CommandCenter Secure Gateway

管理员指南
版本 **5.3**

CCA-0P-v5.3-CHS

2012 年 7 月

255-80-5140-00-0O

FCC 信息

本设备经测试符合 FCC 规则第 15 部分规定的 A 类数字设备限制要求。这些限制旨在合理保护商用安装设备免受有害干扰的影响。本设备产生、使用并辐射射频能量，如果不按说明书安装和使用，可能会对无线通信造成有害干扰。在居民区使用本设备可能会造成有害干扰。

VCCI 信息（日本）

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

事故、灾害、误用、滥用、擅自修改产品或其他不受 Raritan 合理控制的事件造成的产品损坏，或者在非正常工作条件下造成的产品损坏，Raritan 均不承担责任。

目录

CC-SG 管理指南新增内容

根据设备功能增强及设备和/或文档变更情况，修改了 CommandCenter Secure Gateway 管理指南的下列章节，或者增加了相应的信息。

- *设备组数据报告* (p. 228)
- *节点资产报告* (p. 230)
- *备份 **CC-SG*** (p. 236)
- *配置 **IPv4 IP** 故障切换模式或 **IPv6** 双协议堆模式* (p. 258)
- *配置 **IPv4 IP** 隔离模式或 **IPv6** 双协议堆模式* (p. 262)
- ***IPv6** 支持* (p. 264)
- *把 **CC-SG** 主机名注册到 **DNS** 里的 **IP** 地址* (p. 264)
- *日志严重级别示例* (p. 266)
- *配置 **SNMP*** (p. 272)
- ***CC-SG** 群集要求* (p. 275)
- 群集状态定义
- *配置邻居* (p. 279)
- *证书任务* (p. 292)
- *访问控制表* (p. 295)
- *预定任务* (p. 299)
- *启用 **SSH** 访问* (p. 305)
- ***Dominion SX** 串行目标直接端口访问* (p. 313)
- *检查磁盘状态* (p. 357)
- *制作系统快照* (p. 360)
- ***Power IQ** 集成* (p. 362)
- ***E1** 型号设备上的 **LED*** (p. 372)
- ***E1** 型号设备上的声音报警器和红色 **LED*** (p. 373)
- ***CC-SG** 磁盘监视* (p. 401)
- ***Dominion KX2** 双视频端口设置和建议* (p. 405)
- *在 **CC-SG** 上配置和使用双端口视频* (p. 406)
- *利用 **CC-SG** 虚拟设备使用 **VMware** 高可用性或容错* (p. 419)
- *许可常见问题解答* (p. 428)
- *设备信息* (p. 433)

参看版本说明部分详细了解本版本的 CommandCenter Secure Gateway 发生了哪些变化。

Ch 1 简介

CommandCenter Secure Gateway (CC-SG) 管理员指南介绍如何管理和维护 CC-SG。

本指南供那些有所有可用权限的管理员使用。

非管理员用户应该参看 Raritan **CommandCenter Secure Gateway 用户指南**。

在本章内

前提条件

在根据本指南描述的步骤配置 CC-SG 之前，参看 Raritan **CommandCenter Secure Gateway 部署指南**全面了解如何部署 CC-SG 管理的 Raritan 设备。

术语/缩略语

本手册使用下列术语和缩略语：

Access Client — 基于 HTML 的客户机，供那些要访问 CC-SG 管理的节点的普通访问用户使用。Access Client 不允许使用管理功能。

Admin Client — 基于 Java 的 CC-SG 客户机，普通访问用户和管理员均可使用。它是唯一允许执行管理功能的客户机。

关联 — 类别、类别元素与端口和/或设备之间的关系。例如：如果要使“位置”类别与一台设备关联，在 CC-SG 上添加设备和端口之前先创建关联。

类别 — 包含一组值或元素的变量。例如：如果“类别”是“位置”，此类别可能有“纽约市”、“费城”或“数据中心 1”等元素。在把设备和端口添加到 CC-SG 时，使此信息与它们关联。如果在给类别添加设备和端口之前先正确设置关联，会更简单。再比如如果“类别”是“操作系统类型”，此类别可能有 Windows、Unix 或 Linux 等元素。

CIM (Computer Interface Module, 计算机接口模块) — 用于连接目标服务器和 Raritan 设备的硬件。每台目标设备需要一个 CIM，但 Dominion KX101 除外，因为它直接连接目标设备，不需要 CIM。在 CC-SG 上添加设备和配置端口之前，目标服务器应该通电并连接 CIM，CIM 应该连接 Raritan 设备。否则，空 CIM 名称将覆盖 CC-SG 端口名称。在服务器连接 CIM 之后，必须重新启动服务器。

设备组 — 一个用户可以访问的指定设备组。在创建策略时，用设备组控制对设备组里的设备进行的访问。

设备 — CC-SG 管理的 Raritan 产品，例如 Dominion KX、Dominion KX II、Dominion SX、Dominion KSX、IP-Reach、Paragon II System Controller 和配 USTIP 的 Paragon II UMT832。这些设备控制与之相连的目标服务器和系统，也叫做节点。参看 Raritan 支持网站上的 **CC-SG 兼容性指标** 了解支持设备列表。

元素 — 类别的值。例如“纽约市”元素属于“位置”类别，Windows 元素属于“操作系统类型”类别。

幻影端口 — 在管理 Paragon 设备时，如果从系统中去除 CIM 或目标设备，或者（人工或意外）断开其电源，就会出现幻影端口。参看 **Raritan Paragon II 用户指南**。

主机名 — 如果启用 DNS 服务器支持，可以使用主机名。参看*关于网络设置* (p. 257)。

主机名及其全限定域名（FQDN = 主机名 + 后缀）不得超过 257 个字符。主机名由多个部分组成，各个部分之间用英文句点 (.) 分隔开。

每个部分最长 63 个字符，第一个字符必须是字母。其余字符可以是字母、数字或 "-"（连字符或减号）。

每个部分的最后一个字符不能是 "-"。

虽然系统保存输入的大小写字母，但 FQDN 在使用时不区分大小写。

iLO/RILOE 和 iLO2/RILOE2 —CC-SG 可以管理的 HP Integrated Lights Out/Remote Insight Lights Out 服务器。iLO/RILOE 设备的目标可直接通电、断电或重新通电。iLO/RILOE 设备不能被 CC-SG 发现，而是要人工添加为节点。在此指南中,iLO/RILOE 项包括 iLO/RILOE 和 iLO2/RILOE2。

带内访问 — 通过 TCP/IP 网络排除网络目标发生的故障。KVM 和串行设备可以通过下列带内应用程序访问：RemoteDesktop Viewer、SSH Client、RSA Client 和 NC Viewer。

IPMI 服务器（Intelligent Platform Management Interface 智能平台管理接口）— CC-SG 可以控制的服务器。IPMI 既可以自动发现，也可以人工添加。

带外访问 —用 Raritan Remote Console (RRC)、Raritan Console (RC)、Multi-Platform Client (MPC)、Virtual KVM Client (VKC) 或 Active KVM Client (AKC) 等应用程序排除网络里 KVM 或串行网管节点发生的故障。

策略 — 定义 CC-SG 网络内部用户组的访问权。策略应用于用户组，有几个控制参数决定访问日期和时间等控制级别。

节点 — CC-SG 用户可以访问的目标系统，例如服务器、桌面 PC 和其他联网设备。

接口 — 通过 Dominion KX2 连接等带外解决方案或 VNC 服务器等带内解决方案实现的不同的节点访问方式。

节点组 — 一个用户可以访问的指定节点组。在创建策略时，用节点组控制对节点组里的节点进行的访问。

端口 — Raritan 设备和节点之间的连接点。端口仅限于 Raritan 设备端口，标识从此设备到节点的路径。

SASL（Simple Authentication and Security Layer，简单验证和安全层）— 给基于连接的协议增加验证支持所用的方法。

SSH —Putty 或 OpenSSH 等给 CC-SG 提供命令行界面的客户机。CC-SG 命令的子集通过 SSH 管理设备和 CC-SG 自身。

用户组 — 有相同访问权和权限的一组用户。

客户机浏览器要求

如要了解支持的所有浏览器，参看 Raritan 支持网站上的**兼容性指标**。

Ch 2 访问 CC-SG

可以采用几种方法访问 CC-SG：

- 浏览器：CC-SG 支持许多网络浏览器（如要了解支持的所有浏览器，参看 Raritan 支持网站上的**兼容性指标**）。
- 胖客户机：可以在客户计算机上安装 Java Web Start 胖客户机。胖客户机功能非常类似基于浏览器的客户机。
- SSH：通过串行端口连接的远程设备可用 SSH 访问。
- Diagnostic Console（诊断控制台）：只提供紧急维修和诊断，在配置和操作 CC-SG 时不能取代基于浏览器的 GUI。参看 ***诊断控制台*** (p. 319)。

注意：在访问 CC-SG 时，用户可以用浏览器、胖客户机和 SSH 同时建立连接。

在本章内

通过 CC-SG Admin Client 进行基于浏览器的访问

CC-SG Admin Client 是基于 Java 的客户机，根据你的权限提供管理任务和访问任务所需的 GUI。

1. 使用支持的 Internet 浏览器，输入 CC-SG 的 URL，然后输入 /admin：http(s)://*IP address*/admin，例如 ***http://10.0.3.30/admin*** (***https://10.0.3.30/admin***) 或 https://10.0.3.30/admin。

   如果打开 JRE Incompatibility Warning（JRE 不兼容警告）窗口，选择并安装与你的客户计算机相适应的 JRE 版本。在安装 JRE 之后，再试此步骤。参看 **JRE 不兼容** *(p. 6)*。

   也可以继续操作，不安装新版 JRE。

2. 如果显示 Restricted Service Agreement（有限服务协议），请阅读协议文本，然后选择 I Understand and Accept the Restricted Service Agreement（我理解并接受有限服务协议）复选框。
3. 在 Username（用户名）和 Password（密码）字段里分别输入用户名和密码，然后单击 Log In（登录）按钮。
4. 在成功登录之后，打开 CC-SG Admin Client。

JRE 不兼容

如果没有在客户计算机上安装要求的最低版本的 JRE，屏幕显示一条警告消息，不能访问 CC-SG Admin Client。如果 CC-SG 在客户计算机上找不到所需的 JRE 文件，就打开 JRE Incompatibility Warning（JRE 不兼容警告）窗口。

如果打开 JRE Incompatibility Warning（JRE 不兼容警告）窗口，选择并安装与你的客户计算机相适应的 JRE 版本，也可以继续操作，不安装新版 JRE。

在安装 JRE 之后，必须重新启动 CC-SG。

管理员可以配置建议的最低版 JRE，以及 JRE Incompatibility Warning（JRE 不兼容警告）窗口显示的消息。参看***配置定制 JRE 设置*** (p. 271)。

胖客户机访问

CC-SG 胖客户机允许你用 Java Web Start 应用程序连接 CC-SG，而不是通过网络浏览器运行 Applet 来连接 CC-SG。胖客户机的连接速度可能比浏览器快。 运行胖客户机要求的最低 Java 版本是 1.6.0.10。

安装胖客户机

▶ **在 CC-SG 上下载胖客户机：**

注意：如果使用 JRE v1.6.0_20，确保在 Java 控制面板上的 Temporary Internet Files（Internet 临时文件）选项卡上选择 Keep temporary files on my computer（在我的计算机上保存临时文件）。如果不配置此设置，胖客户机不能启动并显示下列消息：不能启动应用程序。

1. 启动网络浏览器，输入下列 URL：`http(s)://<IP_address>/install`，其中 `<IP_address>` 是 CC-SG 的 IP 地址。
   - 如果显示安全警告消息，单击 Start（开始）按钮继续下载。
2. 在下载完成之后显示一个新窗口，你可以在此指定 CC-SG 的 IP 地址。
3. 在 IP to Connect（要连接的 IP）字段里输入你要访问的 CC-SG 设备的 IP 地址。在建立连接之后，可以在 IP to Connect（要连接的 IP）下拉列表上选择此地址。IP 地址存储在桌面上的一个属性文件里。

4. 如果配置 CC-SG 建立安全浏览器连接，必须选择 Secure Socket Layer (SSL) 复选框。如果不配置 CC-SG 建立安全浏览器连接，必须取消 Secure Socket Layer (SSL) 复选框。此设置必须正确无误，否则胖客户机不能连接 CC-SG。
   - 检查 CC-SG 的设置：选择 Administration（管理）> Security（安全）。检查 Encryption（加密）选项卡上的 Browser Connection Protocol（浏览器连接协议）选项。如果选择了 HTTPS/SSL 选项，必须在胖客户机的 IP 地址指定窗口上选择 Secure Socket Layer (SSL) 复选框。如果选择了 HTTP 选项，必须在胖客户机的 IP 地址指定窗口上取消 Secure Socket Layer (SSL) 复选框。
5. 单击 Start（开始）按钮。
   - 如果在机器上使用不支持的 Java Runtime Environment 版本，会显示警告消息。根据提示下载支持的 Java 版本，或者继续使用当前安装的版本。
6. 打开 Login（登录）屏幕。
7. 如果启用 Restricted Service Agreement（有限服务协议），请阅读协议文本，然后选择 I Understand and Accept the Restricted Service Agreement（我理解并接受有限服务协议）复选框。
8. 在 Username（用户名）和 Password（密码）字段里分别输入用户名和密码，然后单击 Login（登录）按钮继续操作。

使用胖客户机

运行胖客户机要求的最低 Java 版本是 1.6.0.10。

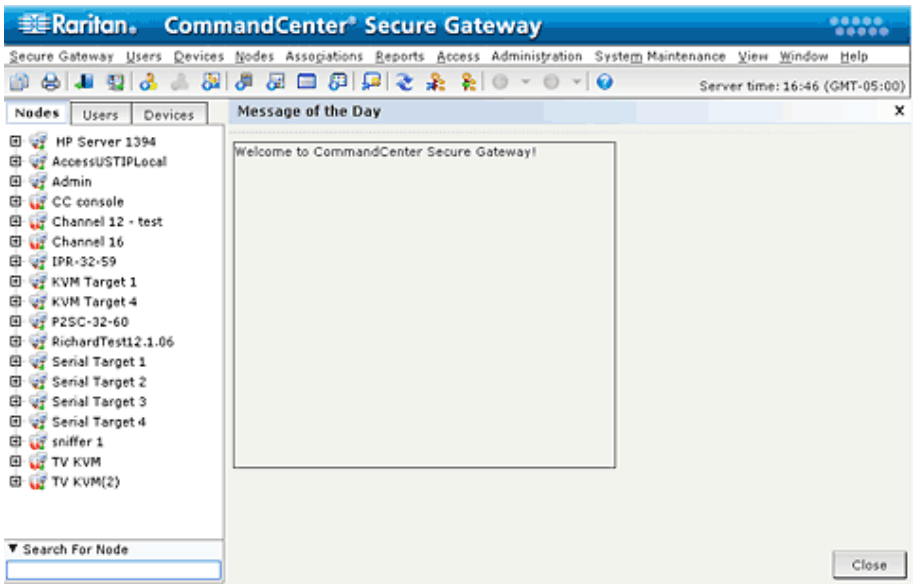
在安装胖客户机之后，可以在客户计算机上采用两种方法访问它。

访问胖客户机：

- 在 Java 控制面板的 Java Application Cache Viewer（Java 应用程序高速缓存查看器）上启动胖客户机。
- 用 Java 控制面板的 Java Application Cache Viewer（Java 应用程序高速缓存查看器）在桌面上安装胖客户机快捷图标。

CC-SG Admin Client

在成功登录之后，打开 CC-SG Admin Client。



Raritan.

- Nodes（节点）选项卡：单击 Nodes（节点）选项卡，树视图显示已知的所有目标节点。单击一个节点，查看 Node Profile（节点配置文件）。接口在父节点下组合在一起。单击 + 号和 - 号展开或折叠树。用右键单击一个接口，然后选择 Connect（连接）选项连接此接口。可以按 Node Name（节点名称 — 字母顺序）或 Node Status（节点状态 — Available (可用)、Busy (忙)、Unavailable (不可用)）排序节点。用右键单击树视图，选择 Node Sorting Options（节点排序选项），然后选择 By Node Name（按节点名称）或 By Node Status（按节点状态）排序节点。
- Users（用户）选项卡：单击 Users（用户）选项卡，树视图显示已注册的所有用户和用户组。单击 + 号和 - 号展开或折叠树。
- Devices（设备）选项卡：单击 Devices（设备）选项卡，树视图显示已知的所有 Raritan 设备。不同的设备类型有不同的图标。端口在父设备下组合在一起。单击 + 号和 - 号展开或折叠树。单击一个端口查看 Port Profile（端口配置文件）。用右键单击一个端口，然后选择 Connect（连接）选项连接此端口。可以按 Port Name（端口名称 — 字母顺序、Port Status（端口状态 — Available [可用]、Busy [忙]、Unavailable [不可用] 或 Port Number（端口编号 — 数字）排序端口。用右键单击树视图，选择 Port Sorting Options（端口排序选项），然后选择 By Node Name（按节点名称）或 By Node Status（按节点状态）排序端口。
- 快捷命令工具栏：此工具栏提供的快捷按钮便于你执行常用命令。
- 操作和配置菜单栏：这些菜单包含操作和配置 CC-SG 所用的命令。可以用右键单击 Nodes（节点）、Users（用户）和 Devices Selection（设备选择）选项卡上的图标，访问其中一些命令。你看到的菜单和菜单项取决于你的用户访问权。
- Server time（服务器时间）：在 CC-SG 的 Configuration Manager（配置管理器）上配置的当前时间和时区。在 Task Manager（任务管理器）上预定任务时，要使用此时间。参看*任务管理器* (p. 297)。此时间可能不同于客户 PC 使用的时间。

Ch 3 入门

必须安装有效许可，才能开始配置并使用 CC-SG。在首次登录之后，应该确认 IP 地址，设置 CC-SG 服务器时间，并检查所安装的固件版本和应用程序版本。可能必须升级固件和应用程序。

在完成首次配置之后，继续进行指导设置。参看***用指导设置配置 CC-SG*** (p. 29)。

在本章内

许可 — 入门 — 新客户和现有客户

必须安装有效许可，才能开始使用 CC-SG 5.0 和更高版本。在安装许可之前，CC-SG 只允许你使用有限功能。参看 ***许可 — 在安装许可之前的有限操作*** (p. 18)。

许可入门：

如果你是 CC-SG 物理设备新客户，参看 ***许可 — 新客户 — 物理设备*** (p. 14)。

如果你是 CC-SG 虚拟设备新客户，参看 ***许可 — 虚拟设备和许可服务器*** (参看 "***许可选择 — 虚拟设备***" p. 17)。

如果你是要升级到 CC-SG 5.0 的现有客户，参看 ***许可 — 现有客户*** (p. 19)。

许可 — 基本许可信息

许可基于在 CC-SG 上配置的节点数。

你购买的物理设备或虚拟设备附带一个可以使用一定数量节点的许可。基本许可启用 CC-SG 功能，包括最多指定节点数量的许可。如果你需要更多节点，还需要给附加节点购买附加许可。如果要使用 WS-API 功能，还需要购买 WS-API 访问附加许可。

物理设备的许可文件和处于非服务器模式（非许可服务器）下的虚拟设备的许可文件与一台特定 CC-SG 设备或 CC-SG 虚拟机的主机 ID 关联。

虚拟设备许可文件与一个特定 CC-SG 许可服务器的主机 ID 关联。

这意味着许可文件并非通用文件。

- 如果你是物理设备新客户，可以在 Raritan Licensing Page（Raritan 许可页）网站下载许可文件。参看 ***许可 — 新客户 — 物理设备*** (p. 14)。
- 如果你是 5.0 之前的现有客户，不必下载许可文件。在把 5.0 之前的 CC-SG 设备升级到 5.0 或更高版本时，把许可文件转换成新格式。根据当前配置的需求，创建、自动安装并注销一个新的基础许可和适用的任何附加许可。参看 ***许可 — 现有客户*** (p. 19)。
- 如果你是 CC-SG 5.3 或更高版本的新虚拟设备客户，应该采用非服务器模式安装虚拟设备，不使用许可服务器。参看 ***许可选择 — 虚拟设备*** (p. 17)。

可用许可

CC-SG 产品	Description（说明）	首次创建许可所需的信息
CC-E1-128	CC-SG E1 设备， 包括 128 个节点的许可	CC-SG 设备的主机 ID
CC-E1-256	CC-SG E1 设备， 包括 256 个节点的许可	CC-SG 设备的主机 ID
CC-E1-512	CC-SG E1 设备， 包括 512 个节点的许可	CC-SG 设备的主机 ID
CC-V1-128	CC-SG V1 设备， 包括 128 个节点的许可	CC-SG 设备的主机 ID
CC-V1-256	CC-SG V1 设备， 包括 256 个节点的许可	CC-SG 设备的主机 ID
CCSG128-VA	CC-SG 虚拟设备， 包括 128 个节点的许可	▪ 非服务器模式： CC-SG 虚拟设备机器的主机 ID ▪ 服务器模式： Windows 许可服务器或 Linux 许可服务器的主机 ID Windows 许可服务器或 Linux 许可服务器的主机名或 IP 地址
CC-2XE1-512	群集套件：两台 CC-SG E1 设备，包括 512 个节点的许可	群集里每台 CC-SG 设备的主机 ID
CC-2XE1-1024	群集套件：两台 CC-SG E1 设备，包括 1024 个节点的许可	群集里每台 CC-SG 设备的主机 ID
CC-2XV1-256	群集套件：两台 CC-SG V1 设备，包括 256 个节点的许可	群集里每台 CC-SG 设备的主机 ID
附加许可	附加节点和 WS-API 等增值服务的许可	CC-SG 设备的主机 ID

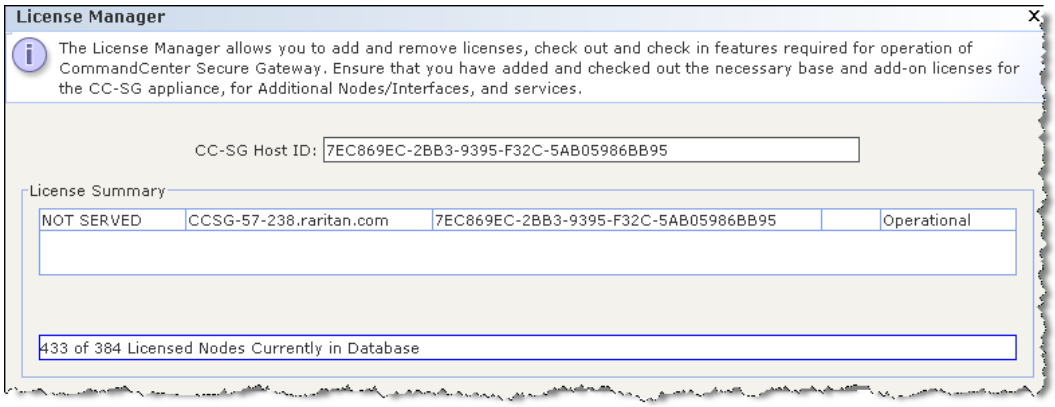
查找数据库保存的主机 ID 和节点数

License Manager（许可管理器）页显示许可信息，包括数据库当前保存的许可节点数。可以在 License Management（许可管理）页上获取主机 ID。在 Raritan 许可门户上创建许可文件时，必须输入 CommandCenter Secure Gateway 主机 ID。参看*许可 — 新客户 — 物理设备* (p. 14)详细了解如何创建新许可文件。

如果在服务器模式下通过许可服务器使用虚拟设备，必须在状态控制台上复制主机 ID。参看*状态控制台* (参看 "*访问状态控制台*" p. 320)。

查看数据库保存的主机 ID 和节点数：

1. 选择 Administration（管理）> License Management（许可管理）。
2. License Management（许可管理）页显示你登录的 CommandCenter Secure Gateway 的主机 ID。可以复制并粘贴主机 ID。 对于在服务器模式下的虚拟 CC-SG，在安装许可服务器之后，License Summary（许可摘要）部分显示主机 ID。对于在服务器模式下和非服务器模式下的 CC-SG，License Manager（许可管理器）页有少许差异。
3. 在本页上检查数据库保存的节点数。可以确定在达到许可极限之前，还能添加多少个节点。

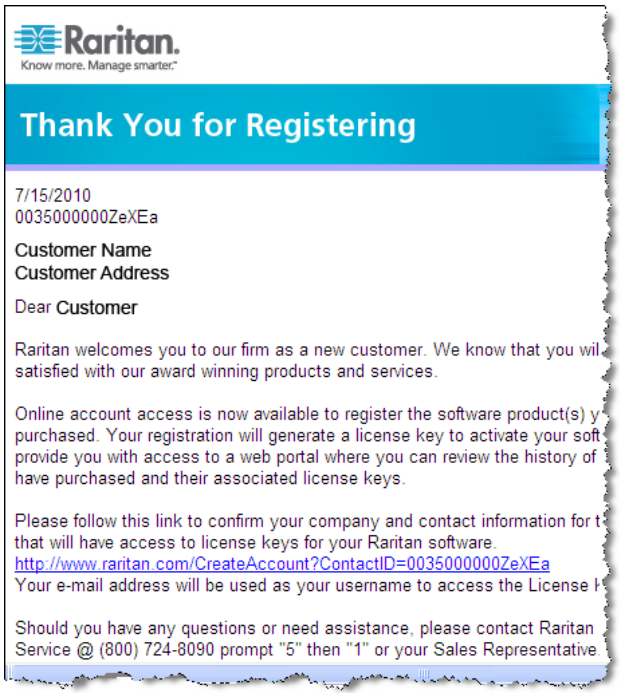


许可 — 新客户 — 物理设备

如果你是刚购买 CC-SG 物理设备的新客户，根据下列步骤确保安装并激活有效许可。

第一步：获得许可：

1. 在购买时指定的许可管理员将收到 Raritan 许可门户通过 licensing@raritan.com 电子邮件地址发来的一封电子邮件，标题为“感谢你注册”。


Raritan.
Know more. Manage smarter.

Thank You for Registering

7/15/2010
0035000000ZeXEa

Customer Name
Customer Address

Dear Customer

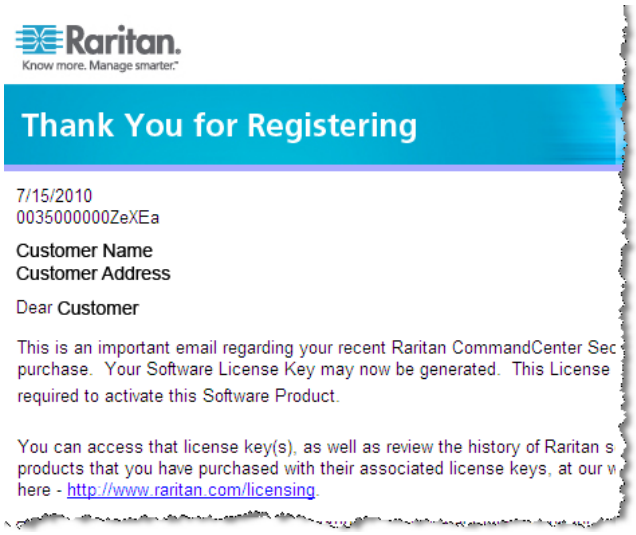
Raritan welcomes you to our firm as a new customer. We know that you wil
satisfied with our award winning products and services.

Online account access is now available to register the software product(s) y
purchased. Your registration will generate a license key to activate your soft
provide you with access to a web portal where you can review the history of
have purchased and their associated license keys.

Please follow this link to confirm your company and contact information for t
that will have access to license keys for your Raritan software.
http://www.raritan.com/CreateAccount?ContactID=0035000000ZeXEa
Your e-mail address will be used as your username to access the License I

Should you have any questions or need assistance, please contact Raritan
Service @ (800) 724-8090 prompt "5" then "1" or your Sales Representative

2. 单击电子邮件上的链接打开 Raritan 网站上的 Software License Key Login（软件许可密钥登录）页。创建一个用户帐号和登录名。用户名是电子邮件地址 。打开 Licensing Account Information（许可帐号信息）页。可以短暂使用许可文件。
3. 查看电子邮件邮箱，阅读 Raritan 许可门户通过 licensing@raritan.com 电子邮件地址发来的另一封电子邮件，标题为“你可以使用 Raritan Commandcenter SG 软件许可密钥了”。


Raritan.
Know more. Manage smarter.

Thank You for Registering

7/15/2010
0035000000ZeXEa

Customer Name
Customer Address

Dear Customer

This is an important email regarding your recent Raritan CommandCenter Sec
purchase. Your Software License Key may now be generated. This License
required to activate this Software Product.

You can access that license key(s), as well as review the history of Raritan s
products that you have purchased with their associated license keys, at our w
here - http://www.raritan.com/licensing.

4. 单击电子邮件上的链接打开 Raritan 网站上的 Software License Key Login（软件许可密钥登录）页，用刚才创建的用户帐号登录。
5. 单击 Product License（产品许可）选项卡。列表显示你购买的许可。你可能只有一份许可，也可能有多份许可。 参看*可用许可* (p. 11)。
6. 如要获取每个许可，单击列表上的项目旁边的 Create（创建）链接，输入 CommandCenter Secure Gateway Host ID（主机 ID）。可以复制 License Management（许可管理）页上的主机 ID 并粘贴在这里。参看*查找数据库保存的主机 ID 和节点数* (p. 13)。
7. 单击 Create License（创建许可）按钮，弹出窗口显示你输入的详细信息。确认主机 ID 是否正确。

警告：确保主机 ID 正确无误！用错误主机 ID 创建的许可无效，需要 Raritan 技术支持团队协助才能解决问题。

8. 单击 OK（确定）按钮创建许可文件。
9. 单击 Download Now（现在下载）按钮保存许可文件。

第二步：安装许可

1. 选择 Administration（管理）> License Management（许可管理）。
2. 单击 Add License（添加许可）按钮。
3. 阅读许可协议，向下翻页阅读全文，然后选择 I Agree（我接受）复选框。

第三步：注销你要激活的许可

必须注销许可，才能激活功能。

- 在列表上选择一个许可，然后单击 Check Out（注销）按钮。注销你要激活的所有许可。

许可 — 群集 — 新客户

群集套件许可允许两台 CC-SG 物理设备作为群集工作并共享许可。在创建并使用群集、在主群集节点上安装并注销许可之前，本系统允许有限操作。群集里的 CC-SG 设备可以暂时作为独立设备工作，便于单独维护每台设备。必须让两台 CC-SG 设备重新加入群集，才能发挥全部功能。虚拟设备不支持群集。

*注意：如果独立宽限期到期，在 CC-SG 重新加入群集之前，它的工作很有限。参看***许可 — 在安装许可之前的有限操作** *(p. 18)*。

在 Raritan 许可门户上创建群集许可文件时，必须输入每台 CC-SG 的主机 ID。在每台 CC-SG 设备的 Administration（管理）> License Management（许可管理）页上查找这些主机 ID 号。

用群集套件许可部署 CC-SG 群集：

参看***配置 CC-SG 群集*** (p. 275)详细了解 CC-SG 群集。

1. 把两台 CC-SG 设备作为群集部署。参看 CC-SG 快速安装指南详细了解如何部署。
2. 查找每台 CC-SG 设备的主机 ID。参看***查找数据库保存的主机 ID 和节点数*** (p. 13)。
3. 获取群集套件许可文件。参看***许可 — 新客户 — 物理设备*** (p. 14)。
4. 创建群集。参看***创建群集*** (p. 276)。
5. 在群集主节点上安装许可文件。在创建群集时，把此文件复制备用节点上。参看***许可 — 新客户 — 物理设备*** (p. 14)详细了解如何安装许可文件。
6. 注销你要激活的许可。确保注销群集套件许可。参看***许可 — 新客户 — 物理设备*** (p. 14)。

许可选择 — 虚拟设备

CC-SG 虚拟设备既可以在服务器模式下利用物理许可服务器或虚拟机许可服务器运行，也可以在非服务器模式下利用与 CC-SG 虚拟设备所在的虚拟机绑定在一起的许可运行。在非服务器模式下，不需要许可服务器。

Raritan 建议所有新安装的虚拟设备采用更为简单的非服务器模式。非服务器模式要求你安装 CC-SG 5.3 和更高版本。不需要改动此前安装的虚拟设备和服务器许可，除非要把它变成非服务器模式。由于要取消配置中的许可服务器，所以必须在 Raritan 许可门户上重新生成新许可。联系 Raritan 技术支持部门寻求协助。

如要详细了解每种安装，下载快速安装指南了解你要使用的许可模式。

访问 www.raritan.com，然后单击支持>固件和文档> CommandCenter Secure Gateway。单击要使用的 CC-SG 版本下面的快速安装指南，然后选择所需的快速安装指南。

- CC-SG 虚拟设备快速安装指南 — 非许可服务器
- CC-SG 虚拟设备和 lmadmin 许可服务器管理快速安装指南
- CC-SG 虚拟设备和 lmgrd 许可服务器管理快速安装指南

注意：可以用两个许可服务器管理器中的任何一个管理许可服务器：lmgrd 或 lmadmin。Flexera lmgrd 是许可服务器命令行管理工具。Flexera lmadmin 是许可服务器图形用户界面管理应用程序，既可以在许可服务器上远程访问它，也可以在本地访问它。必须选择一个管理器，且只安装此管理器。不能同时使用两个管理器。

参看 Flexera™ FlexNet Publisher® 文档详细了解如何管理许可服务器。可以在 www.flexera.com 网站的 Support（支持）> Documentation Center（文档中心）下载 FlexNet Publisher Licensing Toolkit 11.8 的 FlexNet Publisher License Administration Guide（FlexNet Publisher 许可管理指南）。

安装或升级 VMware 工具

VMware 工具是 VMware 推荐的虚拟机部署工具。在 CommandCenter Secure Gateway 虚拟设备上安装 VMware 工具之后，可以在 VMware 发布新版本时根据此步骤升级 VMware 工具。

CC-SG OVF 虚拟软件包默认安装一个版本的 VMware 工具。

▶ 安装或升级 VMware 工具：

1. 登录 vSphere 客户机，然后连接 CC-SG 虚拟设备所在的 ESX 主机。

2. 选择虚拟机，然后单击 Console（控制台）选项卡，打开 Diagnostic Console（诊断控制台）。
3. 用右键单击虚拟机，然后选择 Guest（访客）> Install/Upgrade VMware Tools（安装/升级 VMware 工具）。选择 Interactive Tools Upgrade（互动工具升级），然后单击 OK（确定）按钮把文件加载到虚拟机上供 CC-SG 进行安装。
4. 打开浏览器，登录 Admin Client。
5. 选择 System Maintenance（系统维护）> Install/Upgrade VMware Tools（安装/升级 VMware 工具）。在安装结束之后，显示安装成功消息。

配置虚拟设备和存储服务器备份和快照

在部署 CC-SG 虚拟设备之后，确保通过 VMware® 配置虚拟设备备份，以及虚拟设备所用的存储服务器的备份。

还应该通过 VMware 启用快照。

参看 http://www.vmware.com/support/pubs/vs_pubs.html 上的 VMware 文档详细了解如何配置这些功能。

虚拟设备和远程存储服务器

如果 CC-SG 虚拟设备用远程服务器存储文件，但存储设备连接断了，在存储服务器恢复正常工作之前可能无法访问 CC-SG。系统可能显示 Problems Retrieving Configuration Data（在检索配置数据时出问题）错误消息。

许可 — 在安装许可之前的有限操作

在安装并注销相应许可之前，CC-SG 的工作很有限。只启用下列菜单项。

- Diagnostic Console（诊断控制台）：获取必要信息和日志，配置网络接口。

注意：可以通过 VGA/键盘/鼠标端口（如适用）、串行端口（如适用）或 SSH 访问管理员控制台接口和状态控制台界面。在启用状态控制台界面之后，也可以通过 Web 界面访问它。

- Change Password（更改密码）
- Secure Gateway（安全网关）：查看当日消息、打印、打印屏幕、注销和退出。
- Administration（管理）> Cluster Configuration（群集配置）：配置群集，给群集节点指定角色。创建群集，是在群集许可下工作的必要条件。只有物理设备支持群集。
- Administration（管理）> License Manager（许可证管理器）：允许上载和删除许可文件、许可注销和注册。
- System Maintenance（系统维护）：启用下列菜单项。
  - Restore（恢复）：允许你在错误复位并删除许可之后，把许可恢复到 CC-SG。
  - Maintenance Mode（维护模式）：必要时进入和退出维护模式，从而创建群集或进行升级。
  - Restart（重新启动）
  - Upgrade（升级）
  - Shutdown（关机）
- View（查看）
- Help（帮助）：查看联机帮助文档。

许可 — 现有客户

如果你是现有的 CC-SG 物理设备客户，在把 CC-SG 设备升级到 5.0 或更高版本时，创建并安装一个许可文件，它允许你继续对在升级时配置的节点数量使用 CC-SG。

所有现有客户必须先升级到 5.0，才能升级到比 5.0 高的任何版本。

在升级到 5.0 之后，根据本节所述的步骤确认是否安装了许可文件。

第一步：升级到 5.0：

参看*升级 **CC-SG*** (p. 244)。

第二步：查看许可文件：

1. 在 Admin Client 上选择 Administration（管理）> License Management（许可管理），打开 License Manager（许可管理器）页。
   - License Summary（许可摘要）部分显示高级许可信息。可以查看与许可文件关联的 CC-SG 主机 ID。
   - 页面中央列出正在使用的节点数和允许的节点数。

注意：假如你发现允许的节点数小于当初购买许可时指定的节点数，请联系 Raritan 销售人员。

许可 — 移植

物理设备许可与一台特定 CC-SG 设备关联。在服务器模式下部署的虚拟设备许可和许可服务器与一个特定许可服务器关联。在非服务器模式下部署的虚拟设备许可不使用许可服务器，与 CC-SG 虚拟机关联。

如果这些条件发生变化，给许可文件指定错误的主机 ID，要取消许可服务器过渡到非服务器模式，或者发生许可文件与 CC-SG 系统不匹配的任何情况，必须获取使用正确主机 ID 的新许可文件。

▶ **获取使用不同主机 ID 的新许可文件：**

联系 Raritan 技术支持部门。参看***技术支持联系人*** (p. 2)。

添加许可

如果你购买附加许可，或者必须更换许可，可以把许可添加到 CC-SG。

在更换许可时，先添加基本许可。如果与旧版基本许可关联的附加许可对新基本许可无效，例如它们是不同类型的许可（单机或群集），或者主机 ID 不相同，将自动删除这些附加许可。

参看***许可常见问题解答*** (p. 428)了解完整的许可更换规则。

▶ **添加许可：**

1. 选择 Administration（管理）> License Management（许可管理）。
2. 单击 Add License（添加许可）按钮。
3. 阅读许可协议，向下翻页阅读全文，然后选择 I Agree（我接受）复选框。
4. 单击 Browse（浏览）按钮选择许可文件。
5. 单击 Open（打开）按钮。

   注意：如果你使用许可服务器，CC-SG 将连接许可服务器，并显示在许可服务器上找到的完整功能列表。
6. 选择要激活的功能，然后单击 Check Out（注销）按钮。

确认 IP 地址

1. 选择 Administration（管理）> Configuration（配置）。

2. 单击 Network Setup（网络设置）选项卡。
3. 检查网络设置是否正确，必要时更改设置。参看***关于网络设置*** (p. 257)。**可选。**
4. 单击 Update Configuration（更新配置）按钮提交更改。
5. 单击 Restart Now（现在重新启动）按钮确认设置，重新启动 CC-SG。

许可服务器通信

必须让 CC-SG 虚拟设备和许可服务器保持连接。CC-SG 用此连接确保许可服务器正常工作，确定哪些许可文件可用，何时注册和注销许可。

访问许可

必须始终可以使用许可服务器上已注销的所有许可。如果在许可服务器上移动或删除一个许可文件，CC-SG 在轮询许可服务器时不能确认此许可。如果 CC-SG 在许可服务器上找不到一个已被注销的许可，就停止访问此许可。

为了防止不能访问许可，在许可服务器上移动或删除此许可之前始终要先注册它。

许可服务器断电

如果 CC-SG 不能连接许可服务器，许可仍然有 30 天宽限期。每次登录 CC-SG 时，系统显示一条消息，提醒你在恢复许可服务器连接之前还剩下的可访问天数。

如果在 30 天宽限期后仍然没有恢复许可服务器连接，将注册已被注销的许可，CC-SG 停止访问许可服务器，你只能使用 CC-SG 的部分功能。参看***许可 — 在安装许可之前的有限操作*** (p. 18)。

在许可服务器恢复工作之后，必须再次注销每个许可才能恢复正常工作状态。参看安装和注销许可。

作为服务运行许可服务器管理器

建议你把许可服务器管理器作为服务安装，每当操作系统重新启动时，它都自动启动。

lmadmin 安装详细信息：

在 Windows 机器上安装 lmadmin 时，选择 Run as Service（作为服务运行）复选框启用此配置。在 UNIX 机器上安装 lmadmin 时，参看 FlexNet Publisher 许可管理指南中的**把 lmadmin 许可服务器管理器作为操作系统服务安装**了解此配置。

lmgrd 安装详细信息：

在 Linux 机器上应该把 lmgrd 许可服务器管理器配置为自动启动，在 Windows 机器上把 lmgrd 许可服务器管理器配置为自动启动的服务。

参看 FlexNet Publisher 许可管理指南了解详情：

- 在 UNIX 平台上启动许可服务器管理器，自动启动
- 在 Windows 上启动许可服务器管理器
- 把许可服务器管理器配置为 Windows 服务

在断电之后重新启动许可服务器

如果不作为服务安装许可服务器管理器，当服务器启动时，它不自动启动，你要在断电后重新启动服务器。例如：如果许可服务器在停机后恢复工作状态，或者你移动、添加或删除许可文件，应该重新启动许可服务器。

重新启动许可服务器可以确保 CC-SG 始终同步最新配置。

注意：Windows 许可服务器自动在断电之后进行同步。Linux 在两小时超时之后同步，但在断电之后重新启动它可以立刻进行同步。

用 lmgrd 重新启动许可服务器：

- 运行 `lmdown` 命令正常关闭许可服务器。

用 lmadmin 重新启动许可服务器：

- 参看 FlexNet Publisher 许可管理指南。

用于管理许可服务器的 lmgrd 命令行工具

在安装 lmgrd 许可服务器软件时，安装下列工具。可以在命令行上执行每个工具管理许可服务器。

例如把这些项目值放在尖括号里。

<feature name> 是 Admin Client Administration（管理）> License Manager(许可管理器)页上 Feature(功能)列里的值，例如 CCSG128-VA 是虚拟设备基本许可的功能名称。

<license file name> 是在许可服务器上安装和保存的许可文件的文件名。

参看 Flexera™ FlexNet Publisher® 文档详细了解如何管理许可服务器。可以在 www.flexera.com 网站的 Support（支持）> Documentation Center（文档中心）下载 FlexNet Publisher Licensing Toolkit 11.8 的 FlexNet Publisher License Administration Guide（FlexNet Publisher 许可管理指南）。

命令	Description（说明）
lmborrow	允许用户注销功能，在断开网络连接的情况下在指定的期限内借用功能。
lmdiag	允许用户在不能注销功能的情况下诊断问题。系统将尝试注销功能，并说明尝试成功还是失败。 `lmdiag -c <license file name> <feature name> -n`
lmdown	便于正常关闭所选的许可后台进程。 `lmdown -vendor raritan` 用于关闭 Raritan 供应商后台进程。
lmhostid	允许用户获取当前平台的主机 ID。 包括 –uuid 和 –hostdomain 或 –internet 自变量。
lminstall	允许在可阅读的文本格式和十进制格式之间转换许可。
lmnewlog	把现有报告日志信息移动到新文件里，创建一个与原报告日志文件同名的报告。
lmpath	添加、覆盖或获取当前许可路径设置。

命令	Description（说明）
lmremove	删除指定功能的单用户许可。 可以配置许可服务器管理器，防止他人擅自执行 lmremove。
lmreread	`lmreread -vendor raritan` 用于让 Raritan 供应商后台进程重新读取许可文件和选项文件。
lmswitchr	关闭现有报告日志，用新文件名创建一个新报告日志。 如果已经有一个报告日志文件，还可以用它创建一个新报告日志文件。
lmswitch	关闭现有的供应商后台进程调试日志，用新文件名创建一个新的供应商后台进程调试日志。 如果已经有一个供应商后台进程写入的调试日志文件，还可以用它创建一个新调试日志文件。
lmstat	检索许可服务器并显示许可文件状态、功能可用性和使用信息。 `lmstat -c <license file name> -f <feature name>`
lmver	报告 FLEXnet Publisher 库或二进制文件的版本，例如 lmgrd、lmadmin、lmdown 和供应商后台进程。

登录诊断控制台设置 CC-SG IP 地址

1. 用 *admin/raritan* 登录。用户名和密码区分大小写。
2. 系统提示你更改 Local Console 密码。
   a. 再次输入默认密码 (*raritan*)。
   b. 输入新密码，然后确认（再次输入）新密码。新密码必须是强密码，至少由八个字母和数字字符组成。
3. 在显示欢迎页面时，按 CTRL+X。

4. 选择 Operation（操作）> Network Interfaces（网络接口）> Network Interface Config（网络接口配置），打开 Administrator Console（管理员控制台）。
5. 在 Configuration（配置）字段里选择 DHCP 或 Static（静态）。如果选择 Static（静态），输入静态 IP 地址。必要时指定 DNS 服务器、网络掩码和网关地址。
6. 选择 Save（保存）按钮。稍等几分钟让 CC-SG 重新启动。

默认 CC-SG 设置

IP 地址：192.168.0.192

子网掩码：255.255.255.0

用户名/密码：admin/raritan

登录 CC-SG

1. 启动支持的浏览器，然后输入 CC-SG 的 URL：https://<IP address>/admin。

   例如 https://192.168.0.192/admin。

   注意：浏览器连接默认设置是 HTTPS/SSL 加密。

2. 在显示安全警告窗口时，接受连接。
3. 如果你使用不支持的 Java Runtime Environment 版本，将会显示警告。根据提示下载正确版本，或者继续操作。打开 Login（登录）窗口。
4. 输入默认用户名 (*admin*) 和默然密码 (*raritan*)，然后单击 Login（登录）按钮。

   打开 CC-SG Admin Client。

设置 CC-SG 服务器时间

必须准确维护 CC-SG 的时间和日期，从而提高设备管理功能的可信度。

重要说明 :在任务管理器上预定任务时，要使用 Time/Date configuration（时间/日期配置）。参看*任务管理器* (p. 297)。在客户 PC 上设置的时间可能不同于在 CC-SG 上设置的时间。

只有 CC 超级用户和拥有类似权限的用户才能配置时间和日期。

在群集配置下，禁止更改时区。

配置 CC-SG 服务器时间和日期：

1. 选择 Administration（管理）> Configuration（配置）。
2. 单击 Time/Date（时间/日期）选项卡。
   a. 人工设置日期和时间：
   - Date（日期）— 单击下拉箭头选择 Month（月），用上下箭头选择 Year（年），然后在日历表上选择 Day（日）。
   - Time（时间）— 用上下箭头设置 Hour（时、Minutes（分）和 Seconds(秒)，然后单击 Time zone(时区)下拉箭头选择 CC-SG 所在的时区。

   a. 通过 NTP 设置日期和时间：选择窗口底部的 Enable Network Time Protocol(启用网络时间协议)复选框，然后在 Primary NTP server（主 NTP 服务器）和 Secondary NTP server（备用 NTP 服务器）字段里输入相应的 IP 地址。

   注意：网络时间协议 (Network Time Protocol, NTP) 是使相连计算机的日期数据和时间数据与 NTP 基准服务器的数据实现同步所用的协议。在用给 CC-SG 配置 NTP 之后，可以使 CC-SG 的时钟时间与公共 NTP 基准服务器同步，维持正确一致的时间。
3. 单击 Update Configuration(更新配置)按钮把时间和日期更改应用于 CC-SG。
4. 单击 Refresh（刷新）按钮，Current Time（当前时间）字段重新加载新服务器时间。

选择 System Maintenance（系统维护）> Restart（重新启动），重新启动 CC-SG。

检查兼容性指标

兼容性指标列出与 CC-SG 当前版本兼容的 Raritan 设备固件版本和应用程序软件版本。在添加设备、升级设备固件或选择要使用的应用程序时，CC-SG 都要针对这些数据检查版本。如果固件版本或软件版本不兼容，CC-SG 显示警告消息，不能继续操作。每个 CC-SG 版本仅支持在发布时已有 Raritan 设备的当前/旧的固件版本。可以查看 Raritan 支持网站上的兼容性指标。

检查兼容性指标：

- 选择 Administration（管理）> Compatibility Matrix（兼容性指标）。

检查和升级应用程序版本

检查和升级包括 Raritan Console (RC) 和 Raritan Remote Client (RRC) 在内的 CC-SG 应用程序。

检查应用程序版本：

1. 选择 Administration（管理）> Applications（应用程序）。
2. 在 Application（应用程序）列表上选择应用程序名称。注意 Version（版本）字段里的数字。某些应用程序不自动显示版本号。

升级应用程序：

如果应用程序不是最新版，必须升级应用程序。可以在 Raritan 网站上下载应用程序升级文件。如要了解支持的应用程序版本的完整列表，参看 Raritan 支持网站上的**兼容性指标**。

在升级 CC-SG 之前，最好进入 Maintenance Mode（维护模式）。参看 *进入维护模式* (p. 235)。

1. 把应用程序文件保存到客户 PC 上。
2. 单击 Application name（应用程序名称）下拉箭头，然后在列表上选择必须升级的应用程序。如果看不到要升级的应用程序，必须先添加此应用程序。参看*添加应用程序* (p. 254)。
3. 单击 Browse（浏览）按钮在显示的对话框上选择应用程序，然后单击 Open（打开）按钮。
4. Application Manager（应用程序管理器）屏幕上的 New Application File（新应用程序文件）字段显示应用程序名称。
5. 单击 Upload（上载）按钮。进度窗口显示新应用程序上载进度。在上载完成之后打开一个新窗口，说明应用程序已被添加到 CC-SG 数据库里，可以使用了。

6. 如果 Version（版本）字段不自动更新版本号，在 Version（版本）字段里输入新版本号。对于某些应用程序，Version（版本）字段自动更新版本号。
7. 单击 Update（更新）按钮。

*注意：在升级过程中登录的用户必须先退出 CC-SG，然后再登录，确保启动新版应用程序。同时参看***在升级之后打开旧版应用程序** *(p. 253)*。

Ch 4 用指导设置配置 CC-SG

在完成网络配置之后，指导设置就提供一种简单方法完成首次 CC-SG 配置任务。指导设置界面提示你定义关联，发现设备并添加到 CC-SG，创建设备组和节点组，创建用户组，给用户组指定策略和权限，以及添加用户。在完成指导设置之后，随时可以逐个编辑配置。

指导设置分为四个任务：

- 关联 — 定义组织管理设备所用的类别和元素。参看*指导设置中的关联* (p. 29)。
- 设备设置 — 发现网络设备并把它们添加到 CC-SG。配置设备端口。参看*设备设置* (p. 30)。
- 创建设备组 — 把 CC-SG 管理的设备和节点分成组，给每个组创建完整访问策略。参看*创建设备组* (p. 32)。
- 用户管理 — 把用户和用户组添加到 CC-SG，然后选择 CC-SG 用户访问设备和节点所用的策略和权限。参看*用户管理* (p. 35)。

参看*命名常规* (p. 431)详细了解 CC-SG 的名称长度规则。

在本章内

在使用指导设置之前

在继续进行 CC-SG 配置之前，必须先完成系统配置。

- 配置和安装 Dominion 系列和 IP-Reach 设备（串行设备和 KVM 设备），包括分配 IP 地址。

指导设置中的关联

创建类别和元素

▶ **在指导设置上创建类别和元素：**

1. 在 Guided Setup（指导设置）窗口上单击 Associations（关联），然后单击左面板上的 Create Categories（创建类别）打开 Create Categories（创建类别）面板。

2. 在 Category Name（类别名称）字段里输入你希望设备所属的类别的名称，例如 Location（位置）。
3. 在 Applicable for（适用于）字段里说明你希望此类别可用于设备和/或节点。单击 Applicable for（适用于）下拉菜单，然后在列表上选择一个值。
4. 在 Elements（元素）表上输入此类别中一个元素的名称，例如 Raritan US。
   - 单击 Add New Row（添加新行）图标  ，然后在 Elements（元素）表上添加更多行。
   - 如要删除一个元素，选择它所在的行，然后单击 Delete Row（删除行）图标  。
5. 重复这些步骤，直到把此类别的所有元素添加到 Elements（元素）表上为止。
6. 如要创建另一个类别，单击 Apply（应用）按钮保存此类别，然后重复本节中的步骤添加其他类别。**可选**
7. 在创建类别和元素之后，单击 OK（确定）按钮。Association Summary（关联摘要）面板显示你创建的类别和元素的列表。
8. 单击 Continue（继续）按钮开始下一个任务，即设备设置。根据下一节所述的步骤操作。

设备设置

指导设置的第二个任务是设备设置。设备设置允许你搜索和发现网络设备，把它们添加到 CC-SG。在添加设备时，可以根据类别选择一个与设备关联的元素。

重要说明：在 CC-SG 配置过程中，要确保没有其他用户登录设备。

发现和添加设备

在关联任务结束时，单击 Continue（继续）按钮打开 Discover Devices（发现设备）面板。也可以单击 Device Setup（设备设置），然后单击左面板显示的 Guided Tasks（指导任务）树视图上的 Discover Devices（发现设备）打开 Discover Devices（发现设备）面板。

参看*发现和添加 IPv6 网络设备* (p. 48)详细了解支持的设备，以及如何添加设备。

在指导设置上发现和添加设备：

1. 在 From address（开始地址）和 To address（结束地址）字段里输入要搜索哪个 IP 地址范围内的设备。
2. 在 Device types（设备类型）列表上选择要搜索指定范围内哪个类型的设备。按住 Ctrl 单击设备类型选择多个设备类型。
3. 如果搜索 CC-SG 所在的同一个子网上的设备，选择 Broadcast discovery（广播发现）复选框。取消 Broadcast discovery（广播发现）复选框，发现所有子网上的设备。
4. 单击 Discover（发现）按钮。
5. 如果 CC-SG 在指定的地址范围内发现指定类型的设备，Discover Devices（发现设备）面板下半部的表显示这些设备。单击面板顶部的黑箭头隐藏上半部，从而扩大面板下半部显示的发现结果视图。
6. In the table of discovered devices, select the device you want to add to CC-SG, and then click Add. The Add Device panel opens.对于要添加的不同设备类型，Add Device（添加设备）面板略有不同。
7. 在 Device name（设备名称）和 Description（说明）字段里输入新信息，即可更改设备名称和说明。
8. 确定 Device IP or Hostname（设备 IP 或主机名）字段是否显示你在准备把设备添加到 CC-SG 时指定的 IP 地址，必要时在此字段里输入正确地址。
9. 根据设备类型自动填充 TCP Port Number（TCP 端口号）字段。
10. 在 Username（用户名）和 Password（密码）字段里输入你在准备把设备添加到 CC-SG 时创建的用户名和密码。
11. 在 Heartbeat timeout（检测信号超时）字段里输入设备和 CC-SG 之间的超时秒数。
12. 如果要添加 Dominion SX 或 Dominion KXII v2.2 或更高版本的设备，并且允许对此设备进行本地访问，选择 Allow Direct Device Access（允许直接设备访问）复选框。如果不允许对此设备进行本地访问，取消 Local access: Allowed（本地访问：允许）复选框。

13. 如果要人工添加电源条设备，单击 Number of ports（端口数）下拉箭头，然后选择电源条出口数。
14. 如果要添加 IPMI 服务器，在 Interval（时间间隔）字段里输入可用性检查间隔时间，在 Authentication Method（验证方法）字段里输入验证方法，与在 IPMI 服务器上配置的验证方法相同。
15. 如果要配置设备的所有可用端口，选择 Configure all ports（配置所有端口）复选框。CC-SG 把设备的所有端口添加到 CC-SG，给每个端口创建一个节点。
16. 在面板下半部的 Device Associations（设备关联）部分，单击与你要给此设备指定的每个类别相对应的 Element（元素）列上的下拉箭头，然后在列表上选择要与此设备关联的元素。

    注意：有多个同类元素的节点或设备，将根据类别和元素在定制视图上出现多次。
17. 如果要把此元素应用于此设备和与之相连的节点，选择 Apply to Nodes（应用于节点）复选框。
18. 如果要添加另一台设备，单击 Apply（应用）按钮保存此设备，然后重复上述步骤。**可选。**
19. 在添加设备之后，单击 OK（确定）按钮。Device Summary（设备摘要）面板显示你添加的设备的列表。
20. 单击 Continue（继续）按钮开始下一个任务，即创建设备组。根据下一节所述的步骤操作。

创建设备组

指导设置的第三个任务是创建设备组。创建设备组允许你定义设备组和节点组，指定每个组包括的一组设备或节点。管理员可以按组管理相似的设备和节点，而不是逐个管理每个设备或节点，这样可以节省时间。

添加设备组和节点组

▶ **在指导设置上添加设备组和节点组：**

1. 在设备设置任务结束时，单击 Continue（继续）按钮打开 Devices Groups: New（设备组：新建）面板。也可以单击 Create Groups（创建设备组），然后单击左面板显示的 Guided Tasks（指导任务）树视图上的 Add Device Groups(添加设备组)打开 Devices Groups: New（设备组：新建）面板。
2. 在 Group Name（设备组名称）字段里输入要创建的设备组的名称。

3. 可以采用两种方法把设备添加到设备组：Select Devices（选择设备）和 Describe Devices（描述设备）。Select Devices（选择设备）选项卡允许你在可用设备列表上选择设备，从而选择要给设备组指定哪些设备。Describe Devices（描述设备）选项卡允许你指定设备描述规则，参数符合这些规则的设备将被添加到设备组里。

   - **选择设备**

   a. 单击 Device Group: New（设备组：新建）选项卡上的 Select Devices（选择设备）选项卡。

   b. 在 Available（可用）列表上选择要添加到设备组里的设备，然后单击 Add（添加）按钮把它移动到 Selected（选择）列表上。Selected（选择）列表上的设备将被添加到设备组里。

   c. 如要删除设备组里的一个设备，在 Selected（选择）列表上选择设备名称，然后单击 Remove（删除）按钮。

   d. 可以在 Available（可用）或 Selected（选择）列表上搜索设备。在列表下面的字段里输入搜索词，然后单击 Go（搜索）按钮。

   - **描述设备**

   a. 单击 Device Group: New（设备组：新建）面板上的 Describe Devices（描述设备）选项卡。在 Describe Devices（描述设备）选项卡上创建一个规则表，描述要给设备组指定的设备。

   b. 单击 Add New Row（添加新行）图标  在表上添加一行。

   c. 双击给每一列创建的单元格激活下拉菜单。在每个列表上选择要使用的规则部件。

4. 如果要给此设备组创建一个策略，允许用户随时凭借控制权限访问此设备组里的所有节点和设备，选择 Create Full Access Policy for Group（创建设备组全访问策略）复选框。

5. 如要添加另一个设备组，单击 Apply（应用）按钮保存此设备组，然后重复上述步骤。**可选。**

6. 在添加设备组之后，单击 OK（确定）按钮打开 Nodes Group: New（节点组：新建）面板。也可以单击 Create Groups（创建设备组），然后单击左面板显示的 Guided Tasks（指导任务）树视图上的 Add Node Groups（添加节点组）打开 Node Groups: New（节点组：新建）面板。

7. 在 Group name（节点组名称）字段里输入要创建的节点组的名称。

8. 可以采用两种方法把节点添加到节点组：Select Nodes（选择节点）和 Describe Nodes（描述节点）。Select Nodes（选择节点）部分允许你在可用节点列表上选择节点，从而选择要给节点组指定哪些节点。Describe Nodes（描述节点）部分允许你指定节点描述规则，参数符合这些规则的节点将被添加到节点组里。

   - **选择节点**

   a. 单击 Node Group: New（节点组：新建）面板上的 Select Nodes（选择节点）选项卡。

   b. 在 Available（可用）列表上选择要添加到节点组里的节点，然后单击 Add（添加）按钮把它移动到 Selected（选择）列表上。Selected（选择）列表上的节点将被添加到节点组里。

   c. 如要删除节点组里的一个节点，在 Selected（选择）列表上选择节点名称，然后单击 Remove（删除）按钮。

   d. 可以在 Available（可用）或 Selected（选择）列表上搜索节点。在列表下面的字段里输入搜索词，然后单击 Go（搜索）按钮。

   - **描述节点**

   a. 单击 Node Groups: New（节点组：新建）面板上的 Describe Nodes（描述节点）选项卡。在 Describe Nodes（描述节点）选项卡上创建一个规则表，描述要给节点组指定的节点。

   b. 单击 Add New Row（添加新行）图标  在表上添加一行。

   c. 双击给每一列创建的单元格激活下拉菜单。在每个列表上选择要使用的规则部件。参看 *访问控制策略* (p. 186)。

9. 如要给此节点组创建一个策略，允许用户随时凭借控制权访问节点组里的所有节点，选择 Create Full Access Policy for Group（创建节点组全访问策略）。

10. 如要添加另一个节点组，单击 Apply（应用）按钮保存此节点组，然后重复上述步骤。**可选。**

11. 在添加节点组之后，单击 OK（确定）按钮。Group Summary（组摘要）面板显示你添加的节点组的列表。

12. 单击 Continue（继续）按钮开始下一个任务，即用户管理。根据下一节所述的步骤操作。

用户管理

指导设置的第四个任务是用户管理。用户管理允许你选择权限和策略，管理用户组的访问和活动。权限指定用户组成员可以在 CC-SG 上进行哪些活动。策略指定用户组成员可以查看和修改哪些设备和节点。策略建立在类别和元素之上。在创建用户组之后，可以定义各个用户，把他们添加到用户组。

添加用户组和用户

在创建设备组任务结束时，单击 Continue（继续）按钮打开 Add User Group（添加用户组）面板。也可以单击 User Management（用户管理），然后单击左面板显示的 Guided Tasks（指导任务）树视图上的 Add User Group（添加用户组）打开 Add User Group（添加用户组）面板。

在指导设置上添加用户组和用户：

1. 在 User Group Name（用户组名称）字段里输入要创建的用户组的名称。用户组名称最长 64 个字符。
2. 在 Description（说明）字段里输入用户组说明。
3. 如要设置在此用户组的用户访问启用了此功能的设备时，每个用户允许的最大 KVM 会话数，选择 Limit Number of KVM Sessions per Device（每台设备的最大 KVM 会话数）复选框，在 Max KVM Sessions (1-8)（最大 KVM 会话数[1-8]）字段里选择允许的会话数。**可选。** 参看***限制每个用户允许的 KVM 会话数*** (参看 "***限制每个用户的 KVM 会话数***" p. 172)了解详情。
4. 单击 Privileges（权限）选项卡，然后选择要给用户组指定的 Privileges（权限）或 CC-SG 活动类型对应的复选框。
5. 可以在 Node Access（节点访问）部分指定是否希望用户组有 In band nodes（带内节点）访问权、Out of band nodes（带外节点）访问权和 Power Management（电源管理）功能访问权。选择你要给用户组指定的访问类型对应的复选框。
6. 单击 Policies（策略）选项卡。
7. 在 All Policies（所有策略）列表上选择要给用户组指定的策略，然后单击 Add（添加）按钮把它移动到 Selected Policies（选择的策略）列表上。Selected Policies（选择的策略）列表上的策略将指定给用户组。重复此步骤，给用户组添加其他策略。
8. 如要删除用户组里的一个策略，在 Selected Policies（选择的策略）列表上选择策略名称，然后单击 Remove（删除）按钮。

9. 如果要使远程验证用户与 Active Directory 模块关联，单击 Active Directory Associations（Active Directory 关联）选项卡（如果此时不显示 AD 配置的 Active Directory Associations 选项卡）。选择你希望用户组要关联的每个 Active Directory 模块对应的复选框。
10. 如要添加另一个用户组，单击 Apply（应用）按钮保存此用户组，然后重复上述步骤。**可选。**
11. 在添加用户组之后，单击 OK（确定）按钮打开 Add User（添加用户）面板。也可以单击 User Management（用户管理），然后单击左面板显示的 Guided Tasks（指导任务）树视图上的 Add User（添加用户）打开 Add User（添加用户）面板。
12. 在 Username（用户名）字段里输入要添加的用户的名称，此名称用于登录 CC-SG。
13. 如果希望此用户能登录 CC-SG，选择 Login Enabled（启用登录）复选框。
14. 只有在希望用户通过外部服务器(例如 TACACS+、RADIUS、LDAP 或 AD)进行验证时，才选择 Remote Authentication(远程验证)复选框。如果使用远程验证，不需要密码。如果选择 Remote Authentication(远程验证)复选框，New Password(新密码)和 Retype New Password（再次输入新密码）字段被禁用。
15. 在 New Password（新密码）和 Retype New Password（再次输入新密码）字段里输入用户登录 CC-SG 时所用的密码。
16. 如果要强制用户在下次登录时更改指定的密码，选择 Force Password Change on Next Login（强制在下次登录时更改密码）复选框。
17. 如果要指定强制用户多久更改一次密码，选择 Force Password Change Periodically（强制定期更改密码）复选框。
18. 在 Expiration Period (Days)（到期时间[天]）字段里输入在强制用户更改密码之前可使用的天数。
19. 在 Email address（电子邮件地址）字段里输入用户的电子邮件地址。
20. 单击 User Group（用户组）下拉箭头，然后在列表上选择要给用户指定哪个用户组。
21. 如果要添加另一个用户，单击 Apply（应用）按钮保存此用户，然后重复本节所述的步骤添加其他用户。
22. 在添加用户之后，单击 OK（确定）按钮。User Summary（用户摘要）面板显示你添加的用户组和用户的列表。**可选。**

Ch 5 关联、类别和元素

在本章内

关于关联

可以设置关联，有助于组织管理 CC-SG 管理的设备。每个关联包括一个类别（最高组织结构组）及其相关元素（类别子集）。例如你可能有一台 Raritan 设备，它管理美国数据中心、亚太数据中心和欧洲数据中心的目标服务器。可以设置一个关联，按位置组织管理此设备。然后定制 CC-SG，使其界面根据你选择的类别-位置及其关联元素（美国、亚太和欧洲）显示 Raritan 设备和节点。可以定制 CC-SG，根据自己的喜好来组织管理和显示服务器。

关联术语

- 关联 — 类别、类别元素与节点和设备之间的关系。
- 类别 — 包含一组称为元素的值的变量。例如类别是“位置”，此类别可能有“美国”和“亚太”等元素。再比如如果类别是“操作系统类型”，此类别可能有 Windows、Unix 或 Linux 等元素。
- 元素 — 类别的值。例如“美国”元素属于“位置”类别。

关联 — 定义类别和元素

Raritan 设备和节点按类别和元素组织管理。每个类别/元素对被指定给一个设备和/或节点。

类别就是相似元素所属的组。

类别	元素
OS Type（操作系统类型）	Unix、Windows、Linux
Department（部门）	销售、IT、工程

策略也用类别和元素控制用户对服务器的访问。例如可以用"位置/美洲"这一类别/元素对创建一个策略，控制用户对美洲服务器的访问。参看 ***访问控制策略*** (p. 186)。

可以通过 CSV 文件导入，给一个节点或设备指定多个同类元素。

在把设备和节点添加到 CC-SG 时，把它们链接到预定义的类别和元素。在创建节点组和设备组并给它们指定策略时，将用类别和元素定义每个组有哪些节点和设备。

如何创建关联

可以采用两种方法创建关联：指导设置和关联管理器。

- 指导设置将许多配置任务综合在一个自动化界面上。在首次配置 CC-SG 时，建议使用指导设置。在完成指导设置之后，随时可以逐个编辑配置。参看***用指导设置配置 CC-SG*** (p. 29)。
- 关联管理器只允许你处理关联，不能自动执行任何配置任务。在使用指导设置之后，也可以用关联管理器编辑关联。参看***添加、编辑和删除类别和元素*** (p. 38)。

添加、编辑和删除类别和元素

可以用关联管理器添加、编辑或删除类别和元素。

注意：CC-SG 默认让默认类别名称 System Type（系统类型）和 US States and territories（美国州和领地）保留英文。

添加类别

▶ 添加类别：

1. 选择 Associations（关联）> Association（关联）。
2. 单击 Add（添加）按钮打开 Add Category（添加类别）窗口。
3. 在 Category Name(类别名称)字段里输入类别名称。参看***命名常规*** (p. 431)详细了解 CC-SG 的名称长度规则。
4. 选择 Data Type for Elements（元素数据类型）。
   - 如果值是文本，选择 String（字符串）。
   - 如果值是数字，选择 Integer（整数）。
5. 在 Applicable For（适用于）字段里选择此类别是否应用于：Devices（设备）、Nodes（节点）或 Device and Nodes（设备和节点）。

6. 单击 OK（确定）按钮创建新类别。Category Name（类别名称）字段显示新类别的名称。

删除类别

在删除一个类别时，同时删除已创建的此类别的所有元素。在屏幕刷新或用户退出 CC-SG 再登录之后，Nodes（节点）或 Devices（设备）树视图不再显示被删除的类别。

▶ **删除类别：**

1. 选择 Associations（关联）> Association（关联）。
2. 单击 Category Name（类别名称）下拉箭头，然后选择要删除的类别。
3. 单击屏幕上 Category（类别）面板上的 Delete（删除）按钮删除此类别。打开 Delete Category（删除类别）窗口。
4. 单击 Yes（是）按钮删除此类别。

添加元素

▶ **添加元素：**

1. 选择 Associations（关联）> Association（关联）。
2. 单击 Category Name（类别名称）下拉箭头，然后选择要添加哪个类别的新元素。
3. 单击 Add a new row（添加一行）图标。
4. 在空白行上输入新元素的名称。参看*命名常规* (p. 431)详细了解 CC-SG 的名称长度规则。元素名称区分大小写。
5. 单击 OK（确定）按钮保存更改。

用 CSV 文件导入法添加类别和元素

可以导入包含类别和元素的 CSV 文件，把这些类别和元素添加到 CC-SG。必须具备用户安全管理权限与 CC 设置和控制权限，才能导入和导出类别和元素。

类别和元素 CSV 文件要求

类别和元素 CSV 文件定义类别及其关联元素和类型，以及它们是否应用于设备和/或节点。

- 所有 CATEGORY 记录和 CATEGORYELEMENT 记录是相关的。一个 CATEGORY 记录必须有一个或多个 CATEGORYELEMENT 记录。
- 如果 CC-SG 已经有了 CATEGORY 记录，CATEGORYELEMENT 记录可以没有相应的 CATEGORY 记录。例如：如果要给一个现有类别添加多个元素，不必加一行重新定义新元素所属的类别。
- 导出 CC-SG 上的文件查看备注，包括创建有效 CSV 文件所需的所有标签和参数。 参看*导出类别和元素* (p. 42)。
- 满足所有 CSV 文件的其他要求。参看*常见 CSV 文件要求* (参看 "*通用 CSV 文件要求*" p. 394)。

▶ **在 CSV 文件里添加类别：**

第一列	第二列	第三列	第四列	第五列
ADD	CATEGORY	Category Name（类别名称）	Type（类型）	Apply（应用）
			值： ▪ Integer（整数） ▪ String（字符串） 默认值是 String（字符串）。	值： ▪ Nodes（节点） ▪ Devices（设备） ▪ Both（二者） 默认值是 Both（二者）。

▶ **在 CSV 文件里添加元素：**

第一列	第二列	第三列	第四列
ADD	CATEGORYELEMENT	Category Name（类别名称）	Element Name（元素名称）

类别和元素 CSV 文件示例

ADD, CATEGORY, OS, String, Node

ADD, CATEGORYELEMENT, OS, UNIX

ADD, CATEGORYELEMENT, OS, WINDOWS

ADD, CATEGORYELEMENT, OS, LINUX

ADD, CATEGORY, Location, String, Device

ADD, CATEGORYELEMENT, Location, Aisle 1

ADD, CATEGORYELEMENT, Location, Aisle 2

ADD, CATEGORYELEMENT, Location, Aisle 3

导入类别和元素

在创建 CSV 文件之后，验证此文件是否有错误，然后导入文件。

跳过重复记录，不添加重复记录。

导入 CSV 文件：

1. 选择 Administration（管理）> Import（导入）> Import Categories（导入类别）。
2. 单击 Browse（浏览）按钮选择要导入的 CSV 文件，然后单击 Open（打开）按钮。
3. 单击 Validate（验证）按钮。Analysis Report（分析报告）区显示文件内容。
   - 如果文件无效，显示错误消息。单击 OK（确定）按钮查看页面 Problems（问题）区显示的文件问题说明。单击 Save to File（保存到文件）按钮保存问题列表。编辑 CSV 文件纠正错误，然后再验证一次。参看*排除 CSV 文件问题* (p. 396)。
4. 单击 Import（导入）按钮。
5. 单击 Actions（操作）区查看导入结果。用绿色文字显示成功导入的项目，用红色文字显示导入失败的项目。由于已经有同名项目，或者已经导入了，也用红色文字显示导入失败的项目。
6. 如要查看导入结果详细信息，查看 Audit Trail（审计跟踪）报告。参看*导入审计跟踪项* (p. 395)。

导出类别和元素

导出文件的最前面有备注，说明文件里的每一项。可以根据备注说明，创建要导入的文件。

导出类别和元素：

1. 选择 Administration（管理）> Export（导出）> Export Categories（导出类别）。
2. 单击 Export to File（导出成文件）按钮。
3. 输入文件名，然后选择文件保存位置。
4. 单击 Save（保存）按钮。

在首次把文件保持成 Excel 格式时，必须选择 Save As（另存为），确保选择 CSV 文件类型。之后，Excel 继续把文件另存为 CSV 格式。

如果不正确设置文件类型，文件会损坏，不能导入它。

Ch 6 设备、设备组和端口

如要把与其他 Raritan 设备相连的 Raritan 电源条设备添加到 CC-SG，参看***网管电源条*** (p. 91)。

---

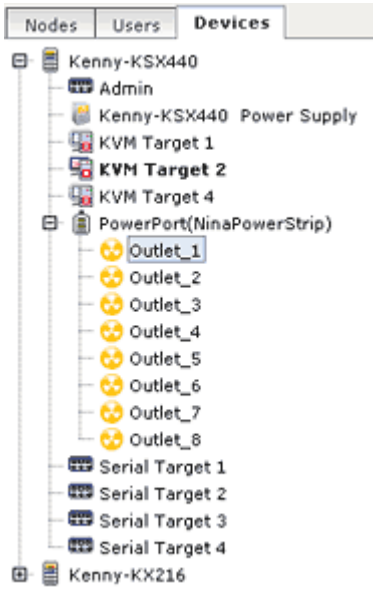
*注意：如要配置 iLO/RILOE 设备、IPMI 设备、Dell DRAC 设备、IBM RSA 设备或其他非 Raritan 设备，使用 Add Node（添加节点）菜单，作为接口添加这些设备。参看***节点、节点组和接口*** (p. 99)。*

在本章内

查看设备

设备选项卡

单击 Devices（设备）选项卡，显示 CC-SG 管理的所有设备。



每台设备的配置端口位于它们所属的设备下面。列表上有配置端口的设备显示 + 号。单击 + 号或 - 号展开或折叠端口列表。

设备和端口图标

为便于识别，KVM 设备、串行设备、电源设备和端口在 Devices（设备）树上使用不同的图标。让鼠标指针停留在 Devices（设备）树上的一个图标上，可以看到有关设备或端口信息的工具提示。

图标	含义
	设备可用
	KVM 端口可用或已连接
	KVM 端口不活动
	串行端口可用

图标	含义
	串行端口不可用
	幻影端口（参看 Raritan **Paragon II 用户指南**详细了解幻影模式。）
	设备暂停
	设备不可用
	电源条
	出口
	刀片服务器机箱可用
	刀片服务器机箱不可用
	刀片服务器可用
	刀片服务器不可用

端口排序选项

在 Devices（设备）选项卡上，配置端口位于父设备下面。可以更改端口排序方式。按状态排列的端口按连接状态字母顺序排序。设备也相应地排序。

在设备选项卡上排序端口：

1. 选择 Devices（设备）> Port Sorting Options（端口排序选项）。
2. 选择 By Port Name（按端口名称）、By Port Status（按端口状态）或 By Port Number（按端口编号），按名称字母顺序、可用性状态或端口数字编号排列端口。

*注意：对于没有集成 KVM 切换器的刀片服务器，例如 HP BladeSystem 服务器，其父设备是 CC-SG 创建的虚拟刀片服务器机箱，而不是 KX2 设备。这些服务器只在虚拟刀片服务器机箱设备内排序，所以它们不按顺序与其他 KX2 端口一起显示，除非你把这些刀片服务器端口恢复到正常 KX2 端口。参看***把刀片服务器端口恢复到正常 KX2 端口** *(p. 65)*。

设备配置文件屏幕

单击 Devices（设备）选项卡上的一台设备打开 Device Profile（设备配置文件）屏幕，显示所选设备的信息。

如果设备关闭了，Device Profile（设备配置文件）屏幕显示的信息是只读信息。可以删除现在关闭的设备。参看*删除设备* (p. 56)。

Device Profile（设备配置文件）有几个选项卡，显示有关设备的信息。

Associations（关联）选项卡

Associations（关联）选项卡包含给节点指定的所有类别和元素。可以选择不同的关联，从而更改关联。参看*关联、类别和元素* (p. 37)。

Location & Contacts（位置和联系人）选项卡

Location & Contacts（位置和联系人）选项卡包含你在处理设备时可能需要的设备位置信息和联系人信息，例如电话号码。可以在字段里输入新信息，从而更改信息。参看*给设备配置文件增加位置和联系人* (p. 55)。

Notes（备注）选项卡

Notes（备注）选项卡包含备注添加工具，用于添加供其他用户阅读的设备备注。此选项卡显示所有备注，包括用户添加备注的日期、他的用户名和 IP 地址。

如果你有设备、端口和节点管理权限，可以单击 Clear（清除）按钮清除节点配置文件里的所有备注。

参看*给设备配置文件增加备注* (p. 55)。

刀片服务器选项卡

IBM BladeCenter 等刀片服务器机箱节点有一个 Blades（刀片服务器）选项卡。Blades（刀片服务器）选项卡包含有关刀片服务器机箱上的刀片服务器的信息。

除了查看刀片服务器信息，还可以在此选项卡上选择尚未配置的刀片服务器对应的复选框来配置它们。

参看*配置刀片服务器机箱设备上的插槽* (p. 61)。

拓扑视图

拓扑视图采用结构化方式显示你的配置里的所有连接设备。

在关闭拓扑视图之前，它取代在选择设备时通常显示的 Device Profile（设备配置文件）屏幕。

打开拓扑视图：

1. 单击 Devices（设备）选项卡，然后选择要查看哪台设备的拓扑视图。
2. 选择 Devices（设备）> Device Manager（设备管理器）> Topology View（拓扑视图），显示所选设备的 Topology View（拓扑视图）。
   - 单击 + 号或 - 号展开或折叠视图。

在设备选项卡上用右键单击选项

可以在 Devices（设备）选项卡上用右键单击设备或端口，显示可用于所选设备或端口的命令菜单。

搜索设备

Devices（设备）选项卡允许你搜索树视图上的设备。搜索结果只有设备，不包括端口名称。可以在 My Profile（我的配置文件）上配置搜索方法。参看*更改默认搜索首选项* (p. 183)。

搜索设备：

- 在 Devices（设备）选项卡下半部的 Search For Device（搜索设备）字段里输入搜索字符串，然后按 Enter。
- 可以在搜索字符串里使用通配符。参看*搜索通配符* (p. 47)。

搜索通配符

通配符	Description（说明）
?	表示任何字符。
[-]	表示范围内的一个字符。
*	表示零个或多个字符。

通配符示例

示例	Description（说明）
KX?	查找 KX1 和 KXZ，但不查找

示例	Description（说明）
	KX1Z。
KX*	查找 KX1、KX、KX1 和 KX1Z。
KX[0-9][0-9]T	查找 KX95T 和 KX66T，但不查找 KXZ 和 KX5PT。

发现和添加 IPv6 网络设备

CC-SG 5.3 和更高版本可以通过 IPv6 发现和添加 Dominion KX2 设备或更高版本的设备。旧版本的 KX2 只能用作仅支持 IPv4 的设备。

Dominion KX1、Dominion SX、Dominion KSX 和 Dominion KX-101 V2 不支持 IPv6。

如果尝试添加旧版 Dominion KX2 设备，CC-SG 会显示警告消息。

Device firmware does not support CC-SG communicating on a IPv6 address. You may try upgrading the device. Do you wish to continue adding the device? If so device will be managed only on IPv4 address.（设备固件不支持 CC-SG 通过 IPv6 地址通信。你可以尝试升级此设备。是否要继续添加此设备？如果添加此设备，只能通过 IPv4 地址管理此设备。）

必须把 KX2 设备升级到 2.5 版本，才能在 CC-SG 管理下通过 IPv6 进行通信。

在利用 CSV 文件导入方式添加设备时，把消息中的所有信息记录在审计跟踪报告里。参看*导入审计跟踪项* (p. 395)。

配置 DNS 服务器监听 IPv6

在用主机名添加设备时，CC-SG 使用 DNS。

确保 DNS 服务器监听给 CC-SG 配置的 DNS 地址。DNS 在 Administration（管理）> Configuration（配置）的 Network Setup（网络设置）选项卡上配置。参看*配置 CC-SG 网络* (p. 257)。

参看 http://technet.microsoft.com/en-us/library/cc783049(ws.10).aspx 了解详情。本文以 Windows DNS 服务器为例加以说明，其中 CC-SG 配置了 DNS IPv6 地址。

▶ **配置 DNS 服务器监听 IPv6：**

1. 安装 Windows 支持工具。
2. 打开 command 提示。

3. 输入下列命令：dnscmd /config /EnableIPv6 1
4. 重新启动 DNS Server（DNS 服务器）服务。

发现设备

发现设备功能搜索所有网络设备。在发现设备之后，如果它们尚未受 CC-SG 管理，可以把它们添加到 CC-SG。

发现设备：

1. 选择 Devices（设备）> Discover Devices（发现设备）。
2. 在 From Address（开始地址）和 To Address（结束地址）字段里输入要发现哪个 IP 地址范围的设备。结束地址应该大于开始地址。From（开始地址）字段和 To（结束地址）字段预先填充本地子网或本地链路的 IP 地址范围。

   注意：预先填充的地址范围可能太大了。可以编辑这些字段，也可以单击 Stop once discovery（每次发现之后停止）按钮停止搜索。

   在 IP 隔离模式下工作时，广播/组播将同时应用于 eth0 接口和 eth1 接口。用指定的地址范围过滤要显示的已发现设备。
3. 如果搜索 CC-SG 所在的同一个子网上的设备，选择 Broadcast discovery（广播发现）复选框。取消 Broadcast discovery（广播发现）复选框，发现不同子网上的设备。
4. 如要搜索特定类型的设备，在 Device types（设备类型）列表上选择类型。默认选择所有设备类型。按住 Ctrl 单击设备类型选择多个设备类型。
5. 选择 Include IPMI Agents（包括 IPMI 代理）复选框，发现那些提供 IPMI 电源控制的目标。
6. 单击 Discover（发现）按钮开始搜索。在发现过程中，随时可以单击 Stop（停止）按钮停止发现过程。列表显示发现的设备。在双协议堆模式下工作时，列表包括每台已发现设备的主机名、IPv6 地址和 IPv4 地址。
7. 如要把一个或多个发现设备添加到 CC-SG，在列表上选择设备，然后单击 Add（添加）按钮打开 Add Device（添加设备）屏幕，预先填充了一些数据。

   如果选择添加多个设备，可以单击屏幕底部的 Previous（上一个）和 Skip（跳过）按钮浏览 Add Device（添加设备）屏幕上你要添加的设备。
8. 对于不同类型的设备，Add Device（添加设备）页面不相同。参看相应的说明了解如何添加 CC-SG 发现的每一类设备。

- 如要了解 KVM 设备或串行设备，参看*添加 KVM 设备或串行设备* (p. 50)。
- 如要了解电源条，参看*添加电源条设备* (p. 52)。
- 如要了解 IP 网络上的 Dominion PX 电源条，参看*添加 Dominion PX 设备* (p. 52)。

9. 单击 Apply（应用）按钮添加发现的设备，继续添加下一个发现设备。单击 OK（确定）按钮添加当前发现的设备，停止发现设备添加过程。

添加设备

必须先把设备添加到 CC-SG，才能配置端口或添加接口，从而访问与端口相连的节点。Add Device（添加设备）屏幕用于添加属性已知并可添加到 CC-SG 的设备。如要搜索要添加的设备，使用 Discover Devices（发现设备）选项。参看*发现设备* (p. 49)。

如要把与其他 Raritan 设备相连的 Raritan 电源条设备添加到 CC-SG，参看*网管电源条* (p. 91)。

把设备添加到 CC-SG：

1. 选择 Devices（设备）> Device Manager（设备管理器）> Add Device（添加设备）。
2. 单击 Device Type（设备类型）下拉箭头，然后在列表上选择要添加的设备的类型。对于你选择的不同的设备类型，你看到的 Add Device（添加设备）页面稍有不同。

- 如要了解如何添加 KVM 设备或串行设备，参看*添加 KVM 设备或串行设备* (p. 50)。
- 如要了解如何添加电源条设备，参看*添加电源条设备* (p. 52)。
- 如要了解如何添加 Dominion PX 设备，参看*添加 Dominion PX 设备* (p. 52)。

添加 KVM 设备或串行设备

KVM 设备和串行设备可以支持 256 位 AES 加密，CC-SG 从 4.1 版开始支持此类加密。如果设备设置为默认加密模式 auto-negotiate（自动协商），设备将与 CC-SG 协商选择与 CC-SG 相适应的适当加密级别。

1. 在 Device name（设备名称）字段里输入设备的名称。参看*命名常规* (p. 431)详细了解 CC-SG 的名称长度规则。
2. 在 Device IP or Hostname（设备 IP 或主机名）字段里输入设备的 IP 地址或主机名。参看*术语/缩写语* (参看 "*术语/缩略语*" p. 2)了解主机名规则。

*注意：部分设备支持 IPv6。参看*发现和添加 **IPv6** 网络设备 *(p. 48)*。

3. 在 Discovery Port（发现端口）字段里输入与设备通信所用的 TCP 通信端口的编号。最多五位在 1 到 65535 之间的数字字符。大多数 Raritan 设备的默认端口号是 5000。
4. 在 Username（用户名）字段里输入登录此设备所用的名称。用户必须有管理访问权。
5. 在 Password（密码）字段里输入访问此设备所需的密码。用户必须有管理访问权。
6. 在 Heartbeat timeout (sec)（检测信号超时[秒]）字段里输入新设备和 CC-SG 之间的超时秒数。
7. 如果要添加 Dominion SX 或 Dominion KX2 v2.2 或更高版本的设备，选择 Allow Direct Device Access（允许直接设备访问）复选框，即使此设备上受 CC-SG 管理，也可以在此设备上直接访问目标服务器。
8. 在 Description（说明）字段里输入此设备的简短说明。**可选。**
9. 选择 Configure all ports（配置所有端口）复选框，自动把此设备的所有端口添加到 Devices（设备）选项卡上，在 Nodes（节点）选项卡上给此设备的每个端口创建一个节点。
   - 用匹配的名称配置相应的节点和端口。
   - 给每个端口创建一个新节点，给此节点创建一个带外接口，刀片服务器机箱节点或通用模拟 KVM 切换器节点除外。
   - 可能给与 KX2 端口相连的刀片服务器机箱设备或通用模拟 KVM 切换器创建一个节点，也可能不创建，取决于在 KX2 上输入了刀片服务器机箱或通用模拟 KVM 切换器的 IP 地址还是主机名。参看 *KX II 用户指南*。CC-SG 默认给刀片服务器机箱节点指定一个网络浏览器界面。
   - 如果已经在 KX2 上给与 KX2 端口直接相连的刀片服务器正确配置了刀片服务器端口组，将在 Devices（设备）选项卡上给这些刀片服务器创建一个虚拟刀片服务器机箱设备。参看 *KX II 用户指南*。
10. 可以配置一个类别和元素列表，更好地描述和组织管理此设备和与之相连的节点。参看*关联、类别和元素* (p. 37)。
11. 对于列出的每个类别，单击 Element（元素）下拉菜单，然后在列表上选择要应用于设备的元素。对于不想使用的每个类别，在 Element（元素）字段里选择空项。

    如果要给相关节点和设备指定元素，选择 Apply to Nodes（应用于节点）复选框。

12. 如果看不到你要使用的类别值或元素值，可以用 Associations（关联）菜单添加更多值。参看***关联、类别和元素*** (p. 37)。
13. 在配置此设备之后，单击 Apply（应用）按钮添加此设备，打开 Add Device（添加设备）空白屏幕，你可以继续添加设备；也可以单击 OK（确定）按钮添加此设备，不继续打开 Add Device（添加设备）屏幕。
14. 如果设备固件版本不兼容 CC-SG，显示一条消息。单击 Yes（是）按钮把此设备添加到 CC-SG。可以在把此设备添加到 CC-SG 之后升级设备固件。参看***升级设备*** (p. 79)。

添加电源条设备

如果电源条物理连接不同的 Raritan 设备，给 CC-SG 添加电源条设备的过程有所不同。参看***网管电源条*** (p. 91)。

如要添加不与其他 Raritan 设备相连的 Dominion PX，参看***添加 Dominion PX 设备*** (p. 52)。

添加 Dominion PX 设备

Dominion PX 设备是仅与 IP 网络相连的电源条设备。Dominion PX 设备不受另一台 Raritan 设备管理。如果要添加受另一台 Raritan 设备管理的电源条，要采用不同的添加步骤。参看***网管电源条*** (p. 91)。

1. 在 Device Name(设备名称)字段里输入设备的名称。参看***命名常规*** (p. 431)详细了解 CC-SG 的名称长度规则。
2. 在 IP Address/Hostname（IP 地址/主机名）字段里输入设备的 IP 地址或主机名。参看***术语/缩写语*** (参看 "***术语/缩略语***" p. 2)了解主机名规则。
3. 在 Username（用户名）字段里输入登录此设备所用的名称。用户必须有管理访问权。
4. 在 Password（密码）字段里输入访问此设备所需的密码。用户必须有管理访问权。

   *警告：如果用户名和密码更改了，CC-SG 将断开与 Dominion PX 设备的连接。如果在 PX 上更改密码，必须在 CC-SG 上修改 PX 设备的密码。参看***编辑设备*** (p. 53)。*
5. 在 Description（说明）字段里输入此设备的简短说明。**可选。**
6. 选择 Configure All Outlets（配置所有出口）复选框，自动把此 Dominion PX 的所有出口添加到 Devices（设备）选项卡上。
7. 可以配置一个类别和元素列表，更好地描述和组织管理此设备。
   - 对于列出的每个类别，在列表上选择要应用于设备的元素。对于不想使用的每个类别，在 Element（元素）字段里选择空项。

- 如果看不到你要使用的类别值或元素值，可以添加它们。参看*关联、类别和元素* (p. 37)。

8. 在配置此设备之后，单击 Apply（应用）按钮添加此设备，打开 Add Device（添加设备）空白屏幕，你可以继续添加设备；也可以单击 OK（确定）按钮添加此设备，不继续打开 Add Device（添加设备）屏幕。

按主机名添加设备

按主机名添加设备意味着所添加的设备、CC-SG 和客户机在同一个域里。如果它们不在同一个域里，用全限定域名 (FQDN) 添加设备。这样在启动接口时，CC-SG 可以提供 FQDN。

在按主机名添加支持双协议堆的设备时，如果主机名解析不同时返回 IPv4 地址和 IPv6 地址，应该按 IP 地址添加设备。CC-SG 显示一条警告消息，说明主机名不能解析成 IPv4 地址和 IPv6 地址。

编辑设备

可以编辑设备：重新命名它，修改其属性，包括更改 PX 设备的用户名和密码。

对设备配置文件所做的更改记录在审计跟踪日志里，包括 Device Name（设备名称）、Device IP/Hostname（设备 IP/主机名）、Discovery Port（发现端口）、HTTP Port（HTTP 端口）、HTTPS Port（HTTPS 端口）、Subnet Mask（子网掩码）、Default Gateway（默认网关）、Allow Direct Device Access（允许直接设备访问）、Heartbeat（检测信号）、Associations（关联）和 Locations（位置）。参看*审计跟踪报告* (p. 223)。

▶ 编辑设备：

1. 单击 Devices（设备）选项卡，然后选择要编辑的设备。
2. 在 Device Profile（设备配置文件）页上按需要更改参数。 按需要更改参数。
   - 当设备在双协议堆模式下工作时，可以编辑 IPv6 address（IPv6 地址）、Prefix Length（前缀长度）和 IPv6 Default Gateway（IPv6 默认网关）。
   - 如果设备使用 DHCP，设置 IPv4 地址即把 IPv4 地址设置为静态 IP 地址。
   - 如果设备使用路由器发现，设置 IPv6 地址即把 IPv6 地址设置为静态 IP 地址。
3. 单击 OK（确定）按钮保存更改。

更改 KX2 设备 HTTP 和/或 HTTPS 端口设置

编辑 KX2 v2.3 或更高版本设备的配置文件，从而更改它的 HTTP 端口和 HTTPS 端口。CC-SG 把新端口号广播到 KX2 设备。

将在 CC-SG 和 KX2 设备之间用新端口进行通信，AKC 和 VKC 等客户机也可能用这些端口直接与 KX2 设备通信。在用户的客户计算机和 CC-SG 之间不用新端口号进行通信。

更改 KX2 设备 HTTP 端口和 HTTPS 端口：

注意：仅限于 KX2 v2.3 和更高版本。

1. 单击 Devices（设备）选项卡，然后选择要编辑的设备。
2. 在 Device Profile（设备配置文件）页上按需要更改参数。 输入 HTTP 端口和 HTTPS 端口的新值。
3. 单击 OK（确定）按钮。

编辑电源条设备或 Dominion PX 设备

可以编辑网管电源条设备或 Dominion PX 设备：重新命名它、修改其属性、查看出口配置状态。

编辑电源条设备：

1. 单击 Devices（设备）选项卡，然后选择要编辑的电源条设备。
2. 在此屏幕上的适当字段里输入新设备属性。必要时编辑与此设备关联的类别和元素。
3. 单击 Outlet（出口）选项卡，查看此电源条的所有出口。
4. 如果一个出口与一个节点关联，单击 Node（节点）超链接打开 Node Profile（节点配置文件）。
5. 如果一个出口与一个节点关联，选择此出口，然后单击 Power Control（电源控制）打开关联节点对应的 Power Control（电源控制）屏幕。
6. 如要删除一个出口，取消出口名称旁边的复选框。
7. 如要配置一个出口，选择出口名称旁边的复选框。
8. 单击 OK（确定）按钮保存更改。在修改设备之后，显示一条消息。

给设备配置文件增加备注

可以用 Notes（备注）选项卡添加供其他用户阅读的设备备注。此选项卡显示所有备注，包括用户添加备注的日期、他的用户名和 IP 地址。

如果你有设备、端口和节点管理权限，可以清除 Notes（备注）选项卡显示的所有备注。

给设备配置文件增加备注：

1. 在 Devices（设备）选项卡上选择一台设备，打开 Device Profile（设备配置文件）页面。
2. 单击 Notes（备注）选项卡。
3. 在 New Note（新建备注）字段里输入备注。
4. 单击 Add（添加）按钮，Notes（备注）列表显示你添加的备注。

清除所有备注：

1. 单击 Notes（备注）选项卡。
2. 单击 Clear Notes（清除备注）按钮。
3. 单击 Yes（是）按钮确认删除 Notes（备注）选项卡上的所有备注。

给设备配置文件增加位置和联系人

输入设备位置详细信息和联系人信息，供设备管理员或用户使用。

给设备配置文件增加位置和联系人：

1. 在 Devices（设备）选项卡上选择一台设备，打开 Device Profile（设备配置文件）页面。
2. 单击 Location & Contacts（位置和联系人）选项卡。
3. 输入 Location（位置）信息。
   - Department（部门）：最多 64 个字符。
   - Site（地点）：最多 64 个字符。
   - Location（位置）：最多 128 个字符。
4. 输入 Contacts（联系人）信息。
   - Primary Contact Name（主联系人姓名）和 Secondary Contact Name（第二联系人姓名）：最多 64 个字符。

- Telephone Number（电话号码）和 Cell Phone（手机号码）：最多 32 个字符。

5. 单击 OK（确定）按钮保存更改。

删除设备

可以删除设备，使它不受 CC-SG 管理。

重要说明：在删除设备时，将删除给该设备配置的所有端口。把与这些端口关联的所有接口从节点上删除。如果这些节点没有其他接口，也把这些节点从 CC-SG 中删除掉。

删除设备：

1. 单击 Devices（设备）选项卡，然后选择要删除的设备。
2. 选择 Devices(设备)> Device Manager(设备管理器)> Delete Device（删除设备）。
3. 单击 OK（确定）按钮删除此设备。在删除设备之后，显示一条消息。

支持 IPv6 的 KX II 设备的证书

为了防止受 CC-SG 管理的、利用 IP 地址添加的、支持 IPv6 的 KX2 设备发生证书错误，要确保证书里的 CN 有带前导 0 的压缩值，且压缩值放在 [] 里。

在与 CC-SG 管理的 KX II 通信时，CC-SG 在 URL 里提供带前导 0 的压缩主机供 jar 下载。这意味着证书有放在 [] 里的带前导 0 的压缩值作为 CN。

还可以把 KX II 设备的主机名用作 CN，在证书签名请求中使用 Subject Alternative Names（SAN, 主题别名），请外部证书机构签署 CSR，并把证书上载到 KX II 上。

例子：

- 正确 CN：

[fd00:c:d:2400:0:2:3:4]

- 错误：

[fd00:c:d:2400::2:3:4]

- 错误：

[fd00:000c:000d:2400:0000:0002:0003:0004]

配置端口

如果在添加设备时，没有选择 Configure all ports（配置所有端口）复选框自动添加设备的全部端口，用 Configure Ports（配置端口）屏幕把设备的个别端口或一组端口添加到 CC-SG。

在配置端口之后，在 CC-SG 上给每个端口创建一个节点，同时创建默认接口。参看*通过配置端口创建的节点* (p. 58)。

配置串行端口

配置串行端口：

1. 单击 Devices（设备）选项卡，然后选择一台串行设备。
2. 选择 Devices（设备）> Port Manager（端口管理器）> Configure Ports（配置端口）。

   单击一个列标题按此属性升序顺序排序端口。再次单击此标题按降序顺序排序端口。
3. 单击你要配置的串行端口对应的 Configure（配置）按钮。
4. 在 Port Name（端口名称）字段里输入端口名称。为便于使用，以端口所连目标服务器的名称开头来命名端口。参看*命名常规* (p. 431)详细了解 CC-SG 的名称长度规则。
5. 在 Node Name（节点名称）字段里输入节点名称，用此端口的一个带外接口创建一个新节点。为便于使用，以端口所连目标服务器的名称开头来命名节点。这意味着在 Port name（端口名称）和 Node Name（节点名称）字段里输入相同的名称。
6. 单击 Access Application（访问应用程序）下拉菜单，然后在列表上选择在连接此端口时要使用的应用程序。如要允许 CC-SG 根据你使用的浏览器自动选择合适的应用程序，选择 Auto-Detect（自动检测）。
7. 单击 OK（确定）按钮添加端口。

配置 KVM 端口

配置 KVM 端口：

1. 单击 Devices（设备）选项卡，然后选择一台 KVM 设备。
2. 选择 Devices（设备）> Port Manager（端口管理器）> Configure Ports（配置端口）。
   - 单击一个列标题按此属性升序顺序排序端口。再次单击此标题按降序顺序排序端口。
3. 单击你要配置的 KVM 端口对应的 Configure（配置）按钮。

4. 在 Port Name（端口名称）字段里输入端口名称。为便于使用，以端口所连目标服务器的名称开头来命名端口。参看***命名常规*** (p. 431)详细了解 CC-SG 的名称长度规则。
5. 在 Node Name（节点名称）字段里输入节点名称，用此端口的一个带外接口创建一个新节点。为便于使用，以端口所连目标服务器的名称开头来命名节点。这意味着在 Port name（端口名称）和 Node Name（节点名称）字段里输入相同的名称。
6. 单击 Access Application（访问应用程序）下拉菜单，然后在列表上选择在连接此端口时要使用的应用程序。如要允许 CC-SG 根据你使用的浏览器自动选择合适的应用程序，选择 Auto-Detect（自动检测）。
7. 单击 OK（确定）按钮添加端口。

通过配置端口创建的节点

在配置设备端口时，自动给每个端口创建一个节点。同时给每个节点创建一个接口。

在自动创建节点时，所使用的名称与它关联的端口相同。如果此节点名称已经有了，在节点名称后面增加一个后缀，例如 Channel1(1)，括号里的数字就是后缀。此后缀不计入节点名称字符数。如果编辑节点名称，新名称不得超过最大字符数。参看***命名常规*** (p. 431)。

编辑端口

可以通过编辑端口更改各种参数，例如端口名称、访问应用程序和串行端口设置。可以进行的更改取决于端口类型和设备类型。

注意：也可以用 Launch Admin 和 KX2 的 Web 界面编辑 Dominion KX2 端口设置。

▶ 编辑 KVM 端口或串行端口的名称或访问应用程序：

某些端口只支持一种访问应用程序，所以不能更改访问应用程序首选项。

1. 单击 Devices（设备）选项卡，然后选择要编辑的端口
2. 必要时在 Port Name（端口名称）字段里输入新端口名称。
3. 单击 Access Application（访问应用程序）下拉菜单，然后在列表上选择在连接此端口时要使用的应用程序。如要允许 CC-SG 根据你使用的浏览器自动选择合适的应用程序，选择 Auto-Detect（自动检测）。
4. 单击 OK（确定）按钮保存更改。

编辑 KSX2 或 KSX 串行端口设置（例如波特率、流控制或奇偶校验/数据位）：

1. 单击 Devices（设备）选项卡，然后选择要编辑的串行端口，或者选择有你要编辑的端口的设备。
2. 选择 Devices（设备）> Device Manager（设备管理器）> Launch Admin（启动管理），打开设备管理页面。
3. 单击 Port Configuration（端口配置）。
4. 单击要编辑的串行端口。
5. 编辑端口设置。
6. 单击 OK（确定）按钮保存更改。关闭管理页面，返回 CC-SG。

编辑 SX 串行端口设置（例如波特率、流控制或奇偶校验/数据位）：

1. 单击 Devices（设备）选项卡，然后选择要编辑的端口打开 Port Profile（端口配置文件）页面。
2. 编辑端口设置。
3. 单击 OK（确定）按钮保存更改。

删除端口

在删除一个端口时，同时删除 Device（设备）上的端口项。如果端口关闭了，Port Profile（端口配置文件）屏幕显示的信息是只读信息。可以删除现在关闭的端口。

重要说明：如果删除与一个节点关联的一个端口，将从此节点上删除此端口提供的关联带外 KVM 接口或串行接口。如果此节点没有其他接口，也把此节点从 CC-SG 中删除掉。

删除端口：

1. 单击 Devices（设备）选项卡，然后选择要删除哪台设备的端口。
2. 选择 Devices（设备）> Port Manager（端口管理器）> Delete Ports（删除端口）。
3. 选择要删除的端口对应的复选框。
4. 单击 OK（确定）按钮删除所选的端口。在删除端口之后，显示一条消息。

配置与 KX2 相连的刀片服务器机箱设备

刀片服务器机箱概述

有两种刀片服务器机箱设备：一种有集成的 KVM 切换器，可以充当支持 IP 的 KVM 切换器，但另一种没有集成的 KVM 切换器。

有集成 KVM 切换器的刀片服务器机箱

对于 Dell PowerEdge 系列和 IBM BladeCenter 系列等集成了 KVM 切换器的刀片服务器机箱，一个机箱通过一个 CIM 连接 KX2。由于只能用一个 CIM 访问此机箱上的所有刀片服务器，所以当一个用户访问一个刀片服务器时，再也没有访问路径供其他用户使用了。

在 CC-SG 上配置所有 KX2 端口时，配置与 KX2 设备相连的*刀片服务器机箱*。参看***添加刀片服务器机箱设备*** (p. 60)。不配置此类刀片服务器机箱上的刀片服务器，所以你稍后必须配置这些刀片服务器。参看***配置刀片服务器机箱设备上的插槽*** (p. 61)。

没有集成 KVM 切换器的刀片服务器机箱

对于 HP BladeSystem 系列等没有集成 KVM 切换器的刀片服务器机箱，每个刀片服务器通过一个 CIM 分别连接 KX2。由于机箱上的每个刀片服务器用一个 CIM 访问设备，当一个用户访问一个刀片服务器时，其他用户仍然可以访问其他刀片服务器。

在 CC-SG 上配置所有 KX2 端口时，配置与 KX2 设备相连的*刀片服务器*。如果已经在 KX2 设备上给这些刀片服务器正确配置了刀片服务器端口组，CC-SG 在 KX2 端口级创建一个*虚拟刀片服务器机箱*作为这些刀片服务器的容器。参看***添加刀片服务器机箱设备*** (p. 60)。否则，CC-SG 的 Devices（设备）选项卡将这些刀片服务器作为正常 KX2 端口显示。

添加刀片服务器机箱设备

刀片服务器机箱设备添加步骤取决于刀片服务器型号。

刀片服务器机箱设备在 Devices（设备）选项卡上始终显示两个名称：没有括号的名称是从 KX2 设备获得的，有括号的名称是 CC-SG 保存的机箱名称。

▶ 添加*集成了* KVM 切换器的刀片服务器机箱设备：

1. 在 KX2 上正确配置刀片服务器机箱。参看 *KX II 用户指南*。
2. 在 CC-SG 上正确配置 KX2 设备。参看***添加 KVM 设备或串行设备*** (p. 50)。

3. CC-SG 检测刀片服务器机箱设备，在一个或两个选项卡上增加刀片服务器机箱图标：
   - 在 Devices（设备）选项卡上，在相连的 KX2 设备下面显示刀片服务器机箱设备。
   - 在 Nodes（节点）选项卡上，如果在 KX2 上输入了刀片服务器机箱的 IP 地址或主机名，作为节点显示刀片服务器机箱，并给它添加一个网络浏览器接口。

---

*注意：对于这种刀片服务器机箱，你稍后必须配置刀片服务器。参看***配置刀片服务器机箱设备上的插槽** *(p. 61)*。

添加*没有集成* KVM 切换器的刀片服务器机箱设备：

1. 在 KX2 上给刀片服务器正确配置刀片服务器端口组。参看 *KX II 用户指南*。
2. 在 CC-SG 上正确配置 KX2 设备。参看***添加 KVM 设备或串行设备*** (p. 50)。
3. CC-SG 自动创建一个*虚拟*刀片服务器机箱，在一个选项卡上增加刀片服务器机箱图标。注意在 Nodes（节点）选项卡上，虚拟刀片服务器机箱不作为节点显示。
   - 在 Devices（设备）选项卡上，在 KX2 设备下面显示虚拟刀片服务器机箱设备，作为刀片服务器的虚拟容器（显示在虚拟刀片服务器机箱下面）。

---

*注意：如果在 CC-SG 上配置 KX2 端口之前，没有给刀片服务器配置刀片服务器端口组，可以选择 Devices（设备）> Device Manager（设备管理器）> Launch Admin（启动管理）设置刀片服务器端口组。然后在 CC-SG 上配置刀片服务器。参看***配置刀片服务器机箱设备上的插槽** *(p. 61)*。

配置刀片服务器机箱设备上的插槽

如果尚未在 CC-SG 上配置刀片服务器或插槽，必须根据本节所述的下列步骤配置它们，否则 Devices（设备）选项卡和 Nodes（节点）选项卡不显示刀片服务器。自动给刀片服务器节点添加一个带外 KVM 接口。

在刀片服务器机箱配置文件上配置插槽：

1. 在 Devices（设备）选项卡上，单击与刀片服务器机箱设备相连的 KX2 设备旁边的 + 号。
2. 选择要配置哪个刀片服务器机箱设备的插槽。
3. 选择 Device Profile（设备配置文件）屏幕上的 Blades（刀片服务器）选项卡。
4. 选择要配置的每个插槽对应的复选框，然后单击 OK（确定）按钮。

在配置端口屏幕上配置插槽：

1. 在 Devices（设备）选项卡上，单击与刀片服务器机箱设备相连的 KX2 设备旁边的 + 号。
2. 选择要配置哪个刀片服务器机箱设备的插槽。
3. 选择 Devices（设备）> Port Manager（端口管理器）> Configure Ports（配置端口）。
   - 如要给多个插槽配置屏幕显示的默认名称，选择要配置的每个插槽对应的复选框，然后单击 OK（确定）按钮给每个插槽配置默认名称。
   - 如要逐个配置每个插槽，单击插槽旁边的 Configure（配置）按钮。然后在 Port Name（端口名称）字段里输入插槽名称，在 Node Name（节点名称）字段里输入节点名称。根据在 Application Manager（应用程序管理器）上给 Blade Chassis: KVM（刀片服务器机箱：KVM）选择的默认应用程序，设置默认 Access Application（访问应用程序）。如要更改设置，单击 Access Application（访问应用程序）下拉菜单，然后在列表上选择首选应用程序。单击 OK（确定）按钮配置插槽。

用配置刀片服务器命令配置插槽：

1. 在 Devices（设备）选项卡上，单击与刀片服务器机箱设备相连的 KX2 设备旁边的 + 号。
2. 选择要配置哪个刀片服务器机箱设备的插槽。
3. 选择 Node（节点）> Configure Blades（配置刀片服务器）。
   - 如要给多个插槽配置屏幕显示的默认名称，选择要配置的每个插槽对应的复选框，然后单击 OK（确定）按钮给每个插槽配置默认名称。
   - 如要逐个配置每个插槽，单击插槽旁边的 Configure（配置）按钮。然后在 Port Name（端口名称）字段里输入插槽名称，在 Node Name（节点名称）字段里输入节点名称。根据在 Application Manager（应用程序管理器）上给 Blade Chassis: KVM（刀片服务器机箱：KVM）选择的默认应用程序，设置默认 Access Application（访问应用程序）。如要更改设置，单击 Access Application（访问应用程序）下拉菜单，然后在列表上选择首选应用程序。单击 OK（确定）按钮配置插槽。

更改刀片服务器状态

本节仅适用于 Dell PowerEdge 系列和 IBM BladeCenter 系列等集成了 KVM 切换器的刀片服务器机箱。

如果不在 KX2 设备上针对相应刀片服务器或插槽启用 Installed（已安装）状态，CC-SG 始终把刀片服务器的端口状态显示为 Down（停止）。如果你确定某些刀片服务器插槽已安装刀片服务器，应该在 KX2 设备上更改其状态，让 CC-SG 正确反映状态。

更改刀片服务器状态：

1. 单击 Devices（设备）选项卡，然后选择要更改哪台 KX2 设备的刀片服务器插槽状态。
2. 选择 Devices（设备）> Device Manager（设备管理器）> Launch Admin（启动管理），打开 KX2 Admin Client。
3. 选择 Device Settings（设备设置）> Port Configuration（端口配置）。
4. 单击要配置的刀片服务器机箱端口。
5. 向下翻页，找到刀片服务器插槽部分。选择已安装刀片服务器的刀片服务器插槽旁边的 Installed（已安装）复选框。
6. 单击 OK（确定）按钮保存更改。

删除刀片服务器机箱设备上的插槽

可以删除不使用的刀片服务器或插槽，让 Devices（设备）和 Nodes（节点）选项卡不再显示它们。

在删除端口屏幕上删除插槽：

1. 在 Devices（设备）选项卡上，单击与刀片服务器机箱设备相连的 KX2 设备旁边的 + 号。
2. 选择要删除哪个刀片服务器机箱设备的插槽。
3. 选择 Devices（设备）> Port Manager（端口管理器）> Delete Ports（删除端口）。
4. 选择要删除的每个插槽对应的复选框，然后单击 OK（确定）按钮删除插槽。

用配置刀片服务器命令删除插槽：

1. 在 Devices（设备）选项卡上，单击与刀片服务器机箱设备相连的 KX2 设备旁边的 + 号。
2. 选择要删除插槽的刀片服务器机箱设备旁边的 + 号。

3. 用右键单击要删除的刀片服务器插槽。
4. 选择 Delete Blade（删除刀片服务器），然后单击 OK（确定）按钮删除插槽。

编辑刀片服务器机箱设备

可以编辑刀片服务器机箱设备：重新命名它，修改其属性，查看插槽配置状态。

编辑刀片服务器机箱：

1. 在 Devices（设备）选项卡上，单击与刀片服务器机箱设备相连的 KX2 设备旁边的 + 号。
2. 选择要编辑的刀片服务器机箱设备。
3. 在此屏幕上的适当字段里输入新设备属性。必要时编辑与此设备关联的类别和元素。
4. 单击 Blades（刀片服务器）选项卡，查看此刀片服务器机箱设备的所有插槽。
5. 如果一个插槽被配置为节点，可以单击 Node（节点）超链接打开 Node Profile（节点配置文件）。**可选。**
6. 单击 OK（确定）按钮保存更改。在修改设备之后，显示一条消息。

删除刀片服务器机箱设备

可以把与 KX2 设备相连的刀片服务器机箱设备从 CC-SG 上删除掉。在把刀片服务器机箱设备从 KX2 设备上删除掉时，Devices（设备）选项卡和 Nodes（节点）选项卡不再显示刀片服务器机箱设备和配置的所有刀片服务器或插槽。

删除刀片服务器机箱设备：

1. 单击 Devices（设备）选项卡，然后选择要删除哪台 KX2 设备的刀片服务器机箱设备。
2. 选择 Devices（设备）> Port Manager（端口管理器）> Delete Ports（删除端口）。
3. 选择要删除的刀片服务器机箱端口对应的复选框。
4. 单击 OK（确定）按钮删除所选的刀片服务器机箱端口。显示一条消息，请你确认删除刀片服务器机箱设备及其所有刀片服务器。

把刀片服务器机箱设备移动到不同的端口

在把刀片服务器机箱设备从一台 KX2 设备或一个端口物理移动到另一台 KX2 设备或另一个端口之后，CC-SG 不能检测刀片服务器机箱设备，不能自动用新端口数据更新刀片服务器机箱设备配置数据。必须再次在 CC-SG 上配置刀片服务器机箱设备。

▶ **把刀片服务器机箱设备移动到不同的 KX2 设备或端口：**

1. 在 CC-SG 上删除刀片服务器机箱设备。参看*删除刀片服务器机箱* (参看 "*删除刀片服务器机箱设备*" p. 64)。
2. 断开刀片服务器机箱，把它重新连接到另一台 KX2 设备或另一个端口。
3. 在 CC-SG 上添加刀片服务器机箱设备。参看*添加刀片服务器机箱设备* (p. 60)。

把刀片服务器端口恢复到正常 KX2 端口

本节仅适用于 HP BladeSystem 系列等没有集成 KVM 切换器的刀片服务器机箱。

可以在 Devices（设备）选项卡上把虚拟刀片服务器机箱下面的刀片服务器重新配置为正常 KX2 端口。

▶ **把刀片服务器恢复到正常 KX2 端口：**

1. 在 Devices（设备）选项卡选择要把哪台 KX2 设备的刀片服务器重新配置为正常 KVM 端口。
2. 把这些刀片服务器的刀片服务器端口组更改为非刀片服务器端口组。
   a. 在 CC-SG 上选择 Devices（设备）> Device Manager（设备管理器）> Launch Admin（启动管理），打开 KX2 Admin Client。
   b. 单击 Port Group Management（端口组管理）。
   c. 单击要更改哪个刀片服务器端口组的组属性。
   d. 取消 Blade Server Group（刀片服务器组）复选框。
   e. 单击 OK（确定）按钮。
   f. 退出 KX2 Admin Client。
3. Devices（设备）选项卡不再显示虚拟刀片服务器机箱。现在可以在 CC-SG 上把刀片服务器端口重新配置为正常 KX2 端口。参看*配置 KVM 端口* (p. 57)。

设备关联、位置和联系人批量复制

批量复制命令允许你把一台设备上的类别、位置和联系人信息复制到多台其他设备上。注意在此过程中，选择的信息即为复制的属性。如果任何所选设备有相同类型的信息，在执行批量复制命令时，用新指定的信息替换现有数据。

批量复制设备关联、位置和联系人信息：

1. 单击 Devices（设备）选项卡，然后在 Devices（设备）树上选择一台设备。
2. 选择 Devices（设备）> Device Manager（设备管理器）> Bulk Copy（批量复制）。
3. 在 Available Devices（可用设备）列表上选择你要把 Device Name（设备名称）字段里的设备的关联、位置和联系人信息复制到哪些设备上。
4. 单击 > 按钮把设备添加到 Selected Devices（选择的设备）列表上。
5. 选择设备，然后单击 < 按钮把它从 Selected Devices（选择的设备）列表上删除掉。
6. 在 Associations（关联）选项卡上选择 Copy Associations（复制关联）复选框复制设备的所有类别和元素。
   - 可以在此选项卡上更改、添加或删除任何数据。修改后的数据被复制到 Selected Devices（选择的设备）列表上的多台设备，以及 Device Name（设备名称）字段当前显示的设备。**可选。**
7. 在 Location and Contacts（位置和联系人）选项卡上选择要复制的信息对应的复选框：
   - 选择 Copy Location Information（复制位置信息）复选框复制 Location（位置）部分显示的位置信息。
   - 选择 Copy Contact Information（复制联系人信息）复选框复制 Contact（联系人）部分显示的联系人信息。
   - 可以在此选项卡上更改、添加或删除任何数据。修改后的数据被复制到 Selected Devices（选择的设备）列表上的多台设备，以及 Device Name（设备名称）字段当前显示的设备。**可选。**
8. 单击 OK（确定）按钮进行批量复制。在复制选择的信息之后，显示一条消息。

配置与 KX2 2.3 或更高版本相连的模拟 KVM 切换器

KX2 v2.3 允许你把通用模拟 KVM 切换器连接到目标端口。对于 CC-SG，通用模拟 KVM 切换器及其端口可以用作节点。

必须先在 KX2 Web 界面上配置它，然后把 KX2 添加到 CC-SG。

添加与 KX2 相连的 KVM 切换器

此步骤利用 Admin Client 添加与 KX2 相连的 KVM 切换器。还可以利用 CSV 导入法添加 KVM 切换器。参看 *设备 CSV 文件要求* (p. 74)。

▶ 添加与 KX2 相连的 KVM 切换器：

1. 在 KX2 上正确配置 KVM 切换器。参看 *Dominion KX II 用户指南*上的*配置和启用分层*以及*配置 KVM 切换器*部分。可以在 http://www.raritan.com/support/online-help/ 上阅读 Dominion KX II 联机帮助。
2. 在 CC-SG 上正确配置 KX2 设备。参看*添加 KVM 设备或串行设备* (p. 50)。
3. CC-SG 检测 KX2 端口连接的 KVM 切换器，在一个或两个选项卡上增加设备图标：
   - 在 Devices（设备）选项卡上，在相连的 KX2 设备下面显示 KVM 切换器。
   - 在 Nodes（节点）选项卡上，如果在 KX2 上输入了 KVM 切换器的 URL，作为节点显示此 KVM 切换器，并给它添加一个网络浏览器接口。

配置与 KX2 相连的模拟 KVM 切换器设备的端口

如果尚未在 CC-SG 上配置模拟 KVM 切换器，必须根据本节所述的下列步骤配置它们，否则 Devices（设备）选项卡和 Nodes（节点）选项卡不显示此模拟 KVM 切换器。自动给 KVM 切换器节点添加一个带外 KVM 接口。

▶ 在 KVM 切换器设备配置文件里配置端口：

1. 在 Devices（设备）选项卡上，单击与 KVM 切换器设备相连的 KX2 设备旁边的 + 号。
2. 选择要配置哪台 KVM 切换器的端口。
3. 选择 Device Profile（设备配置文件）屏幕上的 KVM Switch Port（KVM 切换器端口）选项卡。
4. 选择要配置的每个插槽对应的复选框，然后单击 OK（确定）按钮。

在配置端口屏幕上配置插槽：

1. 在 Devices（设备）选项卡上，单击与 KVM 切换器设备相连的 KX2 设备旁边的 + 号。
2. 选择要配置哪台 KVM 切换器设备的端口。
3. 选择 Devices（设备）> Port Manager（端口管理器）> Configure Ports（配置端口）。
   - 如要给页面显示的多个端口配置默认名称，选择要配置的每个端口对应的复选框，然后单击 OK（确定）按钮给每个端口配置默认名称。
   - 如要逐个配置每个端口，单击端口旁边的 Configure（配置）按钮，然后在 Port Name（端口名称）字段里输入端口名称，在 Node Name（节点名称）字段里输入节点名称。根据在 Application Manager（应用程序管理器）上给 KVM Switch: KVM（KVM 切换器 :KVM）选择的默认应用程序，设置默认 Access Application（访问应用程序）。如要更改设置，单击 Access Application（访问应用程序）下拉菜单，然后在列表上选择首选应用程序。单击 OK（确定）按钮配置端口。

用配置刀片服务器命令配置插槽：

1. 在 Devices（设备）选项卡上，单击与 KVM 切换器设备相连的 KX2 设备旁边的 + 号。
2. 选择要配置哪台 KVM 切换器设备的端口。
3. 选择 Node（节点）> Configure Ports（配置端口）。
   - 如要给页面显示的多个端口配置默认名称，选择要配置的每个端口对应的复选框，然后单击 OK（确定）按钮给每个端口配置默认名称。
   - 如要逐个配置每个端口，单击端口旁边的 Configure（配置）按钮，然后在 Port Name（端口名称）字段里输入端口名称，在 Node Name（节点名称）字段里输入节点名称。根据在 Application Manager（应用程序管理器）上给 KVM Switch: KVM（KVM 切换器 :KVM）选择的默认应用程序，设置默认 Access Application（访问应用程序）。如要更改设置，单击 Access Application（访问应用程序）下拉菜单，然后在列表上选择首选应用程序。单击 OK（确定）按钮配置端口。

设备组管理器

用设备组管理器添加设备组，编辑设备组，删除设备组。在添加新设备组时，可以给此设备组创建全访问策略。参看 *访问控制策略* (p. 186)。

设备组概述

设备组用于把设备分成组。设备组是访问策略的基础，它允许或拒绝访问本组特定设备。参看*添加策略* (p. 186)。设备可以通过 Select（选择）方法进行人工组合，也可以通过 Describe（描述）方法创建一个逻辑表达式描述一组共有属性来进行人工组合。

如果用指导设置创建节点类别和元素，已经创建了按共有属性组织管理设备的方法。CC-SG 自动根据这些元素创建默认访问策略。参看*关联、类别和元素* (p. 37)详细了解如何创建类别和元素。

查看设备组：

- 选择 Associations（关联）> Device Groups（设备组），打开 Device Groups Manager（设备组管理器）窗口。左边显示现有设备组的列表，而主面板显示所选节点组的详细信息。
  - 左边显示现有设备组的列表。单击一个设备组，可以在设备组管理器上查看此组的详细信息。
  - 如果组是任意组合的，显示 Select Devices（选择设备）选项卡，显示组里的节点列表和不在组里的节点列表。
  - 如果组是根据共有属性组合的，显示 Describe Devices（描述设备）选项卡，显示组设备选择规则。
  - 如要搜索设备组列表上的设备，在列表下面的 Search（搜索）字段里输入字符串，然后单击 Search（搜索）按钮。搜索方法通过 My Profile（我的配置文件）屏幕配置。参看*用户和用户组* (p. 166)。
  - 如果按属性查看组，单击 View Devices（查看设备）按钮，Device Group（设备组）显示当前设备的列表。打开 Devices in Devices Group（设备组里的设备）窗口，显示设备及其所有属性。
- 选择 Reports（报告）> Devices（设备）> Device Group Data（设备组数据）。显示现有设备组的列表。双击任何一行查看相应设备组里的设备。

添加设备组

添加设备组：

1. 选择 Associations（关联）> Device Groups（设备组），打开 Device Groups Manager（设备组管理器）窗口。左面板显示现有设备组。
2. 单击工具栏上的 New Group（新建设备组）图标  ， The Device Group: New panel appears.
3. 在 Group Name（设备组名称）字段里输入要创建的设备组的名称。参看*命名常规* (p. 431)详细了解 CC-SG 的名称长度规则。

4. 可以采用两种方法把设备添加到设备组：Select Devices（选择设备）和 Describe Devices（描述设备）。Select Devices（选择设备）选项卡允许你在可用设备列表上选择设备，从而选择要给设备组指定哪些设备。Describe Devices（描述设备）选项卡允许你指定设备描述规则，参数符合这些规则的设备将被添加到设备组里。

用选择设备选项添加设备组：

1. 单击 Device Group: New（设备组：新建）选项卡上的 Select Devices（选择设备）选项卡。
2. 在 Available（可用）列表上选择要添加到设备组里的设备，然后单击 Add（添加）按钮把它移动到 Selected（选择）列表上。Selected（选择）列表上的设备将被添加到设备组里。
   - 如要删除设备组里的一个设备，在 Selected（选择）列表上选择设备名称，然后单击 Remove（删除）按钮。
   - 可以在 Available（可用）或 Selected（选择）列表上搜索设备。在列表下面的字段里输入搜索词，然后单击 Go（搜索）按钮。
3. 选择 Create Full Access Policy for Group（创建设备组全访问策略）复选框给此设备组创建一个策略，允许随时凭借控制权访问设备组里的所有设备。
4. 如要添加另一个设备组，单击 Apply（应用）按钮保存此设备组，然后重复上述步骤。**可选。**
5. 在添加设备组之后，单击 OK（确定）按钮保存更改。

用描述节点选项添加设备组：

1. 单击 Device Group: New（设备组：新建）面板上的 Describe Devices（描述设备）选项卡。在 Describe Devices（描述设备）选项卡上创建一个规则表，描述要给设备组指定的设备。
2. 单击 Add New Row（添加新行）图标  在表上添加一行。
3. 双击给每一列创建的单元格激活下拉菜单。在每个列表上选择要使用的规则部件。
   - Prefix（前缀）— 保留空白，或者选择 NOT（否）。如果选择 NOT（否），此规则将过滤与表达式其他值相反的值。
   - Category（类别）— 选择一个在规则里求值的属性。在这里可以选择你用关联管理器创建的所有类别。如果在此系统上配置了任何刀片服务器机箱，默认有 Blade Chassis（刀片服务器机箱）类别。
   - Operator（运算符）— 选择要在类别项和元素项之间执行的比较运算。有三种运算符可供选择：=（等于）、LIKE（用于查找名称里的元素）和 <>（不等于）。

- Element（元素）— 选择要比较的类别属性值。这里只出现与所选类别关联的元素（例如：如果对“部门”类别求值，这里不出现“位置”元素）。
- Rule Name（规则名称）— 这是给此行上的规则指定的名称。不能编辑规则名称；规则名称用于在 Short Expression（简短表达式）字段里写入说明。

4. 如要添加另一个规则，单击 Add New Row（添加新行）图标  ，然后进行必要配置。在配置多个规则时，允许你提供多个设备求值标准，从而进行更精确的描述。
5. 规则表仅将可用标准用于节点求值。如要输入设备组说明，在 Short Expression（简短表达式）字段里按规则名称添加规则。如果描述只需要一个规则，在字段里输入规则名称。如果要对多个规则求值，在字段里输入一组规则，用逻辑运算符描述规则彼此之间的关系。
   - &— AND（与）运算符。节点必须满足此运算符两边的规则，描述（或部分描述）求值才为真。
   - | — OR（或）运算符。设备必须满足此运算符任一边的规则，描述（或部分描述）求值才为真。
   - (and) — 组合运算符。它将描述划分成几个部分，放在括号里。先对括号里的部分求值，然后将描述的其余部分与节点进行比较。括号组可以嵌入其他括号里。

     示例 1：如果要描述属于工程部的设备，创建 Department = Engineering 规则。这将变成 Rule0。在 Short Expression（简短表达式）字段里输入 Rule0。

     示例 2：如果要描述属于工程部或者位于费城的一组设备，指定所有机器必须有 1GB 内存，必须创建三个规则。Department = Engineering (Rule0) Location = Philadelphia (Rule1) Memory = 1GB (Rule2)。这些规则必须按相互之间的关系排列。由于设备可能属于工程部或位于费城，所以用“或”运算符 | 连接两个规则：Rule0 | Rule1。先用括号把它括起来进行比较：(Rule0 | Rule1)。由于设备必须满足此比较，并且要有 1GB 内存，所以用“与”运算符 & 将这部分和 Rule2 连起来：(Rule0 | Rule1) & Rule2。在 Short Expression（简短表达式）字段里输入这个最终表达式。

注意：应该在 & 和 | 运算符前后各加一个空格。否则在删除表中的任何规则之后，Short Expression（简短表达式）字段可能返回默认表达式，即 Rule0 & Rule1 & Rule2 等。

- 如要删除表上的一行，选择此行，然后单击 Remove Row（删除行）图标  。

- 如要查看哪些设备的参数满足你定义的规则，单击 View Devices（查看设备）。

6. 在 Short Expression（简短表达式）字段里输入描述之后，单击 Validate（验证）按钮。如果描述格式错误，会显示警告消息。如果描述格式正确无误，Normalized Expression（规范表达式）字段显示规范格式的表达式。
7. 单击 View Devices（查看设备）按钮查看哪些节点满足此表达式。打开 Devices in Device Group Results（设备组设备结果）窗口，显示按当前表达式组合的设备。可以用它检查输入的表达式是否正确无误。如果输入错误，可以返回规则表或 Short Expression（简短表达式）字段修改错误。
8. 选择 Create Full Access Policy for Group（创建设备组全访问策略）复选框给此设备组创建一个策略，允许随时凭借控制权访问设备组里的所有设备。
9. 如要添加另一个设备组，单击 Apply（应用）按钮保存此设备组，然后重复上述步骤。**可选。**
10. 在添加设备组之后，单击 OK（确定）按钮保存更改。

描述方法与选择方法

如果你希望设备组建立在节点或设备的某些属性之上，例如类别和元素，要使用描述方法。描述方法的优点是在你添加更多有相同描述属性的设备或节点时，它们被自动添加到设备组里。

如果只想人工创建由特定节点构成的设备组，要使用选择方法。被添加到 CC-SG 的新节点和设备并不自动添加到这些设备组里。在把新节点或设备添加到 CC-SG 之后，必须人工把它们添加到设备组里。

这两种方法不能混用。

在用一种方法创建一个设备组之后，必须用同一种方法编辑此设备组。如果换用另一种方法，将覆盖当前设备组设置。

编辑设备组

编辑设备组：

1. 选择 Associations（关联）> Device Groups（设备组），打开 Device Groups Manager（设备组管理器）窗口。
2. 左面板显示现有设备组。选择要编辑的设备组的名称打开 Device Group Details（设备组详细信息）面板。
3. 在 Group Name（组名称）字段里输入设备组的新名称。**可选。**

4. 用 Select Device（选择设备）或 Describe Devices（描述设备）选项卡编辑设备组包括的设备。参看*添加设备组* (p. 69)。
5. 单击 OK（确定）按钮保存更改。

删除设备组

删除设备组：

1. 选择 Associations（关联）> Device Groups（设备组），打开 Device Groups Manager（设备组管理器）窗口。
2. 左面板显示现有设备组。选择要删除的设备组打开 Device Group Details（设备组详细信息）面板。
3. 选择 Groups（节点组）> Delete（删除）。
4. 打开 Delete Device Group（删除设备组）面板。单击 Delete（删除）按钮。
5. 在显示的确认消息窗口上，单击 Yes（是）按钮。

用 CSV 文件导入法添加设备

可以导入包含设备的 CSV 文件，把这些设备添加到 CC-SG。必须具备设备、端口和节点管理权限与 CC 设置和控制权限，才能导入和导出设备。

必须给你指定一个策略，你才能访问所有相关设备和节点。建议指定 All Nodes（所有节点）和 All Devices（所有设备）全访问策略。

注意：不能用 CSV 文件导入法添加 P2SC 设备。

设备 CSV 文件要求

设备 CSV 文件定义设备和端口，以及把设备添加到 CC-SG 所需的详细信息。

- 对于支持与 SX、KX、KX2 或 KSX2 端口相连的电源条的设备，在配置端口时同时配置电源条。
- 如果配置设备端口，CC-SG 同时给每个端口添加一个节点和带外 KVM 接口或带外串行接口。
- 如要添加刀片服务器，刀片服务器必须通过 CIM 连接 KX2 设备。KX2 设备必须已被添加到 CC-SG，或者包括在同一个 CSV 文件里。
- 如要添加支持 IPv6 的 KX2 设备，参看*发现和添加 IPv6 网络设备* (p. 48)详细了解支持的设备。
- 导出 CC-SG 上的文件查看备注，包括创建有效 CSV 文件所需的所有标签和参数。 参看*导出设备* (p. 78)。
- 满足所有 CSV 文件的其他要求。参看*常见 CSV 文件要求* (参看 "*通用 CSV 文件要求*" p. 394)。

▶ **在 CSV 文件里添加设备：**

列编号	标签或值	详细信息
1	ADD	所有标签的第一列是命令。
2	DEVICE	输入所示的标签。 标签不区分大小写。
3	Device Type（设备类型）	必填字段。 输入如下所示的设备类型： KX、KX2、KSX、KSX2、KX101、KX2-101、IP-Reach、SX 或 PX
4	Device Name（设备名称）	必填字段。 设备名称不能含有空格或特殊字符。 Dominion PX 设备名称不能使用句点。在导入时，句点转换成连字符。
5	IP Address or Hostname（IP 地址或主机名）	必填字段。 支持的设备的 IPv4 地址或 IPv6 地址
6	Username（用户名）	必填字段。
7	Password（密码）	必填字段。

列编号	标签或值	详细信息
8	Heartbeat（检测信号）	在 Admin Client 的 Administration（管理）> Configuration（配置）> Device Settings（设置设置）选项卡上设置默认值。
9	TCP Port（TCP 端口）	在 Admin Client 的 Administration（管理）> Configuration（配置）> Device Settings（设置设置）选项卡上设置默认值。
10	Configure All Ports（配置所有端口）	TRUE 或 FALSE Dominion PX 设备的默认值是 TRUE。 其他所有设备的默认值是 FALSE。 在设置为 TRUE 时，配置所有端口，创建节点和适当的带外接口。 在设置为 FALSE 时，只配置那些在 CSV 文件里有相应的 ADD DEVICE-PORT 记录的端口。
11	Allow Direct Access（允许直接访问）	TRUE 或 FALSE 默认值是 FALSE。 此设置仅用于 SX 和 KX2 v2.2 或更高版本的设备。
12	Description（说明）	可选。

在 CSV 文件里添加端口：

只有在把 Configure All Ports（配置所有端口）设置为 FALSE 添加设备并想逐个指定端口时，才使用 DEVICE-PORT 标签。在导入 CSV 文件时，添加的端口必须是尚未在 CC-SG 上配置的端口。

列编号	标签或值	详细信息
1	ADD	所有标签的第一列是命令 ADD。
2	DEVICE-PORT	输入所示的标签。标签不区分大小写。
3	Device Name（设备名称）	必填字段。
4	Port type（端口类型）	必填字段。 输入如下所示的端口类型： KVM

列编号	标签或值	详细信息
		SERIAL（串行） OUTLET（出口）或 POWER（电源） 用 OUTLET（出口）或 POWER（电源）配置 PX 设备的出口。
5	Port or Outlet Number（端口号或出口号）	必填字段。
6	Port or Outlet Name（端口名称或出口名称）	可选。如果保留空白，将使用默认名称或在设备级指定的名称。
7	Node Name（节点名称）	对于 KVM 端口和串行端口，输入在配置此端口时创建的节点的名称。

在 CSV 文件里添加刀片服务器：

列编号	标签或值	详细信息
1	ADD	所有标签的第一列是命令。
2	DEVICE-BLADE	输入所示的标签。 标签不区分大小写。
3	Device Name（设备名称）	必填字段。
4	Port Number（端口号）	必填字段。
5	Blade Number（刀片服务器编号）	必填字段。
6	Blade Name（刀片服务器名称）	可选。如果保留空白，将使用在设备级指定的名称。如果在 CSV 文件里输入名称，将把它复制到设备级。
7	Node Name（节点名称）	输入在配置此刀片服务器时创建的节点的名称。

添加与 KX2 相连的分层 KVM 切换器：

与分层 KVM 切换器相连的 KX2 端口必须作为 KVM 类型导入。

列编号	标签或值	详细信息
1	ADD	所有标签的第一列是命令 ADD。
2	DEVICE-KVMSWITCHPORT	输入所示的标签。 标签不区分大小写。

列编号	标签或值	详细信息
3	Device Name（设备名称）	必填字段。
4	Port Number（端口号）	KVM 切换器连接的端口。必填字段。
5	KVM Switch Port Number（KVM 切换器端口号）	必填字段。
6	KVM Switch Port Name（KVM 切换器端口名称）	可选。如果保留空白，将使用在设备级指定的名称。如果在 CSV 文件里输入名称，将把它复制到设备级。
7	Node Name（节点名称）	在配置此 KVM 切换器端口时，输入要创建的节点的名称。

在 CSV 文件里给设备指定类别和元素：

必须先在 CC-SG 上创建类别和元素。

可以在 CSV 文件里给一台设备指定同一类别的多个元素。

列编号	标签或值	详细信息
1	ADD	所有标签的第一列是命令。
2	DEVICE-CATEGORYELEMENT	输入所示的标签。 标签不区分大小写。
3	Device Name（设备名称）	必填字段。
4	Category Name（类别名称）	必填字段。
5	Element Name（元素名称）	必填字段。

设备 CSV 文件示例

```
ADD, DEVICE, DOMINION KX2, Lab-Test,192.168.50.123,ST Lab KVM, username, password,,,,

ADD, DEVICE-PORT, Lab-Test, KVM, 1, Mail Server, Mail Server

ADD, DEVICE-PORT, Lab-Test, KVM, 2, DNS Server, DNS Server

ADD, DEVICE-PORT, Lab-Test, KVM, 3

ADD, DEVICE-PORT, Lab-Test, KVM, 4

ADD, DEVICE-CATEGORYELEMENT, Lab-Test, Location, Rack17
```

导入设备

在创建 CSV 文件之后，验证此文件是否有错误，然后导入文件。

跳过重复记录，不添加重复记录。

导入设备：

1. 选择 Administration（管理）> Import（导入）> Import Devices（导入设备）。
2. 单击 Browse（浏览）按钮选择要导入的 CSV 文件，然后单击 Open（打开）按钮。
3. 单击 Validate（验证）按钮。Analysis Report（分析报告）区显示文件内容。
   - 如果文件无效，显示错误消息。单击 OK（确定）按钮查看页面 Problems（问题）区显示的文件问题说明。单击 Save to File（保存到文件）按钮保存问题列表。编辑 CSV 文件纠正错误，然后再验证一次。参看*排除 CSV 文件问题* (p. 396)。
4. 单击 Import（导入）按钮。
5. 单击 Actions（操作）区查看导入结果。用绿色文字显示成功导入的项目，用红色文字显示导入失败的项目。由于已经有同名项目，或者已经导入了，也用红色文字显示导入失败的项目。
6. 如要查看导入结果详细信息，查看 Audit Trail（审计跟踪）报告。参看*导入审计跟踪项* (p. 395)。

导出设备

导出文件的最前面有备注，说明文件里的每一项。可以根据备注说明，创建要导入的文件。

注意：不导出 P2SC 设备。

导出设备：

1. 选择 Administration（管理）> Export（导出）> Export Devices（导出设备）。
2. 单击 Export to File（导出成文件）按钮。
3. 输入文件名，然后选择文件保存位置。
4. 单击 Save（保存）按钮。

升级设备

在有新版设备固件时，可以升级设备。

重要说明：查看兼容性指标，确保新设备固件版本兼容 CC-SG 固件版本。如果必须同时升级 CC-SG 和一台设备或一组设备，先升级 CC-SG，再升级设备。

升级设备：

1. 单击 Devices（设备）选项卡，然后在 Devices（设备）树上选择一台设备。
2. 选择 Devices（设备）> Device Manager（设备管理器）> Upgrade Device（升级设备）。
3. Firmware Name（固件名称）：在列表上选择合适的固件。Raritan 或当地销售商提供此类信息。
4. 单击 OK（确定）按钮升级设备。
   - 升级 SX 和 KX 设备大约需要 20 分钟。
   - 如果设备固件版本不兼容 CC-SG，显示一条消息。单击 Yes（是）按钮升级设备。单击 No（否）按钮取消升级。
5. 显示一条消息。单击 Yes（是）按钮重新启动设备。在设备升级之后，显示一条消息。
6. 为了确保浏览器加载所有升级后的文件，先关闭浏览器窗口，然后打开新浏览器窗口登录 CC-SG。

备份设备配置

可以备份所选设备的所有用户配置文件和系统配置文件。如果设备出问题，可以在 CC-SG 上用你创建的备份文件恢复原来的配置。

CC-SG 可以保存的备份文件最大数是每台设备 3 个备份文件。如果需要更多备份文件，可以把备份文件保存到网络上，然后在 CC-SG 上把它删除掉。也可以选择让 CC-SG 自动删除最旧的备份文件。在选择此选项之后，当你尝试进行第四次备份时，显示一条提示消息。参看***把所有配置数据恢复到 KX2、KSX2 或 KX2-101 设备上*** (p. 83)。

每台设备可以备份配置文件的不同部分。参看你要备份的设备的用户指南了解详情。

注意：在备份 SX 3.0.1 设备时，不备份相连电源条的配置。如果用备份文件恢复 SX 3.0.1 设备，必须重新配置电源条。

备份设备配置：

1. 单击 Devices（设备）选项卡，然后选择要备份的设备。
2. 选择 Devices（设备）> Device Manager（设备管理器）> Configuration（配置）> Backup（备份）。
3. 在 Backup name（备份名称）字段里输入此备份文件的名称。
4. 在 Description（说明）字段里输入简短备份说明。**可选。**
5. 单击 OK（确定）按钮备份设备配置。在备份设备配置之后，显示一条消息。

恢复设备配置

下列几类设备允许你恢复全备份的设备配置。

- KX
- KSX
- KX101
- SX
- IP-Reach

KX2、KSX2 和 KX2-101 设备允许你选择把备份的哪些部分恢复到设备上。

- Protected（保护）：除了网络设置（个性化设置包），对 KX2 设备而言是端口配置设置，所选备份文件的所有内容都被恢复到设备上。可以用 Protected（保护）选项把一台设备的备份文件恢复到相同型号的另一台设备上（仅限于 KX2、KSX2 和 KX2-101）。
- Full（全双工）：所选备份文件的所有内容都被恢复到设备上。
- Custom（定制）：允许你恢复 Device Setting（设备设置）和/或 User and User Group Data Settings（用户和用户组数据设置）。

恢复设备配置（KX、KSX、KX101、SX、IP-Reach）

可以把全备份配置恢复到 KX、KSX、KX101、SX 和 IP-Reach 设备上。

▶ **恢复全备份设备配置：**

1. 单击 Device（设备）选项卡，然后选择要把备份配置恢复到哪台设备上。
2. 选择 Devices（设备）> Device Manager（设备管理器）> Configuration（配置）> Restore（恢复）。
3. 在 Available Backups（可用备份）列表上选择要把哪个备份配置恢复到设备上。
4. 单击 OK（确定）按钮。
5. 单击 Yes（是）按钮重新启动设备。在恢复所有数据之后，显示一条消息。

把除网络设置之外的所有配置数据恢复到 KX2、KSX2 或 KX2-101 设备上

Protected（保护）恢复选项允许你把备份文件里除网络设置之外的所有配置数据恢复到 KX2、KSX2 或 KX2-101 设备上。可以用 Protected（保护）选项把一台设备的备份文件恢复到相同型号的另一台设备上（仅限于 KX2、KSX2 和 KX2-101）。

把除网络设置之外的所有配置数据恢复到 KX2、KSX2 或 KX2-101 设备上：

1. 单击 Device（设备）选项卡，然后选择要把备份配置恢复到哪台设备上。
2. 选择 Devices（设备）> Device Manager（设备管理器）> Configuration（配置）> Restore（恢复）。
3. 在 Available Backups（可用备份）列表上选择要把哪个备份配置恢复到设备上。
4. Restore Type（恢复类型）：选择 Protected（保护）。
5. 单击 OK（确定）按钮。
6. 单击 Yes（是）按钮重新启动设备。在恢复所有用户配置数据和系统配置数据之后，显示一条消息。

把设备设置或用户和用户组数据恢复到 KX2、KSX2 或 KX2-101 设备上

Custom（定制）恢复选项允许你恢复设备设置和/或用户和用户组数据。

把设备设置或用户和用户组数据恢复到 KX2、KSX2 或 KX2-101 设备上：

1. 单击 Device（设备）选项卡，然后选择要把备份配置恢复到哪台设备上。
2. 选择 Devices（设备）> Device Manager（设备管理器）> Configuration（配置）> Restore（恢复）。
3. 在 Available Backups（可用备份）列表上选择要把哪个备份配置恢复到设备上。
4. Restore Type（恢复类型）：选择 Custom（定制）。
5. Restore Options（恢复选项）：选择要恢复到设备上的部件：Device Settings（设备设置）、User and User Group Data（用户和用户组数据）。
6. 单击 OK（确定）按钮。

7. 单击 Yes（是）按钮重新启动设备。在恢复数据之后，显示一条消息。

把所有配置数据恢复到 KX2、KSX2 或 KX2-101 设备上

Full（全部）恢复选项允许你把备份文件里的所有配置数据恢复到 KX2、KSX2 或 KX2-101 设备上。

把所有配置数据恢复到 KX2、KSX2 或 KX2-101 设备上：

1. 单击 Device（设备）选项卡，然后选择要把备份配置恢复到哪台设备上。
2. 选择 Devices（设备）> Device Manager（设备管理器）> Configuration（配置）> Restore（恢复）。
3. 在 Available Backups（可用备份）列表上选择要把哪个备份配置恢复到设备上。
4. Restore Type（恢复类型）：选择 Full（全部）。
5. 单击 OK（确定）按钮。
6. 单击 Yes（是）按钮重新启动设备。在恢复所有用户配置数据和系统配置数据之后，显示一条消息。

保存、上载和删除设备备份文件

可以把 Restore Device Configuration（恢复设备配置）页面上的设备备份文件保存到网络或本地机器上。如果必须在 CC-SG 上给新备份文件腾出存储空间，可以删除设备备份文件。也可以把保存在网络上的设备备份文件上载到 CC-SG 上，用它们恢复设备配置。

保存 CC-SG 上的设备备份文件：

1. 单击 Devices（设备）选项卡，然后选择一台设备。
2. 选择 Devices（设备）> Device Manager（设备管理器）> Configuration（配置）> Restore（恢复）。
3. 选择要保存的设备备份文件。单击 Save to File（保存到文件）按钮。
4. 找到文件保存位置。单击 Save（保存）按钮。

删除 CC-SG 上的设备备份文件：

1. 单击 Devices（设备）选项卡，然后选择一台设备。
2. 选择 Devices（设备）> Device Manager（设备管理器）> Configuration（配置）> Restore（恢复）。
3. 选择要删除的设备备份文件。单击 Delete（删除）按钮。
4. 单击 Yes（是）按钮确认。

把设备备份文件上载到 CC-SG 上：

1. 单击 Devices（设备）选项卡，然后选择一台设备。
2. 选择 Devices（设备）> Device Manager（设备管理器）> Configuration（配置）> Restore（恢复）。
3. 单击 Upload（上载）按钮找到并选择设备备份文件。文件类型是 .rfp。单击 Open（打开）按钮。

   设备备份文件上载到 CC-SG 上，页面显示此文件。

复制设备配置

可以把下列型号的设备的配置从一台设备复制到另一台或多台其他设备上。

- SX
- KX2
- KSX2
- KX2-101

只能在端口数相同的同型号设备之间复制配置，例如只能把 KX2-864 设备的配置复制到其他 KX2-864 设备上。

复制配置命令复制除网络设置（个性化包）之外的所有配置数据，KX2 设备的网络配置为端口配置设置。在此过程中复制所有 Device Settings（设备设置）和 User and User Group Data（用户和用户组数据）。

复制设备配置：

1. 单击 Devices（设备）选项卡，然后在 Devices（设备）树上选择要把哪台设备的配置复制到其他设备上。
2. 选择 Devices（设备）> Device Manager（设备管理器）> Configuration（配置）> Copy Configuration（复制配置）。
3. 选择配置复制方法。
   - 如要复制当前配置数据，选择 Copy From Device（从设备复制）。
   - 如要复制此前保存在 CC-SG 上的备份文件里的配置数据，选择 Copy From Backup File（从备份文件复制），然后在下拉列表上选择备份文件。如果没有备份文件，此选项被禁用。
4. 单击 Device Group（设备组）下拉箭头，然后在列表上选择一个设备组。Available（可用）列显示选择的设备组里的所有设备。

5. 在 Available（可用）列上突出显示你要把此配置复制到哪些设备上，然后单击右箭头把它移动到 Selected（选择）列上。单击左箭头把选择的设备从 Selected（选择）列上删除掉。
6. 单击 OK（确定）按钮把配置复制到 Selected（选择）列上的设备上。
7. 在显示重新启动消息时，单击 Yes（是）按钮重新启动设备。在复制设备配置之后，显示一条消息。

重新启动设备

用重新启动设备功能重新启动设备。

重新启动设备：

1. 单击 Devices（设备）选项卡，然后选择要重新启动的设备。
2. 选择 Devices（设备）> Device Manager（设备管理器）> Restart Device（重新启动设备）。
3. 单击 OK（确定）按钮重新启动设备。
4. 单击 Yes（是）按钮确认让现在访问设备的所有用户退出设备。

对设备执行 ping 命令

可以给设备发出 ping 命令，确定网络设备是否可用。

如果设备在双协议堆模式下工作，CC-SG 按顺序 ping 每个地址，并显示每个地址返回的结果。如果设备按主机名管理，ping 结果还显示主机名。

对设备执行 ping 命令：

1. 单击 Devices（设备）选项卡，然后选择要对哪台设备执行 ping 命令。
2. 选择 Devices（设备）> Device Manager（设备管理器）> Ping Device（对设备执行 ping 命令），打开 Ping Device（对设备执行 ping 命令）屏幕，显示 ping 命令执行结果。

让 CC-SG 暂停管理设备

可以暂停设备，让 CC-SG 暂时停止管理设备，但 CC-SG 并不会失去内部存储的任何配置数据。

如要预订一个任务来暂停或恢复设备管理，参看*预定任务* (p. 299)。

让 CC-SG 暂时停止管理设备：

1. 单击 Devices（设备）选项卡，然后选择要 CC-SG 暂停管理哪台设备。
2. 选择 Devices（设备）> Device Manager（设备管理器）> Pause Management（暂停管理），Device Tree（设备树）显示的设备图标表示设备处于暂停状态。

恢复设备管理

可以让 CC-SG 恢复管理被暂停的设备，将被暂停的设备重新置于 CC-SG 控制之下。

在恢复管理双协议堆设备时启用双协议堆，在退出管理时禁用双协议堆。CC-SG 必须检查 IPv6 地址是否与其他网管设备发生冲突。如果检测到冲突，只用 IPv4 地址管理此设备，并记录并记录错误消息。

Error text includes: "An IPv6 address conflict was detected. 只恢复用 IPv4 地址进行设备管理。）

让 CC-SG 恢复管理被暂停的设备：

1. 单击 Devices（设备）选项卡，然后在 Devices（设备）树上选择被暂停的设备。
2. 选择 Devices（设备）> Device Manager（设备管理器）> Resume Management（恢复管理），Devices（设备）树显示的设备图标表示设备处于活动状态。

用预定任务功能暂停和恢复设备管理

为了一次性暂停或恢复多台设备或多个设备组，可以预定一个任务对设备组逐个执行操作。

暂停/恢复设备管理任务不适用于与网管设备相连的刀片服务器机箱、与网管设备相连的电源条和网管电源条。

在执行此任务时，如果所有设备操作成功，就在日志里记录任务成功。如果此任务完成，但某些设备操作在尝试了允许的次数之后失败了，就在日志里记录任务成功但有异常。如果所有设备操作失败，就在日志里记录任务失败。

用预定任务批量暂停和恢复设备：

1. 选择 Administration（管理）> Tasks（任务）。参看*预定任务* (p. 299)详细了解如何创建新任务，如何配置 Main（主要）选项卡、Recurrence（重复执行）选项卡、Retry（重试）选项卡和 Notification（通知）选项卡。
   - Recurrence（重复执行）：重复执行间隔时间限于几个小时和几天。
   - Retry（重试）：CC-SG 只对暂停或恢复失败的设备重试操作。
2. 在 Task Data（任务数据）选项卡上的 Task Operation（任务操作）字段里选择 Pause/Resume Device Management（暂停/恢复设备管理）。
3. 选择 Pause Management（暂停管理）或 Resume Management（恢复管理）。如果必须执行这两个任务，针对每个操作预定一个任务，并协调好两个任务的间隔时间。
4. 在 Interval (seconds)（间隔时间[秒]）字段里输入在 CC-SG 完成一个操作之后，间隔多久开始执行下一个操作。
5. 如果希望 CC-SG 不对那些可能要求重新启动的任何所选设备执行暂停或恢复操作，选择 Skip Device if Restart Required（在要求重新启动时跳过设备）复选框。
6. 在 Device Group（设备组）下拉列表上选择一个设备组，然后选择任务要包括的设备。在 Available（可用）列表上选择要包括的设备，然后单击箭头按钮把它们移动到 Selected（已选择）列表上。暂停或恢复操作将包括 Selected（已选择）列表上的设备。
   - 如果选择了 Skip Device if Restart Required（在要求重新启动时跳过设备）复选框，在运行此任务时，将跳过那些可能要求重新启动的任何所选设备。
7. 单击 OK（确定）按钮。

设备电源管理器

用设备电源管理器查看电源条设备的状态（包括电压、电流和温度），管理电源条设备的所有电源出口。设备电源管理器提供以电源条为中心的出口视图。

在使用设备电源管理器之前，必须在电源条与 Dominion SX 或 Dominion KSX 设备之间建立物理连接。在添加电源条设备时，必须定义哪台 Raritan 设备要提供连接。这将使它与 SX 串行端口或提供电源条管理的 KSX 专用出口关联。

查看设备电源管理器：

1. 在 Devices（设备）选项卡上选择一台电源条设备。
2. 选择 Devices（设备）> Device Power Manager（设备电源管理器）。
3. Outlets Status（出口状态）面板列出出口。可能要翻页，才能看到所有出口。
   - 在每个出口对应的下拉列表上选择 On（通电）或 Off（断电），给出口通电或断电。
   - 在下拉列表上选择 Recycle（重新通电），重新启动与出口相连的设备。

启动设备管理页面

如果启动管理命令可用于所选的设备，可以用它访问设备的管理员界面。

启动设备管理页面：

1. 单击 Devices（设备）选项卡，然后选择要启动哪台设备的管理员界面。
2. 选择 Devices（设备）> Device Manager（设备管理器）> Launch Admin（启动管理），打开所选设备对应的管理员界面。

断开用户

管理员可以终止一台设备上的任何用户会话。这包括正在设备上执行任何操作的用户，例如连接端口，备份设备配置，恢复设备配置或升级设备固件。

在终止用户与设备之间的会话之前，允许完成固件升级、设备配置备份和恢复。其他所有操作将立即终止。

对于 Dominion SX 设备，只能断开直接登录设备的用户，以及通过 CC-SG 连接设备的用户。

让用户断开设备：

1. 单击 Devices（设备）选项卡，然后选择要用户断开哪台设备。
2. 选择 Deviecs（设备）> Device Manager（设备管理器）> Disconnect Users（断开用户）。
3. 在 Disconnect Users（断开用户）表上选择要断开哪个用户的会话。
4. 单击 Disconnect（断开）按钮让用户断开设备。

特别访问 **Paragon II** 系统设备

Paragon II System Controller (P2-SC)

Paragon II System Integration 用户可以把自己的 P2-SC 设备添加到 CC-SG 设备树上，通过 CC-SG 的 P2-SC Admin 应用程序配置这些设备。参看 Raritan **Paragon II System Controller 用户指南**详细了解如何使用 P2-SC Admin。

在把 Paragon System 设备（Paragon System 包括 P2-SC 设备、相连的 UMT 设备和相连的 IP-Reach 设备）添加到 CC-SG 之后，Devices（设备）树显示此设备。

在 CC-SG 上访问 Paragon II System Controller：

1. 单击 Devices(设备)选项卡，然后选择 Paragon II System Controller。
2. 选择 Devices(设备)> Device Manager(设备管理器)> Launch Admin（启动管理），用新浏览器窗口启用 Paragon II System Controller 应用程序。可以配置 PII UMT 设备。

IP-Reach 和 UST-IP 管理

可以直接在 CC-SG 界面上对与 Paragon System 相连的 IP-Reach 和 UST-IP 设备执行管理诊断。

在把 Paragon System 设备添加到 CC-SG 之后，Devices（设备）树显示此设备。

▶ **访问远程用户工作站管理：**

1. 单击 Devices（设备）选项卡，然后选择 Paragon II System Controller。
2. 选择 Devices（设备）> Device Manager（设备管理器）> Launch User Station Admin（启动用户工作站管理）。

Ch 7 网管电源条

在使用电源条时，可以在 CC-SG 上采用三种方法配置电源控制。

1. 支持的所有 Raritan 电源条可以连接另一台 Raritan 设备，可以作为电源条设备添加到 CC-SG。Raritan 电源条包括 Dominion PX 电源条和 RPC 电源条。参看“兼容性指标”部分了解支持的版本。如要在 CC-SG 上配置这种网管电源条，必须了解电源条物理连接哪种 Raritan 设备。参看*在 CC-SG 上配置被另一台设备管理的电源条* (p. 92)。
2. Dominion PX 电源条可以直接连接 IP 网络，可以作为 PX 设备添加到 CC-SG。如果 PX 电源条直接连接 IP 网络，不必把它们连接到另一台 Raritan 设备。
3. 可以配置 Raritan Power IQ 服务接口实现多供应商 PDU 支持。参看***Power IQ IT 设备电源控制*** (p. 362)。

无论采用哪种连接方法，都必须把网管电源条接口添加到节点上，在出口及其供电节点之间建立电源关联。参看*网管电源条连接接口* (p. 130)。

Dominion PX 特殊说明

无论选择用哪种方法配置 PX，都应该采用一种方法配置所有电源关联，即要么作为网管设备的电源条，要么作为 PX 设备，但不能同时作为二者。如果 Dominion PX 受 Power IQ 管理，可以给一个节点创建一个 Power Control - Managed Power Strip（电源控制 – 网管电源条）接口或 Power Control – Power IQ Proxy（电源控制 – Power IQ Proxy）接口，但不能同时给两个节点创建接口。

此外，可以把 PX 连接到管理设备并配置电源关联，也可以把同一台 PX 设备连接到 IP 网络，用 PX web 客户机查看和收集电源数据。参看 Raritan 网站上支持部分的固件和文档下的 Raritan **Dominion PX 用户指南**。

在本章内

在 CC-SG 上配置被另一台设备管理的电源条

可以在 CC-SG 上把被网电源条连接到下列其中一台设备：

- Dominion KX
- Dominion KX2
- Dominion KX2-101
- Dominion SX 3.0
- Dominion SX 3.1
- Dominion KSX
- Dominion KSX2
- Paragon II/Paragon II System Controller (P2SC)
- Power IQ — 参看 ***Power IQ IT 设备电源控制*** (p. 362)

必须了解网管电源条物理连接哪个 Raritan 设备。

*注意：也可以把 Dominion PX 电源条连接到 IP 网络，但不连接其他任何 Raritan 设备。参看***网管电源条** *(p. 91)详细了解如何给这些电源条配置电源控制。*

在 CC-SG 上配置网管电源条：

1. 在设备、电源条和电源条供电的节点之间建立所有物理连接。参看 **RPC 快速设置指南**、**Dominion PX 快速设置指南**和 **CC-SG 部署指南**详细了解电源条、设备和节点之间的物理连接。
2. 把管理设备添加到 CC-SG。对于不同的 Raritan 设备，操作步骤有所不同。参看与电源条相连的设备对应的章节：
   - ***配置与 KX、KX2、KX2-101、KSX2 和 P2SC 相连的电源条*** (p. 93)
   - ***配置与 SX 3.0 和 KSX 相连的电源条*** (p. 94)
   - ***配置与 SX 3.1 相连的电源条*** (p. 95)
3. 配置出口。参看***配置电源条出口*** (p. 97)。
4. 使每个出口与其供电节点关联。参看***网管电源条连接接口*** (p. 130)。

配置与 KX、KX2、KX2-101、KSX2 和 P2SC 相连的电源条

CC-SG 自动检测与 KX、KX2、KX2-101、KSX2 和 P2SC 设备相连的电源条。可以在 CC-SG 上执行下列任务，配置和管理与这些设备相连的电源条。

添加与 KX、KX2、KX2-101、KSX2 或 P2SC 设备相连的电源条设备

在把与电源条相连的 KX、KX2、KX2-101、KSX2 或 P2SC 设备添加到 CC-SG 时，自动添加电源条。在 Devices（设备）选项卡上，在电源条相连的设备下面显示电源条。

接下来的步骤：

1. 配置出口。参看*配置电源条出口* (p. 97)。
2. 使每个出口与其供电节点关联。参看*网管电源条连接接口* (p. 130)。

把 KX、KX2、KX2-101、KSX2 或 P2SC 的电源条移动到不同的端口

在把电源条从一台 KX、KX2、KX2-101、KSX2 或 P2SC 设备或一个端口物理移动到另一台 KX、KX2、KX2-101、KSX2 或 P2SC 设备或另一个端口时，CC-SG 自动检测电源条，自动更新设备关联。你不必另外把电源条添加到 CC-SG。

*注意：如果把电源条从 P2SC 端口上物理删除掉，但不把它插入另一个端口，CC-SG 并不把它从旧端口上删除掉。你必须对电源条相连的 UMT 执行部分或全部数据库复位，才能在 Devices（设备）选项卡上删除此电源条。参看 **Raritan P2SC 用户指南**。*

删除与 KX、KX2、KX2-101、KSX2 或 P2SC 设备相连的电源条

不能在 CC-SG 上删除与 KX、KX2、KX2-101、KSX2 或 P2SC 设备相连的电源条。必须物理断开电源条和设备，才能在 CC-SG 上删除电源条。在物理断开电源条和设备时，Devices（设备）选项卡不再显示电源条和配置的所有出口。

配置与 SX 3.0 和 KSX 相连的电源条

可以在 CC-SG 上执行下列任务，配置和管理与 SX 3.0 或 KSX 设备相连的电源条。

注意：电源条必须物理连接 KSX 设备的 Power Port（电源端口）。

- ***添加与 SX 3.0 或 KSX 设备相连的电源条*** (p. 94)
- ***删除与 SX 3.0 或 KSX 设备相连的电源条*** (p. 95)
- ***更改电源条的设备或端口关联 (SX 3.0, KSX)*** (p. 95)

添加与 SX 3.0 或 KSX 设备相连的电源条

1. 把 SX 3.0 或 KSX 设备添加到 CC-SG。参看***添加 KVM 设备或串行设备*** (p. 50)。
2. 选择 Devices（设备）> Device Manager（设备管理器）> Add Device（添加设备）。
3. 单击 Device type（设备类型）下拉菜单，然后选择 PowerStrip（电源条）。
4. 在 Power Strip Name（电源条名称）字段里输入电源条的名称。让光标停留在此字段上，可以看到名称允许的字符数。不允许使用空格。
5. 单击 Number of Outlets（出口数）下拉菜单，然后选择此电源条的出口数。
6. 单击 Managing Device（管理设备）下拉菜单，然后选择此电源条相连的 SX 3.0 或 KSX 设备。
7. 单击 Managing Port（管理端口）下拉菜单，然后选择此电源条相连的 SX 3.0 或 KSX 设备的端口。
8. 在 Description（说明）字段里输入此电源条的简短说明。**可选。**
9. 如果要自动把此电源条的每个出口添加到 Devices（设备）选项卡上，选择 Configure All Outlets（配置所有出口）。如果现在不配置所有出口，可以稍后配置这些出口。参看***配置电源条出口*** (p. 97)。**可选。**
10. 对于列出的每个类别，单击 Element（元素）下拉菜单，然后选择要应用于此设备的元素。对于不想使用的每个类别，在 Element（元素）字段里选择空项。参看***关联、类别和元素*** (p. 37)。**可选。**
11. 在配置此电源条时，单击 Apply（应用）按钮添加此设备，打开 Add Device（添加设备）空白屏幕，你可以继续添加设备；也可以单击 OK（确定）按钮添加此电源条，不继续打开 Add Device（添加设备）屏幕。

接下来的步骤：

1. 配置出口。参看*配置电源条出口* (p. 97)。
2. 使每个出口与其供电节点关联。参看*网管电源条连接接口* (p. 130)。

删除与 SX 3.0 或 KSX 设备相连的电源条

即使电源条仍然物理连接 SX 3.0、KSX 或 P2SC 设备，仍然可以删除此电源条。如果物理断开电源条及其关联的 SX 3.0、KSX 或 P2SC 设备，Devices（设备）选项卡上的设备下面仍然显示此电源条。如要不显示此电源条，必须删除此电源条。

1. 在 Devices（设备）选项卡上选择要删除的电源条。
2. 选择 Devices（设备）> Device Manager（设备管理器）> Delete Device（删除设备）。
3. 单击 OK（确定）按钮删除此电源条。在删除电源条之后，显示一条消息。Devices（设备）选项卡不再显示电源条图标。

更改电源条的设备或端口关联 (SX 3.0, KSX)

如果把电源条从一台 SX 3.0 或 KSX 设备或一个端口物理移动到另一台 SX 3.0 或 KSX 设备或另一个端口上，必须在 CC-SG 上更改 PowerStrip Profile（电源条配置文件）里的关联。

1. 在 Devices（设备）选项卡上选择要移动的电源条。
2. 单击 Managing Device（管理设备）下拉菜单，然后选择此电源条相连的 SX 3.0 或 KSX 设备。
3. 单击 Managing Port（管理端口）下拉菜单，然后选择此电源条相连的 SX 3.0 或 KSX 设备的端口。
4. 单击 OK（确定）按钮。

配置与 SX 3.1 相连的电源条

可以在 CC-SG 上执行下列任务，配置和管理与 SX 3.1 设备相连的电源条。

- *添加与 SX 3.1 设备相连的电源条* (p. 96)
- *把 SX 3.1 的电源条移动到不同的端口* (p. 96)
- *删除与 SX 3.1 设备相连的电源条* (p. 97)

添加与 SX 3.1 设备相连的电源条

添加与 SX 3.1 设备相连的电源条的步骤取决于 SX 3.1 设备是否已被添加到 CC-SG。

如果电源条连接 SX 3.1 设备，且此设备尚未添加到 CC-SG：

1. 把 SX 3.1 设备添加到 CC-SG。参看*添加 KVM 设备或串行设备* (p. 50)。
2. CC-SG 自动检测并添加电源条。在 Devices（设备）选项卡上，在电源条相连的 SX 3.1 设备下面显示此电源条。

如果 SX 3.1 设备已被添加到 CC-SG，电源条稍后被连接到此设备：

1. 把 SX 3.1 设备添加到 CC-SG。参看*添加 KVM 设备或串行设备* (p. 50)。
2. 配置 SX 3.1 设备的端口。参看*配置端口* (p. 57)。
3. 在 Devices（设备）选项卡上选择电源条连接的 SX 3.1 设备。
4. 单击设备图标旁边的 + 号展开端口列表。
5. 用右键单击电源条连接的 SX 3.1 端口，然后在弹出菜单上选择 Add Powerstrip（添加电源条）。
6. 输入电源条出口数，然后单击 OK（确定）按钮。

接下来的步骤：

1. 配置出口。参看*配置电源条出口* (p. 97)。
2. 使每个出口与其供电节点关联。参看*网管电源条连接接口* (p. 130)。

把 SX 3.1 的电源条移动到不同的端口

在把电源条从一台 SX 3.1 设备或一个端口物理移动到另一台 SX 3.1 设备或另一个端口时，必须在旧 SX 3.1 端口上删除此电源条，并把它添加到新 SX 3.1 端口。参看*删除与 SX 3.1 设备相连的电源条* (p. 97)和*添加与 SX 3.1 设备相连的电源条* (p. 96)。

删除与 SX 3.1 设备相连的电源条

即使电源条仍然物理连接 SX 3.1 设备，仍然可以删除此电源条。如果物理断开电源条及其关联的 SX 3.1 设备，Devices（设备）选项卡上的设备下面仍然显示此电源条。如要不显示此电源条，必须删除此电源条。

▶ **删除与 SX 3.1 设备相连的电源条：**

1. 在 Devices（设备）选项卡上选择要删除的电源条。
2. 选择 Devices（设备）> Device Manager（设备管理器）> Delete Device（删除设备）。
3. 单击 OK（确定）按钮删除电源条。在删除电源条之后，显示一条消息。Devices（设备）选项卡不再显示电源条图标。

配置电源条出口

在使电源条出口与节点关联之前，必须配置出口：把网管电源条接口添加到节点。参看*网管电源条连接接口* (p. 130)。

▶ **在电源条配置文件上配置出口：**

1. 在 Devices（设备）选项卡上，单击与电源条相连的设备旁边的 + 号。
2. 选择要配置哪个电源条的出口。
3. 在 Device Profile: PowerStrip（设备配置文件：电源条）屏幕上选择 Outlets（出口）选项卡。
4. 选择要配置的每个出口对应的复选框，然后单击 OK（确定）按钮。

在 Devices（设备）选项卡上，电源条图标下面显示这些出口。

▶ **在 Configure Ports（配置端口）屏幕上配置出口：**

1. 在 Devices（设备）选项卡上，单击与电源条相连的设备旁边的 + 号。
2. 选择要配置哪个电源条的出口。
3. 选择 Devices（设备）> Port Manager（端口管理器）> Configure Ports（配置端口）。
   - 如要给多个出口配置屏幕显示的默认名称，选择要配置的每个出口对应的复选框，然后单击 OK（确定）按钮给每个出口配置默认名称。
   - 如要逐个配置每个出口，单击出口旁边的 Configure（配置）按钮，然后在 Port name（端口名称）字段里输入出口名称。单击 OK（确定）按钮配置端口。

删除出口：

1. 在 Devices（设备）选项卡上，单击与电源条相连的设备旁边的 + 号。
2. 单击电源条旁边的 + 号。
3. 选择 Devices（设备）> Port Manager（端口管理器）> Delete Ports（删除端口）。
4. 选择要删除的每个出口对应的复选框，然后单击 OK（确定）按钮删除出口。

Ch 8 节点、节点组和接口

本章讨论如何查看、配置和编辑节点及其关联接口，如何创建节点组。简单讨论如何连接节点。参看 Raritan **CommandCenter Secure Gateway 用户指南**详细了解如何连接节点。

在本章内

节点和接口概述

关于节点

每个节点表示一个可通过 CC-SG 采用带内（直接 IP）方法或带外（连接 Raritan 设备）方法访问的目标。例如节点可以是机架上与 Raritan KVM over IP 设备相连的服务器、配有 HP iLO 卡的服务器、运行 VNC 的联网 PC 或使用远程串行管理连接的联网基础设施。

在把与节点相连的设备添加到 CC-SG 之后，可以人工把这些节点添加到 CC-SG。在添加设备时，也可以在 Add Device（添加设备）屏幕上选择 Configure all ports（配置所有端口）复选框，自动创建节点。此选项允许 CC-SG 自动添加所有设备端口，给每个端口添加一个节点和一个带外 KVM 接口或串行接口。随时可以编辑这些节点、端口和接口。

节点名称

节点名称必须是唯一的。如果你尝试用现有节点名称人工添加一个节点，CC-SG 会提示你名称重复。当 CC-SG 自动添加节点时，编号系统确保节点名称是唯一的。

参看*命名常规* (p. 431)详细了解 CC-SG 的名称长度规则。

关于接口

在 CC-SG 上通过接口访问节点，必须给每个新节点添加至少一个接口。可以添加不同类型的接口实现不同类型的访问，例如带外 KVM 接口、串行接口、电源控制接口、带内 SSH/RDP/VNC 接口、DRAC/RSA/ILO、Web 接口或 Telnet 访问接口，视节点类型而定。

一个节点可以有多个接口，但只能有一个带外串行接口或带外 KVM 接口。例如一台 Windows 服务器可能有一个带外 KVM 接口连接键盘端口、鼠标端口和监视器端口，还有一个出口管理与服务器相连的出口。

即使你配置 CC-SG 使用代理模式，某些接口也只能在直连模式下工作。这些接口包括 ILO、RSA、Microsoft RDP、DRAC、网络浏览器和 VMware Viewer。Java RDP 接口可以在代理模式下使用。 参看*关于连接模式* (p. 267)。

查看节点

在 CC-SG 上，可以在 Nodes（节点）选项卡上查看所有节点，选择节点查看其 Node Profile（节点配置文件）。

节点选项卡

在单击 Nodes（节点）选项卡时，采用树结构显示你可以访问的所有节点。

节点按名称字母顺序排序，或者按可用性状态分成组。按可用性状态分成组的节点，在可用性组里按字母顺序排序。如要切换排序方式，用右键单击树，单击 Node Sorting Options（节点排序选项），然后单击 By Node Name（按节点名称）或 By Node Status（按节点状态）排序节点。

参看*设备和节点定制视图* (p. 191)详细了解如何采用不同的方式查看节点选项卡。

节点配置文件

单击 Nodes（节点）选项卡上的一个节点打开 Node profile（节点配置文件）页面。Node Profile（节点配置文件）页有几个选项卡，显示有关节点的信息。

Interfaces（接口）选项卡

Interfaces（接口）选项卡包括节点的所有接口。可以在此选项卡上添加、编辑和删除接口，选择默认接口。支持虚拟媒体的节点有一个附加列，显示虚拟媒体是被启用还是禁用了。

Associations（关联）选项卡

Associations（关联）选项卡包含给节点指定的所有类别和元素。可以选择不同的关联，从而更改关联。

参看*关联、类别和元素* (p. 37)。

Location & Contacts（位置和联系人）选项卡

Location & Contacts（位置和联系人）选项卡包含你在处理设备时可能需要的设备位置信息和联系人信息，例如电话号码。可以在字段里输入新信息，从而更改信息。

参看*给节点配置文件增加位置和联系人* (p. 108)。

Notes（备注）选项卡

Notes（备注）选项卡包含备注添加工具，便于用户添加供其他用户阅读的设备备注。此选项卡显示所有备注，包括用户添加备注的日期、他的用户名和 IP 地址。

如果你有设备、端口和节点管理权限，可以清除节点配置文件里的所有备注。单击 Clear（清除）按钮。

参看*给节点配置文件增加备注* (p. 108)。

Audit（审计）选项卡

可以在 Audit（审计）选项卡上查看访问节点的原因。如果针对用户组启用了节点审计，用户必须在连接节点之前输入访问原因。

如果禁用审计，或者已经输入了访问原因，不显示 Audit（审计）选项卡。

参看*配置用户组访问审计* (p. 172)。

Control System Data（控制系统数据）选项卡

VMware Virtual Center 等控制系统服务器节点有 Control System Data（控制系统数据）选项卡。Control System Data（控制系统数据）选项卡包含来自控制系统服务器的信息，每次打开选项卡时自动刷新。可以访问虚拟基础设施拓扑视图，链接关联的节点配置文件，或者连接控制系统打开 Summary（摘要）选项卡。

Virtual Host Data（虚拟主机数据）选项卡

VMware ESX 服务器等虚拟主机节点有 Virtual Host Data（虚拟主机数据）选项卡。Virtual Host Data（虚拟主机数据）选项卡包含来自虚拟主机服务器的信息，每次打开选项卡时自动刷新。可以访问虚拟基础设施拓扑视图，链接关联的节点配置文件，或者连接虚拟主机打开 Summary（摘要）选项卡。如果你有设备、端口和节点管理权限，可以重新启动和强制重新启动虚拟主机服务器。

Virtual Machine Data（虚拟机数据）选项卡

VMware Virtual Machines 等虚拟机节点有 Virtual Machine Data（虚拟机数据）选项卡。Virtual Machine Data（虚拟机数据）选项卡包含来自虚拟机的信息，每次打开选项卡时自动刷新。可以访问虚拟基础设施拓扑视图，链接关联的节点配置文件，或者连接虚拟主机打开 Summary（摘要）选项卡。

刀片服务器选项卡

IBM BladeCenter 等刀片服务器机箱节点有一个 Blades（刀片服务器）选项卡。Blades（刀片服务器）选项卡包含有关刀片服务器机箱上的刀片服务器的信息。

节点和接口图标

为便于识别，节点在 Nodes（节点）树上使用不同的图标。让鼠标指针停留在 Nodes（节点）树上的一个图标上，可以看到有关节点信息的工具提示。

图标	含义
	节点可用 — 节点至少有一个活动接口。
	节点不可用 — 节点没有活动接口。

服务帐号

服务帐号概述

服务帐号是你给多个接口指定的特殊登录证书。给要求频繁更改密码的一组接口指定一个服务帐号，可以节省时间。可以更新服务帐号的登录证书，使用此服务帐号的每个接口均反映此更改。

服务帐号不能用于带外接口或网管电源条接口。

- 对于 DRAC、iLO 和 RSA 接口，登录证书应用于嵌入式处理器卡，而不应用于基础操作系统。
- 对于 RDP、SSH 和 Telnet 接口，登录证书应用于操作系统。
- 对于 VNC 接口，登录证书应用于 VNC 服务器。
- 对于网络浏览器界面，登录证书应用于在界面上指定的 URL 上的可用表单。

查看服务帐号：

- 选择 Nodes（节点）> Service Accounts（服务帐号），打开 Service Accounts（服务帐号）页。
- 单击列标题按此属性升序顺序排序表。再次单击此标题按降序顺序排序表。 **可选。**

字段	Description（说明）
Service Account Name（服务帐号名称）	在接口对话框和 Assign Service Account（指定服务帐号）页面上，用此名称标识服务帐号。
Username（用户名）	在给接口指定服务帐号时，此用户名用作登录证书的一部分。
Password（密码）	在给接口指定服务帐号时，此密码用作登录证书的一部分。
Retype Password（再次输入密码）	此字段用于确保正确输入密码。
Description（说明）	此说明可以包括你要添加的有关服务帐号的任何附加信息。

添加、编辑和删除服务帐号

添加服务帐号：

1. 选择 Nodes（节点）> Service Accounts（服务帐号），打开 Service Accounts（服务帐号）页。
2. 单击 Add Row（添加行）图标  在表上添加一行。
3. 在 Service Account Name（服务帐号名称）字段里输入此服务帐号的名称。
4. 在 Username（用户名）字段里输入用户名。
5. 在 Password（密码）字段里输入密码。
6. 在 Retype Password（再次输入密码）字段里再次输入密码。
7. 在 Description（说明）字段里输入此服务帐号的说明。
8. 单击 OK（确定）按钮。

编辑服务帐号：

1. 选择 Nodes（节点）> Service Accounts（服务帐号），打开 Service Accounts（服务帐号）页。
2. 查找要编辑的服务帐号。
3. 编辑字段。不能编辑 Service Account Name（服务帐号名称）字段。

注意：在更改用户名或密码时，CC-SG 更新使用此服务帐号的所有接口，以便使用新登录证书。

4. 单击 OK（确定）按钮。

删除服务帐号：

1. 选择 Nodes（节点）> Service Accounts（服务帐号），打开 Service Accounts（服务帐号）页。
2. 选择要删除的服务帐号。
3. 单击 Delete Row（删除行）按钮。 
4. 单击 OK（确定）按钮。

更改服务帐号密码

更改服务帐号密码：

1. 选择 Nodes（节点）> Service Accounts（服务帐号），打开 Service Accounts（服务帐号）页。
2. 查找要更改哪个服务帐号的密码。
3. 在 Password（密码）字段里输入新密码。
4. 在 Retype Password（再次输入密码）字段里再次输入密码。
5. 单击 OK（确定）按钮。

注意：在更改用户名或密码时，CC-SG 更新使用此服务帐号的所有接口，以便使用新登录证书。

给接口指定服务帐号

可以给多个接口指定一个服务帐号。指定了服务帐号的每个接口用相同的登录信息建立连接。

在更改用户名或密码时，CC-SG 更新使用此服务帐号的所有接口，以便使用新登录证书。

也可以在配置接口时选择一个服务帐号。参看***添加、编辑和删除接口*** (p. 122)。

你必须有设备、端口和节点管理权限，才能给接口指定服务帐号。参看***添加、编辑和删除用户组*** (p. 169)。

给接口指定服务帐号：

1. 选择 Nodes（节点）> Assign Service Accounts（指定服务帐号），打开 Assign Service Accounts（指定服务帐号）页面。
2. 在 Service Account Name（服务帐号名称）字段里选择要给节点指定哪个服务帐号。
3. 在 Available（可用）列表上选择要给哪些接口指定此服务帐号。按住 Ctrl 或 Shift 单击接口选择多个接口。

   *提示：在 Find（查找）字段里输入节点名称，在列表上突出显示此名称。在不完整名称后面输入 *，在列表上突出显示所有类似名称。*

   单击列标题按字母顺序排序列表。
4. 单击 Add（添加）按钮把所选接口移动到 Selected（选择）列表上。
5. 单击 OK（确定）按钮把服务帐号指定给 Selected（选择）列表上的所有节点。

注意：在更改用户名或密码时，CC-SG 更新使用此服务帐号的所有接口，以便使用新登录证书。

添加、编辑和删除节点

添加节点

把节点添加到 CC-SG：

1. 单击 Nodes（节点）选项卡。
2. 选择 Nodes（节点）> Add Node（添加节点）。
3. 在 Node Name（节点名称）字段里输入节点名称。在 CC-SG 上，所有节点名称必须是唯一的。参看***命名常规*** (p. 431)详细了解 CC-SG 的名称长度规则。
4. 在 Description（说明）字段里输入此节点的简短说明。**可选。**
5. 必须配置至少一个接口。单击 Add Node(添加节点)界面上 Interfaces（接口）部分的 Add（添加）按钮添加一个接口。参看***添加接口*** (p. 122)。
6. 可以配置一个 Categories（类别）和 Elements（元素）列表，更好地描述和组织管理此节点。参看***关联、类别和元素*** (p. 37)。**可选。**
   - 对于列出的每个类别，单击 Element（元素）下拉菜单，然后在列表上选择要应用于节点的元素。

   注意：CC-SG 默认让默认类别名称 System Type（系统类型）和 US States and territories（美国州和领地）保留英文。

   - 对于不想使用的每个类别，在 Element（元素）字段里选择空项。
   - 如果看不到你要使用的类别值或元素值，可以用 Associations（关联）菜单添加这些值。参看***关联、类别和元素*** (p. 37)。
7. 单击 OK（确定）按钮保存更改。把节点添加到节点列表上。

重要说明：如果把刀片服务器机箱从一个 Dominion 设备端口移到另一个 Dominion 设备端口，丢失在 CC-SG 上给此刀片服务器机箱节点添加的接口，但保留其他所有信息。

通过配置端口创建的节点

在配置设备端口时，自动给每个端口创建一个节点。同时给每个节点创建一个接口。

在自动创建节点时，所使用的名称与它关联的端口相同。如果此节点名称已经有了，在节点名称后面增加一个后缀，例如 Channel1(1)，括号里的数字就是后缀。此后缀不计入节点名称字符数。如果编辑节点名称，新名称不得超过最大字符数。参看***命名常规*** (p. 431)。

编辑节点

可以编辑节点：更改节点名称、说明、接口、默认接口或关联。

▶ **编辑节点：**

1. 单击 Nodes（节点）选项卡，然后选择要编辑的节点打开 Node Profile（节点配置文件）屏幕。
2. 根据需要编辑字段。
3. 单击 OK（确定）按钮保存更改。

*注意 1：在更改刀片服务器机箱的节点名称时，并不更改机箱名称。如要修改机箱名称，可以在 Device Profile（设备配置文件）屏幕上编辑它。参看***编辑刀片服务器机箱设备** *(p. 64)*。

注意 2：在更改虚拟主机节点或虚拟控制系统节点的节点名称时，同时更改 Virtualization（虚拟化）表上的名称。

删除节点

在删除节点时，把它从 Nodes（节点）选项卡上删除掉。用户不能再访问此节点。在删除节点时，删除所有接口、关联和关联端口。

▶ **删除节点：**

1. 在 Nodes（节点）选项卡上选择要删除的节点。
2. 选择 Nodes（节点）> Delete Node（删除节点），打开 Delete Node（删除节点）屏幕。
3. 单击 OK（确定）按钮删除节点。
4. 单击 Yes（是）按钮确认删除节点，同时删除所有接口和关联端口。在删除之后，显示所有删除项的列表。

给节点配置文件增加位置和联系人

输入节点位置详细信息和联系人信息，供节点管理员或用户使用。

给节点配置文件增加位置和联系人：

1. 在 Nodes（节点）选项卡上选择一个节点打开 Node Profile（节点配置文件）页。
2. 单击 Location & Contacts（位置和联系人）选项卡。
3. 输入 Location（位置）信息。
   - Department（部门）：最多 64 个字符。
   - Site（地点）：最多 64 个字符。
   - Location（位置）：最多 128 个字符。
4. 输入 Contacts（联系人）信息。
   - Primary Contact Name（主联系人姓名）和 Secondary Contact Name（第二联系人姓名）：最多 64 个字符。
   - Telephone Number（电话号码）和 Cell Phone（手机号码）：最多 32 个字符。
5. 单击 OK（确定）按钮保存更改。

给节点配置文件增加备注

可以用 Notes（备注）选项卡添加供其他用户阅读的节点备注。此选项卡显示所有备注，包括用户添加备注的日期、他的用户名和 IP 地址。

如果你有设备、端口和节点管理权限，可以清除 Notes（备注）选项卡显示的所有备注。

给节点配置文件增加备注：

1. 在 Nodes（节点）选项卡上选择一个节点打开 Node Profile（节点配置文件）页。
2. 单击 Notes（备注）选项卡。
3. 在 New Note（新建备注）字段里输入备注。
4. 单击 Add（添加）按钮，Notes（备注）列表显示你添加的备注。

清除所有备注：

1. 单击 Notes（备注）选项卡。

2. 单击 Clear Notes（清除备注）按钮。
3. 单击 Yes（是）按钮确认删除 Notes（备注）选项卡上的所有备注。

在 CC-SG 上配置虚拟基础设施

虚拟基础设施术语

CC-SG 使用下列虚拟基础设施部件术语。

术语	定义	示例
控制系统	控制系统是管理服务器。控制系统管理一个或多个虚拟主机。	VMware Virtual Center
虚拟主机	虚拟主机是包含一个或多个虚拟机的物理硬件。	VMware ESX
虚拟机	虚拟机是位于虚拟主机上的虚拟服务器。可以把一个虚拟主机上的虚拟机移动到不同的虚拟主机上。	VMware Virtual Machine (VM)
VI Client 接口	控制系统节点和虚拟主机节点有一个 VI Client 接口，提供虚拟化系统基础设施客户机应用程序访问。	VMware Virtual Infrastructure Web Access
VMW Viewer 接口	虚拟机节点有一个 VMW Viewer 接口，提供虚拟机查看器应用程序访问。	VMware Virtual Machine Remote Console
VMW Power 接口	虚拟机节点有一个 VMW Power 接口，通过 CC-SG 提供节点电源控制。	不适用

虚拟节点概述

可以在 CC-SG 上配置要访问的虚拟基础设施。Virtualization（虚拟化）页有两个向导工具：Add Control System（添加控制系统）向导和 Add Virtual Host（添加虚拟主机）向导，便于你正确添加控制系统、虚拟主机及其虚拟机。

在完成配置之后，可以在 CC-SG 上作为节点访问所有控制系统、虚拟主机和虚拟机。每种虚拟节点有一个访问接口和一个出口。

- 控制系统节点和虚拟主机节点配置有一个 VI Client 接口。VI Client 接口提供虚拟化系统基础设施客户机访问。对于 VMware Control Centers，VI Client 接口通过 VMware Virtual Infrastructure Web Access 提供控制中心服务器访问。对于 VMware ESX 服务器，VI Client 接口通过 VMware Virtual Infrastructure Web Access 提供 ESX 服务器访问。
- 虚拟机节点有一个 VMW Viewer 接口和一个 VMW Power 接口。VMW Viewer 接口提供虚拟机查看器应用程序访问。对于 VMW 虚拟机，VMW Viewer 接口提供虚拟机 Remote Console 访问。VMW Power 接口通过 CC-SG 提供节点电源控制。
- 从 CC-SG 5.0 开始，可以访问 VMware Remote Console 的 Devices（设备）菜单，从而在 CC-SG 上访问 vSphere 4.0 节点。这样可以建立至虚拟节点的设备连接和镜像文件。
- 如果 ESXi 虚拟节点将许可用于免费试用版 VMware 产品，CC-SG 不能管理或访问这些节点。

添加有虚拟主机和虚拟机的控制系统

在添加控制系统时，向导指导你添加控制系统包括的虚拟主机和虚拟机。

添加有虚拟主机和虚拟机的控制系统：

1. 选择 Nodes（节点）> Virtualization（虚拟化）。
2. 单击 Add Control System（添加控制系统）。
3. Hostname/IP Address（主机名/IP 地址）：输入控制系统的 IP 地址或主机名。最多 255 个字符。支持 IPv6。
4. Connection Protocol（连接协议）：指定控制系统和 CC-SG 之间的 HTTP 或 HTTPS 通信。
5. TCP Port（TCP 端口）：输入 TCP 端口。默认端口是 443。
6. Check Interval (seconds)（检查间隔时间[秒]）：输入控制系统和 CC-SG 之间的超时秒数。
7. 输入验证信息：

- 如要用服务帐号进行验证，选择 Use Service Account Credentials（使用服务帐号证书）复选框。在 Service Account Name（服务帐号名称）菜单上选择要使用的服务帐号。

  或者

- 在 Username（用户名）和 Password（密码）字段里分别输入用户名和密码进行验证。每个字段最多 64 个字符。

8. 如要让访问此控制系统的用户自动登录 VI Client 接口，选择 Enable Single Sign On For VI Client（允许 VI Client 单点登录）复选框。**可选。**
9. 然后单击 Next（下一步）按钮，CC-SG 发现控制系统的虚拟主机和虚拟机。
   - 单击列标题按此属性升序顺序排序表。再次单击此标题按降序顺序排序表。 **可选。**
10. 给 CC-SG 添加虚拟机给每个虚拟机创建一个节点。同时配置每个关联的虚拟主机。即使虚拟主机与多个虚拟机关联，也只添加一个虚拟主机。
    - 添加一个虚拟机：
      - 选择要添加的虚拟机旁边的 Configure（配置）复选框。
      - 如要把 VNC 接口、RDP 接口或 SSH 接口添加到虚拟主机节点和虚拟机节点，选择虚拟机旁边的复选框。**可选。**
    - 添加所有虚拟机：
      - 选择 Configure（配置）列最上面的复选框选择所有虚拟机。
      - 如要把 VNC 接口、RDP 接口或 SSH 接口添加到所有虚拟主机节点和所有虚拟机节点，选择 VNC 列、RDP 列或 SSH 列最上面的复选框。**可选。**
    - 添加多个虚拟机：
      - 按住 Ctrl 或 Shift 单击虚拟机选择多个要添加的虚拟机。
      - 在 Check/Uncheck Selected Rows（选择/取消选择的行）部分选择 Virtual Machine（虚拟机）复选框。
      - 如要把 VNC 接口、RDP 接口或 SSH 接口添加到即将创建的虚拟主机节点和虚拟机节点，在 Check/Uncheck Selected Rows（选择/取消选择的行）部分选择 VNC 复选框、RDP 复选框或 SSH 复选框。**可选。**
      - 单击 Check（选择）按钮。
11. 然后单击 Next（下一步）按钮，CC-SG 显示要添加的接口类型的列表。可以给每种接口类型添加名称和登录证书。

12. 对于每种接口类型，输入一个名称和一个登录证书。被添加到配置的每个虚拟机节点和虚拟主机节点的所有接口，将共享此名称和登录证书。**可选。**

    如果要给每个接口逐个添加名称和登录证书，不要填写这些字段。

    如果不填写名称字段，接口使用节点名称。

    a. 输入接口名称。最多 32 个字符。
       - Virtual Host VI Client Interfaces（虚拟主机 VI Client 接口）
       - VMware Viewer Interfaces（VMware Viewer 接口）
       - Virtual Power Interfaces（虚拟出口）
       - RDP Interface（RDP 接口）、VNC Interface（VNC 接口）和 SSH Interface（SSH 接口）（如指定）

    b. 必要时输入登录证书。某些接口类型不需要登录证书。
       - 如要使用服务帐号，选择 Use Service Account Credentials（使用服务帐号证书）复选框，然后选择服务帐号名称。

       或者

       - 输入接口类型对应的用户名和密码。每个字段最多 64 个字符。

13. 单击 OK（确定）按钮。

    CC-SG：

    - 给每个虚拟机创建一个节点。每个虚拟机节点有一个 VMW Viewer 接口、一个 VMW Power 接口和你指定的其他任何带内接口。虚拟机节点的名称与虚拟主机系统的虚拟机名称相同。
    - 给每个虚拟主机创建一个节点。每个虚拟主机节点有一个 VI Client 接口。虚拟主机节点的名称与其 IP 地址或主机名相同。
    - 给控制系统创建一个节点。控制系统节点有一个 VI Client 接口。控制系统节点的名称为 Virtual Center 加上 IP 地址，例如 Virtual Center 192.168.10.10。

添加有虚拟机的虚拟主机

在添加虚拟主机时，向导指导你添加虚拟主机包括的虚拟机。

添加有虚拟机的虚拟主机：

1. 选择 Nodes（节点）> Virtualization（虚拟化）。
2. 单击 Add Virtual Host（添加虚拟主机）。
3. 选择 Nodes（节点）> Virtualization（虚拟化）。

4. 单击 Add Virtual Host（添加虚拟主机）。
5. Hostname/IP Address（主机名/IP 地址）：输入虚拟主机的 IP 地址或主机名。最多 255 个字符。支持 IPv6。
6. Connection Protocol（连接协议）：指定虚拟主机和 CC-SG 之间的 HTTP 或 HTTPS 通信。
7. TCP Port（TCP 端口）：输入 TCP 端口。默认端口是 443。
8. Check Interval (seconds)（检查间隔时间[秒]）：输入虚拟主机和 CC-SG 之间的超时秒数。
9. 输入验证信息：
   - 如要用服务帐号进行验证，选择 Use Service Account Credentials（使用服务帐号证书）复选框。在 Service Account Name（服务帐号名称）菜单上选择要使用的服务帐号。

     或者
   - 在 Username（用户名）和 Password（密码）字段里分别输入用户名和密码进行验证。每个字段最多 64 个字符。
10. 如要让访问此虚拟主机的用户自动登录 VI Client 接口，选择 Enable Single Sign On For VI Client（允许 VI Client 单点登录）复选框。**可选。**
11. 然后单击 Next（下一步）按钮，CC-SG 发现虚拟主机的虚拟机。
    - 单击列标题按此属性升序顺序排序表。再次单击此标题按降序顺序排序表。 **可选。**
12. 给 CC-SG 添加虚拟机给每个虚拟机创建一个节点。同时配置每个关联的虚拟主机。即使虚拟主机与多个虚拟机关联，也只添加一个虚拟主机。
    - 添加一个虚拟机：
      - 选择要添加的虚拟机旁边的 Configure（配置）复选框。
      - 如要把 VNC 接口、RDP 接口或 SSH 接口添加到虚拟主机节点和虚拟机节点，选择虚拟机旁边的复选框。**可选。**
    - 添加所有虚拟机：
      - 选择 Configure（配置）列最上面的复选框选择所有虚拟机。
      - 如要把 VNC 接口、RDP 接口或 SSH 接口添加到所有虚拟主机节点和所有虚拟机节点，选择 VNC 列、RDP 列或 SSH 列最上面的复选框。**可选。**
    - 添加多个虚拟机：

- 按住 Ctrl 或 Shift 单击虚拟机选择多个要添加的虚拟机。
- 在 Check/Uncheck Selected Rows（选择/取消选择的行）部分选择 Virtual Machine（虚拟机）复选框。
- 如要把 VNC 接口、RDP 接口或 SSH 接口添加到即将创建的虚拟主机节点和虚拟机节点，在 Check/Uncheck Selected Rows（选择/取消选择的行）部分选择 VNC 复选框、RDP 复选框或 SSH 复选框。**可选。**
- 单击 Check（选择）按钮。

13. 然后单击 Next（下一步）按钮，CC-SG 显示要添加的接口类型的列表。可以给每种接口类型添加名称和登录证书。
14. 对于每种接口类型，输入一个名称和一个登录证书。被添加到配置的每个虚拟机节点和虚拟主机节点的所有接口，将共享此名称和登录证书。**可选。**

如果要给每个接口逐个添加名称和登录证书，不要填写这些字段。

如果不填写名称字段，接口使用节点名称。

---

a. 输入接口名称。最多 32 个字符。
   - VI Client Interfaces（VI Client 接口）
   - VMware Viewer Interfaces（VMware Viewer 接口）
   - Virtual Power Interfaces（虚拟出口）
   - RDP Interface（RDP 接口）、VNC Interface（VNC 接口）和 SSH Interface（SSH 接口）（如指定）

b. 必要时输入登录证书。某些接口类型不需要登录证书。
   - 如要使用服务帐号，选择 Use Service Account Credentials（使用服务帐号证书）复选框，然后选择服务帐号名称。

   或者

   - 输入接口类型对应的用户名和密码。每个字段最多 64 个字符。

15. 单击 OK（确定）按钮。

CC-SG：

- 给每个虚拟机创建一个节点。每个虚拟机节点有一个 VMW Viewer 接口、一个 VMW Power 接口和你指定的其他任何带内接口。虚拟机节点的名称与虚拟主机系统的虚拟机名称相同。
- 给每个虚拟主机创建一个节点。每个虚拟主机节点有一个 VI Client 接口。虚拟主机节点的名称与其 IP 地址或主机名相同。

编辑控制系统、虚拟主机和虚拟机

可以编辑在 CC-SG 上配置的控制系统、虚拟主机和虚拟机，更改它们的属性。可以取消虚拟机对应的 Configure（配置）复选框，把虚拟机节点从 CC-SG 上删除掉。

*注意：如要更改虚拟主机节点或控制系统节点的节点名称，可以编辑节点。参看***编辑节点** *(p. 107)。Virtualization（虚拟化）表也显示名称更改。*

▶ **编辑控制系统、虚拟主机和虚拟机：**

1. 选择 Nodes（节点）> Virtualization（虚拟化）。
2. 单击列标题按此属性升序顺序排序表。再次单击此标题按降序顺序排序表。 **可选。**
3. 选择要编辑的控制系统或虚拟主机。
4. 单击 Edit（编辑）按钮。
5. 根据需要更改信息。参看***添加有虚拟主机和虚拟机的控制系统*** (p. 110) 和***添加有虚拟机和虚拟主机*** (参看 "***添加有虚拟机的虚拟主机***" p. 112) 了解完整的字段说明。
6. 然后单击 Next（下一步）按钮。
7. 把一个或多个虚拟机从 CC-SG 上删除掉。
   - 如要删除一个虚拟机，取消 Configure（配置）复选框。
   - 如要删除多个虚拟机，按住 Ctrl 或 Shift 单击虚拟机选择多个虚拟机。在 Check/Uncheck Selected Rows（选择/取消选择的行）部分选择 Virtual Machine（虚拟机）复选框，然后单击 Uncheck（取消）。
8. 如要把 VNC 接口、RDP 接口或 SSH 接口添加到虚拟主机节点和虚拟机节点，选择每个虚拟机旁边的复选框。

   *不能在本页上把 SSH 接口、VNC 接口和 RDP 接口从虚拟机节点或虚拟主机节点上删除掉。必须在节点配置文件上删除这些接口。参看***删除接口** *(p. 135)。*
9. 然后单击 Next（下一步）按钮。如果选择删除虚拟机，显示一条警告消息。
10. 对于每种接口类型，输入一个名称和一个登录证书。被添加到配置的每个虚拟机节点和虚拟主机节点的所有接口，将共享此名称和登录证书。**可选。**如果要给每个接口逐个添加名称和登录证书，不要填写这些字段。
    a. 输入接口名称（最多 32 个字符）。

- Virtual Host VI Client Interfaces（虚拟主机 VI Client 接口）
- VMware Viewer Interfaces（VMware Viewer 接口）
- Virtual Power Interfaces（虚拟出口）
- RDP Interface（RDP 接口）、VNC Interface（VNC 接口）和 SSH Interface（SSH 接口）（如指定）

b. 输入登录证书：

- 如要使用服务帐号，选择 Use Service Account Credentials（使用服务帐号证书）复选框，然后选择服务帐号名称。

或者

- 输入接口类型对应的用户名和密码。每个字段最多 64 个字符。

11. 单击 OK（确定）按钮。

删除控制系统和虚拟主机

可以把控制系统和虚拟主机从 CC-SG 上删除掉。

在删除控制系统时，并不删除与之关联的虚拟主机和虚拟机。

在删除虚拟主机时，并不删除与之关联的控制系统和虚拟机。

在删除控制系统或虚拟主机时，并不自动删除与之关联的虚拟机节点。参看*删除虚拟机节点* (p. 116)。

删除控制系统和虚拟主机：

1. 选择 Nodes（节点）> Virtualization（虚拟化）。
2. 在列表上选择要删除的控制系统和虚拟主机。按住 Ctrl 单击项选择多项。
3. 单击 Delete（删除）按钮。

删除虚拟机节点

可以采用两种方法删除虚拟机节点：

- 使用 Delete Node（删除节点）功能。参看*删除节点* (p. 107)。
- 取消虚拟机对应的 Configure（配置）复选框。参看*编辑控制系统、虚拟主机和虚拟机* (p. 115)。

删除虚拟基础设施

根据下列步骤把整个虚拟基础设施从 CC-SG 上删除掉，包括控制系统、虚拟主机和虚拟机。

删除虚拟基础设施：

1. 取消每个虚拟机对应的 Configure（配置）复选框，删除所有虚拟机节点。参看*编辑控制系统、虚拟主机和虚拟机* (p. 115)。
2. 删除控制系统和虚拟主机。参看*删除控制系统和虚拟主机* (p. 116)。

   删除虚拟基础设施的所有部件，包括控制系统节点、虚拟主机节点、虚拟机节点及其接口。

vSphere 4 用户必须安装新插件

在把虚拟环境从旧版本升级到 vSphere 4 时，必须把 VMware Remote Console 插件从浏览器上删除掉。在删除插件之后，下次在 CCSG 上连接虚拟机时，将安装正确的 vSphere4 插件。

删除 Internet Explorer 上的旧插件：

1. 选择 Tools(工具)> Manage Add-Ons(管理插件)> Enable or Disable Add-Ons（启用或禁用插件）。
2. 在 Show（显示）列表上选择 Add-Ons that have been used by Internet Explorer（Internet Explorer 使用的插件）。
3. 向下翻到 VMware Remote Console Plug-in（VMware Remote Console 插件），然后选择此插件。
4. 此时应该激活 Delete Active-X（删除 Active-X）按钮，单击此按钮删除旧插件。
   - 如果没有激活 Delete（删除）按钮，打开 Control Panel（控制面板）> Add/Remove Programs（添加/删除程序）查找旧版 VI Client。如果安装了 VI Client 2.5，把它卸载掉。在卸载 VI Client 2.5 之后，卸载此插件。

删除 Firefox 用户使用的旧插件：

1. 选择 Tools（工具）>Add-Ons（插件）。
2. 单击 Plug-Ins（插件）选项卡。
3. 选择旧插件，然后单击 Disable（禁用）按钮。

安装新插件：

1. 在删除旧插件之后，登录 CCSG 并连接虚拟机。

2. 系统提示你安装 vSphere 4 插件。

VCenter 要求的最低权限

必须在 VCenter 应用程序上设置一些最低权限，让 CC-SG 访问 VCenter 并管理与之关联的节点和接口。

在 vSphere 4.1/5.0 上设置最低权限：

- Host（主机）> Configuration（配置）> System Management（系统管理）
- Host（主机）> Configuration（配置）> Maintenance（维护）
- Virtual Machine（虚拟机）> Interation（交互操作）> Power On（通电）
- Virtual Machine（虚拟机）> Interation（交互操作）> Power Off（断电）
- Virtual Machine（虚拟机）> Interation（交互操作）> Suspend（暂停）
- Virtual Machine（虚拟机）> Interation（交互操作）> Reset（复位）
- Virtual Machine(虚拟机)> Interation(交互操作)> Console Interaction（控制台交互操作）
- Tasks（任务）> Create（创建）
- Scheduled Tasks（计划任务）> Create Tasks（创建任务）
- Scheduled Tasks（计划任务）> Run Tasks（运行任务）

此外，应该还可以在 VMware Remote Console 上利用 Virtual Machine（虚拟机）> Interation（交互操作）> Device Connection（设备连接）连接/断开媒体设备和网络设备。

在不添加 VCenter 的情况下人工安装 VMware Remote Console 插件

当 VCenter 处于 CC-SG 环境下时，Internet Explorer 提示你自动下载 VMware Remote Console 插件和在 VCenter 上找到的插件。

可能会显示此错误消息：Failed to run vmware remote console plugin. Either the browser is not supported or you have a previous version of the console installed.（无法运行 VMware Remote Console 插件。要么是不支持浏览器，要么是你安装了旧版控制台。）

如果尚未添加 VCenter，只添加了主机，不显示插件提示。必须在网站上人工下载插件。

插件文件名是 vmware-vmrc-win32-x86.exe。对于 64 位操作系统，可能必须下载不同的插件。

使虚拟基础设施与 CC-SG 同步

同步功能确保 CC-SG 有最新的虚拟基础设施信息。同步功能更新每个虚拟机节点的特定信息和虚拟基础设施拓扑信息。

可以配置每天自动同步已配置的所有控制系统和虚拟主机。也可以随时对所选的控制系统和虚拟主机执行同步功能。

同步虚拟基础设施

可以对 CC-SG 和虚拟基础设施执行同步功能。

在选择要同步的控制系统时，无论是否选择关联的虚拟主机，都要同时同步这些虚拟主机。

同步虚拟基础设施：

1. 选择 Nodes（节点）> Virtualization（虚拟化）。
2. 在节点列表上选择要同步的节点。按住 Ctrl 单击项选择多项。
3. 单击 Synchronize（同步）按钮。如果在上次同步之后，虚拟基础设施更改了，就更新 CC-SG 上的信息。
   - Configured in Secure Gateway（在安全网关上配置的）列显示在 CC-SG 上配置的虚拟机数或虚拟主机数。
   - Last Synchronization Date（上次同步日期）显示上次同步的日期和时间。
   - Node Status（节点状态）栏显示虚拟节点的状态。

启用或禁用虚拟基础设施每日同步

可以配置 CC-SG 和虚拟基础设施自动同步。每天在你指定的时间自动同步。

启用虚拟基础设施每日同步：

1. 选择 Nodes（节点）> Virtualization（虚拟化）。
2. 选择 Enable Daily Automatic Synchronization（启用每日自动同步）复选框。
3. 在 Start Time（开始时间）字段里输入你希望每天在哪个时间开始同步。
4. 单击 Update（更新）按钮。

禁用虚拟基础设施每日同步：

1. 选择 Nodes（节点）> Virtualization（虚拟化）。
2. 取消 Enable Daily Automatic Synchronization（启用每日自动同步）复选框。
3. 单击 Update（更新）按钮。

重新启动或强制重新启动虚拟主机节点

可以重新启动或强制重新启动虚拟主机服务器。当虚拟主机服务器处于维护模式时，重新启动操作让虚拟主机服务器正常重新启动。强制重新启动操作强制虚拟主机服务器重新启动，即使服务器不在维护模式下也重新启动。

如要使用这些命令，你必须具备节点带内访问权限和节点电源控制权限。你还必须在一个指定了策略的用户组里，可以访问要重新启动或强制重新启动的节点。

重新启动或强制重新启动虚拟主机节点：

1. 选择要重新启动或强制重新启动的虚拟主机节点。
2. 单击 Virtual Host Data（虚拟主机数据）选项卡。
3. 单击 Reboot（重新启动）或 Force Reboot（强制重新启动）。

访问虚拟拓扑视图

虚拟拓扑视图是树结构，显示与所选节点关联的控制系统、虚拟主机和虚拟机之间的关系。

你必须具备设备、端口和节点管理权限，才能打开拓扑视图。

在虚拟节点配置文件上打开拓扑视图：

1. 在节点配置文件上，单击包含节点虚拟化信息的选项卡：Virtual Machine Data（虚拟机数据）选项卡、Virtual Host Data（虚拟主机数据）选项卡或 Control System（控制系统）选项卡，视节点类型而定。
2. 单击 Topology View（拓扑视图）链接，用新窗口打开拓扑视图。在 CC-SG 上配置的虚拟节点作为链接显示。
   - 双击节点链接打开虚拟节点对应的 Node Profile（节点配置文件）。
   - 双击接口链接也可以连接节点。
   - 双击虚拟出口链接打开节点对应的 Power Control（电源控制）页面。

连接节点

在给一个节点添加一个接口之后，就可以通过此接口采用几种不同的方法连接此节点。参看 Raritan **CommandCenter Secure Gateway 用户指南**。

连接节点：

1. 单击 Nodes（节点）选项卡。
2. 选择要连接的节点，并：
   - 在 Interfaces（接口）表上单击要连接的接口的名称。

   或者
   - 在 Nodes（节点）选项卡上展开要连接的节点下面的接口列表。双击要连接的接口的名称，或者用右键单击接口，然后选择 Connect（连接）。

Access Client Firefox 用户必须下载 JNLP 文件

每当建立带外 KVM 端口连接时，系统提示 Access Client Firefox 用户下载 .JNLP 文件。

选择 Do this automatically for files like this from now on（从此以后自动下载此类文件）复选框，让 Firefox 为未来建立的连接自动下载此文件。

对节点执行 ping 命令

可以在 CC-SG 上对节点执行 ping 命令，确保连接处于活动状态。

对节点执行 ping 命令：

1. 单击 Nodes（节点）选项卡，然后选择要执行 ping 命令的节点。
2. 选择 Nodes（节点）> Ping Node（对节点执行 ping 命令），屏幕显示 ping 命令执行结果。

添加、编辑和删除接口

添加接口

部分接口类型支持 IPv6。参看*给使用 **IPv6** 的节点添加接口* (p. 135)。

*注意：控制系统、虚拟主机和虚拟机等虚拟节点的接口，只能用 Nodes（节点）> Virtualization（虚拟化）下的虚拟化工具添加。参看*在 **CC-SG** 上配置虚拟基础设施 *(p. 109)*。

▶ 添加接口：

1. 对于现有节点：单击 Nodes（节点）选项卡，然后选择要将接口添加到哪个节点。打开 Node Profile（节点配置文件）屏幕，然后单击 Interfaces（接口）部分的 Add（添加）按钮。

   如果要添加新节点：单击 Add Node（添加节点）屏幕上 Interfaces（接口）部分的 Add（添加）按钮。

   打开 Add Interface（添加接口）窗口。

2. 单击 Interface Type（接口类型）下拉菜单，然后选择要与节点建立的连接的类型：

   In-Band Connections（带内连接）：

   - In-Band - DRAC KVM（带内 - DRAC KVM）：选择此选项，通过 DRAC 接口建立至 Dell DRAC 服务器的 KVM 连接。必须同时配置一个 DRAC Power 接口。
   - In-Band - iLO Processor KVM（带内 - iLO Processor KVM）：选择此选项，通过 iLO 或 RILOE 接口建立至 HP 服务器的 KVM 连接。
   - In-Band - RDP（带内 — RDP）：选择此选项，通过 Java 或 Microsoft Remote Desktop Protocol 建立至节点的 KVM 连接。
   - In-Band - RSA KVM（带内 - RSA KVM）：选择此选项，通过 RSA 接口建立至 IBM RSA 服务器的 KVM 连接。必须同时配置一个 RSA Power 接口。
   - In-Band - SSH（带内 - SSH）：选择此选项，建立至节点的 SSH 连接。
   - In-Band - VNC（带内 - VNC）：选择此选项，通过 VNC 服务器软件建立至节点的 KVM 连接。

     参看*带内连接接口* (参看 "*带内连接接口 — **RDP**、**VNC**、**SSH**、**RSA KVM**、**iLO Processor KVM**、**DRAC KVM** 和 **TELNET***" p. 124)。

- In-Band - UCS KVM（带内 — UCS KVM）：选择此选项，用 Cisco Integrated Management Controller (CIMC) 建立至 Cisco UCS 机箱里刀片服务器的 KVM 连接。

  参看 ***Cisco UCS KVM 连接接口*** (p. 127)

Out-of-Band Connections（带外连接）：

- Out-of-Band - KVM（带外 - KVM）：选择此选项，通过 Raritan KVM 设备（KX、KX101、KSX、IP-Reach 或 Paragon II）建立至节点的 KVM 连接。
- Out-of-Band - Serial（带外 - 串行）：选择此选项，通过 Raritan 串行设备（SX 或 KSX）建立至节点的串行连接。

  参看***带外 KVM 连接接口和带外串行连接接口*** (p. 127)。

Power Control Connections（电源控制连接）：

- Power Control - DRAC（电源控制 - DRAC）：选择此选项，建立至 Dell DRAC 服务器的电源控制连接。
- Power Control - iLO Processor（电源控制 - iLO Processor）：选择此选项，建立至 HP iLO/RILOE 服务器的电源控制连接。
- Power Control - IPMI（电源控制 - IPMI）：选择此选项，通过 IPMI 连接建立至节点的电源控制连接。
- Power Control - Integrity ILO2（电源控制 — Integrity ILO2）：选择此选项，建立至 HP Integrity 服务器或支持 Integrity ILO2 的其他服务器的电源控制连接。
- Power Control - Power IQ Proxy（电源控制 — Power IQ Proxy）：选择此选项，建立至 Power IQ IT 设备的电源控制连接。
- Power Control - RSA（电源控制 - RSA）：选择此选项，建立至 RSA 服务器的电源控制连接。

  参看 ***DRAC 电源控制连接接口*** (p. 128)

  ILO Processor、Integrity ILO2 和 RSA 电源控制连接接口 (p. 129)

  Power IQ Proxy 电源控制连接接口 (p. 131)

Managed Powerstrip Connections（网管电源条连接）：

- Managed PowerStrip（网管电源条）：选择此选项，通过 Raritan 电源条或 Dominion PX 设备建立至节点的电源控制连接。

  参看***网管电源条连接接口*** (p. 130)。

Web Browser Connections（网络浏览器连接）：

- Web Browser（网络浏览器）：选择此选项，建立至使用嵌入 Web 服务器的设备的连接。

参看*网络浏览器接口* (p. 132)。

3. 根据你选择的接口的类型，Name（名称）字段显示默认名称。可以更改名称。在 Nodes（节点）列表上，接口旁边显示此名称。参看*命名常规* (p. 431)详细了解 CC-SG 的名称长度规则。

带内连接接口 — RDP、VNC、SSH、RSA KVM、iLO Processor KVM、DRAC KVM 和 TELNET

带内连接包括 RDP、VNC、SSH、RSA KVM、iLO Processor KVM、DRAC KVM 和 TELNET。

Microsoft RDP 接口、SSH 接口、Telnet 接口、VNC 接口和 DRAC（仅 iDRAC6）接口支持 IPv6 地址。Java RDP 接口、RSA KVM 接口和 iLO Processor KVM 接口不支持 IPv6 地址。 See ***Adding Interfaces for Nodes Using IPv6*** (参看 "*给使用 IPv6 的节点添加接口*" p. 135).

Telnet 不是安全访问方法。所有用户名、密码和流量均采用明文方式传送。

添加带内连接接口：

1. 在 IP Address/Hostname（IP 地址/主机名）字段里输入此接口的 IP 地址或主机名。
2. 在 TCP Port（TCP 端口）字段里输入此连接的 TCP 端口。**可选。**
3. 对于 RDP 接口，选择 Java 或 Windows，然后选择 Console（控制台）或 Remote User（远程用户）。当控制台用户访问一个节点时，断开其他所有用户。多个远程用户可以同时访问一个节点。
4. 输入验证信息：
   - 如要用服务帐号进行验证，选择 Use Service Account Credentials（使用服务帐号证书）复选框。在 Service Account Name（服务帐号名称）菜单上选择要使用的服务帐号。

   或者

   - 在 Username（用户名）和 Password（密码）字段里分别输入用户名和密码进行验证。对于 VNC 接口，只需输入密码。
5. 选择你使用的语言对应的键盘布局。此选项不能用于 Microsoft RDP 接口。
6. 在 Description（说明）字段里输入此接口的说明。**可选。**
7. 单击 OK（确定）按钮保存更改。

DRAC 5 连接详细信息

在使用 Internet Explorer 连接 DRAC 5 服务器时，必须在 DRAC 5 上安装有效证书，否则 Internet Explorer 出错。

如果证书没有经过信任 CA 签名，还要把此证书安装在浏览器的 Trusted Root CA（信任的根证书颁发机构）里。

还必须禁用 Internet Explorer 下载信息栏，才能访问 DRAC5 .jnlp 文件。

禁用 Internet Explorer 下载信息栏：

1. 单击 Tools（工具）> Internet Options（Internet 选项）。
2. 在 Security（安全）选项卡上选择 Internet 区域。
3. 单击 Custom Level（定制级别）按钮向下翻到 Downloads（下载）。
4. 单击 Automatic prompting for file downloads（自动提示文件下载）下面的 Enable（启用）。
5. 单击 OK（确定）按钮返回 Internet Options（Internet 选项）对话框。
6. 在 Security（安全）选项卡上选择 Intranet 区域。
7. 单击 Custom Level（定制级别）按钮向下翻到 Downloads（下载）。
8. 单击 Automatic prompting for file downloads（自动提示文件下载）下面的 Enable（启用）。
9. 单击 OK（确定）按钮。

用 Internet Explorer 9 连接 DRAC 接口：

1. 在 Internet Explorer 9 上选择 Tools（工具）> Options（选项）。
2. 在 Privacy（隐私）选项卡上把滑动条设置为 Low（低），允许 cookies 访问 DRAC 接口。
3. 在提示 Do you want to open or save vkvm.jnlp（要打开还是保存 vkvm.jnlp）时，单击 Open（打开）按钮启动 DRAC 接口。

Microsoft RDP 连接详细信息

- 如果使用 Windows XP 客户机，必须安装 Terminal Server Client 6.0 或更高版本，才能在 CC-SG 上连接 Microsoft RDP 接口。用此链接把 Terminal Server Client 升级到 6.0：http://support.microsoft.com/kb/925876。
- 仅 Internet Explorer。
- Microsoft RDP 不能用于代理模式连接。参看*关于连接模式* (p. 267)。
- 支持的目标服务器包括 Vista、Win2008 服务器和 Windows 7，以及此前的所有 Windows 版本，包括 Windows XP 目标和 Windows 2003 目标。
- 如要详细了解 Microsoft RDP，包括用法说明，访问：http://www.microsoft.com/downloads/details.aspx?FamilyID=469eee3a-45b4-4b40-b695-b678646a728b&displaylang=en
- 在给 Windows 7 添加 RDP 接口时， 确保 Windows 7 防火墙允许 ICMPv4 和 ICMPv6。

Java RDP 连接详细信息

- Java RDP 接口支持 Windows XP 目标和 Windows 2003 目标。
- Java RDP 可用于代理模式连接。参看*关于连接模式* (p. 267)。
- 在给 Windows 7 添加 RDP 接口时， 确保 Windows 7 防火墙允许 ICMPv4 和 ICMPv6。

VNC 连接详细信息

IPv6 支持：

并非所有 VNC 版本都支持 IPv6。

RealVNC 支持 IPv6。必须在 RealVNC 服务器设置上选择 Prefer On（首选开），否则 IPv6 和 VNC 不能与 CC-SG 一起工作。

如果把 TightVNC 服务器设置更改为 Prefer On（首选开），TightVNC 客户机不能与 CC-SG 一起工作。

免费版 RealVNC 不支持 IPv6。

个人版 RealVNC 支持 IPv6，但这是只有 30 天试用期的试用版，在试用期结束之后必须购买许可才能继续使用。

企业版 RealVNC 在购买许可之后支持 IPv6。

Windows 7 VNC 连接：

在给 Windows 7 添加 VNC 接口时，确保 Windows 7 防火墙允许 ICMPv4 和 ICMPv6。

带外 KVM 连接接口和带外串行连接接口

添加带外 KVM 连接接口或带外串行连接接口：

1. Application name（应用程序名称）：在列表上选择通过此接口连接节点时要使用的应用程序。
   - 如要让 CC-SG 根据你使用的浏览器自动选择应用程序，选择 Auto-Detect（自动检测）。
   - 使用 Active KVM Client 有前提条件。参看*使用 AKC 的前提条件* (参看 "*使用 AKC 的前提*" p. 255)和*启用 AKC 下载服务器证书验证* (p. 270)。
2. Raritan Device Name（Raritan 设备名称）：选择能提供此节点访问的 Raritan 设备。注意必须先把设备添加到 CC-SG，此列表才会显示它。
3. Raritan Port Name（Raritan 端口名称）：选择能提供此节点访问的 Raritan 设备的端口。必须先在 CC-SG 上配置端口，此列表才会显示它。对于串行连接，自动根据端口配置填充 Baud Rate（波特率）字段、Parity（奇偶校验）字段和 Flow Control（流控制）字段。
4. 在 Description（说明）字段里输入此接口的说明。**可选。**
5. 单击 OK（确定）按钮保存更改。

Cisco UCS KVM 连接接口

UCS-KVM 连接便于你用 Cisco Integrated Management Controller (CIMC) 建立至 Cisco UCS 机箱里刀片服务器的 KVM 连接并访问它们。

添加 Cisco UCS KVM 连接接口：

1. 输入接口名称。参看*命名常规* (p. 431)详细了解 CC-SG 的名称长度规则。
2. 在 Chassis IP/Hostname(机箱 IP/主机名)字段里输入 Cisco UCS IP 地址或主机名。
3. 在 TCP Port（TCP 端口）字段里输入此连接的 TCP 端口。默认端口是 443。
4. 在 Blade IP/Hostname（刀片服务器 IP/主机名）字段里输入刀片服务器 IP 地址或主机名。
5. 输入验证信息：
   - 如要用服务帐号进行验证，选择 Use Service Account Credentials（使用服务帐号证书）复选框。在 Service Account Name（服务帐号名称）菜单上选择要使用的服务帐号。

或者

- 在 Username（用户名）和 Password（密码）字段里分别输入用户名和密码进行验证。指定在访问机箱和刀片服务器时所用的帐号的户名和密码。

6. 在 Description（说明）字段里输入此接口的说明。**可选。**
7. 单击 OK（确定）按钮保存更改。

Cisco UCS 详细信息

Cisco UCS 5100 系列刀片服务器机箱和部件是 Cisco Unified Computing System (UCS) 的组成部分。在配置 KVM 和 IPMI 功能之后，CC-SG 用户可以用刀片服务器 Cisco Integrated Management Controller (CIMC) 访问这些功能。

添加 Cisco UCS 刀片服务器电源控制：

给节点添加一个 IPMI 电源控制接口。参看 ***IPMI 电源控制连接接口*** (p. 130)。

给 Cisco UCS 刀片服务器添加 Serial Over Lan (SOL) 访问：

给节点添加一个 SSH 接口。参看***带内连接接口 — RDP、VNC、SSH、RSA KVM、iLO Processor KVM、DRAC KVM 和 TELNET*** (p. 124)。

DRAC 电源控制连接接口

添加 DRAC 电源控制连接接口：

1. 在 IP Address/Hostname（IP 地址/主机名）字段里输入此接口的 IP 地址或主机名。
2. 在 TCP Port（TCP 端口）字段里输入此连接的 TCP 端口。**仅 DRAC 5。** DRAC 4 不需要 TCP 端口。
3. 输入验证信息：
   - 如要用服务帐号进行验证，选择 Use Service Account Credentials（使用服务帐号证书）复选框。在 Service Account Name（服务帐号名称）菜单上选择要使用的服务帐号。

   或者

   - 在 Username（用户名）和 Password（密码）字段里分别输入用户名和密码进行验证。
4. 在 Description（说明）字段里输入此接口的说明。**可选。**
5. 单击 OK（确定）按钮保存更改。

ILO Processor、Integrity ILO2 和 RSA 电源控制连接接口

iLO 连接或 RSA 连接不支持 IPv6。

添加 ILO Processor、Integrity ILO2 和 RSA 电源控制连接接口：

1. 在 IP Address/Hostname（IP 地址/主机名）字段里输入此接口的 IP 地址或主机名。
2. 输入验证信息：
   - 如要用服务帐号进行验证，选择 Use Service Account Credentials（使用服务帐号证书）复选框。在 Service Account Name（服务帐号名称）菜单上选择要使用的服务帐号。

   或者

   - 在 Username（用户名）和 Password（密码）字段里分别输入用户名和密码进行验证。
3. 在 Description（说明）字段里输入此接口的说明。**可选。**
4. 单击 OK（确定）按钮保存更改。

RSA 接口详细信息

在创建带内 RSA KVM 接口或 Power 接口时，CC-SG 放弃与此接口关联的用户名和密码，在 RSA 服务器上创建两个用户帐号。这样，可以同时对 RSA 服务器进行 KVM 访问和电源访问。

新用户名：

- cc_kvm_user
- cc_power_user

这些用户名取代你在创建接口时输入的用户名。CC-SG 使用这些新用户帐号，通过这些接口连接 RSA 服务器。

不要删除、编辑或更改 RSA 服务器上的这些用户帐号的密码，否则 CC-SG 不能用这些接口建立连接。

如果此前使用服务帐号创建接口，CC-SG 不在 RSA 服务器上创建用户帐号。在这些端口上使用服务帐号时，不能同时对 RSA 服务器进行 KVM 访问和电源访问。

RSA 与 JRE 的兼容性

IBM RSA II v1.14 兼容 JRE v1.6.0_10 和 v1.6.0_11。

CC-SG 还支持更高版本的 JRE，但更高版本的 JRE 不支持 IBM RSA II 卡。

网管电源条连接接口

在创建网管电源条接口，把 KX 指定为管理设备时，用关联节点的名称重新命名你指定的出口。

添加网管电源条连接接口：

1. Managing Device（管理设备）：
   - 选择电源条连接的 Raritan 设备。此设备必须已被添加到 CC-SG。

   或者
   - 如果电源控制接口使用 IP 网络上未连接其他 Raritan 设备的 PX 设备，选择 Dominion PX。
2. Managing Port（管理端口）：选择电源条连接的 Raritan 设备的端口。如果选择 PX 作为管理设备，此字段被禁用。
3. Power Strip Name（电源条名称）：选择给节点供电的电源条或 PX 设备。必须先在 CC-SG 上配置电源条或 PX 设备，此列表才会显示它。
4. Outlet Name（插座名称）：选择节点所插的出口的名称。**可选。**
5. 在 Description（说明）字段里输入此接口的说明。
6. 单击 OK（确定）按钮保存更改。

注意：可以给刀片服务器机箱节点添加网管电源条接口，但不能给刀片服务器节点添加网管电源条接口。

IPMI 电源控制连接接口

添加 IPMI 电源控制连接接口：

1. 在 IP Address/Hostname（IP 地址/主机名）字段里输入此接口的 IP 地址或主机名。
2. 在 UDP Port（UDP 端口）字段里输入此接口的 UDP 端口号。
3. 验证：选择连接此接口所用的验证方案。
4. 在 Check Interval (seconds)（检查间隔时间[秒]）字段里输入此接口的检查间隔时间。
5. 输入验证信息：
   - 如要用服务帐号进行验证，选择 Use Service Account Credentials（使用服务帐号证书）复选框。在 Service Account Name（服务帐号名称）菜单上选择要使用的服务帐号。

   或者

- 在 Username（用户名）和 Password（密码）字段里分别输入用户名和密码进行验证。**可选。**

6. 在 Description（说明）字段里输入此接口的说明。**可选。**
7. 单击 OK（确定）按钮保存更改。

IBM IMM 模块连接详细信息

可以用 IPMI 电源控制接口连接标准版本的 IBM IMM 模块，通过 CC-SG 执行电源控制操作。支持接通电源、断开电源和重新通电功能。

参看 ***IPMI 电源控制连接接口*** (p. 130)。

注意：KVM 不能通过 CC-SG 访问 IBM IMM 模块。

Power IQ Proxy 电源控制连接接口

如果要用 CC-SG 控制已作为节点添加到 CC-SG 的 Power IQ IT 设备的电源，添加 Power IQ Proxy 电源控制接口。使你能控制与不受 CC-SG 管理的 PDU 相连的节点的电源。

添加 IQ Proxy 电源控制连接接口：

1. 输入 IT 设备的 External Key（外部键）。Power IQ 的外部键必须与 CC-SG 的外部键相同。最多 255 个字符。不允许使用逗号。默认值是节点名称。可以更改此值。
   - 如果 IT 设备已被添加到 Power IQ，在 Data Center（数据中心）选项卡上的 IT 设备页上找到外部键，在 External Key（外部键）字段里输入此外部键。
   - 如果 IT 设备尚未被添加到 Power IQ，接受外部键默认值或更改此值，但确保在把 IT 设备添加到 Power IQ 时使用相同的值。可以采用导出方法，迅速创建一个包含所有节点信息和接口信息的文件。参看***导出节点*** (p. 161)。
2. 在 Managing Device（管理设备）字段里选择管理 IT 设备的 Power IQ。必须先把此设备的信息添加到 CC-SG，此字段才会显示它。参看***配置 Power IQ 服务*** (p. 363)。
3. 在 Description（说明）字段里输入此接口的说明。
4. 单击 OK（确定）按钮保存更改。

网络浏览器接口

可以添加一个网络浏览器接口，建立至使用嵌入式 Web 服务器（例如 Dominion PX）的设备的连接。 See ***Example: Adding a Web Browser Interface to a PX Node*** (参看 "*示例 :给 PX 节点添加网络浏览器接口*" p. 134).对于集成了 KVM 切换器的刀片服务器机箱，如果在 KX2 设备上给它指定了 URL 或 IP 地址，自动添加一个网络浏览器接口。

也可以用网络浏览器界面连接任何 Web 应用程序，例如与 RSA、DRAC 或 ILO Processor 卡关联的 Web 应用程序。

如果 Web 应用程序需要的信息不仅仅是用户名和密码（例如会话 ID），网络浏览器接口不允许自动登录。

用户必须具备节点带内访问权限，才能访问网络浏览器接口。

必须配置 DNS，否则不解析 URL。如果输入 IP 地址，不必配置 DNS。

网络浏览器接口支持 IPv6 地址。参看*给使用 IPv6 的节点添加接口* (p. 135)。

添加网络浏览器界面：

1. 网络浏览器接口的默认名称是 Web Browser（网络浏览器）。可以在 Name（名称）字段里更改此名称。参看*命名常规* (p. 431)详细了解 CC-SG 的名称长度规则。
2. 在 TCP Port（TCP 端口）字段里输入此连接的 TCP 端口。如果在 URL 上使用 HTTPS，必须把 TCP 端口设置为 443。**可选。**
3. 在 URL 字段里输入 Web 应用程序的 URL 或域名。注意必须输入 Web 应用程序要读取的用户名和密码所在的 URL。最多 255 个字符。使用下列正确格式：
   - http(s)://192.168.1.1/login.asp
   - http(s)://www.example.com/cgi/login
   - http(s)://example.com/home.html
   - http(s)://[fd07:2fa:6cff:2500:20f:3dff:fef6:fa1e]/index.html
4. 输入验证信息：**可选。**
   - 如要用服务帐号进行验证，选择 Use Service Account Credentials（使用服务帐号证书）复选框。在 Service Account Name（服务帐号名称）菜单上选择要使用的服务帐号。

   或者

   - 在 Username（用户名）和 Password（密码）字段里分别输入用户名和密码进行验证。输入访问此接口所需的用户名和密码。

注意：对于 DRAC、ILO 和 RSA Web 应用程序，不要输入用户名和密码，否则连接失败。

5. 在 Username Field（用户名字段）和 Password Field（密码字段）里输入在 Web 应用程序登录屏幕上使用的用户名字段和密码字段的字段名称。必须查看登录屏幕的 HTML 源代码找到字段名称，而非字段标签。参看***添加网络浏览器接口注意事项*** (参看 "***添加网络浏览器界面注意事项***" p. 133)。
6. 在 Description（说明）字段里输入此接口的说明。**可选。**
7. 单击 OK（确定）按钮保存更改。

添加网络浏览器界面注意事项

如要配置网络浏览器接口，必须在 HTML 源代码里搜集信息，以便确定 Username（用户名）和 Password（密码）字段的实际字段名称。所有供应商采用不同的方式实现这些验证字段，不同的设备采用不同的字段名称，同种设备的不同固件版本所用的字段名称也不同。为此，没有一种统一的字段名称查找方法。参看下面的步骤，选择一种可用方法。

你可能需求软件工程师或系统管理员协助，才能查找和识别正确的字段名称。

查找字段名称注意事项：

1. 在 Web 应用程序登录页面的 HTML 源代码里搜索字段标签，例如 Username 和 Password。
2. 在找到字段标签之后，查看标签旁边类似下面这样的代码：
   `name="user"`

   引号里面的单词就是字段名。

示例：给 PX 节点添加网络浏览器接口

可以把 Dominion PX 管理的电源条作为节点添加到 CC-SG，然后可以给节点添加网络浏览器接口，使用户能访问 Dominion PX 的 Web 管理应用程序。

▶ **使用下列值给 Dominion PX 节点添加一个网络浏览器接口：**

URL：<DOMINION PX IP ADDRESS>/auth.asp

TCP 端口：80

Username（用户名）：Dominion PX 管理员的用户名

Password（密码）：Dominion PX 管理员的密码

Username Field（用户名字段）= login

Password Field（密码字段）= password

接口添加结果

在给节点添加接口之后，Add Node（添加节点）或 Node Profile（节点配置文件）屏幕的 Interfaces（接口）表和 Default Interface（默认接口）下拉菜单显示此接口。可以单击下拉菜单，然后选择在建立至节点的连接时要使用的默认接口。

在保存对 Add Node（添加节点）或 Node Profile（节点配置文件）屏幕所做的更改之后，接口名称还出现在 Nodes（节点）列表上，位于可通过它访问的节点下面。

在添加网管电源条接口，把 KX 指定为管理设备之后，用关联节点的名称重新命名你指定的出口。

编辑接口

▶ **编辑接口：**

1. 单击 Nodes（节点）选项卡，然后选择要编辑的节点接口打开 Node Profile（节点配置文件）页。
2. 在 Interfaces（接口）选项卡上选择要编辑的接口所在的行。
3. 单击 Edit（编辑）按钮。
4. 根据需要编辑字段。参看*添加接口* (p. 122)详细了解各个字段。某些字段是只读字段。
5. 单击 OK（确定）按钮保存更改。

删除接口

可以把除下列节点之外的节点上的任何接口删除掉：

- 虚拟机节点上的 VMW Viewer 接口或 VMW Power 接口。
- 集成了 KVM 切换器、在 KX2 设备上指定了 URL 或 IP 地址的刀片服务器机箱的网络浏览器接口。

删除节点接口：

1. 单击 Nodes（节点）选项卡。
2. 单击要删除哪个节点的接口。
3. 在 Interfaces（接口）表上单击要删除的接口所在的行。
4. 单击 Delete（删除）按钮显示一条确认消息。
5. 单击 Yes（是）按钮删除接口。

给使用 IPv6 的节点添加接口

CC-SG 支持用 IPv6 访问有下列接口类型的节点：

- Microsoft RDP
- SSH
- Telnet
- VNC
- Web
- 仅 DRAC for iDRAC6

CC-SG 把给其他接口类型配置的 IPv6 网络地址视为无效目的地。

添加接口书签

如果频繁通过一个特殊接口访问一个节点，可以给此接口添加书签，这样可以在浏览器上选择它。

在任何浏览器上添加接口书签：

1. 在 Nodes（节点）选项卡上选择要给哪个接口添加书签。必须展开节点，才能查看接口。
2. 选择 Nodes(节点)> Bookmark Node Interface(添加节点接口书签)。
3. 选择 Copy URL to Clipboard（把 URL 复制到剪贴板）。
4. 单击 OK（确定）按钮把 URL 复制到剪贴板上。

5. 打开新浏览器窗口，并把 URL 粘贴到地址栏。
6. 按 Enter 连接此 URL。
7. 把此 URL 作为书签（也称为 Favorite[收藏夹]）添加到浏览器收藏夹。

在 Internet Explorer 上添加接口书签（把接口添加到收藏夹）：

1. 在 Nodes（节点）选项卡上选择要给哪个接口添加书签。必须展开节点，才能查看接口。
2. 选择 Nodes（节点）> Bookmark Node Interface（添加节点接口书签）。
3. 选择 Add Bookmark（添加书签）（仅限于 IE）。
4. Bookmark Name（书签名称）字段显示书签默认名称。可以更改此名称，也就是 Internet Explorer 的 Favorites（收藏夹）列表显示的名称。
5. 单击 OK（确定）按钮打开 Add Favorite（添加收藏夹）窗口。
6. 单击 OK（确定）按钮把书签添加到 Favorites（收藏夹）列表上。

访问书签接口：

1. 打开浏览器窗口。
2. 在浏览器的书签列表上选择书签接口。
3. 在打开 CC-SG Access Client 时，用此接口的登录证书登录。打开接口连接。

获取所有接口的书签 URL：

- 可以在 Node Asset Report（节点资产报告）上获取所有节点的书签 URL。参看 *节点资产报告* (p. 230)。

配置节点直接端口访问

可以用 Bookmark Node Interface（添加节点接口书签）功能配置节点直接端口访问。

参看*添加接口书签* (p. 135)。

节点关联、位置和联系人批量复制

批量复制命令允许你把一个节点上的类别、元素、位置和联系人信息复制到多个其他节点上。注意在此过程中，选择的信息即为复制的属性。如果任何所选节点有相同类型的信息，在执行批量复制命令时，用新指定的信息替换现有数据。

批量复制节点关联、位置和联系人信息：

1. 单击 Nodes（节点）选项卡，然后选择一个节点。
2. 选择 Nodes（节点）> Bulk Copy（批量复制）。
3. 在 Available Nodes（可用节点）列表上选择要把 Node Name（节点名称）字段里节点的关联、位置和联系人信息复制到哪些节点上。
4. 单击>按钮把节点添加到 Selected Nodes（选择的节点）列表上。
5. 选择节点，然后单击<按钮把它从 Selected Nodes（选择的节点）列表上删除掉。
6. 在 Associations（关联）选项卡上选择 Copy Node Associations（复制节点关联）复选框复制节点的所有类别和元素。
   - 可以在此选项卡上更改、添加或删除任何数据。修改后的数据被复制到 Selected Nodes（选择的节点）列表上的多个节点，以及 Node Name（节点名称）字段当前显示的节点。**可选。**
7. 在 Location and Contacts（位置和联系人）选项卡上选择要复制的信息对应的复选框：
   - 选择 Copy Location Information（复制位置信息）复选框复制 Location（位置）部分显示的位置信息。
   - 选择 Copy Contact Information（复制联系人信息）复选框复制 Contact（联系人）部分显示的联系人信息。
   - 可以在此选项卡上更改、添加或删除任何数据。修改后的数据被复制到 Selected Nodes（选择的节点）列表上的多个节点，以及 Node Name（节点名称）字段当前显示的节点。**可选。**
8. 单击 OK（确定）按钮进行批量复制。在复制选择的信息之后，显示一条消息。

使用聊天工具

聊天工具给连接同一个节点的用户提供一种相互通信方式。必须连接一个节点，才能针对此节点启动聊天会话。只有连接同一个节点的用户，才能相互聊天。

启动聊天会话：

1. 选择 Nodes（节点）> Chat（聊天）> Start Chat Session（启动聊天会话）。
2. 在左下角字段里输入消息，然后单击 Send（发送）按钮。左上角字段显示消息，所有用户都能看到这些消息。

加入正在进行的聊天会话：

- 选择 Nodes（节点）> Chat（聊天）> Show Chat Session（显示聊天会话）。

结束聊天会话：

1. 单击聊天会话上的 Close（关闭）按钮，显示一条确认消息。
   - 单击 Yes（是）按钮针对所有参与者关闭聊天会话。
   - 单击 No（否）退出聊天会话，但其他人仍然可以聊天。

用 CSV 文件导入法添加、更新和删除节点

可以导入包含节点和接口的 CSV 文件，在 CC-SG 上添加、更新和删除节点和接口。

必须具备设备、端口和节点管理权限与 CC 设置和控制权限，才能导入和导出节点。

必须给你指定一个策略，你才能访问所有相关设备和节点。建议指定 All Nodes（所有节点）和 All Devices（所有设备）全访问策略。

必须给你指定一个策略，你才能访问所有相关设备，导入或导出带外 KVM 接口或带外串行接口和 Power 接口。

不导出或导入控制系统、虚拟主机和虚拟机等虚拟基础设施节点和接口。

可以导入一个 CSV 文件添加、更新和删除此文件里的所有节点和接口。

添加节点 CSV 文件要求

节点 CSV 文件定义节点和接口，以及把它们添加到 CC-SG 所需的详细信息。

- 节点名称必须是唯一的。如果输入重复节点名称，CC-SG 在节点名称后面添加一个用括号括起来的数字使其变成唯一名称，然后添加节点。如果还在 CSV 文件里给节点指定类别和元素，在出现重复节点名称时，可能会把类别和元素指定给错误的节点。为此，输入每个节点的唯一名称。或者先导入节点，在 CC-SG 上检查其名称，然后导入一个独立文件，把类别和元素指定给正确的节点名称。
- 如要添加带外接口，不必事先在 CC-SG 上配置关联接口。
- 不能导入虚拟基础设施节点和接口。使用 Nodes(节点)> Virtualization（虚拟化）上的选项。
- 在 CSV 文件里，把 ADD NODE 命令之后的第一个接口指定为节点默认接口。
- 导出 CC-SG 上的文件查看备注，包括创建有效 CSV 文件所需的所有标签和参数。 参看*导出节点* (p. 161)。
- 满足所有 CSV 文件的其他要求。参看*常见 CSV 文件要求* (参看 "*通用 CSV 文件要求*" p. 394)。
- 部分接口支持 IPv6。参看*带内连接接口 — RDP、VNC、SSH、RSA KVM、iLO Processor KVM、DRAC KVM 和 TELNET* (p. 124) 和*网络浏览器接口* (p. 132)。参看 *Microsoft RDP 连接详细信息* (p. 126)、*Java RDP 连接详细信息* (p. 126)和 *VNC 连接详细信息* (p. 126)了解详情。

在 CSV 文件里添加节点：

列编号	标签或值	详细信息
1	ADD	所有标签的第一列是命令。
2	NODE	输入所示的标签。 标签不区分大小写。
3	Node Name（节点名称）	必填字段。
4	Description（说明）	可选。

在 CSV 文件里添加带外 KVM 接口：

列编号	标签或值	详细信息
1	ADD	所有标签的第一列是命令。
2	NODE-OOBKVM-INTERFAC	输入所示的标签。

列编号	标签或值	详细信息
	E	标签不区分大小写。
3	Node Name（节点名称）	输入与 Raritan Port Name（Raritan 端口名称）相同的值。
4	Raritan Device Name（Raritan 设备名称）	必填字段。 此设备必须已被添加到 CC-SG。
5	Port Number（端口号）	必填字段。
6	Blade Slot/KVM Switch Port（刀片服务器插槽/KVM 切换器端口）	如果此节点与一个刀片服务器关联，输入插槽编号。 如果此节点与一台分层通用模拟 KVM 切换器关联，输入端口号。
7	Raritan Port Name（Raritan 端口名称）	如果保留空白，CC-SG 将使用设备的现有端口名称。如果输入新名称，把名称复制到设备上，SX 设备除外。
8	Interface Name（接口名称）	输入与 Raritan Port Name（Raritan 端口名称）相同的值。
9	Description（说明）	可选。

在 CSV 文件里添加带外串行接口：

列编号	标签或值	详细信息
1	ADD	所有标签的第一列是命令。
2	NODE-OOBSERIAL-INTERFACE	输入所示的标签。 标签不区分大小写。
3	Node Name（节点名称）	输入与 Raritan Port Name（Raritan 端口名称）相同的值。
4	Raritan Device Name（Raritan 设备名称）	必填字段。
5	Port Number（端口号）	必填字段。
6	Raritan Port Name（Raritan 端口名称）	如果保留空白，CC-SG 将使用设备的现有端口名称。如果输入新名称，把名称复制到设备上，SX 设备除外。
7	Interface Name（接口名称）	输入与 Raritan Port Name（Raritan 端口名称）相同的值。

列编号	标签或值	详细信息
8	Baud Rate（波特率）	仅适用于 SX 端口。
9	Parity（奇偶校验）	仅适用于 SX 端口。
10	Flow Control（流控制）	仅适用于 SX 端口。
11	Description（说明）	可选。

在 CSV 文件里添加 RDP 接口：

CSV 文件的列编号	标签或值	详细信息
1	ADD	所有标签的第一列是命令。
2	NODE-RDP-INTERFACE	输入所示的标签。 标签不区分大小写。
3	Node Name（节点名称）	必填字段。
4	Interface Name（接口名称）	必填字段。
5	IP Address or Hostname（IP 地址或主机名）	必填字段。
6	TCP Port（TCP 端口）	默认端口是 3389。
7	Service Account Name（服务帐号名称）	可选。
8	Username（用户名）	可选。
9	Password（密码）	可选。
10	User Type（用户类型）	REMOTE 或 CONSOLE 默认值是 REMOTE。
11	Keyboard Type（键盘类型）	US（美国英文）、UK（英国英文）、Arabic（阿拉伯文）、Danish（丹麦文）、German（德文）、Spanish（西班牙文）、Finnish（芬兰文）、French(法文)、Belgian(比利时)、Croatian（克罗地亚文）、Italian（意大利文）、Japanese（日文）、Lithuanian(立陶宛文)、Latvian（拉托维亚文）、Macedonian(马其顿文)、Norwegian(挪威文)、Polish（波兰文）、Portuguese(葡萄牙文)、Brazilian（巴西葡萄牙文）、

CSV 文件的列编号	标签或值	详细信息
		Russian（俄文）、Slovenian（斯洛文尼亚文）、Swedish（瑞典文）或 Turkish（土耳其文） 默认值是 US（美国英文）。
12	Description（说明）	可选。
13	RDP Type（RDP 类型）	Java 或 Microsoft 默认值是 Java。

在 CSV 文件里添加 SSH 接口或 TELNET 接口：

列编号	标签或值	详细信息
1	ADD	所有标签的第一列是命令。
2	SSH 接口： NODE-SSH-INTERFACE TELNET 接口： NODE-TELNET-INTERFACE	输入所示的标签。 标签不区分大小写。
3	Node Name（节点名称）	必填字段。
4	Interface Name（接口名称）	必填字段。
5	IP Address or Hostname（IP 地址或主机名）	必填字段。
6	TCP Port（TCP 端口）	SSH 的默认端口是 22。 TELNET 的默认端口是 23。
7	Service Account Name（服务帐号名称）	可选。如果指定用户名和密码，保留空白。
8	Username（用户名）	可选。如果指定服务帐号，保留空白。
9	Password（密码）	可选。
10	Description（说明）	可选。

在 CSV 文件里添加 VNC 接口：

列编号	标签或值	详细信息
1	ADD	所有标签的第一列是命令。

列编号	标签或值	详细信息
2	NODE-VNC-INTERFACE	输入所示的标签。 标签不区分大小写。
3	Node Name（节点名称）	必填字段。
4	Interface Name（接口名称）	必填字段。
5	IP Address or Hostname（IP 地址或主机名）	必填字段。
6	TCP Port（TCP 端口）	默认端口是 5900。
7	Service Account Name（服务帐号名称）	可选。如果指定密码，保留空白。
8	Password（密码）	可选。如果指定服务帐号，保留空白。
9	Description（说明）	可选。

在 CSV 文件里添加 DRAC KVM、DRAC Power、ILO KVM、ILO Power、Integrity ILO2 Power 或 RSA Power 接口：

在导入 DRAC 接口、ILO 接口和 RSA 接口时，必须指定 KVM interface（KVM 接口）和 Power interface（Power 接口），否则导入失败。

列编号	标签或值	详细信息
1	ADD	所有标签的第一列是命令。
2	DRAC KVM 接口： NODE-DRAC-KVM-INTERFACE DRAC Power 接口： NODE-DRAC-POWER-INTERFACE iLO KVM 接口： NODE-ILO-KVM-INTERFACE iLO Power 接口： NODE-ILO-POWER-INTERFACE Integrity ILO2 Power 接口： NODE-INT-ILO2-POWER-INTERFACE RSA Power 接口： NODE-RSA-POWER-INTERFACE	输入所示的标签。 标签不区分大小写。

列编号	标签或值	详细信息
3	Node Name（节点名称）	必填字段。
4	Interface Name（接口名称）	必填字段。
5	IP Address or Hostname（IP 地址或主机名）	必填字段。
6	Service Account Name（服务帐号名称）	必须输入服务帐号，或者输入用户名和密码。 如果指定用户名和密码，保留空白。
7	Username（用户名）	必须输入服务帐号，或者输入用户名和密码。 如果指定服务帐号，保留空白。
8	Password（密码）	必须输入服务帐号，或者输入用户名和密码。 如果指定服务帐号，保留空白。
9	Description（说明）	可选。
10*	TCP Port（TCP 端口）	* 对于 NODE-DRAC-POWER-INTERFACE，只指定 TCP 端口。 默认端口是 22。

在 CSV 文件里添加 UCS KVM 接口：

指定在访问机箱和刀片服务器时所用的帐号的户名和密码。

列编号	标签或值	详细信息
1	ADD	所有标签的第一列是命令。
2	NODE-UCS-KVM-INTERFACE	输入所示的标签。 标签不区分大小写。
3	Node Name（节点名称）	必填字段。
4	Interface Name（接口名称）	必填字段。
5	UCS Chassis IP address or hostname（UCS 机箱 IP 地址或主机名）	必填字段。
6	TCP Port（TCP 端口）	默认端口是 443。

列编号	标签或值	详细信息
7	Blade IP address or hostname（刀片服务器 IP 地址或主机名）	
8	Service Account Name（服务帐号名称）	可选。如果指定用户名和密码，保留空白。
9	Username（用户名）	可选。如果指定服务帐号，保留空白。
10	Password（密码）	可选。如果指定服务帐号，保留空白。
11	Description（说明）	可选。

在 CSV 文件里添加 RSA KVM 接口：

在导入 DRAC 接口、ILO 接口和 RSA 接口时，必须指定 KVM interface（KVM 接口）和 Power interface（Power 接口），否则导入失败。

列编号	标签或值	详细信息
1	ADD	所有标签的第一列是命令。
2	NODE-RSA-KVM-INTERFACE	输入所示的标签。 标签不区分大小写。
3	Node Name（节点名称）	必填字段。
4	Interface Name（接口名称）	必填字段。
5	IP Address or Hostname（IP 地址或主机名）	必填字段。
6	TCP Port（TCP 端口）	默认端口是 2000
7	Service Account Name（服务帐号名称）	如果指定用户名和密码，保留空白。
8	Username（用户名）	如果指定服务帐号，保留空白。
9	Password（密码）	如果指定服务帐号，保留空白。
10	Description（说明）	可选。

在 CSV 文件里添加 IPMI 电源控制接口：

列编号	标签或值	详细信息
1	ADD	所有标签的第一列是命令。
2	NODE-IPMI-INTERFACE	输入所示的标签。

列编号	标签或值	详细信息
		标签不区分大小写。
3	Node Name（节点名称）	必填字段。
4	Interface Name（接口名称）	必填字段。
5	IP Address or Hostname（IP 地址或主机名）	必填字段。
6	UDP Port（UDP 端口）	默认端口是 623
7	Authentication（验证）	MD5、None、OEM 或 PASSWORD 默认值是 PASSWORD。
8	Interval（时间间隔）	输入检查间隔秒数。默认端口是 550。
9	Service Account Name（服务帐号名称）	如果指定用户名和密码，保留空白。
10	Username（用户名）	如果指定服务帐号，保留空白。
11	Password（密码）	如果指定服务帐号，保留空白。
12	Description（说明）	可选。

在 CSV 文件里添加网管电源条接口：

列编号	标签或值	详细信息
1	ADD	所有标签的第一列是命令。
2	NODE-POWER-INTERFACE	输入所示的标签。 标签不区分大小写。
3	Node Name（节点名称）	必填字段。
4	Interface Name（接口名称）	必填字段。
5	Powerstrip Name（电源条名称）	必填字段。
6	Outlet（出口）	必填字段。
7	Managing Device（管理设备）	电源条相连的设备的名称。 对于除 Dominion PX 之外的所有电源条，这是必填字段。
8	Managing Port（管理端口）	电源条相连的设备端口的名称。 对于除 Dominion PX 之外的所有电

列编号	标签或值	详细信息
		源条，这是必填字段。
9	Description（说明）	可选。

在 CSV 文件里添加网络浏览器接口：

列编号	标签或值	详细信息
1	ADD	所有标签的第一列是命令。
2	NODE-WEB-INTERFACE	输入所示的标签。 标签不区分大小写。
3	Node Name（节点名称）	必填字段。
4	Interface Name（接口名称）	必填字段。
5	URL	必填字段。
6	TCP Port（TCP 端口）	默认端口是 80。
7	Service Account Name（服务帐号名称）	可选。如果指定用户名和密码，保留空白。
8	Username（用户名）	可选。如果指定服务帐号，保留空白。
9	Password（密码）	可选。如果指定服务帐号，保留空白。
10	Username Field（用户名字段）	可选。参看*添加网络浏览器接口注意事项* (参看 "*添加网络浏览器界面注意事项*" p. 133)
11	Password Field（密码字段）	可选。参看*添加网络浏览器接口注意事项* (参看 "*添加网络浏览器界面注意事项*" p. 133)
12	Description（说明）	可选。

在 CSV 文件里添加 Power IQ Proxy 电源控制接口：

参看 ***Power IQ IT 设备电源控制*** (p. 362)详细了解如何配置此类接口。

列编号	标签或值	详细信息
1	ADD	所有标签的第一列是命令 ADD。
2	NODE-POWER-PIQ-INTERFACE	输入所示的标签。 标签不区分大小写。
3	Node Name（节点名称）	必填字段。

列编号	标签或值	详细信息
4	Interface Name（接口名称）	必填字段。
5	External Key（外部键）	▪ 如果 IT 设备已被添加到 Power IQ，在 Data Center（数据中心）选项卡上的 IT 设备页上找到外部键，在此字段里输入外部键。 ▪ 如果 IT 设备尚未被添加到 Power IQ，输入一个文本值，但确保在把 IT 设备添加到 Power IQ 时使用相同的值。可以采用导出方法，迅速创建一个包含所有节点信息和接口信息的文件。参看*导出节点* (p. 161)。
6	Managing Power IQ Name（管理 Power IQ 名称）	输入管理 IT 设备的 Power IQ 的名称。此名称必须与 Access（访问）> Power IQ Services（Power IQ 服务）> Power IQ Device Name Configuration（Power IQ 设备名称配置）对话框上 Power IQ Device Name（Power IQ 设备名称）字段里的值相同。 参看*配置 Power IQ 服务* (p. 363)。
7	Description（说明）	可选。

▶ 在 CSV 文件里给节点指定类别和元素：

必须先在 CC-SG 上创建类别和元素。

可以在 CSV 文件里给一个节点指定同一类别的多个元素。

类别和元素只支持 ADD 命令。不能用 CSV 导入法更新或删除类别和元素。

列编号	标签或值	详细信息
1	`ADD`	所有标签的第一列是命令。
2	`NODE-CATEGORYELEMENT`	输入所示的标签。 标签不区分大小写。
3	Node Name（节点名称）	必填字段。
4	Category Name（类别名称）	必填字段。
5	Element Name（元素名称）	必填字段。

更新节点 CSV 文件要求

在用 CSV 文件更新节点和接口时，此文件必须使用 UPDATE 命令，并定义旧名称和新名称才能更改所有名称。

CC-SG 按顺序处理 CSV 文件的每一行。在更改名称之后，不再保存旧名称，只能用新名称查找节点。

在 CSV 文件里输入新名称时，在此之后的所有行在引用节点时必须使用新节点名称。例如：如果在第一行重新命名一个节点，在第二行更新此节点的其中一个接口，必须在第二行使用此节点的新名称。

- 节点名称必须是唯一的。如果 CSV 文件包含的新名称是重复名称，在验证文件时显示警告消息。必须修改重复名称，才能导入文件。
- 如要更新接口详细信息但不更新接口名称，在 CSV 文件的 interface name 列和 new interface name 列输入当前接口名称。
- 不能更新类别和元素。
- 不能更新带外 KVM 接口或带外串行接口对应的访问应用程序选择。
- 不能更新虚拟基础设施节点和接口。使用 Nodes(节点)> Virtualization（虚拟化）上的选项。
- 不能更新 Power IQ Proxy 电源控制接口。使用 Power IQ 同步。参看*同步 Power IQ 和 CC-SG* (p. 366)。
- 导出 CC-SG 上的文件查看备注，包括创建有效 CSV 文件所需的所有标签和参数。 参看*导出节点* (p. 161)。
- 满足所有 CSV 文件的其他要求。参看*常见 CSV 文件要求* (参看 "*通用 CSV 文件要求*" p. 394)。

用 CSV 更新节点名称

列编号	标签或值	详细信息
1	UPDATE	所有标签的第一列是命令。
2	NODE	输入所示的标签。 标签不区分大小写。
3	Node Name（节点名称）	必填字段。 当前节点名称。
4	New Node Name(新节点名称）	必填字段。 新节点名称。 在 CSV 文件里的其他行引用此节点

列编号	标签或值	详细信息
		时，要使用新名称。
5	Description（说明）	可选。

用 CSV 更新带外 KVM 接口或带外串行接口

列编号	标签或值	详细信息
1	`UPDATE`	所有标签的第一列是命令。
2	带外 KVM 接口：`NODE-OOBKVM-INTERFACE`，带外串行接口：`NODE-OOBSERIAL-INTERFACE`	输入所示的标签。 标签不区分大小写。
3	Node Name（节点名称）	必填字段。 此接口所属的节点。
4	Interface Name（接口名称）	必填字段。 当前接口名称。
5	New Interface Name（新接口名称）	必填字段。 新接口名称。
6	Description（说明）	可选字段。

用 CSV 更新 RDP 接口

列编号	标签或值	详细信息
1	`UPDATE`	所有标签的第一列是命令。
2	`NODE-RDP-INTERFACE`	输入所示的标签。 标签不区分大小写。
3	Node Name（节点名称）	必填字段。 此接口所属的节点。
4	Interface Name（接口名称）	必填字段。 当前接口名称。

列编号	标签或值	详细信息
5	New Interface Name（新接口名称）	必填字段。 新接口名称。
6	IP Address/Hostname（IP 地址/主机名）	
7	TCP Port（TCP 端口）	默认端口是 3389。
8	Service Account Name（服务帐号名称）	可选。
9	Username（用户名）	可选。
10	Password（密码）	可选。
11	User Type（用户类型）	REMOTE 或 CONSOLE 默认值是 REMOTE。
12	Keyboard Type（键盘类型）	US（美国英文）、UK（英国英文）、Arabic（阿拉伯文）、Danish（丹麦文）、German（德文）、Spanish（西班牙文）、Finnish（芬兰文）、French（法文）、Belgian（比利时）、Croatian（克罗地亚文）、Italian（意大利文）、Japanese（日文）、Lithuanian（立陶宛文）、Latvian（拉托维亚文）、Macedonian（马其顿文）、Norwegian（挪威文）、Polish（波兰文）、Portuguese（葡萄牙文）、Brazilian（巴西葡萄牙文）、Russian（俄文）、Slovenian（斯洛文尼亚文）、Swedish（瑞典文）或 Turkish（土耳其文） 默认值是 US（美国英文）。
13	Description（说明）	可选。
14	RDP Type（RDP 类型）	Java 或 Microsoft 默认值是 Java。

用 CSV 更新 SSH 接口或 Telnet 接口

列编号	标签或值	详细信息
1	UPDATE	所有标签的第一列是命令。
2	SSH 接口： NODE-SSH-INTERFACE TELNET 接口： NODE-TELNET-INTERFACE	输入所示的标签。 标签不区分大小写。
3	Node Name（节点名称）	必填字段。
4	Interface Name（接口名称）	必填字段。
5	New Interface Name（新接口名称）	必填字段。
6	IP Address or Hostname（IP 地址或主机名）	必填字段。
7	TCP Port（TCP 端口）	SSH 的默认端口是 22。 TELNET 的默认端口是 23。
8	Service Account Name（服务帐号名称）	可选。如果指定用户名和密码，保留空白。 输入新服务帐号名称更新它。
9	Username（用户名）	可选。如果指定服务帐号，保留空白。 输入新用户名更新它。
10	Password（密码）	可选。 输入新密码更新它。
11	Description（说明）	可选。

用 CSV 更新 VNC 接口

列编号	标签或值	详细信息
1	UPDATE	所有标签的第一列是命令。
2	NODE-VNC-INTERFACE	输入所示的标签。 标签不区分大小写。

列编号	标签或值	详细信息
3	Node Name（节点名称）	必填字段。
4	Interface Name（接口名称）	必填字段。
5	New Interface Name（新接口名称）	必填字段。
6	IP Address or Hostname（IP 地址或主机名）	必填字段。
7	TCP Port（TCP 端口）	默认端口是 5900。
8	Service Account Name（服务帐号名称）	可选。如果指定密码，保留空白。 输入新服务帐号名称更新它。
9	Password（密码）	可选。如果指定服务帐号，保留空白。 输入新密码更新它。
10	Description（说明）	可选。

用 CSV 更新网络浏览器接口

列编号	标签或值	详细信息
1	`UPDATE`	所有标签的第一列是命令。
2	`NODE-WEB-INTERFACE`	输入所示的标签。 标签不区分大小写。
3	Node Name（节点名称）	必填字段。
4	Interface Name（接口名称）	必填字段。
5	New Interface Name（新接口名称）	必填字段。
6	URL	必填字段。
7	TCP Port（TCP 端口）	默认端口是 80。
8	Service Account Name（服务帐号名称）	可选。如果指定用户名和密码，保留空白。 输入新服务帐号名称更新它。
9	Username（用户名）	可选。如果指定服务帐号，保留空白。 输入新用户名更新它。

列编号	标签或值	详细信息
10	Password（密码）	可选。如果指定服务帐号，保留空白。 输入新密码更新它。
11	Username Field（用户名字段）	可选。参看*添加网络浏览器接口注意事项* (参看 "*添加网络浏览器界面注意事项*" p. 133)
12	Password Field（密码字段）	可选。参看*添加网络浏览器接口注意事项* (参看 "*添加网络浏览器界面注意事项*" p. 133)
13	Description（说明）	可选。

用 CSV 更新 DRAC KVM、DRAC Power、iLO KVM、iLO Power、Integrity iLO2 Power 或 RSA Power 接口

在导入 DRAC 接口、ILO 接口和 RSA 接口时，必须指定 KVM interface（KVM 接口）和 Power interface（Power 接口），否则导入失败。

列编号	标签或值	详细信息
1	`UPDATE`	所有标签的第一列是命令。

2	DRAC KVM 接口：
	`NODE-DRAC-KVM-INTERFACE`
	DRAC Power 接口：
	`NODE-DRAC-POWER-INTERFACE`
	iLO KVM 接口：
	`NODE-ILO-KVM-INTERFACE`
	iLO Power 接口：
	`NODE-ILO-POWER-INTERFACE`
	Integrity ILO2 Power 接口：
	`NODE-INT-ILO2-POWER-INTERFACE`
	RSA Power 接口：
	`NODE-RSA-POWER-INTERFACE`
		输入所示的标签。
		标签不区分大小写。

3	Node Name（节点名称）	必填字段。

列编号	标签或值	详细信息
4	Interface Name（接口名称）	必填字段。 当前接口名称。
5	New Interface Name（新接口名称）	必填字段。新接口名称。
6	IP Address or Hostname（IP 地址或主机名）	必填字段。
7	Service Account Name（服务帐号名称）	必须输入服务帐号，或者输入用户名和密码。 如果指定用户名和密码，保留空白。 输入新服务帐号名称更新它。
8	Username（用户名）	必须输入服务帐号，或者输入用户名和密码。 如果指定服务帐号，保留空白。 输入新用户名更新它。
9	Password（密码）	必须输入服务帐号，或者输入用户名和密码。 如果指定服务帐号，保留空白。 输入新密码更新它。
10	Description（说明）	可选。
11*	TCP Port（TCP 端口）	* 对于 NODE-DRAC-POWER-INTERFACE，只指定 TCP 端口。 默认端口是 22。

用 CSV 更新 RSA KVM 接口

在导入 DRAC 接口、ILO 接口和 RSA 接口时，必须指定 KVM interface（KVM 接口）和 Power interface（Power 接口），否则导入失败。

列编号	标签或值	详细信息
1	UPDATE	所有标签的第一列是命令。
2	NODE-RSA-KVM-INTERFACE	输入所示的标签。 标签不区分大小写。

列编号	标签或值	详细信息
3	Node Name（节点名称）	必填字段。
4	Interface Name（接口名称）	必填字段。 当前接口名称。
5	New Interface Name（新接口名称）	必填字段。 新接口名称。
6	IP Address or Hostname（IP 地址或主机名）	必填字段。
7	TCP Port（TCP 端口）	默认端口是 2000
8	Service Account Name（服务帐号名称）	如果指定用户名和密码，保留空白。 输入新服务帐号名称更新它。
9	Username（用户名）	如果指定服务帐号，保留空白。 输入新用户名更新它。
10	Password（密码）	如果指定服务帐号，保留空白。 输入新密码更新它。
11	Description（说明）	可选。

用 CSV 更新 IPMI 接口

列编号	标签或值	详细信息
1	`UPDATE`	所有标签的第一列是命令。
2	`NODE-IPMI-INTERFACE`	输入所示的标签。 标签不区分大小写。
3	Node Name（节点名称）	必填字段。
4	Interface Name（接口名称）	必填字段。 当前接口名称。
5	New Interface Name（新接口名称）	必填字段。 新接口名称。
6	IP Address or Hostname（IP 地址或主机名）	必填字段。

列编号	标签或值	详细信息
7	UDP Port（UDP 端口）	默认端口是 623
8	Authentication（验证）	MD5、None、OEM 或 PASSWORD 默认值是 PASSWORD。
9	Interval（时间间隔）	输入检查间隔秒数。默认端口是 550。
10	Service Account Name（服务帐号名称）	如果指定用户名和密码，保留空白。 输入新服务帐号名称更新它。
11	Username（用户名）	如果指定服务帐号，保留空白。 输入新用户名更新它。
12	Password（密码）	如果指定服务帐号，保留空白。 输入新密码更新它。
13	Description（说明）	可选。

用 CSV 更新 UCS KVM 接口

指定在访问机箱和刀片服务器时所用的帐号的户名和密码。

列编号	标签或值	详细信息
1	UPDATE	所有标签的第一列是命令。
2	NODE-UCS-KVM-INTERFACE	输入所示的标签。 标签不区分大小写。
3	Node Name（节点名称）	必填字段。
4	Interface Name（接口名称）	必填字段。 当前接口名称。
5	New Interface Name（新接口名称）	必填字段。 新接口名称。
6	Chassis IP address or hostname（机箱 IP 地址或主机名）	必填字段。
7	TCP Port（TCP 端口）	默认端口是 443。
8	Blade IP address or hostname（刀片服务器 IP	必填字段。

指定在访问机箱和刀片服务器时所用的帐号的户名和密码。

列编号	标签或值	详细信息
	地址或主机名）	
9	Service Account Name（服务帐号名称）	可选。如果指定用户名和密码，保留空白。 输入新服务帐号名称更新它。
10	Username（用户名）	可选。如果指定服务帐号，保留空白。 输入新用户名更新它。
11	Password（密码）	可选。如果指定服务帐号，保留空白。 输入新密码更新它。
12	Description（说明）	可选。

删除节点 CSV 文件要求

在用 CSV 文件删除接口时，节点至少要有一个接口，否则删除操作失败。

不能删除节点的类别和元素。

用 CSV 删除节点

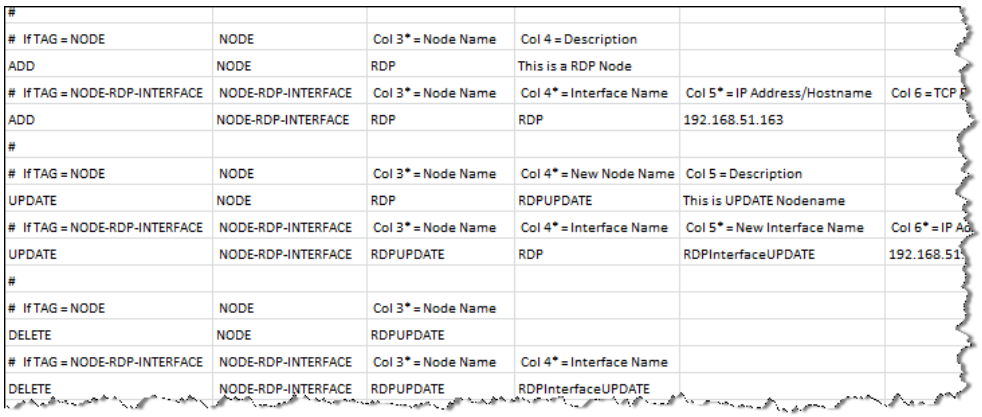
列编号	标签或值	详细信息
1	DELETE	所有标签的第一列是命令。
2	NODE	输入所示的标签。 标签不区分大小写。
3	Node Name（节点名称）	必填字段。

用 CSV 删除接口

列编号	标签或值	详细信息
1	DELETE	所有标签的第一列是命令。
2	NODE-OOBKVM-INTERFACE NODE-OOBSERIAL-INTERFACE	输入所示的标签。 标签不区分大小写。 可以删除所有接口。

列编号	标签或值	详细信息
	NODE-RDP-INTERFACE NODE-SSH-INTERFACE NODE-TELNET-INTERFACE NODE-VNC-INTERFACE NODE-WEB-INTERFACE NODE-DRAC-KVM-INTERFACE NODE-DRAC-POWER-INTERFACE NODE-ILO-KVM-INTERFACE NODE-ILO-POWER-INTERFACE NODE-INT-ILO2-POWER-INTERFACE NODE-RSA-KVM-INTERFACE NODE-RSA-POWER-INTERFACE NODE-IPMI-INTERFACE NODE-UCS-KVM-INTERFACE	
3	Node Name（节点名称）	必填字段。
4	Interface Name（接口名称）	必填字段。

节点 CSV 文件示例



#					
# If TAG = NODE	NODE	Col 3* = Node Name	Col 4 = Description		
ADD	NODE	RDP	This is a RDP Node		
# If TAG = NODE-RDP-INTERFACE	NODE-RDP-INTERFACE	Col 3* = Node Name	Col 4* = Interface Name	Col 5* = IP Address/Hostname	Col 6 = TCP P
ADD	NODE-RDP-INTERFACE	RDP	RDP	192.168.51.163	
#					
# If TAG = NODE	NODE	Col 3* = Node Name	Col 4* = New Node Name	Col 5 = Description	
UPDATE	NODE	RDP	RDPUPDATE	This is UPDATE Nodename	
# If TAG = NODE-RDP-INTERFACE	NODE-RDP-INTERFACE	Col 3* = Node Name	Col 4* = Interface Name	Col 5* = New Interface Name	Col 6* = IP Ad
UPDATE	NODE-RDP-INTERFACE	RDPUPDATE	RDP	RDPInterfaceUPDATE	192.168.51
#					
# If TAG = NODE	NODE	Col 3* = Node Name			
DELETE	NODE	RDPUPDATE			
# If TAG = NODE-RDP-INTERFACE	NODE-RDP-INTERFACE	Col 3* = Node Name	Col 4* = Interface Name		
DELETE	NODE-RDP-INTERFACE	RDPUPDATE	RDPInterfaceUPDATE		

导入节点

在创建 CSV 文件之后，验证此文件是否有错误，然后导入文件。

跳过重复记录，不添加重复记录。

1. 选择 Administration（管理）> Import（导入）> Import Nodes（导入节点）。
2. 单击 Browse（浏览）按钮选择要导入的 CSV 文件，然后单击 Open（打开）按钮。
3. 单击 Validate（验证）按钮。Analysis Report（分析报告）区显示文件内容。
   - 如果文件无效，显示错误消息。单击 OK（确定）按钮查看页面 Problems（问题）区显示的文件问题说明。单击 Save to File（保存到文件）按钮保存问题列表。编辑 CSV 文件纠正错误，然后再验证一次。参看*排除 CSV 文件问题* (p. 396)。
4. 单击 Import（导入）按钮。
5. 单击 Actions（操作）区查看导入结果。用绿色文字显示成功导入的项目，用红色文字显示导入失败的项目。由于已经有同名项目，或者已经导入了，也用红色文字显示导入失败的项目。
6. 如要查看导入结果详细信息，查看 Audit Trail（审计跟踪）报告。参看*导入审计跟踪项* (p. 395)。

导出节点

导出文件的最前面有备注，说明文件里的每一项。可以根据备注说明，创建要导入的文件。

导出节点：

1. 选择 Administration（管理）> Export（导出）> Export Nodes（导出节点）。
2. 单击 Export to File（导出成文件）按钮。
3. 输入文件名，然后选择文件保存位置。
4. 单击 Save（保存）按钮。

添加、编辑和删除节点组

节点组概述

节点组用于把节点分成组。在授予或拒绝节点组访问权时，节点组是访问策略的基础。参看*添加策略* (p. 186)。节点可以通过 Select（选择）方法进行人工组合，也可以通过 Describe（描述）方法创建一个逻辑表达式描述共有属性来进行人工组合。

如果利用指导设置给节点创建类别和元素，已经创建了按共有属性组织管理节点的方法。CC-SG 自动根据这些元素创建默认访问策略。参看*关联、类别和元素* (p. 37)详细了解如何创建类别和元素。

查看节点组：

- 选择 Associations（关联）> Node Groups（节点组），打开 Node Groups Manager（节点组管理器）窗口。左边显示现有节点组的列表，而主面板显示所选节点组的详细信息。
  - 左边显示现有节点组的列表。在节点组管理器上单击一个节点组，可以查看此节点组的详细信息。
  - 如果节点组是任意组合的，显示 Select Nodes（选择节点）选项卡，显示节点组节点列表和非节点组节点列表。
  - 如果节点组是根据共有属性组合的，显示 Describe Nodes（描述节点）选项卡，显示节点组节点选择规则。
  - 如要在节点组列表上搜索节点，在列表下面的 Search（搜索）字段里输入字符串，然后单击 Search（搜索）按钮。搜索方法通过 My Profile（我的配置文件）屏幕配置。参看*用户和用户组* (p. 166)。

- 如果按属性查看节点组，单击 View Nodes（查看节点）按钮显示 Node Group（节点组）里当前节点的列表。打开 Nodes In Node Group（节点组里的节点）窗口，显示节点及其所有属性。

添加节点组

添加节点组：

1. 选择 Associations(关联)> Node Group(节点组)，打开 Node Groups Manager（节点组管理器）窗口。
2. 选择 Groups（节点组）> New（新建）。显示节点组模板。
3. 在 Group name（节点组名称）字段里输入要创建的节点组的名称。参看*命名常规* (p. 431)详细了解 CC-SG 的名称长度规则。
4. 可以采用两种方法把节点添加到节点组：Select Nodes（选择节点）和 Describe Nodes（描述节点）。Select Nodes（选择节点）方法允许你在可用节点列表上选择节点，把它们任意指定给节点组。Describe Nodes（描述节点）方法允许你指定节点描述规则，参数符合该描述的节点被添加到节点组里。

描述方法与选择方法

如果你希望设备组建立在节点或设备的某些属性之上，例如类别和元素，要使用描述方法。描述方法的优点是在你添加更多有相同描述属性的设备或节点时，它们被自动添加到设备组里。

如果只想人工创建由特定节点构成的设备组，要使用选择方法。被添加到 CC-SG 的新节点和设备并不自动添加到这些设备组里。在把新节点或设备添加到 CC-SG 之后，必须人工把它们添加到设备组里。

这两种方法不能混用。

在用一种方法创建一个设备组之后，必须用同一种方法编辑此设备组。如果换用另一种方法，将覆盖当前设备组设置。

选择节点

用选择节点选项添加节点组：

1. 单击 Select Nodes（选择节点）选项卡。
2. 单击 Device Name（设备名称）下拉菜单，然后选择一个设备过滤 Available（可用）列表，只显示那些与此设备有相同接口的节点。
3. 在 Available(可用)列表上选择要添加到节点组的节点，然后单击 Add（添加）按钮把它移动到 Selected（选择）列表上。Selected（选择）列表上的节点将被添加到节点组里。

- 如要删除节点组里的一个节点，在 Selected（选择）列表上选择节点名称，然后单击 Remove（删除）按钮。
- 可以在 Available（可用）或 Selected（选择）列表上搜索节点。在列表下面的字段里输入搜索词，然后单击 Go（搜索）按钮。

4. 如果要创建一个策略，始终允许访问此节点组里的节点，选择 Create Full Access Policy For This Group（给此节点组创建全访问策略）复选框。
5. 在把节点添加到节点组之后，单击 OK（确定）按钮创建节点组。节点组被添加到左边的 Node Groups（节点组）列表上。

描述节点

用描述节点选项添加节点组：

1. 单击 Select Nodes（选择节点）选项卡。
2. 单击 Add New Row（添加新行）图标  在表中添加一行创建新规则。规则格式类似表达式，可与节点进行比较。
3. 双击行上的每一列把适当的单元格变成下拉菜单，然后给每个部件选择适当的值：
   - Prefix（前缀）— 保留空白，或者选择 NOT（否）。如果选择 NOT（否），此规则将过滤与表达式其他值相反的值。
   - Category（类别）— 选择一个在规则里求值的属性。在这里可以选择你用关联管理器创建的所有类别。还包括 Node Name（节点名称）和 Interface（接口）。如果在此系统上配置了任何刀片服务器机箱，默认有 Blade Chassis（刀片服务器机箱）类别。
   - Operator（运算符）— 选择要在类别项和元素项之间执行的比较运算。有三种运算符可供选择：=（等于）、LIKE（用于查找名称里的元素）和 <>（不等于）。
   - Element（元素）— 选择要比较的类别属性值。这里只出现与所选类别关联的元素（例如：如果对“部门”类别求值，这里不出现“位置”元素）。
   - Rule Name（规则名称）— 这是给此行上的规则指定的名称。这些值不能编辑。用这些值在 Short Expression（简短表达式）字段里编写描述。

     例如规则可能是 Department = Engineering，表示它描述 Department 类别设置为 Engineering 的所有设备。这与你在 Add Node（添加节点）操作过程中配置关联时的情形完全相同。

4. 如果要添加另一个规则，再次单击 Add New Row（添加新行）图标，进行必要的配置。在配置多个规则时，允许你提供多个节点求值标准，从而进行更精确的描述。

   - 如要删除一个规则，在表上突出显示此规则，然后单击 Remove Row（删除行）图标  。

5. 规则表将可用标准用于节点求值。如要编写节点组描述，在 Short Expression（简短表达式）字段里按 Rule Name（规则名称）添加规则。如果描述只需要一个规则，在字段里输入规则名称。如果要对多个规则求值，在字段里输入一组规则，用逻辑运算符描述规则彼此之间的关系。

   - &— AND（与）运算符。节点必须满足此运算符两边的规则，描述（或部分描述）求值才为真。
   - | — OR（或）运算符。节点必须满足此运算符任一边的规则，描述（或部分描述）求值才为真。
   - (and) — 组合运算符。它将描述划分成几个部分，放在括号里。先对括号里的部分求值，然后将描述的其余部分与节点进行比较。括号组可以嵌入其他括号里。

     示例 1：如果要描述属于工程部的节点，创建 Department = Engineering 规则。这将变成 Rule0。然后在 Short Expression（简短表达式）字段里输入 Rule0。

     示例 2：如果要描述属于工程部或者位于费城的一组设备，指定所有机器必须有 1GB 内存，必须创建三个规则。Department = Engineering (Rule0) Location = Philadelphia (Rule1) Memory = 1GB (Rule2)。这些规则必须按相互之间的关系排列。由于设备可能属于工程部或位于费城，所以用“或”运算符 | 连接两个规则：Rule0 | Rule1。先用括号把它括起来进行比较：(Rule0 | Rule1)。由于设备必须满足此比较，并且要有 1GB 内存，所以用“与”运算符 & 将这部分和 Rule2 连起来：(Rule0 | Rule1) & Rule2。在 Short Expression（简短表达式）字段里输入这个最终表达式。

注意：应该在 & 和 | 运算符前后各加一个空格。否则在删除表中的任何规则之后，Short Expression（简短表达式）字段可能返回默认表达式，即 Rule0 & Rule1 & Rule2 等。

---

6. 在 Short Expression（简短表达式）字段里输入描述之后，单击 Validate（验证）按钮。如果描述格式错误，会显示警告消息。如果描述格式正确无误，Normalized Expression（规范表达式）字段显示规范格式的表达式。

7. 单击 View Nodes（查看节点）按钮查看哪些节点满足此表达式。打开 Nodes in Node Group（节点组里的节点）窗口，显示将按当前表达式组合的节点。可以用它检查输入的表达式是否正确无误。如果输入错误，可以返回规则表或 Short Expression（简短表达式）字段修改错误。
8. 如果要创建一个策略，始终允许访问此节点组里的节点，选择 Create Full Access Policy For This Group（给此节点组创建全访问策略）复选框。
9. 在描述此节点组里的节点之后，单击 OK（确定）按钮创建节点组。节点组被添加到左边的 Node Groups（节点组）列表上。

编辑节点组

编辑节点组，更改组成员关系和说明。

编辑节点组：

1. 选择 Associations（关联）> Node Group（节点组）打开 Node Groups Manager（节点组管理器）窗口。
2. 在 Node Group（节点组）列表上单击要编辑的节点。Node Groups（节点组）窗口显示此节点的详细信息。
3. 参看 Select Nodes（选择节点）或 Describe Nodes（描述节点）部分的说明详细了解如何配置节点组。
4. 单击 OK（确定）按钮保存更改。

删除节点组

删除节点组：

1. 选择 Associations（关联）> Node Group（节点组）打开 Node Groups Manager（节点组管理器）窗口。
2. 在左边的 Node Group（节点组）列表上选择要删除的节点。
3. 选择 Groups（节点组）> Delete（删除）。
4. 打开 Delete Node Group（删除节点组）面板。单击 Delete（删除）按钮。
5. 在显示的确认消息窗口上，单击 Yes（是）按钮。

Ch 9 用户和用户组

创建用户帐号，给用户指定访问 CC-SG 所需的用户名和密码。

用户组定义其成员的一组权限。不能给用户指定权限，只能给用户组指定权限。所有用户必须属于至少一个用户组。

CC-SG 维护一个集中用户列表和用户组列表，用于验证和授权。

也可以配置 CC-SG 使用外部验证。参看***远程验证*** (参看 "***Remote Authentication（远程验证）***" p. 199)。

还必须创建访问策略，给用户组指定这些策略。参看***访问控制策略*** (p. 186)。

在本章内

用户选项卡

单击 Users（用户）选项卡，显示 CC-SG 上的所有用户组和用户。

用户位于他们所属的用户组下面。列表显示指定了用户的用户组，用户组旁边有一个 + 号。单击 + 号展开或折叠列表。活动用户（当前登录 CC-SG 的用户）用粗体显示。

Users（用户）选项卡便于你在树视图上搜索用户。

默认用户组

CC-SG 配置了三个默认用户组：CC-Super User（CC 超级用户）、System Administrators（系统管理员）和 CC Users（CC 用户）。

CC 超级用户组

CC 超级用户组有全管理权和访问权。此组只能有一个用户成员。默认用户名是 admin。可以更改默认用户名。不能删除 CC 超级用户组。不能更改给 CC 超级用户组指定的权限，不能给它添加成员，不能删除此组里的唯一用户。CC 超级用户组成员始终要使用强密码。强密码要求如下：

- 密码至少要有一个小写字母。
- 密码至少要有一个大写字母。
- 密码至少要有一个数字。
- 密码至少要有一个特殊字符（例如感叹号或 &）。

注意：不能采用 CSV 文件导入法对 CC 超级用户组进行任何更改。

系统管理员组

系统管理员组有全管理权和访问权。不能更改这些权限。可以添加或删除成员。

CC 用户组

CC 用户组有带内节点和带外节点访问权。可以更改 CC 用户组权限，可以添加或删除成员。

重要说明：很多菜单项只有在选择了适当的用户组或用户之后才能选择。

添加、编辑和删除用户组

添加用户组

先创建用户组，有助于在添加用户时组织管理用户。在创建用户组时，给用户组指定一组权限。指定了用户组的用户将继承这些权限，例如：如果创建一个用户组，并给它指定用户管理权限，那么给此用户组指定的所有用户都能看到和执行 User Manager（用户管理器）菜单上的命令。参看*用户组权限* (p. 382)。

配置用户组涉及四个基本步骤：

- 命名用户组，并输入用户组说明。
- 选择用户组要拥有的权限。
- 选择用户组在访问节点时使用的接口类型。
- 选择策略指定用户组可以访问哪些节点。

添加用户组：

1. 选择 Users(用户)> User Group Manager(用户组管理器)> Add User Group（添加用户组），打开 Add User Group（添加用户组）界面。
2. 在 User Group Name（用户组名称）字段里输入用户组的名称。用户组名称必须是唯一的。参看*命名常规* (p. 431)详细了解 CC-SG 的名称长度规则。
3. 在 Description（说明）字段里输入用户组简短说明。**可选。**
4. 如要设置在此用户组的用户访问启用了此功能的设备时，每个用户允许的最大 KVM 会话数，选择 Limit Number of KVM Sessions per Device（每台设备的最大 KVM 会话数）复选框，在 Max KVM Sessions (1-8)（最大 KVM 会话数[1-8]）字段里选择允许的会话数。**可选。** 参看*限制每个用户允许的 KVM 会话数* (参看 "*限制每个用户的 KVM 会话数*" p. 172)了解详情。
5. 单击 Privileges（权限）选项卡。
6. 选择要给用户组指定的每个权限对应的复选框。
7. 权限表下面的 Node Access(节点访问)区有三种节点访问权限：Node Out-of-Band Access（节点带外访问）、Node In-Band Access（节点带内访问）和 Node Power Control（节点电源控制）。选择要给用户组指定的每种节点访问权对应的复选框。
8. 单击 Device/Node Policies（设备/节点策略）选项卡，显示策略表。

   All Policies（所有策略）表列出 CC-SG 上的所有可用策略。每个策略表示一个规则，允许或拒绝访问一组节点。参看*访问控制策略* (p. 186)详细了解策略，以及如何创建策略。

9. 在 All Policies（所有策略）列表上选择要给用户组指定的策略，然后单击 Add（添加）按钮把它移动到 Selected Policies（选择的策略）列表上。Selected Policies（选择的策略）列表上的策略允许或拒绝访问受此策略控制的节点或设备。参看*给用户组指定策略* (p. 190)详细了解策略如何交互操作。

   重复此步骤，给用户组添加其他策略。

   - 如果允许此用户组访问所有可用节点，在 Add Policies（添加策略）列表上选择 Full Access Policy（全访问策略），然后单击 Add（添加）按钮。
   - 如果要把一个策略从用户组上删除掉，在 Selected Policies（选择的策略）列表上选择策略名称，然后单击 Remove（删除）按钮。

10. 在给此用户组配置策略之后，单击 Apply（应用）按钮保存此用户组，然后创建另一个用户组。重复本节中的步骤添加其他用户组。**可选。**
11. 单击 OK（确定）按钮保存更改。

编辑用户组

编辑用户组，更改用户组的现有权限和策略。

注意：不能编辑 CC 超级用户组的权限或策略。

编辑用户组：

1. 单击 Users（用户）选项卡。
2. 单击 Users（用户）选项卡上的用户组打开 User Group Profile（用户组配置文件）。
3. 在 User Group Name（用户组名称）字段里输入用户组的新名称。**可选。**
4. 在 Description（说明）字段里输入用户组的新说明。**可选。**
5. 如要设置在此用户组的用户访问启用了此功能的设备时，每个用户允许的最大 KVM 会话数，选择 Limit Number of KVM Sessions per Device（每台设备的最大 KVM 会话数）复选框，在 Max KVM Sessions (1-8)（最大 KVM 会话数[1-8]）字段里选择允许的会话数。**可选。** 参看*限制每个用户允许的 KVM 会话数* (参看 "*限制每个用户的 KVM 会话数*" p. 172)了解详情。
6. 单击 Privileges（权限）选项卡。
7. 选择要给用户组指定的每个权限对应的复选框。取消权限，把它从用户组上删除掉。
8. 单击 Node Access（节点访问）区的下拉菜单，查看此组在访问时使用的每种接口类型，选择 Control（控制）。

9. 单击下拉菜单，查看此组在访问时不使用的每种接口类型，选择 Deny（拒绝）。
10. 单击 Policies（策略）选项卡。显示两个策略表。
11. 对于要给组添加的每个策略，在 All Policies（所有策略）上选择策略，然后单击 Add（添加）按钮把它移动到 Selected Policies（选择的策略）列表上。Selected Policies（选择的策略）列表上的策略允许或拒绝用户访问受此策略控制的节点（或设备）。
12. 对于要从用户组上删除的每个策略，在 Selected Policies（选择的策略）列表上选择策略名称，然后单击 Remove（删除）按钮。
13. 单击 OK（确定）按钮保存更改。

删除用户组

如果用户组没有任何成员，可以删除它。

删除用户组：

1. 单击 Users（用户）选项卡。
2. 单击要删除的用户组。
3. 选择 Users（用户）> User Group Manager（用户组管理器）> Delete User Group（删除用户组）。
4. 单击 OK（确定）按钮删除用户组。

限制每个用户的 KVM 会话数

可以限制在与 Dominion KXII、KSXII 和 KX (KX1) 设备建立会话时，每个用户允许的 KVM 会话数。这样，可以防止任何用户一次使用全部可用通道。

当一个用户尝试与一个节点建立的连接数量超过此极限时，显示一条警告消息，包括有关当前会话的信息。把事件记录在访问报告里，显示*拒绝连接*消息。用户必须断开一个设备会话，才能开始另一个新会话。

完整消息是：

Connection Denied: Exceeds the allotted number of sessions for the KVM switch this node is attached to.If possible, please disconnect an existing session to the same KVM switch.（拒绝连接。超过此节点相连的 KVM 切换器的指定会话数。如有可能，请断开与此 KVM 切换器的一个现有会话。）

消息还列出至 KVM 切换器的所有活动连接。

*注意：可以按消息文本过滤访问报告，确定哪些设备的流量大。参看***访问报告** *(p. 225)*。

KVM 会话数极限按用户组设置。在指导设置或 CSV 导入过程中人工添加或编辑用户组时，可以启用会话数限制。参看***添加用户组*** (p. 169)。

只有在达到 Dominion KXII 设备的最大连接数时，Dominion KXII 才发出警告。把事件记录在访问报告里，显示*拒绝连接*消息。

完整消息是：

Connection Denied: Exceeds the number of available video channels on the KVM switch this node is attached to.（拒绝连接：超过此节点相连的 KVM 切换器的可用视频通道数。）

配置用户组访问审计

可以要求用户组成员在访问节点之前输入访问原因，否则不允许他们访问节点。给你选择的用户组里的所有用户显示一个对话框。在建立节点连接之前，用户必须输入访问原因。此功能应用于使用所有类型的接口（包括电源控制接口）进行的所有类型的访问。

访问原因记录在 Node Profile's Auditing（节点配置文件审计）选项卡上的 Audit Trail（审计跟踪）里。

配置用户组访问审计：

1. 选择 Users（用户）> Node Auditing（节点审计）。

2. 选择 Require Users to Enter Access Information When Connecting to a Node（要求用户在连接节点时输入访问信息）复选框。
3. 在 Message to Users（给用户显示的消息）字段里输入在用户尝试访问节点时可以看到的消息。提供默认消息。最多 256 个字符。
4. 单击箭头按钮把要启用组访问审计的用户组移动到 Selected（选择）列表上。按住 Ctrl 单击项选择多项。

*提示：在 Find（查找）字段里输入用户组名称，在列表上突出显示此用户组。在不完整名称后面输入 *，在列表上突出显示所有类似名称。*

单击列标题按字母顺序排序列表。

5. 单击 Update（更新）按钮。

添加、编辑和删除用户

添加用户

在把用户添加到 CC-SG 时，必须指定一个用户组，把给此用户组指定的权限指定给此用户。

▶ **添加用户：**

1. 在 Users（用户）选项卡上选择要把用户添加到哪个组。
2. 选择 Users（用户）> User Manager（用户管理器）> Add User（添加用户）。
3. 在 Username（用户名）字段里输入要添加的用户的名称，在登录 CC-SG 时要使用此名称。参看***命名常规*** (p. 431)详细了解 CC-SG 的名称长度规则。
4. 在 Full Name（全名）字段里输入用户的名字和姓氏。参看***命名常规*** (p. 431)详细了解 CC-SG 的名称长度规则。
5. 如果希望此用户能登录 CC-SG，选择 Login Enabled（启用登录）复选框。
6. 只有在希望用户通过外部服务器（例如 TACACS+、RADIUS、LDAP 或 AD）进行验证时，才选择 Check Remote Authentication（检查远程验证）复选框。如果使用远程验证，不需要密码，New Password（新密码）和 Retype New Password（再次输入新密码）字段被禁用。
7. 在 New Password（新密码）和 Retype New Password（再次输入新密码）字段里输入用户登录 CC-SG 时所用的密码。

*注意：参看**命名常规** (p. 431)详细了解 CC-SG 的名称长度规则。*

*如果启用了强密码，输入的密码必须符合现有规则的要求。屏幕顶部的信息栏显示消息，有助于用户了解密码要求。参看***高级管理** *(p. 251)了解强密码详情。*

8. 选择 Force Password Change on Next Login（强制在下次登录时更改密码）复选框，强制用户在下次登录时更改指定的密码。
9. 选择 Force Password Change Periodically（强制定期更改密码）复选框，指定强制用户多久更改一次密码。
10. 如果选择此选项，在 Expiration Period (Days)（到期时间[天]）字段里输入在强制用户更改密码之前可使用的天数。
11. 在 Email address（电子邮件地址）字段里输入用户的电子邮件地址。此地址用于发送用户通知。
12. 在 Telephone Number（电话号码）字段里输入用户的电话号码。
13. 单击 User Groups（用户组）下拉菜单，然后选择要把用户添加到哪个组。
    - 可能选择 Require User to Enter Information When Connecting to a Node（要求用户在连接节点时输入信息）复选框，也可能不显示，取决于你选择的用户组。如果选择此选项，要求此用户在访问节点时输入信息。参看***配置用户组访问审计*** (p. 172)。
14. 在配置此用户之后，单击 Apply（应用）按钮保存此用户，然后再创建另一个用户；也可以单击 OK（确定）按钮保存此用户，不再创建其他用户。Users（用户）选项卡显示你创建的用户，此用户位于所属的用户组下面。

编辑用户

在编辑用户时，不能更改用户所属的组。参看***给用户指定组*** (p. 175)。

编辑用户：

1. 在 Users（用户）选项卡上，单击 + 号展开你要编辑的用户所在的用户组，然后选择用户打开 User Profile（用户配置文件）。
2. 取消 Login enabled（启用登录）复选框，禁止此用户登录 CC-SG。选择 Login enabled（启用登录）复选框，允许此用户登录 CC-SG。
3. 只有在希望用户通过外部服务器(例如 TACACS+、RADIUS、LDAP 或 AD）进行验证时，才选择 Remote Authentication（远程验证）复选框。如果使用远程验证，不需要密码，New Password（新密码）和 Retype New Password（再次输入新密码）字段被禁用。
4. 在 New Password（新密码）和 Retype New Password（再次输入新密码）字段里输入新密码，更改此用户的密码。

*注意：如果启用了强密码，输入的密码必须符合现有规则的要求。屏幕顶部的信息栏显示消息，有助于用户了解密码要求。参看***高级管理** *(p. 251)了解强密码详情。*

5. 如果要强制用户在下次登录时更改指定的密码，选择 Force Password Change on Next Login（强制在下次登录时更改密码）复选框。
6. 在 Email address（电子邮件地址）字段里输入要添加的新电子邮件地址，或者更改用户配置的电子邮件地址。此地址用于发送用户通知。
7. 单击 OK（确定）按钮保存更改。

删除用户

在删除用户时，把他从 CC-SG 上彻底删除掉。在删除不再需要的用户帐号时，这很有用。

即使一个用户属于多个用户组，这个过程也删除此用户的所有实例。参看***删除用户组里的用户*** (参看 "***删除用户组用户***" p. 176)了解在删除用户组里的用户时，如何不把他从 CC-SG 上删除掉。

▶ **删除用户：**

1. 在 Users（用户）选项卡上，单击 + 号展开你要删除的用户所在的用户组，然后选择用户打开 User Profile（用户配置文件）。
2. 选择 Users（用户）> User Manager（用户管理器）> Delete User（删除用户）。
3. 单击 OK（确定）按钮把用户从 CC-SG 上删除掉。

给用户指定组

用此命令给现有用户指定另一个用户组。采用这种方法指定的用户被添加新用户组里，但仍然属于此前给他们指定的用户组。如要移动用户，可以一起使用此命令和 Delete User From Group（删除组用户）命令。

▶ **给用户指定用户组：**

1. 在 Users（用户）选项卡上选择要给用户指定哪个用户组。
2. 选择 Users（用户）> User Group Manager（用户组管理器）> Assign User Group（给用户指定组）。
3. User group name（用户组名称）字段显示所选的用户组。
4. Users not in group（非用户组用户）列表显示尚未指定目标用户组的用户。
   - 在此列表上选择要添加的用户，然后单击>按钮把他移动到 Users in group（用户组用户）列表上。

- 单击>>按钮把所有非用户组用户移动到 Users in group（用户组用户）列表上。
- 在 Users in group（用户组用户）列表上选择要删除的用户，然后单击<按钮删除他们。
- 单击<<按钮删除 Users in group（用户组用户）列表上的所有用户。

5. 在把所有用户移动到合适的列上之后，单击 OK（确定）按钮。Users in group（用户组用户）列表上的用户被添加到所选的用户组。

删除用户组用户

在删除一个用户组用户时，只把此用户从指定的用户组里删除掉。此用户仍然在其他指定用户组里。在删除一个用户组用户时，并不把此用户从 CC-SG 上删除掉。

如果一个用户只属于一个用户组，不能把他从用户组里删除掉。只能把此用户从 CC-SG 上删除掉。

删除用户组用户：

1. 在 Users（用户）选项卡上，单击 + 号展开你要删除的用户组用户所在的用户组，然后选择用户打开 User Profile（用户配置文件）。
2. 选择 Users（用户）> User Manager（用户管理器）> Delete User From Group（删除组用户），打开 Delete User（删除用户）屏幕。
3. 单击 OK（确定）按钮把用户从用户组里删除掉。

用 CSV 文件导入法添加用户

可以导入包含用户信息的 CSV 文件，把这些用户信息添加到 CC-SG。

如果邻居里有多台 CC-SG 设备，很容易导出一台 CC-SG 上的用户，再把它导入另一台 CC-SG，确保在本地验证的所有用户均在两个成员上。

必须具备用户管理权限与 CC 设置和控制权限，才能导入和导出用户信息。

用户 CSV 文件要求

导出功能允许你添加用户组、用户和 AD 模块，指定策略、权限和用户组。

- 必须已经在 CC-SG 上创建了策略。导入时，给用户组指定策略。不能通过导入法创建新策略。
- 用户组名称区分大小写。
- 用户名不区分大小写。
- 必须在 CSV 文件里给每个定义的 USERGROUP 定义 USERGROUP-PERMISSIONS 和 USERGROUP-POLICY 标签，才能创建用户组。
- 导出 CC-SG 上的文件查看备注，包括创建有效 CSV 文件所需的所有标签和参数。 参看*导出用户* (p. 182)。
- 满足所有 CSV 文件的其他要求。参看*常见 CSV 文件要求* (参看 "*通用 CSV 文件要求*" p. 394)。

▶ 在 CSV 文件里添加用户组：

列编号	标签或值	详细信息
1	ADD	所有标签的第一列是命令。
2	USERGROUP	输入所示的标签。 标签不区分大小写。
3	User Group Name（用户组名称）	必填字段。 用户组名称区分大小写。
4	Description（说明）	必填字段。
5	Limit Max Number of KVM Sessions per Device（限制每台设备的最大 KVM 会话数）	TRUE 或 FALSE 默认值是 FALSE。
6	Maximum number of KVM sessions allowed per user（每个用户允许的最大 KVM 会话数）	输入 1-8 之间的数。 默认值为 2。

在 CSV 文件里给用户组指定权限：

输入值 TRUE，给用户组指定权限。输入值 FALSE，拒绝给用户组指定权限。

列编号	标签或值	详细信息
1	ADD	所有标签的第一列是命令。
2	USERGROUP-PERMISSIONS	输入所示的标签。 标签不区分大小写。
3	User Group Name（用户组名称）	必填字段。 用户组名称区分大小写。
4	CC Setup and Control（CC 设置和控制）	TRUE 或 FALSE
5	Device Configuration Upgrade Management（设备配置和升级管理）	TRUE 或 FALSE
6	Device Port Node Management（设备、端口和节点管理）	TRUE 或 FALSE
7	User Management（用户管理）	TRUE 或 FALSE
8	User Security Management（用户安全管理）	TRUE 或 FALSE
9	Node IBA（节点 IBA）	TRUE 或 FALSE 默认值是 TRUE
10	Node OOB（节点 OOB）	TRUE 或 FALSE 默认值是 TRUE
11	Node Power（节点电源）	TRUE 或 FALSE

在 CSV 文件里给用户组指定策略：

列编号	标签或值	详细信息
1	ADD	所有标签的第一列是命令。
2	USERGROUP-POLICY	输入所示的标签。 标签不区分大小写。

列编号	标签或值	详细信息
3	User Group Name（用户组名称）	必填字段。 用户组名称区分大小写。
4	Policy Name（策略名称）	必填字段。

在 CSV 文件里使 AD 模块与用户组关联：

列编号	标签或值	详细信息
1	ADD	所有标签的第一列是命令。
2	USERGROUP-ADMODULE	输入所示的标签。 标签不区分大小写。
3	User Group Name（用户组名称）	必填字段。 用户组名称区分大小写。
4	AD Module Name（AD 模块名称）	必填字段。

把用户添加到 CC-SG：

列编号	标签或值	详细信息
1	ADD	所有标签的第一列是命令。
2	USER	输入所示的标签。 标签不区分大小写。
3	User Group Name（用户组名称）	必填字段。 用户组名称区分大小写。 必须把用户添加到一个用户组。可以使用 USERGROUP-MEMBER 标签，把用户添加到多个用户组。
4	User Name（用户名）	必填字段。
5	Password（密码）	必填字段。
6	User's Full Name（用户全名）	可选。
7	Email Address（电子邮件地址）	可选。 电子邮件地址用于发送系统通知。
8	Telephone Number（电话号码）	可选。

列编号	标签或值	详细信息
9	Login Enabled（启用登录）	TRUE 或 FALSE 默认值是 TRUE Login enabled（启用登录）允许用户登录 CC-SG。
10	Remote Authentication（远程验证）	TRUE 或 FALSE
11	Force Password Change Periodically（强制定期更改密码）	TRUE 或 FALSE
12	Expiration Period（到期时间）	如果 Force Password Change Periodically（强制定期更改密码）设置为 TRUE，指定密码使用天数。输入 1-365 之间的数。

- 把用户添加到用户组：

列编号	标签或值	详细信息
1	ADD	所有标签的第一列是命令。
2	USERGROUP-MEMBER	输入所示的标签。 标签不区分大小写。
3	User Group Name（用户组名称）	必填字段。 用户组名称区分大小写。
4	User Name（用户名）	必填字段。

用户 CSV 文件示例

ADD, USERGROUP, Windows Administrators, MS IT Team

ADD, USERGROUP-PERMISSIONS, Windows Administrators, FALSE, TRUE, TRUE, TRUE, TRUE, TRUE, TRUE, TRUE

ADD, USERGROUP-POLICY, Windows Administrators, Full Access Policy

ADD, USERGROUP-ADMODULE, Windows Administrators, AD-USA-57-120

ADD, USERGROUP-MEMBER, Windows Administrators, user1

ADD, USERGROUP-MEMBER, Windows Administrators, user2

ADD, USER, Windows Administrators, user1, password, userfirstname userlastname, user1@company.com, 800-555-1212, TRUE,,,

ADD, USER, Windows Administrators, user2, password, userfirstname userlastname, user2@raritan.com, 800-555-1212, TRUE,,,

ADD, USERGROUP-MEMBER, System Administrators, user1

ADD, USERGROUP-MEMBER, CC Users, user2

导入用户

在创建 CSV 文件之后，验证此文件是否有错误，然后导入文件。

跳过重复记录，不添加重复记录。

1. 选择 Administration（管理）> Import（导入）> Import Users（导入用户）。
2. 单击 Browse（浏览）按钮选择要导入的 CSV 文件，然后单击 Open（打开）按钮。
3. 单击 Validate（验证）按钮。Analysis Report（分析报告）区显示文件内容。
   - 如果文件无效，显示错误消息。单击 OK（确定）按钮查看页面 Problems（问题）区显示的文件问题说明。单击 Save to File（保存到文件）按钮保存问题列表。编辑 CSV 文件纠正错误，然后再验证一次。参看*排除 CSV 文件问题* (p. 396)。
4. 单击 Import（导入）按钮。
5. 单击 Actions（操作）区查看导入结果。用绿色文字显示成功导入的项目，用红色文字显示导入失败的项目。由于已经有同名项目，或者已经导入了，也用红色文字显示导入失败的项目。
6. 如要查看导入结果详细信息，查看 Audit Trail（审计跟踪）报告。参看*导入审计跟踪项* (p. 395)。

导出用户

具有在 CC-SG 上创建的用户帐号的所有用户，都包括在导出文件里。但不包括 AD 验证的用户，除非他们有在 CC-SG 上创建的用户帐号。

导出文件包括用户配置文件上的用户和详细信息、用户组、用户组权限和策略、关联的 AD 模块。

密码作为空白字段导出。

导出用户：

1. 选择 Administration（管理）> Export（导出）> Export Users（导出用户）。
2. 单击 Export to File（导出成文件）按钮。
3. 输入文件名，然后选择文件保存位置。
4. 单击 Save（保存）按钮。

你的用户配置文件

My Profile（我的配置文件）允许所有用户查看帐号详细信息，更改部分详细信息，定制使用设置。这是唯一的 CC 超级用户帐号名称更改方法。

查看你的配置文件：

选择 Secure Gateway（安全网关）> My Profile（我的配置文件），打开 Change My Profile（更改我的配置文件）屏幕，显示帐号详细信息。

更改密码

1. 选择 Secure Gateway（安全网关）> My Profile（我的配置文件），
2. 选择 Change Password (For Local Authentication Only)（更改密码[仅限于本地验证]）复选框。
3. 在 Old Password（旧密码）字段里输入当前密码。
4. 在 New Password（新密码）字段里输入新密码。如果要求强密码，显示一条消息。
5. 在 Retype New Password（再次输入新密码）字段里再次输入新密码。
6. 单击 OK（确定）按钮保存更改。

更改你的名称

可以更改自己的用户名。可以更改与用户名关联的名字和姓氏。

▶ 更改你的名称：

1. 选择 Secure Gateway（安全网关）> My Profile（我的配置文件），
2. 在 Full Name（全名）字段里输入自己的名字和姓氏。参看*命名常规* (p. 431)详细了解 CC-SG 的名称长度规则。

更改默认搜索首选项

1. 选择 Secure Gateway（安全网关）> My Profile（我的配置文件），
2. 在 Search Preference（搜索首选项）区选择搜索节点、用户和设备所用的首选方法。
   - Filter by Search Results（按搜索结果过滤）— 允许使用通配符，把显示的节点、用户或设备限制在符合搜索条件的所有名称。
   - Find Matching String（查找匹配字符串）— 不支持通配符，在输入时突出显示最匹配的节点、用户或设备。在单击 Search（搜索）按钮之后，列表只显示那些包含搜索条件的项。
3. 单击 OK（确定）按钮保存更改。

更改 CC-SG 默认字体大小

1. 选择 Secure Gateway（安全网关）> My Profile（我的配置文件），
2. 单击 Font Size（字体大小）下拉菜单调节标准 CC-SG 客户机使用的字体大小。
3. 单击 OK（确定）按钮保存更改。

更改电子邮件地址

1. 选择 Secure Gateway（安全网关）> My Profile（我的配置文件），
2. 在 Email address（电子邮件地址）字段里输入要添加的新地址，或者更改 CC-SG 发送通知所用的地址。
3. 单击 OK（确定）按钮保存更改。

更改 CC-SG 超级用户的用户名

必须用 CC 超级用户帐号登录 CC-SG，才能更改 CC 超级用户的用户名。默认 CC 超级用户的用户名是 *admin*。

1. 选择 Secure Gateway（安全网关）> My Profile（我的配置文件），

2. 在 Username（用户名）字段里输入新名称。
3. 单击 OK（确定）按钮保存更改。

退出用户

可以按个人或按用户组，让当前登录用户退出 CC-SG。

退出用户：

1. 在 Users（用户）选项卡上，单击 + 号展开你要在 CC-SG 上退出哪个用户组里的用户，然后选择用户。
   - 如要选择多个用户，按住 Shift 单击其他用户。
2. 选择 Users（用户）> User Manager（用户管理器）> Logout User（退出用户），打开 Logout User（退出用户）屏幕，列出所选的用户。
3. 单击 OK（确定）按钮让这些用户退出 CC-SG。

退出用户组里的所有用户：

1. 在 Users（用户）选项卡上选择要退出 CC-SG 的用户组。
   - 如要退出多个用户组，按住 Shift 单击其他用户组。
2. 选择 Users（用户）> User Group Manager（用户组管理器）> Logout User（退出用户），打开 Logout User（退出用户）屏幕，列出所选用户组里的活动用户。
3. 单击 OK（确定）按钮让这些用户退出 CC-SG。

批量复制用户

可以对用户使用批量复制命令，把一个用户的用户组从属关系复制到另一个用户或一组用户。如果接受这些从属关系的用户现在有组从属关系，将删除现有的从属关系。

对用户执行批量复制：

1. 在 Users（用户）选项卡上，单击 + 号展开你要复制哪个用户组的用户策略和权限，然后选择用户。
2. 选择 Users（用户）> User Manager（用户管理器）> Bulk Copy（批量复制）。Username（用户名）字段显示要复制哪个用户的策略和权限。
3. 在 All Users（所有用户）列表上选择哪些用户将接受 Username（用户名）字段显示的用户策略和权限。
   - 单击>按钮把用户名移动到 Selected Users（选择的用户）列表上。

- 单击>>按钮把所有用户移动到 Selected Users（选择的用户）列表上。
- 在 Selected Users（选择的用户）列表上选择用户，然后单击<按钮删除此用户。
- 单击<<按钮删除 Users in group（用户组用户）列表上的所有用户。

4. 单击 OK（确定）按钮复制。

Ch 10 访问控制策略

策略是一些规则，定义用户可以访问哪些节点和设备，何时可以访问它们，是否启用虚拟媒体权限（如适用）。最简单的策略创建方法，是把节点和设备分成节点组和设备组，然后创建策略允许或拒绝访问每个组里的节点和设备。在创建策略之后，把它指定给用户组。参看*给用户组指定策略* (p. 190)。

CC-SG 有全访问策略。如果要让所有用户随时可以访问所有节点和设备，给所有用户组指定全访问策略。

如果你完成了指导设置，已经创建了许多基本策略。参看*用指导设置配置 CC-SG* (p. 29)。

用策略控制访问：

- 创建节点组，组织管理你要针对哪些节点创建访问规则。参看*添加节点组* (p. 162)。
- 创建设备组，组织管理你要针对哪些设备创建访问规则。参看*添加设备组* (p. 69)。
- 针对节点组或设备组创建策略，指定何时可以访问节点组或设备组。参看*添加策略* (p. 186)。
- 把策略应用于用户组。参看*给用户组指定策略* (p. 190)。

在本章内

添加策略

如果创建一个策略拒绝访问 (Deny) 一个节点组或设备组，还必须创建一个策略允许访问 (Control) 所选的节点组或设备组。当 Deny 策略不起作用时，用户不会自动获得 Control 权限。

添加策略：

1. 选择 Associations（关联）> Policies（策略），打开 Policy Manager（策略管理器）窗口。

2. 单击 Add（添加）按钮打开一个对话框，要求你输入策略名称。
3. 在 Enter policy name（输入策略名称）字段里输入新策略的名称。参看*命名常规* (p. 431)详细了解 CC-SG 的名称长度规则。
4. 单击 OK（确定）按钮把新策略添加到 Policy Manager（策略管理器）屏幕上的 Policy Name（策略名称）列表上。
5. 单击 Device Group（设备组）下拉箭头，然后选择此策略要控制哪个设备组的访问权。
6. 单击 Node Group（节点组）下拉箭头，然后选择此策略要控制哪个节点组的访问权。
7. 如果策略只涉及一类组，只选择此类型的值。
8. 单击 Days（日期）下拉箭头，然后选择在星期几执行此策略：All days（整个星期）、Weekday（工作日，星期一到星期五）和 Weekend（周末，星期六和星期天），或者选择 Custom（定制，选择特定日期）。
9. 选择 Custom（定制）选项，然后选择自己设置的日期。激活各个日期复选框。
10. 选择此策略的每个执行日期对应的复选框。
11. 在 Start Time（开始时间）字段里输入此策略开始生效的时间。时间必须是 24 小时格式。
12. 在 End Time（结束时间）字段里输入此策略结束当天的时间。时间必须是 24 小时格式。
13. 在 Device/Node Access Permission（设备/节点访问权限）字段里选择 Control（控制），定义此策略在指定时间和日期允许访问所选节点组或设备组。选择 Deny（拒绝），定义此策略在指定时间和日期拒绝访问所选节点组或设备组。
14. 如果在 Device/Node Access Permission（设备/节点访问权限）字段里选择了 Control（控制），激活 Virtual Media Permission（虚拟媒体权限）部分。在 Virtual Media Permission（虚拟媒体权限）字段里选择一个选项，在指定时间和日期允许或禁止访问所选节点组或设备组里的可用虚拟媒体：
    - Read-Write（读写）选项启用虚拟媒体读写权限
    - Read-only（只读）选项启用虚拟媒体只读权限
    - Deny（拒绝）选项拒绝所有虚拟媒体访问
15. 单击 Update（更新）按钮把新策略添加到 CC-SG，在显示的确认消息窗口上单击 Yes（是）按钮。

编辑策略

在编辑策略时，所做的更改不影响当前登录 CC-SG 的用户。更改将在下次登录时生效。

为了确保所作的更改尽快生效，先进行维护模式，然后编辑策略。在进入维护模式之后，所有当前用户退出 CC-SG，直到你退出维护模式之后，用户才能再次登录。参看***维护模式*** (p. 235)。

编辑策略：

1. 在 Associations（关联）菜单上单击 Policies（策略）打开 Policy Manager（策略管理器）窗口。
2. 单击 Policy Name（策略名称）下拉箭头，然后在列表上选择要编辑的策略。
3. 如要编辑策略名称，单击 Edit（编辑）按钮打开 Edit Policy（编辑策略）窗口。在 Name（名称）字段里输入策略的新名称，然后单击 OK（确认）按钮更改策略名称。**可选。**
4. 单击 Device Group（设备组）下拉箭头，然后选择此策略要控制哪个设备组的访问权。
5. 单击 Node Group（节点组）下拉箭头，然后选择此策略要控制哪个节点组的访问权。
6. 如果策略只涉及一类组，只选择此类型的值。
7. 单击 Days（日期）下拉箭头，然后选择在星期几执行此策略：All（整个星期）、Weekday（工作日，星期一到星期五）和 Weekend（周末，星期六和星期天），或者选择 Custom（定制，选择特定日期）。
8. 选择 Custom（定制）选项，然后选择自己设置的日期。激活各个日期复选框。
9. 选择此策略的每个执行日期对应的复选框。
10. 在 Start Time（开始时间）字段里输入此策略开始生效的时间。时间必须是 24 小时格式。
11. 在 End Time（结束时间）字段里输入此策略结束当天的时间。时间必须是 24 小时格式。
    - 在 Device/Node Access Permission（设备/节点访问权限）字段里：
    - 选择 Control（控制），定义此策略在指定时间和日期允许访问所选节点组或设备组。
    - 选择 Deny（拒绝），定义此策略在指定时间和日期拒绝访问所选节点组或设备组。

12. 如果在 Device/Node Access Permission（设备/节点访问权限）字段里选择了 Control（控制），激活 Virtual Media Permission（虚拟媒体权限）部分。在 Virtual Media Permission（虚拟媒体权限）字段里选择一个选项，在指定时间和日期允许或禁止访问所选节点组或设备组里的可用虚拟媒体：
    - Read-Write（读写）选项启用虚拟媒体读写权限
    - Read-only（只读）选项启用虚拟媒体只读权限
    - Deny（拒绝）选项拒绝所有虚拟媒体访问
13. 单击 Update（更新）按钮保存更改。
14. 在显示的确认消息窗口上，单击 Yes（是）按钮。

删除策略

可以删除不再需要的策略。

删除策略：

1. 选择 Associations（关联）> Policies（策略），打开 Policy Manager（策略管理器）窗口。
2. 单击 Policy Name（策略名称）下拉箭头，然后选择要删除的策略。
3. 单击 Delete（删除）按钮。
4. 在显示的确认消息窗口上，单击 Yes（是）按钮。

虚拟媒体支持

CC-SG 给与支持虚拟媒体的 KX2、KSX2 和 KX2-101 设备相连的那些节点提供远程虚拟媒体支持。如要详细了解如何在自己的设备上访问虚拟媒体，参看：

- **Dominion KX II 用户指南**
- **Dominion KSX II 用户指南**
- **Dominion KXII-101 用户指南**

参看*添加策略* (p. 186)详细了解如何在 CC-SG 上创建策略，给用户组指定虚拟媒体权限。

给用户组指定策略

必须给用户组指定策略，策略才会生效。在给用户组指定策略之后，用户组成员的访问权就受此策略的控制。参看*用户和用户组* (p. 166)详细了解如何给用户组指定策略。

如果一个用户属于多个用户组，此用户的权限比给这些用户组指定的权限大。

例如：

策略 123：允许访问服务器 1 2 3。

策略 456：允许访问服务器 4 5 6。

用户组 A：给用户组 A 指定策略 123。

用户组 B：给用户组 B 指定策略 456。

用户同时属于用户组 A 和用户组 B，允许此用户访问服务器 1 2 3 4 5 6。

然后创建策略拒绝 1：拒绝访问服务器 1。

给用户组 A 指定策略拒绝 1，用户只能访问服务器 2 3 4 5 6。

如果给用户组 B 指定策略拒绝 1，而不是给用户组 A 指定此策略，用户可以访问服务器 1 2 3 4 5 6。

Ch 11 设备和节点定制视图

定制视图允许你使用类别、节点组和设备组来指定在左面板以不同方式显示节点和设备。

在本章内

定制视图的类型

有三种类型的定制视图：“按类别查看”、“按节点组过滤”和“按设备组过滤”。

按类别查看

在应用按类别查看定制视图之后，节点列表或设备列表显示用你指定的类别描述的所有节点和所有设备。没有指定类别的节点或设备将显示为 unassociated（未关联）。

按节点组过滤

在应用按节点组过滤定制视图之后，节点列表只显示你指定的节点组。组织结构的第一层是节点组名称。如果一个节点属于在定制视图上定义的多个节点组，它可能在列表上出现多次。如果节点不属于在定制视图上指定的一个节点组，列表不显示这些节点。

按设备组过滤

在应用按设备组过滤定制视图之后，设备列表只显示你指定的设备组。组织结构的第一层是设备组名称。如果一台设备属于在定制视图上定义的多个设备组，它可能在列表上出现多次。如果设备不属于在定制视图上指定的一个设备组，列表不显示这些设备。

在 Admin Client 上使用定制视图

节点定制视图

添加节点定制视图

添加节点定制视图：

1. 单击 Nodes（节点）选项卡。
2. 选择 Nodes(节点)> Change View(更改视图)> Create Custom View（创建定制视图），打开 Custom View（定制视图）屏幕。
3. In the Custom View panel, click Add. The Add Custom View window opens.
4. 在 Custom View Name（定制视图名称）字段里输入新定制视图的名称。
5. 在 Custom View Type（定制视图类型）部分：
   - 选择 Filter by Node Group（按节点组过滤）创建定制视图，只显示你指定的节点组。
   - 选择 View by Category（按类别查看）创建定制视图，按你指定的类别显示节点。
6. 单击 OK（确定）按钮。
7. 在 Custom View Details（定制视图详细信息）部分：
   a. 在 Available（可用）列表上选择定制视图要包括的项，然后单击 Add（添加）按钮把它移动到列表上。重复此步骤添加其他所需的项。
   b. 根据你希望每个组在 Nodes（节点）选项卡上的显示顺序，排列 Selected（选择）列表上的项。选择一项，然后单击上下箭头按钮把它移动到希望的位置。
   c. 如果必须删除列表上的一项，选择此项，然后单击 Remove(删除）按钮。
8. 单击 Save（保存）按钮。在添加定制视图之后，显示一条确认消息。
9. 如要应用新定制视图，单击 Set Current（设置当前值）按钮。

应用节点定制视图

把定制视图应用于节点列表：

1. 选择 Nodes（节点）> Change View（更改视图）> Custom View（定制视图），打开 Custom View（定制视图）屏幕。
2. 单击 Name（名称）下拉箭头，然后在列表上选择一个定制视图。
3. 单击 Apply View（应用视图）按钮。

或者

- 选择 Nodes（节点）> Change View（更改视图）。定义的所有定制视图均为弹出菜单上的选项。选择要应用的定制视图。

更改节点定制视图

1. 单击 Nodes（节点）选项卡。
2. 选择 Nodes(节点)> Change View(更改视图)> Create Custom View（创建定制视图），打开 Custom View（定制视图）屏幕。
3. 单击 Name（名称）下拉箭头，然后在列表上选择一个定制视图。Custom View Details（定制视图详细信息）面板显示包括项的详细信息及其顺序。

更改定制视图名称：

1. 单击 Custom View（定制视图）面板上的 Edit（编辑）按钮打开 Eidt Custom View（编辑定制视图）窗口。
2. 在 Enter new name for custom view（输入定制视图新名称）字段里输入定制视图的新名称，然后单击 OK（确定）按钮。Custom View（定制视图）屏幕上的 Name（名称）字段显示新视图名称。

更改定制视图内容：

1. 在 Custom View Details（定制视图详细信息）部分：
   a. 在 Available（可用）列表上选择定制视图要包括的项，然后单击 Add（添加）按钮把它移动到列表上。重复此步骤添加其他所需的项。
   b. 根据你希望每个组在 Nodes（节点）选项卡上的显示顺序，排列 Selected（选择）列表上的项。选择一项，然后单击上下箭头按钮把它移动到希望的位置。
   c. 如果必须删除列表上的一项，选择此项，然后单击 Remove（删除）按钮。
2. 单击 Save（保存）按钮。在添加定制视图之后，显示一条确认消息。

3. 如要应用新定制视图，单击 Set Current（设置当前值）按钮。

删除节点定制视图

▶ **删除节点定制视图：**

1. 单击 Nodes（节点）选项卡。
2. 选择 Nodes(节点)> Change View(更改视图)> Create Custom View（创建定制视图），打开 Custom View（定制视图）屏幕。
3. 单击 Name（名称）下拉箭头，然后在列表上选择一个定制视图。Custom View Details（定制视图详细信息）面板显示包括项的详细信息及其顺序。
4. 单击 Custom View（定制视图）面板上的 Delete（删除）按钮，显示 Delete Custom View（删除定制视图）确认消息。
5. 单击 Yes（是）按钮。

指定节点默认定制视图

▶ **指定节点默认定制视图：**

1. 单击 Nodes（节点）选项卡。
2. 选择 Nodes(节点)> Change View(更改视图)> Create Custom View（创建定制视图），打开 Custom View（定制视图）屏幕。
3. 单击 Name（名称）下拉箭头，然后在列表上选择一个定制视图。
4. 单击 Custom View（定制视图）面板上的 Set as Default（设置为默认值）按钮。在下次登录时，默认使用所选的定制视图。

给所有用户指定节点默认定制视图

如果你有 CC 设置和控制权限，可以给所有用户指定默认定制视图。

▶ **给所有用户指定节点默认定制视图：**

1. 单击 Nodes（节点）选项卡。
2. 选择 Nodes(节点)> Change View(更改视图)> Create Custom View（创建定制视图），
3. 单击 Name（名称）下拉箭头，然后选择要指定为系统默认视图的定制视图。
4. 选择 System View(整个视图)复选框，然后单击 Save(保存)按钮。

登录 CC-SG 的所有用户将看到根据所选择制视图排序的 Nodes（节点）选项卡。用户可以更改定制视图。

设备定制视图

添加设备定制视图

添加设备定制视图：

1. 单击 Devices（设备）选项卡。
2. 选择 Devices（设备）> Change View（更改视图）> Create Custom View（创建定制视图），打开 Custom View（定制视图）屏幕。
3. In the Custom View panel, click Add. The Add Custom View window appears.
4. 在 Custom View Name（定制视图名称）字段里输入新定制视图的名称。
5. 在 Custom View Type（定制视图类型）部分：
   - 选择 Filter by Device Group（按设备组过滤）创建一个定制视图，只显示你指定的设备组。
   - 选择 View by Category（按类别查看）创建一个定制视图，按你指定的类别显示设备。
6. 单击 OK（确定）按钮。
7. 在 Custom View Details（定制视图详细信息）部分：
   a. 在 Available（可用）列表上选择定制视图要包括的项，然后单击 Add（添加）按钮把它移动到列表上。重复此步骤添加其他所需的项。
   b. 根据你希望每个组在 Nodes（节点）选项卡上的显示顺序，排列 Selected（选择）列表上的项。选择一项，然后单击上下箭头按钮把它移动到希望的位置。
   c. 如果必须删除列表上的一项，选择此项，然后单击 Remove（删除）按钮。
8. 单击 Save（保存）按钮。在添加定制视图之后，显示一条确认消息。
9. 如要应用新定制视图，单击 Set Current（设置当前值）按钮。

应用设备定制视图

把定制视图应用于设备列表：

1. 选择 Devices（节点）> Change View（更改视图）> Custom View（定制视图），打开 Custom View（定制视图）屏幕。
2. 单击 Name（名称）下拉箭头，然后在列表上选择一个定制视图。
3. 单击 Set Current（设置当前值）按钮应用定制视图。

或者

选择 Devices（设备）> Change View（更改视图）。定义的所有定制视图均为弹出菜单上的选项。选择要应用的定制视图。

更改设备定制视图

1. 单击 Devices（设备）选项卡。
2. 选择 Devices（设备）> Change View（更改视图）> Create Custom View（创建定制视图），打开 Custom View（定制视图）屏幕。
3. 单击 Name（名称）下拉箭头，然后在列表上选择一个定制视图。Custom View Details（定制视图详细信息）面板显示包括项的详细信息及其顺序。

更改定制视图名称：

1. 单击 Custom View（定制视图）面板上的 Edit（编辑）按钮打开 Eidt Custom View（编辑定制视图）窗口。
2. 在 Enter new name for custom view（输入定制视图新名称）字段里输入定制视图的新名称，然后单击 OK（确定）按钮。Custom View（定制视图）屏幕上的 Name（名称）字段显示新视图名称。

更改定制视图内容：

1. 在 Custom View Details（定制视图详细信息）部分：
   a. 在 Available（可用）列表上选择定制视图要包括的项，然后单击 Add（添加）按钮把它移动到列表上。重复此步骤添加其他所需的项。
   b. 根据你希望每个组在 Nodes（节点）选项卡上的显示顺序，排列 Selected（选择）列表上的项。选择一项，然后单击上下箭头按钮把它移动到希望的位置。
   c. 如果必须删除列表上的一项，选择此项，然后单击 Remove（删除）按钮。

2. 单击 Save（保存）按钮。在添加定制视图之后，显示一条确认消息。
3. 如要应用新定制视图，单击 Set Current（设置当前值）按钮。

删除设备定制视图

▶ **删除设备定制视图：**

1. 单击 Devices（设备）选项卡。
2. 选择 Devices（设备）> Change View（更改视图）> Create Custom View（创建定制视图），打开 Custom View（定制视图）屏幕。
3. 单击 Name（名称）下拉箭头，然后在列表上选择一个定制视图。Custom View Details（定制视图详细信息）面板显示包括项的详细信息及其顺序。
4. 单击 Custom View（定制视图）面板上的 Delete（删除）按钮，显示 Delete Custom View（删除定制视图）确认消息。
5. 单击 Yes（是）按钮。

指定设备默认定制视图

▶ **指定设备默认定制视图：**

1. 单击 Devices（设备）选项卡。
2. 选择 Devices（设备）> Change View（更改视图）> Create Custom View（创建定制视图），打开 Custom View（定制视图）屏幕。
3. 单击 Name（名称）下拉箭头，然后在列表上选择一个定制视图。
4. 单击 Custom View（定制视图）面板上的 Set as Default（设置为默认值）按钮。在下次登录时，默认使用所选的定制视图。

给所有用户指定设备默认定制视图

如果你具备设备、端口和节点管理权限，可以给所有用户指定默认定制视图。

▶ **给所有用户指定设备默认定制视图：**

1. 单击 Devices（设备）选项卡。
2. 选择 Devices（设备）> Change View（更改视图）> Create Custom View（创建定制视图），
3. 单击 Name（名称）下拉箭头，然后选择要指定为系统默认视图的定制视图。

4. 选择 System Wide（整个系统）复选框，然后单击 Save（保存）按钮。

登录 CC-SG 的所有用户将看到根据所选择制视图排序的 Devices（设备）选项卡。用户可以更改定制视图。

Ch 12 Remote Authentication（远程验证）

在本章内

验证和授权概述

CC-SG 用户可以在 CC-SG 上进行本地验证和授权，也可以采用下列支持的目录服务器进行远程验证：

- Microsoft Active Directory (AD)
- Netscape Lightweight Directory Access Protocol (LDAP)
- TACACS+
- RADIUS

可以使用任意数量的远程服务器进行外部验证。例如可以配置三个 AD 服务器、两个 iPlanet (LDAP) 服务器和三个 RADIUS 服务器。

只有 AD 服务器可用于远程用户授权。

LDAP 实现技术采用 LDAP v3。

所有目录服务都支持 IPv6。

验证流程

如果启用远程验证，验证和授权步骤如下：

1. 用户用适当的用户名和密码登录 CC-SG。
2. CC-SG 连接外部服务器，给它发送用户名和密码。
3. 用户名和密码要么被接受，要么被拒绝后返回来。如果验证被拒绝，会导致登录失败。
4. 如果验证成功，就进行授权。CC-SG 检查输入的用户名是否匹配在 CC-SG 上创建或从 AD 上导入的组，并根据指定的策略授予权限。

如果禁用远程验证，验证和授权均在 CC-SG 本地进行。

用户帐号

如要进行远程验证，必须把用户帐号添加到验证服务器。除了用 AD 进行验证和授权，所有远程验证服务器都要求在 CC-SG 上创建用户。在验证服务器和 CC-SG 上使用的用户的用户名必须相同，但密码可以不同。只有在禁用远程验证之后，才使用本地 CC-SG 密码。参看*用户和用户组* (p. 166)详细了解如何添加要进行远程验证的用户。

注意：如果使用远程验证，用户必须联系管理员，在远程服务器上更改密码。不能在 CC-SG 上更改远程验证用户的密码。

LDAP 和 AD 标识名

在 LDAP 或 AD 服务器上配置远程验证用户时，必须输入用户名，并按标识名格式搜索。全标识名格式如 RFC2253 (http://www.rfc-editor.org/rfc/rfc2253.txt) 所述。

如要配置 CC-SG，必须了解如何输入标识名，以及标识名各部分应该按什么顺序排列。

指定 AD 标识名

AD 标识名应遵循这种结构。不必同时指定 common name（公用名）和 organization unit（机构单位）：

- common name (cn), organizational unit (ou), domain component (dc)

指定 LDAP 标识名

Netscape LDAP 和 eDirectory LDAP 标识名应遵循这种结构：

- user id (uid), organizational unit (ou), organization (o)

指定 AD 用户名

在 username 中指定 cn=administrator,cn=users,dc=xyz,dc=com，在 AD 服务器上验证 CC-SG 用户时，如果 CC-SG 用户与一个导入的 AD 组关联，将通过这些证书授予用户访问权。注意可以指定多个公用名、机构单位和域部件。

指定基本 DN

也可以输入一个标识名，指定从哪里开始搜索用户。在 Base DN（基本 DN）字段里输入标识名，指定可以在哪个 AD 容器里找到用户。例如输入：ou=DCAdmins,ou=IT,dc=xyz,dc=com，搜索 xyz.com 域下 DCAdmins 和 IT 机构单位的所有用户。

指定验证和授权模块

在 CC-SG 上作为模块添加所有外部服务器之后，指定是否希望 CC-SG 用每个模块进行验证和/或授权。

指定验证和授权模块：

1. 选择 Administration（管理）> Security（安全）。
2. 单击 Authentication（验证）选项卡。一个表显示配置的所有外部验证和授权服务器。
3. 对于列出的每个服务器：
   a. 如果希望 CC-SG 用此服务器进行用户验证，选择 Authentication（验证）复选框。
   b. 如果希望 CC-SG 用此服务器给用户授权，选择 Authorization（授权）复选框。只有 AD 服务器可用于授权。
4. 单击 Update（更新）按钮保存更改。

确定外部验证和授权服务器顺序

CC-SG 将按你指定的顺序查询已配置的外部验证和授权服务器。如果选择的第一个选项不可用，CC-SG 尝试使用第二个，然后尝试使用第三个，依次类推，直到成功为止。

确定 CC-SG 使用外部验证和授权服务器的顺序：

1. 选择 Administration（管理）> Security（安全）。
2. 单击 Authentication（验证）选项卡。一个表显示配置的所有外部验证和授权服务器。

3. 在列表上选择一个服务器，然后单击上下箭头键排列使用顺序。
4. 单击 Update（更新）按钮保存更改。

AD 和 CC-SG 概述

CC-SG 可以验证和授权从 AD 域控制器上导入的用户，不要求在 CC-SG 本地定义这些用户。这样，可以在 AD 服务器上单独维护用户。在 CC-SG 上把 AD 服务器配置为模块之后，CC-SG 可以查询给定域的所有域控制器。可以在 CC-SG 上使 AD 模块与 AD 服务器同步，确保 CC-SG 有最新的 AD 用户组授权信息。

不要添加重复 AD 模块。如果在用户尝试登录时，显示 You are not a member of any group（你不是任何用户组的成员）消息，表示你可能配置了重复 AD 模块。检查你配置的模块，看看它们是否描述有重叠的域范围。

把 AD 模块添加到 CC-SG

重要说明：在开始此过程之前，先创建适当的 AD 用户组，给它们指定 AD 用户。同时确保在配置管理器上配置了 CC-SG DNS 和 Domain Suffix（域前缀）。参看*配置 CC-SG 网络* (p. 257)。

把 AD 模块添加到 CC-SG：

1. 选择 Administration（管理）> Security（安全）。
2. 单击 Authentication（验证）选项卡。
3. 单击 Add（添加）按钮打开 Add Module（添加模块）窗口。
4. 单击 Module Type（模块类型）下拉菜单，然后在列表上选择 AD。
5. 在 Module name（模块名称）字段里输入 AD 服务器的名称。
   - 最多 31 个字符。
   - 可以使用所有可打印字符。
   - 模块名称是可选的，只用于区别 AD 服务器模块和你在 CC-SG 上配置的其他任何模块。模块名称与实际 AD 服务器名称没有关联。
6. 单击 Next（下一步）按钮打开 General（常规）选项卡。

AD 常规设置

必须在 General（常规）选项卡上添加信息，允许 CC-SG 查询 AD 服务器。

不要添加重复 AD 模块。如果在用户尝试登录时，显示 You are not a member of any group（你不是任何用户组的成员）消息，表示你可能配置了重复 AD 模块。检查你配置的模块，看看它们是否描述有重叠的域范围。

1. 在 Domain（域）字段里输入要查询的 AD 域。例如：如果 AD 域安装在 xyz.com 域里，在 Domain（域）字段里输入 xyz.com。CC-SG 和要查询的 AD 服务器必须在同一个域上配置，或者在彼此信任的不同域上配置。

   注意：CC-SG 将查询指定域对应的所有已知域控制器。

2. 分别在 Primary DNS Server IP Address（主 DNS 服务器 IP 地址）字段和 Secondary DNS Server IP Address（备用 DNS 服务器 IP 地址）字段里输入主 DNS 服务器 IP 地址和备用 DNS 服务器 IP 地址，或者选择 Use default CC-SG DNS（使用默认 CC-SG DNS）复选框，使用在 CC-SG 配置管理器部分配置的 DNS。参看***高级管理*** (p. 251)。

3. 如果要连接 AD 服务器，但不指定用户名和密码，选择 Anonymous Bind（匿名绑定）复选框。如果使用此选项，确保 AD 服务器允许匿名查询。

   注意：默认情况下， Windows 2003 不允许匿名查询。Windows 2000 服务器允许某些匿名操作，查询结果取决于每个对象的权限。

4. 如果不使用匿名绑定，在 User name（用户名）字段里输入在查询 AD 服务器时所用的用户帐号的用户名。所需的格式取决于 AD 版本和配置。使用下列其中一种格式。

   raritan.com 域里名为 User Name、登录名为 UserN 的用户可以这么输入：

   - cn=UserName,cn=users,dc=Raritan,dc=com
   - UserName@raritan.com
   - Raritan/UserName

   注意：指定的用户必须有权在 AD 域里执行搜索查询。例如用户可能属于 AD 里的一个用户组，其 Group scope（组范围）设置为 Global（全局），Group type（组类型）设置为 Security（安全）。

5. 在 Password（密码）和 Confirm Password（确认密码）字段里输入查询 AD 服务器所用的用户帐号的密码。最多 32 个字符。

注意：在完成 Advanced（高级）、Group（用户组）和 Trust（信任）设置之后，启用 Test Connection（测试连接）按钮。返回此选项卡，用给定参数测试至 AD 服务器的连接。应该显示成功连接确认消息。如果不显示确认消息，仔细检查设置并纠正错误，然后再试一次。

6. 单击 Next（下一步）按钮打开 Advanced（高级）选项卡。参看 ***AD 高级设置*** (p. 204)。

AD 高级设置

配置高级 AD 设置：

1. 单击 Advanced（高级）选项卡。
2. 输入 AD 服务器监听所用的端口号。默认端口是 389。如果 LDAP 使用安全连接，可能必须更改此端口。安全 LDAP 连接的标准端口是 636。
3. 如果要使用安全通道建立连接，选择 Secure Connection for LDAP（LDAP 安全连接）复选框。如果选择此复选框，CC-SG 用 LDAP over SSL 连接 AD。AD 配置可能不支持此选项。
4. 指定基本 DN（目录级/项），在此之下执行验证搜索查询。CC-SG 可以从此基本 DN 开始向下执行递归搜索。

示例	Description（说明）
dc=raritan,dc=com	在整个目录结构上进行用户项搜索查询。
cn=Administrators,cn=Users,dc=raritan,dc=com	只在 Administors 子目录（项）上进行用户项搜索查询。

5. 在 Filter（过滤器）字段里输入用户属性，把搜索查询限制在那些符合此标准的项上。默认过滤器是 objectclass=user，表示只搜索用户类型的项。
6. 指定用户项搜索查询执行方式。
   - 如果通过小程序登录的用户有权在 AD 服务器上执行搜索查询，选择 Use Bind（使用绑定）复选框。如果按 Bind username pattern（绑定用户名模式）指定用户名模式，此模式将与在小程序上输入的用户名组合在一起，用组合用户名连接 AD 服务器。

     示例：如果在小程序上指定了 cn={0},cn=Users,dc=raritan,dc=com 和 TestUser，CC-SG 用 cn=TestUser,cn-Users,dc=raritan,dc=com 连接 AD 服务器。

- 选择 Use Bind After Search（在搜索之后使用绑定）复选框，用你在 General（常规）选项卡上指定的用户名和密码连接 AD 服务器。在指定的基本 DN 里搜索项，检查它是否符合指定的过滤标准，属性 samAccountName 是否与在小程序上输入的用户名相同。然后使用在小程序上输入的用户名和密码，尝试第二个连接。第二个绑定确保用户输入的密码正确无误。
- 选择 Follow Referrals（利用引用）复选框，如果在 CC-SG 搜索 AD 服务器时遇到引用对象，允许 AD 利用引用完成搜索。
- 如要让已经登录 CC-SG 域的用户在用 Internet Explorer 访问 CC-SG 时可以利用集成 Windows 验证使用单点登录，选择 Enable Integrated Windows Authentication（启用集成 Windows 验证）复选框。参看***给单点登录设置集成 Windows 验证*** (p. 212)。

7. 单击 Next（下一步）按钮打开 Groups（用户组）选项卡。

AD 用户组设置

可以在 Groups（用户组）选项卡上指定要从哪个准确位置导入 AD 用户组。

重要说明：必须指定用户组设置，才能导入 AD 里的用户组。

1. 单击 Groups（用户组）选项卡。
2. 指定基本 DN（目录级/项），在此下面搜索包含待授权用户的用户组。

示例	Description（说明）
dc=raritan,dc=com	在整个目录结构上对组里的用户进行搜索查询。
cn=Administrators,cn=Users,dc=raritan,dc=com	只在 Administors 子目录(项)上对组里的用户进行搜索查询。

3. 在 Filter（过滤器）字段里输入用户的属性，把组用户搜索查询限制在那些符合此标准的项上。

   例如：如果基本 DN 指定为 cn=Groups,dc=raritan,dc=com，过滤器指定为 (objectclass=group)，将返回 Groups（用户组）项里组类型的所有项。

4. 单击 Next（下一步）按钮打开 Trusts（信任）选项卡。参看 ***AD 信任设置*** (p. 206)。

AD 信任设置

可以在 Trusts（信任）选项卡上设置此新 AD 域和任何现有域之间的信任关系。信任关系允许不同域里的验证用户访问资源。信任关系可以是 incoming（入站）、outgoing（出站）、bidirectional（双向）或 disabled（禁用）。如果希望代表 AD 里不同树系的 AD 模块可以相互访问信息，应该建立信任关系。在 CC-SG 上配置的信任应该匹配在 AD 上配置的信任。

1. 单击 Trusts（信任）选项卡。如果配置了多个 AD 域，Trusts（信任）选项卡列出其他所有域。
2. 对于 Trust Partner（信任伙伴）列上的每个域，单击 Trust Direction（信任方向）下拉菜单，然后选择要在各个域之间建立的信任的方向。在更改一个 AD 模块时，在所有 AD 模块上更新信任方向。
   - Incoming（入站）：信任来自此域的信息。
   - Outgoing（出站）：信任到达所选域的信息。
   - Bidirectional（双向）：信任每个域进出方向的信息。
   - Disabled（禁用）：不在域之间交换信息。
3. 单击 Apply（应用）按钮保存更改，然后单击 OK（确定）按钮保存 AD 模块并退出窗口。

   在 Security Manager（安全管理器）屏幕上的 External AA Servers（外部 AA 服务器）下面显示新 AD 模块。
4. 如果希望 CC-SG 用 AD 模块验证用户，选择 Authentication（验证）复选框。如果希望 CC-SG 用 AD 模块给用户授权，选择 Authorization（授权）复选框。
5. 单击 Update（更新）按钮保存更改。
6. 单击 General（常规）选项卡，然后单击 Test Connection（测试连接）确认设置。 应该显示成功连接确认消息。如果不显示确认消息，仔细检查设置并纠正错误，然后再试一次。

编辑 AD 模块

在配置 AD 模块之后，随时可以编辑这些模块。

编辑 AD 模块：

1. 选择 Administration（管理）> Security（安全）。
2. 单击 Authentication（验证）选项卡。一个表显示配置的所有外部验证和授权服务器。

3. 选择要编辑的 AD 模块，然后单击 Edit（编辑）按钮。
4. 单击 Edit Module（编辑模块）窗口上的每个选项卡查看已配置的设置。根据需要进行更改。参看 ***AD 常规设置*** (p. 203)、***AD 高级设置*** (p. 204)、***AD 用户组设置*** (p. 205)和 ***AD 信任设置*** (p. 206)。
5. 如果更改连接信息，单击 Test Connection（测试连接）按钮用给定参数测试至 AD 服务器的连接。应该显示成功连接确认消息。如果不显示确认消息，仔细检查设置并纠正错误，然后再试一次。
6. 单击 OK（确定）按钮保存更改。
7. 必须同步你更改的 AD 用户组，也可以同步所有 AD 模块，使模块上的所有组和所有用户同步。参看***使所有用户组与 AD 同步*** (p. 209)和***同步所有 AD 模块*** (p. 210)。

导入 AD 用户组

必须在 AD 模块上指定用户组设置，才能从 AD 服务器上导入用户组。参看 ***AD 用户组设置*** (p. 205)。

在更改导入的用户组或用户之后，必须同步你更改的 AD 用户组，使导入的用户组映射到 AD 上的适当用户组，并同步所有 AD 模块，使所有模块上的所有用户组和所有用户同步。参看***使所有用户组与 AD 同步*** (p. 209)和***同步所有 AD 模块*** (p. 210)。

可以从 AD 上导入相互嵌套的用户组。

*注意：在尝试导入 AD 用户组之前，确保在配置管理器上配置了 CC-SG DNS 和 Domain Suffix（域前缀）。参看***高级管理*** *(p. 251)。*

导入 AD 用户组：

1. 选择 Administration（管理）> Security（安全）。
2. 单击 Authentication（验证）选项卡。一个表显示所有配置的验证和授权服务器。
3. 选择要从哪个 AD 服务器上导入 AD 用户组。
4. 单击 Import AD User Groups（导入 AD 用户组），获取 AD 服务器存储的用户组值列表。如果 CC-SG 还没有任何用户组，可以在这里导入它们，然后给它们指定访问策略。
5. 选择要导入 CC-SG 的用户组。
   - 导入用户组的名称最多 64 个字符。
   - 如要搜索用户组，在 Search for User Group（搜索用户组）字段里输入搜索字符串，然后单击 Go（搜索）按钮。
   - 单击一个列标题按此列上的信息排序用户组列表。

- 单击 Select all（全选）按钮选择导入所有用户组。
- 单击 Deselect all（全部取消）按钮取消所选的所有用户组。

6. 在 Policies（策略）列上，在列表上选择一个 CC-SG 访问策略，把它指定给所选的用户组。
7. 单击 Import（导入）按钮导入所选的用户组。

提示：如要检查是否正确导入了组，查看刚才导入的组的权限，单击 Users（用户）选项卡，然后选择导入的组打开 User Group Profile（用户组配置文件）屏幕。确定 Privileges（权限）和 Device/Node Policies（设备/节点策略）选项卡上的信息是否正确。单击 Active Directory Associations（Active Directory 关联）选项卡查看此用户组关联的 AD 模块的有关信息。

使 AD 与 CC-SG 同步

可以采用几种方法使 CC-SG 上的信息与 AD 服务器上的信息同步。

- 所有模块每日同步：可以启用预定同步功能，让 CC-SG 每天在你选择的时间与所有 AD 模块同步。参看***同步所有 AD 模块*** (p. 210)。只有在用 AD 进行授权时，才需要此类同步。
- 用报告管理器实现预定同步：参看***预定任务*** (p. 299)。
- 按需同步：随时可以执行两种同步：
  1. **所有 Active Directory 模块：**此选项执行的同步与所有模块每日同步相同，但随时可以用它实现同步。只有在用 AD 进行授权时，才需要此类同步。参看***同步所有 AD 模块*** (p. 210)。
  2. **所有用户组：**在更改用户组之后，用此选项实现同步。在同步所有用户组时，可以把导入用户组和本地用户组映射到作为 AD 模块一部分的用户组。在同步用户组时，不更新 CC-SG 上的访问信息。既可以通过每天同步，也可以通过所有模块按需同步来同步所有 AD 模块，从而更新访问信息。参看***使所有用户组与 AD 同步*** (p. 209)。

使所有用户组与 AD 同步

如果更改了一个用户组，例如把用户组从一个 AD 模块移动到另一个 AD 模块，应该同步所有用户组。也可以在 User Group Profile（用户组配置文件）的 Active Directory Associations（Active Directory 关联）选项卡上人工更改用户组与 AD 之间的关联。

如果更改了用户或域控制器，应该同步所有 AD 模块。参看*同步所有 AD 模块* (p. 210)。

在同步 AD 用户组时，CC-SG 检索所选 AD 模块上的用户组，将其名称与 CC-SG 上的用户组进行对比，然后确定匹配情况。CC-SG 显示匹配情况，你可以选择让 AD 上的哪些用户组与 CC-SG 关联。这并不更新 CC-SG 上的用户访问信息。在同步 AD 用户组时，仅仅把 AD 上的用户组名称映射到 CC-SG。

使所有用户组与 AD 同步：

1. 选择 Administration（管理）> Security（安全）。
2. 单击 Authentication（验证）选项卡。一个表显示所有配置的验证和授权服务器。
3. 选择要让哪个 AD 服务器的用户组与 CC-SG 上的用户组同步。
4. 在 On Demand Synchronization（按需同步）列表上选择 All User Groups（所有用户组），然后单击 Synchronize Now（现在同步）按钮。
5. 显示一个列表，列出在 AD 模块上找到的、名称与 CC-SG 上的用户组匹配的所有用户组。选择要同步的用户组，然后单击 OK（确定）按钮。

   在成功同步所选模块上的所有导入用户组之后，显示一条确认消息。

同步所有 AD 模块

每当更改或删除 AD 上的用户，更改 AD 上的用户权限，或者更改域控制器时，都应该同步所有 AD 模块。

在同步所有 AD 模块时，CC-SG 检索所有已配置的 AD 模块上的用户组，将其名称与此前导入 CC-SG 的用户组或与 CC-SG 上的 AD 模块关联的用户组进行比较，刷新 CC-SG 本地高速缓存。CC-SG 本地高速缓存包含每个域的所有域控制器，与 CC-SG 上的模块关联的所有用户组，以及已知 AD 用户的用户信息。如果用户组从 AD 模块上删除了，CC-SG 也在本地高速缓存上删除与被删除用户组之间的所有关联。这样可以确保 CC-SG 有最新的 AD 用户组信息。

同步所有 AD 模块：

1. 选择 Administration（管理）> Security（安全）。
2. 单击 Authentication（验证）选项卡。一个表显示所有配置的验证和授权服务器。
3. 在 On Demand Synchronization（按需同步）列表上选择 All Active Directory Modules（所有 Active Directory 模块），然后单击 Synchronize Now（现在同步）按钮。在成功同步所有 AD 模块之后，显示一条确认消息。

如果在 MSFT Windows Server 2003 AD 上更改用户密码，在接下来的约 30 分钟内，新密码和旧密码均有效。在此期间，用户可以用任一个密码登录 CC-SG。这是因为在全面更新新密码之前，AD 要高速缓存旧密码 30 分钟。

启用或禁用所有 AD 模块每日同步

如要设置更频繁的同步，可以预定一个任务自动同步所有 AD 模块。参看 *预定任务* (p. 299)。

启用所有 AD 模块每日同步：

1. 选择 Administration（管理）> Security（安全）。
2. 单击 Authentication（验证）选项卡。一个表显示所有配置的验证和授权服务器。
3. 选择 Daily Synchronization of All Modules（所有模块每日同步）复选框。
4. 单击 Synchronization Time（同步时间）字段里的上下箭头，然后选择 CC-SG 在哪个时间执行所有 AD 模块每日同步。

5. 单击 Update（更新）按钮保存更改。

禁用所有 AD 模块每日同步：

1. 选择 Administration（管理）> Security（安全）。
2. 单击 Authentication（验证）选项卡。一个表显示所有配置的验证和授权服务器。
3. 取消 Daily Synchronization of All Modules（所有模块每日同步）复选框。
4. 单击 Update（更新）按钮保存更改。

更改 AD 每日同步时间

在启用每日同步之后，可以指定自动同步时间。每日同步默认时间是 23:30。

更改 AD 每日同步时间：

1. 选择 Administration（管理）> Security（安全）。
2. 选择 Authentication（验证）选项卡。确保选择 Daily Synchronization of All Modules（所有模块每日同步）复选框。
3. 单击屏幕下半部 Synchronization Time（同步时间）字段里的上下箭头，然后选择 CC-SG 在哪个时间执行所有 AD 模块每日同步。
4. 单击 Update（更新）按钮保存更改。

重新命名和移动 AD 用户组

重新命名 AD 用户组：

如果已导入 CC-SG 的 AD 用户组在 AD 里的名称发生变化，在此之后执行同步或受影响的 AD 用户首次登录时，CC-SG 检测名称变化，并在审计跟踪里记录警告消息。

`User group <group name> has been renamed to <group new name> in AD module <module name>.`（用户组`<group name>`在 AD 模块`<module name>`里的名称已被重新命名为`<group new name>`。）

删除或移动 AD 用户组：

如果删除已导入 CC-SG 的 AD 用户组，或者把它移出 AD 用户组搜索值范围，CC-SG 在审计跟踪里记录警告消息。同时删除此用户组的 AD 关联。

`User group <group name> cannot be found in AD module <module name>.`（在 AD 模块`<module name>`里找不到用户组`<group name>`。）

在搜索值范围内移动 AD 用户组：

如果在搜索值范围内移动 AD 用户组，不记录警告消息，此用户组照常工作。

给单点登录设置集成 Windows 验证

基于集成 Windows 验证的单点登录使已经登录 CC-SG 域的用户能在不输入证书的情况下用 Internet Explorer 访问 CC-SG。

利用集成 Windows 验证实现单点登录的最低要求

- 单点登录只支持 Kerberos。
- CC-SG Access Client 和 CC-SG Admin Client 支持单点登录。
- Windows 客户机安装的 Internet Explorer 支持 Kerberos 和集成 Windows 验证。

给单点登录配置集成 Windows 验证

基于下列假设说明如何配置单点登录。

域： raritan.com

域登录名：example_user

主机名： example

信任域：nj.raritan.com; eu.raritan.com

1. 在 AD 服务器上配置 Service Principal Name（服务主体名称）。
   a. 在 Active Directory 上，在 CC-SG 域下创建 example_user 用户帐号。在下列说明中，raritan.com 是域，登录名是 example_user。
   b. 禁用 User has to change password at next logon（用户在下次登录时必须更改密码）。
   c. 指定密码。
   d. 假设 CC-SG 主机名是 example。在 AD 服务器上运行下列命令给 CC-SG 设置服务主体名称。

```
Setspn -A HTTP/example example_user
Setspn -A HTTP/example.raritan.com example_user
```

2. 在 CC-SG 上启用单点登录
   a. 登录 CC-SG Admin Client。
   b. Edit Example AD module: In the General tab, use Service Principal Name for Username.在 Username（用户名）字段里输入的域名应该是全大写字符。

```
example_user@EXAMPLE.RARITAN.COM
```

   c. 更改密码。每当在 AD 上更改 example_user 的密码时，也必须在这里更改密码。

注意：对于其他所有信任域，不必进行这些更改。让登录名在其他域里保持原样。

   d. 在 Advanced（高级）选项卡上选择 Other（其他）下面的 Enable Integrated Windows Authentication（启用集成 Windows 验证）复选框。针对其他希望允许单点登录的所有信任域启用此选项。
   e. 单击 OK（确定）按钮保存设置。

注意：如果已经给 nj.raritan.com 和 eu.raritan.com 模块启用了集成 Windows 验证，登录这些信任域的用户应该也能利用单点登录访问 example.raritan.com。

3. 配置 Internet Explorer 浏览器使用 Windows 验证。IE 的大多数设置使用默认设置。

   a. 配置本地内部网域

      - 选择 Tools（工具）> Internet Options（Internet 选项）> Security（安全）> Local intranet（本地内部网）> Sites（站点）。
      - 确保在 Local intranet（本地内部网）弹出窗口上选择 Include all sites that bypass the proxy server（包括不使用代理服务器的所有站点）选项和 Include all local (intranet) sites not listed in other zones（包括没有列在其他区域的所有本地[内部网]站点）选项。
      - 或者单击 Advanced（高级）按钮，在 Local intranet (Advanced)（本地内部网[高级]）对话框上添加用户用户 CC-SG 所用的所有相关域名。例如添加 example.raritan.com 和 example，然后单击 OK（确定）按钮。

   b. 配置内部网验证

      - 选择 Tools（工具）> Internet Options（Internet 选项）> Security（安全）> Local intranet（本地内部网）> Custom Level（自定义级别）。
      - 在 Security Settings（安全设置）对话框上翻到 User Authentication（用户验证）部分。选择 Automatic logon only in Intranet zone（只在内部网区域自动登录）。单击 OK（确定）按钮。
      - 选择 Tools（工具）> Internet Options（Internet 选项）> Advanced（高级）> Security（安全），然后选择 Enable Integrated Windows Authentication（启用集成 Windows 验证）。

排除集成 Windows 验证单点登录故障

- 确保给 CC-SG 设置正确的时间，此时间与域的时间设置同步。默认最大差异是 5 分钟。
- 用主机名访问 CC-SG，例如 example 或 example.raritan.com，确保可以在内部网访问 CC-SG。
- 确保客户机操作系统可以向 Active Directory 获取 Kerberos ticket。可能必须在 Window 7 操作系统上启用 DES。

  参看 http://technet.microsoft.com/en-us/library/dd560670%28WS.10%29.aspx 了解详情。

关于 LDAP 和 CC-SG

在 CC-SG 启动并输入用户名和密码之后，通过 CC-SG 转发或直接向 LDAP 服务器发送查询。如果用户名和密码匹配 LDAP 上的信息，就验证用户。然后根据 LDAP 服务器上的本地用户组给用户授权。

把 LDAP (Netscape) 模块添加到 CC-SG

把 LDAP (Netscape) 模块添加到 CC-SG：

1. 选择 Administration（管理）> Security（安全）。
2. 单击 Authentication（验证）选项卡。
3. 单击 Add（添加）按钮打开 Add Module（添加模块）窗口。
4. 单击 Module Type（模块类型）下拉菜单，然后在列表上选择 LDAP。
5. 在 Module name（模块名称）字段里输入 LDAP 服务器的名称。
6. 单击 Next（下一步）按钮打开 General（常规）选项卡。

LDAP 常规设置

1. 单击 General（常规）选项卡。
2. 在 IP Address/Hostname（IP 地址/主机名）字段里输入 LDAP 服务器的 IP 地址或主机名。参看*术语/缩写语* (参看 "*术语/缩略语*" p. 2) 了解主机名规则。
3. 在 Port（端口）字段里输入端口值。默认端口是 389。
4. 如果使用安全 LDAP 服务器，选择 LDAP over SSL。
5. 如果 LDAP 服务器允许匿名查询，选择 Anonymous Bind（匿名绑定）。对于匿名绑定，不必输入用户名和密码。

   注意：默认情况下， Windows 2003 不允许匿名查询。Windows 2000 服务器允许某些匿名操作，查询结果取决于每个对象的权限。

6. 如果不使用匿名绑定，在 User name（用户名）字段里输入用户名。输入标识名 (DN) 指定查询 LDAP 服务器所用的证书。对于 DN，输入公用名、机构单位和域。

   例如输入 uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot。用逗号分隔开各个值，但逗号前后不要有空格。值可以有空格，例如 Command Center。

7. 在 Password（密码）和 Confirm Password（确认密码）字段里输入密码。

8. 如要指定从哪里开始搜索用户，在 Base DN（基本 DN）字段里输入一个标识名。例如 ou=Administrators,ou=TopologyManagement,o=NetscapeRoot 搜索域下面的所有机构单位。
9. 如要把搜索范围缩小到特殊对象类型，在 Filter（过滤器）字段里输入一个值。例如 (objectclass=person) 把搜索范围缩小到人对象。
10. 单击 Test Connection（测试连接）按钮用给定参数测试 LDAP 服务器。应该显示成功连接确认消息。如果不显示消息，仔细检查设置并纠正错误，再试一次。
11. 单击 Next（下一步）按钮进入 Advanced（高级）选项卡，给 LDAP 服务器设置高级配置选项。

LDAP 高级设置

1. 单击 Advanced（高级）选项卡。
2. 如果要用加密方法把密码发送到 LDAP 服务器，选择 Base 64。如果要把密码作为纯文本发送到 LDAP 服务器 ,选择 Plain Text(纯文本）。
3. Default Digest（默认摘要）：选择用户密码默认加密方法。
4. 在 User Attribute（用户属性）和 Group Membership Attribute（组成员属性）字段里输入用户属性参数和组成员属性参数。这些值应该从 LDAP 目录模式获得。
5. 在 Bind Username Pattern（绑定用户名模式）字段里输入绑定模式。
   - 如果希望 CC-SG 把在登录时输入的用户名和密码发送到 LDAP 服务器进行验证，选择 Use bind（使用绑定）。如果不选择 Use bind（使用绑定），CC-SG 将在 LDAP 服务器上搜索用户名，如果找到用户名，就检索 LDAP 对象，在本地比较关联密码和输入密码。
   - 在某些 LDAP 服务器上，密码不能作为 LDAP 对象的一部分检索。选择 Use bind after search（在搜索之后使用绑定）复选框，告诉 CC-SG 把密码和 LDAP 对象再次绑定在一起，并把它发送回服务器进行验证。
6. 单击 OK（确定）按钮保存更改。在 Security Manager（安全管理器）屏幕上的 External AA Servers（外部 AA 服务器）下面显示新 LDAP 模块。
7. 如果希望 CC-SG 用 LDAP 模块验证用户，选择 Authentication（验证）复选框。
8. 单击 Update（更新）按钮保存更改。

Sun One LDAP (iPlanet) 配置设置

如果用 Sun One LDAP 服务器进行远程验证，如下配置：

参数名称	SUN One LDAP 参数
IP Address/Hostname（IP 地址/主机名）	<Directory Server IP Address>
User Name（用户名）	CN=<Valid user id>
Password（密码）	<Password（密码）>
BaseDN（基本 DN）	O=<Organization>
Filter（过滤器）	(objectclass=person)
Passwords（密码，高级屏幕）	纯文本
Password Default Digest（密码默认摘要，高级）	SHA
Use Bind（使用绑定）	不选择
Use Bind After Search（在搜索之后使用绑定）	选择

OpenLDAP (eDirectory) 配置设置

如果用 OpenLDAP 服务器进行远程验证，如下配置：

参数名称	Open LDAP 参数
IP Address/Hostname（IP 地址/主机名）	<Directory Server IP Address>
User Name（用户名）	CN=<有效用户 ID>, O=<机构>
Password（密码）	<Password（密码）>
User Base（用户库）	O=accounts, O=<Organization>
User Filter（用户过滤器）	(objectclass=person)
Passwords（密码，高级屏幕）	Base64
Password Default Digest（密码默认摘要，高级）	Crypt（加密）
Use Bind（使用绑定）	不选择
Use Bind After Search（在搜索之后使用绑定）	选择

IBM LDAP 配置设置

如果用 IBM LDAP 服务器进行远程验证，如下配置：

参数名称	IBM LDAP 参数
IP Address/Hostname（IP 地址/主机名）	<Directory Server IP Address>
User Name（用户名）	CN=<Valid user id>
Password（密码）	<Password（密码）>
User Base（用户库）	例如： cn=users,DC=raritan,DC=com,DC=us
User Filter（用户过滤器）	(objectclass=person)
Passwords（密码，高级屏幕）	Base64
Password Default Digest(密码默认摘要，高级）	无
User Attribute（用户属性）	uid
Group Membership Attribute（组成员属性）	保留空白
Bind Username Pattern（绑定用户名模式）	例如： cn={0},cn=users,DC=raritan,DC=com,DC=us
Use Bind（使用绑定）	不选择
Use Bind After Search(在搜索之后使用绑定）	选择

关于 TACACS+ 和 CC-SG

用 TACACS+ 服务器远程验证的 CC-SG 用户，必须在 TACACS+ 服务器和 CC-SG 上创建。TACACS+ 服务器和 CC-SG 上的用户名必须相同，但密码可以不同。参看*用户和用户组* (p. 166)。

添加 TACACS+ 模块

添加 TACACS+ 模块：

1. 选择 Administration（管理）> Security（安全）。
2. 单击 Authentication（验证）选项卡。
3. 单击 Add（添加）按钮打开 Add Module（添加模块）窗口。
4. 选择 Module Type（模块类型）> TACACS+。
5. 在 Module name（模块名称）字段里输入 TACACS+ 服务器的名称。
6. 然后单击 Next（下一步）按钮打开 General（常规）选项卡。

TACACS+ 常规设置

1. 在 IP Address/Hostname(IP 地址/主机名)字段里输入 TACACS+ 服务器的 IP 地址或主机名。参看*术语/缩写语* (参看 "*术语/缩略语*" p. 2)了解主机名规则。
2. 在 Port Number（端口号）字段里输入 TACACS+ 服务器监听的端口号。默认端口号是 49。
3. 在 Authentication Port（验证端口）字段里输入验证端口。
4. 在 Shared Key（共享密钥）和 Shared key confirm（共享密钥确认）字段里输入共享密钥。最多 128 个字符。
5. 单击 OK（确定）按钮保存更改。在 Security Manager（安全管理器）屏幕上的 External AA Servers（外部 AA 服务器）下面显示新 TACACS+ 模块。
6. 如果希望 CC-SG 用 TACACS+ 模块验证用户，选择 Authentication（验证）复选框。
7. 单击 Update（更新）按钮保存更改。

关于 RADIUS 和 CC-SG

用 RADIUS 服务器远程验证的 CC-SG 用户，必须在 RADIUS 服务器和 CC-SG 上创建。RADIUS 服务器和 CC-SG 上的用户名必须相同，但密码可以不同。参看*用户和用户组* (p. 166)。

添加 RADIUS 模块

添加 RADIUS 模块：

1. 选择 Administration（管理）> Security（安全）。

2. 单击 Authentication（验证）选项卡。
3. 单击 Add（添加）按钮打开 Add Module（添加模块）窗口。
4. 单击 Module Type(模块类型)下拉菜单，然后在列表上选择 RADIUS。
5. 在 Module name（模块名称）字段里输入 RADIUS 服务器的名称。
6. 单击 Next（下一步）按钮打开 General（常规）选项卡。

RADIUS 常规设置

1. 单击 General（常规）选项卡。
2. 在 IP Address/Hostname（IP 地址/主机名）字段里输入 RADIUS 服务器的 IP 地址或主机名。参看*术语/缩写语* (参看 "*术语/缩略语*" p. 2)了解主机名规则。
3. 在 Port Number（端口号）字段里输入端口号。默认端口号是 1812。
4. 在 Authentication Port（验证端口）字段里输入验证端口。
5. 在 Shared Key（共享密钥）和 Shared key confirm（共享密钥确认）字段里输入共享密钥。
6. 单击 OK（确定）按钮保存更改。
7. 在 Security Manager(安全管理器)屏幕上的 External AA Servers(外部 AA 服务器）下面显示新 RADIUS 模块。如果希望 CC-SG 用 RADIUS 模块验证用户，选择 Authentication（验证）复选框。
8. 单击 Update（更新）按钮保存更改。

用 RADIUS 进行双因素验证

同时使用支持双因素验证的 RSA RADIUS 服务器和 RSA Authentication Manager，CC-SG 可以通过动态令牌使用双因素验证方案。

在这种环境下，用户在登录 CC-SG 时先在 Username（用户名）字段里输入用户名，在 Password(密码)字段里输入固定密码，然后在 Password（密码）字段里输入动态令牌值。

CC-SG 配置与上述标准 RADIUS 远程验证配置相同。参看*双因素验证* (p. 404)。

Ch 13 报告

在本章内

使用报告

任何报告的默认过滤器是用户策略，例如报告不显示用户没有访问权的节点或设备。

排序报告数据

- 单击一个列标题按此列上的值排序报告数据。数据按字母升序、数字升序或时间先后顺序刷新。
- 再次单击列标题按降序排序数据。

调整报告列宽

你选择的列宽在下次登录并运行报告时变成默认报告视图。

1. 让鼠标指针停留在标题行上的列分隔线上，直到指针变成双向箭头为止。
2. 单击并左右拖动鼠标，即可调节列宽。

查看报告详细信息

- 双击一行查看报告详细信息。
- 在突出显示一行时，按 Enter 查看详细信息。

打开一个对话框显示所选报告的所有详细信息，并不仅仅显示你在报告屏幕上看到的详细信息。例如节点 Access Report（访问报告）屏幕不显示 Interface Type（接口类型）和 Message（消息），但 Node Access Details（节点访问详细信息）对话框显示这些信息。

浏览有多页的报告

- 单击报告底部的箭头图标，浏览由多页构成的报告。

打印报告

CC-SG 有两个打印选项。可以在屏幕显示报告时打印报告页面（打印截屏），也可以打印完整报告（包括每一项的详细信息）。

注意：打印选项对所有 CC-SG 均有效。

打印报告截屏：

1. 生成要打印的报告。
2. 选择 Secure Gateway（安全网关）> Print Screen（打印屏幕）。

打印所有报告详细信息：

1. 生成要打印的报告。确保在 Entries to Display（要显示的项）字段里选择 All（全部）。
2. 选择 Secure Gateway（安全网关）> Print（打印）。

把报告保存成文件

可以把报告保存成 .CSV 文件，然后用 Excel 打开。在把报告保存成文件时，保存报告的所有详细信息，而不仅仅保存你在报告屏幕上看到的详细信息。例如节点 Access Report（访问报告）屏幕不显示 Type（类型）和 Message（消息）列，但在保存并用 Excel 打开 Access Report（访问报告）之后，可以看到这两列。

1. 生成要保存成文件的报告。
2. 单击 Save to File（保存到文件）按钮。
3. 输入文件名，然后选择文件保存位置。
4. 单击 Save（保存）按钮。

清除 CC-SG 上的报告数据

可以清除 Audit Trail（审计跟踪）报告和 Error Log（错误日志）报告显示的数据。在清除这些报告时，删除与所用搜索条件相匹配的所有数据。例如：如果搜索从 2008 年 3 月 26 日到 2008 年 3 月 27 日的所有 Audit Trail（审计跟踪）项，只删除这些记录。3 月 26 日之前和 3 月 27 日之后的项仍然保留在 Audit Trail（审计跟踪）里。

清除数据从 CC-SG 上永久删除掉。

清除 CC-SG 上的报告数据：

1. 在 CC-SG 上生成要删除数据的报告。
2. 单击 Purge（清除）按钮。
3. 单击 Yes（是）按钮确认。

隐藏或显示报告过滤器

某些报告在报告屏幕顶部显示一组过滤条件。可以隐藏过滤部分，从而扩大报告显示区。

隐藏或显示报告过滤器：

- 单击屏幕顶部的 Filter（过滤器）工具栏隐藏过滤部分。
- 再次单击 Filter（过滤器）工具栏显示过滤部分。

报告里的 IP 地址

在双协议堆模式下运行 CC-SG 时，同时允许 IPv4 地址和 IPv6 地址，报告列标签变成这两种地址。

审计跟踪报告

CC-SG 维护系统事件审计跟踪：审计跟踪记录各种事件，例如设备或节点添加、编辑或删除，以及其他系统修改。

注意：当用户连接做成书签的端口时，审计跟踪记录一项，但在关闭在建立连接时所用的浏览器实例之前，并不记录退出项。

生成审计跟踪报告：

1. 选择 Reports（报告）> Audit Trail（审计跟踪）。

2. 在 Start Date and Time（开始日期和时间）和 End Date and Time（结束日期和时间）字段里设置报告的日期范围。单击默认日期的每个部分（月、日、年、时、分、秒）选择它，然后单击上下箭头调节到希望的数字。
3. 可以在 Message Type（消息类型）、Message（消息）、Username（用户名）和 User IP address（用户 IP 地址）字段里输入其他参数限制报告包含的数据。除了 Message Type（消息类型）字段，这些字段均接受通配符。
   - 如要把报告仅限于一种消息，在 Message Type（消息类型）字段里选择一种类型。
   - 如要按与一个活动关联的消息文本限制报告，在 Message（消息）字段里输入文本。
   - 如要把报告仅限于特定用户的活动，在 Username（用户名）字段里输入此用户的用户名。
   - 如要把报告仅限于特定 IP 地址的活动，在 User IP address（用户 IP 地址）字段里输入此用户的 IP 地址。
4. 在 Entries to Display（要显示的项数）字段里选择报告屏幕要显示的项数。
5. 单击 Apply（应用）按钮生成报告。
   - 如要清除报告里的记录，单击 Purge（清除）按钮。参看*清除 CC-SG 上的报告数据* (p. 223)。

错误日志报告

CC-SG 把错误消息存储在一系列可以访问的错误日志文件里，这些消息有助于排除问题。错误日志包括与错误条件关联的审计跟踪部分项。

生成错误日志报告：

1. 选择 Reports（报告）> Error Log（错误日志）。
2. 在 Start Date and Time（开始日期和时间）和 End Date and Time（结束日期和时间）字段里设置报告的日期范围。单击默认日期的每个部分（月、日、年、时、分、秒）选择它，然后单击上下箭头调节到希望的数字。
3. 可以在 Message（消息）、Username（用户名）和 User IP address（用户 IP 地址）字段里输入其他参数限制报告包含的数据。这些字段接受通配符。
   - 如要按与一个活动关联的消息文本限制报告，在 Message（消息）字段里输入文本。

- 如要把报告仅限于特定用户的活动，在 Username（用户名）字段里输入此用户的用户名。
- 如要把报告仅限于特定 IP 地址的活动，在 User IP address（用户 IP 地址）字段里输入此用户的 IP 地址。

4. 在 Entries to Display（要显示的项数）字段里选择报告屏幕要显示的项数。
5. 单击 Apply（应用）按钮生成报告。
   - 单击 Purge（清除）按钮删除错误日志。参看***清除 CC-SG 上的报告数据*** (p. 223)。

访问报告

生成访问报告，查看有关被访问的设备和节点的信息，以及哪些用户何时访问设备和节点等信息。

生成访问报告：

1. 选择 Reports（报告）> Access Report（访问报告）。
2. 选择 Devices（设备）或 Nodes（节点）。
3. 在 Start Date and Time（开始日期和时间）和 End Date and Time（结束日期和时间）字段里设置报告的日期和时间范围。单击默认日期的每个部分（月、日、年、时、分、秒）选择它，然后单击上下箭头调节到希望的数字。
4. 可以在 Device name（设备名称）、Node name（节点名称）、Username（用户名）和 User IP address（用户 IP 地址）字段里输入其他参数限制报告包含的数据。这些字段接受通配符。
   - 如要按与一个活动关联的消息文本限制报告，在 Message（消息）字段里输入文本。
   - 如要把报告仅限于特定设备，在 Device Name(s)（设备名称）字段里输入设备名称。
   - 如要把报告仅限于特定节点，在 Node Name(s)（节点名称）字段里输入端口名称。
   - 如要把报告仅限于特定用户的活动，在 Username(s)（用户名）字段里输入此用户的用户名。
   - 如要把报告仅限于特定 IP 地址的活动，在 IP Address(es)（IP 地址）字段里输入此用户的 IP 地址。
5. 在 Entries to Display（要显示的项数）字段里选择报告屏幕要显示的项数。
6. 单击 Apply（应用）按钮生成报告。

可用性报告

可用性报告显示所有设备连接或所有节点连接的状态。此报告提供 CC-SG 管理网络里所有设备和所有节点的完整可用性信息。

生成可用性报告：

1. 选择 Reports（报告）> Availability Report（可用性报告）。
2. 选择 Nodes（节点）或 Devices（设备）。
3. 单击 Apply（应用）按钮。

活动用户报告

活动用户报告显示当前用户和用户会话。可以在报告上选择活动用户，让他们断开 CC-SG。

生成活动用户报告：

- 选择 Reports（报告）> Users（用户）> Active Users（活动用户）。

让用户断开 CC-SG 上的活动会话：

1. 在 Active Users（活动用户）报告上选择要断开的用户名。
2. 单击 Logout（退出）按钮。

封锁用户报告

封锁用户报告显示当前因为登录失败次数过多而被 CC-SG 封锁的用户。可以在此报告上解除对用户的封锁。参看*封锁设置* (p. 288)。

生成封锁用户报告：

- 选择 Reports（> Users（用户）> Locked Out Users（锁定用户）。

解除 CC-SG 用户封锁：

- 选择要解除封锁的用户，然后单击 Unlock User（解除用户封锁）按钮。

所有用户数据报告

用户数据报告显示 CC-SG 数据库里所有用户的某些数据。

生成所有用户数据报告：

- 选择 Reports（报告）> Users（用户）> All User Data（所有用户数据）。
  - User Name（用户名称）字段显示所有 CC-SG 用户的用户名。
  - 如果用户可以登录 CC-SG，Enabled（启用）字段显示 true，否则显示 false，视是否在 User Profile（用户配置文件）上选择了 Login Enabled（启用登录）选项而定。参看*添加用户* (p. 173)。
  - Password Expiration（密码到期）字段显示在强制用户更改密码之前可使用的天数。参看*添加用户* (p. 173)。
  - Groups（组）字段显示用户所属的用户组。
  - Privileges（权限）字段显示给用户指定的 CC-SG 权限。参看*用户组权限* (p. 382)。
  - Email（电子邮件）字段显示在 User Profile（用户配置文件）上指定的用户的电子邮件地址。
  - User Type（用户类型）字段显示 local（本地）或 remote（远程），视用户的访问方法而定。

用户组数据报告

用户组数据报告显示用户数据及其关联用户组数据。

生成用户组数据报告：

1. 选择 Reports（报告）> Users（用户）> User Group Data（用户组数据）。
2. 双击 User Group（用户组）查看指定的策略。

设备资产报告

设备资产报告显示当前受 CC-SG 管理的设备的数据。

按主机名添加的设备在报告里只按主机名显示。按 IP 地址添加的设备按 IP 地址显示。如果给 CC-SG 配置了双协议堆模式，报告和详细信息对话框显示那些支持 IPv6 的设备的 IPv4 地址和 IPv6 地址。

生成设备资产报告：

- 选择 Reports（报告）> Devices（设备）> Device Asset Report（设备资产报告），生成所有设备的报告。

按设备类型过滤报告数据：

- 选择设备类型，然后单击 Apply（应用）按钮。应用所选的过滤器，重新生成报告。
  - Device Name（设备名称）字段用红字显示版本与**兼容性指标**不相符的设备。

设备组数据报告

设备组数据报告显示设备组信息。

只有详细信息对话框显示设备主机名和 IP 地址。

生成设备组数据报告：

1. 选择 Reports（报告）> Devices（设备）> Device Group Data（设备组数据）。
2. 双击一行显示设备组里的设备。

查询端口报告

查询端口报告按端口状态显示所有端口。

生成查询端口报告：

1. 选择 Reports（报告）> Ports（端口）> Query Port（查询端口）。
2. 在 Port Status/Availability（端口状态/可用性）部分选择报告要包括的端口状态。选择多个复选框，包括有所有选择状态的端口。如果指定 Status（状态）选项，必须至少选择一个 Availability（可用性）选项。

状态类型	端口状态	定义
	全部	所有端口。
Status（状态）：		
	Up（运行）	
	Down（停机）	由于设备关闭或不可用，不能连接端口。
Availability（可用性）：		
	Idle（空闲）	端口已配置，可以连接端口。
	Connected（已连接）	
	Busy（忙）	用户连接了此端口。
	Power on（通电）	
	Power off（断电）	
Unconfigured（未配置）：		
	New（新）	端口连接了目标服务器，但端口尚未配置。
	Unused（未使用）	端口未连接目标服务器，且端口尚未配置。

3. 选择 Ghosted Ports（幻影端口）包括幻影端口。当 CIM 或目标服务器与 Paragon 系统断开或断电时（人工或意外），形成幻影端口。参看 Raritan **Paragon II 用户指南**。**可选。**
4. 选择 Paused Ports（暂停端口）或 Locked Ports（封锁端口）包括被暂停或封锁的端口。当 CC-SG 暂停管理设备时，形成暂停端口。在升级设备时，形成封锁端口。**可选。**
5. 在 Entries to Display（要显示的项数）字段里选择报告屏幕要显示的数据行数。

   注意：在作为任务生成报告时，不应用此首选项。

6. 单击 Apply（应用）按钮生成报告。

节点资产报告

节点资产报告显示 CC-SG 管理的所有节点的节点名称、接口名称和类型、设备名称和类型、节点组。可以过滤报告，只包括与指定节点组、接口类型、设备类型或设备对应的节点的数据。

生成节点资产报告：

1. 选择 Reports（报告）> Nodes（节点）> Node Asset Report（节点资产报告）。
2. 选择要应用于报告的过滤条件：All Nodes（所有节点）、Node Group（节点组）、Device Group（设备组）或 Devices（设备）。
   - 如果选择 Node Group（节点组）、Interface Type（接口类型）或 Device Group（设备组），在相应的菜单上选择一个参数。
   - 如果选择 Devices（设备），在 Available（可用）列表上选择报告要包括哪些设备的节点资产，然后单击 Add（添加）按钮把它移动到 Selected（选择）列表上。
3. 单击 Apply（应用）按钮生成报告。生成节点资产报告。

获取接口的书签 URL：

1. 生成节点资产报告，双击一个节点打开详细信息对话框。
2. 单击 Save to File（保存到文件）按钮所有报告信息保存成 .csv 文件。
3. URL 列上有每个节点的直接链接。URL 由客户机浏览器访问 CC-SG 所用的 URL 构成。例如：如果客户机浏览器使用 https://<hostname、IPv4 或 [IPv6]>/admin，且客户机把主机名解析成 <IPv4 或 IPv6>，要用 <IPv4 或 IPv6> 创建书签。这样，CC-SG 可以继续在 NAT 后面工作。
4. 可以用此信息创建一个有每个节点链接的网页，而不是给每个节点逐个添加书签。参看*添加接口书签* (p. 135)。

活动节点报告

对于有活动连接的每个节点，活动节点报告包括每个活动接口的名称和类型、连接模式、关联设备、时间戳、当前用户和用户 IP 地址。可以在此报告上查看活动节点列表，可以断开节点。

生成活动节点报告：

- 选择 Reports（报告）> Nodes（节点）> Active Nodes（活动节点）。如果当前有活动节点，生成活动节点报告。

让节点断开活动会话：

- 在 Active Nodes（活动节点）报告上选择要断开的节点，然后单击 Disconnect（断开）。

节点创建报告

节点创建报告列出在指定时间范围内进行的所有成功和失败的节点创建尝试。可以指定是要查看所有节点创建尝试，还是只查看可能的重复节点创建尝试。

生成节点创建报告：

1. 选择 Reports（报告）> Nodes（节点）> Node Creation（节点创建）。
2. 选择 All Nodes（所有节点）或 Potential Duplicates（可能重复的节点）。Potential Duplicates（可能重复的节点）选项把报告仅限于那些有“可能重复”标记的节点。
3. 如果选择 All Nodes（所有节点），在 Start Date and Time（开始日期和时间）和 End Date and Time（结束日期和时间）字段里设置报告的日期范围。单击默认日期的每个部分（月、日、年、时、分、秒）选择它，然后单击上下箭头调节到希望的数字。
4. 单击 Apply（应用）按钮生成节点创建报告。
   - Result（结果）字段显示 Success（成功）、Failed（失败）或 Potential Duplicate（可能重复），描述节点创建尝试结果。

节点组数据报告

节点组数据报告显示每个组的所有节点列表、可访问每个节点组的用户组、节点组定义规则（如适用）。报告显示详细节点列表，可以双击报告上的一行查看详细信息，也可以把报告保存成 CSV 文件。参看*把报告保存成文件* (p. 222)。

字节资产报告显示每个节点所属的节点组的列表。参看 *节点资产报告* (p. 230)。

生成节点组数据报告：

1. 选择 Reports（报告）> Users（用户）> Node Group Data（节点组数据）。
2. 双击一行显示节点组里的节点。

AD 用户组报告

AD 用户组报告显示从针对验证和授权配置的 AD 服务器上导入 CC-SG 的用户组里的所有用户。报告不包括在本地通过 CC-SG 添加到 AD 用户组的用户。

生成 AD 用户组报告：

1. 选择 Reports（报告）> Active Directory > AD Users Group Report（AD 用户组报告）。
2. AD Server（AD 服务器）列表包括在 CC-SG 上配置的用于验证和授权的所有 AD 服务器。选择报告要包括的每个 AD 服务器对应的复选框。
3. 在 AD User Groups（AD 用户组）部分，Available（可用）列表包括从你在 AD Server（AD 服务器）列表上选择的 AD 服务器导入 CC-SG 的所有用户组。选择报告要包括的用户组，然后单击 Add（添加）按钮把它移动到 Selected（选择）列表上。
4. 单击 Apply（应用）按钮生成报告。

预定报告

预定报告显示在任务管理器上预定的报告。可以在 Scheduled Reports（预定报告）屏幕上找到 Upgrade Device Firmware（升级设备固件）报告和 Restart Device（重新启动设备）报告。预定报告只能用 HTML 格式查看。参看*任务管理器* (p. 297)。

访问预定报告：

1. 选择 Reports（报告）> Scheduled Reports（预定报告）。
2. 选择一种 Report Type（报告类型）。
3. 选择一个 Report Owner（报告所有者）。
4. 在 Report Name（报告名称）字段里输入报告名称按名称过滤报告。可以输入完整名称，也可以只输入名称的一部分。匹配不区分大小写。不允许使用通配符。
5. 在 Start Date and Time（开始日期和时间）和 End Date and Time（结束日期和时间）字段里设置报告的日期范围。单击默认日期的每个部分（月、日、年、时、分、秒）选择它，然后单击上下箭头调节到希望的数字。
6. 单击 Apply（应用）按钮生成预定报告列表。

查看预定报告：

1. 在列表上选择报告。
2. 单击 View Report（查看报告）按钮。

注意：审计跟踪、错误日志和访问报告等人工生成的报告显示所有项，但根据预定任务生成的报告最多只显示 10,000 行。

删除预定报告：

1. 单击要删除的报告。按住 Ctrl 或 Shift 单击报告选择多个报告。
2. 单击 Delete Reports（删除报告）按钮。
3. 单击 Yes（是）按钮确认。

升级设备固件报告

Upgrade Device Firmware（升级设备固件）报告位于 Scheduled Reports（预定报告）列表上。在运行升级设备固件任务时，生成此报告。查看报告了解任务的实时状态信息。在任务完成之后，报告信息变为静态信息。

参看*预定报告* (p. 233)详细了解如何查看报告。

Ch 14 系统维护

在本章内

维护模式

维护模式限制 CC-SG 访问，使管理员能连续执行各种操作。例如更改闲置计时器或备份 CC-SG，就是最好在维护模式下执行的操作。这样可以确保针对所有用户更改闲置定时器等系统设置。

在可配置的时间到期之后，提示当前用户退出系统，进入维护模式的管理员除外。在维护模式下，其他管理员可以登录 CC-SG，但非管理员禁止登录。每当 CC-SG 进入或退出维护模式时，都生成一个 SNMP 陷阱。

注意 1：维护模式仅在独立 CC-SG 设备上可用，在群集配置下不可用。

注意 2：只有在进入维护模式之后，才能升级 CC-SG。

预定任务和维护模式

当 CC-SG 处于维护模式时，不能执行预定任务。参看***任务管理器*** (p. 297)。在 CC-SG 退出维护模式之后，尽快执行预定任务。

进入维护模式

1. 选择 System Maintenance（系统维护）> Maintenance Mode（维护模式）> Enter Maintenance Mode（进入维护模式）。

2. Password（密码）：输入密码。只有具备 CC 设置和控制权限的用户才能进入维护模式。
3. Broadcast message（广播消息）：输入给那些要退出 CC-SG 的用户显示的消息。
4. Enter maintenance mode after (min)（在此之后进入维护模式(分)）：输入 CC-SG 在进入维护模式之前要等待的分钟数 (0-720)。输入零立即进入维护模式。

   如果指定时间超过 10 分钟，立刻给用户显示广播消息，然后在发生事件之前每 10 分钟和 5 分钟重复显示一次。
5. 单击 OK（确定）按钮。
6. 单击确认对话框上的 OK（确定）按钮。

退出维护模式

1. 选择 System Maintenance（系统维护）> Maintenance Mode（维护模式）> Exit Maintenance Mode（退出维护模式）。
2. 单击 OK（确定）按钮退出维护模式。
3. 在 CC-SG 退出维护模式之后，显示一条消息。所有用户现在可以正常访问 CC-SG 了。

备份 CC-SG

最好先进入维护模式，再备份 CC-SG。进入维护模式可以保证在进行备份时，不更改数据库。

最多可以在 CC-SG 上存储 50 个备份文件。在存储 50 个备份文件之后，除非把 CC-SG 上的部分旧备份文件删除掉，否则不能再创建任何新备份文件。参看*保存和删除备份文件* (p. 238)。

在作为任务运行 CC-SG 备份时选择 Automatic Delete when Maximum Reached（在达到最大备份文件数时自动删除）复选框，在达到备份文件最大数时自动删除最旧的备份文件。只有在创建**备份 CC-SG** 任务时，才能使用此设置。在作为**备份 CC-SG** 任务的组成部分删除备份文件时，每个被删除的文件都在审计日志里有一条记录。参看*预定任务* (p. 299)。

备份 CC-SG：

1. 选择 System Maintenance（系统维护）> Backup（备份）。
2. 在 Backup Name（备份名称）字段里输入此备份的名称。
3. 在 Description（说明）字段里输入简短备份说明。**可选。**

4. 选择一种 Backup Type（备份类型）：Full（全）或 Standard（标准）。参看*全备份和标准备份有什么区别？* (p. 238)
5. 如果在 Administration（管理）> Tasks（任务）页上把此备份设置为任务，选择 Automatic Delete When Maximum Reached（在达到备份文件最大数时自动删除）复选框，让 CC-SG 在达到备份文件最大数时自动删除本地存储器存储的最旧的备份文件。在 Maximum Backup Files（备份文件最大数）字段里设置最大数。The default number is 50 backup files.**可选。**
6. 如要把此备份文件的副本保存到外部服务器上，选择 Backup to Remote Location（备份到远程位置）复选框。**可选。**
   a. 选择连接远程服务器所用的 Protocol（协议）：FTP 或 SFTP。
   b. 在 IP Address/Hostname（IP 地址/主机名）字段里输入服务器 IP 地址或主机名。支持 IPv6。
   c. 如果所选协议不使用默认端口 (FTP:21, SFTP: 22)，在 Port Number（端口号）字段里输入所用的通信端口。
   d. 在 Username（用户名）字段里输入远程服务器的用户名。
   e. 在 Password（密码）字段里输入远程服务器的密码。
   f. 在 Directory (Relative Path)（目录[相对路径]）字段里指定在远程服务器的哪个位置保存备份文件。
      - 此字段保留空白，把备份文件保存到 FTP 服务器上的默认 home 目录。
      - 输入至默认 home 目录的相对路径，把备份文件保存到 FTP 服务器上默认 home 目录下的子目录。例如如要把备份文件保存到默认 home 目录下的 Backups 文件夹，在 Directory (Relative Path)（目录[相对路径]）字段里输入 `Backups`。
   g. 在 Filename (leave blank to use the default filename convention)（文件名[保留空白使用默认文件名常规]）字段里输入在远程服务器上保存的备份文件的文件名，或者保留空白使用默认名称。默认名称包含 backup、日期和时间。
   h. 如果要把当前远程服务器设置另存为默认值，单击 Save As Default（另存为默认值）。显示一条确认消息。单击 OK（确定）按钮。**可选。**
7. 单击 OK（确定）按钮。

   在备份完成之后，显示一条消息。备份文件保存在 CC-SG 文件系统里，如果在 Backup to Remote Location（备份到远程位置）字段里指定了远程位置，同时保存到远程服务器上。日后可以恢复此备份文件。参看*恢复 **CC-SG*** (p. 239)。

重要说明：CC-SG 备份文件包括邻居配置，所以要在备份时记住或写下其

设置。在确定备份文件是否适合要恢复的 CC-SG 设备时，这非常有用。

全备份和标准备份有什么区别？

标准备份：

标准备份包括所有 CC-SG 页上所有字段里的所有数据，但不包括下列页上的数据：

- Administration（管理）> Configuration Manager（配置管理器）> Network（网络）选项卡
- Administration（管理）> Cluster Configuration（群集配置）

也不备份 CC-SG 存储的 CC-SG 备份文件。可以在 System Maintenance（系统维护）> Restore（恢复）页上查看 CC-SG 存储的备份文件列表。

同时，标准备份不包括字段里的临时数据，例如报告页上的日期范围。

全备份：

全备份包括标准备份中的所有数据，同时备份 CC-SG 固件文件、设备固件文件、应用程序文件和日志。应用程序文件包括 RRC、MPC、RC 和 VNC。

保存和删除备份文件

在 Restore CommandCenter（恢复 CommandCenter）屏幕上保存和删除 CC-SG 存储的备份文件。保存备份命令允许你在另一台 PC 上保存备份文件副本。可以创建备份文件档案。可以把保存在其他位置的备份文件上载到其他 CC-SG 设备上恢复，从而把一个 CC-SG 的配置复制到另一个 CC-SG 上。

删除不需要的备份文件，可以节省 CC-SG 空间。

保存备份文件

1. 选择 System Maintenance（系统维护）> Restore Command Center（恢复 Command Center）。
2. 在 Available Backups（可用备份）列表上选择要保存到 PC 上的备份文件。
3. 单击 Save to File（保存到文件）按钮打开 Save（保存）对话框。
4. 输入文件名，然后选择文件保存位置。
5. 单击 Save（保存）按钮把备份文件保存到指定位置。

删除备份文件

1. 在 Available Backups（可用备份）列表上选择要删除的备份文件。
2. 单击 Delete（删除）按钮打开确认对话框。
3. 单击 OK（确定）按钮把备份文件从 CC-SG 系统上删除掉。

恢复 CC-SG

可以用你创建的备份文件恢复 CC-SG。

重要说明：CC-SG 备份文件包括邻居配置，所以要在备份时记住或写下其设置。在确定备份文件是否适合要恢复的 CC-SG 设备时，这非常有用。

恢复 CC-SG：

1. 选择 System Maintenance（系统维护）> Restore（恢复），打开 Restore CommandCenter（恢复 CommandCenter）页，显示 CC-SG 可用的备份文件列表。可以看到备份类型、备份日期、说明、在哪个版本的 CC-SG 上备份的、备份文件大小。
2. 如果要用 CC-SG 系统之外的备份文件恢复系统，必须先把备份文件上载到 CC-SG。**可选。**
   a. 单击 Upload（上载）按钮。
   b. 在对话框上找到并选择备份文件。可以检索客户网络上任何地方的文件。
   c. 单击 Open（打开）按钮把此文件上载到 CC-SG。在上载完成之后，Available Backups（可用备份）表显示此备份文件。
3. 在 Available Backups（可用备份）表上选择要恢复的备份文件。
4. 必要时选择对此备份文件执行哪种恢复：
   - Standard（标准）— 只把关键数据恢复到 CC-SG 上，包括 CC-SG 配置信息、设备配置、节点配置和用户配置。参看*全备份和标准备份有什么区别？* (p. 238)
   - Full（全）— 恢复备份文件存储的所有数据、所有日志、所有固件文件、所有应用程序文件和所有许可文件。参看*全备份和标准备份有什么区别？* (p. 238)这要求备份文件是全备份文件。查看 Available Backups（可用备份）表的 Type（类型）列，看看可以使用哪些全备份文件。
   - Custom（定制）— 允许你在 Restore Options（恢复选项）区下面选择要把备份文件的哪些部分恢复到 CC-SG 上。选择下列每一项，把它包括在恢复中：

- Restore Data（恢复数据）— CC-SG 配置、设备配置、节点配置和用户数据。选择 Data（数据），恢复全备份文件的标准备份部分。参看*全备份和标准备份有什么区别？* (p. 238)
- Restore Logs（恢复日志）— CC-SG 存储的错误日志和事件报告。
- Restore CC firmware（恢复 CC 固件）— 存储的用于更新 CC-SG 服务器的固件文件。
- Restore firmware binaries（恢复固件二进制文件）— 存储的用于更新 CC-SG 管理的 Raritan 设备的固件文件。
- Restore Application（恢复应用程序）— 存储的供 CC-SG 用于把用户连接到节点的应用程序。
- Restore Licenses（恢复许可）— 访问 CC-SG 功能和节点所用的存储许可文件。参看 *可用许可* (p. 11)。

5. 在 Restore after (min.)（在此之后恢复[分]）字段里输入 CC-SG 在执行恢复操作之前要等待的分钟数 (0-60)。这样，用户有时间完成工作并退出系统。

   如果指定时间超过 10 分钟，立刻给用户显示广播消息，然后在发生事件之前每 10 分钟和 5 分钟重复显示一次。

6. 在 Broadcast Message（广播消息）字段里输入一条消息，通知其他 CC-SG 用户要执行恢复操作。

7. 单击 Restore（恢复）按钮。CC-SG 等待你指定的时间，然后用所选备份恢复配置。在开始恢复之后，其他所有用户退出系统。

   如果备份文件损坏了，显示一条消息，并把它写入审计跟踪。不能用损坏的备份文件恢复 CC-SG。

复位 CC-SG

可以复位 CC-SG 清除数据库，或者把其他部件复位到出厂默认设置。在使用任何复位选项之前，应该执行备份操作，把备份文件保存到另一个位置。

建议你使用所选的默认选项。

*注意：在复位 CC-SG 时，并不删除 CC-SG 设备保存的 CC-SG 备份文件。必须人工删除每个文件，才能把它从 CC-SG 上删除掉。参看*保存和删除备份文件 *(p. 238)*。

选项	Description（说明）
Full Database（全数据库）	此选项删除现有的 CC-SG 数据库，用出厂默认值创建一个新数据

选项	Description（说明）
	库。网络设置、SNMP 代理、固件和诊断控制台设置不是 CC-SG 数据库的组成部分。 复位 SNMP 配置和陷阱。不复位 SNMP 代理。 无论是否选择 IP ACL Tables（IP ACL 表）选项，在使用 Full Database Reset（全数据库复位）时，都复位 IP-ACL 设置。 复位 CC-SG 时删除邻居配置，所以 CC-SG 不再“记住”老邻居。 在删除数据库时，删除所有设备、节点和用户。删除所有远程验证和授权服务器。 CC 超级用户帐号复位到默认值。在复位操作完成之后，必须用默认用户名 admin 和默认密码 raritan 登录。
Save Personality Settings（保存个性化设置）	只有在选择 Full CC-SG Database Reset（全 CC-SG 数据库复位）之后，才能选择此选项。 在重构 CC-SG 数据库时，此选项保存此前配置的某些选项。 ▪ Enforce Strong Passwords（强制强密码）。 ▪ Direct vs. Proxy Connections to Out-of-Band nodes（带外节点直接连接和代理连接）。 ▪ Inactivity Timer setting（闲置计时器设置）。
Network Settings（网络配置）	此选项把网络设置复位到出厂默认值。 ▪ Host name（主机名）：CommandCenter ▪ Domain name（域名）：localdomain ▪ Mode（模式）：IP Failover（IP 故障切换） ▪ Configuration（配置）：Static（静态） ▪ IP Address（IP 地址）：192.168.0.192 ▪ Netmask（网络掩码）：255.255.255.0 ▪ Gateway（网关）：none（无） ▪ Primary DNS（主 DNS）：none（无） ▪ Secondary DNS（备用 DNS）：none（无） ▪ Adapter Speed（适配器速度）：Auto（自动）
SNMP Configuration（SNMP 配置）	此选项把 SNMP 设置复位到出厂默认值。 ▪ Port（端口）：161 ▪ Read-only Community（只读公用名）：public ▪ Read-write Community（读写公用名）：private ▪ System Contact, Name, Location（系统联系人、名称、位置）：none（无）

选项	Description（说明）
	▪ SNMP Trap Configuration（SNMP 陷阱配置） ▪ SNMP Trap Destinations（SNMP 陷阱目的地）
Default Firmware（默认固件）	此选项把所有设备固件文件复位到出厂默认值。此选项不更改 CC-SG 数据库。
Upload Firmware to Database After Reset（在复位后把固件上载到数据库）	此选项把当前 CC-SG 版本的固件文件加载到 CC-SG 数据库里。
Diagnostic Console（诊断控制台）	此选项把 Diagnostic Console（诊断控制台）设置复位到出厂默认值。
IP-ACL Tables（IP-ACL 表）	此选项删除 IP-ACL 表上的所有项。 无论是否选择 IP ACL Tables（IP ACL 表）选项，在使用 Full Database Reset（全数据库复位）时，都复位 IP-ACL 设置。
Licenses（许可）	此选项删除 CC-SG 上的所有许可文件。

复位 CC-SG：

1. 在复位之前备份 CC-SG，把备份文件保存到远程位置。参看***备份 CC-SG*** (p. 236)。
2. 选择 System Maintenance（系统维护）> Reset（复位）。
3. 选择复位选项。
4. 输入你的 CC-SG 密码。
5. Broadcast message（广播消息）：输入给那些要退出 CC-SG 的用户显示的消息。
6. 输入 CC-SG 在执行复位操作之前要等待的分钟数 (0-720)。

   如果指定时间超过 10 分钟，立刻给用户显示广播消息，然后在发生事件之前每 10 分钟和 5 分钟重复显示一次。
7. 单击 OK（确定）按钮显示一条消息确认复位。

在复位 CC-SG 时，切勿切断 CC-SG 电源，切勿给 CC-SG 重新通电，切勿中断 CC-SG，否则可能会丢失 CC-SG 数据。

重新启动 CC-SG

重新启动命令用于重新启动 CC-SG 软件。在重新启动 CC-SG 时，让所有活动用户退出 CC-SG。

在重新启动时，并不给 CC-SG 重新通电。如要执行完整的重新启动操作，必须使用 Diagnostic Console（诊断控制台）或 CC-SG 设备上的电源开关。

1. 选择 System Maintenance（系统维护）> Restart（重新启动）。
2. 在 Password（密码）字段里输入密码。
3. Broadcast message（广播消息）：使用默认消息，或者编辑默认消息。给那些要退出 CC-SG 的用户显示此消息。
4. Restart after (min)（在此之后重新启动(分钟)）：输入 CC-SG 在重新启动之前要等待的分钟数 (0-720)。

   如果指定时间超过 10 分钟，立刻给用户显示广播消息，然后在发生事件之前每 10 分钟和 5 分钟重复显示一次。
5. 单击 OK（确定）按钮重新启动 CC-SG。

升级 CC-SG

在发布新版固件时，可以升级 CC-SG 的固件。可以在 Raritan 网站的 Support（支持）部分找到固件文件。如要把 CC-SG 从 v3.x 升级到 v4.1，必须先把它升级到 v4.0。如要把 CC-SG 从 v4.x 升级到 v5.0 以上的任何版本，必须先把它升级到 v5.0。

CC-SG v4.0 或更高版本不兼容 G1 硬件，切勿把 CC-SG G1 设备升级到 v4.0 或更高版本。

把固件文件下载到客户 PC 上，然后进行升级。

只有具备 CC 设置和控制权限的用户才能升级 CC-SG。

应该在升级之前备份 CC-SG，把备份文件发送到 PC 上妥善保存。参看 ***备份 CC-SG*** (p. 236) 和***保存备份文件*** (p. 238)。

应该在升级之前检查 CC-SG 的磁盘状态。 See ***Check Disk Status*** (参看 "***检查磁盘状态***" p. 357).**如果有迹象表明必须更换驱动器或驱动器有问题，或者必须重构 RAID 阵列或阵列状态有问题，请在升级固件之前联系 Raritan 技术支持部门。**

如果使用 CC-SG 群集，必须在升级之前删除群集。单独升级每个 CC-SG 节点，然后重新创建群集。

重要说明：如果必须同时升级 CC-SG 和一台设备或一组设备，先升级 CC-SG，然后升级设备。

CC-SG 要重新启动，这是升级过程的组成部分。在升级过程中，切勿停止升级过程，切勿人工重新启动设备，切勿切断设备电源，切勿给设备重新通电。

升级 CC-SG：

1. 把固件文件下载到客户 PC。
2. 用具备 CC 设置和控制权限的帐号登录 CC-SG Admin Client。
3. 进入 Maintenance Mode（维护模式）。参看***进入维护模式*** (p. 235)。
4. 在 CC-SG 进入维护模式之后，选择 System Maintenance（系统维护）> Upgrade（升级）。
5. 单击 Browse（浏览）按钮找到并选择 CC-SG 固件文件 (.zip)，然后单击 Open（打开）按钮。
6. 单击 OK（确定）按钮把固件文件上载到 CC-SG。

在把固件文件上载到 CC-SG 之后，显示一条成功消息，说明 CC-SG 已开始升级过程。此时，所有用户断开 CC-SG 连接。

7. 必须等到升级完成，才能再次登录 CC-SG。可以通过 Diagnostic Console（诊断控制台）监视升级过程。
   a. 用管理员帐号访问 Diagnostic Console（诊断控制台）。参看***访问管理员控制台*** (p. 326)。
   b. 选择 Admin（管理）> System Logfile Viewer（系统日志文件查看器）。选择 sg/upgrade.log，然后选择 View（查看）查看升级日志。
   c. 等待升级过程运行。当你在 upgrade.log 里看到 Upgrade completed（升级完成）消息时，表示升级过程完成了。也可以等待 SNMP 陷阱 ccImageUpgradeResults 显示 success（成功）消息。
   d. 服务器必须重新启动。当你在 upgrade.log 里看到 Linux reboot（Linux 重新启动）消息时，表示开始重新启动。

   注意：对于从 CC-SG 3.x 升级到 4.0.x，系统重新启动两次，这是正常现象。

   ---

   e. 在系统重新启动之后大约两分钟，可以通过管理员帐号重新访问 Diagnostic Console（诊断控制台），并监视升级过程进度。**可选。**
8. 单击 OK（确定）按钮退出 CC-SG。
9. 清除浏览器高速缓存，然后关闭浏览器窗口。参看***清除浏览器高速缓存*** (p. 246)。
10. 清除 Java 高速缓存。参看***清除 Java 高速缓存*** (p. 246)。
11. 启动新浏览器窗口。
12. 用具备 CC 设置和控制权限的帐号登录 CC-SG Admin Client。
13. 选择 Help（帮助）> About Raritan Secure Gateway（关于 Raritan Secure Gateway），检查版本号确定升级是否成功。
    - 如果版本并没有升级，重复上面的步骤。
    - 如果升级成功，继续下一步。
14. 退出 Maintenance Mode（维护模式）。参看***退出维护模式*** (p. 236)。
15. 备份 CC-SG。参看***备份 CC-SG*** (p. 236)。

清除浏览器高速缓存

对于不同版本的浏览器，下列说明稍有不同。

清除 Internet Explorer 的浏览器高速缓存：

1. 单击 Tools（工具）> Internet Options（Internet 选项）。
2. 在 General（常规）选项卡上单击 Delete Files（删除文件）按钮，然后单击 OK（确定）按钮确认。

在 FireFox 2.0 和 3.0 上：

1. 选择 Tools（工具）> Clear Private Data（清除隐私数据）。
2. 确保选择 Cache（高速缓存），然后单击 Clear Private Data Now（现在清除隐私数据）。

清除 Java 高速缓存

对于不同版本的 Java 和不同的操作系统，下列说明稍有不同。

在安装了 Java 1.6 的 Windows XP 上：

1. 选择 Control Panel（控制面板）> Java。
2. 单击 General（常规）选项卡上的 Settings（设置）。
3. 在打开的对话框上单击 Delete Files（删除文件）。
4. 确保选择 Applications and Applets（应用程序和小程序）复选框，然后单击 OK（确定）按钮。

升级群集

根据下列建议步骤升级 CC-SG 群集。只有 CC-SG 物理设备能构成群集。

CC-SG 群集许可是一种特殊许可文件，供群集里的两台 CC-SG 设备共享。参看*群集许可* (p. 279)了解详情。

如果根据此步骤升级主节点失败，参看*主节点升级失败* (p. 247)。

升级群集：

1. 选择 Administration（管理）> Cluster Configuration（群集配置），强制从主节点切换到备用节点。单击 Configuration（配置）选项卡上的 Switch Primary and Backup（切换主节点和备用节点）。参看*切换主节点状态和备用节点状态* (p. 277)了解详情。
   - 备用节点变成主节点，此前的主节点进入等待状态。

2. 在新的主节点上选择 System Maintenance（系统维护）> Shutdown（关机）关闭 CC-SG 应用程序。
   - 在关闭 CC-SG 应用程序之后，设备仍然处于通电状态，仍然可以通过 Diagnostic Console（诊断控制台）访问。参看***关闭 CC-SG*** (p. 248) 了解详情。
3. 重新启动此前的、已进入等待状态的主节点。参看***用诊断控制台重新启动 CC-SG*** (p. 339) 详细了解如何重新启动。
   - 重新启动后的 CC-SG 设备再次进入主节点状态，已关闭的备用节点被视为处于失败状态。
4. 选择 Administration（管理）> Cluster Configuration（群集配置）删除群集，然后单击 Delete Cluster（删除群集）按钮。
5. 进入 Maintenance Mode（维护模式），然后升级主节点。参看***进入维护模式*** (p. 235)和***升级 CC-SG*** (p. 244)。
6. 如果主节点升级成功，选择 Diagnostic Console（诊断控制台），然后选择 Operation（操作）> Admin（管理）> Factory Reset（出厂复位）> Full CC-SG Database Reset（全 CC-SG 数据库复位）选项对备用节点执行出厂复位。参看***复位 CC-SG 出厂配置*** (p. 343)。
   - 如果主节点升级失败，参看***主节点升级失败*** (p. 247)。
7. 升级已复位的备用节点。参看***升级 CC-SG*** (p. 244)。
8. 重新创建群集。参看***创建群集*** (p. 276)。主节点的数据与备份节点同步。

主节点升级失败

如果根据***升级群集*** (p. 246)所述的步骤升级主节点失败，根据下列步骤完成群集升级。

1. 如果主节点升级失败，选择 System Maintenance（系统维护）> Shutdown（关机）关闭 CC-SG 应用程序。在关闭 CC-SG 应用程序之后，设备仍然处于通电状态，仍然可以通过 Diagnostic Console（诊断控制台）访问。参看***关闭 CC-SG*** (p. 248) 了解详情。
2. 重新启动备用节点。参看***用诊断控制台重新启动 CC-SG*** (p. 339) 详细了解如何重新启动。
3. 备用节点进入主节点状态。
4. 联系 Raritan 技术支持部门确定为什么升级失败。

迁移 CC-SG 数据库

如要用新的 CC-SG 物理设备取代旧设备，或者要从 CC-SG 物理设备迁移到 CC-SG 虚拟设备，要遵循下列建议步骤。

迁移要求

- 两台 CC-SG 设备必须运行相同版本的固件，且固件版本为 5.1 或更高版本。
- 必须拥有原 CC-SG 的有效许可，迁移后的 CC-SG 才能正常工作。

迁移 CC-SG 数据库

迁移 CC-SG 数据库：

1. 暂停管理所有设备。可选。如果使用 CC-SG v5.1 或更高版本固件，可以预订一个任务暂停所有设备。参看*预定任务* (p. 299)。
2. 对要迁移的 CC-SG 执行全备份。确保选择 Full（全复位）备份类型，把备份文件保存到远程位置。参看*备份 CC-SG* (p. 236)。
3. 在要迁移的 CC-SG 上选择 System Maintenance（系统维护）> Shutdown（关机）关闭 CC-SG 应用程序。
4. 在要迁移到的 CC-SG 上上载全备份文件，然后执行全恢复。确保选择 Full（全恢复）恢复类型。参看*恢复 CC-SG* (p. 239)。

   注意：要迁移到的 CC-SG 必须拥有有效许可才能正常工作。完成全恢复不需要有效许可。
5. 恢复管理所有设备。如果使用 CC-SG v5.1 或更高版本固件，可以预订一个任务恢复所有设备。参看*预定任务* (p. 299)。
6. 运行 Device Availability（设备可用性）报告查看网管设备的状态。参看*可用性报告* (p. 226)。
7. 在新的 CC-SG 成功运行之后，复位原 CC-SG 上的数据库，防止两个数据库同时上线造成冲突。访问 Diagnostic Console（诊断控制台），然后选择 Operation（操作）> Admin（管理）> Factory Reset（出厂复位）> Full CC-SG Database Reset（全 CC-SG 数据库复位）选项复位数据库。参看*复位 CC-SG 出厂配置* (p. 343)。

关闭 CC-SG

在关闭 CC-SG 时，只关闭 CC-SG 软件，不断开 CC-SG 设备电源。

在 CC-SG 关闭之后，所有用户退出系统。在通过 Diagnostic Console（诊断控制台）或给 CC-SG 重新通电来重新启动 CC-SG 之前，用户不能登录系统。

关闭 CC-SG：

1. 选择 System Maintenance（系统维护）> Shutdown（关机）。

2. 在 Password（密码）字段里输入密码。
3. 接受默认消息，或者在 Broadcast message（广播消息）字段里输入给所有当前在线用户显示的消息（例如可以给用户一点时间在 CC-SG 上完成任务，告诉他们系统何时恢复正常工作状态）。在关闭 CC-SG 时，断开所有用户。
4. 在 Shutdown after (min)（在此之后关机[分钟]）字段里输入 CC-SG 在执行关机操作之前要等待的分钟数 (0-720)。

   如果指定时间超过 10 分钟，立刻给用户显示广播消息，然后在发生事件之前每 10 分钟和 5 分钟重复显示一次。
5. 单击 OK（确定）按钮关闭 CC-SG。

关机后重新启动 CC-SG

在关闭 CC-SG 之后，用下列两种方法之一重新启动设备：

- 使用诊断控制台。参看***用诊断控制台重新启动 CC-SG*** (p. 339)。
- 给 CC-SG 设备重新通电。

断开 CC-SG 电源

如果 CC-SG 在运行时断电，它会记住上次的电源状态。在交流电源恢复供电之后，CC-SG 自动重新启动。但如果 CC-SG 在关机后断电，在交流电源恢复供电之后，它仍然处于关机状态。

重要说明：不要按 POWER（电源）按钮强制关闭 CC-SG。建议用诊断控制台的 CC-SG System Power OFF（CC-SG 系统关机）命令关闭 CC-SG。参看*在诊断控制台上关闭 CC-SG 系统* (p. 341)。

关闭 CC-SG：

1. 卸掉前盖，按住 POWER（电源）按钮。
2. 等待大约一分钟，CC-SG 正常关机。

   注意：在关闭 CC-SG 设备时，给通过诊断控制台登录 CC-SG 的用户显示一条很短的广播消息。在关闭 CC-SG 设备时，不给通过网络浏览器或 SSH 登录 CC-SG 的用户显示消息。
3. 如果必须拔掉交流电源线，先让关机过程结束，再拔掉电源线。这是让 CC-SG 完成所有事务、关闭数据库、让磁盘驱动器进入安全断电状态所必需的。

结束 CC-SG 会话

可以采用两种方法结束 CC-SG 会话。

- 退出系统结束会话，让客户机窗口处于打开状态。参看***退出 CC-SG*** (p. 250)。
- 退出系统结束会话，关闭客户机窗口。参看***退出 CC-SG*** (p. 250)。

退出 CC-SG

1. 选择 Secure Gateway（安全网关）> Logout（退出），打开 Logout（退出）窗口。
2. 单击 Yes（是）按钮退出 CC-SG。在退出系统之后，打开 CC-SG 登录窗口。

退出 CC-SG

1. 选择 Secure Gateway（安全网关）> Exit（退出）。
2. 单击 Yes（是）按钮退出 CC-SG。

Ch 15 高级管理

在本章内

配置当日消息

当日消息允许你输入一条消息，让所有用户在登录时看到。你必须具备 CC 设置和控制权限，才能配置当日消息。

配置当日消息：

1. 选择 Administration（管理）> Message of the Day Setup（当日消息设置）。
2. 如果要在所有用户登录之后给他们显示消息，选择 Display Message of the Day for All Users（给所有用户显示当日消息）。**可选。**
3. 如果要在 CC-SG 上输入消息，选择 Message of the Day Content（当日消息内容）复选框；如果要加载现有文件里的消息，选择 Message of the Day File（当日消息文件）复选框。
   - 如果选择 Message of the Day Content（当日消息内容）：
   a. 在显示的对话框上输入消息。

b. 单击 Font Name（字体名称）下拉菜单，然后选择消息显示字体。

c. 单击 Font Size（字体大小）下拉菜单，然后选择消息文本字体大小。

- 如果选择 Message of the Day File（当日消息文件）：

a. 单击 Bowse（浏览）按钮找到消息文件。

b. 在打开的对话框上选择文件，然后单击 Open（打开）按钮。

c. 单击 Preview（预览）按钮检查文件内容。

4. 单击 OK（确定）按钮保存更改。

配置访问节点所用的应用程序

关于访问节点所用的应用程序

CC-SG 提供多种应用程序供你访问节点。可以用 Application Manager（应用程序管理器）查看每种设备类型对应的应用程序，给每种设备类型添加新应用程序，删除每种设备类型的应用程序，给每种设备类型设置默认应用程序。

查看 CC-SG 提供的应用程序：

1. 选择 Administration（管理）> Applications（应用程序）。
2. 单击 Application name（应用程序名称）下拉菜单查看 CC-SG 提供的应用程序的列表。

检查和升级应用程序版本

检查和升级包括 Raritan Console (RC) 和 Raritan Remote Client (RRC) 在内的 CC-SG 应用程序。

检查应用程序版本：

1. 选择 Administration（管理）> Applications（应用程序）。
2. 在 Application（应用程序）列表上选择应用程序名称。注意 Version（版本）字段里的数字。某些应用程序不自动显示版本号。

升级应用程序：

如果应用程序不是最新版，必须升级应用程序。可以在 Raritan 网站上下载应用程序升级文件。如要了解支持的应用程序版本的完整列表，参看 Raritan 支持网站上的**兼容性指标**。

在升级 CC-SG 之前，最好进入 Maintenance Mode（维护模式）。参看 ***进入维护模式*** (p. 235)。

1. 把应用程序文件保存到客户 PC 上。
2. 单击 Application name（应用程序名称）下拉箭头，然后在列表上选择必须升级的应用程序。如果看不到要升级的应用程序，必须先添加此应用程序。参看***添加应用程序*** (p. 254)。
3. 单击 Browse（浏览）按钮在显示的对话框上选择应用程序，然后单击 Open（打开）按钮。
4. Application Manager（应用程序管理器）屏幕上的 New Application File（新应用程序文件）字段显示应用程序名称。
5. 单击 Upload（上载）按钮。进度窗口显示新应用程序上载进度。在上载完成之后打开一个新窗口，说明应用程序已被添加到 CC-SG 数据库里，可以使用了。
6. 如果 Version（版本）字段不自动更新版本号，在 Version（版本）字段里输入新版本号。对于某些应用程序，Version（版本）字段自动更新版本号。
7. 单击 Update（更新）按钮。

---

*注意：在升级过程中登录的用户必须先退出 CC-SG，然后再登录，确保启动新版应用程序。同时参看*在升级之后打开旧版应用程序 *(p. 253)*。

在升级之后打开旧版应用程序

如果你尝试用最新版应用程序建立连接，结果却打开旧版应用程序，应清除 Java 高速缓存。如果在升级 CC-SG 之后没有清除 Java 高速缓存，可能会发生这种情况。

参看***清除 Java 高速缓存*** (p. 246)。

添加应用程序

在把应用程序添加到 CC-SG 时，必须指定此应用程序适用于哪种设备类型。如果设备提供 KVM 访问和串行访问，设备列出两次，每次对应一种方法。

添加应用程序：

1. 选择 Administration（管理）> Applications（应用程序）。
2. 单击 Add（添加）按钮打开 Add Applications（添加应用程序）对话框。
3. 在 Application name（应用程序名称）字段里输入应用程序的名称。
4. 在 Available（可用）列表上选择此应用程序适用于哪些 Raritan 设备，然后单击 Add（添加）按钮把它添加到 Selected（选择）列表上。
   - 如要删除使用此应用程序的设备，在 Selected（选择）列表上选择此设备，然后单击 Remove（删除）按钮。
5. 单击 OK（确定）按钮打开 Open（打开）对话框。
6. 找到并选择应用程序文件（通常是 .jar 或 .cab 文件），然后单击 Open（打开）按钮。
7. 把选择的应用程序加载到 CC-SG 上。

删除应用程序

删除应用程序：

1. 选择 Administration（管理）> Applications（应用程序）。
2. 在 Application Name（应用程序名称）下拉菜单上选择一个应用程序。
3. 单击 Delete（删除）按钮打开确认对话框。
4. 单击 Yes（是）按钮删除应用程序。

使用 AKC 的前提

为了使用 AKC：

- 确保当前不阻止来自正在访问的设备的 IP 地址的 cookies。
- Windows Vista、Windows 7 和 Windows 2008 服务器用户应该确保正在访问的设备的 IP 地址位于浏览器的 Trusted Sites Zone（信任网站区域），在访问设备时不在 Protected Mode（保护模式）下。

启用 AKC 下载服务器证书验证

如果设备或 CC-SG 管理员启用了 Enable AKC Download Server Certificate Validation（启用 AKC 下载服务器证书验证）选项：

- 管理员必须把有效证书上载到设备上，或者在设备上生成自签名证书。证书必须有有效主机名。
- 每个用户必须把 CA 证书（或自签名证书）添加到浏览器的 Trusted Root CA 仓库。

在 CC-SG Admin Client 上启动 AKC 时，必须事先安装 JRE™ 1.6.0_10 或更高版本。

配置默认应用程序

关于默认应用程序

可以给每种设备类型指定希望 CC-SG 默认使用的应用程序。

查看指定的默认应用程序

查看指定的默认应用程序：

1. 选择 Administration（管理）> Applications（应用程序）。
2. 单击 Default Applications（默认应用程序）选项卡查看和编辑各种接口和端口类型对应的当前默认应用程序。在配置节点允许通过所选接口进行访问时，在此列出的应用程序变成默认选项。

给接口或端口类型设置默认应用程序

给接口或端口类型设置默认应用程序：

1. 选择 Administration（管理）> Applications（应用程序）。
2. 单击 Default Applications（默认应用程序）选项卡。
3. 选择要给哪个 Interface Type（接口类型）或 Port Type（端口类型）设置默认应用程序。

4. 双击此行上的 Application（应用程序）箭头。值变成下拉菜单。不能更改灰色值。
5. 选择在连接所选 Interface Type（接口类型）或 Port Type（端口类型）时使用的默认应用程序。
   - Auto-Detect（自动检测）：CC-SG 根据客户机浏览器自动检测合适的应用程序。
6. 单击 OK（确定）按钮保存更改。这些默认设置仅应用于新端口。如要把这些设置应用于现有设备的端口，单击 Apply Selections to Exisitng Devices（把选择应用于现有设备），然后选择要更改的设备并单击 OK（确定）按钮。

管理设备固件

CC-SG 存储 Raritan 设备固件，你可以用固件升级它管理的设备。用固件管理器把设备固件文件上载到 CC-SG 上，或者删除 CC-SG 上的设备固件文件。在上载固件文件之后，可以访问此文件，用它升级设备。参看 *升级设备* (p. 79)。

上载固件

可以把不同版本的设备固件上载到 CC-SG 上。当新固件版本可用时，会在 Raritan 网站上公布。

把固件上载到 CC-SG 上：

1. 选择 Administration（管理）> Firmware（固件）。
2. 单击 Add（添加）按钮添加新固件文件，打开搜索窗口。
3. 找到并选择要上载到 CC-SG 上的固件文件，然后单击 Open（打开）按钮。在上载完成之后，Firmware Name（固件名称）字段显示新固件。

删除固件

删除固件：

1. 选择 Administration（管理）> Firmware（固件）。
2. 单击 Firmware Name（固件名称）下拉箭头，然后选择要删除的固件。
3. 单击 Delete（删除）按钮显示一条确认消息。
4. 单击 Yes（是）按钮删除固件。

配置 CC-SG 网络

可以在配置管理器上配置 CC-SG 管理的网络的网络设置。

重要说明：如要更改一台已经是邻居成员的 CC-SG 设备的 IP 地址，必须先把它从邻居配置中删除掉，否则不能把 CC-SG 从邻居中删除掉。

关于网络设置

CC-SG 提供两种网络设置模式：

- IP Failover（IP 故障切换）模式：参看*什么是 IP 故障切换模式？* (p. 258)
- IP Isolation（IP 隔离）模式：参看*什么是 IP 隔离模式？* (p. 261)

重要说明：如果新部署设备，强烈建议使用 IP 故障切换模式。

CC-SG 还允许使用静态 IP 地址或 DHCP 分配的 IP 地址。参看*建议的 CC-SG DHCP 配置* (p. 263)了解在 CC-SG 上使用 DHCP 的最佳方式。

既可以在 IPv4 地址模式下使用 CC-SG，也可以在双协议堆模式下使用 CC-SG，后者同时使用 IPVv 地址和 IPv6 地址。

关于 CC-SG LAN 端口

CC-SG 提供两个主 LAN 端口：主 LAN 和备用 LAN。参看下表了解 CC-SG 型号上主 LAN 端口和备用 LAN 端口的位置。

V1 LAN 端口：

型号	主 LAN 名称	主 LAN 位置	备用 LAN 名称	备用 LAN 位置
V1-0 或 V1-1	LAN1	左边 LAN 端口	LAN2	右边 LAN 端口

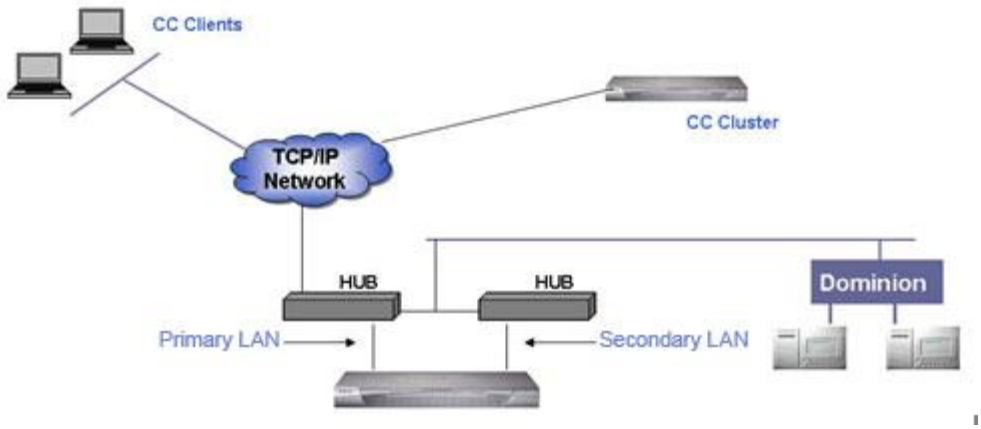
E1 LAN 端口：

型号	主 LAN 名称	主 LAN 位置	备用 LAN 名称	备用 LAN 位置
E1-0	无标记	设备背板中央两个端口中的上面一个 LAN 端口	无标记	设备背板中央两个端口中的下面一个 LAN 端口
E1-1	LAN1	左边 LAN 端口	LAN2	右边 LAN 端口

什么是 IP 故障切换模式？

IP 故障切换模式允许你用两个 CC-SG LAN 端口实现网络故障切换和冗余。在此模式下，每次只有一个 LAN 端口活动。

参看*关于 CC-SG LAN 端口* (p. 257)了解每个 CC-SG 型号上主 LAN 端口和备用 LAN 端口的位置。



如果连接主 LAN，且接收到 Link Integrity（链路完整性）信号，CC-SG 就用此 LAN 端口进行所有通信。如果主 LAN 没有接收到 Link Integrity（链路完整性）信号，且连接备用 LAN，CC-SG 就切换到给备用 LAN 分配的 IP 地址。将使用备用 LAN，直到主 LAN 恢复正常工作为止。当主 LAN 恢复正常工作时，CC-SG 自动切换到主 LAN。

在发生故障期间，只要有一个 LAN 连接可用，客户机应该感觉不到任何服务中断。

Setup for IP Failover Mode

IP 故障切换模式设置：

在 CC-SG 网络上实现 IP 故障切换模式时：

- 两个 CC-SG LAN 端口必须连接同一个 LAN 子网。
- 为了提高可靠性，可以把每个 LAN 端口连接到同一个子网上的不同交换机或集线器上。**可选。**

配置 IPv4 IP 故障切换模式或 IPv6 双协议堆模式

在 CC-SG 上配置 IP 故障切换模式：

1. 选择 Administration（管理）> Configuration（配置）。

2. 单击 Network Setup（网络设置）选项卡。
3. 选择 IP Failover（IP 故障切换）模式。
4. 在 Host name（主机名）字段里输入 CC-SG 主机名。参看*术语/缩写语* (参看 "*术语/缩略语*" p. 2)了解主机名规则。包括最高级域，例如 .com。最高级域必须是 2-6 个字符。
5. 如只使用 IPv4，填写 IPv4 部分的字段，切记不要选择 IPv6 复选框。如要使用双协议堆模式，选择 IPv6 复选框，然后填写 IPv4 部分和 IPv6 部分的字段。在 IPv4 和双协议堆模式之间来回切换时，CC-SG 要重新启动。系统提示你现在或稍后重新启动，而且必须输入密码、广播消息和重新启动时间。确认你要使用的任何服务不依赖要禁用的模式。
6. 在 IPv4 地址部分的 Configuration（配置）下拉列表上选择 DHCP 或 Static（静态）。

   DHCP：

   - 如果选择 DHCP，在保存此网络设置并重新启动 CC-SG 之后，自动填充 Primary DNS（主 DNS）、Secondary DNS（备用 DNS）、Domain Suffix（域后缀）、IP address（IP 地址）、Subnet mask（子网掩码）和 Default gateway（默认网关）字段（如果配置 DHCP 服务器提供这些信息）。
   - 如果 DNS 服务器接受动态更新，CC-SG 利用 DHCP 服务器提供的这些信息动态注册到 DNS 服务器。
   - 参看*建议的 CC-SG DHCP 配置* (p. 263)。

   Static（静态）：

   - 如果选择 Static（静态），在 Primary DNS（主 DNS）、Secondary DNS（备用 DNS）、Domain Suffix（域后缀）、IP address（IP 地址）、Subnet mask（子网掩码）和 Default gateway（默认网关）字段里输入相应的信息。
7. 如要在双协议堆模式下运行，填写 IPv6 部分的字段。如果跳过此步骤，只使用 IPv4。
   a. 选择 Enable IPv6（启用 IPv6）复选框。
   b. 在 Configuration（配置）下拉列表上选择 Router Discovery（路由器发现）或 Static（静态）。
8. 如果选择 Router Discovery（路由器发现），自动填充部分字段：Global/Unique Local IPv6 Address（全局/唯一本地 IPv6 地址）、Prefix Length（前缀长度）、Default Gateway IPv6 Address（默认网关 IPv6 地址）、Link-Local IPv6 Address（链路本地 IPv6 地址）和 Zone ID（域 ID）。

a. 如果选择 Static（静态），输入 Global/Unique Local IPv6 Address（全局/唯一本地 IPv6 地址）、Prefix Length（前缀长度）和 Default Gateway IPv6 Address（默认网关 IPv6 地址）。

9. 单击 Adapter Speed（适配器速度）下拉箭头，然后在列表上选择一个线路速度。确保你选择的线路速度与交换机的适配器端口设置相同。如果交换机使用 1Gbps 线路速度，选择 Auto（自动）。
10. 如果在 Adapter Speed（适配器速度）字段里选择了 Auto（自动），Adapter Mode（适配器模式）字段被禁用，自动选择 Full Duplex（全双工）。如果在 Adapter Speed（适配器速度）字段里选择的选项不是 Auto（自动），在 Adapter Mode（适配器模式）下拉列表上选择一种双工模式。
11. 单击 Update Configuration（更新配置）按钮保存更改。如果启用或禁用 IPv6，必须重新启动 CC-SG。其他所有更改要求重新启动 CC-SG。在 CC-SG 重新启动之前，更改不生效。
    - 如果现在要自动重新启动 CC-SG，单击 Reboot Now/Restart Now（现在重新启动）按钮。
    - 如果要稍后人工重新启动 CC-SG，单击 Reboot Later/Restart Later（稍后重新启动）按钮。参看***重新启动 CC-SG*** (p. 243)。CC-SG 在必要时重新启动。
        - 单击 Cancel（取消）按钮返回 Network Setup（网络设置）面板，不保存更改。如要保存更改，必须单击 Update Configuration（更新配置）按钮，然后选择一个重新启动选项。

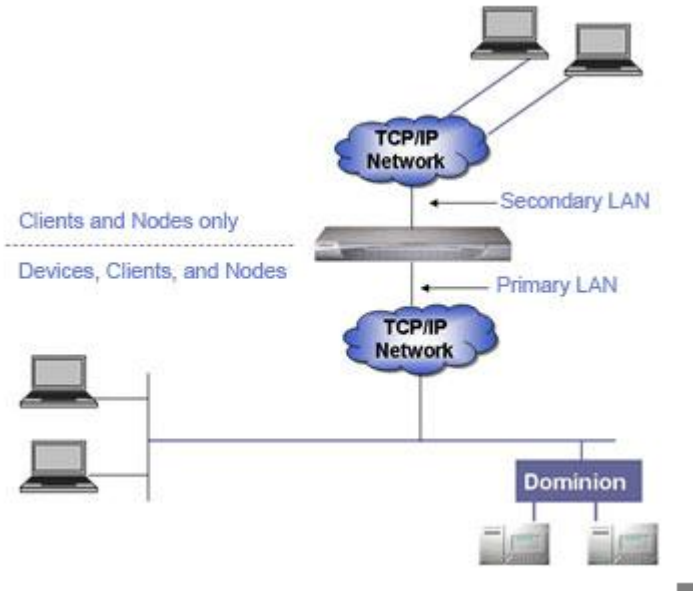
注意：如果给 CC-SG 配置了 DHCP，在成功注册到 DNS 服务器之后，可以通过主机名访问 CC-SG。

什么是 IP 隔离模式？

IP 隔离模式允许你把客户机和设备放在不同的子网上，把它们隔离开，强制客户机通过 CC-SG 访问这些设备。在此模式下，CC-SG 管理两个独立 IP 域之间的流量。IP 隔离模式不具备故障切换功能。如果任一个 LAN 连接失败，用户就无法访问设备。

参看*关于 CC-SG LAN 端口* (p. 257)了解每个 CC-SG 型号上主 LAN 端口和备用 LAN 端口的位置。

注意：在使用 IP 隔离模式时，不能配置群集。



Setup for IP Isolation Mode

IP 隔离模式设置：

在 CC-SG 网络上实现 IP 隔离模式时：

- 每个 CC-SG LAN 端口必须连接不同的子网。
- Raritan 设备只能连接主 LAN。
- 要隔离的客户机连接备用 LAN。不需要隔离的客户机可以连接主 LAN。参看*配置直接模式和代理模式组合* (p. 268)。

  注意：备用 LAN 上的隔离客户机将使用代理模式。主 LAN 上的客户机可以使用直接模式。把连接模式设置为 Both（二者），配置此组合模式。

- 在 CC-SG 的 Network Setup（网络设置）面板上指定至多一个默认网关。必要时用诊断控制台添加更多静态路由。参看*编辑静态路由* (p. 334)。

配置 IPv4 IP 隔离模式或 IPv6 双协议堆模式

▶ **在 CC-SG 上配置 IP 隔离模式：**

1. 选择 Administration（管理）> Configuration（配置）。
2. 单击 Network Setup（网络设置）选项卡。
3. 在 Host name（主机名）字段里输入 CC-SG 主机名。参看*术语/缩写语* (参看 "*术语/缩略语*" p. 2)了解主机名规则。如果配置了 DNS 和域后缀，在单击 Update Configuration（更新配置）按钮保存配置时，也更新 Host name（主机名）字段，显示全限定域名。
4. 如只使用 IPv4，填写 IPv4 部分的字段，切记不要选择 IPv6 复选框。如要使用双协议堆模式，选择 IPv6 复选框，然后填写 IPv4 部分和 IPv6 部分的字段。在 IPv4 和双协议堆模式之间来回切换时，CC-SG 要重新启动。系统提示你现在或稍后重新启动，而且必须输入密码、广播消息和重新启动时间。确认你要使用的任何服务不依赖要禁用的模式。
5. 选择 IP Isolation（IP 隔离）模式。
6. 在左栏上配置主 LAN，在右栏上配置备用 LAN。
7. 在 IPv4 配置部分的 Configuration（配置）下拉列表上选择 DHCP 或 Static（静态）。

   DHCP：

   - 如果选择 DHCP，在保存此网络设置并重新启动 CC-SG 之后，自动填充 Primary DNS（主 DNS）、Secondary DNS（备用 DNS）、Domain Suffix（域后缀）、IP address（IP 地址）、Subnet mask（子网掩码）和 Default gateway（默认网关）字段（如果配置 DHCP 服务器提供这些信息）。
   - 如果 DNS 服务器接受动态更新，CC-SG 利用 DHCP 服务器提供的这些信息动态注册到 DNS 服务器。
   - 参看*建议的 CC-SG DHCP 配置* (p. 263)。

   Static（静态）：

   - 如果选择 Static（静态），在 Primary DNS（主 DNS）、Secondary DNS（备用 DNS）、Domain Suffix（域后缀）、IP address（IP 地址）和 Subnet mask（子网掩码）字段里输入相应的信息。
   - 只指定一个默认网关，而不是两个。

8. 如要在双协议堆模式下运行，填写 IPv6 部分的字段。如果跳过此步骤，只使用 IPv4。
   a. 选择 Enable IPv6（启用 IPv6）复选框。
   b. 在 Configuration（配置）下拉列表上选择 Router Discovery（路由器发现）或 Static（静态）。
9. 如果选择 Router Discovery（路由器发现），自动填充部分字段：Global/Unique Local IPv6 Address(全局/唯一本地 IPv6 地址）、Prefix Length（前缀长度）、Default Gateway IPv6 Address（默认网关 IPv6 地址）、Link-Local IPv6 Address(链路本地 IPv6 地址)和 Zone ID（域 ID）。
10. 如果选择 Static（静态），输入 Global/Unique Local IPv6 Address（全局/唯一本地 IPv6 地址）、Prefix Length(前缀长度)和 Default Gateway IPv6 Address（默认网关 IPv6 地址）。
11. 单击 Adapter Speed（适配器速度）下拉箭头，然后在列表上选择一个线路速度。确保你选择的线路速度与交换机的适配器端口设置相同。如果交换机使用 1Gbps 线路速度，选择 Auto（自动）。
12. 如果在 Adapter Speed（适配器速度）字段里选择了 Auto（自动），Adapter Mode（适配器模式）字段被禁用，自动选择 Full Duplex（全双工）。如果在 Adapter Speed（适配器速度）字段里选择的选项不是 Auto（自动），单击 Adapter Mode（适配器模式）下拉箭头，然后在列表上选择一种双工模式。
13. 单击 Update Configuration（更新配置）按钮保存更改。 CC-SG reboots.

建议的 CC-SG DHCP 配置

检查下列建议的 DHCP 配置。确保 DHCP 服务器设置正确，才能配置 CC-SG 使用 DHCP。

- 配置 DHCP 给 CC-SG 静态分配 IP 地址。
- 配置当 DHCP 给 CC-SG 分配 IP 地址时，DHCP 和 DNS 服务器自动把 CC-SG 注册到 DNS。
- 配置 DNS 接受来自 CC-SG 的未验证动态域名系统 (DDNS) 注册请求。

IPv6 支持

在 CC-SG 上输入 IPv6 地址时，可以使用压缩格式和零压缩表示法。CC-SG 在存储和显示 IPv6 地址时展开此地址。

不支持利用 IPv6 进行下列通信。

- DHCPv6
- 群集
- 网络邻居
- 手机号码
- KX2 2.5 或更高版本的 OOB-KVM 接口只支持 IPv4
- OOB-串行接口
- IPMI 支持，例如对于 PX1 PDU
- SSH、Telnet、Web、VNC、MS-RDP 和 iDRAC6 之外的带内接口
- Power IQ
- 通过 SSH 访问 CC-SG
- 许可服务器
- 系统级访问控制表

把 CC-SG 主机名注册到 DNS 里的 IP 地址

如果在网络内配置 CC-SG，且 DNS 服务器可用，CC-SG 自动在 DNS 里添加一项把 CC-SG 主机名解析成配置的静态 IP。

如果在网络外配置 CC-SG，或者不允许更新 DNS 服务器，应该在 DNS 里人工添加一项反映此信息。

配置日志活动

可以配置 CC-SG 向外部日志服务器报告，指定在每个日志里报告的消息级别。

配置 CC-SG 日志活动：

1. 选择 Administration（管理）> Configuration（配置）。
2. 单击 Logs（日志）选项卡。
3. 如要指定 CC-SG 使用外部日志服务器，在 Primary Server（主服务器）下面的 Server Address（服务器地址）字段里输入 IP 地址。

4. 单击 Level to Forward（转发级别）下拉箭头，然后选择一个事件严重性级别。此级别或更高级别的所有事件将被发送到日志服务器上。参看 *日志严重级别示例* (p. 266)。
5. 如要配置外部备用日志服务器，重复第三步第四步，填写 Secondary Server（备用服务器）下面的字段。
6. 在 CommandCenter Log（CommandCenter 日志）下面，单击 Level to Forward（转发级别）下拉菜单，然后选择一个严重性级别。此级别或更高级别的所有事件将记录在 CC-SG 自己的内部日志里。
7. 单击 Update Configuration（更新配置）按钮保存更改。

清除 CC-SG 内部日志

可以清除 CC-SG 内部日志。此操作不删除在外部日志服务器上记录的任何事件。

注意：审计跟踪报告和错误日志报告建立在 CC-SG 内部日志之上。如果清除 CC-SG 内部日志，同时清除这两个报告。也可以逐个清除这两个报告。参看 **清除 CC-SG 上的报告数据** *(p. 223)*。

▶ **清除 CC-SG 内部日志：**

1. 选择 Administration（管理）> Configuration（配置）。
2. 单击 Logs（日志）选项卡。
3. 单击 Purge（清除）按钮。
4. 单击 Yes（是）按钮。

日志严重级别示例

你选择的严重级别决定要把哪几类事件转发到系统日志。

- OFF（关）

在设置为关时，不把任何事件转发到系统日志。

- FATAL（致命）

导致执行停止的内部故障，例如磁盘故障、两个硬盘被拆除或网络连接断开。

- ERROR（错误）

用错误用户名和密码登录。

- WARN（警告）

用现有名称添加用户或设备。

- INFO（信息）

添加或删除用户、设备等。

- DEBUG（调试）

成功登录和退出，以及用错误用户名和密码登录。

配置 CC-SG 服务器时间和日期

必须准确维护 CC-SG 的时间和日期，从而提高设备管理功能的可信度。

重要说明 :在任务管理器上预定任务时，要使用 Time/Date configuration（时间/日期配置）。参看*任务管理器* (p. 297)。在客户 PC 上设置的时间可能不同于在 CC-SG 上设置的时间。

只有 CC 超级用户和拥有类似权限的用户才能配置时间和日期。

在群集配置下，禁止更改时区。

配置 CC-SG 服务器时间和日期：

1. 选择 Administration（管理）> Configuration（配置）。
2. 单击 Time/Date（时间/日期）选项卡。
   a. 人工设置日期和时间：
   - Date（日期）— 单击下拉箭头选择 Month（月），用上下箭头选择 Year（年），然后在日历表上选择 Day（日）。

- Time（时间）— 用上下箭头设置 Hour（时、Minutes（分）和 Seconds（秒），然后单击 Time zone（时区）下拉箭头选择 CC-SG 所在的时区。

a. 通过 NTP 设置日期和时间：选择窗口底部的 Enable Network Time Protocol（启用网络时间协议）复选框，然后在 Primary NTP server（主 NTP 服务器）和 Secondary NTP server（备用 NTP 服务器）字段里输入相应的 IP 地址。

注意：网络时间协议 (Network Time Protocol, NTP) 是使相连计算机的日期数据和时间数据与 NTP 基准服务器的数据实现同步所用的协议。在用给 CC-SG 配置 NTP 之后，可以使 CC-SG 的时钟时间与公共 NTP 基准服务器同步，维持正确一致的时间。

3. 单击 Update Configuration（更新配置）按钮把时间和日期更改应用于 CC-SG。
4. 单击 Refresh（刷新）按钮，Current Time（当前时间）字段重新加载新服务器时间。
5. 选择 System Maintenance（系统维护）> Restart（重新启动），重新启动 CC-SG。

连接模式：直接和代理

关于连接模式

CC-SG 给带内连接和带外连接提供三种连接模式：Direct（直连）、Proxy（代理）和 Both（二者）。

- 直连模式允许你直接连接节点或端口，不通过 CC-SG 传输数据。直连模式通常提供较快的连接。
- 代理模式允许你连接节点或端口，通过 CC-SG 传输所有数据。代理模式增加了 CC-SG 服务器的负荷，可能会导致连接速度下降。但如果你更关心连接安全，建议你使用代理模式。必须在防火墙上开放 CC-SG TCP 端口 80、8080、443 和 2400。

注意：从 CC-SG 4.2 开始，在使用 Dominion KXII 2.1.10 或更高版本时，代理模式支持 KVM 数据加密。在此配置下，根据 KXII 设备上的安全设置加密 KVM 数据。Dominion KXII 2.1.10 之外的其他设备不支持加密。

- 二者模式允许你配置 CC-SG 同时使用直连模式和代理模式。在二者模式下，代理模式是默认模式，但如果用指定范围内的客户机 IP 地址建立连接，可以配置 CC-SG 使用直连模式。

注意：即使你配置 CC-SG 使用代理模式，某些接口也只能在直连模式下工作。这些接口包括 ILO、RSA、Microsoft RDP、DRAC、网络浏览器

和 VMware Viewer。Java RDP 接口可以在代理模式下使用。 参看*关于接口* (p. 100)。

给所有客户机连接配置直接模式

▶ **给所有客户机连接配置直接模式：**

1. 选择 Administration（管理）> Configuration（配置）。
2. 单击 Connection Mode（连接模式）选项卡。
3. 选择 Direct（直接）模式。
4. 单击 Update Configuration（更新配置）按钮。

给所有客户机连接配置代理模式

▶ **给所有客户机连接配置代理模式：**

1. 选择 Administration（管理）> Configuration（配置）。
2. 单击 Connection Mode（连接模式）选项卡。
3. 选择 Proxy（代理）模式。
4. 单击 Update Configuration（更新配置）按钮。

配置直接模式和代理模式组合

在配置 CC-SG 使用直接模式和代理模式组合时，代理模式是默认连接模式，直接模式用于你指定的客户机 IP 地址。

▶ **配置直接模式和代理模式组合：**

1. 选择 Administration（管理）> Configuration（配置）。
2. 单击 Connection Mode（连接模式）选项卡。
3. 选择 Both（二者）。
4. 在 Address（地址）字段里输入 IPv4 地址或 IPv6 地址，然后在 Prefix Length（前缀长度）字段里指定应通过直接模式连接节点和端口的地址范围。IPv4 地址的前缀长度为 1-32，IPv6 地址的前缀长度为 1-128。
5. 单击 Add（添加）按钮。
6. 单击 Update Configuration（更新配置）按钮。

设备设置

可以配置某些应用于所有设备的设置，配置每种设备类型的默认端口号。

配置设备默认端口号：

1. 选择 Administration（管理）> Configuration（配置）。
2. 单击 Device Settings（设备设置）选项卡。
3. 在表上选择一个设备类型，然后双击 Default Port（默认端口）值。
4. 输入新默认端口值。
5. 单击 Update Configuration（更新配置）按钮保存更改。

配置设备超时持续时间：

1. 选择 Administration（管理）> Configuration（配置）。
2. 单击 Device Settings（设备设置）选项卡。
3. 在 Heartbeat (sec)（检测信号[秒]）字段里输入新超时持续时间。有效范围是 30-50,000 秒。
4. 单击 Update Configuration（更新配置）按钮保存更改。

启用或禁用所有电源操作警告消息：

选择 Display Warning Message For All Power Operations（显示所有电源操作警告消息）复选框启用警告消息，在执行请求的电源操作之前提示用户。只有发出电源操作的用户能看到此消息。用户可以单击消息上的 Yes（是）按钮确认电源操作，或者单击 No（否）按钮取消电源操作。

1. 选择 Administration（管理）> Configuration（配置）。
2. 单击 Device Settings（设备设置）选项卡。
3. 选择 Display Warning Message For All Power Operations（显示所有电源操作警告消息）复选框启用警告消息。取消此复选框禁用警告消息。
4. 单击 Update Configuration（更新配置）按钮保存更改。

启用 AKC 下载服务器证书验证

如果使用 AKC 客户机，可以选择使用 Enable AKC Download Server Certificate Validation（启用 AKC 下载服务器证书验证）功能，也可以选择不使用此功能。

注意：在 IPv4 和 IPv6 双协议堆模式下使用 Enable AKC Download Server Certificate Validation（启用 AKC 下载服务器证书验证）功能时，Microsoft® ClickOnce® 要求服务器证书 CN 不包含零压缩格式的 IPv6 地址。如果服务器证书 CN 包含零压缩格式的 IPv6 地址，不能成功下载并启动 AKC。但对于此格式的 IPv6 地址，这可能会与浏览器性能发生冲突。在公用名 (CN) 中使用服务器主机名，或者在证书的 Subject Alternative Name（主题别名）中包括压缩格式或非压缩格式的 IPv6 地址。

选项 1：不启用 AKC 下载服务器证书验证，默认设置

如果不启用 AKC 下载服务器证书验证： 所有 Dominion 设备用户和 CC-SG Bookmark and Access Client 用户必须：

- 确保当前不阻止来自正在访问的设备的 IP 地址的 cookies。
- Windows Vista、Windows 7 和 Windows 2008 服务器用户应该确保正在访问的设备的 IP 地址位于浏览器的 Trusted Sites Zone（信任网站区域），在访问设备时不在 Protected Mode（保护模式）下。

选项 2：启用 AKC 下载服务器证书验证

如果启用 AKC 下载服务器证书验证：

- 管理员必须把有效证书上载到设备上，或者在设备上生成自签名证书。证书必须有有效主机名。
- 每个用户必须把 CA 证书（或自签名证书）添加到浏览器的 Trusted Root CA 仓库。

在使用 Windows Vista® 操作系统和 Windows 7® 操作系统时安装自签名证书：

1. 把 CommandCenter Secure Gateway IP 地址加入信任网站区域，确保关闭保护模式。
2. 启动 Internet Explorer®，把 CommandCenter Secure Gateway IP 地址用作 URL。显示证书错误消息。
3. 选择“查看证书”。
4. 单击“常规”选项卡上的“安装证书”，然后把证书安装在“信任根 CA”仓库里。
5. 在安装证书之后，应该把 CommandCenter Secure Gateway IP 地址从信任网站区域删除掉。

启用 AKC 下载服务器证书验证：

1. 选择 Device Settings（设备设置）> Device Services（设备服务），打开 Device Service Settings（设备服务设置）页。
2. 选择“启用 AKC 下载服务器证书验证”复选框，也可以继续禁用此功能（默认）。
3. 单击“确定”按钮。

配置定制 JRE 设置

当用户尝试访问 CC-SG 但其 JRE 版本不符合你指定的最低版本要求时，CC-SG 显示一条警告消息。参看**兼容性指标**了解支持的最低 JRE 版本。选择 Administration（管理）> Compatibility Matrix（兼容性指标）。

如果尝试登录 CC-SG 的用户没有安装指定版本的 JRE，就打开 JRE Incompatibility Warning（JRE 不兼容警告）窗口。窗口上有几个选项，可以下载默认的最低版本 JRE。你可以更改消息，以便包括任何文本和下载链接选项。用户可以下载新版 JRE，也可以继续用当前安全的 JRE 访问 CC-SG。

启用或禁用登录定制 JRE：

1. 在启用或禁用此功能之前，备份 CC-SG，把备份文件保存到远程位置。参看*备份 **CC-SG*** (p. 236)。
2. 选择 Administration（管理）> Configuration（配置）。
3. 然后单击 Custom JRE（定制 JRE）选项卡。
4. 选择 Enable Custom JRE for Login（启用登录定制 JRE）复选框启用此选项。取消此复选框禁用此选项。
5. 在 Require Minimum JRE（要求的最低 JRE 版本）字段里输入要求的最低 JRE 版本。必须输入完整版本号，版本号至少由三部分组成。例如 1.6.0 是正确的版本号。1.6 是错误版本号。对于 JRE "Update" 版本，用下划线表示。例如 1.6.0_5 是 JRE v1.6.0 Update 5 的正确版本号。
6. 单击 Update（更新）按钮。

定制 JRE Incompatibility Warning（JRE 不兼容警告）窗口显示的消息：

1. 选择 Administration（管理）> Configuration（配置）。
2. 然后单击 Custom JRE（定制 JRE）选项卡。
3. 利用 HTML 代码，输入 JRE Incompatibility Warning（JRE 不兼容警告）窗口显示的消息。

4. 单击 Update（更新）按钮。

恢复默认消息和最低 JRE 版本：

1. 选择 Administration（管理）> Configuration（配置）。
2. 然后单击 Custom JRE（定制 JRE）选项卡。
3. 单击 Restore Default（恢复默认值）。
4. 单击 Update（更新）按钮。

清除默认消息和最低 JRE 版本：

1. 选择 Administration（管理）> Configuration（配置）。然后单击 Custom JRE（定制 JRE）选项卡。
2. 单击 Clear（清除）按钮。

配置 SNMP

Simple Network Management Protocol 允许 CC-SG 把 SNMP 陷阱（事件通知）推送到网络上的现有 SNMP 管理器上。你应该接受 SNMP 基础设施培训，才能配置 CC-SG 使用 SNMP。

CC-SG 还支持与 HP OpenView 等第三方解决方案一起执行 SNMP GET/SET 操作。为了支持这些操作，你必须提供 SNMP 代理标识符信息，例如下列 MIB-II System Group 对象：sysContact、sysName 和 sysLocation。这些标识符提供有关网管节点的联系人信息、管理信息和位置信息。参看 RFC 1213 了解详情。

可以启用 SNMP v3，允许根据 User-based Security Model（基于用户的安全模型）和 View-based Access Control Model（基于视图的访问控制模型）进行加密。CC-SG 支持 SNMP v3 陷阱。

配置 SNMP 代理

可以设置的代理数没有限制。

在 CC-SG 上配置 SNMP 代理：

1. 选择 Administration（管理）> Configuration（配置）。
2. 单击 SNMP 选项卡。
3. 在 Listening Port（监听端口）字段里输入 SNMP 代理的端口号。默认端口是 161。
4. 如要启用 SNMP v1/v2 代理，选择 Enable SNMP v1/v2（启用 SNMP v1/v2）复选框。

a. 输入只读公用串。默认值是 public。

b. 输入读写公用串。默认值是 private。

c. 如要输入多个公用串，用逗号把它们分隔开。

5. 如要启用 SNMP v3 代理，选择 Enable SNMP v3（启用 SNMP v3）复选框。

a. 单击复选框下面表里的 Add a row（添加一行）图标  。 显示一行字段，填写所有五个字段。

b. 在 Security Name（安全名称）字段里输入 SNMP 管理器用户名。安全名称长度为 1-32 个字符。

c. 在 Authentication Protocol（验证协议）下拉列表上选择 MD5 或 SHA。

d. 在 Authentication Password（验证密码）字段里输入验证密码。密码长度为 8-64 个字符。为了实现最高安全，验证密码不应与隐私密码相同。如果两个密码相同，某些 MIB 浏览器不能正常工作。

e. 在 Privacy Protocol（隐私协议）下拉列表上选择 None（无）、DES 或 AES。

f. 在 Privacy Passphrase（隐私密码）字段里输入隐私密码。密码长度为 8-64 个字符。为了实现最高安全，验证密码不应与隐私密码相同。如果两个密码相同，某些 MIB 浏览器不能正常工作。

6. 在 System Contact（系统联系人）、System Name（系统名称）和 System Location（系统位置）字段里输入有关网管节点的信息。

7. 单击 Update Agent Configuration（更新代理配置）按钮保存更改。

用 Raritan MIB 文件更新 SNMP 代理

由于 CC-SG 推送自己的一组 Raritan 陷阱，所以必须用（包含 Raritan SNMP 陷阱定义的）定制 MIB 文件更新所有 SNMP 管理器。参看 ***SNMP 陷阱*** (p. 392)。可以在 Raritan 支持网站上找到 MIB 定制文件。

配置 SNMP 陷阱和通知

配置 SNMP 陷阱和通知：

1. 选择 Administration（管理）> Configuration（配置）。

2. 单击 SNMP 选项卡。

3. 在 SNMP 选项卡上确认是否在 Agents（代理）选项卡上配置了代理。单击 Traps（陷阱）选项卡。

4. 选择 Enable SNMP Traps（启用 SNMP 陷阱）复选框，允许把 SNMP v1/v2c 陷阱从 CC-SG 发送到 SNMP 主机。如果只想设置 SNMP v3 陷阱，跳过此步骤到第六步。

5. 单击复选框下面表里的 Add a row（添加一行）图标  。 显示一行字段，填写所有四个字段。

   a. 在 Host（主机）字段里输入陷阱目的地主机 IP 地址。

   b. 在 Port（端口）字段里输入 SNMP 主机使用的陷阱目的地主机端口号。默认端口是 162。

   c. 在 Version（版本）下拉列表上选择 v2 或 v1。

   d. 在 Community（公用名）字段里输入 SNMP 主机使用的公用串。

6. 选择 Enable SNMP v3 Notifications（启用 SNMP v3 通知）复选框，允许把 SNMP v3 通知从 CC-SG 发送到 SNMP 主机。如果只想设置 SNMP v1/v2c 陷阱，跳过此步骤，确保填写第四步和第五步，然后继续第七步。

   a. 单击复选框下面表里的 Add a row（添加一行）图标  。 显示一行字段，填写所有六个字段。

   b. 在 Host（主机）字段里输入陷阱目的地主机 IP 地址。

   c. 在 Port（端口）字段里输入 SNMP 主机使用的陷阱目的地主机端口号。默认端口是 162。

   d. 在 Security Name（安全名称）字段里输入 SNMP 管理器用户名。安全名称长度为 1-32 个字符。

   e. 在 Authentication Protocol（验证协议）下拉列表上选择 MD5 或 SHA。

   f. 在 Authentication Password（验证密码）字段里输入验证密码。密码长度为 8-64 个字符。为了实现最高安全，验证密码不应与隐私密码相同。如果两个密码相同，某些 MIB 浏览器不能正常工作。

   g. 在 Privacy Protocol（隐私协议）下拉列表上选择 None（无）、DES 或 AES。

   h. 在 Privacy Passphrase（隐私密码）字段里输入隐私密码。密码长度为 8-64 个字符。为了实现最高安全，验证密码不应与隐私密码相同。如果两个密码相同，某些 MIB 浏览器不能正常工作。

7. 在页面下半部的 Trap Sources（陷阱源）列表上选择想要 CC-SG 推送到 SNMP 主机的陷阱对应的复选框。陷阱分为两类：系统日志陷阱包括 CC-SG 设备本身的状态通知，例如硬盘故障；应用程序日志陷阱包括 CC-SG 应用程序事件通知，例如用户帐号更改。

a. 如要按类型启用陷阱，选择 System Log（系统日志）复选框和 Application Log（应用程序日志）复选框。

b. 选择各个陷阱对应的复选框启用各个陷阱。

c. 参看 MIB 文件了解提供的 SNMP 陷阱的列表。参看 ***SNMP 陷阱*** (p. 392)了解详情。

8. 单击 Update Trap Configuration（更新陷阱配置）按钮保存更改。

配置 CC-SG 群集

一个 CC-SG 群集使用两个 CC-SG 节点，其中一个是主节点，另一个是备用节点，在主节点发生故障时使用备份节点加强安全。两个节点共享活动用户和活动连接的数据，在两个节点之间复制所有状态数据。

CC-SG 群集中的设备必须知道主 CC-SG 节点的 IP，才能向主节点通知状态改变事件。如果主节点发生故障，备用节点立即承担主节点的所有功能。这要求初始化 CC-SG 应用程序和用户会话，在主 CC-SG 节点上发起的所有当前会话将会终止。与主节点相连的设备将确认主节点不再响应，于是响应备用节点发出的请求。

注意：在用胖客户机访问 CC-SG 时，如果主节点发生故障，不自动重定向到备用节点。必须人工输入备用节点的 IP 地址，胖客户机才能访问备用节点。

CC-SG 群集要求

- 群集里的主节点和备用节点必须在相同版本的硬件（V1 或 E1）上运行相同版本的固件。
- 如要使用群集，必须给 CC-SG 网络配置 IP 故障切换模式。IP 隔离模式配置不支持群集。参看***关于网络设置*** (p. 257)。
- 群集不支持 IPv6。
- 主节点的日期/时间和时区设置不复制到备用节点上。在创建群集之前，必须在每个 CC-SG 上配置这些设置。

访问 CC-SG 群集

在创建群集之后，用户可以直接访问主节点，如果他们把浏览器指向备用节点，把他们重定向到主节点。

重定向对已下载的 Admin Client 小程序不起作用，因为必须关闭浏览器并建立一个新会话，指向新的主系统。

通过 SSH 访问 CC-SG 必须针对特定的主节点。

创建群集

应该在创建群集之前，备份两个 CC-SG 设备上的配置。

▶ **创建群集：**

1. 选择 Administration（管理）> Cluster Configuration（群集配置）。
2. Primary Secure Gateway IP Address/Hostname（主安全网关 IP 地址/主机名）字段显示你当前访问的 CC-SG，表示这是主节点。
3. 在 Backup Secure Gateway IP Address/Hotsname（备用安全网关 IP 地址/主机名）字段里输入备用节点。确保指定的 CC-SG 的固件版本和硬件类型与主节点相同。用下列方法之一指定：
   - 单击 Discover Secure Gateways（发现安全网关），扫描并显示在你当前访问的同一个子网上的所有 CC-SG 设备，然后在 CC-SG 发现设备列表上单击选择一个状态为 Standalone（独立）的 CC-SG。
   - 可以在 Backup Secure Gateway IP Address/Hostname（备用安全网关 IP 地址/主机名）字段里输入 IP 地址或主机名指定另一个子网上的 CC-SG，然后单击 Check Bachup（检查备用）确定它的固件版本和硬件类型是否与主节点相同。
4. 在 Cluster name（群集名称）字段里输入此群集的名称。
5. 分别在 Username for Backup Secure Gateway（备用安全网关用户名）和 Password for Backup Secure Gateway（备用安全网关密码）字段里输入备份节点的有效用户名和密码。
6. 选择 Redirect by Hostname（按主机名重定向）复选框，指定应该通过 DNS 实现从备用节点到主节点的重定向访问。**可选。**参看 ***访问 CC-SG 群集*** (p. 275)。如果使用主机名而非 IP 地址，DNS 服务器应该包含 CC-SG IP 地址反向解析记录，确保可以解析主机名。
7. 单击 Create Cluster（创建群集）按钮，显示一条消息。
8. 单击 Yes（是）按钮。

   重要说明：在开始创建群集之后，切勿在 CC-SG 上执行其他任何功能，直到创建过程结束为止。
9. 单击任何消息屏幕上的 OK（确定）按钮继续操作。备用节点重新启动，这个过程可能需要几分钟时间。
10. 在群集创建完毕之后显示一条消息，说明成功加入了备用节点。

删除备用 CC-SG 节点

单击 Secondary Node（备用节点），删除指定的备用节点。这并不把备用 CC-SG 设备从配置中删除掉。

在 CC-SG 设备上删除备用节点状态：

1. 在 Cluster Configuration（群集配置）表上选择 Secondary CC-SG Node（备用 CC-SG 节点）。
2. 单击 Remove Backup Node（删除备用节点）。
3. 单击 Yes（是）按钮删除备用节点状态。

配置群集设置

不能更改群集配置的时区。

配置群集设置：

1. 选择 Administration（管理）> Cluster Configuration（群集配置）。
2. 在 Configuration（配置）选项卡上修改或配置设置。
   - 必要时修改群集名称。
   - 对于 Time Interval（时间间隔），输入 CC-SG 应多久检查一次与另一个节点的连接。有效范围是 5-20 秒。

   注意：如果较小的时间间隔，检查检测信号所产生的网络流量就会增加。如果群集里的节点彼此相距很远，可能要设置较大的时间间隔。

   - 对于 Failure Threshold（故障阈值），输入在 CC-SG 节点由于没有响应而被认为发生故障之前，需要连续传输的检测信号数。有效范围是 2-10 个检测信号。
3. 单击 Update（更新）按钮保存更改。

切换主节点状态和备用节点状态

当备用节点处于 Joined（加入）状态时，可以切换主节点和备用节点的角色。当备用节点处于 Waiting（等待）状态时，禁止切换。

在切换角色之后，此前的主节点处于 Waiting（等待）状态。如要恢复群集配置，把 Waiting（等待）节点作为备用节点加入群集。

参看***恢复群集*** (p. 278)。

切换主节点状态和备用节点状态：

1. 选择 Administration（管理）> Cluster Configuration（群集配置）。

2. 在 Configuration（配置）选项卡上单击 Switch Primary And Backup（切换主节点和备用节点）。
3. 把新的备用节点作为备用节点加入群集。参看***恢复群集*** (p. 278)。

恢复群集

当群集由于一个节点发生故障而崩溃，或者发生故障的备用节点进入等待状态时，可以重构群集，恢复主节点状态和备用节点状态。

如果主节点和备用节点彼此断开连接，备用节点担当主节点的角色。在连接恢复之后，可能有两个主节点。不能恢复有两个主节点的群集。只有在有一个主节点和一个等待节点时，才能进行恢复。

可以采用两种方法恢复有两个主节点的群集。登录每个主节点删除群集，然后再创建群集。或者登录其中一个主节点，重新启动此主节点，让它进入等待状态，根据说明恢复群集。

恢复群集：

1. 选择 Administration（管理）> Cluster Configuration（群集配置）。
2. 单击 Recovery（恢复）选项卡，可以在指定时间自动重构群集，也可以立刻重构群集。
   - 单击 Rebuild Now（现在重构）按钮立刻恢复群集。
   - 选择 Enable Automatic Rebuild（启用自动重构）复选框，在 From Time（开始时间）和 To Time（结束时间）字段里指定群集重构时间。单击 Update（更新）按钮保存更改。

注意：如果群集中的 CC-SG 设备不使用相同时区，当主节点发生故障，备用节点变成新的主节点时，指定的自动重构时间仍然沿用旧主节点的时区。

删除群集

在彻底删除群集时，删除你输入的群集信息，让主 CC-SG 节点和备用 CC-SG 节点恢复到独立状态。此外，除了网络设置（个性化包），备用节点上的所有配置数据（包括 CC-SG 超级用户密码）均复位到默认值。

删除群集：

1. 选择 Administration（管理）> Cluster Configuration（群集配置）。
2. 然后单击 Delete Cluster（删除群集）按钮。
3. 单击 Yes（是）按钮删除主节点状态和备用节点状态。
4. 在删除群集之后，显示一条消息。

升级群集

参看*升级群集* (p. 246)。

群集许可

既可以利用节点数相同的单机许可运行 CC-SG 群集，也可以利用群集套件许可运行 CC-SG 群集。

群集许可不同于单机许可，它包含群集里两台 CC-SG 设备的主机 ID。运行群集里的两台 CC-SG 设备只需一组许可。

必须把群集许可添加到 CC-SG 主设备上。在创建群集时，自动把许可复制到备用节点上。

在把 CC-SG 群集升级到 v5.0 或更高版本时要遵循下列固件升级步骤，确保在每台 CC-SG 上创建一组相同的许可。参看*升级群集* (p. 246)。

由于群集里的每台 CC-SG 必须能作为主节点接管群集，所以它们的许可节点数量必须始终保持相等。群集套件许可从主节点上被复制到备用节点上，自动确保许可节点数量相等。如果使用单机许可运行群集，在加入群集时通过许可节点数量检查来执行此任务。

在加入群集时检查备用节点的主机 ID，确保它与许可文件的内容保持一致。如果主机 ID 不匹配许可文件，备用节点不能加入群集。

在首次用群集套件许可创建群集时，在备用节点成功加入群集之前，CC-SG 主节点处于有限工作模式下。

在主节点进入工作状态之后，可以针对固件升级等维护活动临时删除群集，然后按需要重新创建群集。必须在 30 天宽限期内重新创建群集。每次临时删除群集时，都有 30 天宽限期。

配置邻居

邻居是一组 CC-SG 设备，最多 10 台设备。在 Admin Client 上设置邻居之后，用户可以使用 Access Client，通过单点登录方式访问同一个邻居里的多台 CC-SG 设备。

在设置或管理邻居配置之前，要牢记邻居要求：

- 一台 CC-SG 设备只能属于一个邻居。
- 同一个邻居里的所有 CC-SG 设备必须有相同的固件版本。
- 邻居里的 CC-SG 设备必须是独立 CC-SG 设备，或者是群集 CC-SG 设备的主节点。
- 邻居可以同时包括 CC-SG 物理设备和 CC-SG 虚拟设备。
- 邻居成员必须在 IPv4 网络上。邻居不支持 IPv6 通信。

创建邻居

可以登录要创建邻居、但还不是任何邻居的成员的 CC-SG 设备。在创建邻居之后，邻居里的所有成员共享相同的邻居信息。如果任何邻居成员是群集 CC-SG 设备的主节点，邻居配置同时显示备用节点的 IP 地址或主机名。

创建邻居：

1. 选择 Administration（管理）> Neighborhood（邻居）。
2. 在 Neighborhood Name（邻居名称）字段里输入邻居名称。
3. 单击 Create Neighborhood（创建邻居）按钮。
4. Secure Gateway IP Address/Hostname（安全网关 IP 地址/主机名）表显示当前 CC-SG 的 IP 地址或主机名。可以单击下拉箭头来回切换长/短主机名和 IP 地址。
5. 在表上添加一台或多台 CC-SG 设备。
   a. 单击下一个空行，也可以按 Tab 键或上下箭头键。
   b. 输入要添加的新 CC-SG 设备的 IP 地址或主机名，然后按 Enter。参看*术语/缩写语* (参看 "*术语/缩略语*" p. 2)了解主机名规则。确保在证书和要访问的 CC-SG 的 URL 里使用相同的 IP 地址或主机名。参看*邻居证书要求* (p. 284)。
   c. 重复上述步骤，直到添加完所有 CC-SG 设备为止。
6. 单击 Next（下一步）按钮。
   - 如果找不到一台或多台 CC-SG 设备，显示一条消息，在表里用黄色突出显示这些 CC-SG 设备。删除这些设备，或者修改它们的 IP 地址或主机名，然后单击 Next（下一步）按钮。
7. CC-SG 的 Neighborhood Configuration（邻居配置）表显示 CC-SG 设备列表及其固件版本和状态。

   *注意：自动停用不符合邻居要求的 CC-SG 设备。参看***配置邻居** *(p. 279)。*

8. 必要时调整邻居配置。**可选。**
   - 如要更改任何 CC-SG 的 Secure Gateway Name（安全网关名称），单击要更改的名称，输入新名称，然后按 Enter。默认名称是 CC-SG 短主机名。名称是当 Access Client 用户在邻居成员之间来回切换时看到的名称，所以必须是唯一名称。
   - 如要停用任何 CC-SG 设备，取消设备旁边的 Activate（激活）复选框。被停用的 CC-SG 设备作为独立设备工作，不作为邻居成员之一给 Access Client 用户显示。

- 单击列标题按此属性升序顺序排序表。再次单击此标题按降序顺序排序表。

9. 如要返回上一个屏幕，单击 Back（返回）按钮重复前面的步骤。**可选。**
10. 单击 Finish（完成）按钮。

注意：Raritan 建议你：

*(1) 给所有邻居成员配置相同的 Restricted Service Agreement（有限服务协议）设置和文本。参看*门户 *(p. 291)。*

(2) 如果启用了 SSH，用信任/官方证书验证每个邻居成员。

编辑邻居

在一台 CC-SG 设备上设置邻居配置之后，同一个邻居里的所有 CC-SG 设备共享相同的邻居信息。因此，可以登录邻居里的任何一台 CC-SG 设备更改邻居配置。

注意：当你单击 Neighborhood Configuration（邻居配置）面板上的 Send Update（发送更新）按钮时，发出你对邻居成员所做的所有更改。但当前已登录邻居的用户在退出并重新登录之前，并不知道这些更改。

添加邻居成员

▶ **把新 CC-SG 设备添加到邻居里：**

1. 选择 Administration（管理）> Neighborhood（邻居）。
2. 单击 Add Member（添加成员）按钮打开 Add Member（添加成员）对话框。
3. 添加 CC-SG 设备。可以添加的 CC-SG 设备数量取决于现有邻居成员的数量，一个邻居最多可以有 10 个成员。
   a. 单击下一个空行，也可以按 Tab 键或上下箭头键。
   b. 在 IP address（IP 地址）字段里输入要添加的 CC-SG 设备的 IP 地址或主机名。参看***术语/缩写语*** (参看 "***术语/缩略语***" p. 2)了解主机名规则。
   c. 重复上述步骤，直到添加完所有 CC-SG 设备为止。
   d. 单击 OK（确定）按钮。
4. 如果新 CC-SG 设备满足邻居要求并被找到，Neighborhood Configuration（邻居配置）表就显示它们。否则显示一条消息，返回 Add Member（添加成员）对话框，然后在此对话框上进行必要更改。
5. 选择每台新 CC-SG 设备旁边的 Active（活动）复选框。

6. 如要更改任何 CC-SG 的 Secure Gateway Name（安全网关名称），单击要更改的名称，输入新名称，然后按 Enter。默认名称是 CC-SG 短主机名。**可选。**
7. 单击 Send Update（发送更新）按钮保存更改，把最新邻居信息分发给其他成员。

管理邻居配置

可以停用或重新命名邻居配置里的任何 CC-SG 设备。在停用 CC-SG 设备之后，Access Client 上的 Neighborhood members（邻居成员）列表显示它不可用。也可以刷新邻居配置里所有成员的数据，例如固件版本或设备状态。

停用或重新命名邻居里的 CC-SG 设备，或者检索最新数据

1. 选择 Administration（管理）> Neighborhood（邻居）。
2. 单击列标题按此属性升序顺序排序表。再次单击此标题按降序顺序排序表。 **可选。**
3. 现在管理成员。
   - 如要停用一台 CC-SG 设备，取消此设备旁边的 Active（活动）复选框。
   - 如要更改 Secure Gateway Name（安全网关名称），单击要更改的名称，输入新名称，然后按 Enter。名称必须是唯一的。
   - 如要检索所有 CC-SG 设备的最新数据，单击 Refresh Member Data（刷新成员数据）。
   - 如要在用户切换到另一台 CC-SG 设备时永久终止当前连接，选择 Disconnect Active Sessions when Switching Secure Gateways（在切换安全网关时断开活动会话）复选框。否则，取消此复选框。
   - 如要允许那些访问一个邻居成员的用户搜索所有邻居成员，并利用搜索结果启动目标服务器连接，选择 Enable Extended Network Neighborhood Search（启用扩展网络邻居搜索）复选框。取消此复选框禁用扩展网络邻居搜索。参看扩展网络邻居搜索。
4. 单击 Send Update（发送更新）按钮保存更改，把最新邻居信息分发给其他成员。

扩展网络邻居搜索

在启用扩展网络邻居搜索之后，用户可以在 Access Client 上选择搜索并访问任何邻居成员上的节点。

在执行搜索时，可以指定搜索是扩展到“在邻居里”的所有成员，还是“仅限本地”。

在执行扩展网络邻居搜索之后显示邻居搜索结果时，显示邻居节点的状态、可用性和节点数据。在显示搜索结果之后，并不实时更新这些邻居节点数据。

注意：同时显示主 CC-SG 上虚拟机节点的虚拟机数据，但不显示邻居 CC-SG 上虚拟机节点的虚拟机数据。

在对 All Nodes（所有节点）组执行电源控制操作时，如果正在进行扩展邻居搜索，并不包括 CC-SG 设备上的节点。All Nodes（所有节点）组是在主 CC-SG 上创建的，不能包含任何邻居节点。

删除邻居成员

当不再需要邻居里的一台 CC-SG 设备时，可以在邻居配置里把它删除掉，也可以停用它。否则，当 Access Client 用户尝试切换到这些设备时，却发现不能访问它们。例如在下列情况下，邻居成员变得不合时宜：

- 把 CC-SG 设备设置为群集配置里的备用 CC-SG 节点，这不符合邻居要求。
- 复位 CC-SG 设备，致使设备删除邻居配置，恢复到出厂默认设置。

在删除成员时，确保邻居里至少有两台 CC-SG 设备，否则 CC-SG 将删除此邻居。

▶ 删除邻居里的一台 CC-SG 设备

1. 选择 Administration（管理）> Neighborhood（邻居）。
2. 单击要删除的 CC-SG 设备，再单击 Remove Member（删除成员）按钮。重复上述步骤，直到删除你要删除的所有 CC-SG 设备为止。
3. 单击 Send Update（发送更新）按钮保存更改，把最新邻居信息分发给其他成员。

重要说明：如要更改一台已经是邻居成员的 CC-SG 设备的 IP 地址，必须先把它从邻居配置中删除掉，否则不能把 CC-SG 从邻居中删除掉。

刷新邻居

可以在 Neighborhood Configuration（邻居配置）面板上检索所有邻居成员的最新状态。

1. 选择 Administration（管理）> Neighborhood（邻居）。
2. 单击 Refresh Member Data（刷新成员数据）。
3. 单击 Send Update（发送更新）按钮保存更改，把最新邻居信息分发给其他成员。

邻居证书要求

为了确保在使用邻居时证书不出错，必须遵循下列步骤。

1. 确保在创建邻居时和在通过 URL 访问 CC-SG 时，在证书里把相同的 IP 地址或主机名用于每个 CC-SG 邻居成员。为了确保证书正确无误，要生成并安装与访问 URL/DNS 名称同名的（自签名或 CA 签名）证书。参看 *证书* (p. 292)。
2. 在启动 CC-SG 时，将显示证书错误。给邻居里的每台 CC-SG 设备安装证书。
3. 把证书存储在信任仓库里。
4. 对于 Internet Explorer 浏览器，在两个地方添加每台 CC-SG 的 IP/主机名。选择 Internet options（Internet 选项），单击 Security（安全）选项卡，然后单击 Trusted Sites（信任站点）图标。同时在 Trusted Sites（信任站点）列表和 Privacy（隐私）> Sites（站点）选项卡上添加每台 CC-SG 的 IP/主机名。确保 IP 或主机名与访问 CC-SG 所用的 URL 完全相同。
5. 对于 Internet Explorer 8 和 Internet Explorer 9 浏览器，选择 Internet options（Internet 选项）> Privacy（隐私）选项卡。把 Internet zone（Internet 区域）设置为 Accept all cookies（接受所有 cookies）。
6. 确保 Internet Explorer 浏览器列出作为邻居成员的所有 CC-SG IP 地址/主机名。选择 Internet Options（Internet 选项）> Content（内容）> Certificates（证书），然后单击 Trusted Root Certification Authorities（信任根证书颁发机构）选项卡查看 IP 地址/主机名。

删除邻居

删除邻居：

1. 登录任何一台要删除邻居配置的 CC-SG 设备。
2. 选择 Administration（管理）> Neighborhood（邻居）。
3. 单击 Delete Neighborhood（删除邻居）按钮。

4. 单击 Yes（是）按钮确认删除。

升级邻居

同一个邻居里的所有 CC-SG 设备必须使用相同的固件版本。当 CC-SG 设备是活动邻居成员时，不能升级升级它们。停用每个成员进行升级，然后再激活它，并刷新邻居配置。

▶ 升级邻居：

1. 在升级每台 CC-SG 设备之前，先停用它。参看***管理邻居配置*** (p. 282)。
2. 根据最佳升级方法逐个升级每台 CC-SG 设备。参看***升级 CC-SG*** (p. 244)。
3. 再次激活已升级的邻居成员。参看***管理邻居配置*** (p. 282)。
4. 刷新邻居。参看***刷新邻居*** (p. 284)。

安全管理器

安全管理器用于管理 CC-SG 如何给用户提供访问。可以用安全管理器配置验证方法、SSL 访问、AES 加密、强密码规则、封锁规则、登录门户、证书和访问控制表。

远程验证

参看***远程验证*** (参看 "***Remote Authentication（远程验证）***" p. 199)详细了解如何配置远程验证服务器。

AES 加密

可以配置 CC-SG，用 AES-128 或 AES-256 加密客户机和 CC-SG 服务器之间的通信。在要求 AES 加密时，所有用户必须用支持 AES 的客户机访问 CC-SG。如果要求 AES 加密，而你尝试用不支持 AES 的浏览器访问 CC-SG，不能连接 CC-SG。

检查浏览器的 AES 加密

CC-SG 支持 AES-128 加密和 AES-256 加密。如果不知道浏览器是否使用 AES，请与浏览器制造商核实。

可尝试使用要核实加密方法的浏览器浏览以下网站：***https://www.fortify.net/sslcheck.html*** ***https://www.fortify.net/sslcheck.html***。此网站将检测浏览器的加密方法，并显示检测报告。Raritan 与此网站没有隶属关系。

注意：Internet Explorer 6 不支持 AES-128 加密或 AES-256 加密。

AES-256 要求和支持的配置

只有下列网络浏览器支持 AES-256 加密：

- Firefox 2.0.0.x 和更高版本
- Internet Explorer 7

注意：只有 Windows Vista 运行的 Internet Explorer 7 支持 AES-128 加密或 AES-256 加密。Windows XP 不支持任何 AES 加密。

除了浏览器支持，AES-256 加密还要求安装 Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6。

在浏览器上启用 AES-256 加密

1. 在 ***http://java.sun.com/javase/downloads/index.jsp*** (***http://java.sun.com/javase/downloads/index.jsp***) 上下载 JCE Unlimited Strength Jurisdiction Policy Files 6。
2. 把文件解压到 Java 目录下的 `\lib\security\` 子目录里，例如 `C:\Program Files\Java 1.6.0\lib\security\`。

要求在客户机和 CC-SG 之间使用 AES 加密

可以在安全管理器上配置 CC-SG，要求客户机和 CC-SG 服务器之间的会话使用 AES 加密。

1. 选择 Administration（管理）> Security（安全）。
2. 打开 Encryption（加密）选项卡。
3. 选择 Require AES Encryption between Client and Server（要求在客户机和服务器之间使用 AES 加密）复选框。
4. 在选择此选项之后显示一条消息，提示你客户机必须使用 AES 加密才能连接 CC-SG。单击 OK（确定）按钮确认。

- 单击 Key Length（密钥长度）下拉箭头，然后选择加密级别：128 或 256。
- CC-SG Port（CC-SG 端口）字段显示 80。
- Browser Connection Protocol（浏览器连接协议）字段显示选择的 HTTPS/SSL。

5. 单击 Update（更新）按钮保存更改。

配置浏览器连接协议：HTTP 或 HTTPS/SSL

可以在安全管理器上配置 CC-SG 使用来自客户机的常规 HTTP 连接，也可以要求使用 HTTPS/SSL 连接。必须重新启动 CC-SG，对此设置所做的更改才会生效。

默认设置是 HTTPS/SSL。

配置浏览器连接协议：

1. 选择 Administration（管理）> Security（安全）。
2. 打开 Encryption（加密）选项卡。
3. 选择 HTTP 或 HTTP/SSL 选项，指定客户机在连接 CC-SG 时要使用的浏览器连接协议。
4. 单击 Update（更新）按钮保存更改。

登录设置

Login Settings（登录设置）选项卡允许你配置 Strong Password Settings（强密码设置）和 Lockout Settings（封锁设置）。

查看登录设置

1. 选择 Administration（管理）> Security（安全）。
2. 单击 Login Settings（登录设置）选项卡。

要求所有用户使用强密码

1. 选择 Administration（管理）> Security（安全）。
2. 单击 Login Settings（登录设置）选项卡。
3. 选择 Strong Passwords Required for All Users（要求所有用户使用强密码）复选框。
4. 选择 Maximum Password Length（最大密码长度）。构成密码的字符数不得超过这个最大字符数。

5. 选择 Password History Depth（密码历史深度）。此数字指定在历史记录里保留多少个不能重复使用的旧密码。例如：如果 Password History Depth（密码历史深度）设置为 5，表示用户不能重复使用在此之前用过的 5 个旧密码。
6. 选择 Password Expiration Frequency（密码到期频率）。所有密码在设置的天数之后到期。在密码到期之后，当用户下次登录时，要求他们选择新密码。
7. 选择 Strong Password Requirements（强密码要求）：
   - 密码至少要有一个小写字母。
   - 密码至少要有一个大写字母。
   - 密码至少要有一个数字。
   - 密码至少要有一个特殊字符（例如感叹号或 &）。
8. 单击 Update（更新）按钮保存更改。

关于 CC-SG 密码

所有密码必须复合管理员配置的所有规则。在配置强密码规则之后，未来的所有密码必须复合这些规则。如果新规则比原来的规则严格，所有现有用户在下次登录时都要更改自己的密码。强密码规则仅适用于在本地存储的用户配置文件。在验证服务器上的密码规则必须由验证服务器管理。

此外，用户名和密码中任何四个相邻字符不能相同。

强密码规则要求用户在创建密码时遵循严格规则，使密码更难以被人猜出来，从理论上讲更安全。默认情况下，CC-SG 不启用强密码。CC 超级用户始终要求使用包括所有强密码参数的强密码。

在更改密码规则时，可以用 Message of the Day（当日消息）功能给用户提前显示通知，告诉他们新标准是什么。

封锁设置

管理员可以指定在达到指定的登录失败次数之后，锁定 CC-SG 用户和 SSH 用户。可以针对本地验证用户、远程验证用户或所有用户启用此功能。

注意：在默认情况下，admin 帐号在三次登录失败之后被封锁五分钟。对于 admin，不能配置封锁前后的失败登录次数。

▶ **启用封锁：**

1. 选择 Administration（管理）> Security（安全）。
2. 单击 Login Settings（登录设置）选项卡。

3. 选择 Lockout Enabled for Local Users（对本地用户启用封锁）复选框，对本地验证用户启用封锁功能。选择 Lockout Enabled for Remote Users（对远程用户启用封锁）复选框，对远程验证用户启用封锁功能。
4. 在封锁用户之前，默认登录失败次数是三次。可以输入 1-10 之间的数更改此值。
5. 选择锁定策略：
   - Lockout for Period（封锁时间）：指定一个时间（分钟），用户在这段时间被封锁，不能再次登录。默认数是五分钟。可以指定 1-1440 分钟（24 小时）之间的时间。在指定时间到期之后，用户可以再次登录。在封锁时间内，管理员随时可以覆盖此值，允许用户重新登录 CC-SG。
   - Lockout Until Admin Allows Access（封锁至管理员允许访问）：用户被封锁，直到管理员解除用户帐号封锁为止。
6. 在 Lockout Notification Email（封锁通知电子邮件）字段里输入电子邮件地址。在发生封锁时，给此电子邮件地址发送通知。如果此字段保留空白，不发送通知。**可选。**
7. 在 Administrator's Telephone（管理员电话号码）字段里输入电话号码。在发生封锁时，发送的电子邮件通知里有此电话号码。**可选。**
8. 单击 Update（更新）按钮保存更改。

禁用封锁：

在禁用封锁时，当前没有登录 CC-SG 的所有用户都可以登录。

1. 选择 Administration（管理）> Security（安全）。
2. 打开 Login Settings（登录设置）选项卡。
3. 取消 Lockout Enabled for Local Users（对本地用户启用封锁）复选框，对本地验证用户禁用封锁功能。取消 Lockout Enabled for Remote Users（对远程用户启用封锁）复选框，对远程验证用户禁用封锁功能。
4. 单击 Update（更新）按钮保存更改。

允许同时在多个客户机上用一个用户名登录

可以允许同一个用户名有多个并发 CC-SG 会话。

1. 选择 Administration（管理）> Security（安全）。
2. 单击 Login Settings（登录设置）选项卡。
   - 选择 Super User（超级用户）复选框允许同时在多个客户机上用 CC 超级用户帐号登录。
   - 选择 System Administrators（系统管理员）复选框允许系统管理员用户组里的用户同时登录。

- 选择 Other Users（其他用户）复选框允许其他所有用户同时登录。

3. 单击 Update（更新）按钮保存更改。

配置闲置计时器

可以配置闲置计时器，指定在让用户退出 CC-SG 之前， CC-SG 会话可以闲置多长时间。

如果用户打开了任何节点连接，会话即被认为是活动会话，在闲置计时器到期之前，用户不会退出系统。

配置闲置计时器：

1. 选择 Administration（管理）> Security（安全）。
2. 单击 Login Settings（登录设置）选项卡。
3. 在 Inactivity Time（闲置时间）字段里输入希望的时间极限。
4. 单击 Update（更新）按钮保存更改。

配置移动客户机超时

移动客户机超时确保在超时结束时关闭闲置的 Mobile Access Client 会话和 Mobile KVM Client (MKC) 会话 这样可以释放被闲置会话占用的资源，例如在不当关闭目标服务器连接时。被突然断开的管理员用户还可以利用超时功能，在设置了登录限制的情况下再次登录。如果会话处于活动状态，并不关闭会话。

默认移动客户机超时是 8 分钟。始终启用移动客户机超时。

此超时只适用于移动客户机访问，并取代闲置计时器和任何设备特定的闲置超时值。这样可以定义较短的超时，并把它应用于移动客户机访问。

触摸左上角的 X 关闭浏览器窗口，在浏览器保持打开状态时关闭设备，让浏览器窗口位于后台，都是不当关闭会话的例子。

由于闲置而被关闭的移动客户机会话将写入审计日志，同时附上一条消息：SessionID {0} 发生闲置超时。如果启用超时，还生成 ccPortConnectionTerminated SNMP 通知。

配置移动客户机超时：

1. 选择 Administration（管理）> Security（安全）。
2. 单击 Login Settings（登录设置）选项卡。
3. 在 Mobile Client Timeout（移动客户机超时）字段里设置会话在关闭之前可以闲置的分钟数（5-30 分钟）。
4. 单击 Update（更新）按钮。

门户

门户设置允许管理员配置徽标和访问协议，在用户访问 CC-SG 时问候他们。

配置门户设置：

1. 选择 Administration（管理）> Security（安全）。
2. 打开 Portal（门户）选项卡。

徽标

可以把一个小图形文件上载到 CC-SG，作为登录页的横幅。徽标文件的最大大小是 998 x 170 像素。

上载徽标：

1. 单击 Portal（门户）选项卡上 Logo（徽标）区的 Browse（浏览）按钮打开 Open（打开）对话框。
2. 在对话框上选择要用作徽标的图形文件，然后单击 Open（打开）按钮。
3. 单击 Preview（预览）按钮预览徽标。右边显示所选的图形文件。
4. 单击 Update（更新）按钮保存更改。

有限服务协议

可以配置一条消息，在登录屏幕上的登录字段左边显示。这可以用作有限服务协议，或者作为用户访问 CC-SG 时要同意的声明。如果用户接受有限服务协议，在日志文件和审计跟踪报告里添加一项记录。

给 CC-SG 登录屏幕增加有限服务协议：

1. 选择 Require Acceptance of Restricted Service Agreement（要求接受有限服务协议）复选框，要求用户单击登录屏幕上的协议框，才能输入登录信息。
2. 输入消息：
   a. 如果要直接输入横幅文本，选择 Restricted Service Agreement Message（有限服务协议消息）。
      - 在显示的文本字段里输入协议消息。文本消息最大长度是 10,000 个字符。
      - 单击 Font（字体）下拉菜单，然后选择消息字体。
      - 单击 Size（大小）下拉菜单，然后选择消息字体大小。
   b. 如果要加载文本文件 (.txt) 里的消息，选择 Restricted Service Agreement Message File（有限服务协议消息文件）。

- 单击 Browse（浏览）按钮显示对话框。
- 在对话框上选择要使用的消息所在的文本文件，然后单击 Open（打开）按钮。文本消息最大长度是 10,000 个字符。
- 单击 Preview（预览）按钮预览文件里的文本。在横幅消息字段上面显示预览情况。

3. 单击 Update（更新）按钮保存更改。在用户下次访问 CC-SG 时，更新登录屏幕。

证书

可以在 Certificate（证书）选项卡上生成证书签名请求 (CSR) 发送到证书机构申请数字身份证书，生成自签名证书，或者导入和导出证书及其私有密钥。

证书任务

导入的证书应该是 PEM 格式。

在创建证书时，包括所有 Subject Alternative Names（主题别名）确保名称相同。

Java 客户机在下载 jar 时检查下载 URL 里的主机名是否完全相同。

注意：屏幕下半部的按钮将从 Export（导出）变成 Import（导入），再变成 Generate（生成），取决于所选的证书选项。

导出当前证书和私有密钥：

1. 选择 Administration（管理）> Security（安全）。
2. 单击 Certificate（证书）选项卡。
3. 选择 Export current certificate and private key（导出当前证书和私有密钥）。
4. 单击 Export（导出）按钮。Certificate（证书）面板显示证书，Private Key（私有密钥）面板显示私有密钥。
5. 在每个面板上选择文本，按 Ctrl+C 复制文本。可以按需要把文本粘贴到任何地方。

生成证书签名请求，导入粘贴的证书和私有密钥：

把 CSR 提交给证书服务器，证书服务器将发出一份签名证书。还从证书服务器导出根证书，保存在文件里。在收到证书签发机构发出的签名证书之后，可以导入签名证书、根证书和私有密钥。

1. 选择 Administration（管理）> Security（安全）。

2. 单击 Certificate（证书）选项卡。
3. 单击 Generate Certificate Signing Request（生成证书签名请求），然后单击 Generate（生成）按钮打开 Generate Certificate Signing Request（生成证书签名请求）窗口。
4. 在字段里输入要求的数据。
   a. 加密模式：如果在 Administration（管理）> Security（安全）> Encryption（加密）屏幕上选择了 Require AES Encryption between Client and Server(要求在客户机和服务器之间使用 AES 加密）复选框，AES-128 是默认值。如果不要求使用 AES，DES 3 是默认值。
   b. Private Key Length（私有密钥长度）：默认值是 1024。
   c. Validity Period (days)（有效期(天)）：最多 4 个数字字符。
   d. Country Code（国家代码）：CSR 标记是国家名称。
   e. State or Province（州/省）：最多 64 个字符。输入完整州名/省名。不要输入缩写。
   f. City/Locality（城市/地区）：CSR 标记是地区名称。最多 64 个字符。
   g. Registered Company Name（公司注册名称）：CSR 标记是机构名称。最多 64 个字符。
   h. Division/Department Name（事业部/部门名称）：CSR 标记是机构单位名称。最多 64 个字符。
   i. Fully Qualified Domain Name（全限定域名）：CSR 标记是公用名。
   j. Administrator Email Address（管理员电子邮件地址）：输入负责证书请求的管理员的电子邮件地址。
   k. Challenge Password（挑战密码）：最多 64 个字符。
5. 单击 OK（确定）按钮生成 CSR。Certificate（证书）屏幕上的相应字段显示 CSR 和私有密钥。
6. 选择 Certificate Request(证书请求)字段里的文本 ,然后按 Ctrl+C 复制文本。用 Notepad 等 ASCII 编辑器把 CSR 粘贴到文件里，然后保存成 .cer 文件。
7. 选择 Private Key（私有密钥）字段里的文本，然后按 Ctrl+C 复制文本。用 Notepad 等 ASCII 编辑器把私有密钥粘贴到文件里，然后保存成 .txt 文件。
8. 把 .cer 文件提交给证书服务器，获取一份签名证书。
9. 在证书服务器上下载或导出根证书，然后保存成 .cer 文件。此证书不同于在下一步骤中由证书服务器发出的签名证书。

10. 单击 CA 文件旁边的 Browse（浏览）按钮选择根证书文件。
11. 在收到证书服务器发出的签名证书之后，选择 Import pasted certificate and private key（导入粘贴的证书和私有密钥）。
12. 复制签名证书的文本，然后按 Ctrl+V 把它粘贴到 Certificate（证书）字段里。
13. 复制此前保存成 .txt 文件的私有密钥的文本，然后按 Ctrl+V 把它粘贴到 Private Key（私有密钥）字段里。
14. 如果 CSR 是 CC-SG 生成的，在 Password（密码）字段里输入 raritan。如果其他应用程序生成 CSR，使用此应用程序的密码。

注意：如果导入证书用根 CA (certificate authority) 和子根 CA 签名，只使用根证书或子根证书将会失败。为了解决这个问题，把根证书和子根证书复制并粘贴到一个文件里，然后导入它们。

生成自签名证书请求：

1. 选择 Administration（管理）> Security（安全）。
2. 单击 Certificate（证书）选项卡。
3. 选择 Generate Self Signed Certificate（生成自签名证书），然后单击 Generate（生成）按钮打开 Generate Self Signed Certificate（生成自签名证书）窗口。
4. 在字段里输入要求的数据。
   a. 加密模式：如果在 Administration（管理）> Security（安全）> Encryption（加密）屏幕上选择了 Require AES Encryption between Client and Server(要求在客户机和服务器之间使用 AES 加密）复选框，AES-128 是默认值。如果不要求使用 AES，DES 3 是默认值。
   b. Private Key Length（私有密钥长度）：默认值是 1024。
   c. Validity Period (days)（有效期(天)）：最多 4 个数字字符。
   d. Country Code（国家代码）：CSR 标记是国家名称。
   e. State or Province（州/省）：最多 64 个字符。输入完整州名/省名。不要输入缩写。
   f. City/Locality（城市/地区）：CSR 标记是地区名称。最多 64 个字符。
   g. Registered Company Name（公司注册名称）：CSR 标记是机构名称。最多 64 个字符。
   h. Division/Department Name（事业部/部门名称）：CSR 标记是机构单位名称。最多 64 个字符。

i. Fully Qualified Domain Name（全限定域名）：CSR 标记是公用名。

j. Administrator Email Address（管理员电子邮件地址）：输入负责证书请求的管理员的电子邮件地址。

k. Challenge Password（挑战密码）：最多 64 个字符。

5. 单击 OK(确定)按钮生成证书。Certificate(证书)屏幕上的 Certificate（证书）和 Private Key（私有密钥）字段显示加密证书和私有密钥。

访问控制表

IP 访问控制表指定要拒绝还是允许哪个客户机 IP 地址范围访问 CC-SG。访问控制表上的每一项就是一个规则，决定一个组里的一个用户是否能用某个 IP 地址访问 CC-SG。也可以设置在操作系统层面上应用于整个 CC-SG 系统的规则（选择 System [系统]，而不是用户组）。在创建规则之后，可以在列表上排列规则，指定它们的应用顺序。列表顶部的规则的优先级比列表上位置较低的规则高。

IPv6 地址不能用于系统级规则。对于其他所有规则，规则的两个 IP 地址必须是同类地址，即两个地址必须都是 IPv4 地址或 IPv6 地址。

查看访问控制表：

1. 选择 Administration（管理）> Security（安全）。
2. 单击 Access Control List（访问控制表）选项卡。

给访问控制表添加规则：

1. 选择 Administration（管理）> Security（安全）。
2. 单击 Access Control List（访问控制表）选项卡。
3. 单击 Add Row（添加行）图标  在表上添加一行。
4. 在 Starting IP（开始 IP）字段里输入开始 IP 值，在 Ending IP（结束 IP）字段里输入结束 IP 值，指定要把规则应用于哪个 IP 地址范围。
5. 单击 Group（组）下拉箭头，然后选择要把规则应用于哪个用户组。选择 System（系统）把规则应用于整个 CC-SG 系统。
6. 单击 Action（操作）下拉箭头，然后选择 Allow（允许）或 Deny（拒绝）指定 IP 范围内的指定用户是否可以访问 CC-SG。
7. 单击 Update（更新）按钮保存更改。

给访问控制表添加一个允许或拒绝操作系统级访问的规则：

1. 选择 Administration（管理）> Security（安全）。

2. 单击 Access Control List（访问控制表）选项卡。
3. 单击 Add Row（添加行）图标  在表上添加一行。
4. 在 Starting IP（开始 IP）字段里输入开始 IP 值，在 Ending IP（结束 IP）字段里输入结束 IP 值，指定要把规则应用于哪个 IP 地址范围。
5. 选择 Group（组）> System（系统）。
6. 单击 Action（操作）下拉箭头，然后选择 Allow（允许）或 Deny（拒绝）指定 IP 范围内的指定用户是否可以访问 CC-SG。
7. 单击 Update（更新）按钮保存更改。

更改 CC-SG 应用规则的顺序：

1. 选择 Administration（管理）> Security（安全）。
2. 单击 Access Control List（访问控制表）选项卡。
3. 在列表上选择要上下移动的规则。
4. 单击上下箭头，直到规则移动到希望的位置为止。
5. 单击 Update（更新）按钮保存更改。

删除访问控制表上的规则：

1. 选择 Administration（管理）> Security（安全）。
2. 单击 Access Control List（访问控制表）选项卡。
3. 选择要删除的规则，然后单击 Remove Row（删除行）图标。 
4. 单击 Update（更新）按钮保存更改。

通知管理器

用通知管理器配置外部 SMTP 服务器，以便在 CC-SG 上外向发送通知。通知功能用电子邮件发送预定报告、用户封锁报告、预定任务失败状态或成功状态。参看*任务管理器* (p. 297)。在配置 SMTP 服务器之后，可以选择给指定的收件人发送一封测试电子邮件，通知收件人测试结果。

配置外部 SMTP 服务器

1. 选择 Administration（管理）> Notifications（通知）。
2. 选择 Enable SMTP Notification（启用 SMTP 通知）复选框。

3. 在 SMTP host（SMTP 主机）字段里输入 SMTP 主机。参看***术语/缩写语*** (参看 "***术语/缩略语***" p. 2)了解主机名规则。支持 IPv6。
4. 在 SMTP port（SMTP 端口）字段里输入有效的 SMTP 端口号。
5. 在 Account name（帐号名称）字段里输入登录 SMTP 服务器所用的有效帐号名称。**可选。**询问电子邮件服务器管理员，是否需要此帐号信息。
6. 在 Password（密码）和 Re-enter Password（再次输入密码）字段里输入帐号名称的密码。**可选。**询问电子邮件服务器管理员，是否需要此帐号信息。
7. 在 From(发件人)字段里输入有效电子邮件地址，用于标识 CC-SG 发出的邮件。
8. 在 Sending retries（重发次数）字段里输入在发送过程失败后，重发电子邮件的次数。
9. 在 Sending retry interval (minutes)（重发间隔[分钟]）字段里输入重发之间的间隔分钟数 (0-60)。
10. 如果要采用 Secure Sockets Layer (SSL) 安全发送电子邮件，选择 Use SSL（使用 SSL）。
11. 单击 Test Configuration（测试配置）给指定的 SMTP 帐号发送一封测试电子邮件。应该检查发送情况，确保邮件到达目的地。
12. 单击 Update Configuration（更新配置）按钮保存更改。

任务管理器

用任务管理器按天、星期、月或年预定 CC-SG 任务。可以预定任务运行一次，或者按指定的时间间隔在每个星期的指定日期周期性运行。例如可以预定在每三个星期的星期五执行设备备份，或者预定在每个星期一通过电子邮件把特定报告发送给一个或多个收件人。

注意：任务管理器使用在 CC-SG 上设置的服务器时间预定任务，而不使用在客户 PC 上设置的时间。每个 CC-SG 页面的右上角显示服务器时间。

任务类型

可以预定下列任务：

- Active Directory 同步
- 备份 CC-SG
- 备份设备配置（个别设备或设备组）
- 暂停和恢复设备管理
- 复制设备配置（个别设备或设备组）
- 设备组电源控制
- 出口电源控制
- 清除日志
- 重新启动设备
- 恢复设备配置（不适用于设备组）
- 升级设备固件（个别设备或设备组）
- 生成所有报告

预定顺序任务

你可能要按顺序预定任务，确保按希望的顺序执行任务。例如你可能要为给定设备组预定一个升级设备固件任务，在此之后立即预定一个资产管理报告任务，以便确定是否升级了正确的固件版本。

通过电子邮件发送任务通知

在任务完成之后，可以给指定的收件人发送一封电子邮件。可以在通知管理器上指定把电子邮件发给谁，可以选择通过 SSL 安全发送电子邮件。参看*通知管理器* (p. 296)。

预定报告

通过电子邮件把预定报告发送给你指定的收件人。可以给要通过电子邮件发送的报告指定 CSV 或 HTML 版本。

状态为 Finished（完成）的所有报告在 CC-SG 上按 HTML 格式存储 30 天。只能在 Reports（报告）菜单上选择 Scheduled Reports（预定报告），用 HTML 格式查看已完成的报告。参看*预定报告* (p. 233)。

查找和查看任务

可以查看列表上按你选择的标准过滤的任务。可以查看每个任务的详细信息和历史记录。

注意：如果任务被更改或更新了，此前的历史记录不再适用，Last Execution Date（上次执行日期）字段变成空白。

查看任务：

1. 选择 Administration（管理）> Tasks（任务）。
2. 如要搜索任务，用上下按钮选择要查看哪个日期范围内的任务。
3. 在每个列表上选择一个或多个（按住 Ctrl 单击）任务、状态或所有者，可以进一步过滤列表。
4. 单击 View Tasks（查看任务）按钮查看任务列表。

查看任务历史记录：

- 选择任务，然后单击 Task History（任务历史记录）按钮。

查看任务详细信息：

- 双击任务打开任务详细信息对话框。

预定任务

本节讨论大多数可以预定的任务。参看***预定设备固件升级任务*** (参看 "***安排设备固件升级时间***" p. 301)详细了解如何预定设备固件升级。

预定任务：

1. 选择 Administration（管理）> Tasks（任务）。
2. 单击 New（新建）按钮。
3. 在 Main（主要）选项卡上输入任务的名称和说明。名称长度为 1-32 个字母数字字符或下划线，不能包含空格。
4. 单击 Task Data（任务数据）选项卡。
5. 单击 Task Operation（任务操作）下拉菜单，然后选择你要预定的任务。注意对于选择的不同任务，需要填写数据的字段有所不同。参看下列各节了解每种任务的详细说明。
   - **Active Directory 同步**：参看***同步所有 AD 模块*** (p. 210)。
   - 备份 **CommandCenter**：参看***备份 CC-SG*** (p. 236) 详细了解备份，以及如何配置自动删除最旧的备份文件。

- **备份设备配置：**参看*备份设备配置* (p. 80)。
- **暂停/恢复设备管理：**参看*让 CC-SG 暂停管理设备* (p. 86)和*恢复管理* (参看 "*恢复设备管理*" p. 86)了解如何暂停和恢复各个设备管理。参看*用预定任务暂停和恢复设备管理* (参看 "*用预定任务功能暂停和恢复设备管理*" p. 87)详细了解如何预定任务暂停和恢复多台设备或多个设备组。
- **复制设备配置：**参看*复制设备配置* (p. 84)。
- **节点组电源控制：**参看节点组电源控制。
- **出口电源控制：**参看 **CC-SG 用户指南**。
- **Power IQ 同步**：参看*同步 Power IQ 和 CC-SG* (p. 366)。
- **清除日志：**参看*配置日志活动* (p. 264)。
- **重新启动设备：**参看*重新启动设备* (p. 85)。
- **恢复设备配置：**参看*恢复设备配置* (p. 81)（不适用于设备组）。
- **升级设备固件（个别设备或设备组）：**参看*预定设备固件升级* (参看 "*安排设备固件升级时间*" p. 301)。
- **生成所有报告：**参看*报告* (p. 221)。

6. 单击 Recurrence（重复执行）选项卡。对于升级设备固件任务，禁用 Recurrence（重复执行）选项卡。
7. 在 Period（周期）字段里单击预定任务执行周期对应的单选按钮。
   a. Once（一次）：用上下箭头选择任务开始时间。
   b. Periodic（定期）:用上下箭头选择任务开始时间。在 Repeat Count（重复次数）字段里输入执行任务的次数。在 Repeat Interval（重复间隔）字段里输入两次重复之间的间隔时间。单击下拉菜单，在列表上选择时间单位。如要设置任务按选择的间隔无休止运行，或者直到你更改或删除此任务为止，选择 Ongoing - until the task is changed or canceled（正在进行 — 直到更改或取消此任务为止）复选框。禁用 Repeat Count（重复次数）。设置 Repeat Interval（重复间隔）。
   c. Daily（每天）：如果你希望在每个星期的七天里重复执行任务，单击 Every day（每天）单选按钮。如果你希望在星期一到星期五的每一天重复执行任务，单击 Every weekday（每个工作日）单选按钮。
   d. Weekly（每个星期）：用上下箭头选择几个星期执行一次任务，然后选择要执行任务的每个星期的每一天旁边的复选框。
   e. Monthly（每个月）：在 Days（日）字段里输入要执行任务的日期，然后选择要执行任务的指定日期所在月份旁边的复选框。

f. Yearly（每年）：单击下拉菜单，在列表上选择要执行任务的月份。用上下箭头选择要执行任务的月日。

8. 对于每天、每个星期、每个月和每年执行的任务，必须在 Range of recurrence（重复执行范围）部分添加任务开始时间和结束时间。用上下箭头选择 Start at time（开始时间）和 Start date（开始日期）。如果任务无限期执行下去，单击 No end date（无结束日期）旁边的单选按钮，或者单击 End date（结束日期）旁边的单选按钮，用上下箭头选择要停止重复执行任务的日期。
9. 单击 Retry（重试）选项卡。
10. 如果任务失败，CC-SG 可以根据在 Retry（重试）选项卡上指定的稍后时间再次尝试执行任务。在 Retry count（重试次数）字段里输入 CC-SG 再次尝试执行任务的次数。在 Retry Interval（重试间隔）字段里输入两次重试之间的间隔时间。单击下拉菜单，在列表上选择时间单位。

重要说明：如果预定任务升级 SX 或 KX 设备，把 Retry Interval（重试间隔）设置为 20 分钟以上，因为成功升级这些设备需要大约 20 分钟时间。

11. 单击 Notification（通知）选项卡。
12. 指定在任务成功或失败之后，把通知发送到哪个电子邮件地址。默认使用当前登录用户的电子邮件地址。用户电子邮件地址在 User Profile（用户配置文件）上配置。如要添加另一个电子邮件地址，单击 Add（添加）按钮，在打开的窗口上输入电子邮件地址，然后单击 OK（确定）按钮。如果任务成功，默认发送一封电子邮件。如要通知收件人任务失败，单击 On Failure（失败时）。
13. 单击 OK（确定）按钮保存更改。

安排设备固件升级时间

可以给一个设备组里相同类型的多台设备（例如 KX 或 SX）预定升级任务。在开始升级任务之后，Reports（报告）> Scheduled Reports（预定报告）菜单显示 Upgrade Device Firmware（升级设备固件）报告，可以实时查看升级状态。如果在 Notification（通知）选项卡上指定通过电子邮件发送报告，可以通过电子邮件发送报告。

参看 Raritan 用户指南了解每种设备的预计升级时间。

预定设备固件升级时间：

1. 选择 Administration（管理）> Tasks（任务）。
2. 单击 New（新建）按钮。
3. 在 Main（主要）选项卡上输入任务的名称和说明。用你选择的 Name（名称）标识此任务和与之关联的报告。

4. 单击 Task Data（任务数据）选项卡。
5. 指定设备升级详细信息：
   a. Task Operation（任务操作）：选择 Upgrade Device Firmware（升级设备固件）。
   b. Device Group（设备组）：选择要升级的设备所在的设备组。
   c. Device Type（设备类型）：选择要升级的设备的类型。如果必须升级多个类型的设备，必须针对每种类型预定一个升级任务。
   d. Concurrent Upgrades（同时升级数）：指定在升级过程中应该同时开始传输文件的设备的数量。最大数是 10。在一个文件传输完之后，开始传输另一个新文件，这样可以确保立即进行最大数量的同时传输。
   e. Upgrade File（升级文件）：选择要升级到哪个固件版本。只显示与所选设备类型相适应的可用升级文件供你选择。
6. 指定升级时间：
   a. Start Date/Time（开始日期/时间）：选择升级任务的开始日期和时间。开始日期/时间必须比当前日期/时间晚。
   b. Restrict Upgrade Window（限制升级窗口）和 Latest Upgrade Start Date/Time（最晚升级开始日期/时间）：如果必须在特定时间范围内完成所有升级任务，用这些字段指定最晚升级开始日期和时间。选择 Restrict Upgrade Window（限制升级窗口），激活 Latest Upgrade Start Date/Time（最晚升级开始日期/时间）字段。
7. 指定要升级哪些设备，以及按什么顺序升级。把优先级较高的设备放在列表顶部。
   a. 在 Available（可用）列表上选择要升级的每台设备，然后单击 Add（添加）按钮把它移动到 Selected（选择）列表上。
   b. 在 Selected（选择）列表上选择一台设备，根据希望的升级顺序，用箭头按钮把它移动到希望的地方。
8. 指定如果升级失败，是否再试一次。
   a. 单击 Retry（重试）选项卡。
   b. Retry Count（再试次数）：输入在升级失败之后，CC-SG 再试次数。
   c. Retry Interval（再试间隔）：输入两次再试之间的间隔时间。默认间隔时间是 30 分钟、60 分钟和 90 分钟。这些值是最佳再试间隔时间。
9. 指定要接收成功和失败通知的电子邮件地址。默认使用当前登录用户的电子邮件地址。用户电子邮件地址在 User Profile（用户配置文件）上配置。

a. 单击 Notification（通知）选项卡。

b. 单击 Add（添加）按钮，在打开的窗口上输入电子邮件地址，然后单击 OK（确定）按钮。

c. 如果希望在升级失败时发送电子邮件，选择 On Failure（失败后）。

d. 如果希望在所有升级任务成功完成时发送电子邮件，选择 On Success（成功后）。

10. 单击 OK（确定）按钮保存更改。

在开始运行升级任务时，随时可以在预定时间范围内打开 Upgrade Device Firmware（升级设备固件）报告查看升级状态。参看*升级设备固件报告* (p. 234)。

更改预定任务

可以在预定任务执行之前更改它。

▶ **更改预定任务：**

1. 选择要更改的任务。
2. 单击 Edit（编辑）按钮。
3. 根据需要更改任务设置。参看*预定任务* (p. 299)和*预定设备固件升级任务* (参看 "*安排设备固件升级时间*" p. 301)了解选项卡说明。
4. 单击 Update（更新）按钮保存更改。

重新预定任务

任务管理器上的“另存为”功能允许你重新预定已经完成但你希望再次运行的任务。这也是创建与已完成任务相似的新任务的便捷方法。

▶ **重新预定任务：**

1. 选择 Administration（管理）> Tasks（任务）。
2. 在 Task Manager（任务管理器）页上选择要重新预定的任务。用过滤条件搜索任务。
3. 单击 Save As（另存为）。
4. 在打开的 Save As Task（另存任务）窗口上，自动用此前配置的任务信息填充各个选项卡。
5. 根据需要更改任务设置。参看*预定任务* (p. 299)和*预定设备固件升级任务* (参看 "*安排设备固件升级时间*" p. 301)了解选项卡说明。
6. 单击 OK（确定）按钮保存更改。

预定与另一个任务相似的任务

可以把此前配置的任务作为模板，预定一个有相似设置的新任务。

▶ **预定与另一个任务相似的任务：**

- 参看*重新预定任务* (p. 303)。

删除任务

可以删除任务，把它从任务管理器上删除掉。不能删除当前正在运行的任务。

▶ **删除任务：**

- 选择任务，然后单击 Delete（删除）按钮。

通过 SSH 访问 CC-SG

在 CC-SG 上用 Putty 或 OpenSSH Client 等 Secure Shell (SSH) 客户机访问 SSH (v2) 服务器命令行界面。CC-SG 命令的子集通过 SSH 管理设备和 CC-SG 自身。

SSH 客户机用户由 CC-SG 验证，后者把现有验证和授权策略应用于 SSH 客户机。可供 SSH 客户机使用的命令由 SSH 客户机用户所属的用户组的权限决定。

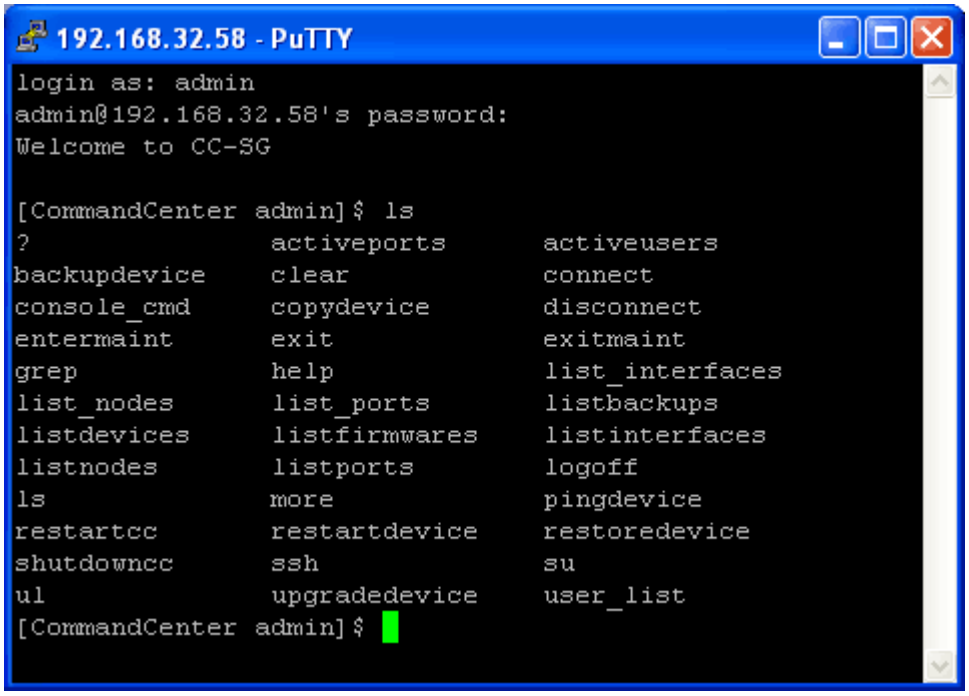
用 SSH 访问 CC-SG 的管理员不能注销 CC 超级用户 SSH 用户，但可以注销包括系统管理员在内的其他所有 SSH 客户机用户。

▶ **通过 SSH 访问 CC-SG：**

1. 启动 SSH 客户机，例如 PuTTy。
2. 指定 CC-SG 的 IP 地址。
3. 指定 SSH 端口号。默认端口是 22。可在安全管理器上配置 SSH 访问端口。参看*安全管理器* (p. 285)。
4. 打开连接。
5. 用 CC-SG 用户名和密码登录。
6. 显示 shell 提示符。

显示所有 SSH 命令：

- 在 shell 提示符下输入 ls，显示所有可用的命令。



启用 SSH 访问

在 Admin Client 上启用 SSH 访问，允许用户用 SSH 访问 CC-SG。

启用 SSH 访问：

1. 选择 Administration（管理）> Security（安全）。
2. 在 Encryption（加密）选项卡上选择 Enable SSH Access（启用 SSH 访问）复选框。
3. 设置其他 SSH 访问 选项：
   a. 在 SSH Server Port（SSH 服务器端口）字段里输入 SSH 访问所用的端口号。默认端口是 22。
   b. 选择 Enable SSH DPA(启用 SSH DPA)复选框，允许用 SSH 直接连接 SX 串行端口目标。如果不选择此复选框，拒绝用直接端口访问法连接串行端口目标。
4. 单击 Update（更新）按钮。

获取 SSH 命令帮助

可以立刻获取所有命令的有限帮助。也可以每次获取一个命令的详细帮助。

获取一个 SSH 命令的帮助：

1. 在 shell 提示符下输入要获取哪个命令的帮助，后跟一个空格和 -h。例如：

   ```
   connect -h
   ```

2. 屏幕显示有关此命令、参数和用法的帮助信息。

获取所有 SSH 命令的帮助：

1. 在 shell 提示符下输入下列命令：

   ```
   help
   ```

2. 屏幕显示每个 SSH 命令的简短说明和示例。

SSH 命令和参数

下表列出可以在 SSH 上使用的所有命令。必须在 CC-SG 上获得适当的权限，才能访问每个命令。

某些命令有附加参数，必须输入附加参数才能执行命令。如要进一步了解如何输入命令，参看*命令提示* (p. 309)。

列出活动端口：

```
activeports
```

列出活动用户：

```
activeusers
```

备份设备配置：

```
backup device <[-host <host>] | [-id <device_id>]>
backup_name [description]
```

清除屏幕：

```
clear
```

建立到串行端口的连接：

如果 <port_name> 或 <device_name> 有空格，要使用引号。

```
connect [-d <device_name>] [-e <escape_char>] <[-i
<interface_id>] | [-n <port_name>] | [port_id]>
```

把一台设备的设备配置复制到另一台设备上。仅限于端口数相同的 SX 设备：

```
copydevice <[-b <backup_id>] | [source_device_host]>
target_device_host
```

关闭端口连接：

```
disconnect <[-u <username>] [-p <port_id>] [-id
<connection_id>]>
```

进入维护模式：

```
entermaint  minutes [message]
```

退出维护模式：

```
exitmaint
```

- **搜索管道输出流中的文本：**

```
grep search_term
```

- **显示所有命令的帮助屏幕：**

```
help
```

- **列出可用的设备配置备份文件：**

```
listbackups <[-id <device_id>] | [host]>
```

- **列出可用设备：**

```
listdevices
```

- **列出可用于升级的固件版本：**

```
listfirmwares [[-id <device_id>] | [host]]
```

- **列出所有接口：**

```
listinterfaces [-id <node_id>]
```

- **列出所有节点：**

```
listnodes
```

- **列出所有端口：**

```
listports  [[-id <device_id>] | [host]]
```

- **退出用户：**

```
logoff  [-u <username>] message
```

- **列出所有命令：**

```
ls
```

- **指定分页：**

```
more [-p <page_size>]
```

- **对设备执行 ping 命令：**

```
pingdevice <[-id <device_id>] | [host]>
```

- **重新启动 CC-SG：**

```
restartcc minutes [message]
```

重新启动设备：

```
restartdevice <[-id <device_id>] | [host]>
```

恢复设备配置：

```
restoredevice <[-host <host>] | [-id <device_id>]>
[backup_id]
```

关闭 CC-SG：

```
shutdowncc minutes [message]
```

打开至 SX 设备的 SSH 连接：

```
ssh  [-e <escape_char>] <[-id <device_id>] | [host]>
```

更改用户：

```
su [-u <user_name>]
```

升级设备固件：

```
upgradedevice <[-id <device_id>] | [host]>
```

列出所有当前用户：

```
userlist
```

退出 SSH 会话：

```
exit
```

命令提示

- 对于传送 IP 地址的命令，例如 `upgradedevice`，可以用主机名取代 IP 地址。参看***术语/缩写语*** (参看 "***术语/缩略语***" p. 2)了解主机名规则。
- `copydevice` 和 `restartdevice` 命令只适用于部分 Raritan 设备。这些命令不支持 Dominion SX 和 IPMI 服务器。
- 方括号里的命令部分是可选的，不一定要使用命令的这部分。
- Some commands contains two segments separated by the "Or" sign:|

  必须输入命令的一部分，但未必要输入两部分。

- 尖括号里的命令部分表示你必须输入的文本。在输入命令时，不要输入尖括号。例如：

命令语法	设备 ID 值	你应该输入
`ssh -id <device_id>`	100	`ssh -id 100`

- 默认换码符是波浪号 (tilde)，后跟一个点。例如：

  `~.`

  参看***终止 SSH 连接*** (p. 312)详细了解如何使用换码符和 exit 命令。

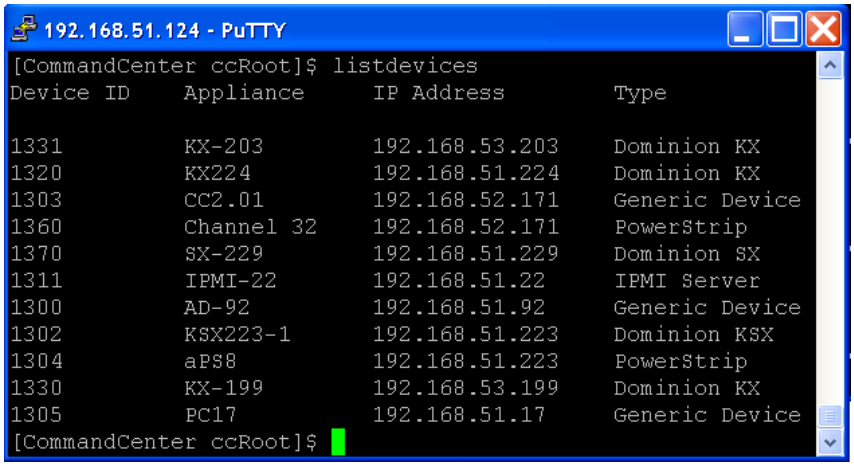
在 Linux 终端或客户机上使用换码符时，可能会出问题。Raritan 建议你在建立端口连接时定义一个新换码符。命令是 `connect [-e <escape_char>] [port_id]`。例如为了在连接端口 2360 时把 m 定义为换码符，输入 `connect -e m 2360`。

建立至串行设备的 SSH 连接

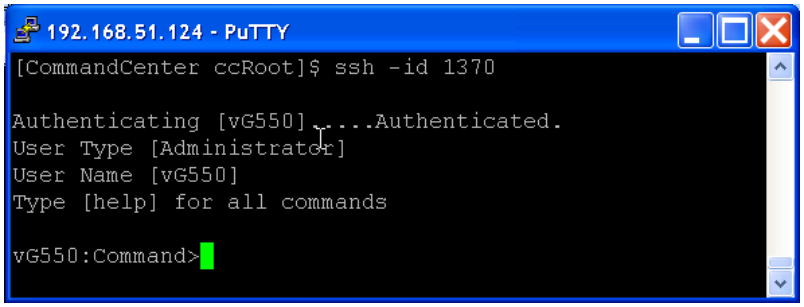
可以建立至串行设备的 SSH 连接，以便对设备执行管理操作。在建立连接之后，可以使用串行设备支持的管理命令。

注意：在连接之前，确保串行设备已被添加到 CC-SG。

1. 输入 `listdevices`，确保串行设备已被添加到 CC-SG。



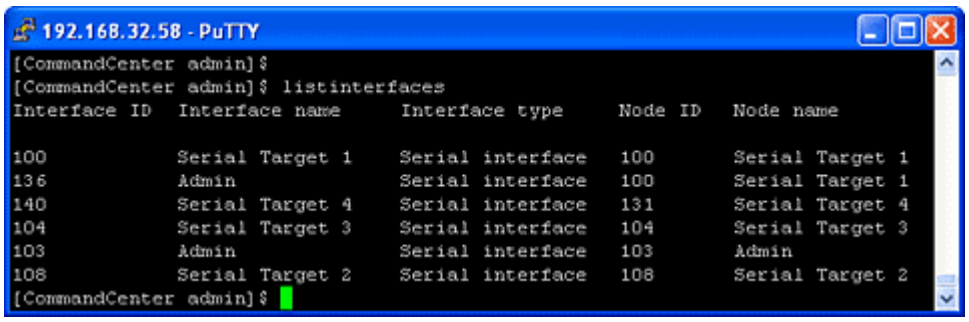
2. 输入 ssh -id <device_id> 连接设备。
   以上图为例，可以输入 ssh -id 1370 连接 SX-229。



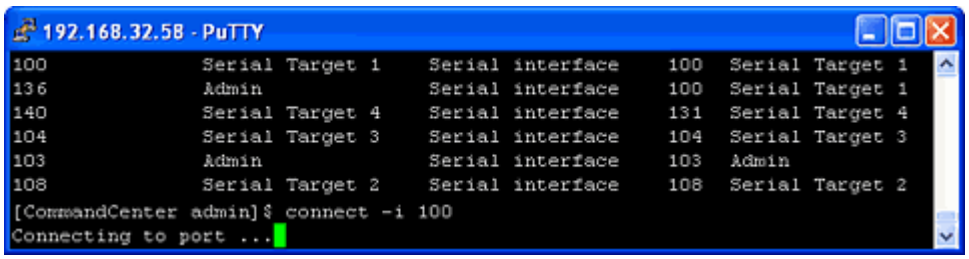
通过带外接口用 SSH 连接节点

可以通过与节点关联的带外接口，用 SSH 连接节点。SSH 连接使用代理模式。

1. 输入 listinterfaces 查看节点 ID 和关联接口。



2. 输入 connect -i <interface_id> 连接与接口关联的节点。



3. 可以在显示的提示符下输入特定命令或别名。

命令	别名	Description（说明）
quit	q	终止连接，返回 SSH 提示符。
get_write	gw	获取写访问权。让 SSH 用户在目标服务器上执行命令，而浏览器用户只能观察活动。
get_history	gh	获取历史记录。显示在目标服务器上执行的最

命令	别名	Description（说明）
		近几个命令和执行结果。
send_break	sb	发送中断。中断由浏览器用户发起的目标服务器循环。
help	?,h	打印帮助屏幕。

终止 SSH 连接

可以只建立至 CC-SG 的 SSH 连接，也可以先建立至 CC-SG 的连接，然后建立至 CC-SG 管理的端口、设备或节点的连接。可以采用几种不同的方法终止这些连接，视你要终止的连接在哪一方而定。

退出至 CC-SG 的整个 SSH 连接：

此命令终止通过 CC-SG 建立的整个 SSH 连接，包括任何端口连接、设备连接或节点连接。

- 在提示符下输入下列命令并按 Enter：

```
exit
```

终止一个端口连接、设备连接或节点连接，而其余仍然连接 CC-SG：

可以用换码符终止一个端口连接、设备连接或节点连接，而至 CC-SG 的 SSH 连接仍然处于打开状态。

默认换码符是波浪号 (tilde)，后跟一个点。

- 在提示符下输入下列命令并按 Enter：

```
~.
```

在 Linux 终端或客户机上使用换码符时，可能会出问题。Raritan 建议你在建立端口连接时定义一个新换码符。命令是 `connect [-e <escape_char>] [port_id]`。例如为了在连接端口 2360 时把 m 定义为换码符，输入 `connect -e m 2360`。

Dominion SX 串行目标直接端口访问

CC-SG 允许用 SSH 直接端口访问法访问 CC-SG 管理的 Dominion SX 设备的串行目标。必须先启用此选项。参看*启用 SSH 访问* (p. 305)。

所有 SSH 直通会话都由 CC-SG 代理。

在 SSH 会话过程中，用户可以利用可配置的换码符在必要时切换到目标服务器上的端口菜单，并在端口上使用可用命令，例如写入锁定和历史记录。

最多允许 30 个并行会话。

用直接端口访问法命名串行目标端口和节点

在用直接端口访问法访问 Dominion SX 的串行目标时，以及在不使用 CC-SG 的情况下访问 Dominion SX 的端口时，建议你让目标的端口名称和节点名称相同。

如果端口名称和节点名称不相同，你必须知道这两个名称，并根据接入点使用正确的名称。例如根据你是通过 CC-SG 访问，还是通过 SX 直接访问。

CC-SG 要求使用唯一节点名称。根据这些步骤在 CC-SG 上进行所有更改，确保把唯一名称广播到端口，使名称保持一致，防止连接错误目标。

▶ **用直接端口访问法命名串行目标端口和节点：**

1. 在 CC-SG 上配置 SX 端口时，把节点名称和端口名称设置为相同名称。端口名称广播到 SX。
2. 每个 CC-SG 节点只配置一个串行接口。这样可以确保节点名称是与端口名称相同的唯一名称。
3. 在更改 CC-SG 节点名称时，同时把端口名称更改为相同的名称，使 SX 端口名称与关联节点保持一致。新端口名称广播到 SX。

直接端口访问 SSH 命令

用下列命令与 Dominion SX 设备目标建立直接端口连接。Dominion SX 设备必须受 CC-SG 管理。为了实现直接端口访问，要在一个命令中使用 CC-SG 用户名、节点名称、会话换码符、CC-SG 主机名或 IP 地址。

▶ **命令示例：**

```
ssh -l
username[:ccsg_node_name[:[escape_mode][:escape_char]
]]{hostname | IP_address}
```

直接端口访问命令参数

参数	详细信息
`username`	要建立连接的用户的 CC-SG 用户名。 用户必须拥有目录访问权。
`ccsg_node_name`	串行目标的节点名称。此名称必须与端口名称相同。参看*用直接端口访问法命名串行目标端口和节点* (p. 313)。 ▪ 不允许在名称中使用冒号 ":"。 ▪ ":" 只能用作用户名分隔符，ccsg_node_name、escape_mode 和 escape_character。 ▪ 如果名称包含空格字符，必须用双引号引起来。 ▪ 名称中的左圆括号 "(" 和右圆括号 ")" 必须加上反斜杠 \ 换码。 示例："Port32(2)" 中的圆括号换码 `ssh -l admin:Port32\(2\) 10.0.20.11`
`escape_mode`	可选。escape_mode 参数修改默认换码方式。 `control` 或 `none` control 是默认方式，可以是左空格。即使左空格也使用 ：。 按端口更改 escape_mode，更改只在会话期间有效。更改不是永久性更改。
`escape_char`	可选。escape_char 参数用于修改默认换码符。 默认换码符是]。 按端口更改 escape_char，更改只在会话期间有效。更改不是永久性更改。
`hostname|IP_address`	负责管理 Dominion SX 的 CC-SG 的主机名或 IP 地址。

示例：在 DPA 上把换码符修改为左方括号

▶ **在直接端口访问会话中把换码符修改为左方括号：**

```
ssh -l username:ccsg_node_name::[ {hostname|IP_address}
```

在连接目标之后，用户按 Control+[切换到端口菜单。

示例：在 DPA 上把换码方式修改为无

▶ **在直接端口访问会话中把换码方式修改为无：**

```
ssh -l username:ccsg_node_name:none
{hostname|IP_address}
```

在连接目标之后，用户按默认换码符 Control+] 切换到端口菜单。

串行管理端口

CC-SG 上的串行管理端口可以直接连接 Raritan 串行设备，例如 Dominion SX 或 KSX。

可以用 HyperTerminal 或 PuTTY 等终端仿真程序，通过 IP 地址连接 SX 或 KSX。在终端仿真程序上设置波特率，使其匹配 SX 或 KSX 的波特率。

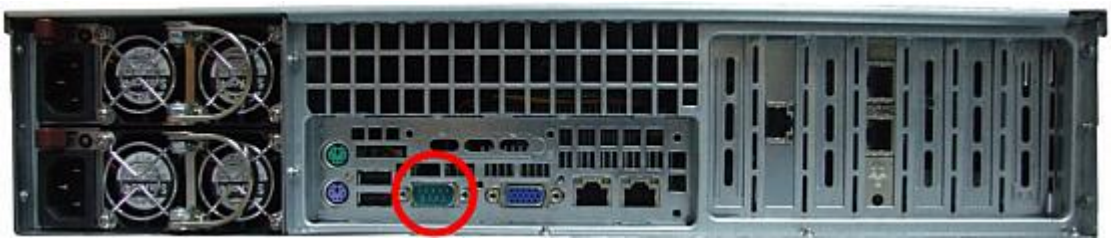
▶ **SX 要求：**

用 ASCSDB9F 适配器把 CC-SG 设备连接到 SX。使用默认 SX 端口设置：9600bps，Parity（奇偶检验）= None（无）/8，Flow Control（流控制）= None（无），Emulation（枚举）= VT100。

▶ **V1 串行管理端口：**

▶ **E1 串行管理端口：**

- 或者 -



关于终端仿真程序

很多 Windows 操作系统有 HyperTerminal。Windows Vista 没有 HyperTerminal。

PuTTY 是免费程序，可以在 Internet 上下载。

建议管理员妥善保存 CC-SG 序列号，尤其是虚拟设备的 CC-SG 序列号。如果技术支持部门需要凭借 FS2 密码给你提供协助，你需要提供序列号。

查找 CC-SG 序列号

▶ **查找 CC-SG 序列号：**

1. 登录 Admin Client。
2. 选择 Help（帮助）> About Raritan Secure Gateway（关于 Raritan Secure Gateway），
3. 打开新窗口显示 CC-SG 序列号。

Web 服务 API

你必须接受最终用户协议，才能把 Web 服务 API 客户机添加到 CC-SG。最多可以添加五个 WS-API 客户机。参看 CC-SG Web 服务 API 指南详细了解如何使用 API。

添加 Web 服务 API：

1. 选择 Access（访问）> Add Web Services API（添加 Web 服务 API）。此选项仅供有 CC 设置和控制权限的用户使用。
2. 阅读最终用户协议。
   - 可以通过复制并粘贴文本来保存协议，或者选择 Secure Gateway（安全网关）> Print（打印）。
   - 在完成配置之后，此协议也可以在 Access（访问）菜单上访问。
3. 单击 Accept（接受）按钮打开 New Web Services API Configuration（新 Web 服务 API 配置）窗口。
4. 输入有关 Web 服务客户机的必要数据。
   - Web Services Client Name（Web 服务客户机名称）：最多 64 个字符。
   - License Key（许可密钥）：Raritan 提供的许可密钥。每台 CC-SG 设备必须有一个唯一许可密钥。
   - IP Address/Hostname（IP 地址/主机名）：最多 64 个字符。
   - HTTPS Web Services Port（HTTPS Web 服务端口）：只读字段。在生成信任关系时，CC-SG 使用端口 9443。
   - Licensed Vendor Name（许可供应商名称）：最多 64 个字符。
5. 生成自签名证书。
   a. 加密模式：如果在 Administration（管理）> Security（安全）> Encryption（加密）屏幕上选择了 Require AES Encryption between Client and Server（要求在客户机和服务器之间使用 AES 加密）复选框，AES-128 是默认值。如果不要求使用 AES，DES 3 是默认值。
   b. Private Key Length（私有密钥长度）：默认值是 1024。
   c. Validity Period (days)（有效期(天)）：最多 4 个数字字符。
   d. Country Code（国家代码）：CSR 标记是国家名称。
   e. State or Province（州/省）：最多 64 个字符。输入完整州名/省名。不要输入缩写。

f. City/Locality（城市/地区）：CSR 标记是地区名称。最多 64 个字符。

g. Registered Company Name（公司注册名称）：CSR 标记是机构名称。最多 64 个字符。

h. Division/Department Name（事业部/部门名称）：CSR 标记是机构单位名称。最多 64 个字符。

i. Fully Qualified Domain Name（全限定域名）：CSR 标记是公用名。

j. Administrator Email Address（管理员电子邮件地址）：输入负责证书请求的管理员的电子邮件地址。

k. Challenge Password（挑战密码）：最多 64 个字符。

注意：Challenge Password（挑战密码）仅供 CC-SG 在内部用于生成证书。你不必记住密码。

---

l. Password（密码）：输入密钥存储器密码。凭此密码打开要在第七步保存的 .P12 文件。如果复制生成的证书并把它导入自己的密钥存储器，不必记住此密钥存储器密码。

6. 单击 Generate Certificate（生成证书）。Certificate（证书）字段显示文本。
7. 单击 Save to File（保存成文件）按钮把证书保存成 .P12 文件。或者复制生成的证书，把它导入自己的密钥存储器。
8. 单击 Add（添加）按钮保存更改。

CC-NOC

在 CC-SG 4.2 之前，不能在 CC-SG 上访问 CC-NOC。

Ch 16 诊断控制台

诊断控制台是在本地提供 CC-SG 访问的非图形菜单界面。可以通过串行端口或 KVM 端口访问诊断控制台。参看*通过 VGA/键盘/鼠标端口访问诊断控制台* (p. 319)。也可以通过 PuTTY 或 OpenSSH Client 等 Secure Shell (SSH) 客户机访问诊断控制台。参看*通过 SSH 访问诊断控制台* (p. 319)。

诊断控制台有两个界面：

1. Status Console（状态控制台）。参看*关于状态控制台* (p. 320)。
2. Administrator Console（管理员控制台）。参看*关于管理员控制台* (p. 326)。

注意：在通过 SSH 访问诊断控制台时，状态控制台和管理员控制台继承了 SSH 客户机外观设置和键盘绑定。这些外观设置可能与本指南所述的设置有差异。

在本章内

访问诊断控制台

通过 VGA/键盘/鼠标端口访问诊断控制台

1. 个 VGA 监视器、PS2 键盘和鼠标插入 CC-SG 设备背板上。
2. 按 Enter，屏幕显示 login 提示符。

通过 SSH 访问诊断控制台

1. 在与 CC-SG 有网络连接的客户 PC 上启动 SSH 客户机，例如 PuTTY。
2. 如果 CC-SG 已注册到 DNS 服务器，指定 CC-SG 的 IP 地址或 IP 主机名。
3. 指定端口号 23。默认 SSH 端口是 22。如果不把端口更改为 23，SSH 客户机只访问 CC-SG 命令行界面，不访问诊断控制台。
4. 单击允许你建立连接的按钮，打开一个窗口提示你输入登录名。

状态控制台

关于状态控制台

- 可以用状态控制台检查 CC-SG 的健康状况，CC-SG 使用的各种服务的健康状况，以及所连接的网络的健康状况。
- 在默认情况下，状态控制台不需要密码。
- 可以配置 CC-SG，通过 Web 接口提供状态控制台信息。必须启用与 Web 状态控制台有关的选项。参看*通过网络浏览器访问状态控制台* (p. 320)。通过 Web 提供的状态控制台信息可以采用帐号和密码加以保护。

访问状态控制台

可以采用不同的方法查看状态控制台信息：VGA/键盘/鼠标端口、SSH 或网络浏览器。

通过 VGA/键盘/鼠标端口或 SSH 访问状态控制台

▶ **通过 VGA/键盘/鼠标端口或 SSH 访问状态控制台：**

1. 访问诊断控制台。参看*访问诊断控制台* (p. 319)。
2. 在 login 提示符下输入 status。
3. 显示当前系统信息。

通过网络浏览器访问状态控制台

为了通过 Web 检索状态控制台信息，必须在诊断控制台上启用相关选项，Web 服务器必须正常工作。

▶ **1: 在诊断控制台上启用与 Web 状态控制台有关的选项：**

1. 选择 Operation（操作）> Diagnostic Console Config（诊断控制台配置）。
2. 在 Ports（端口）列表上选择 Web。
3. 在 Status（状态）列表上选择 Web 旁边的 Status（状态）复选框。
4. 单击 Save（保存）按钮。

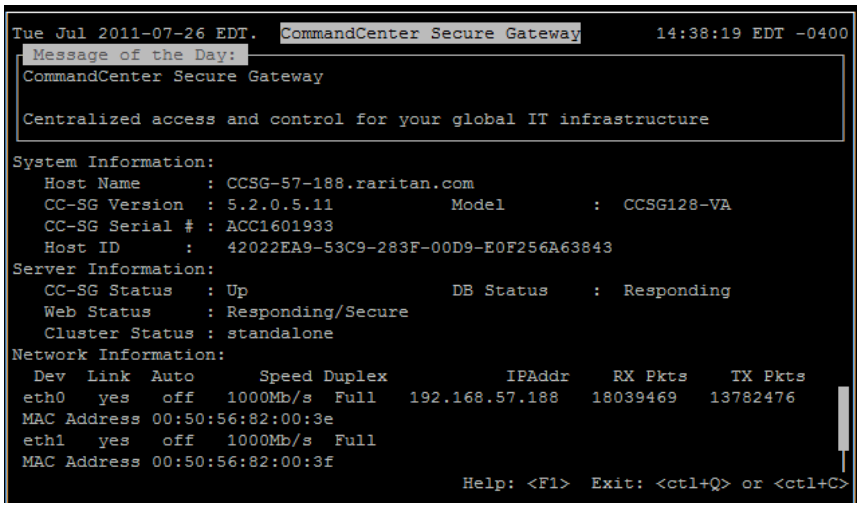
2: 通过网络浏览器访问状态控制台：

1. 使用支持的 Internet 浏览器，输入下列 URL：`http(s)://<IP_address>/status/` where `<IP_address>` is the IP address of the CC-SG.注意必须在 /status 后面加斜杠 (/)，例如 `https://10.20.3.30/status/`。
2. 打开状态页面。本页显示的信息与状态控制台显示的信息相同。

状态控制台信息

通过 VGA/键盘/鼠标端口或 SSH 访问状态控制台

在 login 提示符下输入 status 之后，显示只读状态控制台。



此屏幕动态显示系统健康状况信息，以及 CC-SG 及其子部件是否正常工作。此屏幕上的信息大约每五秒钟更新一次。

状态控制台由四个主要部分组成：

- CC-SG 标题、日期和时间
- 当日消息
- 系统、服务器和网络状态
- 导航键提示

CC-SG 标题、日期和时间

CC-SG 标题固定不变，所以用户知道自己连接一台 CC-SG 设备。

屏幕顶部的日期和时间是上次轮询 CC-SG 数据的时间。日期和时间反映 CC-SG 服务器保存的时间值。

当日消息

Message of the Day（当日消息）字段显示在 CC-SG Admin Client 上输入的当日消息的前五行。每行最多 78 个字符，不支持任何特殊格式。

系统、服务器和网络状态

屏幕的这个部分显示各个 CC-SG 部件的状态信息。下表说明 CC-SG 和 CC-SG 数据库的信息和状态：

信息	Description（说明）
Host Name（主机名）	CC-SG 全限定域名，由设备的主机名和相关的域名构成。
CC-SG Version（CC-SG 版本）	CC-SG 当前固件版本，由五位数构成。
CC-SG Serial #（CC-SG 序列号）	CC-SG 序列号。
Model（型号）	CC-SG 型号。
Host ID（主机 ID）	CC-SG 设备授权号。
CC-SG Status（CC-SG 状态）	负责处理大多数用户请求的 CC-SG 服务器的状态。可能的状态包括：
	Up（运行） — CC-SG 可用，可以接受用户请求。
	Down（停机） — CC-SG 可能停机了，也可能正在重新启动。如果 Down（停机）状态持续很久，尝试重新启动 CC-SG。
	Restarting（正在重新启动） — CC-SG 正在重新启动。
DB Status（数据库状态）	CC-SG 服务器使用内部数据库，这是操作的一部分。数据库必须运行并响应，CC-SG 才能正常工作。可能的状态包括：
	Responding（正在响应） — CC-SG 数据库可用。
	Up（运行） — 某些数据库例程正在运行，但不响应本地请求。
	Restoring（正在恢复） — CC-SG 正在恢复，暂时停止数据库查询。
	Down（停机） — 数据库服务器尚未启动。
Web Status（Web 状态）	对 CC-SG 服务器进行的大多数访问都是通过 Web 进行的。此字段显示 Web 服务器状态，可能的状态包括：
	Responding/Unsecured（正 — Web 服务器正在运行，正在响

信息	Description（说明）	
	在响应/不安全）	应 http（不安全）请求。
	Responding/Secured（正在响应/安全）	Web 服务器正在运行，正在响应 https（安全）请求。
	Up（运行）	某些 Web 服务器进程正在运行，但不响应本地请求。
	Down（停机）	Web 服务器当前不可用。
RAID Status（RAID 状态）	CC-SG 把数据存储在两个镜像 (RAID-1) 磁盘上。RAID 磁盘可能的状态包括：	
	Active（活动）	RAID 正常工作。
	Degraded（降级）	一个或多个磁盘驱动器有问题。联系 Raritan 技术支持部门寻求协助。
Cluster Status（群集状态）	CC-SG 可与另一台 CC-SG 共同构成群集。参看***配置 CC-SG 群集*** (p. 275)。如果此字段显示 standalone（独立），说明 CC-SG 不在群集配置里。否则，此字段显示群集状态。	
Cluster Peer（群集同层）	如果 CC-SG 在群集配置里，此字段显示群集里另一台 CC-SG 设备的 IP 地址。	
Network Information（网络信息）	对于每个网络接口，有一个可以翻页的表显示其信息。对于虚拟 CC-SG，在此列出的各列下面显示每个网卡的 MAC 地址。	
	MAC 地址	对于虚拟 CC-SG ,为每个列出的网卡的 MAC 地址。
	Dev（设备）	接口内部名称。
	Link（链路）	Link Integrity（链路完整性）状态，即此端口是否通过完好电缆连接正常工作的 Ethernet 交换机端口。
	Auto（自动）	说明是否把自动协商应用于此端口。
	Speed（速度）	The speed that this interface is operating: 10, 100 or 1000 Mbits per second.
	Duplex(双工）	说明接口是全双工还是半双工。
	IPAddr(IP 地址）	此接口当前的 Ipv4 地址。
	RX -Pkts（接收的数据包）	自从 CC-SG 启动以来，通过此接口接收的 IP 数据包数。
	TX -Pkts（发送的数据包）	自从 CC-SG 启动以来，通过此接口发送的 IP 数据包数。

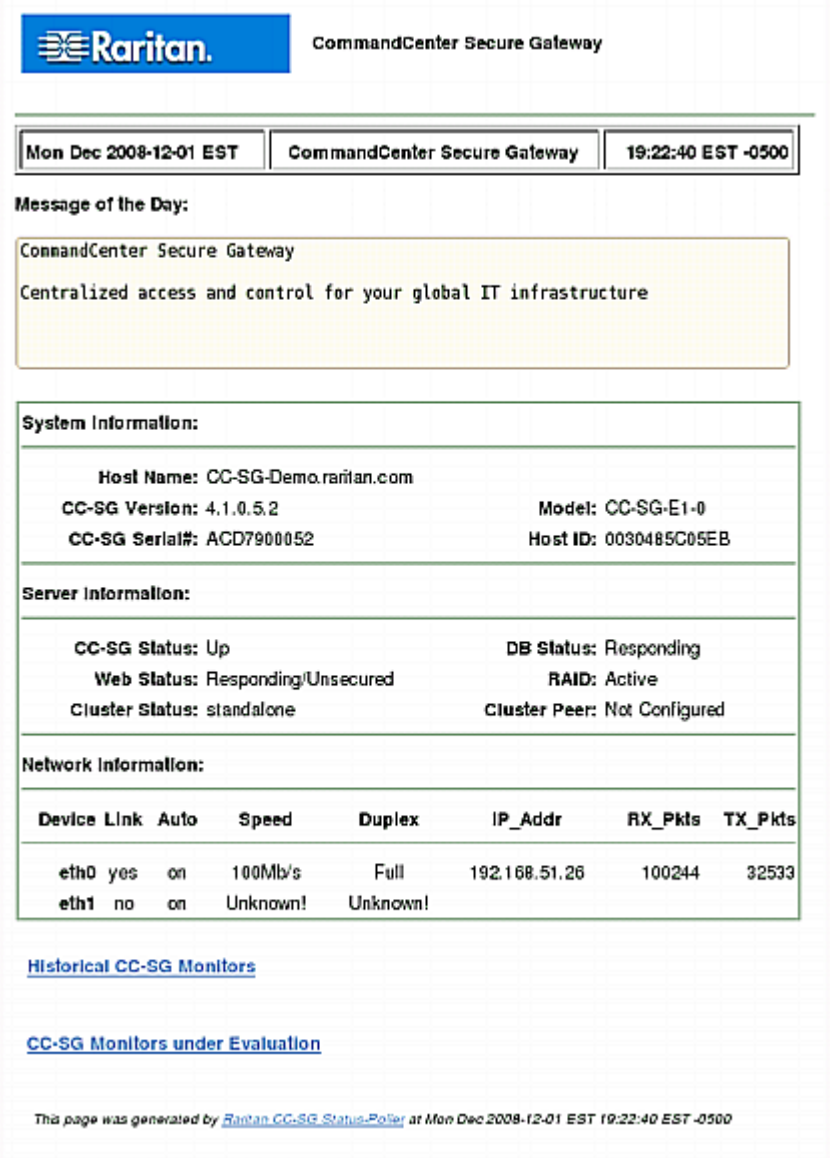
导航键提示

屏幕最下面一行显示键盘组合键，这些组合键用于调用帮助及退出状态控制台。除了下面说明的键，状态控制台不接受其他任何键输入。

- 按 F1 调用帮助屏幕，显示可用选项和诊断控制台版本。
- 按 Ctrl+L 清除当前屏幕，显示更新信息。最快可以每秒更新一次屏幕。
- 按 Ctrl+Q 或 Ctrl+C 退出状态控制台。
- 如果 Network Information（网络信息）屏幕显示的数据有几页，可以按箭头键上下左右翻页。

通过网络浏览器访问状态控制台

在通过网络浏览器连接状态控制台之后，显示状态控制台只读网页。



网页显示的信息与状态控制台相同，大约每五秒钟更新一次信息。如要了解网页底部的 CC-SG 监视器链接，参看*显示历史数据趋势分析报告* (p. 350)和 ***CC-SG** 磁盘监视* (p. 401)。

管理员控制台

关于管理员控制台

管理员控制台允许你设置一些初始参数，提供初始网络配置，调试日志文件，执行一些有限诊断和重新启动 CC-SG。

管理员控制台默认登录证书如下：

- Username（用户名）：admin
- Password（密码）：raritan

重要说明：诊断控制台 admin 帐号是独立的，不同于在 Java CC-SG Admin Client 和 html Access Client 上使用的 CC 超级用户 admin 帐号和密码。更改其中一个密码，并不影响另一个密码。

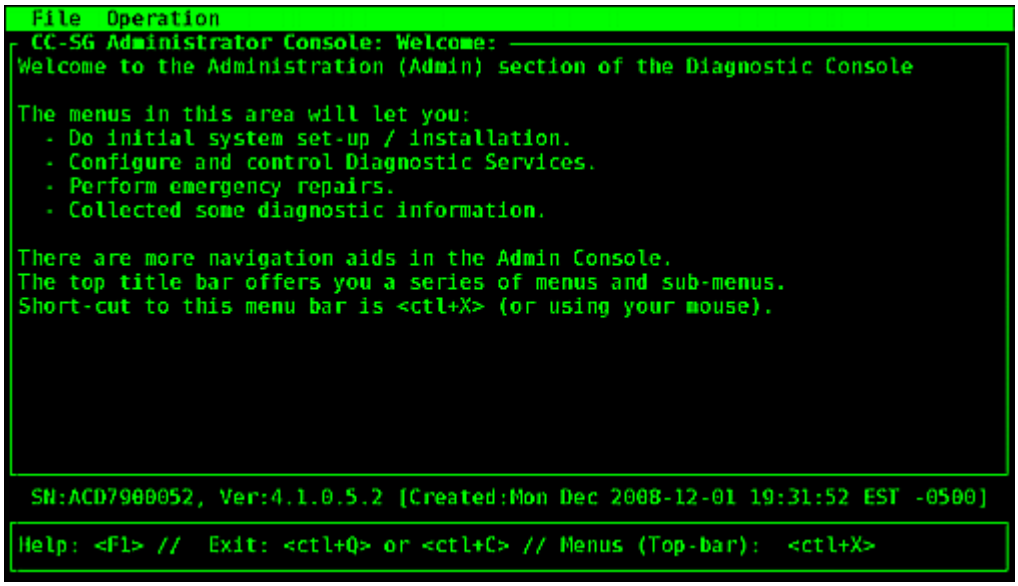
访问管理员控制台

管理员控制台显示的所有信息是静态信息。如果通过 CC-SG Admin Client 或诊断控制台更改配置，必须在配置生效之后重新登录管理员控制台，才能在管理员控制台上看到这些更改。

访问管理员控制台：

1. 在 login 提示符下输入 admin。
2. 输入 CC-SG 密码。默认密码是 raritan。在首次登录时，此密码到期，必须选择新密码。输入此密码，按提示输入新密码。参看 *诊断控制台密码设置* (p. 345)详细了解如何设置密码强度。

显示 Administrator Console（管理员控制台）主屏幕。



管理员控制台屏幕

管理员控制台屏幕由四个主要部分组成：

- **菜单栏：**

  可以激活菜单栏执行管理员控制台功能。按 Ctrl+X 激活菜单栏；如果通过 SSH 客户机访问管理员控制台，可以用鼠标单击菜单项。

File（文件）菜单有一个选项可用于退出诊断控制台。Operation（操作）菜单有四个菜单命令，每个命令可能有一个或多个子菜单。如要了解每个菜单命令和子菜单，参看管理控制台的其他各部分。

- **主显示区：**

  显示内容取决于选择的操作。

- **状态栏：**

  状态栏位于导航键栏上面。它显示某些重要的系统信息，包括 CC-SG 序列号、固件版本、主显示区加载或更新信息的时间。在向 Raritan 技术支持部门报告你遇到的问题时，制作这些信息的截屏可能很有用。

- **导航键栏**：

  参看*导航管理员控制台* (p. 328)。

导航管理员控制台

用键盘组合键导航管理员控制台。对于某些会话，也可以用鼠标导航。但是，并非在所有 SSH 客户机或 KVM 控制台上都可以使用鼠标。

按	操作
Ctrl+X	激活菜单栏。在菜单上选择菜单命令，执行各种管理员控制台操作。
F1	打开帮助屏幕，显示可用选项和诊断控制台版本。
Ctrl+C 或 Ctrl+Q	退出诊断控制台。
Ctrl+L	清除屏幕，刷新信息（但不更新或刷新信息本身）。
选项卡	移动到下一个可用选项。
Space bar	选择当前选项。
Enter	选择当前选项。
箭头键	移动到一个选项内的不同字段。

编辑诊断控制台配置

可以通过串行端口 (COM1) 和 VGA/键盘/鼠标 (KVM) 端口访问诊断控制台，也可以通过 SSH 客户机访问诊断控制台。如果要访问状态控制台，还可以使用 Web 访问方法。

对于每种端口类型，可以配置是否允许输入状态登录名或管理员登录名，现场支持人员是否可以通过此端口访问诊断控制台。对于 SSH 客户机，可以配置应该使用哪个端口号，只要其他 CC-SG 服务不使用此端口即可。对于通过 Web 访问状态控制台，可以指定一个旨在限制访问的、不同于系统里其他任何帐号的帐号。否则，可通过 Web 访问 CC-SG 的任何用户均可访问状态控制台网页。

重要说明：切记不要封锁所有 admin 访问或现场支持访问。

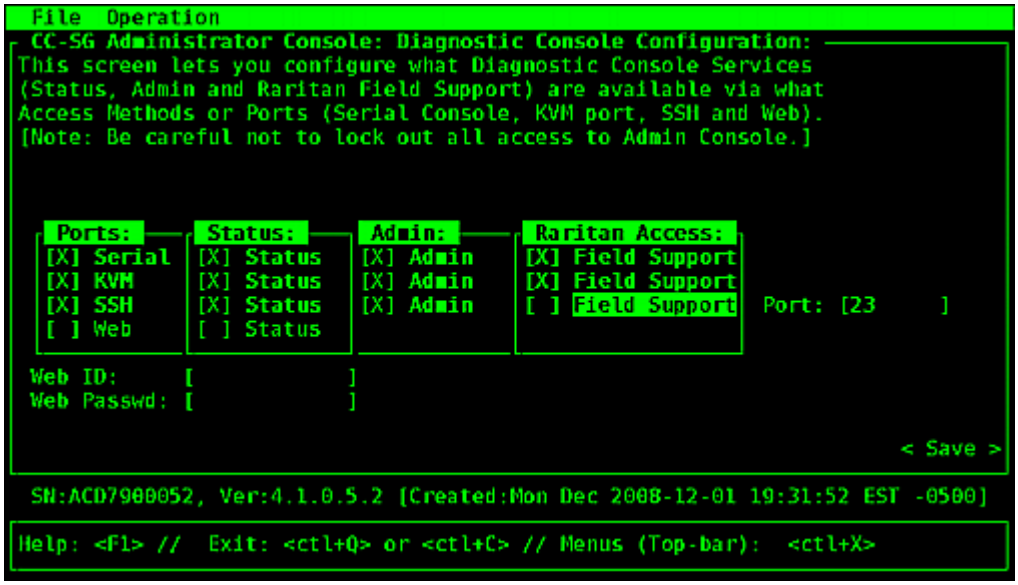
▶ **编辑诊断控制台配置：**

1. 选择 Operation（操作）> Diagnostic Console Config（诊断控制台配置）。
2. 确定如何配置和访问诊断控制台。

有四种诊断控制台访问方法：串行端口 (COM1)、KVM 控制台、SSH（IP 网络） 和 Web。诊断控制台提供三种服务：状态显示、管理员控制台、Raritan 现场支持。此屏幕允许你通过各种访问方法选择哪些服务可用。

如果启用 Web 选项和 Status（状态）选项，只要 Web 服务器正常工作，始终可以访问状态控制台网页。如要限制状态控制台网页访问，输入一个帐号和密码。

3. 在 Port（端口）字段里输入通过 SSH 访问诊断控制台所用的端口号。默认端口是 23。
4. 单击 Save（保存）按钮。



编辑网络接口配置（网络接口）

可以在网络接口配置上执行初始设置任务，例如设置 CC-SG 主机名和 IP 地址。

1. 选择 Operation（操作）> Network Interfaces（网络接口）> Network Interface Config（网络接口配置），
2. 如果已经配置了网络接口，显示一条警告消息，告诉你应该用 CC-SG Admin Client 配置接口。如果要继续，单击 Yes（是）按钮。
3. 在 Host Name（主机名）字段里输入主机名。在保存之后，更新此字段，显示全限定域名（如已知）。参看*术语/缩写语* (参看 "*术语/缩略语*" p. 2)了解主机名规则。
4. 在 Mode（模式）字段里选择 IP Isolation（IP 隔离）或 IP Failover（IP 故障切换）。参看*关于网络设置* (p. 257)。

5. 在 Configuration（配置）字段里选择 DHCP 或 Static（静态）。
   - 如果选择 DHCP，且正确配置了 DHCP 服务器，在保存设置、退出并重新进入管理控制台之后，自动填充 DNS 信息、域后缀、IP 地址、默认网关和子网掩码。
   - 如果选择 Static（静态），输入 IP Address（IP 地址[必填]）、Netmask（子网掩码[必填]）、Default Gateway（默认网关[可选]）、Primary DNS（主 DNS [可选]）和 Secondary DNS（备用 DNS [可选]），在 Domain Suffix（域后缀[可选]）字段里输入域名。
   - 即使用 DHCP 分配接口 IP 配置，仍然要输入格式正确的 IP 地址和子网掩码。
6. 在 Adapter Speed（适配器速度）字段里选择一个线路速度。滚动列表上有 10 Mbps、100 Mbps 和 1000 Mbps 三个值（每次只能看到一个值），用箭头键选择值。按空格键选择显示的选项。对于 1Gbps 线路速度，选择 AUTO（自动）。
7. 如果没有给 Adapter Speed（适配器速度）选择 Auto（自动），单击 Adapter Duplex（适配器双工），然后在列表上用箭头键选择一种双工模式（FULL [全双工]或 HALF [半双工]）（如适用）。虽然任何时候都可以选择一种双工模式，但只有在 Adapter Speed（适配器速度）不是 Auto（自动）时才有意义并发生作用。
8. 如果选择了 IP Isolation（IP 隔离）模式，重复这些步骤配置第二个网络接口。
9. 单击 Save（保存）按钮。CC-SG 重新启动：退出所有 CC-SG GUI 用户，终止其会话。显示警告屏幕，说明即将重新配置网络，以及它对相关 CC-SG GUI 用户的影响。选择 <Yes（是）>按钮继续。

   诊断控制台状态屏幕显示系统进度。在 KVM 端口上，按 Alt+F2 并输入 status 登录，可以选择另一个终端会话。按 Alt+F1，可以返回原终端会话。按 F1 至 F6，可以使用六个可用终端会话。

编辑 IPv6 网络接口配置

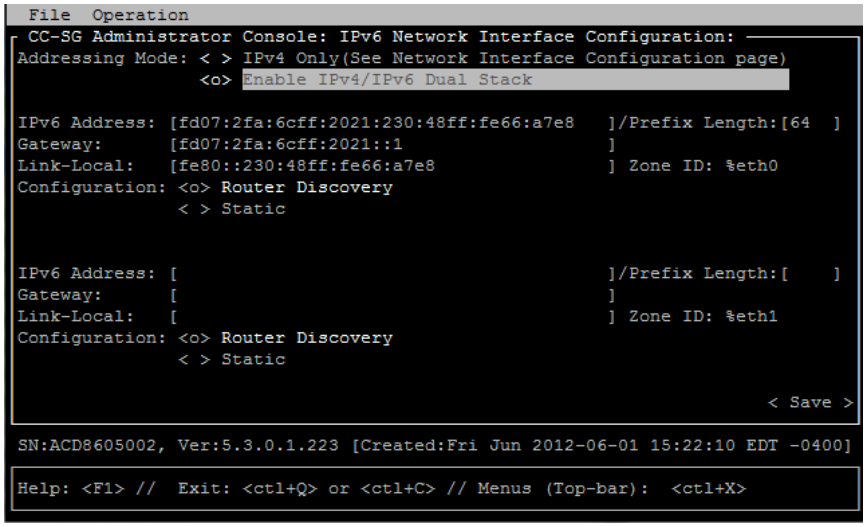
在 IPv6 Network Interface Configuration（IPv6 网络接口配置）页上启用或禁用双协议堆。需要重新启动 CC-SG。

如果只使用 IPv4，选择 IPv4 Only（仅 IPv4），然后进入 Operation（操作）> Network Interface Configuration（网络接口配置）页输入设置。参看*编辑网络接口配置* (参看 "*编辑网络接口配置（网络接口）*" p. 329)。

在输入 IPv6 网络信息之前，必须先在 Operation（操作）> Network Interface Configuration(网络接口配置)页上选择 IP Isolation mode(IP 隔离模式）或 IP Failover mode（IP 故障切换模式）。参看*编辑网络接口配置* (参看 "*编辑网络接口配置（网络接口）*" p. 329)。

1. 如要给 CC-SG 配置双协议堆 IPv6 网络，选择 Enable IPv4/IPv6 Dual Stack（启用 IPv4/IPv6 双协议堆）。
2. 选择 Router Discovery（路由器发现）或 Static（静态）。

   在 Admin Console 上，Global/Unique Local IPv6 Address 标记为 IPv6 Address（IPv6 地址）。
3. 如果选择 Router Discovery（路由器发现），自动填充部分字段：Global/Unique Local IPv6 Address(全局/唯一本地 IPv6 地址）、Prefix Length（前缀长度）、Default Gateway IPv6 Address（默认网关 IPv6 地址）、Link-Local IPv6 Address(链路本地 IPv6 地址)和 Zone ID（域 ID）。
4. 如果选择 Static（静态），输入 Global/Unique Local IPv6 Address（全局/唯一本地 IPv6 地址）、Prefix Length(前缀长度)和 Default Gateway IPv6 Address（默认网关 IPv6 地址）。



5. 单击 Save（保存）按钮。CC-SG 重新启动：退出所有 CC-SG GUI 用户，终止其会话。显示警告屏幕，说明即将重新配置网络，以及它对相关 CC-SG GUI 用户的影响。选择 <Yes（是）>按钮继续。
6. 诊断控制台状态屏幕显示系统进度。在 KVM 端口上，按 Alt+F2 并输入 status 登录，可以选择另一个终端会话。按 Alt+F1，可以返回原终端会话。按 F1 至 F6，可以使用六个可用终端会话。

Ping IP 地址

用 ping 命令检查 CC-SG 计算机和特定 IP 地址之间的连接是否正常工作。

注意：有些网站明确禁止 ping 请求。如果 ping 操作失败，确定目标和中间网络是否允许 ping 操作。

1. 选择 Operation（操作）> Network Interfaces（网络接口）> Ping。
2. 在 Ping Target（Ping 目标）字段里输入要检查哪个目标的 IP 地址或主机名（如果在 CC-SG 上正确配置了 DNS）。
3. 选择：**可选。**

选项	说明
Show other received ICMP packets（显示接收的其他 ICMP 数据包）	详细输出，除了 ECHO_RESPONSE 数据包，还列出接收的其他 ICMP 数据包。很少见。
No DNS Resolution（无 DNS 解析）	不把地址解析成主机名。
Record Route（记录路由）	记录路由。启用 IP 记录路由选项，在 IP 报头内存储数据包路由。
Use Broadcast Address（使用广播地址）	允许 ping 广播消息。
Adaptive Timing（自适应定时）	自适应 ping。根据往返时间自动调节数据包之间的时间间隔，使网络上没有响应的检测数据包不超过一个。最小时间间隔是 200 毫秒。

4. 输入 ping 命令执行秒数、要发送的 ping 请求数和 ping 数据包大小。默认值是 56 字节，加上 8 字节 ICMP 报头数据，总共 64 字节 ICMP 数据。如果保留空白，将使用默认值。**可选。**
5. 单击 Ping 按钮。如果结果显示一系列响应，表示连接正常工作。响应时间说明连接速度有多快。如果显示 timed out（超时）错误而非响应，表示计算机和域之间的连接不工作。参看***编辑静态路由*** (p. 334)。

6. 按 Ctrl+C 终止会话。

注意：按 CTRL+Q 键显示到目前为止的会话统计摘要，继续 ping 目标。

使用跟踪路由

跟踪路由常用于排除网络故障。显示数据包经过的所有路由器，便于你确定从自己的计算机到网络上特定目的地要经过的路径。它列出到达目的地所经过的所有路由器，或者列出到失败并放弃数据包时经过的所有路由器。以外，它还告诉你从一台路由器到另一台路由器，每一"跳"有多长。这有助你确定路由问题，或者确定哪个防火墙阻止你访问站点。

对 IP 地址或主机名执行跟踪路由：

1. 选择 Operation（操作）> Network Interfaces（网络接口）> Traceroute（跟踪路由）。
2. 在 Traceroute Target（跟踪路由目标）字段里输入要检查哪个目标的 IP 地址或主机名。
3. 选择：**可选。**

选项	Description（说明）
Verbose（详细）	详细输出，除了 TIME_EXCEEDED 和 UNREACHABLE，还列出接收的其他 ICMP 数据包。
No DNS Resolution（无 DNS 解析）	不把地址解析成主机名。
Use ICMP (vs. normal UDP)（使用 ICMP [相对于正常 UDP]）	使用 ICMP ECHO 代替 UDP 数据报。

4. 输入跟踪路由命令在出站检测数据包里使用多少跳（默认是 30），在检测数据包里使用的 UDP 目的地端口（默认是 33434），以及跟踪路由数据包的大小。如果保留空白，将使用默认值。**可选。**
5. 单击窗口右下角的 Traceroute（跟踪路由）按钮。
6. 按 Ctrl+C 或 Ctrl+Q 终止跟踪路由会话。显示 Return? 提示符，按 Enter 返回 Traceroute（跟踪路由）菜单。当 Traceroute（跟踪路由）由于"到达目的地"或"超过跳数"事件而终止时，也显示 Return? 提示符。

编辑静态路由

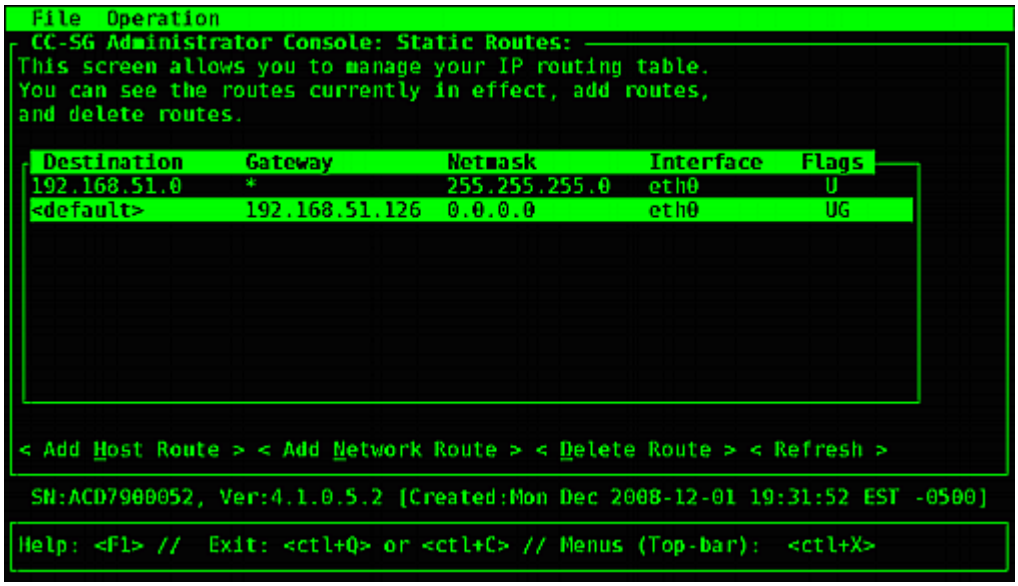
可以在静态路由上查看当前 IP 路由表，可以修改、添加和删除路由。谨慎使用和替换静态路由实际上可以有效提高网络性能，你可以给重要业务应用程序保留带宽。单击鼠标选择值，或者使用 Tab 键和箭头键导航并按 Enter 选择值。

注意：也可以设置 IPv6 网络静态路由。选择 Operation（操作）> Network Interfaces（网络接口）> Static Routes（静态路由）。在 CC-SG 重新启动或执行故障切换之后，并不保存这些路由。。

查看或更改静态路由：

1. 选择 Operation（操作）> Network Interfaces（网络接口）> Static Routes（静态路由）。
2. 打开当前 IP 路由表页面。可以选择 Add Host Route（添加主机路由）或 Add Network Route（添加网络路由），把相关 IP 路由添加到路由表上。可以选择路由表上的项，可以选择 Delete Route（删除路由）删除路由表上的路由。单击 Refresh（刷新）按钮更新路由表里的路由信息。
   - Add Host Route（添加主机路由）接受目的地主机 IP 地址和/或网关 IP 地址或接口名称，如状态控制台所示。
   - Add Network Route（添加网络路由）与此类似，但接受目的地网络地址和子网掩码。
   - 对于在表上选择或突出显示的每一项，可以选择 Delete Route（删除路由）删除此路由。唯一例外是 CC-SG 不允许你删除与当前主机和接口关联的路由。

虽然可以删除包括默认网关在内的其他所有路由，但这样做会严重影响与 CC-SG 的通信。



在诊断控制台上查看日志文件

可以用日志查看器同时查看一个或多个日志文件，这样可以一次浏览多个文件，检查系统活动情况。

只有在关联列表活动（例如用户进入日志文件列表区或选择新排序选项）时， 才更新 Logfile（日志文件）列表。文件名前面有时间戳，表示日志文件最近何时收到新数据，或者日志文件的大小。

时间戳和文件大小缩写：

时间戳：

- s = 秒
- m = 分钟
- h = 小时
- d = 天

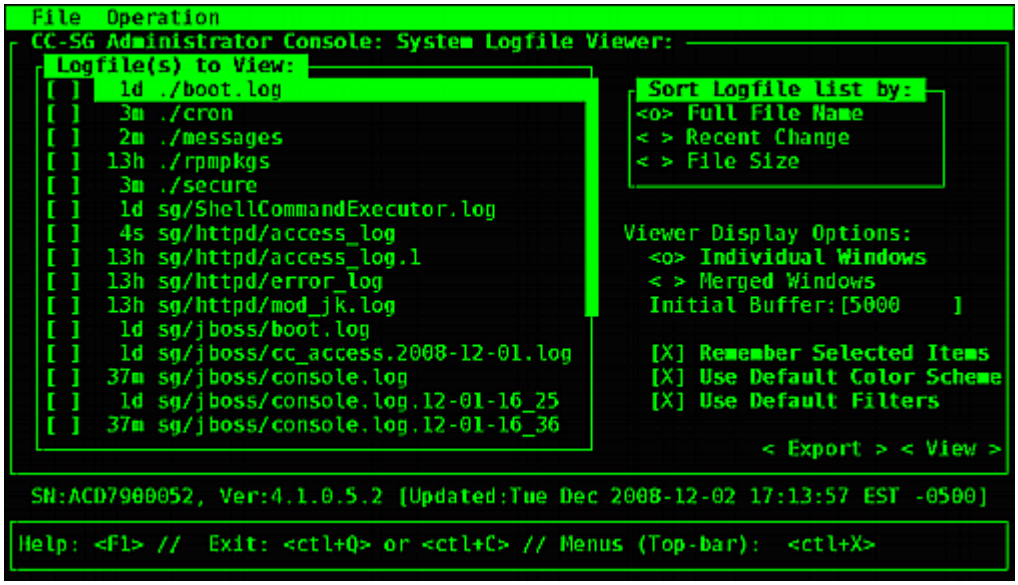
文件大小：

- B = 字节
- K = 千字节（1,000 字节）
- M = 兆字节（1,000,000 字节）
- G = 千兆字节（1,000,000,000 字节）

查看日志文件：

1. 选择 Operation（操作）> Admin（管理）> System Logfile Viewer（系统日志文件查看器）。
2. 日志查看器屏幕分成四个主要部分：
   - 系统上当前可用的日志文件列表。如果列表长度比显示窗口长，可以用箭头键滚动列表。
   - 日志文件列表排序条件。日志文件可以按全文件名、最近更改的日志文件或最大文件大小进行排序。
   - Viewer Display（查看器显示）选项。
   - Export / View（导出/查看）选择器。

3. 单击鼠标或用箭头键导航，按空格键选择一个日志文件，给它标上 X。可以同时查看多个日志文件。



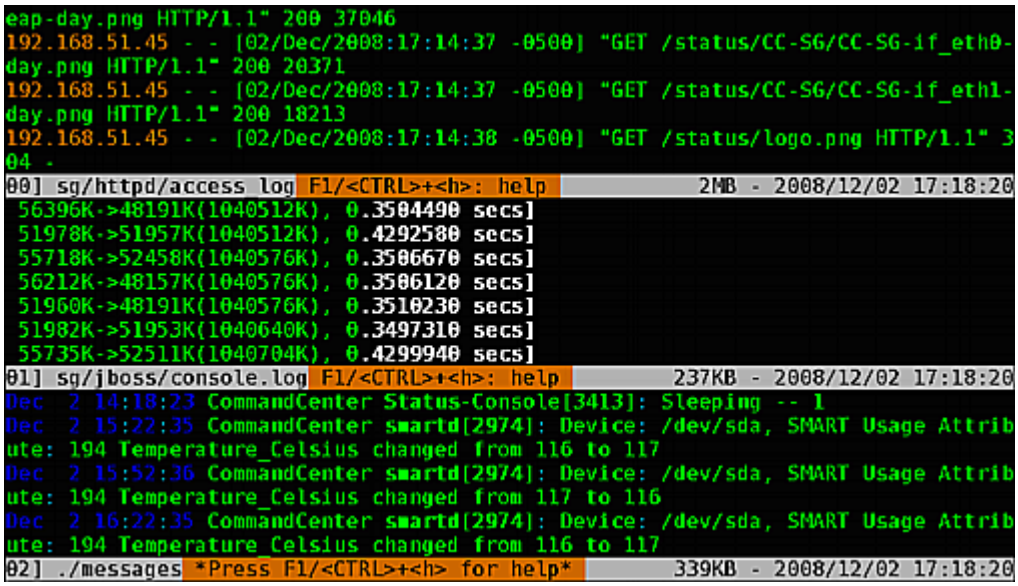
排序 Logfiles to View（要查看的日志文件）列表：

Sort Logfile list by（日志文件列表排序方式）选项控制 Logfile to View（要查看的日志文件）列表按什么顺序显示日志文件。

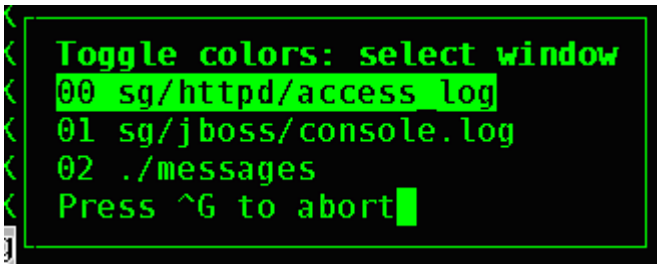
选项	说明
Individual Windows（单独窗口）	用单独的子窗口显示所选的日志。
Merged Windows（合并窗口）	把所选的多个日志合并到一个显示窗口上。
Initial Buffer（初始缓冲区）	设置初始缓冲区或历史记录大小。默认值是 5000。本系统配置为缓冲所接收的所有新信息。
Remember Selected Items（记住选择的项）	如果选择此复选框，将记住当前的日志文件选择（如有）。否则在每次生成新日志文件列表时，复位上次的选择。如果要逐个浏览文件，这很有用。
Use Default Color Scheme（使用默认色彩方案）	如果选择此复选框，在查看部分日志文件时将使用标准色彩方案。注意：在查看日志文件时，可以用 multitail 命令更改色彩方案。
Use Default Filters（使用默认过滤器）	如果选择此复选框，将对部分日志文件应用自动过滤器。
Export（导出）	此选项把选择的所有日志文件打包，使其可以通过 Web 访问，这样可以检索它们，并把它们转发给 Raritan 技术支持部门。客户不能访问此数据包的内容。导出的日志文件最长保存 10 天，之后系统自动删除这些文件。

选项	说明
View（查看）	查看选择的日志。

在选择 View（查看）和 Individual Windows（单独窗口）时，显示 LogViewer：



- 在查看日志文件时，输入 Q、Ctrl+Q 或 Ctrl+C 返回上一个屏幕。
- 可以更改日志文件颜色，突出显示重要部分。输入 C 更改日志文件的颜色，在列表上选择一个日志。

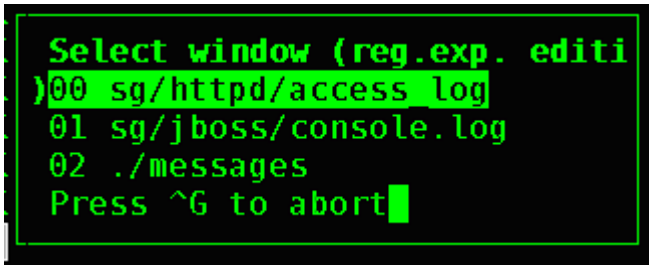


- 输入 I 显示系统信息。

注意：在此管理员控制台会话启动时，系统加载的信息是静态信息 — 用 TOP 工具动态监视系统资源。

用正则表达式过滤日志文件：

1. 如果选择查看几个日志文件，输入 e 添加或编辑正则表达式，在列表上选择一个日志。



2. 输入 A 添加一个正则表达式。例如为了显示 sg/jboss/console.log 日志文件里 WARN 消息中的信息，输入 WARN，然后选择 match。

注意：此屏幕还显示 console.log 的默认过滤方案，删除大部分 Java 堆消息。

用诊断控制台重新启动 CC-SG

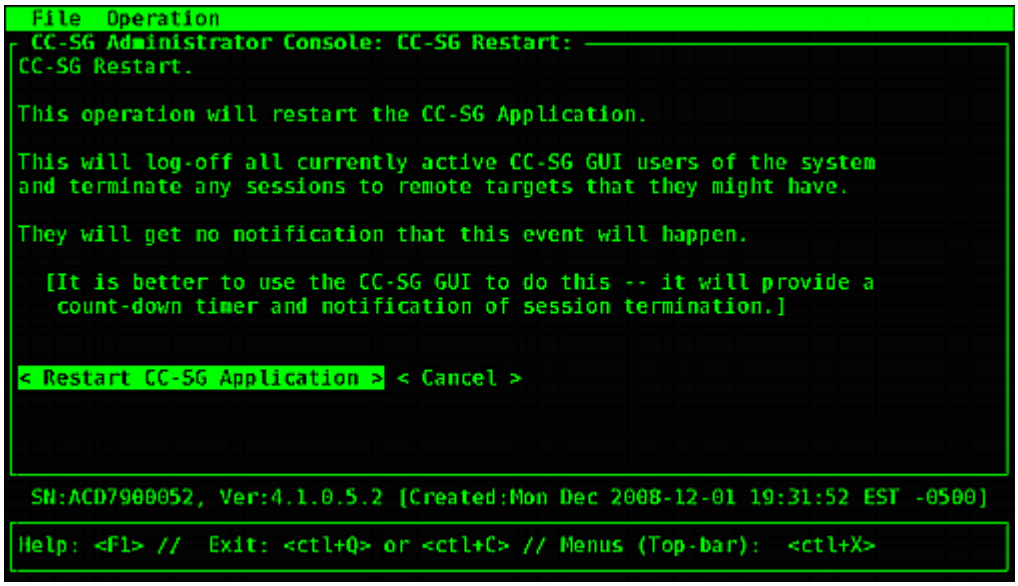
在重新启动 CC-SG 时，退出当前的所有 CC-SG 用户，终止他们的远程目标服务器会话。

重要说明：强烈建议你在 Admin Client 上重新启动 CC-SG，除非绝对

有必要在诊断控制台上重新启动它。参看*重新启动 CC-SG* (p. 243)。在诊断控制台上重新启动 CC-SG 时，不通知用户要重新启动 CC-SG。

用诊断控制台重新启动 CC-SG：

1. 选择 Operation（操作）> Admin（管理）> CC-SG Restart（CC-SG 重新启动）。
2. 单击 Restart CC-SG Application（重新启动 CC-SG 应用程序）按钮，或者按 Enter。在下一个屏幕上确认重新启动，继续操作。



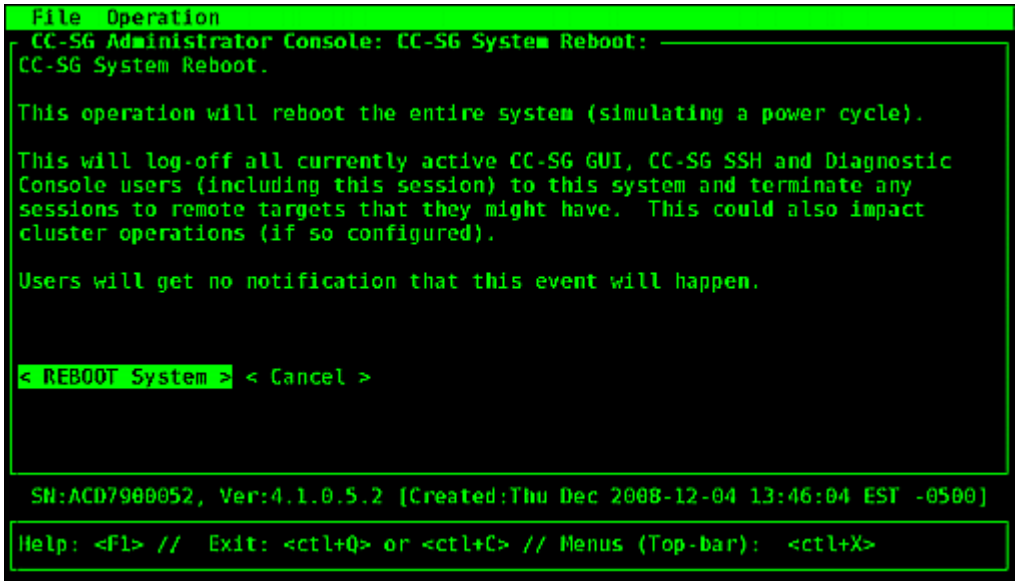
用诊断控制台重新启动 CC-SG

此选项重新启动整个 CC-SG，模拟重新通电操作。用户不会收到通知。CC-SG 用户、SSH 用户和诊断控制台用户（包括此会话）被注销。终止所有远程目标服务器连接。

重新启动 CC-SG：

1. 选择 Operation（操作）> Admin（管理）> CC-SG System Reboot（CC-SG 系统重新启动）。

2. 单击 REBOOT System（重新启动系统）或按 Enter 重新启动 CC-SG。在下一个屏幕上确认重新启动，继续操作。



在诊断控制台上关闭 CC-SG 系统

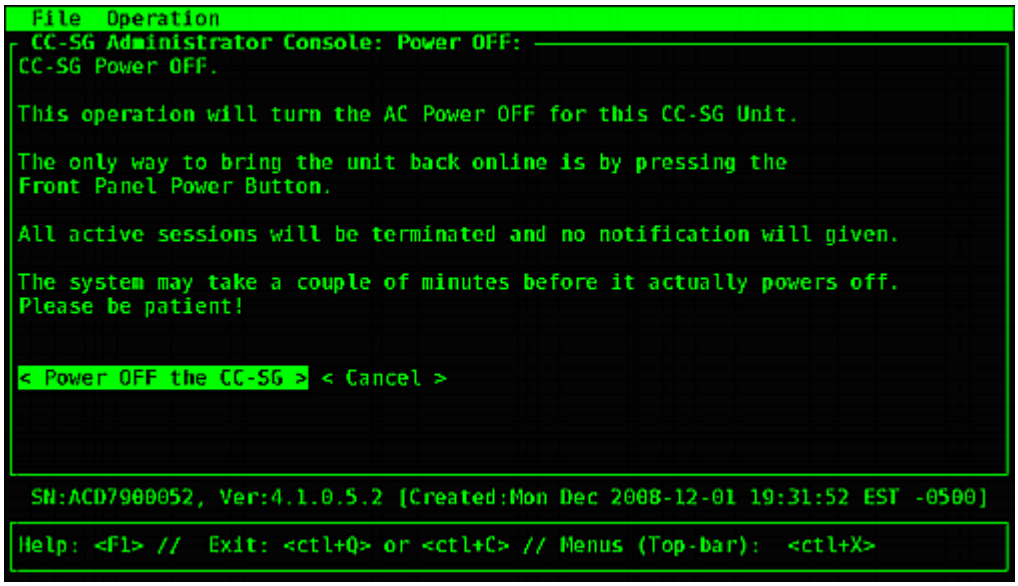
此选项将关闭 CC-SG 设备。登录用户不会收到通知。CC-SG 用户、SSH 用户和诊断控制台用户（包括此会话）被注销。终止所有远程目标服务器连接。

给 CC-SG 设备重新通电的唯一方法是按设备面板上的电源按钮。

▶ **关闭 CC-SG：**

1. 选择 Operation（操作）> Admin（管理）> CC-SG System Power OFF（CC-SG 系统关机）。

2. 单击 Power OFF the CC-SG（关闭 CC-SG）或者按 Enter，断开 CC-SG 的交流电源。在下一个屏幕上确认关机操作，继续操作。



用诊断控制台复位 CC 超级用户密码

此选项把 CC 超级用户帐号的密码复位到出厂默认值。

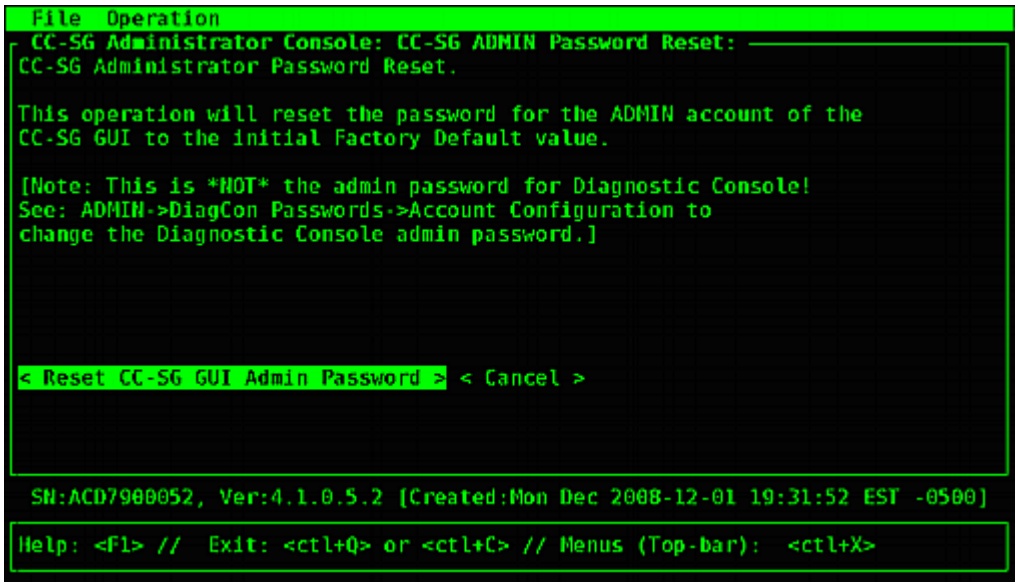
出厂默认密码：raritan

*注意：这不是诊断控制台管理用户的密码。参看***诊断控制台密码设置** *(p. 345)*。

复位 CC-SG GUI 管理密码：

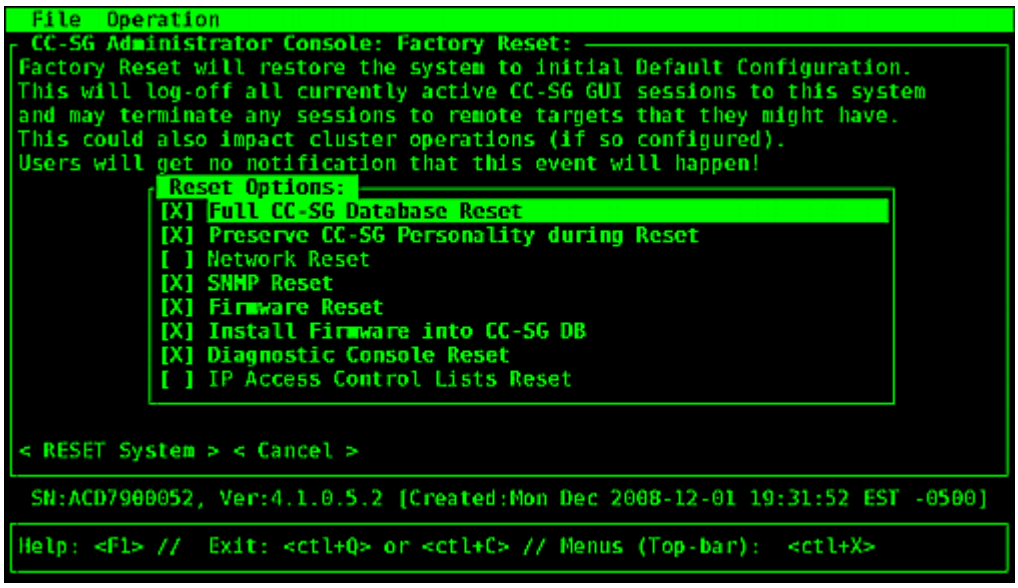
1. 选择 Operation（操作）> Admin（管理）> CC-SG ADMIN Password Reset（CC-SG 管理密码复位）。

2. 单击 Reset CC-SG GUI Admin Password（复位 CC-SG 管理密码）或者按 Enter，把管理密码更改回出厂默认值。在下一个屏幕上确认密码复位，继续操作。



复位 CC-SG 出厂配置

此选项把 CC-SG 系统的所有配置或部分配置复位到出厂默认值。所有 CC-SG 活动用户在不通知的情况下被注销，停止 SNMP 处理。



建议你使用所选的默认选项。

选项	说明
Full CC-SG Database Reset（全 CC-SG 数据库复位）	此选项删除现有的 CC-SG 数据库，用出厂默认值创建一个新数据库。网络设置、SNMP 设置、固件和诊断控制台设置不是 CC-SG 数据库的组成部分。 无论是否选择 IP ACL Tables（IP ACL 表）选项，在使用 Full Database Reset（全数据库复位）时，都复位 IP-ACL 设置。 复位 CC-SG 时删除邻居配置，所以 CC-SG 不再“记住”老邻居。
Preserve CC-SG Personality during Reset（复位时保留 CC-SG 个性化设置）	在选择 Full CC-SG Database Reset（全 CC-SG 数据库复位）时，激活此选项。 在重新创建 CC-SG 数据库时，保存此前配置的某些选项。 ▪ Secure Communication between PC Clients and CC-SG（加密 PC 客户机和 CC-SG 之间的通信） ▪ Enforce Strong Passwords（强制强密码） ▪ Direct vs. Proxy Connections to Out-of-Band nodes（带外节点直接连接和代理连接） ▪ Inactivity Timer setting（闲置计时器设置）
Network Reset（网络复位）	此选项把网络设置复位到出厂默认值。 ▪ Host name（主机名）：CommandCenter ▪ Domain name（域名）：localdomain ▪ Mode（模式）：IP Failover（IP 故障切换） ▪ Configuration（配置）：Static（静态） ▪ IP Address（IP 地址）：192.168.0.192 ▪ Netmask（子网掩码）：255.255.255.0 ▪ Gateway（网关）：none（无） ▪ Primary DNS（主 DNS）：none（无） ▪ Secondary DNS（备用 DNS）：none（无） ▪ Adapter Speed（适配器速度）：Auto（自动）
SNMP Reset（SNMP 复位）	此选项把 SNMP 设置复位到出厂默认值。 ▪ Port（端口）：161 ▪ Read-only Community（只读公用名）：public ▪ Read-write Community（读写公用名）：private ▪ System Contact, Name, Location（系统联系人、名称、位置）：无 ▪ SNMP Trap Configuration（SNMP 陷阱配置） ▪ SNMP Trap Destinations（SNMP 陷阱目的地）

选项	说明
Firmware Reset（固件复位）	此选项把所有设备固件文件复位到出厂默认值。此选项不更改 CC-SG 数据库。
Install Firmware into CC-SG DB（把固件安装到 CC-SG 数据库）	此选项把当前 CC-SG 版本的固件文件加载到 CC-SG 数据库里。
Diagnostic Console Reset（诊断控制台复位）	此选项把 Diagnostic Console（诊断控制台）设置复位到出厂默认值。
IP Access Control Lists Reset（IP 访问控制表复位）	此选项删除 IP-ACL 表上的所有项。 无论是否选择 IP Access Control Lists reset（IP 访问控制表复位）选项，在使用 Full Database Reset（全数据库复位）时，都复位 IP-ACL 设置。 参看 *访问控制表* (p. 295)。

把 CC-SG 复位到出厂配置：

1. 选择 Operation（操作）> Admin（管理）> Factory Reset（出厂复位）。
2. 选择复位选项。
3. 单击 Reset System（复位系统）。
4. 界面显示警告消息和进度条。进度条说明当前复位状态，在复位结束之前，不能控制 CC-SG。

在复位 CC-SG 时，切勿切断 CC-SG 电源，切勿给 CC-SG 重新通电，切勿中断 CC-SG，否则可能会丢失 CC-SG 数据。

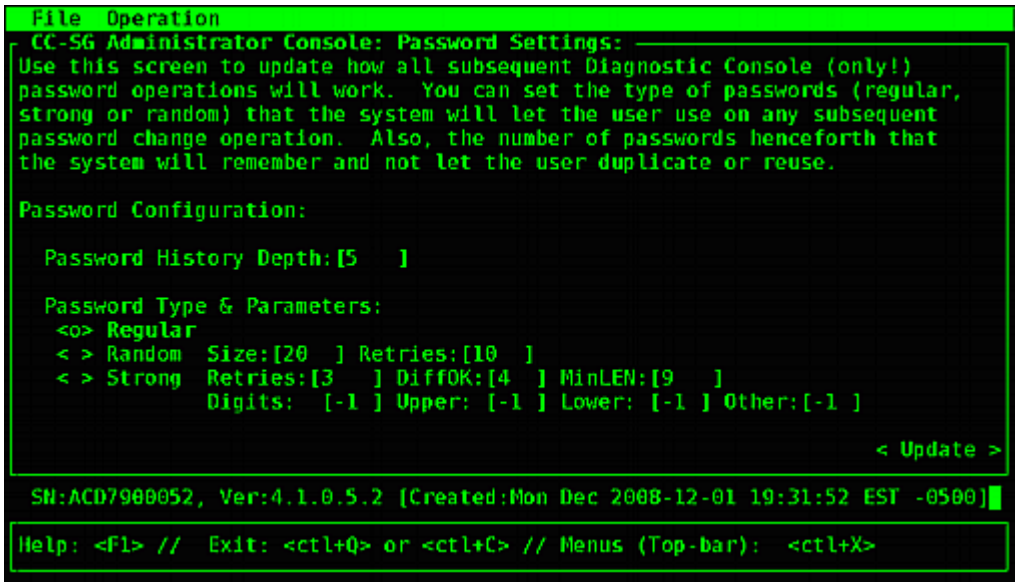
诊断控制台密码设置

此选项允许你配置密码强度（status 和 admin）和密码属性，例如设置密码有效天数（应该通过 Account Configuration [帐号配置]菜单配置）。这些菜单上的操作仅适用于诊断控制台帐号（status 和 admin）和密码，不适用于常规 CC-SG GUI 帐号和密码。

配置诊断控制台密码：

1. 选择 Operation（操作）> Admin（管理）> DiagCon Passwords（诊断控制台密码）> Password Configuration（密码配置）。

2. 在 Password History Depth（密码历史深度）字段里输入要记住的密码数。默认设置是 5。



3. 给 admin 密码和 status（如果启用）密码选择 Regular（常规）、Random（随机）或 Strong（强）。

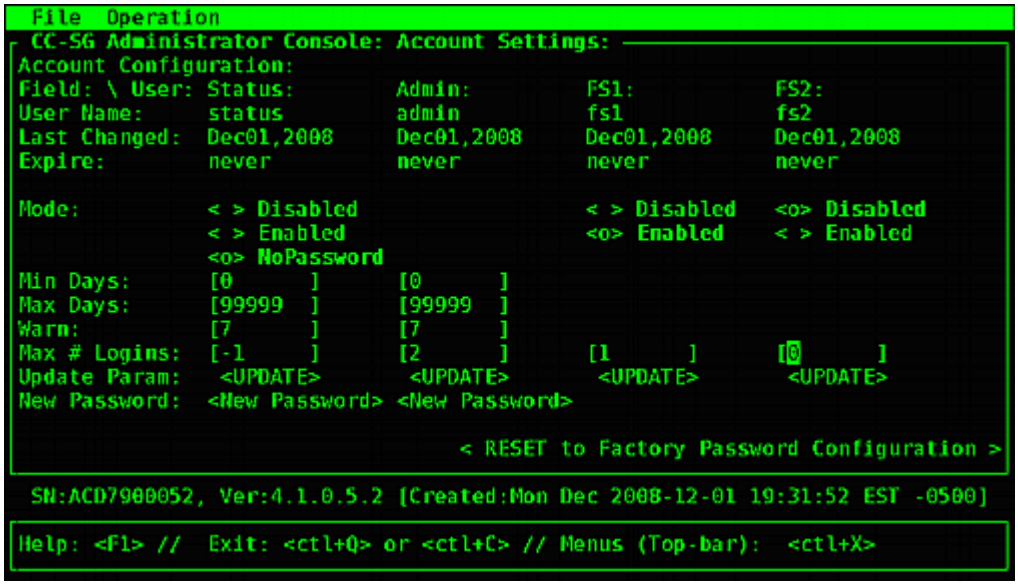
密码设置	说明
Regular（常规）	这是标准选项。密码至少有 4 个字符，限制较少。这是系统默认的密码配置。
Random（随机）	提供随机生成的密码。配置最大密码位数（最小 14 位，最大 70 位，默认 20 位）和再试次数（默认 10 次），后者是询问是否接受新密码的次数。可以接受随机密码（输入新密码两次），也可以拒绝随机密码。不能自己选择密码。
Strong（强）	强制使用强密码。 再试次数是在显示错误消息之前提示你的次数。 DiffOK 表示新密码相对于旧密码可以有多少个相同字符。 MinLEN 是密码要求的最小长度。指定密码要求多少位、多少个大写字母、多少个小写字母和多少个其他（特殊）字符。 正数表示可累加到“简单”数的、此类字符的最大“信用”数。 负数表示密码至少要有多少个此类字符。因此，数字 -1 表示每个密码至少要有一个此类字符。

诊断控制台帐号配置

默认情况下，status 帐号不需要密码，但可以配置它使用密码。可以配置 admin 密码的其他属性，可以启用或禁用 Field Support（现场支持）帐号。

配置帐号：

1. 选择 Operation（操作）> Admin（管理）> DiagCon Passwords（诊断控制台密码）> Account Configuration（帐号配置）。
2. 可以在显示的屏幕上查看每个帐号的设置：Status、Admin、FS1 和 FS2。



此屏幕分成三个主要部分：

- 顶部显示有关系统帐号的只读信息。
- 中间显示与每个 ID 相关的各种参数，还有一组按钮，便于你更新这些参数，或者给帐号设置新密码。
- 下半部是把密码配置恢复到出厂默认值（或者系统最初交付时的状态）。

3. 如果希望 status 帐号使用密码，选择它下面的 Enabled（启用）复选框。
4. 可以给 Admin 和 Status 帐号配置：

设置	说明
User/User Name（用户/用户名）	（只读）。这是此帐户的当前用户名或 ID。

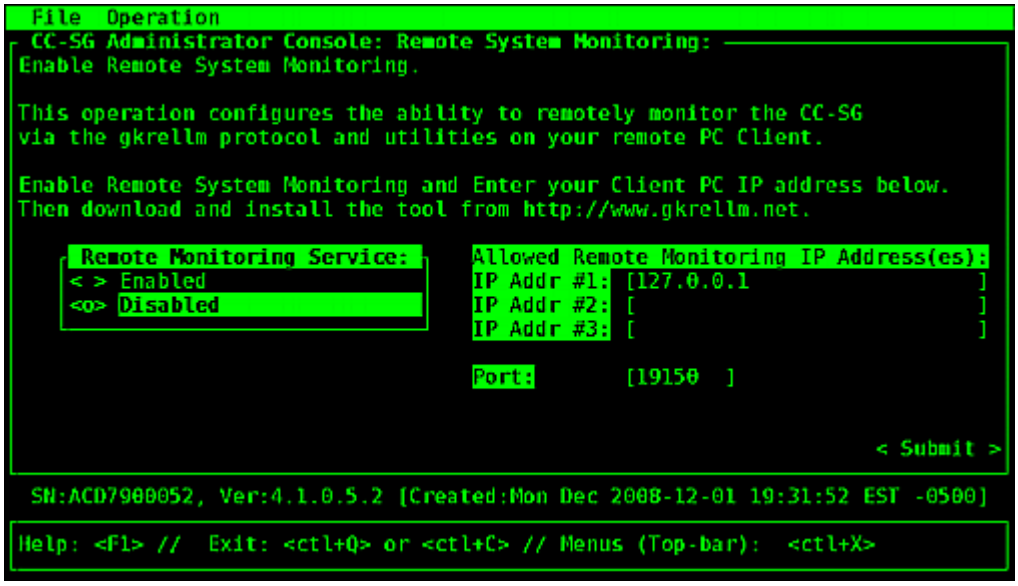
设置	说明
Last Changed（上次更改日期）	（只读）。这是上次更改此帐户的密码的日期。
Expire（到期）	（只读）。这是必须更改此帐号的密码的日期。
Mode（模式）	可配置选项：帐号是被禁用（不允许登录）、启用（需要验证令牌），还是允许访问且不需要密码。（不要同时封锁 Admin 和 FS1 帐号，否则不能使用诊断控制台。）
Min Days（最少天数）	密码最小有效天数。默认端口是 0。
Max Days（最大天数）	密码最大有效天数。默认端口是 99999。
Warning（警告）	在密码到期之前，提前多少天发出警告消息。
Max # of Logins（最大登录数）	一个帐号允许的最大同时登录数。负数表示没有限制（status 登录名的默认值是 -1）。0 表示任何人都不能登录。正数表示可以同时登录的用户数（admin 登录名的默认值是 2）。
UPDATE	保存对此 ID 所做的任何更改。
New Password（新密码）	输入帐号的新密码。

配置远程系统监视

可以启用远程系统监视功能，从而使用 GKrellM 工具。GKrellM 工具采用图形视图显示 CC-SG 设备的资源利用率。此工具类似 Windows 任务管理器的 Performance（性能）选项卡。

1: 启用 CC-SG 设备远程系统监视：

1. 选择 Operation（操作）> Utilities（工具）> Remote System Monitoring（远程系统监视）。



2. 在 Remote Monitoring Service（远程监视服务）字段里选择 Enabled（启用）。
3. 在 Allowed Remote Monitoring IP Addresses（允许远程监视 IP 地址）字段里输入要监视 CC-SG 设备的客户 PC 的 IP 地址。最多可以输入三个 IP 地址。
4. GKrellM 工具的默认端口是 19150。你可以更改此端口。
5. 选择 Submit（提交）按钮。

2: 下载远程系统监视客户机软件：

1. 访问 www.gkrellm.net。
2. 下载并安装与你的客户 PC 相适应的软件包。

3: 配置要监视 CC-SG 的远程系统监视客户机：

根据 Read Me 文件里的说明，把 CC-SG 设备设置为要监视的目标。

Windows 用户必须用命令行找到 Gkrellm 安装目录，运行在 Read Me 文件里指定的命令。

显示历史数据趋势分析报告

历史数据趋势分析功能收集 CPU 利用率、内存利用率、Java 堆空间和网络流量等信息。把这些信息纳入一个报告里，你可以在 CC-SG 上作为网页查看此报告。报告包括 CC-SG 状态和历史数据链接。

如果 CC-SG 系统时间和日期变成较早的时间和日期，历史数据趋势分析报告停止收集数据。当时间和日期到原时间和日期时，再次开始收集数据。如果 CC-SG 系统时间和日期变成较晚的时间和日期，报告显示的数据不连续。

1: 启用历史数据趋势分析显示：

1. 选择 Operation（操作）> Diagnostic Console Config（诊断控制台配置）。
2. 在 Ports（端口）列表上选择 Web。
3. 在 Status（状态）列表上选择 Web 旁边的 Status（状态）复选框。
4. 单击 Save（保存）按钮。

2: 查看历史数据趋势分析报告：

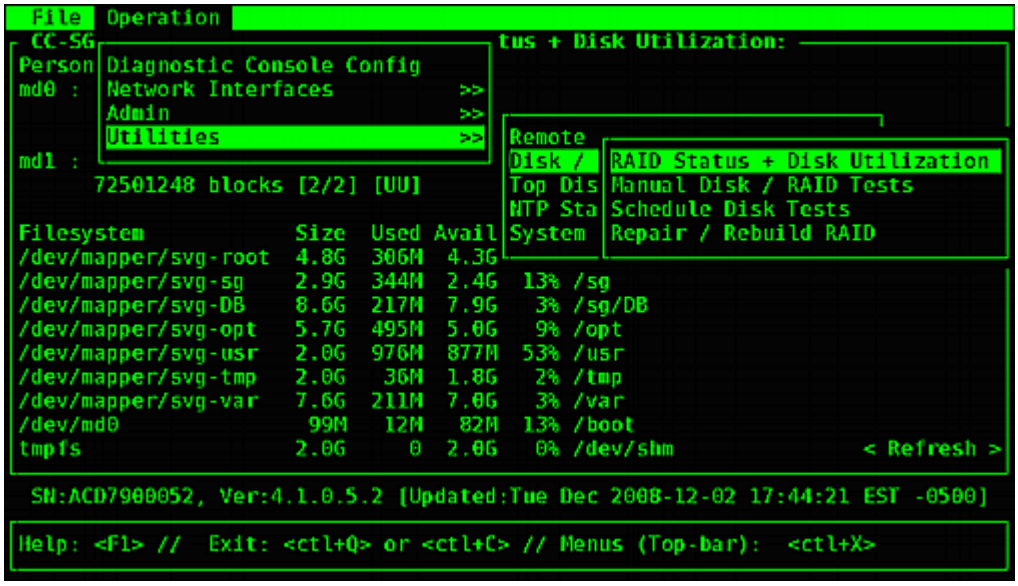
1. 使用支持的 Internet 浏览器，输入下列 URL：`http(s)://<IP_address>/status/` where `<IP_address>` is the IP address of the CC-SG.注意必须在 /status 后面加斜杠 (/)，例如 `https://10.20.3.30/status/`。
2. 打开状态页面。本页显示的信息与状态控制台显示的信息相同。参看***状态控制台*** (p. 320)。
   - 单击 Historical CC-SG Monitors（历史 CC-SG 监视器）链接，查看 CPU 利用率、内存利用率、Java 堆空间和网络流量等信息。单击每个图，在新页上查看详细信息。

显示 RAID 状态和磁盘利用率

此选项显示 CC-SG 磁盘状态，包括磁盘空间大小、活动和运行状态、RAID-1 状态和各个文件系统当前使用的磁盘空间数量。

显示 CC-SG 磁盘状态：

1. 选择 Operation（操作）> Utilities（工具）> Disk/RAID Utilities（磁盘/RAID 工具）> RAID Status + Disk Utilization（RAID 状态和磁盘利用率）。



2. 单击 Refresh（刷新）按钮或者按 Enter，刷新显示信息。在升级或安装时，刷新功能特别有用，你可以看到 RAID 磁盘的重构和同步进度。

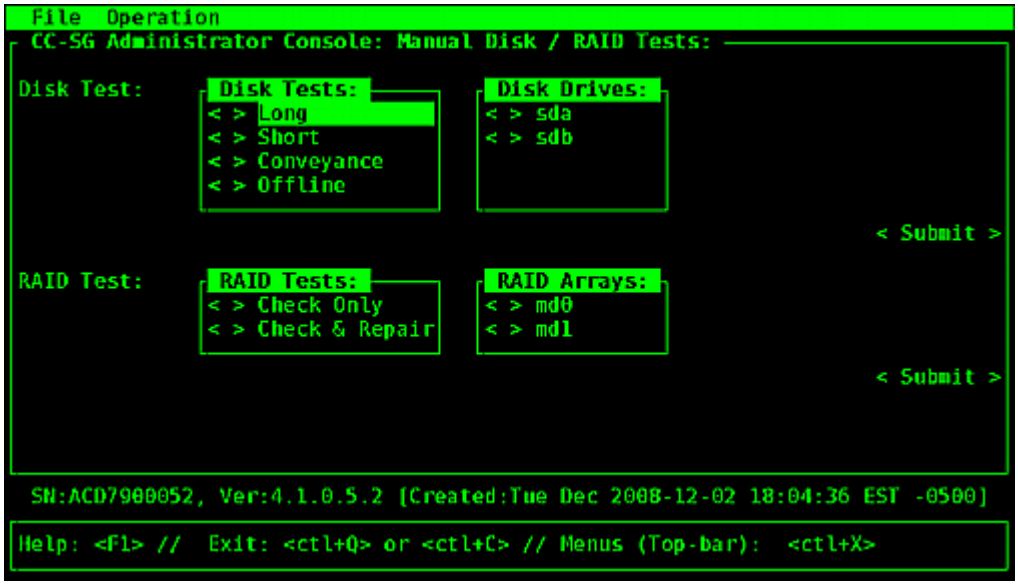
注意：如果显示上述屏幕，表示磁盘驱动器已全面同步，可以使用全 RAID-1 保护。md0 和 md1 阵列的状态都是 [UU]。

测试磁盘或 RAID 测试

可以人工测试 SMART 磁盘驱动器，或者执行 RAID 检查和修复操作。

测试磁盘驱动器，或者执行 RAID 检查和修复操作：

1. 选择 Operation（操作）> Utilities（工具）> Disk/RAID Utilities（磁盘/RAID 工具）> Manual Disk/RAID Tests（人工测试磁盘/RAID）。



2. 测试 SMART 磁盘驱动器：
   a. 在 Disk Test（磁盘测试）部分选择测试类型，以及要测试的磁盘驱动器。
   b. 选择 Submit（提交）按钮。
   c. 预定测试时间，显示 SMART 信息屏幕。
   d. 在到如此屏幕所示的时间之后，可以在 Repair/Rebuild RAID（修复/重构 RAID）屏幕上查看结果。参看***修复或重构 RAID 磁盘*** (p. 355)。
3. 执行 RAID 测试和修复操作：
   a. 在 RAID Test（RAID 测试）部分选择测试类型，以及要测试的 RAID Array（RAID 阵列）。md0 阵列是小启动分区，而 md1 阵列是系统的其余部分。
   b. 选择 Submit（提交）按钮。
   c. RAID Status+Disk Utilization（RAID 状态和磁盘利用率）屏幕显示测试进度。参看***显示 RAID 状态和磁盘利用率*** (p. 351)。**可选。**

d. 在测试完毕之后，可以在 Repair/Rebuild RAID（修复/重构 RAID）屏幕上查看结果。参看***修复或重构 RAID 磁盘*** (p. 355)。如果给定阵列的 Mis-Match（失配）列显示非零值，表示可能有问题，应该联系 Raritan 技术支持部门寻求协助。

预定磁盘测试

可以给磁盘驱动器安排 SMART 测试，定期测试磁盘驱动器。磁盘驱动器固件执行这些测试，可以在 Repair/Rebuild（修复/重构）屏幕上查看测试结果。参看***修复或重构 RAID 磁盘*** (p. 355)。

在 CC-SG 工作时，可以执行 SMART 测试。这些测试对 CC-SG 性能影响很小，但 CC-SG 活动会大大延长 SMART 测试时间。因此，建议你不要进行频繁测试。

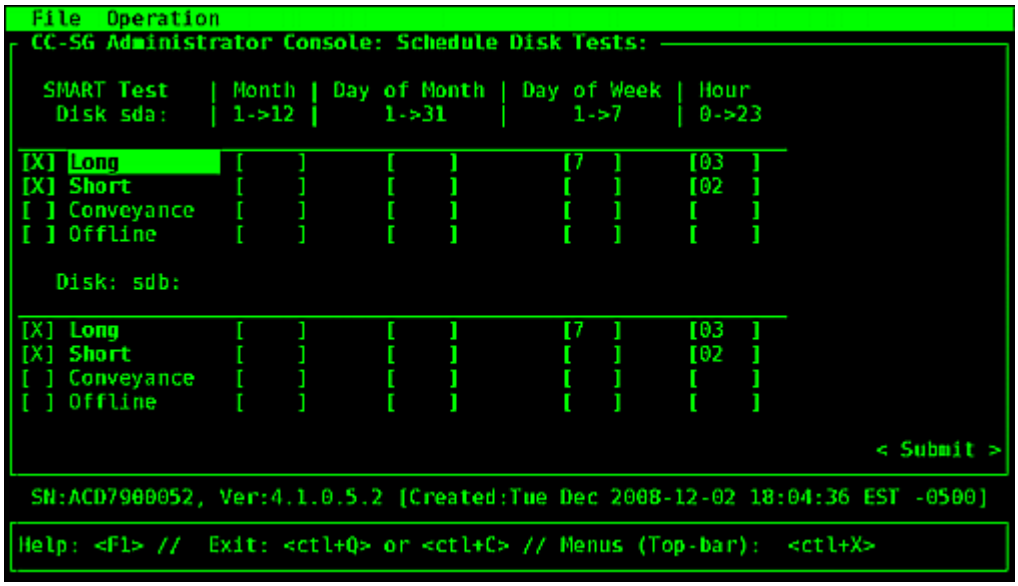
在预定 SMART 测试时，切记下列原则：

- 每次只能针对一个驱动器执行一项测试。
- 如果正在测试一个驱动器，不要预定另一项测试。
- 如果预定两项测试在相同的时间段执行，优先执行测试时间较长的测试。
- 在指定的时间范围内执行测试，未必在时点上执行测试。
- 切勿把 SMART 测试预定在磁盘活动较多的时段，例如 CC-SG 高负荷时段或每天午夜和中午低负荷时段。

注意：CC-SG 预定了一个每天凌晨 2 点执行的 Short（短）测试，还有一个每个星期天凌晨 3 点执行的 Long（长）测试。这些预定测试适用于两种磁盘驱动器。

更改磁盘测试预定：

1. 选择 Operation（操作）> Utilities（工具）> Disk/RAID Utilities（磁盘/RAID 工具）> Schedule Disk Tests（预定磁盘测试）。



2. 单击鼠标或用箭头键移动光标，按空格键选择测试类型，给它标上 X。不同的测试类型所需的时间不同。
   - 在系统负荷不大的情况下，Short（短）测试大约两分钟即可完成。
   - Conveyance（传输）测试大约需要五分钟。
   - Long（长）测试大约需要五十分钟。
   - OffLine（离线）测试最多需要五十分钟。
3. 指定此测试的执行日期和时间。分别在 Month（月）、Day of Month（日）、Day of the Week（星期）和 Hour（小时）字段里输入一个数。
   - 在 Day of the Week（星期）字段里，1 表示星期一，7 表示星期天。
   - Hour（小时）必须是 24 小时格式。

   注意：空白字段可以表示任何值。
4. 选择 Submit（提交）按钮。

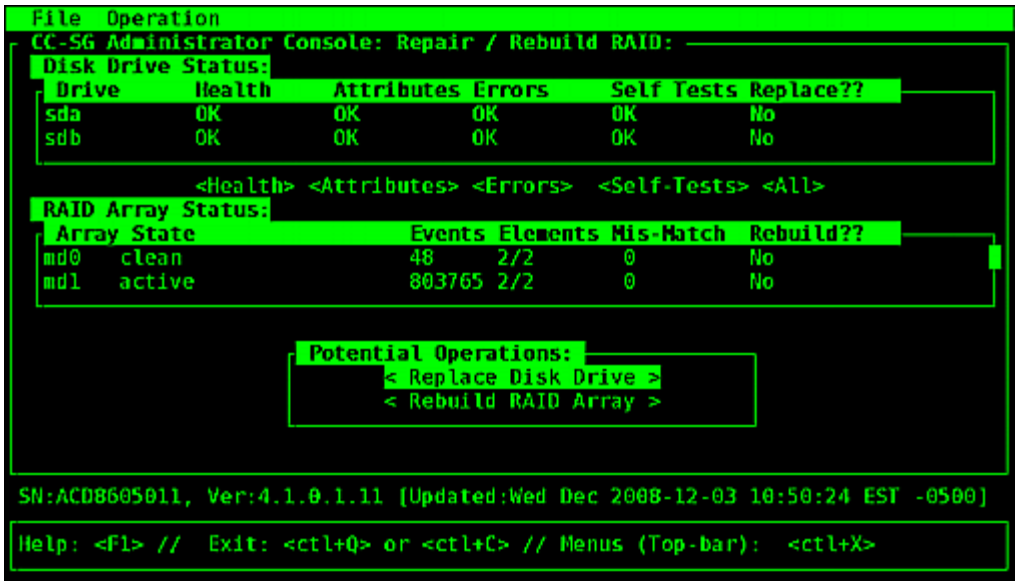
修复或重构 RAID 磁盘

此选项显示磁盘驱动器和 RAID 阵列的某些详细状态信息，说明是否应该更换磁盘驱动器或重构 RAID-1 镜像阵列。在更换或热交换磁盘驱动器之前，向 Raritan 订购备件。

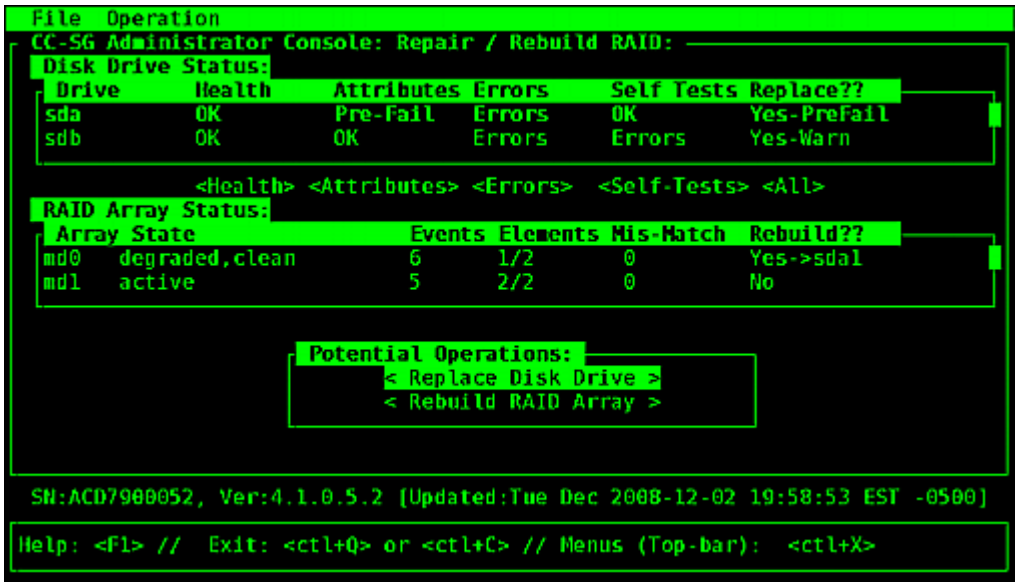
修复或重构 RAID：

1. 选择 Operation（操作）> Utilities（工具）> Disk/RAID Utilities（磁盘/RAID 工具）> Repair/Rebuild RAID（修复/重构 RAID）。
2. 如果任何一项均不在 Replace??（更换??）或 Rebuild??（重构??）列下面显示 No（否），联系 Raritan 技术支持部门寻求协助。

- 正常系统：



- 不正常系统显示存在多个问题：



当你用 Tab 键或单击鼠标在 Disk Drive Status（磁盘驱动器状态）、RAID Array Status（RAID 阵列状态）和 Potential Operations（潜在操作）字段之间来回移动时，系统更新屏幕显示的信息。

3. 可以选择 Disk Drive Status（磁盘驱动器状态）表下面的任何按钮，显示详细 SMART 信息。**可选。**

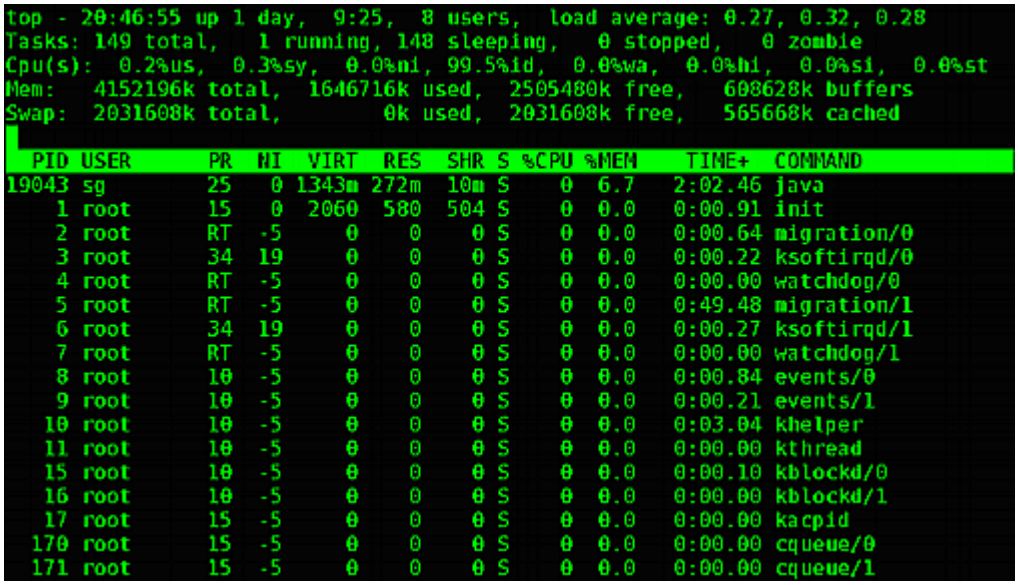
4. 选择 Replace Disk Drive（更换磁盘驱动器）或 Rebuild RAID Array（重构 RAID 阵列），根据屏幕上的说明操作，直到完成操作为止。

用诊断控制台查看 Top 显示

Top 显示允许你查看当前运行的进程列表及其属性，以及整个系统的健康状况。

显示 CC-SG 正在运行的进程：

1. 选择 Operation（操作）> Utilities（工具）> Top 显示。
2. 查看正在运行的所有进程、睡眠进程、停止进程和进程总数。



3. 输入 h 查看 top 命令帮助屏幕。F1（帮助）在这里不起作用。

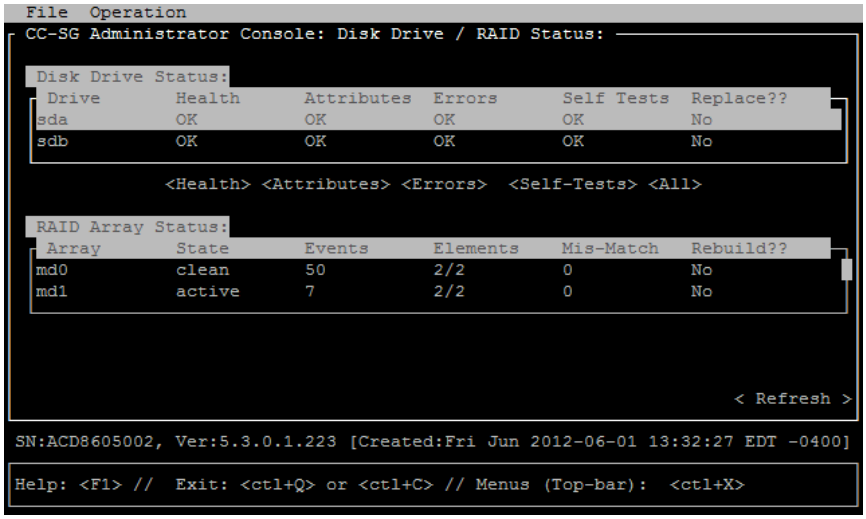
检查磁盘状态

在开始升级 CC-SG 固件之前，先确认 CC-SG 磁盘状态。**如果有迹象表明必须更换驱动器或驱动器有问题，或者必须重构 RAID 阵列或阵列状态有问题，请在升级固件之前联系 Raritan 技术支持部门。** 参看***升级 CC-SG*** (p. 244)。

检查磁盘状态：

1. 选择 Operation（操作）> Utilities（工具）> Disk Drive/RAID Status（磁盘驱动器/RAID 状态）。在不能执行 Replace Disk Drive（更换磁盘驱动器）操作和 Rebuild RAID Array（重构 RAID 阵列）操作的情况下，可以用此选项查看磁盘状态。

2. 确认不需要更换磁盘驱动器，且磁盘状态没有任何问题。



显示 NTP 状态

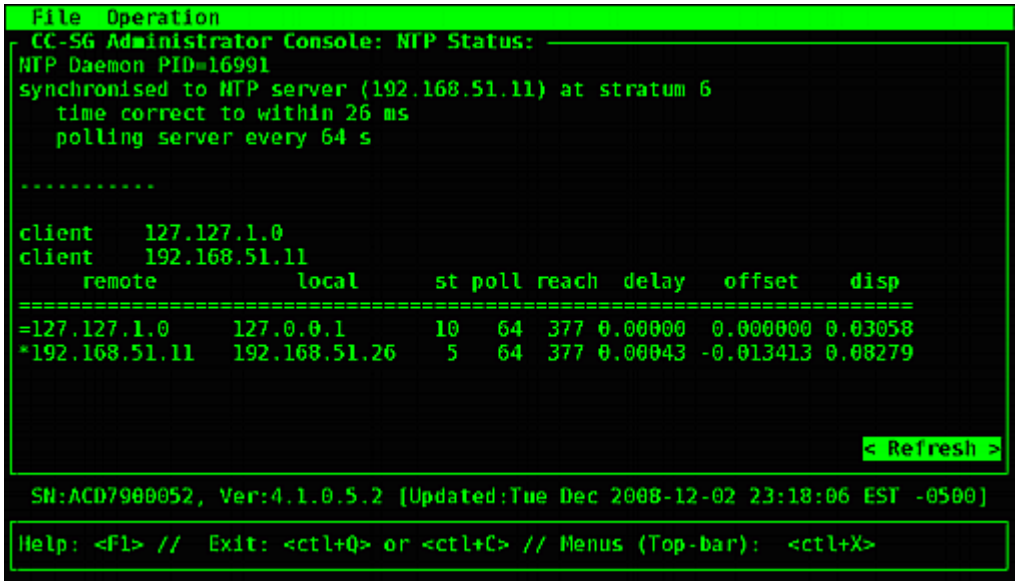
如果在 CC-SG 上配置了并运行 NTP，可以显示 NTP 时间后台进程的状态。NTP 后台进程只能在 CC-SG 管理员 GUI（即 Admin Client）上配置。

显示 CC-SG 运行的 NTP 后台进程的状态：

1. 选择 Operation（操作）> Utilities（工具）> NTP Status Display（NTP 状态显示）。

- 没有启用 NTP，或者配置错误：

- NTP 配置正确且运行：



制作系统快照

当 CC-SG 不能正常工作时，如果你能捕捉并给 Raritan 技术支持部门提供 CC-SG 存储的系统日志、配置或数据库等信息，对分析和排除故障非常有用。

1: 制作 CC-SG 快照：

1. 选择 Operation（操作）> Utilities（工具）> System Snapshot（系统快照）。
2. 单击或选择 Yes（是）。打开 System Snapshot（系统快照）菜单。
3. 确认屏幕显示的每个 %Used（已使用百分比）值是否低于 60%，确保有足够空间供快照操作使用。否则要终止快照操作并执行清理操作，也可以联系 Raritan 技术支持部门寻求协助。
4. System Snapshot（系统快照）选项分为两个部分。
   - Snapshot Configuration（快照配置）显示可制作快照的 CC-SG 数据的列表。
   - Snapshot Operations（快照操作）显示在激活快照操作之后，可以执行的操作的列表。
5. 通常不必更改默认快照选择，除非 Raritan 技术支持部门要求你这么做。如果要求你这么做，单击鼠标或用箭头键移动光标，按空格键选择希望的快照选项，给它标上 X。默认选择 Clean-up JBoss heap dump（清理 JBoss 堆转储）选项。在执行快照之后，自动删除 JBoss 堆转储文件。
6. 单击或选择 Submit（提交）按钮继续执行快照操作。
7. 在快照过程中，你会看到屏幕迅速滚动显示项目列表。有时 CC-SG 暂停滚动，这是正常现象。
8. 在快照操作结束之后，CC-SG 显示快照信息，包括：
   - CC-SG 快照文件的位置和文件名
   - 大小
   - MD5 校验和

   快照信息仅供参考，不必把它们记录下来。
9. 按 Enter 返回 System Snapshot（系统快照）菜单。

2: 检索 CC-SG 快照文件：

1. 使用支持的 Internet 浏览器，输入下列 URL：`http(s)://<IP_address>/upload/`，其中 `<IP_address>` 是 CC-SG 的 IP 地址。注意必须在 `/upload` 后面加斜杠 (/)，例如 `https://10.20.3.30/upload/`。
2. 打开 Enter Network Password（输入网络密码）对话框。在 User Name（用户名）和 Password（密码）字段里输入诊断控制台 admin 帐号的用户名和密码，单击 OK（确定）按钮登录。
3. 列出 CC-SG 制作的所有可用快照文件。

注意：CC-SG 保存快照文件 10 天，所以应该及时检索这些文件。

4. 单击有适当文件名的快照文件，也就是名为 snapshot 的快照文件，这是最新的快照文件。这些文件经过压缩、加密和签名，必须按二进制模式传输它们。
5. 在 IE 上保存文件时，单击 Save As（另存为）对话框上的 Save as type（保存类型）下拉列表，然后选择 All Files（所有文件）把它另存为原始文件。

更改诊断控制台的视频分辨率

Raritan 建议你调节诊断控制台视频分辨率，让监视器正确显示菜单。

调节视频分辨率

1. 重新启动 CC-SG。参看***用诊断控制台重新启动 CC-SG*** (p. 340)。
2. 在显示下列消息时，在五秒钟之内按任意键（例如 Esc 或箭头键）进入 GRUB 菜单。

   `Press any key to enter the menu`（按任意键进入菜单）

   `Booting CentOS (x.x.x) in x seconds....`（将在 x 秒后启动 `CentOS (x.x.x)....`）
3. 用上下箭头键突出显示 1024x768/24-bit（1024x768/24 位）选项，按 Enter。

Ch 17 Power IQ 集成

如果你有 CC-SG 和 Power IQ，可以采用几种方法一起使用它们。

不支持用 IPv6 与 Power IQ 通信。

1. 通过 CC-SG 控制 Power IQ IT 设备的电源。

   例如：如果要控制作为 CC-SG 节点的 Power IQ IT 设备的电源，可以在 CC-SG 上用 Power IQ Proxy 接口发出电源控制命令。

2. 利用 CSV 文件导入和导出，在两个系统之间共享数据。

   例如：如果在 IP 网络上与 CC-SG 一起部署了大量 Dominion PX 设备，可以在 CC-SG 上导出含有所有节点名称的 CSV 文件，按规定编辑文件，然后把它导入 Power IQ。参看*导出 **Dominion PX** 数据在 **Power IQ** 上使用* (p. 369)。

   如果与 Power IQ 一起部署了大量 Dominion PX 设备，你可能想把最新的 IT 设备名称作为节点导入 CC-SG，可以在 Power IQ 上导出一个文件，按规定编辑文件，然后把它导入 CC-SG。参看*从 **Power IQ** 导入电源条* (p. 367)。

3. 在同步 Power IQ 和 CC-SG 时，自动把在 Power IQ 上配置的 IT 设备导入 CC-SG。参看*配置 **Power IQ** 和 **CC-SG** 同步* (p. 365)。

在本章内

Power IQ IT 设备电源控制

可以用 CC-SG 控制已作为节点添加到 CC-SG 的 Power IQ IT 设备的电源。

使你能控制与不受 CC-SG 管理的 PDU 相连的节点的电源。

配置 Power IQ 服务

必须先配置 Power IQ 服务，才能把 Power IQ Proxy 接口添加到节点，或者同步 Power IQ 和 CC-SG，把 IT 设备作为节点添加到 CC-SG。这是通过 CC-SG Access（访问）菜单配置的。

你必须具备 CC 设置和控制权限，才能配置 Power IQ 服务。

配置 Power IQ 服务：

1. 确保在 Power IQ 上启用 Web API。单击设置选项卡上安全和加密部分的其他安全设置。

   选择 Web API 设置部分的启用 Web API 复选框，然后单击保存按钮。

2. 确保在 Power IQ 上启用电源控制。单击 Settings（设置）选项卡上 Appliance Administration（设备管理）部分的 Power Control Options（电源控制选项）。选择 Enable Power Control（启用电源控制）复选框，然后单击 Save（保存）按钮。

3. 在 CC-SG Admin Client 上选择 Access（访问）> Power IQ Services（Power IQ 服务）> Add Power IQ Services（添加 Power IQ 服务）。打开 New Power IQ Services Configuration（新建 Power IQ 服务配置）对话框。

4. 在 Power IQ Device Name（Power IQ 设备名称）字段里输入设备名称。提供此服务的 Power IQ 设备的名称必须是唯一名称。CC-SG 不接受重复名称。参看*命名常规* (p. 431)详细了解 CC-SG 的名称长度规则。

5. 在 IP Address/Hostname（IP 地址/主机名）字段里输入设备的 IP 地址或主机名。参看*术语/缩写语* (参看 "*术语/缩略语*" p. 2)了解主机名规则。

6. 在 Heartbeat timeout (sec)（检测信号超时[秒]）字段里输入新设备和 CC-SG 之间的超时秒数（30-50,000 秒）。

7. 输入验证信息：

   - 如要用服务帐号进行验证，选择 Use Service Account Credentials（使用服务帐号证书）复选框。在 Service Account Name（服务帐号名称）菜单上选择要使用的服务帐号。

   或者

   - 在 Username（用户名）和 Password（密码）字段里分别输入用户名和密码进行验证。

8. 在 Description（说明）字段里输入此设备的简短说明。**可选。**

9. 单击 Test Connection（测试连接）按钮。参看***排除 Power IQ 连接故障*** (p. 364)了解错误消息。如果要使用同步功能，参看***配置 Power IQ 和 CC-SG 同步*** (p. 365)。

排除 Power IQ 连接故障

了解可能显示的错误消息和解决办法，排除 Power IQ 连接故障。

确定问题根源，编辑配置解决问题。参看***配置 Power IQ 服务*** (p. 363)。

消息	分辨率
不能与使用此 <IP> 的管理设备 <Name> 通信。	此错误消息可能说明几种情况。 ▪ 连接被远程拒绝了。在远程地址或端口上监听不到进程。 ▪ 检查防火墙。由于防火墙封锁，或者中间路由器停机了，无法访问远程主机。 ▪ 主机未知。不能根据输入的主机名解析 IP 地址。
验证失败。	用户名和密码错误。
不能与使用此 <IP> 的管理设备 <Name> 通信，确保启用了它的 Web API。	没有在 Power IQ 上启用 Web API。登录 Power IQ，选择 Settings（设置）> Web API，选择 Enable Web API（启用 Web API），然后单击 Save（保存）按钮。

配置 Power IQ IT 设备电源控制

在配置 Power IQ 服务之后，可以配置 CC-SG 添加所需的节点和接口。

1. 添加要控制电源的 IT 设备。参看***添加节点*** (p. 106)。
2. 给节点添加 Power IQ Proxy 电源控制接口。参看***添加接口*** (p. 122)和 ***Power IQ Proxy 电源控制连接接口*** (p. 131)。

配置 Power IQ 和 CC-SG 同步

CC-SG 与 Power IQ 同步，把在 Power IQ 上配置的 IT 设备作为节点添加到 CC-SG。在同步时，CC-SG 给新确定的每台 IT 设备创建一个使用 PowerIQ Proxy 接口的节点。当 CC-SG 检测到重复节点时，你选择的同步策略决定是合并、重新命名还是拒绝节点。

随时可以进行人工同步，也可以设置一个重复执行的任务。参看*任务管理器* (p. 297)。

还可以选择添加 Power IQ 里的所有 IT 设备，还是设置一个过滤器，让 CC-SG 只同步此过滤器允许的那些 IT 设备。

第一步 — 添加至要与 CC-SG 同步的 Power IQ 的连接：

- 参看*配置 Power IQ 服务* (p. 363)。

第二步 — 创建过滤器（可选）：

过滤器是可选的。如果不创建过滤器，将根据同步策略把在 Power IQ 上配置的所有 IT 设备添加到 CC-SG。过滤器只适用于所选的 Power IQ 实例。

1. 选择 Access（访问）> Power IQ Services（Power IQ 服务），然后选择要同步的 Power IQ 的名称。
2. 在 Synchronization（同步）部分的 Field（字段）列表上选择一个字段名称。在此列出的字段名称指的是在 Power IQ 里的字段。
3. 在 Operator（运算符）列表上选择一个搜索运算符。
   - LIKE 将返回指定字段里的值包含指定文本的 IT 设备。例如 "windows"、"windows2k" 和 "win7" 包含值 "win"。
   - EQUAL 只返回准确包含指定字段里的值的 IT 设备。
4. 在指定字段里用指定的运算符输入要搜索的值。
5. 单击 OK（确定）按钮保存，或者让此对话框保持打开状态，继续第三步。

第三步 — 创建同步策略：

注意：同步策略应用于在 CC-SG 上配置的所有 Power IQ 实例。参看 **Power IQ 同步策略** *(p. 366) 详细了解每个策略和其他同步结果。*

1. 在 Synchronization（同步）部分选择同步策略对应的单选按钮：
   - Consolidate Nodes（合并节点）
   - Rename Duplicate Nodes（重新命名重复节点）

- Reject Duplicate Nodes（拒绝重复节点）

2. 单击 OK（确定）按钮保存设置。参看*同步 Power IQ 和 CC-SG* (p. 366)详细了解人工同步和利用任务同步。

同步 Power IQ 和 CC-SG

在配置同步设置之后，随时可以进行人工同步。也可以创建一个任务，重复执行同步。

你必须拥有设备、端口和节点管理权限，才能进行同步。

参看*配置 Power IQ 和 CC-SG 同步* (p. 365)和 *Power IQ 同步策略* (p. 366)详细了解如何配置同步设置。

现在同步 Power IQ 和 CC-SG：

在单击 Synchronize Now（现在同步）按钮时，只同步所选的 Power IQ 实例。如果要定时同步所有 Power IQ 实例，可以创建一个任务。参看下一步。

1. 选择 Access（访问）> Power IQ Services（Power IQ 服务），然后选择要同步的 Power IQ 实例。
2. 确定过滤器和策略是否正确，然后单击 Synchronize Now（现在同步）按钮。
3. 打开 Synchronization Status Message（同步状态消息）对话框。阅读消息了解同步结果。

利用任务同步 Power IQ 和 CC-SG：

1. 创建“PowerIQ 同步”任务。参看*预定任务* (p. 299)。

Power IQ 同步策略

当 CC-SG 检测到重复节点时，你选择的同步策略决定是合并、重新命名还是拒绝节点。

参看*配置 Power IQ 和 CC-SG 同步* (p. 365)，设置同步策略。

同步策略：

- Consolidate Nodes（合并节点）：

  如果在一个 Power IQ 上检索到一台（用外部键确定的）IT 设备，此节点将用一个 Power IQ Proxy 接口连接每个 Power IQ。CC-SG 允许一个节点有重复接口名称。

- Rename Duplicate Nodes（重新命名重复节点）：

  如果在多个 Power IQ 上检索到一台（用外部键确定的）IT 设备，将用一个 Power IQ Proxy 接口给每个 Power IQ 创建一个节点。CC-SG 重新命名这些节点，添加一个有括号的数字，使它们变成唯一节点。例如 `node`、`node(2)` 和 `node(3)`。

- Reject Duplicate Nodes（拒绝重复节点）：

  如果在多个 Power IQ 上检索到一台（用外部键确定的）IT 设备，将给第一个节点创建一个节点和一个 Power IQ Proxy 接口，拒绝后续实例，并把它们记录为错误。这是默认设置。

其他同步结果：

在同步时，如果不存在用外部键确定的 IT 设备，且此节点只有一个与之关联的 Power IQ Proxy 接口，把此节点从 CC-SG 上删除掉。

如果此节点除一个与之关联的 Power IQ Proxy 接口之外还有其他接口，只把 Power IQ Proxy 接口从 CC-SG 上删除掉。

如果把一个 Power IQ 实例从 CC-SG 上删除掉，结果是一样的。

在 Power IQ 上导入和导出 Dominion PX 数据

必须具备 CC 设置和控制权限与设备、端口和节点管理权限，才能在 Power IQ 上导入和导出 Dominion PX 数据。

从 Power IQ 导入电源条

可以在 Power IQ 上导入 Dominion PX 设备及其出口名称。如果 Dominion PX 设备受 CC-SG 管理，必须先把这些设备删除掉。导入操作添加 Dominion PX 设备，配置并命名在 CSV 文件里指定的出口。

在导入过程中，忽略 CSV 文件里的非 Dominion PX 设备和出口。

可以使用 Power IQ 服务，给与 Dominion PX 设备和不能从 Power IQ 导入的其他供应商的电源条相连的 Power IQ IT 设备创建节点。参看 ***Power IQ IT 设备电源控制*** (p. 362)。

第一步：在 Power IQ 上导出 CSV 文件。

1. 登录 Power IQ，打开仪表盘。
2. 单击 Outlet Naming（出口命名）。
3. 单击 Import（导入）旁边的链接，把当前出口名称导出成 CSV 文件。
4. 打开或保存文件。本文件包含 Power IQ 上的所有出口。

第二步：编辑 CSV 文件

1. 编辑导出的 CSV 文件。
2. 删除 PX Name（PX 名称）列。添加一行命令，以便稍后添加每台 Dominion PX 设备。
3. 在所有行的最前面插入两列。
   a. 在第一列输入 ADD 命令。
   b. 在第二列输入 OUTLETS 标签。
4. 给要添加的每台 PX 设备插入一行。

列编号	标签或值	详细信息
1	ADD	所有标签的第一列是命令。
2	PX-DEVICE	输入所示的标签。 标签不区分大小写。
3	PX device's IP Address or hostname（PX 设备 IP 地址或主机名）	必填字段。
4	Username（用户名）	必填字段。
5	Password（密码）	必填字段。
6	Configure All Outlets（配置所有出口）	TRUE 或 FALSE 默认值是 FALSE。
7	Description（说明）	可选。

第三步：把编辑过的 CSV 文件导入 CC-SG

1. 在 CC-SG Admin Client 上选择 Administration（管理）> Import（导入）> Import Powerstrips（导入电源条）。
2. 单击 Browse（浏览）按钮选择要导入的 CSV 文件，然后单击 Open（打开）按钮。
3. 单击 Validate（验证）按钮。Analysis Report（分析报告）区显示文件内容。
   - 如果文件无效，显示错误消息。单击 OK（确定）按钮查看页面 Problems（问题）区显示的文件问题说明。单击 Save to File（保存到文件）按钮保存问题列表。编辑 CSV 文件纠正错误，然后再验证一次。参看*排除 CSV 文件问题* (p. 396)。
4. 单击 Import（导入）按钮。

5. 单击 Actions（操作）区查看导入结果。用绿色文字显示成功导入的项目，用红色文字显示导入失败的项目。由于已经有同名项目，或者已经导入了，也用红色文字显示导入失败的项目。
6. 如要查看导入结果详细信息，查看 Audit Trail（审计跟踪）报告。参看 ***导入审计跟踪项*** (p. 395)。

导出 Dominion PX 数据在 Power IQ 上使用

可以把在 CC-SG 上配置的 Dominion PX 设备的数据导出成 CSV 文件。导出到文件里的数据可以用作 CSV 文件的一部分，再把这些数据导入 Power IQ。这些信息包括 Dominion PX 设备、Outlet Names（出口名称）和 IT Device Names（IT 设备名称）。

只能导出与 IP 网络相连的 Dominion PX 设备。不包括作为网管电源条部署的 Dominion PX 电源条，在 IP 网络上不能作为设备访问这些电源条。

注意：导出的 Power IQ 数据可以在编辑后导入 Power IQ，仅此而已。不能把此文件导入 CC-SG。

第一步：在 CC-SG 上导出 CSV 文件：

1. 单击 Administration（管理）> Export（导出）> Export Power IQ Data（导出 Power IQ 数据）。
2. 单击 Export to File（导出成文件）按钮。
3. 输入文件名，然后选择文件保存位置。
4. 单击 Save（保存）按钮。

第二步：编辑 CSV 文件并导入 Power IQ：

导出文件分为三个部分。阅读 CSV 文件里的备注了解如何把每个部分用作 Power IQ 多标签 SCV 导入文件的组成部分。

参看 Raritan 网站上支持部分的固件和文档页上的 *Power IQ 用户指南*和 *CSV 导入模板*。

Ap A V1 和 E1 规格

在本章内

V1 型号

V1 总体规格

体积	1U
尺寸 (DxWxH)	24.21”x 19.09” x 1.75” 615 mm x 485 mm x 44 mm
重量	10.80 千克（23.80 磅）
电源	单电源（1 x 300 瓦）
工作温度	10° - 35° (50°- 95°)
平均故障间隔时间	36,354 小时
KVM 管理端口	（DB15 + PS2 或 USB 键盘/鼠标）
串行管理端口	DB9
控制台端口	2 个 USB 2.0 端口

V1 环境要求

工作时	
湿度	8%-90% 相对湿度
海拔	正常工作海拔 0-10,000 英尺，贮存 40,000 英尺（估计）
振动	5-55-5 HZ，0.38 mm，1 分/周期； 每个轴 (X,Y,Z) 30 分钟
冲击	不适用
不工作时	
温度	-40° - +60° (-40°-140°)

工作时	
湿度	5%-95% 相对湿度
海拔	正常工作海拔 0-10,000 英尺，贮存 40,000 英尺（估计）
振动	5-55-5Hz，0.38mm，1 分/周期； 每个轴 (X,Y,Z) 30 分钟
冲击	不适用

E1 型号

E1 总体规格

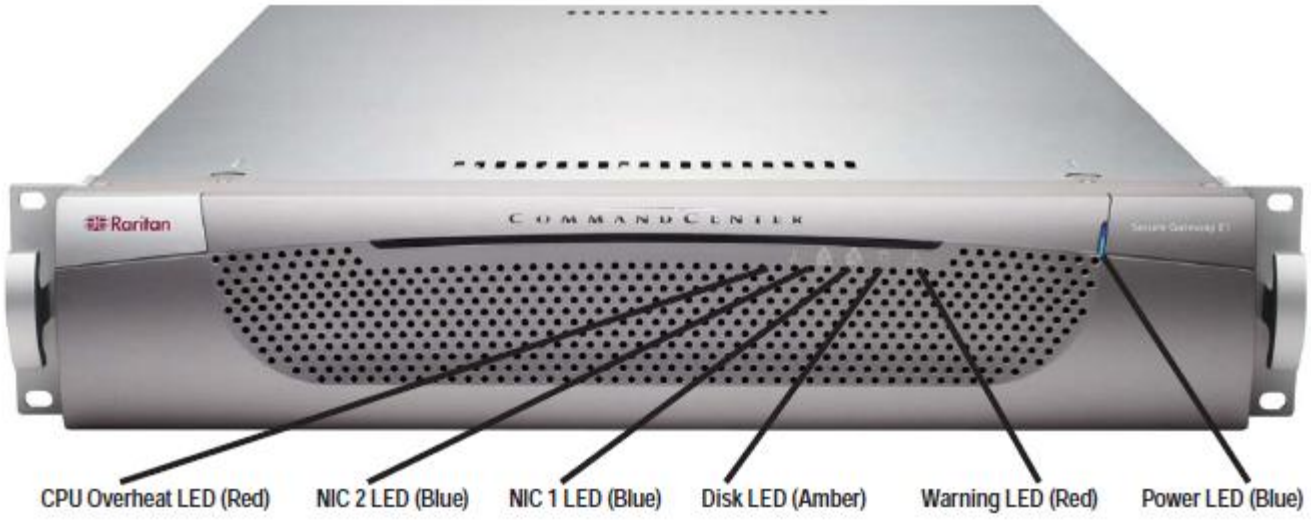
体积	2U
尺寸 (DxWxH)	27.05”x 18.7” x 3.46”-687 mm x 475 mm x 88 mm
重量	20 千克（44.09 磅）
电源	SP502-2S 热插拔 500W 2U 电源
工作温度	0-50°C
平均故障间隔时间	53,564 小时
KVM 管理端口	PS/2 键盘和鼠标端口，1 个 VGA 端口
串行管理端口	快速 UART 16550 串行端口
控制台端口	2 个 USB 2.0 端口

E1 环境要求

工作时	
湿度	5-90%，不凝结
海拔	海平面至 7,000 英尺
振动	每个垂直轴 X、Y 和 Z 上 10Hz-500Hz 扫频，0.5g 恒定加速度，持续一个小时
冲击	每个垂直轴 X、Y 和 Z 上 5 g，持续 11ms，使用 ½ 正弦波

工作时 不工作时	
温度	-40°C-70°C
湿度	5-90%，不凝结
海拔	海平面至 40,000 英尺
振动	每个垂直轴 X、Y 和 Z 上 10Hz-300Hz 扫频，2g 恒定加速度，持续一个小时
冲击	每个垂直轴 X、Y 和 Z 上 30g，持续 11ms，使用 ½ 正弦波

E1 型号设备上的 LED



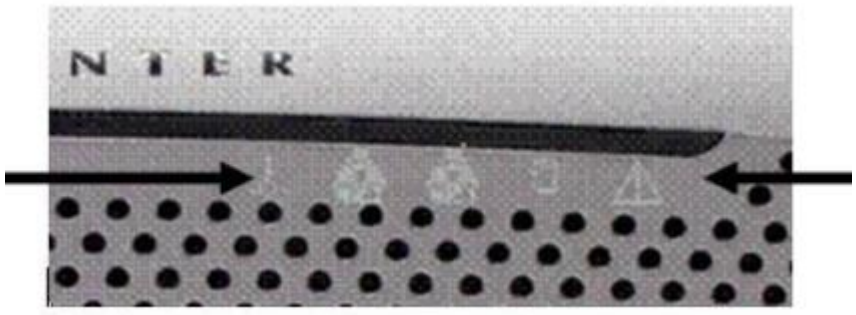
1	CPU 过热 LED — 红色	参看 ***E1 型号设备上的声音报警器和红色 LED*** (p. 373)。
2	网卡 2/LAN 2 LED — 蓝色	灯亮表示 LAN 2 有活动。
3	网卡 1/LAN 1 LED — 蓝色	灯亮表示 LAN 1 有活动。
4	磁盘 LED — 淡黄色	灯亮表示硬盘有活动。
5	警告 LED — 红色	参看 ***E1 型号设备上的声音报警器和红色 LED*** (p. 373)。
6	电源 LED — 蓝色	灯亮表示 CC-SG 设备通电。

E1 型号设备上的声音报警器和红色 LED

E1 设备有两个红色指示灯。

电源故障和过热。两个指示灯都伴有声音警报。

过热 LED



电源故障 LED

电源故障 LED 亮通常是设备的两根电源线没有全部插好造成的，也可能是电源发生实际故障造成的。

过热 LED 亮表示系统过热，通常是散热器松脱或安装不当造成的，也可能是风扇不转等因素造成的。参看 ***E1 一般性规格*** (参看 "***E1 总体规格***" p. 371)了解工作温度。

Ap B CC-SG 和网络配置

本附录介绍典型 CC-SG 部署的网络要求，包括地址、协议和端口。介绍如何针对外部访问、内部安全和路由策略执行配置网络。给 TCP/IP 网络管理员提供详细信息。TCP/IP 管理员的职责可能比 CC-SG 管理员的职责大。本附录协助管理员把 CC-SG 及其部件纳入站点的安全访问策略和路由策略中。

附表列出 CC-SG 及其相关部件所需的协议和端口。

在本章内

CC-SG 网络所需的开放端口：执行摘要

应该打开下列端口：

端口号	协议	用途	详细信息
80	TCP	通过 HTTP 访问 CC-SG	不加密。
443	TCP	通过 HTTPS (SSL) 访问 CC-SG 和 在直接模式下对 Dominion SX 相连的节点进行节点访问	SSL/AES-128/AES-256 加密。
8080	TCP	CC-SG 到 PC 客户机	SSL/AES-128/AES-256 加密（如配置）。
2400	TCP	节点访问（代理模式）	必须给要在外部访问的 Raritan 设备打开此端口。只有在访问 CC-SG 时，才需要打开表上的其他端口。 如果在 Dominion KX II 2.1.10 或更高版本设备上设置了加密，就使用加密。
5000	TCP	节点访问（直接模式）	必须给要在外部访问的 Raritan 设备打开此端口。只有在访问 CC-SG 时，才需要打开表上的其

端口号	协议	用途	详细信息
			他端口。 AES-128/AES-256 加密（如配置）。
供控制系统节点使用的 80 和 443 供虚拟主机节点和虚拟机节点使用的 80、443、902 和 903	TCP	虚拟节点访问	不适用
51000	TCP	SX 目标访问（直接模式）	AES-128/AES-256 加密（如配置）。

▶ 所需开放端口可能有例外：

如果所有 CC-SG 访问都使用 HTTPS 地址，端口 80 可以关闭。

如果用 CC-SG 代理模式建立经过防火墙的连接，端口 5000 和 51000 可以关闭。

CC-SG 通信通道

说明每个通信通道。对于每个通信通道，附表包括：

- 通信各方使用的符号 IP 地址。实体之间的任何通信路径必须支持这些地址。
- 通信发起方向。这对你的特定站点策略可能很重要。对于给定的 CC-SG 角色，相应通信方之间的路径必须可用，在网络发生故障时可用作替代性重新路由路径。
- CC-SG 使用的端口号和协议。
- 端口是否可配置，这意味着 Admin Client 或诊断控制台提供一个字段，如果默认端口号与其他网络应用程序的端口发生冲突或出于安全考虑，可以把默认端口号更改为不同的端口。
- 通信方法详细信息，即通过通信通道采用加密方法传送的消息。

CC-SG 和 Raritan 设备

CC-SG 的主要作用是管理和控制 Dominion KX II 等 Raritan 设备。CC-SG 通常通过 TCP/IP 网络（LAN、WAN 或 VPN）与这些设备通信，TCP 和 UDP 协议使用如下：

通信方向	端口号	协议	可配置？	详细信息
CC-SG 到本地广播	5000	UDP	是	检测信号
CC-SG 到远程 LAN IP	5000	UDP	是	检测信号
CC-SG 到 Raritan 设备	5000	TCP	是	RDM 协议 RC4/AES-128/AES-256 加密
Raritan 设备到 CC-SG	5001	UDP	否	检测信号
CC-SG 到 Dominion PX	623 443	UDP	否 否	
在直接模式下 CC-SG 到 Dominion KXII	443	TCP	否	

CC-SG 群集

在使用可选的 CC-SG 群集功能时，下列端口必须可供互联子网使用。如果不使用可选群集功能，不必打开这些端口。

群集里的每个 CC-SG 可能位于不同的 LAN 上。但是，设备之间的互联应该非常可靠，不容易发生拥塞现象。

在 CC-SG 群集里，主节点要建立并维护几个至备用节点的 TCP/IP 连接。这些连接可能长期闲置，但这是群集正常工作所必需的。

确保基于 VPN 或通过防火墙的所有 CC-SG 到 CC-SG 群集连接不超时，不被封锁。如果这些连接超时，会导致群集发生故障。

通信方向	端口号	协议	可配置？	详细信息
CC-SG 到本地广播	10000	UDP	否	检测信号
CC-SG 到远程 LAN IP	10000	UDP	否	检测信号
CC-SG 到 CC-SG	5432	TCP	否	从主 PostgreSQL 数据库服务器上的 HA-JDBC 到备用 PostgreSQL 数据库服务器上的 HA-JDBC。 不加密。

通信方向	端口号	协议	可配置？	详细信息
CC-SG 到 CC-SG	8732	TCP	否	主/备用服务器同步群集控制数据交换。 MD5 加密。
CC-SG 到 CC-SG	3232	TCP	否	主/备用 SNMP 同步配置更改转发。 不加密。

访问基础设施服务

可以配置 CC-SG 使用几个符合行业标准的服务，例如 DHCP、DNS 和 NTP。使用这些端口和协议，使 CC-SG 能与这些可选服务器通信。

通信方向	端口号	协议	可配置？	详细信息
DHCP 服务器到 CC-SG	68	UDP	否	IPv4 DHCP 标准
CC-SG 到 DHCP 服务器	67	UDP	否	IPv4 DHCP 标准
NTP 服务器到 CC-SG	123	UDP	否	NTP 标准
CC-SG 到 DNS	53	UDP	否	DNS 标准

PC 客户机到 CC-SG

PC 客户机采用下列三种模式之一连接 CC-SG：

- 通过网络浏览器的 Admin Client 或 Access Client。CC-SG 支持 SSL v2、SSL v3 和 TLS v1 浏览器连接。可以在浏览器上配置这些加密方法
- 通过 SSH 命令行界面 (CLI)
- Diagnostic Console（诊断控制台）

通信方向	端口号	协议	可配置？	详细信息
PC 客户机到 CC-SG	443	TCP	否	客户机-服务器通信。 SSL/AES-128/AES-256 加密（如配置）。
PC 客户机到 CC-SG	80	TCP	否	客户机-服务器通信。 不加密。如果启用 SSL，端口 80 被重定向到端口 443。
PC 客户机到 CC-SG	8080	TCP	否	客户机-服务器通信。

通信方向	端口号	协议	可配置？	详细信息
				SSL/AES-128/AES-256 加密（如配置）。 在 CC-SG 上打开端口 8080，而不是在 PC 客户机上打开。
PC 客户机到命令行 SSH	22	TCP	是	客户机-服务器通信。 SSL/AES-128/AES-256 加密（如配置）。
PC 客户机到诊断控制台	23	TCP	是	客户机-服务器通信。 SSL/AES-128/AES-256 加密（如配置）。

PC 客户机到节点

CC-SG 的另一个重要作用是把 PC 客户机连接到各种节点。这些节点可以采用串行连接或 KVM 控制台连接来连接 Raritan 设备（叫做带外连接）。另一种模式是使用带内访问方法，例如 VNC、RDP 或 SSH。

PC 客户机与节点通信的另一方面是：

- PC 客户机是通过 Raritan 设备还是带内访问方法直接连接节点。这叫直接模式。
- PC 客户机通过 CC-SG 连接节点，CC-SG 在这里充当应用程序防火墙。这叫代理模式。

通信方向	端口号	协议	可配置？	详细信息
客户机通过代理到 CC-SG，再到节点	2400 （在 CC-SG 上）	TCP	否	客户机-服务器通信。 不加密。
客户机到 Raritan 设备，再到带外 KVM 节点 （直接模式）	5000 （在 Raritan 设备上）	TCP	是	客户机-服务器通信。 SSL/AES-128/AES-256 加密（如配置）。
客户机到 Raritan Dominion SX 设备，再到带外串行节点 （直接模式）	51000 （在 Raritan 设备上）	TCP	是	客户机-服务器通信。 SSL/AES-128/AES-256 加密（如配置）。

CC-SG 和 IPMI、iLO/RILOE、DRAC、RSA 客户机

可能必须给 CC-SG 打开其他端口，才能管理 iLO/RILOE 和 iLO2/RILOE2 服务器等第三方设备。可以直接对 iLO/RILOE 设备目标执行通电/断电和重新通电操作。Intelligent Platform Management Interface (IPMI) 服务器也可以用 CC-SG 控制。Dell DRAC 和 RSA 目标也可以用 CC-SG 管理。

注意：某些带内接口要求打开其他端口。参看相应的指南了解详情。

通信方向	Port Number（端口号）	协议	可配置？	详细信息
CC-SG 到 IPMI	623	TCP	否	IPMI 标准
CC-SG 到 iLO/RILOE（使用 HTTP 端口）	80 或 443	TCP	否	供应商制定的标准
CC-SG 到 DRAC	80 或 443	TCP	否	供应商制定的标准
CC-SG 到 RSA	80 或 443	TCP	否	供应商制定的标准

CC-SG 和 SNMP

Simple Network Management Protocol 允许 CC-SG 把 SNMP 陷阱（事件通知）推送到网络上的现有 SNMP 管理器上。CC-SG 还支持与 HP OpenView 等第三方企业管理解决方案一起执行 SNMP GET/SET 操作。

通信方向	Port Number（端口号）	协议	可配置？	详细信息
SNMP 管理器到 CC-SG	161	UDP	是	SNMP 标准
CC-SG 到 SNMP 管理器	162	UDP	是	SNMP 标准

CC-SG 内部端口

CC-SG 用几个端口执行内部功能，其本地防火墙功能阻止对这些端口的访问。 However, some external scanners may detect these as “blocked” or “filtered.”不需要在外部访问这些端口，可以进一步封锁这些端口。当前使用的端口是：

- 1088
- 1098
- 2222
- 4444
- 4445
- 8009
- 8083
- 8093

除了这些端口，CC-SG 可能还使用 32xxx（或以上）范围内的 TCP 端口和 UDP 端口。不需要在外部访问这些端口，可以封锁这些端口。

通过支持 NAT 的防火墙访问 CC-SG

如果防火墙使用 NAT (Network Address Translation) 和 PAT (Port Address Translation)，应该用代理模式建立经过此防火墙的所有连接。必须在防火墙上给外部连接配置端口 80（非 SSL）或 443 (SSL)、8080 和 2400，以便把流量转发到 CC-SG（因为 PC 客户机在这些端口上发起会话）。

注意：建议不要让非 SSL 流量通过防火墙。

必须给使用防火墙的连接配置代理模式。参看***连接模式：直接和代理*** (p. 267)。CC-SG 将应 PC 客户机请求连接各种目标。但是，如果 PC 客户机到目标的 TCP/IP 连接通过防火墙，CC-SG 将终止此连接。

通过 RDP 访问节点

必须打开端口 3389，才能通过 RDP 访问节点。

通过 VNC 访问节点

必须打开端口 5800 或 5900，才能通过 VNC 访问节点。

通过 SSH 访问节点

必须打开端口 22，才能通过 SSH 访问节点。

远程系统监视端口

在启用远程系统监视功能时，默认打开端口 19150。参看***配置远程系统监视*** (p. 349)。

Ap C 用户组权限

下表列出必须给用户指定哪些权限，才能访问 CC-SG 菜单项。

* “无”表示不需要特殊权限。能访问 CC-SG 的任何用户，都可以查看和访问这些菜单和命令。

菜单 > 子菜单	菜单项	需要的权限	说明
Secure Gateway（安全网关）	所有用户均可访问此菜单。		
	My Profile(我的配置文件)	无*	
	Message of The Day（当日消息）	无*	
	Print（打印）	无*	
	Print Screen（打印屏幕）	无*	
	Logout（退出）	无*	
	Exit（关闭）	无*	
Users（用户）	只有具备用户管理权限的用户才能访问此菜单和用户树。		
> User Manager(用户管理器)	> Add User（添加用户）	用户管理	
	（编辑用户）	用户管理	通过 User Profile（用户配置文件）
	> Delete User（删除用户）	用户管理	
	> Delete User from Group（删除组用户）	用户管理	
	> Logout User(s)（退出用户）	用户管理	
	> Bulk Copy(批量复制)	用户管理	
> User Group Manager(用户组管理器)	> Add User Group（添加用户组）	用户管理	

菜单 > 子菜单	菜单项	需要的权限	说明
	（编辑用户组）	用户管理	通过 User Group Profile（用户组配置文件）
	> Delete User Group（删除用户组）	用户管理	
	> Assign Users to Group（给用户指定组）	用户管理	
	> Logout Users（退出用户）	用户管理	
	Node Auditing（节点审计）	用户管理	
Devices（设备）	只有具备下列任何一种权限的用户才能访问此菜单和设备树： 设备、端口和节点管理 设备配置和升级管理		
	Discover Devices（发现设备）	设备、端口和节点管理	
> Device Manager（设备管理器）	> Add Device（添加设备）	设备、端口和节点管理	
	（编辑设备）	设备、端口和节点管理	通过 Device Profile（设备配置文件）
	> Delete Device（删除设备）	设备、端口和节点管理	
	> Bulk Copy（批量复制）	设备、端口和节点管理	
	> Upgrade Device（升级设备）	设备配置和升级管理	
>> Configuration（配置）	>> Backup（备份）	设备配置和升级管理	
	>> Restore（恢复）	设备配置和升级管理	
	>> Copy Configuration（复	设备配置和升级管理	

菜单 > 子菜单	菜单项	需要的权限	说明
	制配置）		
	> Restart Device（重新启动设备）	设备、端口和节点管理，或者设备配置和升级管理	
	> Ping Device（Ping 设备）	设备、端口和节点管理，或者设备配置和升级管理	
	> Pause Management（暂停管理）	设备、端口和节点管理，或者设备配置和升级管理	
	> Device Power Manager（设备电源管理器）	设备、端口和节点管理，节点电源控制	
	> Launch Admin（启动管理）	设备、端口和节点管理，或者设备配置和升级管理	
	> Launch User Station Admin（启动用户工作站管理）	设备、端口和节点管理	
	> Disconnect Users（断开用户）	设备、端口和节点管理，或者设备配置和升级管理	
	> Topology View（拓扑视图）	设备、端口和节点管理	
> Change View（更改视图）	> Create Custom View（创建定制视图）	设备、端口和节点管理，或者设备配置和升级管理	
	> Tree View（树视图）	设备、端口和节点管理，或者设备配置和升级管理	
> Port Manager（端口管理器）	> Connect（连接）	设备、端口和节点管理，节点带外访问	
	> Configure Ports（配置端口）	设备、端口和节点管理	
	> Disconnect Port（断开端口）	设备、端口和节点管理	
	> Delete Ports（删除端口）	设备、端口和节点管理	
	> Port Power Manager（端口电	设备、端口和节点管理，节点电源控制	

菜单 > 子菜单	菜单项	需要的权限	说明
	源管理器）		
	> Add Powerstrip（添加电源条）	设备、端口和节点管理	
> Port Sorting Options（端口排序选项）	> By Port Name（按端口名称）	设备、端口和节点管理，或者设备配置和升级管理	
	> By Port Status（按端口状态）	设备、端口和节点管理，或者设备配置和升级管理	
	> By Port Number（按端口号）	设备、端口和节点管理，或者设备配置和升级管理	
Nodes（节点）	只有具备下列任何一种权限的用户才能访问此菜单和节点树： 设备、端口和节点管理 节点带内访问 节点带外访问 节点电源控制		
	Add Node(添加节点）	设备、端口和节点管理	
	（编辑节点）	设备、端口和节点管理	通过 Node Profile（节点配置文件）
	Delete Node（删除节点）	设备、端口和节点管理	
	<interfaceName（接口名称）>	节点带内访问或 节点带外访问	
	Disconnect(断开）	下列任何一种权限： 节点带内访问或 节点带外访问或 设备、端口和节点管理或 设备配置和升级管理	
	Virtualization（虚拟化）	设备、端口和节点管理	
	Bulk Copy（批量复制）	设备、端口和节点管理	
	Power Control(电	电源控制	

菜单 > 子菜单	菜单项	需要的权限	说明
	源控制）		
	Service Accounts（服务帐号）	设备、端口和节点管理	
	Assign Service Accounts（指定服务帐号）	设备、端口和节点管理	
	Group Power Control（设备组电源控制）	电源控制	
	Configure Blades（配置刀片服务器）	设备、端口和节点管理	
	Ping Node（Ping 节点）	设备、端口和节点管理	
	Bookmark Node Interface（添加节点接口书签）	节点带内访问或 节点带外访问	
> Node Sorting Options（节点排序选项）	> By Node Name（按节点名称）	下列任何一种权限： 设备、端口和节点管理或 节点带内访问或 节点带外访问或 电源控制	
	> By Node Status（按节点状态）	下列任何一种权限： 设备、端口和节点管理或 节点带内访问或 节点带外访问或 节点电源控制	
> Chat（聊天）	> Start Chat Session（启动聊天会话）	节点带内访问或 节点带外访问或 节点电源控制	
	> Show Chat Session（显示聊天会话）	节点带内访问或 节点带外访问或	

菜单 > 子菜单	菜单项	需要的权限	说明
		节点电源控制	
	> End Chat Session（结束聊天会话）	节点带内访问或 节点带外访问或 节点电源控制	
> Change View（更改视图）	> Create Custom View（创建定制视图）	下列任何一种权限： 设备、端口和节点管理或 节点带内访问或 节点带外访问或 节点电源控制	
	> Tree View(树视图）	下列任何一种权限： 设备、端口和节点管理或 节点带内访问或 节点带外访问或 节点电源控制	
Associations（关联）	只有具备用户安全管理权限的用户才能访问此菜单。		
	> Association（关联）	用户安全管理	包括可以添加、修改和删除。
	> Device Groups（设备组）	用户安全管理	包括可以添加、修改和删除。
	> Node Groups（节点组）	用户安全管理	包括可以添加、修改和删除。
	> Policies（策略）	用户安全管理	包括可以添加、修改和删除。
Reports（报告）	具备任何管理权限的用户（只具备用户安全管理权限的用户除外）都可以访问此菜单。		
	Audit Trail（审计跟踪）	CC 设置和控制	
	Error Log（错误日志）	CC 设置和控制	
	Access Report（访问报告）	设备、端口和节点管理	

菜单 > 子菜单	菜单项	需要的权限	说明
	Availability Report（可用性报告）	设备、端口和节点管理，或者设备配置和升级管理	
> Users（用户）	> Active Users(活动用户）	用户管理	
	> Locked out Users（封锁用户）	CC 设置和控制	
	> All Users Data（所有用户数据）	查看所有用户数据：用户管理 查看自己的用户数据：无	
	> User Group Data（用户组数据）	用户管理	
> Devices(设备）	> Device Asset Report（设备资产报告）	设备、端口和节点管理，或者设备配置和升级管理	
	> Device Group Data（设备组数据）	设备、端口和节点管理	
	> Query Port（查询端口）	设备、端口和节点管理	
> Nodes（节点）	> Node Asset Report（节点资产报告）	设备、端口和节点管理	
	> Active Nodes（活动节点）	设备、端口和节点管理	
	> Node Creation（节点创建）	设备、端口和节点管理	
	> Node Group Data（节点组数据）	设备、端口和节点管理	
> Active Directory	AD Users Group Report（AD 用户组报告）	CC 设置和控制，或用户管理	
	Scheduled Reports（预定报告）	CC 设置和控制或 设备配置和升级管理	

菜单 > 子菜单	菜单项	需要的权限	说明
Access（访问）			
	Add Web Services API（添加 Web 服务 API）	CC 设置和控制	
Administration（管理）	只有具备下列任何一种权限的用户才能访问此菜单： CC 设置和控制 设备、端口和节点管理、用户管理与用户安全管理的组合		
	Guided Setup（指导设置）	下列全部权限： 设备、端口和节点管理、用户管理与用户安全管理	
	Message of the Day Setup（当日消息设置）	CC 设置和控制	
	Applications（应用程序）	CC 设置和控制	
	Firmware（固件）	CC 设置和控制或 设备配置和升级管理	
	Configuration（配置）	CC 设置和控制	
	Cluster Configuration（群集配置）	CC 设置和控制	
	Neighborhood（邻居）	CC 设置和控制	
	Security（安全）	CC 设置和控制	
	Notifications（通知）	CC 设置和控制	
	Tasks（任务）	CC 设置和控制	
	Compatibility Matrix（兼容性指标）	设备、端口和节点管理，或者设备配置和升级管理	
> Import（导入）	Import Categories（导入类别）	CC 设置和控制与 用户安全管理	

菜单 > 子菜单	菜单项	需要的权限	说明
	Import Users（导入用户）	CC 设置和控制与用户管理	
	Import Nodes（导入节点）	CC 设置和控制与设备、端口和节点管理	
	Import Devices（导入设备）	CC 设置和控制与设备、端口和节点管理	
	Import Powerstrips（导入电源条）	CC 设置和控制与设备、端口和节点管理	
> Export（导出）	Export Categories（导出类别）	CC 设置和控制与用户安全管理	
	Export Users（导出用户）	CC 设置和控制与用户管理	
	Export Nodes（导出节点）	CC 设置和控制与设备、端口和节点管理	
	Export Devices（导出设备）	CC 设置和控制与设备、端口和节点管理	
	Export Power IQ Data（导出 Power IQ 数据）	CC 设置和控制与设备、端口和节点管理	
System Maintenance（系统维护）			
	Backup（备份）	CC 设置和控制	
	Restore（恢复）	CC 设置和控制	
	Reset（复位）	CC 设置和控制	
	Restart（重新启动）	CC 设置和控制	
	Upgrade（升级）	CC 设置和控制	

菜单 > 子菜单	菜单项	需要的权限	说明
	Shutdown（关机）	CC 设置和控制	
> Maintenance Mode（维护模式）	> Enter Maintenance Mode（进入维护模式）	CC 设置和控制	
	> Exit Maintenance Mode（退出维护模式）	CC 设置和控制	
View（查看）		无*	
Window（窗口）		无*	
Help（帮助）		无*	

Ap D SNMP 陷阱

CC-SG 提供下列 SNMP 陷阱：

SNMP 陷阱	说明
ccUnavailable	CC-SG 应用程序不可用。
ccAvailable	CC-SG 应用程序可用。
ccUserLogin	CC-SG 用户已登录。
ccUserLogout	CC-SG 用户已退出。
ccPortConnectionStarted	CC-SG 会话已启动。
ccPortConnectionStopped	CC-SG 会话已停止。
ccPortConnectionTerminated	CC-SG 会话已终止。
ccImageUpgradeStarted	CC-SG 镜像文件升级已开始。
ccImageUpgradeResults	CC-SG 镜像文件升级结果。
ccUserAdded	新用户已被添加到 CC-SG。
ccUserDeleted	用户已从 CC-SG 上删除。
ccUserModified	CC-SG 用户已被修改。
ccUserAuthenticationFailure	CC-SG 用户验证失败。
ccLanCardFailure	C-SG 探测到 LAN 网卡发生故障。
ccHardDiskFailure	CC-SG 探测到硬盘发生故障。
ccLeafNodeUnavailable	CC-SG 探测到叶节点连接失败。
ccLeafNodeAvailable	CC-SG 探测到叶节点不能访问。
ccIncompatibleDeviceFirmware	CC-SG 检测到使用不兼容固件的设备。
ccDeviceUpgrade	CC-SG 已升级设备固件。
ccEnterMaintenanceMode	CC-SG 已进入维护模式。
ccExitMaintenanceMode	CC-SG 已退出维护模式。
ccUserLockedOut	CC-SG 用户已被封锁。
ccDeviceAddedAfterCCNOCNotification	在收到 CC-NOC 通知之后，CC-SG 已添加设备。
ccScheduledTaskExecutionFailure	执行预定任务失败原因。
ccDiagnosticConsoleLogin	用户已登录 CC-SG 诊断控制台。

SNMP 陷阱	说明
ccDiagnosticConsoleLogout	用户已退出 CC-SG 诊断控制台。
ccUserGroupAdded	新用户组已被添加到 CC-SG。
ccUserGroupDeleted	CC-SG 用户组已被删除。
ccUserGroupModified	CC-SG 用户组已被修改。
ccSuperuserNameChanged	CC-SG 超级用户用户名已被更改。
ccSuperuserPasswordChanged	CC-SG 超级用户密码已被更改。
ccLoginBannerChanged	CC-SG 登录横幅已被更改。
ccMOTDChanged	CC-SG 当日消息 (MOTD) 已被更改。
ccDominionPXReplaced	Dominion PX 设备已被另一台 Dominion PX 设备取代。
ccSystemMonitorNotification	CC-SG 内存用完了。
ccNeighborhoodActivated	CC-SG 邻居已被激活。
ccNeighborhoodUpdated	CC-SG 邻居已被更新。
ccDominionPXFirmwareChanged	Dominion PX 固件版本已被更改。
ccClusterFailover	主 CC-SG 节点发生故障，备用 CC-SG 节点现在作为新的主 CC-SG 节点工作。
ccClusterBackupFailed	备用 CC-SG 节点发生故障。
ccClusterWaitingPeerDetected	主 CC-SG 节点检测到备用节点处于等待模式。
ccClusterOperation	群集操作已执行。
ccCSVFileTransferred	CSV 文件已被导入。
ccPIQAvailable	CC-SG 探测到 Power IQ 可用
ccPIQUnavailable	CC-SG 探测到 Power IQ 不可用

Ap E CSV 文件导入

本附录提供更详细的 CSV 文件导入信息。

在本章内

通用 CSV 文件要求

创建 CSV 文件的最佳方法，是在 CC-SG 上导出文件，把导出的 CSV 文件用作创建 CSV 文件的模板。导出文件的最前面有备注，说明文件里的每一项。可以根据备注说明，创建要导入的文件。

建议你创建 Microsoft Excel 等电子表格程序格式的导入文件。在单元格里输入各项。在保存文件时，选择 CSV 文件类型。这样，自动在每个单元格末尾添加逗号，按用逗号分隔开的列组织管理数据。可以用文本编辑器创建 CSV 文件，但必须在每项末尾人工添加逗号。

在首次把文件保持成 Excel 格式时，必须选择 Save As（另存为），确保选择 CSV 文件类型。之后，Excel 继续把文件另存为 CSV 格式。

如果不正确设置文件类型，文件会损坏，不能导入它。

- 所有导入文件都必须是 ASCII 文本。
- 每行的第一列必须是命令 `ADD`。基本结构是 Command（命令）、Tag（标签）、Attribute（属性），其中 `ADD` 是命令。
- 不支持列名称。可以在每行数据前面加上备注行，备注行以 `#` 符号开头。
- 使用字段默认值，输入字段值，或者让字段保留空白。
- 参看***命名常规*** (p. 431)详细了解 CC-SG 的名称长度规则。
- 如果用文本编辑器创建 CSV 文件，而不使用电子表格程序，必须采用不同的方式使用逗号和双引号。含有逗号和双引号的值，必须整个放在双引号里。还必须在值里的双引号字符前面加上一个双引号字符。

  例如：

值有特殊字符	格式化 CSV 文件
DeviceA,B	"DeviceA,B"
Device"A"	"Device""A"""

导入审计跟踪项

在审计跟踪里记录被导入 CC-SG 的每一项。跳过的重复项不记录在审计跟踪里。

在审计跟踪的 Message Type Configuration（消息类型配置）下面，下列操作各有一项记录。

- 已开始 CSV 文件导入
- 已完成 CSV 文件导入，包括添加成功的记录数、添加失败的记录数和被忽略的重复记录数。

在导入记录时发生的每次更改，在审计跟踪里都有一项。这些项记录在 Import started（开始导入）项和 Import completed（完成导入）项之间。它们被记录在不同的消息类型下，视你执行的导入类型而定。

- 用户导入记录在 User maintenance（用户维护）下
- 设备导入记录在 Device/node/port（设备/节点/端口）下
- 节点导入记录在 Device/node/port（设备/节点/端口）下
- 类别导入记录在 Configuration（配置）下
- 电源条导入记录在 Device/node/port（设备/节点/端口）下

在审计报告页上使用按日期和时间过滤字段，查找有关导入的所有项。

导入的每个记录，在审计跟踪里可能记录了几项。

排除 CSV 文件问题

排除 CSV 文件验证问题：

Import（导入）页的 Problems（问题）部分显示错误消息。错误消息说明在验证过程中，发现 CSV 文件有问题。

可以把错误列表保持成 CSV 文件。

每个错误保护 CSV 文件出错行号。

参看导出文件最前面的备注，这些备注有助你纠正错误。在纠正文件错误之后，再验证一次。

排除 CSV 文件导入问题：

Import（导入）页的 Problems（问题）部分显示警告消息和错误消息，告诉你在导入时发现的问题。

如果显示错误，不导入文件错误行上的信息。

不导入重复项，审计跟踪也不反映重复项。

Ap F 故障排除

- 在网络浏览器上启动 CC-SG 需要一个 Java 插件。如果机器安装的插件版本错误，CC-SG 将指导你完成安装步骤。如果机器没有 Java 插件，CC-SG 不能自动启动。在这种情况下，必须卸载或禁用旧版 Java，建立 CC-SG 串行端口连接才能正常操作。
- 如果不加载 CC-SG，检查网络浏览器设置。
  - 确保在 Internet Explorer 上启用 Java (Sun)。
  - 在 Control Panel（控制面板）上打开 Java 插件，调节浏览器设置。
- 如果在添加设备时出问题，确保设备的固件版本正确无误。
- 如果设备与 CC-SG 之间的网络接口电缆断开，等待配置的检测信号时间（分钟），然后插回网络接口电缆。在配置的检测信号周期内，设备以单机模式运行，可通过 RRC、MPC 或 RC 访问。
- 如果显示错误消息，说明客户机版本与服务器版本不一致，且结果无法预测，应该清除浏览器高速缓冲和 Java 高速缓存，重新启动浏览器。参看***清除浏览器高速缓存*** (p. 246)和***清除 Java 高速缓存*** (p. 246)。
- 如果在用 Internet Explorer 通过 MPC 接口访问 KX2 端口时出问题，应该清除浏览器高速缓存，然后重新访问此端口。参看***清除浏览器高速缓存*** (p. 246)。
- 如果内存利用率急剧攀升，或者浏览器会话停止响应你的操作，可能必须增大客户机的 Java 堆大小。
  a. 在 Control Panel（控制面板）上打开 Java 插件。
  b. 单击 Java 选项卡。
  c. 单击 Java Applet Runtime Settings（Java 小程序运行时设置）组里的 View（查看）。
  d. 选择当前运行的 Java 版本所在的行，在 Java Runtime Parameters（Java 运行时参数）列输入 `-Xmx<size>m`。例如：如果要把 Java 堆大小增加到 300MB，输入 `-Xmx300m`。

  建议你把 Java 堆大小设置为客户计算机内存的一半以上。例如：如果客户计算机有 1.0GB RAM，把此参数设置为 `-Xmx512m`。
- 如果使用相同客户机和 Firefox 访问多台 CC-SG 设备，可能显示 Secure Connection Failed（安全连接失败）消息，说明你的证书无效。可以清除浏览器上的无效证书继续访问设备。
  a. 在 Firefox 上选择 Tools（工具）> Options（选项）。
  b. 单击 Advanced（高级）按钮。
  c. 单击 Encryption（加密）选项卡。

d. 单击 View Certificates（查看证书），在列表上找到 Raritan。

e. 选择 CommandCenter 项，然后单击 Delete（删除）按钮。单击 OK（确定）按钮确认。

Ap G 诊断工具

CC-SG 备有几个诊断工具，对你或 Raritan 技术支持人员分析和排除 CC-SG 问题根源非常有用。

在本章内

内存诊断

CC-SG 实现了 Memtest86+ 诊断程序，可以在 GRUB 菜单上调用此程序。无论发生哪种内存问题，都可以执行 Memtest86+ 诊断测试排除故障。

1: 运行 Memtest86+ 诊断程序：

1. 重新启动 CC-SG。参看*用诊断控制台重新启动* ***CC-SG*** (p. 340)。
2. 在显示下列消息时，在五秒钟之内按任意键（例如 Esc 或箭头键）进入 GRUB 菜单。

   `Press any key to enter the menu`（按任意键进入菜单）

   `Booting CentOS (x.x.x) in x seconds....`（将在 x 秒后启动 `CentOS (x.x.x)....`）
3. 用上下箭头键突出显示 Memtest86+ vX.X 选项(其中 vX.X 是当前版本号），È⁰ó°´ Enter。
4. CC-SG 加载并运行 Memtest86+ 诊断程序。让程序运行完毕，直到 Pass（通过）列显示 1 为止。如要进行全面测试，让程序运行几个小时甚至整个晚上。
5. 查看下列各项，确定内存是否出错。
   - Memory（内存）：内存总量应该与 CC-SG 型号相适应：G1 需要 512MB，V1 需要 2048MB，E1 需要 4096MB。
   - Errors（错误）：本列应该显示 0。
   - Error display area（错误显示区）：位于 WallTime（系统时间）行下面。如果这里不显示任何信息，表示没有错误。

   如果显示的信息说明有内存错误，你可以：
   - 截取包含内存错误的 Memtest86+ 屏幕，联系 Raritan 技术支持部门寻求协助。

- 关闭 CC-SG，重新安装 DIMM 内存条，确保内存条接触良好。运行 Memtest86+ 诊断程序，确定内存问题是否解决了。

2: 终止 Memtest86+ 诊断程序：

1. 按 Esc。
2. CC-SG 复位并重新启动。

调试模式

虽然启用调试模式对排除故障帮助很大，但它可能会影响 CC-SG 操作和性能。因此，**只有在 Raritan 技术支持人员告诉你启用调试模式时，才启用它。**在排除故障之后，必须关闭调试模式。

1: 打开调试模式：

1. 使用支持的 Internet 浏览器，输入下列 URL：`http(s)://<IP_address>:8080/jmx-console/`，其中 `<IP_address>` 是 CC-SG 的 IP 地址。例如 `https://10.20.3.30:8080/jmx-console/`。
2. 在 Username（用户名）字段里输入 admin。
3. 在 Password（密码）字段里输入超级用户密码。
4. 向下翻页，直到你看到 `com.raritan.cc.bl.logger` 为止。
5. 单击此超链接：`service=LoggerService`。屏幕显示调试选项列表。
6. 把 Raritan 技术支持人员要求的调试选项值从 INFO（信息）更改为 DEBUG（调试）。
7. 单击窗口底部的 Apply Changes（应用更改）按钮。
8. 再现问题，制作快照。参看*制作系统快照* (p. 360)。

2: 关闭调试模式：

1. 在上一节介绍的前四个步骤之后，打开调试选项窗口。
2. 把调试选项的值从 DEBUG（调试）更改为 INFO（信息）。
3. 单击窗口底部的 Apply Changes（应用更改）按钮。

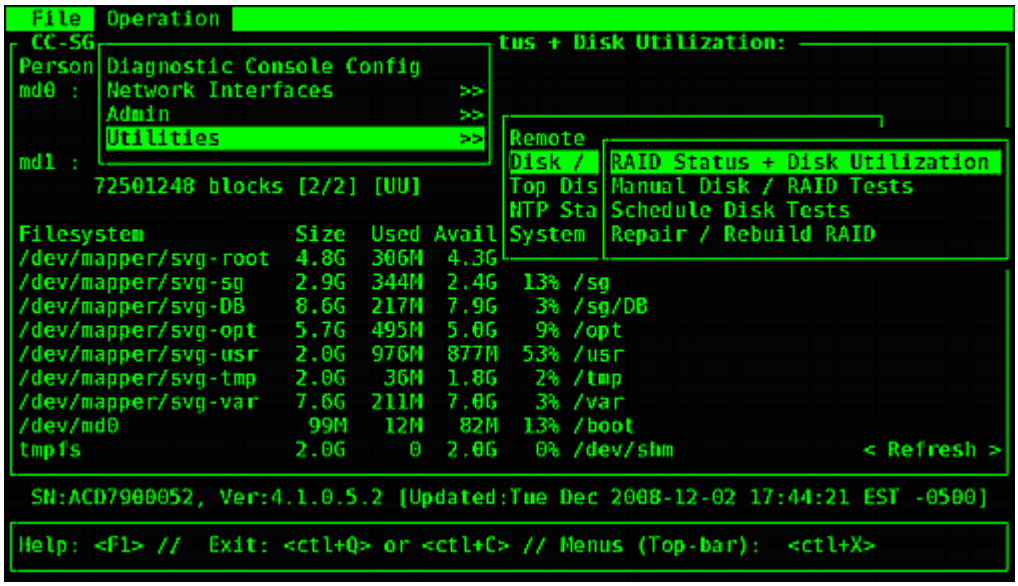
CC-SG 磁盘监视

如果一个或多个文件系统的 CC-SG 磁盘空间用完了，可能会对操作造成不利影响，甚至造成工程数据丢失。因此，应该监视 CC-SG 磁盘利用率，采取纠正措施防止或解决潜在的问题。可以通过诊断控制台或网络浏览器进行磁盘监视。如果你是经验丰富的用户，可以使用 gkrellm 远程监视。参看*配置远程系统监视* (p. 349)。

重要说明：对于群集配置里的 CC-SG 设备，必须同时监视两台 CC-SG 设备。

通过诊断控制台监视磁盘空间

1. 登录诊断控制台，调用磁盘状态页。参看*显示 RAID 状态和磁盘利用率* (p. 351)。
2. 检查与磁盘有关的信息，必要时采取措施。
   - 两个 RAID 分区应该显示 [UU]，而不是 [U_] 或 [_U]。否则表示磁盘发生故障，必须联系 Raritan 技术支持部门。
   - 任何一个文件系统的 Use%（使用百分比）值（屏幕上的第五列）不应超过 50%。不同的文件系统存储不同的数据，相应的纠正措施也不相同。



文件系统	数据	纠正措施
/sg/DB	CC-SG 数据库	联系 Raritan 技术支持部门
/opt	CC-SG 备份和快照	1. 把所有新快照文件保存在远程客户 PC 上。参看*制作系*

文件系统	数据	纠正措施
		统快照 (p. 360)了解检索步骤。 2. 进入 System Snapshot（系统快照）菜单。参看*制作系统快照* (p. 360)。 3. 选择 Pre-Clean-up SNAP（预清理上载）区域。 4. 选择 Pre-Clean-up UPLOAD（预清理上载）区域。 5. 取消 SNAP。 6. 取消 Package & Export（打包和导出）。 7. 单击或选择 Submit（提交）按钮。 8. 如果仍然存在空间问题，用 Admin Client 连接 CC-SG，把 CC-SG 备份文件上载到客户 PC 上，然后把它们从 CC-SG 上删除掉。
/var	日志文件和系统升级文件	联系 Raritan 技术支持部门
/tmp	临时区（供快照使用）	1. 进入 System Snapshot（系统快照）菜单。参看*制作系统快照* (p. 360)。 2. 取消 SNAP。 3. 取消 Package & Export（打包和导出）。 4. 选择 Clean-up /tmp（清理 /tmp）。 5. 单击或选择 Submit（提交）按钮。
/sg	CC-SG 管理的设备固件文件。	在 Admin Client 上选择 Administration（管理）> Firmware（固件），确认要添加的固件文件是否不存在。 如果目录利用率超过 85%，删除不再需要的设备固件文件。在 Admin Client 上选择 Administration（管理）> Firmware（固件），选择要删除的固件文件，然后单击 Delete（删除）按钮。

通过网络浏览器监视磁盘空间

此方法只适用于 CC-SG 4.0 或更高版本。必须在诊断控制台上启用与 Web 状态控制台有关的选项，才能用网络浏览器监视磁盘空间。参看*通过网络浏览器访问状态控制台* (p. 320)。

1. 使用支持的 Internet 浏览器，输入下列 URL：`http(s)://<IP_address>/status/` where `<IP_address>` is the IP address of the CC-SG.注意必须在 /status 后面加斜杠 (/)，例如 `https://10.20.3.30/status/`。
2. 打开状态页面。本页显示的信息与状态控制台显示的信息相同。

3. 单击页面底部 Evaluation（求值）下面的 CC-SG Monitors（CC-SG 监视器）。
4. 检查与磁盘有关的信息，必要时采取措施。参看上一节了解详情。

注意：如果发生本节未提及的文件系统问题，或者你采取的纠正措施不能解决问题，联系 Raritan 技术支持部门寻求协助。

Ap H 双因素验证

可以配置 CC-SG，通过关联的 RSA 验证管理器指向支持双因素验证的 RSA RADIUS 服务器。CC-SG 充当 RADIUS 客户机，把用户验证请求发送到 RSA RADIUS 服务器。验证请求包括用户 ID、固定密码和动态令牌代码。

在本章内

支持双因素验证的环境

下列双因素验证部件可与 CC-SG 一起使用。

- Windows Server 2003 集成的 RSA RADIUS Server 6.1
- Windows Server 2003 集成的 RSA Authentication Manager 6.1
- RSA Secure ID SID700 硬件令牌

旧版 RSA 产品应该也可与 CC-SG 一起使用，但未经验证。

双因素验证设置要求

必须完成下列任务，才能进行双因素验证设置。参看 RSA 文档。

1. 导入令牌。
2. 创建一个 CC-SG 用户，给他指定一个令牌。
3. 生成用户密码。
4. 给 RADIUS 服务器创建一个代理主机。
5. 为 CC-SG 创建一个代理主机（类型：通信服务器）。
6. 创建一个 RADIUS CC-SG 客户机。

双因素验证已知问题

RSA RADIUS 的 New PIN 模式需要挑战密码/PIN，无法正常工作。相反，必须给在这种模式下的所有用户指定固定密码。

Ap I Dominion KX2 双视频端口设置和建议

在本章内

概述

远程用户可以利用扩展桌面配置远程访问有两个显示卡的服务器。为此，要创建双端口视频组。

可以利用扩展桌面配置在两台监视器上观看目标服务器桌面，而不是只用一台标准监视器。在选择双端口视频组之后，同时打开此组里的所有端口通道。 参看*创建双视频端口组* (p. 412)了解如何创建双端口视频组。

阅读本节了解双端口视频组重要信息。

注意：KX2-108 和 KX2-116 等只有一个 KVM 通道的 CommandCenter Secure Gateway 设备不支持双视频端口组。

在 CC-SG 上配置和使用双端口视频

对 CC-SG 而言，双视频端口是带外 KVM 端口。如果端口位于端口组里，适用下列配置说明。

在 Admin Client 上配置双视频端口：

配置主端口时，同时配置辅端口。不能控制辅端口。只能连接或断开主端口。只在主端口上选择连接应用程序。应用程序选择适用于辅端口。

利用 CSV 文件导入法配置双视频端口：

在导入双视频端口组时，必须同时配置两个端口，否则导入操作失败。错误消息说明必须给双显示器端口组配置主端口和辅端口。

删除双视频端口：

在删除双视频端口组的一个端口时，删除主端口。删除主端口时，同时删除辅端口。

在用 CSV 文件导入法删除端口时，必须指定两个端口，否则删除操作失败。

连接与一个双视频端口关联的节点：

只能连接或断开与主端口（主节点）关联的节点。只能给主端口添加接口。不能控制与辅端口关联的节点。

配置包含双视频端口的节点组：

在给节点组选择节点时，选择双视频端口中的一个端口即自动选择另一个端口。只能把端口成对添加到节点组里，或者把节点组里的端口成对删除掉。

在使用双视频端口时使用书签和直接连接 URL：

书签和直接连接 URL 可用于双视频端口组的主节点和辅节点，但不能成功连接辅节点。拒绝辅节点连接请求。

给尝试利用书签或 URL 连接辅端口的用户显示错误消息：Connection to port denied.Contact your system administrator.（拒绝连接端口。请联系系统管理员。）

配置双视频端口访问：

你必须拥有对双视频端口组里两个端口/节点的访问权。最好确保在 CC-SG 上把主节点和辅节点同时添加到同一个节点组里。

如果你无权访问两个端口，Admin Client 将显示主节点但禁用所有控制，节点配置文件的 Info（信息）部分显示一条消息说明用户还需要辅端口节点访问权。Admin Client 将显示主节点但禁用所有超链接和控制，并显示一条消息说明用户还需要辅端口节点访问权。

采用 KX2 设备级独占模式连接双视频端口：

当 KX2 在设备级独占模式下工作时，如果任一个端口忙，KX2 拒绝所有两种连接请求。当 VM 共享模式要求独占访问时，也发生这种情况。

在启用 KVM 会话限制的情况下使用双视频端口：

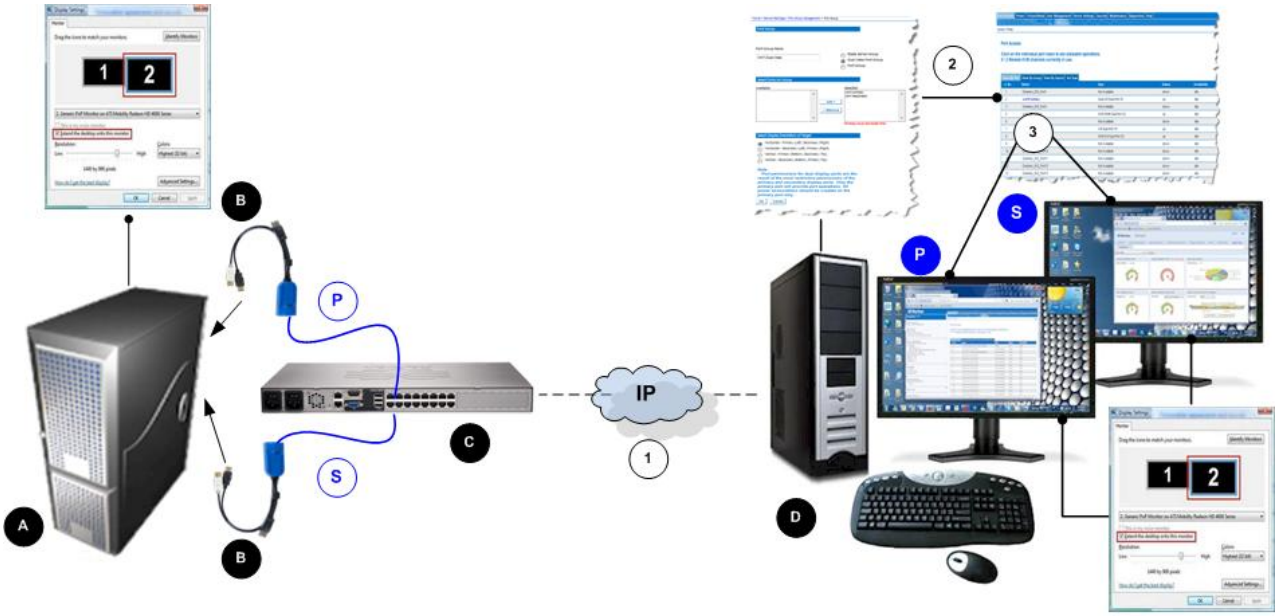
在启用 KVM 会话限制之后，两个会话都必须可供用户使用，否则拒绝所有两个连接。

双端口视频组配置示例

下列步骤用常规示例加以说明。实际配置可能会有差异，视所用的 CIM 的类型、指定为主端口的端口、要连接的 CommandCenter Secure Gateway 端口等因素而定。

在此示例中，我们使用：

- 一台有两个视频端口的目标服务器
- 目标服务器视频端口 1 是主端口，目标服务器视频端口 2 是辅端口
- 一台 CommandCenter Secure Gateway-832 设备
- 一个 D2CIM-DVUSB-DP CIM
- 运行 Microsoft® Windows 7® 操作系统的目标服务器和客户机
- 智能鼠标模式
- 目标服务器和远程客户机扩展桌面视图，以便配置 CommandCenter Secure Gateway 支持“水平 — 主端口（左），辅端口（右）”显示方向



图示符号	
A	目标服务器

图示符号	
B	数字 CIM
C	CommandCenter Secure Gateway
D	远程客户机
P	目标服务器第一个视频端口到 CommandCenter Secure Gateway 的连接
S	目标服务器第二个视频端口到 CommandCenter Secure Gateway 的连接
1	CommandCenter Secure Gateway 和远程客户机之间的 IP 连接
2	在 CommandCenter Secure Gateway 上创建双视频端口组
3	启动双视频端口组
P	主端口显示（在 CommandCenter Secure Gateway 的 Port Group Management [端口组管理]页上定义）
S	辅端口显示（在 CommandCenter Secure Gateway 的 Port Group Management [端口组管理]页上定义）

第一步：配置目标服务器显示设置

在 CommandCenter Secure Gateway 上给目标服务器配置的方向设置必须与目标服务器操作系统的实际配置相同。建议在连接客户机时使用相同的屏幕方向。

参看双视频端口组显示方向、校准和鼠标模式了解显示方向和鼠标模式。

注意：参看目标服务器用户手册或操作系统用户手册了解如何正确配置显示设置。

配置目标服务器显示设置和鼠标设置：

1. 在目标服务器上给每个视频端口配置目标服务器显示方向，使其与远程客户机的显示方向相同。

   例如如果在远程客户机的两台监视器上使用从左到右的扩展桌面方向，给目标服务器设置相同的显示方向。

2. 确保已给目标服务器视频设置了支持的分辨率和刷新速度。参看支持的视频分辨率。

注意： 如果目标服务器的主显示器和辅显示器设置为不同的分辨率，鼠标可能不同步，必须定期在目标服务器窗口左上角重新同步鼠标。

第二步：把目标服务器连接到 CommandCenter Secure Gateway

可以根据现有端口连接或新端口连接创建双端口视频组。这里假设要创建新连接。如果要根据现有连接创建双端口视频组，参看***第四步：创建双视频端口组*** (p. 411)。

连接设备：

1. 如果尚未安装目标服务器，根据制造商提供的说明书安装目标服务器并通电。
2. 把每个 CIM 的视频插头插入目标服务器的视频输出端口，把 USB 电缆插入目标服务器上空闲的 USB 端口。
3. 用五类/六类电缆把每个 CIM 连接到 CommandCenter Secure Gateway。
4. 用随机提供的电源线把 CommandCenter Secure Gateway 接到交流电源上，把它连接到 CommandCenter Secure Gateway 网络端口（必要时）并配置 CommandCenter Secure Gateway。参看入门了解如何开始使用 CommandCenter Secure Gateway。
5. 在有网络连接并安装了 Microsoft .NET® 和/或 Java Runtime Environment®（JRE® 可以在 ***Java 网站 http://java.sun.com/***下载）的任何工作站上登录 CommandCenter Secure Gateway。
6. 启动支持的网络浏览器，例如 Internet Explorer® 或 Firefox®。
7. 输入 URL：*http://IP-ADDRESS* 或 *http://IP-ADDRESS/akc* (.NET)，其中 IP-ADDRESS 是给 CommandCenter Secure Gateway 分配的 IP 地址。也可以使用 https 和管理员分配的 CommandCenter Secure Gateway DNS 名称（假定配置了 DNS 服务器），或者只在浏览器地址栏输入 IP 地址（CommandCenter Secure Gateway 始终把 IP 地址由 HTTP 重定向到 HTTPS）。
8. 输入用户名和密码。单击 Login（登录）按钮。
9. 配置目标服务器鼠标模式。

   例如如果在远程客户机上使用智能鼠标模式，把目标服务器设置为使用智能鼠标模式。参看鼠标设置了解你使用的操作系统要求的鼠标模式设置。

第三步：配置鼠标模式和端口

在通过目标服务器视频端口把目标服务器连接到 CommandCenter Secure Gateway 之后，CommandCenter Secure Gateway 检测此连接，Port Configuration（端口配置）页显示视频端口。参看配置标准目标服务器了解配置步骤。

在配置端口之后，可以把端口组合成双视频端口组。

*注意：如果已配置了现有端口，不必再配置这些端口。参看***创建双视频端口组** *(p. 412)**了解如何创建双视频端口组。*

在连接目标服务器之后，配置目标服务器鼠标模式。例如如果在远程客户机上使用智能鼠标模式，把目标服务器设置为使用智能鼠标模式。参看鼠标设置了解你使用的操作系统要求的鼠标模式设置。

第四步：创建双视频端口组

参看***创建双视频端口组*** (p. 412)。

创建双视频端口组

可以利用双视频端口组功能把两个视频端口组合成一个端口组。在必须连接有两个显示卡/端口的服务器并在同一个远程客户机上同时访问两个端口时，可以使用此功能。

注意：KX2-108 和 KX2-116 等只有一个 KVM 通道的 CommandCenter Secure Gateway 设备不支持双视频端口组。

注意：在创建双视频端口组之后，可以在 Local Console 和 Remote Console 上访问此端口组。但是，Local Console 不支持扩展桌面。

Port Access（端口访问）页作为 Dual Port（双端口）类型显示双视频端口组。在 Port Access（端口访问）页上，主端口和辅端口分别作为 Dual Port(P)（双端口 (P)）和 Dual Port(S)（双端口 (S)）显示。例如如果 CIM 类型是 DCIM，显示 DCIM Dual Port (P)（DCIM 双端口 (P)）。

每个端口组必须有一个主端口和一个辅端口。把应用于主端口的配置应用于同组里的所有辅端口。如果把一个端口从端口组里删除掉，此端口即被视为独立端口，可以把新配置应用于此端口。

在远程客户机上访问双端口视频组时连接主端口，打开 KVM 连接窗口显示双端口组的主端口和辅端口。

必要时可以在一台或多台远程客户机上启动会话，并在监视器上观看会话。

在 CommandCenter Secure Gateway 上给目标服务器配置的方向设置必须与目标服务器操作系统的实际配置相同。建议在连接客户机时使用相同的屏幕方向。

重要说明：参看双视频端口组一节了解可能会影响特定操作系统环境的限制和建议。

创建双端口视频组：

1. 选择 Device Settings（设备设置）> Port Group Management（端口组管理），打开 Port Group Management（端口组管理）页，显示现有的所有端口组。
2. 单击 Add（添加）按钮打开 Port Group（端口组）页，Select Ports for Group（给组选择端口）部分显示所有可用端口。

   注意：如果一个端口已经是刀片服务器端口组、另一个双视频端口组或标准端口组的组成部分，此端口不再是其中一个选项，因为一个端口只能属于一个端口组。
3. 选择 Dual Video Port Group（双视频端口组）单选按钮。

4. 单击 Select Ports for Group（给组选择端口）部分显示的要指定为主端口的端口， 然后单击 Add（添加）按钮把它添加到 Selected（选择）文本字段里。确保先添加主端口。

   *注意：应用于端口组里每个端口的权限应该相同。如果权限不相同，要把限制最多的端口权限应用于端口组。例如如果把 VM Access Deny（VM 拒绝访问）应用于一个端口，把 VM Access Read-Write（VM 读写访问）应用于另一个端口，要把 VM Access Deny（VM 拒绝访问）应用于此端口组。参看***权限和双视频端口组访问权** *(p. 417)**了解端口权限如何影响双视频端口组。*

5. 单击要指定为辅端口的端口， 然后单击 Add（添加）按钮把它添加到 Selected（选择）文本字段里。
6. 选择页面方向。选择最适合监视器设置的方向。
7. 单击 OK（确定）按钮创建端口组。

   Port Access（端口访问）页作为 Dual Port（双端口）类型显示双视频端口组。在 Port Access（端口访问）页上，主端口和辅端口分别作为 Dual Port(P)（双端口 (P)）和 Dual Port(S)（双端口 (S)）显示。例如如果 CIM 类型是 DCIM，显示 DCIM Dual Port (P)（DCIM 双端口 (P)）。

注意：当双视频端口目标服务器连接分层设备时，只应通过分层设备访问目标服务器，不应通过基础设备访问目标服务器。

第五步：启动双端口视频组

在创建双视频端口组之后，Port Access（端口访问）页显示双视频端口组。单击主端口远程连接双视频端口组需要两个 KVM 通道。如果两个通道都不可用，不显示 Connect（连接）链接。

在 CommandCenter Secure Gateway 上配置的会话超时要有用于双视频端口组的两个端口。

启动双视频端口组：

- 在 Port Access（端口访问）页上单击主端口名称，然后单击 Connect（连接）按钮。立刻启动两个连接，每个窗口显示一个连接。

在打开窗口之后，可以根据自己使用的显示设置移动窗口。例如如果使用扩展桌面模式，可以在两个监视器之间来回移动端口窗口。

双端口视频建议

把目标服务器的主显示器和辅显示器设置为相同的视频分辨率，使鼠标保持同步，最大限度地减少定期同步次数。

根据希望的显示方向，上显示（垂直方向）或左显示（水平方向）应该是指定的主显示方向。显示器有活动菜单，可以选择虚拟媒体、音频、智能卡和鼠标操作。

为了实现直观的鼠标运动和控制，下列各项的显示方向应该相同：客户机 PC 的主显示器和辅显示器、CommandCenter Secure Gateway 双视频端口组配置、目标服务器的主显示器和辅显示器。

只有下列 Client Launch Settings（客户机启动设置）要应用于双端口视频显示：

- 在启动 KVM 客户机时，选择标准显示模式或全屏窗口模式。
- 启用视频缩放。
- 启用在全屏模式下固定菜单工具栏。

在一台客户机监视器上采用全屏模式显示双视频端口时，建议不要使用单鼠标模式。访问和观看另一个显示器需要退出单鼠标模式。

支持的鼠标模式

目标服务器操作系统	支持的鼠标模式	备注
所有 Windows® 操作系统	智能鼠标模式、标准鼠标模式和单鼠标模式	如果目标服务器显示卡支持拉伸模式，绝对鼠标模式也能正常工作。 在拉伸模式下，目标服务器把双显示器视为一个虚拟显示器进行管理。在扩展模式下的情形与此相反，目标服务器把显示器视为两个独立显示器。建议在扩展模式下使用智能鼠标模式。
Linux®	智能模式和标准鼠标模式	如果 Linux® VKC/MPC 用户使用单鼠标模式，可能会发生显示问题和鼠标运动问题。Raritan 建议 Linux 用户不要使用单鼠标模式。
Mac® 操作系统	单鼠标模式	在 Mac 双视频端口目标服务

目标服务器操作系统	支持的鼠标模式	备注
		器上，鼠标不同步。

双视频支持要求的 CIM

下列数字 CIM 支持双视频端口功能：

- D2CIM-VUSB
- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-DP
- D2CIM-DVUSB-HDMI
- DCIM-USBG2

参看数字 CIM 目标服务器时间设置和视频分辨率了解数字 CIM 重要信息。参看支持的计算机接口模块 (CIM) 规格了解 CIM 规格。

如果断开与主视频端口或辅视频端口相连的原 DCIM，并换用另一个 CIM，就把此端口从双端口视频组里删除掉。 必要时把此端口重新添加到端口组。

注意：使用的 CIM 视目标服务器的要求而定。

双端口视频组可用性说明

在使用双端口视频组功能时，会影响下列功能。

- 在 VKC、AKC 和 MPC 客户机的 Tools（工具）> Options（选项）> Client Launch Settings（客户机启动设置）上配置的 Client Launch Settings（客户机启动设置）要如下应用于双视频端口组：
  - 要应用 Window Mode（窗口模式）设置
  - 不应用 Monitor(监视器)设置，要应用在 Port Group Management（端口组管理）页上配置的 Display Orientation（显示方向）。
  - 不应用 Other - Enable Single Mouse Cursor（其他 — 启用单鼠标光标）设置
  - 要应用 Other - Enable Scale Video（其他 — 启用缩放视频）设置
  - 要应用 Other - Pin Menu Toolbar（其他 — 固定菜单工具栏）设置

- 如果在主目标服务器窗口和辅目标服务器窗口之间拖放对象，在把对象从一个窗口移动到另一个窗口时，要求先释放鼠标键，然后再按鼠标键。
- 在 Linux® 和 Mac® 目标服务器上，在激活 Caps Scroll 和 Num Lock 键时，主端口窗口的状态栏显示 Caps Lock 指示器，但辅端口窗口的状态栏并不显示指示器。
- 在全屏模式下打开双端口目标服务器时，可能不启用 MPC 菜单。如要激活菜单，可以切换到另一个端口窗口，然后再切换回原端口窗口。

权限和双视频端口组访问权

应用于端口组里每个端口的权限应该相同。如果权限不相同，要把限制最多的端口权限应用于端口组。

例如如果把 VM Access Deny（VM 拒绝访问）应用于一个端口，把 VM Access Read-Write（VM 读写访问）应用于另一个端口，要把 VM Access Deny（VM 拒绝访问）应用于此端口组。

如果用户没有适当权限访问作为双视频端口组组成部分的端口，只显示他/她有权访问的端口。如果用户无权访问任何一个端口，系统拒绝访问。

当用户尝试访问不可用的端口或自己无权访问的端口时，显示一条消息说明端口不可用或他/她无权访问此端口。

在使用双视频端口组时的 Raritan 客户机导航

导航

在客户机上使用全屏模式时，如下切换端口：

- VKC

  按 Alt+Tab

  对于 Mac® 客户机，先按 F3，然后选择端口显示

- AKC

  用鼠标单击显示窗口外面，然后按 Alt+Tab

- MPC

  在 Connected server(s)（已连接服务器）工具栏上选择端口

直接端口访问和双端口视频组

直接端口访问允许用户绕过设备的 Login（登录）对话框和 Port Access（端口访问）页。此功能还允许用户在 URL 不包含用户名和密码的情况下，直接输入用户名和密码访问目标服务器。

如果访问作为双端口视频组组成部分的目标服务器，要用主端口同时启动主端口和辅端口。拒绝与辅端口建立直接端口连接，并应用常规权限规则。参看***创建双视频端口组*** (p. 412)了解双端口视频组功能。 参看启用通过 URL 进行直接端口访问了解直接端口访问。

端口页显示双端口视频组

注意：在创建端口组时，定义双视频主端口。

注意： 单击主端口远程连接双视频端口组需要两个 KVM 通道。如果两个通道都不可用，不显示 Connect（连接）链接。

对于双视频端口组，在远程客户机上建立连接时，端口扫描包括主端口，但不包括辅端口。在 Local Port（本地端口）上建立连接时，可以同时包括主端口和辅端口。

参看端口访问页（Remote Console 显示）了解 Port（端口）页显示的信息，参看扫描端口了解如何执行扫描。

Ap J 利用 CC-SG 虚拟设备使用 VMware 高可用性或容错

对高可用性或容错感兴趣的虚拟机管理员必须熟悉当前使用的 vSphere Availability Guide ESX 的版本。

高可用性：

- 高可用性实现断电快速恢复 — 在断电之后，新的高可用性 vCCSG 实例可以在 3-5 分钟内正常提供服务。
- 在检测到最初运行 vCCSG 虚拟机的主机发生故障之后，另一台主机上的 vCCSG 虚拟机自动启动。
- 如果虚拟机发生故障，但主机没有发生故障，将重新启动虚拟机。注意这是根据检测信号和 I/O 监视结果作出的决定。在测试和确认时要谨记这一点。

正如 vSphere 可用性指南 ESX 4.1 的虚拟机和应用程序监视一节所述，“正常工作的虚拟机偶尔会停止发生检测信号。为了避免不必要地复位此类虚拟机，虚拟机监视服务还监视虚拟机的 I/O 活动。如果在故障间隔时间内没有接收到检测信号，就检查 I/O 统计间隔时间（群集级属性）。I/O 统计间隔时间确定虚拟机在过去两分钟（120 秒钟）内是否有任何磁盘活动或网络活动。如果没有任何活动，就复位虚拟机。”

容错：

- 容错实现连续可用性。在几秒钟内激活虚拟 CCSG 的第二个实例，使连接不中断并恢复数据流，把数据丢失率降到极低的水平。
- 两个虚拟机同时运行，其中一个是主虚拟机，另一个是备用虚拟机，但只有主虚拟机做出响应
- 当主虚拟机发生故障时，备用虚拟机接替它的工作，使连接不中断或数据不丢失。新的备用虚拟机启动并提供连续保护

比较：

高可用性的优点是缩短恢复时间，但可能会丢失数据；容错的优点是提高资源利用率，但可能会使性能下降。

容错要求群集具备高可用性。高可用性建立在下列基础之上：

- 允许在多个主机上进行虚拟机存储空间访问的共享存储器
- 采用高可用性存储器（存储空间是虚拟机）
- 冗余网络接口
- 冗余存储器路径

其他主要要求是在发生故障时，有可用资源确保高可用性正常工作。此任务通过准入控制来执行，如果允许通过禁用准入控制来超额预订故障切换容量，可以通过给虚拟机指定优先级并定义虚拟机重新启动策略来管理超额预订资源引发的资源争用问题。同时监视资源可用性确保高可用性群集连续可用。

群集高可用性设置：

- 打开高可用性群集的 Edit Settings（编辑设置）对话框配置 VMware 高可用性设置
- Cluster Features（群集功能）— 启用 VMware 高可用性
- VMware HA（VMware 高可用性）— 在高可用性模式下工作时启用主机监视，启用准入控制确保故障切换容量可用，设置准入控制策略满足群集可承受的主机故障数
- Virtual Machine Options（虚拟机选项）— 默认设置是中等重新启动优先级，在决定"隔离"虚拟机的主机上关闭虚拟机
- VM Monitoring（虚拟机监视）— 默认禁用虚拟机监视，只能设置为虚拟机监视
- Monitoring Sensitivity（监视灵敏度）— High（高）

在完成群集配置并给群集指定主机和虚拟机之后，可以测试高可用性故障切换。

虚拟机容错设置：

容错在一个虚拟机上运行 — 假定高可用性群集已配置并可用。容错也对主机、处理器和联网有额外要求。

vSphere 可用性指南 ESX 4.1 有两节详细说明容错兼容性对群集、主机和虚拟机的要求。包括一段在容错对中混用 ESX 和 ESXi — 即使最初侥幸成功了，也不要这么做 — 的重要须知。

至少有两个运行相同容错版本或主机版本号的容错主机。vSphere Client 的主机 Summary（摘要）选项卡显示容错版本号。

注意：对于 ESX/ESXi 4.1 之前的主机，此选项卡列出主机版本号。补丁可能会造成所安装的 ESX 和 ESXi 的主机版本号不相同。为了确保主机支持容错，切勿在容错对中混用 ESX 主机和 ESXi 主机。

容错对主机的要求

主要要求是主机必须有容错处理器，必须有容错许可，必须通过容错认证。确保在 BIOS 上启用了硬件虚拟化支持。vSphere Client 的主机 Summary（摘要）选项卡显示版本和容错配置信息。

如果尚未配置主机支持容错，但知道主机具备容错功能，可以检查 BIOS 设置。例如在 Dell R610 主机上，确保把 BIOS > Processor Settings（处理器设置） > Virtualization Technology（虚拟化技术）设置为 Enabled（启用）。

容错对虚拟机的要求

- 只有一个 vCPU 的虚拟机支持容错。
- 切勿给虚拟机连接不支持的设备。

用右键单击虚拟机节点，然后 Fault Tolerance（容错）> Turn On Fault Tolerance（启用容错）选项启用容错。如果上述各项配置错误，系统会显示错误消息，必须修改某些设置。

参看 vSphere 可用性指南 ESX 4.1 中的表 3-1 支持容错的功能部件和设备及校正措施了解详情。

可能的错误和校正措施：

对称多处理器虚拟机。只有一个 vCPU 的虚拟机支持容错。

把虚拟机配置为一个 vCPU。把虚拟机配置为一个 vCPU，很多工作负荷的性能很好。

在给虚拟机启用容错时显示错误消息：The virtual machine has more than one virtual CPU.（虚拟机有多个虚拟 CPU。）

打开 Edit Settings（编辑设置）对话框把 vCPU 数设置为 1。

物理设备或远程设备支持的 CD-ROM 或软盘虚拟设备。删除 CD-ROM 或软盘虚拟设备，或者用共享存储器安装的 ISO 重新配置支持。在给虚拟机启用容错时显示错误消息：Device 'CD-ROM1' has a backing type that is not supported.（'CD-ROM1' 设备有不支持的支持类型。）

打开 Edit Settings（编辑设置）对话框把此设备从硬件设备列表上删除掉。如果需要此设备，可以在禁用容错之后重新添加此设备执行维护功能。

虚拟机在不支持容错的监视器模式下运行。断开虚拟机电源，然后启用容错。此限制取决于 CPU 版本和你运行的客户机的类型。必须先断开虚拟机电源，然后再启用容错。

在修改这些设置之后，接通虚拟机电源，然后启用容错。

Ap K 常见问题解答

在本章内

常见问题解答

问题	解答
常规	
什么是 CC-SG？	CC-SG 是一种网络管理设备，用于整合和集成通常在数据中心部署的、与 Raritan IP 产品相连的多台服务器和网络设备。
为什么要使用 CC-SG？	随着在数据中心部署的服务器和设备越来越多，管理变得越来越复杂。CC-SG 允许系统管理员在一台设备上访问和管理所有服务器、设备和用户。
CC-SG 支持哪些 Raritan 产品？	参看 Raritan 网站上支持部分固件和文档下的兼容性指标。
CC-SG 如何与其他 Raritan 产品集成在一起？	CC-SG 采用独创的专用搜索和发现技术，确定和连接有已知网络地址的所选 Raritan 设备。在连接和配置 CC-SG 之后，与 CC-SG 相连的设备是透明的，操作和管理极其简单。
CC-SG 的状态是否受制于它代理的设备的状态？	不。由于 CC-SG 软件安装在专用服务器上，即使 CC-SG 代理的设备关机了，你仍然可以访问 CC-SG。
在推出 CC-SG 更新软件时，能否升级到更新版本？	可以。请联系 Raritan 授权销售代表，或者直接联系 Raritan。
CC-SG 可以连接多少节点和/或 Dominion 设备和/或	可以连接的节点数和/或 Dominion 数和/或 IP-Reach 设备数没有限制，但实际连接数并不是无

问题	解答
IP-Reach 设备？	限的：主服务器的处理器性能和内存容量决定实际上可以连接多少节点。
如果不能给 CC-SG 添加控制台端口/串行端口，该怎么办？	假设控制台/串行设备是 Dominion，确保满足下列条件： —Dominion 设备处于活动状态。 —Dominion 设备尚未达到配置的最大用户帐号数。
Raritan CC-SG 支持哪个版本的 Java？	参看 Raritan 网站上支持部分固件和文档下的兼容性指标。
管理员在 CC-SG 数据库里为我添加了一个新节点。如何才能在我的节点树上看到它？	如要更新节点树看到新指定的节点，单击工具栏上的 Refresh（刷新）按钮。切记在刷新 CC-SG 时，关闭当前的所有控制台会话。
未来如何支持 Windows 桌面？	在防火墙上配置适当的端口，可以从防火墙外部访问 CC-SG。下列端口是标准端口： 80: 用于通过网络浏览器进行 HTTP 访问 443: 用于通过网络浏览器进行 HTTPS 访问 8080: 用于 CC-SG 服务器操作 2400: 用于代理模式连接 5001: 用于 IPR/DKSX/DKX/ P2-SC 事件通知 如果两个群集节点之间有防火墙，必须打开下列端口，群集才能正常工作： 8732: 用于群集节点检测信号 5432: 用于群集节点数据库复制
大型系统设计要遵循哪些原则？有哪些限制或前提条件？	Raritan 提供两种服务器扩展模型：数据中心模型和网络模型。 数据中心模型使用 Paragon，可以扩展到一个数据中心的数千个系统。这是扩展一个位置最有效、最经济的方式。它还通过 IP-Reach 和 IP 用户工作站 (UST-IP) 支持网络模型。 网络模型扩展 TCP/IP 网络范围，通过 CC-SG 整合网络访问，所以用户不必知道访问设备的 IP 地址或拓扑。它还提供便捷的单点登录机制。
在把刀片服务器机箱从一个 KX2 端口移动到另一个 KX2 端口之后，CC-SG 是否自动检	在把刀片服务器机箱移动到另一个 KX2 端口或另一台设备之后，CC-SG 不自动检测并更新刀片服务器机箱配置。失去刀片服务器机箱配置，所以你必须

问题	解答
测并更新刀片服务器机箱配置？	再次在 CC-SG 上配置刀片服务器机箱。
如果刀片服务器节点和虚拟主机节点指的是同一台服务器，如何合并它们？	应该在配置刀片服务器插槽之前配置虚拟化功能。在配置刀片服务器插槽时，输入与虚拟主机节点相同的名称，在显示消息时选择将此接口添加到现有节点。

验证常见问题解答

问题	解答
验证	
可以给 CC-SG 创建多少用户帐号？	查看你的许可限制。可以给 CC-SG 创建的用户帐号数没有限制，但实际帐号数并不是无限的。主服务器上数据库的大小、处理器性能和内存容量决定实际可以创建多少用户帐号。
能否给特定用户指定特定节点访问？	可以，但你必须有管理员权限。管理员可以按用户指定特定节点。
如果我们有 1,000 多个用户，如何进行管理？是否支持 Active Directory？	CC-SG 使用 Microsoft Active Directory、Sun iPlanet 或 Novell eDirectory。如果验证服务器已经有用户帐号了，CC-SG 支持用 AD/TACACS+/RADIUS/LDAP 验证进行远程验证。
LDAP、AD 和 RADIUS 等目录服务和安全工具有哪些可用的验证选项？	CC-SG 允许本地验证和远程验证。 支持的远程验证服务器包括：AD、TACACS+、RADIUS 和 LDAP。
在正确输入有效用户名和密码登录 CC-SG 时，为什么显示 Incorrect username and/or password（用户名和/或密码错误）消息？	在 AD 里检查用户帐号。如果 AD 设置为 Logon To（登录）域里的特定计算机，你不能登录 CC-SG。在这种情况下，删除 AD 里的 Logon To（登录）限制。

安全常见问题解答

问题	解答
安全	

问题	解答
有时在尝试登录时，会显示 login is incorrect（登录名错误）消息，但我确定输入的用户名和密码正确无误。为什么会这样？	每当你开始登录 CC-SG 时，发出一个会话特定的 ID。此 ID 有超时功能，如果你不在超时之前登录设备，会话 ID 即失效。在 CC-SG 上人工刷新页面，或者关闭当前浏览器，打开新浏览器重新登录。这样可以提供附加安全保护，任何人都不能调用 Web 高速缓冲存储的信息来访问设备。
密码安全性如何？	密码用 MD5 加密，这是单向散列加密方法。这样可以提供附加安全保护，防止未经授权的用户访问密码列表。
有时我离开工作站一段时间后，单击 CC-SG 的任何菜单时，显示 No longer logged in（没有登录）消息。为什么会这样？	CC-SG 给每个用户会话定时。如果在预先定义的时间内没有活动，CC-SG 就退出用户。时间长度预设为 60 分钟，但可以重新配置。建议用户在完成会话之后退出 CC-SG。
由于 Raritan 有服务器根访问权，政府机构使用 CC-SG 时可能会出问题。客户能否具有根访问权？Raritan 能否提供一种审计/责任方法？	在 Raritan 发出设备之后，任何一方都没有服务器根访问权。
SSL 是否同时是内部和外部加密方法（不仅仅 WAN，也包括 LAN）？	两者。无论会话源头是 LAN 还是 WAN，都要加密。
CC-SG 是否支持 CRL 表，即无效证书 LDAP 表？	否。
CC-SG 是否支持客户机证书请求？	否。

日志常见问题解答

问题	解答
日志	
审计跟踪报告上的事件时间似乎不正确。为什么会这样？	日志事件时间是根据客户计算机上的时间设置记录的。你可以调整计算机的时间和日期设置。
审计/日志功能能否跟踪到谁接通或断开电源插头？	不记录直接关电，但通过 CC-SG 进行的电源控制被记录到审计日志里。

性能常见问题解答

问题	解答
性能	
作为 CC-SG 管理员，我添加了 500 多个节点，并把它们全部指定给自己。现在记录到 CC-SG 所需的时间很长。	作为管理员，如果你给自己指定了很多节点，CC-SG 在记录过程中要下载所有节点的全部信息，使整个过程变得很长。管理员帐号主要用于管理 CC-SG 配置，建议不要给它们指定很多节点。
每个客户机的带宽用量有多大？	通过 TCP/IP 远程访问串行控制台，其网络活动与 telnet 会话相当。但最大带宽限制在控制台端口本身的 RS232 带宽加上 SSL/TCP/IP 开销。 Raritan Remote Client (RRC) 控制 KVM 控制台远程访问。此应用程序的带宽是可以调节的，可以在 LAN 带宽和远程拨号用户带宽之间调节。

组合常见问题解答

问题	解答
组合	
是否可以把一台给定服务器放在多个组内？	可以。正如一个用户可以属于多个用户组，一台设备也可以属于多个设备组。 例如 NYC 组里的 Sun 也可以是 Sun 组的一部分："Ostype = Solaris"，同时是 New York 组的一部分："location = NYC"。
主动用控制台端口登录对其他应用有什么影响？例如某些 Unix 不允许通过网络接口进行 admin 登录。	控制台通常被视为安全可靠的最终登录途径。某些 Unix 系统只允许在控制台上进行根登录。出于安全原因，其他系统可能不允许多次登录，所以如果管理员在控制台上登录，其他访问即被拒绝。最后，如果有必要阻止其他所有访问，管理员也可以在控制台上禁用网络接口。 控制台上的正常命令活动造成的影响，并不比在其他任何接口上运行同样的命令大。但是，由于它独立于网络，因负荷太大而不能响应网络登录的系统仍然支持控制台登录。因此，控制台访问的另一个好处就是可以诊断和排除系统问题和网络问题。
如果在物理移动/更换 CIM 并更改逻辑数据库时出问题，	每个 CIM 有一个序列号和目标系统名称。我们的系统假设在切换器之间移动 CIM 连接时，CIM 仍然与命名

问题	解答
你建议如何处理？例如：如果把目标服务器上的 CIM 从一个端口端口移动到另一个端口上（可以是相同设备，也可以是不同设备），结果会怎么样？端口名称会发生什么情况？节点会发生什么情况？接口会发生什么情况？	目标相连。CC-SG 上的端口和接口自动反映 CIM 移动；自动更新端口名称和接口名称，反映它们发生的变化。在与端口关联的节点下面显示接口。但是，节点名称保持不变。必须人工编辑节点，重新命名节点。这种模式假定有关的所有端口事先都被配置了。如果把目标服务器和 CIM 物理移动到一个未配置的不同端口上，可以在 CC-SG 上配置此端口，自动创建节点。

互通性常见问题解答

问题	解答
互通性	
CC-SG 如何与刀片服务器机箱产品集成在一起？	CC-SG 可以采用透明直通方式支持有 KVM 接口或串行接口的任何设备。
CC-SG 可以在多大程度上集成第三方 KVM 工具，直到第三方 KVM 端口或设备？	如果第三方 KVM 供应商不公开第三方 KVM 切换器通信协议，第三方 KVM 交换机集成一般通过键盘宏来实现。集成紧密程度视第三方 KVM 切换器的功能而定。
如何通过任何 IP-Reach 设备降低四个并发路径这一限制，包括潜在的八路径设备的路线图？	目前最好的实现方法是把 IP-Reach 设备和 CC-SG 整合在一起。Raritan 计划以后增加每台设备的并发访问路径数。由于优先开发其他项目，尚未完成这些计划的开发工作，但我们欢迎你提出市场需求建议和八路径解决方案用例建议。

授权常见问题解答

问题	解答
授权	
是否可以通过 RADIUS/TACACS/LDAP 实现授权？	LDAP 和 TACACS 只用于远程验证，不用于授权。

用户体验常见问题解答

问题	解答
用户体验	
关于通过网络端口或本地串行接口（例如 COM2）进行控制台管理：登录会发生什么情况？CC-SG 是否捕获本地管理？	通过 CC-SG 控制台登录 CC-SG，与在运行 CC-SG 的操作系统 (Linux) 上获得根权限相同。系统日志记录此事件，但用户在 CC-SG 控制台上输入的信息会丢失。

许可常见问题解答

如果必须更换已安装的许可，要遵循下列规则。

必须先更换基本许可。	例如：如果用群集许可 CC-2XE1-512 和 CCL-512 更换单机许可 CC-E1-512 和 CCL-512，必须先更换基本许可 CC-E1-512，再更换附加许可 CCL-512。 注意如果单机和群集的附加许可 CCL-512 相同，单机许可文件只有一个主机 ID，而群集许可文件有两个主机 ID。在此情况下，也要更换附加许可。
如果基本许可和附加许可的类型不相同，在更换基本许可时清除所有附加许可。	如果用群集基本许可更换单机基本许可，将自动清除附加许可，可能需要有正确主机 ID 的新许可，反之亦然。
如果基本许可和附加许可的类型相同，且主机 ID 相匹配，在更换基本许可时并不清除所有附加许可。	例如可以用 CC-E1-512 取代 CC-E1-256。如果两个许可的主机 ID 相同，附加许可仍然有效。
如果使用单机许可运行群集，必须删除群集才能更换单机许可，然后重新加入群集。	由于群集成员不共享单机许可，所以在使用单机许可的群集里的每台 CC-SG 必须有相同的许可节点数。 为了在两台 CC-SG 设备之间共享许可，客户可能宁可过渡到群集许可，而不是增加每台 CC-SG 设备的许可节点数量。 临时删除群集，更换许可，然后重新创建群集。
在更换基本许可时，要求用户先注销许可。	在更换许可之后打开 License Manager（许可管理器）页检查可用许可，并按需要注销许可。不自动注销许可。参看安装和注销许可。
在更换许可取消许可服务器并过渡到非服务器模式时，删除已上载的所有许可。	在上载非服务器基本移植许可之后，CC-SG 必须重新启动。再次登录 CC-SG 时，CC-SG 进入有限工作模式，你可以上载其他功能许可并注销所有许可，从而退出有限工作模式。

Ap L 键盘快捷键

在 Java Admin Client 上可以使用下列键盘快捷键。

操作	键盘快捷键
刷新	F5
打印面板	Ctrl+P
帮助	F1
在关联表上插入行	Ctrl+I

Ap M 命名常规

本附录介绍 CC-SG 使用的命名常规。在命名 CC-SG 配置的任何部分时，要遵守最大字符长度限制。

在本章内

用户信息

CC-SG 上的字段	CC-SG 允许的字符数
Username（用户名）	64
Full Name（全名）	64
User Password（用户密码[常规密码]）	6-16
User Password（用户密码[强密码]）	可配置 最少：8 最多：16-64
User Email Address（用户电子邮件地址）	60
User Phone Number（用户电话号码）	32
User Group Name（用户组名称）	64
User Group Description（用户组说明）	160

节点信息

CC-SG 上的字段	CC-SG 允许的字符数
Node Name（节点名称）	64

CC-SG 上的字段	CC-SG 允许的字符数
Node Description（节点说明）	160
Notes（备注）	256
Audit Information（审计信息）	256

位置信息

CC-SG 上的字段	CC-SG 允许的字符数
Department（部门）	64
Site（地点）	64
Location（位置）	128

联系人信息

CC-SG 上的字段	CC-SG 允许的字符数
Primary Contact Name（主联系人姓名）	64
Telephone Number（电话号码）	32
Cell Phone（手机号码）	32
Secondary Contact Name（第二联系人姓名）	64
Telephone Number（电话号码）	32
Cell Phone（手机号码）	32

服务帐号

CC-SG 上的字段	CC-SG 允许的字符数
Service Account Name（服务帐号名称）	64
User Name（用户名）	64
Password（密码）	64
Description（说明）	128

设备信息

CC-SG 上的字段	CC-SG 允许的字符数
Device Name（设备名称）	64
PX Device Names（PX 设备名称）不能使用句点。在导入有句点的 PX 设备名称时，句点转换成连字符。	
Device Description（设备说明）	160
Device IP/Hostname（设备 IP/主机名）	64
Username（用户名）	64
Password（密码）	64
Notes（备注）	256

设备名称不能使用空格 ( ) 和句点 (.) 字符。

设备名称可以使用其他任何特殊字符，但不能以特殊字符开头，必须以字母数字字符开头。

当设备名称包含小于 (<) 字符或大于 (>) 字符时，在主屏幕显示的 Device Updated Successfully（设备已成功更新）消息中的设备名称在显示时可能不包括小于字符或大于字符，视这些字符所在的位置而定。

例如所有字符用引号引起来：

- "KX2-<232>" 显示大于符号，但不显示小于符号。
- "KX2-232,/<>?" 不显示大于符号和小于符号。

端口信息

CC-SG 上的字段	CC-SG 允许的字符数
Port Name（端口名称）	32

关联

CC-SG 上的字段	CC-SG 允许的字符数
Category Name（类别名称）	32
Element Name（元素名称）	32

CC-SG 上的字段	CC-SG 允许的字符数
Device Group Name（设备组名称）	40
Node Group Name（节点组名称）	40

管理

CC-SG 上的字段	CC-SG 允许的字符数
Cluster Name（群集名称）	64
Neighborhood Name（邻居名称）	64
Authentication Module Name（验证模块名称）	31
Backup Name（备份名称）	64
Backup File Description（备份文件说明）	255
Broadcast Message（广播消息）	255

Ap N 诊断控制台启动消息

在 CC-SG v4.0 之前，每当 CC-SG 诊断控制台启动时，屏幕显示许多消息。这些消息是标准的 Linux 诊断和警告消息，通常不暗示系统有任何问题。下表简单介绍几种常见消息。

消息	Description（说明）
hda:	此消息说明系统上的某个东西尝试与 DVD-ROM 驱动器通信。在不同的情况下，均可调用此消息。例如： • 用户开关 DVD-ROM 驱动器门，或者 • 操作系统在启动时检查 DVD-ROM 驱动器，发现驱动器里没有光盘。 在其他情况下也可以调用此消息，本节不讨论其他情况。
avc:	此消息来自内部安全审计和控制系统：SELinux 子系统。系统发出警告消息，但不执行任何安全策略，所以这并不表示系统存在任何问题。
ipcontracks:	每当 CC-SG 启动时，始终显示此消息，所以这是正常现象。

注意从 CC-SG v4.0 开始，CC-SG 不再显示这些消息，但仍然可以在内部日志里查看这些消息。因此，在把 CC-SG 从 3.x 升级到 4.x 时，诊断控制台不显示这些消息了。

索引

R

S

T

V

W

二划

三划

四划

五划

六划

七划

八划

九划

十划

十一划

十二划

十三划

十四划

十六划

美国/加拿大/拉丁美洲

星期一至星期五
上午 8:00 - 傍晚 8:00 东部时间
电话：800-724-8090 或 732-764-8886
对于 CommandCenter NOC：按 6，然后按 1
对于 CommandCenter Secure Gateway：按 6，然后按 2
传真:732-764-8887
有关 CommandCenter NOC 的电子邮件：tech-ccnoc@raritan.com
有关其他所有产品的电子邮件：tech@raritan.com

中国

北京

星期一至星期五
上午 9:00 - 下午 6:00 当地时间
电话：+86-10-88091890

上海

星期一至星期五
上午 9:00 - 下午 6:00 当地时间
电话：+86-21-5425-2499

广州

星期一至星期五
上午 9:00 - 下午 6:00 当地时间
电话：+86-20-8755-5561

印度

星期一至星期五
上午 9:00 - 下午 6:00 当地时间
电话：+91-124-410-7881

日本

星期一至星期五
上午 9:30 - 下午 5:30 当地时间
电话：+81-3-3523-5991
电子邮件：support.japan@raritan.com

欧洲

欧洲

星期一至星期五
上午 8:30 - 下午 5:00 GMT+1 中欧时间
电话：+31-10-2844040
电子邮件：tech.europe@raritan.com

英国

星期一至星期五
上午 8:30 - 下午 5:00 GMT
电话：+44(0)20-7090-1390

法国

星期一至星期五
上午 8:30 - 下午 5:00 GMT+1 CET
电话：+33-1-47-56-20-39

德国

星期一至星期五
上午 8:30 - 下午 5:30 GMT+1 CET
电话：+49-20-17-47-98-0
电子邮件：rg-support@raritan.com

澳大利亚墨尔本

星期一至星期五
上午 9:00 - 下午 6:00 当地时间
电话：+61-3-9866-6887

台湾

星期一至星期五
上午 9:00 - 下午 6:00 GMT-5 标准时间 GMT-4 夏令时
电话：+886-2-8919-1333
电子邮件：support.apac@raritan.com