Dell™ 远程控制台交换机系统
用户指南

注、注意与警告

注："注"表示有助于您更好地使用计算机的重要信息。

注意："注意"表示如果不遵照说明可能会损坏硬件或造成数据丢失。

警告："警告"表示可能导致财产损坏、人身伤害或死亡。

590-1021-511C

1082DS/2162DS/4322DS 型号远程控制台交换机

2012 年 **7** 月

目录

产品概述 1

特点与优点 **1**
减少缆线堆放 2
KVM 交换功能 2
多平台支持 2
真正的串行功能 3
本地和远程用户界面 3
支持虚拟媒体和智能卡的交换机 3
板载 Web 界面 3
使用标准的 TCP/IP 网络访问交换机 4
加密 4
视频 4
闪存升级 4
堆叠扩充 4
Avocent 管理软件插件 5
FIPS 加密模块 5

简单配置 **7**

安全注意事项 **8**

一般信息 **9**

LAN 选项 **10**

安装 11

RCS 快速安装 **11**

开始 **13**
设置网络 14

机架安装 RCS **14**

机架安装的安全注意事项 14
安装 Dell ReadyRails 系统 15
安装 RCS 19

连接 RCS 硬件 23
连接 SIP 26
添加堆叠交换机 29
与旧式交换机进行级联 31
添加 PEM(可选) 33

配置远程控制台交换机 35
设置内置 Web 服务器 35
通过防火墙连接到 OBWI 35

验证连接 37
后面板以太网连接 LED 37
后面板电源状态 LED 38

调整目标设备上的鼠标设置 38

本地和远程配置 39

本地用户界面 (UI) 39
过滤 40

OBWI 40

使用用户界面 42

启动会话 44

扫描模式 45

查看系统信息 45

RCS 工具 46
重新启动 RCS 46
升级 RCS 固件 47
保存和恢复 RCS 配置以及 RCS 用户数据库 48

网络设置 **49**

DNS 设置 **51**

NTP 设置 **51**

SNMP 设置 **51**

审计事件设置 **52**

设置事件目的地 **52**

端口 — 配置 SIP **53**
升级 SIP 53

电源设备设置 **54**
关联目标设备和电源插座 55
电源插座分组 57
默认插座名称 58
分配插座名称 59
本地端口上的 Local Session 页面 63

本地端口 UI 设置 **64**

调制解调器设置 **64**

设置端口安全设置 **65**

会话 **65**
配置一般会话 66
配置 KVM 会话 66
配置本地虚拟媒体会话 67
配置串行会话 69

设置用户帐户 **69**
管理本地帐户 69
访问级别 70
Avocent 管理软件设备 IP 地址 71

LDAP **71**

超级管理员 **72**

活动会话 **72**
关闭会话 72

视频查看器窗口 73
更改工具栏 75

启动会话 **76**
会话超时 76

窗口大小 **76**

调整视图 **77**

刷新图像 **78**

视频设置 **79**
其他视频调整 79
目标视频设置 81
自动视频调试 81
视频测试模式 81
针对不同供应商的视频设置 81

颜色设置 **82**
调整颜色深度 82
对比度和亮度 82

噪声设置 **82**
检测阈值 82

鼠标设置 **83**
调整鼠标选项 83
光标类型 83
鼠标缩放 85
鼠标校准和同步 86

虚拟媒体 **87**
配置要求 87
共享与抢占的注意事项 87
Virtual Media 对话框 88
打开虚拟媒体会话 88
关闭虚拟媒体会话 91

智能卡 **91**

键盘传递 **92**

宏 **93**

保存视图 **94**

关闭会话 **94**

RCS 的 LDAP 功能 95

Active Directory 结构 **95**
域控制器计算机 95
对象类 96
属性 96
架构扩展 96

Standard 架构与 Dell Extended 架构对比 **98**

标准安装 **98**

配置 Override Admin 帐户 **99**

配置 DNS 设置 **99**

配置网络时间协议 (NTP) 设置 **100**

配置 LDAP 身份验证参数 **101**
启用 LDAP 身份验证 101
输入身份验证参数 — Operational Modes 104
输入扩展选项 — Active Directory LDAP 105

输入身份验证参数 — Standard LDAP 105
输入身份验证参数 — Custom IP Port Assignments 105
完成 LDAP 配置 106
二级 LDAP Settings — Standard Configuration 107
设置 RCS 以执行 Standard LDAP 查询 108
搜索配置设置 109
查询模式选择设置 110
组配置参数 110
二级 LDAP Settings — Active Directory Configuration 112

LDAP SSL 证书 115
启用域控制器上的 SSL 115
登录超时 119

CA 证书信息显示 120

配置群组对象 121
Standard 架构的 Active Directory 对象概述 122
Dell Extended 架构 Active Directory 对象概述 124

使用 Dell 架构扩展配置 Active Directory 以访问 RCS 128
扩展 Active Directory 架构(可选) 128
安装 Dell Extension to the Active Directory Users and Computers Snap-In(可选) 129
打开 Active Directory 用户和计算机插件 129

使用 Dell 架构扩展将用户和权限添加到 Active Directory 130
创建 SIP 对象 130
创建权限对象 130

使用 Dell 关联对象语法 131
创建关联对象 132
将对象添加到关联对象 132

控制台重定向访问安全 133

使用 Active Directory 登录 RCS 134

LDAP 实施过程中的目标设备命名要求 134

常见问题解答 135
附录 A：终端操作 139
控制台 Boot 菜单选项 139
控制台 Main 菜单选项 140
附录 B：使用 SIP 141
ACS 控制台服务器端口脚位排列 141
Cisco 端口脚位排列 142
附录 C：MIB 和 SNMP 陷阱 143
附录 D：缆线脚位排列信息 149
调制解调器脚位排列 149
控制台/设置端口脚位排列 149
附录 E：UTP 缆线 151
UTP 铜缆 151
布线标准 151
缆线安装、维护和安全说明 152
附录 F：Sun 高级键仿真 155
附录 G：技术规格 157
附录 H：技术支持 161

1

产品概述

Dell 1082DS/2162DS/4322DS RCS (RCS) 数字 KVM(键盘、视频和鼠标) over IP 和串行控制台交换机通过综合模拟和数字技术实现对数据中心服务器灵活集中的控制，便于远程分支办公室在没有训练有素的操作员的情况下进行操作、激活和维护。基于 IP 的 RCS 使您可以通过 RCS 软件或板载 web 界面 (OBWI) 随时随地灵活控制目标设备管理操作并安全地进行远程访问。

特点与优点

RCS 为企业客户提供以下特性和选项：

- 大幅度减少缆线数量
- 虚拟媒体 (VM) 功能，可配置用于模拟(本地) 或数字(远程) 连接
- 智能卡/通用访问卡 (CAC) 功能
- 采用 Secure Shell (SSH) 和 Telnet 的真正的串行功能
- 支持增强的视频分辨率，从目标到远程的原生分辨率高达 1600 x 1200 或 1680 x 1050(宽屏)
- 可选双电源型号以提供冗余
- 可选的用于管理智能电源设备的支持功能
- 双独立本地端口视频路径(专用于 ACI)
- 双堆栈 IPv4 (DHCP) 和 IPv6(DHCPv6 和无状态自动配置) ，以实现同时访问

- 通过 10/100/1000BaseT LAN 端口可访问目标设备。
- 支持兼容 V.34、V.90 或 V.92 调制解调器的 MODEM 端口，当以太网连接不可用时，该端口可用于访问交换机
- FIPS 支持

减少缆线堆放

随着服务器密度的不断增加，缆线数量一直是每个网络管理员关心的主要问题。RCS 采用新型的服务器接口转换器 (SIP) 和单一的行业标准的非屏蔽双绞线 (UTP)，可大幅度减少机架中的 KVM 缆线数量。这样服务器密度可以更高，同时具有更好的空气流通和冷却能力。

KVM 交换功能

RCS 支持由目标设备直接供电的 SIP，当交换机未开机时具有“保持加电”功能。采用 CAT 5 设计的 SIP 在提供最佳分辨率和视频设置的同时大大减少了缆线混乱的情况。SIP 的内置存储器为所连接的每台设备指定并保留唯一的设备名称和电子识别号码 (EID)，从而简化了配置。

提供 PS/2 和 USB 两种 SIP，允许与设备直接进行 KVM 连接。还提供 USB2+CAC SIP。RCS 提供 8、16 或 32 个用于连接 SIP 的模拟机架接口 (ARI) 端口。利用 SIP，您可以连接额外的交换机，以扩充 RCS 系统。这种灵活性使您可以随着数据中心的发展扩充容量。

多平台支持

Dell SIP 可以与 RCS 配合使用以支持 PS/2、USB、USB2 和 USB2+CAC 设备环境。通过将 OBWI 与这些模块配合使用，您可以轻松进行跨平台交换。

与 Avocent® IQ 模块智能缆线的互操作性也可用于将设备连接到 RCS。提供 PS/2、USB、Sun® 和串行模块选项。有关更多信息，请参阅产品相应的《Avocent 安装人员/用户指南》，或访问 avocent.com/manuals 获取更多信息。

真正的串行功能

RCS 支持通过 Telnet 提供真正串行功能的 SIP。通过 SIP，您可以从 OBWI 启动 SSH 会话或启动串行查看器，以连接到与 RCS 相连的串行目标设备。

本地和远程用户界面

您可以通过直接连接到本地端口使用本地用户界面（本地 UI）来管理 RCS，也可以使用远程 OBWI 管理您的交换机。OBWI 基于 web 浏览器，可从交换机直接启动，并且所有与交换机相连的设备都会被自动检测到。

支持虚拟媒体和智能卡的交换机

通过 RCS，您可以从任何目标设备上查看位于虚拟媒体上的数据，或将数据移动、复制到目标设备上。通过实现操作系统安装、操作系统恢复、硬盘恢复或复制、BIOS 更新和目标设备备份，您可以更有效地管理远程系统。

您还可以通过 RCS 将智能卡与交换机系统配合使用。智能卡是一种可存储和处理信息的袖珍卡。CAC 等智能卡可用于存储身份和身份信息，方便访问计算机、网络和实施安保措施的房间或建筑。

虚拟媒体和智能卡读卡器可直接连接到交换机上的 USB 端口。另外，虚拟媒体和智能卡读卡器可以连接到任何运行远程 OBWI、Dell RCS 软件或 Avocent 管理软件和通过以太网连接到交换机的远程工作站上。

注：要与目标设备进行虚拟媒体或智能卡会话，首先必须使用 SIP 将目标设备连接到交换机。

板载 Web 界面

OBWI 提供与 RCS 软件类似的管理功能，但不要求配备软件服务器或进行任何安装。OBWI 可从交换机直接启动，并且所有与 RCS 相连的服务器都会被自动检测到。您可以通过 web 浏览器使用 OBWI 来配置 RCS。您可从 OBWI 启动查看器以便与目标设备建立 KVM 和虚拟媒

体会话。OBWI 还支持 LDAP 身份验证，而该身份验证方法可实现通过单一界面管理多台 RCS 的权限许可。

使用标准的 TCP/IP 网络访问交换机

交换机提供无需代理的远程控制和访问。在连接的服务器或客户端上不需要安装特殊的软件或驱动程序。

注：客户端通过 Internet 浏览器连接到交换机。

您可以通过以太网或使用客户端的 V.34、V.90 或 V.92 调制解调器访问交换机和所有相连的系统。客户端可以位于任何提供有效网络连接的位置。

加密

本 RCS 支持对键盘/鼠标、视频和虚拟媒体会话进行 128 位 SSL (ARCFOUR) 以及 AES、DES 和 3DES 加密。

视频

本 RCS 可为模拟 VGA、SVGA 和 XGA 视频提供最佳分辨率。取决于交换机和服务器之间的缆线长度，您可以获得的分辨率高达 1600 x 1200 或 1680 x 1050(宽屏) 。

闪存升级

您可随时升级 RCS 和 SIP，以确保一直使用最新的固件版本。闪存升级可以通过 OBWI 或串行控制台启动。本 RCS 可以配置为自动进行 SIP 的固件升级。有关更多信息，请参阅第 47 页上的“升级 RCS 固件”。

堆叠扩充

本 RCS 的特点在于允许通过交换机上的每个模拟机架接口 (ARI) 端口堆叠更多的 Dell RCS。堆叠交换机的连接方式以与其他设备相同。这些堆叠的交换机使您可以在一个系统中连接多达 1024 台服务器。请参阅第 29 页上的“添加堆叠交换机”。

Avocent 管理软件插件

Avocent 管理软件可与交换机配合使用，使 IT 管理员可通过基于 web 的单一用户界面远程访问、监控和控制多个平台上的目标设备。有关更多信息，请参阅 Avocent 管理软件的《技术公告》。

FIPS 加密模块

RCS 交换机支持 FIPS 140-2 级别 1 加密安全要求。 FIPS 操作模式可通过 OBWI 或本地端口来启用或禁用，并在重新启动后执行。 当 FIPS 启用时，重新启动交换机需要大约两分钟才能完成 FIPS 模式完整性检查。 此外，当 FIPS 启用时，如果键盘、鼠标或视频加密设置为 128 位 SSL (ARCFOUR) 或 DES，加密等级将自动更改为 AES。


注：FIPS 操作模式最初为禁用状态，必须启用才能进行操作。


注：Setup 端口的出厂默认设置将自动禁用 FIPS 模块。


注：FIPS 模式可通过 DSView 软件插件进行更改。

RCS 交换机采用嵌入式 FIPS 140-2 经验证的加密模块(证书编号 1051) ，该模块按照 FIPS 140-2 实施指南第 G.5 节的指导原则在 Linux PPC 平台上运行。

FIPS 模式可通过 OBWI、本地端口或 DSView 插件启用/禁用。 启用或禁用 FIPS 模式需要重新启动交换机。固件升级至本版本或将状态设置为默认状态(Setup Port 菜单) 将禁用 FIPS 模式。

在 FIPS 模式中，加密类型将被限制为 AES 或 3DES。当 FIPS 启用时，如果键盘/鼠标或视频加密设置为 128 位 SSL 或 DES，加密等级将自动更改为 AES。在 FIPS 启用状态下，这些文件将采用 FIPS 兼容的算法 AES 来保存(或恢复) 。当 FIPS 禁用时，作为外部文件从装置保存或恢复到装置的用户数据库和装置配置文件将采用 DES 进行加密(或解密) 。

即使用户没有在 OBWI 的 Save(或 Load) 对话框中填写 Password 参数，情况也是如此，在这种情况下，将使用默认 OEM 密码来加密或解密。

启用 FIPS 模块的一个结果是导致之前保存的用户数据库与装置配置文件不兼容。在这种情况下，您可以暂时禁用 FIPS 模块，重新启动装置，恢复之前保存的数据库或配置文件，重新启用 FIPS 模块，重新启动装置，然后在 FIPS 模块启用的情况下重新将文件保存为外部文件。只要装置在 FIPS 模式启用的情况下运行，新保存的外部文件就能与装置兼容。

相反的情况同样适用，即在 FIPS 模块启用的情况下保存的数据库与配置文件不兼容，而无法恢复到未启用 FIPS 模块的装置或固件版本较低且不支持 FIPS 模块的装置时。

简单配置

图 1.1. RCS 配置示例

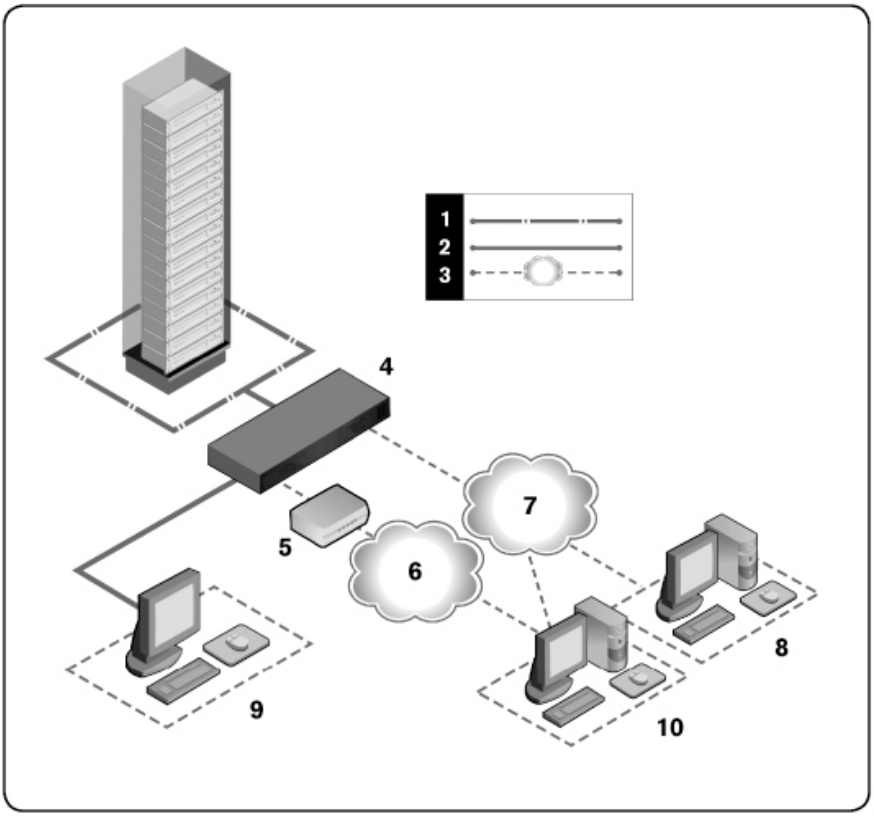


表 1.1：图 1.1 的说明

编号	说明	编号	说明
1	UTP 连接	6	电话网络
2	KVM 连接至 RCS	7	以太网
3	远程 IP 连接	8	Avocent 管理软件服务器
4	RCS	9	模拟用户（本地 UI）
5	调制解调器	10	数字用户（带 Internet 浏览器的计算机，用于支持远程 OBWI 或 Dell RCS 软件）

安全注意事项

使用以下安全指导方针有助于确保您个人的人身安全和防止您的系统和工作环境遭受可能的损害。

△ **注意：系统中的电源会产生高压和有危害的能量，可能会造成人身伤害。只有经过培训的维护技术人员才有资格打开机盖以及接触系统内部的任何组件。此警告适用于 Dell™ 远程控制台交换机、Dell™ PowerEdge™ 服务器和 Dell PowerVault™ 存储系统。**

本文档仅适用于 Dell 1082DS/2162DS/4322DS 远程控制台交换机。同时您应阅读并遵守其他安全说明：

- 《Dell 远程控制台交换机用户指南》
- 《Dell 安全数据表》(Dell Safety Sheet)
- 《Dell RTF 法规技术公告》(Dell RTF Regulatory Tech Bulletin)

一般信息

- 注意并遵守维修标志。
- 不要维修本系统文档中没有述及的任何产品。
- 打开或取下标有闪电三角形符号的机盖可能会遭到电击。
- 这些隔室内的组件只能由经过培训的维修技术人员进行维修。
- 本产品包含不可维修组件。不要尝试打开。

如果发生任何以下情况，请从电源插座上拔下本产品的电源插头，然后更换该部件或与经过培训的服务提供商联系：

- 电源线、延长线或插头损坏。
- 有物体落入产品内。
- 产品进水。
- 产品曾跌落或受损。
- 在遵守操作说明的情况下，产品仍不能正常工作。

- 确保系统远离任何辐射源和热源。另外，不要阻塞通风孔。
- 不要将食物或液体溅洒到系统组件上，并且切勿在潮湿的环境下使用本产品。如果系统受潮，请参阅故障排除指南中的相应部分，或者与经过培训的服务提供商联系。
- 仅与认可的设备配合使用。
- 在取下机盖或接触内部组件之前，请先让产品冷却。
- 仅使用电源额定标签上标示的外部电源类型作为本产品的电源。如果您不清楚规定的电源类型，请向您的服务提供商或当地电力公司咨询。

注：为避免损坏系统，请确保电源上的电压选择开关(如果提供) 切换到与您所在地区供应的交流电源最接近的档位。请同时确保您的显示器和所连接的设备的电源额定值适合使用。

- 请确保显示器和所连接的设备的电源额定值适合采用您所在地区供应的电源。
- 仅使用本产品随附的电源线。
- 为防止电击，请将系统和外围设备的电源线插入正确接地的电源插座。这些缆线配有三相插头，有助于确保正确接地。不要使用适配器插头或拆除缆线的接地极。
- 注意延长线和插线板的额定值。确保插在美式插线板上所有产品的额定电流总值不超过美式插线板额定电流限值的 80%。
- 为防止系统受到电源电压突然瞬时增加或降低的影响，请使用浪涌抑制器、线路调节器或不间断电源 (UPS)。
- 仔细布设系统缆线和电源线。将缆线布设在不会踩到或踢到的位置。确保缆线上没有放置任何物体。
- 不要改装电线或插头。如需现场改装，请向持证的电工或电力公司咨询。请务必遵守当地/国家的布线规定。

LAN 选项

- 不要在雷雨天气连接或使用。因为闪电可能带来电击的危险。
- 不要在潮湿的环境中连接或使用。

2

安装

RCS 使用以太网或调制解调器连接，通过网络在操作员和连接到交换机的目标设备之间传输 KVM 和串行信息。RCS 使用 TCP/IP 进行以太网通讯。为获得最佳系统性能，请使用 100BaseT 或 1000BaseT 专用交换网络。您也可以使用 10BaseT 以太网。

RCS 使用点对点协议 (PPP) 通过 V.34、V.90 或 V.92 调制解调器进行通讯。您可以使用 OBWI 或 Avocent 管理软件来执行 KVM 和串行交换任务。有关 Avocent 管理软件的更多信息，请访问 http://www.avocent.com。

RCS 产品套件包括 RCS、RCS 软件和 OBWI。您可以选择使用 RCS 软件或 OBWI 管理系统。OBWI 可以管理单台 RCS 及其连接，而 RCS 软件则可以管理多台交换机及其连接。如果您打算仅使用 OBWI，则无需安装 RCS 软件。

注：RCS 软件可以用于管理多台交换机。有关更多信息，请参阅产品相应的《安装人员/用户指南》。

注：请确保所有 RCS 的固件已升级为最新版本。有关通过 OBWI 升级 RCS 的信息，请参阅第 46 页上的"RCS 工具"。

RCS 快速安装

以下为快速安装列表。要开始将 RCS 安装到机架中以及要获得详细的安装说明，请参阅第 13 页上的"开始"。

1 将每台服务器上的鼠标加速调整为 Slow(慢) 或 None(无) 。

2 安装 RCS 硬件，并将服务器接口转换器 (SIP) 或 Avocent® IQ 模块连接至每台服务器或堆叠交换机。用 CAT 5 缆线将每个 SIP 或

Avocent IQ 模块连接到 RCS，并将键盘、显示器和鼠标连接器连接到 RCS 的模拟端口。

3 将本地端口外围设备连接到 RCS 背面板上相应的端口，然后设置网络配置。可以在此处或在 RCS 软件中设置 IP 地址。Dell 建议使用静态 IP 地址来简化配置。

4 使用本地端口，通过 OBWI 界面输入所有服务器名称。

要设置 RCS 软件（请参阅《RCS 软件用户指南》）：

1 在每个客户端工作站上安装 RCS 软件。

2 在客户端工作站上启动 RCS 软件。

3 单击 **New RCS task** 按钮将新交换机添加到 RCS 软件数据库。如果按上述步骤配置了 IP 地址，则选择 **Yes**, the product already has an IP address；否则请选择 **No**, the product does not have an IP address。

RCS 软件将查找 RCS 和与其相连的所有 SIP，并在 Explorer 中显示名称。

注：使用 RCS 软件，除了可以添加和管理 Dell RCS 之外，您还可以添加和管理某些 Avocent 交换机。

4 在 Explorer 中，根据需要设置服务器属性并按相应的位置、地点或文件夹将服务器分组。

5 通过 OBWI 创建用户帐户。有关更多信息，请参阅第 69 页上的“设置用户帐户”。

6 设置一台客户端工作站后，选择 **File - Database - Save** 以保存包含所有设置的数据库副本。

7 在第二台客户端工作站上，单击 **File - Database - Load**，然后浏览至已保存的文件。选择该文件，然后单击 Load。

8 如果本地用户在您加载此文件后添加、删除或重命名任何 SIP，您可以通过选择 RCS 并单击 **Resync** 来重新同步本地交换机。要控制一台已连接的服务器，请在 Explorer 中将其选中，然后单击 **Connect Video** 任务按钮以在查看器中启动服务器会话。

9 在查看器中，调整服务器视频的分辨率（选择 View - Scaling）和质量（选择 View - Color）。

开始

以下为远程控制台交换机的装箱清单。安装 RCS 前，请备好正确安装所需的物品。

- 远程控制台交换机
- 跳线
- 0U 安装支架
- 1U 安装支架配件套件（此套件包含另外两条预安装到 RCS 上的导轨）
- 用于 SETUP 和 MODEM 的缆线和适配器
- 《远程控制台交换机系统用户指南》（在 CD 上）
- 《Dell 安全数据表》(Dell Safety Sheet)
- 《Dell RTF 法规技术公告》(Dell RTF Regulatory Tech Bulletin)

其他需要的物品：

- Dell SIP 或 Avocent IQ 模块（每台连接的设备需要配备一个）
- CAT 5 跳线缆线（每台连接的设备需要配备一根，最长 45 米）

可选物品：

- 兼容 V.34、V.90 或 V.92 的调制解调器和缆线
- 电源控制设备
- 端口扩展模块 (PEM)

注：如果服务器通过 PEM 连接，则将无法建立虚拟媒体会话或 CAC 会话。

设置网络

本交换机利用 IP 地址对交换机和目标设备进行唯一识别。RCS 既支持动态主机配置协议 (DHCP)，又支持静态 IP 地址分配。请务必为每台交换机预留 IP 地址，并且当交换机连接到网络时，每个 IP 地址可以保持静态。

键盘

USB 键盘和鼠标可以连接到 RCS 的模拟端口。

注：RCS 的模拟端口还支持多键盘和多鼠标。然而，同时使用多个输入设备可能导致不可预见的后果。

机架安装 RCS

您可以将 RCS 放置在机架搁板上，也可以将交换机直接安装到 19 英寸宽、符合 EIA-310-E 标准的机架（四柱式、双柱式或螺纹式）内。提供的 Dell ReadyRails™ 系统用于进行 1U 前机架、1U 后机架和双柱安装。ReadyRails 系统包括两个独立包装的导轨组件和两条安装在 RCS 侧面且随其一起装运的导轨。此外，还配有一个安装支架用于 0U 配置，以及配有一个冲压板用于后机架安装。

警告：上述内容可作简单参考。开始前，请阅读《安全、环境和法规信息手册》中的安全说明。

注：本文档中的图示并不代表特定交换机。

机架安装的安全注意事项

- 机架装载：机架超载或负载不均衡可能会导致搁板或机架故障，从而导致设备损坏，并可能造成人身伤害。将机架安放在一个持久、稳固的位置，然后开始装入。从机架的底部开始安装组件，然后再到顶部。不要超过机架的额定装载量。
- 电源注意事项：请仅使用设备规定的电源。机架中安装多个电气组件时，请确保这些组件的总额定功率不超过电路的容量。电源和延长线超载存在火灾和电击危险。

- 环境温度的升高：如果在闭合组合架上安装，机架环境的工作温度可能会高于室内环境温度。切勿超出交换机的最高环境温度 (50°C)。
- 空气流通减少：设备采用机架安装时，必须严格保证设备安全操作所需的空气流通量。
- 可靠的接地：请保持机架安装式设备可靠接地。要特别注意供电连接，而非对分支电路的直接连接(例如使用美式插线板) 。
- 安装产品时，背面板不得朝下。

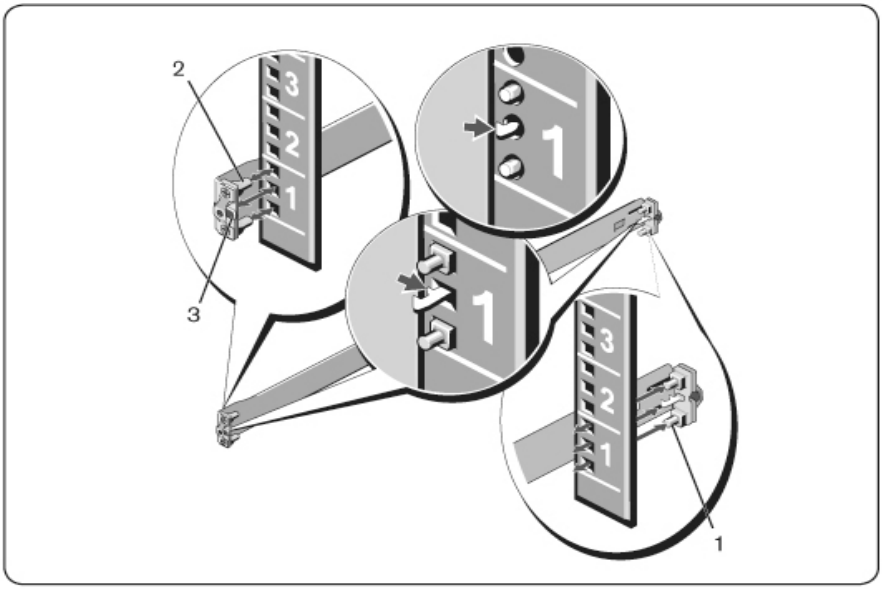
安装 Dell ReadyRails 系统

通过 ReadyRails 系统，您可以轻松地配置机架，以便安装 RCS。可以使用 1U 免工具安装法或三种 1U 工具安装法(双柱平壁式安装、双柱中央式安装或四柱螺纹安装) 之一安装 ReadyRails 系统。

1U 免工具配置(四柱方孔或无螺纹圆孔)

1 使 ReadyRails 凸耳朝外，将一条导轨置于左右垂直机架柱之间。对齐后凸缘导轨销钉，并将其安装到后垂直机架柱凸缘中。如图 2.1 所示，第 1 项及其放大图显示了销钉在方孔和无螺纹圆孔中的形态。

图 2.1. 1U 免工具配置



2 对齐前凸缘销钉（第 2 项），并将其安装到垂直机架柱前面的孔中。

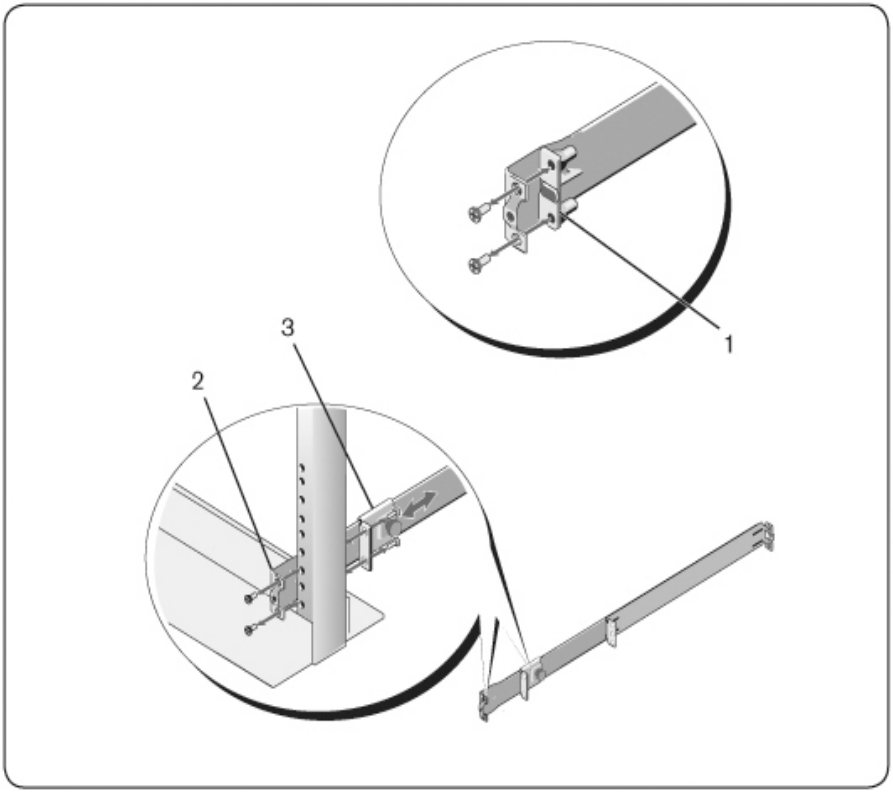
3 对第二条导轨重复此步骤。

4 要拆除各条导轨，拉动各个凸耳上的弹片释放按钮（第 3 项），然后取下各条导轨。

双柱平壁式安装配置

1 对于这种配置，必须拆除各个 ReadyRails 组件前面的铸件（图 2.2，第 1 项）。使用 Torx™ 螺丝刀拧下各个前凸耳上的两颗螺钉（导轨的设备侧），然后拆下各个铸件。保管好这些铸件，以便日后机架所需。无需拆除后凸缘铸件。

图 2.2. 双柱平壁式安装配置



2 使用两颗用户自备的螺钉将一条导轨安装到前机架柱凸缘上(第 2 项) 。

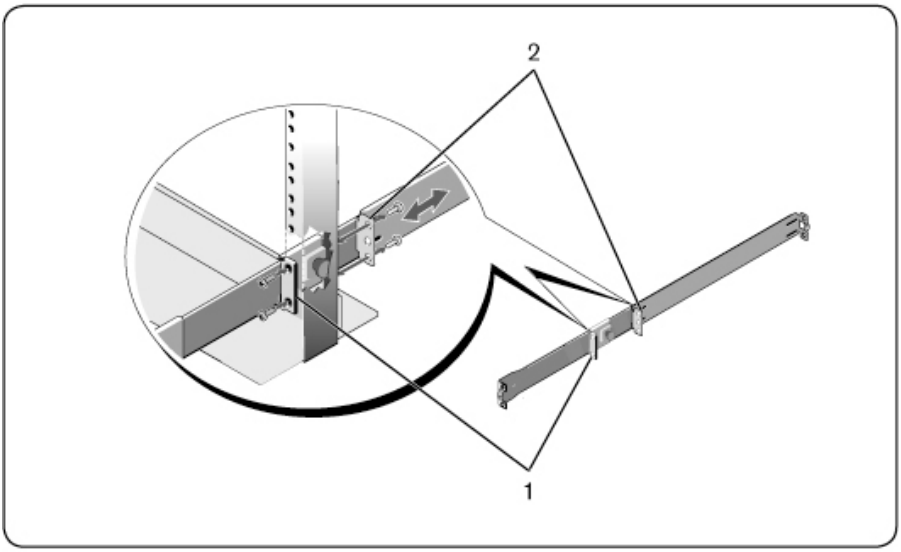
3 朝垂直机架柱向前滑动滑块，并使用两颗用户自备的螺钉将滑块固定到机架柱凸缘上(第 3 项) 。

4 对第二条导轨重复此步骤。

双柱中央式安装配置

1 向后滑动滑块，直到卡入到位，然后使用两颗用户自备的螺钉将其固定到前机架柱凸缘上（图 2.3，第 1 项）。

图 2.3. 双柱中央式安装配置



2 朝机架柱滑动后面的滑块，然后使用两颗用户自备的螺钉将其固定到机架柱凸缘上（第 2 项）。

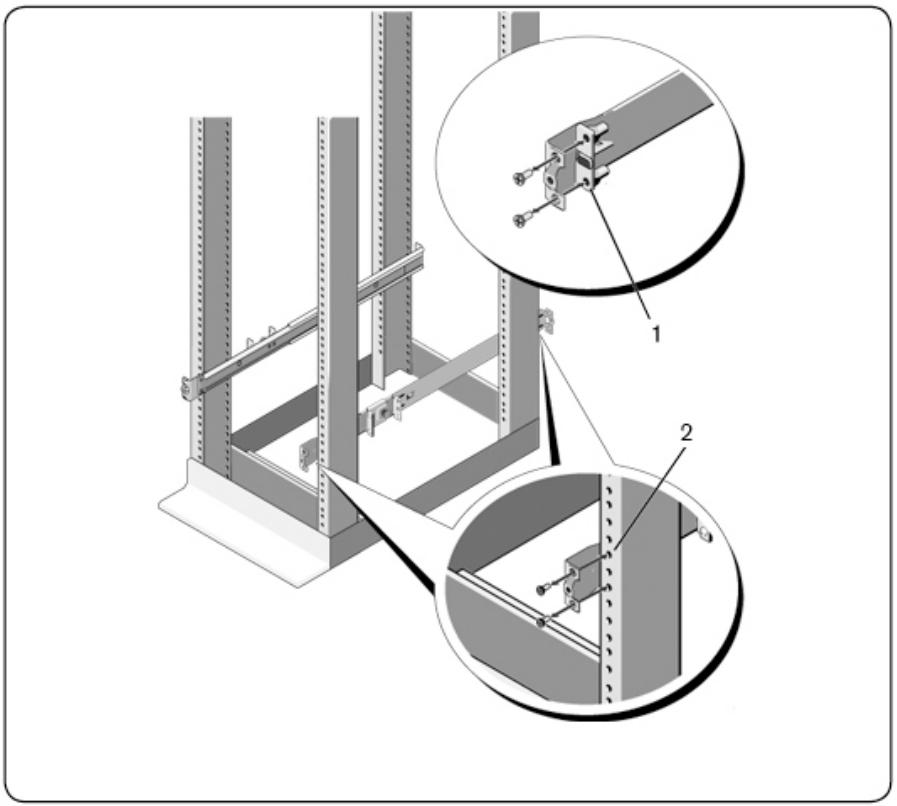
3 对第二条导轨重复此步骤。

四柱螺纹配置

1 对于这种配置，必须拆除各个 ReadyRails 组件末端的凸耳铸件。使用 Torx™ 螺丝刀拧下各个凸耳上的两颗螺钉，然后拆下各个铸件（图 2.4，第 1 项）。保管好这些铸件，以便日后机架所需。

2 对于每个导轨，在各个末端使用两颗用户自备的螺钉将前后凸缘安装到机架柱凸缘上(第 2 项) 。

图 2.4. 四柱螺纹配置



安装 RCS

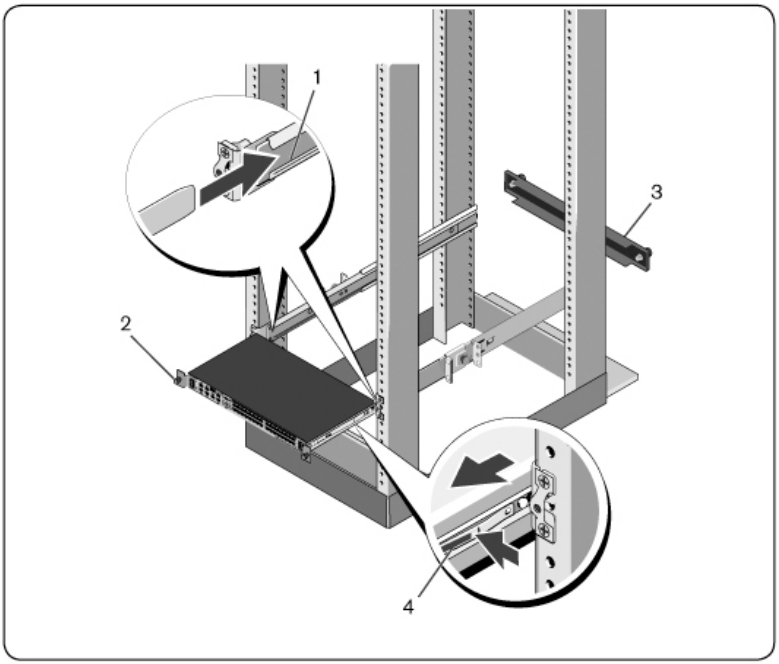
您可以将交换机安装到 1U 后机架、1U 前机架、1U 双柱(平壁式和中央式) 和 0U 配置中。以下为 1U 后机架、1U 前机架和 0U 配置的

示例。对于 1U 双柱（平壁式和中央式）配置，您可以使用与四柱配置相同的方式将交换机滑入导轨中。

1U 后机架安装

1 将连接交换机的导轨末端插入 ReadyRails 组件，然后将交换机推入机架（图 2.5，第 1 项）。

图 2.5. 1U 后机架安装



2 使用翼形螺钉固定各个交换机导轨（第 2 项）。

3 （可选）将冲压板（第 3 项）安装到机架前面的导轨上，然后拧紧翼形螺钉。

要从机架上拆下交换机：

1 松开翼形螺钉，并将交换机组件拉出机架，直到到达止动位置。止动位置用于重新定位导轨夹；并非为了便于维修。

2 找到交换机导轨上的蓝色插片（第 4 项）。

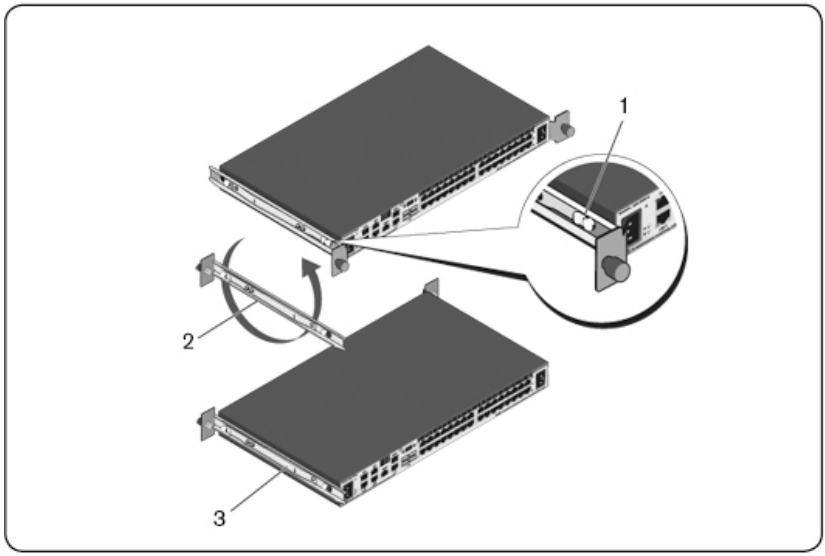
3 向内按压插片，并继续拉动组件，直到交换机导轨从 ReadyRails 组件上松脱。

1U 前机架安装

安装前，必须重新配置连接交换机的导轨。

1 在各个交换机导轨上，拉起前支座下方的插片，从交换机上拉起导轨时向前滑动导轨（图 2.6，第 1 项）。

图 2.6. 旋转交换机导轨



2 将各条导轨旋转 180°（第 2 项），然后将各条导轨重新安装到交换机上（第 3 项）。

3 有关在 ReadyRails 系统上插入和拆除交换机组件的方法，请参阅 1U 后机架说明。

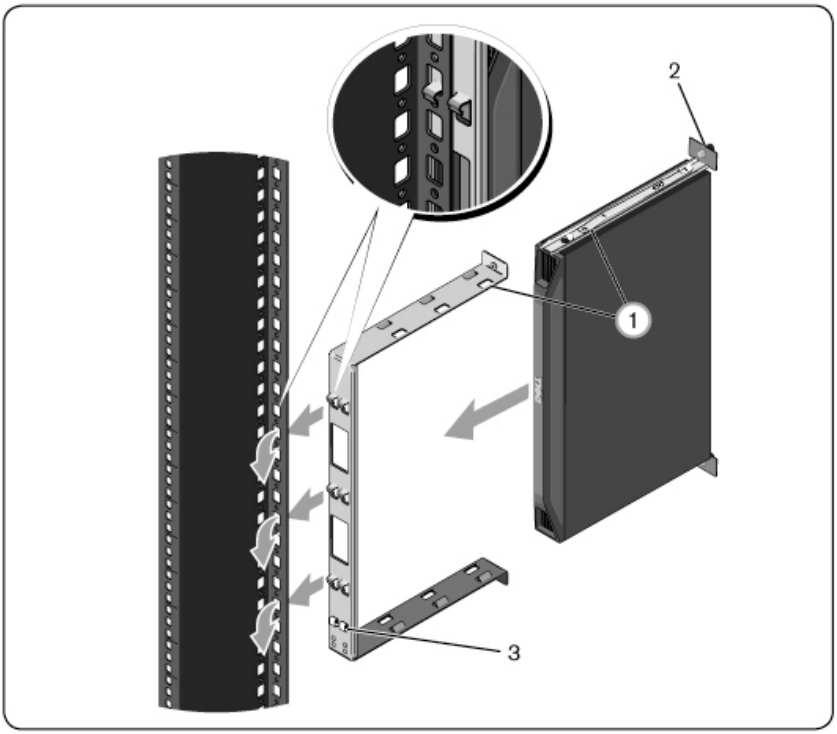
注：此配置不需要安装冲压板。

0U RCS 安装

1 对齐 0U 安装支架，并将其安装到交换机导轨上（图 2.7，第 1 项）。拧紧翼形螺钉（第 2 项）。

2 将安装支架挂钩插入机架孔中并向下按，直到蓝色按钮跳出并将支架锁紧到位。

图 2.7. 0U 安装



要拆除交换机组件，按下蓝色按钮(第 3 项) 松开支架，然后从机架柱中拉出组件。

连接 RCS 硬件

下图所示为 RCS 硬件的一种可能的配置。

图 2.8. 基本 RCS 配置

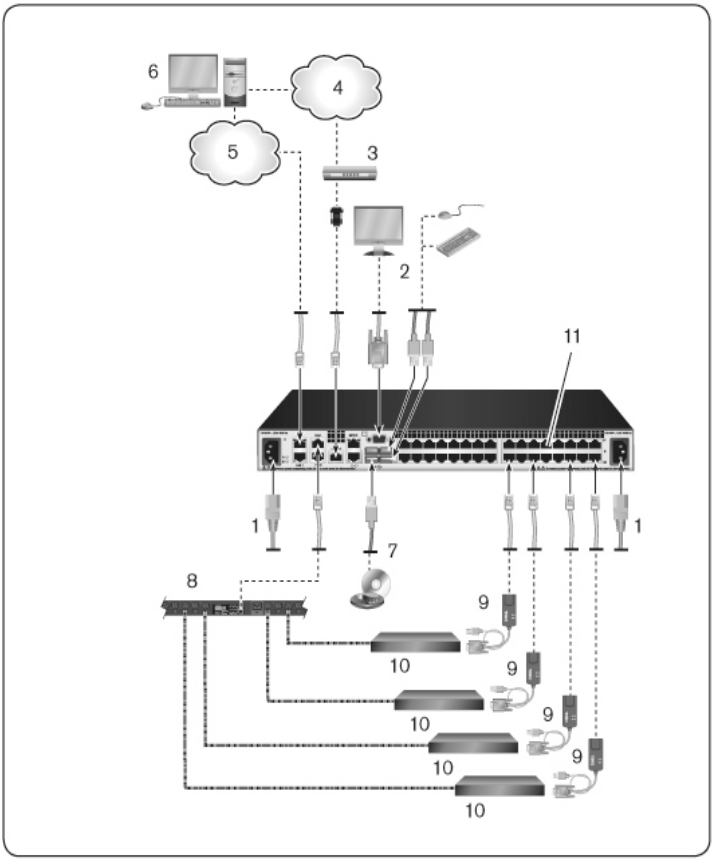


表 2.1：基本 RCS 配置说明

编号	说明	编号	说明
1	跳线	7	外部虚拟媒体

编号	说明	编号	说明
2	模拟用户	8	电源控制设备
3	调制解调器	9	SIP
4	电话网络	10	目标设备
5	网络	11	RCS(图示为 32 端口型号)
6	数字用户		

要连接并启动交换机：

注意：为降低电击或损坏设备的危险，不要拔掉跳线的接地插头。接地插头是一个重要的安全特性。将跳线插入一个任何时候都能方便插拔的接地的插座。要切断设备的电源，请从电源或设备本身拔掉跳线。

注：如果所在建筑物具有 3 相交流电，请确保计算机和显示器在同一个相上，以避免可能发生的与相位相关的视频和/或键盘问题。

注：所支持的从交换机到设备的缆线的最大长度可达 30 米。

- 不要拔掉电源接地插头。接地插头是一个重要的安全特性。
- 将跳线接入一个任何时候都能方便插拔的接地的插座。
- 要切断产品的电源，请从电源或设备本身拔掉跳线。
- 交流接入插座是本产品断电的主要断开点。对于拥有多个交流接入插座的产品，必须断开所有交流电源线，才能彻底断电。
- 本产品的外壳内没有用户可自行维修的部件。不要打开或拆除产品机盖。

1 将 VGA 显示器以及 USB 键盘和鼠标缆线连接到有适当标记的端口。

2 将 UTP 缆线(4 对，最长为 45 米) 的一端连接到带编号的可用端口。将另一端连接到 SIP 的 RJ-45 接头上。

3 将 SIP 连接到目标设备背面的相应端口。对所有需要连接的目标设备重复步骤 2 和 3。

注：在连接 Sun Microsystems 目标设备时，必须在本地端口上使用多同步显示器，才能与同时支持 VGA 和绿色同步 (sync-on-green) 或合成同步 (Composite) 信号的 Sun 计算机相匹配。

4 将用户自备的连入以太网网络的 UTP 缆线连接到 RCS 背面的 LAN 端口。网络用户将通过此端口访问 RCS。将冗余 LAN 端口插入独立的以太网交换机可在一个以太网交换机出现故障时提供额外冗余。

5 （可选）用户也可以通过兼容 ITU V.92、V.90 或 V.24 的调制解调器访问交换机。将 RJ-45 缆线的一端连接到交换机的 MODEM 端口。将另一端插入随附的 RJ-45 至 DB-9（公）适配器，然后将该适配器连接到调制解调器背面的相应端口。

注：使用调制解调器连接取代 LAN 连接将会限制交换机的性能。

6 （可选）通过将 CAT 5 缆线的一端连接到交换机的 PDU1 端口，将受支持的 PDU 连接到 RCS。再把另一端连接到 PDU。将目标设备的电源线连接到 PDU。再将 PDU 连接到电源。如需要，重复此步骤将第二个 PDU 连接到 PDU2 端口。

7 打开每台目标设备的电源，然后找到交换机随附的跳线。将其中一端连接到交换机背面的电源接口上。将另一端连接到适当的电源。如果使用的 RCS 配有双电源，则应将第二根跳线连接到 RCS 背面的第二个电源接口中，并将另一端插入其他电源。

注：将冗余电源插入独立的分支电路，以在一个外部交流电源断开时另外提供冗余。

8 （可选）将虚拟媒体设备或智能卡读卡器连接到交换机上的任意 USB 端口。

注：所有的虚拟媒体会话都必须使用 USB2 或 USB2+CAC SIP。

连接 SIP

将 SIP 连接到每台服务器：

1 找到 RCS 的 SIP。

2 如果您使用 PS/2 SIP 连接，请将 SIP 缆线的带有不同颜色标记的端口连接到将要连接到此 RCS 的第一台服务器的相应键盘、显示器和鼠标端口。如果您使用 USB 连接，则请将 SIP 的插头连接到将要连接到此 RCS 的第一台服务器上的 USB 端口。

3 将用于连接 SIP 和 RCS 的 CAT 5 缆线的一端连接到 SIP 的 RJ-45 连接器。请参阅图 2.9。

4 将 CAT 5 缆线的另一端连接到 RCS 背面的 Avocent 机架接口 (ARI) 端口。

5 对要连接的所有服务器重复步骤 2-4。

注：在维修之前，请关闭 RCS 电源。一定要将跳线从电源上断开。

注：除了 Dell SIP 以外，本 RCS 还可以连接到使用 Avocent IQ 模块(包含 Sun 和串行 IQ 模块) 的设备。

图 2.9. SIP 连接

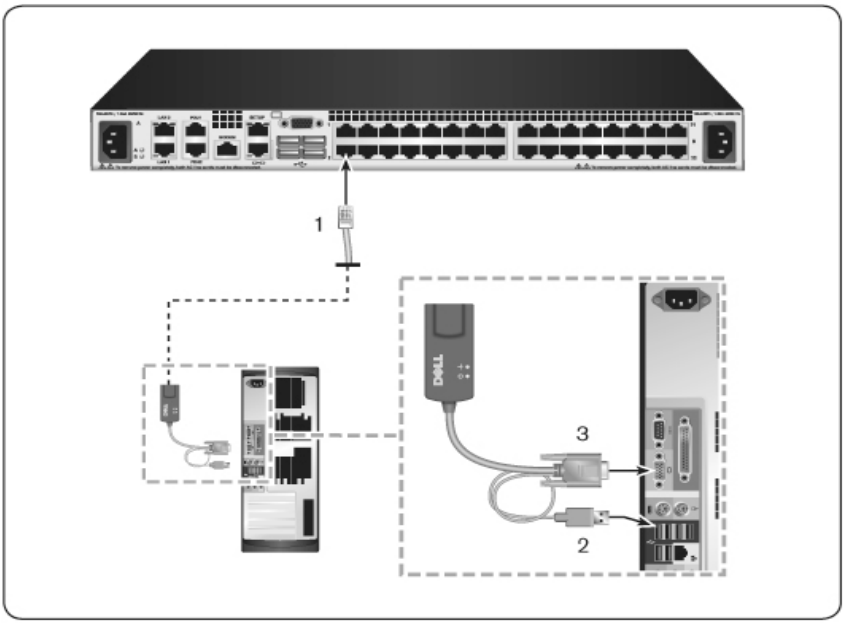


表 2.2：图 2.9 的说明

编号	说明
1	CAT 5
2	USB 连接
3	VGA 连接

要使用 UTP 连接器将 SIP 连接到串行设备：

1 将 SIP RJ-45 连接器连接到串行设备。

-或-

将 SIP 连接到 RJ-45 至 9 针母式适配器。将适配器连接到串行设备的串行端口。

2 将 UTP 缆线（4 对，最长为 45 米）的一端连接到交换机背面带编号的可用端口。将另一端连接到 SIP 的 RJ-45 连接器上。

3 将 USB-to-barrel 电源线连接到 SIP 上的电源连接器。将 USB-to-barrel 电源线上的 USB 连接器连接到串行目标设备上的任何可用 USB 端口。

添加堆叠交换机

注：本 RCS 不支持 EL80-DT。

注：堆叠配置中支持 M1000e Modular Enclosure。将 CAT5 缆线的一端连接到 RCS 交换机的目标端口。将另一端连接到模拟控制台接口 (ACI) 兼容的 RJ45 端口（位于 M1000e 机箱背面的 iKVM 模块上）。M1000e Modular Enclosure 组件的固件升级无法通过此堆叠配置实现。

您最多可以堆叠两层交换机，使用户可以连接多达 1024 台服务器。在堆叠系统中，主交换机的每个目标端口都将连接至每台堆叠交换机的 ACI 端口。然后，每台堆叠交换机可以通过 SIP 或 Avocent IQ 模块连接到一台设备。

要堆叠多台交换机：

1 将 UTP 缆线的一端连接到交换机的目标端口。

2 将该 UTP 缆线的另一端连接到堆叠交换机背面的 ACI 端口。

3 将设备连接到堆叠交换机。

4 对所有要连接到系统的堆叠交换机重复这些步骤。

注：系统将自动"合并"这两台交换机。所有连接到堆叠交换机的交换机均将显示在本地 UI 的主交换机列表内。

注：本交换机支持每个主交换机目标端口堆叠一台交换机。堆叠交换机不能再堆叠更多交换机。

注：当与 RCS 进行级联时，不支持 8 端口或 16 端口的模拟控制台交换机作为堆叠配置中的初级设备。初级设备必须是 RCS。

图 2.10. 将 UTP 模拟交换机与 RCS 进行堆叠

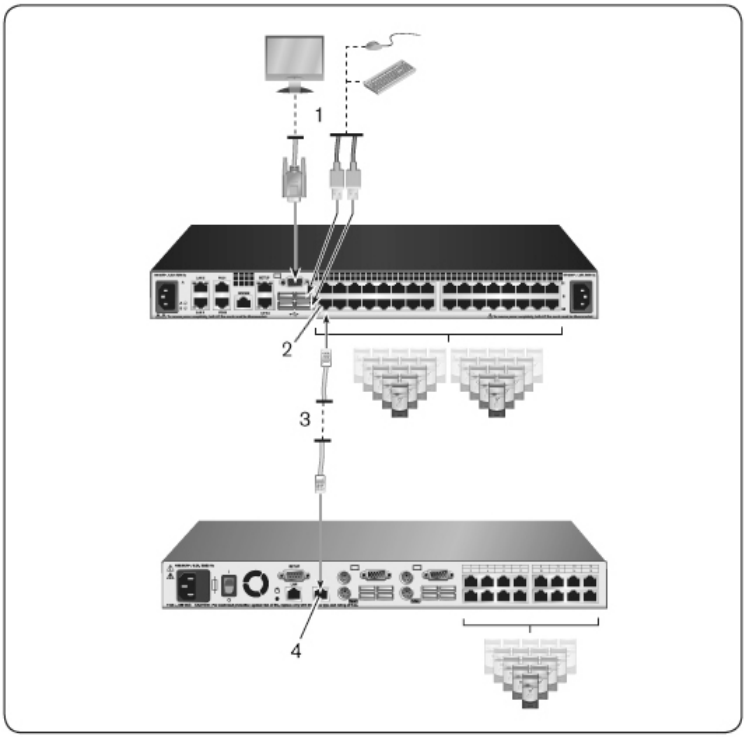


表 2.3：图 2.10 的说明

编号	说明
1	本地用户
2	ARI 连接
3	UTP 连接
4	ACI 连接

与旧式交换机进行级联

要添加旧式交换机(可选项) ：

1 将交换机安装到机架上。找到连接 RCS 和旧式交换机的 UTP 缆线。

2 将 UTP 缆线的一端连接到控制台交换机的 ARI 端口。

3 将 UTP 缆线的另一端连接到 PS/2 SIP。

4 按照交换机生产厂商建议的方式将 SIP 连接到旧式交换机。

5 对您要连接到交换机的所有旧式交换机重复步骤 1-4。

注：RCS 每个 ARI 端口仅支持一台交换机。不可以在此第一台交换机下再级联另一台交换机。

注：当与 RCS 进行级联时，不支持将 8 端口或者 16 端口的模拟控制台交换机作为初级设备。初级设备必须是 RCS。

图 2.11. 级联旧式交换机

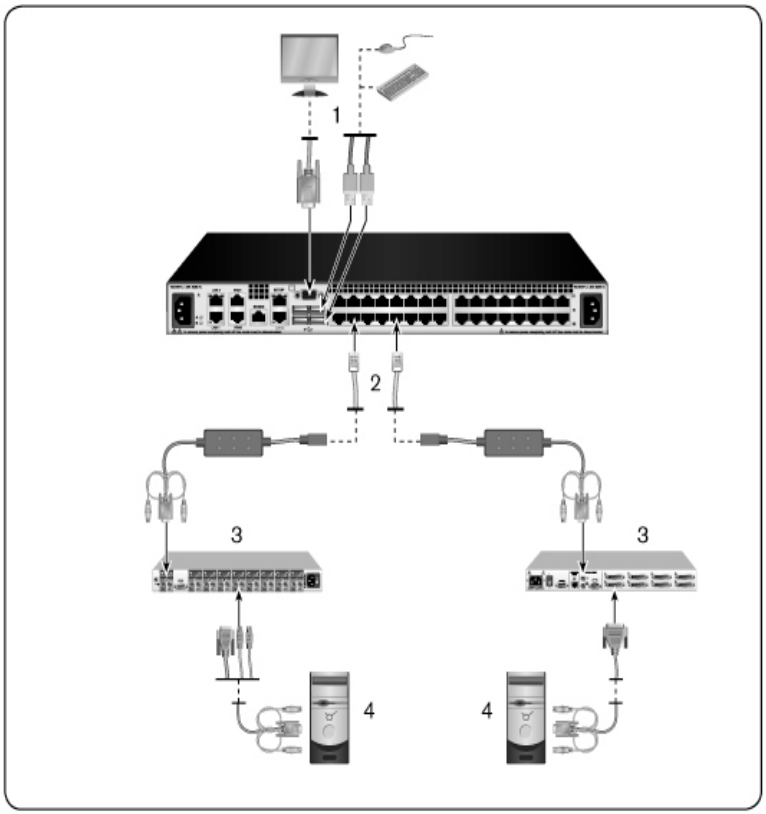


表 2.4：图 2.11 的说明

编号	说明
1	本地用户
2	ARI 连接

编号	说明
3	PS2 连接
4	目标连接

添加 PEM(可选)

端口扩展模块 (PEM) 允许您将每个 ARI 端口扩展至可容纳八台设备，而不是一台。请参见下图及其说明表。

注：PEM 以被动的方式工作。因此，当一个用户访问连接到 PEM 的一台设备时，随后试图访问连接到 PEM 的任何设备的任何用户都将被阻挡。

注：不支持在 PEM 之后使用 VM 或 CAC SIP。

注：真正的串行 SIP 无法在 PEM 之后正常运行。

要添加 PEM(可选) ：

1 将 PEM 安装到机架上。使用最多九条 UTP 缆线，一条将 RCS 连接到 PEM，其余八条将 PEM 连接到每台设备所连接的 SIP。

2 将准备用于连接 PEM 和 RCS 的 UTP 缆线的一端连接到 PEM 上与其他连接器稍微隔开的 RJ-45 连接器。将 UTP 缆线的另一端连接到 RCS 背面所需的 ARI 端口。

3 将准备用于连接 PEM 和每台设备的 SIP 的 UTP 缆线连接到聚集在 PEM 背面的八个 RJ-45 连接器中的一个。

4 将 UTP 缆线的另一端连接到第一个 SIP。

5 对要连接的所有设备重复步骤 3-4。

图 2.12. 带 PEM 的 RCS 配置

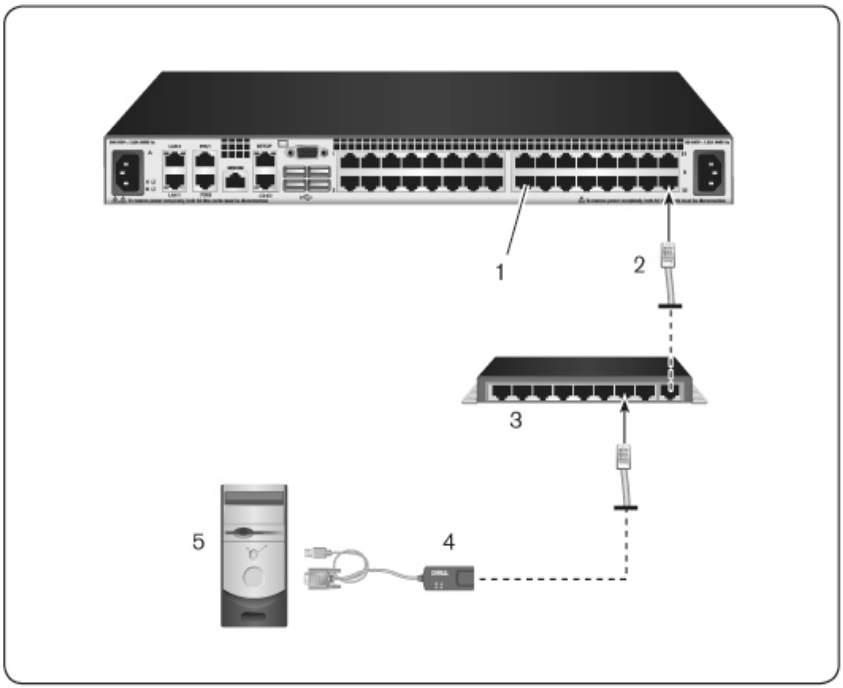


表 2.5：图 2.12 的说明

编号	说明
1	ARI 端口
2	UTP
3	PEM
4	SIP 或 Avocent IQ 模块
5	服务器

配置远程控制台交换机

完成所有物理连接后，您将需要配置交换机以便在整个交换机系统中使用。配置方式有两种。

要使用 Avocent 管理软件配置交换机，请参阅适用的《Avocent 安装人员/用户指南》以获取详细说明。

要使用本地 UI 配置交换机：

请参阅第 49 页上的"网络设置"，以获取有关使用本地 UI 配置初始网络设置的详细说明。

设置内置 Web 服务器

您可以使用嵌入式 web 服务器访问交换机，该服务器可以处理大多数日常交换机任务。请先通过交换机背面板的 SETUP 端口或本地 UI 指定 IP 地址，再使用 web 服务器访问交换机。有关使用交换机用户界面的详细说明，请参阅第 3 章。

通过防火墙连接到 OBWI

对于使用 OBWI 进行访问的交换机安装配置，如果需要外部访问，则必须在防火墙中打开以下端口。

表 2.6：防火墙中的 OBWI 端口

端口号	功能
TCP 22	用于 SSH，以便与 SIP 进行串行会话。
TCP 23	用于 Telnet（启用 Telnet 时）。
TCP 80	用于初始下载视频查看器。RCS 管理员可更改该值。
TCP 443	由 web 浏览器使用，用于管理交换机和启动 KVM 会话。RCS 管理员可更改该值。

端口号	功能
TCP 2068	用于传输交换机上的 KVM 会话数据（鼠标和键盘）或视频
TCP/UDP 3211	用于进行发现。
TCP 389	（可选）由 LDAP 目录服务使用；标准访问端口
TCP 636	（可选）由 LDAP 目录服务使用；安全/SSL 端口
TCP 3268	（可选）由 Microsoft Active Directory 服务使用；标准访问端口
TCP 3269	（可选）由 Microsoft Active Directory 服务使用；安全/SSL 访问端口

以下图示和表格为典型配置，其中用户计算机位于防火墙的外部，而交换机常驻于防火墙的内部。

图 2.13. 典型的 RCS 防火墙配置

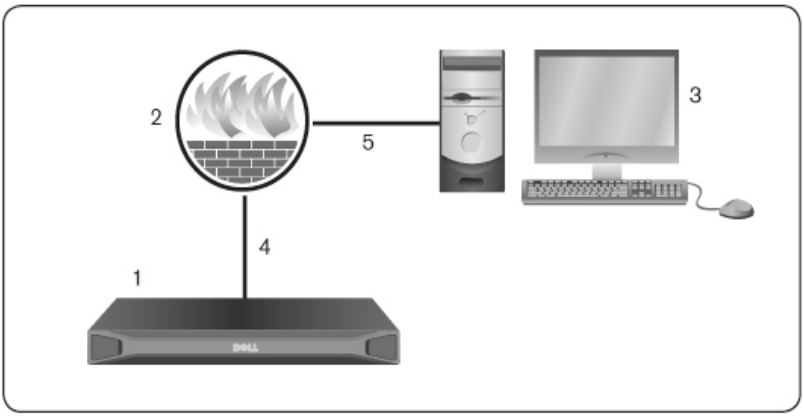


表 2.7：图 2.13 的说明

编号	说明
1	RCS
2	防火墙
3	用户计算机
4	防火墙将 HTTP 请求和 KVM 流量转发至交换机
5	用户浏览至防火墙的外部 IP 地址

要配置防火墙：

要从防火墙外部访问交换机，请配置防火墙，以便使防火墙将端口 22、23(如果启用 telnet) 、80、443、2068 和 3211 的通讯从其外部界面转发至内部界面，从而到达 KVM 交换机。有关特定端口的转发说明，请参阅防火墙手册。

注：端口 80 和 443 可由管理员重新配置。

有关启动 OBWI 的信息，请参阅第 40 页上的“OBWI”。

验证连接

后面板以太网连接 LED

在 RCS 上，后面板配有两个指示以太网 LAN1 连接状态的 LED 和两个指示以太网 LAN2 连接状态的 LED。

- 绿色的 LED 会在网络建立有效连接时亮起，在端口上有活动时闪烁。
- 双色 LED 可能会亮绿色或琥珀色。
  - 通讯速度为 1000M 时亮绿色。
  - 通讯速度为 100M 时亮琥珀色。
  - 通信速度为 10M 时不会亮起。

后面板电源状态 LED

每个 RCS 的后面板都配有一个 LED 用于指示各自的电源。双电源型号(16 端口和 32 端口) 具有两个电源 LED，而 8 端口型号只有一个 LED。交换机启动且工作正常时，LED 将亮绿色。

- 如果电源未加电或出现故障，LED 将不会亮起。
- 设备处于待命状态时，LED 将亮起。
- 交换机正在启动或正在升级时，LED 将闪烁。
- 如果出现电源故障、环境温度过高或风扇故障等不良情况，LED 将闪烁“SOS”信号。只要故障存在，LED 将持续闪烁“SOS”信号。

本交换机可防止在模块断电时与所连接的设备的串行连接中断。但是，用户可以通过在串行会话查看器中按 **Serial Break** 断开与所连接设备的串行连接。

调整目标设备上的鼠标设置

要使远程用户能控制连接到本交换机的计算机，必须先设置目标鼠标速度并关闭鼠标加速。对于运行 Microsoft® Windows®(Windows NT®、2000、XP、Server 2003) 的机器，请使用默认的 PS/2 鼠标驱动程序。

为确保本地鼠标的移动与远程光标显示保持同步，通过 KVM 交换机访问远程系统的所有用户帐户的鼠标加速都必须设置为“无”。每个远程系统的鼠标加速也必须设置为“无”。不得使用特殊指针，并且要确保指针踪迹、*Ctrl* 键显示指针位置、指针阴影和指针隐藏等指针可见性选项已关闭。

注：如果您无法在 Windows 操作系统上禁用鼠标加速，或您不想调整所有目标设备的设置，您可以在视频查看器窗口中使用 *Tools - Single Cursor Mode* 命令。此命令将使视频查看器窗口处于“隐形鼠标”模式，这样您就可以在所查看目标系统的鼠标指针与客户端计算机的鼠标指针之间手动切换控制。

3

本地和远程配置

RCS 具备两种“point-and-click”界面：本地用户界面(本地 UI) 和远程 OBWI。使用这些界面提供的配置选项，您可以根据具体应用自定义交换机、控制任何相连的设备以及处理所有基本的 KVM 或串行交换机需求。

注：本地 UI 和远程 OBWI 几乎完全相同。除非另有说明，否则本章节中的所有信息均适用于这两种界面。

使用其中任意一种界面您都可以启动两种不同的会话窗口：

- 视频查看器窗口，通过它您可以实时控制连接到交换机的单个目标设备的键盘、显示器和鼠标功能。您还可以在视频查看器窗口内使用预定义的全局宏执行操作。有关使用视频查看器的说明，请参阅第 4 章。
- 串行查看器窗口，您在其中可以使用命令或脚本管理单个串行目标设备。

本地用户界面 (UI)

本交换机背面具有一个本地端口。通过此端口，您可以将键盘、显示器和鼠标直接连接到交换机并使用本地 UI。

您可以选择以下任何配置的键击来打开本地 UI 或在本地 UI 和活动会话之间切换：<Print Screen>、<Ctrl + Ctrl>、<Shift + Shift> 和 <Shift + Shift>。默认为 <PrintScreen> 和 <Ctrl-Ctrl>。

要启动本地 UI：

1 将显示器、键盘和鼠标缆线连接到交换机。有关更多信息，请参阅第 23 页上的“连接 RCS 硬件”。

2 按任何已启用的击键启动本地 UI。

3 如果启用了本地 UI 身份验证，请输入您的用户名和密码。

注：如果交换机已添加到 Avocent 管理软件服务器，则将访问 Avocent 管理软件服务器以便对用户进行身份验证。如果没有将交换机添加到 Avocent 管理软件服务器，或无法连接 Avocent 管理软件服务器，则将访问交换机本地用户数据库以便对用户进行身份验证。默认的本地用户名为 Admin，没有密码。本地用户数据库的用户名区分大小写。

本地端口用户界面中连接的目标设备可通过从左侧导航栏选择的两个单独的画面查看和管理。如果目标设备少于 20 个，建议使用 Target List-Basic 画面进行导航。如果目标设备多于 20 个，Target List-Full 画面将提供其他的导航工具。在 Target List-Full 画面中，您可以通过输入页码、使用页面导航按钮或使用过滤器来进行导航。Basic 和 Full 画面都可以设置为默认画面，以便选择目标设备。

过滤

输入用于检索匹配项目的文本字符串，即可过滤目标设备列表。过滤可以提供更短且更精确的项目列表。执行过滤时，将在 Name 列搜索指定的文本字符串。搜索不区分大小写。过滤时，您可将星号 (*) 用作通配符放到文本字符串的前面或后面。例如，输入 **emailserver*** 并单击 *Filter*，则会显示开头包含 emailserver 的项目（如 emailserver、emailserverbackup 等）。

OBWI

交换机 OBWI 是一种基于 web 浏览器的远程用户界面。有关系统设置的详细信息，请参阅第 23 页上的“连接 RCS 硬件”。下表列出了 OBWI 支持的操作系统和浏览器。请务必使用最新版本的 Web 浏览器。

表 3.1：OBWI 支持的操作系统

操作系统	浏览器	
	Microsoft® Internet Explorer 6.0 版 (SP1) 及更高	Firefox 2.0 版及更高
Microsoft Windows 2000 Workstation 或 Server (SP2) 版	是	是
Microsoft Windows Server® 2003 Standard、Enterprise 或 Web 版	是	是
Microsoft Windows Server® 2008 Standard、Enterprise 或 Web 版	是	是
Windows XP Professional (SP3) 版	是	是
Windows Vista® Business (SP1) 版	是	是
Red Hat Enterprise Linux® 4 和 5 Standard 版、Enterprise 版或 Web Edition 版(该操作系统可能不支持智能卡)	否	是
Sun Solaris® 9 和 10(该操作系统可能不支持智能卡)	否	是
Novell SUSE Linux Enterprise 10 和 11(该操作系统可能不支持智能卡)	否	是
Ubuntu 8 Workstation(该操作系统可能不支持智能卡)	否	是

要登录交换机 OBWI：

1 启动 web 浏览器。

2 在浏览器的地址栏中，输入分配给要访问的交换机的 IP 地址或主机名。格式为：http://xxx.xx.xx.xx 或 https://hostname as the format。

注：如果使用 IPv6 模式，则必须用方括号将 IP 地址括起。格式为：http://[<ipaddress-]。

3 当浏览器连接上交换机时，请输入您的用户名和密码，然后单击 *Login*。将出现交换机 OBWI。

注：默认用户名是 Admin，没有密码。

要从防火墙外部登录交换机 OBWI，重复上述步骤，但是要输入防火墙的外部 IP 地址。

注：RCS 将尝试检测您的 PC 上是否已安装 Java。如果没有安装，您需要先安装 Java 才能使用板载 web 界面。您还需要将 JNLP 文件与 Java WebStart 关联起来。

注：必须安装 1.6.0_11 或更高版本的 Java Runtime Environment (JRE) 才能使用板载 web 界面。

注：登录板载 web 界面后，如要启动新会话，您将不必再次登录，除非您已注销或会话已超过管理员指定的非活动超时时间。

使用用户界面

通过身份验证后，将出现用户界面。您可以查看、访问和管理您的交换机，还可以指定系统设置和更改配置设置。下图显示了用户界面窗口区域。随后的表格提供了窗口说明。

图 3.1. 用户界面窗口

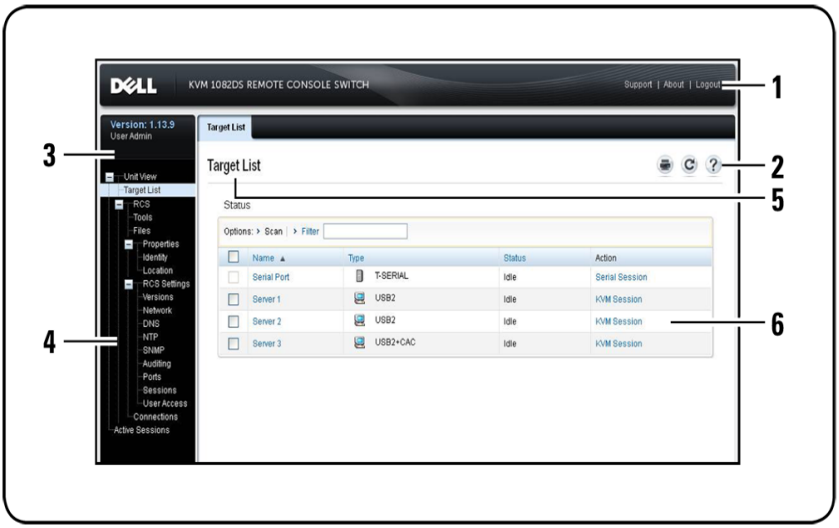


表 3.2：用户界面说明

编号	说明
1	顶部选项栏：使用顶部选项栏联系技术支持部门、查看软件常规信息或注销 OBWI 会话。
2	第二选项栏：此选项栏用于打印 web 页面、刷新当前 web 页面或访问 Help 工具。
3	版本显示区：产品的固件版本和登录用户的用户名显示在顶部选项栏的左侧。

编号	说明
4	侧面导航栏：侧面导航栏用于选择要显示的信息。您可以使用侧面导航栏显示要窗口以便指定设置或执行操作。
5	导航选项卡：选定的选项卡在内容区显示系统信息。某些选项卡具有子选项卡，单击这些子选项卡可显示和修改某个类别中的详细信息。
6	内容区：内容区用于显示或更改交换机 OBWI 系统。

启动会话

注：需要安装 Java 1.6.0_11 或更高版本才能启动会话。

要启动会话：

1 在侧面导航栏中，选择 Target List。将会出现一个可用设备列表。

2 适用操作（即 KVM Session 或 Serial Session）将显示在 Action 列中，并且将根据选定的目标设备启动会话。如果有多个操作适用于指定的目标设备，请单击下拉箭头并从列表中选择适用的操作。

如果目标设备当前正在使用，而您的抢占级别等于或高于当前用户的抢占级别，则可以通过强制连接到设备进行访问。

RCS 还允许通过 PuTTY 等外部 Telnet 或 SSH 应用程序与串行 SIP 进行串行会话。Telnet 和 SSH 会话仅用于连接到串行 SIP，不得用于访问或管理 RCS 或 KVM 目标设备。

要从 Telnet 或 SSH 应用程序启动串行会话：

1 输入串行 SIP 所连接的 RCS 主机的 IP 地址。

2 输入 <RCS-用户名>：<串行-SIP-名称>，例如 jsmith:router。

3 输入 RCS 用户的密码。

注：Telnet 功能默认为禁用。要启用 Telnet 支持，请参阅第 69 页上的“配置串行会话”。

要从本地 UI 切换到活动会话（仅限本地用户）：

1 在侧面导航栏中，选择 **Local Session**。

2 选择 **Resume Active Session** 复选框。将出现视频查看器窗口。

扫描模式

在扫描模式中，交换机将扫描多台目标设备。扫描顺序是根据列表中目标设备排列的位置决定的。您还可以配置转到扫描序列中的下一台目标设备之前需等待的时间。

注：如果通过调制解调器进行连接，Scan 按钮将被禁用。

要将目标设备添加到扫描列表：

1 在侧面导航栏中，选择 **Unit View - Target List** 打开 Target List 画面。

2 选中您要扫描的目标设备旁边的复选框。

3 单击 **Scan**。

要配置扫描时间：

1 在侧面导航栏中，选择 **Ports - Local Port UI** 打开 Local Port UI Settings 画面。

2 在 Scan Mode 标题下的 Scan Time 字段中输入秒数 (3-255) 。

3 单击 **Save**。

查看系统信息

您可以在用户界面的以下画面中查看交换机和目标设备信息。

表 3.3：系统信息

类别	选择项：	查看内容：
RCS	*Unit View - RCS - Tools*	RCS 名称和类型，RCS 工具(维护、诊断、证书和陷阱 MIB)
	Unit View - RCS - Files	RCS 配置、用户数据库和目标设备
	Unit View - RCS - Properties - Identity	部件编号、序列号和 EID
	Unit View - RCS - Properties - Location	地点、部门和位置
	Unit View - RCS Settings - Versions	当前应用程序和引导程序版本
目标设备	*Unit View - Target List*	相连目标设备的列表，以及每台设备的名称、类型、状态和操作 单击一台目标设备可以查看以下额外信息：名称、类型、EID、可用会话选项以及连接路径。

RCS 工具

在 Tools - Maintenance - Overview 画面中，您可以查看装置名称和类型，也可以执行基本的装置任务。

重新启动 RCS

要重新启动 RCS：

1 在侧面导航栏中，选择 **Unit View - RCS - Tools - Maintenance - Overview** 打开 Unit Maintenance 画面。

2 单击 *Reboot*。

3 出现一个对话框，警告您将断开所有活动会话。单击 *OK*。

注：如果使用的是本地 UI，交换机重新启动时将出现空白画面。如果使用的是远程 OBWI，将显示一条消息提示您界面正在等待装置完成重新启动。

升级 RCS 固件

您可以将 RCS 更新到最新版本的固件。

在使用升级文件对闪存存储器进行重新编程后，本交换机将执行软重设，这将终止所有的 SIP 会话。在 SIP 进行固件更新时，目标设备可能不可见，也可能会显示为脱机状态。闪存更新完成后，目标设备将正常显示。

注意：在进行固件更新或重启目标电源期间断开 SIP 可能会使模块出现永久性故障，导致 SIP 必须退回工厂返修。

要升级交换机固件：

1 在侧面导航栏中，选择 *Unit View - RCS - Tools - Maintenance - Upgrade* 选项卡打开 Upgrade RCS Firmware 窗口。

2 单击 *Upgrade* 打开 Upgrade Appliance Firmware 画面。

3 选择以下方法之一加载固件文件：*Filesystem*、*TFTP*、*FTP* 或 *HTTP*。

注：Filesystem 选项仅在远程 OBWI 上可用。

4 如果选择了 Filesystem，选择 *Browse* 以指定固件升级文件的位置。

-或-

如果选择了 TFTP，输入服务器 IP 地址和要加载的固件文件。

-或-

如果选择了 FTP 或 HTTP，输入服务器 IP 地址和要加载的固件文件，以及用户名和密码。

5 单击 *Upgrade*。

保存和恢复 RCS 配置以及 RCS 用户数据库

您可以将交换机配置保存为文件。配置文件将含有受管理的装置的相关信息。您还可以保存交换机上的本地用户数据库。保存文件后，您也可以将之前保存的配置文件或本地用户数据库恢复到交换机。

要保存受管理装置的配置或用户数据：

1 在侧面导航栏中，单击 *Unit View - RCS - Files* 选项卡。

2 单击 *RCS Configuration* 选项卡或 *User Database* 选项卡，然后单击 *Save* 选项卡。

3 选择文件保存方式：**Filesystem**、**TFTP**、**FTP** 或 **HTTP PUT**。

4 如果选择了 TFTP，输入服务器 IP 地址和要加载的固件文件名。

-或-

如果选择了 FTP 或 HTTP，输入服务器 IP 地址、用户名、用户密码和要加载的固件文件名。

5 如果要给数据加密，下载前请输入加密密码。

6 单击 *Download*。将打开 Save As 对话框。

7 导航至所需位置，然后输入一个文件名。单击 **Save**。

要恢复受管理装置的配置或用户数据：

1 在侧面导航栏中，单击 *Unit View - RCS - Files* 选项卡。

2 单击 *RCS Configuration* 选项卡或 *User Database* 选项卡，然后单击 *Restore* 选项卡。

3 选择文件保存方式：**Filesystem**、**TFTP**、**FTP** 或 **HTTP**。

4 如果选择了 Filesystem，选择 *Browse* 以指定固件升级文件的位置。

-或-

如果选择了 TFTP，输入服务器 IP 地址和要加载的固件文件名。

-或-

如果选择了 FTP 或 HTTP，输入服务器 IP 地址、用户名、用户密码和要加载的固件文件名。

5 单击 **Browse**。导航至所需位置，然后选择文件名。单击 **Upload**。

6 如果原始文件已加密，请输入解密密码。

7 出现成功画面后，重新启动受管理的装置以启用恢复的配置。请参阅第 46 页上的“重新启动 RCS”。

要恢复失败的闪存升级：

如果进行闪存后，RCS 没有启动到新的固件版本，您可以采用以下步骤恢复到之前的固件版本。

1 将串行缆线连接到 RCS 背面板上的 SETUP 端口。

2 在连接到 Setup 端口的 PC 上运行终端程序。串行端口设置应该为：9600 波特、8 位数据位、1 位停止位、无奇偶校验和无流量控制。

3 启动 RCS。

4 在终端程序中，出现 Hit any key to stop autoboot 提示时按任意键。将显示一个菜单。

5 输入 <1>(启动备用) ，然后按 <Enter>。RCS 将自动重新启动到之前的固件版本。

6 RCS 重新启动后，您可以尝试进行闪存升级。

网络设置

注：只有交换机管理员才能更改网络对话框设置。其他用户只有查看权限。

在侧面导航栏中，单击 **Network** 显示 General、IPv4 和 IPv6 选项卡。

要配置一般网络设置：

1 单击 *Network* 选项卡，然后单击 **General** 选项卡以显示 RCS General Network Settings 画面。

2 从 LAN Speed 下拉菜单中选择以下选项之一：*Auto-Detect*、*10 Mbps Half Duplex*、*10 Mbps Full Duplex*、*100 Mbps Half Duplex*、*100 Mbps Full Duplex* 或 *1 Gbps Full Duplex*。

注：更改以太网模式后必须重新启动。

3 在 ICMP Ping Reply 下拉菜单中选择 *Enabled* 或 *Disabled*。

4 确认或修改 HTTP 或 HTTPS 端口。默认设置为 HTTP 80 和 HTTPS 443。

5 单击 *Save*。

要配置 IPv4 网络设置：

1 单击 **IPv4** 选项卡显示 IPv4 Settings 画面。

2 单击填充或清空 **Enable IPv4** 复选框。

3 在 Address、Subnet 和 Gateway 字段中输入所需信息。使用点标记格式 (xxx.xxx.xxx.xxx) 输入 IPv4 地址。

4 在 DHCP 下拉菜单中选择 *Enabled* 或 *Disabled*。

注：如果启用 DHCP，则您在 Address、Subnet 和 Gateway 字段中输入的任何信息都将被忽略。

5 单击 *Save*。

要配置 IPv6 网络设置：

1 单击 **IPv6** 选项卡显示 IPv6 Settings 画面。

2 单击填充或清空 **Enable IPv6** 复选框。

3 在 Address、Subnet 和 Prefix Length 字段中输入所需信息。使用十六进制标记格式 FD00:172:12:0:0:0:0:33 格式或其缩写格式 FD00:172:12::33 输入 IPv6 地址。

4 在 DHCP 下拉菜单中选择 *Enabled* 或 *Disabled*。

注：如果启用 DHCPv6，您在 Address、Gateway 和 Prefix length 字段中输入的任何信息都将被忽略。

5 单击 *Save*。

DNS 设置

您可以选择手动分配 DNS 服务器或使用通过 DHCP 或 DHCPv6 获得的地址。

要手动配置 DNS 设置：

1 在侧面导航栏中，选择 *DNS* 显示 RCS DNS Settings 画面。

2 选择 *Manual*、*DHCP*(如果启用 IPv4) 或 *DHCPv6*(如果启用 IPv6) 。

3 如果选择了 *Manual*，请在 Primary、Secondary 和 Tertiary 字段中输入 DNS 服务器编号。

4 单击 *Save*。

NTP 设置

交换机必须拥有访问当前时间的权限以检验证书是否过期。您可以配置交换机向 NTP 请求时间更新。请参阅第 5 章的"配置网络时间协议 (NTP) 设置"。

SNMP 设置

SNMP 是用于在网络管理应用程序和交换机之间传递管理信息的协议。其他 SNMP 管理器可以通过访问 MIB-II 与您的交换机进行通讯。打开 SNMP 画面后，OBWI 将从设备中检索 SNMP 参数。

在 SNMP 画面中，您可以输入系统信息和团体字符串。还可以指定哪些工作站可以管理交换机以及从该交换机接收 SNMP 陷阱。如果选择了 **Enable SNMP**，设备将通过 UDP 端口 161 响应 SNMP 请求。

要配置一般 SNMP 设置：

1 单击 **SNMP** 打开 SNMP 画面。

2 单击启用 **Enable SNMP** 复选框，使交换机可通过 UDP 端口 161 响应 SNMP 请求。

3 在 Name 字段中输入系统的完全限定域名，并在 Contact 字段中输入节点联系人。

4 输入 Read、Write 和 Trap 团体名称。这些名称指定的是在 SNMP 操作中必须使用的团体字符串。Read 和 Write 字符串仅适用于通过 UDP 端口 161 的 SNMP，并用作保障交换机访问安全的密码。这些值的长度最多为 64 个字符。这些字段不能保留空白。

5 在 Allowable Managers 字段中最多可键入 4 个允许管理此交换机的管理工作站的地址。或者，您可以保留这些字段为空以允许任何工作站都可以管理 RCS。

6 单击 **Save**。

审计事件设置

事件是交换机向管理工作站发送的通知，表示该交换机发生事件，需要引起进一步的注意。

要启用各个事件：

1 单击 **Auditing** 打开 Events 画面。

2 通过单击列表中事件所对应的复选框指定要生成通知的事件。

-或-

选择或清空 Event Name 旁边的复选框可选择或取消选择整个列表。

3 单击 **Save**。

设置事件目的地

您可以配置要发送到 SNMP 陷阱目的地和 Syslog 服务器的审计事件。在 Events 画面上启用的事件将被发送到 Event Destination 画面上列出的所有服务器。

1 单击 **Auditing** 和 **Destinations** 选项卡打开 Events Destinations 画面。

2 在 SNMP Trap Destination 字段中最多可键入 4 个管理工作站和 Syslog 服务器的地址，此交换机将向这些工作站和服务器发送事件。

3 单击 **Save**。

端口 — 配置 SIP

您可以通过交换机显示所连接的 SIP 列表以及有关每个 SIP 的以下信息：EID(电子识别号码) 、端口、状态、应用程序、界面类型和 USB 速度。您可以单击其中一个 SIP 查看以下附加信息：交换机类型、引导程序版本、应用程序版本、硬件版本、FPGA 版本、可用版本和升级状态。

还可以执行以下任务：删除脱机 SIP、升级 SIP 固件、设置 USB 速度或停用缆线。

要删除脱机 SIP：

1 在侧面导航栏中，单击 *Ports - SIPs* 打开 SIP 画面。

2 单击 *Delete Offline*。

升级 SIP

通过 SIP 的闪存升级功能，RCS 管理员可将 SIP 更新到最新版本的固件。使用交换机用户界面或 Avocent 管理软件可执行此更新操作。

在使用升级文件对闪存存储器进行重新编程后，本交换机将执行软重设，这将终止所有的 SIP 会话。SIP 进行固件更新时，目标设备可能会显示为脱机状态，也可能不会显示。闪存更新完成后，目标设备将正常显示。

如果 RCS 配置为自动升级 SIP，则更新交换机时将自动更新 SIP。要更新交换机固件，请参阅第 46 页上的“RCS 工具”或 Avocent 管理软件

联机帮助。如果在正常升级过程中出现问题，必要时还可能会强制升级 SIP。

注：请访问 http://www.dell.com 获取固件升级文件。

要更改 SIP 自动升级功能：

1 在侧面导航栏中，单击 *Ports - SIPs* 打开 SIP 画面。

2 选择要升级的 SIP 旁边的复选框，然后单击 *Enable Auto-Upgrade*。

注意：在进行固件更新或重启目标电源期间断开 SIP 可能会使模块出现永久性故障，导致 SIP 必须退回工厂返修。

要升级 SIP 固件：

1 在侧面导航栏中，*单击 Ports - SIPs* 打开 SIP 画面。

2 选择要修改的 SIP 旁边的复选框。

3 选择 *Choose an operation* 并选择 *Upgrade*。

4 如果设置正确，请单击 *Upgrade*。

要设置 USB 速度：

注：本部分仅适用于 USB2 SIP。

1 在侧面导航栏中，单击 *Ports - SIPs* 打开 SIP 画面。

2 选择要修改的 SIP 旁边的复选框。

3 选择 *Choose an operation* 并选择 *Set USB 1.1 Speed* 或 *Set USB 2.0 Speed*。

电源设备设置

注：您必须具备管理员权限才能更改电源控制设备设置。

注：有关支持的 PDU 列表，请访问 www.dellkvm.com。

在 RCS Power Devices 画面中，您可以查看所连接的电源设备列表以及有关每台电源设备的以下信息：名称、端口、状态、版本、型号、蜂鸣器、警报和温度。您也可以选择一台电源设备，然后选择 **Settings**

查看有关该电源设备的以下详细信息：名称、说明、状态、版本、插座、供应商名称、型号和输入馈电。

如果目标设备连接到电源控制设备插座，则可以打开、关闭或重启（关闭后再打开）目标设备的电源。

要打开、关闭或重启目标设备电源：

1 在侧面导航栏中，单击 *Ports - Power Devices* 打开 Power Devices 画面。

2 单击要配置的设备名称，然后选择 *Outlet List*。

3 选择要配置的插座左侧的复选框。

4 根据需要，单击 *On*、*Off* 或 *Cycle*。

要删除脱机电源设备：

1 在侧面导航栏中，单击 *Ports - Power Devices* 打开 Power Devices 画面。

2 单击 *Delete Offline*。

要更改最短打开时间、关闭时间或唤醒状态：

1 在侧面导航栏中，单击 *Ports - Power Devices* 打开 Power Devices 画面。

2 单击要配置的设备名称，然后选择 *Outlets*。

3 单击要修改的插座名称。

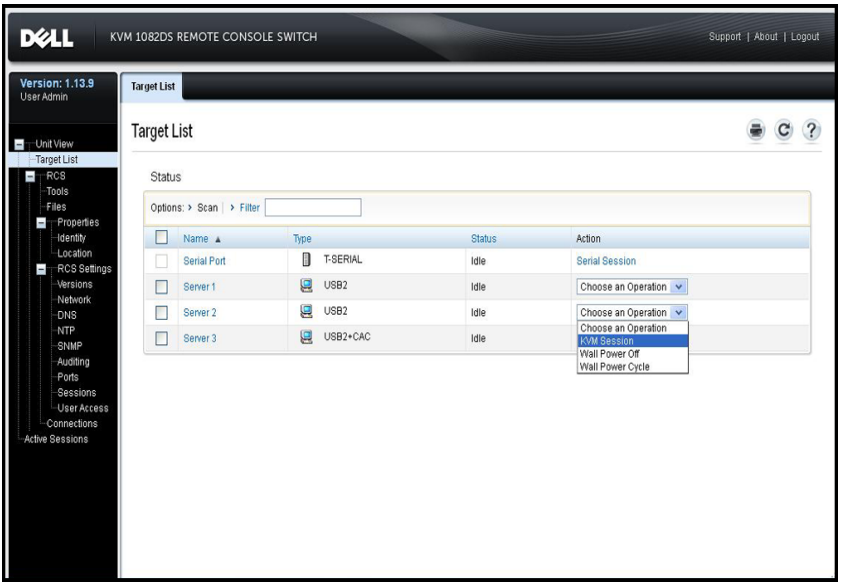
4 使用下拉窗口更改所需设置，然后单击 *Save*。

关联目标设备和电源插座

在 OBWI Target List 页面中，可为连接了插座的目标选择电源控制操作。选择 Ports - Power Devices 选项卡，然后单击一个设备名称将会显示 Device Settings、Device Firmware Upgrade 和 Outlet List 选项卡。单击 Outlet List 选项卡以显示与目标设备关联的插座。

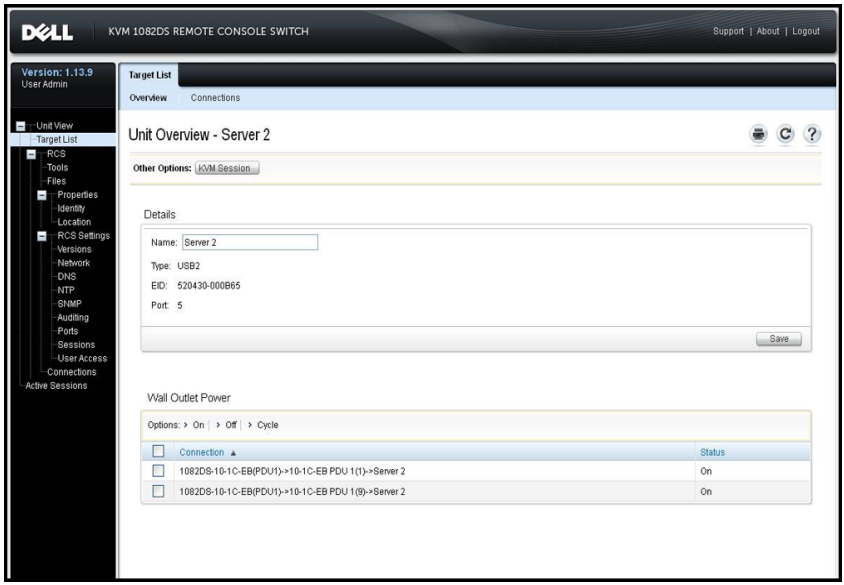
下图中，名为 Server2 的目标设备已连接电源插座。单击 Action 列中的下拉菜单箭头显示其他可用的电源操作。

图 3.2. Target List



下图中，Server2 的目标 Unit Overview 页面显示了 Wall Socket Power 列表，从中可以看出 PDU 1 的插座 1 和插座 9 连接至 Server2。

图 3.3. 目标概述 Server2



电源插座分组

插座可以与目标服务器进行关联以便于控制。要对插座(或关联到服务器的插座) 进行分组，要命名的首个设备必须使用 Manual name 字段。第二个以及后续设备必须使用 Link to Target Device 菜单，然后从下拉列表中选择首个设备的目标名称。

在 Target List 页面执行的电源操作适用于所有适用插座。在 Unit Overview 页面中可对指定目标设备的电源插座执行电源控制操作。下图中，名为 Group2 的目标设备包括 PDU 1 的插座 4 和插座 5。

要将插座 4 和 5 分为一组：

1 选择插座 4 以显示 *Power Devices Outlet Settings* 页面。

2 选择 *Manual* 并输入 Group2。

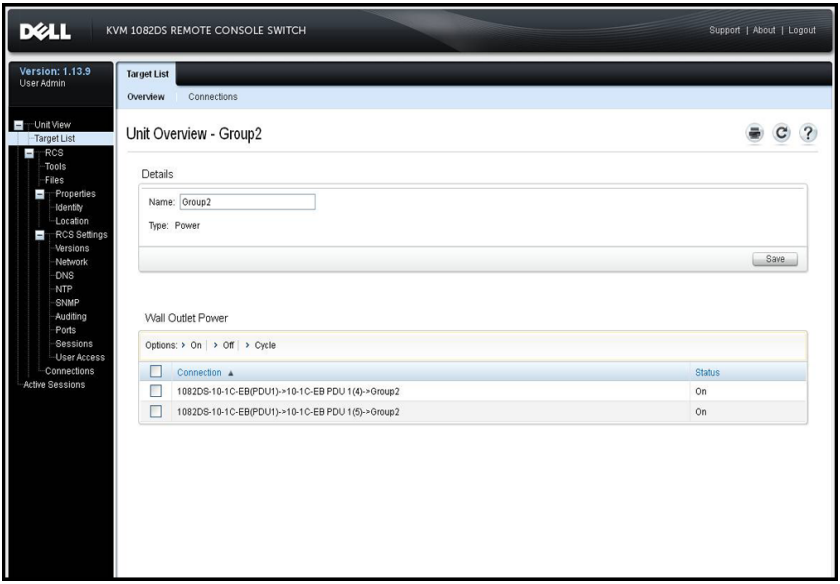
3 单击 *Save*。

4 选择插座 5 以显示 *Power Devices Outlet Settings* 页面。

5 选择 *Link to Target Device*，然后从下拉菜单中选择 *Group2*。

6 单击 *Save*。返回到 Outlet List 后，插座 4 和 5 将拥有相同的名称。

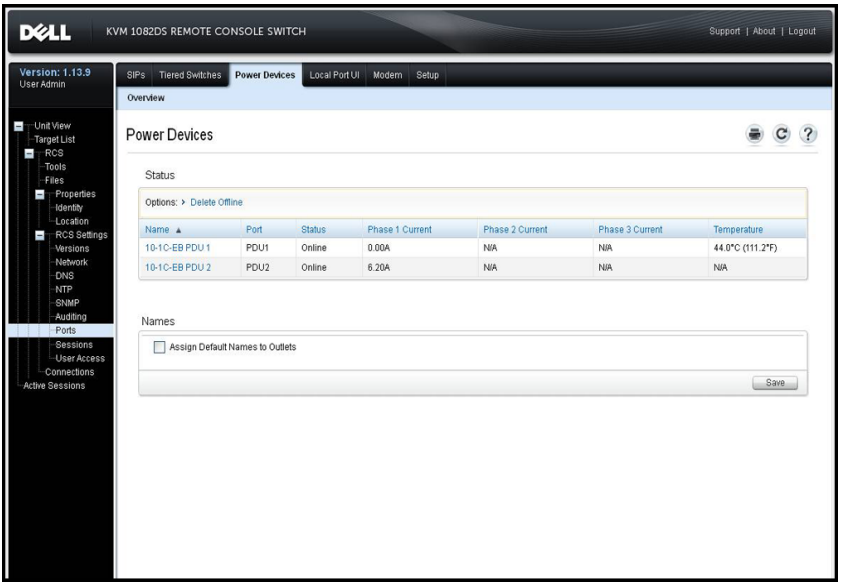
图 3.4. Group2 的目标设备概述



默认插座名称

在 Power Devices 页面中，复选框“Assign Default Names to Outlets”控制是否为电源设备的电源插座指定默认名称，如下图所示。只有带名称的电源插座才会列在 Target 页面中。清空“Assign Default Names to Sockets”复选框并保存后即可删除默认分配的电源插座名称。勾选“Assign Default Names to Outlets”并保存后即可为没有名称的电源插座分配默认名称。

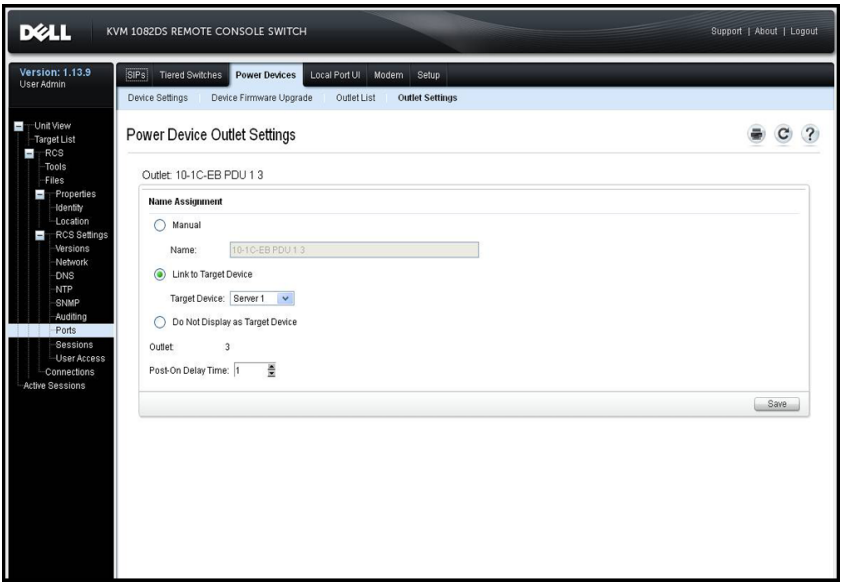
图 3.5. RCS Power Devices 页面



分配插座名称

在 Power Device Socket Settings 页面中，有三个选项可用于分配插座名称，如下图所示。这些选项为 Manual Name 分配、Link to Target Device 和 Do Not Display as Target Device。

图 3.6. Power Device Outlet Settings 页面



- Manual Name 分配选项可为插座指定唯一名称。该名称在所有 SIP 和电源插座名称中必须是唯一的。尝试手动指定非唯一的名称将会出错，并且该名称不会被保存。
- Link to Target Device 分配选项可将插座关联到另一个目标名称 (插座或 SIP) ，以便对命名的目标进行电源控制。插座连接到 SIP 目标设备名称后，通常该插座实际上会为与该 SIP 相连的服务器供电。
- Do Not Display as Target Device 选项可使插座名称留空，使其不会在 Target List 页面中显示。该选项可用于备用插座，以将其从 Target List 页面中删除。

访问控制继承

通过将电源插座关联到目标来更改其名称时，插座将继承为该目标名称配置的访问控制。添加 SIP 后，如果从 SIP 检索到的名称与现有目标的名称相符，则新的 SIP 将继承该目标设备的访问控制。重命名目

标设备后，该目标的所有 SIP 和插座都将被重命名，并且它们还将继承之前为旧的目标名称配置的访问控制。

重命名目标设备

在 Target List - Overview 页面中，可将设备的名称更改为任何唯一的目标名称。该名称在所有目标集合（包括 SIP 和电源插座）中必须唯一。重命名目标后，所有连接到该目标的插座也将被指定新的目标名称。

目标设备的优先级状态

在 Target List 页面中，关联了电源插座的目标可控制多个设备。目标所显示的状态值将被选作所有设备状态值中的最高优先级。下表列出了优先次序（从高到低）中可能的状态值和适用的目标设备类型。

表 3.4：目标状态值

状态值	适用于：		状态说明
	SIP	电源插座	
使用中	x	不适用	会话处于活动状态
路径已封锁	x	不适用	其他会话正在使用连接目标的路径
正在升级	x	不适用	SIP 正在升级
打开	不适用	x	已打开一个或多个插座
关闭	不适用	x	已关闭一个或多个插座
无电源	x	不适用	未检测到 SIP 上的电源
局部电源	不适用	x	目标的插座部分处于打开状态，部分处于关闭状态

状态值	适用于：		状态说明
	SIP	电源插座	
锁定关闭	不适用	x	已解锁一个或多个插座
关闭	不适用	x	已关闭一个或多个插座
锁定打开	不适用	x	已锁定一个或多个插座
空闲	x	不适用	无活动的会话；SIP 已加电
打开	不适用	x	插座已打开

当目标设备具有多个通过名称关联的电源插座并且它们的电源状态不统一时，RCS 可能会将锁定关闭的插座状态视为关闭，将锁定打开的插座状态视为打开。下表列出了两个插座状态值组合所产生状态值。

表 3.5：多个插座状态值和显示的状态

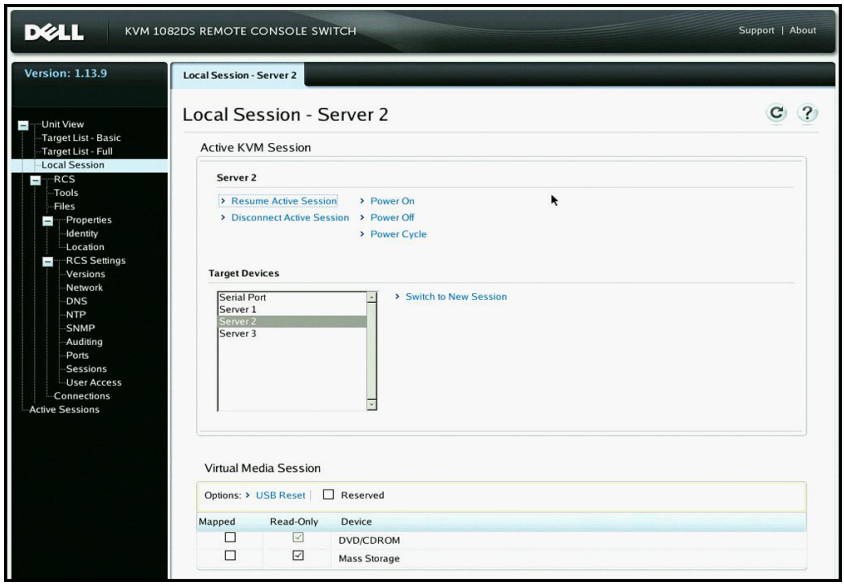
插座 1 状态	插座 2 状态	结果状态
关	关	关
关	开	局部电源
开	开	已加电
锁定打开	开	已加电
锁定打开	锁定打开	锁定打开
锁定打开	关	局部电源
锁定关闭	开	局部电源

插座 1 状态	插座 2 状态	结果状态
锁定关闭	锁定关闭	锁定关闭
锁定关闭	关	已断电
锁定打开	锁定关闭	局部电源

本地端口上的 Local Session 页面

在本地端口的 Local Session 页面上，当活动会话的目标具有关联的电源插座时，在页面的该活动会话下将显示三个电源控制。下图显示了名为 Server2 的目标的活动本地端口会话所显示的电源控制。

图 3.7. 带电源控制的 Local Session 页面



本地端口 UI 设置

要更改本地 UI 的调用方式：

1 在侧面导航栏中，选择 *Ports - Local Port UI* 打开 Local Port UI Settings 画面。

2 在 Invoke Local Port UI 标题下，单击列表中一个或多个方式旁边的复选框。

3 单击 *Save*。

您可以打开或关闭本地端口用户界面身份验证并选择一个用户访问级别。如果打开本地端口用户界面身份验证，您将需要登录才能使用界面。

您还可以选择本地端口的键盘语言、扫描模式时间、启用/禁用本地端口密码以及选择用户抢占级别。用户的抢占级别决定了他们是否能够断开另一用户与目标设备的串行或 KVM 会话。抢占级别分为 1 - 4 级别，4 为最高级别。例如，抢占级别为 4 的用户可以抢占其他级别为 4 及 1、2 或 3 级别的用户。

要更改本地端口用户身份验证（仅限管理员）：

1 在侧面导航栏中，选择 **Ports - Local Port UI** 打开 Local Port UI Settings 画面。

2 选择或取消选择 **Disable Local Port User Authentication** 复选框。

3 如果勾选 **Disable Local Port User Authentication**，在 User Access Level 下拉菜单中选择以下选项之一：**User**、**User Administrator** 或 **RCS Administrator**。

4 单击 **Save**。

调制解调器设置

通过 RCS Modem Settings 画面，您可以配置多个调制解调器的设置，并查看以下调制解调器设置：本地地址、远程地址、子网掩码和网

关。

有关将交换机连接到调制解调器的信息，请参阅第 23 页上的“连接 RCS 硬件”。

要配置调制解调器设置：

1 在侧面导航栏中，单击 **Ports - Modem** 打开 Modem Settings 画面。

2 启用或禁用 **Modem sessions can preempt digital sessions** 复选框。

3 选择 Authentication Timeout 时间（ 30 至 300 秒），和 Inactivity Timeout 时间（ 1 至 60 分钟）。

4 选择 **Save**。

设置端口安全设置

通过串行设置端口，您可以更改装置的网络配置、启用调试信息和对装置进行复位。

要启用密码以限制对串行设置端口的访问：

1 在侧面导航栏中，选择 *RCS Settings - Ports - Setup* 以显示 Setup Port Settings 页面。

2 单击以启用 *Enable Setup Port Security* 框。

3 输入并确认密码。

4 单击 *Save*。

会话

在 Active Sessions 画面中，您可以查看活动会话列表以及有关每个会话的以下信息：目标设备、所有者、远程主机、持续时间和类型。

配置一般会话

要配置常规会话设置：

1 在侧面导航栏中，选择 *Sessions - General*。将出现 General Session Settings 画面。

2 选择或取消选择 *Enable Inactivity Timeout* 复选框。

3 在 Inactivity Timeout 字段中，输入您希望会话关闭之前经过的不活动时间（1 至 90 分钟）。

4 在 Login Timeout 字段中，输入一个不活动时间（21 至 120 秒），在经过该时间后您必须重新登录。

5 选择或取消选择 Enable Preemption Timeout 复选框。

6 在 Preemption Timeout 字段中，输入通知您会话即将被抢占的提示的显示时间（1 至 120 秒）。

7 选择适用的会话共享选项（Enabled、Automati、Exclusive 或 Stealth）。

8 将 Input Control Timeout 选择为 1 至 50，其中 1 表示十分之一秒。

9 单击 **Save**。

配置 KVM 会话

要配置 KVM 会话设置：

1 在侧面导航栏中，选择 Sessions - KVM。将出现 KVM Session Settings 画面。

2 选择键盘和鼠标信号的加密等级（128 位 SSL (**ARCFOUR**)、DES、3DES 或 *AES*）以及视频信号的加密等级（128 位 SSL(**ARCFOUR**)、DES、3DES、**AES** 或 None）。

3 在 Keyboard 下拉菜单中选择语言。

4 如果您的硬件中包含了 USB2+CAC SIP，则选择视频分辨率。

5 单击 **Save**。

配置本地虚拟媒体会话

要设置虚拟媒体选项：

1 在侧面导航栏中，选择 **Sessions - Virtual Media** 打开 Virtual Media Session Settings 画面。

2 启用或禁用 *Virtual Media locked to KVM Sessions* 复选框。

3 启用或禁用 **Allow Reserved Sessions** 复选框。

4 在 Virtual Media Access Mode 的下拉菜单中选择以下选项之一：*Read-Only* 或 *Read-Write*。

5 选择要支持的加密级别之一。

6 单击 *Save*。

7 选择要启用虚拟媒体的每个 SIP 旁边的复选框，然后单击 *Enable VM*。

-或-

选择要禁用虚拟媒体的每个 SIP 旁边的复选框，然后单击 *Disable VM*。

虚拟媒体选项

您可以使用 Virtual Media Session Settings 画面中提供的选项决定交换机在虚拟媒体会话过程中的行为。表格 3.4 列出了可用于设置虚拟媒体会话的选项。

有关在 KVM 会话中使用虚拟媒体的信息，请参阅第 87 页上的“虚拟媒体”。

表 3.6：虚拟媒体会话设置

设置	说明
Session Settings:Virtual Media locked to KVM Session	该锁定选项指定虚拟媒体会话是否锁定到目标设备的 KVM 会话。若启用了锁定(默认设置) ，则当 KVM 会话关闭时，虚拟媒体会话也会关闭。若禁用锁定，则 KVM 会话关闭时，虚拟媒体会话仍保持活动状态。
Session Settings:Allow Reserved Sessions	确保只有用您的用户名才可访问某一虚拟媒体连接，其他用户不能建立到该目标设备的 KVM 连接。当相关联 KVM 会话断开时，取决于 Virtual Media 对话框中的 Locked 设置，虚拟媒体会话也可能会被断开。
Drive Mappings:Virtual Media Access Mode	您可以将映射的驱动器的访问模式设置为只读或读写。当访问模式为只读时，用户不能在客户端服务器的映射驱动器中写入数据。如果访问模式设为读写，则用户可以在映射驱动器中读写数据。如果映射驱动器设计为只读(例如 CD/DVD 驱动器、DVD-ROM 驱动器或 ISO 映像) ，那么所配置的读写访问模式将被忽略。当读写驱动器(如大容量存储设备或 USB 可移动媒体) 被映射时，如想防止用户写入数据，那么设置为只读模式会很有帮助。 可同时映射一个 DVD 驱动器和一个大容量存储设备。CD 驱动器、DVD 驱动器或 ISO 磁盘镜像文件将被映射为虚拟 CD/DVD 驱动器。
Encryption Level	您可以为虚拟媒体会话配置加密级别。包括：None(默认) 、128-bit SSL (ARCFOUR)、DES、3DES 和 AES。
Virtual Media Access per SIP：启用 VM/禁用 VM	Virtual Media Access per the SIP 部分列出了所有虚拟媒体 SIP。列表包含每根缆线的相关详细信息，包括启用或禁用每根缆线的虚拟媒体的选项。

本地用户

本地用户还可以在 Local Session 画面中确定虚拟媒体的行为。除了连接和断开虚拟媒体会话外，您可以配置下表中的设置。

表 3.7：本地虚拟媒体会话设置

设置	说明
CD ROM/ DVD ROM	允许与首个检测到的 CD-ROM 或 DVD-ROM(只读) 驱动器建立虚拟媒体会话。启用此复选框可以建立到目标设备的虚拟媒体 CD-ROM 或 DVD-ROM 连接。禁用此复选框可以终止到目标设备的虚拟媒体 CD-ROM 或 DVD-ROM 连接。
Mass Storage	允许与首个检测到的大容量存储驱动器建立虚拟媒体会话。启用此复选框可以建立到目标设备的虚拟媒体大容量存储驱动器连接。禁用此复选框可以终止到目标设备的虚拟媒体大容量存储驱动器连接。
Reserved	确保只有用您的用户名才可访问某一虚拟媒体连接，其他用户不能建立到该目标设备的 KVM 连接。

配置串行会话

要配置串行会话设置：

1 在侧面导航栏中，单击 *Sessions - Serial* 以显示 Serial Session Settings 画面。

2 启用或禁用 *Telnet Access Enabled* 复选框。

3 单击 **Save**。

设置用户帐户

管理本地帐户

交换机 OBWI 通过由管理员定义用户帐户来提供本地和登录的安全性。通过选择侧面导航栏中的 *User Accounts*，管理员可以添加和删除用

户、定义用户抢占和访问级别以及更改密码。

访问级别

添加用户帐户后，可将用户分配到下列任意一个访问级别：RCS Administrator、User Administrator 和 User。

表 3.8：各访问级别允许的操作

操作	RCS Admin	User Administrator	Users
配置界面系统级别设置	是	否	否
配置访问权限	是	是	否
添加、更改和删除用户帐户	是，适用于所有访问级别	是，仅适用于 User 和 User Administrator	否
更改您自己的密码	是	是	是
访问目标设备	是，所有目标设备	是，所有目标设备	是，如果允许

要添加新的用户帐户（仅限 User Administrator 或 RCS Administrator）：

1 在侧面导航栏中，选择 *User Accounts - Local User Accounts* 打开 Local User Accounts 画面。

2 单击 *Add* 按钮。

3 在空白处输入新用户的名称和密码。

4 选择新用户的访问级别。

5 选择任何您想要分配到用户帐户的可用目标设备，然后单击 **Add**。

注：User Administrator 和 RCS Administrator 可以访问所有目标设备。

6 单击 *Save*。

要删除用户帐户（仅限 User Administrator 或 RCS Administrator）：

1 在侧面导航栏中，选择 *User Accounts - Local Accounts* 打开 Local User Accounts 画面。

2 单击要删除的每个帐户左侧的复选框，然后单击 *Delete*。

要编辑用户帐户（仅限 Administrator 或活动用户）：

1 在侧面导航栏中，选择 *User Accounts - Local Accounts*。将显示 Local User Accounts 画面。

2 单击要编辑的用户名称。将出现用户资料。

3 在此画面中填写用户信息，然后单击 *Save*。

Avocent 管理软件设备 IP 地址

您可以通过指定 Avocent 管理软件服务器的 IP 地址来联系和注册未受管理的交换机。

要配置服务器 IP 地址：

1 在侧面导航栏中，选择 *User Accounts* - **Avocent**。将显示 Avocent Management Software Settings 画面。

2 输入您要联系的服务器 IP 地址。最多允许输入四个地址。

3 使用滚动条选择所需的重试时间间隔。

4 要取消关联已在服务器上注册的 RCS，请单击 **Disassociate** 按钮。

5 单击 *Save*。

LDAP

Dell 1082DS/2162DS/4322D RCS 可以通过本地数据库对用户进行身份验证和授权，也可使用支持 LDAP（轻型目录访问协议）的 Dell RCS 软件或 OBWI 通过外部可升级的分布式目录服务对用户进行身份验证和授权。有关在 RCS 上配置和使用 LDAP 的更多信息，请参阅 LDAP 部分。

超级管理员

如果发生网络故障，可以使用一个无需通过 LDAP 服务器的身份验证即可登录设备的帐户。请参阅第 5 章的“配置超级管理员帐户”。

活动会话

在 Active Sessions 画面中，您可以查看活动会话列表以及有关每个会话的以下信息：目标设备、所有者、远程主机、持续时间和类型。

关闭会话

要关闭会话：

1 在侧面导航栏中，选择 *Active Sessions* 以显示 RCS Active Sessions 画面。

2 单击所需目标设备旁边的复选框。

3 单击 *Disconnect*。

注：如果存在相关联的锁定虚拟媒体会话，则此会话也将被断开。

要关闭会话（仅限本地用户）：

1 **在侧面导航栏中，选择 Local Session。**

2 选择 **Disconnect Active Session** 复选框。

4

视频查看器窗口

视频查看器用于通过 OBWI 与连接到交换机的目标设备进行 KVM 会话。当使用视频查看器连接设备时，目标设备的桌面将显示在单独的窗口中，其中包括本地和目标设备光标。

交换机 OBWI 软件使用一个基于 Java 的程序来显示视频查看器窗口。首次打开时，交换机 OBWI 将自动下载并安装视频查看器。

注：需要安装 Java 1.6.0_11 或更高版本才能启动会话。

注：交换机 OBWI 不会安装 Java Resource Engine (JRE)。您可访问以下地址免费下载 JRE：http://www.sun.com。

注：交换机 OBWI 利用系统内存在视频查看器窗口中存储和显示图像。每个打开的视频查看器窗口都占用额外的系统内存。在客户端服务器中，若色彩设置为 8 位色，则每个视频查看器窗口将占用 1.4 MB 内存，若为 16 位色的设置，则占用 2.4 MB 内存，32 位色的设置则占用 6.8 MB 内存。如果尝试开启多于系统内存允许的视频查看器窗口数量(通常为四个) ，将会显示内存不足的错误信息，并且不会打开缩要求的视频查看器窗口。

如果您尝试访问的服务器当前正在被另一用户查看，而您的抢占级别等于或高于该用户的抢占级别，则系统将提示您抢占该用户。RCS Administrator 还可以通过 Active Session 页面断开活动用户的连接。有关更多信息，请参阅 RCS第 72 页上的“活动会话”。

图 4.1. 视频查看器窗口(正常窗口模式)

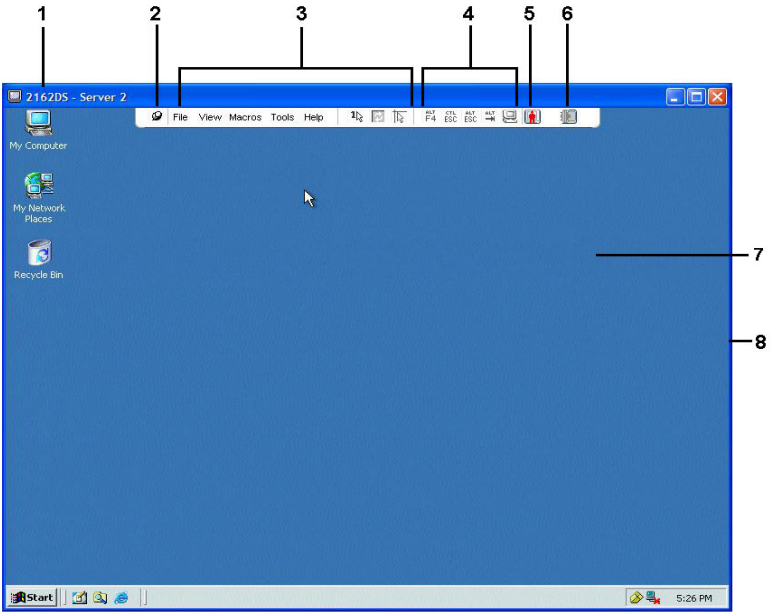


表 4.1：视频查看器说明

编号	说明
1	标题栏：显示被查看的目标设备的名称。在全屏模式下，标题栏会消失，目标设备的名称出现在菜单和工具栏之间。
2	图钉按钮：锁定菜单和工具栏的显示，以便始终显示。

编号	说明
3	菜单和工具栏：通过它可以使用视频查看器窗口的多项功能。如果没有使用图钉功能，菜单和工具栏将是显示/隐藏状态。将光标移到工具栏上，即可显示菜单和工具栏。工具栏上可以显示多达十种命令和/或宏组按钮。默认情况下，工具栏上会出现 Single Cursor Mode、Refresh、Automatic Video Adjust 和 Align Local Cursor 按钮。有关更多信息，请参阅第 75 页上的“更改工具栏”和第 93 页上的“宏”。
4	Macro 按钮：可发送至目标设备的常用键盘序列。
5	连接状态指示器：指示连接到此服务器 RCS 的用户状态。模式包括独占、基本主动连接、主用户活动共享、次级用户活动共享、被动共享、隐匿和扫描。
6	智能卡状态指示器：指示智能卡读卡器中有无智能卡。视频查看器画面智能卡图标变为灰色表示智能卡选项不可用或被禁用。如果智能卡已被映射，则该图标将变为绿色。
7	显示区域：访问服务器桌面。
8	框架：单击并按住框架，可调整视频查看器窗口的大小。

更改工具栏

您可以选择一段时间，当视频查看器窗口工具栏在显示/隐藏状态下（即未被图钉锁定在位置上时），经过该时间后工具栏会被隐藏。

要指定工具栏的隐藏时间：

1 在视频查看器窗口菜单中选择 Tools - Session Options。

-或-

单击 Session Options 按钮。

将会出现 Session Options 对话框。

2 单击 **Toolbar** 选项卡。

3 使用箭头键指定工具栏隐藏之前经过的秒数。

4 单击 OK 保存更改并关闭该对话框。

启动会话

注：当使用非代理连接时，通过较慢网络连接的视频传输效果可能会低于最佳情况。由于某些色彩设置(如灰度) 会比其他设置(如最佳颜色) 占用更少的网络带宽，因此改变色彩设置可提高视频性能。为在较慢的网络连接中获得最佳视频性能，请使用如灰度/最佳压缩或低色/高压缩的色彩设置。有关更多信息，请参阅第 77 页上的"调整视图"。

注：如果用户连接到的目标设备的屏幕分辨率高于本地计算机，视频查看器窗口将显示目标设备的部分屏幕，通过滚动条可查看屏幕的剩余部分。通过调整目标设备、本地计算机或两者的分辨率，用户可以查看整个屏幕。

要从交换机 Explorer 窗口启动 KVM 会话：

1 单击一台列于 Target List 画面中的设备，打开设备概览窗口。

2 单击 *KVM Session* 链接在新窗口中打开视频查看器。

会话超时

如果在指定时间内会话窗口中没有活动，此远程会话就会超时。会话超时值可以在 RCS KVM Session Settings 窗口中配置。指定的会话超时值将在下次访问交换机 OBWI 时使用。

要启用、禁用或配置会话超时：

1 在侧面菜单中，选择 *Unit View - RCS - RCS Settings - Sessions - General*。

2 在 *Enable Activity Timeout* 框中选择所需设置。

3 如有必要，选择不活动超时时间限制。

4 单击 *Save*。

窗口大小

注：如果视频查看器窗口处于全屏模式，或者对于共享会话的非主用户，View - Scaling 命令不可用。

首次使用交换机 OBWI 时，无论何时打开视频查看器窗口，其显示分辨率均为 1024 x 768，直到用户更改该值。可以将每个视频查看器窗口设置为不同的分辨率。

启用自动缩放后，若窗口大小在会话中发生变化，则交换机 OBWI 可自动调节视频查看器的显示。如果在会话中目标设备的分辨率在任何时候发生改变，该显示将会自动调节。

要更改视频查看器窗口的分辨率：

1 选择 *View - Scaling* 命令。

2 选择所需的分辨率。

调整视图

使用视频查看器窗口菜单或任务按钮可以：

- 校准鼠标光标。
- 刷新画面。
- 启用或禁用全屏模式。启用全屏模式后，图像将调整为适合桌面大小的尺寸（高达 1600 x 1200 或 1680 x 1050 [宽屏]）。如果桌面有更高的分辨率，则会出现以下情况：
  - 全屏图像在桌面居中，并且视频查看器窗口周围的区域为黑色。
  - 锁定菜单和工具，以便始终显示。
- 启用会话图像的全面、自动或手动缩放：
  - 如果选择全面缩放，则桌面窗口保持不变，设备的图像将根据窗口大小缩放。
  - 如果选择自动缩放，则桌面窗口将更改分辨率以匹配正在查看的目标设备的分辨率。
  - 如果选择手动缩放，则可显示一个图像缩放分辨率的下拉菜单。
- 更改会话图像的颜色深度。

要对齐鼠标光标：

单击视频查看器窗口工具栏上的 *Align Local Cursor* 按钮。本地光标应与远程设备的光标保持一致。

注：如果光标没有保持一致，请关闭所连接的设备的鼠标加速。

要刷新画面，在视频查看器窗口中单击 *Refresh Image* 按钮，或在视频查看器菜单选择 *View - Refresh*。此时，将完全重新生成数字化视频图像。

要启用全屏模式，单击 *Maximize* 按钮或在视频查看器窗口菜单中选择 *View - Full Screen*。桌面窗口将消失，只能看见被访问的设备桌面。屏幕最大将调整到 1600 x 1200 或 1680 x 1050(宽屏) 。如果桌面有更高的分辨率，那么在全屏图像的周围会有黑色的背景。会出现浮动的工具栏。

要禁用全屏模式，单击浮动工具栏上的 *Full Screen Mode* 按钮以返回到桌面窗口。

要启用全面缩放，在视频查看器窗口菜单中选择 *View - Scaling*，然后选择 **Full Scale**。设备图像会自动缩放到桌面窗口的分辨率。

要启用手动缩放，在视频查看器窗口菜单中选择 *View - Scaling*。选择尺寸以缩放窗口。可用的手动缩放尺寸会因您使用的系统而有所不同。

刷新图像

在 *Manual Video Adjust* 对话框中单击 Refresh Image 按钮以完全重新生成数字化视频图像。

注：您也可在视频查看器窗口菜单中选择 *View - Refresh* 来刷新图像。

视频设置

其他视频调整

通常，视频查看器窗口的自动调整功能可以对视频进行优化以获得最佳的图像效果。然而，用户可以在 Dell 技术支持部门的帮助下通过在视频查看器窗口菜单中选择 *Tools - Manual Video Adjust* 命令或单击 *Manual Video Adjust* 按钮对视频进行微调。这将显示 Manual Video Adjust 对话框。视频调试是针对每个目标设备的设置。

用户还可以通过观察对话框左下角处的数据包速率，以验证支持静态画面所需的每秒数据包速度级别。

要手工调试窗口的视频质量：

注：以下视频调整操作只能在 Dell 技术支持部门的帮助下进行。

1 在视频查看器窗口菜单中选择 *Tools - Manual Video Adjust*。

-或-

单击 *Manual Video Adjust* 按钮。

将出现 Manual Video Adjust 对话框。

图 4.2. Manual Video Adjust 对话框

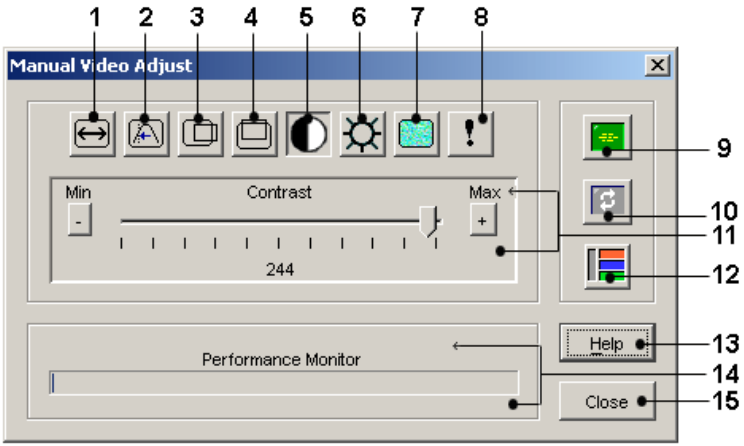


表 4.2：图 4.2 的说明

编号	说明	编号	说明
1	图像捕获宽度	9	自动视频调整
2	像素采样/微调	10	刷新图像
3	图像捕获水平位置	11	调整栏
4	图像捕获垂直位置	12	视频调试模式
5	对比度	13	帮助
6	亮度	14	性能监视器
7	噪声阈值	15	关闭按钮
8	优先级阈值		

2 单击与要调整的功能对应的图标。

3 移动 Contrast 滚动条，然后单击 *Min* (-) 或 *Max* (+) 按钮调整每个按下图标的参数。调整效果将立刻显示在视频查看器窗口。

4 完成后，单击 *Close* 退出 Manual Video Adjust 对话框。

目标视频设置

图像捕获宽度、像素采样/微调、图像捕获水平位置和图像捕获垂直位置的调试将影响到目标视频如何捕获和数字化。一般不会更改这些设置。

这些图像捕获参数通过“自动调试”功能自动更改。需要在目标视频上使用专门的图像以进行独立的精确调试。

自动视频调试

大多数情况下，您不需要改变默认的视频设置。系统会自动调节和应用优化的视频参数。当视频参数设置为在静态画面下无 (0) 视频数据包传输时，交换机 OBWI 的性能最佳。

您可以轻松地在 Manual Video Adjust 对话框中单击 *Auto Adjust Video* 按钮以将视频参数调整为理想设置。

注：您也可在视频查看器窗口菜单中选择 *Tools - Automatic Video Adjust* 或单击 *Automatic Video Adjust* 工具栏图标自动调整视频。

视频测试模式

在 Manual Video Adjust 对话框中单击 *Video Test Pattern* 按钮切换为在视频测试模式下显示。再次单击 *Video Test Pattern* 按钮将切换回正常的视频图像。

针对不同供应商的视频设置

视频设置根据制造商的不同而具有明显的差异。Dell 拥有一个包含各种显卡最优视频设置的在线数据库，尤其是针对 Sun 指定的显卡。该信息可从 Dell 网站的 Knowledge Base 或致电 Dell 技术支持部获得。

颜色设置

调整颜色深度

Dambrackas Video Compression® (DVC) 算法使用户能在远程会话窗口调整可视颜色的数量。您可以选择显示更多颜色以获得最佳保真度，或选择更少颜色以减少网络中的数据传输量。

可使用最佳可用颜色（更新较慢）、最佳压缩（更新最快）、最佳颜色和最佳压缩组合或灰度查看视频查看器窗口。

通过在远程会话窗口中选择 *View Color* 命令，您可以指定每个端口和通道的颜色深度。每个通道的这些设置会分别储存。

对比度和亮度

如果视频查看器窗口的图像太暗或太亮，可选择 *Tools - Automatic Video Adjust* 或单击 *Automatic Video Adjust* 按钮。在 Video Adjustments 对话框中也有此命令。大多数情况下，此命令可以校正视频问题。

当多次单击 *Automatic Video Adjust* 都不能将对比度和亮度设置到所需要的程度时，手工调整对比度和亮度可能会有帮助。增加亮度。在移动对比度前不要增加 10 个以上的增量。通常，对比度应该移动得非常少。

噪声设置

检测阈值

有些情况下，视频传送中的噪音会使数据包/秒的计数增大，这种现象可以从光标移动区域出现的小点变化看出。改变阈值可得到“更平静”的画面，并可改善光标的跟踪效果。

如果使用的是标准视频压缩，您可以修改 Noise Threshold 和 Priority Threshold。单击 *Auto Adjust Video* 可以恢复默认阈值。

注：将噪声阈值减至零将引起恒定的图像刷新，导致高的网络占用率和图像闪动。建议将噪声阈值设置为能维持系统有效运行的最高水平，而且使鼠标光标移开后，仍然能恢复像素颜色。

注：调整噪声阈值时，请使用滚动条进行大幅度的调整，使用滑块两端的加号 (+) 和减号 (-) 按钮进行微调。

有关更改颜色深度的信息，请参阅第 77 页上的“调整视图”。

鼠标设置

调整鼠标选项

视频查看器窗口鼠标选项影响光标类型、光标模式、缩放比例、校准和重新设置。鼠标设置是针对具体设备的，即对于每台设备可以进行不同的设置。

注：如果设备不支持断开和再连接鼠标的能力(几乎所有较新的 PC 都支持) ，鼠标将被禁用，设备必须重新启动。

光标类型

视频查看器窗口为本地鼠标光标提供了五种显示选择。也可选择无光标或默认光标。

在单光标模式中，视频查看器窗口的本地(第二个光标关闭，只有目标设备的鼠标指针是可见的。仅显示目标设备远程光标的移动。无需使用本地光标时，可使用单光标模式。

图 4.3. 显示本地和远程光标的视频查看器窗口

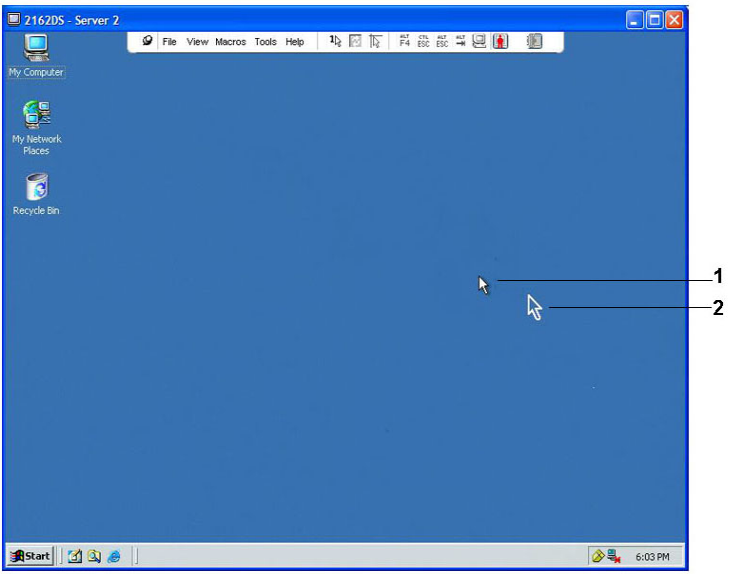


表 4.3：图 4.3 的说明

编号	说明
1	远程光标
2	本地光标

视频查看器窗口的标题栏显示了光标模式的状态，其中包括用于退出单光标模式的击键。您可以在 Session Options 对话框中定义退出单光标模式的击键。

注：当使用可以在击键到达客户端服务器之前将其捕捉的设备时，应该避免使用那些击键恢复鼠标指针。

要进入单光标模式，在视频查看器窗口菜单选择 *Tools - Single Cursor Mode* 或单击 *Single Cursor Mode* 按钮。本地光标不再显示，所有的光标移动都与目标设备相关。

要选择用于退出单光标模式的键：

1 在视频查看器窗口菜单中选择 *Tools - Session Options*。

-或-

单击 *Session Options* 按钮。

将会出现 Session Options 对话框。

2 单击 *Mouse* 选项卡。

3 在 Single Cursor 模式区域的下拉菜单中选择终止击键。

4 单击 *Save* 以保存设置。

启用单光标模式时，按此指定键可返回到常规桌面模式。

要退出单光标模式，在键盘上按标题栏指定的键。

要更改鼠标光标设置：

1 在视频查看器窗口菜单中选择 *Tools - Session Options*。

-或-

单击 *Session Options* 按钮。

将会出现 Session Options 对话框。

2 单击 *Mouse* 选项卡。

3 在 Local Cursor 区域选择一种鼠标光标的类型。

4 单击 *OK* 以保存设置。

鼠标缩放

某些早期版本的 Linux 不支持可调整的鼠标加速。对于必须使用这些早期版本的安装情况，您可以选择三个预设的鼠标缩放比例选项，或者设置自定义的缩放比例。预设设置为 Default (1:1)、High (2:1) 或 Low (1:2)：

- 按照 1:1 的缩放比例，鼠标在桌面窗口上的每次移动将向目标设备发送相同的鼠标移动信号。
- 按照 2:1 的缩放比例，相同的鼠标移动发送 2 倍的鼠标移动信号。
- 按照 1:2 的缩放比例，此值为 1/2 倍。

要设置鼠标缩放比例：

1 在视频查看器窗口菜单中选择 *Tools - Session Options*。

-或-

单击 *Session Options* 按钮。

将会出现 Session Options 对话框。

2 单击 *Mouse* 选项卡。

3 要使用其中一项预设设置，请勾选相应的单选按钮。

-或-

要设置自定义的缩放比例：

a. 单击 *Custom* 单选按钮以启用 X 和 Y 字段。

b. 在 X 和 Y 字段中键入一个缩放比例值。对于每个鼠标输入，鼠标移动被乘以相应的 X 和 Y 比例系数。有效输入范围为 0.25-3.00。

鼠标校准和同步

由于交换机 OBWI 不能从鼠标获得持续的反馈，因此交换机鼠标可能会与主机系统鼠标失去同步。如果鼠标或键盘不能再正常响应，您可以校准鼠标以再次建立正常的跟踪。

通过校准功能可使本地光标与远程目标设备的光标保持一致。通过复位功能可以模拟鼠标和键盘重新连接，就如同将其断开连接后再重新连接一样。

要重新校准光标，单击视频查看器窗口工具栏上的 *Align Local Cursor* 按钮。

虚拟媒体

客户端服务器的用户可通过虚拟媒体功能将本地物理驱动器映射为目标设备的虚拟驱动器。客户端服务器也可将 ISO 或软盘映像文件添加并映射为目标设备的虚拟驱动器。可同时映射一个 CD 驱动器和一个大容量存储器设备。

- CD/DVD 驱动器、磁盘映像文件（如 ISO 或软盘映像文件）将被映射为虚拟 CD/DVD-ROM 驱动器。
- 软盘驱动器、USB 存储设备或其他媒体类型则被映射为虚拟大容量存储设备。

有关使用 OBWI 配置虚拟媒体设置的信息，请参阅第 67 页上的“配置本地虚拟媒体会话”。

配置要求

目标设备必须支持虚拟媒体，并通过 USB2 或 USB2+CAC SIP 连接到 KVM 交换机。

目标设备自身必须可以使用要对其进行虚拟映射的 USB2 兼容媒体类型。即如果目标设备不支持便携式 USB 存储设备，那么就不可以在客户端服务器中将这种设备映射为目标设备的虚拟媒体驱动器。

用户（或用户所属的用户组）必须具有与目标设备建立虚拟媒体会话和/或保留的虚拟媒体会话的权限。请参阅第 69 页上的“设置用户帐户”。

每次仅能与目标设备进行一个活动的虚拟媒体会话。

共享与抢占的注意事项

KVM 和虚拟媒体会话是各自独立的，因此具有很多共享、保留或抢占会话的选项。Avocent 管理软件可以灵活地满足系统需求。

例如，可将 KVM 和虚拟媒体会话锁定在一起。在这种模式中，当 KVM 会话被断开时，与之相关联的虚拟媒体会话也被断开。如果会话没有锁定在一起，那么在 KVM 会话关闭时虚拟会话仍然处于活动

状态。当用户使用虚拟媒体会话执行一项高强度任务(例如加载操作系统) ，并且要在操作系统加载的过程中与不同的目标设备建立 KVM 会话以执行其他功能时，此功能很有必要。

若目标设备进行活动虚拟媒体会话而没有相关联的活动 KVM 会话，则会发生两种情况：原始用户(用户 A) 可重新连接或其他用户(用户 B) 可连接到该通道。您可以在“虚拟媒体”对话框中设置一个选项(已保留) ，仅允许用户 A 通过 KVM 会话访问该通道。

如果用户 B 可以访问该会话(未启用“已保留”选项) ，则用户 B 可以控制正用于虚拟媒体会话中的媒体。通过在堆叠环境中使用“已保留”选项，仅用户 A 可以访问下级交换机，在上级交换机和下级交换机之间的 KVM 通道将保留给用户 A。

Virtual Media 对话框

通过 Virtual Media 对话框，您可以映射和取消映射虚拟媒体。此对话框显示了客户端服务器中所有可被映射为虚拟驱动器的物理驱动器。您还可以添加 ISO 和软盘映像文件，然后通过 Virtual Media 对话框将其映射。

设备在映射后，Virtual Media 对话框的 Details 视图将显示自设备被映射以来传输的数据量和映射的时间。

您可以将该虚拟媒体会话指定为已保留。如果会话被保留，而且相关 KVM 会话将被关闭，另一用户不能够与该目标设备进行 KVM 会话。如果会话未被保留，则可以打开另一个 KVM 会话。

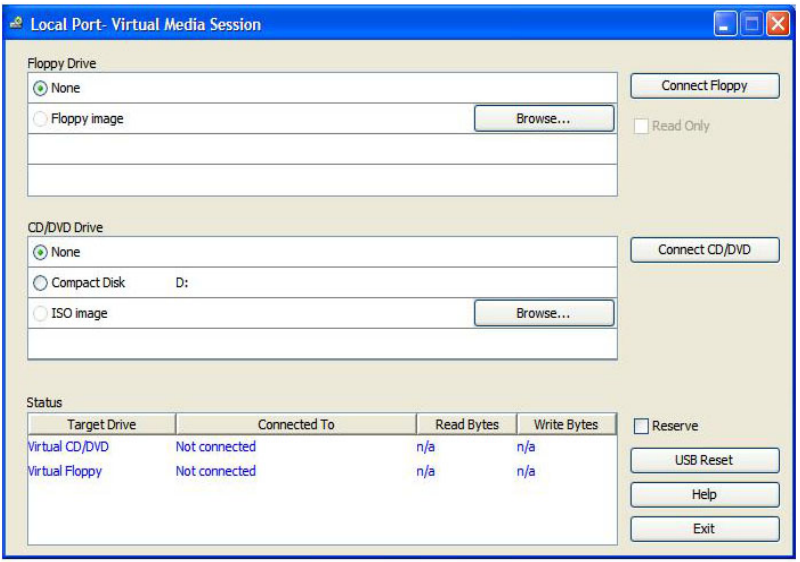
在 Virtual Media 对话框中也可复位 SIP。此操作将复位目标设备上所有形式的 USB 媒体，所以应当谨慎使用，并只在目标设备无响应时使用。

打开虚拟媒体会话

要启动虚拟媒体会话：

在视频查看器菜单中，选择 *Tools - Virtual Media*。将会出现 Virtual Media 对话框。要将该会话设置为已保留的会话，请单击 *Details*，然后选择 *Reserved* 复选框。

图 4.4. 视频查看器 Virtual Media 对话框



要映射虚拟媒体驱动器：

1 在视频查看器菜单中，选择 *Tools - Virtual Media* 打开虚拟媒体会话。

2 要将物理驱动器映射为虚拟媒体驱动器：

a. 在 Virtual Media 对话框中，单击要映射的驱动器旁边的 *Mapped* 复选框。

b. 如果需要将映射驱动器限制为只读访问，请单击驱动器旁边的 *Read Only* 复选框。如果虚拟媒体会话设置已被预先设置为所有映射驱动器必须为只读模式，那么该复选框已经启用并且不能更改。

如果会话设置启用了读写访问模式，而您需要将某一驱动器限制为只读访问，那么可以启用 *Read Only* 复选框。

3 要将 ISO 或软盘映像添加并映射为虚拟媒体驱动器：

a. 在 Virtual Media 对话框中，单击 *Add Image*。

b. 将会出现通用文件对话框，显示含有磁盘映像文件（也即后缀名为 .iso 或 .img 的文件）的目录。选择所需的 ISO 或软盘映像文件，单击 *Open*。

-或-

如果客户端服务器的操作系统支持拖放功能，在通用文件对话框中选择所需的 ISO 或软盘映像文件，并拖到 Virtual Media 对话框中。

c. 将对文件头进行检验以确保正确。如果正确，通用文件对话框将关闭，被选中的映像文件会出现在 Virtual Media 对话框中，单击其中的 *Mapped* 复选框可映射该文件。

d. 重复 a 到 c 步骤可继续添加所需的 ISO 或软盘映像文件。您可以添加任意数量的映像文件（受内存容量的限制），但一次仅能映射一个虚拟 CD 或 DVD 或者虚拟大容量存储器。

若试图映射多个驱动器（一个 CD 或 DVD 和一个大容量存储设备）或多个特定驱动器（多个 CD 或 DVD 或大容量存储设备），将会显示提示消息。若需要映射一个新的驱动器，则须先取消映射已有的映射驱动器，然后映射新的驱动器。

物理驱动器或映像被映射后，可在目标设备上使用。

要取消映射虚拟媒体驱动器：

1 在 Virtual Media 对话框中，取消勾选要取消映射的驱动器旁边的 *Mapped* 复选框。

2 系统提示要求确认。请确认或取消该操作。

3 重复操作取消映射其他虚拟媒体驱动器。

要显示虚拟媒体驱动器的详细信息：

在 Virtual Media 对话框中，单击 *Details*。对话框将会展开为显示 Details 表格。每行表示：

- Target Drive — 映射驱动器的名称，如“Virtual CD 1”或“Virtual CD 2”。
- Mapped to — 与 Client View 的 Drive 列中的 Drive 信息相同。
- Read Bytes 和 Write Bytes — 自开始映射起已传送的数据量。
- Duration — 自驱动器开始映射起已用的时间。

要关闭 Details 视图，请再次单击 *Details*。

要复位目标设备上所有的 USB 设备：

注：USB 复位功能将复位目标设备上的每个 USB 设备，包含鼠标和键盘。该功能应仅当目标设备停止响应时使用。

1 在 Virtual Media 对话框中，单击 *Details*。

2 将会出现 Details 视图。单击 *USB Reset*。

3 出现一则警告消息，提示复位可能导致的影响。请确认或取消复位。

4 要关闭 Details 视图，请再次单击 *Details*。

关闭虚拟媒体会话

要关闭 Virtual Media 对话框：

1 单击 *Exit*。

2 如果系统有任何映射驱动器，将显示消息提示驱动器将被取消映射。请确认或取消此操作。

如果用户尝试断开与锁定的虚拟媒体会话相关联的虚拟媒体会话或活动 KVM 会话，将显示确认消息，提示将丢失所有虚拟媒体映射。

智能卡

您可以将智能卡读卡器连接到客户端服务器上可用的 USB 端口，并在交换机系统上访问所连接的目标设备。然后启动 KVM 会话以打开视频查看器并映射智能卡。

注：对于所有智能卡读卡器，您必须使用 Dell USB2+CAC SIP 或 Avocent VMC IQ 模块。

视频查看器工具条最右侧的智能卡图标显示了智能卡状态。下表对智能卡状态图标进行了说明。

表 4.4：智能卡图标

图标	说明
	智能卡读卡器中无智能卡，或智能卡读卡器未连接。
	智能卡读卡器中有智能卡，但尚未被映射。
	智能卡已被映射（绿色图标）。

要映射智能卡：

1 打开 KVM 会话以显示视频查看器窗口菜单。

2 将智能卡插入与客户端服务器相连的智能卡读卡器。

3 在视频查看器窗口菜单中，单击 *Tools - Map Smart Card*。

4 如果没有将任何智能卡映射到目标设备，则 No Card Mapped 选项旁边将会有一个点。在此选项下的列表中选择智能卡，以映射智能卡。

要取消映射智能卡，单击视频查看器窗口菜单上的 *X* 关闭 KVM 会话，选择 *Tools - No Card Mapped*，然后从智能卡读卡器上取下智能卡或从客户端服务器上取下智能卡读卡器。

键盘传递

使用视频查看器窗口时用户输入的击键可能有两种解释方式，这取决于视频查看器窗口的屏幕模式。

- 如果视频查看器窗口处于全屏模式，所有击键和键盘组合（除 *Ctrl-Alt-Del* 外）都将被传送至正在查看的远程目标设备。

- 如果视频查看器窗口是处于常规桌面模式，您可以通过键盘传递模式控制远程目标设备或本地计算机是否可以识别某些击键或击键组合。

必须使用 Session Options 对话框指定键盘传递。启用键盘传递且视频查看器窗口处于活动状态时，键盘传递功能会将所有击键和击键组合（除 *Ctrl-Alt-Del* 外）传送给正在查看的远程目标设备。当本地桌面处于活动状态时，用户输入的击键和击键组合将会对本地计算机起作用。

注：Ctrl-Alt-Del 键盘组合仅能通过宏传送至远程目标设备。

注：日本键盘的 ALT-Han/Zen 击键组合将始终被传递到远程目标设备，无论屏幕模式或键盘传递模式的设置如何。

要指定键盘传递：

1 在视频查看器窗口菜单中选择 *Tools - Session Options*。

-或-

单击 *Session Options* 按钮。

将会出现 Session Options 对话框。

2 单击 *General* 选项卡。

3 选择 *Pass-through all keystrokes in regular window mode*。

4 单击 *OK* 保存设置。

宏

交换机 OBWI 预配置了适用于 Windows、Linux 和 Sun 平台的宏。

要发送宏，在视频查看器窗口菜单中选择 *Macros - <所需的宏>*，或在视频查看器菜单的可用按钮中选择所需的宏。

保存视图

您可以将视频查看器的显示画面保存为文件，或者保存在剪贴板中以便粘贴到文字处理器或其他程序中。

要将视频查看器窗口捕获至文件：

1 在视频查看器窗口菜单中选择 *File - Capture to File*。

-或-

单击 *Capture to Clipboard* 按钮。

将会出现 Save As 对话框。

2 输入文件名，并选择保存此文件的位置。

3 单击 *Save* 以将此画面保存至文件。

要将视频查看器窗口捕获至剪贴板，在视频查看器窗口菜单中选择 *File - Capture to Clipboard*，或单击 *Capture to Clipboard* 按钮。图像数据将保存至剪贴板。

关闭会话

要关闭视频查看器窗口会话：

在视频查看器窗口中选择 *File - Exit*。

5

RCS 的 LDAP 功能

LDAP 是一种用于通过 TCP/IP 访问和更新目录的协议标准。Dell RCS 软件和 OBWI 同时支持 Standard 架构和 Dell Extended 架构，并提供包括身份验证、私密性和完整性在内的强大安全特性。

注：Windows 2008 Server 要求在 IPv6 模式下使用 LDAP。

注：在 Microsoft Windows® 2000 和 Windows Server 2003 操作系统上支持使用 Microsoft Active Directory 来识别 RCS 用户。

Active Directory 结构

Active Directory (AD) 部署由包含对象分层结构的分布式数据库组成。每个对象与一个对象类关联，该对象类决定在该对象中可存储何种类型的数据。该分层结构从代表 AD 域的对象开始，展开后即形成由域名组成的分层结构，此分层结构可以采用与通常用于描述 DNS 名称空间的树状图相同的方式代表。Dell RCS 设计用于支持采用浅或深分层名称结构的单个域树。

域控制器计算机

与域分层结构相关联的是相应的域控制器计算机分层结构，LDAP 服务就是由这些计算机中的 AD 提供。每个域可能拥有多个对等的域控制器，而且可能分布于多个地理位置。Dell RCS 系列产品设计用于同时支持 AD 这些方面的特性。Dell RCS 采用 DNS 来确定每个域控制器的网络坐标，以便从容应对网络上出现某些域控制器不可用的情况。为达到此目的，采用了 DNS SRV 记录，因此根据在 SRV 记录中配置的管理设置，Dell RCS 总是首先尝试联系位置最接近的替代域控制器。

对象类

在每个域中，有另一个对象分层结构，该分层结构设计用于存储关于各种实体和实体组的信息。此类实体在 AD 中由用于定义“容器”的对象类代表，容器有助于组织对象组。其他对象类代表诸如网络用户、计算机、打印机或网络服务等实体。应特别注意两种类型的容器对象类：组和组织单元 (OU)。这两种对象类使 AD 管理员能够定义实体组，从而简化访问控制和其他管理策略的应用。例如，某个域可能配置有一个名为“工程”的 OU 容器，该容器包含多个根据功能命名的群组对象，如“硬件”、“软件”和“支持”；每个组配置有包含用户对象（或许还包括计算机对象）的成员列表。但是，可以通过嵌套组配置另一个分层结构；将一个组对象的名称放入另一个组对象的成员中就形成了嵌套。这里应该注意的是，每个 AD 组对象拥有一个与之关联的范围，该范围用于配置该组被允许与其他组所形成的嵌套关系的类型；例如，如果将范围设置为“通用”，则该组可能参与跨域嵌套，但是当范围设置为“本地”时，则该组可能无法参与此类嵌套。可在 Microsoft 提供的 AD 产品文档中查阅有关嵌套的规则。Dell RCS 系列产品设计用于支持为 AD 定义的所有嵌套规则。

属性

AD 中还使用另一个分层结构。与每个对象类关联的是一组“属性”，属性用于存储与所代表的实体有关的特定信息。例如，与用户对象类关联的是名为 SAM ACCOUNT NAME 的属性类型以及名为 FIRST NAME、SURNAME、PASSWORD 等的其他属性类型。Dell 远程控制台交换机系列产品使用 SAM ACCOUNT 和PASSWORD 属性对用户（这两种属性的正式 AD 名称分别为 sAMAccountName 和unicodePWD）进行身份验证。

架构扩展

AD 附带许多对象类，其中包括计算机和用户对象默认容器、组织单元容器类和代表计算机和用户实体的类。可以将 AD 扩展为包括一些新的对象类，如 Dell 提供用于简化访问控制管理的新对象类；此等扩展通常被称为“架构扩展”，并且是本文档所介绍的 Dell Extended 架构特性的核心部分。这些架构扩展提供自定义的对象类来代表 Dell

RCS、访问控制信息、以及一种用于将特定访问控制信息与 Dell RCS 和用户特定实例关联的容器类型。应特别注意 AD 中使用的每个属性类型和对象类必须拥有一个称之为对象标识符 (OID) 的全球唯一标识符。这些唯一标识符最终由国际认可的管理机构管理。其次，对于 AD，OID 空间由 Microsoft 管理。Dell 已经获取了在 Dell Extended 架构特性中使用的自定义对象类和属性类型的 OID 空间。以下是 Dell 所获取的 OID 概要：

Dell 扩展为：dell

Dell base OID 为：1.2.840.113556.1.8000.1280

RCS LinkID 范围为：12070 到 12079

Dell RCS 系列产品还设计为仅使用 AD 附带类中的对象类工作；此选项被称为 Standard 架构。在此选项中，计算机对象类用于代表 Dell RCS，标准群组对象用于将特定访问控制信息与 Dell RCS 和用户的特定实例相关联。在这种情况下，访问控制信息被存储在群组对象中特定的属性类型中。

AD 中的分层结构会使您访问目录对象中所存储信息的能力复杂化。为了避免与分层结构体系导航相关的潜在延迟，Dell 远程控制台交换机系列产品设计为使用被称为全局目录 (GC) 的 AD 特性。GC 通过提供对存储于完整 AD 数据库中数据的子集的访问，以及将所有的分层结构体系和地理分布“折叠”成一个相对扁平的结构来提供“快速查找”服务。GC 的查询使用与完整 AD 数据库所用的相同 LDAP 目录查询来完成。在一个企业，AD 产品还至少需要配置一台域控制器以提供 GC 服务，但是在实际 AD 运用中可以配置任何或全部的域控制器以提供 GC 服务。Dell RCS 系列产品使用 DNS 确定每个 GC 服务器的网络坐标，以便 Dell RCS 能够正确处理网络上有些 GC 服务器不可用的情况。为达到此目的，采用了 DNS SRV 记录，因此根据在 SRV 记录中配置的管理设置，Dell RCS 总是首先尝试联系位置“最接近”的替代 GC 服务器。

Standard 架构与 Dell Extended 架构对比

为了在众多客户环境中提供强大的灵活性，Dell 提供一组可以由用户根据所需结果进行配置的对象。Dell 已将该架构扩展以包括关联、设备和权限对象。关联对象用于将具有特定权限的用户或组与一个或多个 SIP 连接起来。设备对象定义 Active Directory 结构中的单个 RCS，且权限对象通过关联对象与设备对象连接以分配使用许可。

此模式为管理员提供了对不同的用户、权限和远程控制台交换机上的 SIP 组合的最大灵活性而不会添加太多的复杂性。

在安装 Dell 架构扩展前，管理员应该仔细阅读本章的介绍和说明以决定哪个架构适用于其特定安装。更改架构对象将会导致它在整个 Active Directory 内应用，因此创建后无法删除。仅可将其禁用。由于这个原因，所以在更改架构前应该仔细权衡其益处。

安装 Dell 架构扩展的主要益处就是消除了混淆。使用标准 Active Directory 架构时，远程控制台交换机与计算机设备对象的匹配最为严密，而且配置成一个整体。由于 RCS 不是计算机，所以不会应用全部的架构功能。在正确配置以这种方式指定的 RCS 时应格外小心。

此外，使用 Dell 架构扩展更易于搜索和识别交换机设备。使用计算机设备对象配置的交换机将随着 Active Directory 结构内的每台计算机设备一起进行搜索。

使用任何一种架构，RCS 均可同样地进行身份验证，而且使用任何一种方法均不会丧失任何功能。管理员可自由选择适用于其安装环境的任何一种方法。已经为使用和不使用 Dell 架构扩展的安装提供了说明。仅适用于一个架构配置的章节和说明均已做出标记，在不使用它们的安装环境中可将其忽略。

标准安装

在 Dell RCS 可以使用 Active Directory 进行身份验证之前，必须：

1 配置 Override Admin 帐户

2 配置 DNS 设置

3 设置网络时间协议

4 配置身份验证参数

5 配置群组对象

6 创建并下载 CA 根证书

7 设置登录超时

配置 Override Admin 帐户

如果发生网络故障，可以使用一个无需通过 LDAP 服务器的身份验证即可登录设备的帐户。在配置其他设置前，应该配置此帐户。要在板载 web 界面中配置超级管理员帐户：

1 单击 *User Accounts*，然后单击 *Override Admin*。

2 输入您要分配给用户的用户名和密码，然后在 Verify Password 字段中输入密码进行确认。

3 单击 **Save**。

注：您必须以管理员身份登录才能使用此选项。

配置 DNS 设置

必须至少指定一个 DNS 服务器，LDAP 客户端才可以解析名称。

Network 子类别显示 RCS 的名称并允许您更改网络设置，包括 IP 地址、子网掩码、网关、LAN 速度和 DHCP/BootP 设置。所显示的 RCS 名称将与 SNMP 类 System Name 字段中指定的名称相同。

Network 子类别允许最多输入和维护 3 个 DNS 服务器。这些 DNS 服务器用于解析 LDAP 身份验证面板上所提供的 DNS 名称。

注：必须至少配置一台 DNS 服务器才能让 LDAP 功能起作用。主服务器不可用时，RCS 软件将根据此处的配置自动进行故障转移以备份 DNS 服务器。

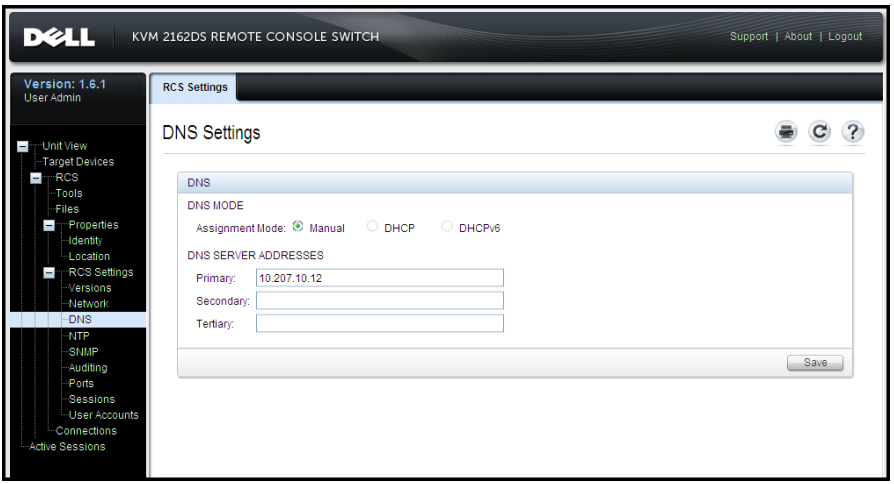
注：您可以使用 RCS 的串行管理界面配置 DNS 服务器地址。有关使用串行管理界面的信息，请查阅 RCS 说明文档。

要在板载 web 界面中配置 DNS 设置：

1 单击 *DNS* 打开 DNS Settings 画面。

2 指定 DNS 模式，输入服务器地址，然后单击 **Save**。

图 5.1. OBWI - DNS 设置



配置网络时间协议 (NTP) 设置

交换机必须拥有访问当前时间的权限以检验证书是否过期。您可以配置交换机向 NTP 请求时间更新。要在板载 web 界面中配置 NTP 设置：

1 单击 *NTP* 打开 NTP 画面。

2 单击 **Enable NTP** 框。

3 在所提供的框内输入网络时间源名称。您还可以设置以小时计的时间间隔以指定请求时间更新的频率。如果时间间隔设置为 0，则只会在 RCS 启动期间或更改 Global - NTP 菜单时发出请求。

4 单击 Save。

配置 LDAP 身份验证参数

通过身份验证面板，RCS 管理员可以配置访问 LDAP 目录服务所需的参数。 当接收到用户的访问请求时，RCS 可使用 LDAP 协议发送用户名、密码和其他信息到目录服务，以确定用户拥有哪些授权许可。

注：确立 LDAP 配置的术语是 KVM User、KVM User Admin 和 KVM Appliance Admin，分别对应 User、User Administrator 和 RCS Administrator。 访问级别未更改，但根据指示使用新的术语。

启用 LDAP 身份验证

通过 LDAP Configuration Options 画面上的 Operational Modes 部分，您可以选择用于用户身份验证的 LDAP 服务的正确类型。 可用模式有：

- Standard LDAP 目录服务(非 Microsoft)
- Microsoft Active Directory 服务
- 禁用 LDAP 身份验证

如果选择使用其他身份验证方法(非 LDAP) ，则 LDAP 身份验证将被自动禁用。 要使用 LDAP 目录服务，需要取消选择这个方法。

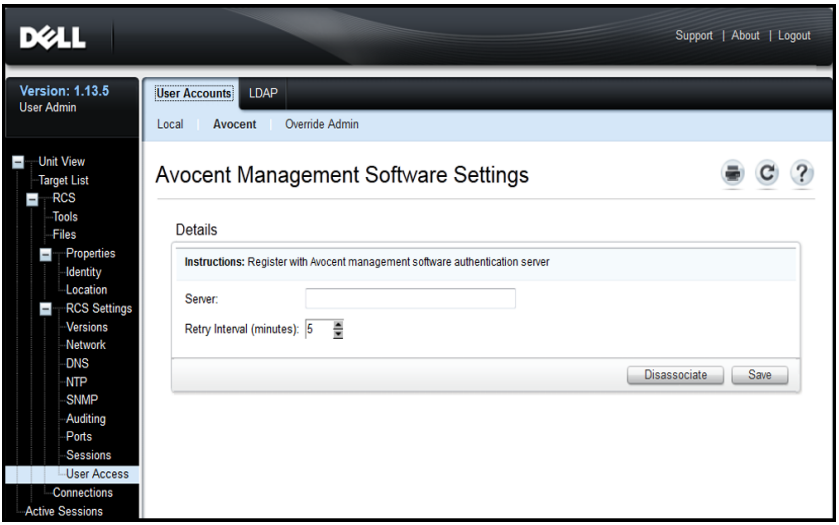
要恢复使用 LDAP 身份验证的功能：

1 在 User Access 下，选择 *Avocent* 选项卡，请参阅图 5.2。

2 单击 *Disassociate* 取消选择使用 Avocent 管理身份验证服务器。

3 单击 *Save*。

图 5.2. Avocent 身份验证画面

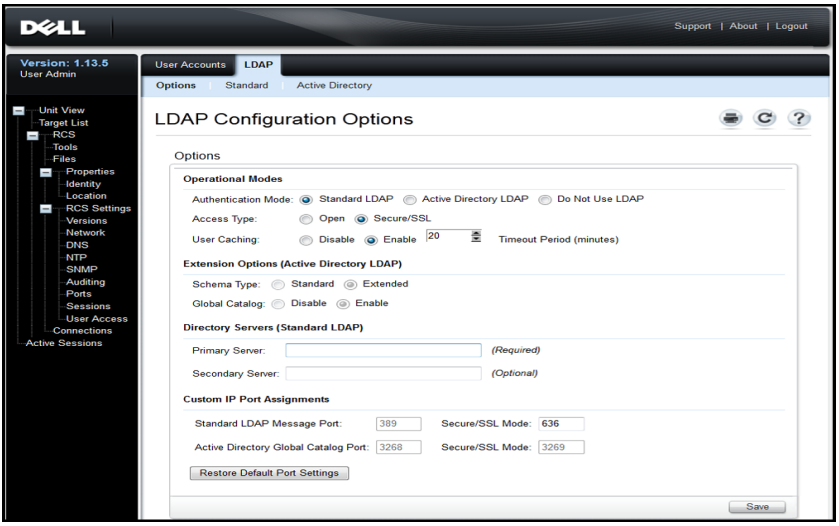


注：可以从外部中断 Avocent 身份验证关联，而无需执行这些步骤。但是，如果 Avocent 服务器关联创建用于用户身份验证，则必须通过此步骤明确移除关联，才能继续进行 LDAP 身份验证配置。

要启用 LDAP 身份验证：

1 在 User Access 下，选择 LDAP 选项卡，请参阅图 5.3。

图 5.3. LDAP Configuration Options 画面



2 在 Operational Modes 部分中选择一个可用的 LDAP Authentication Modes。

3 必须设置配置选项以完全启用 LDAP 身份验证。 本章对每个选项都做了详细说明。

4 单击 *Save*。

要禁用 LDAP 身份验证，请选择 *Do Not Use LDAP* 选项，并单击 *Save*。此画面上的所有其他选项将被禁用，且不允许对字段进行编辑。 另外，Standard 和 Active Directory 选项卡下面的其他配置画面也将被禁用。

禁用 LDAP 身份验证时，用户访问将由本地定义的用户访问列表或 Avocent 管理软件（ 请参阅有关“用户访问”的章节） 来裁定。

启用 LDAP 身份验证时，本地定义的用户访问列表将优先于 LDAP 目录服务器的访问请求。 用户访问需要首先检查 RCS 定义的用户。 如果未找到匹配，请求将按照配置发送至 LDAP 目录服务器。

输入身份验证参数 — Operational Modes

Access type

LDAP 目录服务器可设置为在 Open 或 Secure 模式(使用 SSL — 安全套接字层加密) 下运行。 选定模式必须与主机目录服务器的模式相匹配。 选择 Secure/SSL 模式时，请参阅标题为“LDAP SSL 证书”的章节，以获取有关符合加密操作要求的指导。

User caching

只要通过 LDAP 成功完成用户身份验证，RCS 就会在选定时间段内保留从 LDAP 目录服务器获得的结果。 如果在这段时间内生成了另一个访问请求(通常会导致重复的目录服务器请求) ，则此请求将在 RCS 上进行本地处理。 这样会导致即时响应，使用户能够继续工作并最大程度地减小延迟。

此配置选项的三种设置为 disable、enable 和 timeout period。

Disable — 不允许用户缓存，并且始终向 LDAP 目录服务器询问有关所需的每位用户和每个时间的身份验证状态，以获取指导。 默认情况下，User Caching 为禁用。

Enable — 保存最近经 LDAP 目录服务器确定的用户授权请求的结果。当在预先确定的时间段内接收到相同的授权请求时，使用这些先备结果可为新的请求提供服务。

Timeout Period — 确定时间段的时长。 值以分钟为单位。 在框中仅输入数字，或使用箭头控制。

- 默认超时值： 15 分钟
- 最小超时值：1 分钟
- 最大超时值：1000 分钟

注：与所有配置更新一样，您必须单击 *Save* 来确认更改。 LDAP 配置更改通常能立即应用于 RCS，无需重新启动。

输入扩展选项 — Active Directory LDAP

选择 Active Directory 模式时，管理员必须确定将采用 Standard 还是 Extended 架构。另外，管理员还应声明是否要使用 Microsoft Global Catalog 选项。

输入身份验证参数 — Standard LDAP

使用 Standard LDAP(非 Microsoft Active Directory LDAP) 时，需要直接进入至少一个相关的目录服务器地址。在 Primary Server 和 Secondary Server 字段中输入地址。需要进入主服务器。

服务器地址可按以下形式之一输入：

- DNS 地址(例如：myldapserver.com)
- IPv4 地址(例如：10.20.255.255)
- IPv6 地址(例如：fe80::200:f8af:fe20:76ce)

输入身份验证参数 — Custom IP Port Assignments

本节允许更改通常用于 LDAP 的行业标准 IP 端口号。在大多数情况下，无需更改这些值。但是，如果您正在使用的 LDAP 目录服务器的管理员需要不同的端口分配，则可以在此处输入。

根据具体配置，LDAP 最多可使用四个不同的 IP 端口，每次可使用两个端口。这四个端口各自的插槽将在 LDAP Configuration Options 画面中显示。同一画面上的其他设置将用于确定可改变的端口。下表定义了启用可用端口插槽并允许对其进行编辑的情况。

表 5.1：编辑 IP 端口分配

启用和可自定义的端口插槽列表	Open 模式	Secure/SSL 模式

不使用 Global Catalog	Standard LDAP Message Port	Standard LDAP Message Port — Secure/SSL 模式
使用 Global Catalog	Standard LDAP Message Port 和 Active Directory Global Catalog Port	Standard LDAP Message Port — Secure/SSL 模式和 Active Directory Global Catalog Port — Secure/SSL 模式

如果需要随时恢复原始的行业标准 IP 端口指定，单击“Restore Default Port Settings”按钮。 所有四个端口的值都将返回其原始值，它们是：

Standard LDAP Message Port — 389

使用 SSL 模式的 Standard LDAP Message Port — 636

使用 Global Catalog 服务器的 Active Directory — 3268

使用 Global Catalog 服务器/SSL 的 Active Directory — 3269

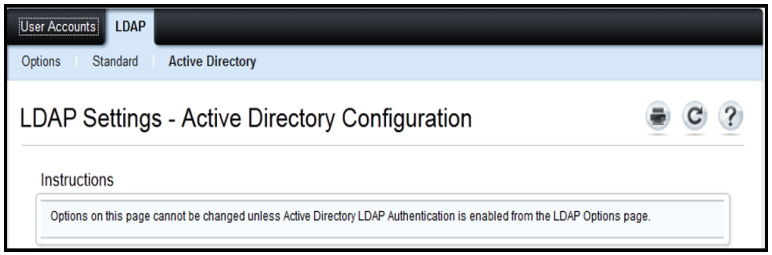
IP 端口号允许的范围为 1 到 65535。 与 LDAP 目录服务器使用的端口号不匹配将导致建立与该服务器的通信失败。

完成 LDAP 配置

对于 Standard 和 Active Directory LDAP 模式，需要其他参数来确保已正确连接至 LDAP 目录服务器。以下部分将对各参数进行论述。但是您应明白，OBWI 页面中建立有“联锁”，可帮助管理员确保在相应页面进行参数更新。

例如，如果您要选择 Active Directory LDAP 选项卡，您可能看到屏幕显示以下内容，请参阅图 5.4。

图 5.4. 通知消息 — LDAP 模式未启用



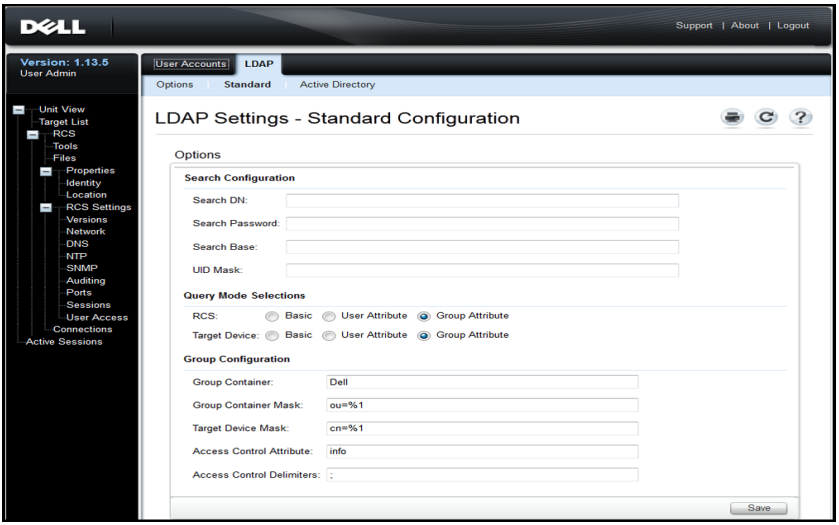
出现这种情况时，表示 Active Directory 模式尚未启用或已启用但未保存。 您应返回 LDAP Options 画面，选择 *Active Directory LDAP*，记下页面中该模式的次级参数，然后单击 *Save* 再返回本画面。

Standard LDAP 模式未启用时会出现相同的显示。

二级 LDAP Settings — Standard Configuration

与 LDAP Active Directory 配置一样，Standard LDAP 身份验证、搜索和查询参数可通过远程 OBWI 配置。 本节中的设置可通过 OBWI 窗口的 User Access/LDAP/Standard 选项卡访问，请参阅图 5.5。

图 5.5. 二级 LDAP Settings — Standard Configuration



注：虽然本节说明的是与 Standard LDAP 目录服务器建立的连接的设置参数，但请注意：本节说明也可用于与更多 Active Directory 服务的常规版本建立连接。

设置 RCS 以执行 Standard LDAP 查询

注：在使用带有 Active Directory 的任何查询模式之前，必须更新 Active Directory，这样选定的查询模式才能为用户分配合适的授权级别。

要设置组查询：

1 以管理员权限登录 LDAP 目录服务器软件。

2 创建一个用作组容器的组织单元 (OU)。

3 创建一个与交换机系统同名的计算机对象，用于查询 RCS(在 OBWI 的 RCS Overview 画面中指定) ，或者创建一个与相连的目标设备同名的计算机对象，用于查询目标设备。名称必须完全相同，并且区分大小写。

4 用于组查询的装置名称和目标设备名称均存储在装置中。在远程 OBWI 的 Appliance Overview 画面中指定的装置名称和目标设备名称必须由大小写字母、数字和连字符的任意组合组成，且必须与 LDAP 服务器上的对象名称相匹配。

5 在组容器组织单元下创建一个或多个组。

6 将用户名及目标设备和装置对象添加到在步骤四 (4) 中创建的组内。

7 指定用于执行 Access Control 属性的属性值。

搜索配置设置

成功连接 LDAP 需要进行四个设置。 分别为：Search DN、Search Password、Search Base 和 UID Mask。

Search DN

Search DN 定义一个管理员级用户，装置可使用其登录目录服务。在目标设备通过身份验证后，目录服务将允许其访问目录，以执行在 LDAP 查询页面上指定的用户身份验证查询。每个搜索值必须用逗号隔开。典型的条目类似于：

```
cn=Administrator,cn=Users,dc=MyDomainName,dc=com
```

Search password

如果搜索选项要求密码，则将使用 Search password。 它将对 Search DN 字段中指定的管理或用户进行身份验证。 任何可打印的 ASCII 字符都可以。

Search base

Search Base 定义所有开始进行 LDAP 搜索的起点。默认值为 dc=yourDomainName 和 dc=com。每个搜索组件必须用逗号隔开。例如，要定义 test.com 的搜索库，值应为 dc=test, dc=com。

UID mask

UID mask 指定 LDAP 目标设备进行用户 ID 搜索的搜索条件。格式为 <名称>=<%1>。默认值为 sAMAccountName=%1，与 Microsoft Active

Directory 服务的默认值相对应。

查询模式选择设置

配置装置和目标设备的查询模式参数。 装置用于对尝试访问控制台交换机的管理员和用户进行进行身份验证。目标设备用于对尝试访问所连接目标设备的用户进行身份验证。

有三个可用的查询模式。分别为 basic、user attribute 和 group attribute。

Basic

向目录服务发送用户的用户名和密码查询。通过有效用户身份验证后，用户即可访问装置和任何所连接的目标设备。

User attribute

向目录服务发送用户的用户名、密码和 Access Control 属性查询。Access Control 属性从 Active Directory 内的用户对象中读取。如果未找到值，用户将无法访问装置或目标设备。

Group attribute

在使用 Appliance 查询模式时，向目录服务发送装置和所连接目标设备的用户名、密码和组查询，而当使用 Target Device 查询模式时，则向目录服务发送选定目标设备的用户名、密码和群组查询。在使用 Appliance 查询模式时，如果找到了包含用户和装置名称的群，用户即取得访问装置或目标设备的权限。在使用 Target Device 查询模式时，如果找到了包含用户和目标设备 ID 的群，用户即取得选定目标设备的权限。

注：根据所选查询模式，此画面上的多个配置项目将按其适用性启用或禁用。

组配置参数

有多个可用的组配置参数。

组容器

Group container 用于将管理员在 Active Directory 中创建的组织单元 (OU) 指定为组对象的位置。组对象可包含用户、计算机、联系人和其他组，每一项都可分配特定的访问级别。

Group container mask

Group container mask 定义 Group Container 的类型，通常为 OU。默认值为 ou=%1。

Target device mask

Target device mask 定义目标设备的搜索过滤器。默认值为 cn=%1。

Access control 属性

Access control 属性指定查询模式设置为 User Attribute 或 Group Attribute 时使用的属性名称。默认属性名称为**"info"**。

Access control delimiters

LDAP 标准将分号 (;) 指定为用于分隔单一命名属性中的多个属性。在正常应用中，不需要对其进行更改。例如，假设 LDAP 目录中有一个白板标记对象，则属性"Color"将用于确定此标记的颜色。

Color:red;blue;green;black;purple

"Color"是属性的名称，其余部分代表属性的值 — 在此示例中是一个复合值。对于复合值，分号是用于标记一个组成部分的末尾和下一个组成部分的开端的分隔符。

在少数情况下，LDAP 管理员可能需要将分号用作值本身的一部分。在这种情况下，分隔符字符需要更改为其他字符。如果是这样，使用该字段可指定将用于识别 Access Control 属性分隔方法的所有字符 (至少需要一个字符，也可使用多个字符) 。例如，将分隔符字段设置为 **#$;**(三个字符)

Color:red#blue$green;black#purple

这些分隔符也将找到与上述示例相同的五个组成值的成分。 LDAP 管理员应确保所定义的任何 Access Control Delimiter 字符不会作为其他地方的任何属性的值出现或用于分隔符以外的其他目的。

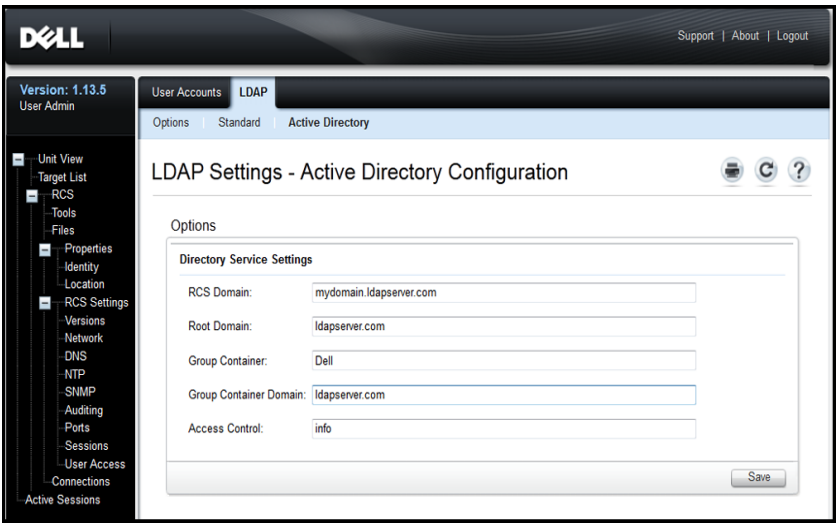
如上图所示，Access Control 属性 (ACA) 由一个名称和一个值的组合组成。 默认情况下，我们会搜索与用户和目标设备相匹配的 LDAP 目录条目，查找命名为“info”的属性。 找到后，这些属性的值将告诉我们用户在该设备上的授权级别。 如果 LDAP 服务管理员想要使用 info 以外的属性，可通过上述字段进行自定义。

由于用户可能是多个组的成员，且每个组对于不同的设备可能具有不同的授权级别，因此运行的 Tally 会保存这些结果。根据 LDAP 标准，报告的最终授权级别是在为受监视的特定用户和设备找到的所有正结果中发现的最高(最自由) 的级别。

二级 LDAP Settings — Active Directory Configuration

本节中的设置可通过 OBWI 窗口的 User Access/LDAP/Active Directory 选项卡访问，请参阅图 5.6。

图 5.6. 二级 LDAP Settings — Active Directory Configuration



如果您计划安装 Dell Extended 架构，只需输入将要使用的 RCS 和 Root Domains。

如果您决定不使用 Dell Extended 架构，则将安装环境中的 RCS 和访问受控的 SIP 配置为 Active Directory 中的计算机对象。要这样做，首先需要配置一个组织单元以容纳将用户与访问受控的 RCS 及其相连的 SIP 相关联的群组对象。这可以是先前创建的 OU 或为此特别创建的 OU，但是它在 Group Container 域的所有 OU 中必须是唯一的。

接着，选择 LDAP 目录中一个用于包含任意访问控制信息的属性。这应该是能够存储字符串值的先前未使用过的属性。(默认值为组对象的"info"属性。)

最后，您将需要在 OBWI 窗口提供的空白处输入 Group Container 的位置、Group Container Domain 和 Access Control 属性。

有关图 5.6 中所显示字段的更多详细说明，请参阅表 5.2。

表 5.2：Active Directory 配置字段说明

字段	说明
RCS Domain	RCS Domain 字段包含选择用于容纳代表 RCS 和 SIP 的所有对象的 Active Directory Domain 的名称。
Root Domain	Active Directory Forest 中最上面的域。

字段	说明
Group Container（仅限于 Standard 架构配置）	此字段在选择 Standard 架构时可用，包含在 Active Directory 中组织单元 (OU) 对象的部分辨别名。OU 用于容纳将用户与访问受控的远程控制台交换机及其相连的 SIP 相关联的群组对象。 例如，假设所选 OU 的辨别名为：ou=KVM-AccessControls，dc=MyCom，dc=com。在这种情况下，Group Container 字段应设置为“KVM-AccessControls”。输入 Group Container 字段的名称在 Group Container 域的所有 OU 对象中都必须是唯一的。 您可以选择使用先前创建的 OU 作为 Group Container，或为此特别创建一个 OU。 默认的 Group Container 是 KVM。
Group Container Domain（仅限于 Standard 架构配置）	此字段在选择 Standard 架构时可用，是群组容器所属 Active Directory 域的 DNS 名。
Access Control 属性（仅限于 Standard 架构配置）	该字段值指定 LDAP 目录中用于包含任意访问控制信息的属性，并仅在选择 Standard 架构时启用。 Access Control 属性选自 LDAP 目录对象中的属性，该 LDAP 目录对象代表成员包括用户和 RCS 或您正在尝试访问的相连计算机的群组。 当使用 Standard 架构时，Group Container 中的群组对象必须拥有一个属性，用于包含与该群组相关联的许可级别。Access Control 属性字段在选择 Standard 架构时可用，其中包含所选属性的名称。所选的属性必须能够存储字符串值；例如，默认属性是可通过 Active Directory 用户和计算机 (ADUC) 插件访问的“info”。使用 ADUC，可通过访问群对象的“Notes”属性设置 info 属性的值。

LDAP SSL 证书

所有的 LDAP 协议交换(RCS 和 Active Directory 服务器之间) 受到 SSL 保护。在 LDAP 协议受到 SSL 保护时，它被称作 LDAPS(通过安全套接字层的轻型目录访问协议) 。每个 LDAPS 连接以协议“握手”开始，而“握手”触发从响应的 Active Directory 服务器到 RCS 的安全证书传输。一旦接收，则 RCS 负责验证证书。为了验证证书，RCS 必须配置一份根证书颁发机构 (CA) 的证书。在进行此操作前，首先必须产生证书。

启用域控制器上的 SSL

如果您打算使用 Microsoft Enterprise Root CA 自动分配所有的域控制器 SSL 证书，必须执行以下步骤在每个域控制器上启用 SSL(如果您之前没有这样做的话) 。

1 将 Microsoft Enterprise Root CA 安装在域控制器上。

   a. 选择**开始 — 控制面板 — 添加或删除程序**。

   b. 选择**添加/删除 Windows 组件**。

   c. 在“Windows 组件向导”中，选择**证书服务**复选框。

   d. 选择 **Enterprise root CA** 作为 CA 类型，并单击**下一步**。

   e. 输入此 CA 的公用名称，单击**下一步**，然后单击**完成**。

2 通过为每个控制器安装 SSL 证书在每个域控制器上启用 SSL。

   a. 单击**开始 — 管理工具 — 域安全策略**。

   b. 展开“公钥策略”文件夹，右键单击**自动证书申请设置**，并单击**自动证书申请**。

   c. 在“自动证书申请安装向导”中，单击**下一步**，并选择**域控制器**。

3 单击**下一步**，然后单击**完成**。

可在 Linux 中使用 openssl 创建认证/私钥文件。Openssl 可在网站 openssl.org 中下载。以下说明中包含在 <> 中的文本，表示用户需要根据该行末尾的标准设置一个值。

注：以下说明中包含在 <尖括号> 中的文本，表示用户需要根据该行末尾的标准设置一个值。

创建要导入的证书：

1 在 Linux 命令提示符窗口中，输入 **openssl**，然后按 <Enter>。用户将看到 OpenSSL 提示符。

OpenSSL> genrsa -out privatekey.pem <512>

Generating RSA private key, 512 bit long modulus

.....++++++++++++

.....++++++++++++

e is 65537 (0x10001)

OpenSSL> req -new -key privatekey.pem -x509 -out certificate.pem-batch-days <365>

2 在辨别名(DN中输入将整合到您的证书申请中的信息。某些字段可能有默认值。根据需要，您可以键入“.”将字段留空。

Country Name(2 个字母代码) [GB]:<US>

State or Province Name(全称) [Berkshire]:<Texas>

Locality Name(如城市) [Newbury]:<Austin>

Organization Name(如公司) [My Company Ltd]:<Dell, Inc.>

Organizational Unit Name(如部门) []:<Round Rock>

公用名(如您的名称或服务器主机名) []:<RCS

DNS 名称或 IP>

Email Address []:<support@dell.com>

OpenSSL> quit

3 在 Linux 命令提示符窗口中，键入 **cat certificate.pem privatekey.pem > webserver.pem**，然后将文件从 UNIX 换行转换为 DOS 回车/换行，方法是键入 **unix2dos webserver.pem**。

要导出 CA 证书：

1 在 Windows 操作系统中，要打开证书颁发机构管理工具，请单击**开始 — 所有程序 — 管理工具 — 证书颁发机构**。

2 您可通过右键单击树形视图中的颁发机构，然后选择**属性**查看证书颁发机构的属性。将会打开“CA 属性”对话框。

3 单击**常规**选项卡和**查看证书**按钮，打开“证书”对话框。

4 单击**详细信息**选项卡，然后单击**复制到文件**按钮。将会打开“证书导出向导”。

5 单击**下一步**开始使用向导。

6 在“导出文件格式”画面上选择 **Base64 编码 X.509 (.CER)** 单选按钮，并单击**下一步**按钮。

7 在**要导出的文件**画面上输入或浏览导出证书的文件名和路径。单击**下一步**按钮。

8 单击**完成**按钮。

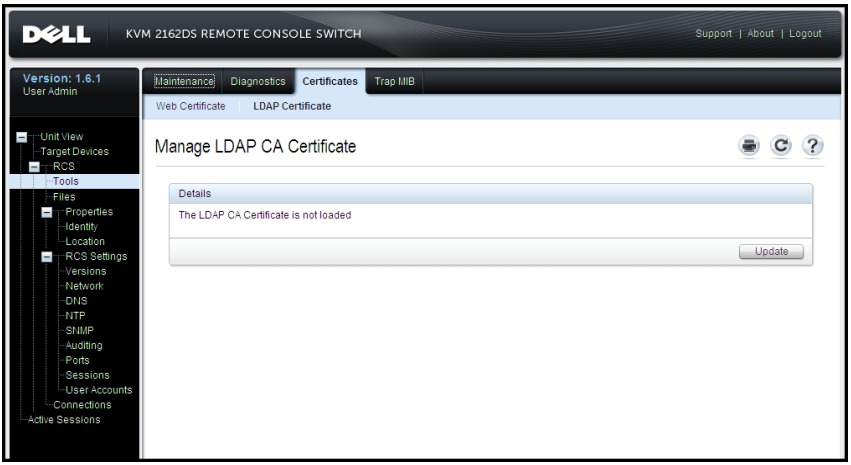
导出的证书文件已正确格式化并可由 OpenSSL 读取。

通常只需要上传 CA 证书一次，但是如果证书被作废、证书过期，或从串行控制台菜单中选择了“Restore Factory Defaults”，则必须再次上传证书。

注：以上说明适用于 Microsoft Root CA 证书。对于其他 CA，请与 CA 供应商联系。

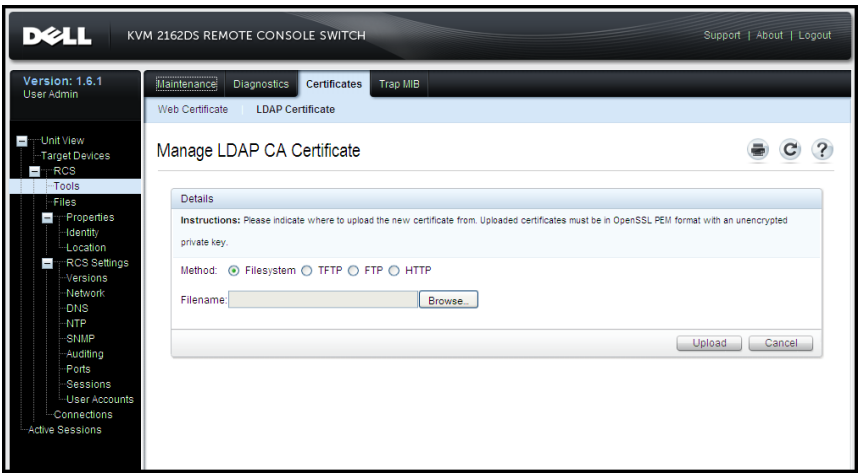
注：必须启用网络时间协议 (NTP) 以便 LDAPS 正常工作。

图 5.7. OBWI - LDAP 证书



单击 Update 后将显示以下窗口。

图 5.8. OBWI — 更新 LDAP 证书



您可浏览证书并将其打开。一旦打开证书并显示其内容，则用户可以将证书发送给 RCS。

登录超时

针对因目录树较大而导致 LDAP 身份验证执行缓慢的情况，Sessions 窗口提供登录超时功能，默认超时为 30 秒。登录超时是指用户按 Login 对话框上的 **OK** 按钮到 RCS 无响应的时间。RCS 还将会使用此值确定 LDAP 请求身份验证的超时。

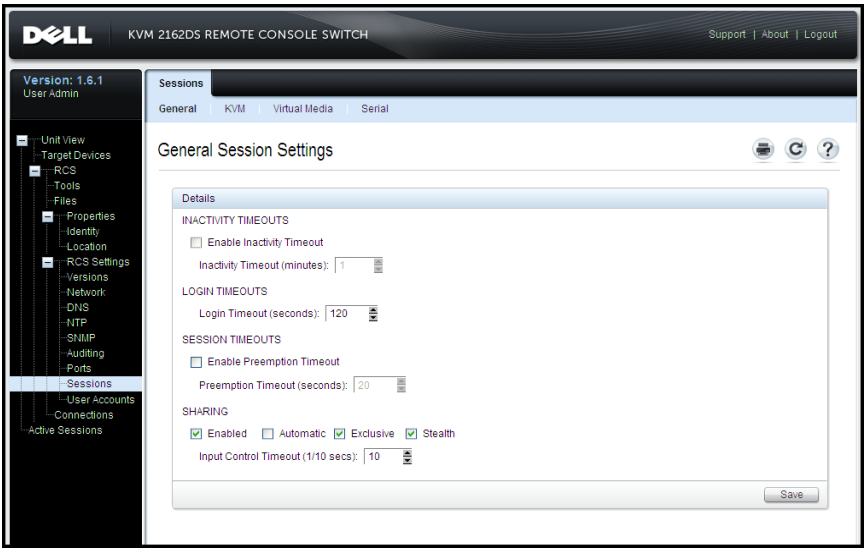
要在板载 web 界面中指定登录超时：

1 单击 **Sessions** 打开 General Session Settings 画面。

2 在 Login Timeout 菜单中指定秒数。

3 单击 **Save**。

图 5.9. OBWI - 登录超时



注：Login Timeout 与 User Login Caching 功能不同。后者会在登录完成后的一段时间内缓存验证结果，以消除重复的 LDAP 通信请求。

CA 证书信息显示

仅当公钥长度小于或等于 2048 比特时，RCS 才可在此窗口中显示完整的 CA 证书信息。当公钥大于 2048 位时，此窗口中的主题、签发者和有效日期数据将不完整显示。[1]

以下显示的是 CA 证书信息的示例：

1 从客户端下载 CA 证书至 RCS。

2 在串行控制台主菜单中输入 **option** 8 以显示 LDAP CA 证书。

RCS 将显示以下类型的信息：

Begin CA certificate information display
subject= /DC=msft/DC=ldaptest/CN=MyCertificate
issuer= /DC=msft/DC=ldaptest/CN=MyCertificate
notBefore=Dec 7 20:09:56 2005 GMT
notAfter=Dec 7 20:18:34 2010 GMT
serial=7BA146C0221A08B447B989292074329F
MD5 Fingerprint=
CB:6D:70:30:31:E5:1B:C0:90:BB:DB:32:B2:C9:D1:5A
End CA certificate information display

执行下述说明中的步骤，以在 Microsoft Windows Server 2003 平台上安装 RCS 软件：

1 选择**开始**菜单。

2 右键单击**我的电脑**，然后选择**属性**。

3 选择**高级**选项卡。

4 单击**性能设置**按钮。

5 选择**数据执行保护**选项卡。

6 选择单选按钮**只为关键 Windows 程序和服务启用数据执行保护**。

7 单击**确定**。

8 再次单击“系统属性”对话框的**确定**按钮。

配置群组对象

通过将用户加入 Group Container 中的群组，可以将访问控制应用到特定的 Active Directory 用户帐户。群组成员必须还包含代表允许用户访问的 RCS 和 SIP 的对象。授予的访问级别由群组对象（Standard 架构）或关联对象（Extended 架构）中的特定属性值决定。有三个可用的许可级别。按照权限递增的顺序，它们是 KVM User、KVM User Admin 和级别最高的 KVM Appliance Admin。

注：如果不使用 KVM User 访问级别，则不需要配置 SIP 对象，因为在默认情况下两种管理员权限均可访问所有 SIP。

表 5.3：各访问级别允许的操作

操作	KVM Appliance Admin	KVM User Admin	KVM User
抢占	允许抢占另一个 KVM Appliance Admin 或 KVM User Admin。必须通过将 TD 加入目录的适当群组对象中为每个目标设备配置许可。	允许抢占另一个 User Admin。必须通过将目标设备加入目录的适当群组对象中为每个目标设备配置许可。	否
配置网络参数和全局设置	是 — 必须通过将 RCS 加入目录的适当群组对象中为每个 RCS 配置权限。	否	否
重启	是 — 必须通过将 RCS 加入目录的适当群组对象中为每个 RCS 配置权限。	否	否
闪存升级	是 — 必须通过将 RCS 加入目录的适当群组对象中为每个 RCS 配置权限。	否	否

操作	KVM Appliance Admin	KVM User Admin	KVM User
管理用户帐户	是 — 必须通过将 RCS 加入目录的适当群组对象中为每个 RCS 配置权限。	是 — 必须通过将 RCS 加入目录的适当群组对象中为每个 RCS 配置权限。	否
配置端口设置	是 — 必须通过将 RCS 加入目录的适当群组对象中为每个 RCS 配置权限。	否	否
目标设备访问	是 — 必须通过将 RCS 加入目录的适当群组对象中为每个 RCS 配置权限。	是 — 必须通过将 RCS 加入目录的适当群组对象中为每个 RCS 配置权限。	是，如果由管理员配置。必须通过将 TD 加入目录的适当群组对象中为每个目标设备配置许可。

必须配置 AD 用户帐户以接收 RCS 管理员 (KVM Appliance Admin) 权限，然后该帐户才允许修改身份验证面板中的任何字段。特别指出，仅 RCS 管理员可修改身份验证设置。

Standard 架构的 Active Directory 对象概述

对于网络上您想要将其与 Active Directory 整合以便进行身份验证和授权的每个物理 RCS，您必须至少创建一个计算机对象来代表它。您还需要为每个 SIP 创建一个计算机对象，该 SIP 连接至将使用 KVM User 权限级别控制的 RCS。管理员级别群组无需代表 SIP 的计算机对象。KVM User Group 中的用户仅可访问在同一 KVM User Group 中的 SIP。在默认情况下，具有管理员权限的用户拥有访问所有 SIP 的权限。

要为 RCS 设置群组对象：

1 创建包含与您的交换机安装环境相关的群组对象的组织单元。

2 在此组织单元内，创建 3 个群组对象以代表用户权限级别。分别用于 KVM Appliance Administrators、KVM User Administrators 和 KVM Users。

3 使用 MSADUC 工具，打开 KVM 装置管理员群组对象并选择 Notes 属性。在 Notes 字段中为该组输入访问级别 (KVM Appliance Admin) 并保存。对于其他 2 个群组对象，使用其各自的名称重复此步骤。

注：所有 access control 属性值的单一语法为：

"[<任意文本字符串> <分隔符>] <权限级别> [<分隔符> <任意文本字符串>]"

其中：<权限级别>： ＝“KVM User”或“KVM User Admin”或“KVM Appliance Admin”

<分隔符>：:= 以下任何一个或多个：<换行符> 或 <c/r> 或 <逗号> 或 <分号> 或 <制表符>

<任意文本字符串>是任何字母数字字符并可能是零(即空) 字符串。

方括号表示可选项目，例如：下列模板表示一个可选的字符串和分隔符，后面是所需的权限级别："[<任意文本字符串> <分隔符>] <权限级别1>"。

4 创建一个计算机对象以代表 RCS。

5 对于访问受限为 KVM User 权限级别的服务器，为与其相连的每个 SIP 创建计算机对象。

6 将代表交换机的计算机对象添加到适当的群组对象。

7 将用户对象添加到适合其访问级别的群组对象。

8 将用于访问受控的 SIP 的计算机对象添加到 KVM User Group。

Dell Extended 架构 Active Directory 对象概述

对于网络上您想要将其与 Active Directory 整合以便进行身份验证和授权的每个物理 RCS，您必须至少创建一个 RCS 设备对象来代表物理交换机和一个关联对象。关联对象用于将具有特定权限的用户或组与一个或多个 SIP 连接起来。此模型为管理员提供了对不同的用户、RCS 权限和 RCS 上的 SIP 组合的最大灵活性而不会添加太多的复杂性。

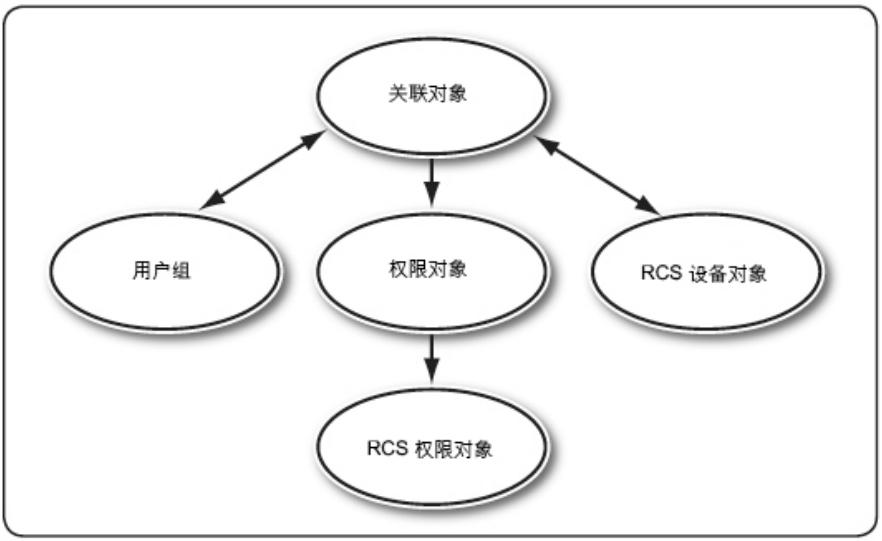
RCS 设备对象是到 RCS 的连接，用于查询 Active Director 以进行身份验证和授权。在将 RCS 添加到网络时，管理员必须使用 RCS 的 Active Directory 名称配置 RCS 及其设备对象，以便用户可以使用 Active Directory 进行身份验证和授权。管理员还将需要将远程控制台交换机添加到至少一个关联对象以便用户进行身份验证。

您可以创建任意数量的关联对象，而且每个关联对象可以按需要与任意数量的用户、用户组或 RCS 设备对象连接。用户和 RCS 设备对象可以是企业内任何域的成员。

但是，每个关联对象可能仅可连接一个权限对象（或连接用户、用户组或 RCS 设备对象）。权限对象允许管理员控制哪个用户对特定的 SIP 拥有何种权限。

下图显示了关联对象提供进行所有身份验证和授权所需的连接。

图 5.10. Active Directory 对象的典型设置

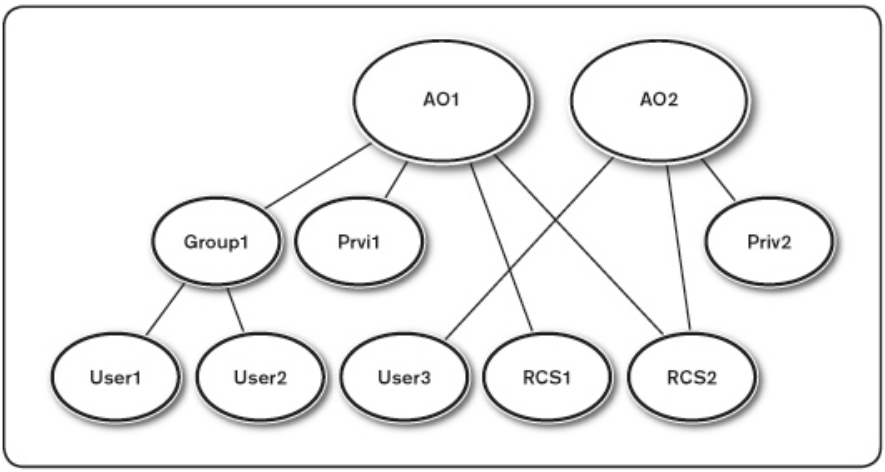


您可以按需要创建任意数量的关联对象。但是，您必须创建至少一个关联对象，而且您必须为网络上您想要将其与 Active Directory 整合以便进行身份验证和授权的每个 RCS 配备一个 RCS 设备对象。关联对象允许任意数量的用户和/或组以及 RCS 设备对象。然而，每个关联对象仅拥有一个权限对象。关联对象连接对 RCS 拥有权限的用户。

此外，您可以在单个或多个域内设置 Active Directory 对象。例如，您拥有 2 台 RCS(RCS1 和 RCS2) 和 3 个 Active Directory 用户 (User1、User2、和 User3) 。您想要授予 User1 和 User2 对 2 台 RCS 的管理员权限并授予 User3 对 RCS2 的登录权限。

下图显示在此方案中设置 Active Directory 对象的方法。

图 5.11. 在单个域内设置 Active Directory 对象



为单域方案设置对象，请执行以下任务：

1 创建 2 个关联对象。

2 创建 2 个 RCS 设备对象 RCS1 和 RCS2，分别表示 2 台 RCS。

3 创建 2 个权限对象 Priv1 和 Priv2，其中 Priv1 拥有所有权限(管理员) ，而 Priv2 拥有登录权限。

4 将 User1 和 User2 分组到 Group1。

5 将 Group1 添加为关联对象 1 (AO1) 的成员，Priv1 为 AO1 中的权限对象，且 RCS1 和 RCS2 为 AO1 中 RCS 设备。

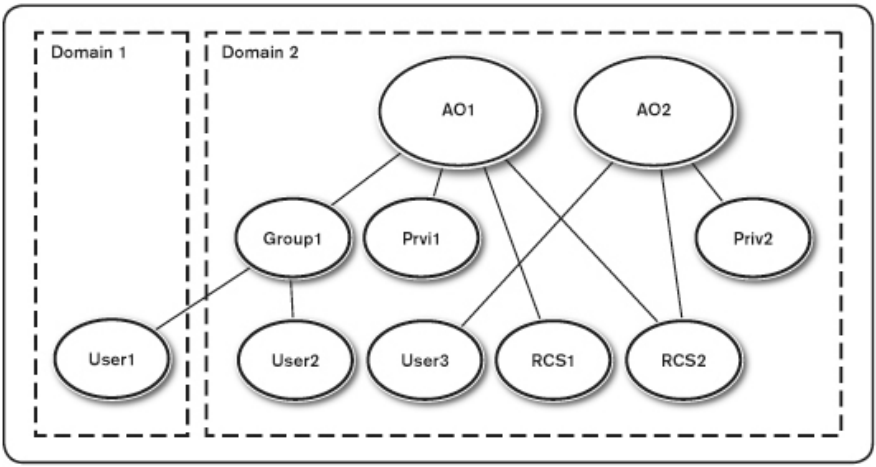
6 将 User3 添加为关联对象 2 (AO2) 的成员，Priv2 为 AO2 中的权限对象，以及 RCS2 为 AO2 中 RCS 设备。

有关详细说明，请参阅“使用 Dell 架构扩展将 RCS 用户和权限添加到 Active Directory”。

下图显示在多个域中设置 Active Directory 对象的方法。在此方案中，您拥有 2 台 RCS(RCS1 和 RCS2) 和 3 个 Active Directory 用户 (User1、User2、和 User3) 。

User1 在 Domain1 中，User2 和 User 3 在 Domain2 中。您想要授予 User1 和 User2 对 2 台 RCS 的管理员权限并授予 User3 对 RCS2 的登录权限。

图 5.12. 在多个域内设置 Active Directory 对象



要为多域方案设置对象，请执行以下任务：

1 确保域林功能处于本地模式或 Windows 2003 模式。

2 在任何一个域内创建 2 个关联对象：AO1(通用范围和 AO2。该图显示 Domain2 中的对象。

3 创建 2 个 RCS 设备对象 RCS1 和 RCS2，分别表示 2 台 RCS。

4 创建 2 个权限对象 Priv1 和 Priv2，其中 Priv1 拥有所有权限(管理员) ，而 Priv2 拥有登录权限。

5 将 User1 和 User2 分组到 Group1。Group1 的分组范围必须为“通用”。

6 将 Group1 添加为关联对象 1 (AO1) 的成员，Priv1 为 AO1 中的权限对象，且 RCS1 和 RCS2 为 AO1 中 RCS 设备。

7 将 User3 添加为关联对象 2 (AO2) 的成员，Priv2 为 AO2 中的权限对象，以及 RCS2 为 AO2 中 RCS 设备。

使用 Dell 架构扩展配置 Active Directory 以访问 RCS

在您可以使用 Active Directory 访问 RCS 之前，必须按编号顺序执行以下步骤配置 Active Directory 软件和 RCS：

1 扩展 Active Directory 架构。

2 扩展 Active Directory 用户和计算机插件。

3 将 RCS 用户及其权限添加到 Active Directory。

扩展 Active Directory 架构(可选)

扩展 Active Directory 架构会将 Dell 组织单元、架构类和属性、范例权限和关联对象添加到 Active Directory 架构。

注：在扩展架构前，您必须拥有对域林架构主机灵活单主机操作 (FSMO) 角色所有者的 Schema Admin 权限。

您可以使用 2 种不同的方法扩展架构。您可以使用 Dell Schema Extender 实用程序或者使用 LDIF 脚本文件。

注：如果使用 LDIF 脚本文件，则不会添加 Dell 组织单元。

可通过访问 dell.com/support 获得 LDIF 文件和 Dell Schema Extender。

要使用 LDIF 文件，请查阅 LDIF 文件目录下自述文件中的说明。要使用 Dell Schema Extender 扩展 Active Directory 架构，请执行“使用 Dell Schema Extender”中的步骤。

您可以从任何位置复制和运行 Schema Extender 或 LDIF 文件。

使用 Dell Schema Extender

注：Dell Schema Extender 使用 SchemaExtenderOem.ini 文件。为了确保 Dell Schema Extender 实用程序正常运行，请勿修改此文件名。

1 单击 Welcome 画面上的 **Next**。

2 阅读警告然后再单击 **Next**。

3 选择 Use Current Log In Credentials 或者输入具有架构管理员权限的用户名和密码。

4 单击 **Next** 运行 Dell Schema Extender。

5 单击 **Finish**。

安装 Dell Extension to the Active Directory Users and Computers Snap-In (可选)

在 Active Directory 中扩展架构时，您还必须扩展 Active Directory 用户和计算机管理单元以便管理员可以管理 RCS 设备、用户和用户组、RCS 关联以及 SIP 权限。Dell Extension to the Active Directory User's and Computers Snap-In 是可以在使用 Dell Systems Management Consoles CD 安装系统管理软件时安装的选项。有关安装系统管理软件的更多说明，请查阅《Dell OpenManage Software Quick Installation Guide》。

注：您必须在每个管理 Active Directory RCS 对象的系统上安装 Administrator Pack。该安装在以下"打开 Active Directory 用户和计算机插件"部分中介绍。如果不安装 Administrator Pack，则无法查看容器中的 Dell SIP 对象。

注：有关 Active Directory 用户和计算机插件的更多信息，请查阅 Microsoft 说明文档。

打开 Active Directory 用户和计算机插件

要打开 Active Directory 用户和计算机插件，请执行以下步骤：

如果您在域控制器中，则单击**开始 — 管理工具 — Active Directory 用户和计算机**。

-或-

如果您使用的不是域控制器，则必须在本地系统上安装相应的 Microsoft Administrator Pack。要安装此 Administrator Pack，请单击**开始**

— 运行，键入 <MMC>，然后按 <Enter>。这会打开 Microsoft 管理控制台 (MMC)。

1 单击控制台 1 窗口中的**文件**(或 Windows 2000 系统上的“控制台”) 。

2 单击**添加/删除插件**。

3 选择 **Active Directory 用户和计算机管理单元**，然后单击**添加**。

4 单击**关闭**然后单击**确定**。

使用 Dell 架构扩展将用户和权限添加到 Active Directory

Dell 扩展 Active Directory 用户和计算机管理单元允许您通过创建 SIP、关联和权限对象添加 RCS 用户和权限。要添加每种类型的对象，请执行每个小节中的步骤。

创建 SIP 对象

1 在 MMC“控制台根节点”窗口中，右键单击一个容器。

2 选择**新建 — Dell SIP 对象**。这会打开“新建对象”窗口。

3 键入新对象的名称。此名称必须与您在第 35 页上的“配置远程控制台交换机”步骤 4 中键入的 RCS 名称保持一致。

4 选择 **SIP 设备对象**。

5 单击**确定**。

创建权限对象

权限对象必须在与其相关联的关联对象所在的同一域内创建。

1 在“控制台根节点”(MMC) 窗口中，右键单击一个容器。

2 选择**新建 — Dell SIP 对象**，打开“新建对象”窗口。

3 键入新对象的名称。

4 选择**权限对象**。

5 单击**确定**。

6 右击您所创建的权限对象，并选择**属性**。

7 单击 RCS **权限**选项卡并选择您希望用户可以拥有的 RCS 权限。

使用 Dell 关联对象语法

使用 Dell 关联对象语法，对象类型将默认为 Dell LDAP 架构中的用户和组。在 Dell Extended 架构中，Dell 为四个新对象类添加了唯一的对象 ID：

- KVM RCS 对象
- KVM SIP 对象
- 权限对象
- 关联对象

这些新对象类是根据默认 Active Directory 类别的各种组合(层级与 Dell 的唯一属性类型进行定义。每个 Dell 唯一属性类型都是根据默认 Active Directory 属性语法定义。

使用的默认 Microsoft Active Directory 对象类包括用户和组。用户类别一般表示包含了单个实体信息的 Active Directory 对象。组表示用于嵌套的容器，并包含了一系列对象的信息。

每个 KVM RCS 对象代表 Active Directory 内一个单独的远程控制台交换机。由于这些交换机是单个实体，因此在 LDAP 默认的语言中，它们是用户对象而不是组对象。

每个权限对象定义一个独特的权限复合集。每个复合集被看作单独的实体，因此它是用户对象而不是组对象。

关联对象包含一系列授予特定用户帐户的关于特定 RCS 和/或特定 SIP 的权限信息。RCS 对象中的用户帐户可根据以下任意组合来指定：

- 单个帐户
- Active Directory 用户帐户安全组

- 多个 Active Directory 用户帐户安全组

同样地，由于关联对象中有多个 RCS 和/或 SIP，且因为关联对象可以用相同的方式使用安全组，因此它自身也定义为组对象。

创建关联对象

关联对象来源于群组且必须包含群组类型。关联范围指定了关联对象的安全群组类型。当您创建关联对象时，您必须选择适用于您想要添加的对象类型的关联范围。例如，选择“通用”是指关联对象仅当 Active Directory 域在本地模式或以上模式运行时可用。

创建关联对象：

1 在“控制台根节点”(MMC) 窗口中，右键单击一个容器。

2 选择**新建 — Dell SIP 对象**，打开“新建对象”窗口。

3 键入新对象的名称。

4 选择**关联对象**。

5 选择关联对象的范围。

6 单击**确定**。

将对象添加到关联对象

通过使用“关联对象属性”窗口，您可以关联用户或用户组、权限对象和 SIP 对象或 SIP 设备组。

注：在使用 Windows 2000 模式或更高模式时，必须使用“通用组”以便跨域使用您的用户或 SIP 对象。

您可以添加用户和 SIP 设备群组。创建 Dell 相关群组的方式与创建其他群组一样。

添加用户或用户组：

1 右键单击关联对象并选择**属性**。

2 选择**用户**选项卡，然后单击**添加**。

3 键入用户或用户组名，然后单击**确定**。

单击“权限对象”选项卡将权限对象添加到在对 SIP 设备进行身份验证时定义用户或用户组权限的关联中。

注：您只能将一个权限对象添加到关联对象。

添加权限：

1 选择**权限对象**选项卡，然后单击**添加**。

2 键入权限对象名称，然后单击**确定**。

单击“产品”选项卡将一个或多个 SIP 设备添加到关联中。关联的设备可指定已定义的用户或用户组可用的与网络相连的 SIP 设备。

注：您可以将多个 SIP 设备添加到关联对象。

添加 SIP 设备或 SIP 设备组：

1 选择**产品**选项卡，然后单击**添加**。

2 键入 SIP 设备或 SIP 设备组名，然后单击**确定**。

3 在“属性”窗口中，单击**应用**，然后单击**确定**。

控制台重定向访问安全

在任何 RCS 安装中，任何用户权限都允许用户启动板载 web 界面。该用户可使用的板载 web 界面功能受限于在 RCS 中建立的用户权限级别。带有 Dell Extended 架构的 LDAP 通过允许管理员限制用户访问板载 web 界面为 RCS 管理添加了额外的安全性。

使用板载 web 界面的授权依据是否在 Dell 权限对象 (DPO) 的 KVM RCS Privilege 选项卡中配置用户权限级别而定。DPO 的 KVM SIP Privileges 选项卡中的 Console Redirection Access 复选框为无法查看板载 web 界面的用户提供方法，以通过 RCS 客户端启动与 SIP 子集的视频查看器会话。此授权由 DPO 中设置的配置参数和 Dell 关联对象 (DAO) 中包含的 SIP 对象的组合控制。

若您希望用户具备访问板载 web 界面的授权，但又不想让他们可以从 RCS 客户端启动查看器会话，请执行以下步骤：

1 为每个允许用户访问的 SIP 创建一个 Dell SIP 对象。

2 为每位要控制的用户创建一个 Active Directory 用户帐户。

3 创建一个 DPO。不要勾选 KVM RCS Privileges 选项卡三个框中的任何一个。勾选 KVM SIP Privileges 选项卡上的 Console Redirection Access 框。

注：如果勾选了任何 KVM RCS Privileges 复选框和勾选了 Console Redirection Access 框，与在 KVM RCS Privileges 复选框中勾选的权限级别关联的一般用户权限将优先于在 Console Redirection Access 勾选的权限，同时用户仍能查看 AMP。

4 创建一个 DAO。

5 打开步骤 4 中创建的 DAO 的属性对话框。

a. 添加步骤 2 中创建的所有用户帐户。

b. 添加步骤 3 中创建的 DPO。

c. 添加步骤 1 中创建的 SIP 对象。

使用 Active Directory 登录 RCS

您可以通过 RCS 软件或 OBWI 使用 Active Directory 登录 RCS。

登录语法对所有三种方法是一样的：

<用户名@域> 或 <域>\<用户名> 或 <域>/<用户名>（其中用户名为 1–256 字节的 ASCII 字符串）。在用户名和域名中不允许使用空格和特殊字符（如 \、/ 或 @）。

注：您不可指定 NetBIOS 域名，如 Americas，因为无法解析这些名称。

注：如果没有包括域名，则使用远程控制台交换机中的本地数据库对用户进行身份验证。

LDAP 实施过程中的目标设备命名要求

若您遇到以下错误：

Login Failure.Reason:Access cannot be granted due to Authentication Server errors

请确认已经在 Active Directory 中创建了 SIP 对象，并且其名称与通过控制台交换机上的 OBWI 分配给 SIP 的名称一致。

Dell Standard 架构和 Dell Extended 架构使用 Microsoft Windows Active Directory 中的特定对象类来代表 SIP。Microsoft 标准命名惯例禁止这些对象类使用特殊字符或空格。若要在一个已配置的环境中使用 LDAP，而环境中目标设备当前在 SIP 的名称又包括了空格或特殊字符，则需要重新取一个不带空格或特殊字符的名称。

对 SIP 中的目标设备进行重新命名应通过控制台交换机中的 OBWI 完成，然后再通过 RCS 软件进行重新同步。请注意，OBWI 允许向分配给 SIP 的名称输入空格，而 Active Directory 则不允许。您必须根据 Microsoft Active Directory 的规则命名 SIP 对象。

常见问题解答

下表列出了常见问题和解答。

表 5.4：常见问题

我可以使用跨越多个目录林的 Active Directory 登录远程控制台交换机吗？	RCS Active Directory 查询算法仅支持单个目录林中的单个树。
在混合模式下（即目录林中的域控制器使用不同的操作系统，如 Microsoft Windows NT® 4.0、Windows 2000 或 Windows Server 2003），可以使用 Active Directory 登录远程控制台交换机吗？	是。在混合模式下，RCS 查询进程所使用的所有对象（其中包括用户、SIP 设备对象和关联对象）必须在同一个域。如果在混合模式下，Dell 扩展 Active Directory 用户和计算机插件会检查模式并限制用户以创建跨域对象。

RCS 与 Active Directory 一起使用支持多域环境吗？	是。必须在本地模式或 Windows 2003 模式下运行域林功能级别。此外，关联对象、远程控制台交换机用户对象和 SIP 设备对象群组(包括关联对象必须为通用组。
这些 Dell 扩展对象(Dell 关联对象、Dell 远程控制台交换机设备和 Dell 权限对象可以在不同的域吗？	关联对象和权限对象必须在同一个域。Dell 扩展 Active Directory 用户和计算机插件会强制在同一域内创建这两个对象。其他的对象可以在不同的域。
对域控制器 SSL 配置有任何限制吗？	是。目录林中所有的 Active Directory 服务器的 SSL 证书必须由相同的根 CA 签发，因为 RCS 仅允许上传一个信任的 CA SSL 证书。

如果我无法通过使用 Active Directory 身份验证登录 RCS，该怎么办？我如何对这个问题进行故障排除？	解答如下： 如果没有指定域名，则使用本地数据库。在 AD 身份验证不能正常工作的时候登录，使用默认的本地 admin 帐户。 确保您已勾选了 RCS Active Directory 配置页面上的 Enable Active Directory 复选框（RCS 软件）或 Use LDAP Authentication 复选框（板载 web 界面）。 确保 RCS Networking 配置页面的 DNS 设置正确。 确保至少一台在 NTP 面板上指定的服务器启用了网络时间协议。 确保已经从 Active Directory 根 CA 将 Active Directory 证书上传到 RCS。 检查域控制器 SSL 证书以确保它们没有过期。 • 确保“远程控制台交换机名称”、“根域名”和“RCS 域名”与 Active Directory 环境配置一致。 确保在登录期间使用正确的用户域名而非 NetBIOS 名。

A

附录 A：终端操作

通过控制台菜单界面还可对每台 RCS 进行交换机级配置。该菜单界面可通过 SETUP 端口进行访问。所有终端命令均可以通过运行终端仿真软件的终端或 PC 执行。

注：首选方法是通过本地 UI 配置所有设置。

要将终端连接到交换机：

1 使用随附的 RJ-45 到 DB-9(母式) 适配器和扁平 RJ-45 缆线，将终端或运行终端仿真软件(如 HyperTerminal) 的 PC 连接到交换机背面板的 SETUP 端口。终端设置为 9600 位/秒 (bps)、8 位、1 停止位、无奇偶校验和无流量控制。

2 打开各个目标设备，然后打开交换机。交换机初始化完成后，控制台菜单将显示以下消息：**Press any key to continue。**

控制台 Boot 菜单选项

交换机在启动时，您可以按任意键查看启动菜单。在此菜单中，您可以选择四个选项之一。

- Boot Normal
- Boot Alternate Firmware
- Reset Factory Defaults
- Full-Factory Reset

控制台 Main 菜单选项

启动后，主菜单将显示产品名称和版本。在此菜单中，您可以选择四个选项之一。

- Network configuration：使用此菜单选项可配置 RCS 的网络设置。
- Debug messages：此菜单选项可开启控制台状态消息。由于开启状态消息会明显降低性能，因此请仅在 Dell™ 技术支持部门要求这样做时才启用调试消息。查看完消息之后，按任意键退出此模式。
- Reset RCS：使用此菜单选项可执行交换机的软重置。
- Exit：此菜单选项用于返回就绪提示符状态。如果启用了控制台菜单界面密码，您必须退出 Main 菜单，以便下一个用户登录时会显示提示输入用户名和密码的登录画面。

B

附录 B：使用 SIP

管理员通过本地用户界面或远程 OBWI 可为每个串行 SIP 端口选择 Avocent ACS 控制台服务器或 Cisco 脚位排列。ACS 为默认值。

要将脚位排列更改为 Cisco 模式：

1 选择 *Unit View - RCS - RCS Settings - Ports - SIPs*。

2 单击所需 SIP。

3 选择 *Settings - Pinout*。

注：如果使用的是 DB-9 适配器，则选择 ACS 控制台服务器脚位配列。

ACS 控制台服务器端口脚位排列

下表列出了 SIP 的 ACS 控制台服务器串行端口脚位排列。

表 B.1：ACS 控制台服务器串行端口脚位排列

针脚编号	信号名称	输入/输出
1	RTS — 请求发送	输出
2	DTR — 数据终端就绪	输出
3	TXD — 传输数据	输出
4	GND — 信号接地	不适用
5	CTS — 可以发送	输入
6	RXD — 接收数据	输入

针脚编号	信号名称	输入/输出
7	DCD/DSR — 数据集就绪	输入
8	N/C — 未连接	不适用

Cisco 端口脚位排列

下表列出了 SIP 的 Cisco 串行端口脚位排列。

表 B.2：Cisco 串行端口脚位排列

针脚编号	信号名称	输入/输出
1	CTS — 可以发送	输入
2	DCD/DSR — 数据集就绪	输入
3	RXD — 接收数据	输入
4	GND — 信号接地	不适用
5	N/C — 未连接	不适用
6	TXD — 传输数据	输出
7	DTR — 数据终端就绪	输出
8	RTS — 请求发送	输出

C

附录 C：MIB 和 SNMP 陷阱

Dell RCS 可以将审计事件发送至 SNMP 管理器。SNMP 陷阱在 SNMP 陷阱 MIB 定义。

使用 Save Trap MIB 功能可从 RCS 上载陷阱 MIB 文件。上载的陷阱 MIB 文件然后可以加载到 SNMP 陷阱接收应用程序。

审计事件也可以发送至“syslog”目的地。在陷阱 MIB 文件中定义的每个陷阱的“--#SUMMARY”注解指定了每条 syslog 消息相应的格式。

本附录介绍了 RCS 可能会生成的陷阱事件。尽管我们努力在本附录中使用最新的信息，但如需最准确的陷阱信息，请参考陷阱 MIB 文件。

SNMP 管理器可以使用 IPv4 或 IPv6 协议访问 RCS 的 MIB-II 对象。

根据设计，RCS 中的企业特定的 MIB 对象无法使用 SNMP 访问。

RCS 陷阱定义使用下列征求意见文档 (RFC) 中所描述的结构。

- RFC-1155-SMI

  描述用于与基于 TCP/IP 的互联网配合使用的管理信息定义的常见结构和身份验证方案。

- RFC-1212

  描述用于制作简明和叙述性的 MIB 模块的格式。

- RFC-1213-MIB

  描述在基于 TCP/IP 的互联网中用于与网络管理协议配合使用的互联网标准 MIB-II。

- RFC-1215

描述 SNMP 标准化陷阱和提供一个定义企业特定的陷阱的方法。每个陷阱报告的特定对象在从 RCS 上载的陷阱 MIB 文件中定义。以下是一个生成的陷阱事件的列表。

表 C.1：生成的陷阱事件

陷阱事件	陷阱编号
开始重新启动	1
用户登录	2
用户注销	3
目标会话已启动	4
目标会话已停止	5
目标会话已终止	6
陷阱 7 至 9 被否决	7-9
映像文件升级已启动	10
映像文件升级结果	11
用户已添加	12
用户已删除	13
用户已修改	14
用户已锁定	15
用户已解锁	16
用户身份验证失败	17
SIP 已添加	18

陷阱事件	陷阱编号
SIP 已移除	19
SIP 已移动	20
目标设备名称已更改	21
堆叠交换机已添加	22
堆叠交换机已移除	23
堆叠交换机名称已更改	24
配置文件已加载	25
用户数据库文件已加载	26
认证机构证书已加载	27
SIP 映像升级已启动	28
SIP 映像升级结果	29
SIP 已重新启动	30
虚拟媒体会话已开始	31
虚拟媒体会话已停止	32
虚拟媒体会话已终止	33
虚拟媒体会话已保留	34
虚拟媒体会话未保留	35
虚拟媒体驱动器已映射	36
虚拟媒体驱动器取消映射	37

陷阱事件	陷阱编号
陷阱 38 至 44 被否决	38-44
屏幕分辨率已更改	45
聚集目标设备状态已更改	46
出厂默认值设置	47
电源出现故障	48
电源已恢复	49
Pdu 设备联机	50
Pdu 设备脱机	51
Pdu 插座打开命令	52
Pdu 插座关闭命令	53
Pdu 插座重启命令	54
PDU 插座打开检测失败	55
Pdu 插座关闭检测失败	56
Pdu 状态插座开启	57
Pdu 状态插座关闭	58
Pdu 端口名称已更改	59
Pdu 插座名称已更改	60
Pdu 输入馈电总负载高	61
Pdu 输入馈电总负载低	62

陷阱事件	陷阱编号
Pdu 设备名称已更改	63
Pdu 输入馈电名称已更改	64
Pdu 插座锁定命令	65
Pdu 插座解锁命令	66
Pdu 状态插座锁定	67
Pdu 状态插座解锁	68
Pdu 映像文件升级已开始	69
Pdu 映像文件升级结果	70
Pdu 电路名称已更改	71
Pdu 设备总负载高	72
Pdu 电路总负载高	73
Pdu 插座总负载高	74
风扇故障	75
温度范围	76
智能卡已插入	77
智能卡已移除	78

D

附录 D：缆线脚位排列信息

注：所有交换机的调制解调器和控制台/设置端口都具有 8 针模块化插孔。

调制解调器脚位排列

以下图示和表格为调制解调器脚位排列情况和说明。

图 D.1. 调制解调器脚位排列

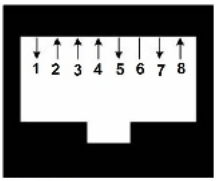


表 D.1：调制解调器脚位排列说明

针脚编号	说明	针脚编号	说明
1	请求发送 (RTS)	5	传输数据 (TXD)
2	数据集就绪 (DSR)	6	信号地线 (SG)
3	数据载波检测 (DCD)	7	数据终端就绪 (DTR)
4	接收数据 (RXD)	8	可以发送 (CTS)

控制台/设置端口脚位排列

以下图示和表格为控制台/设置端口脚位排列情况和说明。

图 D.2. 控制台/设置端口脚位排列

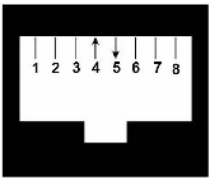


表 D.2：控制台/设置端口脚位排列说明

针脚编号	说明	针脚编号	说明
1	未连接	5	传输数据 (TXD)
2	未连接	6	信号地线 (SG)
3	未连接	7	未连接
4	接收数据 (RXD)	8	未连接

E

附录 E：UTP 缆线

本附录介绍了连接介质的各个方面。RCS 系统使用 UTP 缆线。交换机系统的性能有赖于高质量的连接。缆线质量差或安装或维护不良会降低交换机系统的性能。

注：此附录仅供参考。安装前，请咨询本地管理部门和/或布线顾问。

UTP 铜缆

以下是 RCS 支持的三种 UTP 缆线的基本定义：

- CAT 5（4 对）高性能缆线由绞合在一起的配对导线构成，主要用于数据传输。成对绞合可以使缆线免受一些不必要的干扰。CAT 5 缆线一般用于 10 或 100 Mbps 的网络。
- CAT 5E（增强型）缆线的特性与 CAT 5 相同，只是按照更为严格的标准制造。
- CAT 6 缆线的制造标准比 CAT 5E 缆线更严格。在相同频率下，CAT 6 的标准频率范围比 CAT 5E 更大，性能要求也显著提高。

布线标准

采用 RJ-45 接头的 8 导线（4 对）UTP 缆线有两种支持的布线标准：EIA/TIA 568A 和 B。这两种标准适合于采用 UTP 缆线规格的安装。RCS 系统支持其中任意一种布线标准。下表描述了每个针脚的标准。

表 E.1：UTP 布线标准

固定	EIA/TIA 568A	EIA/TIA 568B
1	白色/绿色	白色/橙色
2	绿色	橙色
3	白色/橙色	白色/绿色
4	蓝色	蓝色
5	白色/蓝色	白色/蓝色
6	橙色	绿色
7	白色/棕色	白色/棕色
8	棕色	棕色

缆线安装、维护和安全说明

以下是一些在安装或维护缆线之前要阅读的重要安全注意事项：

- 每条 UTP 最大布线长度不得超过 9.1 米。
- 始终保持成对绞合直至终接点，或未绞合长度不超过 12.7 毫米。终接时，绝缘层剥脱不能超过 25.4 毫米。
- 如果要弯曲缆线，则弯度不能太大，半径不得小于 25.4 毫米。缆线弯度太大或扭结会永久性损坏缆线的内部结构。
- 使用缆线扎带固定缆线时，用力要适中。不要扎得太紧。
- 有必要对缆线进行交叉连接时，要使用规定的接线排、跳线面板和组件。不要在任何位置接合或桥接缆线。
- 使 UTP 缆线尽量远离潜在的电磁干扰源，如电缆、变压器和照明装置。不要将缆线捆系在电线管上或将缆线放在电气装置上。

- 每安装一段线路，一定要用缆线测试仪检测一下。只进行调试是不够的。
- 一定要安装插座，以避免灰尘和污染物落到触点上。插座触点必须正面朝上置于齐平安装板上，或置于表面安装盒的左侧/右侧/下方。
- 一定要留出多余的缆线，整齐盘放在天花板中或最近的隐蔽位置。在工作插座侧至少要留出 1.5 米，在跳线面板侧至少要留出 4.5 米。
- 开始布线前，要确定是采用 568A 还是采用 568B 布线标准。所有的插座和跳线面板布线要采用同一种布线方案。在同一系统中，不要混合使用 568A 和 568B 两种布线标准。
- 一定要遵守所有当地和国家防火和建筑规范。一定要对穿过防火墙的所有缆线采取防火措施。必要时，使用阻燃缆线。

附录 F：Sun 高级键仿真

本地端口 USB 键盘上的击键顺序可以模仿标准 Type 5（美国）Sun 键盘上的某些键。要启用 Sun Advanced Key Emulation 模式并使用这些键，请按住 <Ctrl+Shift+Alt>，然后按 <Scroll Lock> 键。Scroll Lock 发光二极管闪烁。您可以象使用 Sun 键盘上的高级键一样使用下表中指定的键。例如：对于 <Stop + A>，请按住 <Ctrl+Shift+Alt>，并按 <Scroll Lock>，然后按 <F1 + A>。

这些击键组合将与 Dell USB、USB2 和 USB2+CAC SIP 以及 Avocent USB、USB2 和 VMC IQ 模块配合使用。除 <F12> 之外，Microsoft Windows 无法识别这些击键组合。使用 <F12> 执行 Windows 按键。完成后，请按住 <Ctrl+Shift+Alt>，然后按 <Scroll Lock> 键关闭 Sun Advanced Key Emulation 模式。

表 F.1：Sun 键仿真

Compose	应用程序[1]
Compose	小键盘
Power	F11
Open	F7
Help	Num Lock
Props	F3
Front	F5
Stop	F1

Again	F2
Undo	F4
Cut	F10
Copy	F6
Paste	F8
Find	F9
Mute	小键盘 /
Vol.+	小键盘 +
Vol.-	小键盘 -
Command(左) [2]	F12
Command(左) [2]	Win (GUI) 左 [1]
Command(右) [2]	Win (GUI) 右 [1]

尾注：

(1) Windows 95 104 键键盘。

(2) Command 键是 Sun Meta(钻石) 键。

附录 G：技术规格

表 G.1：RCS 技术规格

端口数	1082DS：8 2162DS：16 4322DS：32
类型	Dell PS/2、USB、USB2、USB2+CAC 和串行 SIP。Avocent PS/2、PS2M、USB、Sun、USB2、VMC 和串行模块。
接头	8 针模块 (RJ-45)
同步类型	独立的水平与垂直同步
输入视频分辨率	标准 640 x 480 @ 60 Hz 800 x 600 @ 75 Hz 960 x 700 @ 75 Hz 1024 x 768 @ 75 Hz 1280 x 1024 @ 75 Hz 1600 x 1200 @ 60 Hz 宽屏 800 x 500 @ 60 Hz 1024 x 640 @ 60 Hz 1280 x 800 @ 60 Hz 1440 x 900 @ 60 Hz 1680 x 1050 @ 60 Hz

支持的缆线	最长为 45 米的 4 对 UTP
尺寸	
形态因数	1U 或 0U 机架安装
单位	1.72 x 17.00 x 9.20(高度 x 宽度 x 深度)
重量(不包括缆线)	1082DS：3.0 千克 2162DS：3.2 千克 4322DS：3.4 千克
SETUP 端口	
编号	1
协议	RS-232 串行
连接器	8 针模块 (RJ-45)
本地端口	
数量/类型	1 VGA/4 USB
网络连接	
编号	2
协议	10/100/1000 以太网
连接器	8 针模块 (RJ-45)
USB 设备端口	
编号	4

协议	USB 2.0
MODEM 端口	
编号	1
协议	RS-232 串行
接头	8 针模块 (RJ-45)
PDU 端口	
编号	2
协议	RS-232 串行
连接器	8 针模块 (RJ-45)
电源规格	
接头	1082DS：1 IEC C14 2162DS：2 IEC C14 4322DS：2 IEC C14
类型	内置
电源	18 瓦
散热系数	47 英热/小时
交流输入范围	100 - 240 VAC
AC 频率	50/60 赫兹，自动感应
额定交流输入电流	1.25 安

交流输入功率(最大)	40 瓦
环境大气状况额定值	
温度	工作温度：0 至 50 摄氏度；非工作温度：-20 至 70 摄氏度
湿度	工作湿度：20% 至 80 % 相对湿度(非冷凝非操作：5% 至 95% 相对湿度；最高湿球温度：38.7 摄氏度
安全及 EMC 标准认证和标志	UL/cUL、CE - EU、N (Nemko)、GOST、C-Tick、NOM/NYCE、MIC (KCC)、SASO、TUV-GS、IRAM、 FCC、ICES、VCCI、SoNCAP、SABS、Bellis、FIS/Kvalitet、Koncar、INSM、 Ukrtest、STZ、KUCAS 本产品获得的安全认证和 EMC 认证使用以下一个或多个标记：CMN(证书型号) 、MPN(厂商部件号) 或"销售级别型号"标记。EMC 和/或安全报告及证书中引用的标记打印在产品粘贴的标签上。

附录 H：技术支持

我们的技术支持人员将协助您解决在安装或操作 Dell 产品时遇到的任何问题。如果发生问题，请按下列步骤尽快取得服务。

解决问题：

1 查看此手册中相关的章节，确定此故障是否能通过所列的操作步骤得到解决。

2 访问以下网址搜索知识库或使用在线服务申请表：dell.com/support。

3 给离您最近的 Dell 技术支持点打电话。