CommandCenter Secure Gateway

管理员指南

版本 **4.1**

CCA-0I-v4.1-CHS

2008 年 12 月

255-80-5140-00

FCC Information

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential environment may cause harmful interference.

VCCI Information (Japan)

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。

1F61
I.T.E.

目录

被管配电盘 61

节点、节点组和接口 68

报告 148

高级管理 175

诊断控制台 233

V1 和 E1 规格 274

CC-SG 和网络配置 277

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。

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

入门指导：CC-SG 基础

本章介绍一些最常见的用例，有助于用户迅速熟悉 CC-SG 的实际应用。注意本节介绍常见示例，可能会随你的实际配置和操作而有所不同。

在本章

配置和强制实行强密码

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）。该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）：
   - 密码必须包含至少一个小写字母。
   - 密码必须包含至少一个大写字母。
   - 密码必须包含至少一个数字。

- 密码必须包含至少一个特殊字符（例如感叹号或 &）。

8. 单击 Update（更新）按钮保存更改。

参看*登录设置* (p. 202)，详细了解登录安全。

升级 CC-SG 固件版本

在发布新版固件时，你可以升级 CC-SG 的固件。可以在 Raritan 网站的“支持”部分找到固件文件。如要将 CC-SG 从 v3.x 升级到 v4.1，必须先将它升级到 v4.0。

CC-SG v4.0 或更高版本不兼容 G1 硬件。切勿将 CC-SG G1 设备升级到 v4.0 或更高版本。

将固件文件下载到客户机 PC 上，然后再进行升级。

只有具备 CC 设置和控制权的用户才能升级 CC-SG。

应该在升级之前备份 CC-SG，将备份文件发送到 PC 上妥善保存。参看*备份 CC-SG* (p. 163) 和*保存备份文件* (p. 165)。

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：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。

CC-SG 重新引导，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，切勿人工重启设备，切勿切断设备电源，切勿给设备重新通电。

▶ 升级 CC-SG：

1. 将固件文件下载到客户机 PC。
2. 用具备 CC 设置和控制权的帐号登录 CC-SG Admin Client。
3. 进入 Maintenance Mode（维护模式）。参看*进入维护模式* (p. 162)。
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，将固件文件上载到 CC-SG。

   在固件文件被上载到 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. 240)。
   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）按钮查看升级日志。
   c. 等待升级过程运行。当你在 upgrade.log 里看到 "Upgrade completed" 消息时，表示升级过程完成了。也可以等待 SNMP 陷阱 ccImageUpgradeResults 显示 "success" 消息。
   d. 服务器必须重新引导。当你在 upgrade.log 里看到 "Linux reboot" 消息时，表示开始重新引导。服务器关机并重新引导。

   注意：对于从 CC-SG 3.x 升级到 4.0.x，系统重新引导两次，这是正常现象。

   e. 在系统重新引导之后大约两分钟，可以通过管理员帐号重新访问诊断控制台，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. 171)。
10. 清除 Java 高速缓存。参看*清除 **Java** 高速缓存* (p. 172)。
11. 启动新浏览器窗口。
12. 用具备 CC 设置和控制权的帐号登录 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. 163)。

备份 CC-SG。参看*备份 **CC-SG*** (p. 163)。

控制节点组电源和监视电源控制操作

节点组电源控制

可以对一个节点组里有关联电源接口的所有节点执行通电、断电、重新通电或正常关机操作。

如果必须断开一个节点组里所有节点的电源，以便对安装机架重新布线，或者必须对一个节点组执行其他维护，这种操作很有用。

参看 **CC-SG 用户指南**里的通过多个接口控制节点电源的注意事项，详细了解如何给有多个电源控制接口的节点设置电源控制操作。

1. 单击 Nodes（节点）选项卡。
2. 选择 Nodes（节点）> Group Power Control（组电源控制）。显示 Group Power Control（组电源控制）屏幕。
3. 单击 Node Group（节点组）下拉箭头，在列表上选择要控制哪个节点组的电源。
4. 在 Available（可用）列表上选择要对哪个特定接口执行电源控制，单击 Add（添加）按钮将它移动到 Selected（选择）列表上。重复此步骤，直到将所有必要接口添加到 Selected（选择）列表上为止。如果必须删除一个接口，在 Selected（选择）列表上选择该接口，然后单击 Remove（删除）按钮。
5. 根据你希望 CC-SG 执行电源操作的顺序，排列 Selected（选择）列表上的接口。在 Selected（选择）列表上选择一个接口，单击上下箭头键将它移动到希望的位置。
6. 单击 Operation（操作）下拉箭头，在列表上选择 Power On（通电）、Power Off（断电）、Power Cycle（重新通电）、Graceful Shutdown（正常关机）或 Suspend（暂停）。
7. 如果在 Operation（操作）字段里了选择 Power On（通电）、Power Off（断电）、Graceful Shutdown（正常关机）或 Suspend（暂停），在 Sequence Interval (seconds)（顺序间隔(秒)）字段里输入接口之间的间隔秒数 (0-120)。
8. 单击 OK（确定）按钮，通过所选接口发送电源操作请求。显示确认消息。
9. 打开 Power Status Messages（电源状态消息）窗口，显示电源控制操作状态。在收到有关电源控制操作的新消息时，该窗口更新这些消息。让此窗口保持打开状态，直到所有电源控制操作完成为止，这样可以监视进度。

   参看 ***电源状态消息*** (p. xxiii)，详细了解 CC-SG 如何报告电源控制操作是成功还是失败了。

电源状态消息

在开始执行电源控制操作时，打开 Power Status Messages（电源状态消息）窗口。应该让此窗口保持打开状态，直到所有电源控制操作完成为止。

可以调节 Power Status Messages（电源状态消息）窗口的大小，使其最小化或最大化。可以选择窗口显示的文本，进行复制和粘贴操作。

在收到有关电源控制操作状态的消息时，Power Status Messages（电源状态消息）窗口更新这些消息。

在下列情况下，Power Status Messages（电源状态消息）窗口显示一条新消息：

- 发送电源控制操作请求
- 电源控制操作失败
- 电源控制操作成功完成
- 请求的所有电源控制操作成功完成

▶ **在关闭 Power Status Messages（电源状态消息）窗口时如何获得最新状态：**

- 当电源控制操作失败时，显示一条提示消息，说明操作失败了。
- 当整个操作成功完成时，浏览器窗口底部的状态栏显示一条提示消息。
- 只有在操作失败时，才显示提示消息。对于成功操作，不显示提示消息。

在有限的时间内升级多台设备

可以针对一个设备组里相同类型的多台设备（例如 KX 或 SX）安排一个升级任务。一旦开始升级任务，Reports（报告）> Scheduled Reports（预定报告）菜单就显示 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）选项卡上指定一个选项，可以通过电子邮件发送此报告。

参看《Raritan 用户指南》了解每种设备的预计升级时间。

▶ **安排设备固件升级时间：**

1. 选择 Administration（管理）> Tasks（任务）。
2. 单击 New（新建）。

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）标识该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。如果要升级多个类型的设备，必须针对每种类型安排一个升级任务。
   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 and Latest Upgrade Start Date/Time（限制升级窗口和最晚升级开始日期/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）启用 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。将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各台设备，单击 Add（添加）按钮将它移动到 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，用箭头按钮将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（再试）选项卡。
   b. Retry Count（再试次数）：输入 CC-SG 针对失败升级再试的次数。
   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 秒、60 秒和 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. 160)。

给所有用户指定默认节点定制视图

如果你有 CC 设置和控制权，可以给所有用户指定默认定制视图。

▶ **给所有用户指定默认节点定制视图：**

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）。
3. 单击 Name（名称）下拉箭头，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定制视图排序的 Nodes（节点）选项卡。用户可以更改定制视图。

参看*定制视图* (参看 "设备和节点自定义视图" p. 122)，详细了解定制视图的类型，以及如何创建定制视图。

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

前期准备

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“位置”类别可能有“纽约市”、“费城”或“数据中心 1”等元素。在将设备和端口添加到 CC-SG 时，使此信息与它们关联在一起。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“操作系统类型”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。

CommandCenter NOC (CC NOC) — 网络监视设备，用于审计和监视 CC-SG 管理的服务器、设备和 Raritan 设备的状态。

设备组 — 一个用户可以访问的定义的设备组。在创建策略时，用设备组控制对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. 180)。

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 — CC-SG 可以管理的 HP Integrated Lights Out/Remote Insight Lights Out 服务器。iLO/RILOE 设备的目标可以直接通电/断电和重新通电。CC-SG 不能发现 iLO/RILOE 设备，必须用人工方法作为节点添加这些设备。

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) 或 Multi-Platform Client (MPC) 等应用程序排除网络里 KVM 或串行被管节点发生的故障。

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定义的节点组。在创建策略时，用节点组控制对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，标识从该设备到节点的路径。

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 等客户机，给 CC-SG 提供命令行界面。SSH 只支持设备管理和 CC-SG 管理所用的部分 CC-SG 命令。

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”。

2 访问 CC-SG

可以采用几种方式访问 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。
- 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. 233)。

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: https://*IP address*/admin，例如 ***https://10.0.3.30/admin*** (https://10.0.3.30/admin)。

   如果显示 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. 输入 Username（用户名）和 Password（密码），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。

如果显示 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. 189)。

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。使用胖客户机代替浏览器的优点是，客户机的速度和效率要胜过浏览器。 运行胖客户机要求的最低 Java 版本是 1.5.0.10。

安装胖客户机

▶ 在 CC-SG 上下载胖客户机：

1. 启动网络浏览器，输入此 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。

5. 在 CC-SG 上检查设置：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。
6. 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。
7. 显示 Login（登录）屏幕。
8. 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。
9. 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 1.5.0.10。 还支持 Java v1.6.0。

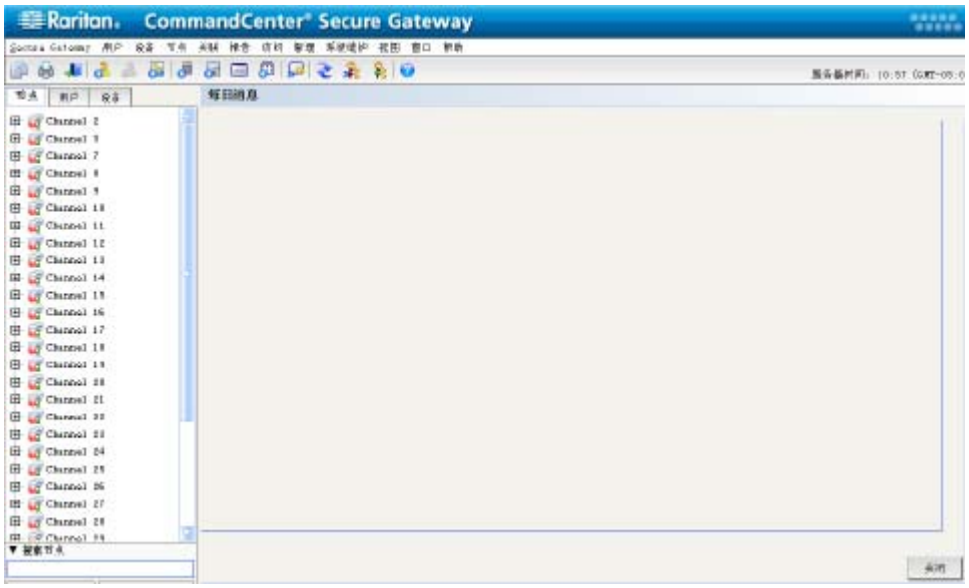
在安装胖客户机之后，可以在客户计算机上采用两种方法访问它。

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。



- 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，选择 Connect（连接）即可连接该接口。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，选择 Connect(连接)即可连接该端口。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。
- Quick Commands（快速命令）工具栏：此工具栏提供的快捷按钮便于你执行常用命令。
- Operation and Configuration（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）上安排任务时，要使用此时间。参看*任务管理器* (p. 212)。此时间与客户 PC 所用的时间可能不同。

3 起步

在首次登录 CC-SG 之后，应该确认 IP 地址，设置 CC-SG 服务器时间，检查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。

一旦完成首次配置，继续进行“指导设置”。参看*用指导设置配置 CC-SG* (p. 13)。

在本章内

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. 180)。**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。

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 Task Manager（任务管理器）上安排任务时，要使用 Time/Date configuration（时间/日期配置）。参看*任务管理器* (p. 212)。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（月份），用上下箭头选择 Year（年份），然后单击日历表上的 Day（日）。
- Time（时间）— 用上下箭头设定 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，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 NTP 配置 CC-SG 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，将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：

如果应用程序版本不是最新版，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. 162)。

1. 将应用程序文件保存到客户 PC。
2. 单击 Application name（应用程序名称）下拉箭头，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，必须先添加该应用程序。参看 *添加应用程序* (p. 177)。
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。

4 用指导设置配置 CC-SG

一旦完成网络配置，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，随时可以编辑个别配置。

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. 13)。
- 设备设置 — 发现网络设备，将它们添加到 CC-SG。配置设备端口。参看*设备设置* (p. 14)。
- 创建组 — 将 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*创建组* (p. 16)。
- 用户管理 — 将用户和用户组添加到 CC-SG，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. 18)。

参看*命名常规* (p. 310)，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 系列以及 IP-Reach 设备（串行和 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“位置”。
3. 在 Applicable for（适用于）字段里说明你希望该类别可用于设备和/或节点。单击 Applicable for（适用于）下拉菜单，在列表上选择一个值。
4. 在 Elements（元素）表上输入该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，在表上添加更多行。
   - 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，直到将该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。**任选**
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，将它们添加到 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 Associations（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。

▶ **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 Mask（掩码）字段里输入要搜索的设备的子网掩码。
3. 在 Device types（设备类型）列表上选择要搜索哪个指定范围内的设备的类型。按住 Ctrl 键单击设备类型，可以选择多个设备类型。
4. 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。
5. 单击 Discover（发现）按钮。
6. 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。
7. 在发现设备表上选择要添加到 CC-SG 的设备，然后单击 Add（添加）按钮。打开 Add Device（添加设备）面板。对于要添加的不同设备类型，Add Device（添加设备）面板略有不同。
8. 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。
9. 确定 Device IP or Hostname（设备 IP 或主机名）字段是否显示你在准备将设备添加到 CC-SG 时指定的 IP 地址，必要时在此字段里输入正确地址。
10. 根据设备类型自动填充 TCP Port Number（TCP 端口号）字段。
11. 在 Username（用户名）和 Password（密码）字段里输入你在准备将设备添加到 CC-SG 时创建的用户名和密码。
12. 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。
13. 如果要添加 Dominion SX 设备，并且允许对该设备进行本地访问，选择 Allow Direct Device Access（允许直接设备访问）复选框。如果不允许对该设备进行本地访问，取消 Local access: Allowed（本地访问：允许）复选框。
14. 如果要人工添加配电盘设备，单击 Number of ports（端口数）下拉箭头，选择配电盘的出口数。
15. 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的间隔，而在 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。
16. 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 将设备的所有端口添加到 CC-SG，给每个端口创建一个节点。
17. 在面板下半部的 Device Associations（设备关联）部分，单击与你要给该设备指定的每个类别相对应的 Element（元素）栏上的下拉箭头，在列表上选择要与该设备关联的元素。

18. 如果要将该元素应用于该设备和与之相连的节点，选择 Apply to Nodes（应用于节点）复选框。
19. 如果要添加另一台设备，单击 Apply（应用）按钮保存此设备，重复上述步骤。**可选。**
20. 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。
21. 单击 Continue（继续）按钮开始下一个任务，即创建组。根据下一节所述的步骤操作。

创建组

指导设置的第三个任务是创建组。创建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 Device Setup（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（组名称）字段里输入要创建的设备组的名称。
3. 可以采用两种方法将设备添加到组：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组里。
   - **选择设备**
   a. 单击 Device Group: New（设备组：新建）面板上的 Select Devices（选择设备）选项卡。
   b. 在 Available（可用）列表上选择要添加到组的设备，然后单击 Add（添加）按钮，将设备移到 Selected（选择）列表上。Selected（选择）列表上的设备将被添加到组。
   c. 如要删除组里的一个设备，在 Selected（选择）列表上选择设备名称，然后单击 Remove（删除）按钮。

d. 可以搜索 Available（可用）列表或 Selected（选择）列表上的设备。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组件。

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

5. 如要添加另一个设备组，单击 Apply（应用）按钮保存此组，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（组名称）字段里输入要创建的节点组的名称。

8. 可以采用两种方法将节点添加到组：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组里的节点，然后单击 Add（添加）按钮将它移到 Selected（选择）列表上。Selected（选择）列表上的节点将被添加到组里。

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

d. 可以搜索 Available（可用）列表或 Selected（选择）列表上的节点。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组件。参看 *访问控制策略* (p. 117)。

9. 如要给此节点组创建一个策略，选择 Create Full Access Policy for Group（给组创建全访问策略），允许用户随时凭借控制权访问组里的所有节点。
10. 如要添加另一个节点组，单击 Apply（应用）按钮保存此组，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，将他们添加到用户组。

添加用户组和用户

在 Create Groups（创建组）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. 单击 Privileges（权限）选项卡，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。
4. 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。选择你要给组指定的访问类型对应的复选框。
5. 单击 Policies（策略）选项卡。
6. 在 All Policies（所有策略）列表上选择要给用户组指定的策略，单击 Add（添加）按钮将它移到 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。
7. 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。
8. 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。
9. 如要添加另一个用户组，单击 Apply（应用）按钮保存此组，重复上述步骤。**可选。**
10. 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。
11. 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。
12. 如果希望此用户能登录 CC-SG，选择 Login Enabled（允许登录）复选框。

13. 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），New Password（新密码）字段和 Retype New Password（再次输入新密码）被禁用。
14. 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。
15. 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。
16. 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。
17. 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。
18. 在 Email address（电子邮件地址）字段里输入用户的电子邮件地址。
19. 单击 User Group（用户组）下拉箭头，在列表上选择要给用户指定哪个用户组。
20. 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。
21. 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。**

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 CC-SG 管理的设备。每个关联包括一个类别（最高组织的组）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“位置”类别可能有“美国”和“亚太”等元素。再比如“操作系统类型”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。因此，在将 Raritan 设备添加到 CC-SG 之前，必须定义类别和元素。

类别就是相似元素所属的组。例如为了按位置将 Raritan 设备分成组，可以定义一个“位置”类别，它包含“纽约”、“费城”和“新奥尔良”等元素。

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/纽约”这一类别/元素对创建一个策略，控制用户对纽约服务器的访问。

下面列举其他典型的类别和元素关联配置：

类别	元素
位置	纽约、费城、新奥尔良
操作系统类型	Unix、Windows、Linux

类别	元素
部门	销售、IT、工程

关联配置应该很简单，以便实现服务器/节点组织目标和用户访问目标。一个节点只能指定给一个类别的一个元素。例如，不能给一台目标服务器同时指定“操作系统类型”类别的 Windows 和 Unix 元素。

如果服务器相似，必须随机组织管理，下面的组织管理方法很有用：

类别	元素
usergroup1	usergroup1node
usergroup2	usergroup2node
usergroup3	usergroup3node

在将设备和节点添加到 CC-SG 时，将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，随时可以编辑个别配置。参看*用指导设置配置 **CC-SG*** (p. 13)。
- 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*关联管理器* (p. 22)。

关联管理器

可以用关联管理器添加、编辑或删除类别和元素。

注意：CC-SG 默认将默认类别名称 System Type（系统类型）和 US States and territories（美国各州和领地）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. 310)，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。

编辑类别

注意字符串值不能更改为整数值，反之亦然。如果必须进行此类更改，要删除类别，再添加新类别。

▶ 编辑类别：

1. 选择 Associations（关联）> Association（关联）。
2. 单击 Category Name（类别名称）下拉箭头，选择要编辑的类别。
3. 单击屏幕上 Category（类别）面板上的 Edit（编辑）按钮，编辑该类别。打开 Edit Category（编辑类别）窗口。
4. 在 Category Name（类别名称）字段里输入新类别的名称。
5. 单击 Applicable For（适用于）下拉箭头，将此类别更改为 Device（设备）、Node（节点）或 Device and Node（设备和节点）。
6. 单击 OK（确定）按钮保存更改。Category Name（类别名称）字段显示更新后的类别名称。

删除类别

在删除一个类别时，将删除该类别中已创建的所有元素。一旦屏幕刷新，或者用户退出 CC-SG 后再登录，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，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，删除该类别。打开 Delete Category（删除类别）窗口。
4. 单击 Yes（是）按钮删除该类别。

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，选择要添加新元素的类别。
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. 310)，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。

编辑元素

▶ **编辑元素：**

1. 选择 Associations（关联）> Association（关联）。
2. 单击 Category Name（类别名称）下拉箭头，选择要编辑哪个类别的元素。
3. 双击 Elements（元素）列表上要编辑的元素。
4. 给 Elements（元素）列表上的元素输入新值。元素区分大小写。
5. 单击 OK（确定）按钮更新元素，或者单击 Close（关闭）按钮关闭窗口。

删除元素

在删除一个元素时，删除该元素的所有关联，关联字段变成空白。

▶ **删除元素：**

1. 选择 Associations（关联）> Association（关联）。
2. 单击 Category Name（类别名称）下拉箭头，选择要删除哪个类别的元素。
3. 在 Elements（元素）列表上选择要删除的元素，然后单击 Remove Row（删除行）图标。
4. 单击 OK（确定）按钮保存更改。

6 设备、设备组和端口

如要将与其他 Raritan 设备相连的 Raritan 配电盘设备添加到 CC-SG，参看*被管配电盘* (p. 61)。

---

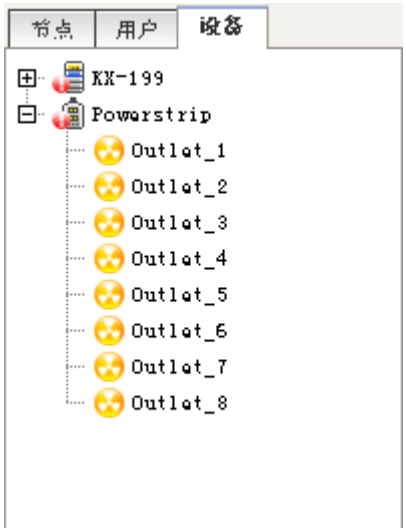
*注意：如要配置 iLO/RILOE 设备、IPMI 设备、Dell DRAC 设备、IBM RSA 设备或其他非 Raritan 设备，使用 Add Node（添加节点）菜单，作为接口添加这些设备。参看*节点、节点组和接口 *(p. 68)*。

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一个 + 号。单击 + 号或 - 号展开或折叠端口列表。

设备和端口图标

为了便于识别，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
	串行端口不可用
	幻影端口（参看 Raritan《**Paragon II 用户指南**》了解幻影模式详情。）
	设备暂停

图标	含义
	设备不可用
	配电盘
	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。

▶ 排序 Devices（设备）选项卡上的端口：

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，除非你将这些刀片服务器端口恢复到正常 KX2 端口。参看***将刀片服务器端口恢复到正常 KX2 端口** *(p. 45)*。

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. 36)。

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. 21)。

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. 35)。

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。该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 Device, Port, and Node Management（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. 35)。

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. 41)。

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，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。

在设备选项卡中右键单击选项

在“设备”选项卡内可右键单击设备或端口，即可显示所选设备或端口的可用命令菜单。

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. 114)。

▶ **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 键。
- 可以在搜索字符串里使用通配符。参看*搜索通配符* (p. 29)。

搜索通配符

通配符	说明
?	表示任何字符。
[-]	表示一个范围内的字符。
*	表示零个或多个字符。

通配符示例

示例	说明
KX?	查找 KX1 和 KXZ，但不查找 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，可以将它们添加到 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。指定一个要应用于该范围的掩码。如果不指定掩码，将发送广播地址 255.255.255.255，广播到所有本地网络。如要发现多个子网上的设备，必须指定掩码。
3. 如果搜索 CC-SG 所在子网上的设备，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 键单击设备类型，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。
7. 如要将一个或多个发现设备添加到 CC-SG，在列表上选择设备，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. 31)。
   - 如要了解配电盘，参看*添加配电盘设备* (p. 33)。
   - 如要了解 IP 网络上的 Dominion PX 配电盘，参看*添加 **Dominion PX** 设备* (p. 33)。
9. 单击 Apply（应用）按钮添加设备，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

必须先将设备添加到 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. 30)。

如要将与其他 Raritan 设备相连的 Raritan 配电盘设备添加到 CC-SG，参看*被管配电盘* (p. 61)。

▶ 将设备添加到 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，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. 31)。
- 如要了解如何添加配电盘设备，参看*添加配电盘设备* (p. 33)。
- 如要了解如何添加 Dominion PX 设备，参看*添加 **Dominion PX** 设备* (p. 33)。

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，但 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. 310)，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* ("术语/缩略语" p. 2)，了解主机名规则。
3. 在 TCP Port Number（TCP 端口号）字段里输入与设备通信所用的 TCP 通信端口的编号。最长 5 个数字字符。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. 在添加 Dominion SX 设备时，Allow Direct Device Access（允许直接设备访问）复选框便于你允许或拒绝通过本地端口访问设备。在此设备受 CC-SG 管理时，如果允许用户直接访问此设备，选择此复选框。
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，自动将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，给该节点创建一个带外接口，刀片服务器机箱节点除外。
   - 可能给与 KX2 端口相连的刀片服务器机箱设备创建一个节点，也可能不创建，取决于在 KX2 上输入了刀片服务器机箱 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接口。
   - 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，更好地描述和组织此设备和与之相连的节点。参看*关联、类别和元素* (p. 21)。
11. 对于列出的每个类别，单击 Element（元素）下拉菜单，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. 21)。
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，将设备添加到 CC-SG。可以在将设备添加到 CC-SG 之后升级设备固件。参看*升级设备* (p. 46)。

添加配电盘设备

如果配电盘物理连接不同的 Raritan 设备，给 CC-SG 添加配电盘设备的过程有所不同。参看*被管配电盘* (p. 61)。

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. 33)。

添加 Dominion PX 设备

Dominion PX 设备是仅与 IP 网络相连的配电盘设备。Dominion PX 设备不受另一台 Raritan 设备管理。如果要添加受另一台 Raritan 设备管理的配电盘，要采用不同的添加步骤。参看*被管配电盘* (p. 61)。

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. 310)，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* ("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. 34)*。

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，自动将此 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. 21)。

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。

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。

▶ **编辑设备：**

1. 单击 Devices（设备）选项卡，选择要编辑的设备。
2. 在 Device Profile（设备配置文件）屏幕上根据需要更改参数。
3. 单击 OK（确定）按钮保存更改。

编辑配电盘设备或 Dominion PX 设备

可以编辑配电盘设备或 Dominion PX 设备：重新命名它、修改其属性，查看出口配置状态。

▶ **编辑配电盘设备：**

1. 单击 Devices（设备）选项卡，选择要编辑的配电盘设备。
2. 在此屏幕上的适当字段里输入新设备属性。如有必要，编辑与此设备关联的类别和元素。
3. 单击 Outlet（出口）选项卡，查看此配电盘的所有出口。
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，选择该出口，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。该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 Device, Port, and Node Management（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）按钮确认清除。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. 输入位置信息。
   - 部门：最多 64 个字符。
   - 地点：最多 64 个字符。
   - 位置：最多 128 个字符。
4. 输入联系人信息。
   - 主联系人姓名和第二联系人姓名：最多 64 个字符。

- 电话号码和手机号码：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：在删除设备时，将删除给该设备配置的所有端口。从节点上删除与这些端口关联的所有接口。如果这些节点没有其他接口，这些节点也从 CC-SG 上删除掉。

▶ 删除设备：

1. 单击 Devices（设备）选项卡，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）按钮删除该设备。在删除设备之后，显示一条消息。

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）屏幕将设备的个别端口或一组端口添加到 CC-SG。

一旦配置端口，就在 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. 37)。

配置串行端口

▶ 配置串行端口：

1. 单击 Devices（设备）选项卡，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）。

   单击一个栏标题，按该属性升序顺序排序端口。再次单击该标题，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，以端口所连目标的名称开头来命名端口。参看*命名常规* (p. 310)，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，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，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）。
   - 单击一个栏标题，按该属性升序顺序排序端口。再次单击该标题，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，以端口所连目标的名称开头来命名端口。参看*命名常规* (p. 310)，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，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。如果你编辑节点名称，新名称不得超过最大字符数。参看*命名常规* (p. 310)。

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。你可以进行的更改取决于端口类型和设备类型。

▶ 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，选择要编辑的端口。
2. 如有必要，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，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，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，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

在删除端口时，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，将从该节点上删除该端口提供的关联带外 KVM 接口或串行接口。如果该节点没有其他接口，该节点也从 CC-SG 中删除掉。

▶ 删除端口：

1. 单击 Devices（设备）选项卡，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 访问该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. 40)。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* (参看 "配置刀片服务器机箱设备上的插槽" p. 41)。

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，一个机箱通过一个 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. 40)。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 上配置 KX2 设备。参看***添加 KVM 设备或串行设备*** (p. 31)。
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. 41)*。

▶ **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 上配置 KX2 设备。参看***添加 KVM 设备或串行设备*** (p. 31)。

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. 41)**。*

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，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，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 设备上给相应刀片服务器或端口启用 Installed（已安装）状态，CC-SG 始终将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，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，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），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。如有必要，编辑与此设备关联的 Categories（类别）和 Elements（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

可以将与 KX2 设备相连的刀片服务器机箱设备从 CC-SG 上删除掉。在将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，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。

将刀片服务器机箱设备移到不同的端口

在将刀片服务器机箱设备从一台 KX2 设备或一个端口物理移到另一台 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。

▶ 将刀片服务器机箱设备移到不同的 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. 44)。
2. 断开刀片服务器机箱，将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. 40)。

将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）选项卡上将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。

▶ **将刀片服务器恢复到正常 KX2 端口：**

1. 在 Devices（设备）选项卡选择要将哪台 KX2 设备的刀片服务器重新配置为正常 KVM 端口。
2. 将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 上将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. 37)。

设备关联、位置和联系人批量复制

批量复制命令允许你将一台设备上的类别、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，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）列表上选择你要将 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，将设备添加到 Selected Devices（选择的设备）列表上。
5. 选择该设备，单击 < 按钮将它从 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。

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，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 可以保存的最大备份文件数是每台设备 3 个备份文件。如果需要更多备份文件，可以将一个备份文件保存到网络上，然后在 CC-SG 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***将所有配置数据恢复到 KX2、KSX2 或 KX2-101 设备上*** (p. 50)。

每一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，了解详细信息。

注意：在备份 SX 3.0.1 设备时，不备份相连的配电盘的配置。如果用备份文件恢复 SX 3.0.1 设备，必须重新配置配电盘。

▶ **备份设备配置：**

1. 单击 Devices（设备）选项卡，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（备份配置）。
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。**任选。**
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 设备允许你选择将备份配置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），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）选项将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（全部）：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（用户和用户组设置）。

恢复设备配置（KX、KSX、KX101、SX、IP-Reach）

可以将全备份配置恢复到 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，选择要将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）列表上选择要将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。

将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）恢复选项允许你将备份文件里的所有配置数据（除网络设置外）恢复到 KX2 或 KX2-101 设备上。可以用 Protected（保护）选项将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）。

▶ **将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，选择要将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）列表上选择要将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之后，显示一条消息。

仅将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/或用户和用户组设置。

▶ **仅将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，选择要将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）列表上选择要将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组件：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。

将所有配置数据恢复到 KX2、KSX2 或 KX2-101 设备上

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

▶ 将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，选择要将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）列表上选择要将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

可以将 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空间，可以删除设备备份文件。也可以将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，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. 找到要保存该文件的位置。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，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）按钮确认删除。

▶ **将设备备份文件上载到 CC-SG 上：**

1. 单击 Devices（设备）选项卡，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，页面显示该文件。

复制设备配置

可以将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，例如只能将 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，所以在此过程中全部复制 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，在 Devices（设备）树上选择要将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，在列表上选择一个设备组。Available（可用）栏显示选择的设备组里的所有设备。

5. 在 Available（可用）栏上突出显示你要将此配置复制到哪些设备上，然后单击右箭头，将它移到 Selected（选择）栏上。单击左箭头，将选择的设备从 Selected（选择）栏上删除掉。
6. 单击 OK（确定）按钮，将配置复制到 Selected（选择）栏上的设备上。
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，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。

▶ **对设备执行 ping 命令：**

1. 单击 Devices（设备）选项卡，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）。显示 Ping Device（对设备执行 ping 命令）屏幕，显示 ping 命令执行结果。

让 CC-SG 暂停设备管理

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配置数据。

▶ **让 CC-SG 暂时停止管理设备：**

1. 单击 Devices（设备）选项卡，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 的控制之下。

▶ 让 CC-SG 恢复管理被暂停的设备：

1. 单击 Devices（设备）选项卡，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。

设备电源管理器

用设备电源管理器查看配电盘设备的状态（包括电压、电流和温度），管理配电盘设备的所有电源出口。设备电源管理器提供以配电盘为中心的出口视图。

在使用设备电源管理器之前，必须在配电盘和 Dominion SX 或 Dominion KSX 设备之间建立物理连接。在添加配电盘设备时，必须定义哪台 Raritan 设备要提供连接。这将使它与 Dominion SX 串行端口或提供配电盘管理的 Dominion KSX 专用电源接口关联在一起。

▶ 查看设备电源管理器：

1. 在 Devices（设备）选项卡上选择配电盘设备。
2. 选择 Devices（设备）> Device Power Manager（设备电源管理器）。
3. 出口在 Outlets Status（出口状态）面板上列出。可能要翻页，才能看到所有出口。
   - 单击每个出口对应的 On（通电）或 Off（断电）单选按钮，接通或断开出口。
   - 单击 Recycle（重新通电）按钮，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，可以用它访问该设备的管理员界面。

▶ 启动设备管理页面：

1. 单击 Devices（设备）选项卡，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）。显示所选设备的管理员界面。

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，允许完成固件升级与设备配置备份和恢复操作。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，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 用户可以将自己的 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。

在将 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）树显示该设备。

▶ **在 CC-SG 上访问 Paragon II System Controller：**

1. 单击 Devices（设备）选项卡，选择 Paragon II System Controller。
2. 用右键单击 Paragon II System Controller，然后单击 Launch Admin（启动管理），用新浏览器窗口启动 Paragon II System Controller 应用程序。然后可以配置 PII UMT 设备。

IP-Reach 和 UST-IP 管理

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

在将 Paragon System 设备添加到 CC-SG 之后，Devices（设备）树显示该设备。

▶ **访问远程用户站管理：**

1. 单击 Devices（设备）选项卡，选择 Paragon II System Controller。
2. 用右键单击 Paragon II System Controller，选择 Remote User Station Admin（远程用户站管理）。显示 Remote User Station Admin（远程用户站管理）屏幕，列出连接的所有 IP-Reach 和 UST-IP 设备。
3. 单击你要操作的设备所在行上的 Launch Admin（启动管理），激活 Raritan Remote Console，用新窗口启动蓝色设备配置屏幕。

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，可以给该组创建全访问策略。参看*访问控制策略* (p. 117)。

设备组概述

设备组用于将设备分成组。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. 118)。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. 21)，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该组的详细信息。
  - 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，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. 105)。
- 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（新建组）图标。打开 Device Group: New（设备组：新建）面板。
3. 在 Group Name（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. 310)，详细了解 CC-SG 的名称长度规则。
4. 可以采用两种方法将设备添加到组：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组里的设备，然后单击 Add（添加）按钮将它移到 Selected（选择）列表上。Selected（选择）列表上的设备将被添加到组里。
   - 如要删除组里的一台设备，在 Selected（选择）列表上选择设备名称，单击 Remove（删除）按钮。
   - 可以搜索 Available（可用）列表或 Selected（选择）列表上的设备。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（给组创建全访问策略）复选框，给此设备组创建一个策略，允许用户随时凭借控制权访问组里的所有设备。
4. 如要添加另一个设备组，单击 Apply（应用）按钮保存此组，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组件。
   - 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。这里只显示与所选类别关联的元素（例如：如果对 Department 类别求值，这里不显示 Location 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，用逻辑运算符描述每个规则之间的关系。

- &— “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，选择该行，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（设备组结果中的设备）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（给组创建全访问策略）复选框，给此设备组创建一个策略，允许用户随时凭借控制权访问组里的所有设备。

9. 如要添加另一个设备组，单击 Apply（应用）按钮保存此组，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，它们被自动添加到组里。

如果只想人工创建由特定节点构成的组，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组里。在将新节点或设备添加到 CC-SG 之后，必须人工将它们添加到组里。

这两种方法不能混用。

一旦用一种方法创建一个组，必须用同一种方法编辑该组。如果换用另一种方法，将覆盖当前组设置。

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。选择要编辑哪个设备组的名称。显示 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。**任选。**
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. 56)。
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。显示 Device Group Details（设备组详细信息）面板。
3. 选择 Groups（组）> Delete（删除）。

4. 显示 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。

7 被管配电盘

在使用配电盘时，在 CC-SG 上可以采用两种方法配置电源控制。

1. 支持的所有 Raritan 配电盘可以连接另一台 Raritan 设备，可以作为配电盘设备添加到 CC-SG。Raritan 配电盘包括 Dominion PX 和 RPC 配电盘。参看“兼容性指标”部分，了解支持的版本。如要在 CC-SG 上配置这种被管配电盘，必须了解配电盘物理连接哪种 Raritan 设备。参看*在 **CC-SG** 上配置被另一台设备管理的配电盘* (p. 62)。
2. Dominion PX 配电盘可以直接连接 IP 网络，可以作为 PX 设备添加到 CC-SG。如果 PX 配电盘直接连接 IP 网络，它们不必连接另一台 Raritan 设备。

无论采用哪种连接方法，你都必须将被管配电盘接口添加到节点上，在出口及其供电节点之间建立电源关联。参看*被管配电盘连接接口* (p. 92)。

▶ Dominion PX 特殊说明

无论你用哪种方法配置 PX，都应该采用一种方法配置所有电源关联，即要么作为被管设备的配电盘，要么作为 PX 设备，但不能同时作为二者。

此外，可以将 PX 连接到管理设备上配置电源关联，也可以将同一台 PX 设备连接到 IP 网络上，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配电盘

可以在 CC-SG 上将被管配电盘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)

必须了解被管配电盘物理连接哪种 Raritan 设备。

*注意：也可以将 Dominion PX 配电盘连接到 IP 网络，但不连接其他任何 Raritan 设备。参看*被管配电盘 *(p. 61)，详细了解如何给这些配电盘配置电源控制。*

▶ 在 CC-SG 上配置被管配电盘：

1. 在设备、配电盘和配电盘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》，详细了解配电盘、设备和节点之间的物理连接。
2. 将管理设备添加到 CC-SG。对于不同的 Raritan 设备，操作步骤有所不同。参看与配电盘相连的设备对应的章节：
   - ***配置 KX、KX2、KX2-101、KSX2 和 P2SC 连接的配电盘*** (p. 63)
   - ***配置 SX 3.0 和 KSX 连接的配电盘*** (p. 64)
   - ***配置 SX 3.1 连接的配电盘*** (p. 65)
3. 配置插座。参看***配置配电盘的出口*** (p. 67)。
4. 使每个出口与其供电节点关联。参看***被管配电盘连接接口*** (p. 92)。

配置 KX、KX2、KX2-101、KSX2 和 P2SC 连接的配电盘

CC-SG 自动检测 KX、KX2、KX2-101、KSX2 和 P2SC 设备连接的配电盘。可以在 CC-SG 上执行下列任务，配置和管理这些设备连接的配电盘。

- *添加与 KX、KX2、KX2-101、KSX2 或 P2SC 设备相连的配电盘设备* (p. 63)
- *将 KX、KX2、KX2-101、KSX2 或 P2SC 的配电盘移动到不同的端口* (p. 63)
- *删除与 KX、KX2、KX2-101、KSX2 或 P2SC 设备相连的配电盘* (p. 63)

添加与 KX、KX2、KX2-101、KSX2 或 P2SC 设备相连的配电盘设备

在将与配电盘相连的 KX、KX2、KX2-101、KSX2 或 P2SC 设备添加到 CC-SG 时，自动添加配电盘。在 Devices（设备）选项卡上，在配电盘相连的设备下面显示配电盘。

接下来的步骤：

1. 配置插座。参看*配置配电盘的出口* (p. 67)。
2. 使每个出口与其供电节点关联。参看*被管配电盘连接接口* (p. 92)。

将 KX、KX2、KX2-101、KSX2 或 P2SC 的配电盘移动到不同的端口

在将配电盘从一台 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 设备或另一个端口上时，CC-SG 自动检测配电盘，自动更新设备关联。你不必另外将配电盘添加到 CC-SG。

注意：在从 P2SC 端口上实际删除并不连接其他端口的配电盘时，CC-SG 不从旧端口上删除配电盘。你必须对配电盘相连的 UMT 执行部分或全部数据库复位，才能在 Devices（设备）选项卡上删除配电盘。参看《Raritan P2SC 用户指南》。

删除与 KX、KX2、KX2-101、KSX2 或 P2SC 设备相连的配电盘

不能在 CC-SG 上删除与 KX、KX2、KX2-101、KSX2 或 P2SC 设备相连的配电盘。必须物理断开配电盘和设备，才能在 CC-SG 上删除配电盘。在物理断开配电盘和设备时，Devices（设备）选项卡不再显示配电盘和配置的所有出口。

配置 SX 3.0 和 KSX 连接的配电盘

可以在 CC-SG 上执行下列任务，配置和管理 SX 3.0 或 KSX 设备连接的配电盘。

注意：配电盘必须物理连接 KSX 设备的 Power Port（电源端口）。

- ***添加与 SX 3.0 或 KSX 设备相连的配电盘*** (p. 64)
- ***删除与 SX 3.0 或 KSX 设备相连的配电盘*** (p. 65)
- ***更改配电盘的设备或端口关联 (SX 3.0, KSX)*** (p. 65)

添加与 SX 3.0 或 KSX 设备相连的配电盘

1. 将 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. 31)。
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，选择 Select PowerStrip（选择配电盘）。
4. 在 Power Strip Name（配电盘名称）字段里输入配电盘的名称。让光标停留在该字段上，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，选择此配电盘的出口数。
6. 单击 Managing Device（管理设备）下拉菜单，选择此配电盘相连的 SX 3.0 或 KSX 设备。
7. 单击 Managing Port（管理端口）下拉菜单，选择此配电盘相连的 SX 3.0 或 KSX 设备的端口。
8. 在 Description（说明）字段里输入此配电盘的简短说明。**任选。**
9. 如果要自动将此配电盘的每个出口添加到 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***配置配电盘的出口*** (p. 67)。**任选。**
10. 对于列出的每个类别，单击 Element（元素）下拉菜单，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。参看***关联、类别和元素*** (p. 21)。**任选。**
11. 在配置此配电盘之后，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）按钮添加此配电盘，不继续打开 Add Device（添加设备）屏幕。

接下来的步骤：

1. 配置插座。参看*配置配电盘的出口* (p. 67)。
2. 使每个出口与其供电节点关联。参看*被管配电盘连接接口* (p. 92)。

删除与 SX 3.0 或 KSX 设备相连的配电盘

即使配电盘仍然物理连接 SX 3.0、KSX 或 P2SC 设备，仍然可以删除此配电盘。如果物理断开配电盘及其关联的 SX 3.0、KSX 或 P2SC 设备，Devices（设备）选项卡上的设备下面仍然显示该配电盘。如要不显示配电盘，必须删除配电盘。

1. 在 Devices（设备）选项卡上选择要删除的配电盘。
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）按钮删除配电盘。在删除配电盘之后，显示一条消息。Devices（设备）选项卡不再显示配电盘图标。

更改配电盘的设备或端口关联 (SX 3.0, KSX)

如果将配电盘从一台 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（配电盘配置文件）里的关联。

1. 在 Devices（设备）选项卡上选择要移动的配电盘。
2. 单击 Managing Device（管理设备）下拉菜单，选择此配电盘相连的 SX 3.0 或 KSX 设备。
3. 单击 Managing Port（管理端口）下拉菜单，选择此配电盘相连的 SX 3.0 或 KSX 设备的端口。
4. 单击 OK（确定）按钮。

配置 SX 3.1 连接的配电盘

可以在 CC-SG 上执行下列任务，配置和管理 SX 3.1 设备连接的配电盘。

- *添加 SX 3.1 设备连接的配电盘* (p. 66)
- *将 SX 3.1 的配电盘移动到不同的端口* (p. 66)
- *删除 SX 3.1 设备连接的配电盘* (p. 66)

添加 SX 3.1 设备连接的配电盘

添加 SX 3.1 设备连接的配电盘的步骤取决于 SX 3.1 设备是否已经被添加到 CC-SG。

如果配电盘连接 SX 3.1 设备，该设备尚未被添加到 CC-SG：

1. 将 SX 3.1 设备添加到 CC-SG。参看*添加 KVM 设备或串行设备* (p. 31)。
2. CC-SG 检测并自动添加配电盘。在 Devices（设备）选项卡上，在配电盘相连的 SX 3.1 设备下面显示配电盘。

如果 SX 3.1 设备已经被添加到 CC-SG，配电盘稍后被连接到该设备：

1. 将 SX 3.1 设备添加到 CC-SG。参看*添加 KVM 设备或串行设备* (p. 31)。
2. 配置 SX 3.1 设备的端口。参看*配置端口* (p. 36)。
3. 在 Devices（设备）选项卡上选择配电盘连接的 SX 3.1 设备。
4. 单击设备图标旁边的 + 号展开端口列表。
5. 用右键单击配电盘连接的 SX 3.1 端口，在弹出菜单上选择 Add Powerstrip（添加配电盘）。
6. 输入配电盘的出口数，然后单击 OK（确定）按钮。

接下来的步骤：

1. 配置插座。参看*配置配电盘的出口* (p. 67)。
2. 使每个出口与其供电节点关联。参看*被管配电盘连接接口* (p. 92)。

将 SX 3.1 的配电盘移动到不同的端口

在将配电盘从一台 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 端口上删除该配电盘，将它添加到新 SX 3.1 端口。

删除 SX 3.1 设备连接的配电盘

即使配电盘仍然物理连接 SX 3.1 设备，仍然可以删除此配电盘。如果物理断开配电盘及其关联的 SX 3.1 设备，Devices（设备）选项卡上的设备下面仍然显示该配电盘。如要不显示配电盘，必须删除配电盘。

▶ **删除 SX 3.1 设备连接的配电盘：**

1. 在 Devices（设备）选项卡上选择要删除的配电盘。

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）按钮删除配电盘。在删除配电盘之后，显示一条消息。Devices（设备）选项卡不再显示配电盘图标。

配置配电盘的出口

在使配电盘出口与节点关联之前，必须配置出口：将被管配电盘接口添加到节点。参看*被管配电盘连接接口* (p. 92)。

▶ 在配电盘配置文件上配置出口：

1. 在 Devices（设备）选项卡上，单击与配电盘相连的设备旁边的 + 号。
2. 选择要配置哪个配电盘的出口。
3. 在 Device Profile: PowerStrip（设备配置文件：配电盘）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，配电盘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，单击与配电盘相连的设备旁边的 + 号。
2. 选择要配置哪个配电盘的出口。
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，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，单击与配电盘相连的设备旁边的 + 号。
2. 单击配电盘旁边的 + 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，单击 OK（确定）按钮删除出口。

8 节点、节点组和接口

本节讨论如何查看、配置和编辑节点及其关联接口，以及如何创建节点组。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。

在将与节点相连的设备添加到 CC-SG 之后，可以人工将这些节点添加到 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。随时可在编辑这些节点、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. 310)，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来提供不同类型的访问，例如带外 KVM 接口、串行接口、电源控制接口、带内 SSH/RDP/VNC 接口或 DRAC/RSA/ILO 接口，视节点类型而定。

一个节点可以有多个接口，但只有一个带外串行接口或 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，还有一个电源接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、RDP、DRAC、网络浏览器和 VMware Viewer。参看*关于连接模式* (p. 187)。

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，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可以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* (参看 "设备和节点自定义视图" p. 122)，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）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。支持虚拟介质的节点有一个附加栏，显示虚拟介质是被启用还是被禁用了。

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. 21)。

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. 77)。

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。该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 Device, Port, and Node Management（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. 77)。

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. 110)。

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 Device, Port, and Node Management（设备、端口和节点管理）权限，可以重新引导和强制重新引导虚拟主机服务器。

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

为了便于识别，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。可以更新服务帐号里的登录证书，使用服务帐号的每个接口均反映此变化。

服务帐号不能用于带外接口或被管配电盘接口。

- 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。
- 对于网络浏览器接口，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，按该属性升序顺序排序表。再次单击该标题，按降序顺序排序端口。 **可选。**

字段	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，用此用户名作为登录证书的一部分。
Password（密码）	在给接口指定服务帐号时，用此密码作为登录证书的一部分。
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. 找到要编辑的服务帐号。
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 更新使用该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 更新使用该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 更新使用该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. 89)。

你必须有 Device, Port, and Node Management（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. 108)。

▶ **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）列表上选择要给哪个接口指定服务帐号。按住 Ctrl+click 或 Shift+click 键，立刻选择多个接口。

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

   单击栏标题，按字母顺序排序列表。

4. 单击 Add（添加）按钮，将所选接口移动到 Selected（选择）列表上。

5. 单击 OK（确定）按钮。服务帐号被指定给 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 更新使用该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

▶ **将节点添加到 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. 310)，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）屏幕上 Interfaces（接口）部分的 Add（添加）按钮添加一个接口。参看*添加接口* (p. 89)。
6. 可以配置一个类别和元素列表，更好地描述和组织此节点。参看*关联、类别和元素* (p. 21)。**可选。**
   - 对于列出的每个类别，单击 Element（元素）下拉菜单，在列表上选择要应用于节点的元素。

     注意：CC-SG 默认将默认类别名称 System Type（系统类型）和 US States and territories（美国各州和领地）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* (参看 "关联、类别和元素" p. 21)。
7. 单击 OK（确定）按钮保存更改。节点被添加到节点列表上。

重要：如果将刀片服务器机箱从一个 KX II 端口移到另一个 KX II 端口，在 CC-SG 上给该刀片服务器机箱节点添加的接口将丢失。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。如果你编辑节点名称，新名称不得超过最大字符数。参看 ***命名常规*** (p. 310)。

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

注意：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，应该在 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. 43)*。

删除节点

在删除节点时，将它从 Nodes（节点）选项卡上删除掉。用户不能再访问该节点。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）。显示 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。在删除结束之后，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，供设备管理员或用户使用。

▶ **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）页面。
2. 单击 Location & Contacts（位置和联系人）选项卡。
3. 输入位置信息。
   - 部门：最多 64 个字符。
   - 地点：最多 64 个字符。
   - 位置：最多 128 个字符。
4. 输入联系人信息。
   - 主联系人姓名和第二联系人姓名：最多 64 个字符。
   - 电话号码和手机号码：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。该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 Device, Port, and Node Management（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）按钮确认清除。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 用下列术语命名虚拟基础设施组件。

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”。可以将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）页面有两个向导工具：Add Control System（添加控制系统）向导和 Add Virtual Host（添加虚拟主机）向导，有助于正确添加控制系统、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。每种虚拟节点配置有一个访问接口和一个电源接口。

- 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。
- 虚拟机节点配置有一个 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 接口提供虚拟机远程控制台访问。VMW Power 接口通过 CC-SG 提供节点电源控制。

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 64 个字符。
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. 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，按该属性升序顺序排序表。再次单击该标题，按降序顺序排序端口。 **可选。**
10. 给 CC-SG 添加虚拟机给每个虚拟机创建一个节点。同时配置每个相关的虚拟主机。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。
      - 如要将 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。
      - 如要将 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 单击鼠标，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。
      - 如要将 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）。
11. 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，将共享该名称和登录证书。**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. 输入接口的名称。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（虚拟电源接口）
   - 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（如需要）。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与 VMware Virtual Center 相同。

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 64 个字符。

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. 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，按该属性升序顺序排序表。再次单击该标题，按降序顺序排序端口。 **可选。**
12. 给 CC-SG 添加虚拟机给每个虚拟机创建一个节点。同时配置每个相关的虚拟主机。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。
      - 如要将 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。
      - 如要将 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 单击鼠标，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。
- 如要将 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）。

13. 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，将共享该名称和登录证书。**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. 输入接口的名称。最多 32 个字符。
   - VI Client Interfaces（VI Client 接口）
   - VMware Viewer Interfaces（VMware Viewer 接口）
   - Virtual Power Interfaces（虚拟电源接口）
   - 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（如需要）。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，将虚拟机从 CC-SG 上删除掉。

▶ **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，按该属性升序顺序排序表。再次单击该标题，按降序顺序排序端口。 **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. 79) 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. 81)，了解完整的字段说明。
6. 单击 Next（下一步）按钮。
7. 将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 单击鼠标选择多个虚拟机。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. 如要将 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。

   *不能在本页面上将 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. 96)*。

9. 单击 Next（下一步）按钮。如果你选择删除虚拟机，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，将共享该名称和登录证书。**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（虚拟电源接口）
- 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

可以将控制系统和虚拟主机从 CC-SG 上删除掉。

在删除控制系统时，并不删除相关的虚拟主机和虚拟机。

在删除虚拟主机时，并不删除相关的控制系统和虚拟机。

在删除控制系统或虚拟主机时，并不自动删除相关的虚拟机节点。参看*删除虚拟机节点* (p. 85)。

▶ 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 单击鼠标，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. 76)。
- 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. 84)。

删除虚拟基础设施

根据下列步骤将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. 84)。
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. 85)。

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

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。

你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，无论是否选择相关的虚拟主机，都要同时同步虚拟主机。

▶ **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 单击鼠标，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 Secure Gateway 上配置的）栏显示在 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，你必须有 Node In-Band Access（节点带内访问）和 Node Power Control（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，显示与所选节点相关的控制系统、虚拟主机和虚拟机之间的关系。

你必须有 Device, Port, and Node Management（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）。
   - 用右键单击接口链接，也可以连接节点。
   - 双击虚拟电源接口链接，打开该节点对应的 Power Control（电源控制）页面。

连接节点

一旦给一个节点添加了一个接口，就可以通过该接口采用几种不同的方法连接该节点。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，选择 Connect（连接）。

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，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

*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. 78)*。

▶ **添加接口：**

1. 如果添加现有节点：单击 Nodes（节点）选项卡，选择要给哪个节点添加接口。显示 Node Profile（节点配置文件）屏幕，单击 Interfaces（接口）部分的 Add（添加）按钮。

   如果添加新节点：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，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，用 Remote Desktop Protocol（例如 Windows 服务器上的 Remote Desktop Connection）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* (p. 91)。

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. 91)。

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 - 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、**RSA** 电源控制连接接口和 **ILO Processor** 电源控制连接接口* (参看 "DRAC 连接接口、RSA 连接接口和 ILO Processor 电源控制连接接口" p. 92)和 ***IPMI** 电源控制连接接口* (p. 93)。

Managed Powerstrip Connections（被管配电盘连接）：

- Managed PowerStrip（被管配电盘）：选择此选项，通过 Raritan 配电盘或 Dominion PX 设备建立至节点的电源控制连接。

  参看*被管配电盘连接接口* (p. 92)。

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. 94)。

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. 310)，详细了解 CC-SG 的名称长度规则。

带内连接接口

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

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（UDP 端口）字段里输入此接口的 UDP 端口。**任选。**
3. 对于 RDP 接口，选择 Console（控制台）或 Remote User（远程用户）。当 Console（控制台）用户访问一个节点时，断开其他所有用户。多个 Remote Users（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。
6. 在 Description（说明）字段里输入此接口的说明。**任选。**
7. 单击 OK（确定）按钮保存更改。

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）。

2. Raritan Device Name（Raritan 设备名称）：选择能提供此节点访问的 Raritan 设备。注意必须先将设备添加到 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，Baud Rate（波特率）、Parity（奇偶校验）和 Flow Control（流控制）字段自动根据端口配置填充值。
4. 在 Description（说明）字段里输入此接口的说明。**任选。**
5. 单击 OK（确定）按钮保存更改。

DRAC 连接接口、RSA 连接接口和 ILO Processor 电源控制连接接口

▶ **添加 DRAC 连接接口、RSA 连接接口和 ILO Processor 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（UDP 端口）字段里输入此接口的 UDP 端口。**任选。**
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。**任选。**
5. 单击 OK（确定）按钮保存更改。

被管配电盘连接接口

在创建被管配电盘接口，将 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。

▶ **添加被管配电盘连接接口：**

1. Managing Device（管理设备）：
   - 选择配电盘连接的 Raritan 设备。该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）：选择配电盘连接的 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（配电盘名称）：选择给节点供电的配电盘或 PX 设备。必须先在 CC-SG 上配置配电盘或 PX 设备，此列表才会显示它。
4. Outlet Name（出口名称）：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被管配电盘接口，但不能给刀片服务器节点添加被管配电盘接口。

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. Authentication（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。**任选。**
6. 在 Description（说明）字段里输入此接口的说明。
7. 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 Web 服务器（例如 Dominion PX）的设备的连接。参看*示例：给 PX 节点添加网络浏览器接口* (p. 95)。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接口连接任何 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。

用户必须有 Node In-Band Access（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。

▶ 添加网络浏览器接口：

1. Web Browser Interface（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. 310)，详细了解 CC-SG 的名称长度规则。
2. 在 TCP Port（UDP 端口）字段里输入此接口的 UDP 端口。如果在 URL 上使用 HTTPS，必须将 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 120 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
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（用户名）和 Password（密码）字段里输入 Web 应用程序登录屏幕所需的用户名和密码。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* (p. 95)。
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。

添加网络浏览器接口注意事项

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施这些验证字段，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的帮助，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，查看标记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*

Dominion PX 管理的配电盘可以作为节点添加到 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 Port（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）下拉菜单显示该接口。可以单击下拉菜单，选择在建立至节点的连接时要使用的默认接口。

对保存对 Add Node（添加节点）或 Node Profile（节点配置文件）屏幕所做的更改之后，该接口的名称还出现在它提供访问的节点下面的 Nodes（节点）列表上。

在添加被管配电盘接口，将 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，选择要编辑哪个节点的接口。打开 Node Profile（节点配置文件）页面。
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. 89)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

可以将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。

▶ **删除节点上的接口：**

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。显示确认消息。
5. 单击 Yes（是）按钮删除接口。

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（将 URL 复制到剪贴板上）。
4. 单击 OK（确定）按钮。URL 被复制到剪贴板上。
5. 打开新浏览器窗口，将 URL 粘贴到地址栏。
6. 按 Enter 键，连接此 URL。
7. 将此 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（将接口添加到收藏夹）：

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，将书签添加到 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. 在显示 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. 157)。

配置节点直接端口访问

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

参看*添加接口书签* (p. 97)。

节点关联、位置和联系人批量复制

批量复制命令允许你将一个节点上的类别、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，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）列表上选择要将 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，将节点添加到 Selected Nodes（选择的节点）列表上。
5. 选择节点，单击 < 按钮将它从 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，才能针对该节点启动聊天会话。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，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，但其他人仍然可以了解。

添加、编辑和删除节点组

节点组概述

节点组用于将节点分成组。节点组是访问策略的基础，允许或拒绝访问此特定节点组。参看*添加策略* (p. 118)。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. 21)，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。单击一个节点组，在节点组管理器上查看该组的详细信息。

- 如果组是任意组合的，显示 Select Nodes（选择节点）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 Nodes（描述节点）选项卡，显示组节点选择规则。
- 如要搜索节点组列表上的节点，在列表下面的 Search（搜索）字段里输入字符串，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. 105)。
- 如果按属性查看组，单击 View Nodes（查看节点）按钮，Node Group（节点组）显示当前节点的列表。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（组）> New（新建）。显示一个节点组模板。
3. 在 Group name（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. 310)，详细了解 CC-SG 的名称长度规则。
4. 可以采用两种方法将节点添加到组：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，将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，它们被自动添加到组里。

如果只想人工创建由特定节点构成的组，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组里。在将新节点或设备添加到 CC-SG 之后，必须人工将它们添加到组里。

这两种方法不能混用。

一旦用一种方法创建一个组，必须用同一种方法编辑该组。如果换用另一种方法，将覆盖当前组设置。

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，选择一个设备过滤 Available（可用）列表，只显示那些与该设备有相同接口的节点。
3. 在 Available（可用）列表上选择要添加到组里的节点，单击 Add（添加）按钮将它移到 Selected（选择）列表上。Selected（选择）列表上的节点将被添加到组里。
   - 如要删除组里的一个节点，在 Selected（选择）列表上选择节点名称，单击 Remove（删除）按钮。
   - 可以搜索 Available（可用）列表或 Selected（选择）列表上的节点。在列表下面的字段里输入搜索词，单击 Go（搜索）按钮。
4. 如果要创建一个策略，始终允许访问此组里的节点，选择 Create Full Access Policy For This Group（给组创建全访问策略）复选框。
5. 在将节点添加到组之后，单击 OK（确定）按钮创建节点组。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，将适当的单元格变成下拉菜单，然后给每个组件选择适当的值：
   - 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。这里只显示与所选类别关联的元素（例如：如果对 Department 类别求值，这里不显示 Location 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，在表上突出显示该规则，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，用逻辑运算符描述每个规则之间的关系。
   - &— “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。

     例如：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，始终允许访问此组里的节点，选择 Create Full Access Policy For This Group（给组创建全访问策略）复选框。
9. 在描述此组里的节点之后，单击 OK（确定）按钮创建节点组。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）窗口显示该节点的详细信息。
3. 参看选择节点或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（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。

9 用户和用户组

创建用户帐号，以便给用户指定访问 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* ("远程认证" p. 130)。

也可以创建访问策略，给用户组指定这些策略。参看*访问控制策略* (p. 117)。

在本章内

Users（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。默认用户名为 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，不能删除该组里的唯一用户。CC 超级用户组成员始终要使用强密码。强密码要求如下：

- 密码必须包含至少一个小写字母。
- 密码必须包含至少一个大写字母。
- 密码必须包含至少一个数字。
- 密码必须包含至少一个特殊字符（例如感叹号或 &）。

系统管理员组

系统管理员组有全管理权和访问权。与 CC 超级用户组不同，可以更改系统管理员组的权限，可以添加或删除成员。

CC 用户组

CC 用户组有带内和带外节点访问权。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对用户进行组织。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，给它指定用户管理权限，那么给该组指定的所有用户都能看到和执行用户管理器菜单上的命令。参看*用户组权限* (p. 285)。

配置用户组涉及四个基本步骤：

- 命名组，输入组说明。
- 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）。显示 Add User Group（添加用户组）屏幕。
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* ("命名常规" p. 310)，详细了解 CC-SG 的名称长度规则。
3. 在 Description（说明）字段里输入简短组说明。**任选。**
4. 单击 Privileges（权限）选项卡。
5. 选择要给用户组指定的每个权限对应的复选框。
6. 权限表下面是 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对应的复选框。
7. 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. 117)，详细了解策略，以及如何创建策略。
8. 在 All Policies（所有策略）列表上选择要给用户组指定的策略，单击 Add（添加）按钮将它移动到 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。

   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），单击 Add（添加）按钮。
- 如果要将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，单击 Remove（删除）按钮。

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

编辑用户组

在编辑用户组时，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。显示 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。**任选。**
4. 在 Description（说明）字段里输入用户组的新说明。**任选。**
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。取消权限，将它从用户组上删除掉。
7. 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接口类型，选择 Control（控制）。
8. 单击下拉菜单，查看此组在访问时不使用的接口类型，选择 Deny（拒绝）。
9. 单击 Policies（策略）选项卡。显示两个策略表。
10. 对于要给组添加的每个策略，在 All Policies（所有策略）上选择策略，单击 Add（添加）按钮将它移动到 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）。
11. 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，单击 Remove（删除）按钮。
12. 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。

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）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，将要启用组访问审计的用户组移动到 Selected（选择）列表上。按住 Ctrl 单击鼠标，选择多项。

   *提示：在 Find（查找）字段里输入用户组名称，在列表上突出显示该用户组。在不完整名称后面输入 *，在列表上突出显示所有类似名称。*

   单击栏标题，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

在将一个用户添加到 CC-SG 时，必须指定一个用户组，将给该用户组指定的权限指定给该用户。

▶ 添加用户：

1. 在 Users（用户）选项卡上选择要将用户添加到哪个组。
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. 310)，详细了解 CC-SG 的名称长度规则。
4. 如果希望此用户能登录 CC-SG，选择 Login Enabled（允许登录）复选框。
5. 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。
6. 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. 310)，详细了解 CC-SG 的密码长度规则。*

   *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. 175)，了解强密码的详细信息。*

7. 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。
8. 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。
9. 如果选择，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。
10. 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。
11. 在 Telephone Number（电话号码）字段里输入用户的电话号码。
12. 单击 User Groups（用户组）下拉菜单，选择要将用户添加到哪个组。

- 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，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. 110)。

13. 在配置此用户之后，单击 Apply（应用）按钮保存此用户，再创建另一个用户，或者单击 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，该用户位于所属的用户组下面。

编辑用户

在编辑用户时，不能更改所属的组。参看*给用户指定组* (p. 113)。

▶ 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，选择该用户。显示 User Profile（用户配置文件）。
2. 取消 Login enabled（允许登录）复选框，禁止此用户登录 CC-SG。选择 Login enabled（允许登录）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（再次键入新密码）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. 175)，了解强密码的详细信息。*

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，将他从 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。

即使用户属于多个用户组，这个过程也删除该用户的所有实例。参看***删除用户组里的用户*** (参看 "删除组用户" p. 114)，了解在删除用户组里的用户时，如何不将他从 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，选择该用户。显示 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，将用户从 CC-SG 上就用删除掉。

给用户指定组

用此命令给现有用户指定另一个组。采用这种方法指定的用户被添加新组里，但仍然属于此前给他们指定的组。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（非组用户）列表显示尚未指定目标组的用户。
   - 在此列表上选择要添加的用户，单击 > 按钮将他移动到 Users in group（组内用户）列表上。
   - 单击 >> 按钮，将所有非组用户移动到 Users in group（组用户）列表上。
   - 在 Users in group（组用户）列表上选择要删除的用户，单击 < 按钮删除他们。
   - 单击 << 按钮，删除 Users in group（组用户）列表上的所有用户。
5. 在将所有用户移动到合适的栏上之后，单击 OK（确定）按钮。Users in group（组用户）列表上的用户被添加到所选的用户组。

删除组用户

在删除一个组用户时，只将该用户从指定的组里删除掉。该用户仍然在其他指定组里。在删除一个组用户时，并不将该用户从 CC-SG 上删除掉。

如果一个用户只属于一个组，不能将他从组里删除掉。只能将该用户从 CC-SG 上删除掉。

▶ **删除组用户：**

1. 在 Users（用户）选项卡上，单击 + 号展开你要删除的组用户所在的用户组，选择该用户。显示 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）。显示 Delete User（删除用户）屏幕。
3. 单击 OK（确定）按钮，将用户从组里删除掉。

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 > My Profile（我的配置文件）。显示 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 > 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。

更改默认搜索首选项

1. 选择 Secure Gateway > 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，将显示的节点、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 > My Profile（我的配置文件）。
2. 单击 Font Size（字体大小）下拉菜单，调整标准 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 > 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 > 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。

注销用户

可以按个人或按用户组，在 CC-SG 上注销活动用户。

▶ 注销用户：

1. 在 Users（用户）选项卡上，单击 + 号展开你要在 CC-SG 上注销哪个用户组里的用户，选择该用户。
   - 如要选择多个用户，按住 Shift 键单击其他用户。

2. 选择 Users（用户）> User Manager（用户管理器）> Logout User（注销用户）。显示 Logout User（注销用户）屏幕，列出所选的用户。
3. 单击 OK（确定）按钮，在 CC-SG 上注销这些用户。

▶ **注销用户组里的所有用户：**

1. 在 Users（用户）选项卡上选择要在 CC-SG 上注销的用户组。
   - 如要注销多个用户组，按住 Shift 键单击其他用户组。
2. 选择 Users（用户）> User Group Manager（用户组管理器）> Logout User（注销用户）。显示 Logout User（注销用户）屏幕，列出所选组里的活动用户。
3. 单击 OK（确定）按钮，在 CC-SG 上注销这些用户。

批量复制用户

可以对用户使用批量复制命令，将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上。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，选择该用户。
2. 选择 Users（用户）> User Manager（用户管理器）> Bulk Copy（批量复制）。Username（用户名）字段显示要复制的用户的策略和权限。
3. 在 All Users（所有用户）列表上选择哪些用户将接受 Username（用户名）字段显示的用户的策略和权限。
   - 单击 > 按钮将用户名移动到 Selected Users（选择的用户）列表上。
   - 单击 >> 按钮将所有用户移动到 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，单击 < 按钮删除该用户。
   - 单击 << 按钮删除 Users in group（组用户）列表上的所有用户。
4. 单击 OK（确定）按钮复制。

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，是否启用了虚拟介质权限（如适用）。创建策略最简单的方式是将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，将它指定给用户组。参看*给用户组指定策略* (p. 121)。

CC-SG 有一个全访问策略。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. 13)。

▶ 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. 100)。
- 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. 56)。
- 针对节点组或设备组创建策略，指定何时可以访问该节点组或设备组。参看*添加策略* (p. 118)。
- 将策略应用于用户组。参看*给用户组指定策略* (p. 121)。

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。

注意：当 CC-SG 处于 Proxy（代理）模式或 Both（二者）模式时，不能授予用户虚拟介质访问权。参看连接模式：直接和代理 ("连接模式：直接和代理" p. 187)。

▶ **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。显示一个对话框，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. 310)，详细了解 CC-SG 的名称长度规则。
4. 单击 OK（确定）按钮。新策略被添加到 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，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，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，只选择该类型的值。
8. 单击 Days（日期）下拉箭头，选择在一个星期的哪几天执行此策略：All days（全部）、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，选择自己设置的日期。各个日期复选框被启用。
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），Virtual Media Permission（虚拟介质权限）部分被启用。在 Virtual Media Permission（虚拟介质权限）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介质：
    - Read-Write（读写）启用虚拟介质读写权限
    - Read-only（只读）启用虚拟介质只读权限
    - Deny（拒绝）拒绝所有虚拟介质访问
15. 单击 Update（更新）按钮将新策略添加到 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，先进入维护模式，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. 162)。

▶ **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，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。在字段里输入策略的新名称，单击 OK（确认）按钮更改策略名称。**任选。**
4. 单击 Device Group（设备组）下拉箭头，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，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，只选择该类型的值。
7. 单击 Days（日期）下拉箭头，选择在一个星期的哪几天执行此策略：All（每天）、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，选择自己设置的日期。各个日期复选框被启用。
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），Virtual Media Permission（虚拟介质权限）部分被启用。在 Virtual Media Permission（虚拟介质权限）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介质：
    - Read-Write（读写）启用虚拟介质读写权限
    - Read-only（只读）启用虚拟介质只读权限
    - Deny（拒绝）拒绝所有虚拟介质访问
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，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。

虚拟介质支持

CC-SG 给与支持虚拟介质的 KX2、KSX2 和 KX2-101 设备相连的那些节点提供远程虚拟介质支持。如要详细了解如何通过自己的设备访问虚拟介质，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. 118)，详细了解如何在 CC-SG 上创建策略，给用户组指定虚拟介质权限。

给用户组指定策略

必须给用户组指定策略，策略才会生效。一旦给用户组指定策略，组成员的访问权就受该策略的控制。参看*用户和用户组* (p. 105)，详细了解如何给用户组指定策略。

11 设备和节点自定义视图

“自定义视图”允许使用类别、节点组和设备组来指定在左侧面板内以不同方式来显示节点和设备。

在本章内

自定义视图的类型

有三种类型的自定义视图：“按类别查看”、“按节点组筛选”和“按设备组筛选”。

按类别查看

在应用 View by Category（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 Filter by Node Group（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 Filter by Device Group（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。如果一个设备属于在定制视图上定义的多个设备组，它可能在列表中出现多次。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 中使用自定义视图

节点自定义视图

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）。显示 Custom View（定制视图）屏幕。
3. 单击 Custom View（定制视图）面板上的 Add（添加）按钮。打开 Add Custom View（添加定制视图）窗口。
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，单击 Add（添加）按钮将它移到列表上。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，单击上下箭头按钮将它移动到希望的位置。
   c. 如果必须删除列表上的一项，选择该项，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）。

应用节点定制视图

▶ **将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）。显示 Custom View（定制视图）屏幕。
2. 单击 Name（名称）下拉箭头，在列表上选择一个定制视图。
3. 单击 Apply（应用）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）。显示 Custom View（定制视图）屏幕。
3. 单击 Name（名称）下拉箭头，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，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，单击 Add（添加）按钮将它移到列表上。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，单击上下箭头按钮将它移动到希望的位置。
   c. 如果必须删除列表上的一项，选择该项，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）。

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）。显示 Custom View（定制视图）屏幕。
3. 单击 Name（名称）下拉箭头，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。

指定默认节点定制视图

▶ **指定默认节点定制视图：**

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）。显示 Custom View（定制视图）屏幕。
3. 单击 Name（名称）下拉箭头，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。

给所有用户指定默认节点定制视图

如果你有 CC 设置和控制权，可以给所有用户指定默认定制视图。

▶ **给所有用户指定默认节点定制视图：**

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）。
3. 单击 Name（名称）下拉箭头，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定制视图排序的 Nodes（节点）选项卡。用户可以更改定制视图。

设备自定义视图

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）。显示 Custom View（定制视图）屏幕。
3. 单击 Custom View（定制视图）面板上的 Add（添加）按钮。显示 Add Custom View（添加定制视图）窗口。
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，单击 Add（添加）按钮将它移到列表上。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，单击上下箭头按钮将它移动到希望的位置。
   c. 如果必须删除列表上的一项，选择该项，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）。

应用设备定制视图

▶ **将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）。显示 Custom View（定制视图）屏幕。
2. 单击 Name（名称）下拉箭头，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）。显示 Custom View（定制视图）屏幕。
3. 单击 Name（名称）下拉箭头，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，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，单击 Add（添加）按钮将它移到列表上。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，单击上下箭头按钮将它移动到希望的位置。
   c. 如果必须删除列表上的一项，选择该项，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）。

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）。显示 Custom View（定制视图）屏幕。
3. 单击 Name（名称）下拉箭头，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。

指定默认设备定制视图

▶ **指定默认设备定制视图：**

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）。显示 Custom View（定制视图）屏幕。
3. 单击 Name（名称）下拉箭头，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。

给所有用户指定默认设备定制视图

如果你有 Device, Port, and Node Management（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。

▶ **给所有用户指定默认设备定制视图：**

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）。
3. 单击 Name（名称）下拉箭头，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定制视图排序的 Devices（设备）选项卡。用户可以更改定制视图。

12 远程认证

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。

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，会导致失败登录尝试。
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，必须将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. 105)，详细了解如何添加要远程验证的用户。

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。不必同时指定公用名和机构单位。

- 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

通过在 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该用户访问权。注意可以指定多个公用名、机构单位和域组件。

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 机构单位里的所有用户。

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 用该服务器进行用户验证，选择 Authentication（验证）复选框。
   b. 如果希望 CC-SG 用该服务器给用户授权，选择 Authorization（授权）复选框。只有 AD 服务器能用于授权。
4. 单击 Update（更新）按钮保存更改。

建立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。

▶ **建立 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，单击上下箭头键排列优先使用顺序。
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，不必在 CC-SG 上定义这些用户。这样，可以在 AD 服务器上单独维护用户。在 CC-SG 上将 AD 服务器配置为模块之后，CC-SG 可以查询给定域对应的所有域控制器。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。

将 AD 模块添加到 CC-SG

重要说明：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. 179)。

▶ 将 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，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。
   - 最大字符数是 31。
   - 可以使用所有可打印字符。
   - 模块名称是任选的，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）按钮继续。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。

不要重复添加 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）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. 175)。

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：Windows 2003 默认不允许匿名查询。Windows 2000 服务器允许某些匿名操作，其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。需要的格式取决于 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 内的一个组，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。最长 32 个字符。

6. 单击 Test Connection（测试连接），用给定的参数测试 AD 服务器连接。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，再试一次。
7. 单击 Next（下一步）按钮继续。打开 Advanced（高级）选项卡。

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. 指定一个基本 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	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，将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，该模式将与在小程序上输入的用户名合并在一起，用合并用户名连接 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 是否等于在小程序上输入的用户名。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提供的密码正确无误。

7. 单击 Next（下一步）按钮继续。打开 Groups（组）选项卡。

AD 组设置

可以在 Groups（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：在从 AD 上导入组之前，必须指定组设置。

1. 单击 Groups（组）选项卡。
2. 指定一个基本 DN（目录级/项），在此下面搜索包含待授权用户的组。

示例	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，将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（组）项里组类型的所有项。

4. 单击 Next（下一步）按钮继续。打开 Trusts（信任）选项卡。

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）栏上的每个域，单击 Trust Direction（信任方向）下拉菜单，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）：信任来自该域的信息。
   - 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 LDAP 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。

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，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. 134)、***AD 高级设置*** (p. 135)、***AD 组设置*** (p. 136)和 ***AD 信任设置*** (p. 136)。
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，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. 139)和*同步所有 **AD** 模块* (p. 140)。

导入 AD 用户组

在从 AD 服务器导入组之前，必须在 AD 模块上指定组设置。参看 ***AD 组设置*** (p. 136)。

在更改导入的组或用户之后，必须同步你更改的 AD 用户组，使导入的组映射到 AD 上的适当组，并同步所有 AD 模块，使所有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. 139)和***同步所有 AD 模块*** (p. 140)。

可以从 AD 导入嵌套组。

*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. 175)*。*

▶ **导入 AD 用户组：**

1. 选择 Administration（管理）> Security（安全）。
2. 单击 Authentication（验证）选项卡。所有配置的验证和授权服务器显示在一个表里。
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），检索 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 的组。
   - 导入用户组名称最多 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，单击 Go（搜索）按钮。
   - 单击一个列标题，按该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，将它指定给所选的组。
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，并查看刚才导入的组的权限，单击 Users（用户）选项卡，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，查看该用户组关联的 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. 140)。只有在用 AD 进行授权时，才需要此类同步。
- 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. 140)。
  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，可以将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. 139)。

使所有用户组与 AD 同步

如果更改了一个用户组，例如将用户组从一个 AD 模块移动到另一个 AD 模块上，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. 140)。

在同步 AD 用户组时，CC-SG 检索所选 AD 模块上的用户组，将其名称与此前从 AD 上导入的用户组进行对比，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，仅仅将 AD 上的组名称映射到 CC-SG 上。

▶ **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。所有配置的验证和授权服务器显示在一个表里。
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），单击箭头按钮。
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，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

无论何时更改或删除 AD 上的用户，更改 AD 上的用户权限，或者更改域控制器，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对比，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 也从本地高速缓存上删除与被删除组之间的所有关联。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。所有配置的验证和授权服务器显示在一个表里。
3. 在 On Demand Synchronization（按需同步）列表上选择 All Active Directory Modules（所有 Active Directory 模块），单击箭头按钮。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

▶ 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。所有配置的验证和授权服务器显示在一个表里。
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，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。所有配置的验证和授权服务器显示在一个表里。
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。

更改每日 AD 同步时间

在启用每日同步之后，可以指定自动同步时间。默认每日同步时间是 23:30。

▶ **更改每日 AD 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，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。

关于 LDAP 和 CC-SG

一旦 CC-SG 启动并且输入了用户名和密码，则通过 CC-SG 或直接向 LDAP 服务器发送一条查询。如果用户名和密码匹配 LDAP 中的信息，则用户认证通过。然后将根据 LDAP 服务器上的本地用户组对用户进行授权。

将 LDAP (Netscape) 模块添加到 CC-SG

▶ **将 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，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）按钮继续。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* ("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 Secure Connection for LDAP（LDAP 安全连接）。
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，其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。输入一个标识名 (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. 如要将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) 将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. 如果要用加密方法将密码发送到 LDAP 服务器，选择 Base 64。如果要将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 将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 将密码和 LDAP 对象再次绑定在一起，并将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，使用下面这样的参数设置：

参数名称	SUN One LDAP 参数
IP Address/Hostname（IP 地址/主机名）	<目录服务器 IP 地址>
User Name（用户名）	CN=<有效用户 id>
Password（密码）	<密码>
BaseDN（基本 DN）	O=<机构>
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，使用下面这样的参数设置：

参数名称	Open LDAP 参数
IP Address/Hostname（IP 地址/主机名）	<目录服务器 IP 地址>
User Name（用户名）	CN=<有效用户 ID>, O=<机构>
Password（密码）	<密码>
User Base（用户库）	O=帐号, O=<机构>
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）	加密
Use Bind（使用绑定）	不选择

参数名称	Open LDAP 参数
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. 105)。

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. 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* ("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。最长 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. 105)。

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，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）按钮继续。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* ("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，然后在 Password（密码）字段里输入固定密码，再在 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. 301)。

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

- 单击一个栏标题，按该栏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。
- 再次单击栏标题，按降序排序数据。

调整报告栏宽

你选择的栏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栏分隔线上，直到指针变成双向箭头为止。
2. 单击并左右拖动鼠标，即可调节栏宽。

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 键查看详细信息。

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 > 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 > Print（打印）。

将报告保存到文件

可以将报告保存成 .CSV 文件，然后用 Excel 打开。在将报告保存到文件时，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. 生成要保存到文件的报告。
2. 单击 Save to File（保存到文件）按钮。
3. 输入文件名，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）。
3. 单击 Yes（是）按钮确认删除。

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。

审计跟踪报告

CC-SG 审计跟踪报告显示审计日志和访问。它捕捉设备或节点添加、编辑或删除操作，以及其他修改。

CC-SG 的审计跟踪记录下列事件：

- CC-SG 启动时间
- CC-SG 停止时间
- 用户登录 CC-SG 的时间
- 用户退出 CC-SG 的时间
- 用户建立节点连接的时间

▶ **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。单击选择默认日期的每个部分（月、日、年、时、分），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。
   - 如要将报告限制在一种消息，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。
   - 如要将报告限制在特定用户的活动，在 Username（用户名）字段里输入该用户的用户名。
   - 如要将报告限制在特定 IP 地址的活动，在 User IP address（用户 IP 地址）字段里输入该用户的 IP 地址。
4. 在 Entries to Display（要显示的项）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。
   - 如要清除报告记录，单击 Purge（清除）按钮。参看*清除 CC-SG 上的报告数据* (p. 150)。

错误日志报告

CC-SG 将错误信息存储在一系列可以访问的错误日志文件里，这些信息有助于排除问题。错误日志包括一部分与错误条件关联的审计跟踪项。

▶ **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。单击选择默认日期的每个部分（月、日、年、时、分），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。
   - 如要将报告限制在特定用户的活动，在 Username（用户名）字段里输入该用户的用户名。

- 如要将报告限制在特定 IP 地址的活动，在 User IP address（用户 IP 地址）字段里输入该用户的 IP 地址。

4. 在 Entries to Display（要显示的项）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. 150)。

访问报告

生成访问报告，即可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。单击选择默认日期的每个部分（月、日、年、时、分），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。
   - 如要将报告限制在特定设备，在 Device Name(s)（设备名称）字段里输入设备名称。
   - 如要将报告限制在特定节点，在 Node Name(s)（节点名称）字段里输入端口名称。
   - 如要将报告限制在特定用户的活动，在 Username(s)（用户名）字段里输入该用户的用户名。
   - 如要将报告限制在特定 IP 地址的活动，在 IP Address(es)（IP 地址）字段里输入该用户的 IP 地址。
5. 在 Entries to Display（要显示的项）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 所管理的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. 在活动用户报告上选择要断开的用户名称。
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失败登录尝试过多而被 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. 204)。

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，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（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（允许登录）选项而定。参看*添加用户* (p. 111)。
  - Password Expiration（密码到期）字段里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* ("添加用户" p. 111)。
  - 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. 285)。
  - 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。

▶ **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）。生成所有设备资产报告。

▶ **按设备类型过滤报告数据：**

- 选择设备类型，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。

▶ **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，显示组设备列表。

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
	All（全部）	所有端口。
Status（状态）：		
	Up（打开）	

状态类型	端口状态	定义
	Down（关闭）	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，可连接端口。
	Connected（连接）	
	Busy（忙）	用户连接此端口。
	Power on（通电）	
	Power off（断电）	
Unconfigured（未配置）：		
	New（新）	端口连接目标服务器，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（手动或意外），形成幻影端口。参看 Raritan《Paragon II 用户指南》。**任选。**
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。**任选。**
5. 在 Entries to Display（要显示的项）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，单击 Add（添加）按钮将它移动到 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。

▶ 获取所有接口的书签 URL：

1. 生成节点资产报告，双击一个节点查看详细信息对话框。
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 栏上有每个节点的直接链接。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. 97)。

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，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）选项将报告限制在那些有“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）选择值，然后单击上下箭头调节到希望的数。
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节点组信息。

▶ **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，显示组节点列表。

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 的所有组用户。报告不包括在本地通过 CC-SG 被添加到 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）列表中选择的 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，单击 Add（添加）按钮将它移动到 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. 212)。

▶ **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. 输入 Report Name（报告名称）字段里输入报告名称，按名称过滤。可以输入完整名称，也可以输入部分名称。报告名称不区分大小写。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。单击选择默认日期的每个部分（月、日、年、时、分），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 键单击鼠标选择多个报告。
2. 单击 Delete Reports（删除报告）按钮。
3. 单击 Yes（是）按钮确认删除。

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。任务一旦完成，报告信息即变为静态信息。

参看*预定报告* (p. 159)，详细了解如何查看报告。

CC-NOC 同步报告

CC-NOC 同步报告列出 CC-SG 预定的、CC-NOC 在特定发现日期监视的所有目标及其 IP 地址。这里还显示在配置的范围内发现的任何新目标。参看*添加 CC-NOC* (p. 219)。可以将此报告上的目标从 CC-SG 数据库里清除掉。

▶ 生成 CC-NOC 同步报告：

1. 选择 Reports（报告）> CC-NOC Synchronization（CC-NOC 同步）。

2. 选择 Last Discovered Date（上次发现日期），单击 Get Targets（获取目标）按钮。Targets Discovered（发现的目标）显示在上次发现日期发现的目标或此前发现的目标。
   - 如果要从 CC-SG 数据库里清除一个目标，选择要清除的目标，单击 Purge（清除）按钮。
   - 如果要从 CC-SG 数据库里清除整个目标列表，单击 Purge All（全部清除）按钮。

14 系统维护

在本章内

维护模式

维护模式限制对 CC-SG 的访问，使管理员可以不中断地执行各种操作，例如升级 CC-SG。

在可配置时间到期之后，提示当前用户（进入维护模式的管理员除外）退出系统。在维护模式下，其他管理员可以登录 CC-SG，但非管理员不能登录。每当 CC-SG 进入或退出维护模式时，生成一个 SNMP 陷阱。

注意：维护模式仅在独立 CC-SG 设备上可用，在群集配置下不可用。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 处于维护模式下时，不能执行预定任务。参看*任务管理器* (p. 212)。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）：输入在用户退出 CC-SG 时显示的消息。
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

最好在进入维护模式之后备份 CC-SG。进入维护模式可以保证在进行备份时，不更改数据库。

▶ **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）。
   - Custom（定制）— 允许你在 Backup Options（备份选项）区下面选择要将哪些部分添加到备份上。选择下列每一项，将它包括在备份中。

- Data（数据）— CC-SG 配置、设备配置、节点配置和用户数据（标准）。
- Logs（日志）— CC-SG 存储的错误日志和事件报告。
- CC firmware files（CC 固件文件）— 存储的用于更新 CC-SG 服务器的固件文件。
- Device firmware files（设备固件文件）— 存储的用于更新 CC-SG 管理的 Raritan 设备的固件文件。
- Application files（应用程序文件）— 存储的供 CC-SG 用于将用户连接到节点的应用程序。

- Full（全）— 备份 CC-SG 存储的所有数据、所有日志、所有固件文件和所有应用程序文件。这种备份生成的备份文件最大。
- Standard（标准）— 只备份 CC-SG 上的关键数据。此备份包括 CC-SG 配置信息、设备配置、节点配置和用户配置。这种备份生成的备份文件最小。

5. 如要将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。**
6. 选择连接远程服务器所用的 Protocol（协议）：FTP 或 SFTP。
7. 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。
8. 如果不使用所选协议的默认端口 (FTP:21, SFTP: 22)，在 Port Number（端口号）字段里输入所用的通信端口。
9. 在 Username（用户名）字段里输入远程服务器用户名。
10. 在 Password（密码）字段里输入远程服务器密码。
11. 在 Directory（目录）字段里指定在远程服务器的哪个目录下存储备份文件。必须指定绝对目录路径。
12. 在 Filename（文件名）字段里输入要在远程服务器上保存的备份文件的文件名。
13. 如果要将当前远程服务器设置保存为默认值，单击 Save As Default（另存为默认值）。**可选。**
14. 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. 165)。

重要：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。

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。可以将保存在其他位置的备份文件上载到其他 CC-SG 设备上恢复，从而将一个 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。显示 Save（保存）对话框。
4. 输入文件名，选择文件保存位置。
5. 单击 Save（保存）按钮，将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。显示确认对话框。
3. 单击 OK（确定）按钮，将备份文件从 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：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）屏幕，显示 CC-SG 可用的备份文件列表。你可以看到备份类型、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，必须先将备份文件上载到 CC-SG。**可选。**

a. 单击 Upload（上载）按钮。

b. 浏览备份文件，在对话框上选择该文件。可以在客户网络的任何地方检索备份文件。

c. 单击 Open（打开）按钮，将此文件上载到 CC-SG。在上载完成之后，Available Backups（可用备份）表显示该备份文件。

3. 在 Available Backups（可用备份）表上选择要恢复的备份文件。

4. 如适用，选择在此备份文件上执行哪种恢复：

- Standard（标准）— 只将关键数据恢复到 CC-SG 上。包括 CC-SG 配置信息、设备配置、节点配置和用户配置。
- Full（全）— 恢复备份文件存储的所有数据、所有日志、所有固件文件和所有应用程序文件。这要求备份文件是全备份文件。
- Custom（定制）— 允许你在 Restore Options（恢复选项）区下面选择要将备份文件的哪些部分恢复到 CC-SG 上。选择下列每一项，将它包括在恢复中。
  - Restore Data（恢复数据）— CC-SG 配置、设备配置、节点配置和用户数据。
  - 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 用于将用户连接到节点的应用程序。

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，然后用所选备份文件恢复配置。在开始恢复时，其他用户退出系统。

复位 CC-SG

可以复位 CC-SG 清除数据库，或者将其他组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，将备份文件保存到另一个位置。

建议你使用所选的默认选项。

选项	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，Full Database（全数据库）复位均复位 IP-ACL 设置。 复位时删除邻居配置，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 Super User 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。
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。 ▪ Secure Communication between PC Clients and CC-SG（PC 客户机和 CC-SG 之间的安全通信）。 ▪ 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）。

选项	说明
Network Settings（网络设置）	此选项将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）：Primary/Backup（主/备用） ▪ 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 Configuration（SNMP 配置）	此选项将 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） ▪ SNMP Trap Configuration（SNMP 陷阱配置） ▪ SNMP Trap Destinations（SNMP 陷阱目标）
Default Firmware（默认固件）	此选项将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（在复位后将固件上载到数据库）	此选项将当前 CC-SG 版本的固件文件加载到 CC-SG 数据库。
Diagnostic Console（诊断控制台）	此选项将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，Full Database（全数据库）复位均复位 IP-ACL 设置。

▶ **复位 CC-SG：**

1. 在复位之前备份 CC-SG，将备份文件保存到远程位置。参看 ***备份 CC-SG*** (p. 163)。
2. 选择 System Maintenance（系统维护）> Reset（复位）。

3. 选择复位选项。
4. 输入 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，所有活动用户退出 CC-SG。

在重新启动时，不给 CC-SG 重新通电。如要执行完整的重新引导操作，必须使用诊断控制台或 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）：输入给那些要退出 CC-SG 的用户显示的消息。
4. Restart after (min)（在此之后重新启动[分]）：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，你可以升级 CC-SG 的固件。可以在 Raritan 网站的“支持”部分找到固件文件。如要将 CC-SG 从 v3.x 升级到 v4.1，必须先将它升级到 v4.0。

CC-SG v4.0 或更高版本不兼容 G1 硬件。切勿将 CC-SG G1 设备升级到 v4.0 或更高版本。

将固件文件下载到客户机 PC 上，然后再进行升级。

只有具备 CC 设置和控制权的用户才能升级 CC-SG。

应该在升级之前备份 CC-SG，将备份文件发送到 PC 上妥善保存。参看 ***备份 CC-SG*** (p. 163) 和***保存备份文件*** (p. 165)。

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：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。

CC-SG 重新引导，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，切勿人工重启设备，切勿切断设备电源，切勿给设备重新通电。

▶ **升级 CC-SG：**

1. 将固件文件下载到客户机 PC。
2. 用具备 CC 设置和控制权的帐号登录 CC-SG Admin Client。
3. 进入 Maintenance Mode（维护模式）。参看***进入维护模式*** (p. 162)。
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，将固件文件上载到 CC-SG。

   在固件文件被上载到 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. 240)。

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）按钮查看升级日志。

c. 等待升级过程运行。当你在 upgrade.log 里看到 "Upgrade completed" 消息时，表示升级过程完成了。也可以等待 SNMP 陷阱 ccImageUpgradeResults 显示 "success" 消息。

d. 服务器必须重新引导。当你在 upgrade.log 里看到 "Linux reboot" 消息时，表示开始重新引导。服务器关机并重新引导。

注意：对于从 CC-SG 3.x 升级到 4.0.x，系统重新引导两次，这是正常现象。

---

e. 在系统重新引导之后大约两分钟，可以通过管理员帐号重新访问诊断控制台，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. 171)。
10. 清除 Java 高速缓存。参看***清除 Java 高速缓存*** (p. 172)。
11. 启动新浏览器窗口。
12. 用具备 CC 设置和控制权的帐号登录 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. 163)。
15. 备份 CC-SG。参看***备份 CC-SG*** (p. 163)。

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 6.0 或更高版本的浏览器高速缓存：

1. 选择 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 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），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，单击 OK（确定）按钮。

关闭 CC-SG

在关闭 CC-SG 时，只关闭 CC-SG 软件，不切断 CC-SG 设备电源。

在 CC-SG 关闭之后，所有用户退出系统。在通过诊断控制台或给 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 CommandCenter（关闭 CommandCenter）。
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. 252)。
- 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 自动重新引导。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：切勿按 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. 254)。

▶ **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。

- 注销系统结束会话，让客户机窗口处于打开状态。参看*注销 CC-SG* (p. 173)。
- 退出系统结束会话，关闭客户机窗口。参看*退出 CC-SG* (p. 174)。

注销 CC-SG

1. 选择 Secure Gateway > Logout（注销）。打开 Logout（注销）窗口。
2. 单击 Yes（是）按钮退出 CC-SG。在注销之后，打开 CC-SG 登录窗口。

退出 CC-SG

1. 选择 Secure Gateway > Exit（退出）。
2. 单击 Yes（是）按钮退出 CC-SG。

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。你必须有 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（显示所有用户的当日消息）。**任选。**
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，选择消息显示字体。

c. 单击 Font Size（字体大小）下拉菜单，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，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，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：

如果应用程序版本不是最新版，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. 162)。

1. 将应用程序文件保存到客户 PC。

2. 单击 Application name（应用程序名称）下拉箭头，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，必须先添加该应用程序。参看*添加应用程序* (p. 177)。
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。

添加应用程序

在将应用程序添加到 CC-SG 时，必须指定该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. 从 Available（可用）列表上选择该应用程序适用于哪些 Raritan 设备，单击 Add（添加）按钮将它添加到 Selected（选择）列表。
   - 如要删除一台使用该应用程序的设备，在 Selected（选择）列表上选择该设备，单击 Remove（删除）按钮。
5. 单击 OK（确定）按钮。显示 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），单击 Open（打开）按钮。
7. 所选的应用程序加载到 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。显示确认对话框。
4. 单击 Yes（是）按钮删除应用程序。

配置默认应用程序

关于默认应用程序

可为每种设备类型指定希望 CC-SG 默认使用那种应用程序。

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. 选择要给哪个接口或端口类型设置默认应用程序。
4. 双击该行上的 Application（应用程序）箭头。值变成下拉菜单。灰色值不能更改。
5. 选择在连接所选接口或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 Update（更新）按钮保存更改。

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。用固件管理器将设备固件文件上载到 CC-SG 上，或者删除上面的设备固件文件。一旦上载固件文件，就可以访问该文件，用它升级设备。参看*升级设备* (p. 46)。

上载固件

可以将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。

▶ **将固件上载到 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，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，选择要删除的固件。
3. 单击 Delete（删除）按钮。显示确认消息。
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：如要更改一台已经是*邻居成员* (参看 "什么是邻居？" p. 196)的 CC-SG 设备的 IP 地址，必须先将它从邻居配置中删除掉，否则不能将 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：

- 主/备用模式：参看*什么是主/备用模式？* (p. 180)
- 主动/主动模式：参看*什么是主动/主动模式？* ("什么是活动/活动模式？" p. 183)

重要：强烈建议你在新部署设备时使用主/备用模式。

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*** ("CC-SG 的建议 DHCP 配置" p. 185)，了解在 CC-SG 上使用 DHCP 的最佳方式。

关于 CC-SG LAN 端口

CC-SG 有两个主要 LAN 端口：主 LAN 和备用 LAN。主/备用模式和活动/活动模式要求你采用不同的方式连接 CC-SG LAN 端口。

参看下表，了解 CC-SG 设备上主 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：**

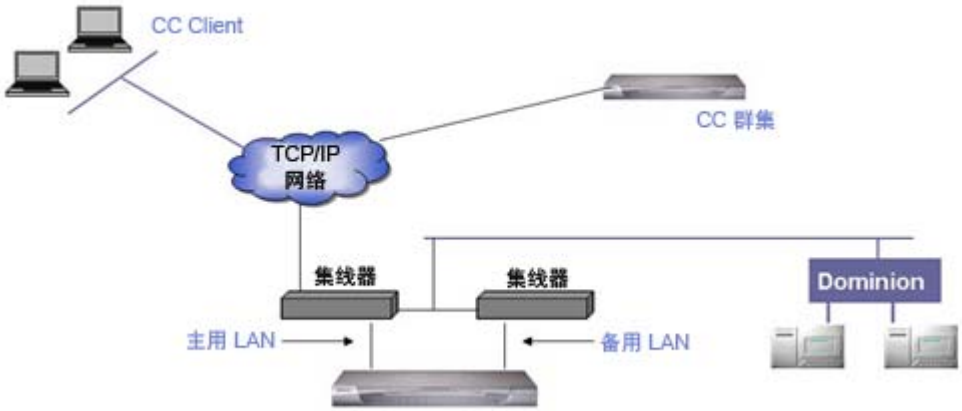
型号	主 LAN 名称	主 LAN 位置	备用 LAN 名称	备用 LAN 位置
E1-0	无标记	设备背板中央两个端口中的上面一个 LAN 端口	无标记	设备背板中央两个端口中的下面一个 LAN 端口
E1-1	LAN1	左边 LAN 端口	LAN2	右边 LAN 端口

什么是主/备用模式？

主/备用模式允许你用两个 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。

重要：强烈建议你在新部署设备时使用主/备用模式。

参看*关于 **CC-SG LAN** 端口* (p. 180)，了解每个 CC-SG 设备上主 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 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，且连接了备用 LAN，CC-SG 切换到给备用 LAN 分配的 IP 地址。将使用备用 LAN，直到主 LAN 恢复正常为止。当主 LAN 恢复正常时，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。

▶ 主/备用模式设置：

在 CC-SG 网络上实现主/备用模式时：

- 两个 CC-SG LAN 端口必须连接同一个 LAN 子网。
- 为了提高可靠性，可以将每个 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。**

▶ 在 CC-SG 上配置主/备用模式：

1. 选择 Administration（管理）> Configuration（配置）。
2. 单击 Network Setup（网络设置）选项卡。
3. 选择 Primary/Backup mode（主/备用模式）。
4. 在 Host name（主机名）字段里输入 CC-SG 主机名。参看*术语/缩写语* ("术语/缩略语" p. 2)，了解主机名规则。在单击 Update Configuration（更新配置）按钮保存配置时，如果配置了 DNS 和域后缀，也更新 Host name（主机名）字段，显示全限定域名 (Fully-Qualified Domain Name, FQDN)。
5. 单击 Configuration（配置）下拉箭头，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 CC-SG 接受动态更新，它利用 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* ("CC-SG 的建议 DHCP 配置" p. 185)。

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。

6. 单击 Adapter Speed（适配器速度）下拉箭头，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）。
7. 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，在列表上选择一种双工模式。
8. 单击 Update Configuration（更新配置）按钮保存更改。这些更改在 CC-SG 重新启动后才会生效。
   - 如果现在要自动重新启动 CC-SG，单击 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 Restart Later（稍后重新启动）按钮。参看*重新启动 **CC-SG*** (p. 169)。
     - 单击 Cancel（取消）按钮返回 Network Setup（网络设置）面板，不保存你做的更改。如要保存更改，必须单击 Update Configuration（更新配置）按钮，然后单击 Restart Now（现在重新启动）按钮或 Restart Later（稍后重新启动）按钮。

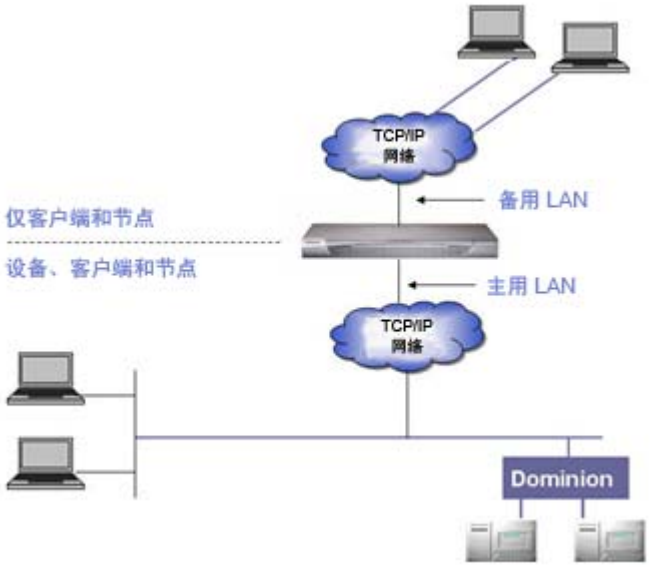
注意：如果给 CC-SG 配置了 DHCP，在成功注册到 DNS 服务器之后，可以通过主机名访问 CC-SG。

什么是活动/活动模式？

活动/活动模式允许你用 CC-SG 管理分布在两个独立网络上的设备和节点。在此模式下，CC-SG 管理两个独立 IP 域之间的流量。活动/活动模式不具备故障切换功能。如果任何一个 LAN 连接失败，用户就无法访问设备和节点。

参看*关于 **CC-SG LAN** 端口* (p. 180)，了解每个 CC-SG 型号上主 LAN 端口和备用 LAN 端口的位置。

注意：在使用活动/活动模式时，不能配置群集。



活动/活动模式设置：

在 CC-SG 网络上实现活动/活动模式时：

- 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。
- 客户机和节点可以连接主 LAN 或备用 LAN。
- 在 CC-SG 的 Network Setup（网络设置）面板上指定至多一个默认网关。如有必要，用诊断控制台添加更多静态路由。参看*编辑静态路由* (p. 247)。

在 CC-SG 上配置活动/活动模式：

1. 选择 Administration（管理）> Configuration（配置）。
2. 单击 Network Setup（网络设置）选项卡。

3. 选择 Active/Active（活动/活动）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*** ("术语/缩略语" p. 2)，了解主机名规则。在单击 Update Configuration（更新配置）按钮保存配置时，如果配置了 DNS 和域后缀，也更新 Host name（主机名）字段，显示全限定域名 (Fully-Qualified Domain Name, FQDN)。
5. 在左栏上配置主 LAN，在右栏上配置备用 LAN：
6. 单击 Configuration（配置）下拉箭头，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***CC-SG 的建议 DHCP 配置*** (p. 185)。

   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。
7. 单击 Adapter Speed（适配器速度）下拉箭头，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）。
8. 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，在列表上选择一种双工模式。
9. 单击 Update Configuration（更新配置）按钮保存更改。CC-SG 重新启动。

CC-SG 的建议 DHCP 配置

请检查以下建议的 DHCP 配置。确保 DHCP 服务器正确设置后，才能配置 CC-SG 使用 DHCP。

- 配置 DHCP 静态分配 CC-SG 的 IP 地址。
- 配置当 DHCP 为 CC-SG 分配 IP 地址时， DHCP 和 DNS 服务器自动将 CC-SG 注册到 DNS。
- 配置 DNS 接受来自 CC-SG 的未认证动态域名系统 (DDNS) 注册请求。

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，选择一个事件严重性级别。此级别和更高级别的所有事件将被发送到日志服务器上。
5. 如要配置外部备用日志服务器，重复第 3 步第 4 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，选择一个严重性级别。此级别和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，这两个报告也被清除掉。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. 150)。*

▶ **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。

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 Task Manager（任务管理器）上安排任务时，要使用 Time/Date configuration（时间/日期配置）。参看*任务管理器* **(p. 212)。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（月份），用上下箭头选择 Year（年份），然后单击日历表上的 Day（日）。
   - Time（时间）— 用上下箭头设定 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，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 NTP 配置 CC-SG 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，将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）、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。
- 代理模式允许你通过 CC-SG 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。你只需在防火墙上打开三个 CC-SG TCP 端口（80、443 和 2400）。如果在 KXII 设备上启用了 AES，代理模式不用 SSH 加密在 CC-SG 和 KXII 设备之间传输的 KVM 数据。
- 二者模式允许你配置 CC-SG 同时使用直连模式和代理模式。在二者模式中，代理模式是默认模式，但如果连接是用指定范围内的客户机 IP 地址建立的，可以配置 CC-SG 使用直连模式。

重要：当 CC-SG 处于代理模式或二者模式时，不能授权用户访问虚拟介质。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、RDP、DRAC、网络浏览器和 VMware Viewer。参看*关于接口* (p. 69)。

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 Net Address（网络地址）和 Net Mask（网络掩码）字段里，指定通过直接模式连接节点和端口的客户机 IP 地址范围，再单击 Add（添加）按钮。
5. 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，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 秒到 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）或 No（否）按钮，确认或取消电源操作。

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。取消该复选框，禁用警告消息。
4. 单击 Update Configuration（更新配置）按钮保存更改。

配置定制 JRE 设置

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，CC-SG 将给用户显示一条警告消息。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 并将备份文件保存到远程位置。参看*备份 **CC-SG*** (p. 163)。
2. 选择 Administration（管理）> Configuration（配置）。
3. 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。取消该复选框，禁用此选项。
5. 在 Require Minimum JRE（要求最低 JRE）字段里输入要求的最低 JRE 版本。必须输入完整版本号，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. 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. 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）。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 将 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，你必须输入 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被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。

▶ 在 CC-SG 上配置 SNMP：

1. 选择 Administration（管理）> Configuration（配置）。
2. 单击 SNMP 选项卡。
3. 选择 Enable SNMP Daemon（启用 SNMP 后台进程）复选框启用 SNMP 操作。
4. 如要给第三方企业管理解决方案标识 CC-SG 运行的 SNMP 代理，在 Agent Configuration（代理配置）下面输入代理信息。输入代理端口（默认是 161）。输入 Read-Only Community（只读公用名）字符串（默认值是 public）和 Read-Write Community（读写公用名）字符串（默认值是 private）。允许输入多个公用字符串，中间用逗号分隔开。在 System Contact（系统联系人）、System Name（系统名称）和 System Location（系统位置）字段里输入有关被管节点的信息。
5. 单击 Update Agent Configuration（更新代理配置）按钮保存更改。
6. 选择 Enable SNMP Traps（启用 SNMP 陷阱）复选框，允许将 SNMP 陷阱从 CC-SG 发送到 SNMP 主机。
7. 在 Trap Destinations（陷阱目标）部分输入 SNMP 主机使用的 Trap Destination Host IP address（陷阱目标主机 IP 地址）和 Port number（端口号）。默认端口是 162。
8. 在 Trap Destinations（陷阱目标）部分输入 SNMP 主机使用的 Community string（公用名）字符串和 Version（版本 [v1 或 v2]）。

9. 选择你希望 CC-SG 推送到 SNMP 主机的陷阱前面的复选框：Trap Sources（陷阱源）下面有一个分成不同的两类的 SNMP 陷阱列表：System Log（系统日志）陷阱和 Application Log（应用程序日志）陷阱，前者包括硬盘故障等 CC 设备状态通知，而后者是 CC 应用程序里的事件生成的通知（例如用户帐号通知）。如要按类型启用陷阱，选择 System Log（系统日志）和 Application Log（应用程序日志）复选框。可以选择或取消各个陷阱对应的复选框，逐个启用或禁用陷阱。用 Selected（选择）列标题内的复选框启用所有陷阱，或者取消所有复选框。参看 MIB 文件，了解提供的 SNMP 陷阱的列表。参看 MIB 文件了解详情。
10. 单击 Add（添加）按钮，将此目标主机添加到配置主机列表上。在此列表上设置的管理器没有数量限制。
11. 单击 Update Trap Configuration（更新陷阱配置）按钮保存更改。

MIB 文件

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. 294)。定制 MIB 文件可以在 Raritan 支持网站上找到。

配置 CC-SG 群集

何谓 CC-SG 群集？

一个 CC-SG 群集使用两个 CC-SG 节点，一个主用一个备用，在主用节点失效时可实现备份安全。两个节点共享活动用户和活动连接的数据，所有状态数据在两个节点之间复制。

CC-SG 群集中的设备必须知道主用 CC-SG 节点的 IP，才能向主用节点通知状态改变事件。如果主用节点失效，备用节点立即承担主用节点的所有功能。这需要初始化 CC-SG 应用程序和用户会话，主用 CC-SG 节点上发起的所有当前会话将会终止。主用节点上连接的设备将发现主用节点不再响应，于是响应由备用节点发出的请求。

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。
- CC-SG 网络必须处于主/备用模式，才能建立群集。群集不支持活动/活动配置。参看*关于网络设置* (p. 180)。
- 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。

关于 CC-SG 群集和 CC-NOC

在群集配置下，只有主节点与 CC-NOC 通信。无论 CC-SG 何时变成主节点，都将自己的 IP 地址和备用节点的 IP 地址发送给 CC-NOC。

访问 CC-SG 群集

在创建群集之后，用户可以直接访问主节点，如果他们将浏览器指向备用节点，将它们重定向到主节点。重定向对已经下载的 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

在创建群集之前，应该备份两个 CC-SG 设备的配置。

▶ 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 的固件版本和硬件型号与主节点相同。用下列方法之一指定：
   - 单击 Discover Secure Gateways（发现安全网关），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。
   - 也可以在 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型号是否与主节点相同。
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. 单击 Create Cluster（创建群集）按钮。显示一条消息。
7. 单击 Yes（是）按钮。

重要：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。

8. 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。
9. 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。

配置群集设置

不能在群集配置上更改时区。

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。
   - 如有必要，修改群集名称。
   - 在 Time Interval（时间间隔）字段里输入 CC-SG 应多久检查一次与另一节点的连接。有效范围是 5-20 秒。

   注意：如果时间间隔设置得很小，检测信号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。

   - 在 Failure Threshold（故障阈值）字段里输入在 CC-SG 节点由于没有响应而被视为发生故障之前，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

当备用节点处于等待状态时，可以更改主节点和备用节点的角色。

处于等待状态的 CC-SG 节点不接收来自主节点的更新信息。因此，在切换主节点和备用节点时，将丢失在进入等待状态之后发生的所有变化。

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）。

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。你应该登录到每个主节点删除群集，然后再创建群集。

▶ 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 Super-User 密码）均恢复到默认值。

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。你应该登录到每个主节点删除群集，然后再创建群集。

▶ 删除群集：

1. 选择 Administration（管理）> Cluster Configuration（群集配置）。
2. 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。

配置邻居

什么是邻居？

邻居是一组 CC-SG 设备，最多 10 台。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。

创建邻居

可以登录到要创建邻居、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）。
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，按 Enter 键。参看*术语/缩写语* ("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。
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，再单击 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** (参看 "什么是邻居？" p. 196)的 CC-SG 设备。*

8. 如有必要，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，按 Enter 键。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（启用）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，按该属性升序顺序排序表。再次单击该标题，按降序顺序排序端口。
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）。

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. 205)。*

(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。

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

▶ **将一台新的 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* ("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，按 Enter 键。默认名称是 CC-SG 短主机名。**可选。**
7. 单击 Send Update（发送更新）保存更改，将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（访问客户机）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，按该属性升序顺序排序表。再次单击该标题，按降序顺序排序端口。 **可选。**
3. 现在管理成员。
   - 如要停用一台 CC-SG 设备，取消该设备旁边的 Actie（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，按 Enter 键。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会话，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。

4. 单击 Send Update（发送更新）保存更改，将最新邻居信息分发给其他成员。

删除邻居成员

当邻居里的一台 CC-SG 设备变得不合时宜时，可以将它从邻居配置里删除掉，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：

- 将 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* (参看 "什么是邻居？" p. 196)。
- 复位 CC-SG 设备，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）。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）保存更改，将最新邻居信息分发给其他成员。

重要：如要更改一台已经是*邻居成员* (参看 "什么是邻居？" p. 196)的 CC-SG 设备的 IP 地址，必须先将它从邻居配置中删除掉，否则不能将 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）保存更改，将最新邻居信息分发给其他成员。

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。

安全管理器

“安全管理器”用于管理 CC-SG 如何提供到用户的访问。使用“安全管理器”可配置认证方法、SSL 访问、AES 加密、严格密码规则、锁定规则、登录门户、证书和访问控制列表。

远程验证

参看*远程验证* ("远程认证" p. 130)，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。在要求使用 AES 加密时，所有用户必须用支持 AES 的客户机访问 CC-SG。如果要求使用 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 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。

也可以尝试用要核实加密方法的浏览器访问下列网站：
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 与此网站无关。

注意：Internet Explorer 6 不支持 AES-128 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 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. 将这些文件解压到 `\lib\securiry\` 下的 Java 目录，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，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 使用客户机建立的常规 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。

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。

设置通过 SSH 访问 CC-SG 所用的端口号

可以在安全管理器上设置通过 SSH 访问 CC-SG 所用的端口号。参看*通过 SSH 访问 CC-SG* (p. 222)。

设置通过 SSH 访问 CC-SG 所用的端口号：

1. 选择 Administration（管理）> Security（安全）。
2. 在 Encryption（加密）选项卡上，在 SSH Server Port（SSH 服务器端口）字段里输入通过 SSH 访问 CC-SG 所用的端口号。
3. 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）。该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）：
   - 密码必须包含至少一个小写字母。
   - 密码必须包含至少一个大写字母。
   - 密码必须包含至少一个数字。
   - 密码必须包含至少一个特殊字符（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）功能给用户显示高级通知，告诉他们新标准是什么。

封锁设置

在达到指定的失败登录尝试次数之后，管理员可以封锁 CC-SG 用户、CC-NOC 用户与 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：默认情况下，admin 帐号在三次登录尝试失败之后，被封锁五分钟。对于 admin，不能配置封锁前后的失败登录尝试次数。

▶ 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，默认失败登录尝试次数是三次。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。如果此字段空白，不发送通知。**任选。**
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，发送的通知电子邮件里有此电话号码。**任选。**
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。

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

可以将一个小图形文件上载到 CC-SG，作为登录页面的横幅。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。显示 Open（打开）对话框。
2. 在对话框上选择要用作徽标的图形文件，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，然后才能输入登录信息。
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，选择消息字体。
      - 单击 Size（大小）下拉菜单，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，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

在“证书”选项卡中，可生成证书签名请求 (CSR) 发送到证书机构申请数字身份证书、生成一个自签名证书，或者导入和导出证书及其私有密钥。

证书任务

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。

导出当前证书和专用密钥：

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（导出当前证书和专用密钥）。
4. 单击 Export（导出）按钮。Certificate（证书）面板显示证书，Private Key（专用密钥）面板显示专用密钥。
5. 在每个面板上选择文本，按 Ctrl+C 复制文本。可以按需要将文本粘贴到任何地方。

生成证书签名请求，导入粘贴证书和专用密钥：

CSR 将被提交给证书服务器，证书服务器将发出一份签名证书。根证书也将从证书服务器上导出，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、根证书和专用密钥。

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）。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. Encryption Mode（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（专用密钥）：1024 是默认值。

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。输入完整州名或省名。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（注册公司名称）：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。注册公司名称必须有自己的 CSR 域名。如果注册公司没有自己的域名，签名服务机构拒绝签名请求。

j. Challenge Password（挑战密码）：最多 64 个字符。

k. 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。

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 和专用密钥。
6. 选择 Certificate Request（证书请求）字段里的文本，按 Ctrl+C 复制文本。用 Notepad 等 ASCII 编辑器将 CSR 粘贴到文件里，保存成 .cer 文件。
7. 选择 Private Key（专用密钥）字段里的文本，按 Ctrl+C 复制文本。用 Notepad 等 ASCII 编辑器将专用密钥粘贴到文件里，保存成 .txt 文件。
8. 将 .cer 文件提交给证书服务器，获取一份签名证书。
9. 从证书服务器下载或导出根证书，保存为 .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（导入粘贴证书和专用密钥）。

12. 复制签名证书的文本，按 Ctrl+V 将它粘贴到 Certificate（证书）字段里。
13. 复制此前保存成 .txt 文件的专用密钥的文本，按 Ctrl+V 将它粘贴到 Private Key（专用密钥）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 CSR 是其他应用程序生成的，使用该应用程序的密码。

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，将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），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. Encryption Mode（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（专用密钥）：1024 是默认值。
   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。输入完整州名或省名。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（注册公司名称）：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。注册公司名称必须有自己的 CSR 域名。如果注册公司没有自己的域名，签名服务机构拒绝签名请求。

j. Challenge Password（挑战密码）：最多 64 个字符。

k. 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。

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（专用密钥）字段显示证书和专用密钥。

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到整个 CC-SG 系统的规则(选择 System(系统)，而不是一个用户组)。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。列表项部的规则的优先级比列表上位置较低的规则高。

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，指定要将规则应用于哪个 IP 地址范围。
5. 单击 Group（组）下拉箭头，选择要将规则应用于哪个用户组。选择 System（系统），将规则应用于整个 CC-SG 系统。
6. 单击 Action(操作)下拉箭头，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，指定要将规则应用于哪个 IP 地址范围。
5. 选择 Group（组）> System（系统）。
6. 单击 Action（操作）下拉箭头，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。
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，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. 212)。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* ("术语/缩略语" p. 2)，了解主机名规则。
4. 在 SMTP port（SMTP 端口）字段里输入有效 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。**
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。**
7. 在 From（自）字段里输入有效电子邮件地址，用于标识从 CC-SG 发出的邮件。
8. 在 Sending retries（重发次数）字段里输入在发送进程失败后，重复发送电子邮件的次数。
9. 在 Sending retry interval (minutes)（重发间隔[分]）字段里输入两次重发间隔的分钟数 (0-60)。
10. 如果要用 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进行设备备份，或者预定在每个星期一通过电子邮件将特定报告发送给一个或多个收件人。

注意：任务管理器用在 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 屏幕的右上角显示服务器时间。

任务类型

可以预定下列任务：

- 备份 CC-SG
- 备份设备配置（个别设备或设备组）
- 复制设备配置（个别设备或设备组）
- 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，确保执行希望的操作。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

在完成任务之后，给指定收件人发送一封电子邮件。可以在通知管理器上指定在哪里发送电子邮件，可以选择通过 SSL 安全发送电子邮件。参看*通知管理器* (p. 211)。

预定报告

预定报告通过电子邮件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 上存储 30 天。可以在 Reports（报告）菜单上选择 Scheduled Reports（预定报告），用 HTML 格式查看完成报告。参看*预定报告* (p. 159)。

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 键单击）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，单击 Task History（任务历史记录）。

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. 216)，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）。
3. 在 Main（主）选项卡上输入任务名称（1-32 个字符、字母数字字符或下划线，无空格）和说明。
4. 单击 Task Data（任务数据）选项卡。
5. 单击 Task Operation（任务操作）下拉菜单上选择要预定的任务。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：
   - **备份 CommandCenter**：参看*备份 **CC-SG*** (p. 163)
   - **备份设备配置**：参看*备份设备配置* (p. 47)
   - **复制设备配置**：参看*复制设备配置* (p. 51)

- **组电源控制：**参看 *节点组电源控制* (p. xxii)
- **出口电源控制：**参看 **CC-SG 用户指南**
- **清除日志：**参看*配置日志活动* (p. 185)
- **重新启动设备：**参看*重新启动设备* (p. 52)
- **恢复设备配置：**参看*恢复设备配置* (p. 48)（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. 216)
- **生成所有报告：**参看*报告* (p. 148)

6. 单击 Recurrence（重复执行）选项卡。对于升级设备固件任务，Recurrence（重复执行）选项卡被禁用。
7. 在 Period（周期）字段里单击预定任务执行时段对应的单选按钮。
   a. Once（一次）：用上下箭头选择任务 Start time（开始时间）。
   b. Periodic（定期）：用上下箭头选择任务 Start time（开始时间）。在 Repeat Count（重复次数）字段里输入任务执行次数。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。
   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。如果你希望在从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，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日期所在的月份。
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（再试）选项卡。

10. 如果任务失败，CC-SG 可以根据在 Retry（再试）选项卡上指定的稍后时间再次尝试执行任务。在 Retry count（再试次数）字段里输入 CC-SG 再次尝试执行任务的次数。在 Retry Interval（再试间隔）字段里输入两次再试之间的间隔时间。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，将 Retry Interval（再试间隔）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时，将通知发送到哪个电子邮件地址。默认情况下，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，单击 OK（确定）按钮。默认情况下，如果任务成功，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

可以针对一个设备组里相同类型的多台设备（例如 KX 或 SX）安排一个升级任务。一旦开始升级任务，Reports（报告）> Scheduled Reports（预定报告）菜单就显示 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）选项卡上指定一个选项，可以通过电子邮件发送此报告。

参看《Raritan 用户指南》了解每种设备的预计升级时间。

▶ 安排设备固件升级时间：

1. 选择 Administration（管理）> Tasks（任务）。
2. 单击 New（新建）。
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）标识该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。如果要升级多个类型的设备，必须针对每种类型安排一个升级任务。

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 and Latest Upgrade Start Date/Time（限制升级窗口和最晚升级开始日期/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）启用 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。将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各台设备，单击 Add（添加）按钮将它移动到 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，用箭头按钮将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（再试）选项卡。

   b. Retry Count（再试次数）：输入 CC-SG 针对失败升级再试的次数。

   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 秒、60 秒和 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. 160)。

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. 根据需要更改设置。参看*预定任务* (p. 214)和*预定设备固件升级任务* (参看 "安排设备固件升级时间" p. 216)，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）页面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）按钮。
4. 在打开的 Save As Task（另存任务）窗口上，选项卡自动填充此前配置的任务的信息。
5. 根据需要更改设置。参看*预定任务* (p. 214)和*预定设备固件升级任务* (参看 "安排设备固件升级时间" p. 216)，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

可以将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. 218)。

删除任务

可以删除设备，将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，单击 Delete（删除）按钮。

CommandCenter NOC

将 CommandCenter NOC (CC-NOC) 添加到系统里，可以给串行目标系统和 KVM 目标系统提供监视、报告和提示服务，从而扩大目标管理功能。参看 Raritan CommandCenter NOC 文档，详细了解如何安装和操作 CC-NOC。

如要在 CC-SG 和 CC-NOC 之间建立有效连接，应该同步每个系统上的时间设置。如果要使用 NTP 服务器，必须配置 CC-NOC 和 CC-SG。

添加 CC-NOC

必须给 CC-NOC 管理员提供生成的通行码，由管理员在五分钟内在 CC-NOC 上配置它。避免通过电子邮件或其他电子手段发送通行码，以免被自动化系统截获。在两个互信方之间通过电话或书面方式交换通行码，可以更好地防止通行码被自动截获。

1. 在 Access（访问）菜单上单击 CC-NOC Configuration（CC-NOC 配置）。
2. 单击 Add（添加）按钮。
3. 选择要添加的 CC-NOC 的软件版本，然后单击 Next（下一步）。目前只有 CC-NOC 5.2 or later（CC-NOC 5.2 或更高版本）一个选项。
4. 在 CC-NOC Name（CC-NOC 名称）字段里输入 CC-NOC 的描述性名称。最长为 50 个字母数字字符。
5. 在 CC-NOC IP/Hostname（CC-NOC IP/主机名）字段里输入 CC-NOC 的 IP 地址或主机名。这是必填字段。参看*术语/缩写语* ("术语/缩略语" p. 2)，了解主机名规则。
6. 如要检索 CC-NOC 数据库里的每日目标信息，在 IP Range From（开始 IP 范围）和 IP Range To（结束 IP 范围）字段里输入发现范围。CC-SG 请求 CC-NOC 将此 IP 范围内的设备的事件发送到 CC-SG。此范围与在 CC-NOC 上配置的发现范围相关。参看 Raritan《**CommandCenter NOC 管理员指南**》。在输入范围时，牢记下列规则：

IP 地址范围	说明
如果在此输入的 CC-SG 范围是在 CC-NOC 上配置的范围的子集...	...CC-NOC 返回此范围内的所有已知目标设备信息。
如果在此输入的 CC-SG 范围包括在 CC-NOC 上配置的范围的一部份（非空交集）...	...CC-NOC 返回此相交范围内的所有已知目标设备信息。
如果 CC-SG 范围是在 CC-NOC 上配置的范围的超集...	...CC-NOC 返回此范围内的所有已知目标设备信息。从本质上讲，CC-NOC 返回在 CC-NOC 范围内定义的目标。
如果 CC-SG 范围与在 CC-NOC 上配置的范围不重叠...	...CC-NOC 不返回任何目标设备信息。

注意：用 CC-NOC Synchronization（CC-NOC 同步）报告查看 CC-SG 预定的目标。此报告还显示 CC-NOC 发现的任何新目标。参看 **CC-NOC 同步报告** *(p. 160)。*

7. 指定 Synchronization Time（同步时间），预定何时在 CC-NOC 数据库里检索目标信息。在发现目标或目标不受管理时，刷新数据库。默认值是在客户机上设置的当前时间。你可能要预定一个同步任务在非高峰时间执行，使同步操作不影响其他进程的性能。
8. 在 Heartbeat Interval（检测信号间隔）字段里输入 CC-SG 多久（秒）给 CC-NOC 发送一次检测信号消息。这可以确认 CC-NOC 是否依然运行且可用。默认值是 60 秒。有效范围是 30-120 秒。
9. 在 Failed Heartbeat Attempts（失败检测信号尝试次数）字段里输入在 CC-NOC 节点由于没有响应而被视为不可用之前，必须传输多少个连续检测信号。默认值是 2 个检测信号。有效范围是 2-4 个检测信号。
10. 单击 Next（下一步）按钮。
11. 如果你是 CC-NOC 管理员，在 CC-NOC 字段里输入通行码，或者给 CC-NOC 管理员提交两个通行码。

重要：为了提高安全性，在 CC-SG 生成通行码之后，必须在五分钟内在 CC-NOC 上输入通行码。这可以最大限度地降低入侵者通过暴力攻击系统的机会。采用口头或书面方式交换通行码。

在证书交换过程结束之后，在 CC-SG 和 CC-NOC 之间建立一条安全通道。CC-NOC 数据被复制到 CC-SG 上。单击 OK（确定）按钮完成此过程。如果不在五分钟内完成此过程，就发生超时现象，尚未在 CC-SG 上保存的数据和任何存储证书均被删除。必须重复此过程。

注意：CommandCenter NOC 只能添加到独立 CC-SG 设备或群集 CC-SG 设备的主节点。

编辑 CC-NOC

▶ 编辑 CC-NOC

1. 选择 Access（访问）> CC-NOC Configuration（CC-NOC 配置）。
2. 在列表上选择一个 CC-NOC，单击 Edit（编辑）按钮。
3. 根据需要更改配置。

启动 CC-NOC

▶ 在 CC-SG 上启动 CC-NOC：

1. 选择 Access（访问）> CC-NOC Configuration（CC-NOC 配置）。
2. 在 CC-NOC Configuration（CC-NOC 配置）屏幕上选择一个可用的 CC-NOC。
3. 单击 Launch（启动）。让你连接到配置的 CC-NOC。

删除 CC-NOC

1. 选择 Access（访问）> CC-NOC Configuration（CC-NOC 配置）。
2. 在 CC-SG 上选择要删除的 CC-NOC，单击 Delete（删除）按钮。显示确认消息。
3. 单击 Yes（是）按钮删除 CC-NOC。在删除 CC-NOC 之后，显示一条消息。

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。SSH 只支持设备管理和 CC-SG 管理所用的部分 CC-SG 命令。

SSH 客户机用户由 CC-SG 验证，后者将现有验证和授权策略应用于 SSH 客户机。可供 SSH 客户机使用的命令取决于 SSH 客户机用户所属的用户组的权限。

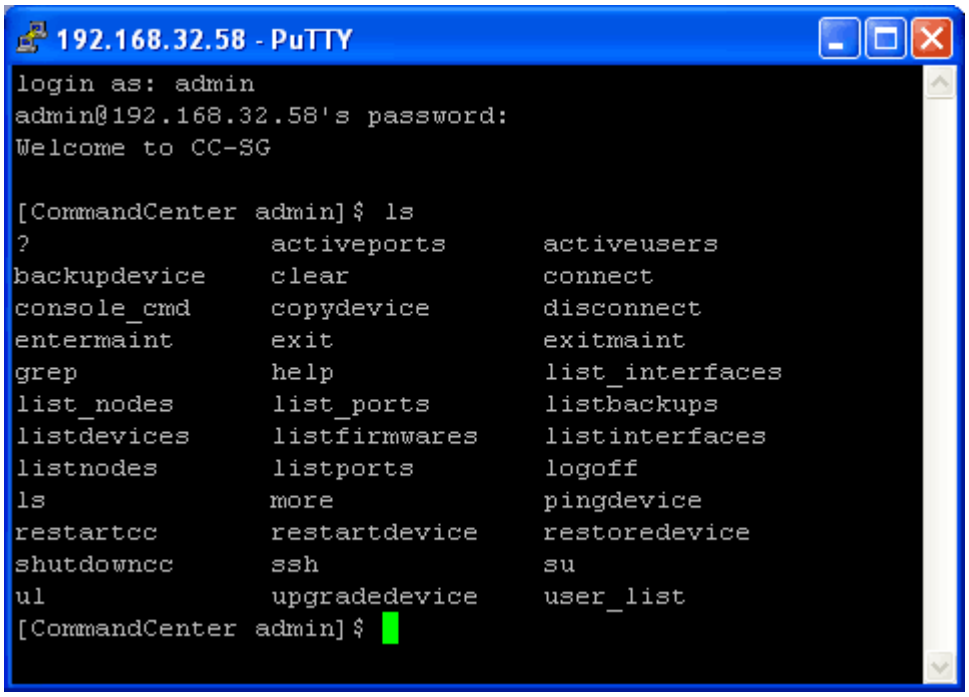
用 SSH 访问 CC-SG 的管理员不能退出 CC Super-User SSH 用户，但可以退出包括管理员在内的其他所有 SSH 客户机用户。

▶ 通过 SSH 访问 CC-SG：

1. 启动 PuTTy 等 SSH 客户机。
2. 指定 CC-SG IP 地址。
3. 指定 SSH 端口号。默认值是 22。可以在安全管理器上配置 SSH 访问端口。参看*安全管理器* (p. 200)。
4. 建立连接。
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，显示所有可用命令。



获取 SSH 命令帮助

可以立刻获取所有命令有限帮助。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. 屏幕显示有关该命令、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. 226)。

▶ **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]>
```

▶ **将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
```

▶ 获取所有命令的帮助：

```
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]]
```

▶ 注销用户：

```
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 `upgradedevice` 等传送 IP 地址的命令，可以用主机名取代 IP 地址。参看*术语/缩写语* ("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，你不一定要使用这部分命令。
- 某些命令由两部分组成，用“或”符号 | 分隔开。

  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	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. 229)，详细了解如何使用换码符和 exit 命令。

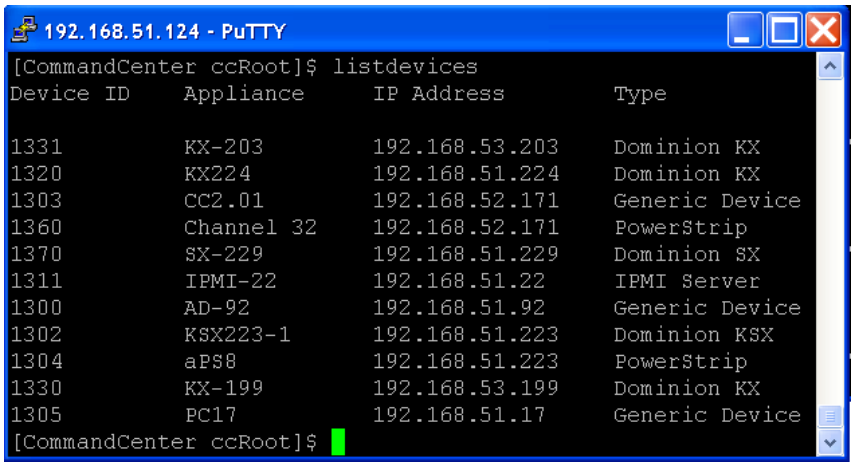
在 Linux 终端或客户机上使用换码符时，可能会出问题。Raritan 建议你在建立端口连接时定义一个新换码符。命令是 `connect [-e <escape_char>] [port_id]`。例如为了在连接端口 2360 时将 "m" 定义为换码符，输入 `connect -e m 2360`。

建立至串行设备的 SSH 连接

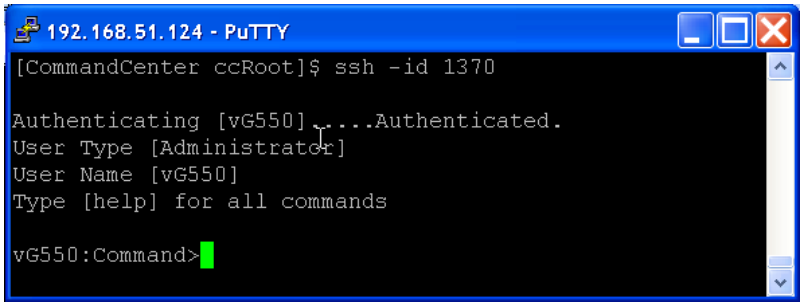
可以建立至串行设备的 SSH 连接，以便对设备执行管理操作。在建立连接之后，可以使用串行设备支持的管理命令。

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。



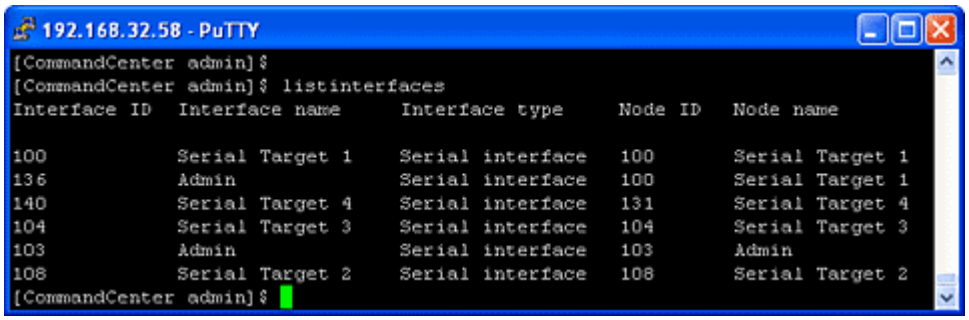
2. 输入 `ssh -id <device_id>` 连接设备。
   以上图为例，可以输入 `ssh -id 1370` 连接 SX-229。



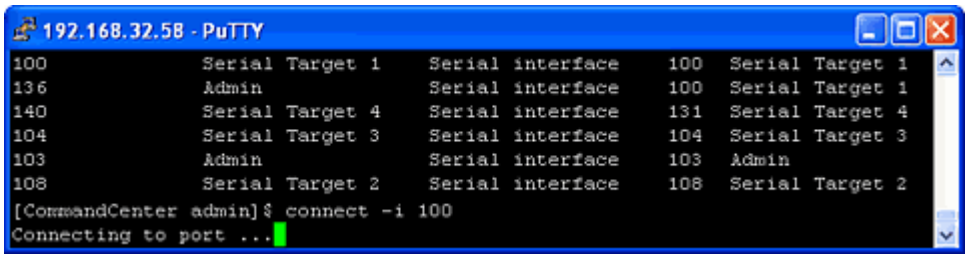
通过带外接口用 SSH 连接节点

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	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。

命令	别名	说明
get_history	gh	获取历史记录。显示在目标服务器上执行的最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 键：

```
exit
```

▶ 终止端口连接、设备连接或节点连接，但保持至 CC-SG 的连接：

可以用换码符终止端口连接、设备连接或节点连接，但保持至 CC-SG 的 SSH 连接。

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 键：

```
~.
```

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 时将 "m" 定义为换码符，输入 connect -e m 2360。

串行管理端口

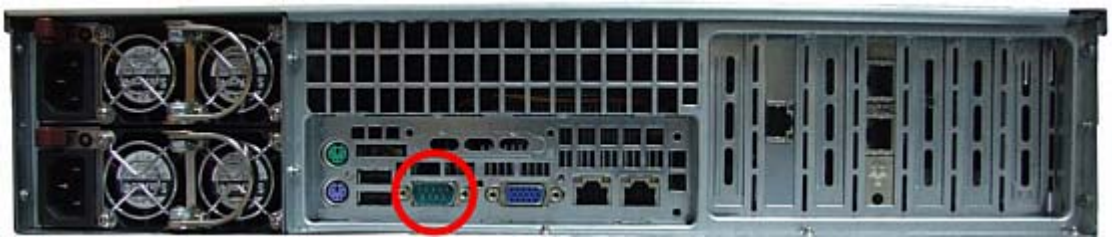
CC-SG 上的串行管理端口可以直接连接 Raritan 串行设备，例如 Dominion SX 或 KSX。

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。

▶ **V1 串行管理端口：**

▶ **E1 串行管理端口：**

- 或者 -



关于终端仿真程序

HyperTerminal 在很多 Windows OS 中提供。HyperTerminal 在 Windows Vista 上不提供。

PuTTY 是一款免费程序，可从 Internet 上下载。

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

目前不能激活 Web 服务应用程序编程接口 (WS API)。参看 http://www.raritan.com/web-services-api，了解有关此功能的最新信息。

你必须接受最终用户协议，才能将 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 SDK 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 > 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）。打开 New Web Services API Configuration（新建 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。
   - 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。
   - Certify Vendor Name（证实供应商名称）：打开 Raritan Vendor Certification（供应商验证）页面。

- Client Application URL（客户机应用程序 URL）：在指定 URL 之后，有一个菜单项允许你在 CC-SG 上访问 Web 服务客户机应用程序。

5. 生成自签名证书。
   a. Encryption Mode（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（专用密钥）：1024 是默认值。
   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。输入完整州名或省名。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（注册公司名称）：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。注册公司名称必须有自己的 CSR 域名。如果注册公司没有自己的域名，签名服务机构拒绝签名请求。
   j. Challenge Password（挑战密码）：最多 64 个字符。
   k. 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。
6. 单击 Generate Certificate（生成证书）。Certificate（证书）字段显示文本。
7. 单击 Save to File（保存到文件）按钮，将证书保存成 .P12 文件。
8. 单击 Add（添加）按钮保存更改。

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. 233)。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. 233)。

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. 234)。
2. Administrator Console（管理员控制台）。参看*关于管理员控制台* (p. 240)。

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 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. 将 VGA 监视器、PS2 键盘和鼠标连接到 CC-SG 设备背板上。
2. 按 Enter 键，屏幕显示 login 提示符。

通过 SSH 访问诊断控制台

1. 在通过网络连接 CC-SG 的客户机 PC 上启动 PuTTY 等 SSH 客户机。
2. 如果 CC-SG 已注册到 DNS 服务器，指定 CC-SG IP 地址或主机名。
3. 指定端口号 23。默认 SSH 端口是 22。如果不将端口更改为 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。
- 状态控制台默认不需要密码。
- 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. 234)。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. 233)。
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。

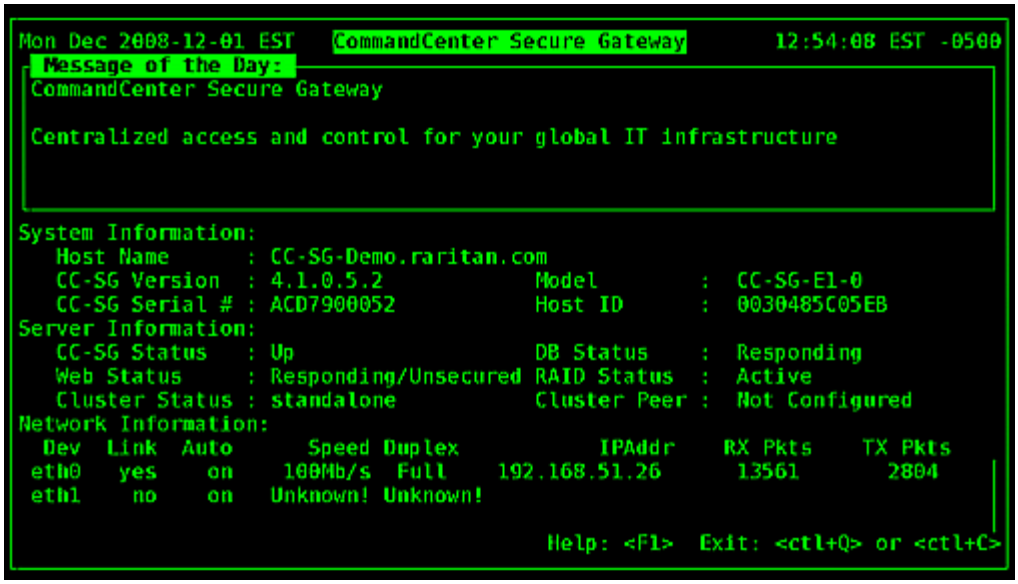
▶ **2: 通过网络浏览器访问状态控制台：**

1. 在支持的网络浏览器上输入此 URL：`http(s)://<IP_address>/status/`，其中 `<IP_address>` 是 CC-SG IP 地址。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。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

在登录提示符下输入 status 之后，打开只读状态控制台。



此屏幕动态显示系统健康状况信息，以及 CC-SG 及其子组件是否正常工作。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
- 近日消息
- 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。每一行最多 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 组件的状态信息。下表说明 CC-SG 和 CC-SG 数据库的信息和状态：

信息	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）	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。

信息	说明	
	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（正在响应/不安全）	Web 服务器正在运行，正在响应 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 将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. 192)。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(网络端口）	对于每个网络接口，有一个可以翻页的表显示其信息。	
	Dev（设备）	接口内部名称。

信息	说明	
	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）	说明是否将自动协商应用于此端口。
	Speed（速度）	此接口的工作速度：10Mbps、100Mbps 或 1000Mbps。
	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（发送的数据包）	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。

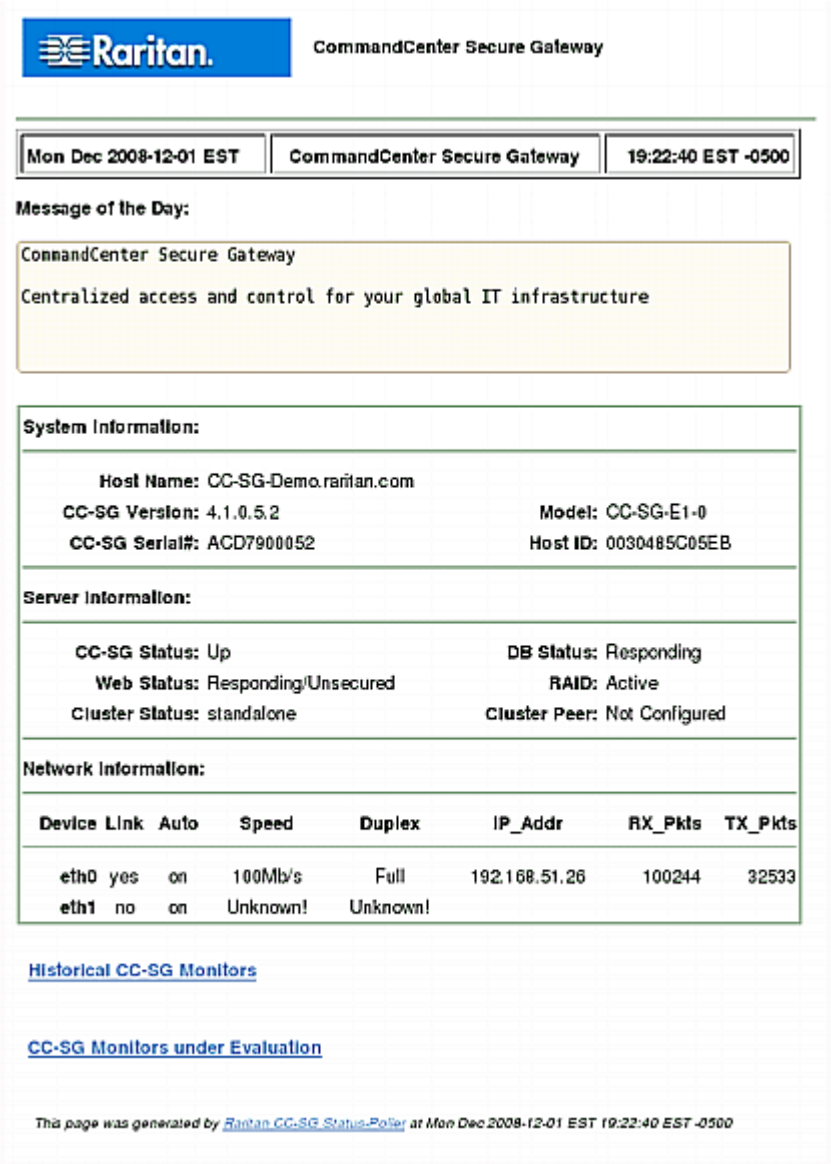
导航键提示

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和退出状态控制台。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 打开帮助屏幕，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。最快可以每秒钟更新一次屏幕。
- 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. 263)和 ***CC-SG 磁盘监视*** (p. 299)。

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：诊断控制台管理员帐号是独立的，不同于在 Java CC-SG Admin Client 和 html Access Client 上使用的 CC Super User 管理员帐号和密码。更改其中一个密码，并不影响另一个密码。

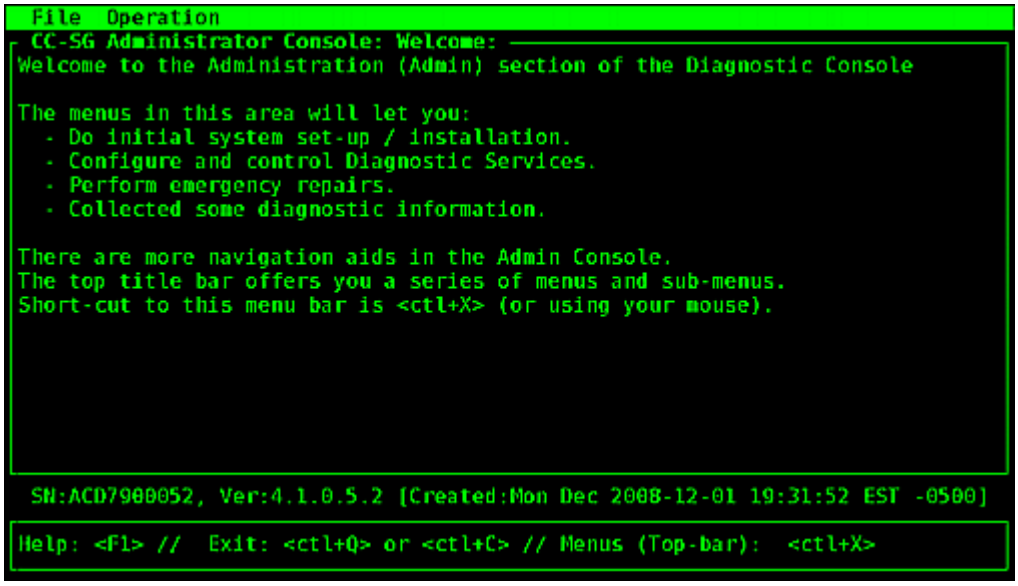
访问管理员控制台

管理员控制台显示的所有信息是静态信息。如果通过 CC-SG GUI 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. 259)，详细了解如何设置密码强度。

打开 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. 242)。

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。

按键	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）。
Tab	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) 或 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 status 或 admin 登录，现场支持人员是否可以通过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 服务不使用该端口即可。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。

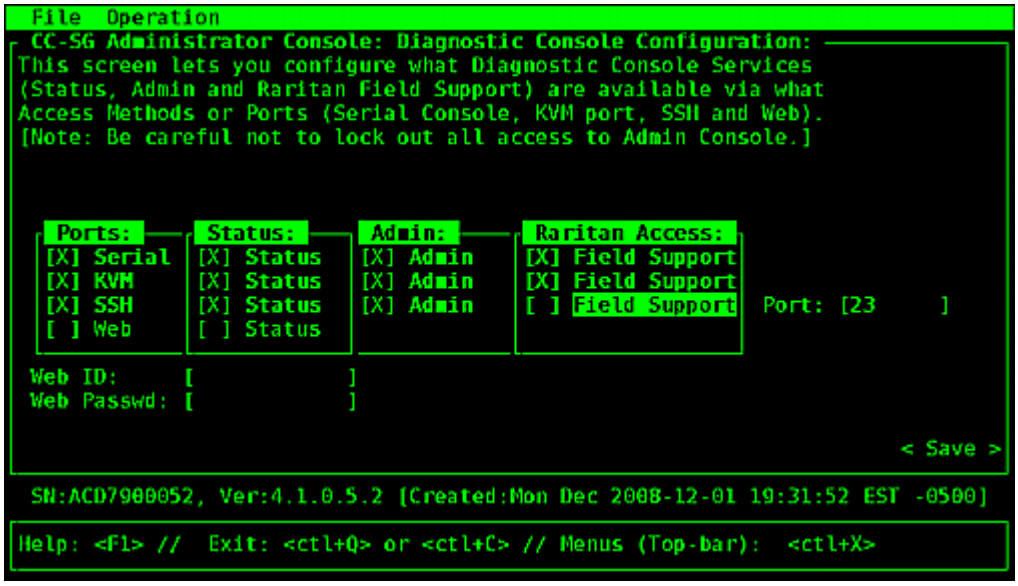
重要：切记不要封锁所有 Admin 访问或现场支持访问。

▶ **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机制：串行端口 (COM1)、KVM 控制台、SSH（IP 网络） 和 Web。诊断控制台有三个服务：状态显示、管理员控制台和 Raritan 现场支持。此屏幕允许你选择通过各种访问机制访问哪些服务。

   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。

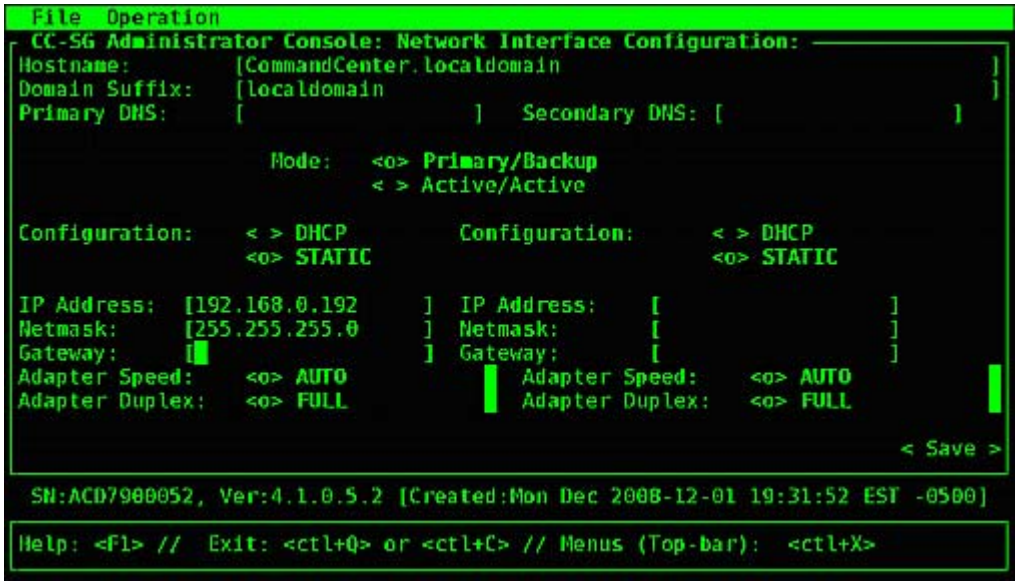


编辑网络接口配置（网络接口）

可以在 Network Interface Configuration（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 GUI (Admin Client) 配置接口。如果要继续配置，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* ("术语/缩略语" p. 2)，了解主机名规则。

4. 在 Mode（模式）字段里选择 Primary/Backup Mode（主/备用模式）或 Active/Active Mode（活动/活动模式）。参看*关于网络设置* (p. 180)。

   - 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 确定接口的 IP 配置，仍然要输入格式正确的 IP 地址和子网掩码。

5. 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 10Mbps、100Mbps 和 1000Mbps 三个值（每次只能看到一个值），用箭头键选择值。按 Space bar 选择显示的选项。对于 1Gbps 线路速度，选择 AUTO（自动）。

6. 如果没有给适配器速度选择 Auto（自动），单击 Adapter Duplex（适配器双工），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，但只有在适配器速度不是 Auto（自动）时才有意义并发生作用。
7. 如果选择了 Active/Active Mode（活动/活动模式），重复这些步骤配置第二个网络接口。
8. 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，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：某些网站明确封锁 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）字段里输入要检查的目标的 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）	不将地址解析成主机名。
Record Route（记录路由）	记录路由。将 IP 记录路由选项设置为开，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。

选项	说明
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 命令执行持续时间(秒)、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。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. 247)。
6. 按 Ctrl+C 终止会话。

注意：按 CTRL+Q 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标要经过的路径。它列出到达目标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）字段里输入要检查的目标的 IP 地址或主机名。
3. 选择：**可选。**

选项	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）	不将地址解析成主机名。

选项	说明
Use ICMP (vs. normal UDP)（使用 ICMP [相对于正常 UDP]）	使用 ICMP ECHO，而不使用 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 目标端口（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）。
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。由于发生 destination reached（到达目标）或 hop count exceeded（超过跳数）事件，在跟踪路由会话终止时，也显示 Return? 提示符。

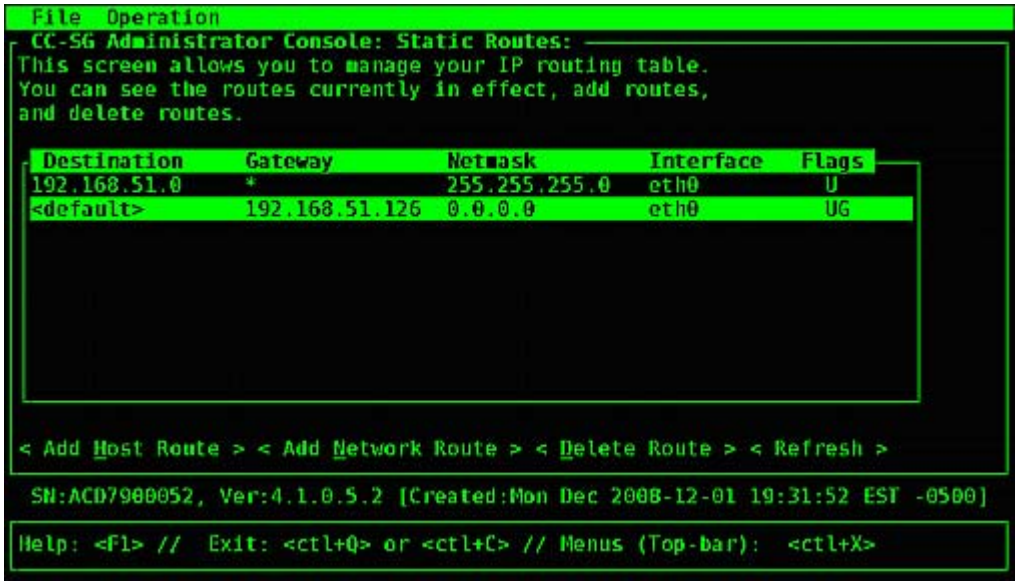
编辑静态路由

可以在 Static Routes（静态路由）上查看当前 IP 路由表，可以修改、添加或删除路由。谨慎使用和替换静态路由，实际上可以有效提高网络性能，这样你可以给重要业务应用程序保留带宽，在每个接口连接一个独立 IP 域的活动/活动网络设置中也可能很有用。参看*关于网络设置* (p. 180)。单击鼠标或者使用 Tab 键和箭头键导航，按 Enter 键选择值。

▶ 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。可以选择 Add Host Route（添加主机路由）或 Add Network Route（添加网络路由），将相关 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。选择 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）接受目标主机 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）与此相类似，但接受目标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）删除该路由。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 LogViewer 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）之后， 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

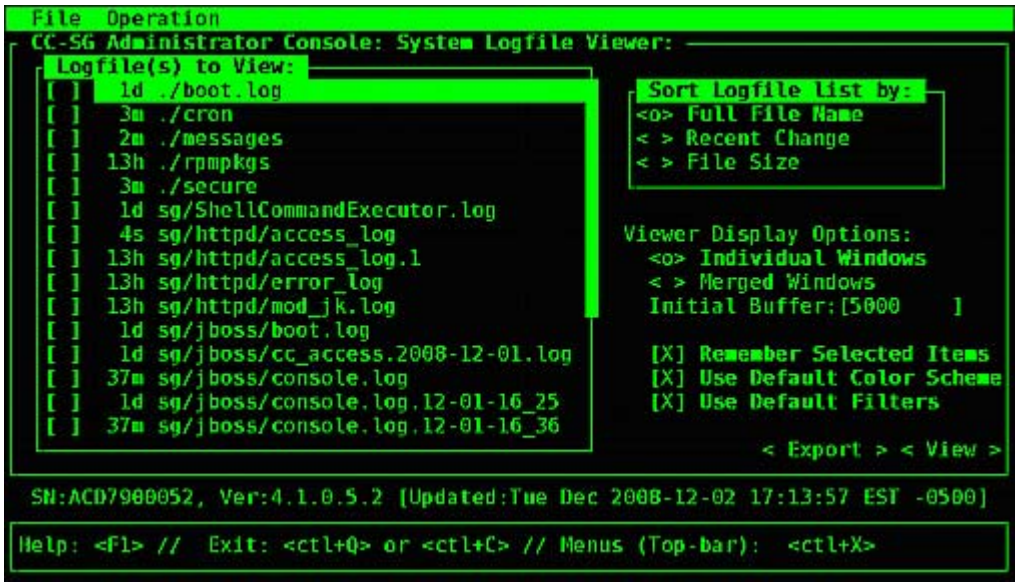
文件大小：

- 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. Logviewer 屏幕分成四个主要部分：
   - 系统上当前可用的 Logfile（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。
   - Logfile List（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 selector（导出/查看选择器）。

3. 单击鼠标或用箭头键移动光标，按 Space bar 选择日志文件，给它标上 X。可以同时查看多个日志文件。



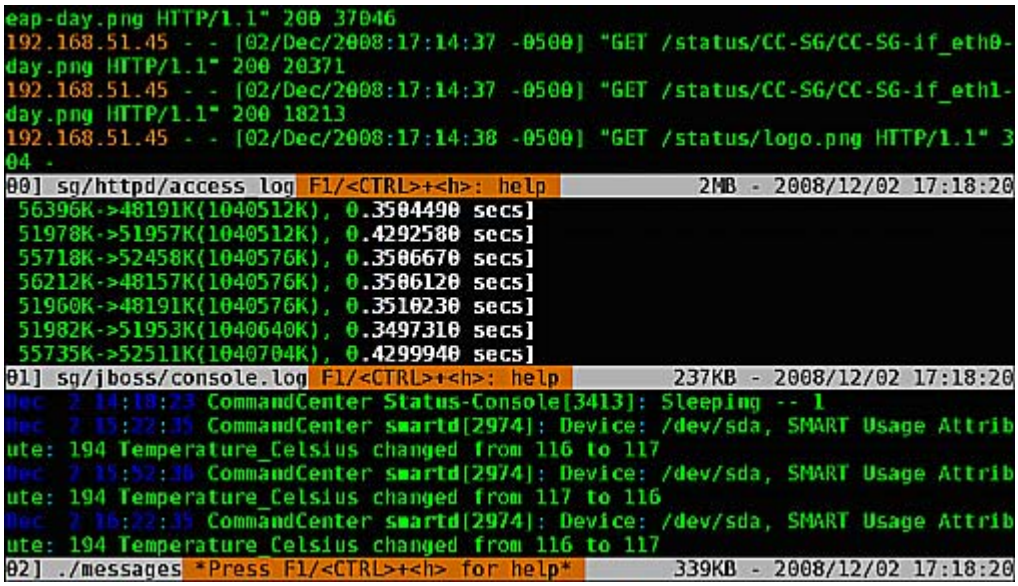
▶ **排序要查看的日志文件列表：**

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。

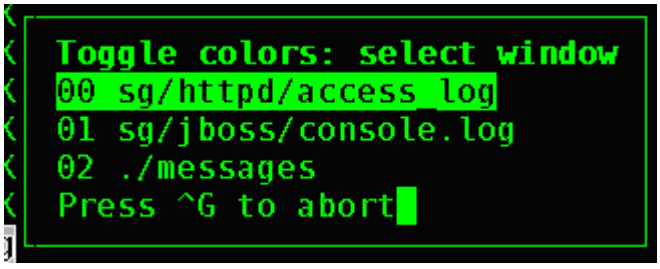
选项	说明
Individual Windows（单独窗口）	用单独的子窗口显示所选的日志。
Merged Windows（合并窗口）	将所选的多个日志合并到一个显示窗口上。
Initial Buffer（初始缓冲区）	设置初始缓冲区或历史记录大小。默认值是 5000。本系统被配置为缓冲接收的所有新信息。
Remember Selected Items（记住选择的项）	如果选择此复选框，将记住当前选择的日志文件（如有）。否则在每次生成新日志文件列表时，复位上次的选择。如果要逐个浏览文件，这很有用。
Use Default Color Scheme（使用默认色彩方案）	如果选择此复选框，在查看部分日志文件时使用标准色彩方案。注意：在查看一个或多个日志文件之后，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。

选项	说明
Export（导出）	此选项将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。
View（查看）	查看选择的日志。

如果在选择 Individual Windows（单独窗口）之后选择 View（查看），LogViewer 显示：



- 在查看日志文件时，按 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。

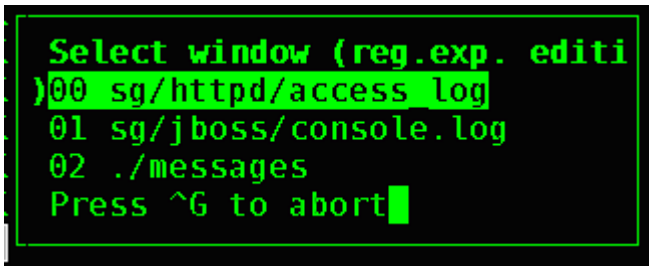


- 输入 I 显示系统信息。

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，可以用 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 添加正则表达式。例如为了显示有关 sg/jboss/console.log 日志文件里 WARN 消息的信息，输入 WARN，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

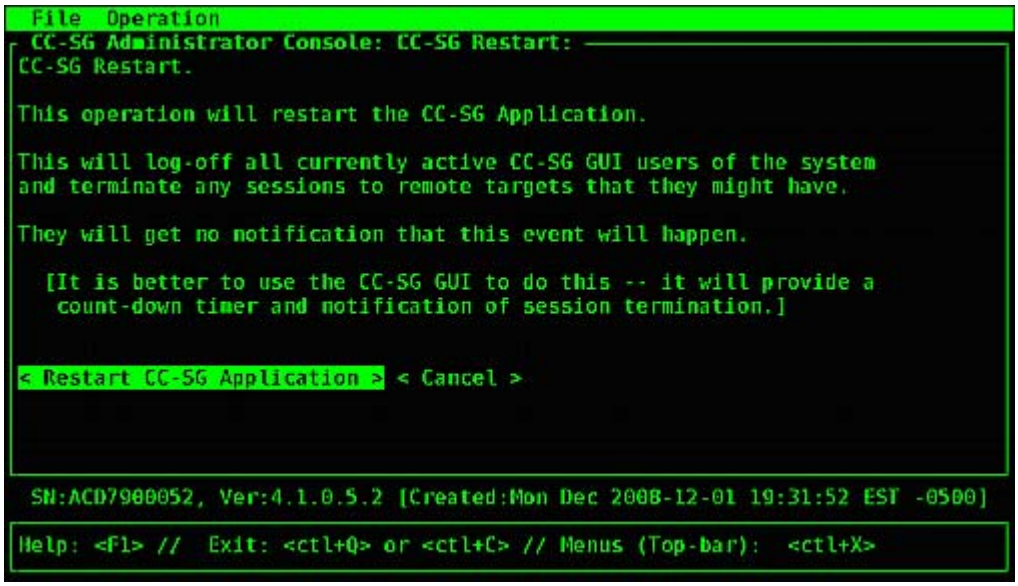
在重新启动 CC-SG 时，退出所有当前 CC-SG 用户，终止他们的远程目标服务器会话。

重要：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. 169)**。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。



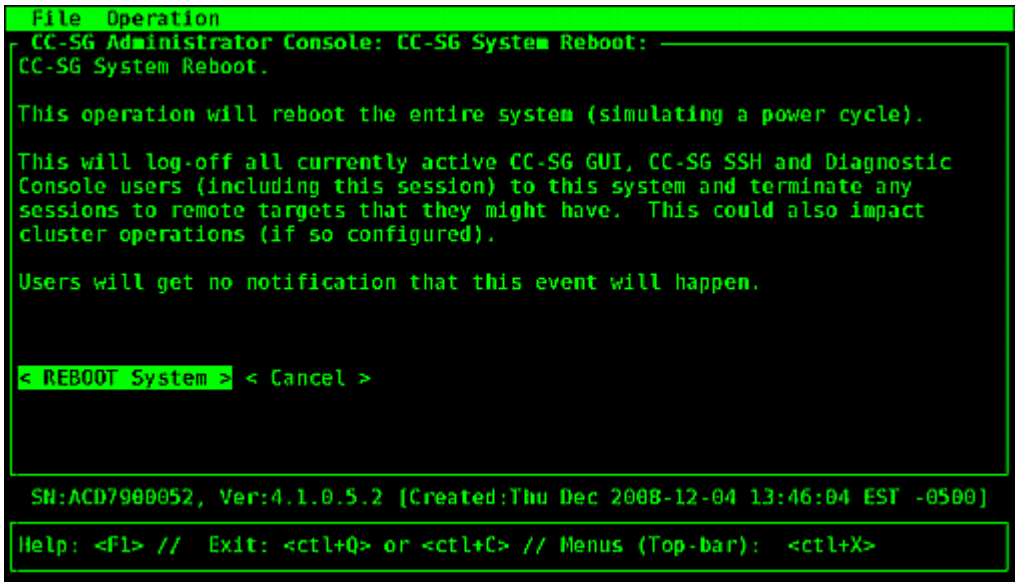
用诊断控制台重新引导 CC-SG

此选项重新引导整个 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。

▶ 重新引导 CC-SG：

1. 选择 Operation（操作）> Admin（管理）> CC-SG System Reboot（CC-SG 系统重新引导）。

2. 单击 REBOOT System（重新引导系统）或按 Enter，重新引导 CC-SG。在下一个屏幕上确认重新引导，继续操作。



在诊断控制台上关闭 CC-SG 系统

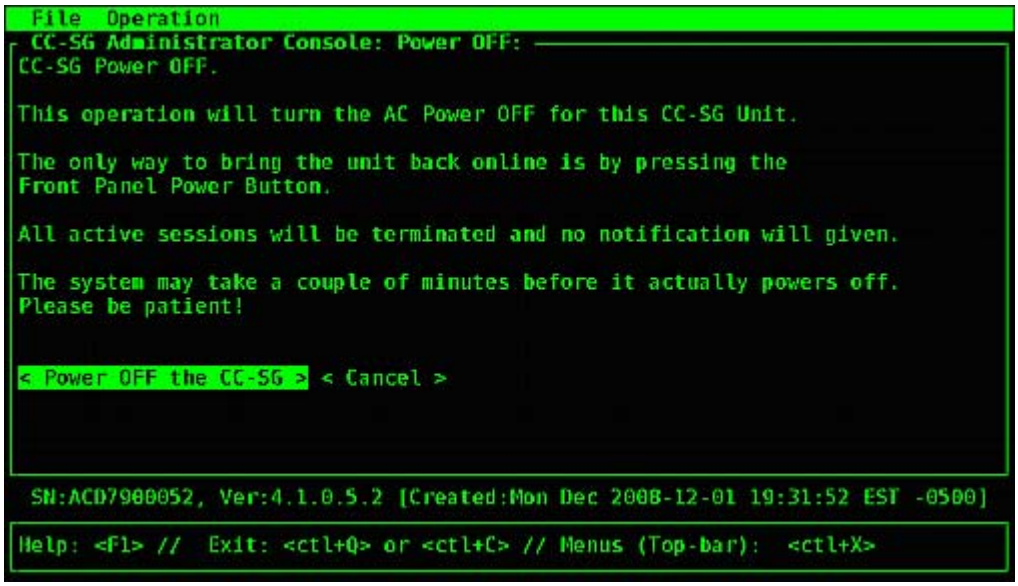
此选项将关闭 CC-SG 设备。登录用户不会收到通知。CC-SG 用户、SSH 用户和诊断控制台用户（包括此会话）被注销。终止所有远程目标服务器连接。

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 Super-User 密码

此选项将 CC Super-User 帐号的密码复位到出厂默认值。

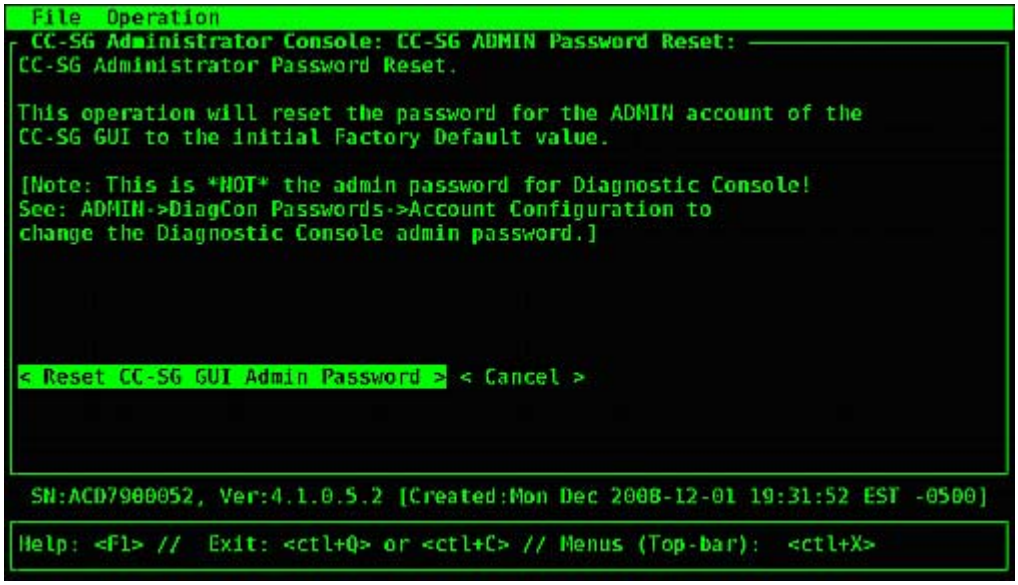
出厂默认密码：raritan

*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. 259)*。

▶ 复位 CC-SG GUI 管理员密码：

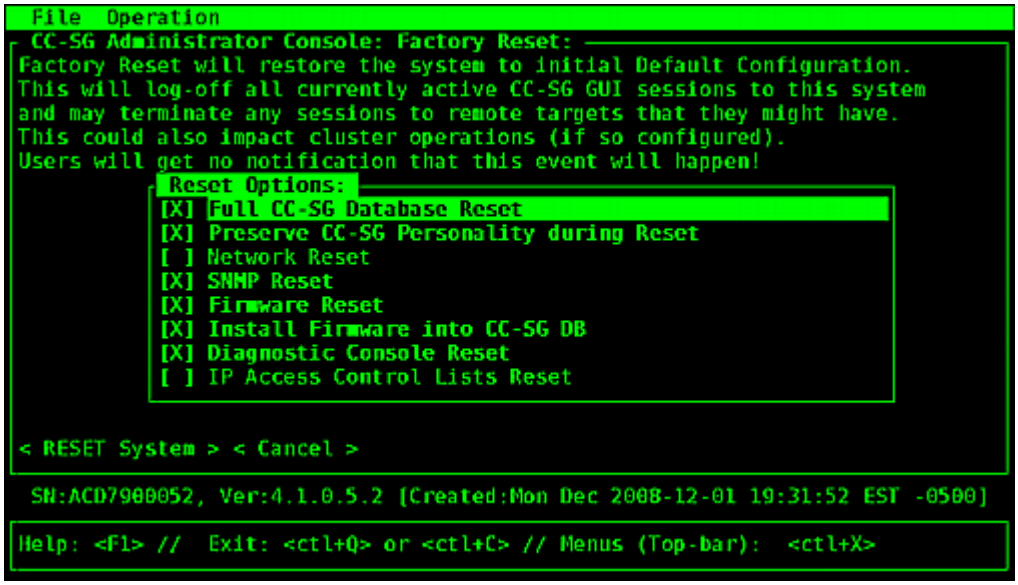
1. 选择 Operation（操作）> Admin（管理）> CC-SG ADMIN Password Reset（CC-SG 管理员密码复位）。

2. 单击 Reset CC-SG GUI Admin Password（复位 CC-SG 管理员密码）或者按 Enter，将管理员密码恢复到出厂默认值。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 (Admin)

此选项将 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，Full Database（全数据库）复位均复位 IP-ACL 设置。 复位时删除邻居配置，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，启用此选项。 在重构 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（PC 客户机和 CC-SG 之间的安全通信） ▪ 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）	此选项将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）：Primary/Backup（主/备用） ▪ 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）

选项	说明
SNMP Reset（SNMP 复位）	此选项将 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） ▪ SNMP Trap Configuration（SNMP 陷阱配置） ▪ SNMP Trap Destinations（SNMP 陷阱目标）
Firmware Reset（固件复位）	此选项将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（将固件安装到 CC-SG 数据库）	此选项将当前 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）	此选项将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，Full Database（全数据库）复位均复位 IP-ACL 设置。 参看 *访问控制表* (p. 210)。

▶ 将 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. 选择 Reset System（复位系统）。
4. 屏幕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。

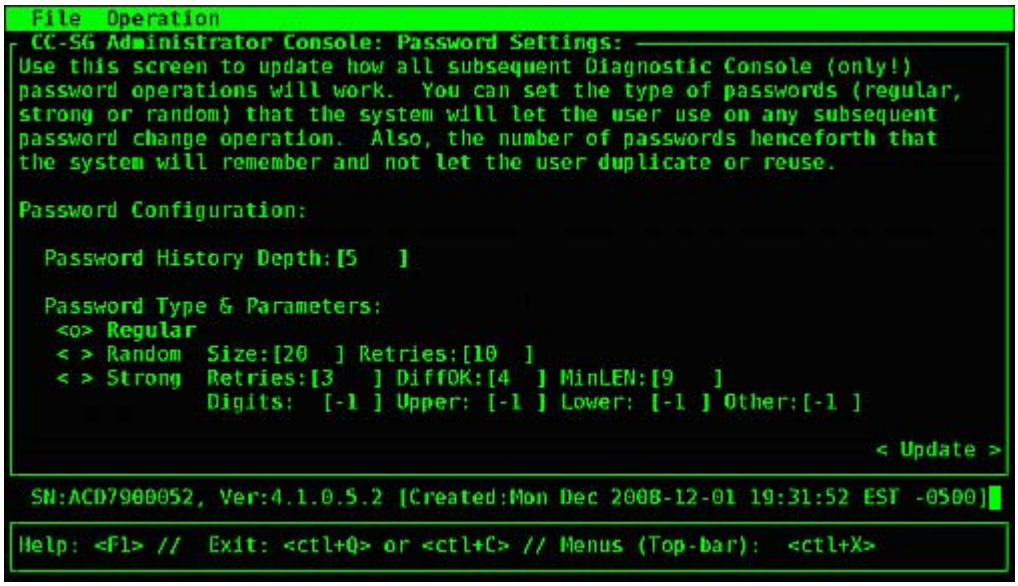
在复位时，切勿切断 CC-SG 电源，切勿给 CC-SG 重新通电，切勿中断 CC-SG，否则可能会丢失 CC-SG 数据。

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，例如设置密码在更改之前最多可以使用的天数（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，不影响常规 CC-SG GUI 帐号或密码。

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 和 status（如启用）密码选择 Regular（正常）、Random（随机）或 Strong（强）。

密码设置	说明
Regular（正常）	这是标准选择。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，最大 70，默认 20）和重试次数（默认 10），后者是询问你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。

密码设置	说明
Strong（强）	强制使用强密码。 Retries（重试次数）是在显示错误消息之前提示你的次数。 DiffOK 表示新密码可以使用旧密码中的多少个字符。 MinLEN 是密码要求的最少字符数。指定密码要求多少位，多少大写字母，多少小写字母和多少其他（特殊）字符。 正数表示此类字符的最大数。 负数表示密码至少要有多少个给定类的字符。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

status 帐号默认不要求密码，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：

- 上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（用于更新这些参数）和给帐号设置的新密码。
- 下部将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：

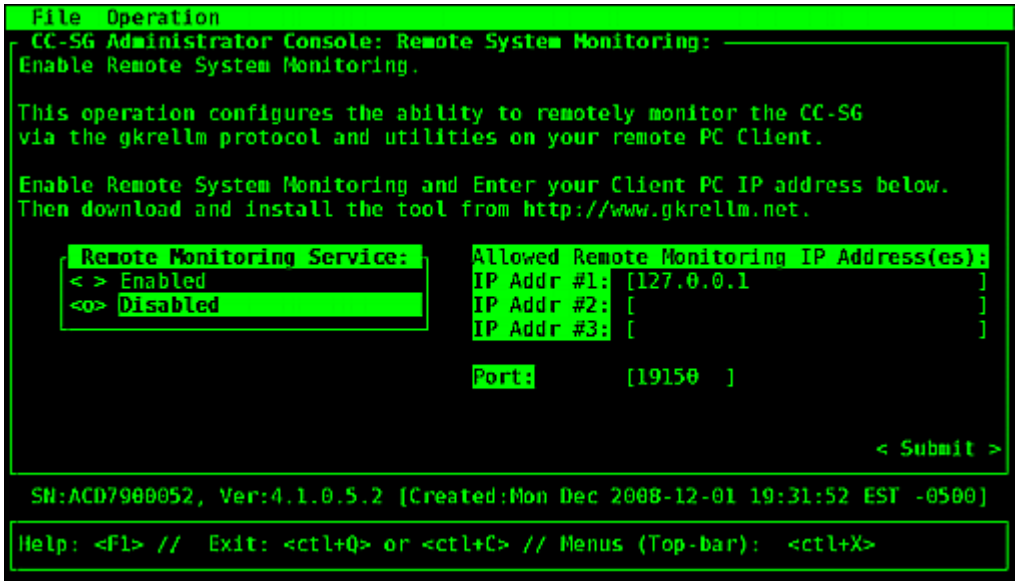
设置	说明
User/User Name（用户/用户名）	（只读）。这是此帐号的当前用户名或 ID。
Last Changed（上次更改日期）	（只读）。这是上次更改此帐号密码的日期。
Expire（到期）	（只读）。这是必须更改此帐号密码的日期。
Mode（模式）	可配置选项：帐号是禁用（不允许登录）、启用（需要验证令牌）还是允许访问但不需要密码。（切勿同时封锁 Admin 和 FS1 帐号，否则不能使用诊断控制台。）
Min Days（最少天数）	两次更改密码间隔的最少天数。默认值是 0。
Max Days（最大天数）	密码最大有效天数。默认值是 99999。
Warning（警告）	在密码到期之前，提前多少天发出警告消息。
Max # of Logins（最大登录数）	帐号允许的最大同时登录数。负数表示没有限制（status 登录的默认值为 -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 登录的默认值是 2）。
UPDATE（更新）	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 任务管理器的性能选项卡。

▶ 1: 给 CC-SG 设备启用远程系统监视：

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 设备的客户机 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。可以更改此端口。
5. 选择 Submit（提交）。

▶ 2: 下载远程系统监视客户机软件：

1. 访问 www.gkrellm.net。
2. 下载并安装与客户机 PC 相适应的软件包。

▶ 3: 配置远程系统监视客户机与 CC-SG 一起工作：

根据 Read Me 文件里的说明，将 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。将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。

▶ 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：

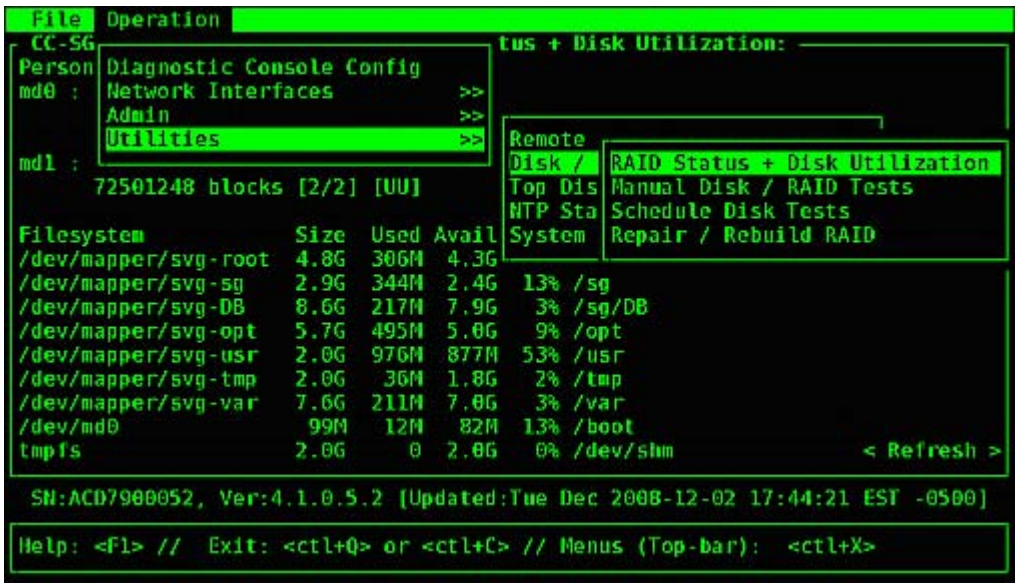
1. 在支持的网络浏览器上输入此 URL：`http(s)://<IP_address>/status/`，其中 `<IP_address>` 是 CC-SG IP 地址。注意必须在 /status 后面加斜杠 (/)，例如 `https://10.20.3.30/status/`。
2. 打开状态页。本页显示的信息与状态控制台显示的信息相同。参看*状态控制台* (p. 234)。
   - 单击 Historical CC-SG Monitors（历史 CC-SG 监视器）链接，查看 CPU 利用率、内存利用率、Java 堆空间和网络流量等信息。单击每个图，在新页面上查看详细信息。

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）按钮或按 Enter，刷新显示信息。在升级或安装时，刷新显示信息特别有用，你可以看到 RAID 磁盘的重构和同步进度。

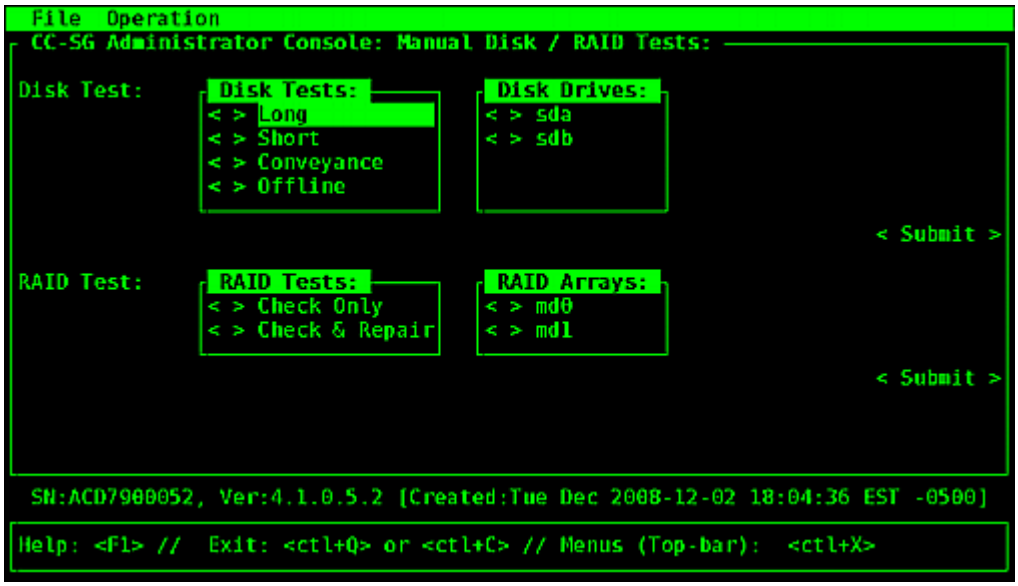
注意：在显示上述屏幕时，表示磁盘驱动器已全面同步，可以使用全 RAID-1 保护。md0 和 md1 阵列的状态都是 [UU]。

测试磁盘或 RAID

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）。
   c. 安排测试时间，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. 268)。
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 阵列是小引导分区，而 md1 阵列是系统的其余部分。
   b. 选择 Submit（提交）。

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. 264)。**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. 268)。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。

安排磁盘测试时间

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. 268)。

在使用 CC-SG 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，建议你不要安排进行频繁测试。

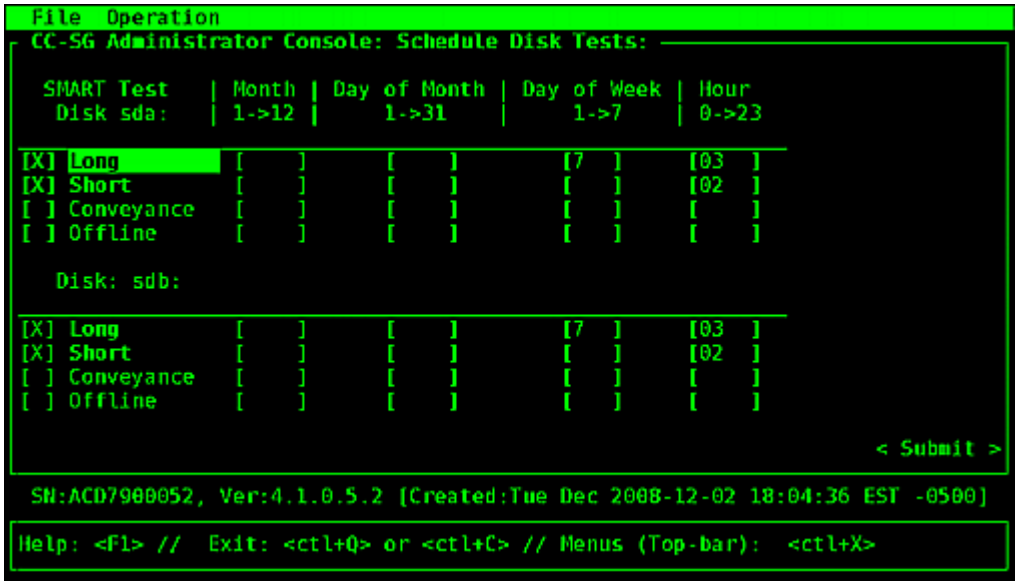
在安排 SMART 测试时间时，切记下列原则：

- 每次只能针对给定驱动器执行一项测试。
- 如果正在测试驱动器，不要安排另一项测试。
- 如果安排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。
- 切勿将 SMART 测试安排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。

▶ 更改磁盘测试时间：

1. 选择 Operation（操作）> Utilities（工具）> Disk/RAID Utilities（磁盘/RAID 工具）> Schedule Disk Tests（安排磁盘测试时间）。



2. 单击鼠标或用箭头键移动光标，按 Space bar 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）。

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。

- 系统正常：

```
File  Operation
CC-SG Administrator Console: Repair / Rebuild RAID:
Disk Drive Status:
 Drive      Health     Attributes Errors     Self Tests Replace??
 sda        OK         OK         OK         OK         No
 sdb        OK         OK         OK         OK         No

            <Health> <Attributes> <Errors>  <Self-Tests> <All>
RAID Array Status:
 Array State                    Events Elements Mis-Match  Rebuild??
 md0   clean                    48     2/2      0         No
 md1   active                   803765 2/2      0         No

                    Potential Operations:
                          < Replace Disk Drive >
                          < Rebuild RAID Array >

SN:ACD8605011, Ver:4.1.0.1.11 [Updated:Wed Dec 2008-12-03 10:50:24 EST -0500]

Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

- 系统不正常，显示存在多个问题：

```
File  Operation
CC-SG Administrator Console: Repair / Rebuild RAID:
Disk Drive Status:
 Drive      Health     Attributes Errors     Self Tests Replace??
 sda        OK         Pre-Fail   Errors     OK         Yes-PreFail
 sdb        OK         OK         Errors     Errors     Yes-Warn

            <Health> <Attributes> <Errors>  <Self-Tests> <All>
RAID Array Status:
 Array State                    Events Elements Mis-Match  Rebuild??
 md0   degraded,clean           6      1/2      0         Yes->sda1
 md1   active                   5      2/2      0         No

                    Potential Operations:
                          < Replace Disk Drive >
                          < Rebuild RAID Array >

SN:ACD7900052, Ver:4.1.0.5.2 [Updated:Tue Dec 2008-12-02 19:58:53 EST -0500]

Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

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 Display（Top 显示）。
2. 查看正在运行的所有进程、休眠进程、停止进程和进程总数。

```
top - 20:46:55 up 1 day,  9:25,  8 users,  load average: 0.27, 0.32, 0.28
Tasks: 149 total,   1 running, 148 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.2%us,  0.3%sy,  0.0%ni, 99.5%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:   4152196k total,  1646716k used,  2505480k free,   608628k buffers
Swap:  2031608k total,        0k used,  2031608k free,   565668k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
19043 sg        25   0 1343m 272m  10m S    0  6.7   2:02.46 java
    1 root      15   0  2060  580  504 S    0  0.0   0:00.91 init
    2 root      RT  -5     0    0    0 S    0  0.0   0:00.64 migration/0
    3 root      34  19     0    0    0 S    0  0.0   0:00.22 ksoftirqd/0
    4 root      RT  -5     0    0    0 S    0  0.0   0:00.00 watchdog/0
    5 root      RT  -5     0    0    0 S    0  0.0   0:49.48 migration/1
    6 root      34  19     0    0    0 S    0  0.0   0:00.27 ksoftirqd/1
    7 root      RT  -5     0    0    0 S    0  0.0   0:00.00 watchdog/1
    8 root      10  -5     0    0    0 S    0  0.0   0:00.84 events/0
    9 root      10  -5     0    0    0 S    0  0.0   0:00.21 events/1
   10 root      10  -5     0    0    0 S    0  0.0   0:03.04 khelper
   11 root      10  -5     0    0    0 S    0  0.0   0:00.00 kthread
   15 root      10  -5     0    0    0 S    0  0.0   0:00.10 kblockd/0
   16 root      10  -5     0    0    0 S    0  0.0   0:00.00 kblockd/1
   17 root      15  -5     0    0    0 S    0  0.0   0:00.00 kacpid
  170 root      15  -5     0    0    0 S    0  0.0   0:00.00 cqueue/0
  171 root      15  -5     0    0    0 S    0  0.0   0:00.00 cqueue/1
```

3. 输入 `h` 查看 top 命令帮助屏幕。F1（帮助）在这里不起作用。

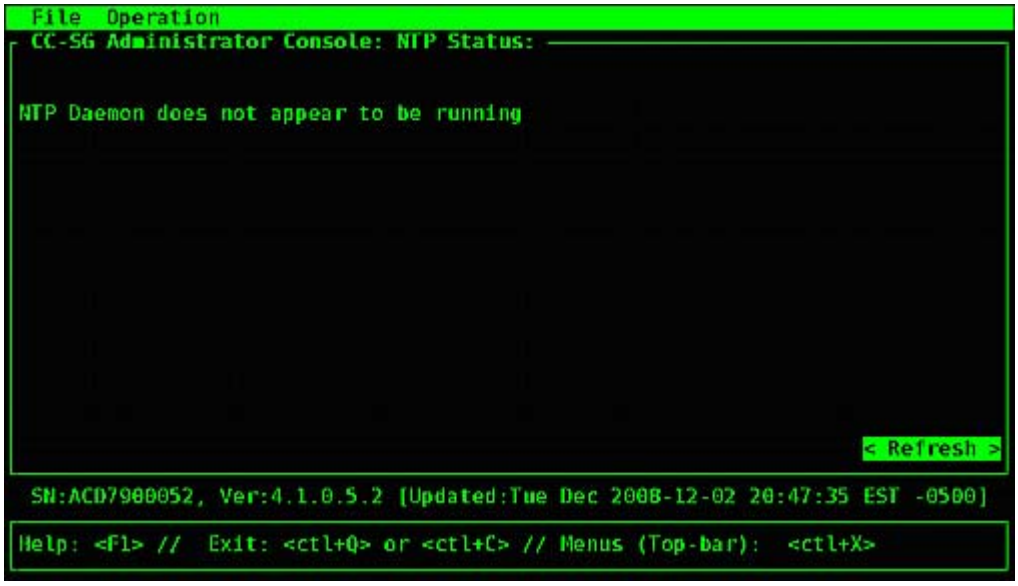
显示 NTP 状态

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 (Admin Client) 上配置。

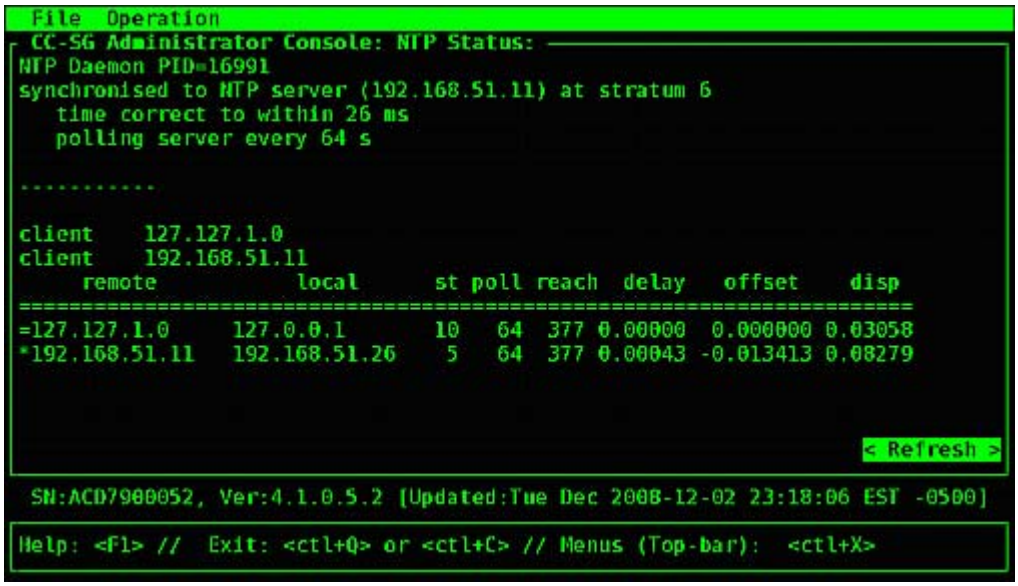
▶ 显示 CC-SG 运行的 NTP 后台进程的状态：

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 Space bar 选择希望的快照选项，给它标上 X。
6. 单击或选择 Submit（提交），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. 在支持的网络浏览器上输入此 URL：`http(s)://<IP_address>/upload/`，其中 `<IP_address>` 是 CC-SG 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管理员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，选择 All Files（所有文件），将它另存为原始文件。

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. ***重新引导 CC-SG*** (参看 "用诊断控制台重新引导 CC-SG" p. 253)。
2. 当它显示下列消息时，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 秒后引导 `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。

A V1 和 E1 规格

在本章内

V1 型号

V1 总体规格

体积	1U
尺寸 (DxWxH)	615 mm x 485 mm x 44 mm (24.21"x 19.09" x 1.75")
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，0.38mm，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	5-55-5 HZ，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)	687 mm x 475 mm x 88 mm (27.05"x 18.7" x 3.46")
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 5g，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

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。本附录协助管理员将 CC-SG 及其组件纳入站点的安全访问策略和路由策略中。

附表列出 CC-SG 及其相关组件所需的协议和端口。

在本章内

CC-SG 网络要求打开的端口：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	SSL/AES-128/AES-256 加密。
8080	TCP	CC-SG 至 PC 客户机	SSL/AES-128/AES-256 加密（如配置）。
2400	TCP	节点访问（代理模式）	不加密。
5000	TCP	节点访问（直连模式）	必须给要在外部访问的 Raritan 设备打开这些端口。只有在访问 CC-SG 时，才需要打开表上的其他端口。 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

端口号	协议	用途	详细信息
51000	TCP	SX 目标访问（直连模式）	AES-128/AES-256 加密（如配置）。

▶ **要求开放的端口可能有例外：**

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任何连接，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：

- 通信各方使用的象征性 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，在端口默认值与其他应用程序的端口发生冲突时或出于安全考虑，你可以将端口号默认值更改成不同的值。
- 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

通信方向	端口号	协议	可配置？	详细信息
CC-SG 到 Dominion PX	623	UDP	否	

CC-SG 群集

在使用可选的 CC-SG 群集功能时，下列端口必须可用于互联子网。如果不使用可选的群集功能，不必打开这些端口。

群集里的每台 CC-SG 可能位于不同的 LAN 上。但设备之间的互联应该非常可靠，不容易发生拥塞现象。

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。
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。必须使用这些端口和协议，CC-SG 才能与这些任选服务器通信。

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

通信方向	端口号	协议	可配置？	详细信息
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 的命令行界面
- 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。 SSL/AES-128/AES-256 加密（如配置）。
PC 客户机到 CLI 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 的另一种重要作用是将 PC 客户机连接到各个节点。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。这叫直连模式。
- PC 客户机通过 CC-SG 连接到节点，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
客户机通过代理到节点模式连接 CC-SG	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 （直连模式）	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 （直连模式）	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

CC-SG 的另一个重要作用是管理第三方设备，例如 iLO/RILOE (HP Integrated Lights Out/Remote Insight Lights Out) 服务器。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。

通信方向	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

通信方向	端口号	协议	可配置？	详细信息
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 将 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执行 SNMP GET/SET 操作。

通信方向	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 和 CC-NOC

CC-NOC 是可与 CC-SG 一起部署的任选设备。CC-NOC 是 Raritan 网络监视设备，用于审计和监视 CC-SG 管理的服务器、设备和 Raritan 设备的状态。

通信方向	端口号	协议	可配置？	详细信息
CC-SG 到 CC-NOC	9443	TCP	否	NOC Web 服务。 SSL/AES128 加密。

CC-SG 内部端口

CC-SG 用几个端口执行内部功能，其本地防火墙功能封锁对这些端口的访问。但是，某些外部扫描器可能将这些端口视为“封锁”或“过滤”。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。

通过启用了 NAT 的防火墙访问 CC-SG

如果防火墙使用 NAT (Network Address Translation) 和使用 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，以便将流量转发到 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. 187)。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，采用通过 RDP 访问节点。

通过 VNC 访问节点

必须打开端口 5800 或 5900，采用通过 VNC 访问节点。

通过 SSH 访问节点

必须打开端口 22，采用通过 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. 262)。

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（退出）	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	
	（Editing users [编辑用户]）	用户管理	通过用户配置文件
	> 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
	（Editing user groups [编辑用户组]）	用户管理	通过用户组配置文件
	> 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		
	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	
	（Editing devices [编辑设备]）	设备、端口和节点管理	通过设备配置文件
	> 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	

菜单 > 子菜单	菜单项	需要的权限	说明
	>> Copy Configuration（复制配置）	设备配置和升级管理	
	> 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，以及节点电源控制	
	> 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	

菜单 > 子菜单	菜单项	需要的权限	说明
	> Port Power Manager（端口电源管理器）	设备、端口和节点管理，节点电源控制	
	> Add Powerstrip（添加 PDU）	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	
	（Editing Nodes [编辑节点]）	设备、端口和节点管理	通过节点配置文件
	Delete Node（删除节点）	设备、端口和节点管理	
	<interfaceName>	节点带内访问或 节点带外访问	
	Disconnect（断开）	下列任何一项： 节点带内访问 节点带外访问 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	

菜单 > 子菜单	菜单项	需要的权限	说明
	Bulk Copy（批量复制）	设备、端口和节点管理	
	Power Control（电源控制）	Power Control（电源控制）	
	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（组电源控制）	Power Control（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（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）	下列任何一项： 设备、端口和节点管理 节点带内访问 节点带外访问或 电源控制	
	> By Node Status（按节点状态）	下列任何一项： 设备、端口和节点管理 节点带内访问 节点带外访问或 节点电源控制	
> Chat（聊天）	> Start Chat Session（开始聊天会话）	节点带内访问 节点带外访问或 节点电源控制	

菜单 > 子菜单	菜单项	需要的权限	说明
	> Show Chat Session（显示聊天会话）	节点带内访问 节点带外访问或 节点电源控制	
	> End Chat Session（结束聊天会话）	节点带内访问 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）	下列任何一项： 设备、端口和节点管理 节点带内访问 节点带外访问或 节点电源控制	
	> Tree View（树视图）	下列任何一项： 设备、端口和节点管理 节点带内访问 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（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	

菜单 > 子菜单	菜单项	需要的权限	说明
	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	
	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	

菜单 > 子菜单	菜单项	需要的权限	说明
	Scheduled Reports（预定报告）	CC 设置和控制	
	CC-NOC Synchronization（CC-NOC 同步）	CC 设置和控制	
Access（访问）			
	CC-NOC Configuration（CC-NOC 配置）	CC 设置和控制	
	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，用户安全管理		
	Guided Setup（指导设置）	下列全部： 设备、端口和节点管理，用户管理，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）	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	

菜单 > 子菜单	菜单项	需要的权限	说明
	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	
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	
	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（视图）		无*	
Window（窗口）		无*	
Help（帮助）		无*	

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 用户登录了。
ccUserLogout	CC-SG 用户退出了。
ccPortConnectionStarted	CC-SG 会话启动了。
ccPortConnectionStopped	CC-SG 会话停止了。
ccPortConnectionTerminated	CC-SG 会话终止了。
ccImageUpgradeStarted	CC-SG 映像升级开始了。
ccImageUpgradeResults	CC-SG 映像升级结果。
ccUserAdded	新用户被添加到 CC-SG 上。
ccUserDeleted	用户从 CC-SG 上删除了。
ccUserModified	CC-SG 用户已被修改了。
ccUserAuthenticationFailure	CC-SG 用户验证失败。
ccLanCardFailure	C-SG 检测到 LAN 网卡发生故障。
ccHardDiskFailure	CC-SG 检测到硬盘发生故障。
ccLeafNodeUnavailable	CC-SG 检测到叶节点连接失败。
ccLeafNodeAvailable	CC-SG 检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 进入了维护模式。
ccExitMaintenanceMode	CC-SG 退出了维护模式。
ccUserLockedOut	CC-SG 用户被封锁了。
ccDeviceAddedAfterCCNOCNotification	在收到 CC-NOC 通知之后，CC-SG 已添加了设备。
ccScheduledTaskExecutionFailure	执行预定任务失败的原因。
ccDiagnosticConsoleLogin	用户登录了 CC-SG 诊断控制台。

SNMP 陷阱	说明
ccDiagnosticConsoleLogout	用户退出了 CC-SG 诊断控制台。
ccNOCAvailable	CC-SG 检测到 CC-NOC 可用。
ccNOCUnavailable	CC-SG 检测到 CC-NOC 不可用。
ccUserGroupAdded	新用户组被添加到 CC-SG 了。
ccUserGroupDeleted	CC-SG 用户组被删除了。
ccUserGroupModified	CC-SG 用户组被修改了。
ccSuperuserNameChanged	CC-SG Superuser 用户名被更改了。
ccSuperuserPasswordChanged	CC-SG Superuser 密码被更改了。
ccLoginBannerChanged	CC-SG 登录横幅被更改了。
ccMOTDChanged	CC-SG 当日消息被更改了。
ccDominionPXReplaced	Dominion PX 设备被另一台 Dominion PX 设备取代了。
ccSystemMonitorNotification	CC-SG 内存用完了。
ccNeighborhoodActivated	CC-SG 邻居被激活了。
ccNeighborhoodUpdated	CC-SG 邻居被更新了。
ccDominionPXFirmwareChanged	Dominion PX 固件版本被更改了。
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。

E 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 浏览器上启用 Java（Sun）。
  - 在控制面板上打开 Java 插件，调节浏览器设置。
- 如果在添加设备时出问题，确定设备的固件版本是否正确。
- 如果设备和 CC-SG 之间的网络接口电缆断开了，等待配置的检测信号时间（分钟），再插好网络接口电缆。在配置的检测信号周期内，设备按单机模式运行，可以通过 RRC、MPC 或 RC 访问。
- 如果显示错误消息，说明客户机版本和服务器版本不一致，且结果无法预测，应该清除浏览器高速缓存和 Java 高速缓存，重新启动浏览器。参看*清除浏览器高速缓存* (p. 171)和*清除 **Java** 高速缓存* (p. 172)。
- 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，然后重新访问该端口。参看*清除浏览器高速缓存* (p. 171)。
- 如果内存用量急剧攀升，或者浏览器会话停止响应你的操作，可能必须给客户机增大 Java 堆大小。
  a. 在控制面板上打开 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. 选择你要运行的当前 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：如果要将 Java 堆大小增加到 300MB，输入 `-Xmx300m`。

F 诊断控制台工具

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: 执行 Memtest86+ 诊断程序：

1. ***重新引导 CC-SG*** (参看 "用诊断控制台重新引导 CC-SG" p. 253)。
2. 当它显示下列消息时，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 秒后引导 `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），按 Enter。
4. CC-SG 加载并执行 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一个夜晚。
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 类型相适应：G1 需要 512M，V1 需要 2048M，E1 需要 4096M。
   - 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。执行 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 执行复位和重新引导操作。

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. 在支持的网络浏览器上输入此 URL：`http(s)://<IP_address>:8080/jmx-console/`，其中 `<IP_address>` 是 CC-SG 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 Super-User 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. 将 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，*制作截屏* (参看 "制作系统快照" p. 272)。

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. 将调试选项的值从 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。

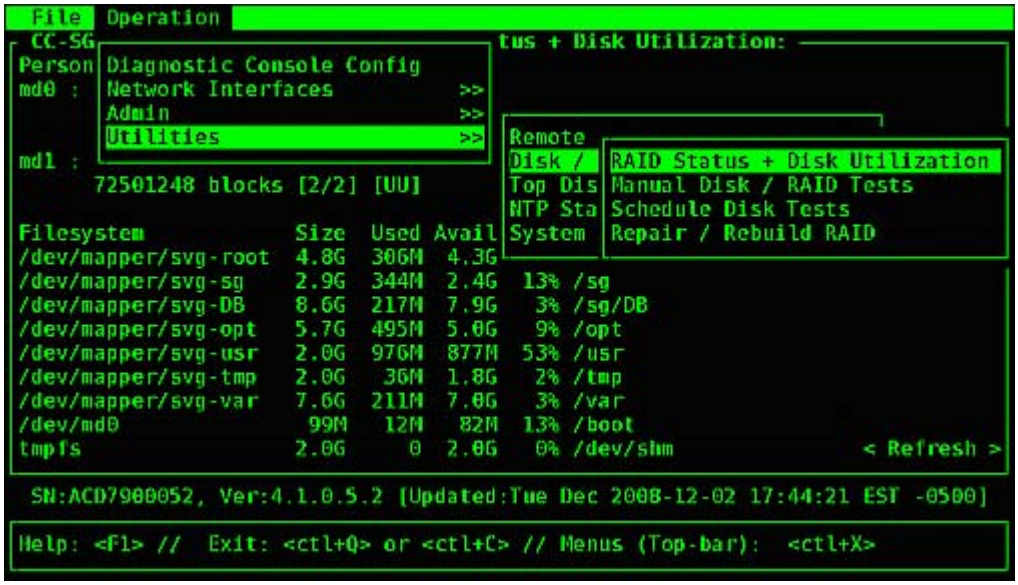
CC-SG 磁盘监视

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. 262)。

重要：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***磁盘状态屏幕*** (参看 "显示 RAID 状态和磁盘利用率" p. 264)。
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%。不同的文件系统包含不同的数据，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

文件系统	数据	纠正措施
/opt	CC-SG 备份和快照	1. 将所有新快照文件保存在远程客户机 PC 上。参看*制作系统快照* (p. 272)了解检索步骤。 2. 进入*系统快照菜单* (参看 "制作系统快照" p. 272)。 3. 选择 Pre-Clean-up SNAP（预清理 SNAP）区域。 4. 选择 Pre-Clean-up UPLOAD（预清理 SNAP）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）。 8. 如果仍然存在空间问题，用 Admin Client 连接 CC-SG，将 CC-SG 备份文件上载到客户机 PC，然后将它们从 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*系统快照菜单* (参看 "制作系统快照" p. 272)。 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）。

▶ 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. 234)。

1. 在支持的网络浏览器上输入此 URL：`http(s)://<IP_address>/status/`，其中 `<IP_address>` 是 CC-SG IP 地址。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。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。

G 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，将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

下列双因素验证组件可与 CC-SG 一起使用。

- Windows Server 2003 上的 RSA RADIUS Server 6.1
- Windows Server 2003 上的 RSA Authentication Manager 6.1
- RSA Secure ID SID700 硬件令牌

旧版 RSA 产品版应该也可以使用 CC-SG，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. 给 CC-SG 创建一个代理主机（类型：Communication Server(通信服务器)）。
6. 创建一个 RADIUS CC-SG 客户机。

双因素认证已知问题

RSA RADIUS 的 New PIN 模式需要一个挑战密码/PIN，将无法工作。相反，在这种方案中的所有用户都必须指定固定密码。

H 常见问题解答

在本章内

一般常见问题解答

问题	答案
一般	
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？	随着部署的数据中心服务器和设备越来越多，管理变得越来越复杂。CC-SG 允许系统管理员或经理在一台设备上访问和管理所有服务器、设备和用户。
什么是 CommandCenter NOC？	CommandCenter NOC 是一种网络监视设备，用于审计和监视通过 CC-SG 访问的服务器、设备和 Raritan 设备的状态。
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 软件更新版本时，能否升级到更新版本？	是。请联系 Raritan 授权销售代表，或者直接联系 Raritan。

问题	答案
CC-SG 可以连接多少节点和/或 Dominion 设备和/或 IP-Reach 设备？	可以连接的节点数、Dominion 数和/或 IP-Reach 设备数没有限制，但实际连接数并不是无限的：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 Microsoft Internet Explorer 是首选网络浏览器，能否优化其性能？	在访问控制台时，如要优化 Microsoft IE 性能，禁用 JIT compiler for virtual machine enabled（启用虚拟主机 JIT 编译器）、Java logging enabled（启用 Java 日志）和 Java console enabled（启用 Java 控制台）选项。在主菜单上选择 Tools（工具）> Internet Options（Internet 选项）> Advanced（高级）。向下滚动找到上面的项目，确保没有选择这些项目。
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 数据库里为你添加了一个新节点。在我的节点树上如何才能看到它？	如要更新节点树并看到新指定的节点，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

问题	答案
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。
在将刀片服务器机箱从一个 KX2 端口移到另一个 KX2 端口之后，CC-SG 是否自动检测并更新刀片服务器机箱配置？	在将刀片服务器机箱移到另一个 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	答案
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。

问题	答案
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（登录到）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（登录到）限制。

安全常见问题解答

问题	答案
安全	
有时在尝试登录时，会显示“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。
有时在工作站闲置一段时间之后，在单击 CC-SG 的任何菜单时，显示“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 同时是内部和外部加密方法吗（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？	不。

问题	答案
CC-SG 是否支持客户机证书请求？	不。

日志常见问题解答

问题	答案
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	答案
性能	
作为 CC-SG 管理员，我添加了 500 多个节点，并将它们全部指定给自己。现在登录 CC-SG 要花很长时间。	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/设置，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	答案
组合	

问题	答案
是否可以将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组，一台设备也可以属于多个组。 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，如果有必要封锁其他所有访问，管理员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，你建议如何处理？例如，将目标服务器上的 CIM 从一个端口物理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？	每个 CIM 有一个序列号和目标系统名称。我们的系统假设在交换机之间移动 CIM 连接时，CIM 仍然与命名目标有关联。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。如果将目标服务器和 CIM 移动到一个未配置的不同端口上，可以在 CC-SG 上配置该端口，自动创建节点。

互通性常见问题解答

问题	答案
互通性	
CC-SG 如何与 Blade Chassis 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 交换机通信协议，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 交换机的功能而定。

问题	答案
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将 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	答案
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	答案
用户体验	
关于通过网络端口或本地串行端口（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，是否会丢失数据？	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。Syslog 将记录此事件，但用户在 CC-SG 控制台上输入的信息会丢失。

I 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

J 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，要遵守最大字符数限制。

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
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
Node Description（节点说明）	160

CC-SG 上的字段	CC-SG 允许的字符数
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
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

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
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

CC-SG 上的字段	CC-SG 允许的字符数
Backup File Description（备份文件说明）	255
Broadcast Message（广播消息）	255

K 诊断控制台引导消息

在 CC-SG v4.0 之前，每当 CC-SG 诊断控制台引导时，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	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 • 操作系统在引导时检查 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 引导时，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，在将 CC-SG 从 3.x 升级到 4.x 时，诊断控制台不显示消息了。

索引

W

一划

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

周一至周五
8 a.m. - 8 p.m.（东部时间）
电话：800-724-8090 或 732-764-8886
有关 CommandCenter NOC：按 6，然后按 1
有关 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
有关所有其他产品的电子邮件：tech@raritan.com

中国

北京

周一至周五
9 a.m. - 6 p.m.（当地时间）
电话：+86-10-88091890

上海

周一至周五
9 a.m. - 6 p.m.（当地时间）
电话：+86-21-5425-2499

广州

周一至周五
9 a.m. - 6 p.m.（当地时间）
电话：+86-20-8755-5561

印度

周一至周五
9 a.m. - 6 p.m.（当地时间）
电话：+91-124-410-7881

日本

周一至周五
9:30 a.m. - 5:30 p.m.（当地时间）
电话：+81-3-3523-5994
电子邮件：support.japan@raritan.com

欧洲

欧洲

周一至周五
8:30 a.m. - 5 p.m. GMT+1（中部欧洲时间）
电话：+31-10-2844040
电子邮件：tech.europe@raritan.com

英国

周一至周五
8:30 a.m. - 5 p.m. GMT+1（中部欧洲时间）
电话：+44-20-7614-77-00

法国

周一至周五
8:30 a.m. - 5 p.m. GMT+1（中部欧洲时间）
电话：+33-1-47-56-20-39

德国

周一至周五
8:30 a.m. - 5 p.m. GMT+1（中部欧洲时间）
电话：+49-20-17-47-98-0

韩国

周一至周五
9 a.m. - 6 p.m.（当地时间）
电话：+82-2-5578730

澳大利亚墨尔本

周一至周五
9:00 a.m. - 6 p.m.（当地时间）
电话：+61-3-9866-6887

台湾

周一至周五
9 a.m. - 6 p.m. GMT-5（标准）GMT-4（夏令时）
电话：+886-2-8919-1333
电子邮件：tech.rap@raritan.com