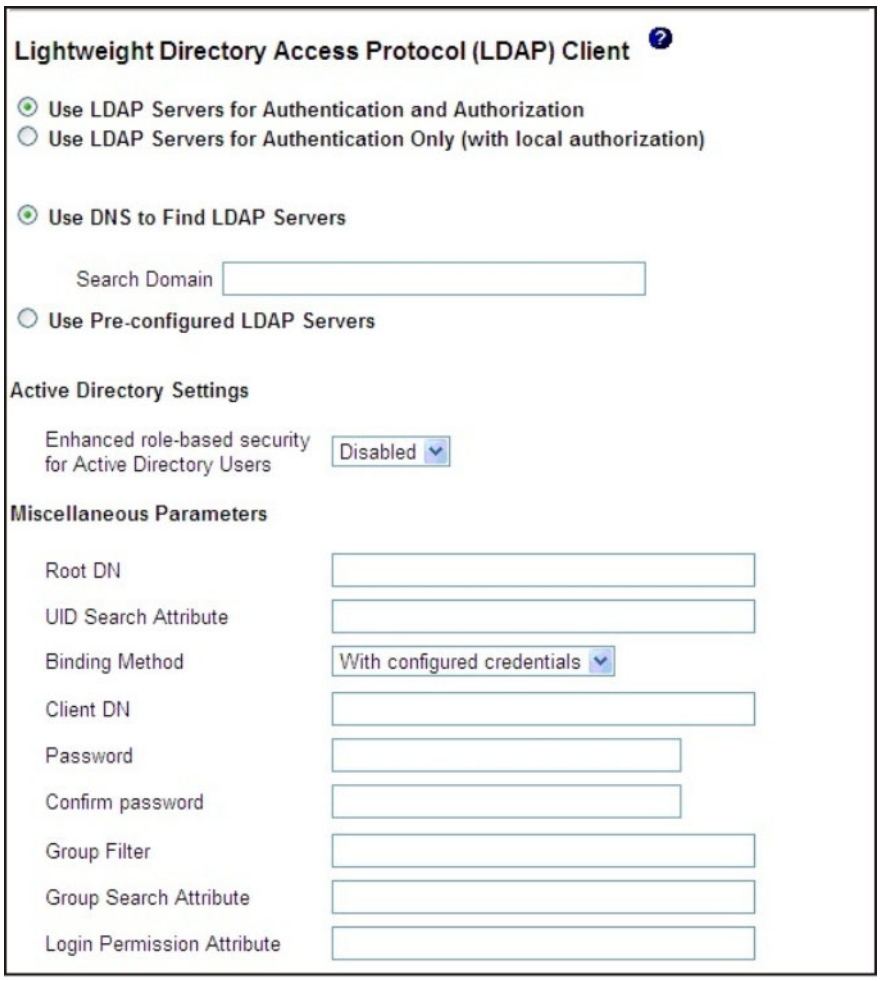
遗留 LDAP 认证和授权

遗留 LDAP 认证和授权是用于 IMM 的原始模型。遗留 LDAP 认证和授权支持 Active Directory、Novell eDirectory、OpenLDAP 环境，并依靠存储在 LDAP 服务器上的配置信息将许可权与用户关联。遗留 LDAP 认证和授权用于通过 LDAP 服务器认证和授权用户。如果在 IMM 上对 Active Directory 用户禁用了增强型基于角色安全性，那么允许您为 IMM 配置 LDAP 搜索属性。

要为 IMM 配置遗留 LDAP 认证和授权，请完成以下步骤：

1. 在导航窗格中，单击 **Network Protocols**。
2. 向下滚动至 **Lightweight Directory Access Protocol (LDAP) Client** 部分。
3. 选择 **Use LDAP Servers for Authentication and Authorization**。
4. 为 **Enhanced role-based security for Active Directory Users** 字段选择 **Disabled**。
5. 选择以下选项之一以动态发现或手动配置要用于认证的 LDAP 服务器：
   - 选择 **Use DNS to find LDAP Servers** 以基于 DNS SVR 记录动态发现 LDAP 服务器。
   - 选择 **Use Pre-Configured LDAP Servers**（缺省选择）以手动配置 LDAP 服务器。
6. 如果您在使用 DNS 来动态发现 LDAP 服务器，请配置 LDAP 服务器的域名，然后继续执行步骤 第 67 页的 8。您必须指定 LDAP 服务器的标准域名。在 **Search Domain** 字段中输入 LDAP 服务器的域名

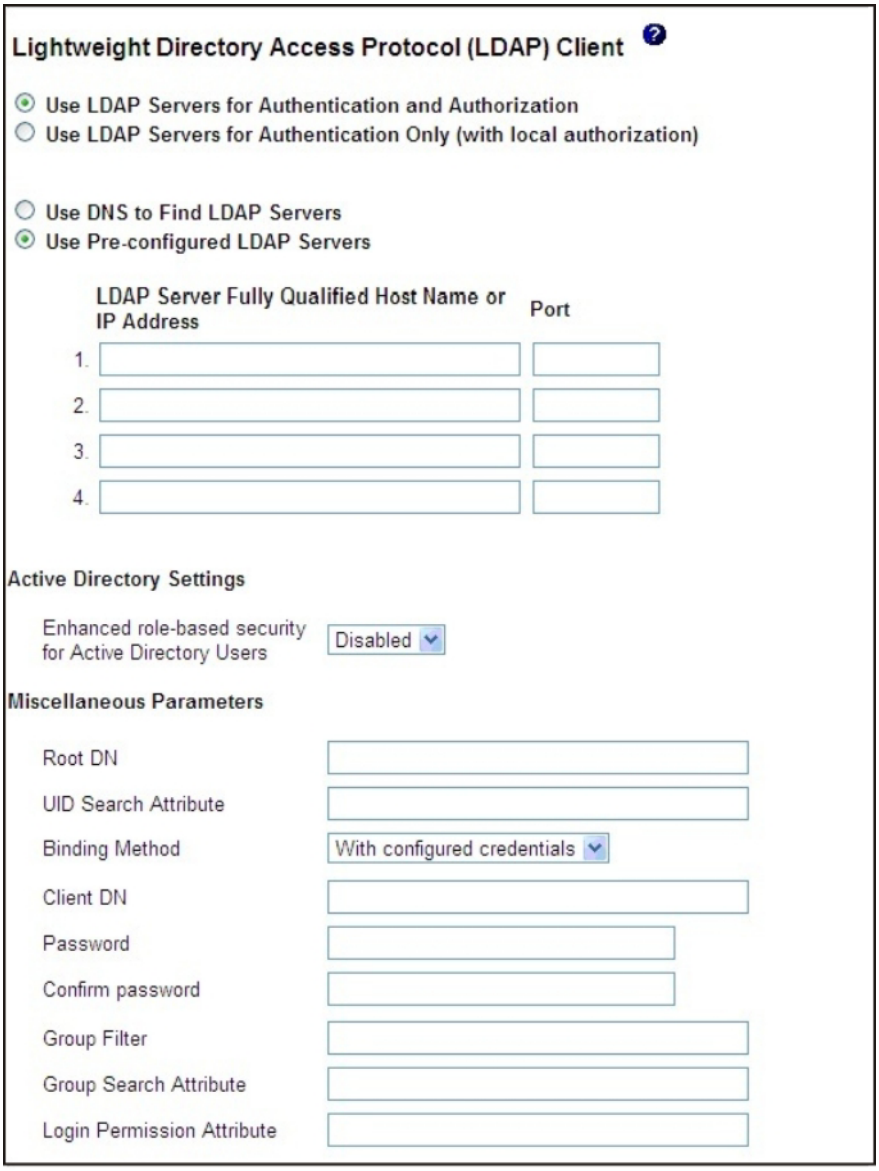
在使用 DNS 来动态发现 LDAP 服务器时，以下窗口显示“LDAP Client”窗口。



7. 如果您手动配置 LDAP 服务器，请配置 **LDAP Server Host Name or IP Address** 和 **Port** 字段，然后继续执行步骤 第 67 页的 8。

   注：使用 IP 地址或标准主机名最多可以配置四个 LDAP 服务器。

在手动配置 LDAP 服务器时，以下窗口显示“LDAP Client”窗口。



8. 通过从 **Enhanced role-based security for Active Directory Users** 菜单选择 **Disabled** 来配置 Active Directory 设置。
9. 配置其他参数。请参阅以下列表以获取必需参数字段的描述。
   - IMM 将 DN 格式的 **Root DN** 字段用作目录树的根条目。此 DN 将用作所有搜索的基础对象。示例可能类似 `dc=mycompany,dc=com`。
   - **Binding Method** 字段用于到域控制器服务器的初始绑定。使用以下绑定选项之一：
     - Anonymously：

       在不使用 DN 或密码的情况下，初始绑定到域控制器服务器。由于大多数服务器配置为不允许对特定用户记录的搜索请求，所以不鼓励使用该选项。
     - With configured credentials：

       输入要用于初始绑定的客户机 DN 和密码。

– With login credentials：

与在登录过程中提供的凭证绑定。可以使用 DN、部分 DN、标准域名或者通过用户标识（与 IMM 上配置的 **UID Search Attribute** 字段中的信息相匹配）来提供用户标识。如果凭证类似部分 DN（例如，cn=joe），那么将此部分 DN 作为前缀添加到配置的根 DN 以尝试创建匹配用户记录的 DN。如果绑定尝试失败，那么通过将前缀 cn= 添加到登录凭证，然后将字符串的结果添加到配置的根 DN 来进行最终绑定尝试。

- **Group Filter** 字段用于组认证。它指定 IMM 所属的组。如果组过滤器留空，那么组认证将自动成功。如果启用，在用户认证之后进行组认证。尝试将“组过滤器”中的至少一个组与用户所属的组匹配。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，那么组认证将通过。比较是区分大小写的。

  禁用组认证时，用户自己的记录必须包含许可权属性；否则，将拒绝访问。对于匹配过滤器的每个组，将与该组关联的许可权分配到该用户。通过检索登录许可权属性信息找到与组关联的许可权。

  过滤器限制为 511 个字符，且包含一个或多个组名。冒号 (:) 字符必须用于指定多个组名。忽略前导空格和尾随空格，将其他所有空格视为组名的一部分。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 等于 cn=adminGroup,dc=mycompany,dc=com 的组。

  注：先前使用的星号 (*) 不再被视为通配符。出于安全原因，除去通配符概念。

- **Group Search Attribute** 字段由搜索算法用于查找特定用户的组成员资格信息。配置组过滤器名称时，必须从 LDAP 服务器检索用户所属的组的列表。需要该列表才能执行组认证。要检索此列表，发送到 LDAP 服务器的搜索过滤器必须指定与组关联的属性名称。**Group Search Attribute** 字段指定属性名称。

  在 Active Directory 或 Novell eDirectory 环境中，**Group Search Attribute** 字段指定将标识用户所属的组的属性名称。在 Active Directory 中，使用属性 **memberOf**，对于 Novell eDirectory，使用属性 **groupMembership**。在 OpenLDAP 服务器环境中，一般将用户分配到其 objectClass 为 PosixGroup 的组中。在此上下文中，Group Search Attribute 参数指定标识特定 PosixGroup 的成员的属性名称；这通常是 **memberUid**。如果 **Group Search Attribute** 字段留空，那么过滤器中的属性名称缺省为 **memberOf**。

- **Login Permission Attribute** 字段指定与用户的登录许可权关联的属性名称。用户使用 LDAP 服务器成功认证时，有必要检索该用户的登录许可权。

  注：该 **Login Permission Attribute** 字段不得为空；否则，无法检索用户的许可权。如果没有经验证的许可权，登录尝试将失败。

  使用关键字字符串 IBMRBSPermissions= 来搜索 LDAP 服务器返回的属性值。该关键字后面必须紧跟二进制位串（最多为 12 个连续的 0 或 1）。每个位表示一组特定功能。根据其位置将位编号。最左边的位是位置 0 位，最右边的位是位置 11 位。处于特定位置的值 1 启用该特定功能。值 0 将禁用该功能。例如，字符串 IBMRBSPermissions=010000000000。

  IBMRBSPermissions= 关键字可以置于 **Login Permission Attribute** 字段中的任何位置。这允许 LDAP 管理员复用现有属性；因此，阻止 LDAP 模式的扩展并

允许该属性用于其原始用途。现在，该用户可以在该字段的开头、结尾或任何位置添加关键字字符串。使用的属性将允许自由格式的字符串。

下表提供每个位位置的说明。

表 13. 许可权位

位位置	功能	说明
0	始终拒绝	如果设置，那么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	如果设置，那么会给予用户管理员特权。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	如果设置，那么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）。无法使用保存、清除或复原功能修改任何内容。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。如果设置了任何其他位，那么将忽略此位。
3	联网和安全性	如果设置，那么用户可以在 Security、Network Protocols、Network Interface、Port Assignments 和 Serial Port 面板中修改配置。
4	用户帐户管理	如果设置，那么用户可以添加、修改或删除用户并可以在 Login Profiles 面板中更改 Global Login Settings。
5	远程控制台访问	如果设置，那么用户可以访问远程服务器控制台，并且可以在 Serial Port 面板中修改配置。
6	远程控制台和远程磁盘访问	如果设置，那么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。用户还可在 Serial Port 面板中修改配置。
7	远程服务器电源/重新启动访问	如果设置，那么用户可以访问远程服务器的开机、重新启动和服务器超时功能。
8	基本适配器配置	如果设置，那么用户可以在 System Settings 和 Alerts 面板中修改配置参数（Contact、Location 和 Server Timeout 参数除外）。
9	清除事件日志的能力	如果设置，那么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。

表 13. 许可权位 (续)

位位置	功能	说明
10	高级适配器配置	如果设置，那么用户在配置适配器时没有任何限制，并且用户对 IMM 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、复原适配器出厂缺省值、根据配置文件修改和复原适配器配置以及重新启动/重置适配器。不包括服务器电源/重新启动和超时功能。
11	保留	此位位置保留供将来使用（当前已忽略）。

备注：

- 如果未使用位，那么缺省值将针对用户设置为 Read Only。
- 向直接从用户记录中检索到的登录许可权指定优先级。如果用户记录在 **Login Permission Attribute** 字段中不包含名称，那么将尝试从用户所属的组中检索与组过滤器匹配的许可权。在此情况下，会为用户分配所有组的所有位的包含 OR。
- 如果为任何组设置了“始终拒绝”（位位置为 0）位，那么用户将被拒绝访问。“始终拒绝”位优先于所有位。
- 如果用户能够修改基本、联网或安全性相关适配器配置参数，那么应考虑为该用户提供重新启动 IMM（位位置为 10）的能力。如果没有此能力，那么用户可能可以更改参数；但是，参数将不会生效。

配置安全性

您可以使用此部分中的常规过程为敏感数据加密、IMM Web 服务器、IMM 和 IBM Systems Director 之间的连接、IMM 和 LDAP 服务器之间的连接以及密码术管理配置安全性。如果您不熟悉 SSL 证书的使用，请阅读第 72 页的『SSL 证书』中的信息。

要配置 IMM 安全性，请执行以下操作：

1. 配置敏感数据加密：
   a. 在导航窗格中，单击 **Security**。滚动至 **Enable Data Encryption** 部分，然后选择 **Enable** 启用数据加密。要禁用数据加密，请选择 **Disable**。
2. 配置安全 Web 服务器：
   a. 在导航窗格中，单击 **Security**。滚动至 **HTTPS Server Configuration for Web Server** 部分，然后选择 **Disable** 禁用 SSL 服务器。
   b. 要生成或导入证书，请单击导航窗格中的 **Security**，然后滚动至 **HTTPS Server Certificate Management** 部分。请参阅第 73 页的『SSL 服务器证书管理』，以获取有关管理证书的更多信息。
   c. 要启用 SSL 服务器，请单击导航窗格中的 **Security**，然后滚动至 **HTTPS Server Configuration for Web Server** 部分。请参阅第 76 页的『为安全 Web 服务器或 IBM Systems Director over HTTPS 启用 SSL』，以获取有关启用 SSL 的更多信息。
3. 配置 IBM Systems Director 连接：
   a. 要禁用 **Systems Director over HTTPS** 设置，请单击导航窗格中的 **Security**，然后滚动至 **IBM Systems Director over HTTPS Server Configuration** 部分。

b. 要生成或导入证书，请单击导航窗格中的 **Security**，然后滚动至 **IBM Systems Director over HTTPS Server Certificate Management** 部分。有关更多信息，请参阅第 73 页的『SSL 服务器证书管理』。

c. 要启用 SSL 服务器，请单击导航窗格中的 **Security**，然后滚动至 **IBM Systems Director over HTTPS Server Configuration** 部分。请参阅第 76 页的『为安全 Web 服务器或 IBM Systems Director over HTTPS 启用 SSL』，以获取有关启用 SSL 的更多信息。

4. 配置 LDAP 连接的 SSL 安全性：

   a. 要禁用 SSL 客户机，请单击导航窗格中的 **Security**，然后滚动至 **SSL Client Configuration for LDAP Client** 部分。

   b. 要生成或导入证书，请单击导航窗格中的 **Security**，然后滚动至 **SSL Client Certificate Management** 部分。有关更多信息，请参阅第 73 页的『SSL 服务器证书管理』。

   c. 要导入一个或多个可信证书，请单击导航窗格中的 **Security**，然后滚动至 **SSL Client Trusted Certificate Management** 部分。有关更多信息，请参阅 SSL 客户机可信证书管理。

   d. 要启用 SSL 客户机，请单击导航窗格中的 **Security**，然后滚动至 **SSL Client Configuration for LDAP Client** 部分。有关更多信息，请参阅第 76 页的『为安全 Web 服务器或 IBM Systems Director over HTTPS 启用 SSL』。

5. 配置密码术管理：

   a. 在导航窗格中，单击 **Security**，然后滚动至 **Cryptography Management** 部分。选择 **Basic Compatible Mode**。

   b. 在导航窗格中，单击 **Security**，然后滚动至 **Cryptography Management** 部分。选择 **High Security Mode**。

6. 重新启动 IMM，以应用 SSL 服务器配置更改。有关更多信息，请参阅第 82 页的『重新启动 IMM』。

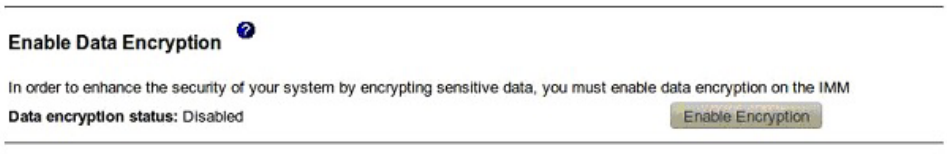
   注：对数据加密和 SSL 客户机配置的更改会立即生效，无需重新启动 IMM。

启用数据加密

缺省情况下，将在不加密的情况下保存敏感数据，以保持与先前版本兼容。要增强系统的安全性，您必须在 IMM 上启用数据加密。

要启用数据加密，请完成以下过程：

1. 在导航窗格中，单击 **Security**。



2. 单击 **Enable Encryption** 以启用数据加密。

   注：

   - 如果需要将 IMM 固件版本 1.42 降级到不提供数据加密的先前版本，那么必须在降级前禁用数据加密。如果在降级前未禁用数据加密，将丢失帐户信息。

- 如果将来需要禁用数据加密，请选择 **Disable Encryption** 来禁用数据加密。

保护 Web 服务器、IBM Systems Director 和安全 LDAP

安全套接字层 (SSL) 是一种用于提供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 IMM 配置为使用 SSL 支持进行两种类型的连接：安全服务器 (HTTPS) 和安全 LDAP 连接 (LDAPS)。 IMM 充当 SSL 客户机或 SSL 服务器，具体取决于连接类型。

下表显示针对安全 Web 服务器连接和安全 LDAP 连接 IMM 的角色。

表 14. IMM SSL 连接支持

连接类型	**SSL** 客户机	**SSL** 服务器
安全 Web 服务器 (HTTPS)	Web 浏览器（例如：Microsoft Internet Explorer）	IMM Web 服务器
安全 IBM Systems Director 连接	IBM Systems Director	IMM Systems Director 服务器
安全 LDAP 连接 (LDAPS)	IMM LDAP 客户机	LDAP 服务器

您可以通过 Security 页面查看或更改 SSL 设置，包括启用或禁用 SSL，以及管理 SSL 的所需证书。

SSL 证书

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。

自签名证书是使用 SSL 的最简单方法，但是该方法会带来安全性风险。使用自签名方法时，针对 SSL 客户机和 SSL 服务器之间首次尝试的连接，SSL 客户机无法验证 SSL 服务器的身份。第三方有可能会冒充服务器，并拦截 IMM 和 Web 浏览器之间的数据流。如果在浏览器和 IMM 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）。

为获取更高安全性，可以使用认证中心签名的证书。要获取已签名的证书，请使用 SSL Certificate Management 页面生成证书签名请求。必须将该证书签名请求发送至认证中心，并进行相应安排以获取证书。收到证书后，通过 **Import a Signed Certificate** 链接将证书导入到 IMM 中，然后可以启用 SSL。

认证中心的功能是验证 IMM 的身份。证书包含认证中心和 IMM 的数字签名。如果某知名认证中心发放了证书，或者认证中心的证书已导入到 Web 浏览器中，那么浏览器可以验证该证书，并明确地识别 IMM Web 服务器。

IMM 需要一个安全 Web 服务器证书和一个安全 LDAP 客户机证书。另外，安全 LDAP 客户机还需要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 服务器证书的认证中心所发出的证书。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。

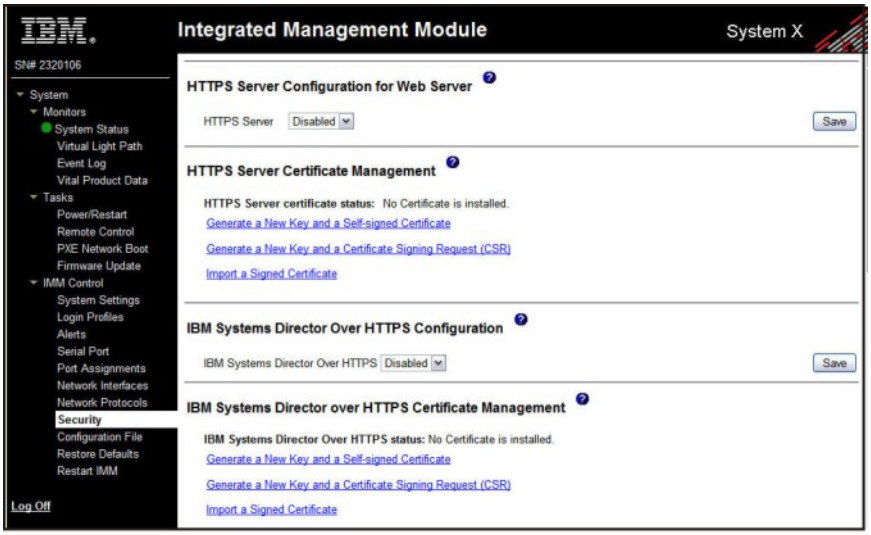
SSL 服务器证书管理

SSL 服务器要求在启用 SSL 前安装有效的证书和对应的专用加密密钥。可以使用两种方法生成专用密钥和所需证书：使用自签名证书和使用认证中心签名的证书。如果您要针对 SSL 服务器使用自签名证书，请参阅『生成自签名证书』以获取更多信息。有关针对 SSL 服务器使用认证中心签名的证书的更多信息，请参阅第 74 页的『生成证书签名请求』。

生成自签名证书

要生成新的专用加密密钥和自签名证书，请完成以下步骤：

1. 单击导航窗格中的 **Security**，将会显示以下页面。



2. 在 **SSL Server Configuration for Web Server** 区域或 **IBM Systems Director Over HTTPS Configuration** 区域中，确保设置为 **Disabled**。如果未将其禁用，请选择 **Disabled**，然后单击 **Save**。

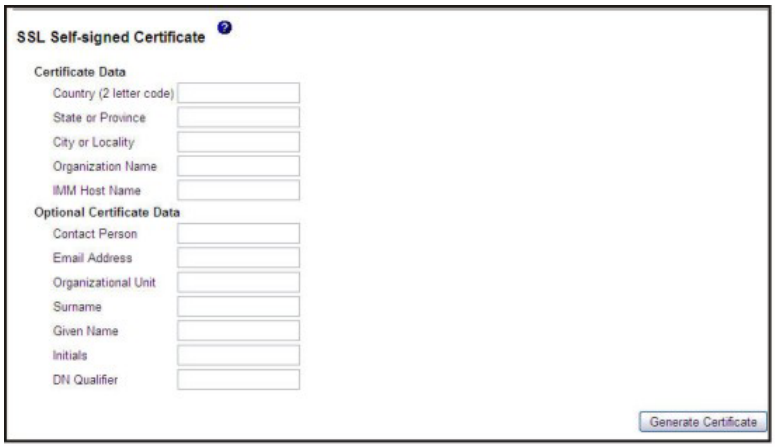
   注：

   a. 必须重新启动 IMM，然后所选值（**Enabled** 或 **Disabled**）才会生效。

   b. 必须安装到位有效的 SSL 证书，然后才能启用 SSL。

   c. 要使用 SSL，必须将客户机 Web 浏览器配置为使用 SSL3 或 TLS。不能使用仅具有 SSL2 支持的较旧的导出级浏览器。

3. 在 **SSL Server Certificate Management** 区域中，选择 **Generate a New Key and a Self-signed Certificate**。此时会显示一个类似于下图中的页面。

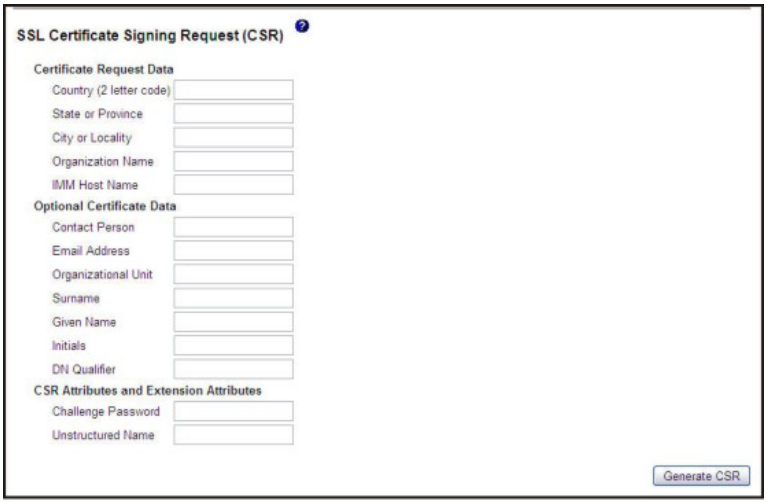


4. 在必填字段及任何适用于您配置的可选字段中输入信息。有关字段的描述，请参阅 “Required certificate data”。 74. 完成输入信息后，单击 **Generate Certificate**。此时会生成新的加密密钥和证书。此过程可能需要几分钟时间。如果安装了自签名证书，那么会显示确认。

生成证书签名请求

要生成新的专用加密密钥和证书签名请求，请完成以下步骤：

1. 在导航窗格中，单击 **Security**。
2. 在 **SSL Server Configuration for Web Server** 区域中，确保禁用 SSL 服务器。如果未将其禁用，请在 **SSL Server** 字段中选择 **Disabled**，然后单击 **Save**。
3. 在 **SSL Server Certificate Management** 区域中，选择 **Generate a New Key and a Certificate-Signing Request**。此时会显示一个类似于下图中的页面。



4. 在必填字段及任何适用于您配置的可选字段中输入信息。这些字段与自签名证书相同，并带有一些附加字段。

   请阅读以下部分中的信息，以获取各公共字段的描述。

   Required certificate data 以下用户输入字段对于生成自签名证书或证书签名请求是必填的：

Country

使用此字段以指示 IMM 实际所在的国家或地区。此字段必须包含 2 字符国家或地区代码。

State or Province

使用此字段以指示 IMM 实际所在的州或省。此字段可以包含最多 30 个字符。

City or Locality

使用此字段以指示 IMM 实际所在的城市或位置。此字段可以包含最多 50 个字符。

Organization Name

使用此字段以指示拥有 IMM 的公司或组织。当该字段用于生成证书签名请求时，发放认证中心可以验证请求证书的组织是否依法享有声明指定公司或组织名称的所有权的权利。此字段可以包含最多 60 个字符。

IMM Host Name

使用此字段以指示当前出现在浏览器 Web 地址栏中的 IMM 主机名。

确保您在此字段中输入的值与 Web 浏览器所识别的主机名精确匹配。浏览器会将已解析 Web 地址中的主机名与证书中出现的名称相比较。要防止浏览器发出证书警告，此字段中所使用的值必须与由浏览器用于连接到 IMM 的主机名相匹配。例如，如果 Web 地址栏中的地址为 http://mm11.xyz.com/private/main.ssi，那么用于 IMM Host Name 字段的值必须为 mm11.xyz.com。如果 Web 地址为 http://mm11/private/main.ssi，那么所使用的值必须为 mm11。如果 Web 地址为 http://192.168.70.2/private/main.ssi，那么所使用的值必须为 192.168.70.2。

此证书属性通常称为通用名称。

此字段可以包含最多 60 个字符。

Contact Person

使用此字段以指示负责 IMM 的联系人的名称。此字段可以包含最多 60 个字符。

Email Address

使用此字段以指示负责 IMM 的联系人的电子邮件地址。此字段可以包含最多 60 个字符。

Optional certificate data 以下用户输入字段对于生成自签名证书或证书签名请求是可选的：

Organizational Unit

使用此字段以指示拥有 IMM 的公司或组织内的单位。此字段可以包含最多 60 个字符。

Surname

使用此字段以获取其他信息，如负责 IMM 的个人的姓氏。此字段可以包含最多 60 个字符。

Given Name

使用此字段以获取其他信息，如负责 IMM 的个人的名字。此字段可以包含最多 60 个字符。

Initials

使用此字段以获取其他信息，如负责 IMM 的个人的姓名首字母。此字段可以包含最多 20 个字符。

DN Qualifier

使用此字段以获取其他信息，如 IMM 的专有名称限定符。此字段可以包含最多 60 个字符。

Certificate-Signing request attributes 除非您选择的认证中心需要，否则以下字段是可选的：

Challenge Password

使用此字段以向证书签名请求分配密码。此字段可以包含最多 30 个字符。

Unstructured Name

使用此字段以获取其他信息，如分配给 IMM 的非结构化名称。此字段可以包含最多 60 个字符。

5. 填写这些信息后，单击 **Generate CSR**。此时会生成新的加密密钥和证书。此过程可能需要几分钟时间。
6. 单击 **Download CSR**，然后单击 **Save** 以将文件保存到工作站。创建证书签名请求时生成的文件为 DER 格式。如果认证中心希望数据为其他某种格式（如 PEM），那么可以使用诸如 OpenSSL (http://www.openssl.org) 之类的工具对文件进行转换。如果认证中心请求您将证书签名请求文件的内容复制到 Web 浏览器窗口中，那么通常应该使用 PEM 格式。

   用于通过 OpenSSL 将证书签名请求从 DER 转换为 PEM 格式的命令与以下示例类似：

   ```
   openssl req -in csr.der -inform DER -out csr.pem -outform PEM
   ```

7. 将证书签名请求发送到认证中心。当认证中心返回已签名证书时，您可能必须将证书转换为 DER 格式。（如果在电子邮件或 Web 页面中以文本形式接收到证书，那么该证书可能为 PEM 格式。）您可以使用由认证中心提供的工具或者使用诸如 OpenSSL (http://www.openssl.org) 之类的工具来更改格式。用于将证书从 PEM 转换为 DER 格式的命令与以下示例类似：

   ```
   openssl x509 -in cert.pem -inform PEM -out cert.der -outform DER
   ```

   在认证中心返回已签名证书之后，请转至步骤 8。
8. 在导航窗格中，单击 **Security**。滚动到 **SSL Server Certificate Management** 区域或 **IBM Systems Director Over HTTPS Certificate Management** 区域。
9. 单击 **Import a Signed Certificate**。
10. 单击 **Browse**。
11. 单击所需的证书文件，然后单击 **Open**。此时在 **Browse** 按钮旁边的字段中会显示文件名（包括完整路径）。
12. 单击 **Import Server Certificate** 以开始该过程。在文件传输到 IMM 上的存储器时，会显示进度指示器。继续显示此页面，直至传输完成。

为安全 Web 服务器或 IBM Systems Director over HTTPS 启用 SSL

完成以下步骤以启用安全 Web 服务器。

注：要启用 SSL，必须安装有效的 SSL 证书。

1. 在导航窗格中，单击 **Security**。所显示的页面会显示已安装有效的 SSL 服务器证书。如果 SSL 服务器证书状态没有显示已安装有效的 SSL 证书，请转至第 73 页的『SSL 服务器证书管理』。
2. 滚动到 **SSL Server Configuration for web Server** 区域或 **IBM Systems Director Over HTTPS Configuration** 区域，在 **SSL Client** 字段中选择 **Enabled**，然后单击 **Save**。下次重新启动 IMM 时，所选值会立即生效。

SSL 客户机证书管理

SSL 客户机要求在启用 SSL 前安装有效的证书和对应的专用加密密钥。可以使用两种方法生成专用密钥和所需证书：使用自签名证书，或者使用认证中心签名的证书。

除了应使用 Security Web 页面的 **SSL Client Certificate Management** 区域而不是使用 **SSL Server Certificate Management** 区域外，为 SSL 客户机生成专用加密密钥和证书的过程与针对 SSL 服务器的过程相同。如果您要针对 SSL 客户机使用自签名证书，请参阅第 73 页的『生成自签名证书』。如果您要针对 SSL 客户机使用认证中心签名的证书，请参阅第 74 页的『生成证书签名请求』，以获取更多信息。

SSL 客户机可信证书管理

安全 SSL 客户机（LDAP 客户机）使用可信证书来准确识别 LDAP 服务器。可信证书可以是签署了 LDAP 服务器证书的认证中心的证书，也可以是 LDAP 服务器的实际证书。启用 SSL 客户机之前，必须将至少一个证书导入到 IMM。最多可以导入三个可信证书。

要导入可信证书，请完成以下步骤：

1. 在导航窗格中，选择 **Security**。
2. 在 **SSL Client Configuration for LDAP Client** 区域中，确保禁用 SSL 客户机。如果未将其禁用，请在 **SSL Client** 字段中选择 **Disabled**，然后单击 **Save**。
3. 滚动到 **SSL Client Trusted Certificate Management** 区域。
4. 单击其中一个 **Trusted CA Certificate 1** 字段旁的 **Import**。
5. 单击 **Browse**。
6. 选择所需的证书文件，然后单击 **Open**。此时在 **Browse** 按钮旁边的框中会显示文件名（包括完整路径）。
7. 要开始导入过程，请单击 **Import Certificate**。在文件传输到 IMM 上的存储器时，会显示进度指示器。继续显示此页面，直至传输完成。

   Remove 按钮现在可用于 Trusted CA Certificate 1 选项。如果要除去可信证书，请单击对应的 **Remove** 按钮。

   可以通过使用 Trusted CA Certificate 2 和 Trusted CA Certificate 3 **Import** 按钮来导入其他可信证书。

为 LDAP 客户机启用 SSL

使用 Security 页面的 **SSL Client Configuration for LDAP Client** 区域来为 LDAP 客户机启用或禁用 SSL。要启用 SSL，必须首先安装有效的 SSL 客户机证书和至少一个可信证书。

要为客户机启用 SSL，请完成以下步骤：

1. 在导航窗格中，单击 **Security**。

   Security 页面显示已安装的 SSL 客户机证书和可信 CA 证书 1。

2. 在 SSL Client Configuration for LDAP Client 页面上的 **SSL Client** 字段中选择 **Enabled**。

   注：

   a. 所选值（Enabled 或 Disabled）会立即生效。

   b. 必须安装到位有效的 SSL 证书，然后才能启用 SSL。

   c. LDAP 服务器必须支持 SSL3 或 TLS 才能与 LDAP 客户机使用的 SSL 实施相兼容。

3. 单击 **Save**。所选值会立即生效。

密码术管理

使用 Security 页面的 **Cryptography Management** 区域，配置 IMM 中 SSL 服务器密码套件的强度，包括 HTTPS 服务器和 IBM System Director over HTTPS。

密码术管理方式具有不同的安全性强度。基本兼容方式为缺省方式，可与较早的固件版本以及未执行更严格安全性需求的浏览器和其他网络客户机兼容。高级安全性方式会将 IMM 限制为使用不短于 128 位的 SSL 对称密钥。

要配置该方式，请完成以下步骤：

1. 在导航窗格中，单击 **Security**。
2. 找到 **Cryptography Management** 区域，然后选择 **Basic Compatible Mode** 或 **High Security Mode**。
3. 单击 **Save**，所选方式将在重新启动 IMM 后生效。

配置 Secure Shell 服务器

Secure Shell (SSH) 功能提供对 IMM 的命令行界面和串行（文本控制台）重定向功能的安全访问。

Secure Shell 用户通过交换用户标识和密码进行认证。在建立加密通道后发送密码和用户标识。用户标识和密码对可以是本地存储的 12 对用户标识和密码之一，也可以存储在 LDAP 服务器上。不支持公用密钥认证。

生成 Secure Shell 服务器密钥

Secure Shell 服务器密钥用于向客户机认证 Secure Shell 服务器的身份。创建新 Secure Shell 服务器专用密钥之前，必须禁用 Secure Shell。启用 Secure Shell 服务器之前，必须创建服务器密钥。

请求新服务器密钥时，将会同时创建 Rivest、Shamir 和 Adelman 密钥与 DSA 密钥，以允许从 SSH V2 客户机对 IMM 进行访问。出于安全性原因，在配置保存和复原操作期间不会备份 Secure Shell 服务器专用密钥。

要创建新 Secure Shell 服务器密钥，请完成以下步骤：

1. 在导航窗格中，单击 **Security**。

2. 滚动到 **Secure Shell (SSH) Server** 区域并确保禁用 Secure Shell 服务器。如果未将其禁用，请在 **SSH Server** 字段中选择 **Disabled**，然后单击 **Save**。
3. 滚动到 **SSH Server Key Management** 区域。
4. 单击 **Generate SSH Server Private Key**。此时会打开进度窗口。请等待操作完成。

启用 Secure Shell 服务器

从 Security 页面上，可以启用或禁用 Secure Shell 服务器。仅在重新启动 IMM 后，进行的选择才会生效。屏幕上显示的值（Enabled 或 Disabled）是上次选择的值和重新启动 IMM 后使用的值。

注：仅当安装了有效的 Secure Shell 服务器专用密钥时，才能启用 Secure Shell 服务器。

要启用 Secure Shell 服务器，请完成以下步骤：

1. 在导航窗格中，单击 **Security**。
2. 滚动到 **Secure Shell (SSH) Server** 区域。
3. 单击 **SSH Server** 字段中的 **Enabled**。
4. 在导航窗格中，单击 **Restart IMM** 以重新启动 IMM。

使用 Secure Shell 服务器

如果您在使用 Red Hat Linux V7.3 中包含的 Secure Shell 客户机，那么要启动到网络地址为 192.168.70.132 的 IMM 的 Secure Shell 会话，请输入类似以下示例的命令：

```
ssh -x -l userid 192.168.70.132
```

其中 -x 指示没有 X Window System 转发，而 -l 指示该会话应该使用用户标识 *userid*。

复原和修改 IMM 配置

您可以整体复原已保存的配置，也可以在将配置复原到 IMM 之前修改已保存的配置中的关键字段。通过在复原配置文件之前对其进行修改，可以设置多个具有类似配置的 IMM。您可以快速指定需要唯一值（名称和 IP 地址）的参数，而不必输入常见共享信息。

要复原或修改当前配置，请完成以下步骤：

1. 登录到要在其之上复原配置的 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **Configuration File**。
3. 在 **Restore IMM Configuration** 区域中，单击 **Browse**。
4. 单击所需的配置文件，然后单击 **Open**。该文件（包括完整路径）出现在 **Browse** 旁边的框中。
5. 如果不希望对配置文件进行更改，请单击 **Restore**。此时会打开一个新窗口，其中包含 IMM 配置信息。请确保这是要复原的配置。如果它不是正确的配置，请单击 **Cancel**。

如果要在复原配置之前对配置文件进行更改，请单击 **Modify and Restore** 以打开可编辑配置摘要窗口。最初，仅会显示允许更改的字段。要在此视图和完整配置摘要视图之间进行更改，请单击窗口顶部或底部的 **Toggle View** 按钮。要修改字段的内容，请单击对应的文本框并输入数据。

注：当单击 **Restore** 或 **Modify and Restore** 时，如果您正在尝试复原的配置文件是由其他类型的服务处理器或者由具有较旧固件（因此功能较少）的同一类型的服务处理器所创建，那么可能会打开警报窗口。此警报消息包含必须在恢复完成后配置的系统管理功能的列表。某些功能需要在多个窗口上配置。

6. 要继续将此文件复原到 IMM，请单击 **Restore Configuration**。当 IMM 上的固件更新时，会显示进度指示器。将会打开确认窗口，以验证更新是否已成功。

   注：Security 页面上的安全性设置不是通过复原操作进行复原。要修改安全性设置，请参阅第 72 页的『保护 Web 服务器、IBM Systems Director 和安全 LDAP』。
7. 收到表明复原过程已完成的确认后，请在导航窗格中单击 **Restart IMM**，然后单击 **Restart**。
8. 单击 **OK** 以确认要重新启动 IMM。
9. 单击 **OK** 以关闭当前浏览器窗口。
10. 要再次登录到 IMM，请启动浏览器，然后遵循常规登录过程。

使用配置文件

在导航窗格中选择 **Configuration File** 以备份和恢复 IMM 配置。

重要信息：备份操作不会保存安全性页面设置，且无法以恢复操作恢复这些设置。

备份当前配置

您可以将当前 IMM 配置的副本下载到运行 IMM Web 界面的客户机计算机。如果意外地更改或损坏了 IMM 配置，请使用此备份副本将其复原。将其用作可修改以通过类似配置对多个 IMM 进行配置的基础。

按照此过程保存的配置信息不包括 System x® 服务器固件配置设置或任何与非 IMPI 用户界面配置不通用的 IPMI 设置。

要备份当前配置，请完成以下步骤：

1. 登录到要在其之上备份当前配置的 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **Configuration File**。
3. 在 **Backup IMM Configuration** 区域中，单击 **view the current configuration summary**。
4. 验证设置，然后单击 **Close**。
5. 要备份此配置，请单击 **Backup**。
6. 为备份输入名称，选择文件将保存在的位置，然后单击 **Save**。

   在 Mozilla Firefox 中，单击 **Save File**，然后单击 **OK**。

   在 Microsoft Internet Explorer 中，单击 **Save this file to disk**，然后单击 **OK**。

复原和修改 IMM 配置

您可以整体复原已保存的配置，也可以在将配置复原到 IMM 之前修改已保存的配置中的关键字段。通过在复原配置文件之前对其进行修改，可以设置多个具有类似配置的 IMM。您可以快速指定需要唯一值（名称和 IP 地址）的参数，而不必输入常见共享信息。

要复原或修改当前配置，请完成以下步骤：

1. 登录到要在其之上复原配置的 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **Configuration File**。
3. 在 **Restore IMM Configuration** 区域中，单击 **Browse**。
4. 单击所需的配置文件，然后单击 **Open**。该文件（包括完整路径）出现在 **Browse** 旁边的框中。
5. 如果不希望对配置文件进行更改，请单击 **Restore**。此时会打开一个新窗口，其中包含 IMM 配置信息。请确保这是要复原的配置。如果它不是正确的配置，请单击 **Cancel**。

   如果要在复原配置之前对配置文件进行更改，请单击 **Modify and Restore** 以打开可编辑配置摘要窗口。最初，仅会显示允许更改的字段。要在此视图和完整配置摘要视图之间进行更改，请单击窗口顶部或底部的 **Toggle View** 按钮。要修改字段的内容，请单击对应的文本框并输入数据。

   注：当单击 **Restore** 或 **Modify and Restore** 时，如果您正在尝试复原的配置文件是由其他类型的服务处理器或者由具有较旧固件（因此功能较少）的同一类型的服务处理器所创建，那么可能会打开警报窗口。此警报消息包含必须在恢复完成后配置的系统管理功能的列表。某些功能需要在多个窗口上配置。
6. 要继续将此文件复原到 IMM，请单击 **Restore Configuration**。当 IMM 上的固件更新时，会显示进度指示器。将会打开确认窗口，以验证更新是否已成功。

   注：Security 页面上的安全性设置不是通过复原操作进行复原。要修改安全性设置，请参阅第 72 页的『保护 Web 服务器、IBM Systems Director 和安全 LDAP』。
7. 收到表明复原过程已完成的确认后，请在导航窗格中单击 **Restart IMM**，然后单击 **Restart**。
8. 单击 **OK** 以确认要重新启动 IMM。
9. 单击 **OK** 以关闭当前浏览器窗口。
10. 要再次登录到 IMM，请启动浏览器，然后遵循常规登录过程。

复原缺省值

如果您具有 Supervisor 访问权，请使用 **Restore Defaults** 链接复原 IMM 的缺省配置。

警告： 当单击 **Restore Defaults** 时，您将丢失对 IMM 进行的所有修改。

要复原 IMM 缺省值，请完成以下步骤：

1. 登录到 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。

2. 在导航窗格中，单击 **Restore Defaults** 以复原 IMM 的缺省设置。如果这是本地服务器，那么您的 TCP/IP 连接将中断，您必须重新配置网络接口以复原连接。
3. 再次登录以使用 IMM Web 界面。
4. 重新配置网络接口以复原连接。有关网络接口的信息，请参阅第 33 页的『配置网络接口』。

重新启动 IMM

使用 **Restart IMM** 链接以重新启动 IMM。仅当您具有 Supervisor 访问权时，才能执行此功能。任何以太网连接都会临时断开。您必须再次登录才能使用 IMM Web 界面。

要重新启动 IMM，请完成以下步骤：

1. 登录到 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **Restart IMM** 以重新启动 IMM。您的 TCP/IP 或调制解调器已中断。
3. 再次登录以使用 IMM Web 界面。

可伸缩分区

通过 IMM，您可以在可伸缩复合体中配置和控制系统。

通过 IMM，您可以在可伸缩复合体中配置和控制系统。如果服务器存在错误，那么 IMM 将向事件日志返回事件代码（请参阅第 91 页的『查看事件日志』）。

1. 登录到要在其之上复原配置的 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **Scalable Partitioning**，然后单击 **Manage Partitions**。

Service Advisor 功能部件

Service Advisor 功能部件检测并收集系统硬件错误事件并自动将数据转发到 IBM 支持以确定问题。Service Advisor 功能部件还可以收集关于系统错误的数据并将数据转发到 IBM 支持。请参阅服务器的文档以查看您的服务器是否支持此功能部件。关于设置、测试和维护 Service Advisor 的指示信息包含在以下主题中。

- 配置 Service Advisor
- 使用 Service Advisor

配置 Service Advisor

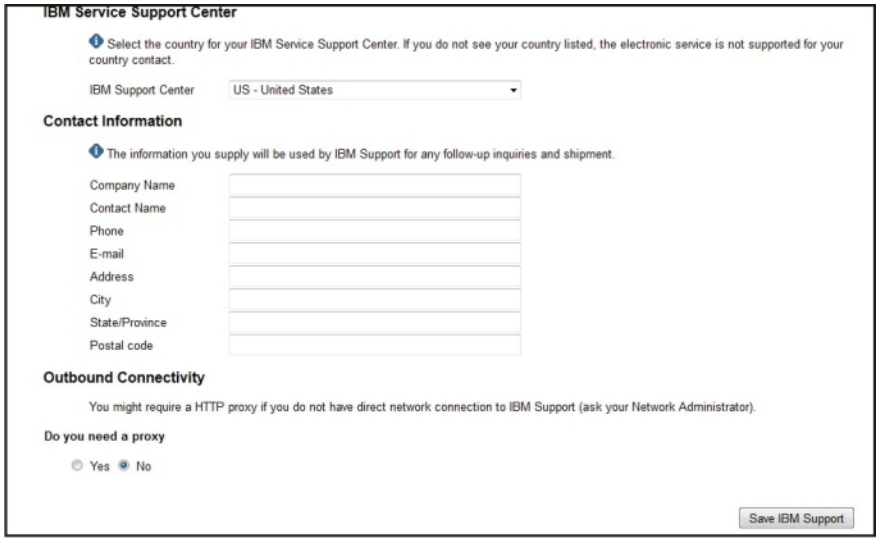
要配置 Service Advisor，请完成以下步骤。

1. 登录到要在其中激活 Service Advisor 的 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **Service Advisor**。
3. 如果这是您首次使用此选项，或者如果 IMM 重置为缺省值，那么您必须阅读和接受许可协议。
   a. 单击 **View Terms and Conditions** 以查看 Service Advisor 协议。

b. 单击 Terms and Conditions 页面上的 **I accept the agreement** 以激活 Service Advisor。

4. 单击 **Service Advisor Settings** 选项卡。

此时会显示一个类似于下图中的页面。



5. 输入服务器管理员的联系信息。请参阅下表以了解 **Contact Information** 字段的说明。

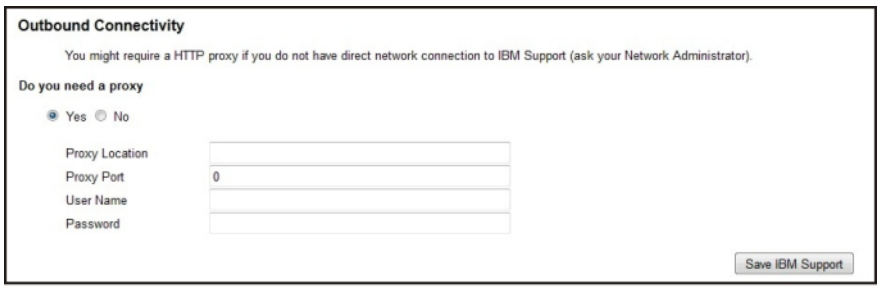
表 15. 联系信息

字段	描述
IBM Service Support Center	在此字段中指定 IBM 服务支持中心的国家或地区代码。这是两个字符的 ISO 国家或地区代码且只适用于具有 IBM 服务支持中心访问权的国家或地区。
Company Name	在此字段中指定联系人的组织或公司名称。该字段可以包含 1 到 30 个字符。
Contact Name	在此字段中指定联系人的组织或公司名称。该字段可以包含 1 到 30 个字符。
Phone	在此字段中指定联系人的电话号码。该字段可以包含 5 到 30 个字符。
Email	在此字段中指定联系人的电子邮件地址。该字段的最大长度为 30 个字符。
Address	在此字段中指定 IMM 实际所在的街道地址。该字段可以包含 1 到 30 个字符。
City	在此字段中指定 IMM 实际所在的城市或位置。
State/Province	在此字段中指定 IMM 实际所在的州或省。该字段可以包含 2 到 3 个字符。
Postal Code	在此字段中指定此服务器的位置的邮政编码。该字段可以包含 1 到 9 个字符（只有字母数字字符才有效）。

6. 如果 IMM 没有到 IBM 支持的直接网络连接，请创建 HTTP 代理。请完成以下步骤以配置出站连接信息。

a. 在 **Do you need a proxy** 字段中，单击 **Yes**。请参阅先前的插图。

此时会显示一个类似于下图中的页面。

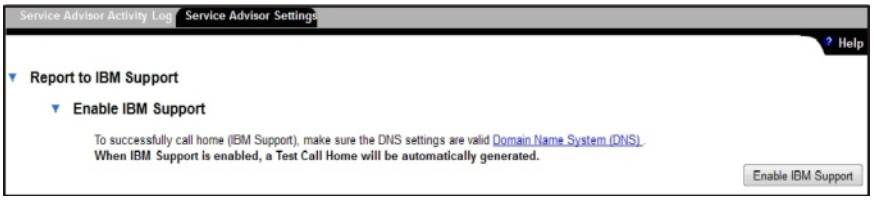


b. 在 **Proxy Location**、**Proxy Port**、**User Name** 和 **Password** 中输入信息。

7. 单击 **Save IBM Support** 以保存您的更改。
8. 单击 **Enable IBM Support**（这位于页面顶部附近）以使 Service Advisor 可以在生成可维护事件代码时联系 IBM 支持。

   注：在启用 IBM 支持之后，将会向 IBM 支持站点发送测试代码。
9. 单击 **Service Advisor Activity Log** 选项卡以查看测试代码的状态。

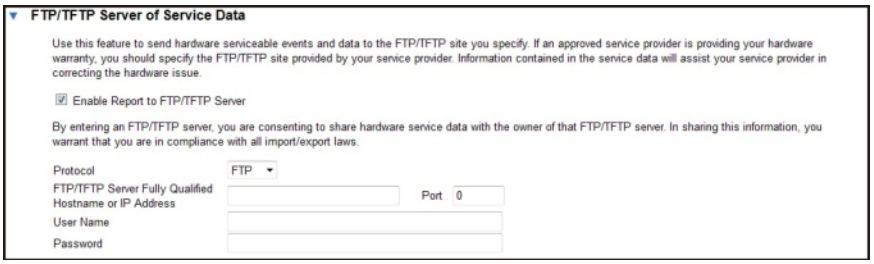
   此时会显示一个类似于下图中的页面。



10. 如果您希望在联系 IBM 支持之前允许另一服务供应商接收事件代码，请单击 **Enable Report to FTP/TFTP Server**。

    注意：输入 FTP/TFTP 服务器，您就同意与该 FTP/TFTP 服务器的所有者共享硬件服务数据。在共享此信息时，您保证遵守所有进口/出口法律。

    此时会显示一个类似于下图中的页面。



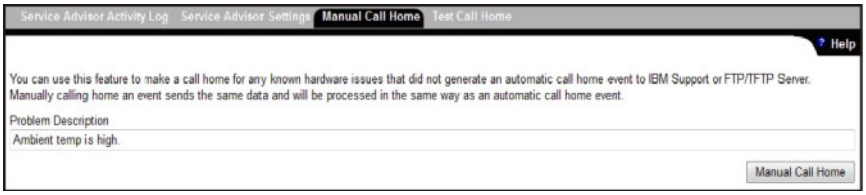
使用 Service Advisor

设置 Service Advisor 之后，您可以查看活动日志或生成测试消息。

请完成以下步骤来为服务器创建硬件问题报告：

1. 登录到要在其中使用 Service Advisor 的 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **Service Advisor**。
3. 单击 **Manual Call Home** 选项卡。

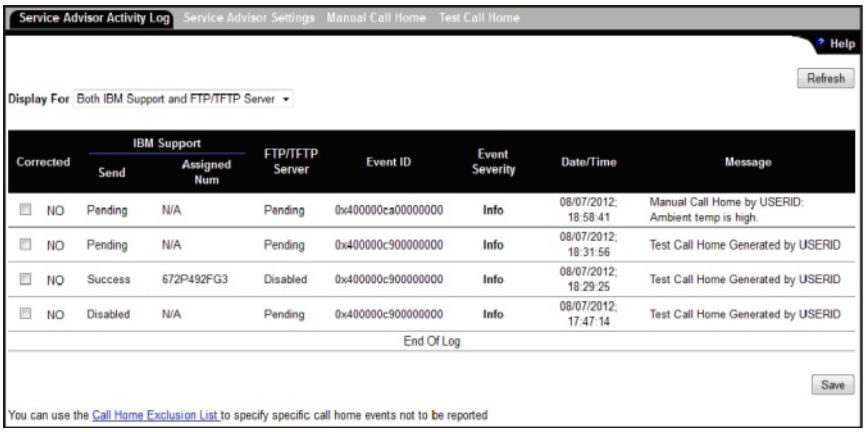
此时会显示一个类似于下图中的页面。



4. 完成以下步骤以手动回拨事件。
   a. 在 **Problem Description** 字段中输入问题描述。
   b. 单击 **Manual Call Home** 按钮。
5. 要生成测试消息，请单击 **Test Call Home** 选项卡；然后选择 **Test Call Home** 按钮。

   备注：
   - 测试回拨菜单使用当前设置来验证 IMM 与 IBM 或 FTP/TFTP 服务器之间的通信路径。
   - 如果测试失败，请验证网络设置。
   - 为了向 IBM 支持报告，Service Advisor 要求在 IMM 上正确设置 DNS 服务器地址。
   - 如果呼叫成功，将分配服务编号或凭单号。在 IBM 支持处开立的凭单将标识为测试凭单。对于测试凭单，无需来自 IBM 支持的任何操作，将关闭此呼叫。
6. 单击 **Service Advisor Activity Log** 选项卡以查看活动日志的状态。

   此时会显示一个类似于下图中的页面。



   备注：
   - 活动日志显示最近五个回拨事件，包括测试回拨和人工回拨事件。
   - **Send** 字段中的结果可以是以下结果之一：

     Success

     在 IBM 或 FTP/TFTP 处成功接收了该呼叫。**Assigned Service Number** 字段包括问题凭单号。

     Pending

     回拨事件正在进行中。

Failed 回拨事件失败。在回拨事件失败时，联系 IBM 支持以报告硬件服务事件。将不会重试失败的回拨事件。

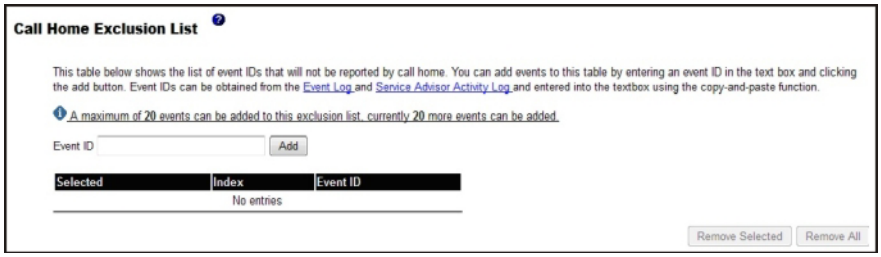
7. 在解决事件之后，单击该事件的 **Corrected** 复选框以便于查找未解决的事件。

   注：如果没有为事件选中 **Corrected** 复选框，在事件首次发生之后五天才*回拨*下次发生的同一事件。

8. 单击 **Refresh** 以显示最新信息。

   注：**Assigned Service Number** 可以用于在与 IBM 支持沟通时引用回拨事件。

9. 要从针对 IBM 支持的报告中除去指定事件，请执行以下步骤：
   a. 单击 **Call Home Exclusion List** 链接。此时会显示一个类似于下图中的页面。



   b. 将十六进制事件标识输入 **Event ID** 字段。
   c. 单击 **Add**。

注销

要注销 IMM 或其他远程服务器，请单击导航窗格中的 **Log Off**。

第 4 章 监控服务器状态

使用导航窗格中 **Monitors** 标题下方的链接，可查看您正在访问的服务器的状态。

在 System Status 页面中，可执行以下操作：

- 监控服务器的电源状态，并查看操作系统的状态
- 查看服务器温度读数、电压阈值和风扇速度
- 查看最新的服务器操作系统故障屏幕捕获
- 查看 IMM 的登录用户的列表

在 Virtual Light Path 页面中，您可以查看服务器上任何点亮的指示灯的名称、颜色和状态。

在 Event Log 页面中，可执行以下操作：

- 查看在 IMM 的事件日志中记录的特定事件
- 查看事件的严重性

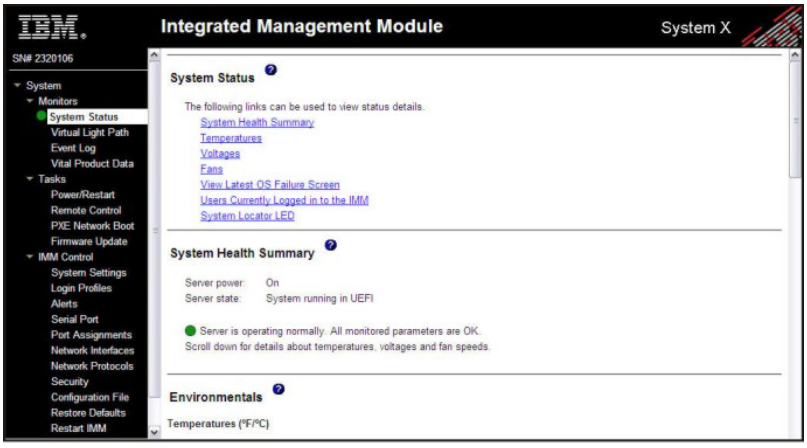
在 Vital Product Data (VPD) 页面中，您可以查看重要产品数据。

查看系统状态

在“System Status”页面上，您可以监控服务器的温度读数、电压阈值和风扇状态。您还可以查看最新的操作系统故障屏幕、登录到 IMM 的用户以及系统定位器指示灯。

要查看服务器的系统运行状况和环境信息，请完成以下步骤：

1. 登录到 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **System Status** 以查看服务器的总体运行状况的动态生成更新。此时会显示一个类似于下图中的页面。



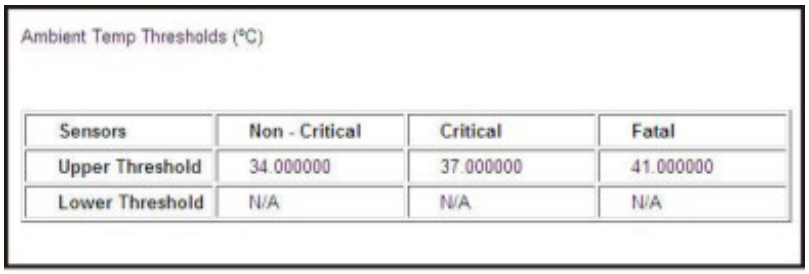
服务器的状态确定在“System Health Summary”页面顶部显示的消息。显示以下符号之一：

- 绿色实心圆圈和短语 Server is operating normally
- 包含 X 的红色圆圈或者包含惊叹号的黄色三角形以及短语 One or more monitored parameters are abnormal

如果受监视参数在正常范围之外运作，那么在“System Health Summary”页面上显示特定异常参数的列表。

3. 向下滚动到页面的 **Environmentals** 部分中的 **Temperature** 区域，其包括温度、电压和风扇转速信息。

IMM 跟踪系统组件（例如，微处理器、主板和硬盘驱动器底板）的当前温度读数和阈值级别。单击温度读数时，将打开新窗口。



“Temperature Thresholds”页面显示 IMM 反应的温度级别。温度阈值是在远程服务器上预设的，无法更改。

针对以下阈值范围测量报告的温度：

非临界　温度达到指定值时，将向配置的远程警报接收方发送温度警报。您必须选中“Alerts”页面的 **SNMP Alerts Settings** 区域中的 **Warning Alerts** 复选框或者“Remote Alert Recipient”页面上的 **Warning Alerts** 复选框以发送此警报。

有关选择警报选项的更多信息，请参阅第 30 页的『配置 SNMP 警报设置』或第 28 页的『配置远程警报接收方』。

临界　温度达到高于警告值（软关闭阈值）的指定值时，将第二个温度警报发送到配置的远程警报接收方，而服务器开始有序操作系统关闭的关闭过程。然后，服务器将自身关闭。您必须选中“Alerts”页面的 **SNMP Alerts Settings** 区域中的 **Critical Alerts** 复选框或者“Remote Alert Recipient”页面上的 **Critical Alerts** 复选框以发送此警报。

有关选择警报选项的更多信息，请参阅第 30 页的『配置 SNMP 警报设置』或第 28 页的『配置远程警报接收方』。

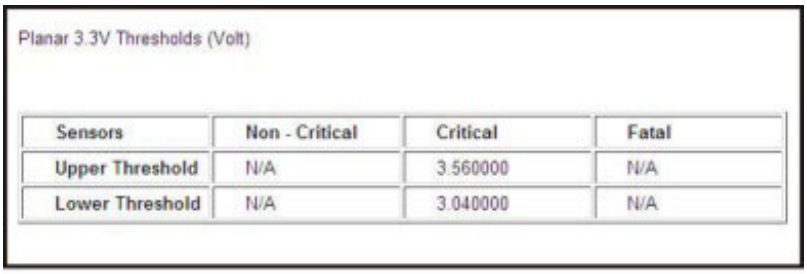
致命　温度达到高于软关闭值的指定值（硬关闭阈值）时，服务器立即关闭并将警报发送到配置的远程警报接收方。您必须选中“Alerts”页面的 **SNMP Alerts Settings** 区域中的 **Critical Alerts** 复选框或者“Remote Alert Recipient”页面上的 **Critical Alerts** 复选框以发送此警报。

有关选择警报选项的更多信息，请参阅第 30 页的『配置 SNMP 警报设置』或第 28 页的『配置远程警报接收方』。

IMM 在达到阈值时生成非临界或临界事件，如有需要，将启动关闭操作。

4. 向下滚动到 **Voltages** 区域。如果任何受监视电源电压在其指定运作范围之外，IMM 将发送警报。

   如果您单击电压读数，将打开新窗口。


Planar 3.3V Thresholds (Volt)

Sensors	Non - Critical	Critical	Fatal
Upper Threshold	N/A	3.560000	N/A
Lower Threshold	N/A	3.040000	N/A

   “Voltage Thresholds”页面显示 IMM 反应的电压范围。电压阈值是在远程服务器上预设的，无法更改。

   IMM Web 界面显示主板和稳压器模块 (VRM) 的电压读数。系统设置将执行以下操作的电压范围：

   非临界　电压低于或高于指定的电压范围时，向配置的远程警报接收方发送电压警报。您必须选中“Alerts”页面的 **SNMP Alerts Settings** 区域中的 **Warning Alerts** 复选框以发送此警报。

   有关选择警报选项的更多信息，请参阅第 30 页的『配置 SNMP 警报设置』。

   临界　电压低于或高于指定的电压范围时，向配置的远程警报接收方发送电压警报，而服务器开始有序操作系统关闭的关闭过程。然后，服务器将自身关闭。您必须选中“Alerts”页面的 **SNMP Alerts Settings** 区域中的 **Critical Alerts** 复选框以发送此警报。

   有关选择警报选项的更多信息，请参阅第 30 页的『配置 SNMP 警报设置』。

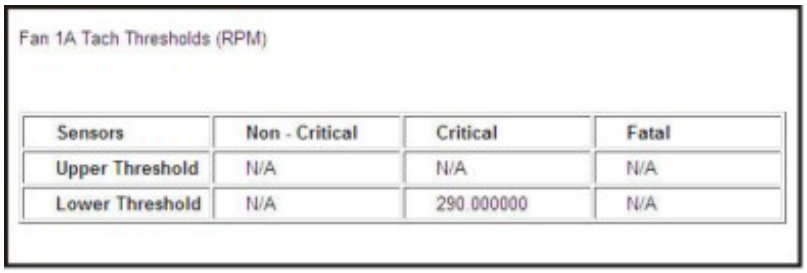
   致命　电压低于或高于指定的电压范围时，服务器立即关闭并向配置的远程警报接收方发送警报。您必须选中“Alerts”页面的 **SNMP Alerts Settings** 区域中的 **Critical Alerts** 复选框以发送此警报。

   注：仅在尚未发送软关闭警报时，才发送硬关闭警报。

   有关选择警报选项的更多信息，请参阅第 30 页的『配置 SNMP 警报设置』。

   IMM 在达到阈值时生成非临界或临界事件，如有需要，将生成任何关闭操作。
   非临界　如果 IMM 指示已达到此阈值，那么将生成警告事件。
   临界　　如果 IMM 指示已达到此阈值，那么将生成临界事件。

5. 向下滚动到 **Fan Speeds (% of max)** 区域。IMM Web 界面显示服务器风扇的运行转速（以最大风扇转速的百分比表示）。如果您单击风扇读数，将打开新窗口。


Fan 1A Tach Thresholds (RPM)

Sensors	Non - Critical	Critical	Fatal
Upper Threshold	N/A	N/A	N/A
Lower Threshold	N/A	290.000000	N/A

风扇转速降低到不可接受级别时或者风扇停止时，您收到风扇警报。您必须选中“Alerts”页面的 **SNMP Alerts Settings** 区域中的 **Critical Alerts** 复选框以发送此警报。

有关选择警报选项的更多信息，请参阅第 30 页的『配置 SNMP 警报设置』。

6. 向下滚动到 **View Latest OS Failure Screen** 区域。单击 **View OS Failure Screen** 以访问服务器停止运行时捕获的操作系统故障屏幕的图像。

   注：

   仅 IMM Premium 提供了操作系统故障截屏功能。有关从 IMM Standard 升级到 IMM Premium 的信息，请参阅第 4 页的『从 IMM Standard 升级至 IMM Premium』。

   如果发生导致操作系统停止运行的事件，那么将触发操作系统看守程序，这使 IMM 捕获操作系统故障屏幕数据并将其存储。IMM 只存储最近的错误事件信息，发生新的错误事件时覆盖更旧的操作系统故障屏幕数据。

   要远程访问服务器操作系统故障屏幕图像，请完成以下步骤：

   a. 登录到 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
   b. 在导航窗格中，单击 **System Health**，然后向下滚动到 **View Latest OS Failure Screen** 区域。
   c. 单击 **View OS Failure Screen**。在屏幕上显示操作系统故障屏幕图像。

7. 向下滚动到 **Users Currently Logged in** 区域。 IMM Web 界面显示登录到 IMM 的每个用户的登录标识和访问方法。
8. 向下滚动到 **System Locator LED** 区域。 IMM Web 界面显示系统定位器指示灯的状态。它还提供按钮来更改指示灯的状态。有关在此区域中显示的图像的含义，请参阅联机帮助。

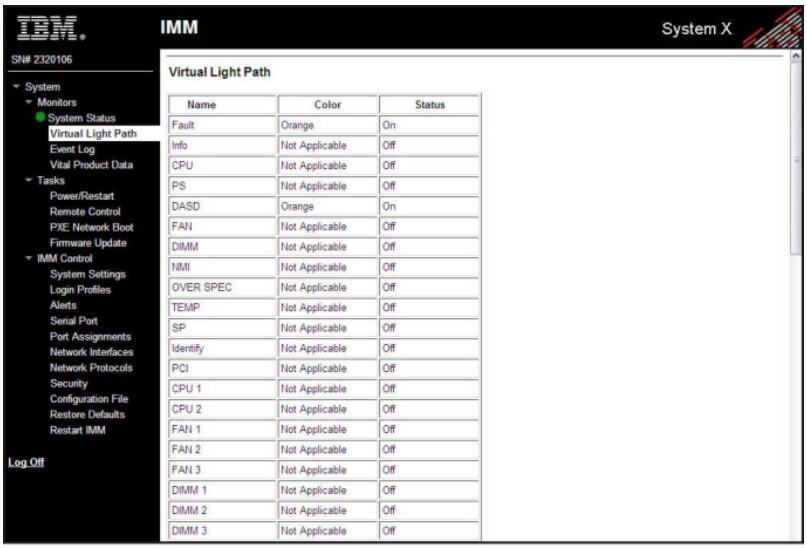
查看虚拟光通路

“虚拟光通路”屏幕显示在服务器上点亮的任何指示灯的名称、颜色和状态。

要访问和查看虚拟光通路，请完成以下步骤：

1. 登录到 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。

2. 在导航窗格中，单击 **Virtual Light Path** 以查看服务器上事件的最近历史记录。此时会显示一个类似于下图中的页面。



3. 向下滚动以查看虚拟光通路的完整内容。

   注： 如果在服务器上没有点亮指示灯，那么 Virtual Light Path 表的 Color 列指示该指示灯颜色不可用。

查看事件日志

注：有关特定事件或消息的说明，请参阅您的服务器文档。
错误代码和消息都显示在以下类型的事件日志中：

- 系统事件日志：该日志包含 POST 和系统管理中断 (SMI) 事件以及由嵌在 IMM 中的 BMC 生成的所有事件。您可以通过 Setup Utility 查看系统事件日志，也可以通过 Dynamic System Analysis (DSA) 程序查看（作为 IPMI 事件日志）。

  系统事件日志的大小受限制。如果日志已满，新条目不会覆盖现有条目；因此，必须定期进行保存，并通过 Setup Utility 清除系统事件日志。进行故障诊断时，您可能必须保存并清空系统事件日志，以使用最新事件来进行分析。

  屏幕左侧列出消息，而屏幕右侧则显示所选消息的详细信息。要从一个条目移到下一个条目，请使用向上方向键 (↑) 和向下方向键 (↓)。

  系统事件日志在事件发生时指示断言事件。当不再发生事件时指示取消断言事件。

  某些 IMM 传感器在到达其设定点时会导致记录断言事件。当不再满足设定点条件时，将记录相应的取消断言事件。然而，并不是所有事件都是断言类型的事件。
- 集成管理模块 **(IMM)** 事件日志：该日志包含对所有 IMM、POST 和系统管理中断 (SMI) 事件进行过滤后得到的子集。您可以通过 IMM Web 界面查看 IMM 事件日志，也可以通过 DSA 程序查看（作为 ASM 事件日志）。
- **DSA** 日志：该日志是由 DSA 程序生成的，并且是由系统事件日志（作为 IPMI 事件日志）、IMM 机箱事件日志（作为 ASM 事件日志）和操作系统事件日志按照时间先后顺序合并而成的。您可以通过 DSA 程序查看 DSA 日志。

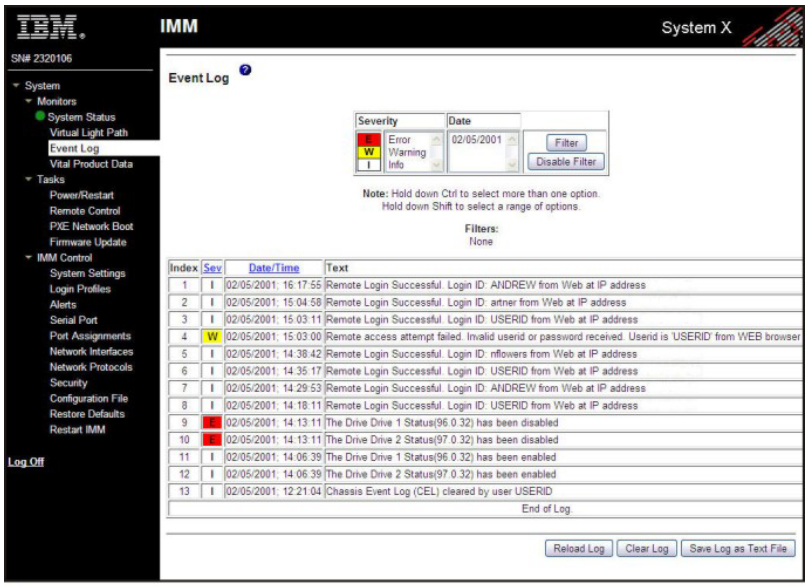
- 机箱事件日志：IMM 为 IPMI 断言和取消断言事件生成文本消息，并在机箱事件日志中为其创建条目。该文本是通过分布式管理任务组织 (DMTF) 规范 DSP0244 和 DSP8007 针对这些事件生成的。此日志还包含除 IPMI 传感器断言和取消断言之外事件的条目，例如，机箱事件日志包括用户更改网络设置或用户登录到 Web 界面时的条目。可通过 IMM Web 界面查看此日志。

从 **Web** 界面查看系统事件日志

注：系统事件日志容量有限。达到该限制时，将按先进先出的顺序删除后更旧的事件。

要访问和查看事件日志，请完成以下步骤：

1. 登录到 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **Event Log** 以查看服务器上事件的最近历史记录。此时会显示一个类似于下图中的页面。



3. 向下滚动以查看事件日志的完整内容。给予事件以下严重性级别：

   参考　此严重性级别分配给您应该记录的事件。

   警告　此严重性级别分配给可能影响服务器性能的事件。

   错误　此严重性级别分配给需要立即关注的事件。

   IMM Web 界面在 severity 列中通过黄色背景上字母 W 来突出警告事件，通过红色背景上的字母 E 来突出错误事件。
4. 单击 **Save Log as Text File** 将事件日志的内容另存为文本文件。单击 **Reload Log** 以刷新事件日志的显示。单击 **Clear Log** 以删除事件日志的内容。

通过 **Setup Utility** 查看事件日志

有关使用 Setup Utility 的完整信息，请参阅服务器随附的文档。

要查看 POST 事件日志或系统事件日志，请完成以下步骤：

1. 开启服务器。

   注：服务器连接到交流电源大约 2 分钟后，电源控制按钮便会激活。
2. 当显示提示 `<F1> Setup` 时，请按 F1 键。如果您同时设置了开机密码和管理员密码，必须输入管理员密码才能查看事件日志。
3. 选择 **System Event Logs** 并执行以下某个过程：
   - 要查看 POST 事件日志，请选择 **POST Event Viewer**。
   - 要查看系统事件日志，请选择 **System Event Log**。

在不重新启动服务器的情况下查看事件日志

如果服务器未挂起，您可以通过一些方法在不重新启动服务器的情况下查看一个或多个事件日志。

如果您安装了 Portable Dynamic System Analysis (DSA) 或 Installable Dynamic System Analysis (DSA)，那么可以用它来查看系统事件日志（作为 IPMI 事件日志）、IMM 事件日志（作为 ASM 事件日志）、操作系统事件日志或这三者合并的 DSA 日志。您还可以使用 DSA Preboot 来查看这些日志，但必须重新启动服务器才能使用 DSA Preboot。要安装 Portable DSA、Installable DSA 或 DSA Preboot，或要下载 DSA Preboot CD 映像，请转至 http://www.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=SERV-DSA&brandind=5000008，或完成以下步骤。

注：IBM Web 站点会定期进行更改。实际的过程可能与本文档中的描述略有不同。

1. 转至 http://www.ibm.com/systems/support/。
2. 在 **Product support** 下单击 **System x**。
3. 在 **Popular links** 下单击 **Software and device drivers**。
4. 在 **Related downloads** 下单击 **Dynamic System Analysis (DSA)**，以显示可下载的 DSA 文件列表。

如果服务器中安装了 IPMItool，那么可以用它来查看系统事件日志。最新版本的 Linux 操作系统中自带了最新版本的 IPMItool。有关 IPMItool 的信息，请转至 http://sourceforge.net/。

注：IBM Web 站点会定期进行更改。实际的过程可能与本文档中的描述略有不同。

1. 请转至 http://publib.boulder.ibm.com/infocenter/toolsctr/v1r0/index.jsp。
2. 在导航窗格中，单击 **IBM System x and BladeCenter Tools Center**。
3. 展开 **Tools reference**，展开 **Configuration tools**，展开 **IPMI tools**，然后单击 **IPMItool**。

有关 IPMI 的概述，请访问 http://publib.boulder.ibm.com/infocenter/systems/index.jsp?topic=/liaai/ipmi/liaaiipmi.htm 或完成以下步骤：

1. 转至 http://publib.boulder.ibm.com/infocenter/systems/index.jsp。
2. 在导航窗格中，单击 **IBM Systems Information Center**。

3. 展开 **Operating systems**，展开 **Linux information**，展开 **Blueprints for Linux on IBM systems**，然后单击 **Using Intelligent Platform Management Interface (IPMI) on IBM Linux platforms**。

您可以通过 IMM Web 界面中的 **Event Log** 链接来查看 IMM 事件日志。

下表描述了可用于查看事件日志的方法，具体使用哪种方法取决于服务器的状态。前两种状态通常不需要重新启动服务器。

表 16. 用于查看事件日志的方法

状态	操作
服务器未挂起且已连接到网络。	使用以下任何方法： • 运行 Portable DSA 或 Installable DSA 来查看事件日志，或者创建可发送给 IBM 服务与支持人员的输出文件。 • 输入 IMM 的 IP 地址并转至 Event Log 页面。 • 使用 IPMItool 来查看系统事件日志。
服务器未挂起且未连接到网络。	在本地使用 IPMItool 来查看系统事件日志。
服务器已挂起。	• 如果安装了 DSA Preboot，重新启动服务器并按 F2 以启动 DSA Preboot 以及查看事件日志。 • 如果未安装 DSA Preboot，插入 DSA Preboot CD，然后重新启动服务器以启动 DSA Preboot 和查看事件日志。 • 此外，还可以重新启动服务器并按 F1 键来启动 Setup Utility，以查看 POST 事件日志或系统事件日志。有关更多信息，请参阅第 93 页的『通过 Setup Utility 查看事件日志』。

查看重要产品数据

服务器启动时，IMM 收集服务器信息、服务器固件信息以及服务器组件重要产品数据 (VPD) 并将其存储在非易失性存储器中。您可以随时从几乎任何计算机访问此信息。Vital Product Data 页面包含关于 IMM 监视的远程受管服务器的关键信息。

要查看服务器组件重要产品数据，请完成以下步骤：

1. 登录到 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **Vital Product Data** 以查看服务器上硬件和软件组件的状态。
3. 向下滚动以查看以下 VPD 读数：

   机器级别 **VPD**

   在此区域中显示服务器的重要产品数据。为了查看 VPD，机器级别 VPD 包括通用唯一标识 (UUID)。

注：机器级别 VPD、组件级别 VPD 和组件活动日志仅在服务器开启时才提供信息。

表 17. 机器级别重要产品数据

字段	功能
Machine type and model	标识 IMM 正在监视的服务器类型和型号。
Serial number	标识 IMM 正在监视的服务器的序列号。
UUID	标识 IMM 正在监视的服务器的通用唯一标识 (UUID)，这是 32 位的十六进制数。

组件级别 **VPD**

在此区域中显示远程受管服务器的组件的重要产品数据。

表 18. 组件级别重要产品数据

字段	功能
FRU name	标识每个组件的现场可更换部件 (FRU)。
Serial number	标识每个组件的序列号。
Mfg ID	标识每个组件的制造商标识。

组件活动日志

您可以在此区域中查看组件活动的记录。

表 19. 组件活动日志

字段	功能
FRU name	标识组件的现场可更换部件 (FRU)。
Serial number	标识组件的序列号。
Mfg ID	标识组件的制造商。
Action	标识为每个组件执行的操作。
Timestamp	标识组件操作的日期和时间。以 *mm/dd/yy* 格式显示日期。以 *hh:mm:ss* 格式显示时间。

IMM VPD

您可以在此区域中查看远程受管服务器的 IMM 固件、System x 服务器固件和 Dynamic System Analysis 固件 VPD。

表 20. IMM、UEFI 和 DSA 固件重要产品数据

字段	功能
Firmware type	指示固件代码的类型。
Version string	指示固件代码的版本。
Release date	指示固件何时发布。

第 5 章 执行 IMM 任务

使用导航窗格中 **Tasks** 标题下方的功能，可直接控制 IMM 和您的服务器的操作。您可执行的任务取决于安装 IMM 的服务器。

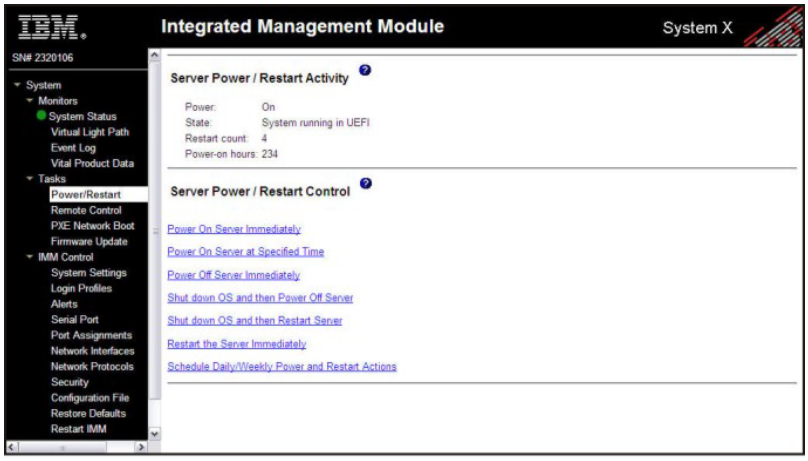
您可以执行以下任务：

- 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
- 更新 IMM 固件

注：一些功能仅在运行受支持的 Microsoft Windows 操作系统的服务器上可用。

查看服务器电源和重新启动活动

Server Power/Restart Activity 区域显示生成 Web 页面时服务器的电源状态。



Power 此字段显示生成当前 Web 页面时服务器的电源状态。

State 此字段显示生成当前 Web 页面时服务器的状态。可能有下列状态：

- 系统电源关闭/状态未知
- 系统开启/正在启动 UEFI
- 系统已在 UEFI 中停止（检测到错误）
- 系统正在 UEFI 中运行
- 正在引导操作系统或操作系统不受支持（如果操作系统未配置为支持针对 IMM 的频带内接口，可能在操作系统中）
- 操作系统已引导

Restart count

此字段显示服务器已重新启动的次数。

注：每次将 IMM 子系统清除为出厂缺省值时，该计数器都会重置为零。

Power-on hours
此字段显示服务器已处于开启状态的总时数。

控制服务器的电源状态

IMM 通过开机、关机和重新启动操作提供对服务器的完整电源控制。此外，还会捕获并显示开机和重新启动统计信息以显示服务器硬件可用性。要执行 **Server Power/Restart Control** 区域中的操作，您必须对 IMM 具有 Supervisor 访问权。

要执行服务器电源和重新启动操作，请完成以下步骤。

注：仅在紧急情况下或者您不在现场且服务器无响应时选择以下选项。

1. 登录到 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **Power/Restart**。向下滚动到 **Server Power/Restart Control** 区域。
3. 单击以下选项之一：

Power on server immediately
开启服务器并启动操作系统。

Power on server at specified time
在指定时间开启服务器并启动操作系统。

Power off server immediately
关闭服务器而不关闭操作系统。

Shut down OS and then power off server
关闭操作系统，然后关闭服务器。

注：如果在尝试了“Shut down OS and then power off server”请求时操作系统处于屏幕保护程序或锁定方式中，那么 IMM 可能无法启动正常关闭。IMM 将在关机延迟时间间隔到期后执行硬重置或关闭，而操作系统可能仍然启动并正常运行。

Shut down OS and then restart server
重新启动操作系统。

注：如果在尝试了“Shut down OS and then restart server”请求时操作系统处于屏幕保护程序或锁定方式中，那么 IMM 可能无法启动正常关闭。IMM 将在关机延迟时间间隔到期后执行硬重置或关闭，而操作系统可能仍然启动并正常运行。

Restart the server immediately
关闭，然后立即开启服务器而不首先关闭操作系统。

Schedule daily/weekly power and restart actions
关闭操作系统，在每天或每周的指定时间关闭服务器（重新启动或不重新启动服务器），并且在每天或每周的指定时间开启服务器。

如果选择其中任何选项，那么会显示确认消息；如果意外选择了某个操作，那么可以将其取消。

注：

1. 仅在 IMM Premium 中提供 IMM 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 4 页的『从 IMM Standard 升级至 IMM Premium』。
2. 仅通过 IMM Web 界面提供远程控制功能部件。您必须使用具有 Supervisor 访问权的用户标识登录到 IMM，才能使用任何远程控制功能部件。

您可以在 IMM Web 界面中使用远程感知功能或远程控制功能部件，以查看服务器控制台并与之交互。您还可以向服务器分配一个您的计算机上的 CD 或 DVD 驱动器、软盘驱动器、USB 闪存驱动器或磁盘映像。

远程控制功能部件提供以下功能：

- 远程查看视频，图形分辨率高达 1280 x 1024 (75 Hz)，而无需考虑服务器状态
- 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、软盘驱动器以及 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 IMM 内存，将其作为虚拟驱动器映射到服务器

更新 IMM 固件和 Java 或 ActiveX applet

要点：IMM 使用 Java applet 或 ActiveX applet 来执行远程感知功能。当 IMM 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 IMM 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，请完成下列步骤：

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 IMM 固件更新后必须单击 **Clear Caching**。

有关更新 IMM 固件的更多信息，请参阅第 109 页的『更新固件』。

启用远程感知功能

注：仅在 IMM Premium 中提供 IMM 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 4 页的『从 IMM Standard 升级至 IMM Premium』。

要启用远程感知功能，请完成以下步骤：

1. 通过拔下电源线来切断服务器电源。
2. 将 Virtual Media Key 安装到主板上的专用插槽中。

3. 将电源重新连接到服务器。

   注：服务器连接到交流电源大约 2 分钟后，电源控制按钮便会激活。

4. 开启服务器。

远程控制

IMM 的远程控制功能部件由两个单独窗口中的两个 Java 应用程序组成：

Video Viewer

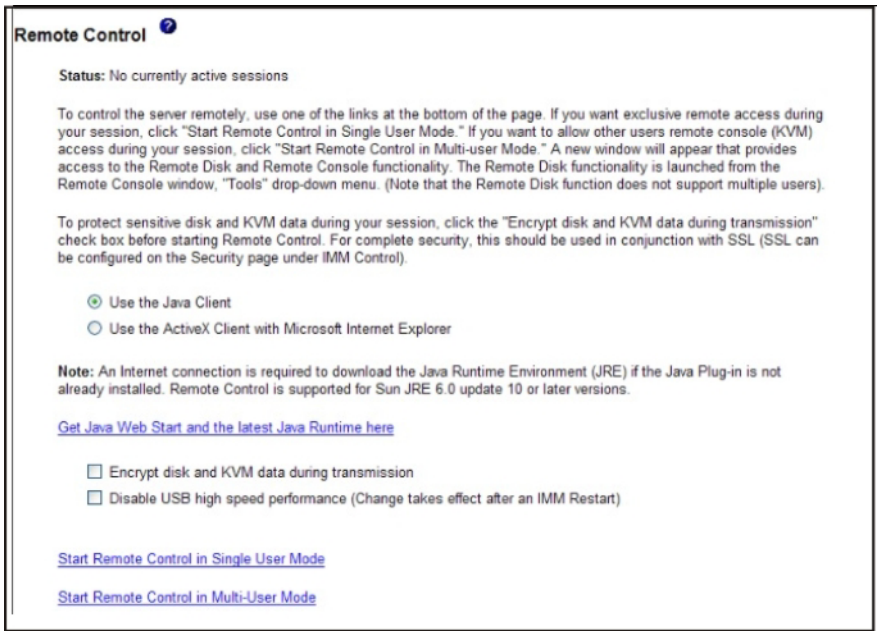
Video Viewer 将远程控制台用于远程系统管理。远程控制台是服务器的交互式图形用户界面 (GUI) 显示，可以在计算机上查看。您在显示器上看到的内容与服务器控制台上的内容完全相同，并且您可以对控制台的键盘和鼠标进行控制。

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。通过它可以将 ISO 和软盘映像文件映射为虚拟驱动器。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。

要远程访问服务器控制台，请完成以下步骤：

1. 登录到 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **Remote Control**。此时会显示一个类似于下图中的页面。



3. 选择以下选项之一：
   - 单击 **Use the Java Client** 以使用 Java applet 来执行远程感知。
   - 单击 **Use the ActiveX Client with Microsoft Internet Explorer** 以在 Windows 操作系统中使用 Internet Explorer，并且要使用 ActiveX applet 来执行远程感知功能。

     注：IMM 固件 V1.28 或更高版本适用于 32 位 ActiveX Remote Presence Client。IMM 固件 V1.30 或更高版本适用于 64 位 ActiveX Client。

4. 要远程控制服务器，请使用 Remote Control 页面底部的链接之一。如果希望在会话期间进行独占远程访问，请单击 **Start Remote Control in Single User Mode**。如果希望在会话期间允许其他用户进行远程控制台 (KVM) 访问，请单击 **Start Remote Control in Multi-user Mode**。此时会打开新窗口来提供对远程磁盘和远程控制台功能的访问。

   如果在打开 Remote Control 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。

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

备注：

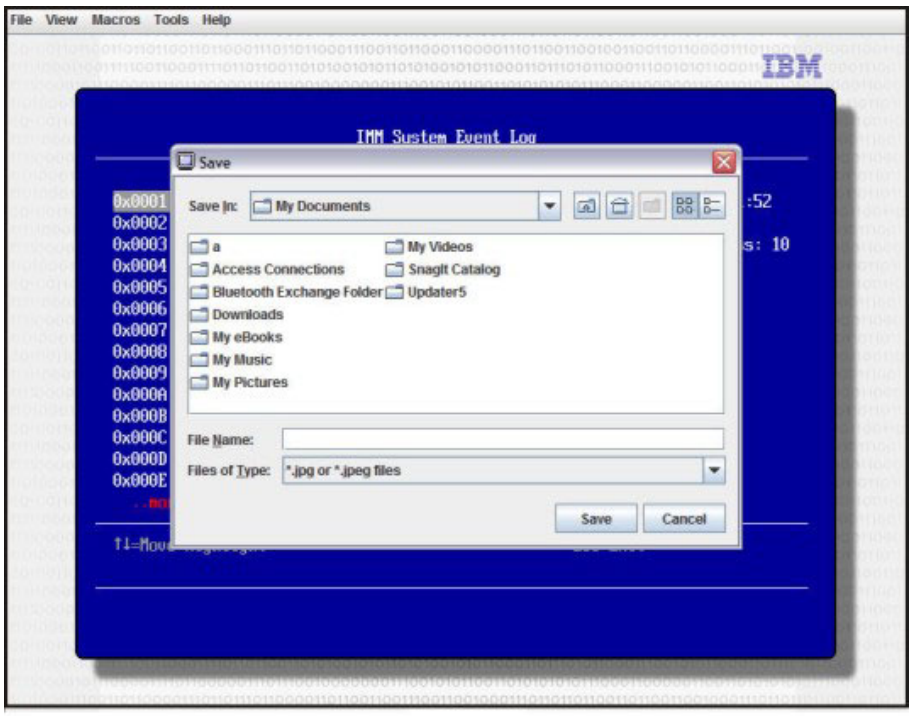
1. 如果当前映射了远程磁盘，请勿关闭 Virtual Media Session 窗口。请参阅第 107 页的『远程磁盘』以获取有关关闭和取消映射远程磁盘的指示信息。
2. 如果在使用 Remote Control 时出现鼠标或键盘问题，请参阅可从 Web 界面中的 Remote Control 页面获取的帮助。
3. 如果使用远程控制来更改 Setup Utility 程序中 IMM 的设置，那么服务器可能会重新启动 IMM。您将丢失远程控制台和登录会话。短暂延迟后，您可以使用新会话再次登录到 IMM，再次启动远程控制台，以及退出 Setup Utility 程序。

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. 系统提示时，对图像文件进行命名并将其保存到您在本地客户机上选择的位置。

注：截屏图像另存为 JPG 或 JPEG 文件类型。



远程控制 **Video Viewer** 视图方式

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

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

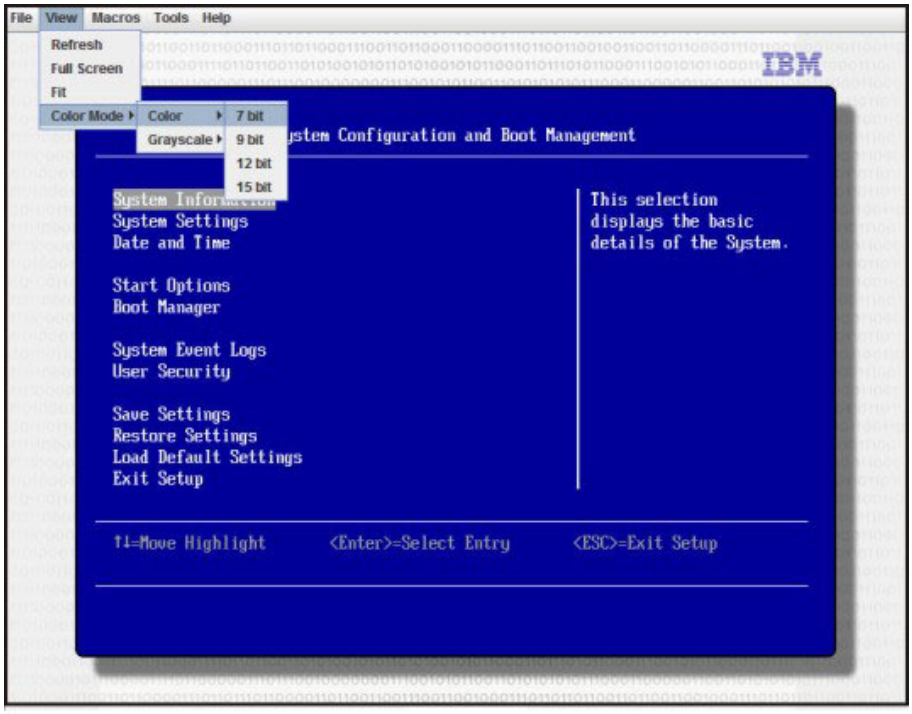
如果您与远程服务器的连接的带宽有限，那么可以通过在 Video Viewer 窗口中调整颜色设置来降低 Video Viewer 的带宽需求。

注：IMM 具有一个菜单项可用于进行色深调整以在低带宽情况下减少传输的数据，而不是远程管理适配器 II 界面中的带宽滑块。

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. 将鼠标指针移至菜单中的 **Color Mode** 上时，会显示两个颜色方式选项：

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

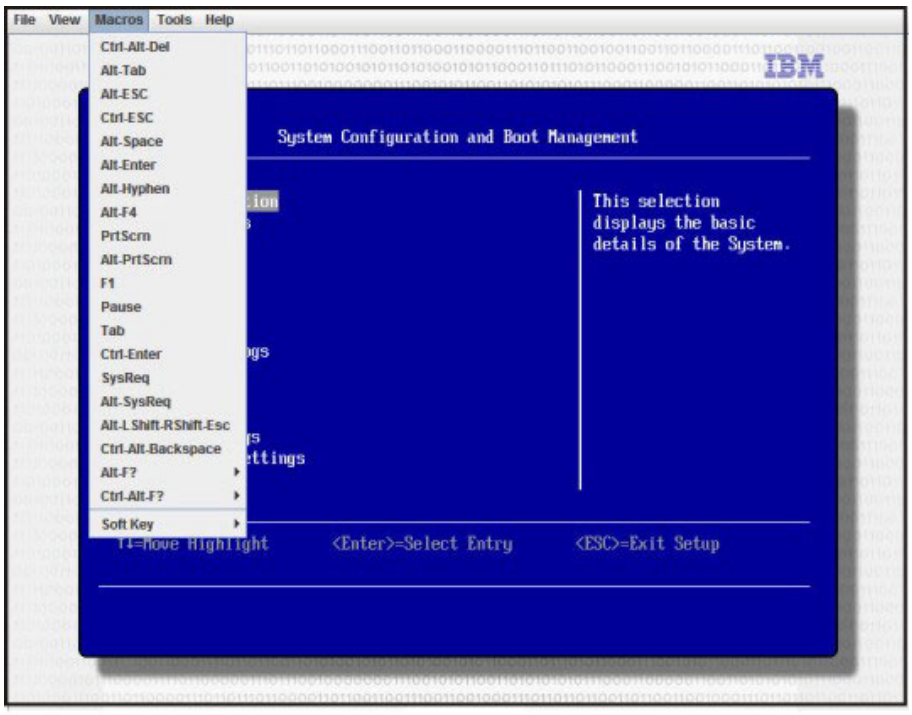


3. 选择颜色或灰度设置。

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。



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**，然后单击 **Add**。此时会打开一个新窗口。
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. 如果是添加新组合，请在弹出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

键盘通过功能部件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. 从菜单中选择 **Session Options**。
3. 显示 Session Options 窗口时，单击 **General** 选项卡。
4. 选中 **Pass all keystrokes to target** 复选框以启用或禁用功能部件。
5. 单击 **OK** 以保存选项。

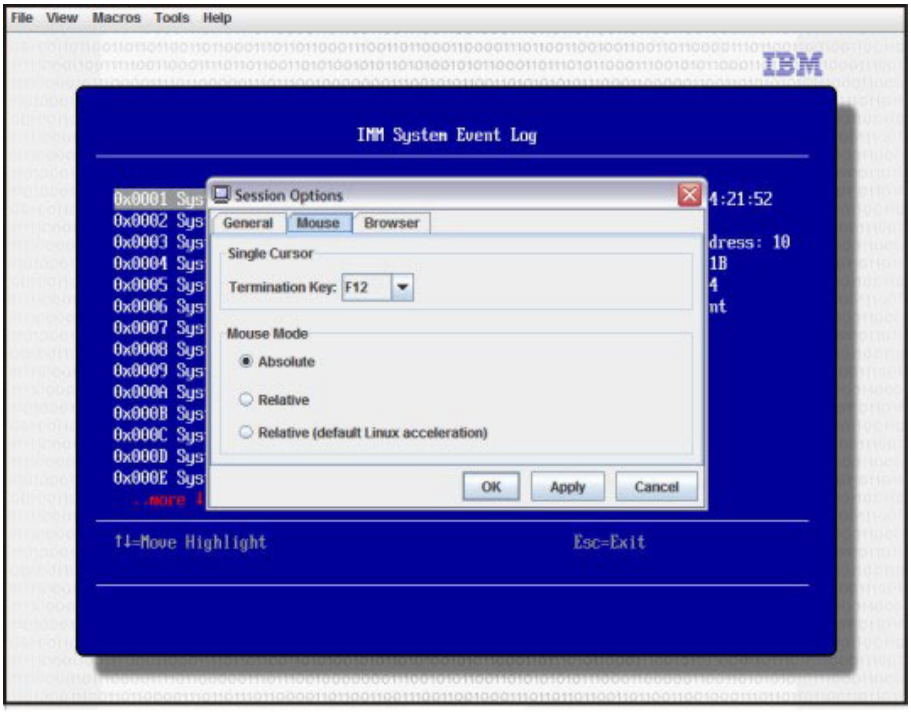
远程控制鼠标支持

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. 当显示 Session Options 窗口时，单击 **Mouse** 选项卡。



4. 选择以下鼠标方式之一：

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）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，请完成以下步骤：

1. 在 Video Viewer 窗口中，单击 **Tools**。
2. 选择 **Single Cursor**。

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以其他方式在 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，请按定义的终止键。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. 将鼠标指针移至菜单中的 **Power** 上时，会显示以下选项：

   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

要查看 Video Viewer 性能统计信息，请完成以下步骤：

1. 在 Video Viewer 窗口中，单击 **Tools**。
2. 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，您可以切换为使用 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。

远程磁盘

在 Virtual Media Session 窗口中，可以向服务器分配一个您的计算机上的 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。您可以使用远程控制功能部件来访问远程磁盘。驱动器和磁盘映像在服务器上显示为 USB 驱动器。

备注：

1. 以下服务器操作系统具有远程磁盘功能所需的 USB 支持：
   - Microsoft Windows Server 2008
   - Microsoft Windows Server 2003
   - Red Hat Linux V4.0 和 V5.0
   - SUSE Linux V10.0
   - Novell NetWare 6.5
2. 客户机服务器需要 Java 1.5 插件或更高版本。
3. 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. 登录到 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **Remote Control**。
3. 在 Remote Control 页面上，单击 **Start Remote Control** 选项之一：
   - 如果希望在会话期间进行独占远程访问，请单击 **Start Remote Control in Single User Mode**。
   - 如果希望在会话期间允许其他用户具有远程控制台 (KVM) 访问权，请单击 **Start Remote Control in Multi-user Mode**。

   此时会打开 Video Viewer 窗口。
4. 要打开 Virtual Media Session 窗口，请单击 Video Viewer 窗口中的 **Tools** > **Launch Virtual Media**。

注：如果在打开 Remote Control 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。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。

通过 IMM 固件 V1.03 和更高版本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。

可以选择软盘映像文件并将软盘映像保存在 IMM 存储器中。这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 IMM Web 界面会话结束后也如此。最多可以在 IMM 卡上存储一个驱动器映像。驱动器或映像内容必须为 1.44 MB 或更小。要上载软盘映像文件，请完成以下步骤：

1. 单击 **RDOC**。
2. 当新窗口打开时，单击 **Upload**。
3. 单击 **Browse** 以选择要使用的映像文件。
4. 在 **Name** 字段中，输入映像的名称，然后单击 **OK** 以上载文件。

   注：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**。

通过 IMM 固件 V1.02 和更低版本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 **Mapped** 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。

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，请清除该驱动器的 **Mapped** 复选框。取消映射驱动器之前，必须确认要取消映射该驱动器。

可以选择软盘映像文件并将软盘映像保存在 IMM 存储器中。这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 IMM Web 界面会话结束后也如此。最多可以在 IMM 卡上存储一个驱动器映像。驱动器或映像内容必须为 1.44 MB 或更小。要上载软盘映像文件，请完成以下步骤：

1. 单击 **RDOC**。
2. 当新窗口打开时，单击 **Upload**。
3. 单击 **Browse** 以选择要使用的映像文件。

4. 在 **Name** 字段中，输入映像的名称，然后单击 **OK** 以上载文件。

   注：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 窗口和 Virtual Media Session 窗口。

设置 PXE 网络引导

要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 (PXE) 网络引导，请完成以下步骤：

1. 登录到 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
2. 在导航窗格中，单击 **PXE Network Boot**。
3. 选中 **Attempt PXE network boot at next server restart** 复选框。
4. 单击 **Save**。

更新固件

使用导航窗格上的 Firmware Update 选项以更新 IMM 固件、System x 服务器固件和 Dynamic System Analysis (DSA) 固件。

要更新固件，请完成以下步骤。

注：IBM Web 站点会定期进行更改。实际的过程可能与本文档中的描述略有不同。

1. 下载适用于安装了 IMM 的服务器的最新固件更新：
   a. 转至 http://www.ibm.com/systems/support/。
   b. 在 **Product support** 下，单击 **System x** 或 **BladeCenter**。
   c. 在 **Popular links** 下单击 **Software and device drivers**。
   d. 单击服务器的适用链接以显示可下载文件的原始位置。
   e. 滚动到 IMM、服务器固件或 DSA 区域，选择固件更新的链接，然后保存更新文件。
2. 登录到 IMM。有关更多信息，请参阅第 11 页的第 2 章，『打开并使用 IMM Web 界面』。
3. 在导航窗格中，单击 **Firmware Update**。
4. 单击 **Browse**。
5. 浏览至要更新的更新包。

   注：
   a. 在服务器已关闭或服务器正在启动时，无法更新 System x 服务器固件。
   b. 要确定将使用的固件文件的类型，请参阅更新包自述文件。在大多数情况下，IMM 可以使用 EXE 或 BIN 文件来执行更新。
6. 单击 **Open**。该文件（包括完整路径）显示在 **Browse** 旁边的框中。

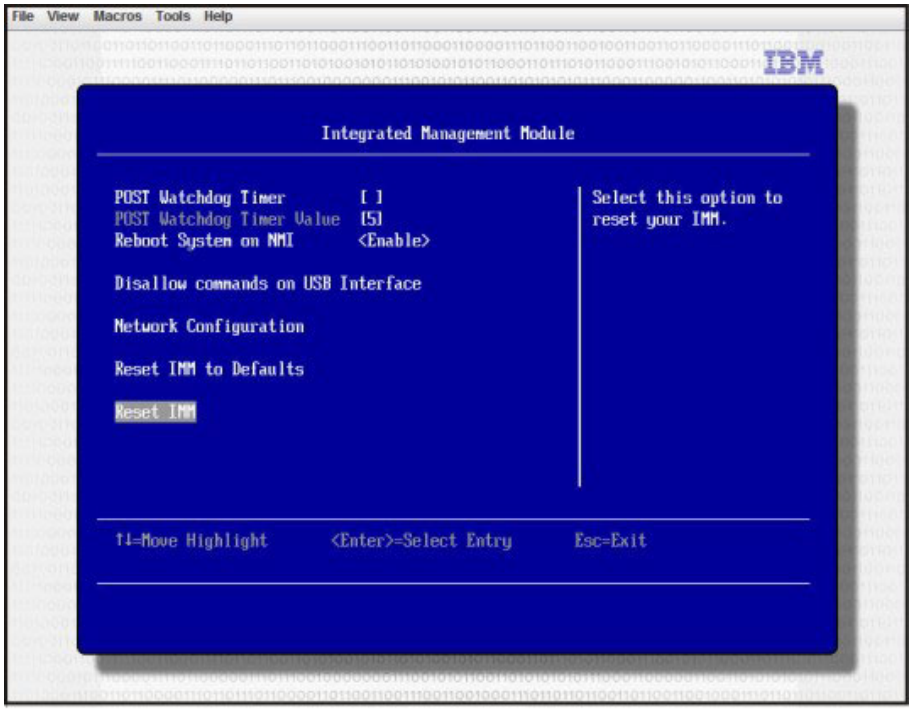
7. 要开始更新过程，请单击 **Update**。在文件传输到 IMM 上的临时存储器时，会显示进度指示器。当文件传输完成时，会打开确认窗口。
8. 验证 Confirm Firmware Update 窗口上显示的文件是否是计划更新的文件。如果不是，请单击 **Cancel**。
9. 要完成更新过程，请单击 **Continue**。在更新固件时，会打开进度指示器。将会打开确认窗口，以验证更新是否已成功。
10. 如果更新的是 IMM 固件，请单击导航窗格中的 **Restart IMM**，然后单击 **Restart**。System x 服务器固件和 DSA 更新不要求重新启动 IMM。这些更新在下次启动服务器时生效。
11. 单击 **OK** 以确认要重新启动 IMM。
12. 单击 **OK** 以关闭当前浏览器窗口。
13. IMM 重新启动后，再次登录到 IMM 以访问该 Web 界面。

通过 Setup Utility 重置 IMM

要通过 Setup Utility 重置 IMM，请完成以下步骤：

1. 开启服务器。

   注：服务器连接到交流电源大约 2 分钟后，电源控制按钮便会激活。
2. 当显示提示 F1 Setup 时，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. 选择 **Reset IMM**。



注：重置 IMM 后，会立即显示以下确认消息：

```
IMM reset command has been sent successfully!! Press ENTER to continue.
```

IMM 重置过程尚未完成。您必须等待大约 4 分钟以使 IMM 进行重置，然后 IMM 才再次可运作。如果尝试在服务器进行重置时访问服务器固件信息，那么在字段中会显示 `Unknown`，并且描述为 `Error retrieving information from IMM`。

使用 IMM 和 IBM System x 服务器固件管理工具和实用程序

本节描述 IMM 和 IBM System x 服务器固件支持的工具和实用程序。您用于管理频带内 IMM 的 IBM 工具无需安装设备驱动程序。但是，如果您选择使用诸如频带内 IPMItool 之类的特定工具，那么必须安装 OpenIPMI 驱动程序。

在 IBM Web 站点上提供了 IBM 系统管理工具和实用程序的更新和下载。要检查工具和实用程序的更新，请完成以下步骤。

注：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. 转至 http://www.ibm.com/systems/support/。
2. 在 **Product support** 下单击 **System x**。
3. 在 **Popular links** 下单击 **Utilities**。

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 IMM。

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

使用 OSA System Management Bridge

OSA System Management Bridge (SMBridge) 是可用于远程管理服务器的工具。您可以通过 IPMI 1.5 和 Serial over LAN (SOL) 协议，使用该工具管理服务器。

有关 SMBridge 的更多信息，请访问 http://www-947.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-62198&brandind=5000008 或完成以下步骤：

1. 转至 http://www.ibm.com/systems/support/。
2. 单击 **System x**。
3. 在 **Support & downloads** 下，单击 **Search**。
4. 在搜索字段中输入 `smbridge`，然后单击 **Search**。
5. 在结果列表中，单击链接 **SMBridge Tool Help - Servers**。

使用 IBM Advanced Settings Utility

需要有 IBM Advanced Settings Utility (ASU) V3.0.0 或更高版本才能管理 IMM。ASU 是一种可用于从多个操作系统平台上的命令行界面修改固件设置的工具。通过它，还可以发出所选的 IMM 设置命令。可以使用频带内或频带外 ASU 来管理和配置 IMM。

注：如果禁用了 USB 频带内接口 (LAN over USB)，那么 ASU 要求安装 IPMI 设备驱动程序。

有关 ASU 的更多信息，请参阅 http://www-947.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-55021&brandind=5000008 或完成以下步骤：

1. 转至 http://www.ibm.com/systems/support/。
2. 单击 **System x**，从 **Product family** 菜单中选择您的服务器，然后单击 **Go**。
3. 从 **Refine results** 菜单中，选择 **Advanced Settings Utility**，然后单击 **Go**。
4. 单击指向 ASU 最新版本的链接。

使用 IBM 闪存实用程序

通过闪存实用程序，您可以更新硬件和服务器固件，并且消除从物理软盘或其他介质手动安装新固件或固件更新的必要性。您可以将 IBM 闪存实用程序用于频带内和频带外的 IMM、服务器固件和 DSA。要查找闪存实用程序，请完成以下步骤：

1. 转至 http://www.ibm.com/systems/support/。
2. 在 **Product support** 下单击 **System x**。
3. 在搜索字段中输入 `flash utility`，然后单击 **Search**。
4. 单击指向适用闪存实用程序的链接。

其他 IMM 管理方法

您可以使用以下用户界面来管理和配置 IMM：

- IMM Web 界面
- SNMPv1
- SNMPv3
- Telnet CLI
- SSH CLI

第 6 章 LAN over USB

与 BMC 和 Remote Supervisor Adapter II 不同，IMM 无需 IPMI 设备驱动程序和 USB 守护程序即可进行频带内 IMM 通信。LAN over USB 接口支持与 IMM 的频带内通信；主板上的 IMM 硬件提供了一个从 IMM 到操作系统的内部以太网 NIC。

注：LAN over USB 在 IMM Web 界面中也称为“USB 频带内接口”。

用于 LAN over USB 接口的 IMM IP 地址会设置为静态地址 169.254.95.118，子网掩码为 255.255.0.0。唯一例外是多节点系统（例如 x3850 X5 或 x3950 X5）的辅助节点中的 IMM，其中 LAN over USB 接口的 IMM 端 IP 地址为 169.254.96.118。

与 LAN over USB 接口的潜在冲突

在某些情况下，IMM LAN over USB 接口会与某些网络配置和/或应用程序产生冲突。例如，Open MPI 尝试使用服务器上的所有可用网络接口。Open MPI 检测到 IMM LAN over USB 接口，并尝试使用该接口与集群环境中的其他系统进行通信。LAN over USB 接口是一个内部接口，因此该接口不能用于与集群中的其他系统进行外部通信。

解决与 IMM LAN over USB 接口的冲突

可以采用以下几种操作来解决 LAN over USB 与网络配置和应用程序的冲突：

- 对于与 Open MPI 的冲突，请配置应用程序，以便其不会尝试使用该接口。
- 禁用接口（在 Linux 下运行 `ifdown`）。
- 除去设备驱动程序（在 Linux 下运行 `rmmod`）。
- 通过以下任一方法禁用 IMM 上的 USB 频带内接口。

  要点：如果禁用 USB 频带内接口，那么将无法通过使用 Linux 或 Windows 闪存实用程序对 IMM 固件执行频带内更新。如果禁用了 USB 频带内接口，请使用 IMM Web 界面上的 Firmware Update 选项来更新固件。有关更多信息，请参阅第 109 页的『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。有关禁用看守程序的更多信息，请参阅第 18 页的『设置服务器超时』。

  – 要从 IMM Web 界面禁用 LAN over USB 接口，请参阅第 21 页的『禁用 USB 频带内接口』。
  – 要从高级管理模块 Web 界面禁用 LAN over USB 接口，请完成以下步骤。
    1. 登录到高级管理模块 Web 界面。
    2. 在导航窗口中，单击 **Blade Tasks** 标题下的 **Blade Configuration**。
    3. 向下滚动到 Blade Configuration Web 页面上的服务处理器 LAN over USB 接口。该部分列出了机箱中所有能够启用和禁用 LAN over USB 接口的刀片服务器。
    4. 选中要启用或禁用的刀片服务器旁的复选框。
    5. 单击 **Disable** 以禁用所选刀片服务器上的 LAN over USB 接口。

手动配置 LAN over USB 接口

要使 IMM 使用 LAN over USB 接口，如果自动设置失败或者您更希望手动设置 LAN over USB，那么可能必须完成其他一些配置任务。固件更新包或 Advanced Settings Utility (ASU) 会尝试自动执行设置。有关不同操作系统上的 LAN over USB 配置的更多信息，请参阅 IBM Web 站点上的 IBM 白皮书 *Transitioning to UEFI and IMM*。

安装设备驱动程序

要使 IMM 使用 LAN over USB 接口，您可能必须安装操作系统驱动程序。如果自动设置失败或者您更希望手动设置 LAN over USB，请使用以下一个过程。有关不同操作系统上的 LAN over USB 配置的更多信息，请参阅 IBM Web 站点上的 IBM 白皮书 *Transitioning to UEFI and IMM*。

安装 Windows IPMI 设备驱动程序

缺省情况下，不会在 Microsoft Windows Server 2003 R2 操作系统中安装 Microsoft IPMI 设备驱动程序。要安装 Microsoft IPMI 设备驱动程序，请完成以下步骤：

1. 从 Windows 桌面单击开始 **>** 控制面板 **>** 添加或删除程序。
2. 单击添加/删除 **Windows** 组件。
3. 从组件列表中，选择管理和监视工具，然后单击详细信息。
4. 选择硬件管理。
5. 单击下一步。安装向导将打开并引导您完成安装。

注：可能需要 Windows 安装 CD。

安装 LAN over USB Windows 设备驱动程序

安装 Windows 时，设备管理器中会显示一个未知 RNDIS 设备。您必须安装用于识别此设备并且是 Windows 操作系统检测和使用 LAN over USB 功能所必需的 Windows INF 文件。INF 的已签名版本包含在所有 Windows 版本的 IMM、UEFI 和 DSA 更新包中。该文件仅需安装一次。要安装 Windows INF 文件，请完成以下步骤：

1. 获取 Windows 版本的 IMM、服务器固件或 DSA 更新包（请参阅第 109 页的『更新固件』以获取更多信息）。
2. 从固件更新包中解压出 `ibm_rndis_server_os.inf` 和 `device.cat` 文件，将其复制到 `\WINDOWS\inf` 子目录中。
3. 对于 **Windows 2003**：通过右键单击 `ibm_rndis_server_os.inf` 文件并选择安装来安装该文件。这会在 `\WINDOWS\inf` 中生成同名的 PNF 文件。 对于 **Windows 2008**：转至计算机管理，然后单击设备管理器并找到 RNDIS 设备。选择属性 **>** 驱动程序 **>** 重新安装驱动程序。将服务器指向 `\Windows\inf` 目录，在此它可以找到 `ibm_rndis_server_os.inf` 文件并安装设备。
4. 转至计算机管理，然后单击设备管理器，右键单击网络适配器并选择扫描硬件更改。此时会出现一条消息确认已找到并安装了以太网设备。新的硬件向导将自动启动。
5. 当出现提示 `Windows 可以连接到 Windows Update 以搜索软件吗？`时，单击否，暂时不。单击 下一步以继续。
6. 当出现提示您想要向导做什么？时，单击从列表或指定位置安装（高级）。单击 下一步以继续。

7. 当出现提示请选择您的搜索和安装选项时，单击不要搜索。我要自己选择要安装的驱动程序。单击 下一步以继续。
8. 当出现提示选择硬件类型，然后单击"下一步"时，单击网络适配器。单击 下一步以继续。
9. 当出现提示完成找到新硬件向导时，单击完成。

   注：此时会显示新本地连接，并且可能声明该连接受限制或无连接。请忽略这个消息。
10. 返回到设备管理器。验证 **IBM USB Remote NDIS Network Device** 是否会出现在网络适配器下。
11. 打开命令提示符，输入 `ipconfig`，并按 Enter 键。此时会显示 IBM USB RNDIS 的本地连接，IP 地址在范围 169.254.*xxx.xxx* 内且子网掩码设置为 255.255.0.0。

安装 LAN over USB Linux 设备驱动程序

当前的 Linux 版本（例如 RHEL5 Update 2 和 SLES10 Service Pack 2）在缺省情况下支持 LAN over USB 接口。在安装这些操作系统期间，将检测并显示该接口。在配置设备时，使用静态 IP 地址 169.254.95.130，子网掩码为 255.255.0.0。

注：较旧的 Linux 分发版可能不检测 LAN over USB 接口并可能需要手动配置。有关在特定 Linux 分发版上配置 LAN over USB 的信息，请参阅 IBM Web 站点上的 IBM 白皮书 *Transitioning to UEFI and IMM*。

IMM LAN over USB 接口要求装入 `usbnet` 和 `cdc_ether` 设备驱动程序。如果尚未安装这些设备驱动程序，请使用 modprobe 命令对其进行安装。当安装了这些驱动程序时，IMM USB 网络接口会在操作系统中显示为网络设备。要发现操作系统已向 IMM USB 网络接口分配的名称，请输入：

```
dmesg | grep -i cdc ether
```

使用 ifconfig 命令将该接口配置为具有范围在 169.254.*xxx.xxx* 内的 IP 地址。例如：

```
ifconfig IMM_device_name 169.254.1.102 netmask 255.255.0.0
```

每次启动操作系统时，便会将此接口配置为具有范围在 169.254.*xxx.xxx* 内的 IP 地址。

第 7 章 命令行界面

使用 IMM 命令行界面 (CLI) 可访问 IMM，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 IMM 认证，然后才能发出任何 CLI 命令。

通过 IPMI 管理 IMM

IMM 最初将 User ID 2 设置成用户名为 USERID，密码为 PASSW0RD（包含数字零而不是字母 O）。此用户具有 Supervisor 访问权。

要点：请在初始配置期间更改此缺省密码以增强安全性。

IMM 还提供以下 IPMI 远程服务器管理能力：

命令行界面

命令行界面使您可通过 IPMI 2.0 协议直接访问服务器管理功能。您可以使用 SMBridge 或 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。通过 SMBridge，还可以将一个或多个命令保存在文本文件中并将该文件作为脚本运行。有关 IPMItool 的更多信息，请参阅第 111 页的『使用 IPMItool』。有关 SMBridge 的更多信息，请参阅第 111 页的『使用 OSA System Management Bridge』。

Serial over LAN

要从远程位置管理服务器，请使用 SMBridge 或 IPMItool 建立 Serial over LAN (SOL) 连接。有关 IPMItool 的更多信息，请参阅第 111 页的『使用 IPMItool』。有关 SMBridge 的更多信息，请参阅第 111 页的『使用 OSA System Management Bridge』。

访问命令行

要访问命令行，请 IMM IP 地址启动 Telnet 或 SSH 会话（请参阅第 31 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 IMM 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 IMM 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`。然后，会将您注销并结束会话。

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 IMMA00096B9E003A
  -r auto
  -d auto
  -m 1500
  -b 00:09:6B:9E:00:3A
  -l 00:00:00:00:00:00
  system>
  ```

- 在命令行界面中，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可能不可用。要查看受支持命令的列表，请使用 help 或 ? 选项，如以下示例中所示：

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

实用程序命令

实用程序命令如下所示：

- exit
- help
- history

exit 命令

使用 **exit** 命令可注销并结束命令行界面会话。

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 IMMA00096B9E003A
-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：

- clearlog
- fans
- readlog
- syshealth
- temps
- volts
- vpd

clearlog 命令

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

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>
```

readlog 命令

使用 **readlog** 命令可显示 IMM 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 -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。

语法：

```
readlog [options]
option:
-f
```

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 IMM 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  9/320
DASD1  66/19  73/23  82/28  88/31  9/332
Amb    59/15  70/21  83/28  90/32  9/355
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)、IMM、服务器固件 (bios) 和 Dynamic System Analysis Preboot (dsa)。将显示与 Web 界面中相同的信息。

语法：

```
vpd sys
vpd IMM
vpd biosvpd dsa
```

示例：

```
system> vpd dsa
Type     Version      ReleaseDate
----     -------      -----------
dsa      D6YT19AUS    02/27/2009
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：

- 电源
- reset

power 命令

使用 **power** 命令来控制服务器电源。要发出 **power** 命令，您必须具有电源和重新启动访问权限。

power on 开启服务器电源。

power off 关闭服务器电源。**-s** 选项先关闭操作系统，然后关闭服务器。

power state 显示服务器电源状态（开启或关闭）以及服务器的当前状态。

power cycle 关闭服务器电源，然后再打开电源。**-s** 选项先关闭操作系统，然后关闭服务器。

语法：

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

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]
options:
-s
```

串行重定向命令

存在一个串行重定向命令：console。

console 命令

使用 **console** 命令可启动针对 IMM 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：

- dhcpinfo
- dns
- gprofile
- ifconfig
- ldap
- ntp
- passwordcfg
- portcfg
- slp

- srcfg
- ssl
- tcpcmdmode
- timeouts
- usbeth
- users

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     : IMMA-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 IMM 的 DNS 配置。

语法：

```
dns
```

注：以下示例显示了启用 DNS 的 IMM 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
-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（enabled 或 disabled）
-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）
-p	首选 DNS 服务器（ipv4 或 ipv6）

gprofile 命令

使用 **gprofile** 命令来显示和配置 IMM 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 *group_name*，最多为 63 个字符的字符串。*group_name* 必须唯一。

选项	描述	值
-a	基于角色的安全性（权限）级别	Supervisor、operator、rbs <角色列表>：ns|uam|rca|rcrda|rpr|bac|ce|aac 使用竖线分隔的值列表来指定角色列表值。
-h	显示命令用法和选项	

语法：

```
gprofile [1 - 16] [options]
options:
-clear state
-n  group_name
-a  security level:
    -ns network and security
    -uam user account management
    -rca remote console access
    -rcrda remote console and remote disk access
    -rpr remote server power/restart access
    -bac basic adapter configuration
    -ce ability to clear event logs
    -aac advanced adapter configuration
-h
```

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。
-dn	域名	有效格式的域名
-ipv6	IPv6 状态	disabled 和 enabled
-lla	链路本地地址 注：仅当启用 IPv6 时，才会显示链路本地地址。	链路本地地址由 IMM 确定。此值是只读的，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 和 128 之间的数字

选项	描述	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	disabled 和 enabled
-sa6	IPv6 无状态自动配置状态	disabled 和 enabled
-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。
-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
-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）。

语法：

```
ifconfig eth0 [options]
options:
-state interface_state
-c config_method
-i static_ip_address
-g gateway_address
-s subnet_mask
-n hostname
-r data_rate
-d duplex_mode
-m max_transmission_unit
-l locally_administered_MAC
```

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 IMMA00096B9E003A
-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 IMM.
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。

ldap 命令

使用 **ldap** 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
-aom	仅认证方式	Enabled 和 disabled
-a	用户认证方法	Local only、LDAP only、local first then LDAP 和 LDAP first then local
-b	绑定方法	Bind with Anonymous、bind with ClientDN and password 和 bind with Login Credential
-c	客户机专有名称	针对 *client_dn* 的字符串，最多包含 63 个字符
-fn	森林名称	Active Directory 环境，针对 *forest_name* 的字符串，最多包含 127 个字符
-d	搜索域	针对 *search_domain* 的字符串，最多包含 31 个字符
-f	组过滤器	针对 *group_filter* 的字符串，最多包含 63 个字符
-g	组搜索属性	针对 *group_search_attr* 的字符串，最多包含 63 个字符
-l	登录许可权属性	针对 *string* 的字符串，最多包含 63 个字符
-p	客户机密码	针对 *client_pw* 的字符串，最多包含 15 个字符
-pc	确认客户机密码	针对 *confirm_pw* 的字符串，最多包含 15 个字符 命令用法为：ldap -p *client_pw* -pc *confirm_pw* 当您更改客户机密码时，此选项是必需的。该选项将 *confirm_pw* 自变量与 *client_pw* 自变量进行比较，如果它们不匹配，该命令将失败。
-r	根条目专有名称 (DN)	针对 *root_dn* 的字符串，最多包含 63 个字符
-rbs	Active Directory 用户的增强型基于角色的安全性	Enabled 和 disabled
s1ip	服务器 1 主机名/IP 地址	针对 *host name/ip_addr* 的字符串（最多包含 63 个字符）或 IP 地址
s2ip	服务器 2 主机名/IP 地址	针对 *host name/ip_addr* 的字符串（最多包含 63 个字符）或 IP 地址
s3ip	服务器 3 主机名/IP 地址	针对 *host name/ip_addr* 的字符串（最多包含 63 个字符）或 IP 地址
-s4ip	服务器 4 主机名/IP 地址	针对 *host name/ip_addr* 的字符串（最多包含 63 个字符）或 IP 地址
s1pn	服务器 1 端口号	针对 *port_number* 的数字端口号，最多包含 5 位数。
s2pn	服务器 2 端口号	针对 *port_number* 的数字端口号，最多包含 5 位数。
s3pn	服务器 3 端口号	针对 *port_number* 的数字端口号，最多包含 5 位数
s4pn	服务器 4 端口号	针对 *port_number* 的数字端口号，最多包含 5 位数
-t	服务器目标名称	启用 -rbs 选项时，此字段指定可通过 Role Based Security Snap-In 与 Active Directory 服务器上的一个或多个角色相关联的目标名称。
-u	UID 搜索属性	针对 *search_attrib* 的字符串，最多包含 23 个字符

选项	描述	值
-v	通过 DNS 获取 LDAP 服务器地址	Off 和 On
-h	显示命令用法和选项	

语法：

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

ntp 命令

使用 **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 和 disabled
-i	网络时间协议服务器的名称或 IP 地址	要用于时钟同步的 NTP 服务器的名称
-f	IMM 时钟与网络时间协议服务器同步的频率（以分钟为单位）	3 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。

语法：

```
ntp [options]
options:
-en state
-i  hostname
-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
```

portcfg 命令

使用 **portcfg** 命令可配置串口。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。

这些参数是在硬件中设置的，不能更改：

- 8 个数据位
- 无奇偶性
- 1 个停止位

下表显示了选项的自变量。

选项	描述	值
-b	波特率	9600、19200、38400、57600、115200 和 230400
-climode	CLI 方式	none、cliems 和 cliuser • none：禁用命令行界面 • cliems：启用命令行界面，使用与 EMS 兼容的击键序列 • cliuser：启用命令行界面，使用用户定义的击键序列

语法：

```
portcfg [options]
portcfg [options]
options:
-b baud_rate
-climode cli_mode
-cliauth cli_auth
```

示例：

```
system> portcfg
-b       : 115200
-climode : 2 (CLI with user defined keystroke sequences) system>
system>
```

portcontrol 命令

使用 **portcontrol** 命令配置 IMM 服务的端口状态。要更改端口状态，请输入选项，后跟值。要更改端口控制状态，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
-ipmi	IPMI 端口	on 或 off

语法：

```
portcontrol [options]
options:
-ipmi status
```

示例：

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

srcfg 命令

使用 **srcfg** 命令可配置串行重定向。输入 srcfg 可显示当前配置。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。

下表显示了 -exitcliseq 选项的自变量。

选项	描述	值
-exitcliseq	退出命令行界面击键序列	用户定义的用于退出 CLI 的击键序列。有关详细信息，请查看此表中 -entercliseq 选项的值。

语法：

```
srcfg [options]
options:
-exitcliseq exitcli_keyseq
```

示例：

```
system> srcfg
-exitcliseq ^[Q
system>
```

ssl 命令

使用 **ssl** 命令可显示并配置安全套接字层 (SSL) 参数。

注： 必须先安装客户机证书，然后才能启用 SSL 客户机。

选项	描述
-ce	启用或禁用 SSL 客户机
-se	启用或禁用 SSL 服务器
-h	列出用法和选项

语法：

```
ssl [options]
options:
-ce on | off
-se on | off
-h
```

参数：以下参数会呈现在 **ssl** 命令的选项状态显示中，并且仅从命令行界面输出：

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

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
-o	操作系统超时	分钟	disabled、2.5、3、3.5 和 4
-l	装入程序超时	分钟	d i s - abled、0.5、1、1.5、2、2.5、3、3.5、4、4.5、5、7.5、10、15、20、30、60 和 120

语法：

```
timeouts [options]
options:
-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。有关启用或禁用此接口的更多信息，请参阅第 21 页的『禁用 USB 频带内接口』。

语法：

```
usbeth [options]
options:
-en <enabled|disabled>
```

示例：

```
system>usbeth
-en : disabled
system>usbeth -en enabled
ok
system>usbeth
-en : disabled
```

users 命令

使用 **users** 命令可访问所有用户帐户及其权限级别，以及创建新用户帐户和修改现有帐户。

请阅读有关 **users** 命令的以下准则：

- 用户号必须介于 1 到 12 之间（包括 1 和 12）。
- 用户名必须少于 16 个字符，并且只能包含数字、字母、句点和下划线。
- 密码长度必须多于 5 且少于 16 个字符，并且必须至少包含一个字母字符和一个非字母字符。
- 权限级别可以是以下一个级别：
  - super (supervisor)
  - ro (read only)
  - 以下值的任何组合，并用“|”分隔：

    am (User account management access)

    rca (Remote console access)

    rcvma (Remote console and virtual media access)

    pr (Remote server power/restart access)

    cel (Ability to clear event logs)

    bc (Adapter configuration [basic])

    nsc (Adapter configuration [network and security])

    ac (Adapter configuration [advanced])

语法：

```
users [options]
options:
-user number
-n username
-p password
-a authority level
```

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 PASSW0RD -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>
```

IMM 控制命令

IMM 控制命令如下所示：

- clearcfg
- clock
- identify
- resetsp
- update

clearcfg 命令

使用 **clearcfg** 命令可将 IMM 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 IMM 的配置后，IMM 将重新启动。

clock 命令

使用 **clock** 命令可根据 IMM 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 或 +10，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）、gtb（英国）、egt（埃及）和 fle（芬兰）。
- 如果为 +10，那么夏令时设置如下：off、ea（东澳）、tas（塔斯马尼亚）和 vlad（符拉迪沃斯托克）。
- 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]
options:
-d mm/dd/yyyy
-t hh:mm:ss
-g gmt offset
-dst on/off/special case
```

示例：

```
system> clock
12/12/2003 13:15:23 GMT-5:00 dst on
system> clock -d 12/31/2004
ok
system> clock
12/31/2004 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]
options:
-s on/off/blink
-d seconds
```

示例：

```
system> identify
-s off
system> identify -s on -d 30
ok
system>
```

resetsp 命令

使用 **resetsp** 命令可重新启动 IMM。您至少应具有高级适配器配置权限才能发出此命令。

update 命令

使用 **update** 命令可更新 IMM 上的固件。要使用此命令，您至少应具有高级适配器配置权限。固件文件（由 *filename* 指定）先从 TFTP 服务器（由其 IP 地址指定）传输到 IMM，然后再进行闪存。 **-v** 选项指定详细方式。

注：请确保 TFTP 服务器正在将要从中下载文件的服务器上运行。

选项	描述
-i	TFTP 服务器 IP 地址
-l	（要进行闪存的）文件名
-v	详细方式

语法：

```
update -i TFTP_server_IP_address -l filename
```

示例：在详细方式中，将按完成百分比实时显示闪存进度。

```
system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Firmware update is in progress. Please wait..
Downloading image - 66%

system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Firmware update is in progress. Please wait..
Image Downloaded.

system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Firmware update is in progress. Please wait..
Image Downloaded.
Flashing image - 45%

system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Firmware update is in progress. Please wait..
Image Downloaded.
Flash operation completed.
system>
```

如果闪存操作未处于详细方式，那么将以连续的 # 字符显示进度。

```
system>update -i 192.168.70.200 -l dsa_d6yt28a_68608_2.upd
Firmware update is in progress. Please wait..
Downloading image: ##################################################
Flashing image: ##################################################
Flash operation completed.
```

Service Advisor 的命令

Service Advisor 的命令如下所示：

- autoftp
- chconfig
- chlog
- chmanual
- events
- sdemail

autoftp 命令

使用 **autoftp** 命令来显示和配置 Service Advisor 的 FTP/TFTP 服务器设置。

注：必须先接受 Service Advisor 条款和条件，然后才使用此命令。

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*、*tftp*、*disabled*
-i	自动化问题报告的 ftp/tftp 服务器 IP 地址或主机名	IP 地址或主机名
-p	ftp/tftp 传输端口	对于 *port_number*，为 1 到 65535 之间的数字
-u	用于问题报告的引号定界的 ftp 用户名	对于 *user_name*，最多为 63 个字符的字符串
-pw	用于问题报告的引号定界的 ftp 密码	对于 *password*，最多为 63 个字符的字符串
注：对于 *ftp* 值，必须设置所有选项（字段 -i、-p、-u 和 -pw）。对于 *tftp* 值，只需要选项 -i 和 -p。		

语法：

```
autoftp [选项]
options:
-m ftp|tftp|disable
-i host name|ip_addr
-p port_number
-u user_name
-pw password
```

chconfig 命令

使用 **chconfig** 命令来显示和配置 IMM 的 Service Advisor 设置。

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。必须先通过此选项接受 Service Advisor 条款和条件，然后才设置其他选项。	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
-ca	机器位置的引号定界地址	对于 *address*，最多为 30 个字符的字符串
-cci	机器位置的引号定界城市	对于 *city*，最多为 30 个字符的字符串
-ce	格式为 *userid@hostname* 的联系人的电子邮件地址	对于 *email_addr*，最多为 30 个字符的字符串
-cn	联系人的引号定界名称	对于 *contact_name*，最多为 30 个字符的字符串

选项	描述	值
-co	联系人的引号定界的组织/公司名称	对于 *company_name*，最多为 30 个字符的字符串
-cph	联系人的引号定界的电话号码	对于 *phone_number*，5 到 30 个字符之间的字符串
-cs	机器位置的州或省	对于 *state/provice*，2 到 3 个字符之间的字符串
-cz	机器位置的引号定界的邮政编码	对于 *postal_code*，最多为 9 个字符的字符串
-loc	HTTP 代理的标准主机名或 IP 地址	对于 *host_name/ip_addr*，最多为 63 个字符的字符串或者 IP 地址
-po	HTTP 代理端口	对于 *port_number*，1 到 65535 之间的数字端口号
-ps	HTTP 代理状态	enabled、disabled
-pw	引号定界的 HTTP 代理密码	对于 *password*，最多为 15 个字符的字符串
-u	引号定界的 HTTP 代理用户名	对于 *user_name*，最多为 30 个字符的字符串
1. 必须先通过选项 -li 接受 Service Advisor 条款和条件，然后才设置其他选项。 2. 需要填写所有 Contact Information 字段以及 IBM Service Support Center 字段，然后才可以启用对 Service Advisor 的 IBM 支持。如果需要代理，必须设置 HTTP 代理字段。		

语法：

```
chconfig [选项]
options:
-li view|accept
-sa service advisor state
-sc country_code
-ca address
-cci city
-ce email_addr
-cn contact_name
-co company_name
-cph phone_number
-cs state/provice
-cz postal_code
-loc host_name/ip_addr
-po port_number
-ps status
-pw password
-u user_name
```

chlog 命令

使用 **chlog** 命令来显示系统或用户生成的最后五个回拨事件。首先列出最近回拨条目。

下表显示了选项的自变量。

注：必须先接受 Service Advisor 条款和条件，然后才使用此命令。

选项	描述	值
-event_index	使用来自活动日志的索引来指定回拨条目	1 到 5 之间的数字
-ack	确认/未确认，已更正回拨事件	yes、no
-s	只显示 IBM 支持的结果	
-f	只显示 FTP/TFTP 服务器的结果	

语法：

```
chlog [选项]
options:
-event_index
-ack yes|no
-s
-f
```

chmanual 命令

使用 **chmanual** 命令生成人工“回拨”事件或“测试回拨”事件。

注：必须先接受 Service Advisor 条款和条件，然后才使用此命令。

下表显示了选项的自变量。

选项	描述	值
-test	生成测试回拨事件	
-desc	引号定界的问题描述	对于 *description*，最多为 100 个字符的字符串

语法：

```
chmanual [选项]
options:
-test
-desc description
```

events 命令

使用 **events** 命令来查看和编辑排除事件。

注：必须先接受 Service Advisor 条款和条件，然后才使用此命令。

下表显示了选项的自变量。

选项	描述	值
-che	查看和编辑排除事件	
-add	将回拨事件添加到回拨排除列表	*event_id* 格式为 0xhhhhhhhhhhhhhhhh
-rm	从回拨排除列表除去回拨事件	*event_id*|*all* 格式为 0xhhhhhhhhhhhhhhhh 或 all

语法：

```
events [选项]
options:-che {-add}|{-rm}
-add event_id
-rm event_id|all
```

sdemail 命令

使用 **sdemail** 命令为指定的接收方配置电子邮件服务信息。

下表显示了选项的自变量。

选项	描述	值
-subj	引号定界的电子邮件主题	对于 *email_subject*，最多为 119 个字符的字符串
-to	接收方的电子邮件地址。该选项可以包含以逗号分隔的多个地址。	对于 *email_addrs*，最多为 119 个字符的字符串

语法：

```
sdemail [选项]
options:
-subj email_subject
-to email_addrs
```

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为您提供帮助。

- 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 IBM 产品的已更新软件、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。

有关您所在国家或地区支持热线支持哪些产品的信息，请访问 http://www.ibm.com/services/supline/products。

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示的保证。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 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，固态设备具有其受控制的最大写循环数，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与其他环境因素（如湿度或温度）发生组合反应可能会对本文档中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 21. 颗粒和气体的限制

污染物	限制
颗粒	• 依据 ASHRAE 标准 52.2[1]，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 71.04-1985[3] • 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
电话：+49 7032 15 29411
电子邮件：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
电话：+49 7032 15 29411
电子邮件：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 목적으로 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 А.
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

[K]

[L]

[M]

[O]

[P]

[Q]

[R]

[S]

[T]

[W]

[X]

[Y]

[Z]

A

B

D

F

I

J

L

M

N

O

P

R

S

T

U

V

W

部件号： 00FH268

Printed in China

(1P) P/N: 00FH268