



Java Desktop System Configuration Manager 发行版 1.1 管理指南

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

文件号码: 819-0955-10
2005 年 2 月

版权所有 2004 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. 保留所有权利。

本产品或文档受版权保护，其使用、复制、发行和反编译均受许可证限制。未经 Sun 及其许可方（如果有）的事先书面许可，不得以任何形式、任何手段复制本产品或文档的任何部分。第三方软件，包括字体技术，均已从 Sun 供应商处获得版权和使用许可。

本产品的某些部分可能是从 Berkeley BSD 系统衍生出来的，并获得了加利福尼亚大学的许可。UNIX 是由 X/Open Company, Ltd. 在美国和其他国家/地区独家许可的注册商标。

Sun、Sun Microsystems、Sun 徽标、docs.sun.com、AnswerBook、AnswerBook2 和 Solaris 是 Sun Microsystems, Inc. 在美国和其他国家/地区的商标或注册商标。所有 SPARC 商标的使用均需获得许可，它们是 SPARC International, Inc. 在美国和其他国家/地区的商标或注册商标。标有 SPARC 商标的产品均基于由 Sun Microsystems, Inc. 开发的体系结构。

OPEN LOOK 和 Sun™ 图形用户界面是 Sun Microsystems, Inc. 为其用户和许可证持有者开发的。Sun 感谢 Xerox 在研究和开发可视或图形用户界面的概念方面为计算机行业所做的开拓性贡献。Sun 已从 Xerox 获得了对 Xerox 图形用户界面的非独占性许可证，该许可证还适用于实现 OPEN LOOK GUI 和在其他方面遵守 Sun 书面许可协议的 Sun 许可证持有者。

本文档按“原样”提供，对所有明示或默示的条件、陈述和担保，包括对适销性、适用性和非侵权性的默示保证，均不承担任何责任，除非此免责声明的适用范围在法律上无效。



050105@10536



目录

序	11
1 概念	13
数据结构	13
生成配置设定	14
策略组	16
2 用法	17
登录	17
▼ 登录 Configuration Manager	17
关于 Java Web Console	18
用户界面	18
报头	19
[浏览] 窗格	20
“用户”选项卡页面	20
搜寻	22
▼ 搜寻实体	22
“主机”选项卡页面	24
策略系统信息库	27
[内容] 窗格	29
“策略”选项卡页面	30
“策略组”选项卡页面	34
“受托者”选项卡页面	35
“角色”选项卡页面	36
“用户”选项卡页面	36
报表	37

▼ 建立报表	37
“报表”窗口	38
退出	39
帮助(H)	39
3 使用命令行界面	41
Configuration Manager CLI 概述	41
使用 CLI	42
调用 CLI 命令	42
CLI 所需的引导信息	42
使用用户名和口令进行验证	42
运行命令	43
表示实体	43
CLI 命令	43
命令摘要	51
A 使用情形	53
背景	53
方案 1 — 防止启动应用程序	53
▼ 锁定应用程序功能	53
方案 2 — 管理分散的配置文件	54
▼ 创建和配置新策略组	54
▼ 为 "Experts" 策略组配置设置	55
方案 3 — 为漫游用户提供解决方案	55
▼ 更改代理设置	55
术语汇编	57

表

表 2-1	策略组操作	28
表 3-1	命令	51
表 3-2	选项	51

图形

图 1-1	树	14
图 1-2	合并	14
图 1-3	保护	15
图 2-1	Configuration Manager 主窗口。	19
图 2-2	[浏览] 窗格	20
图 2-3	“高级筛选”对话框	21
图 2-4	“搜寻”窗口	22
图 2-5	搜寻结果表格	23
图 2-6	“主机”选项卡页面	24
图 2-7	“域树”选项卡页面	25
图 2-8	“高级筛选”窗口	25
图 2-9	“域树”搜寻窗口	26
图 2-10	“策略系统信息库”选项卡	27
图 2-11	“策略组优先级”窗口	29
图 2-12	[内容] 面板	29
图 2-13	“策略”选项卡页面	30
图 2-14	“策略”表格	31
图 2-15	“策略”页面	31
图 2-16	加入新属性	33
图 2-17	“策略组”选项卡页面	34
图 2-18	“受托者”选项卡页面	35
图 2-19	“角色”选项卡页面	36
图 2-20	“用户”选项卡页面	36
图 2-21	“配置报表”对话框	37
图 2-22	“报表”窗口	38

实例

实例 3-1	为实体添加策略组	44
实例 3-2	创建新策略组	45
实例 3-3	删除策略组	45
实例 3-4	导出策略组	46
实例 3-5	导入策略组	47
实例 3-6	列出系统信息库中的策略组	48
实例 3-7	登录	49
实例 3-8	更改策略组的优先级	49
实例 3-9	从实体中删除策略组	50
实例 3-10	重命名策略组	50

序

《Java™ Desktop System Configuration Manager Release 1.1 管理指南》提供有关 Java Desktop System Configuration Manager 的概念和用法的信息。本指南详细介绍了图形用户界面及其功能，还介绍了命令行界面。还介绍了多种使用案例情形，为读者提供常见任务的示例。

本书的组织方式

第 1 章提供 Configuration Manager 的概述。

第 2 章提供有关如何使用 Configuration Manager GUI 的信息。

第 3 章介绍了 Configuration Manager CLI 中使用的命令。

附录 A 提供了常见任务的示例。

术语汇编列出了本书中使用的词汇和短语及它们的定义。

相关书籍

以下书籍提供了有关 Configuration Manager 的其他信息：

- 《Java Desktop System Configuration Manager Release 1.1 Developer Guide》
- 《Java Desktop System Configuration Manager 发行版 1.1 安装指南》

联机访问 Sun 文档

可以通过 docs.sun.comSM Web 站点联机访问 Sun 技术文档。您可以浏览 docs.sun.com 档案或查找某个具体的书的标题或主题。URL 为 <http://docs.sun.com>。

第 1 章

概念

Java™ Desktop System Configuration Manager Release 1.1 是一个工具，可以根据运行桌面应用程序的用户或主机对桌面应用程序的配置设置进行集中管理。Java Desktop System Configuration Manager 允许管理器查看和指定组织层次结构中各元素的配置设置。给定应用程序的一组配置设置称为**配置策略**，可以将这些捆绑在**策略组**中的策略指定给公司组织的某些部分（子组织或用户）或桌面计算机层次结构的某些部分（主机）。

当用户启动桌面会话或由 Configuration Manager 管理的应用程序时，将应用配置策略。系统将检索与运行应用程序的用户或主机相关的所有策略组，这些策略组的设置将与应用程序的本地默认设置和用户的定制设置相集成。策略可以用于为该应用程序提供集中管理的默认设定集合，或用于采用强制设定。

数据结构

Configuration Manager 处理三种不同的层次结构，也称为**树**。要了解 Configuration Manager 用户界面，必须能够区分这三种树：

前两种树为**组织树**和**域树**。组织树表示组织单元（如子组织和用户）之间的关系。树的第一层是组织本身；其下的各层可以是部门及子部门；最后一层是这些部门的成员。域树表示网络元素（如域或主机）之间的关系。树的第一层是整个网络；其下的各层可以是各个子网；最后一层是这些子网中实际存在的计算机。

在 Configuration Manager 中，这些树是通过解释 LDAP 服务器（公司组织结构的典型系统信息库）的内容来获取的。在 LDAP 中，组织树中的一个位置称为一个**实体**。LDAP 服务器中的实体将映射到由 Configuration Manager 识别的组织实体，即“组织”、“角色”、“用户”、“域”和“主机”。有关此过程的详细信息，请参阅《Java Desktop System Configuration Manager 发行版 1.1 安装指南》。

第三种树是**配置策略树**，用于组织配置设定以便于浏览和编辑。该层次结构的第一层通常是应用程序，其下的各层对应于此应用程序的各个组件或模块（以及子组件和子模块），最后一层是实际的配置设定。在处理许多设定（例如 StarSuite™ 或 Mozilla™ 中的设定，其中 HomeUrl 设定可能位于“**首选项**”对话框中的 Mozilla/Navigator/HomeUrl 下）的许多配置系统中都可以看到类似的表示。

可以将配置策略指定给组织结构或域结构中的任何元素，从而形成两个“嵌套树”，一个是包含策略树的组织树，另一个是包含策略树的域树。该结构的图形表示如图 1-1 所示。

Configuration Manager 界面的常规结构允许管理员从组织树或域树中选择某个元素，然后将策略组指定给该元素或编辑该元素的策略。

使用组织树和使用域树的概念是相同的。这两种树之间的主要区别在于组织树由用户组成，而域树由主机组成。将用户和主机放在两个单独的树中可使 **Configuration Manager** 分别提供基于用户的配置和基于主机的配置。由于这两种树之间存在相似之处，因此本文档的大部分章节集中介绍组织树，仅在组织树和域树之间存在差异时才会提到域树。

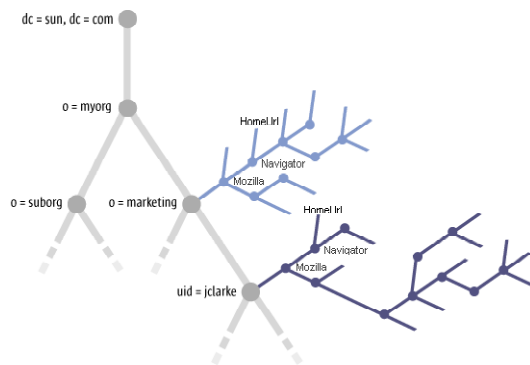


图 1-1 树

生成配置设定

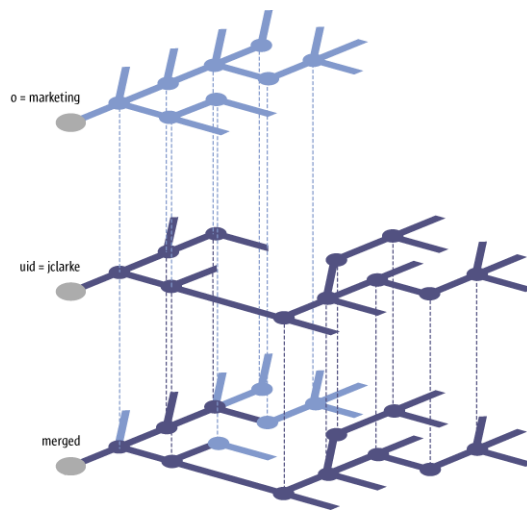


图 1-2 合并

给定实体的配置设定可以通过合并适用于该实体的所有配置策略来获得。这包括实体本身的配置策略以及其父实体的配置策略。例如，用户的设定将包括指定给该用户的策略以及指定给该用户所属组织的策略。合并是按照继承进行的，也就是说，用户继承组织结构的上层级别中指定的设定，这些设定可在用户级别由指定给用户的策略进行修改。图 1-2 说明了此过程。图中显示了 "Marketing" 组织的设定如何被其成员之一、用户 "jclarke" 继承，以及用户 "jclarke" 的策略如何覆盖这些继承的设定中的某些设定。

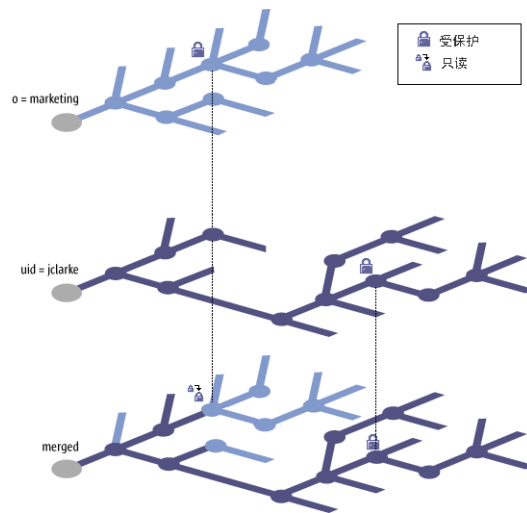


图 1-3 保护

通过保护策略的某些元素可以避免层次结构中较低的层次覆盖继承的设定。这允许管理员定义强制设定，在其下各层策略中或在桌面上运行的被管理的应用程序中无法修改这些强制设定。图 1-3 说明了此过程。图中与 "Marketing" 组织关联的设定是被保护的，因此强制合并将忽略用户 "jclarke" 的策略中指定的值，并提供一个只读值以供在桌面应用程序中使用。

从策略获得的设定按照下列规则与客户机应用程序的本地配置相结合：

- 如果不存在本地用户设定，不受保护的策略设定将用作默认设定。
- 如果不存在本地强制设定，将采用受保护的策略设定。

策略组

管理员可以用以下两种方式为给定的实体设定配置策略：

- 通过为该实体指定策略组。
- 通过修改该实体当前的策略。

策略组是策略的容器，由唯一的名称标识，并且可以通过在 Configuration Manager 中创建指向这些策略组的链接而将它们指定给组织树或域树中的任何实体，从而简化策略的重复使用。策略组可以输入和输出，从而便于维护。

例如，管理员可以创建包含适用于 "Novice" 职员或 "Domain Controller" 主机的设定的策略，将这些策略存储在两个策略组中，然后将这两个策略组指定给符合此说明的组织树或域树中的所有元素。

第 2 章

用法

本章包含有关使用 Java Desktop System Configuration Manager 的信息，其中包括图形用户界面及其功能的说明，还提供了有关如何执行 Configuration Manager 任务的详细信息。

登录

注意 – Configuration Manager 需要 Internet Explorer 5.0 或 Mozilla 1.0 或更高版本。

▼ 登录 Configuration Manager

开始之前 要使用 Configuration Manager，首先要登录 Java™ Web Console。Java Web Console 为访问管理应用程序提供了一个标准登录页面，所有管理应用程序都具有一致的用户界面。

- 步骤**
1. 可通过在浏览器中键入以下 URL 来访问 Java Web Console：
https://<hostname>.<domainname>:6789，其中 <hostname>.<domainname> 是指您在设置过程中指定的服务器名称。例如，
https://myserver.mycompany.com:6789
将显示 Java Web Console“登录”页面，所登录的服务器的名称显示在“用户名”和“口令”文本字段的上方。
 2. 在 Java Web Console“登录”页面中，键入管理员的 LDAP 用户名和口令，然后单击**登录按钮**。
如果验证成功，Java Web Console 将显示会话的开始页面。如果出现登录错误，将返回到“登录”页面并显示错误原因。

3. 单击 **Sun Java™ Desktop System Configuration Manager Release 1.1 链接**。
将启动 Configuration Manager 会话。

注意 – 要在新窗口中启动 Configuration Manager，请在单击该链接之前选定**在新窗口中打开每个应用程序复选框**。

注意 – 要在登录后直接访问 Configuration Manager 应用程序而不经 Java Web Console 的启动页面，请键入安装 Java Web Console 服务器软件的主机的 URL。其中包括主机名、域名、端口和 Configuration Manager 文件名，格式如下：
：`https://<hostname>.<domainname>:6789/apoc`

关于 Java™ Web Console

Java Web Console 旨在为 Sun Microsystems 提供一个通用的、基于 Web 的管理解决方案。Java Web Console 为管理员提供了一个启动管理应用程序的中心位置，所有管理应用程序都具有一致的用户界面。

Java Web Console 基于 Web 模型，允许系统管理员使用浏览器访问管理应用程序。

Java Web Console 具有以下特点：

- 通用的鉴别和授权。
- 通用日志。
- 所有管理应用程序通过基于 HTTPS 的同一端口共用一个入口点。
- 通用的外观。

用户界面

大多数 Configuration Manager 页面的布局都由以下三个窗格组成：

- **标题窗格**（顶部）
- **浏览窗格**（左侧）
- **内容窗格**（右侧）

另外，调出对话框或联机帮助时，将打开独立的浏览器窗口。

报头

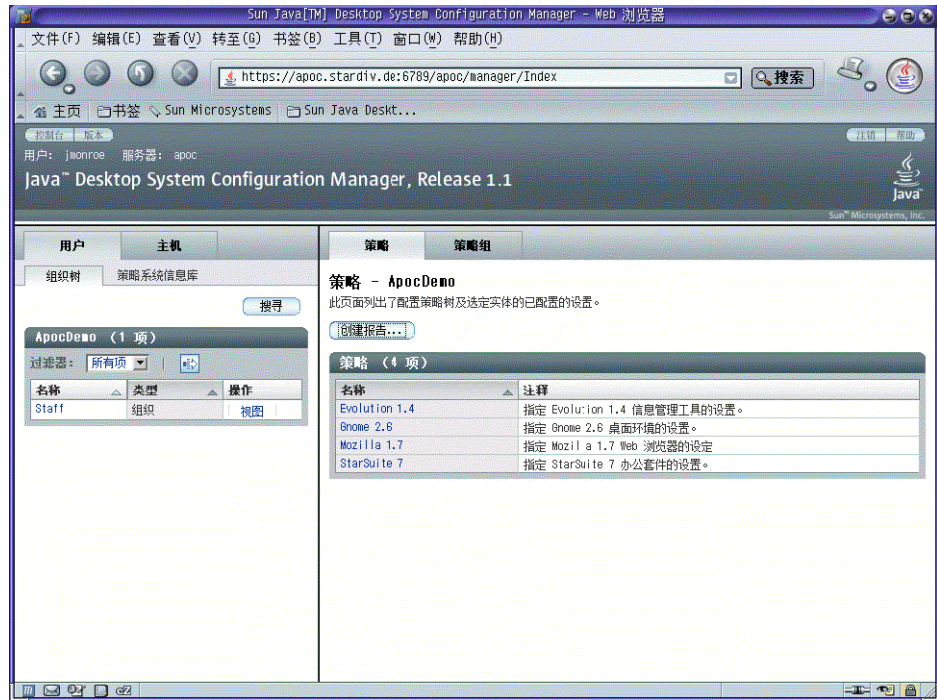


图 2-1 Configuration Manager 主窗口。

报头提供了很多常规链接。标题的上部包括工具栏，其中包括四个链接，从左到右依次为：

- **控制台**链接使您可以返回到 Java Web Console 启动页面。
- **版本**链接可以打开一个窗口，显示 Configuration Manager 的版本信息。
- **注销**链接使您可以退出 Java Web Console 和 Configuration Manager 并返回到“登录”页面。
- **帮助**链接可以打开联机帮助页面。

报头的下部包含：

- 产品名称，即 Sun Java™ Desktop System Configuration Manager Release 1.1。
- 当前登录的管理员的姓名。
- 服务器名称。
- Sun Microsystems 公司徽标。

[浏览] 窗格



图 2-2 [浏览] 窗格

“浏览”窗格允许管理员对“用户”实体树和“主机”实体树执行以下任务：

- 浏览实体树。
- 浏览策略系统信息库。
- 管理策略系统信息库中的策略组。

“浏览”窗格包括两个选项卡页面：**用户**和**主机**。以下各节将详细讨论这些页面。

“用户”选项卡页面

用户选项卡页面允许您浏览组织树并管理组织树的策略组。该页面具有两个子选项卡：**组织树**和**策略系统信息库**。

组织树浏览

可以使用起源路径或浏览表格浏览组织树。

起源路径

起源路径位于**用户**选项卡页面的顶部，它是显示当前实体的路径的区域。每个路径点都是一个链接，一个链接代表一个实体；最后一个链接除外，该链接显示为普通文字，表示当前实体。

要使用起源路径进行浏览，请单击链接。这将更新 [浏览] 面板，使起源路径指向被单击的实体，并且使浏览表格包含该实体的子实体。同时还将更新包含该实体相关联的配置策略数据的 [内容] 面板。

浏览表格

浏览表格位于起源路径的下方，其中列出了当前实体的子实体。“名称”列含有当前实体的所有子实体的名称。“类型”列显示实体的类型。“操作”列包括每行的**查看**链接。


如果实体为组织或者是带有子角色的角色，可以单击列出的相应名称，这将导致下列操作：

- 使选定的子实体成为当前实体。
- 更新 [浏览] 面板，使起源路径指向新的当前实体，并且使浏览表格包含该实体的子实体。
- 更新包含该实体相关联的配置策略的 [内容] 面板。

实体的类型可以是“组织”、“用户”或“角色”。

要在不改变“浏览”窗格中的当前实体的情况下查看列出的实体的详细信息，请单击**查看**链接。此操作将使选定行的背景颜色更改为蓝色，并更新包含选定实体相关联的数据的 [内容] 面板。

蓝色背景的行标记的是其数据当前显示在 [内容] 面板中的实体。

浏览表格的顶部包括筛选下拉式菜单和高级筛选图标。有关详细信息，请参阅第 21 页“高级筛选”。当该表格包含的条目数超过十个时，将显示页面/滚动查看所有数据图标 ，使您可以更改表格条目的视图。

筛选下拉式菜单允许您选择要在浏览表格中显示的实体类型。其中包含以下选项：

- “所有项”将在浏览表格中显示所有类型的实体。
- “组织”仅在浏览表格中显示类型为“组织”的实体。
- “用户”仅在浏览表格中显示类型为“用户”的实体。
- “角色”仅在浏览表格中显示类型为“角色”的实体。


高级筛选



图 2-3 “高级筛选”对话框

“高级筛选”功能使管理员可以定义要显示的实体类型。

▼ 使用“高级筛选”对话框

- 步骤
1. 单击浏览表格顶部的高级筛选图标  打开该对话框。
 2. 在类型部分中，选择要筛选的实体类型。要进行更具体的筛选，请在名称文本字段中键入一个名称。

注意 – 可以在名称文本字段中使用星号 "*" 通配符。

3. 单击该对话框底部的筛选按钮运行筛选。

搜寻

此功能使管理员可以在组织树中搜寻某些实体类型和实体名称。

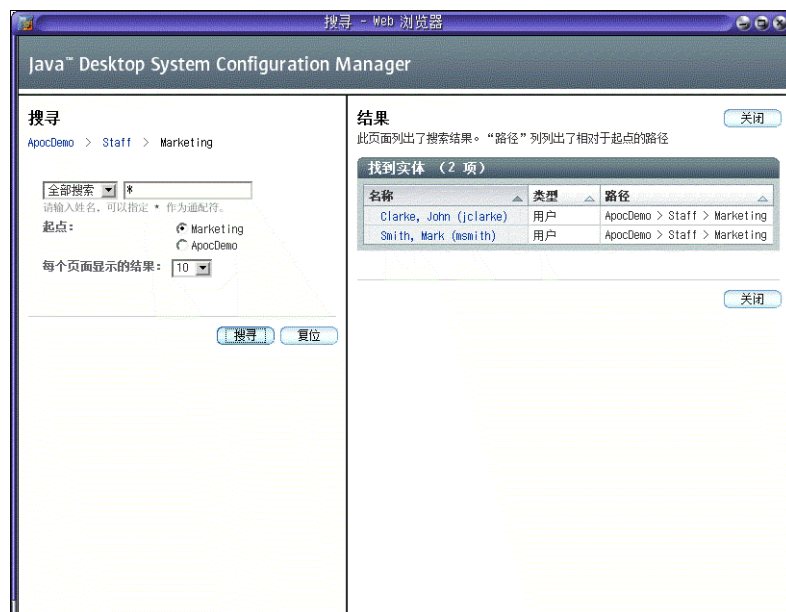


图 2-4 “搜寻”窗口

▼ 搜寻实体

- 步骤
1. 单击“浏览”窗格中的搜寻按钮。
将打开“搜寻”窗口。该窗口包含报头、参数区域（左侧）以及结果区域（右侧）。参数区域在顶部显示当前实体的起源路径。

注意 – 如果已在后台打开“搜寻”窗口，单击主窗口的“浏览”面板中的搜寻按钮将使“搜寻”窗口显示在最前端。“搜寻”窗口的当前实体 (“搜寻”窗口的参数区域中的起源路径显示的实体) 将更新。其他所有参数和结果区域的内容不变。

2. 从起源路径下的列表框中选择所需的实体类型。

要搜寻特定实体类型，请在起源路径下方的下拉式列表中选择该类型。可用的选择包括：

- 全部搜寻
- 搜寻组织
- 搜寻用户
- 搜寻角色
- 搜寻域
- 搜寻主机

3. 要进一步缩小种类结果的范围，请在每个种类类型的可用搜寻字段中键入相应的字符串。

筛选字符串的默认值是“*”，表示“全部”。在搜寻字段键入的字符串中，星号可以作为通配符使用。

注意 – 搜寻功能不区分大小写。

4. 从起始点部分选择一个选项，以决定搜寻的起始点。

所有选择均对组织树进行深度搜寻。不同之处在于搜寻的起始点。从根位置搜寻是从组织树的顶端开始搜寻，而从其他位置搜寻是从组织树的相应位置开始搜寻。

单击起源路径中的任何路径点将使搜寻的当前位置更改到选定实体。

5. 从“结果”中选择要在每个页面列表框中显示的结果数目。

6. 单击搜寻按钮。

一旦搜寻完成，结果区域将显示包含搜寻结果的表格。

7. 要开始另一个搜寻或清除当前的搜寻参数，请单击参数区域中的“重设”按钮。

处理搜寻结果



图 2-5 搜寻结果表格

执行搜寻后，结果表格将显示在“搜寻”窗口的结果区域中。该表格含有三列：

- “名称”列显示实体的名称。
- “类型”列显示实体的类型。
- “路径”列显示实体的路径。该路径是相对于搜寻起始点的路径。

如果搜寻的实体类型为“用户”，结果表格中将出现第四列，即“用户 ID”。

注意 – 可以通过单击相应列标题旁边的箭头来对结果进行排序。例如，要按类型排序，请单击“类型”列旁边的箭头。

要查看结果，请单击“名称”列中对应的名称。这将使 Configuration Manager 主窗口显示在最前端。“内容”窗格将显示该实体所关联的配置策略。“浏览”窗格中也将以蓝色突出显示该实体。

“主机”选项卡页面



图 2-6 “主机”选项卡页面

与主机选项卡页面上列出的实体关联的配置设置将被用于基于主机的配置。

在客户端，基于用户的配置设置是根据用户名从组织树中获取的。基于主机的配置设置是根据用户当前所在的主机的 IP 地址或主机名从域树中获取的。

通过提供基于主机的配置设定，可以轻松地配置依赖于网络环境的设定。典型的情形是，漫游用户具有基于用户的配置，但是仍然可以使用优化的代理配置（取决于该用户当前所在的主机）。

主机选项卡页面包括两个子选项卡，分别称为**域树**和**策略系统信息库**。

“域树”选项卡页面



图 2-7 “域树”选项卡页面

域树显示用户当前所在主机的配置设置。默认情况下，单击**主机**选项卡时将打开域树。

域树中的浏览方式与组织树中的浏览方式相同。有关详细信息，请参阅第 20 页“[组织树浏览](#)”。

域树浏览表格的操作栏中包括**筛选**下拉式菜单，其中提供了以下菜单项：

- “所有项”显示所有类型的实体。
- “域”显示类型为“域”的实体。
- “主机”显示类型为“主机”的实体。

操作栏中还包括**高级筛选**图标，如第 25 页“[高级筛选 - 主机页面](#)”所述。

高级筛选 - 主机页面



图 2-8 “高级筛选”窗口

单击域树浏览表格的操作栏中的高级筛选图标将打开“高级筛选”窗口。它的使用方式与组织树的高级筛选相同。请参阅第 21 页“高级筛选”。域树的高级筛选提供了“域”和“主机”实体类型以供筛选。

域树搜寻

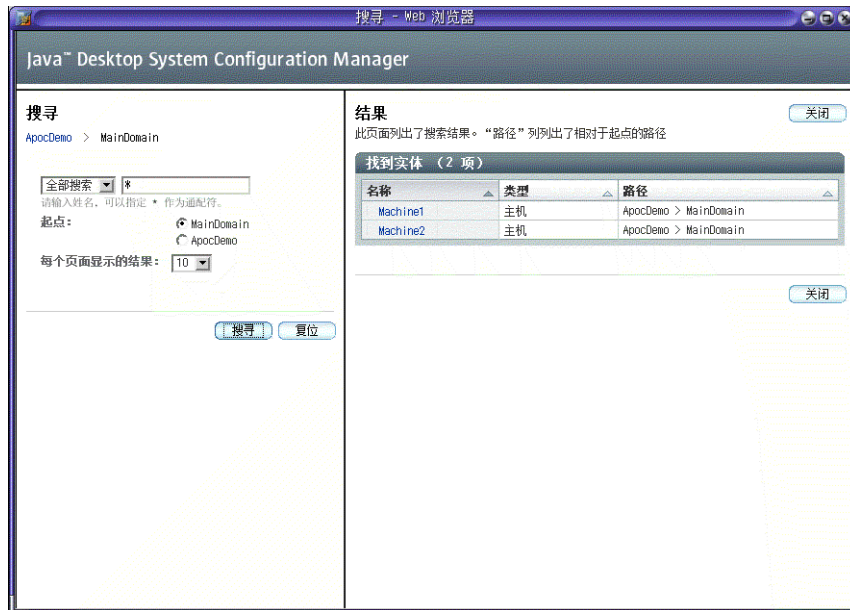


图 2-9 “域树”搜寻窗口

单击域树选项卡中的搜寻按钮时，将显示“域搜寻”窗口。“域搜寻”的操作方式与在组织树中进行搜寻的操作方式相同。有关详细信息，请参阅第 22 页“搜寻”。

策略系统信息库



图 2-10 “策略系统信息库”选项卡

用户选项卡和主机选项卡下都有一个策略系统信息库选项卡。

策略系统信息库是用户策略组或主机策略组的容器。策略组被组织成一个经过排序的列表。顺序由优先级定义。

策略组表格

策略组表格位于页面顶端，其中列出了各个策略组。该表格含有三列：选择列、“名称”列和“优先级”列。请参阅图 2-10。

“选择”列用于标记要应用**策略组操作**下拉式菜单中列出的操作的行。

浏览策略组

要浏览某个策略组，请在“名称”列中单击该策略组的名称。此操作将使选定行的背景颜色更改为蓝色，并更新包含选定策略组相关联的数据的 [内容] 面板。

“优先级”列含有策略组的优先级。当管理员将多个策略组与实体相关联时，将根据此优先级定义策略组的合并顺序。

蓝色背景的行标记的是当前在 [内容] 面板中可查看其数据的策略组。

策略组操作栏

策略组操作下拉式菜单包含以下操作：

表 2-1 策略组操作

名称	操作
新增	将打开对话框窗口，管理员可以在其中输入策略组的（唯一）名称。单击“确定”后，将添加该策略组，并更新 [浏览] 窗格以反映此更改。
删除	将打开弹出式窗口，其中显示用于确认策略组删除操作的警告消息。如果管理员单击“确定”，将删除该策略组，并更新 [浏览] 窗格以反映此更改。
重命名	将打开对话框窗口，管理员可以在其中输入策略组的新（唯一）名称，这将重命名策略组，并更新“浏览”窗格以反映此更改。
编辑优先级	将打开对话框窗口，其中含有用于更改优先级的列表框。
导出	将打开对话框窗口。管理员可以在其中输入要将选定策略组导出到的目标路径。
导入	将打开对话框窗口。管理员可以选择要导入的策略组。单击“确定”，将加入该策略组并更新 [浏览] 窗格以反映此更改。

策略组优先级

有了策略组优先级的概念，您就可以定义合并分层的顺序。如果为实体指定了多个策略组，在合并过程中会使用策略组优先级。在此例中，实体的层次结构不足以确定合并策略组的顺序。而通过为策略组指定优先级则可以解决此问题。

要打开“策略组优先级”对话框，请从**策略组操作**下拉式菜单中选择编辑优先级。



图 2-11 “策略组优先级”窗口

▼ 提高或降低策略组优先级的步骤

- 步骤
1. 从列表中选择策略组。
 2. 单击上移或下移按钮提高或降低优先级。

[内容] 窗格



图 2-12 [内容] 面板

[内容] 面板显示与 [浏览] 面板中选定的实体或策略组相关联的数据。数据被分组到选项卡页面中，通过单击 [内容] 面板顶端的相应选项卡可以访问这些页面。[浏览] 面板中的选择将决定 [内容] 面板中显示的选项卡的编号和类型。

策略选项卡页面是默认的活动选项卡页面。如果在 [浏览] 面板中更改了选择，则只要所做的选择提供当前使用的选项卡页面，该选项卡页面将继续保持活动状态。否则，策略选项卡页面将成为活动的选项卡页面。当某个选项卡页面再次成为活动状态时，将恢复其内部状态（起源路径和排序顺序）。

“策略”选项卡页面



图 2-13 “策略”选项卡页面

可以使用策略选项卡页面浏览配置策略树，其中显示了子组和/或配置设置。

每个策略页面都有一个建立报表按钮。借助该按钮可以使用报表功能。有关详细信息，请参阅第 37 页“报表”。

如果策略页面包含策略表格，将显示清除设定按钮。清除设定按钮可用于删除为选定实体的当前策略定义的所有配置设置，包括关联的子策略的设置。单击清除设定按钮将激活警告对话框，告诉管理员此操作的后果。

配置策略树中的每个根条目表示一个应用程序，例如 Mozilla。应用程序下的树用于组织属于该应用程序的配置设定。

起源路径

起源路径显示在选项卡下页面的顶部。它显示配置策略树中的当前位置。它的作用方式与“浏览”窗格中的起源路径的作用方式相同。请参阅第 20 页“起源路径”。

策略表格



图 2-14 “策略”表格

子组表格位于起源路径的下方。该表格列出配置策略树中当前位置的子组。它包含两列：“名称”和“注解”。

“名称”列含有配置策略树中当前位置的所有子组的名称。名称以链接形式显示。

要浏览配置策略树，请单击名称链接。这将更新“内容”窗格，使起源路径指向配置策略树中的新位置；还将更新“内容”窗格，以显示策略表格。

“注解”列包含子组的简短说明。

策略

策略的配置设置显示在“内容”窗格的策略页面中。



图 2-15 “策略”页面





数据显示在表格中。表格包含四列：含有选择图标的选择列、“状态”列、“名称”列和“值”列。表格中的操作栏具有一个下拉式操作菜单。

▼ 对元素执行操作的步骤

- 步骤
1. 选定所需元素的选择列中的复选框。
 2. 从策略操作下拉式菜单中选择操作。下表说明了所有操作

操作	作用
保护	将选定的元素设定为受保护。
未受保护	删除对选定元素的保护。
清除	删除存储在当前实体的元素中的数据。
采用默认值	使用应用程序的默认设定。

元素名称的左侧有两个图标，用于显示该元素的状态。下表概括了这些图标及其功能：

图标	含义	作用
	此图标说明在组织树的此层设定了元素的值。	-
	此链接形式的图标说明在组织 (或域) 树的更高层设定了元素的值。管理员看到的值是在组织中分层合并或实体层合并的结果。	当单击该图标时, 将定位到设定值的位置。
	此图标说明在组织 (或域) 树的此层设定了元素的保护。保护在组织和配置策略树中会被继承。	-
	此链接形式的图标说明在组织 (或域) 树的更高层设定了元素的保护。此元素或项的保护是组织中分层合并或实体层合并的结果。	单击此图标可以浏览设置保护的层。

通过更改“值”列中的值可以更改数据值。值和状态的更改都必须进行存盘。存盘操作可通过单击存盘按钮来完成。

集合

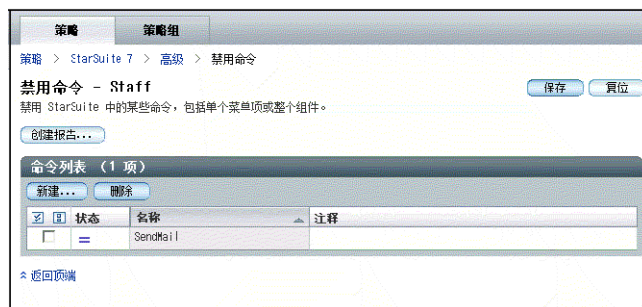


图 2-16 加入新属性

通常, 策略选项卡页面的内容和结构是静态的, 因此某个子组的属性和区域的数目是固定的, 管理员不能进行修改。对于多数管理任务这就足够了。但是, 某些应用程序管理多个项目列表, 管理员可以在其中加入或删除项目。因此, Configuration Manager 提供了集合以提供类似的功能。集合允许管理员在运行时加入或删除属性。

▼ 在集合中加入元素的步骤

- 步骤
1. 单击新建按钮。
 2. 在出现的对话框中输入新元素的名称。
将在集合中添加该元素，并更新主窗口。
 3. 在主窗口中可以编辑该新元素。
 4. 要保存更改，需要显式单击存盘按钮。

更多信息 删除元素

要从集合中删除元素，请选择元素，然后单击删除按钮。

注意 – 一个集合也可以包含另一个或多个集合。要编辑集合，请单击列表中的集合名称。

“策略组”选项卡页面

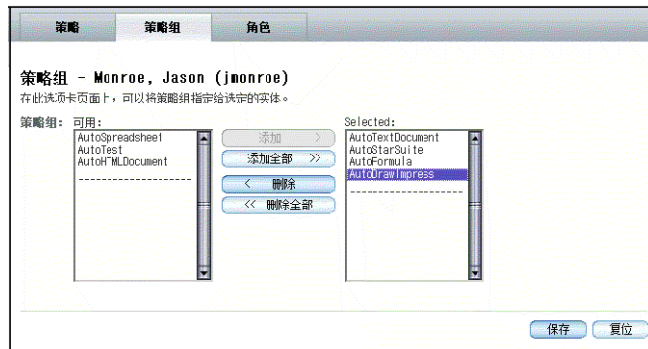


图 2-17 “策略组”选项卡页面

如果已在“浏览”窗格中选定了实体，“内容”窗格中将显示**策略组**选项卡页面。它允许管理员将策略组加入到选定实体中，以及从选定实体中删除策略组。

左侧列表包含当前未指定到该实体的可用策略组。右侧列表包含当前已指定到该实体的策略组。通过选择一个或多个条目，管理员可以向实体添加策略组和从中删除策略组。

添加和删除策略组

▼ 加入左侧的可用列表中列出的策略组的步骤

- 步骤
1. 从可用列表选择一个或多个要加入到实体中的策略组。
 2. 单击加入按钮将选定策略组加入到右侧的选中列表中。
 3. 单击存盘以保存新的指定。

▼ 从实体中删除策略组的步骤

- 步骤
1. 从选中列表中选择要从实体中删除的一个或多个策略组。
 2. 单击删除按钮将删除选定策略组。
 3. 单击存盘将永久删除策略组。

注意 – 还可以单击全部加入和全部删除按钮，将所有策略组加入到选定实体中或从选定实体中删除所有策略组。

“受托者”选项卡页面



图 2-18 “受托者”选项卡页面

如果在“浏览”窗格的“策略系统信息库”选项卡页面中选中了策略组，“内容”窗格中将显示受托者选项卡页面。“受托者”页面列出了选定策略组被指定到的所有实体。

可以在受托者选项卡页面中执行以下操作：

- 删除按钮将中断选定实体与“浏览”窗格中的选定策略组之间的关系。
- “选择”列用于选择要删除的行。
- 单击“名称”列中的实体将刷新 [浏览] 面板，从而使被单击的实体成为 [浏览] 面板中具有蓝色背景的实体。
- “类型”列显示实体的类型。实体的类型可以是“组织”、“用户”或“角色”。
- “路径”列包含组织树或域树中的实体的路径。

“角色”选项卡页面

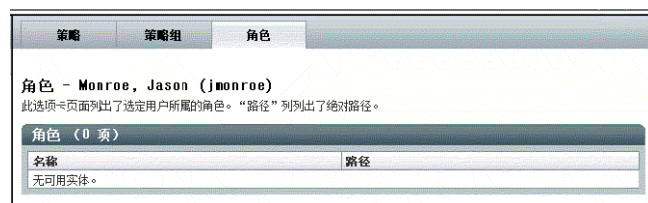


图 2-19 “角色”选项卡页面

如果在“浏览”窗格中选定类型为“用户”的实体，“内容”窗格中将显示**角色**选项卡页面。**角色**选项卡页面列出选定用户所属的所有角色。

此页面含有“名称”和“路径”两列。“名称”包含角色的名称，“路径”包含角色的绝对路径。

“用户”选项卡页面

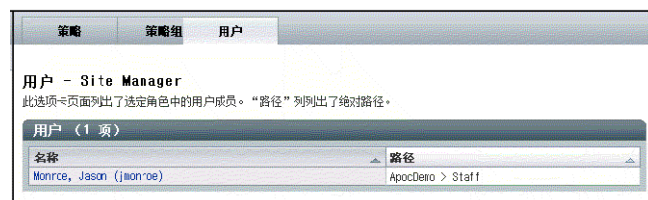


图 2-20 “用户”选项卡页面

在“浏览”窗格中选定角色时，“内容”窗格中将显示**用户**选项卡页面。**用户**页面列出属于选定角色的所有用户。

用户表格包含两列：“名称”和“路径”。“名称”列包含用户的名称，“路径”列包含该用户的绝对路径。显示绝对路径是因为角色中包含的成员可能不位于当前实体下。

报表

报表是所有含有数据的配置设定的只读视图。单击建立报表按钮将触发报表。将显示 [配置报表] 对话框。



图 2-21 “配置报表”对话框

“配置报表”对话框允许您定制以下内容：

- 要使用的树：组织树和/或域树（在用于报表部分设置）。
- 要在生成的报表中显示的列（可以禁用状态路径和说明）。

▼ 建立报表

- 步骤
1. 在“内容”窗格的相应窗口中单击建立报表按钮。
将显示 [配置报表] 对话框。
 2. 定制以下选项的设定：
 - **组织树**选项包含浏览区域中当前选定的组织成员（组织、用户或角色）的全限定路径。
 - **域树**选项包含浏览区域中当前选定的域成员（域或主机）的全限定路径。
 - 可以使用**用于报表**部分中的单选按钮指定报表中要使用的配置设置。可以使用组织树成员的配置设定、域树成员的配置设定或同时使用这两种设定。后一种情况主要用于为管理员提供一种在计算机 b 上列出用户 a 的配置的方法。默认情况下选择单选按钮组中的哪个选项取决于在 [浏览] 面板中选定的选项卡。如果已打开用户选项卡页面，默认情况下将选定**组织树中的设定**选项。相反，如果已打开主

机选项卡页面，将选定域树中的设定选项。

注意 – 当策略组的配置设置显示在“内容”窗格的**策略**选项卡页面中时，如果管理员单击建立报表按钮，将不显示上面的段落中列出的任何用户界面元素，因为策略组与其他任何成员的组合生成报表没有任何意义。策略组的报表始终只包含基于选定策略组的配置设置。

- **状态路径和说明**复选框用于切换“状态路径”和“说明”列在“报表”窗口中的显示。

3. 单击建立报表按钮将关闭“配置报表”对话框。

完成定制后，单击报表将打开选定数据的只读视图。

“报表”窗口

“报表”窗口是进行优化的浏览器窗口，以便于存盘和打印。因此，“报表”页面没有使用任何图像。

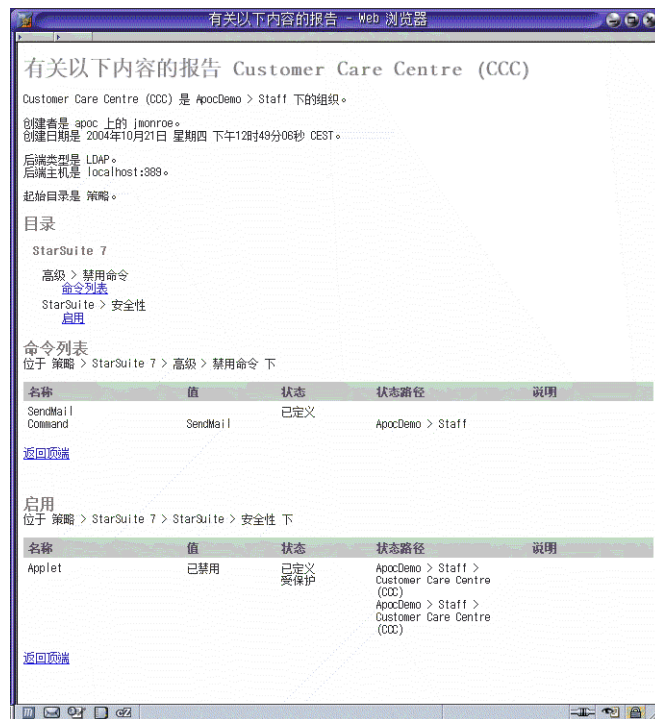


图 2-22 “报表”窗口

报表的主要部分如下所示：

- 主标题
- 环境信息
- 目录
- 包含配置设置的表格

主标题包含“Report -”以及用来生成此报表的组织/域成员的名称的字符串。

环境信息包含使用的组织/域成员、创建者、创建日期、后端存储器类型、主机和位置以及起始子组。

目录提供一组简洁的链接，这些链接指向包含本报表中的配置设置的所有表格。

包含配置设置的表格以子组的形式进行编组。仅列出至少包含所针对的组织成员或域成员的一项配置设置的子组。每个表格都有一个包含子组的名称和位置的标题。适用的情况下，还包含表示子组位置的编号。每一层显示一个附加编号。每个编号的值表示列出的此层的子组的数量。

表格本身包含以下列：

- “名称”列包含配置设置的名称。
- “值”列包含配置设置的值。
- “状态”列包含配置设置的状态。可能值：“已定义”和/或“只读”。“已定义”表示此配置设置已具有值。“只读”表示不能在下面的分层中更改的配置设置。如果配置设置已具有值，那么它始终是已定义的，但如果配置设置不具有值，它将是只读的。
- “状态路径”（可选）包含设置状态的路径。
- “说明”（可选）包含配置设置的简短说明。

表格的奇数行背景以浅色显示来增强可读性。每个表格后面都显示[返回顶部](#)链接。单击该链接将再次显示目录。

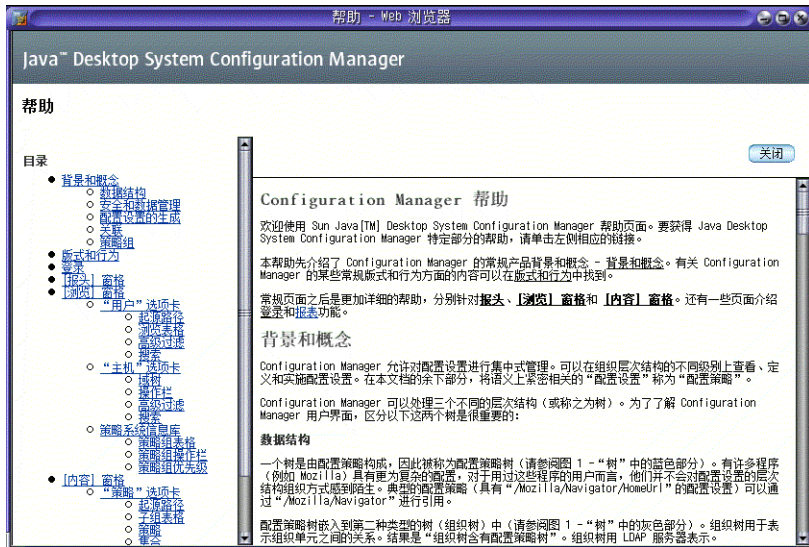
退出

单击标题中的[注销](#)链接将结束 Configuration Manager 会话。

帮助(H)

以三种不同方法提供帮助：

- 单击标题右上方的[帮助](#)链接可以访问主帮助页面。这将打开一个独立的浏览器视窗。



在 [内容] 窗格内浏览时，帮助工具与上下文相关。单击**帮助**滚动帮助页面，到达与当前选项卡页面对应的部分。

- 还提供了内置帮助，为管理员提供当前使用的特定项的简短说明。说明位于每个页面的顶端。

在必要的位置，内联帮助还给出了可配置设置的说明及其接受的值的类型。

- 所有图形图像和链接均提供了“工具提示”。要查看“工具提示”，请将鼠标放在某个图像或链接上。

第 3 章

使用命令行界面

本章介绍 Java Desktop System Configuration Manager 命令行界面 (CLI)，此界面可代替 Configuration Manager 图形用户界面，用来创建、处理、导出和导入配置策略组。

Configuration Manager CLI 概述

CLI 可用来创建、处理、导出/导入和删除策略组。这些策略组可能来自策略组系统信息库，也可能是实体策略组。与 Configuration Manager GUI 一样，CLI 允许将来自策略组系统信息库的策略组以及实体策略组指定/取消指定给实体。CLI 允许以 XML 格式将系统信息库策略组和实体策略组从 ZIP 文件中导出或导入到 ZIP 文件中。这样就可以在导入策略组之前创建、编辑或删除这些文件中的策略设置。

注意 - CLI 没有提供与以下 GUI 功能等效的功能：

- 浏览实体分层结构。
 - 查看合并的实体策略设置。
 - 生成报告。
-

使用 CLI

调用 CLI 命令

CLI 包含 `pgtool` 命令，此命令在单行命令模式下运行，每次执行一个命令。`pgtool` 包含多个子命令、选项和操作数，第 51 页“命令摘要”部分对它们进行了介绍。可以使用完整的关键字或关键字缩写来指定选项。以下命令说明中使用的是完整的关键字，但您也可以从表 3-2 中找到这些关键字所对应的快捷键。

CLI 所需的引导信息

引导信息用于定位并查询存储实体和策略组的数据存储。所需的引导信息包含服务器、端口号、基本标识名 (DN) 和类型。这些信息可以在命令行中指定，也可以从引导文件中获取。

获取引导信息

可以在命令行中指定引导文件的位置。如果不指定，将使用随 CLI 一起安装的引导文件。此文件安装时只包含关键字名称，管理员必须对其进行编辑以提供正确的引导值。

CLI 还允许您在命令行中指定引导信息。用于指定详细引导信息的选项如下：

- `--hostname=<hostname>`（存储系统后端所在的服务器的名称）
- `--base=<base name>`（存储系统后端的基本条目）
- `--port=<port number>`（存储系统后端使用的端口号）
- `--type=<type of back end>`（例如 LDAP）

使用用户名和口令进行验证

每次执行一个命令时，都需要输入用户名和口令。

- CLI 提供了一个 `login` 命令，允许将用户名/口令对存储在管理员主目录中的证书文件中。此文件名为 `.apocpass`，对它的访问受到严格的限制。运行 `login` 命令时，CLI 将检查主目录中是否存在 `.apocpass` 文件。如果该文件存在但不具有正确的权限（即 600），`login` 命令将退出并报告错误。如果已指定用户名，将提示用户输入口令。如果未指定用户名，将提示用户输入用户名和口令。系统将使用匿名访问来验证输入的用户名和口令。如果不支持匿名访问，将提示用户输入授权的 DN 和口令。如果成功通过验证，将在 `.apocpass` 文件中添加一个条目。此条目的关键字由服务器/端口/基本 DN 和用户名组成。

例如，用户 "jmonroe" 可以使用关键字

`cdelab1.ireland.sun.com:389;o=apoc:jmonroe` 为位于端口 389、基本条目为 `o=apoc` 的服务器 `cdelab1.ireland.sun.com` 存储一个口令。存储的值为用户 DN 和口令。通过这种方式，可以存储此存储系统后端的多个用户的用户名/口令对。类似地，也可以为其他存储系统后端存储用户名/口令对。成功运行 `login` 命令后，就可以执行其他 CLI 命令了，无需再指定用户名或口令。

- 对于其他命令，CLI 将首先检查是否存在此用户的 `.apocpass` 文件。如果不存在，将提示用户输入用户名和口令。如果输入的用户名和口令成功通过验证，将执行命令。如果证书文件不存在，但已在命令行中指定了用户名，CLI 将查找与此主机、端口、基本 DN 和用户名对应的条目。如果存在对应的条目，将使用存储的用户 DN 和口令来执行命令；否则，将提示用户输入口令。如果未在命令行中指定用户名，将在 `.apocpass` 文件中搜索使用主机/端口和基本 DN 组合的关键字。如果此组合只有一个对应的条目，将使用存储的用户 DN 和口令来执行命令。如果存在多个条目，将提示用户输入用户名。如果输入的用户名与某个条目匹配，将使用存储的用户 DN 和口令来执行命令。如果输入的用户名与任何条目都不匹配，将提示用户输入口令。提示用户输入口令之后，将使用 `.apocpass` 文件中与此主机/端口/基本 DN 组合对应的条目来验证用户名和口令。如果不存在这样的条目，将使用匿名访问进行验证。

运行命令

每次运行命令时都将创建并初始化与 `policymgr` API 的连接，并在执行命令后立即退出。如果退出命令时显示 `errir`，则说明未对配置策略应用任何更改。

表示实体

实体使用 LDAP DN 进行表示，例如 `uid=jmonroe,ou=People,o=apoc`。

CLI 命令

本节介绍 Configuration Manager 的 CLI 功能。

访问 CLI 帮助

要获取所有可用 CLI 命令的列表，请键入 `pgtool --help`。

访问 CLI 版本信息

要显示版本信息，请键入 `pgtool --version`。

添加

将策略组系统信息库中的策略组指定给实体。

语法

```
add [--username=<name>] [--scope=<user/host>] <name> <entity>
```

--username=<name>: 以配置系统信息库使用的格式表示的系统管理员的用户名, 例如 "jmonroe"。

--scope=<user/host>: 指定策略组的范围, 可以是用户或主机。如果不指定, 则默认范围为用户。

<name>: 指定要为实体指定的策略组的名称。

<entity>: 实体的名称将按照存储系统后端使用的格式指定, 例如, 对于 LDAP 存储系统后端, 将使用标识名来指定实体。

实例 3-1 为实体添加策略组

```
% pgtool add --username=jmonroe UserPolicyGroup1 cn
Role1,o=staff,o=apoc
```

用户 "jmonroe" 将策略组 "UserPolicyGroup1" 指定给实体 "cn=Role1,o=staff,o=apoc"。

创建

create 命令用于创建一个新的空策略组。

语法

```
create [--username=<name>] [--name=<policy group name>]
[--scope=<user/host>] [--entity=<entity name>]
[--priority=<priority integer>]
```

--username=<name>: 以配置系统信息库使用的格式表示的系统管理员的用户名, 例如 "jmonroe"。

--name=<policy group name>: 指定策略组的名称。如果同一层已存在同名同范围的策略组, 命令将退出并报告错误。此选项不能与 --entity 选项一起使用, 因为实体策略组具有受限制的默认名称。

--scope=<user/host>: 指定策略组的范围, 可以是用户或主机。如果不指定, 则默认范围为用户。

--entity=<entity name>: 在其中创建策略组的实体。如果不指定此选项, 策略组将来自策略组系统信息库。此选项不能与 --name 选项一起使用, 因为实体策略组具有受限制的默认名称。

`--priority=<priority integer>`：用于指定策略组优先级的整数 (≥ 1)。此选项不能与 `--entity` 选项一起使用，因为实体策略组具有无法更改的默认优先级。如果指定的优先级与同一层同一范围的某个现有策略组的优先级相同，命令将退出并报告错误。如果不指定优先级，系统将为其指定一个。

实例 3-2 创建新策略组

```
% pgtool create --username=jmonroe --scope=host
--name=NewHostGroup1
```

创建名为 "NewHostGroup1" 的新策略组，其范围为“主机”。

删除

删除策略组。

语法

```
delete [--username=<name>] [--name=<policy group name>]
[--scope=<user/host>] [--entity=<entity name>]
```

`--username=<name>`：以配置系统信息库使用的格式表示的系统管理员的用户名，例如 "jmonroe"。

`--name=<policy group name>`：指定要删除的策略组的名称。此选项不能与 `--entity` 选项一起使用，因为实体策略组具有受限制的默认名称。如果策略组不存在或无法唯一标识，命令将退出并报告错误。

`--scope=<user/host>`：指定策略组的范围，可以是用户或主机。如果不指定，则默认范围为用户。

`--entity=<entity name>`：在其中存储策略组的实体。如果不指定此选项，策略组将来自策略组系统信息库。此选项不能与 `--name` 选项一起使用，因为实体策略组具有受限制的默认名称。

实例 3-3 删除策略组

```
% pgtool delete --username=jmonroe --scope=host
--name=renameNewHostGroup1
```

删除“renameNewHostGroup1”策略组。

导出

将策略组以 ZIP 文件格式导出到指定的目标文件中。这些策略组可能来自策略组系统信息库，也可能是实体策略组。

语法

```
export [--username=<name>] [--name=<policy group name>]
[--scope=<user/host>] [--entity=<entity name>] <target>
```

--username=<name>: 以配置系统信息库使用的格式表示的系统管理员的用户名, 例如 "jmonroe"。

--name=<policy group name>: 指定策略组的名称。此选项不能与 --entity 选项一起使用, 因为实体策略组具有受限制的默认名称。策略组系统信息库中可能存在两个同名的策略组, 一个策略组的范围为用户, 另一个策略组的范围为主机。如果不指定, 则默认范围为用户。

--scope=<user/host>: 指定策略组的范围。可以是用户或主机。如果不指定, 则默认范围为用户。

--entity=<entity name>: 在其中存储策略组的实体。此选项不能与 --name 选项一起使用, 因为实体策略组具有受限制的默认名称。如果不指定此选项, 策略组将来自策略组系统信息库。实体的名称将按照存储系统后端使用的格式指定, 例如, 对于 LDAP 存储系统后端, 将使用标识名来指定实体。

<target>: 存储 ZIP 文件的路径和文件名。如果不指定文件名, 则默认为 /tmp/<policy group name>.zip。如果目标文件不可写, 命令将退出并报告错误。

实例 3-4 导出策略组

```
% pgtool export --scope=host --name=HostPolicyGroup1
--username=jmonroe /tmp/newdir
```

将策略组 "HostPolicyGroup1" 导出到 HostPolicyGroup1.zip 文件中, 该文件是在新目录 /tmp/newdir 中创建的。

导入

从指定的源文件导入以 ZIP 文件格式存储的策略组。可以将策略组导入到策略组系统信息库或实体中。

语法

```
import [--username=<name>] [--name=<policy group name>]
[--scope=<user/host>] [--entity=<entity name>]
[--priority=<priority integer>] <source>
```

--username=<name>: 以配置系统信息库使用的格式表示的系统管理员的用户名, 例如 "jmonroe"。

--name=<policy group name>: 指定策略组的名称。此选项不能与 --entity 选项一起使用, 因为实体策略组具有受限制的默认名称。同一位置不能存在两个具有相同名称和相同范围的策略组。如果不指定策略组的名称, 则默认为 .zip 文件的名称。如果策略组系统信息库中已经存在具有此名称和此范围的策略组, 该策略组将被覆写。

`--scope=<user/host>`: 指定策略组的范围。可以是用户或主机。如果不指定, 则默认范围为用户。

`--entity=<entity name>`: 在其中存储策略组的实体。如果不指定此选项, 策略组将来自策略组系统信息库。此选项不能与 `--name` 选项一起使用, 因为实体策略组具有受限制的默认名称。实体的名称将按照存储系统后端使用的格式指定, 例如, 对于 LDAP 存储系统后端, 将使用标识名来指定实体。

`--priority=<priority integer>`: 用于指定策略组系统信息库中策略组优先级的整数 ($>=1$)。此选项不能与 `--entity` 选项一起使用, 因为实体策略组具有无法更改的默认优先级。如果指定的优先级与系统信息库中具有此范围的某个现有策略组的优先级相同, 命令将退出并报告错误。如果不指定优先级, 系统将为其指定一个。

`<source>`: 存储 ZIP 文件的路径和文件名。

实例 3-5 导入策略组

```
% pgtool import --scope=host --name=NewHostPolicyGroup1
--username=jmonroe --priority=7 /tmp/HostPolicyGroup1.zip
```

从 HostPolicyGroup1.zip 文件中导入名为 "NewHostPolicyGroup1"、范围为“主机”、优先级为 "7" 的策略组。

列表

如果不指定任何选项, 将列出策略组系统信息库中的所有策略组。如果指定了两个存储系统后端, 将列出该用户存储系统后端的策略组系统信息库中的所有策略组。根据指定的选项, `list` 还可以列出指定给某个实体的所有策略组, 或使用某个特定策略组的所有实体。列出策略组时, 将同时列出其详细信息 (如果存在), 例如名称、范围、优先级和实体。实体将按标识名列出。

语法

```
list [--username=<name>] [--scope=<user/host>] [--entity=<entity
name>] [--name =<policy group name>]
```

`--username=<name>`: 以配置系统信息库使用的格式表示的系统管理员的用户名, 例如 "jmonroe"。

`--scope=<user/host>`: 如果只指定了此选项, 将列出策略组系统信息库中具有指定范围的所有策略组。如果不指定, 则默认范围为用户。如果将此选项与 `-entity` 选项一起使用, 将列出指定给该实体的、具有此范围的所有策略组。如果将此选项与 `-name` 选项一起使用, 将列出使用指定范围的指定策略组的所有实体。

`--entity=<entity name>`: 列出指定给某个实体的策略组。

`--name=<policy group name>`: 列出使用指定策略组的实体。

实例 3-6 列出系统信息库中的策略组

```
% pgtool list --username=jmonroe
```

列出管理员“jmonroe”的全局策略组。

```
% pgtool list --username=jmonroe --name=UserPolicyGroup1
```

列出使用策略组“UserPolicyGroup1”的实体。

登录

将后端数据存储的用户名和口令存储在管理员主目录的一个文件中。此用户名和口令以后可用于调用 pgtool 命令。

证书存储在管理员主目录中名为 .apocpass 的文件中。如果此文件已存在但不具有正确的权限，命令将退出并报告错误。如果已输入用户名，将提示管理员输入口令；如果未输入用户名，将提示管理员输入用户名和口令。系统将使用数据存储的匿名访问来验证输入的用户名和口令。如果不支持匿名访问，将提示管理员输入授权的用户名和口令。如果授权的用户名未通过验证，命令将退出并报告错误。如果通过了验证，用户名/口令对将被存储在管理员的 .apocpass 文件中。将使用由主机/端口/基本引导信息和用户名组成的关键字来存储口令。可以将引导文件指定为选项变量，也可以使用上述其他选项指定引导信息。如果不使用上述任一方法，将从通过 pgtool 命令安装的默认引导文件中获取引导信息。如果引导信息不可用或者无法创建证书文件，命令将退出并报告错误。如果成功创建了证书文件，则不需要为使用此存储系统后端的后续 pgtool 命令指定用户名和口令，此时将使用存储在证书文件中的用户名和口令信息。

语法

```
login [--username=<name>] [--file=<bootstrap file>]  
[--hostname=<hostname>] [--port=<port number>] [--base=<base  
name>] [--type=<type of back end>]
```

--username=<name>: 以配置系统信息库使用的格式表示的系统管理员的用户名，例如“jmonroe”。

--file=<bootstrap file>: 引导文件的全限定路径。

--hostname=<hostname>: 所需存储系统后端的主机名。将使用此信息，而不使用引导文件提供的相应信息。

--port=<port number>: 此存储系统后端使用的端口号。

--base=<base name>: 此存储系统后端的基本名称，例如，LDAP 存储系统后端的基本 DN。

--type=<type of back end>: 默认值为 LDAP。

实例 3-7 登录

```
% pgtool login --username=jmonroe [Enter the correct password  
when prompted]
```

创建名为 `~/.apocpass` 的文件，其中包含 "jmonroe" 和 "password" 的条目，此文件的权限为 600。

修改

更改策略组系统信息库中策略组的优先级。

语法

```
modify [--username=<name>] [--scope=<user/host>] <name>  
<priority>
```

`--username=<name>`: 以配置系统信息库使用的格式表示的系统管理员的用户名，例如 "jmonroe"。

`--scope=<user/host>`: 指定策略组的范围，可以是用户或主机。如果不指定，则默认范围为用户。

`<name>`: 指定策略组的名称。

`<priority>`: 用于指定策略组优先级的整数 (≥ 1)。如果指定的优先级与策略组系统信息库中具有此范围的某个现有策略组的优先级相同，命令将失败。

实例 3-8 更改策略组的优先级

```
% pgtool modify --username=jmonroe UserPolicyGroup1 15
```

将策略组 "UserPolicyGroup1" 的优先级更改为 15。

删除

从实体中删除策略组。

语法

```
remove [--username=<name>] [--scope=<user/host>] <name> <entity>
```

`--username=<name>`: 以配置系统信息库使用的格式表示的系统管理员的用户名，例如 "jmonroe"。

`--scope=<user/host>`: 指定策略组的范围，可以是用户或主机。如果不指定，则默认范围为用户。

<name>: 指定了策略组系统信息库中指定给该实体的策略组的名称。

<entity>: 此实体的名称。

实例 3-9 从实体中删除策略组

```
% pgtool remove --username=jmonroe UserPolicyGroup1
cn=Role1,o=staff,o=apoc
```

用户“jmonroe”将策略组“UserPolicyGroup1”从实体“cn=Role1,o=staff,o=apoc”中删除。

重命名

重命名策略组系统信息库中的策略组。

语法

```
rename [--username=<name>] [--scope=<user/host>] <name> <newname>
```

--username=<name>: 以配置系统信息库使用的格式表示的系统管理员的用户名，例如“jmonroe”。

--scope=<user/host>: 指定现有策略组的范围，可以是用户或主机。如果不指定，则默认范围为用户。

<name>: 指定了策略组系统信息库中策略组的当前名称。

<newname>: 策略组的新名称。如果策略组系统信息库中已存在具有此名称和此范围的策略组，命令将退出并报告错误。

实例 3-10 重命名策略组

```
% pgtool rename --username=jmonroe NewUserGroup2
renamedNewUserGroup2
```

将策略组 "NewUserGroup2" 重命名为 "renamedNewUserGroup2"。

命令摘要

表 3-1 命令

命令	描述
add	将策略组系统信息库中的策略组指定给实体。
create	创建新的空策略组。
delete	删除策略组。
export	将策略组以 ZIP 文件格式导出到指定的目标文件中。
import	从指定的源文件中导入以 ZIP 文件格式存储的策略组。
list	列出策略组系统信息库中的策略组，或者列出指定给某个实体的策略组，或者列出具有指定策略组的实体。
login	将此后端数据存储的用户名和口令存储在用户主目录的一个文件中。此用户名和口令以后可用于调用 <code>pgtool</code> 命令。
modify	更改策略组系统信息库中策略组的优先级。
remove	从实体中删除策略组。
rename	重命名策略组系统信息库中的策略组。

表 3-2 选项

选项	描述
<code>-b <base name>, --base=<base name></code>	指定存储系统后端的根条目。此基本条目的格式由使用的存储系统后端决定。例如，LDAP 存储系统后端的根条目为 <code>o=apoc</code> ； <code>--base o=apoc</code> 。
<code>-e <entity>, --entity=<entity></code>	指定表示用户、角色、组织、主机或域的实体。实体的条目格式由使用的存储系统后端决定。例如，用户“jmonroe”的 LDAP 存储系统后端的实体条目为： <code>-e uid=jmonroe,ou=People,o=staff,o=apoc</code>
<code>-f <file>, --file=<file></code>	指定一个全限定文件，该文件将详细列出执行此命令时使用的引导信息。例如： <code>-f /tmp/policymgr.cfg</code>
<code>-h <hostname>, --hostname=<hostname></code>	指定存储系统后端的主机名。例如： <code>--host=server1.sun.com</code>
<code>-i <priority>, --priority=<priority></code>	指定表示策略组优先级的正整数。例如： <code>-i 12</code>

表 3-2 选项 (续)

选项	描述
-m <name>, --name=<name>	指定策略组的名称。例如 : --name=UserPolicyGroup1
-p <port>, --port=<port>	指定存储系统后端的端口号。例如: -p 399
-s <scope>, --scope=<scope>	指定策略组的范围。范围可以是用户或主机, 默认范围为用户。例如: --scope=host
-t <type>, --type=<type>	指定存储系统后端的类型。默认类型为 LDAP。例如: -t LDAP
-u <username>, --username=<username>	指定存储系统后端的管理员的用户名, 此时系统将提示该用户输入口令。如果不使用此选项, 而且用户未使用 pgtool login 子命令, 将提示用户输入用户名和口令。例如 : --username=jmonroe
-?, --help	显示此帮助, 然后退出。
-V, --version	显示版本, 然后退出。

附录 A

使用情形

背景

Magic Insurance, Inc. 是一家国际性公司，决定将他们的整套桌面环境从 Windows NT 移植到 Java Desktop System (JDS) 的 Gnome 桌面。该公司还打算将其主要字处理器从使用 Microsoft Word 转为使用 StarSuite Writer，并将其主要浏览器应用程序从使用 Internet Explorer 转为使用 Mozilla。

John 是公司的 IT 管理员，他负责尽可能轻松地完成移植任务。John 决定使用 JDS 提供的 Configuration Manager 帮助他进行移植。首先，他检查了需要使用 Configuration Manager 为公司解决的三个问题：

- 按照 Customer Care Center (CCC) 部门的经理的要求，防止该部门的职员启动计算机游戏。
- 为每个部门的“专家”和“初学者”群体提供不同的配置设置。这些群体分别包含经验丰富的职员和新职员。
- 为 Company Services Center (CSC) 的职员提供解决方案，这些职员经常去位于世界各地的不同部门。

方案 1 — 防止启动应用程序

John 要防止 CCC 职员启动计算机游戏。

▼ 锁定应用程序功能

在 CCC 部门工作的职员的姓名列在公司的 Configuration Manager 的 LDAP 树的 CCC 组织内。John 决定使用 Gnome 中的“限制应用程序启动”功能从“允许的应用程序”列表中删除所有游戏。

由于职员可以在他们的客户机上取消这一设定，John 对 CCC 组织的该设定实施保护。因此，该设定对于 CCC 组织的所有成员将是只读的。

- 步骤
1. 在“浏览”窗格中，单击用户选项卡，然后找到组织树中的 **Customer Care Center CCC**。
 2. 在“操作”列中，单击 **Customer Care Center CCC** 旁边的查看链接。
 3. 在“内容”窗格中，单击策略选项卡，然后浏览到 **Gnome 2.6 > 锁定**。
 4. 选定应用程序启动旁边的限制复选框。
 5. 从允许的应用程序旁边的列表中选择游戏对应的路径，然后单击删除。
 6. 选定允许的应用程序和应用程序启动复选框。
 7. 在策略操作下拉式列表中，选定“锁定选项”列顶部的保护。
 8. 单击保存。

方案 2 — 管理分散的配置文件

您需要为每个部门的“专家”和“初学者”群体提供不同的配置设置。

▼ 创建和配置新策略组

John 决定创建名为 "Novice" 和 "Expert" 的两个策略组。然后配置每个策略组的设置，并将每个组指定给相应的群体。这样，如果他以后在一个策略组中进行了更改，所做更改将会自动应用于指定了这些策略组的所有群体。John 还可以从群体中删除策略组。

John 需要对初学者禁用的三项功能是“工具”菜单的“配置”和“选项”子菜单，以及在 StarSuite 中执行宏。

注意 – 有关可用命令的完整列表，请参见《StarSuite 7 管理指南》的附录。

开始之前 以下步骤介绍了如何为 "Novice" 策略组配置设置。

- 步骤
1. 在“浏览”窗格中，单击用户选项卡，然后单击策略系统信息库。
 2. 在策略组操作下拉式列表中，选择新建。
 3. 在文本字段中键入 **Novice**，然后单击“确定”。
 4. 在“内容”窗格中，浏览到策略 > StarSuite 7 > StarSuite > 安全性。

5. 在运行宏策略行中，从值列表框中选择永远不。
6. 单击“保存”。
7. 浏览到策略 > StarSuite 7 > 高级 > 禁用命令。
8. 在 CommandList 表中，单击新建。
9. 在文本框中键入 `ConfigureDialog`，然后单击“确定”。
10. 在 CommandList 表中，单击新建。
11. 在文本框中键入 `OptionsTreeDialog`，单击“确定”，然后在“内容”窗格中单击保存。
12. 在“浏览”窗格中，选择组织树，然后找到初学者。
13. 在初学者组织旁边的“操作”列中，单击查看。
14. 在“内容”窗格中，单击策略组选项卡，再单击 `Novice`，然后单击添加。
15. 单击“保存”。
16. 对于要添加 "Novice" 策略组的每个“初学者”群体重复步骤 12 至 15。

▼ 为 "Experts" 策略组配置设置

- 步骤
1. 在“浏览”窗格中，单击用户选项卡，然后单击策略系统信息库。
 2. 在策略组操作列表框中，选择新建。
 3. 在文本框中键入 `Experts`，然后单击“确定”。

注意 – 由于专家设定是默认设定，因此仅需要执行这三个步骤。

方案 3 — 为漫游用户提供解决方案

您需要为 Mozilla 浏览器提供不同的代理设置，这些设置取决于用户登录的主机。例如，运行在北美洲主机上的浏览器的代理设置与运行在欧洲主机上的浏览器的代理设置不同。

▼ 更改代理设置

在此方案中，Mozilla 的个人设置按用户名进行存储，特定于主机的设置存储为基于 IP 的配置。这些设置都存储在中央 LDAP 服务器中。此外，LDAP 树已包含 "North America" 和 "Europe" 域以及这些域成员的相应主机。John 认为最好的解决方案是根据使用的主机在这两个域中更改 Mozilla 的代理设定。

- 步骤
1. 在“浏览”窗格中，单击主机选项卡，然后在域树中找到 **North America**。
 2. 在 **North America** 域旁边的“操作”列中，单击查看。
 3. 在“内容”窗格中，浏览到策略 > **Mozilla 1.7** > 高级 > 代理。
 4. 在使用系统代理设定行的“值”列中，取消选定启用复选框。
 5. 在配置代理以访问 **Internet** 行的“值”列中，选择手动代理配置选项。
 6. 在 **HTTP** 代理行的“值”列中，在文本字段中键入 `proxy.NorthAmerica.com`。
 7. 在 **HTTP** 端口行的“值”列中，在文本字段中键入 `8080`。
 8. 单击保存。
 9. 对 **"Europe"** 域重复步骤 1 至 8，使用代理名称 `proxy.Europe.com` 和 **HTTP** 端口 `9090`。

注意 – 如果 John 愿意，他还可以通过对代理设定实施保护来防止用户更改这些设定。

术语汇编

A

代理

请参阅“Configuration Manager 代理”。

APOC (控制点)

Java™ Desktop System Configuration Manager Release 1.1 的内部代码名称。

C

**Configuration Manager
代理**

位于网络上的管理资源中的模块，可以请求和高速缓存配置策略。

配置策略

一条规则或一个规则集，控制 Configuration Manager 及其点产品的行为。

配置策略组

配置策略的容器，可以链接到组织、组、用户或主机。配置策略组存储在配置策略系统信息库中。

配置策略系统信息库

存储配置策略组的容器。

配置策略模板 (CPT)

一个 XML 文件，包含构成策略的配置设置的数据位置集合、用来显示数据的用户界面的说明以及对数据的约束。



E

实体

一个逻辑对象，可将配置数据指定给该对象。用户、角色/组和组织是 Configuration Manager 可以识别的实体示例。



L

LDAP

轻量目录访问协议 (LDAP)。LDAP 是在 TCP/IP 之上运行的目录服务协议。LDAP 的细节在 RFC 1777“轻量目录访问协议”中定义。



M

合并

客户机请求配置数据时在实体（例如，用户、角色或组织）的上下文中执行的操作。要为实体提供数据，配置客户机首先从注册层装入相关数据，然后依次应用各层的定制（使用组织层次结构确定层及其优先级），直到到达上下文中的实体所属的层。客户机仅能识别角色/组 and 用户实体。



P

策略

请参阅“配置策略”。

策略组

请参阅“配置策略组”。