CA Spectrum®

Network Configuration Manager 用户指南

版本 9.4

ca technologies

本文档包括内嵌帮助系统和以电子形式分发的材料（以下简称“文档”），其仅供参考，CA 随时可对其进行更改或撤销。

未经 CA 事先书面同意，不得擅自复制、转让、翻印、透露、修改或转录本文档的全部或部分内容。本文档属于 CA 的机密和专有信息，不得擅自透露，或除以下协议中所允许的用途，不得用于其他任何用途：(i) 您与 CA 之间关于使用与本文档相关的 CA 软件的单独协议；或者 (ii) 您与 CA 之间单独的保密协议。

尽管有上述规定，但如果您为本文档中所指的软件产品的授权用户，则您可打印或提供合理数量的本文档副本，供您及您的雇员内部用于与该软件相关的用途，前提是所有 CA 版权声明和标识必须附在每一份副本上。

打印或提供本文档副本的权利仅限于此类软件所适用的许可协议的有效期内。如果该许可因任何原因而终止，您应负责向 CA 书面证明已将本文档的所有副本和部分副本已退还给 CA 或被销毁。

在所适用的法律允许的范围内，CA 按照“现状”提供本文档，不附带任何保证，包括但不限于商品适销性、适用于特定目的或不侵权的默示保证。CA 在任何情况下对您或其他第三方由于使用本文档所造成的直接或间接的损失或损害都不负任何责任，包括但不限于利润损失、投资受损、业务中断、信誉损失或数据丢失，即使 CA 已经被提前明确告知这种损失或损害的可能性。

本文档中涉及的任何软件产品的使用均应遵照有关许可协议的规定且根据本声明中的条款不得以任何方式修改此许可协议。

本文档由 CA 制作。

仅提供“有限权利”。美国政府使用、复制或透露本系统受 FAR Sections 12.212、52.227-14 和 52.227-19(c)(1) - (2) 以及 DFARS Section 252.227-7014(b)(3) 的相关条款或其后续条款的限制。

版权所有 © 2014 CA。保留所有权利。此处涉及的所有商标、商品名称、服务标识和徽标均归其各自公司所有。

CA Technologies 产品引用

本指南引用了以下产品：

- CA Spectrum® (CA Spectrum)
- CA Spectrum® Network Configuration Manager (NCM)
- CA Spectrum® Report Manager (Report Manager)
- CA Service Desk

联系技术支持

要获取在线技术帮助以及办公地址、主要服务时间和电话号码的完整列表，请联系技术支持：http://www.ca.com/worldwide。

目录

第 1 章： 简介 11

Network Configuration Manager 功能 11
访问 Network Configuration Manager 12
关键术语 13
配置类型 14
运行配置 14
启动配置 14
配置文件 15
支持的设备 15
访问设备认证数据库 15
设备系列 18
Network Configuration Manager 如何确定设备系列 18
Cisco IOS 设备 18
Cisco NX OS 设备 19
Juniper JUNOS 设备 19
扩展实用工具 20
Network Configuration Manager 先决条件 20
通信模式 21
SSH v2 支持 21
Cisco 设备和 SCP 22
未经请求的设备配置更改通知 22
设备陷阱 22
设备 MIB 对象 23
全局集合 23
维护模式 23
Network Configuration Manager 报告包 24

第 2 章： Network Configuration Manager 配置 25

配置 Network Configuration Manager 25
执行常规配置 25
选择“配置历史记录”设置 26
选择“配置更改报警”设置 27
批准工作流 28
配置 TFTP 服务器 30
配置 FTP 服务器 34
使用远程 TFTP 或 FTP 服务器时的注意事项 36
为单个设备指定 TFTP 或 FTP 服务器 36

选择用于设备配置导出的设置 37
配置设备系列 38
配置设备系列常规设置 39
配置设备系列通信模式 39
配置设备系列掩码 40
配置通知陷阱设置 42
配置单个设备以覆盖设备系列设置 44
在单个设备上访问 Network Configuration Manager 设置 44
在单个设备上启用或禁用 Network Configuration Manager 44
在单个设备上配置未经请求的设备配置捕获 45
在单个设备上指定“配置更改报警”设置 45
在单个设备上配置通信模式 47
在单个设备上配置掩码 48
Network Configuration Manager 扩展实用工具 49
支持的操作 49
创建自定义设备系列 50
将设备放置在设备系列中 52
扩展实用工具脚本配置 53
Perl 模块 58
导入和导出脚本 63
维护脚本备份和历史记录 65
自定义的陷阱 65

第 3 章： 全局同步任务 67

关于全局同步 67
关于 Enterasys/Riverstone SSR 设备 68
配置全局同步 68
排定全局同步 69
运行按需全局同步任务 70
查看单个设备的配置历史记录 70
比较任何两个配置 72
指定参考配置 73
配置警报 74
查看参考配置和运行配置之间的差异 74
查看启动配置和运行配置 75
查看全局同步任务结果 75
来自 Report Manager 的 Network Configuration Manager 报告 76
Report Manager 选项 76
使用 Report Manager 生成网络配置管理报告 77

第 4 章： Network Configuration Manager 设备级任务 81

手动捕获配置 81

将配置手动上传到单个设备 81
不需要批准 82
将配置上传到单个设备（需要批准） 83

第 5 章： Network Configuration Manager 批量任务 85

创建上传任务 85
确定 Enterasys/Riverstone SSR 设备如何响应上传任务 87
创建同步任务 88
创建保存到启动任务 89

第 6 章： 固件上传 91

关于固件上传 91
权限 92
配置设备固件传输设置 92
显示 Cisco 闪存分区信息 93
创建加载固件任务 94
创建重新加载任务 97
创建取消重新加载任务 98
加载设备固件脚本 99

第 7 章： 管理任务 101

使任务与全局集合关联 101
关联新任务 101
关联现有的任务 102
排定批量任务 103
可重用任务 103
排定任务 104
启动和停止任务 106
启动任务 106
停止任务 106
恢复任务 107
删除任务 107
查看任务信息 107
实时查看任务结果 108
查看有关所有批量任务的关键统计信息 108
查看批量任务的详细统计信息 108
任务状况和状态值 109
任务状况 109
任务状态 110

第 8 章： Network Configuration Manager 策略 111

关于 Network Configuration Manager 策略 111
单行策略 112
多行块策略 112
创建策略 113
策略标准 115
建议用于更正操作的上传 121
查看违反 123
修复非遵从设备 130
从策略表修复非遵从设备 130
从策略违反警报修复非遵从设备 131
管理策略 131
编辑策略 132
启用和禁用策略 132
将策略应用于全局集合 133
删除策略 133
查看策略信息 134
查看策略详细信息 134
查看所有策略的关键统计信息 134
查看应用于单个设备的所有策略的关键统计信息 135
查看应用于全局集合的策略的关键统计信息 135
多行块策略示例 135
方案 136
入门 136
定义策略 138
保存和测试策略 142
监控违反 146

附录 A： 支持的设备 149

支持的 Cisco 设备 149
支持的 Cisco 设备 170
支持的 Cisco 设备 177
支持的 Cisco CAT 设备 178
支持的 Cisco NX OS 设备 181
支持的 Enterasys 设备 181
支持的 Enterasys/Riverstone SSR 设备 184
支持的 Extreme 设备 186
支持的 Foundry 设备 190
支持的 Juniper 设备 200
支持的 Lancom 设备 202
支持的 Nortel Baystack 设备 202
支持的 Nortel Passport 设备 203

附录 B： Network Configuration Manager 事件 205

关于 Network Configuration Manager 事件 205
在设备上生成的事件 205
配置更改 205
配置更改事件的关联 206
启动配置与运行配置相同/不同 206
参考配置与运行配置相同/不同 207
设备遵从/非遵从策略 207
设备不遵从策略警报生成的事件 207
捕获成功/失败 208
上传成功/失败 208
上传失败警报生成的事件 208
写入启动成功/失败 209
NCM 在设备上已启用/禁用 209
NCM 已禁用，未执行操作 209
设备固件加载 209
在设备系列中已添加/移除设备 210
针对策略生成的事件 210
策略已启用/禁用 210
策略已修改 210
策略具有违反者 210
违反策略警报生成的事件 210
针对全局同步、捕获、上传和写入启动等任务生成的事件 211
任务已排定/取消排定 211
任务已启动、停止、完成、部分完成 211
任务部分完成警报生成的事件 211
在配置服务器应用程序上生成的事件 212
未经请求的全局通知 212
针对设备系列生成的事件 212

附录 C： Network Configuration Manager 权限 213

第 1 章： 简介

本章提供 Network Configuration Manager (NCM) 的一般概述。

此部分包含以下主题：

Network Configuration Manager 功能 (p. 11)
访问 Network Configuration Manager (p. 12)
关键术语 (p. 13)
配置类型 (p. 14)
支持的设备 (p. 15)
访问设备认证数据库 (p. 15)
设备系列 (p. 18)
扩展实用工具 (p. 20)
Network Configuration Manager 先决条件 (p. 20)
通信模式 (p. 21)
未经请求的设备配置更改通知 (p. 22)
全局集合 (p. 23)
维护模式 (p. 23)
Network Configuration Manager 报告包 (p. 24)

Network Configuration Manager 功能

配置管理是识别和监控构成网络的单个设备和设备系列的配置的过程。设备包括路由器、集线器和交换机。

使用 CA Spectrum Network Configuration Manager 可确保以下优势：

- 通过减少解决网络问题的时间，增加网络的正常运行时间。
- 通过减少需要反应性故障排除和修复的网络问题的发生，降低网络支持成本。
- 通过减少管理系统范围的更改的时间，降低网络运营成本。

网络上的每个设备都配置为提供特定的服务。在设备的配置中包含有关该设备如何运行以及如何自定义的详细信息。

通过 Network Configuration Manager 可以执行以下任务：

- 管理在 CA Spectrum 或 OneClick 中建模的受支持设备的配置。
- 捕获网络设备配置，并将其存储在 CA Spectrum 数据库中。
- 比较运行和启动配置。

- 上传 Perl 配置脚本。
- 加载固件。
- 导出配置。
- 加载配置并将其合并到同一系列类型的一个或多个设备。

  注意：合并内容会将信息附加到现有文件（它不会覆盖或还原）。
- 验证在设备上运行的配置是否正确。
- 设置自动捕获和策略的排定，以确保设备配置可靠。
- 通过验证设备配置来检测性能问题。
- 维护网络设备配置的历史记录以便进行比较和故障排除。
- 创建用于监控配置中内容的策略，并验证设备内容是否遵从策略。

访问 Network Configuration Manager

要从 OneClick 控制台访问 Network Configuration Manager，请从“资源管理器”选项卡中选择“配置管理器”：

展开“配置管理器”节点时，将出现“设备系列”、“策略”和“任务”视图。

注意：有关 OneClick 的详细信息，请参阅 *《操作员指南》*。

关键术语

以下术语对于了解 Network Configuration Manager 很重要。

批准工作流

允许您要求通过 Network Configuration Manager 启动的配置更改在被执行之前获得批准。可以对批准工作流进行设置，以将 CA Service Desk 故障单或 CA Spectrum 授权权限用于批准流程。

批量任务

批量任务是可以在多个设备上运行的任务。以下批量任务是可用的：上传、同步、保存到启动、加载固件任务、重新加载和取消重新加载。

设备系列

一组设备，它们共享访问设备配置的公共方法。Network Configuration Manager 为其提供了即用型支持的设备将自动放置在设备系列中。可以使用扩展实用工具创建更多的设备系列。

全局同步任务

使用排定，收集网络上启用了 Network Configuration Manager 的所有设备的运行配置。选择一个时间段和重复频率，以从网络范围的所有受支持设备捕获配置。通过捕获网络上所有设备的配置，维护运行配置历史记录。

加载固件任务

将固件上传到 Cisco IOS 和支持 SSH 的 Cisco IOS 设备。

Network Configuration Manager 策略

监控配置中的内容，并验证设备内容是否遵从策略。策略指定设备主机配置的特定方面。每次捕获到设备的主机配置文件时，都会检查并比较策略。违反策略的设备可以生成警报，且可以进行半自动修复。在设备上发生配置更改时，将检查策略的遵从性。

参考配置

充当基准以达到参考目的的设备配置。可以将其他配置与参考配置进行比较。如果当前配置与参考不同，则可以在设备上断言警报。

重新加载任务

在上传固件之后，重新加载设备。该任务可用于 Cisco IOS 和支持 SSH 的 Cisco IOS 设备。

可重用任务

一个任务，在被执行后一直存在，且可以重新运行多次而无需重新定义。也可以创建重复的排定，以便按预定的时间运行可重用任务。

保存到启动任务

将当前的运行配置写入一个或多个选定设备的启动配置。设备在 NVRAM（稳定随机存取内存）中保存其配置。可以在多个设备上运行该任务。

单个设备

CA Spectrum 正在监控的网络中设备的表示形式。配置单个设备将覆盖所有的全局设备系列配置。

同步任务

捕获并验证网络上选定设备的策略遵从设备配置，然后实时显示结果。同步任务捕获设备配置时，它将根据与设备有关的所有策略对配置进行验证。可以在多个设备上运行该任务。

上传任务

将新内容合并到一个或多个选定设备的运行配置中。可以在多个设备上运行该任务。

配置类型

以下各节介绍设备的不同配置。

运行配置

运行配置是在设备上加载的配置版本，它定义设备的当前运行方式。运行配置仅对当前的运行时会话有效。

启动配置

启动配置是在设备上存储的配置备份版本。重新启动设备时，将使用启动配置。一些设备具有主要和次要启动配置。在重新启动设备时，该设备会将以前的运行配置替换为启动配置的副本。

配置文件

配置文件包含设备制造商提供的运行配置的属性子集。许多设备允许 Network Configuration Manager 捕获完整的配置文件。可以编辑所捕获的配置文件。

支持的设备

Network Configuration Manager 为以下供应商的设备系列提供了即用型支持：

- Cisco
- Enterasys
- Enterasys
- Riverstone SSR
- Extreme
- Foundry
- Juniper
- Lancom
- Nortel（Baystack 和 Passport）

使用 Network Configuration Manager 扩展实用工具，可以配置不属于为其提供了即用型支持的设备系列之一的设备。

通过查询设备认证数据库，可以获取所有受支持设备的列表。要访问设备认证数据库，请导航到 CA 支持网站。CA Spectrum 产品页上的“Recommended Reading”（建议阅读的内容）部分包含指向“Device and Technology Certification”（设备和技术认证）的链接。有关详细信息，请参阅 *《认证用户指南》*。

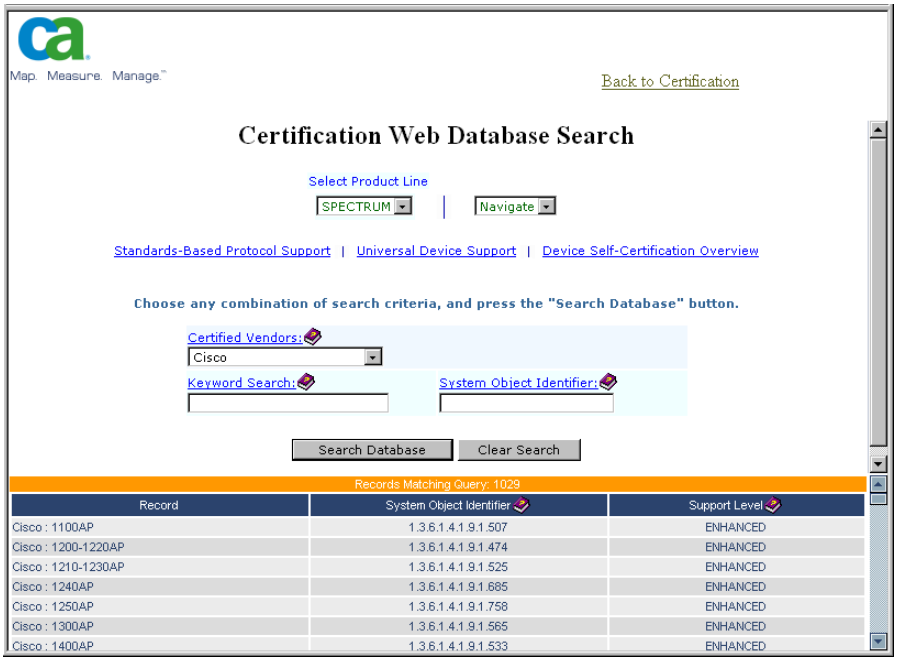
访问设备认证数据库

使用 CA 技术支持网站上的应用程序，您可以搜索 CA Spectrum 认证的所有设备。您可以确定 CA Spectrum 是否支持特定的设备模型，并按固件版本和发行版本进行筛选。还可以确定设备是否受简单认证或增强认证支持。

遵循这些步骤:

1. 导航到 CA 在线支持网站。
2. 访问 CA Spectrum 产品页面。
3. 单击“建议阅读”链接。
4. 单击“设备和技术认证”链接。
5. 在该页面上，单击“搜索引擎”链接。

   将显示“证书 Web 数据库搜索”应用程序。
6. 从“产品系列”下拉列表中选择 Spectrum 产品。



7. 根据需要完成以下搜索条件字段，以查找相关设备：

   获得认证的供应商

   CA Spectrum 已认证的生产一个或多个设备的企业或组织。供应商筛选可将您的搜索范围限定为选定供应商拥有或获得的所有设备。

   关键字搜索

   每个设备的“设备类型名称”字段中的搜索。关键字搜索可将您的搜索范围限定为包含“设备类型名称”字段中特定关键字的所有设备。

系统对象标识符

搜索整个系统对象标识符或部分系统对象标识符。将返回包含您输入的序列的所有设备。

例如，1.3.6.1.4.1.9.1.685 标识了 Cisco 1240AP 设备。

注意：并非所有设备都包含唯一的系统对象标识符。此外，一些设备缺少*系*统对象标识符。

支持级别

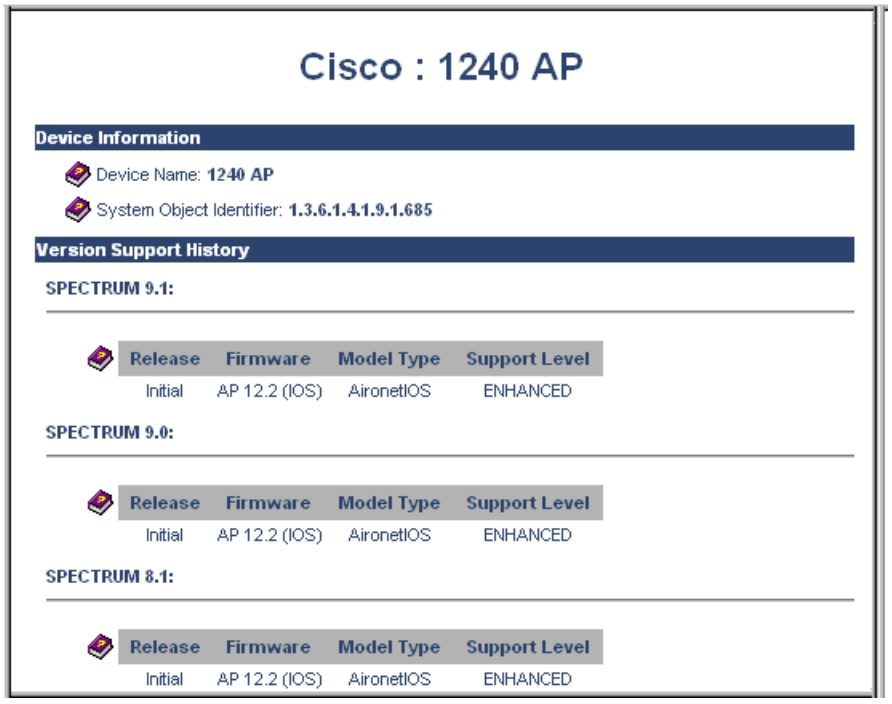
表示当前的 CA Spectrum 认证支持级别。提供了两种认证支持级别。有关详细信息，请参阅概述主题。

8. 单击“搜索数据库”按钮启动基于您的搜索条件的搜索。

   将针对每个设备分行显示结果。此级别的详细信息包括设备名称和模型、系统对象标识符和支持级别。

9. 单击结果表中的特定条目。

   将显示选定设备的详细信息，如下所示：



设备系列

要获得 Network Configuration Manager 支持，设备必须与设备系列关联。为其提供了即用型支持的设备将自动分配给适当的设备系列。一个设备只能属于单个设备系列。

Network Configuration Manager 设备系列提供了用于配置访问方法的中心位置。访问方法用于从其他系列成员访问设备配置。可以在本地设备上覆盖设备系列设置。有关详细信息，请参阅配置设备系列 (p. 38)。

通过 Network Configuration Manager 扩展实用工具，可以按需创建更多的设备系列，从而扩展 Network Configuration Manager 以支持更多的设备和供应商。有关手动创建更多的设备系列以及将设备手动移动到用户创建的设备系列的详细信息，请参阅扩展实用工具 (p. 20)。

Network Configuration Manager 如何确定设备系列

Network Configuration Manager 自动确定为其提供了即用型支持的设备的设备系列。通常，基于供应商做出该确定。有关详细信息，请参阅支持的设备 (p. 149)。

Cisco IOS 设备

对于 Cisco IOS 设备，存在以下设备系列：

- 支持 SSH 的 Cisco IOS （支持 SSH/SCP 通信模式）
- Cisco IOS（不支持 SSH/SCP 通信模式）

要将设备放置到支持 SSH 的 Cisco IOS 系列中，必须满足以下条件：

- 设备描述符必须指示 12.2 (18) 或更高的固件版本。
- 功能集必须包含字母“K9”，指示设备具有 SCP 所需的必要加密功能。
- 在发现时，必须取消阻止对设备的 SSH 访问。

  注意：如果在发现时阻止对设备的 SSH 访问（例如，通过防火墙），则将设备放置在 Cisco IOS 设备系列中。

例如，具有以下说明的设备将放置在支持 SSH 的 Cisco IOS 系列中：

Cisco IOS 软件，7200 软件 (C7200-JK9S-M)，版本 12.3(14)T6，发行软件 (fc2)
技术支持：http://www.cisco.com/techsupport
版权所有 (c) 1986-2006，Cisco Systems, Inc.
由 dchih 编译于 2006 年 1 月 5 日（星期四）05:36

具有以下说明的设备将放置在 Cisco IOS 系列中，且无法使用 SSH/SCP 获取配置：

Cisco 网间操作系统软件
IOS (tm) C2600 软件 (C2600-J1S3-M)，版本 12.3(17a)，发行软件 (fc2)
技术支持：http://www.cisco.com/techsupport
版权所有 (c) 1986-2005，cisco Systems, Inc.
编译于 2005 年 12 月 12 日（星期一）1 点

Cisco NX OS 设备

通过使用 Net::SSH::Expect 模块的脚本支持 Cisco NX OS 设备。要为 Cisco NX OS 设备提供即用型支持，必须使用这些模块设置 Perl 区域。

有关设置 Perl 环境的信息，请参阅 Perl 模块 (p. 58)。

Juniper JUNOS 设备

Network Configuration Manager 利用 JUNOScript API 与 JUNOS 设备进行通信。特别是，JUNOScript API merge 命令用于完成上传，如下所示：

```
<load-configuration format="text" action="merge">
```

JUNOScript 支持是使用 JUNOScript 版本 6.3R1 开发的。新版本的 JUNOScript API 通常向后兼容。

JUNOScript API 命令与 JUNOS CLI 命令不同。因此，Network Configuration Manager 上传必须使用正确的格式，上传才能成功。

有关 JUNOScript API 的详细信息，请参阅 Juniper 的文档网站。

示例：使用 JUNOScript API 格式

以下示例说明从 JUNOS CLI 命令行输入的命令如何与 JUNOScript API 不同。该命令将 snmp 位置字段从设备中删除。

测试设备具有以下配置文本块，用于将 snmp 位置字段值设置为“Boston”：

```
snmp {
     name jun2300-96.4;
     description "Juniper J2300 w/ JUNOS 9.0R4 built 2008-11-18 18:55:38 UTC";
     location Boston;
```

可以从 JUNOS CLI 命令行使用以下命令，在该设备上删除 snmp 位置字段：

```
admin@jun2300-96.4# delete snmp location
```

以下 Network Configuration Manager 上传从设备中删除 snmp 位置字段：

```
snmp {
     delete: location;
}
```

这两个操作是等效的；但是，JUNOScript API 语法必须用于 Network Configuration Manager 上传。

扩展实用工具

通过 Network Configuration Manager 扩展实用工具，可以将 Network Configuration Manager 的功能扩展到其即用型支持之外。通过扩展实用工具，可以执行以下任务：

- 按需创建更多的设备系列。通过使用 Perl 脚本，可以将这些额外的设备系列配置为在更多设备上扩展 Network Configuration Manager 功能。有关创建设备系列的详细信息，请参阅创建自定义设备系列 (p. 50)。有关配置脚本的详细信息，请参阅扩展实用工具脚本配置 (p. 53)。
- 通过将 Perl 脚本用于 Network Configuration Manager 在设备上执行的任何操作，可管理更多的设备和供应商。这些操作包括捕获或写入启动配置等操作； 还包括捕获或上传运行配置、上传设备固件、重新加载设备和在设备上取消重新加载操作。在 Network Configuration Manager 中可以为其中每个操作配置脚本。有关使用自定义脚本执行这些操作的详细信息，请参阅 Network Configuration Manager 扩展实用工具 (p. 49)。
- 为您的安装创建可用于关联配置更改事件信息的自定义陷阱设置。有关详细信息，请参阅配置通知陷阱设置 (p. 42)。

Network Configuration Manager 先决条件

要在托管网络上运行 Network Configuration Manager 并主动维护设备配置的运行历史记录，请执行以下步骤：

- 如果使用的是 SNMP，则用读取/写入团体字符串对设备建模。有关详细信息，请参阅 *《IT 基础架构管理与建模 - 管理员指南》*。
- 如果使用的是 SSH，则验证设备是否启用了 SCP。有关详细信息，请参阅通信模式 (p. 21)。

通信模式

下表列出了在 Network Configuration Manager 中支持的设备的通信模式支持。列中的“X”表示通信模式受该设备系列支持。当 Perl 脚本是与设备进行通信的唯一方式时，系统将通知您脚本使用的方法。

请参阅配置 TFTP 服务器 (p. 30)，为使用 SNMP/TFTP 通信模式的设备启用配置捕获和加载。

设备系列	SNMP/TFTP	Telnet/FTP	SSH/SCP	SSH/TFTP	Perl
Cisco CatOS	X				X
Cisco IOS	X	X			X
支持 SSH 的 Cisco IOS	X	X	X		X
Cisco NX OS					SSH
Cisco PIX OS					Telnet
Enterasys	X				X
Enterasys/Riverstone SSR	X				X
Extreme	X				X
Foundry	X				X
Juniper JUNOS			X		X
Lancom LCOS					TFTP/ Telnet
Nortel Baystack				X	X
Nortel Passport 8600	X				X
Nortel Passport L3	X				X

SSH v2 支持

Network Configuration Manager 仅支持 SSH v2。Network Configuration Manager 不支持 SSH v1。不会将仅支持 SSH v1 的 Cisco 设备自动放置在支持 SSH 的 Cisco IOS 系列中。

Network Configuration Manager 不支持仅支持 SSH v1 的 Juniper 设备。

要支持 SSH v2，请在 Cisco 或 Juniper 设备上安装或更新固件。按照将设备放置在设备系列 (p. 52)中的步骤添加设备。

Cisco 设备和 SCP

Cisco 设备必须已启用安全复制 (SCP)，才能使用 SSH 通信模式。

有关 SCP 的详细信息，请参阅 http://www.cisco.com 上 Cisco IOS 安全复制功能的文档。

未经请求的设备配置更改通知

在发生任何更改后，Network Configuration Manager 会立即尝试捕获设备配置。未经请求的配置更改通知可以是从发生更改的设备发送的陷阱或 MIB 对象。

有些设备在其配置更改时发送 SNMP 陷阱。SpectroSERVER 然后执行捕获并将配置保存在数据库中，以提供已更新的配置数据。根据最新的配置捕获，测试 Network Configuration Manager 策略。有关详细信息，请参阅设备陷阱 (p. 22)。

可以从这些配置陷阱通知解析选定的信息，并将其显示在“主机配置”表中。有关详细信息，请参阅配置通知陷阱设置 (p. 42)。

有些设备会更新 MIB 属性以通知配置更改，以代替发送 SNMP 陷阱或者还发送 SNMP 陷阱。SpectroSERVER 然后在识别到属性中的更改时，轮询 MIB 并捕获新配置。有关详细信息，请参阅设备 MIB 对象 (p. 23)。

Network Configuration Manager 监控一部分受支持设备上的通知。可以扩展 Network Configuration Manager，以监控来自其他受支持设备的更多陷阱和 MIB 对象。

启用未经请求的设备配置更改通知可为网络中的设备提供最新的配置捕获。可以禁用该功能以避免不必要的捕获，这涉及可能会降低网络性能的 TFTP 传输。有关详细信息，请参阅配置常规配置 (p. 25)和在单个设备上配置未经请求的设备配置捕获 (p. 45)。

设备陷阱

Network Configuration Manager 支持以下两个陷阱：

- Cisco：ciscoConfigManEvent 1.3.6.1.4.1.9.9.43.2
- Juniper：jnxCmCfgChange 1.3.6.1.4.1.2636.4.5

接收到其中任一陷阱时，CA Spectrum 将生成事件 0x00821029。此事件然后触发 Network Configuration Manager 以执行捕获。如果要为其他受支持设备触发捕获，请将更多的配置更改陷阱映射到该事件。

设备 MIB 对象

发生任何配置更改时，Network Configuration Manager 会通过要确定的模型属性轮询 MIB 对象。在支持以下 MIB 对象的 Cisco 和 Juniper 设备上，支持该功能：

- CISCO-CONFIG-MAN-MIB：ccmHistoryRunningLastChanged 1.3.6.1.4.1.9.9.43.1.1.1
- JUNIPER-CFGMGMT-MIB：jnxCmCfgChgLatestTime 1.3.6.1.4.1.2636.3.18.1.2

可以将属性轮询机制扩展到其他受支持设备。使用模型类型编辑器创建要为配置更改通知轮询的属性，使其成为已轮询的属性。然后，将 Config_Change_AttrID 属性 (0x12bf8) 的值设置为新创建的已轮询属性的属性 ID。Network Configuration Manager 接下来为配置更改通知监控此属性并执行捕获。

全局集合

通过全局集合可以组织网络设备的视图。一个全局集合包含来自多个供应商的设备。执行批量任务或者创建 Network Configuration Manager 策略时，全局集合很有用。

有关全局集合的详细信息，请参阅 *《IT 基础架构管理与建模 - 管理员指南》*。

详细信息：

将策略应用于全局集合 (p. 133)
使任务与全局集合关联 (p. 101)

维护模式

对处于维护模式的任何设备，禁用 Network Configuration Manager。要验证设备是否处于维护模式，请从“资源管理器”选项卡中选择设备，然后单击“信息”选项卡。在“常规信息”视图下，查看“维护中”选项。如果该选项设置为“是”，则设备处于维护模式。

Network Configuration Manager 报告包

在 CA Spectrum Report Manager 中的网络配置管理报告包下，包括了 Network Configuration Manager 报告选项。Report Manager 提供了大量的报告内容、格式和报告组织选项。可以为组织中对设备配置更改感兴趣的不同受众生成具有相应类型和信息范围的报告。

有关详细信息，请参阅来自 Report Manager 的 Network Configuration Manager 报告 (p. 76)和*《Report Manager 用户指南》*。

第 2 章： Network Configuration Manager 配置

此部分包含以下主题：

配置 Network Configuration Manager (p. 25)
配置设备系列 (p. 38)
配置单个设备以覆盖设备系列设置 (p. 44)
Network Configuration Manager 扩展实用工具 (p. 49)

配置 Network Configuration Manager

本节介绍 Network Configuration Manager 的基本配置。

执行常规配置

选择一些初始设置，以确定 Network Configuration Manager 如何执行配置捕获和关联更改事件。

遵循这些步骤:

1. 在“资源管理器”选项卡中选择“配置管理器”。

   信息和设置将出现在“内容”面板的“信息”选项卡中。

2. 展开“常规配置”子视图。

   将出现“常规配置”选项。

3. 根据需要，修改以下“常规配置”选项：

   未经请求的设备配置捕获

   允许或禁止 Network Configuration Manager 在从设备接收到未经请求的通知时捕获该设备的配置。未经请求的配置更改通知可以是 Network Configuration Manager 监控其更改的陷阱或 MIB 对象。

   关联事件期间(秒)

   指定关联配置更改事件期间的时间。在该期间发生的特定设备的所有配置更改事件都将组合到单个事件中。

   默认值： 120

捕获最新模型化设备的配置

指定如何在全局级别上处理网络上最新模型化的设备。可用的值包括：

在下一个全局同步上

按照全局同步排定，捕获最新模型化的设备。

不捕获

在最新模型化的设备上禁用 Network Configuration Manager。要启用 Network Configuration Manager 功能，请在设备上手动启用 Network Configuration Manager。

立即

立即捕获最新模型化的设备（在它们已模型化后），而不是等待全局同步运行。

任务工作队列大小

指定在每个 CA Spectrum 主机上并行处理的最大设备数。

手动停止正在运行的任务时，接收到停止命令后将处理当前处于队列中的所有设备。

默认值： 10

选择“配置历史记录”设置

以下过程介绍如何控制已捕获配置的存储。可以按为每个设备保留的配置数或者按时间长度，维护已捕获的配置。

重要说明！指定如何存储已捕获的配置时，请考虑对 SpectroSERVER 数据库的影响。如果保留太多的配置，则可能使 SpectroSERVER 数据库中充满配置文件模型。

遵循这些步骤:

1. 在“资源管理器”选项卡中选择“配置管理器”。

   信息和配置将显示在“内容”面板的“信息”选项卡中。

2. 展开“配置历史记录”子视图。

   将出现用于控制如何存储已捕获配置的选项。

3. 选择以下选项之一：

   - **指定每台设备要存储的最大配置数。**该选项基于指定的数字存储每台设备的已捕获配置。

每个设备的最大存储配置

指定每个设备的最大存储配置数。例如，数字 25 表示每个设备的最后 25 个配置驻留在 CA Spectrum 数据库中。

默认值：25

- **指定配置存储的最长天数。**该选项基于时间长度存储已捕获的配置。

存储主机配置的最长天数

指定主机配置在被销毁之前存储的最长天数。

注意：根据捕获配置的频率，指定大时段可能会导致 SpectroSERVER 数据库中充满配置文件模型。

默认值：30（天）

每台设备的最低存储配置

指定每台设备存储的最小主机配置数。为了保持该最小值，即使配置已过期，也会保留它们。

默认值：5

选择“配置更改报警”设置

“配置更改报警”设置控制哪些配置更改事件将触发警报以及生成的警报类型。可以选择“配置更改报警”设置以确定看到的警报。

遵循这些步骤:

1. 在“资源管理器”选项卡中选择“配置管理器”。

   信息和配置将显示在“内容”面板的“信息”选项卡中。

2. 展开“配置更改报警”子视图。

   将显示“配置更改报警”选项。

3. 根据需要，修改以下“配置更改报警”选项：

   报警模式

   指定触发警报的事件。

   任何更改时的警报

   仅对配置更改生成警报。

   任何参考违反时的警报

   仅对参考配置违反生成警报。

任何参考违反或更改时的警报

对参考配置违反和配置更改都生成警报。

无警报

对于任何配置更改，都不生成警报。

默认值：无警报

参考违反报警类型

指定发生参考配置违反时断言的警报或事件的类型。现有的比较掩码用于确定，当前配置和参考配置之间的重大差异。当前配置与参考配置匹配时，将自动清除参考违反警报。

有关设置参考配置的信息，请参阅指定参考配置 (p. 73)。

有效值为“关键警报”、“主要警报”、“次要警报”和“仅事件”。

默认值：仅事件

配置更改报警类型

指定发生任何配置更改时仅断言哪种类型的警报或事件。

有效值为“关键警报”、“主要警报”、“次要警报”和“仅事件”。

默认值：仅事件

批准工作流

通过批准工作流，可以要求通过 Network Configuration Manager 启动的配置更改在被处理之前获得批准。可以对批准工作流进行设置，以将 CA Service Desk 故障单或 CA Spectrum 授权权限用于批准流程。

本节介绍如何配置批准工作流选项。它还介绍在启用了 OneClick 批准工作流模式的情况下如何批准任务。

有关使用任务启动配置更改的信息，请参阅 Network Configuration Manager 设备级任务 (p. 81)和 Network Configuration Manager 批量任务 (p. 85)。

注意：有关详细信息，请参阅*《CA Spectrum 和 CA Service Desk 集成指南》*。

配置工作流选项

通过批准工作流，可以要求通过 Network Configuration Manager 启动的配置更改在被处理之前获得批准。配置批准工作流选项，以确定如何请求和处理批准。

遵循这些步骤:

1. 在“资源管理器”选项卡中选择“配置管理器”。

   信息和配置将显示在“内容”面板的“信息”选项卡中。

2. 展开“工作流”子视图。

   将显示批准工作流选项。

3. 根据需要，修改以下批准工作流设置：

   批准工作流模式

   指定修改设备的所有操作是否都需要批准。这些操作包括上传、保存到启动、加载固件、重新加载和取消重新加载任务。

   已禁用

   指定在 Network Configuration Manager 中启动的配置更改不需要批准。

   ServiceDesk

   指定在 Network Configuration Manager 中启动的配置更改必须通过 CA Service Desk 获得批准。创建任务时，将生成 CA Service Desk 故障单。如果已批准，则任务将置于可以处理它的状态。

   如果选择该选项，则启用“配置”按钮。单击“配置”按钮以调用“ServiceDesk 工作流配置”页，在该页中可以设置以下字段的初始值：

   错误类型 - 在 Service Desk 中配置错误类型值以便与 CA Spectrum 集成使用。有关这些值的详细信息，请参阅 *《CA Service Desk 实施指南》*。

   已批准状态、已拒绝状态、已取消的状态、等候批准状态 - 可用的状态值随错误类型的不同而不同。在 CA Service Desk 中配置状态值以便与 CA Spectrum 集成。有关设置这些值的信息，请参阅 *《CA Spectrum 和 CA Service Desk 集成指南》*。

   注意：如果启用了 Service Desk 批准，且创建任务的用户具有“任务批准者”权限，则 CA Service Desk 批准是可选的。有关详细信息，请参阅 Network Configuration Manager 权限 (p. 213)。

OneClick

指定仅当具有“任务批准者”权限的用户启动或批准时，才可以处理在 Network Configuration Manager 中启动的配置更改。

默认值：已禁用

在批准流程中包含配置更改

指定是否在批准请求中包含配置内容。

默认值：否

注意：用户必须具有“在批准请求中隐藏配置更改”权限，该选项才能生效。有关详细信息，请参阅 Network Configuration Manager 权限 (p. 213)。

在 OneClick 中批准任务

如果启用了 OneClick 批准工作流模式，则具有“任务批准者”权限的用户必须从 OneClick 控制台批准任务。

注意：也可以从电子邮件通知批准或拒绝任务。为任务请求批准时，将生成电子邮件，并将其发送到任务批准者以供批准。通过电子邮件中包含的链接，可以批准或拒绝任务。选择相应的链接。将更新状态以反映任务已批准还是已拒绝。

遵循这些步骤:

1. 在“资源管理器”选项卡的“配置管理器”下，选择“任务”文件夹中的“任务”。

   可用任务将出现在“内容”面板的“列表”选项卡中。

2. 右键单击任务，然后从右键单击菜单中适当地选择“批准任务”、“拒绝任务”或“取消批准请求”。

   将更新任务状态，以分别反映任务是已批准、已拒绝还是已取消。

配置 TFTP 服务器

本节介绍如何在 SpectroSERVER 系统上启动普通文件传输协议 (TFTP) 服务器。TFTP 传输配置文件。该过程包括两个步骤：

- 将您的系统设置为 TFTP 服务器。该步骤随平台的不同而有所不同。
- 在 OneClick 中指定 TFTP 配置设置。

如果具有分布式 SpectroSERVER (DSS) 环境，则 TFTP 服务器必须在每个 SpectroSERVER 上运行才能启用 Network Configuration Manager 功能。

有关支持的设备系列通信模式，请参阅通信模式 (p. 21)。

注意：使用相应的团体名称（读取或写入），验证网络中的每个设备是否已正确建模。

将系统设置为 TFTP 服务器

本节介绍如何将系统设置为 TFTP 服务器。操作说明随平台的不同而有所不同。

配置 Solaris 版本 10 或 11 系统以支持 TFTP

以下过程可设置您的 Solaris（版本 10 或版本 11）系统以支持 TFTP。

遵循这些步骤:

1. 以 root 用户身份登录。
2. 创建/tftpboot 目录，并使用以下命令为所有用户授予对该目录的读/写权限：

   ```
   mkdir /tftpboot
   chmod 777 /tftpboot
   ```

   注意：TFTP 服务器可以在 SpectroSERVER 主机系统以外的系统上运行。但是，SpectroSERVER 计算机必须能够访问 TFTP 服务器的根目录，而且 SpectroSERVER 计算机上的根目录必须与 TFTP 服务器共享。有关详细信息，请参阅使用远程 TFTP 或 FTP 服务器时的注意事项 (p. 36)。
3. 验证 /etc/services 文件是否包含 TFTP 条目。要搜索该条目，请输入以下命令：

   ```
   cd /etc
   grep tftp services
   ```

   您会在 /etc/services 文件中看到以下条目：

   ```
   tftp          69/udp
   ```

   如果该条目未出现，请编辑 services 文件，并将它添加到“Host specific functions”部分中。
4. 在 /etc/inetd.conf 文件中找到以下行，并通过删除这一行开头的英镑字符 (#) 来取消注释该行：

   ```
   #tftp dgram udp6 wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot
   ```
5. 验证该条目以 -s /tftpboot 选项结束。此结尾指定 tftp 目录（在本例中为 /tftpboot）。
6. 运行 inetconv 命令。

7. 验证 tftp 服务已启用：

   ```
   svcs | grep tftp
   ```

   此时将显示以下响应：

   ```
   online Apr_10 svc:/network/tftp/udp6:default
   ```

8. 如果您的系统已设置为 TFTP 服务器，请验证已使用读/写团体字符串对设备建模，以便 TFTP 传输能够正常工作。

9. 如 TFTP 配置设置 (p. 33)中所述，在 OneClick 中配置 TFTP 设置。

配置 Linux 系统以支持 TFTP

以下过程设置 Linux 系统以支持 TFTP。

遵循这些步骤:

1. 以 root 用户身份登录。
2. 通过运行以下命令，验证在系统上是否安装了 TFTP 服务器：

   ```
   %rpm -q tftp-server
   ```

   以下消息表示安装了 TFTP 服务器：

   ```
   tftp-server-<version>.EL3.1
   ```

   如果未出现该消息，则未安装 TFTP 服务器。执行下列步骤：

   a. 从 Red Hat 网站下载 TFTP 程序包，网址为 http://www.redhat.com。

   b. 运行以下命令：

      ```
      % rpm -i <package.rpm>
      ```

   c. 按照 Red Hat 网站中安装 rpm 程序包的说明操作。

3. 使用以下命令，创建 /tftpboot 目录并将该目录的读取/写入权限授予所有用户：

   ```
   mkdir /tftpboot
   chmod 777 /tftpboot
   ```

   注意：TFTP 服务器可以在 SpectroSERVER 主机系统以外的系统上运行。但是，SpectroSERVER 计算机必须能够访问 TFTP 服务器的根目录，而且 SpectroSERVER 计算机上的根目录必须与 TFTP 服务器共享。有关详细信息，请参阅使用远程 TFTP 或 FTP 服务器时的注意事项 (p. 36)。

4. 转到 /etc/xinetd.d 目录。
5. 编辑名为 tftp 的文件，如下所示：

   ```
   Set disable=no
   ```

6. 保存并关闭文件。

7. 运行以下命令之一，以重新启动 xinetd 服务：

   - % service xinetd restart

     将显示以下消息：

     ```
     Stopping xinetd  OK
     Starting xinetd  OK
     ```

     或者

   - % killall -HUP xinetd

8. 验证 TFTP 服务器是否正在运行。

   注意：一种验证方法是运行 Network Configuration Manager 捕获。如果接收到 TFTP 超时错误/事件 0x821001，则它表示 TFTP 未运行。

9. 如 TFTP 配置设置 (p. 33)中所述，在 OneClick 中配置 TFTP 设置。

Windows 上的 TFTP 服务器

TFTP 服务器在 Windows 上通常不可用。如果将 TFTP 通信模式用于任何设备系列，请设置 TFTP 服务器。多个免费或商用应用程序可供使用。

对于远程主机上的 TFTP 服务器，请参阅使用远程 TFTP 或 FTP 服务器时的注意事项 (p. 36)，以将该服务器与 Network Configuration Manager 一起使用。

要配置 Windows 系统以支持 TFTP，请完成TFTP 配置设置 (p. 33)所述的过程。该过程中的步骤适用于您安装的任何 TFTP 服务器。

在 Windows 上配置 TFTP 服务器

本节描述如何在 OneClick 中配置 TFTP 设置。

注意：在执行以下过程之前，请确保您的系统已配置为 TFTP 服务器。有关详细信息，请参阅将系统设置为 TFTP 服务器 (p. 31)。

遵循这些步骤:

1. 在“资源管理器”选项卡中选择“配置管理器”。

   信息和配置将显示在“内容”面板的“信息”选项卡中。

2. 展开“TFTP 配置”子视图。

   将出现“TFTP 配置”表。

3. 根据需要修改以下设置。单击“设置”以编辑特定的字段，并在完成后按 Enter 键。

默认 TFTP 主机

格局的 TFTP 服务器 IP 地址，默认情况下是运行 SpectroSERVER 的主机系统。

此字段可用于全局更改 TFTP 服务器的 IP 地址。有关使用远程主机时的注意事项，请参阅使用远程 TFTP 或 FTP 服务器时的注意事项 (p. 36)。

注意：可以在属性编辑器中配置属性 DefaultTftpHost。

默认的 TFTP 目录

用于运行 TFTP 的路径名。单击“设置”，并输入有效的 TFTP 服务器路径，例如：

- 对于 Unix 系统，输入 /tftpboot
- 对于 Windows，输入 C:\win23app\SPECTRUM\NCM\tftp

注意：TFTP 服务器可以在 SpectroSERVER 主机系统以外的系统上运行。但是，SpectroSERVER 计算机必须能够访问 TFTP 服务器的根目录，而且 SpectroSERVER 计算机上的根目录必须与 TFTP 服务器共享。有关详细信息，请参阅使用远程 TFTP 或 FTP 服务器时的注意事项 (p. 36)。

TFTP 传输超时(秒)

时间间隔，在此之后 TFTP 传输将超时。单击“设置”，并指定与 TFTP 服务器联系时所用的超时值（以秒为单位）。默认值是 50 秒，这意味着在两次数据传输之间有 50 秒间隔。

格局

CA Spectrum 格局（仅用于显示）。

配置 FTP 服务器

配置 Network Configuration Manager，以便在 SpectroSERVER 系统上使用本地 FTP 服务器（请参阅通信模式 (p. 21)，了解支持的设备系列通信模式）。

如果部署的是将 FTP 用于文件传输的设备，请配置 FTP 服务器。我们建议为您的平台安装和配置一个本地 FTP 服务器。对于 Windows 平台，下列链接描述如何安装和配置本地 FTP 服务。

- Windows Server 2008：
  http://technet.microsoft.com/en-us/library/cc732769(WS.10).aspx
- Windows Server 2012：
  http://www.c-sharpcorner.com/UploadFile/cd7c2e/how-to-install-ftp-server-on-windows-server-2012/

遵循这些步骤:

1. 在“资源管理器”选项卡中选择“配置管理器”。

   信息和配置将显示在“内容”面板的“信息”选项卡中。

2. 展开“FTP 配置”子视图。

   将出现“FTP 配置”表。

3. 根据需要修改以下设置。单击“设置”以编辑特定的字段，然后按 Enter 键。

   默认 FTP 主机

   格局的 FTP 服务器 IP 地址。默认情况下，SpectroSERVER 在此主机系统上运行。

   此字段可用于全局更改 FTP 服务器的 IP 地址。有关详细信息，请参阅使用远程 TFTP 或 FTP 服务器时的注意事项 (p. 36)。

   注意：DefaultFtpHost 属性代表此值，可以在属性编辑器中配置该属性。

   FTP 用户名

   FTP 用户名。

   FTP 密码

   FTP 密码。

   默认的 FTP 目录

   用于运行 FTP 的路径名。

   注意：FTP 服务器可以在 SpectroSERVER 主机系统以外的系统上运行。但是，特定的要求适用于该目录。有关详细信息，请参阅使用远程 TFTP 或 FTP 服务器时的注意事项 (p. 36)。

   格局

   CA Spectrum 格局（仅用于显示）。

使用远程 TFTP 或 FTP 服务器时的注意事项

默认情况下，运行 SpectroSERVER 的主机系统也是 TFTP 和 FTP 服务器的主机系统。但是，可以将 TFTP 或 FTP 服务器设置为在不同的主机系统上运行。

要将 TFTP 或 FTP 服务器全局设置为在不同的主机上运行，请按照 TFTP 配置设置 (p. 33)和配置 FTP 服务器 (p. 34)中的说明，使用“默认 TFTP/FTP 主机”和“默认 TFTP/FTP 目录”字段。还可以如为单个设备指定 TFTP 或 FTP 服务器 (p. 36)中所述，通过使用属性编辑器覆盖主机的默认值。

注意：虽然可以按设备覆盖 TFTP 和 FTP 服务器主机系统，但是 TFTP 和 FTP 目录设置适用于整个格局。

使用 TFTP 或 FTP 服务器的远程主机而不是运行 SpectroSERVER 的本地系统时，请注意以下几点：

- 指定的 TFTP 和 FTP 目录都必须可从 CA Spectrum 主机系统以本地方式访问。将 TFTP 或 FTP 服务器的根目录与运行 SpectroSERVER 的计算机共享。
  - 对于 UNIX 系统，必须使用 read/write nfs mount 来挂接远程目录。
- 指定路径名时，应仅使用 UNC 路径；不允许使用局部变量或本地映射的目录。例如，要访问主机“tftpserver”上的共享文件夹“tftpboot”，请将 \\tftpserver\tftpboot 的 UNC 路径指定为默认 TFTP 目录。
- 在 Windows 系统上，UNC 路径不能要求用户名和密码，但要求读取和写入权限。

  注意：由于不支持映射驱动器，因此映射网络驱动器以及提供用户名和密码不会避开该要求。

为单个设备指定 TFTP 或 FTP 服务器

以下过程介绍如何在设备级别上为 TFTP 或 FTP 服务器指定单独的主机系统。

注意：要为格局全局设置 TFTP 或 FTP 主机，请如 TFTP 配置设置 (p. 33)和配置 FTP 服务器 (p. 34)中所述，分别使用“默认 TFTP 主机”和“默认 FTP 主机”字段。虽然可以按设备覆盖 TFTP 和 FTP 服务器主机系统，但是 TFTP 和 FTP 目录设置适用于整个格局。

遵循这些步骤:

1. 在“资源管理器”选项卡中，选择将在单独主机上使用 TFTP 或 FTP 服务器的设备。
2. 单击“内容”面板中的“列表”选项卡，然后选择设备。
3. 从“工具”菜单中选择“实用工具”，然后选择“属性编辑器”。

   将打开“属性编辑器”。
4. 选择“用户定义”文件夹，然后单击“添加”。

   将出现“属性选择器”窗口。
5. 在“属性选择器”窗口的“筛选”字段中输入“host”。选择“NCM_FTP_Host”和“NCM_TFTP_Host”属性，然后单击“确定”。

   这两个属性现在将出现在“用户定义”文件夹之下。
6. 选择“NCM_FTP_Host”和“NCM_TFTP_Host”属性，然后单击添加箭头。

   您可以修改的值将出现在右窗格中。
7. 修改每个属性的以下值：

   无更改

   清除该复选框可启用剩余的字段。

   IP 地址

   输入运行 TFTP 和 FTP 协议的主机系统的 IP 地址。

   注意：如果使用 NAT，则使用公共 IP 地址。

   设为默认值

   如果选中它，则新创建的所有设备都将自动继承该值。
8. 单击“确定”。如果打开“确认”对话框，单击“是”。

   “属性编辑结果”页将显示更改的结果。
9. 单击“关闭”。

选择用于设备配置导出的设置

可以对 Network Configuration Manager 进行配置，将设备配置导出到文本文件，以达到历史存档目的。在 CA Spectrum 和 OneClick 之外，必须手动管理该文件系统。

遵循这些步骤:

1. 在“资源管理器”选项卡中选择“配置管理器”。

   信息和配置将出现在“内容”面板的“信息”选项卡中。

2. 展开“导出配置”子视图。

3. 单击“导出配置”旁边的“设置”。默认值为“不导出”。选择以下选项之一：

   仅导出唯一配置

   仅当设备配置与以前捕获的配置不同时，才导出它们。

   导出唯一的和全局的同步配置

   仅当设备配置与以前捕获的配置不同或者进行全局同步时，才导出它们。例如，如果已将全局同步配置为每天运行一次，则每天为每个设备生成一个文件。有关详细信息，请参阅关于全局同步 (p. 67)。

   导出配置显示在“导出配置”旁边。

4. 单击“导出目录”列中的“设置”。然后，指定一个用于导出 UNIX (Solaris/Linux) 和/或 Windows 的配置文本文件的本地目录。导出文件是用设备名和时间戳命名的。如果要将配置文本文件导出到网络共享，请指定该目录的 UNC 路径。例如，\\Shared_Server\Export\ExportFiles。

5. 按 Enter 键。

   将出现导出目录。

配置设备系列

设备系列提供了一个中心位置，用于配置 Network Configuration Manager 与设备系列中设备的交互。对设备系列进行的配置在该系列中包含的所有设备上都生效。在本地设备级别上，可以覆盖设备系列设置。有关详细信息，请参阅配置单个设备以覆盖设备系列设置 (p. 44)。

要访问设备系列的配置，请从“资源管理器”选项卡中的“设备系列”选择设备系列。然后，在“内容”面板中选择“信息”选项卡。将显示设备系列配置。

通过扩展实用工具，可以配置 Perl 脚本，以处理任何受支持的 Network Configuration Manager 操作的设备交互。有关详细信息，请参阅 Network Configuration Manager 扩展实用工具 (p. 49)。

配置设备系列常规设置

“常规配置”子视图包含配置管理器设置。通过配置管理器，可以为整个设备系列禁用任务。配置管理器设置为“已禁用”时，在该设备系列包含的任何设备上都不执行 Network Configuration Manager 操作。

注意：如果设备系列中的任何设备要求禁用配置管理器，也可以在本地设备级别上禁用它。有关详细信息，请参阅配置单个设备以覆盖设备系列设置 (p. 44)。

遵循这些步骤:

1. 如访问 Network Configuration Manager 设备系列配置中所述，导航到设备系列配置，然后展开“常规配置”子视图。

   将出现选定设备系列的常规配置。

2. 单击“配置管理器”旁边的“设置”，为设备系列启用或禁用 Network Configuration Manager 任务和功能。默认情况下，启用配置管理器。

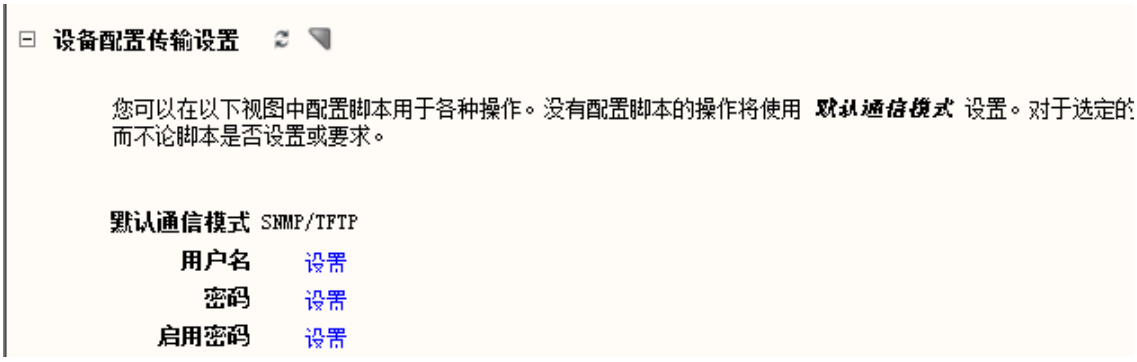
   设备系列与 Network Configuration Manager 进行通信的状态显示在“配置管理器”旁边。

配置设备系列通信模式

为其提供了即用型支持的所有设备系列都具有通信模式，该模式确定 Network Configuration Manager 如何与关联的设备进行交互。具有默认支持的一些设备系列允许您从多种通信模式中进行选择。根据所选的通信模式，可能需要设备用户名、密码和启用密码。

如果使用相同的用户名、密码和启用密码无法访问系列中的所有设备，则可以在本地设备上覆盖用户名和密码。有关详细信息，请参阅配置单个设备以覆盖设备系列设置 (p. 44)。

下图显示了“默认通信模式”设置，该设置出现在“设备配置传输设置”子视图中：



遵循这些步骤:

1. 从“资源管理器”选项卡中的“设备系列”选择设备系列，然后选择“内容”面板中的“信息”选项卡。

   将出现设备系列设置。

2. 展开“设备配置传输设置”子视图。

   将显示设备系列的通信模式配置。

3. 为选定的设备系列选择默认通信模式。

   选定的通信模式将显示在“默认通信模式”旁边。

4. 根据需要修改以下字段：

   用户名

   指定用于访问设备的用户名。

   密码

   指定用于访问设备的密码。

   启用密码

   指定用于配置设备的第二个密码（仅受 Cisco IOS、支持 SSH 的 Cisco IOS 和 Foundry 设备支持）。

   将配置选定设备系列的通信模式。

配置设备系列掩码

配置设备系列掩码，可从配置比较中排除设备配置内容或者对未经授权的用户隐藏敏感信息。掩码配置将在以下各节中进行讨论。

设备系列比较掩码

比较掩码是在与历史配置比较期间隐藏设备配置内容的正则表达式的列表。在比较配置文件期间，将忽略设备配置文件中与比较掩码中的正则表达式匹配的任何行。Network Configuration Manager 提供了预定义掩码的列表，这些掩码显示在比较掩码旁边的窗口中。

可以添加或删除掩码。

可以在本地设备级别上覆盖掩码设置。有关详细信息，请参阅配置单个设备以覆盖设备系列设置 (p. 44)。

添加设备系列查看掩码

查看掩码是对缺少查看整个设备配置文件的 OneClick 权限的用户隐藏设备配置内容的正则表达式的列表。需要有“查看无掩码的配置”权限才能查看“查看掩码”字段的内容。使用该设置可对未经授权的用户隐藏密码或其他内容。可以在本地设备级别上覆盖掩码设置。

遵循这些步骤:

1. 在“比较掩码”或“查看掩码”下选择“添加”。

   将打开“添加”对话框。

2. 键入选定设备系列的掩码。例如，对于注释行，输入：[!#]。提供任何正则表达式。
3. 单击“确定”。

   将出现为掩码输入的内容。已为设备系列中的所有设备设置掩码。

4. 重复上述步骤以输入更多的掩码。

有关在本地设备上覆盖设备系列设置的详细信息，请参阅配置单个设备以覆盖设备系列设置 (p. 44)。

输入掩码

可以输入适用于设备系列中所有设备的掩码。

遵循这些步骤:

1. 在“比较掩码”或“查看掩码”下选择“添加”。

   将打开“添加”对话框。

2. 输入选定设备系列的掩码。例如，对于注释行，输入：[!#]，或者输入任何正则表达式。
3. 单击“确定”。

   将显示为掩码输入的内容。现在已为设备系列中的所有设备设置掩码。

配置通知陷阱设置

可以配置 CA Spectrum，以基于来自设备的陷阱通知自动捕获设备配置。可以为您的安装自定义这些陷阱设置。指定从设备发出的配置更改陷阱通知解析并在“主机配置”表中显示的信息。Network Configuration Manager 使用这些设置关联配置更改事件信息，以便为特定的设备组合事件。

注意：“未经请求的设备配置捕获”设置控制设备的自动配置捕获。有关该功能的详细信息，请参阅未经请求的设备配置更改通知 (p. 22)。

陷阱格式信息随设备系列的不同而不同。为 Cisco CatOS、Cisco IOS、支持 SSH 的 Cisco IOS 和 Juniper JUNOS 设备系列提供了即用型支持。以下示例显示了 Syslog 陷阱，该类陷阱是支持 SSH 的 Cisco IOS 设备系列的默认陷阱：

```
Configured from {SOURCE} by {USER} on {LOCATION}
Configured from {LOCATION} by {SOURCE}
```

以下变量表示从陷阱消息解析出并在“主机配置”表中显示的信息：

SOURCE

对应于“主机配置”表中的“源”列。

USER

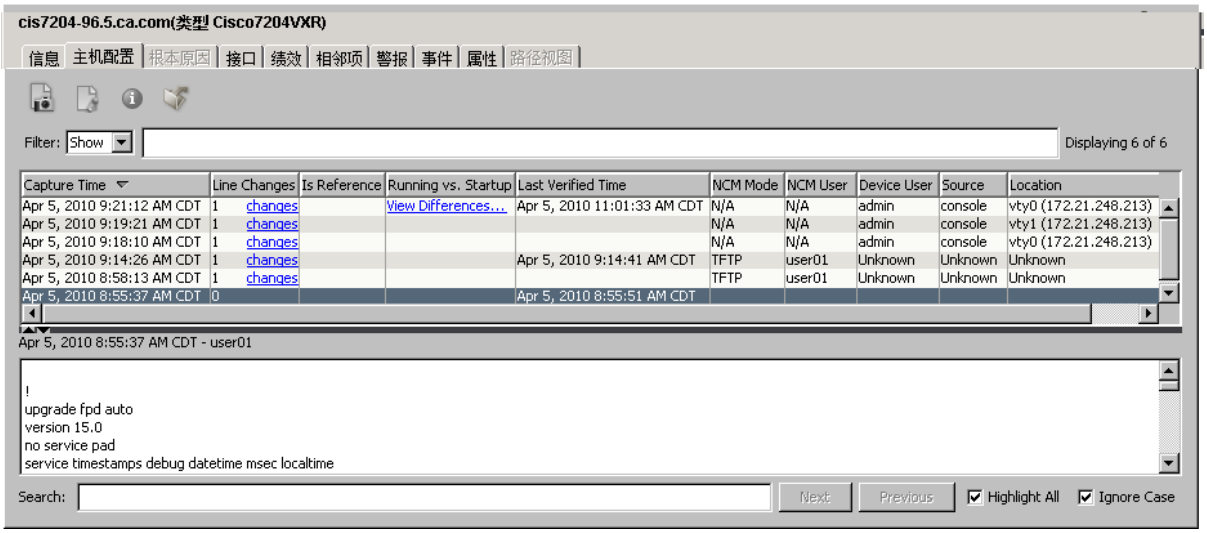
指定进行更改时登录到设备的用户。该值对应于“主机配置”表中的“设备用户”列。

LOCATION

对应于“主机配置”表中的“位置”列。

如果来自 Syslog 服务器的陷阱消息为非默认格式，则也可以指定其他消息格式。

下图显示了支持 SSH 的 Cisco IOS 设备的“主机配置”表，其中包括表的各列：



基于设备陷阱、Syslog 陷阱和事件、Network Configuration Manager 内部陷阱和映射到常规更改事件的任何其他陷阱，对信息进行关联。Network Configuration Manager 常规配置中的“关联事件期间”参数确定关联配置更改事件期间的时间。有关详细信息，请参阅配置常规配置 (p. 25)。

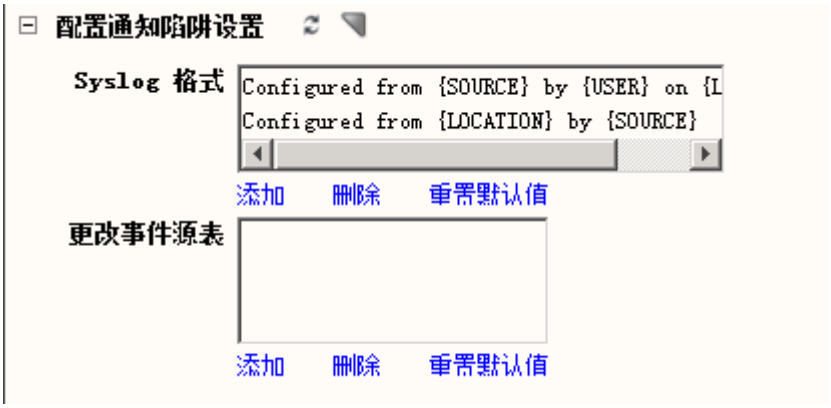
有关事件消息的详细信息，请参阅 Network Configuration Manager 事件 (p. 205)。

为设备系列配置通知陷阱设置。

遵循这些步骤:

1. 如访问 Network Configuration Manager 设备系列配置中所述，导航到设备系列配置，然后展开“配置通知陷阱设置”子视图。

   将出现选定设备系列的配置通知陷阱设置。将使用从 Syslog 服务器接收到的陷阱的基本格式配置该子视图。下图显示了 Cisco IOS 设备系列的默认设置：



2. 要添加 Syslog 格式，请执行以下步骤：
   a. 在“Syslog 格式”框下面单击“添加”。
      将打开“添加”对话框。
   b. 输入包含任何列特定信息（可以通过 {} 中的消息解析出）的陷阱消息的格式，然后单击“确定”。
   新的 Syslog 格式将添加到框中。
3. 要将条目添加到“更改事件源表”，请执行以下步骤：
   a. 在“更改事件源表”框下面单击“添加”。
      将打开“添加”对话框。
   b. 输入源索引条目，然后单击“确定”。
      新条目将添加到表中。

配置单个设备以覆盖设备系列设置

本节介绍如何配置单个设备，以覆盖其关联设备系列的配置。在本地设备级别上，可以覆盖大多数设备系列设置。

在单个设备上访问 Network Configuration Manager 设置

在“Network Configuration Manager”子视图中提供了单个设备的 Network Configuration Manager 设置。

遵循这些步骤:

1. 在“资源管理器”选项卡中选择设备。
   信息和配置将出现在“内容”面板的“信息”选项卡中。
2. 向下滚动页面，并展开“Network Configuration Manager”子视图。
   将出现 Network Configuration Manager 设备配置选项。
   在此处选择的设置将覆盖设备系列设置。

在单个设备上启用或禁用 Network Configuration Manager

可以在本地设备上禁用所有 Network Configuration Manager 操作。必须在关联的设备系列上启用 Network Configuration Manager，该设置才能影响设备。有关详细信息，请参阅配置设备系列常规配置 (p. 39)。

遵循这些步骤:

1. 如在单个设备上访问 Network Configuration Manager 设置 (p. 44)中所述，展开“Network Configuration Manager”子视图。

   将显示 Network Configuration Manager 设备配置选项。

2. 单击“配置管理器”旁边的“设置”，以启用或禁用 Network Configuration Manager 任务和 Network Configuration Manager 功能。

   注意：默认情况下，启用配置管理器。

   与 Network Configuration Manager 通信的当前状态显示在配置管理器旁边。

在单个设备上配置未经请求的设备配置捕获

可以在本地设备上启用或禁用未经请求的设备配置捕获。

注意：必须全局启用未经请求的设备配置捕获，该本地设置才能有效。

有关详细信息，请参阅未经请求的设备配置更改通知 (p. 22)。

遵循这些步骤:

1. 如在单个设备上访问 Network Configuration Manager 设置 (p. 44)中所述，展开“Network Configuration Manager”子视图。

   将出现 Network Configuration Manager 设备配置选项。

2. 单击“未经请求的设备配置捕获”旁边的“设置”以启用或禁用自动设备捕获。

   值将显示在“未经请求的设备配置捕获”旁边。

在单个设备上指定“配置更改报警”设置

可以在本地设备上启用或禁用“配置更改报警”设置。

遵循这些步骤:

1. 如在单个设备上访问 Network Configuration Manager 设置 (p. 44)中所述，展开“Network Configuration Manager”子视图。

   将出现 Network Configuration Manager 设备配置选项。

2. 展开“本地配置更改报警”子视图。

   将出现“本地配置更改报警”选项。

3. 单击“使用本地配置更改报警设置”旁边的“设置”以覆盖全局设置。

   值将出现在“使用本地配置更改报警设置”旁边。

4. 根据需要，修改以下“配置更改报警”选项：

   报警模式

   允许您指定触发警报的事件。

   任何更改时的警报

   仅对配置更改触发警报。

   任何参考违反时的警报

   仅对参考配置违反触发警报。

   任何参考违反或更改时的警报

   对参考配置违反和配置更改都触发警报。

   无警报

   确保不对任何配置更改触发警报。

   默认值：无警报

   参考违反报警类型

   指定发生参考配置违反时断言的警报或事件的类型。现有的比较掩码用于确定，当前配置和参考配置之间的重大差异。当前配置与参考配置匹配时，将自动清除参考违反警报。

   有关设置参考配置的信息，请参阅指定参考配置 (p. 73)。

   有效值为“关键警报”、“主要警报”、“次要警报”和“仅事件”。

   默认值：仅事件

   配置更改报警类型

   指定发生任何配置更改时断言的警报或事件的唯一类型。

   有效值为“关键警报”、“主要警报”、“次要警报”和“仅事件”。

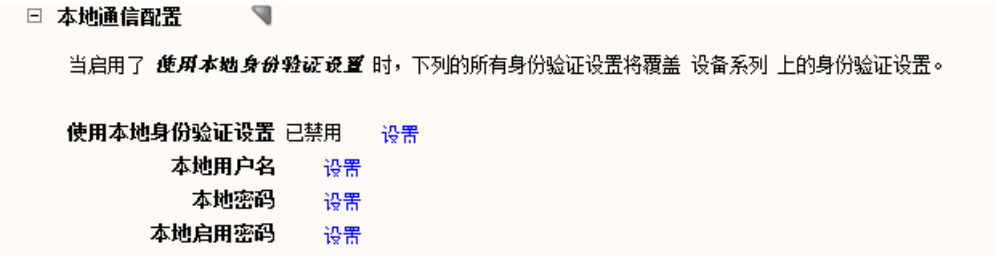
   默认值：仅事件

在单个设备上配置通信模式

为其提供了即用型支持的所有设备都具有确定 Network Configuration Manager 如何与设备交互的通信模式。为其提供了即用型支持的一些设备允许您从多种通信模式中进行选择。根据选定的通信模式，可能需要设备用户名、密码和启用密码。

有关为设备系列配置通信模式的详细信息，请参阅配置设备系列通信模式 (p. 39)。

下图是“本地通信配置”子视图的示例：



在单个设备上配置通信模式。

遵循这些步骤:

1. 如在单个设备上访问 Network Configuration Manager 设置 (p. 44)中所述，展开“Network Configuration Manager”子视图。

   将出现 Network Configuration Manager 设备配置选项。

2. 展开“本地通信配置”子视图。

   将出现“本地通信配置”选项。可用的选项取决于设备类型。

3. 根据需要修改“通信配置”选项：

   使用本地通信模式设置

   指定是否用本地默认通信模式覆盖设备系列通信模式。

   注意：如果在设备系列上为操作配置了脚本，则本地默认通信模式不用于该操作。

   本地默认通信模式

   如果设备允许您从多种通信模式中进行选择，则指定通信模式。

   使用本地身份验证设置

   指定是否覆盖设备系列身份验证设置。启用时，使用在“本地用户名”和“本地密码”字段中指定的值。

   本地用户名

   指定用于访问设备的用户名。

本地密码

指定用于访问设备的密码。

本地启用密码

指定用于配置设备的第二个密码（仅受 Cisco IOS、支持 SSH 的 Cisco IOS 和 Foundry 设备支持）。

将设置选定设备的本地通信配置选项。

在单个设备上配置掩码

通过配置掩码，可以从配置比较中排除脚本内容或者对未经授权的用户隐藏敏感信息。在本地设备级别上配置的掩码将覆盖设备的关联设备系列的掩码设置。单个设备上的掩码配置将在以下各节中进行讨论。

比较掩码

比较掩码是在与历史配置比较期间隐藏设备配置内容的正则表达式的列表。在配置文件比较期间，将忽略设备配置文件中与比较掩码中的正则表达式匹配的任何行。Network Configuration Manager 提供了预定义掩码的列表，这些掩码显示在比较掩码旁边的窗口中。本地设备上的掩码将覆盖设备系列的掩码设置。

查看掩码

查看掩码是对缺少查看整个设备配置文件的 OneClick 权限的用户隐藏设备配置内容的正则表达式的列表。只有具有“查看无掩码的配置”权限的操作员才能访问“查看掩码”字段中的内容。使用掩码可对未经授权的用户隐藏密码或其他内容。本地设备上的掩码将覆盖设备系列的掩码设置。

有关“查看无掩码的配置”权限的详细信息，请参阅 Network Configuration Manager 权限 (p. 213)。

在单个设备上输入掩码

可以为单个设备输入掩码。

遵循这些步骤:

1. 如在单个设备上访问 Network Configuration Manager 设置 (p. 44)中所述，展开“Network Configuration Manager”子视图。

   将显示 Network Configuration Manager 设备配置选项。

2. 展开“本地掩码配置”子视图。

   将显示本地比较和查看掩码选项。

3. 单击“使用本地比较掩码”或“使用本地查看掩码”旁边的“设置”，以覆盖设备系列设置。

   值将显示在选项旁边。

4. 在“本地比较掩码”或“本地查看掩码”下选择“添加”。

   将打开“添加”对话框。

5. 输入选定设备的掩码。例如，对于注释行，输入：[!#]，或者输入任何正则表达式。

6. 单击“确定”以接受您的输入。

   将显示为掩码输入的内容。现在已为选定设备设置掩码。

7. 重复步骤 4 到步骤 6 以输入更多掩码。

Network Configuration Manager 扩展实用工具

通过 Network Configuration Manager 扩展实用工具，可以扩展 Network Configuration Manager 的基本功能。通过将 Perl 脚本用于 Network Configuration Manager 在设备上执行的操作，可以创建设备系列以及管理其他设备和供应商。可以自定义陷阱设置，并使用它们关联配置更改事件信息。

以下各节介绍如何使用扩展实用工具来扩展 Network Configuration Manager 支持。

支持的操作

通过 Network Configuration Manager 扩展实用工具，可以使用 Perl 脚本将 Network Configuration Manager 扩展到其他设备和供应商。通过为 Network Configuration Manager 在设备上执行的任何操作或所有操作提供 Perl 脚本，可以扩展 Network Configuration Manager。以下列表汇总了这些操作：

捕获启动配置

捕获设备启动配置。

捕获运行配置

捕获设备运行配置。

上传运行配置

上传指定的内容并将其合并到设备运行配置中。

写入启动配置

将设备的当前运行配置写入其启动配置。

重新加载设备

重新启动设备。

取消重新加载

取消设备的已排定重新启动。

加载设备固件

在设备上启动指定固件映像的加载。

可以在按需创建的设备系列中为其中每个操作配置脚本。缺少脚本的任何操作，都将作为不受给定设备系列以及其中包含的所有设备支持的操作进行处理。

Cisco PIX OS 即用型设备系列提供了如何使用脚本扩展 Network Configuration Manager 支持的示例。（在这些示例脚本中，Net::Telnet perl 模块*不*支持 IPv6。）

该实用工具还允许您使用 Perl 脚本，改变 Network Configuration Manager 与属于即用型设备系列的设备的交互。

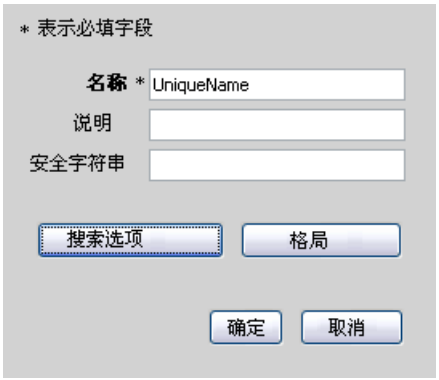
创建自定义设备系列

Network Configuration Manager 为 Cisco、Enterasys、Enterasys/Riverstone SSR、Extreme、Foundry、Juniper、Lancom、Nortel Baystack 和 Nortel Passport 设备系列提供了即用型支持。通过 Network Configuration Manager 扩展实用工具，可以创建自定义设备系列。

遵循这些步骤:

1. 在“导航”面板的“资源管理器”选项卡中，展开“配置管理器”。
2. 右键单击“设备系列”，然后选择“创建设备系列”。

   将打开“创建设备系列”对话框，如下图所示：



3. 在“名称”字段中输入唯一名称。
4. （可选）输入说明和安全字符串。
5. （可选）单击“格局”按钮以选择要在其中放置设备系列的格局。
6. 单击“搜索选项”按钮以搜索特定的设备。

   将打开“搜索选项”对话框。与全局集合一样，设备系列可以同时具有手动添加到系列的静态成员，以及使用指定的搜索标准自动添加的动态成员。有关详细信息，请参阅*《管理员指南》*。

   注意：一个设备只能属于一个设备系列。如果多个设备系列包含适用于同一设备的搜索标准，则要执行搜索的第一个设备系列包含该设备。

7. 完成后单击“确定”。

   设备系列将被创建，并出现在“导航”面板的“资源管理器”选项卡中的“设备系列”下。现在可以添加静态成员。

将设备放置在设备系列中

Network Configuration Manager 自动将为其提供了即用型支持的设备分配给系列。必须将当前与设备系列关联的设备手动移动到用户创建的设备系列。包含定义成员资格的搜索标准、手动创建的设备系列不会拉入已属于某个设备系列的设备。对于拉入新设备的搜索标准，设备当前不能是任何设备系列的成员。

有几个选项可以将设备放置在设备系列中。可以手动建立关联。

遵循这些步骤:

1. 查找设备。
2. 右键单击设备，然后选择“添加至”、“设备系列”。

   将打开“选择设备系列”对话框。
3. 选择要与选定设备关联的设备系列。

   如果未显示合适的设备系列，请通过单击“创建”创建自定义设备系列。有关详细信息，请参阅创建自定义设备系列 (p. 50)。

   设备现在与选定设备系列关联。

对于手动创建的设备系列，可以使用其已定义的搜索标准强制它更新。

遵循这些步骤:

1. 在“导航”面板中右键单击设备系列。
2. 选择“更新设备系列”。

   设备系列将搜索并添加满足搜索标准的所有设备（如果它们当前不属于设备系列）。

有关设备系列搜索标准的详细信息，请参阅创建自定义设备系列 (p. 50)。

也可以将设备还原到为其提供了即用型支持的设备系列之一。

遵循这些步骤:

1. 右键单击当前未与设备系列关联的设备。
2. 选择“重新配置”、“重新评估 NCM 设备系列”。

   重要说明！ Cisco PIX 设备不支持“重新评估 NCM 设备系列”功能。

Network Configuration Manager 重新评估设备，以确定它是否应属于即用型设备系列。

如果 Network Configuration Manager 确定放置是适当的，则设备将添加到设备系列。

注意：对于当前处于手动创建的设备系列中的设备，“重新评估 NCM 设备系列”操作无效。

有关为其提供了即用型支持的设备系列的详细信息，请参阅支持的设备 (p. 149)。

扩展实用工具脚本配置

使用 OneClick，执行与 Network Configuration Manager 脚本的所有交互。Network Configuration Manager 在 CA Spectrum 环境中处理所有的脚本管理。可用的脚本选项将在以下各节中进行讨论。

脚本注意事项

为 Network Configuration Manager 操作配置脚本时，该脚本将用于系列中的所有设备。例如，如果为支持 SSH 的 Cisco IOS 设备系列中的所有受支持操作配置了脚本，则设备系列上的“通信模式”设置和本地设备上任何被覆盖的“通信模式”设置将无效。在该示例中，将使用支持 SSH 的 Cisco IOS 设备系列中包含的所有设备上所有 Network Configuration Manager 操作的脚本。

在仅为 Network Configuration Manager 的一部分操作配置了脚本的情况下，Network Configuration Manager 将在设备系列上选定的或在本地设备上覆盖的通信模式用于没有为其配置脚本的操作。

用户名、密码和启用密码始终作为命令行参数发送到脚本。将使用在设备系列中指定的值，除非在本地设备上已覆盖它们，在这种情况下使用在本地覆盖的值。

默认的脚本命令行参数

默认情况下，Network Configuration Manager 按所示顺序将以下参数提供给每个脚本。如果脚本不利用这些参数，仍然必须编写脚本以接受它们。

- 设备 IP。
- 包含要上传内容的文件的绝对文件名。（仅限上传操作）。
- 设备用户名。

- 设备密码。
- 设备启用密码。

其他的脚本命令行参数

（可选）可以为每个支持的操作配置无限的其他命令行参数。这些参数在命令行上传递到脚本，位于默认参数集之后。这些参数按其在“其他脚本参数”列表中的显示顺序传递。

可以为“上传运行配置”和“加载设备固件”操作配置其他命令行参数，以便在运行时提示用户输入值。在运行时提示时，还可以显示标签和默认值。

错误代码映射

Network Configuration Manager 提供了以下功能：将脚本返回的非零整数值映射到出现错误时显示在 OneClick 中的文字错误消息。这样，脚本创建者就可以提供有关失败模式的详细信息。

脚本错误处理

为了使 Network Configuration Manager 报告基于脚本的操作的成功，脚本必须返回零值。Network Configuration Manager 假定：如果脚本返回非零值，则操作失败。

在 STDERR 缓冲区中返回的其他错误详细信息

如果脚本返回非零值（除了上述错误映射外），则 Network Configuration Manager 还将查找脚本在 STDERR 缓冲区中返回的任何输出。如果找到内容，则它将在 OneClick 中作为其他错误信息显示。

输入配置脚本

Network Configuration Manager 可以使用 Perl 脚本执行以下操作：

捕获启动配置

该脚本必须在 STDOUT 缓冲区中返回设备启动配置。在缓冲区中返回的所有内容都将视为设备启动配置。

捕获运行配置

该脚本必须在 STDOUT 缓冲区中返回设备运行配置。在缓冲区中返回的所有内容都将视为设备运行配置。

上传运行配置

该脚本读取由“绝对文件名”参数标识的文件（有关详细信息，请参阅默认的脚本命令行参数 (p. 53)）。它然后上传文件的内容并将其合并到设备运行配置。

写入启动配置

该脚本可导致设备运行配置写入其启动配置。

重新加载设备

该脚本重新启动设备。

取消重新加载

该脚本取消设备的挂起或排定重新启动。

加载设备固件配置

该脚本将新的固件映像上传到设备，并执行所有必要的操作以使用该固件映像重新加载设备。

可以为这些操作选择配置脚本。

遵循这些步骤:

1. 从“资源管理器”选项卡中选择设备系列。

   信息和配置将显示在“内容”面板的“信息”选项卡中。

2. 展开“设备配置传输设置”子视图。

   将出现脚本操作子视图。

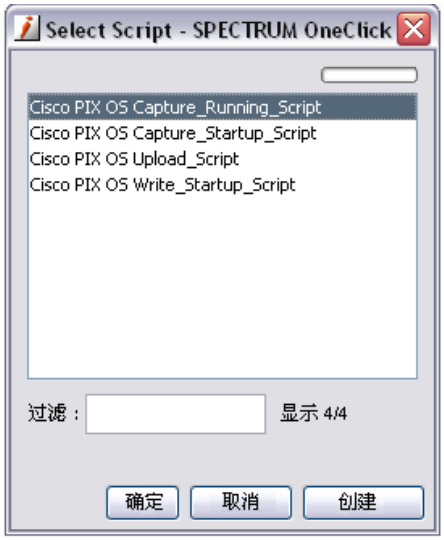
   注意：对于 Cisco IOS 和支持 SSH 的 Cisco IOS 设备系列，“加载设备固件脚本”驻留在“设备固件传输设置”子视图中。

3. 展开相应的脚本操作子视图。

   将显示可用的脚本配置字段。

4. 单击脚本名称旁边的“设置”。

   将打开“选择脚本”对话框，如以下示例所示：

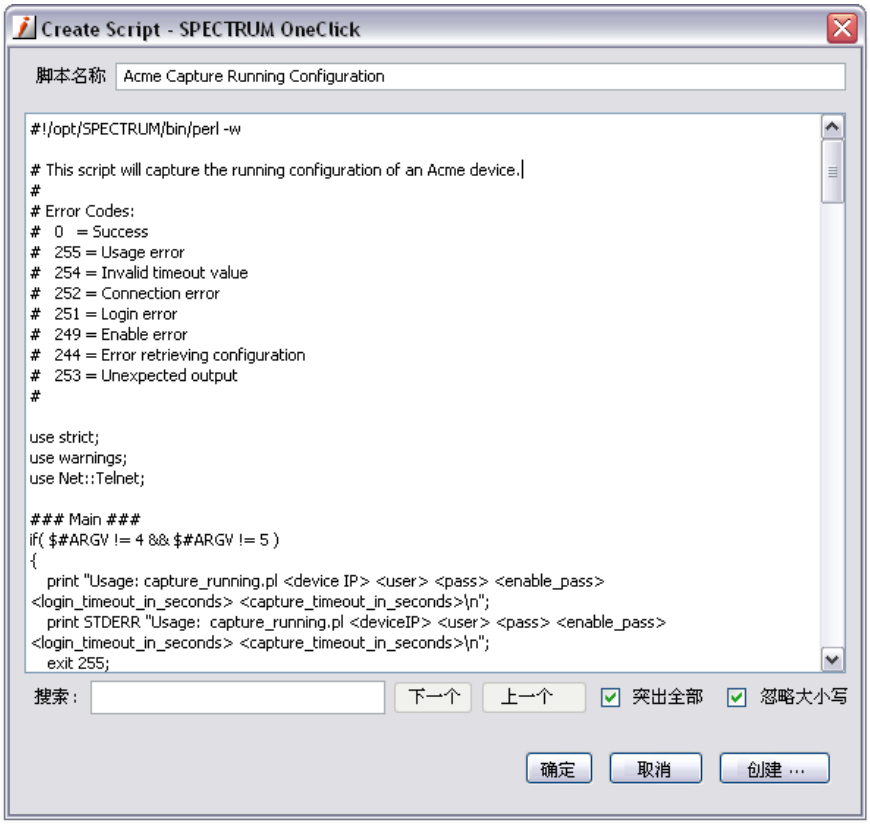


5. 执行下列步骤之一：

   - 如果要使用的脚本可用，请选择该脚本，单击“确定”，然后转到步骤 10。
   - 如果尚未为选定的设备系列创建脚本，请单击“创建”以上传或创建脚本。

6. 在“脚本名称”字段中为脚本提供唯一名称。将脚本粘贴到“脚本名称”下的字段中，或者单击“导入”导入在系统上本地保存的配置文件。

脚本内容将出现在“脚本名称”字段下的字段中，如以下示例所示：



7. （可选）如有必要，请编辑脚本内容。或者，在“搜索”字段中输入标准以在脚本文件中查找特定的行。
8. 完成脚本的导入和配置时，单击“确定”。

   脚本名称将出现在“选择脚本”对话框中。
9. 选择脚本，然后单击“确定”。

   脚本即被加载，且在“脚本内容”字段中是可见的。
10. 添加任何其他脚本参数。

    注意：有关详细信息，请参阅其他的脚本命令行参数 (p. 54)。

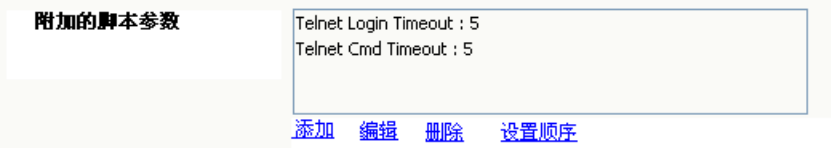
11. 在“其他脚本参数”字段下单击“添加”。

    将打开“添加”对话框。

    a. 输入参数名称和值。如果操作为“上传”，或者任务为“加载固件”，则可以配置参数以提示您在运行时输入值。

    b. 单击“确定”。

    参数将出现在“其他脚本参数”字段中，如以下示例所示：



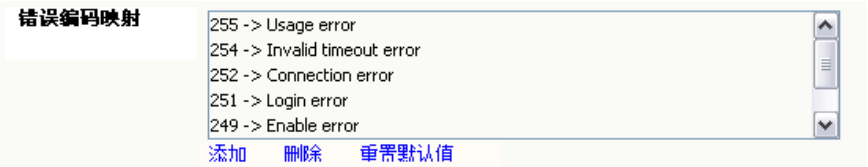
12. 添加任何错误代码映射。有关详细信息，请参阅错误代码映射 (p. 54)。

13. 在“错误代码映射”字段下单击“添加”。

    将打开“添加”对话框。

14. 在“错误代码”字段中输入错误代码，在“错误消息”字段中输入对应的消息，然后单击“确定”。

    错误代码将出现在“错误代码映射”字段中，如以下示例所示：



    可以运行配置脚本了。

Perl 模块

CA Spectrum 附带了运行所提供的即用型 Perl 脚本所需的所有 Perl 模块（用于 Windows/Solaris 平台）。其中包括：

- Net::Telnet

此外，CA Spectrum 还附带了特定的 perl 模块，这些模块在为扩展实用工具开发脚本时可能很有用。这些模块包括：

- Net::SSH
- Net::SSH::Expect
- Expect
- Net::TFTP
- Net::SCP
- Net::FTP

可以在以下位置查看 CA Spectrum 附带的 Perl 模块：

```
/opt/SPECTRUM/lib/perl5
```

重要说明！ 未正确编译和安装的 Perl 模块可能会导致失败或其他预期之外的行为。

将基于 SSH 的 Perl 脚本用于 Network Configuration Manager 操作

CA Spectrum 基于脚本为 Network Configuration Manager 操作提供的即用型支持，是基于 Net::Telnet 模块的。如果要将基于 SSH 的脚本用于 Network Configuration Manager 操作：

- **Windows 和 Solaris** — CA Spectrum 包括完整的 perl 安装和 Net::SSH::Expect 模块。
- **Linux** — 必须将 perl 安装到系统上的单独位置，并将 CA Spectrum 配置为使用该 perl。

CA Spectrum 上的该 Perl 安装和配置必须在 DSS 中基于每个格局完成。必须为已在其上对设备建模以使用基于 SSH 的脚本的每个格局设置 perl。

注意：将 CA Spectrum 配置为使用自定义 Perl 安装后，如果要继续使用 CA Spectrum 的即用型脚本，则自定义 Perl 区域必须已安装 Net::Telnet perl 模块。可以从 www.cpan.org 下载和安装该模块。否则，CA Spectrum 的即用型脚本将失败。

为了设置基于 SSH 的脚本，请按照特定于您平台的说明操作。

在 Windows 上：

1. 安装 Perl。

   CA Spectrum 附带了 Cygwin 的 Perl 完整版本，因此，如果要基于 Net::SSH::Expect 模块使用脚本，则不要求您再进行任何安装。

   如果要基于某个其他模块使用脚本，请根据所用的模块完成以下操作之一：

   - 如果 perl 模块与 Cygwin 以外的 Perl 版本兼容，则我们建议您在 SpectroSERVER 计算机上安装该特定的 Perl，再安装特定的 perl 模块，然后将 CA Spectrum 配置为使用特定的 Perl 安装。（请参阅 将 CA Spectrum 配置为使用自定义 Perl 安装 (p. 61)。）
   - 如果要安装的 perl 模块仅与 Cygwin 的 perl 兼容，且为更改模块（即，它不要求编译 C 库），则可以将它添加到 CA Spectrum Perl 安装。只需将 <模块名称>.pm 文件放置在 $SPECROOT/NT-Tools/SRE/lib/perl5/site_perl/5.8 中即可

- 如果要安装的 perl 模块仅与 Cygwin 的 perl 兼容，还要求编译 C 库，则该模块必须编译且随 CA Spectrum 一起提供。有关该增强请求，请联系 CA Spectrum 支持。

2. 安装基于 SSH 的 perl 模块和 SSH 程序。

   CA Spectrum 附带了 Net::SSH::Expect（及其所需的）模块和 ssh 程序（为 Net::SSH::Expect 所需）。有关如何使用该模块开发脚本的说明，请查看 www.cpan.org 上的 Net::SSH::Expect 文档。

3. 将 CA Spectrum 配置为使用自定义 Perl 安装。

   由于 CA Spectrum 的 perl 是为该目的设置的，因此您无须将 CA Spectrum 配置为使用自定义 perl 安装。

在 Solaris 上

Solaris 上的 CA Spectrum 附带了上面列出的 Perl 模块。要使用 CA Spectrum 附带的模块以外的 perl 模块，必须将 perl 安装到自定义区域。

1. 安装 Perl。

   Perl 在 Solaris 的许多不同版本中可用。可以从 Sun Freeware (www.sunfreeware.com) 下载为您的特定 Solaris 版本编译的 Perl。Perl v5.8.8 已经过测试，它与 Net::SSH::Expect perl 模块兼容。

   注意： SunOS 可能附带了自身的 perl 版本 (v5.005)，但是我们建议不要将该版本用于 Network Configuration Manager 脚本目的，因为可能会遇到通信所需的一些模块的不兼容问题。

2. 安装基于 SSH 的 perl 模块和 SSH 程序。

   如果要使用 Net::SSH::Expect 模块，只需安装 ssh 程序即可。

   Net::SSH::Expect 模块要求安装 ssh 实用工具。如果您的系统尚不包含该实用工具，则可以通过安装 OpenSSH 程序包，从 www.sunfreeware.com 下载并安装它。

   如果要使用其他模块，则可以从 www.cpan.org 下载它们。

   请确保将这些模块安装到上面安装的自定义 Perl 区域。

   通过在安装模块时指定 perl 二进制文件的完整路径，可以完成该操作，例如：

   ```
   <PERL 完整路径>/perl Makefile.pl
   ```

   注意： 一些 Perl 模块依赖于 C/C++ 代码库。为了安装这样的模块，必须安装 gcc 编译器，以便可以链接这些库。这也可以从 www.sunfreeware.com 获取。

3. 将 CA Spectrum 配置为使用自定义 Perl 安装。

请参阅将 CA Spectrum 配置为使用自定义 Perl 安装 (p. 61)，并使 CA Spectrum 指向上面步骤 1 中的 perl 安装区域。

在 Linux 上

1. 安装 Perl。

   操作系统已安装 Perl（检查 /usr/bin/）。该预安装的 Perl 可用于 Network Configuration Manager 脚本。

2. 安装基于 SSH 的 perl 模块和 SSH 程序。

   将需要下载并安装 Net::SSH::Expect 模块、其从属模块和 ssh 实用工具。

   Net::SSH::Expect 的依存关系树类似如下所示：

   Net::SSH::Expect -> Expect -> IO::Pty

   其中“->”表示“需要”关系。

   可以从 www.cpan.org 下载所有这些模块

   请确保将这些模块安装到上面安装的自定义 Perl 区域。

   通过在安装模块时指定 perl 二进制文件的完整路径，可以完成该操作，例如：

   <PERL 完整路径>/perl Makefile.pl

   注意：一些 Perl 模块依赖于 C/C++ 代码库。为了安装这样的模块，必须安装 gcc 编译器，以便可以链接这些库。通过使用 rpm 添加最新的 gcc 程序包，可以安装 gcc 编译器。

3. 将 CA Spectrum 配置为使用自定义 Perl 安装。

   请参阅将 CA Spectrum 配置为使用自定义 Perl 安装 (p. 61)，并使 CA Spectrum 指向上面步骤 1 中的 perl 安装区域。

将 CA Spectrum 配置为使用自定义 Perl 安装

默认情况下，CA Spectrum 配置为使用它附带的 Perl。如果要使用 CA Spectrum 未附带的其他 perl 模块，且已将它们安装到 perl 区域，则可以将 CA Spectrum 配置为使用自定义 perl 安装。要进行该设置，请在 OneClick 的“资源管理器”选项卡中单击“配置管理器”模型。在其“信息”视图中，展开“Perl 配置”子视图。您将发现一个包含每个格局的 Perl 目录配置的表。

请注意，“使用自定义 Perl”选项必须设置为“已启用”，才能指定自定义 perl 目录。否则，将使用 CA Spectrum 附带的默认 Perl。可以将 CA Spectrum 指向您已安装在特定 SpectroSERVER 系统上的自定义 Perl 位置。

遵循这些步骤:

1. 在给定的格局上，将“使用自定义 Perl”设置为“已启用”。
2. 允许使用自定义 Perl 区域后，可以指定“自定义 Perl 目录”。

   注意：“自定义 Perl 目录”必须包含某目录的完整路径名，该目录包含 perl.exe (Windows) 或 perl 程序 (Solaris/Linux)。

例如，如果 perl 程序位于 /usr/local/bin/ 中，则需要将“自定义 Perl 目录”指定为 /usr/local/bin。

注意：一旦将 CA Spectrum 配置为使用自定义 Perl 安装，您可以继续使用 CA Spectrum 默认脚本。但是，您的自定义 Perl 区域必须安装有 Net::Telnet perl 模块。可以从 www.cpan.org 下载和安装该模块。否则，CA Spectrum 默认脚本将失败。

您也可以禁止使用自定义 Perl 区域，而使用默认 CA Spectrum Perl。

将“使用自定义 Perl”设置为“已禁用”（使用 CA Spectrum 默认值）。请注意，禁止使用自定义 Perl 区域时，无法查看或编辑“自定义 Perl 目录”。但是，重新启用“使用自定义 Perl”时，将还原以前指定的自定义 Perl 目录。

使用其他 Perl 模块

如果要基于首选 perl 模块使用脚本，则必须将 perl 模块安装到将使用的区域。

在 Windows 上：

根据要使用的模块，有以下三个选项：

- 如果 perl 模块与 Cygwin 以外的 Perl 版本兼容，则我们建议您在 SpectroSERVER 计算机上安装该特定的 Perl，再安装特定的 perl 模块，然后将 CA Spectrum 配置为使用特定的 Perl 安装。（请参阅将 CA Spectrum 配置为使用自定义 Perl 安装 (p. 61)）。
- 如果要安装的 perl 模块仅与 Cygwin 的 perl 兼容，且为基于文本的模块（即，它不要求编译 C 库），则可以将它添加到 CA Spectrum Perl 安装。只需将 <*模拟名称*>.pm 文件放置在

  $SPECROOT/NT-Tools/SRE/lib/perl5/site_perl/5.8 中即可

- 如果要安装的 perl 模块仅与 Cygwin 的 perl 兼容，还要求编译 C 库，则该模块必须编译且随 CA Spectrum 一起提供。有关该增强请求，请联系 CA Spectrum 支持。

在 Solaris 和 Linux 上

要求将 Perl 安装到 SpectroSERVER 上的单独区域，然后使用该 Perl 安装所需的 perl 模块，并将 CA Spectrum 配置为使用 Perl 安装区域。安装 Perl 后，请参阅要安装的特定 perl 模块的安装说明。然后参阅将 CA Spectrum 配置为使用自定义 Perl 安装 (p. 61)。可以参阅将基于 SSH 的 Perl 脚本用于 Network Configuration Manager 操作 (p. 59)，了解有关如何基于 Net::SSH::Expect 模块使用脚本的详细信息，但可以将该过程用作集成任何 perl 模块的准则。

导入和导出脚本

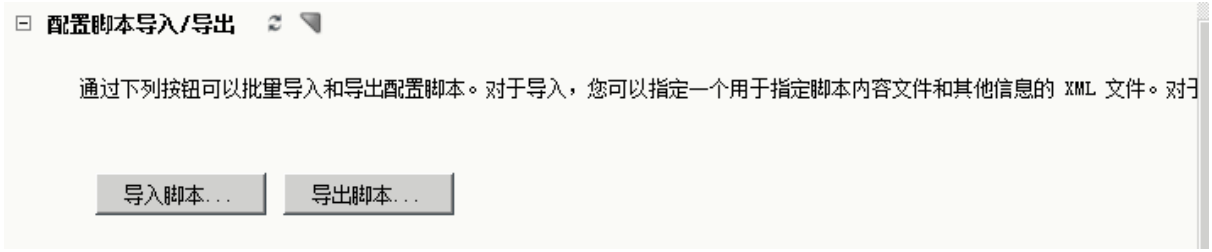
通过 Network Configuration Manager 可以批量导入和导出脚本。脚本将导出到运行 OneClick 客户端的主机服务器的文件系统，或从其导入。

按照以下步骤导出脚本：

1. 在“导航”面板中选择“配置管理器”。
2. 在“内容”面板中选择“信息”选项卡。

   将显示信息和配置。
3. 展开“配置脚本导入/导出”子视图。

   将显示“导入脚本”和“导出脚本”按钮。



4. 单击“导出脚本”。

   将打开“选择要导出的脚本”对话框。
5. 选择要导出的脚本。或者选择多个脚本。

   将打开“另存为”对话框。

6. 选择要保存的位置，并为在导出期间自动生成的 XML 规范文件提供名称。在导出过程中将为每个选定的 Perl 脚本生成文件（使用其指定名称和 .pl 扩展名）。在导出过程中还将生成 XML 规范文件，该文件包含已导出脚本的列表和每个脚本的错误映射信息。然后，XML 规范文件可用于在相同或不同 CA Spectrum 环境中导入脚本。

   选定的 Perl 脚本将导出到您指定的位置。

按照以下步骤导入脚本：

1. 在“导航”面板中选择“配置管理器”。
2. 在“内容”面板中单击“信息”选项卡。

   将显示信息和配置。
3. 展开“配置脚本导入/导出”子视图。

   将显示“导入脚本”和“导出脚本”按钮。
4. 单击“导入脚本”。

   将打开“打开”对话框。
5. 选择描述要导入到 Network Configuration Manager 中的 Perl 脚本的 XML 规范文件。如果要导入以前从 CA Spectrum 导出的脚本，则可以使用在该导出期间生成的 XML 规范文件。

   通过遵循以下示例所示的格式，也可以手动生成 XML 规范文件。

```
<scripts>
  <script>
    <file-name>ABC_Vendor_Capture_Running_Configuration.pl</file-name>
    <display-name>ABC 供应商捕获运行配置</display-name>
    <error-message errorCode="255">用法</error-message>
    <error-message errorCode="99">无效的启用密码</error-message>
    <error-message errorCode="98">意外的响应 Response</error-message>
    <error-message errorCode="97">非法的 Telnet 超时值</error-message>
  </script>
  <script>
    <file-name>XYZ_Vendor_Capture_Running_Configuration.pl</file-name>
    <display-name>XYZ 供应商捕获运行配置</display-name>
    <error-message errorCode="255">用法</error-message>
    <error-message errorCode="99">响应超时</error-message>
    <error-message errorCode="50">连接错误</error-message>
  </script>
  <script>
    <file-name>XYZ_Vendor_Capture_Startup_Configuration.pl</file-name>
    <display-name>XYZ 供应商捕获启动配置</display-name>
  </script>
</scripts>
```

file-name

要导入的 Perl 文件的名称。在导入时，该文件必须与 XML 规范文件存在于同一目录中。

display-name

在 OneClick 中使用的名称，用于标识该脚本。

error-message

（可选）描述由脚本返回的错误代码到出现错误时在 OneClick 中显示的文字错误消息的映射。可以为每个脚本指定多个 error-message 元素。

将导入 Perl 脚本 XML。在设备系列上配置 Network Configuration Manager 操作时，脚本将可用。

注意：导入过程不将脚本与设备系列关联。

维护脚本备份和历史记录

脚本作为模型存储在 CA Spectrum 数据库中，因此 CA Spectrum 每次执行备份时都会得到备份。脚本导出功能提供了一个额外备份以及 Network Configuration Manager 脚本历史记录的跟踪方式，从而在需要时轻松访问并将其重新导入到 CA Spectrum 中。

自定义的陷阱

通过为安装配置自定义的陷阱设置，可以扩展 Network Configuration Manager 的功能。这些设置用于关联配置更改事件信息，以便为特定的设备组合事件。这些设置是在设备系列级别配置的。有关详细信息，请参阅配置通知陷阱设置 (p. 42)。

第 3 章： 全局同步任务

本章介绍如何使用 Network Configuration Manager 在网络上设置全局同步任务。运行全局同步任务时，Network Configuration Manager 将捕获并保存所有的设备配置。

注意：我们建议您在配置 Network Configuration Manager 策略之前捕获设备配置。

此部分包含以下主题：

关于全局同步 (p. 67)
配置全局同步 (p. 68)
排定全局同步 (p. 69)
运行按需全局同步任务 (p. 70)
查看单个设备的配置历史记录 (p. 70)
比较任何两个配置 (p. 72)
指定参考配置 (p. 73)
配置警报 (p. 74)
查看全局同步任务结果 (p. 75)
来自 Report Manager 的 Network Configuration Manager 报告 (p. 76)

关于全局同步

全局同步任务为网络上已启用 Network Configuration Manager 的设备收集运行配置。可以将该任务排定为定期运行。选择一个时间段和重复频率，以从网络范围的所有受支持设备捕获配置。例如，在每天下午 9 点后且上午 5 点前捕获设备配置。通过捕获网络上所有设备的配置，维护运行配置历史记录。

可以设置全局同步，以验证启动配置是否与运行配置相同。如果它们不同，则可以将 Network Configuration Manager 配置为生成警报。全局同步捕获启动配置，并将它与运行配置进行比较以检测更改。有关启动配置和运行配置的说明，请参阅配置类型 (p. 14)。

注意：也可以为网络上的选定设备收集运行配置，并通过创建自动同步任务来实时查看结果。有关详细信息，请参阅创建同步任务 (p. 88)。

关于 Enterasys/Riverstone SSR 设备

在 Enterasys/Riverstone SSR 设备上执行的配置捕获将提供启动配置，而不是运行配置。因此，Network Configuration Manager 维护的设备配置历史记录是 SSR 设备上启动配置的历史记录。有关 SSR 设备如何处理 Network Configuration Manager 配置上传的详细信息，请参阅确定 Enterasys/Riverstone SSR 设备如何响应上传任务 (p. 87)。

配置全局同步

配置全局同步的设置，例如排定。全局同步由全局同步任务（出现在“资源管理器”选项卡中的“任务”下）执行。

遵循这些步骤:

1. 在“资源管理器”选项卡中选择“配置管理器”。

   信息和配置将显示在“内容”面板的“信息”选项卡中。

2. 展开“全局同步”子视图。

   将出现“全局同步”选项。

3. 根据需要修改以下选项：

   全局同步计划

   为全局同步任务指定计划。单击“排定”按钮以访问“选择排定”对话框，可以从该对话框选择默认排定或创建自定义排定。在排定全局同步 (p. 69)中提供了有关排定全局同步任务的详细信息。

   同步任务未在分配时间内完成时断言任务警报

   如果您希望全局同步任务未正确完成时通过警报进行通知，请指定次要、主要或关键警报。如果您管理许多设备，且定期运行排定的全局同步任务，则在排定期间结束时，同步任务将停止，因为捕获配置会占用慢速链路上的带宽。

   包含禁用了 NCM 的设备和设备系列

   指定是否要将已禁用 Network Configuration Manager 的设备包含在“失败设备列表”中。

   默认值：是

验证启动配置是否与运行配置相同

如果要将启动配置与网络中设备的当前运行配置进行比较，请启用该选项。

启动配置不同时断言设备警报

如果要为启动配置与运行配置不同的设备生成警报，请指定次要、主要或关键警报。

排定全局同步

可以将全局同步排定为收集网络上所有设备的运行配置。设备按随机顺序进行处理。

如果排定的全局同步未在分配的时间内完成，则下次执行首先随机处理上次执行中未处理的设备。然后按随机顺序处理所有的剩余设备。

重要说明！ 如果 CA Spectrum 格局存在于多个时区中，则不要排定“一次性”全局同步。执行此类型的任务可导致全局同步仅在最早的时区中运行。

遵循这些步骤:

1. 在“资源管理器”中，选择“任务”文件夹中的“全局同步任务”。
2. 在“内容”面板中选择“列表”选项卡。
3. 单击工具栏中的“排定”按钮。

   将打开“选择排定”对话框。
4. 执行下列步骤之一：
   - 选择默认排定，然后单击“确定”。
   - 创建自定义排定。单击“创建”，指定排定选项，然后单击“确定”。

     自定义排定将添加到可用排定的列表。选择新排定，然后单击“确定”。

   全局同步任务现已排定。排定出现在“列表”表的“排定”列中，且排定图标出现在“任务”文件夹中任务的旁边。

运行按需全局同步任务

运行全局同步任务可收集网络上所有设备的运行配置。设备按随机顺序进行处理。

遵循这些步骤:

1. 在“资源管理器”中，选择“任务”文件夹中的“全局同步任务”。
2. 在“内容”面板中选择“列表”选项卡。
3. 单击“启动选定的任务”图标。

   “同步任务结果”对话框将显示已处理设备的列表和全局同步的结果。

查看单个设备的配置历史记录

可以在 OneClick 中查看单个设备的配置历史记录。有关将配置上传到网络设备的详细信息，请参阅将配置手动上传到单个设备 (p. 81)。

遵循这些步骤:

1. 在“资源管理器”选项卡中选择设备。
2. 验证在“内容”面板中选中了“列表”选项卡，并在“组件详细信息”面板中选择“主机配置”选项卡。

   以下详细信息将出现在“主机配置”表中：

   捕获时间

   列出在设备上首次捕获该行中配置的时间 (M-DD-YYY HH:MM:SS)。

   捕获者

   标识配置了任务的 CA Spectrum OneClick 用户。

   行更改

   列出与设备上的以前配置比较时发生了更改的相关行数。相关更改包括已添加的行、已删除的行和已更改的行。不相关更改是与比较掩码匹配的任何行。比较掩码在设备系列的“掩码配置”设置中进行管理。有关详细信息，请参阅配置设备系列掩码 (p. 40)。

   行更改总计

   列出与设备上的以前配置比较时更改的总行数（相关和不相关）。如果检测到任何更改，则显示更改超链接。

是参考

表示该设备的参考配置。

运行对应于启动

显示启动和运行配置文件中的配置差异（如果适用）。如果存在差异，则显示“查看差异”超链接。

上次验证时间

列出 Network Configuration Manager 上次验证配置是否仍存在于设备上的时间 (M-DD-YYY HH:MM:SS)。

上次验证的用户

标识已访问设备的最后一个用户。

NCM 模式

标识通过 Network Configuration Manager 启动更改时将新配置内容传输到设备所用的方法。

NCM 用户

标识使用 Network Configuration Manager 在设备上启动了配置更改的 CA Spectrum 用户。

设备用户

标识访问了设备并进行了配置更改的用户。

源

标识配置更改的源。

位置

标识配置更改的位置。

违反的策略

标识进行该配置更改后所违反的策略。

遵从策略

指示进行该配置更改后所遵从的策略。

Network Configuration Manager 检测到一个或多个更改时，将创建一个新行。

3. 在“主机配置”表中选择一行。

已捕获主机配置的内容将出现在表下面的框中。

4. （可选）单击“主机配置”表的“行更改”列中的更改超链接（如果适用），以在选定设备的配置中查看已添加的、已删除的、已更改的和不相关的行。

   将打开“配置差异”对话框。突出显示的文本使用以下颜色来指示状态：

   - **绿色**—这些行已添加。
   - **红色**—这些行已删除。
   - **蓝色**—这些行已更改。
   - **灰色**—这些行是不相关的。不相关更改是与比较掩码匹配的行。

   注意：单击“下一步”或“上一步”可在文件的差异之间导航。

5. （可选）单击“主机配置”表的“运行对应于启动”列中的“查看差异”超链接（如果适用），以查看已添加的、已删除的、已更改的和不相关的行。

   “运行对应于启动”对话框显示已捕获设备的运行和启动配置文件之间的差异。启动配置出现在右列中。突出显示的文本使用上一步中列出的颜色来指示状态。

比较任何两个配置

可以比较任何两个主机配置，即使它们属于不同的设备。

遵循这些步骤:

1. 在“资源管理器”选项卡中选择设备。
2. 验证在“内容”面板中选中了“列表”选项卡，并在“组件详细信息”面板中选择“主机配置”选项卡。
3. 右键单击“主机配置”表中要比较的配置，然后选择“开始比较”。
4. 选择要包括在比较中的第二个配置。选择同一设备的配置，或者在“资源管理器”选项卡中选择不同的设备。验证其配置信息显示在“主机配置”表中。

5. 右键单击“主机配置”表中要包括在比较中的第二个配置，然后选择“与 *<name_of_first_configuration>* 进行比较”。

   将打开“配置差异”对话框。突出显示的文本使用以下颜色来指示状态：

   - **绿色**—这些行已添加。
   - **红色**—这些行已删除。
   - **蓝色**—这些行已更改。
   - **灰色**—这些行是不相关的。不相关更改是与比较掩码匹配的行。

   注意：单击“下一步”或“上一步”可在文件的差异之间导航。

指定参考配置

可以为具有关联警报的设备指定参考配置。只要 Network Configuration Manager 确定当前配置与参考配置有很大不同时，就可以在设备上生成警报。

注意：有关警报设置的详细信息，请参阅配置配置更改报警 (p. 27)。

遵循这些步骤:

1. 在“资源管理器”选项卡中，选择设备或设备系列。

   验证在“内容”面板中选中了“列表”选项卡。

2. 在“列表”选项卡中选择要将其最新配置设置为参考的一个或多个设备。

3. 右键单击选定内容，然后选择“设置 NCM 参考配置”。

   此时将打开确认对话框。

4. 选择“是”。

   最新的配置将设置为每个选定设备的参考。“主机配置”表中的“是参考”字段显示选中标记和设置参考的用户。

也可以手动指定参考配置。

遵循这些步骤:

1. 在“资源管理器”选项卡中选择设备。

   验证在“内容”面板中选中了“列表”选项卡，并在“组件详细信息”面板中选择“主机配置”选项卡。

2. 右键单击要用作参考的配置，然后选择“设置参考”。

   该配置将指定为该设备的参考配置。选中标记和设置参考的用户将出现在“主机配置”表的“是参考”字段中。

设置参考配置后，可以更改或删除所指定的参考配置。只能将一个配置设置为设备的参考配置。已设置一个配置时，如果在其他配置上使用“设置参考”或“设置 NCM 参考配置”选项，则将自动清除原始配置，新配置将成为指定的参考配置。要清除参考配置，请对“主机配置”表中的配置使用右键单击菜单中的“取消设置参考”命令。

配置警报

可以指定发生特定配置更改时要触发的警报。本节介绍如何查看触发了警报的配置之间的差异。

有关确定何时触发配置更改警报的详细信息，请参阅配置配置更改报警 (p. 27)和在单个设备上指定配置更改报警设置 (p. 45)。

查看参考配置和运行配置之间的差异

在“警报详细信息”选项卡中，可以查看和比较单个设备的参考配置和当前运行配置之间的差异。

遵循这些步骤:

1. 从“资源管理器”选项卡中选择设备、设备系列或全局集合。
2. 在“内容”面板中选择“警报”选项卡。

   将显示选定项的警报。
3. 选择在“警报标题”列中显示“参考配置和当前运行配置不同”的警报。
4. 在“组件详细信息”面板中选择“警报详细信息”选项卡。

   将显示警报详细信息。
5. 单击“查看差异”超链接。

   “配置差异”屏幕将显示已捕获设备的参考和当前运行文件之间的差异。参考配置出现在右列中。

查看启动配置和运行配置

在“警报详细信息”选项卡中，可以查看和比较单个设备的启动配置和运行配置。

遵循这些步骤:

1. 从“资源管理器”选项卡中选择设备、设备系列或全局集合。
2. 在“内容”面板中选择“警报”选项卡。

   将显示设备、设备系列或全局集合的警报。
3. 选择在“警报标题”列中显示“启动和运行配置不同”的警报。
4. 在“组件详细信息”面板中选择“警报详细信息”选项卡。

   将显示警报详细信息。
5. 单击“查看差异”超链接。

   “运行对应于启动”屏幕显示已捕获设备的运行和启动配置文件之间的差异。

   启动配置出现在左列中。

查看全局同步任务结果

可以查看其全局同步失败和成功的设备的列表。

注意：可以控制是否要将已禁用 Network Configuration Manager 的设备包含在“失败设备列表”中。有关详细信息，请参阅配置全局同步 (p. 68)。

遵循这些步骤:

1. 展开配置管理器，然后在“资源管理器”选项卡中选择“任务”。
2. 选择“全局同步任务”。

   信息和结果将出现在“内容”面板的“信息”选项卡中。
3. 在“筛选”字段中输入名称、类型、条件或设备系列以筛选结果列表。

来自 Report Manager 的 Network Configuration Manager 报告

在 CA Spectrum Report Manager 中的网络配置管理报告包下，包括了 Network Configuration Manager 报告选项。Report Manager 提供了大量的报告内容、格式和报告组织选项。因此，可以为组织中对设备配置更改感兴趣的不同受众生成具有相应类型和信息范围的报告。

Report Manager 选项

Report Manager 为您提供了多个选项，用于生成和管理 Network Configuration Manager 报告：

- 按需生成报告，以查看最新的测试结果。
- 排定一次性或定期的测试报告生成。
- 指定希望 Report Manager 保留已排定测试报告的时间长度或者要保留的报告数。
- 为已排定的测试报告指定电子邮件收件人。
- 为其他 Report Manager 用户排定测试报告。
- 以 PDF、文本和电子表格格式发布报告。

注意：有关 Report Manager 功能的详细信息，请参阅*《Report Manager 用户指南》*。

提供了以下报告：

配置更改: 全部

显示具有配置更改的所有设备的更改摘要。每行表示要与描述其配置更改的数据关联的设备。

配置更改: 组

显示给定全局集合中设备的更改摘要。每行表示要与描述其配置更改的汇总统计关联的设备。

配置更改: 单个设备

显示给定设备上配置更改的列表。每行显示更改时间、谁进行了更改以及更改了多少行。此外，每行都包含指向 Java 小程序的 Web 链接，Java 小程序可显示当前配置和以前配置之间的差异。

详细的配置事件日志: 全部

显示 CA Spectrum 内具有 Network Configuration Manager 活动的所有设备和模型的事件的发生时间反序列表。列表中的每个条目都包括 IP 地址（如果适用）、事件文本、事件代码和事件创建人。

详细的配置事件日志: 组

显示指定全局集合中具有 Network Configuration Manager 活动的所有设备和模型的事件的发生时间反序列表。列表中的每个条目都包括 IP 地址（如果适用）、事件文本、事件代码和事件创建人。

详细的配置事件日志: 选定的设备或模型

显示具有 Network Configuration Manager 活动的指定设备或模型的事件的发生时间反序列表。列表中的每个条目都包括 IP 地址（如果适用）、事件文本、事件代码和事件创建人。

前 N 个配置更改: 全部

显示具有配置更改的“前 N 个”设备的更改摘要，其中“前 N 个”定义为基于当前排序标准的最大记录数。每条记录都表示要与描述其配置更改的汇总统计关联的设备。

前 N 个配置更改: 组

显示全局集合中具有配置更改的“前 N 个”设备的更改摘要。“前 N 个”定义为基于当前排序标准的最大记录数。每条记录都表示要与描述其配置更改的汇总统计关联的设备。

使用 Report Manager 生成网络配置管理报告

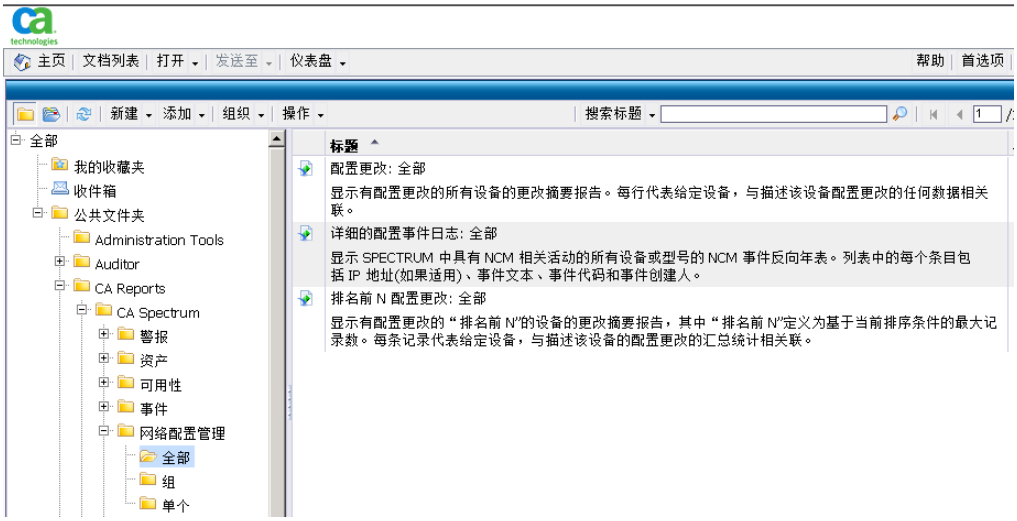
可以使用 CA Spectrum Report Manager 生成网络配置管理报告。

注意：以下示例仅提供 Report Manager 中可用的网络配置管理报告和功能的概述。有关详细信息，请参阅 *《Report Manager 用户指南》*。

遵循这些步骤:

1. 选择要生成的测试类型。

   下图显示了网络配置管理报告选项：



2. 对报告进行配置。选择日期和时间范围的选项，提供报告标题和副标题，然后选择格局。

3. 单击“查看报告”以生成报告。

   将显示报告。下图显示了报告结果的示例：

4. 单击“设备名称”超链接以在设备级别上检查结果。

   下图显示了一个示例。在该视图中，可以单击“查看更改”超链接，在选定设备的配置中查看已添加的、已删除的、已更改的和不相关的行。

第 4 章： Network Configuration Manager 设备级任务

本章介绍如何使用 Network Configuration Manager 手动捕获、导出和上传网络中设备的配置。

此部分包含以下主题：

手动捕获配置 (p. 81)
将配置手动上传到单个设备 (p. 81)

手动捕获配置

在发生任何更改后，Network Configuration Manager 会立即尝试捕获设备配置。未经请求的配置更改通知可以是从发生更改的设备发送的陷阱或 MIB 对象。接收到未经请求的通知时，SpectroSERVER 将执行捕获，并将配置保存在数据库中以提供已更新的配置数据。也可以在 OneClick 中手动捕获设备配置。

遵循这些步骤:

1. 在“资源管理器”选项卡中选择单个设备。

   该设备将出现在“内容”面板的“列表”选项卡中。

2. 在“组件详细信息”面板中，选择“主机配置”选项卡。

   将显示任何先前捕获的结果。

3. 单击“捕获配置”图标。

   将出现捕获的结果。新配置将出现在列表中，或者对当前配置更新上次验证时间。

将配置手动上传到单个设备

可以将配置文件手动上传到网络上的单个设备。上传配置文件时，会将它合并到现有的配置文件中。可以使用该功能使新安装的设备或更换/待机远程设备快速联机。

上传到 Juniper JUNOS 设备系列中的设备时，请使用 JUNOScript API 格式。有关详细信息，请参阅 Juniper JUNOS 设备 (p. 19)。

注意：通过创建批量上传任务，可以上传配置和实时查看结果。有关详细信息，请参阅创建上传任务 (p. 85)。

不需要批准

根据是否启用了批准工作流，将设备配置上传到单个设备的过程有所不同。以下步骤介绍了不需要批准时的过程。

注意：有关工作流批准选项的信息，请参阅配置工作流 (p. 28)。

遵循这些步骤:

1. 在“资源管理器”选项卡中，选择单个设备或设备系列。

   与选定设备系列关联的一个或多个设备将出现在“内容”面板的“列表”选项卡中。

2. 在“组件详细信息”面板中，选择“主机配置”选项卡。

   将显示任何先前捕获的结果。

3. 单击“上传”图标。

   注意：如果需要批准，则出现“需要批准”对话框。转到需要批准 (p. 83)以创建批准请求。

   将出现“上传配置”屏幕，其中包含选定设备的最后已知配置信息，如以下示例所示：

4. 执行以下任一可选步骤：
   - 根据需要编辑配置内容。
   - 在“搜索”字段中输入标准，以查找配置文件中要更改内容的特定行，或者在上传之前验证内容。
   - 选择“还保存到启动”以将该配置写入启动配置。这将导致在重新启动时将配置文件加载到设备中。

     注意：该功能仅受 Cisco、Foundry 和 Nortel Passport L3 设备支持。
   - 单击“打开”导入一个以前导出的、在系统上本地保存的配置文件。
   - 如果要以 txt 或 html 格式保存并导出该配置文件，请单击“另存为”。
5. 单击“上传”将配置文件上传到选定的设备。

   该过程完成后，将出现消息“配置上传已成功”。

   注意：排定任务是批量任务的可用功能。如果要排定上传任务，请参阅 Network Configuration Manager 批量任务 (p. 85)。

将配置上传到单个设备（需要批准）

如果启用了批准工作流，则必须先批准配置更改，才能处理它们。通过为上传请求创建任务，然后在批准之后运行它，可以完成该操作。

注意：有关批准工作流选项的信息，请参阅配置工作流 (p. 28)。

遵循这些步骤:

1. 在“资源管理器”选项卡中，选择单个设备或设备系列。

   与选定设备系列关联的一个或多个设备将出现在“内容”面板的“列表”选项卡中。
2. 在“组件详细信息”面板中，选择“主机配置”选项卡。

   将显示任何先前捕获的结果。
3. 单击“上传”图标。

   将出现“需要批准”对话框。
4. 选择“是”继续操作。

   将出现“创建 NCM 任务”。

5. 创建任务，如下所示：

   a. 在“名称”字段中输入唯一名称。

      注意： Network Configuration Manager 提供了默认名称 (<*任务类型*>.YY-MM-DD_HH:MM.<*用户名*>)。例如，Upload.2006-10-17_15:48:04.Administrator。

   b. 在“说明”字段中输入任务的说明。

   c. 如果希望任务在它运行之后可用，请选择“可重用任务”。

   d. 单击“编辑”以在“上传内容”框中指定用于上传并合并到设备配置中的内容。也可以单击“打开”从文本文件导入内容。进行更改后，可以单击“另存为”以 txt 或 html 格式保存并导出该配置文件。

   e. （可选）在“搜索”字段中输入标准以在配置文件中查找特定的行。

   f. 选择“提交到启动”（如果适用），以在合并新内容后将整个运行配置复制到启动配置。

   g. 选择“失败时发出设备警报”以在任务失败的每个设备上生成警报。

   h. 单击“请求批准”。

   将出现“需要批准”对话框。

6. 选择用户并输入任务批准者的电子邮件地址，输入任务说明（可选），然后单击“确定”以生成请求。

   将出现确认对话框，指示请求创建已成功。将向任务批准者发送一封电子邮件，且生成的任务将出现在“资源管理器”选项卡的“任务”文件夹中。

   注意： 有关电子邮件配置的信息，请参阅*《管理员指南》*。

7. 如启动任务 (p. 106)中所述，检查批准状态并运行任务。

第 5 章： Network Configuration Manager 批量任务

本章介绍如何使用 Network Configuration Manager 创建按需批量上传任务、同步任务和保存到启动任务。这些任务通过捕获和上传主机配置与设备进行交互。可以创建任务以在单个设备上或一系列设备上随时运行。如果要将相同的配置（差异较小，如 IP 地址）迁出到网络上的多个设备，则这些按需任务很有用。

可以将任务定义为可重用。可重用任务在执行后会一直存在，并且可重新运行。如果任务不是可重用的，则运行它之后，将它发送到“Lost and Found”视图，并在 24 小时内清除。

此部分包含以下主题：

创建上传任务 (p. 85)
创建同步任务 (p. 88)
创建保存到启动任务 (p. 89)

创建上传任务

创建自动上传任务可执行批量配置上传。批量上传任务将新内容合并到一个或多个选定设备的运行配置中。设备按随机顺序进行处理。

重要说明！ 如果要上传到 Enterasys/Riverstone SSR 设备，请在继续执行该任务之前参阅确定 Enterasys/Riverstone SSR 设备如何响应上传任务 (p. 87)。如果要上传到 Juniper JUNOS 设备系列中的设备，则必须使用 JUNOScript API 格式；有关详细信息，请参阅 Juniper JUNOS 设备 (p. 19)。

遵循这些步骤:

1. 在“资源管理器”选项卡中，选择单个设备、设备系列、全局集合、搜索结果条目或容器（如 Universe）。
2. 单击“列表”选项卡，然后为上传任务选择设备。
3. 从工具栏上的“创建 NCM 任务”图标选择“上传任务”。

   将打开“上传任务”对话框。

   注意：如果选定的设备未出现在“允许”选项卡中，请单击“禁止”以显示从 Network Configuration Manager 任务中禁用的设备或者缺少必要权限的设备。

4. 单击“继续”。

   将出现“创建任务”对话框。

5. 输入任务信息，如下所示：

   a. （可选）在“名称”字段中输入唯一名称。

      注意： Network Configuration Manager 提供了默认名称 (<*任务类型*>.YY-MM-DD_HH:MM.<*用户名*>)。例如，Upload.2006-10-17_15:48:04.Administrator。

   b. （可选）在“说明”字段中输入任务的说明。

   c. 选择“可重用任务”以使任务变为可重用。

   d. 单击“编辑”以在“上传内容”框中指定用于上传并合并到设备配置中的内容。也可以单击“打开”从文本文件导入内容。进行更改后，可以单击“另存为”以 txt 或 html 格式保存并导出该配置文件。

   e. 在“搜索”字段中输入标准以在配置文件中查找特定的行。

   f. 选择“提交到启动”（如果适用），以在合并新内容后将整个运行配置复制到启动配置。

   g. 选择“失败时发出设备警报”以在任务失败的每个设备上生成警报。

6. 如果需要批准（如“请求批准”按钮所示），请执行以下步骤：

   a. 单击“请求批准”。

      将出现“需要批准”对话框。

   b. 选择用户并输入任务批准者的电子邮件地址，输入任务说明（可选），然后单击“确定”以生成请求。

      将出现一个确认对话框，指示请求已成功创建。将向任务批准者发送一封电子邮件，且生成的任务将出现在“资源管理器”选项卡的“任务”文件夹中。

      注意： 有关电子邮件配置的信息，请参阅*《管理员指南》*。

   c. 如启动任务 (p. 106)中所述，检查批准状态并运行任务。

   注意： 有关批准工作流选项的信息，请参阅配置工作流 (p. 28)。

7. 如果不需要批准（如“保存”按钮所示）：

   a. 单击“保存”。

      将出现“任务已保存”对话框。

b. 执行下列步骤之一：

- 单击“上传”将任务上传到选定的设备。

  将出现“上传任务结果”对话框，且生成的任务将出现在“资源管理器”选项卡的“任务”文件夹中。有关结果对话框的详细信息，请参阅实时查看任务结果 (p. 108)。

- 单击“排定”以排定任务在将来执行。在排定任务 (p. 104)中对排定进行了介绍。

  任务将被保存，并按照其排定运行。

- 单击“关闭”保存任务；它可供稍后运行。通过在“配置管理器”下“资源管理器”选项卡的“任务”中选择任务，可以编辑和运行该任务。

确定 Enterasys/Riverstone SSR 设备如何响应上传任务

Enterasys/Riverstone SSR 设备对配置上传的响应不一致。其中一些设备将运行配置和启动配置都替换为上传的内容。而其他设备则将上传的内容合并到运行配置和启动配置中。在 Enterasys/Riverstone SSR 设备上执行的配置捕获将提供启动配置，而不是运行配置。因此，我们建议测试运行 Enterasys 固件的设备，以验证运行配置和启动配置。

遵循这些步骤:

1. 从“资源管理器”选项卡的搜索结果或容器（如 Universe）中选择单个 SSR 设备。
2. 在“内容”面板中单击“列表”选项卡。
3. 在“组件详细信息”面板中单击“主机配置”选项卡。

   将显示以前捕获的配置。
4. 选择“捕获配置”图标以捕获选定设备的当前配置。
5. 选择“上传”图标。

   将出现“上传配置”屏幕。当前启动配置的内容将显示在底部窗格中。
6. 在“上传配置”屏幕中编辑现有的配置。例如，删除位置行值（或删除行）：

   `system set location “value”`
7. 重新选择“上传”图标，以上传已修改的设备配置。重新选择“捕获配置”图标，以从设备捕获新的配置。

   如果在新捕获的配置中不存在该位置，则表示设备正将运行配置和启动配置都替换为上传的内容（而不是进行合并）。

创建同步任务

创建自动同步任务，可捕获和验证网络上选定设备的策略遵从设备配置，以及实时查看结果。同步任务捕获设备配置时，它将对照与设备有关的所有策略以及（如果指定）设备启动配置来检查配置。设备按随机顺序进行处理。

有关 Network Configuration Manager 策略的详细信息，请参阅 Network Configuration Manager 策略 (p. 111)。

有关以后台模式运行全局同步任务的详细信息，请参阅关于全局同步 (p. 67)。

遵循这些步骤:

1. 在“资源管理器”选项卡中，选择单个设备、设备系列、全局集合、搜索结果条目或容器（如 Universe）。
2. 在“内容”面板中单击“列表”选项卡，然后选择要包括在同步任务中的设备。
3. 从工具栏上的“创建 NCM 任务”图标单击“同步任务”。

   将打开“为同步任务选择设备”对话框。

   注意：如果选定的设备未出现在“允许”选项卡中，请单击“禁止”以显示从 Network Configuration Manager 任务中禁用的设备或者没有必要权限的设备。
4. 输入任务信息，如下所示：
   a. 在“名称”字段中输入唯一名称。

      注意： Network Configuration Manager 提供了默认名称 (<*任务类型*>.YY-MM-DD_HH:MM.<*用户名*>)。例如，Sync.2010-09-09_15:48:04.Administrator。
   b. 在“说明”字段中输入任务的说明。
   c. 选择“启动配置不同时向设备发出警报”和相应的重要级别，以在捕获的配置与其启动配置不同的每个设备上生成警报。
   d. 单击“编辑排定”以排定任务在将来执行。在排定任务 (p. 104)中对排定进行了介绍。
   e. 选择“可重用任务”以使任务变为可重用。
5. 执行下列步骤之一：
   - 单击“保存”保存任务；它可供稍后运行。通过在“配置管理器”下“资源管理器”选项卡的“任务”中选择任务，可以运行该任务。

- 单击“立即运行同步任务”。

  将打开“同步任务结果”对话框，且生成的任务将出现在“资源管理器”选项卡的“任务”文件夹中。有关详细信息，请参阅实时查看任务结果 (p. 108)。

创建保存到启动任务

创建自动的保存到启动任务，可将当前运行配置写入一个或多个选定设备的启动配置。设备在 NVRAM（稳定随机存取内存）中保存其配置。

设备按随机顺序进行处理。

遵循这些步骤:

1. 在“资源管理器”选项卡中，选择单个设备、设备系列、全局集合、搜索结果条目或容器（如 Universe）。
2. 单击“内容”面板中的“列表”选项卡，然后选择要上传的设备。
3. 从工具栏上的“创建 NCM 任务”图标单击“保存到启动任务”。

   将打开“保存到启动任务”对话框。

   注意：如果选定的设备未出现在“允许”选项卡中，请单击“禁止”以显示从 Network Configuration Manager 任务中禁用的设备或者缺少必要权限的设备。
4. 输入任务信息，如下所示：
   a. （可选）在“名称”字段中输入唯一名称。

      注意： Network Configuration Manager 提供了默认名称 (<任务类型>.YY-MM-DD_HH:MM.<用户名>)。例如，WriteStartup.2006-10-17_15:48:04.Administrator。
   b. （可选）在“说明”字段中输入任务的说明。
   c. 选择“可重用任务”以使任务变为可重用。
5. 如果需要批准（如“请求批准”按钮所示），请执行以下步骤：
   a. 单击“请求批准”。

      将出现“需要批准”对话框。

b. 选择用户并输入任务批准者的电子邮件地址，输入任务说明（可选），然后单击“确定”以生成请求。

将出现一个确认对话框，指示请求已成功创建。将向任务批准者发送一封电子邮件，且生成的任务将出现在“资源管理器”选项卡的“任务”文件夹中。

注意：有关电子邮件配置的信息，请参阅*《管理员指南》*。

c. 如启动任务 (p. 106)中所述，检查批准状态并运行任务。

注意：有关批准工作流选项的信息，请参阅配置工作流 (p. 28)。

6. 如果不需要批准，请执行以下任一步骤：

- 单击“排定”以排定任务在将来执行。在排定任务 (p. 104)中对排定进行了介绍。
- 单击“保存”。

  将保存任务以供将来执行。
- 单击“立即运行保存到启动任务”。

  将打开“保存到启动任务结果”对话框，且生成的任务将出现在“资源管理器”选项卡的“任务”文件夹中。有关详细信息，请参阅实时查看任务结果 (p. 108)。

注意：任务设备上的任何“启动和运行配置不同”警报均由该任务自动清除。有关详细信息，请参阅查看启动和运行配置差异 (p. 75)。

第 6 章： 固件上传

本节介绍如何为 Cisco IOS 和支持 SSH 的 Cisco IOS 设备上传固件。通过以下两种方法之一可以完成固件的上传：

- 使用加载固件任务
- 使用扩展实用工具脚本

重要说明！上传固件是高级用户功能，需要专家级知识。错误地修改设备固件可能会使设备处于无效状态。

此部分包含以下主题：

关于固件上传 (p. 91)
权限 (p. 92)
配置设备固件传输设置 (p. 92)
显示 Cisco 闪存分区信息 (p. 93)
创建加载固件任务 (p. 94)
创建重新加载任务 (p. 97)
创建取消重新加载任务 (p. 98)
加载设备固件脚本 (p. 99)

关于固件上传

之所以支持固件上传，是因为如果存在脚本，那么它将使用该脚本。如果脚本不存在，且设备支持 CISCO-FLASH-MIB，则将使用 MIB。

固件上传必须按特定顺序成功完成某些任务，传输才能成功。本节介绍这些任务以及固件上传过程。

注意：这些任务由加载固件任务（在创建加载固件任务 (p. 94)中介绍）或自定义脚本处理。

这些任务如下：

1. **将固件映像从服务器上传到设备。**必须指示设备，将固件映像从已知的服务器（映像服务器）加载到指定的闪存或文件系统名称。完成该上传可能需要数分钟到数小时，具体取决于映像文件的大小和网络带宽。

2. **将启动命令配置上传到设备。**该过程的发生分为三个步骤：
   a. 捕获配置。必须捕获配置，以便可以将新命令插入到当前配置中。
   b. 上传更改。
   c. 写入 NVRAM。必须将修改后的配置写入启动，以便设备在启动时重新加载指定的映像。
3. **运行重新加载脚本。**重新加载命令将直接写入启用模式，它不是配置的一部分。

在每个阶段，系统将适当地使用默认协议或覆盖脚本。

重要说明！如果在其中任何步骤中出现错误，则不存在回滚。设备保持上次的成功状态。

权限

如这些节所述上传固件时，可能需要以下 Network Configuration Manager 权限：

- 加载设备固件
- 重新加载设备
- 排定重新加载

有关详细信息，请参阅 Network Configuration Manager 权限 (p. 213)。

配置设备固件传输设置

本节介绍如何配置用于将固件映像传输到设备的协议和服务器设置。这些设置在设备系列级别上进行且驻留于“设备固件传输设置”子视图（仅对 Cisco IOS 和支持 SSH 的 Cisco IOS 设备系列可用）。这些设备系列中的设备支持 CISCO-FLASH-MIB。

注意：仅 Cisco IOS 和支持 SSH 的 Cisco IOS 设备系列为固件上传提供了即用型支持。对于所有其他设备，可以使用扩展实用工具指定“加载设备固件”脚本。有关详细信息，请参阅 Network Configuration Manager 扩展实用工具 (p. 49)。

遵循这些步骤:

1. 在“资源管理器”选项卡中，从“设备系列”中选择 Cisco IOS 或支持 SSH 的 Cisco IOS 设备系列。

   信息和配置将出现在“内容”面板的“信息”选项卡中。

2. 展开“设备固件传输设置”子视图。

   通过固件传输选项，可以从服务器配置固件映像传输或者提供自定义脚本。

3. 执行下列步骤之一：

   - 根据需要修改固件映像传输协议。
   - 输入“加载设备固件”脚本。有关输入脚本的详细信息，请参阅输入配置脚本 (p. 54)。

   重要说明！如果存在脚本，则使用该脚本，而不管为固件映像传输协议指定了什么。

显示 Cisco 闪存分区信息

为了将新固件映像成功上传到设备，必须具有足够的可用磁盘空间以支持映像。本节介绍尝试固件上传之前查看设备上可用资源的一种便利方式。

注意：使用“创建 NCM 任务”对话框中的“查看分区”按钮，也可以在创建加载固件任务时显示设备的分区信息。有关详细信息，请参阅创建加载固件任务 (p. 94)。

显示 Cisco 闪存分区信息

1. 在“资源管理器”选项卡的“设备系列”中，从 Cisco IOS 或支持 SSH 的 Cisco IOS 设备系列中选择设备。

   在“内容”面板的“信息”选项卡中，将显示设备的信息和配置设置。

2. 展开“Cisco 闪存分区”子视图。

   将出现以下信息：

   名称

   分区名称。

   文件数

   分区中的文件数。

   可用空间

   分区中的可用空间量。必须存在足够的可用磁盘空间，以支持要上传的新固件映像。

   空间总量

   分配给分区的空间总量。

创建加载固件任务

本节介绍如何创建加载固件任务，该任务用于将固件上传到 Cisco IOS 和支持 SSH 的 Cisco IOS 设备。

注意：要完成该任务，需要指定将新固件映像上传到设备上的什么位置。目标位置必须具有足够的可用空间以支持新映像。要在创建任务之前查看设备上的可用资源，请参阅显示 Cisco 闪存分区信息 (p. 93)。

遵循这些步骤:

1. 在“资源管理器”选项卡的“设备系列”中，从 Cisco IOS 或支持 SSH 的 Cisco IOS 设备系列中选择设备。
2. 在“内容”面板中单击“列表”选项卡，然后为加载固件任务选择设备。
3. 从工具栏上的“创建 NCM 任务”图标选择“加载固件任务”。

   将打开“为加载固件任务选择设备”对话框。

   注意：如果选定的设备未出现在“允许”选项卡中，请单击“禁止”以显示从 Network Configuration Manager 任务中禁用的设备或者没有必要权限的设备。
4. 单击“继续”。

   将出现“创建 NCM 任务”对话框。
5. 创建任务，如下所示：
   a. 在“名称”字段中输入唯一名称。

      注意：Network Configuration Manager 提供了默认名称 (<*任务类型*>.YY-MM-DD_HH:MM.<*用户名*>)。例如，LoadFirmware.2006-10-17_15:48:04.Administrator。
   b. 在“说明”字段中输入任务的说明。
   c. 选择“可重用任务”以使任务变为可重用。
   d. 输入映像信息：

      固件映像名称

      映像服务器上固件映像的文件名。

      目标

      映像将位于设备上时的文件名。通常，这与服务器上的名称相同，且值将自动填充。

启动命令

要从其启动的映像的名称。这将用目标名称自动填充。

默认值：启动系统闪存

备份启动命令

出现错误时要从其启动的映像的名称。应该将其设置为设备上当前的可启动映像。这将用目标名称自动填充。

默认值：启动系统闪存

上传固件后重新加载设备

如果选择该选项，则启用“重新加载信息”字段，且在成功上传固件后将重新加载设备。

查看分区

单击“查看分区”可显示“设备分区”对话框，该对话框显示设备上的可用资源。目标位置必须具有足够的可用空间以支持新映像。

e. 输入重新加载信息（如果适用）：

立即重新加载

选择“立即重新加载”可在成功上传固件后立即重新加载设备。如果未选择该选项，请使用“计时”字段排定重新加载。

保存到启动配置(如果已修改)

如果运行配置已修改但未保存，则指示在重新加载开始之前是否将它复制到启动。

Telnet 登录超时

尝试登录到设备时用于 Telnet 连接的超时值（以秒为单位）。

Telnet 命令超时

尝试通过 Telnet 连接执行命令时要使用的超时值（以秒为单位）。

f. 单击“服务器设置”，然后在“编辑服务器设置”对话框中输入以下内容，以覆盖在设备系列级别上设定的传输设置：

协议

要使用的协议。

服务器地址

设备将从其复制固件映像的映像传输服务器地址。

超时(秒)

设备从固件映像服务器复制失败之前的超时期间。

映像目录

映像传输服务器上的子目录，将从其提供文件。

注意：如果映像不从映像服务器的根目录提供，则这可能是必需的。

用户名

映像传输服务器所需的用户名。

注意：这可能不是指定协议所需的。

密码

映像传输服务器所需的密码。

注意：这可能不是指定协议所需的。

6. 如果需要批准（如“请求批准”按钮所示），请执行以下步骤：
   a. 单击“请求批准”。

      将打开“需要批准”对话框。

   b. 选择用户，然后输入任务批准者的电子邮件地址。
   c. （可选）输入任务说明，然后单击“确定”以生成请求。

      将出现一个确认对话框，指示请求已成功创建。将向任务批准者发送一封电子邮件，且生成的任务将出现在“资源管理器”选项卡的“任务”文件夹中。

      注意：有关电子邮件配置的信息，请参阅*《管理员指南》*。

   d. 如启动任务 (p. 106)中所述，检查批准状态并运行任务。

   注意：有关批准工作流选项的信息，请参阅配置工作流 (p. 28)。
7. 如果不需要批准（如“保存”按钮所示）：
   a. 单击“保存”。

      将打开“任务已保存”对话框。

   b. 请执行下列操作之一：
      - 单击“上传固件”以处理任务。

        将打开“上传固件任务结果”对话框，且生成的任务将出现在“资源管理器”选项卡的“任务”文件夹中。有关详细信息，请参阅实时查看任务结果 (p. 108)。

- 单击“排定”以排定任务在将来执行。在排定任务 (p. 104)中对排定进行了介绍。

  任务将被保存，并按照排定运行。
- 单击“关闭”保存任务；它可供稍后运行。通过在“配置管理器”下“资源管理器”选项卡的“任务”中选择任务，可以编辑和运行该任务。

创建重新加载任务

创建重新加载任务可在上传固件后重新加载设备。该任务可用于 Cisco IOS 和支持 SSH 的 Cisco IOS 设备。

注意：在加载固件任务中也选择性地提供了重新加载任务所提供的功能。

遵循这些步骤:

1. 在“资源管理器”选项卡的“设备系列”中，从 Cisco IOS 或支持 SSH 的 Cisco IOS 设备系列中选择设备。
2. 在“内容”面板中单击“列表”选项卡，然后为重新加载任务选择设备。
3. 从工具栏上的“创建 NCM 任务”图标选择“重新加载任务”、“重新加载任务”。

   将打开“为重新加载任务选择设备”对话框。

   注意：如果选定的设备未出现在“允许”选项卡中，请单击“禁止”以显示从 Network Configuration Manager 任务中禁用的设备或者缺少必要权限的设备。
4. 如果需要批准（如“请求批准”按钮所示），请执行以下步骤：
   a. 单击“请求批准”。

      将打开“需要批准”对话框。
   b. 选择用户，然后输入任务批准者的电子邮件地址。
   c. （可选）输入任务说明，然后单击“确定”以生成请求。

      将出现一个确认对话框，指示请求已成功创建。将向任务批准者发送一封电子邮件，且生成的任务将出现在“资源管理器”选项卡的“任务”文件夹中。

      注意：有关电子邮件配置的信息，请参阅*《管理员指南》*。

d. 如启动任务 (p. 106)中所述，检查批准状态并运行任务。

在批准任务后启动它时，将出现“重新加载任务”对话框。

注意：有关批准工作流选项的信息，请参阅配置工作流 (p. 28)。

5. 如果不需要批准，请单击“立即运行重新加载任务”。

将出现“重新加载任务”对话框。

6. 创建任务，如下所示：

a. 输入重新加载信息：

立即重新加载

选择“立即重新加载”可立即重新加载设备。如果未选择该选项，请使用“计时”字段排定重新加载。

热加载

重新热加载（跳过复制映像到 NVRAM 并解压缩的步骤）。

保存到启动配置(如果已修改)

如果运行配置已修改，则指示在重新加载开始之前是否将它复制到启动。

Telnet 登录超时

尝试登录到设备时用于 Telnet 连接的超时值（以秒为单位）。

Telnet 命令超时

尝试通过 Telnet 连接执行命令时要使用的超时值（以秒为单位）。

b. 单击“确定”。

将打开“重新加载设备任务结果”对话框，且生成的任务将出现在“资源管理器”选项卡的“任务”文件夹中。有关详细信息，请参阅实时查看任务结果 (p. 108)。

创建取消重新加载任务

取消重新加载任务用于取消设备上已排定的挂起重新启动。该任务可用于 Cisco IOS 和支持 SSH 的 Cisco IOS 设备。

遵循这些步骤:

1. 在“资源管理器”选项卡的“设备系列”中，从 Cisco IOS 或支持 SSH 的 Cisco IOS 设备系列中选择设备。
2. 在“内容”面板中单击“列表”选项卡，然后为重新加载任务选择设备。

3. 从工具栏上的“创建 NCM 任务”图标选择“重新加载任务”、“取消重新加载任务”。

   将出现“为取消重新加载任务选择设备”对话框。

   注意：如果选定的设备未出现在“允许”选项卡中，请单击“禁止”以显示从 Network Configuration Manager 任务中禁用的设备或者没有必要权限的设备。

4. 如果需要批准（如“请求批准”按钮所示），请执行以下步骤：

   a. 单击“请求批准”。

      将打开“需要批准”对话框。

   b. 选择用户，然后输入任务批准者的电子邮件地址。

   c. （可选）提供任务说明。

   d. 单击“确定”以生成请求。

      将出现一个确认对话框，指示请求已成功创建。将向任务批准者发送一封电子邮件，且生成的任务将出现在“资源管理器”选项卡的“任务”文件夹中。

      注意：有关电子邮件配置的信息，请参阅*《管理员指南》*。

   e. 如启动任务 (p. 106)中所述，检查批准状态并运行任务。

   注意：有关批准工作流选项的信息，请参阅配置工作流 (p. 28)。

5. 如果不需要批准，请执行以下任一任务：

   - 单击“排定”以排定任务在将来执行。在排定任务 (p. 104)中对排定进行了介绍。
   - 单击“保存”。

     将保存任务以供将来执行。退出该过程。
   - 单击“立即运行取消重新加载任务”。

     将打开“取消重新加载设备任务结果”对话框，且生成的任务将出现在“资源管理器”选项卡的“任务”文件夹中。有关详细信息，请参阅实时查看任务结果 (p. 108)。

加载设备固件脚本

加载设备固件脚本可用于在设备上启动指定固件映像的加载，以替换对加载固件任务的、基于 MIB 的内部支持（仅用于支持 CISCO-FLASH-MIB 的 Cisco 设备）。有关使用脚本的详细信息，请参阅Network Configuration Manager 扩展实用工具 (p. 49)。

第 7 章： 管理任务

此部分包含以下主题：

使任务与全局集合关联 (p. 101)
排定批量任务 (p. 103)
启动和停止任务 (p. 106)
查看任务信息 (p. 107)
任务状况和状态值 (p. 109)

使任务与全局集合关联

可以使任务与全局集合关联。通过使任务与全局集合关联，在执行时任务将在支持该任务类型的集合的所有成员上运行。在初始任务创建期间或者任务已存在之后，可以进行任务与全局集合的关联。

注意：用户需要有“在 NCM 任务中包含全局集合”权限，才能使任务与全局集合关联。有关权限的详细信息，请参阅 Network Configuration Manager 权限 (p. 213)。

详细信息：

全局集合 (p. 23)

关联新任务

创建任务时，可以使任务与全局集合关联。

遵循这些步骤:

1. 在“资源管理器”选项卡中选择“全局集合”节点。

   已定义全局集合的列表将出现在“内容”面板的“列表”选项卡中。

   注意：如果全局集合不存在，则必须先创建一个全局集合才能继续。有关详细信息，请参阅*《IT 基础架构建模与管理 - 管理员指南》*。

2. 在“列表”选项卡上，选择要使任务与其关联的全局集合。

   将突出显示全局集合，且启用“创建 NCM 任务”图标。

3. 单击“创建 NCM 任务”图标，然后选择要创建并使其与该全局集合关联的任务。

   将出现任务的“选择设备”对话框。

4. 如 Network Configuration Manager 批量任务 (p. 85)或固件上传 (p. 91)（取决于任务）中所述，继续创建任务。

   在您完成时：

   - 新任务将出现在全局集合的“信息”选项卡上的“NCM 任务”子视图中。
   - 新任务将出现在“资源管理器”选项卡的“任务”文件夹中。查看任务的“信息”选项卡时，任务与之关联的全局集合将出现在“全局集合”子视图中。

   执行任务时，在执行时它将在支持该任务类型的全局集合的所有成员上运行。

关联现有的任务

可以使现有的任务与全局集合关联，也可以在创建任务时执行关联 (p. 101)。可以使用以下过程，将其他全局集合添加到现有的任务或者删除集合。

遵循这些步骤:

1. 在“资源管理器”选项卡中，从“配置管理器”下的“任务”文件夹中选择任务。

   任务的信息将出现在“内容”面板的“信息”选项卡中。

2. 展开“全局集合”子视图。

   与选定任务关联的任何全局集合将出现在表中。

3. 单击表上方的“添加或删除全局集合”图标。

   将打开“任务成员编辑器”对话框。

4. 从“可用的全局集合”窗格（在右侧）中选择全局集合。使用箭头将它们移动到“关联的全局集合”窗格(在左侧)中以便与该任务关联。

   处于“关联的全局集合”窗格中的全局集合将与该任务关联。

5. 单击“保存”，然后在随后出现的确认对话框中单击“是”。

   关联的全局集合将出现在表中。执行任务时，在执行时它将在支持该任务类型的已关联全局集合的所有成员上运行。

排定批量任务

可以排定批量任务。在创建任务时或者任务运行后（对于可重用任务），可以完成排定。

可以排定以下任务：上传任务、同步任务、保存到启动任务、加载固件任务和取消重新加载任务。

注意：无法通过这种机制排定重新加载任务；将改用设备的内部排定机制。如果定义脚本以完成重新加载操作，则脚本必须利用设备的排定机制来排定重新加载任务。有关详细信息，请参阅输入配置脚本 (p. 54)。

一个任务只能与一个排定关联。如果在指定新排定时任务已具有现有的排定，则将删除以前的排定。必须手动删除重复任务；不执行自动清理。

任务在本质上是分布式的。基于本地格局的本地时区，每个“本地”任务都按排定的时间运行。建议的最佳做法是，使所有的 SpectroSERVER 采用相同的时区设置工作。“成功设备列表”和“失败设备列表”表中的“完成时间”列，显示了在特定设备上尝试任务操作的时间。该功能可以帮助确定，在不同时区中有多个格局的情况下在 DSS 中何时运行任务。

注意：需要有 Network Configuration Manager“排定 NCM 任务”权限，才能排定批量任务。

可重用任务

通过将任务定义为可重用，能够保存任务并多次运行它，而不必重新定义它。也可以创建重复的排定，以便按预定的时间自动运行任务。

有关排定任务的信息，请参阅排定任务 (p. 104)。

注意：具有重复排定的任务将自动创建为可重用任务。

在任务创建期间指定“可重用任务”选项时，会将任务指定为可重用。

在以下区域中，可将任务识别为可重用：

- 在“内容”面板的“列表”表的“可重用”字段中
- 在“组件详细信息”面板的“信息”选项卡的“常规任务信息”中

排定任务

通过排定任务，可以定义任务，然后指定它运行的将来日期和时间。将任务排定为仅运行一次或者重复运行。可以在创建任务时设置排定。使用“排定”或“编辑排定”按钮。或者，对于可重用任务，可以随时设置排定。

注意：无法排定从“主机配置”选项卡运行的任务。

遵循这些步骤:

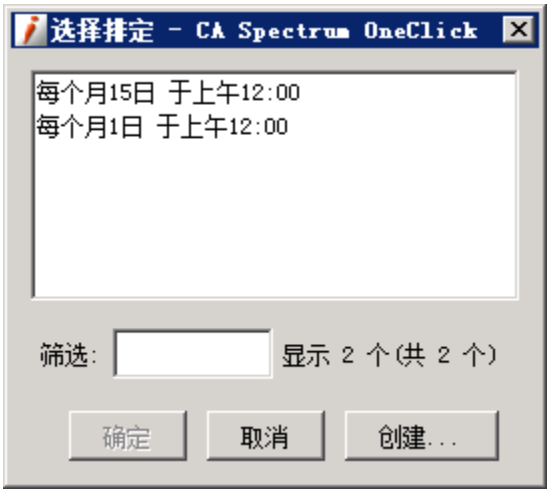
1. 按照 Network Configuration Manager 批量任务 (p. 85)和固件上传 (p. 91)中概述的过程创建以下任一任务：上传任务、同步任务、保存到启动任务、加载固件任务和取消重新加载任务。

   “排定”或“编辑排定”按钮（如果它可用）将出现在创建对话框中。

   注意：如果启用了批准工作流，则“排定”按钮在任务创建期间不可用；只能排定已批准的任务。创建任务后，必须设置排定。有关过程，请参阅下文。

2. 选择“排定”或“编辑排定”按钮。

   将出现“选择排定”对话框，如下图所示：

3. 执行下列步骤之一：

   - 选择默认排定，然后单击“确定”。
   - 创建自定义排定：单击“创建”按钮，指定排定选项，然后单击“确定”。

     自定义排定将添加到列表。选择新排定，然后单击“确定”。

   任务现已排定。排定将出现在“排定”按钮的旁边。

   注意：要删除任务的排定，请选择默认排定“无”。

4. 如果要多次运行该任务，请选择“可重用任务”。如果在上一步中指定了重复排定，则任务应创建为可重用任务。

   注意：不会自动清理可重用任务。

5. 执行下列步骤之一：

   - 保存任务。如果已指定排定，并希望稍后从“列表”选项卡中的“任务”文件夹运行任务，请单击“保存”按钮。将使用关联的排定（如果有）创建任务。
   - 运行任务。如果要立即运行任务，请单击“运行”按钮。

   任务将被保存，并出现在“资源管理器”的“任务”文件夹中，带有“排定任务”图标 。

   在“内容”面板的“列表”表的“排定”字段中，以及“组件详细信息”面板的“信息”选项卡的“常规任务信息”中，提供了排定信息。

由于以下任一原因，也可能在创建任务后创建或修改排定：

- 将任务设置为重复运行之前，希望彻底测试任务。
- 由于需要批准的任务在被批准之前无法排定，因此必须首先创建任务，然后等待批准。
- 站点状况已更改，要求修改排定。

遵循这些步骤:

1. 在“资源管理器”以及“内容”面板的“列表”选项卡中选择任务。

   将出现已定义的所有任务。

2. 选择要创建或修改其排定的任务。必须满足以下条件，任务才有排定资格：

   - 任务必须有运行资格。它是可重用任务（可重用 = 是），或者如果它不可重用，则它尚未运行（处于“非活动”状态）。
   - 如果启用了批准工作流，则任务必须处于“已批准”状态。

   如果任务可以排定，则为其启用工具栏中的“排定”按钮。

   注意：如果未启用“排定”按钮，请验证是否满足资格条件。

3. 单击“排定”按钮。

   将打开“选择排定”对话框。

4. 选择或创建排定。

启动和停止任务

本节介绍如何启动、停止、恢复和删除任务。

启动任务

以下过程介绍如何启动已创建的任务。如果任务尚未运行且为可重用任务，或者如果它们不是可重用任务且根本未运行它们，则可以启动它们。如果启用了批准，则任务必须处于“已批准”状态。

注意：必须先批准需要批准的任何配置更改任务，才能运行它。

遵循这些步骤:

1. 在“资源管理器”选项卡中，从“配置管理器”下的“任务”视图中选择任务。
2. 在“内容”面板中选择“列表”选项卡。

   有关任务的信息将显示在“列表”表中。“状态”列中的值“等候批准”指示请求已生成但尚未批准；值“已批准”指示请求已批准且可以运行。
3. 选择要启动的任务。

   如果可以启动任务，则启用“启动”按钮。
4. 单击“启动选定的任务”图标以运行任务。

   如果任务需要信息，请参阅有关该任务的一节。否则，任务将启动，且更新“任务状态”值。

   根据任务的不同，可能会出现结果对话框。有关详细信息，请参阅实时查看任务结果 (p. 108)。

停止任务

任务正在运行时，可以停止它。

遵循这些步骤:

1. 在“资源管理器”选项卡中的“配置管理器”下选择“任务”。
2. 在“内容”面板中单击“列表”选项卡，然后选择任务。

   注意：只能停止状态为“正在运行”的任务。
3. 单击工具栏中的“停止选定的任务”图标。

   任务将停止，且更新“任务状态”值。

恢复任务

如果任务已停止且将设备保留在“剩余设备列表”中，则可以恢复该任务。恢复任务时，Network Configuration Manager 仅尝试在处于“剩余”列表中的那些设备上运行操作。在以前已成功或者已失败且从“剩余”列表中删除的那些设备上，不会重新尝试该操作。

遵循这些步骤:

1. 在“资源管理器”选项卡中的“配置管理器”下选择“任务”。
2. 在“内容”面板中单击“列表”选项卡，然后选择要恢复的任务。

   注意：只能恢复具有剩余设备（由“剩余”列中的正值表示）的任务。
3. 单击工具栏中的“恢复选定的任务”图标。

   任务将启动，且更新“状态”值。

删除任务

可以在 OneClick 中删除任务。

注意：无法删除正在运行的或者已锁定进行编辑的任务。

遵循这些步骤:

1. 在“资源管理器”选项卡中的“配置管理器”下选择“任务”。
2. 在“内容”面板中单击“列表”选项卡，然后选择要删除的任务。
3. 单击工具栏中的“删除选定的任务”图标。

   将出现“确认删除”对话框。
4. 单击“是”进行删除。

   将删除选定的任务。

查看任务信息

本节介绍如何查看有关已创建的和已运行的任务的信息。

实时查看任务结果

启动上传、同步、保存到启动、加载固件任务、重新加载或取消重新加载任务后，将打开结果对话框。任务的名称、条件、类型和状态（“待处理”、“失败”或“已成功”）将显示在“结果”选项卡中。如果状态为“失败”，则结果出现在“失败原因”字段中。

注意：任务统计信息按 10 秒的轮询周期进行更新。

任务正在运行时，可以在结果对话框中执行以下操作：

- 单击“内容”选项卡以查看正在上传的内容。

  注意：“内容”选项卡仅在“上传任务结果”对话框和“加载固件任务结果”对话框中可用。
- 单击“停止”以取消任务。任务将正在运行的任何设备处理完毕。然后，它停止处理剩余的任何设备。
- 单击“关闭”以在后台运行任务。

查看有关所有批量任务的关键统计信息

可以同时查看所有批量任务的关键统计信息。

遵循这些步骤:

1. 在“资源管理器”选项卡中的“配置管理器”下选择“任务”。
2. 在“内容”面板中选择“列表”选项卡。

   将显示所有批量任务的统计信息。

查看批量任务的详细统计信息

执行不同步骤以查看单个批量任务的详细统计信息。

遵循这些步骤:

1. 从“资源管理器”选项卡的“任务”文件夹中选择任务。
2. 在“内容”面板中单击“信息”选项卡。

   将显示有关任务的信息。

任务状况和状态值

“任务状况”（状况）和“任务状态”值标识任务的当前执行阶段。查看任务结果或统计信息时，任务状况（状况）和任务状态可用。要访问这些视图，请参阅查看任务信息 (p. 107)。

任务状况

以下是可能的任务状况（状况）值：

已批准

已为该任务启用批准工作流模式。该任务已由相应的任务批准者批准，且可以运行。

等候批准

已为该任务启用批准工作流模式。已生成但尚未批准对该任务的请求。

已完成

任务已成功运行且可重用。位于重复排定上且已运行至少一次的任务将具有该状况。

已完成等候销毁

任务已运行且不可重用。任务将在 24 个小时内清除。

已拒绝

已为该任务启用批准工作流模式。生成了对该任务的请求，但已被相应的任务批准者拒绝。

非活动

任务已排定但尚未运行。

正在初始化

CA Spectrum 中的任务准备已启动。

正在运行

任务当前正在运行。可以停止处于该状况的任务。

正在停止

任务已启动，然后被用户停止。

任务状态

以下是可能的“任务状态”值：

失败

任务未成功完成。结果将显示在“失败原因”字段中。

待处理

任务当前正在运行。可以停止处于该状况的任务。

已成功

任务已成功完成。

第 8 章： Network Configuration Manager 策略

本章介绍如何创建和配置 Network Configuration Manager 策略。Network Configuration Manager 策略监控配置中的内容，并验证设备内容是否遵从策略。

注意：我们建议在设置 Network Configuration Manager 策略之前已捕获配置。请参阅全局同步任务 (p. 67)，以在网络上设置全局同步任务。

此部分包含以下主题：

关于 Network Configuration Manager 策略 (p. 111)
创建策略 (p. 113)
修复非遵从设备 (p. 130)
管理策略 (p. 131)
查看策略信息 (p. 134)
多行块策略示例 (p. 135)

关于 Network Configuration Manager 策略

Network Configuration Manager *策略*定义用于监控设备主机配置内容的标准。每次捕获到设备主机配置文件时，都会检查并比较策略。违反策略的设备可以生成警报并接收修正。

可以创建策略，并将其应用于单个设备和全局集合。将策略应用于全局集合时，在每个设备系列的所有全局集合成员上都将实施该策略。有关设置全局集合的详细信息，请参阅Network Configuration Manager 和全局集合 (p. 23)。

可以创建两种类型的策略：单行策略和多行块策略。将在以下各节中对它们进行介绍。

注意：在 Enterasys/Riverstone SSR 设备上执行的配置捕获将提供启动配置，而不是运行配置。因此，确定设备是否遵从 Network Configuration Manager 策略时，将使用启动配置。有关 SSR 设备如何处理 Network Configuration Manager 配置上传的信息，请参阅确定 Enterasys/Riverstone SSR 设备如何响应上传任务 (p. 87)。

单行策略

单行策略将当前定义的主机配置与策略定义进行比较，一次比较一行。将对照策略分析主机配置中的每行数据。在整个配置中检查是否存在单个命令时，这种策略很有用。

示例

假定站点具有一个规定，要求所有交换机必须已启用 http。通过其配置中的以下内容使交换机联机：

```
#http configuration
set ip http server disable
set ip http port 80
```

为了使该设备遵从站点规定，“set ip http server disable”应为“set ip http server enable”。要识别并更正这种情况，可以创建单行策略，以检查配置中是否具有“set ip http server enable”行。如果配置中缺少该行，则可以指定生成警报，以便可以修复该情况。在警报中，可以查看策略违反，然后可以选择通过排定任务以上传更正后的内容来修复设备。

多行块策略

多行块策略将当前定义的主机配置与策略进行比较，一次比较一个块。策略尝试对策略和当前主机配置之间的对应块进行匹配。块是通过开始标记和结束标记指定的；策略仅分析限定块内的数据。监控配置文本（如接口配置）块的设置时，这种策略很有用。大多数设备具有多个接口，其中各个接口的独特设置出现在同一配置文件中。

实施块策略时有两个选项可用：可以将配置内容与一组预定义的策略标准进行比较，或者可以将它与配置历史记录中的上一配置或参考配置进行比较。

与上一配置或参考配置进行比较时，将识别已更改、已添加或已删除的行。要突出显示在块的上下文中发生的更改，与上一配置或参考配置比较很有用；在指定块之外发生的更改将显示为屏蔽的或不相关的更改。

与预定义的策略标准进行比较时，将突出显示违反标准的行。也可以突出显示块内重新排序的行。

示例

假定希望关闭通过其说明中出现的“shutdown”一词识别的某些接口。通过按以下方式定义多行块策略，可以识别这样的设备：

- 通过与指定内容进行比较。可以搜索说明中不包含“shutdown”的所有接口，作为策略定义。这将突出显示在说明中*确实*包含“shutdown”的所有接口，作为策略违反者。
- 通过与其他配置比较。每次发生捕获时，通过将新捕获的配置与参考配置进行比较，可以监控内容。将“shutdown”添加到接口的说明时，该接口将作为策略的违反者突出显示，因为它与参考配置不匹配。

识别设备后，作为建议用于更正操作的上传的一部分，可以对标记为要关闭的那些接口轻松地发出 shutdown 命令。

在多行块策略示例 (p. 135)中详细介绍了该示例的实现。

创建策略

策略定义用于监控设备主机配置内容的标准。可以创建策略，并将其应用于单个设备和全局集合。可以创建两种类型的策略：单行策略和多行块策略。以下过程介绍如何创建 Network Configuration Manager 策略。

注意：在多行块策略示例 (p. 135)中提供了一个示例。

遵循这些步骤:

1. 在“资源管理器”选项卡中选择单个设备。

   设备的信息将显示在“内容”面板的“信息”选项卡中。

2. 展开“网络配置策略”子视图。

   将出现“网络配置策略”表。

3. 单击“创建策略”图标。

   将出现“选择策略类型”对话框。

4. 单击要创建的策略的类型：

   - **单行策略。**创建一次仅比较一行配置的策略。将打开“创建 NCM 策略”对话框。
   - **多行块策略。**创建按限定块比较主机配置的策略。将打开“创建 NCM 块策略”对话框。

5. 在“策略 ID”部分中，输入策略的名称和说明。

6. 在对话框的“策略标准”部分中，配置策略标准，如下所示：
   - 对于单行策略，请参阅单行策略标准 (p. 115)。
   - 对于多行块策略，请参阅多行块策略标准 (p. 115)。
7. 在对话框的“策略操作”部分中，执行以下操作：
   a. 输入警报标准，如下所示：

      违反时发出设备警报

      指示设备不遵从该策略时是否向设备发出警报。这是针对每个非遵从设备的单个警报，可在“警报”选项卡中查看。还可以选择警报的重要级别（“关键”、“主要”或“次要”）。必须启用策略，该选项才能生效。

      违反时发出策略警报

      指示至少一个设备不遵从策略时是否向策略发出警报。这是针对单个策略的单个警报，可在“警报”选项卡中查看。还可以选择警报的重要级别（“关键”、“主要”或“次要”）。必须启用策略，该选项才能生效。

   b. 输入建议用于更正操作的上传。
      - 对于单行策略，请参阅单行策略更正操作 (p. 122)。
      - 对于多行块策略，请参阅多行块策略更正操作 (p. 122)。
   c. 选择“提交到启动”选项，以指示在合并新内容后是否将整个运行配置复制到启动配置。
8. 单击“保存”。

   将出现“保存 NCM 策略”或“保存 NCM 块策略”对话框。
9. 单击“继续”。

   注意：如果单击“退出”，则策略将变为非活动状态，且不检查设备是否遵从该策略；但是，通过在“资源管理器”选项卡的“策略”中选择该策略，可以在将来某个时间启用它。

   将打开“测试 NCM 策略”或“测试 NCM 块策略”对话框。将对照 CA Spectrum 数据库中一个或多个设备的存储配置来测试策略。将显示策略结果，包括更正操作（如果适用），以供您查看。测试策略时，不生成警报。
10. 如果设备不遵从策略：
    a. 单击“查看违反”以了解有关设备为什么不遵从策略的信息。

       将出现“查看违反”对话框。有关“查看违反”对话框的详细信息，请参阅单行策略违反 (p. 124)或多行块策略违反 (p. 125)。
    b. 单击“关闭”。

11. 单击“修复”上传更正内容并将其合并到设备，以使其遵从策略。有关详细信息，请参阅从策略表修复非遵从设备 (p. 130)。

    注意：仅当已提供更正操作时，才启用“修复”。

12. 通过检查数据库中的配置并生成警报（如果适用且必要时），选择“启用策略”以立即应用该策略。

    注意：也可以从“网络配置策略”对话框启用（或禁用）策略。有关详细信息，请参阅从策略表启用和禁用策略 (p. 132)。

13. 单击“完成”。

策略标准

对于单行策略和多行块策略而言，可以指定的策略标准的类型有所不同。本节介绍如何根据已定义的策略类型来指定策略标准。其中包含以下主题：

- 单行策略标准 (p. 115)
- 多行块策略标准 (p. 115)
- 策略标准对话框 (p. 120)

单行策略标准

使用以下过程可指定单行策略的比较标准。

指定单行策略的标准

1. 在“创建 NCM 策略”对话框的“策略标准”部分中，单击“添加”以创建比较标准。

   将打开“策略标准”对话框。

2. 如策略标准对话框 (p. 120)中所述，配置策略标准。

   完成“策略标准”对话框后，新比较标准将出现在表中。

3. 要添加更多的标准或修改现有的标准，请使用“添加”、“编辑”和“删除”按钮。

在创建策略 (p. 113)中介绍了该对话框的剩余部分，包括策略的保存。

多行块策略标准

定义多行块策略时，必须指定两种类型的标准：块定义标准和比较标准。块定义标准定义构成块的开头和结尾的内容；比较标准定义用于对照当前主机配置进行比较的内容。

本节介绍如何定义该标准，其中包含以下主题：

- 关于块 (p. 116)
- 指定多行块策略的标准 (p. 117)
- 与指定内容进行比较 (p. 118)
- 与参考配置或上一配置中的匹配块进行比较 (p. 119)

关于块

使用多行块策略时，需要知道构成设备的主机配置文件中块的内容。在以下支持 SSH 的 Cisco IOS 设备示例中，每个接口都存在类似如下的块。该块将由“interface *name*”行和注释字符“!”定界：

```
interface Loopback0
 description "test 123"
 ip address 138.42.96.6 255.255.255.255
 ip pim sparse-dense-mode
 no ip route-cache cef
 no ip route-cache
 ipv6 address 2002:8A2A:5E12:8A2A:6006::1/128
 ipv6 enable
 ipv6 rip IPv6-1 enable
!
```

定义策略时，将使用该信息。在块策略术语中，该块由以下内容定义：

开始标记：interface *name*

结束标记：!

可以使用文本或正则表达式来定义构成块的开头和结尾的内容。以下介绍在确定有资格作为开始或结束标记的内容时这两个选项有何差异。

注意：定义为开始标记和结束标记的值将作为块的一部分包括在内。

使用文本

使用文本时，包含匹配文本的整个行将与该字段进行匹配。例如，如果将文本类型的“interface”用作开始标记，则这将与包含“interface”一词的每一行匹配，并将它视为块的起始行。

使用正则表达式 (Regex)

使用正则表达式时，只有正则表达式模式（而不是整个行）的完全匹配项才将与该字段进行匹配。例如，如果将“interface abc”指定为结束标记，则只有截至“interface abc”的内容才被视为块的结尾。相反，如果指定了“interface abc.*”（其中“.*”是正则表达式中与行中的任何字符匹配的通配符模式），则与“interface abc”匹配的整个行将被视为块的结尾。

指定多行块策略的标准

以下过程介绍如何指定多行块策略的标准。

遵循这些步骤:

1. 在“创建 NCM 块策略”对话框的“策略标准”部分中，指定以下块定义标准。

   可以使用文本或正则表达式来定义构成块的开头和结尾的内容。有关这两个选项有何差异的其他说明，请参阅关于块 (p. 116)。

   注意：定义为开始标记和结束标记的值将作为块的一部分包括在内。

   开始标记

   指定若干个字符，用于指明在比较中使用的块的开头。策略在主机配置中查找该定界符标记，以识别块的开头。值可以采用文本或正则表达式格式，如选择“文本”或“正则表达式”按钮所示。以下示例是表示“interface”的正则表达式：

   ```
   (?m)^interface .*
   ```

   使用该示例，策略查找以“interface”开头的行。

   结束标记

   指定若干个字符，用于指明在比较中使用的块的结尾。策略将在主机配置中查找该定界符标记，以识别块的结尾。值可以采用文本或正则表达式格式，如选择“文本”或“正则表达式”按钮所示。以下示例是表示字符“!”的正则表达式：

   ```
   (?m)^!.*
   ```

   使用该示例，策略查找块开头之后、表示块的结尾的第一个注释字符（“!”）。

2. 在“比较标准”部分中，选择以下选项之一：

   - **与指定内容进行比较**

     指定策略将当前的主机配置与在该策略中指定的用户定义内容进行比较。有关详细信息，请参阅与指定内容进行比较 (p. 118)。

   - **与来自以下位置的匹配块进行比较**

     指定策略将当前的主机配置与上一配置或参考配置中的内容进行比较。有关详细信息，请参阅与参考配置或上一配置中的匹配块进行比较 (p. 119)。

在创建策略 (p. 113)中介绍了该对话框的剩余部分，包括策略的保存。

与指定内容进行比较

定义多行块策略时，可以显式指定要在当前配置的每个块中检查的内容。以下过程介绍如何在多行块策略中设置用户定义的标准。

设置用户定义的比较标准

1. 在“与指定内容进行比较”选项处于选中状态的“创建 NCM 块策略”对话框中，指定“顺序”。以下是可用的选项：

   与顺序无关

   指示与当前主机配置进行比较时不考虑标准的顺序。将仅基于内容违反策略。

   保持顺序且允许额外行

   指示指定的内容必须按指定的顺序出现以遵从策略；但是，允许在指定的内容之间散布其他内容。如果一些指定的内容未存在于配置中，或者它以其他顺序存在，则将违反策略。策略将忽略不匹配的行。

   保持顺序且不允许额外行

   指示指定的内容必须按指定的顺序出现且连续出现以遵从策略。如果配置块与指定的内容不完全匹配，则将违反策略；块内容中未由指定的内容显式定义的任何额外行将违反策略。

2. 单击“添加”以创建比较标准。

   将出现“策略标准”对话框。

3. 如策略标准对话框 (p. 120)中所述，配置策略标准。

   关闭“策略标准”对话框后，新的比较标准将出现在表中。如果在与主机配置比较时已指定保持顺序，将使用表中的标准顺序。

4. 要添加更多的标准或修改现有的标准，请使用“添加”、“编辑”和“删除”按钮。

与参考配置或上一配置中的匹配块进行比较

定义多行块策略时，可以指定策略将当前的主机配置与以前捕获的配置进行比较，或者与另存为参考配置的内容进行比较。将逐块比较内容。以下过程介绍如何设置策略，以将内容与参考配置或以前捕获的配置进行比较。

注意：测试策略时，设备必须存在参考配置或上一配置；否则，将导致“策略状态”为“不可测试”。

将内容与参考配置或上一配置进行比较

1. 在“与来自以下位置的匹配块进行比较”选项处于选中状态的“创建 NCM 块策略”对话框中，指定将内容与之比较的配置的类型。以下是可用的选项：

   上一配置

   指示当前的主机配置将与最新捕获的配置逐块进行比较。

   参考配置

   指示当前的主机配置将与指定为参考的配置逐块进行比较。有关设置参考配置的信息，请参阅指定参考配置 (p. 73)。

   参考配置或上一配置

   指示当前的主机配置将与已保存的配置逐块进行比较。首先，策略将查找参考配置。如果尚未为特定设备设置参考配置，则将块内容与上一已知配置进行比较。

   注意：测试策略时，如果设备不存在参考配置或上一配置，则将导致“策略状态”为“不可测试”。

2. （可选）执行以下步骤以指定块标识符。

   块标识符用于与两个配置之间的对应块匹配。可以从块中选出特定的文本，并将它用作块标识符。例如，要比较两个配置之间标记有“interface Loopback*n*”的接口，则必须将“interface Loopback.*”指定为块标识符。

   如果未指定块标识符，则块的第一行将用作块标识符。在大多数情况下，该默认值足以标识两个配置之间的匹配块。

   a. 单击“高级”。

      将打开“指定块标识符”对话框。

b. 指定块标识符以及值是文本还是正则表达式。

以下是正则表达式的一个示例，将与以“interface”开头的对应行匹配：

```
(?m)^interface .*
```

以下是表示“interface *name*”的正则表达式示例，其中将仅使用接口名称（与整个行相对）与对应的块匹配：

```
(?m)^interface ([a-z||A-Z||0-9||/]*)
```

注意：使用正则表达式时，将利用正则表达式捕获组选出块标识符。这是高级的正则表达式概念。使用正则表达式时，捕获组 1 将用作块标识符。在该示例中，组 1 是 ([a-z||A-Z||0-9||/]*)，它标识接口的名称。

有关在多块策略中使用文本和正则表达式的详细信息，请参阅关于块 (p. 116)。

c. 单击“确定”。

将关闭“块标识符”对话框。

策略标准对话框

以下过程介绍如何填写“策略标准”对话框，该对话框用于定义单行策略和多行块策略的比较标准。每次捕获设备的主机配置文件时，都将检查并比较您指定的内容。可以从“创建 NCM 策略”对话框调用“策略标准”对话框。

使用“策略标准”对话框定义标准

1. 选择策略的比较类型。可用的比较类型如下：

有行

指示主机配置文件包含指定的所有行。如果满足，则策略是遵从的并通过。

没有行

指示主机配置文件不包含指定的行。如果满足，则策略是遵从的并通过。

包含

指示主机配置文件包含这些词或符号。如果满足，则策略是遵从的并通过。

不包含

指示主机配置文件不包含这些词或符号。如果满足，则策略是遵从的并通过。

包含正则表达式

指示主机配置文件与这些正则表达式匹配。如果匹配，则策略是遵从的并通过。

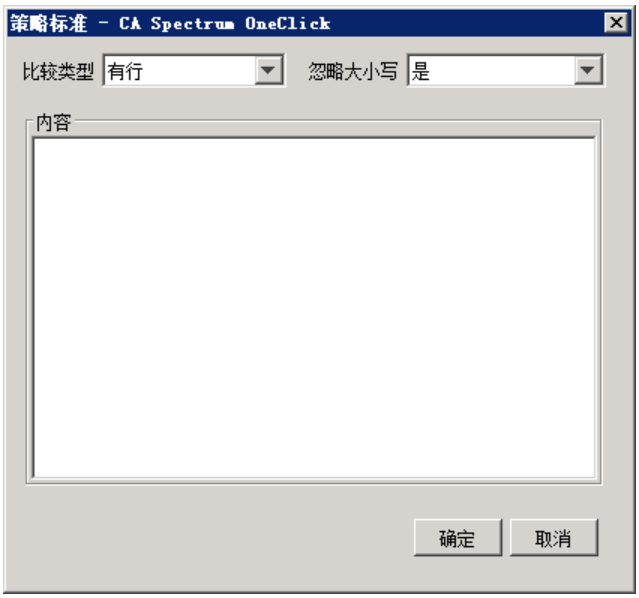
不包含正则表达式

指示主机配置文件与这些正则表达式不匹配。如果不匹配，则策略是遵从的并通过。

2. 指定是否忽略所输入内容的大小写。

   注意：使用正则表达式时，该设置不可用。

3. 单击“内容”框，然后输入内容（整行、子字符串或正则表达式）。以下是一个示例：



4. 单击“确定”。

   将关闭“策略标准”对话框，并返回到“创建 NCM 策略”或“创建 NCM 块策略”对话框，其中新标准将出现在表中。

建议用于更正操作的上传

“建议用于更正操作的上传”的设置在单行策略和多行块策略之间稍有不同。本节介绍如何根据已定义的策略类型来配置更正操作。其中包含以下主题：

- 单行策略更正操作 (p. 122)
- 多行块策略更正操作 (p. 122)

单行策略更正操作

对于单行策略，建议用于更正操作的上传涉及指定这样的内容：合并到运行配置后，将使设备遵从策略。以下过程介绍如何设置该内容。

输入单行策略的更正操作

1. 在“建议用于更正操作的上传”组下单击“编辑”。

   注意：也可以单击“打开”从文本文件导入内容。

   将打开“编辑更正操作”对话框。

2. 输入将修复非遵从设备的一行或多行。这是合并到运行配置后将使设备遵从该策略的内容。

3. 单击“确定”。

   将关闭“编辑更正操作”对话框，并显示更正行。

多行块策略更正操作

对于多行块策略，建议用于更正操作的上传涉及指定这样的内容：合并到运行配置后，将使设备遵从策略。由于块策略在本质上处理多个块或非遵从数据实例，因此必须设置更正操作以对此进行相应处理。以下过程介绍如何设置该内容。

输入多行块策略的更正操作

1. 如果希望更正操作受发生违反的每个块的影响，请选中“针对每个违反块重复”。如果取消选中它，则将仅针对第一个违反块原样上传更正操作。

2. 在“建议用于更正操作的上传”组下单击“编辑”。

   注意：也可以单击“打开”从文本文件导入内容。

   将打开“编辑更正操作”对话框。

3. 输入将修复非遵从设备的一行或多行。这是合并到运行配置后将使设备遵从该策略的内容。使用“插入所提取的内容”按钮将 <extracted_text> 标记插入到更正操作中，在策略运行时会将该标记替换为块特定的内容。以下显示了一个更正操作示例：

   ```
   interface <extracted_text>
   description "Spectrum 在 <extracted_text> 上检测到策略违反"
   !
   ```

   重要说明！修复文本必须是有效而完整的设备配置语句，尤其是重复修复操作时。例如，如果在上一示例结尾处省略了“!”，则更正操作可能无法正确执行，且可能出现意外结果。这是由于语句未正确结束：说明需要以换行符或具有“!”字符的新行结尾。

4. 单击“配置提取的内容”。

   将打开“编辑提取的内容”对话框。

5. 输入要从每个块提取的内容，然后选择它是文本还是正则表达式 (Regex)。

   - 如果是文本，则在更正操作中找到 <extracted_text> 标记的任何位置插入该值。
   - 如果是正则表达式，则在更正操作中找到 <extracted_text> 标记的任何位置插入计算该正则表达式后返回的值。

   以下是一个表示“interface *name*”的正则表达式示例：

   ```
   (?m)^interface ([a-z||A-Z||0-9||/]*)
   ```

   使用该示例，策略将从每个块中提取接口的名称，并将它插入到更正操作中。

   注意：有关在多块策略中使用文本和正则表达式的详细信息，请参阅多行块策略 (p. 112)。

6. 单击“确定”。

   将关闭“编辑更正操作”对话框，并显示更正行。

查看违反

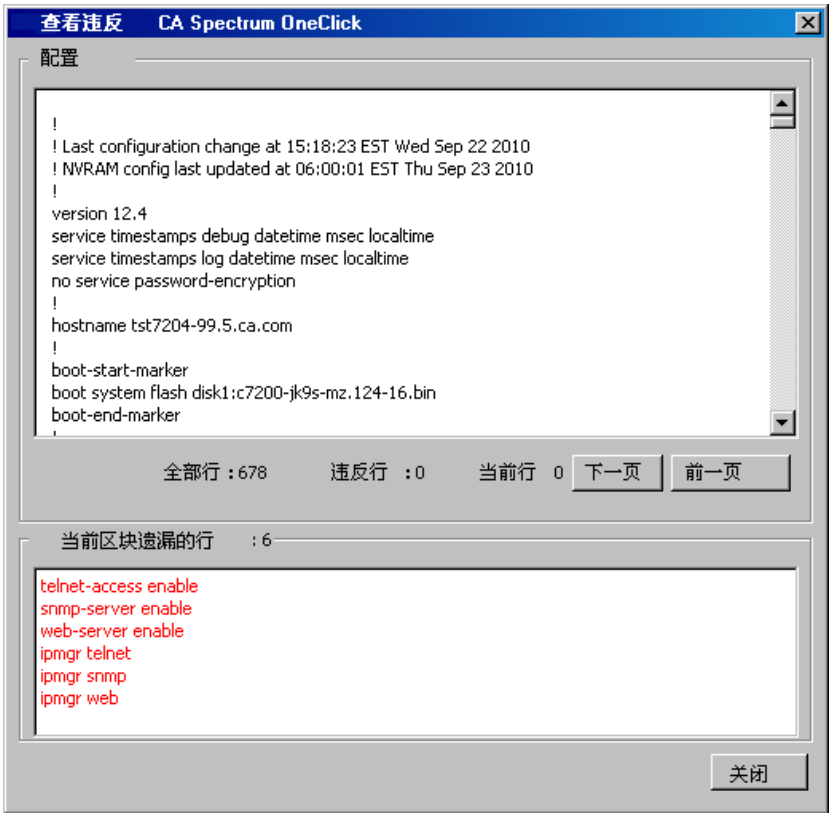
设备不遵从策略时，“查看违反”对话框将提供有关原因的信息。调用的对话框和提供的信息随策略定义的不同而有所不同。该部分包含以下主题：

- 单行策略违反 (p. 124)
- 多行块策略违反 (p. 125)

单行策略违反

所有单行策略的违反将显示在“查看违反”对话框中。

以下示例显示在设备的配置中缺少某些必需命令，因而违反了策略。



所有单行策略的“查看违反”对话框包含以下信息：

配置

完整显示所捕获的主机配置，并突出显示任何违反行。

总行数

提供配置文件中的总行数。

违反行

提供违反策略的行的总数。

当前行

提供配置文件中的当前位置。

下一个

允许您快速前进到下一个违反。

上一个

允许您后退到上一个违反。

当前块中缺少行: *total_number_of_lines*

显示在策略中定义的、在配置文件中找不到的那些行。

注意：对于单行策略，只有一个块。

多行块策略违反

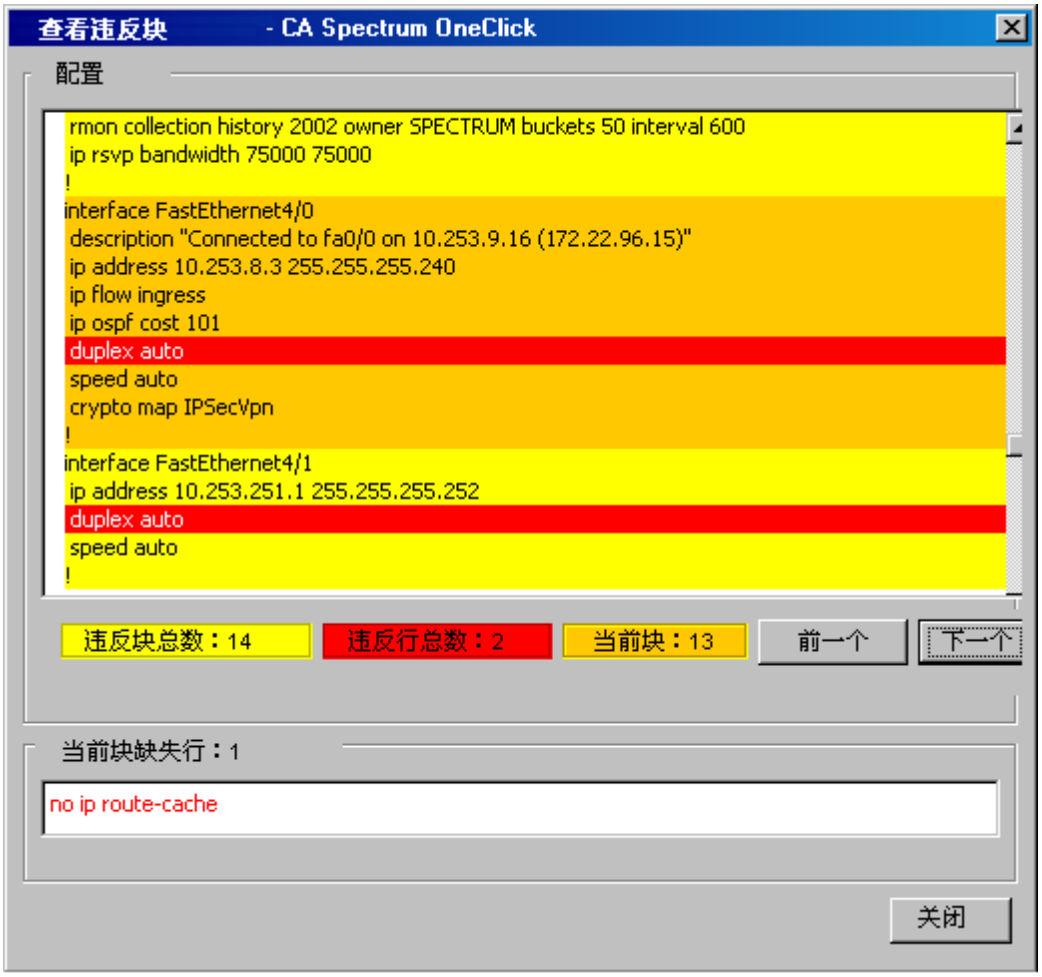
有以下两种类型的标准可用于多行块策略中的比较：用户定义的标准和来自所保存配置的内容。因此，根据要显示的违反内容，出现的“查看违反”对话框有所不同。

与特定内容比较时的违反

用户定义的标准用于多行块策略中的比较时，违反显示在“查看违反块”对话框中。

以下是多行块策略的“查看违反块”对话框的示例，其中当前的主机配置与用户定义的标准进行比较。

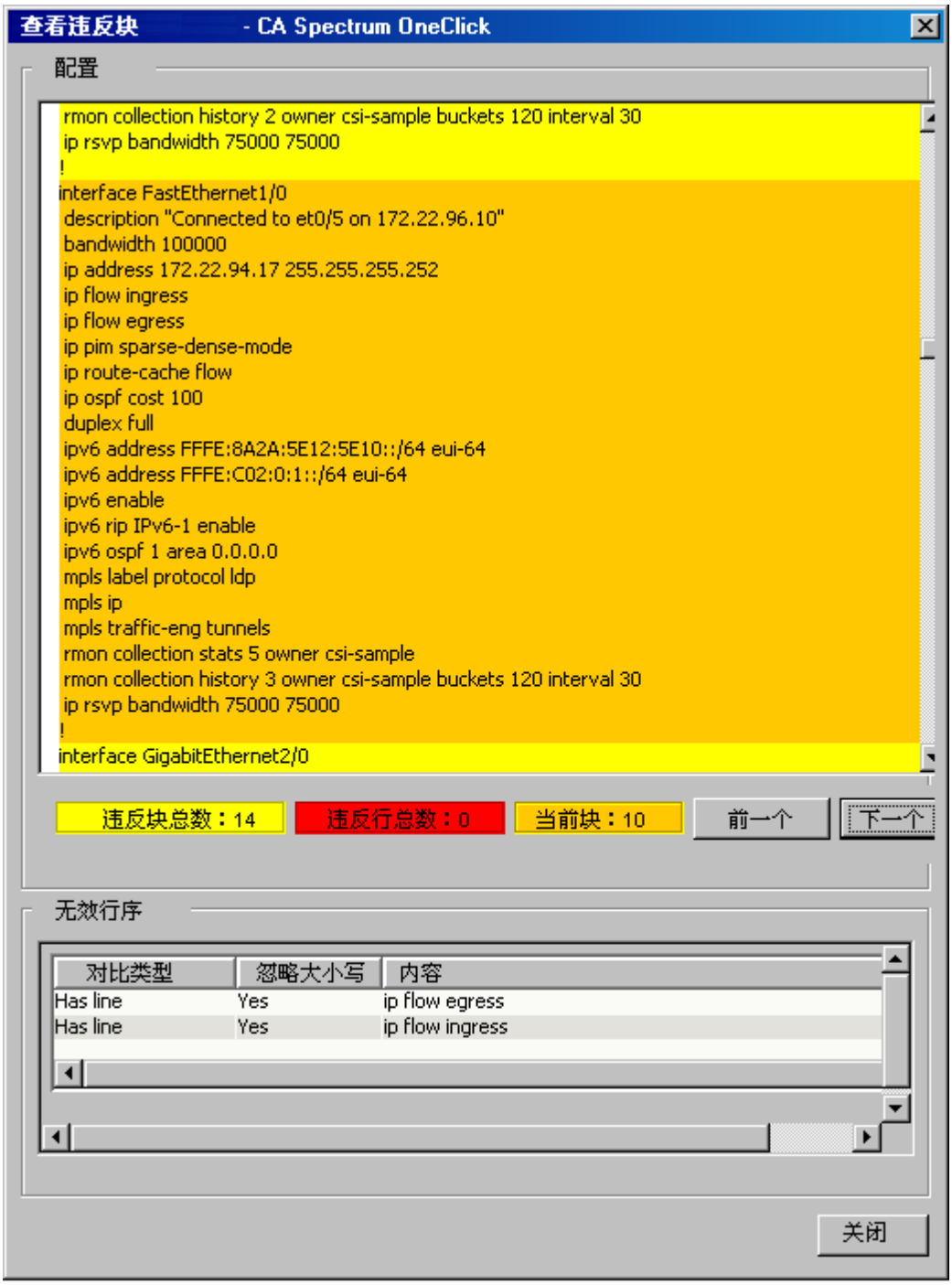
在该示例中，已将策略设置为检查每个接口配置中是否不存在“duplex auto”但存在“no ip route-cache”。对违反进行识别，如下所示：



在下一个示例中，已设置策略，以便在以下命令出现且它们按以下顺序出现时某个配置遵从该策略：

```
ip flow egress
ip flow ingress
```

当前配置违反该策略，因为虽然命令出现了，但是它们未按正确的顺序出现，如下图所示：



根据违反，“查看违反块”对话框可能包含以下信息：

配置

完整显示所捕获的主机配置，并突出显示任何违反行：

- **红色—**这些行包含违反。

块可按颜色进行区分：

- **橙色—**这些行构成了当前块。
- **黄色—**这些行包括在当前块以外的块中。

违反块总数

提供包含违反的块的总数。

违反行总计

提供违反策略的行的总数。

当前块

提供配置文件中的当前位置。对可区分的块编号以便于识别。

上一个

允许您后退到包含违反的上一个块。

下一个

允许您快速前进到包含违反的下一个块。

当前块中缺少行: *total_number_of_lines*

显示在策略中定义的、在配置文件中找不到的那些行。

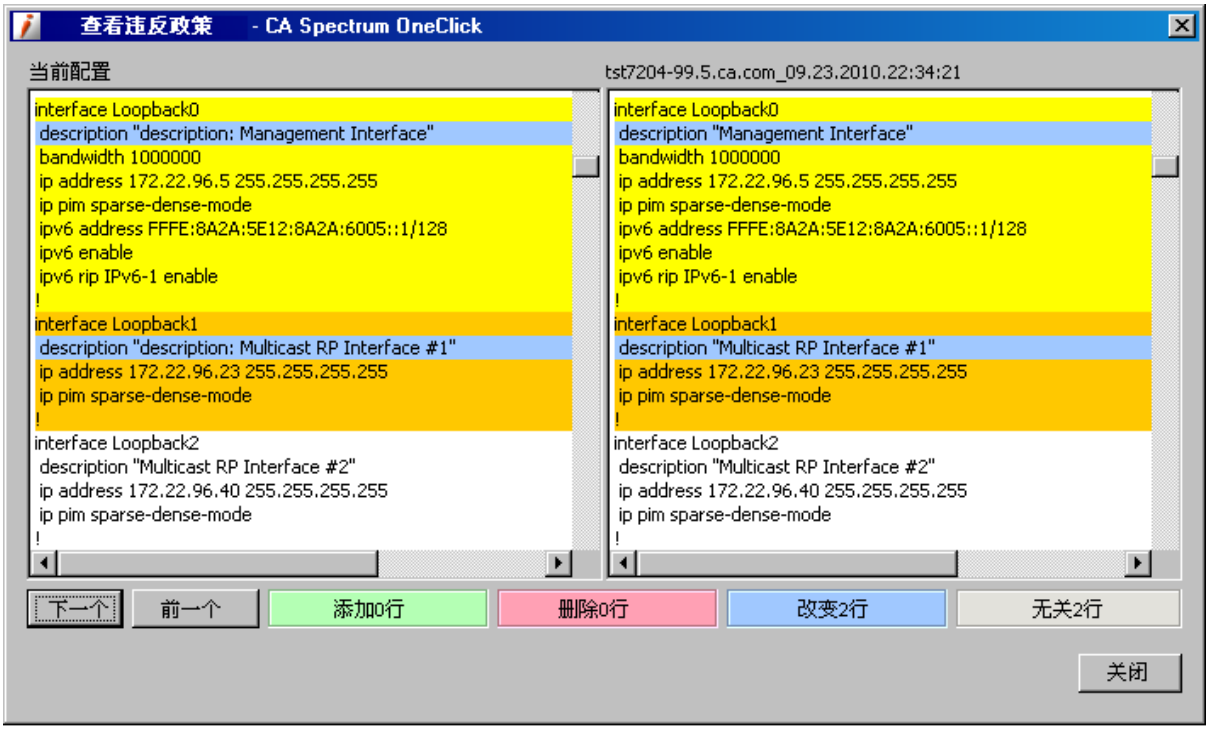
无效的行顺序

显示由于其在配置文件中的出现顺序而违反的内容标准。

与其他配置比较时的违反

已保存的配置用于多行块策略中的比较时，违反将显示在“查看策略违反”对话框中。

以下是多行块策略的“查看策略违反”对话框的示例，其中当前主机配置与参考配置进行比较，且行已更改，因此违反了策略。



当前主机配置位于左窗格中，而参考配置显示在右窗格中。根据以下项，突出显示这两个配置之间的差异。

包含差异的块在整体上突出显示，且可按颜色进行区分：

- **黄色**—这些行构成发生违反的块。
- **橙色**—这些行构成发生违反的块。

对表示差异的单个行进行识别，如下所示：

- **绿色**—这些行已添加。
- **红色**—这些行已删除。
- **蓝色**—这些行已更改。
- **灰色**—这些行不同，但在限定块之外。

单击“下一个”或“上一个”可在文件中的差异之间导航。

修复非遵从设备

除了在设置策略时修复非遵从设备外，还可以在发生违反后启动非遵从设备的修复。该部分包含以下主题：

- 从策略表修复非遵从设备 (p. 130)
- 从策略违反警报修复非遵从设备 (p. 131)

从策略表修复非遵从设备

通过选择单个设备或全局集合，可以从策略表检查并修复策略。例如，可以修复非遵从设备。

遵循这些步骤:

1. 在“资源管理器”选项卡中，选择具有已配置策略的单个设备或全局集合。
2. 在“内容”面板中选择“信息”选项卡。

   将出现有关设备或全局集合的信息。
3. 展开“网络配置策略”。

   将出现“网络配置策略”表。具有非遵从设备的策略在“违反者”列中具有非零值。
4. 选择具有非遵从设备的策略，然后单击“启动修复对话框”图标。

   将出现“修复违反的设备”对话框。
5. 单击“内容”选项卡以查看要为执行修复而上传的内容。
6. 单击“查看违反”以查看每个设备的违反。
7. 单击“修复”。

   将出现“正在创建任务”状态框。“上传任务结果”对话框将显示操作的结果。

从策略违反警报修复非遵从设备

可以从“警报详细信息”选项卡查看违反，并将正确的内容上传或合并到设备以使其遵从策略。直接从策略违反警报修复非遵从设备。

遵循这些步骤:

1. 在“资源管理器”选项卡中选择单个设备、具有已配置策略的全局集合或者策略（从“策略”节点）。
2. 在“内容”面板的“警报”选项卡中，选择“警报标题”列中包含“已违反 NCM 策略”的警报。
3. 在“组件详细信息”面板的“警报详细信息”选项卡中，单击“查看违反详细信息”。

   将打开“修复违反的设备”页。
4. 单击“内容”以查看要为执行修复而上传的内容。单击“查看违反”以查看每个设备的违反。

   将出现“查看违反”页。
5. 单击“修复”。

   将出现“正在创建任务”状态框，后跟“上传任务结果”页。

管理策略

创建策略后，可以编辑它、启用或禁用它、将它应用于全局集合以及删除它。该部分包含以下主题：

- 编辑策略 (p. 132)
- 启用和禁用策略 (p. 132)
- 将策略应用于全局集合 (p. 133)
- 删除策略 (p. 133)

编辑策略

可以编辑现有的 Network Configuration Manager 策略。编辑策略后，必须保存并启用它。

编辑策略

1. 在“资源管理器”选项卡中的“策略”节点下选择策略。
2. 在“内容”面板中选择“列表”选项卡。

   将出现策略列表。
3. 选择策略，然后单击工具栏中的“编辑”图标。

   将出现“编辑 NCM 策略”对话框。
4. 进行必要的更改，然后单击“保存”。

   将禁用策略。启用策略，如从策略表启用和禁用策略 (p. 132)所述。

   注意：（可选）可以编辑策略，方法是选择全局集合，单击“信息”选项卡，然后编辑关联的策略。也可以选择单个设备，单击“信息”选项卡，单击“网络配置策略”，然后编辑关联的策略。

启用和禁用策略

可以从策略表启用和禁用 Network Configuration Manager 策略。

遵循这些步骤:

1. 在“资源管理器”选项卡中的“策略”节点下选择策略。
2. 选择“内容”面板的“列表”选项卡。

   将出现策略列表。
3. 选择策略，然后单击“启用选定的策略”图标。

   启用策略将导致任何指定的警报对所有的非遵从设备和被违反策略立即出现。
4. （可选）选择策略，然后单击“禁用选定的策略”图标以禁用该策略。

   禁用策略将立即清除非遵从设备和被违反策略上的任何现有警报。

注意：通过选择全局集合或单个设备，也可以启用和禁用策略。使用“信息”选项卡管理关联的策略。

将策略应用于全局集合

创建策略后，可以将它应用于全局集合。将策略应用于全局集合后，会在每个设备系列的所有全局集合成员上实施该策略。

将策略应用于全局集合

1. 在“资源管理器”选项卡中选择全局集合。

   全局集合的信息将出现在“内容”面板的“信息”选项卡中。

2. 展开“网络配置策略”子视图。

   将出现“网络配置策略”表。

3. 单击“在全局集合中添加/删除策略”图标。

   将出现“在全局集合中添加/删除策略”对话框。

4. 选择要在该全局集合上实施的那些策略，并将其移动到“应用于”窗口。

   注意：也可以使用“创建”按钮，直接从该对话框创建策略。

5. 单击“确定”。

   已应用的策略出现在“网络配置策略”表中，并将在每个设备系列的全局成员上实施。

详细信息：

全局集合 (p. 23)

删除策略

要删除不再需要的策略，请从“资源管理器”选项卡的“策略”中右键单击策略，然后选择“删除”。

注意：（可选）可以删除策略，方法是选择全局集合，单击“信息”选项卡，然后删除关联的策略。也可以选择单个设备，单击“信息”选项卡，单击“网络配置策略”，然后删除关联的策略。

查看策略信息

本节介绍如何查看策略信息，其中包括以下主题：

- 查看策略详细信息 (p. 134)
- 查看所有策略的关键统计信息 (p. 134)
- 查看应用于全局集合的策略的关键统计信息 (p. 135)
- 查看应用于单个设备的所有策略的关键统计信息 (p. 135)

查看策略详细信息

可以查看 Network Configuration Manager 策略的组件详细信息。

遵循这些步骤:

1. 在“资源管理器”选项卡中选择具有关联策略的单个设备或全局集合。
2. 在“内容”面板中单击“信息”选项卡。

   将出现选定设备或全局集合的信息和配置。
3. 展开“网络配置策略”，然后单击“查看选定模型的组件详细信息”。

   将出现选定策略的“组件详细信息”面板。

   注意：通过从“资源管理器”选项卡的“策略”中选择策略，也可以访问该屏幕。

查看所有策略的关键统计信息

通过在“资源管理器”选项卡中的“配置管理器”下选择“策略”，然后在“内容”面板中选择“列表”选项卡，可以查看策略的关键统计信息。

将出现所有策略的统计信息。

查看应用于单个设备的所有策略的关键统计信息

可以查看应用于单个设备的策略的关键统计信息。

遵循这些步骤:

1. 选择设备，然后单击“信息”选项卡。

   将出现有关设备的信息。

2. 选择“网络配置策略”。

   将出现应用于单个设备的所有策略的统计信息。

查看应用于全局集合的策略的关键统计信息

可以查看应用于全局集合的策略的关键统计信息。

遵循这些步骤:

1. 从“资源管理器”选项卡中选择现有的全局集合。选择“内容”面板的“信息”选项卡。

   信息将出现在“内容”面板中。

2. 选择“网络配置策略”。

   将出现应用于集合的所有策略的统计信息。

多行块策略示例

本节提供如何使用多行块策略的一个示例。以两种不同的方法实现同一用例：通过与指定的内容比较以及与其他配置比较。

注意：本节中提供的内容旨在提供高级别的用例示例。有关本节中引用的任何概念或项的其他信息，请参阅相应的父主题。

该部分包含以下主题：

- 方案 (p. 136)
- 入门 (p. 136)
- 定义策略 (p. 138)
- 保存和测试策略 (p. 142)
- 监控违反 (p. 146)

方案

假定希望关闭通过其说明中出现的“shutdown”一词识别的某些接口。通过按以下方式定义多行块策略，可以识别这样的设备：

- 通过与指定内容进行比较。可以搜索说明中不包含“shutdown”的所有接口，作为策略定义。这将突出显示在说明中*确实*包含“shutdown”的所有接口，作为策略违反者。
- 通过与其他配置比较。每次发生捕获时，通过将新捕获的配置与参考配置进行比较，可以监控内容。将“shutdown”添加到接口的说明时，该接口将作为策略的违反者突出显示，因为它与参考配置不匹配。

识别设备后，作为建议用于更正操作的上传的一部分，可以对标记为要关闭的那些接口轻松地发出 shutdown 命令。

入门

在开始定义策略之前，必须执行以下操作：

- 识别构成块的内容。
- 建立参考配置（如果与参考配置进行比较）。

通过查看设备的已捕获主机配置，可以收集该信息。可使用全局同步任务、同步任务和“捕获配置”图标来捕获配置。

查看设备的已捕获主机配置

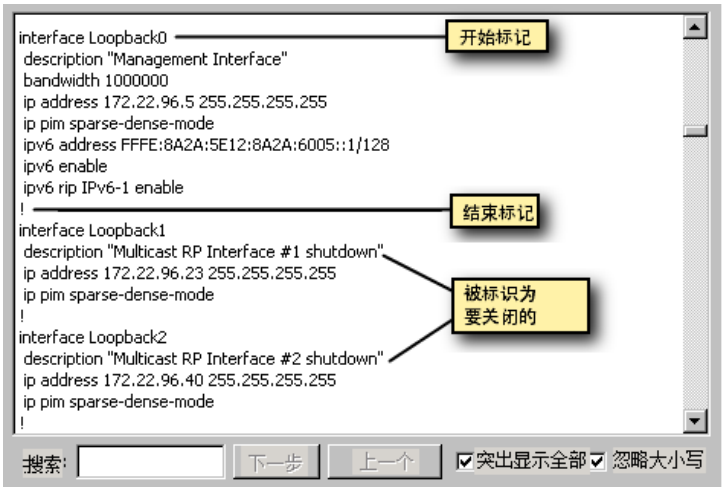
1. 在“资源管理器”选项卡中选择设备。
2. 验证在“内容”面板中选中了“列表”选项卡，并在“组件详细信息”面板中选择“主机配置”选项卡。
3. 在“主机配置”表中单击要查看的已捕获主机配置所在的行。

   已捕获的主机配置将出现在表下面的框中。

注意：有关详细信息，请参阅查看单个设备的配置历史记录 (p. 70)。

识别构成块的内容

下图显示了设备的配置文件的一部分。可以看到，该设备上的每个接口都具有类似的格式，并由开始标记和结束标记定界。此外，请注意“shutdown”出现在几个接口的说明中。



在块策略术语中，该示例中的每个块将由以下内容定义：

开始标记：interface

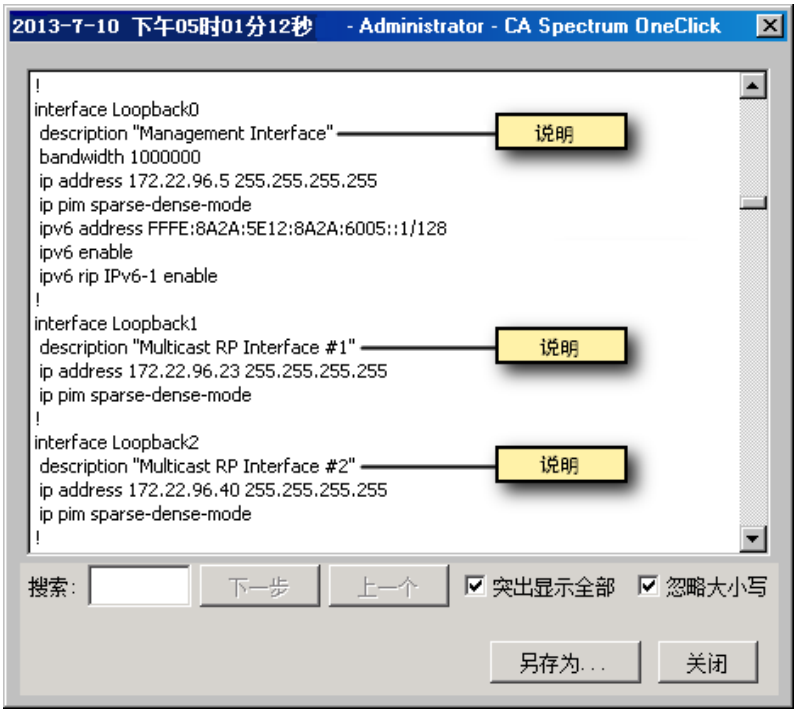
结束标记：!

建立参考配置（如果与参考配置进行比较）

使用“查看设备的已捕获主机配置”中概述的过程，识别包含设备的理想设置的主机配置，然后将该配置指定为其参考配置。有关设置参考配置的信息，请参阅指定参考配置 (p. 73)。

注意：也可以使用上次捕获的配置进行比较，而不是使用参考配置。

下图显示将用作参考配置的配置文件的一部分。请注意，该配置不包含任何接口的说明中的“shutdown”。



详细信息：

全局同步任务 (p. 67)
指定参考配置 (p. 73)
手动捕获配置 (p. 81)
创建同步任务 (p. 88)

定义策略

建立构成块的内容并指定参考配置（如果适用）后，可以定义多行块策略。

请参阅创建策略 (p. 113)中概述的步骤，创建多行块策略，然后调用“创建 NCM 块策略”对话框，该对话框包含以下部分：

- 策略 ID
- 策略标准
- 策略操作

将分别介绍其中每个部分。

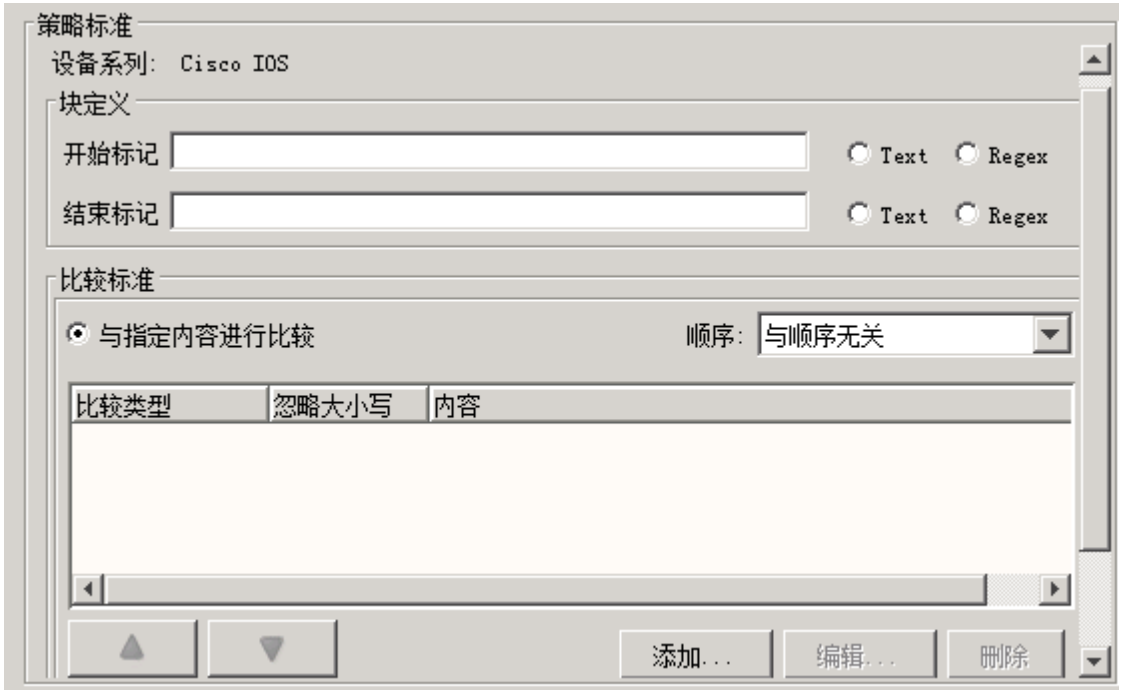
注意：在创建策略 (p. 113)一节中提供了本节中提到的每个字段的其他详细信息。

策略 ID

“策略 ID”信息用于标识策略。按照您站点的合适标准，使用这些字段对策略进行命名。

策略标准

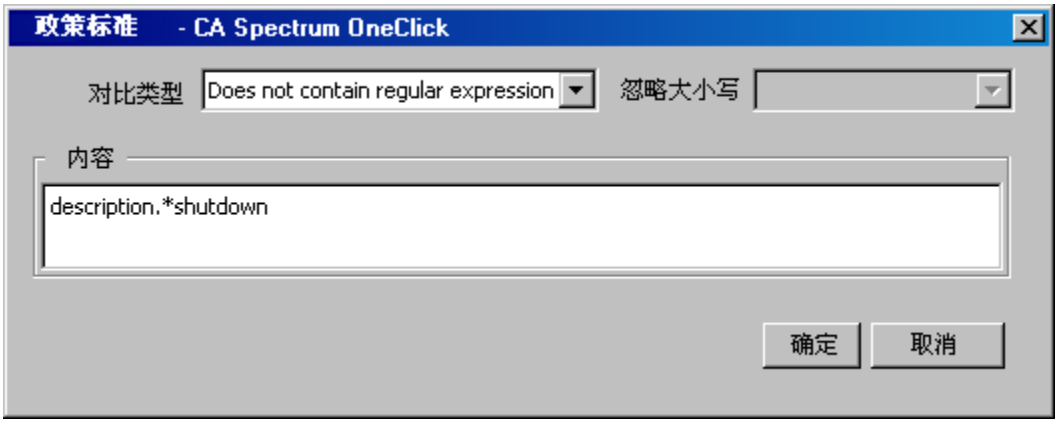
“策略标准”信息定义块定界字段和比较标准（将在下图的后面对其进行介绍）。



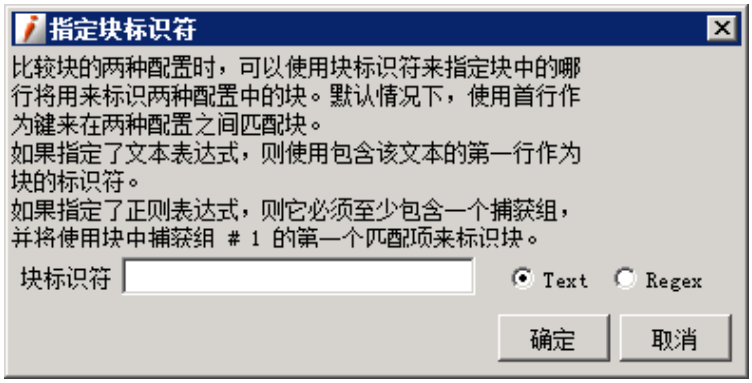
- **块定义。**“开始标记”和“结束标记”字段定义用于标识块的开头和结尾的字符串。在该示例中，正则表达式的值用于指明每个块以字符串“interface *name*”开头并以字符“!”结尾。这些值作为块的一部分包括在内。
- **比较标准。**该部分控制对照策略评估新捕获的配置所用的方法。可以指定将配置与特定的用户定义标准进行比较还是与其他配置进行比较。

  注意：在单个策略中只能包括一组标准。此处显示了两组标准，仅用于演示目的。

  - 选项“与指定内容进行比较”指示，在启用策略之后捕获的每个配置都将与用户定义的标准进行比较。单击“添加”按钮可显示“策略标准”对话框。下图显示了用于查找以“description”开头且包含“shutdown”的行的标准。该策略运行时，在说明中确实包含“shutdown”的接口将识别为违反者。



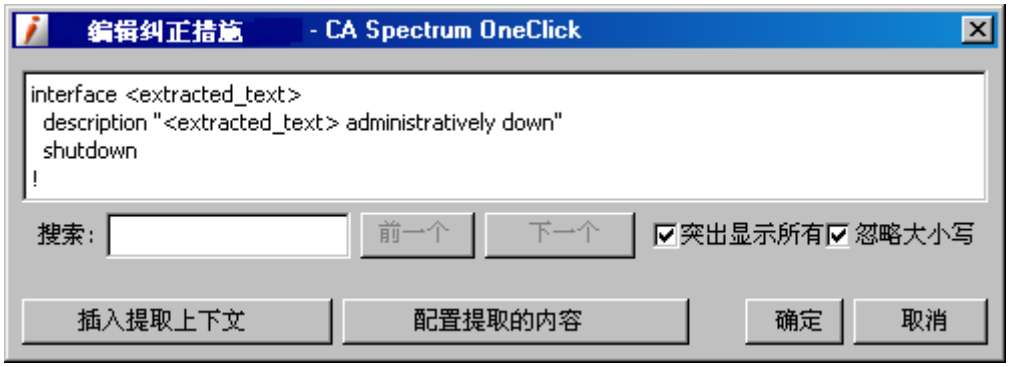
  - 选项“与来自参考配置的匹配块进行比较”指示，在启用策略之后捕获的每个配置都将与指定为设备参考配置的配置进行比较。单击“高级”按钮可指定块标识符，该标识符用于与当前配置和参考配置（或上一配置，如果指定）之间的对应块匹配。以下示例将基于“interface *name*”进行匹配：



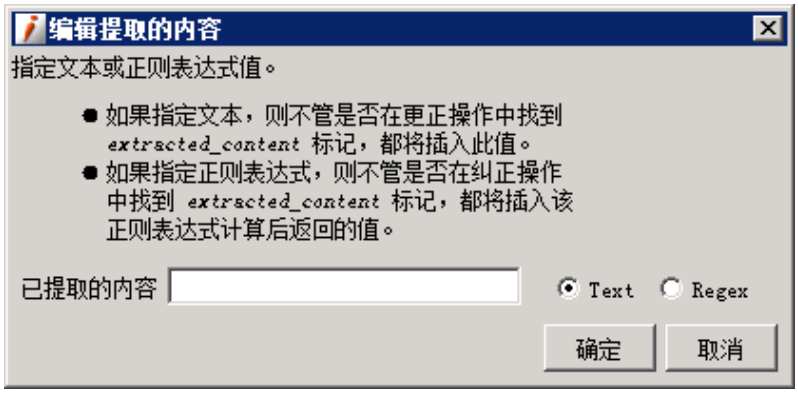
策略操作

“策略操作”选项定义应生成警报的方式，以及发生非遵从性情况时要上传的更正操作。下图显示了该部分（已经填充），后续还将进行介绍：

- 指定发生违反时的警报首选项。可以使警报与设备和/或策略关联。
- 要定义“建议用于更正操作的上传”，请单击“编辑”按钮以显示“编辑更正操作”对话框。在框中，输入将上传到设备的内容。下图显示了将已修改的说明和 shutdown 命令上传到设备的内容：



在该示例中，策略运行时，<extracted_text> 标记将替换为块特定的内容。要将该标记插入到更正操作中，请使用“插入所提取的内容”按钮。要配置将用于替换标记的内容，请单击“配置提取的内容”按钮，这将打开以下对话框：



在该示例中，接口的名称将从每个块提取且用于创建更正操作内容。

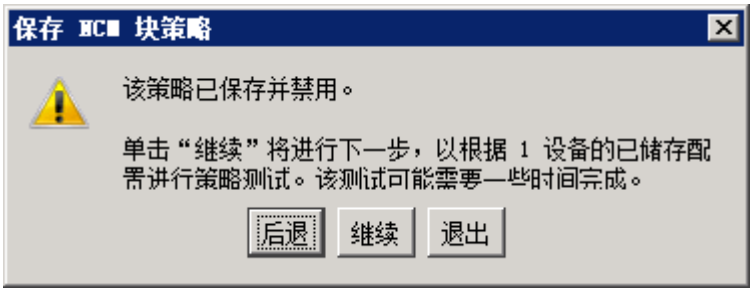
定义更正操作内容后，该内容将出现在“建议用于更正操作的上传”框中。如果要对每个违反实例进行该更改，请选择“针对每个违反块重复”选项；如果将它留空，则仅对第一个实例进行该更改。

保存和测试策略

最初定义策略后，应该对它进行测试再启用它，以确保它像预期的那样运行。

要继续测试策略，请单击“创建 NCM 块策略”对话框中的“保存”以保存设置。在随后出现的“保存”对话框（如下一个图像所示）中，单击“继续”以测试策略。

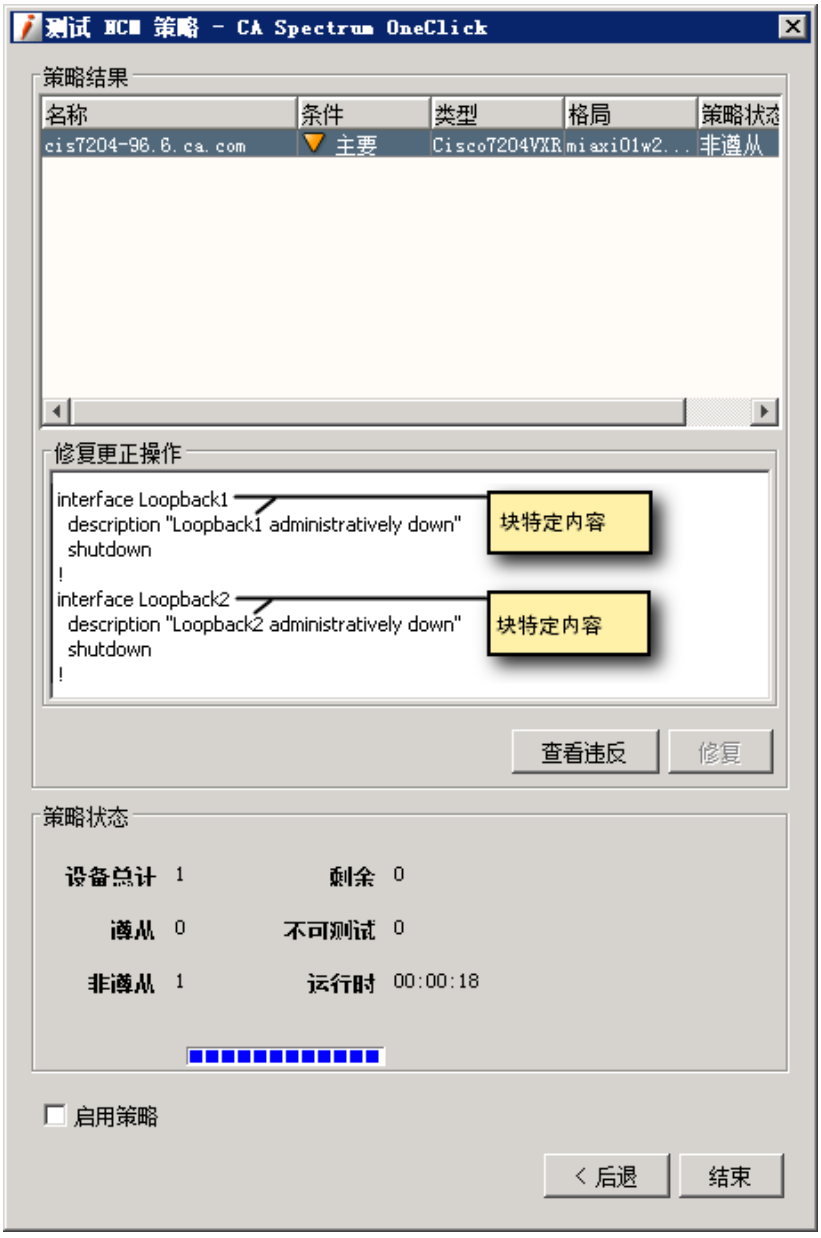
注意：也可以选择“后退”以对策略定义进行其他更改。如果单击“退出”，则将保存策略但禁用它。



将打开“测试 NCM 块策略”对话框，测试开始，状态栏指示其进度。在测试期间，捕获当前的配置并将其与在策略中指定的标准进行比较。将基于块标识符对块进行匹配，然后比较对应块的内容。

注意：根据包括的设备数，完成测试可能需要一段时间。

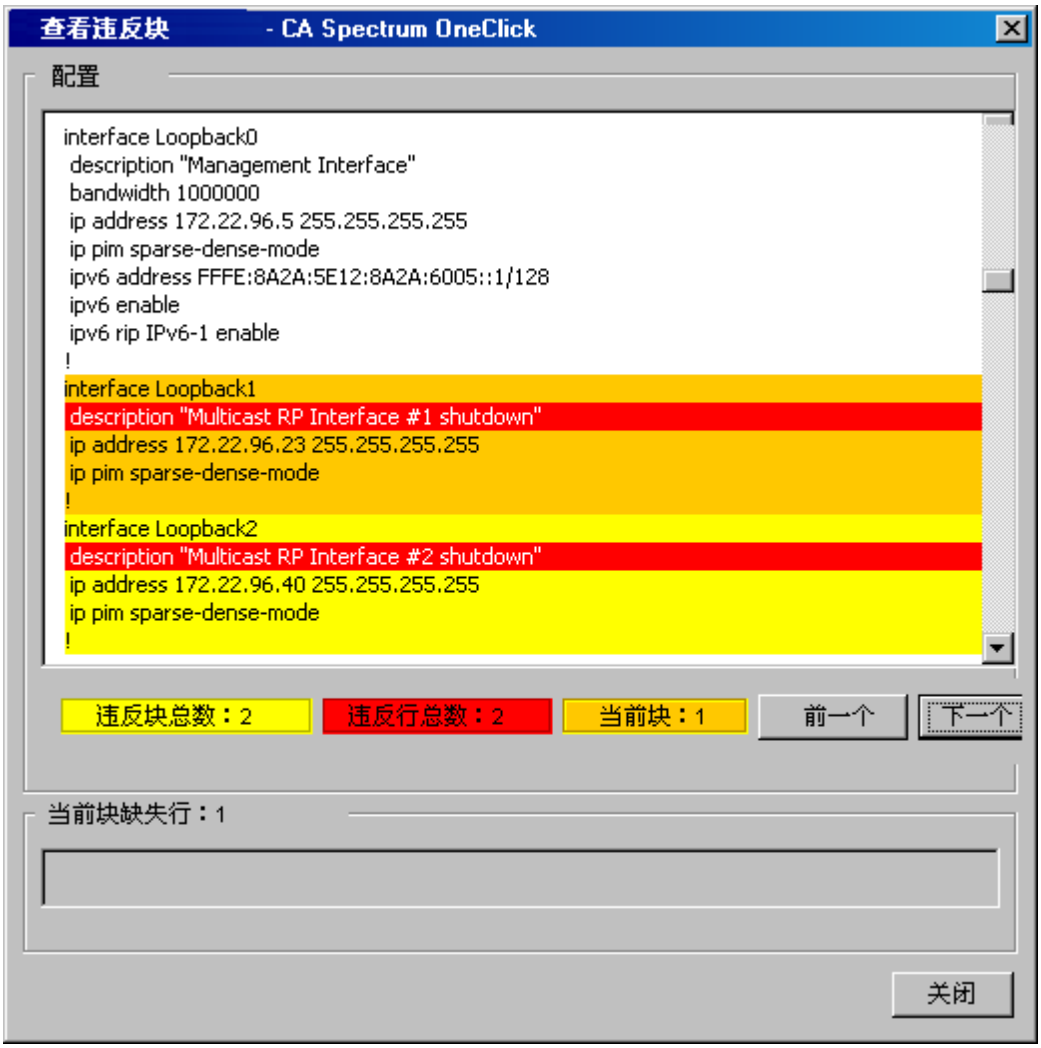
策略测试完成时，将显示策略结果，如下所示：



检测到非遵从性时（如在该示例中），将在“策略状态”部分中报告受影响的设备数，如果已定义它，则还将显示更正操作。请注意，已将 <extracted_text> 标记替换为块特定的内容。

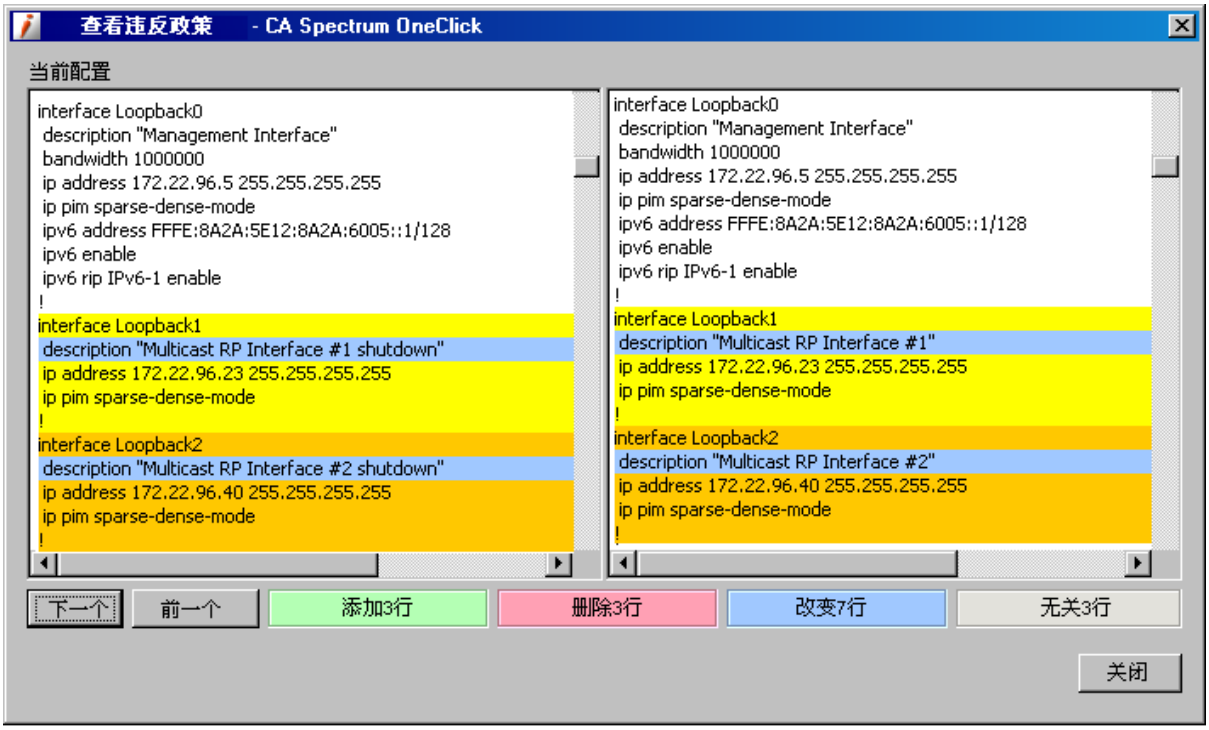
测试完成后，可以从测试对话框执行以下操作：

- 要查看策略违反，请单击“查看违反”。将出现一个显示违反的对话框。
  - 如果将指定的内容用于比较标准，则出现“查看违反块”对话框（如下图所示）。按颜色区分每个块，并突出显示违反行。在该示例中，以“description”开头且包含“shutdown”的行将识别为违反。使用“下一个”和“上一个”按钮，可以滚动浏览违反。



- 如果将其他配置用于比较标准，则出现“查看策略违反”对话框（如下图所示）。按颜色区分每个块，并突出显示差异。在该示例中，其中两个接口的说明内容与定义为参考的内容不匹配。使用“下一个”和“上一个”按钮，可以滚动浏览违反。

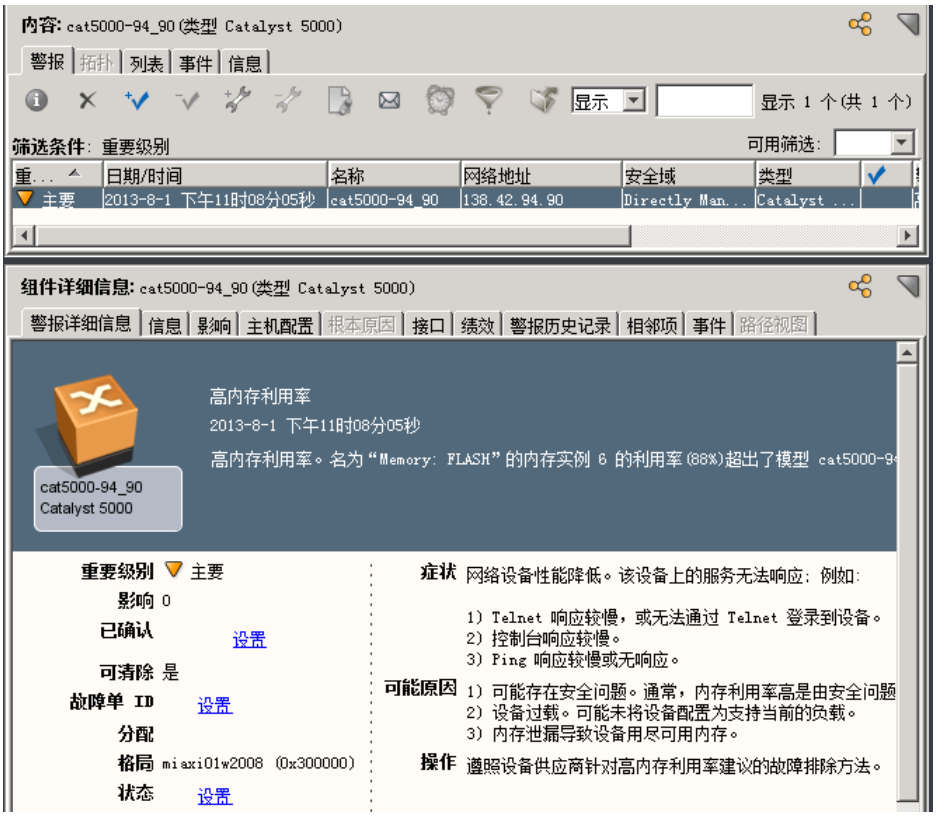
  重要说明！与参考配置进行比较时，请确保查看找到的每个差异，以免无意中执行不适用的更正操作。



- 要更正策略违反并进而使设备遵从策略，请单击“修复”以上传内容，如“修复更正操作”框所述。将创建并执行上传任务，该任务的结果将显示在“上传任务结果”对话框中。
- 如果对测试的结果感到满意，请选择“启用策略”选项，以基于该策略启动自动监控和警报生成；否则，可以单击“后退”并修改策略定义。如果单击“完成”，则将保存策略，但不启用它。

监控违反

启用策略后，它将监控捕获的配置，并将基于您指定的操作提醒您注意任何违反。策略违反生成的警报具有警报标题“已违反 NCM 策略”。下图显示了基于该示例策略生成的警报：



在警报详细信息中，可以单击“查看违反详细信息”，这将打开“修复违反的设备”对话框，如下所示：

在该对话框中，可以使用可用的按钮查看违反，或者如测试策略时所述修复非遵从设备。

注意：也可以从非遵从设备的“内容”面板中的“网络配置策略”表启动该对话框。有关详细信息，请参阅从策略表修复非遵从设备 (p. 130)。

附录 A： 支持的设备

此部分包含以下主题：

支持的 Cisco 设备 (p. 149)
支持的 Cisco 设备 (p. 170)
支持的 Cisco 设备 (p. 177)
支持的 Cisco CAT 设备 (p. 178)
支持的 Cisco NX OS 设备 (p. 181)
支持的 Enterasys 设备 (p. 181)
支持的 Enterasys/Riverstone SSR 设备 (p. 184)
支持的 Extreme 设备 (p. 186)
支持的 Foundry 设备 (p. 190)
支持的 Juniper 设备 (p. 200)
支持的 Lancom 设备 (p. 202)
支持的 Nortel Baystack 设备 (p. 202)
支持的 Nortel Passport 设备 (p. 203)

支持的 Cisco 设备

CA Spectrum Network Configuration Manager 支持以下 Cisco 设备。有关支持的 Catalyst 设备的列表，请参阅支持的 Cisco Catalyst 设备 (p. 170)。有关 PIX 防火墙设备的列表，请参阅支持的 Cisco PIX 防火墙设备 (p. 177)。

该表提供了示例。有关设备支持的最新信息，请访问 CA 设备认证数据库 (p. 15)。

当 Perl 脚本是与设备进行通信的唯一方式时，提供了脚本方法。

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
CiscoDSC9216K9	1.3.6.1.4.1.9.1.521	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco677i	1.3.6.1.4.1.9.1.363	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco741	1.3.6.1.4.1.9.1.94	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco742	1.3.6.1.4.1.9.1.95	*CISCO-CONFIG-COPY-MIB	是	**是	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
Cisco743	1.3.6.1.4.1.9.1.96	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco744	1.3.6.1.4.1.9.1.97	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco751	1.3.6.1.4.1.9.1.81	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco752	1.3.6.1.4.1.9.1.82	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco753	1.3.6.1.4.1.9.1.83	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco761	1.3.6.1.4.1.9.1.98	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco762	1.3.6.1.4.1.9.1.99	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco765	1.3.6.1.4.1.9.1.102	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco766	1.3.6.1.4.1.9.1.103	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco771	1.3.6.1.4.1.9.1.126	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco772	1.3.6.1.4.1.9.1.127	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco775	1.3.6.1.4.1.9.1.128	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco776	1.3.6.1.4.1.9.1.129	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco801	1.3.6.1.4.1.9.1.212	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco802	1.3.6.1.4.1.9.1.213	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco802J	1.3.6.1.4.1.9.1.295	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco803	1.3.6.1.4.1.9.1.214	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco804	1.3.6.1.4.1.9.1.215	*CISCO-CONFIG-COPY-MIB	是	**是	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
Cisco804J	1.3.6.1.4.1.9.1.296	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco805	1.3.6.1.4.1.9.1.245	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco806	1.3.6.1.4.1.9.1.384	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco811	1.3.6.1.4.1.9.1.395	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco813	1.3.6.1.4.1.9.1.396	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco826	1.3.6.1.4.1.9.1.322	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco826QuadV	1.3.6.1.4.1.9.1.321	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco827	1.3.6.1.4.1.9.1.284	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco827H	1.3.6.1.4.1.9.1.446	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco827QuadV	1.3.6.1.4.1.9.1.270	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco828	1.3.6.1.4.1.9.1.382	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco831	1.3.6.1.4.1.9.1.497	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco836	1.3.6.1.4.1.9.1.499	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco837	1.3.6.1.4.1.9.1.495	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco871	1.3.6.1.4.1.9.1.571	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco877	1.3.6.1.4.1.9.1.569	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco878	1.3.6.1.4.1.9.1.570	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco1000	1.3.6.1.4.1.9.1.40	*CISCO-CONFIG-COPY-MIB	是	**是	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
Cisco1003	1.3.6.1.4.1.9.1.41	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco1004	1.3.6.1.4.1.9.1.44	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco1005	1.3.6.1.4.1.9.1.49	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco1020	1.3.6.1.4.1.9.1.43	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco1401	1.3.6.1.4.1.9.1.206	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco1407	1.3.6.1.4.1.9.1.249	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco1417	1.3.6.1.4.1.9.1.250	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco1502	1.3.6.1.4.1.9.1.161	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco1503	1.3.6.1.4.1.9.1.160	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco1538M	1.3.6.1.4.1.9.1.224	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco1548M	1.3.6.1.4.1.9.1.225	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco1601	1.3.6.1.4.1.9.1.113	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco1602	1.3.6.1.4.1.9.1.114	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco1603	1.3.6.1.4.1.9.1.115	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco1604	1.3.6.1.4.1.9.1.116	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco1605	1.3.6.1.4.1.9.1.172	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco1701ADSLBRI	1.3.6.1.4.1.9.1.550	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco1710	1.3.6.1.4.1.9.1.200	*CISCO-CONFIG-COPY-MIB	是	**是	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
Cisco1711	1.3.6.1.4.1.9.1.538	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco1712	1.3.6.1.4.1.9.1.539	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco1720	1.3.6.1.4.1.9.1.201	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco1721	1.3.6.1.4.1.9.1.444	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco1750	1.3.6.1.4.1.9.1.216	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco1751	1.3.6.1.4.1.9.1.326	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco1760	1.3.6.1.4.1.9.1.416	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco1801	1.3.6.1.4.1.9.1.638	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco1811	1.3.6.1.4.1.9.1.641	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco1812	1.3.6.1.4.1.9.1.642	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco1841	1.3.6.1.4.1.9.1.620	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2000	1.3.6.1.4.1.9.1.10	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2102	1.3.6.1.4.1.9.1.15	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2202	1.3.6.1.4.1.9.1.16	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2500	1.3.6.1.4.1.9.1.13	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2501	1.3.6.1.4.1.9.1.17	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2502	1.3.6.1.4.1.9.1.18	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2503	1.3.6.1.4.1.9.1.19	*CISCO-CONFIG-COPY-MIB	是	**是	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
Cisco2504	1.3.6.1.4.1.9.1.20	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2505	1.3.6.1.4.1.9.1.21	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2506	1.3.6.1.4.1.9.1.22	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2507	1.3.6.1.4.1.9.1.23	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2508	1.3.6.1.4.1.9.1.24	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2509	1.3.6.1.4.1.9.1.25	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2501FRADFX	1.3.6.1.4.1.9.1.165	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2501LANFRADFX	1.3.6.1.4.1.9.1.166	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2502LANFRADFX	1.3.6.1.4.1.9.1.167	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2510	1.3.6.1.4.1.9.1.26	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2511	1.3.6.1.4.1.9.1.27	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2512	1.3.6.1.4.1.9.1.28	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2513	1.3.6.1.4.1.9.1.29	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2514	1.3.6.1.4.1.9.1.30	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2515	1.3.6.1.4.1.9.1.31	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2516	1.3.6.1.4.1.9.1.42	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2517	1.3.6.1.4.1.9.1.67	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2518	1.3.6.1.4.1.9.1.68	*CISCO-CONFIG-COPY-MIB	是	**是	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
Cisco2519	1.3.6.1.4.1.9.1.69	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2520	1.3.6.1.4.1.9.1.70	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2521	1.3.6.1.4.1.9.1.71	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2522	1.3.6.1.4.1.9.1.72	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2523	1.3.6.1.4.1.9.1.73	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2524	1.3.6.1.4.1.9.1.74	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2525	1.3.6.1.4.1.9.1.75	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2610	1.3.6.1.4.1.9.1.185	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2610M	1.3.6.1.4.1.9.1.418	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2610XM	1.3.6.1.4.1.9.1.466	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2611	1.3.6.1.4.1.9.1.186	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2611M	1.3.6.1.4.1.9.1.419	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2611XM	1.3.6.1.4.1.9.1.467	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2612	1.3.6.1.4.1.9.1.187	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2613	1.3.6.1.4.1.9.1.195	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2620	1.3.6.1.4.1.9.1.208	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2620XM	1.3.6.1.4.1.9.1.468	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2621	1.3.6.1.4.1.9.1.209	*CISCO-CONFIG-COPY-MIB	是	**是	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
Cisco2621XM	1.3.6.1.4.1.9.1.469	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2650	1.3.6.1.4.1.9.1.319	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2650XM	1.3.6.1.4.1.9.1.470	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2651	1.3.6.1.4.1.9.1.320	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2651XM	1.3.6.1.4.1.9.1.471	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2691	1.3.6.1.4.1.9.1.413	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2801	1.3.6.1.4.1.9.1.619	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2811	1.3.6.1.4.1.9.1.576	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2821	1.3.6.1.4.1.9.1.577	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco2851	1.3.6.1.4.1.9.1.578	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco3000	1.3.6.1.4.1.9.1.6	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco3101	1.3.6.1.4.1.9.1.32	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco3102	1.3.6.1.4.1.9.1.33	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco3103	1.3.6.1.4.1.9.1.34	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco3104	1.3.6.1.4.1.9.1.35	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco3202	1.3.6.1.4.1.9.1.36	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco3204	1.3.6.1.4.1.9.1.37	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco3220	1.3.6.1.4.1.9.1.553	*CISCO-CONFIG-COPY-MIB	是	**是	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
Cisco3250	1.3.6.1.4.1.9.1.479	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco3620	1.3.6.1.4.1.9.1.122	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco3640	1.3.6.1.4.1.9.1.110	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco3660	1.3.6.1.4.1.9.1.205	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco3661Ac	1.3.6.1.4.1.9.1.338	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco3661Dc	1.3.6.1.4.1.9.1.339	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco3662Ac	1.3.6.1.4.1.9.1.340	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco3662AcCo	1.3.6.1.4.1.9.1.342	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco3662Dc	1.3.6.1.4.1.9.1.341	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco3662DcCo	1.3.6.1.4.1.9.1.343	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco371098-HP001	1.3.6.1.4.1.9.1.625	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco371098-HP001	1.3.6.1.4.1.11.2.3.7.11.33.3.1.1	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco3725	1.3.6.1.4.1.9.1.414	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco3745	1.3.6.1.4.1.9.1.436	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco3825	1.3.6.1.4.1.9.1.543	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco3845	1.3.6.1.4.1.9.1.544	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco4000	1.3.6.1.4.1.9.1.7	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco4224	1.3.6.1.4.1.9.1.399	*CISCO-CONFIG-COPY-MIB	是	**是	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
Cisco4500	1.3.6.1.4.1.9.1.14	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco4700	1.3.6.1.4.1.9.1.50	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco6015	1.3.6.1.4.1.9.1.299	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco6100	1.3.6.1.4.1.9.1.251	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco6130	1.3.6.1.4.1.9.1.252	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco6160	1.3.6.1.4.1.9.1.297	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco6200	1.3.6.1.4.1.9.1.192	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco6260	1.3.6.1.4.1.9.1.253	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco6400	1.3.6.1.4.1.9.1.180	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco6400Nrp	1.3.6.1.4.1.9.1.211	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco6400UAC	1.3.6.1.4.1.9.1.464	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7000	1.3.6.1.4.1.9.1.8	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7010	1.3.6.1.4.1.9.1.12	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7120Ae3	1.3.6.1.4.1.9.1.263	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7120At3	1.3.6.1.4.1.9.1.262	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7120E3	1.3.6.1.4.1.9.1.261	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7120Quadt1	1.3.6.1.4.1.9.1.259	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7120Smi3	1.3.6.1.4.1.9.1.264	*CISCO-CONFIG-COPY-MIB	是	**是	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
Cisco7120T3	1.3.6.1.4.1.9.1.260	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7140Dualae3	1.3.6.1.4.1.9.1.268	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7140Dualat3	1.3.6.1.4.1.9.1.267	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7140Duale3	1.3.6.1.4.1.9.1.266	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7140Dualfe	1.3.6.1.4.1.9.1.277	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7140Dualmm3	1.3.6.1.4.1.9.1.269	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7140Dualt3	1.3.6.1.4.1.9.1.265	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7140Octt1	1.3.6.1.4.1.9.1.276	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7150Dualfe	1.3.6.1.4.1.9.1.355	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7150Dualt3	1.3.6.1.4.1.9.1.357	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7150Octt1	1.3.6.1.4.1.9.1.356	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7202	1.3.6.1.4.1.9.1.194	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7204	1.3.6.1.4.1.9.1.125	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7204VXR	1.3.6.1.4.1.9.1.223	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7206	1.3.6.1.4.1.9.1.108	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7206VXR	1.3.6.1.4.1.9.1.222	*CISCO-CONFIG-COPY-MIB	是	**是	是
UBR_7246	1.3.6.1.4.1.9.1.179	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7301	1.3.6.1.4.1.9.1.476	*CISCO-CONFIG-COPY-MIB	是	**是	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
Cisco7304	1.3.6.1.4.1.9.1.439	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7401ASR	1.3.6.1.4.1.9.1.403	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7401VXR	1.3.6.1.4.1.9.1.376	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7505	1.3.6.1.4.1.9.1.48	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7507z	1.3.6.1.4.1.9.1.288	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7506	1.3.6.1.4.1.9.1.47	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7507	1.3.6.1.4.1.9.1.45	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7507mx	1.3.6.1.4.1.9.1.290	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7513	1.3.6.1.4.1.9.1.46	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7513mx	1.3.6.1.4.1.9.1.291	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7513z	1.3.6.1.4.1.9.1.289	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7576	1.3.6.1.4.1.9.1.204	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7603	1.3.6.1.4.1.9.1.401	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7604	1.3.6.1.4.1.9.1.658	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7606	1.3.6.1.4.1.9.1.402	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7609	1.3.6.1.4.1.9.1.509	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco7613	1.3.6.1.4.1.9.1.528	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco9004	1.3.6.1.4.1.9.1.424	*CISCO-CONFIG-COPY-MIB	是	**是	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
Cisco10005	1.3.6.1.4.1.9.1.437	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco10008	1.3.6.1.4.1.9.1.438	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco10400	1.3.6.1.4.1.9.1.272	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco10720	1.3.6.1.4.1.9.1.397	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco12004	1.3.6.1.4.1.9.1.181	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco12006	1.3.6.1.4.1.9.1.590	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco12008	1.3.6.1.4.1.9.1.182	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco12010	1.3.6.1.4.1.9.1.348	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco12012	1.3.6.1.4.1.9.1.173	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco12016	1.3.6.1.4.1.9.1.273	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco12404	1.3.6.1.4.1.9.1.423	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco12406	1.3.6.1.4.1.9.1.388	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco12410	1.3.6.1.4.1.9.1.394	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco12416	1.3.6.1.4.1.9.1.385	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco3631Co	1.3.6.1.4.1.9.1.425	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoAGS+	1.3.6.1.4.1.9.1.11	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoAPEC	1.3.6.1.4.1.9.1.39	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoAPRC	1.3.6.1.4.1.9.1.38	*CISCO-CONFIG-COPY-MIB	是	**是	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
CiscoAS5200	1.3.6.1.4.1.9.1.109	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoAS5300	1.3.6.1.4.1.9.1.162	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoAS5350	1.3.6.1.4.1.9.1.313	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoAS5350XM	1.3.6.1.4.1.9.1.679	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoAS5400	1.3.6.1.4.1.9.1.274	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoAS5400XM	1.3.6.1.4.1.9.1.668	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoAS5800	1.3.6.1.4.1.9.1.188	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoAS5850	1.3.6.1.4.1.9.1.308	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoCacheEngine	1.3.6.1.4.1.9.1.240	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoCrs1Fabric	1.3.6.1.4.1.9.1.739	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoCRS16S	1.3.6.1.4.1.9.1.613	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoCrs18LineCard	1.3.6.1.4.1.9.1.738	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoCRS8S	1.3.6.1.4.1.9.1.643	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoCS500	1.3.6.1.4.1.9.1.9	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoFastHubBMMFX	1.3.6.1.4.1.9.1.178	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoFastHubBMMTX	1.3.6.1.4.1.9.1.177	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoFastHub216T	1.3.6.1.4.1.9.1.169	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoGS	1.3.6.1.4.1.9.1.1	*CISCO-CONFIG-COPY-MIB	是	**是	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
CiscoIGESM	1.3.6.1.4.1.9.1.592	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoIGS	1.3.6.1.4.1.9.1.5	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoLocalDirector	1.3.6.1.4.1.9.1.244	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco MC3810	1.3.6.1.4.1.9.1.286	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cisco MC3810	1.3.6.1.4.1.9.1.157	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoME6340ACA	1.3.6.1.4.1.9.1.713	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoME6340DCA	1.3.6.1.4.1.9.1.714	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoME6340DCB	1.3.6.1.4.1.9.1.715	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoMicroWebServer2	1.3.6.1.4.1.9.1.176	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoMWR1900	1.3.6.1.4.1.9.1.398	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoMWR1941DC	1.3.6.1.4.1.9.1.520	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoOlympus	1.3.6.1.4.1.9.1.358	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoOpticalRegenerator	1.3.6.1.4.1.9.1.254	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro316C	1.3.6.1.4.1.9.1.148	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro316T	1.3.6.1.4.1.9.1.147	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro741	1.3.6.1.4.1.9.1.84	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro742	1.3.6.1.4.1.9.1.85	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro743	1.3.6.1.4.1.9.1.86	*CISCO-CONFIG-COPY-MIB	是	**是	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
CiscoPro744	1.3.6.1.4.1.9.1.87	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro751	1.3.6.1.4.1.9.1.76	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro752	1.3.6.1.4.1.9.1.77	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro753	1.3.6.1.4.1.9.1.78	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro761	1.3.6.1.4.1.9.1.88	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro762	1.3.6.1.4.1.9.1.89	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro765	1.3.6.1.4.1.9.1.92	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro766	1.3.6.1.4.1.9.1.93	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro1003	1.3.6.1.4.1.9.1.51	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro1004	1.3.6.1.4.1.9.1.52	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro1005	1.3.6.1.4.1.9.1.53	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro1020	1.3.6.1.4.1.9.1.54	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro1601	1.3.6.1.4.1.9.1.117	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro1602	1.3.6.1.4.1.9.1.118	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro1603	1.3.6.1.4.1.9.1.119	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro1604	1.3.6.1.4.1.9.1.120	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro2500PCE	1.3.6.1.4.1.9.1.55	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro2501	1.3.6.1.4.1.9.1.56	*CISCO-CONFIG-COPY-MIB	是	**是	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
CiscoPro2502	1.3.6.1.4.1.9.1.130	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro2503	1.3.6.1.4.1.9.1.57	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro2504	1.3.6.1.4.1.9.1.131	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro2505	1.3.6.1.4.1.9.1.58	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro2506	1.3.6.1.4.1.9.1.132	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro2507	1.3.6.1.4.1.9.1.59	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro2508	1.3.6.1.4.1.9.1.133	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro2509	1.3.6.1.4.1.9.1.60	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro2510	1.3.6.1.4.1.9.1.134	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro2511	1.3.6.1.4.1.9.1.61	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro2512	1.3.6.1.4.1.9.1.135	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro2513	1.3.6.1.4.1.9.1.136	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro2514	1.3.6.1.4.1.9.1.62	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro2515	1.3.6.1.4.1.9.1.137	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro2516	1.3.6.1.4.1.9.1.63	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro2517	1.3.6.1.4.1.9.1.138	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro2518	1.3.6.1.4.1.9.1.139	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro2519	1.3.6.1.4.1.9.1.64	*CISCO-CONFIG-COPY-MIB	是	**是	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
CiscoPro2520	1.3.6.1.4.1.9.1.104	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro2521	1.3.6.1.4.1.9.1.65	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro2522	1.3.6.1.4.1.9.1.105	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro2523	1.3.6.1.4.1.9.1.140	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro2524	1.3.6.1.4.1.9.1.106	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro2525	1.3.6.1.4.1.9.1.141	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro3116	1.3.6.1.4.1.9.1.149	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro3620	1.3.6.1.4.1.9.1.123	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro3640	1.3.6.1.4.1.9.1.124	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro4500	1.3.6.1.4.1.9.1.66	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoPro4700	1.3.6.1.4.1.9.1.142	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoProtocolTranslator	1.3.6.1.4.1.9.1.4	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoRPM	1.3.6.1.4.1.9.1.199	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoRPMPR	1.3.6.1.4.1.9.1.457	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoRpmXf	1.3.6.1.4.1.9.1.440	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoSC3640	1.3.6.1.4.1.9.1.189	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoSN5420	1.3.6.1.4.1.9.1.407	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoSN5428	1.3.6.1.4.1.9.1.475	*CISCO-CONFIG-COPY-MIB	是	**是	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
CiscoSOHO76	1.3.6.1.4.1.9.1.354	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoSOHO91	1.3.6.1.4.1.9.1.498	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoSOHO97	1.3.6.1.4.1.9.1.496	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoSOHO77	1.3.6.1.4.1.9.1.353	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoSOHO96	1.3.6.1.4.1.9.1.500	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoTrouter	1.3.6.1.4.1.9.1.3	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoTS	1.3.6.1.4.1.9.1.2	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoWS3020Hpq	1.3.6.1.4.1.9.1.748	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoWS3030Del	1.3.6.1.4.1.9.1.749	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoWSC3750G-24PS	1.3.6.1.4.1.9.1.747	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoWSC6504E	1.3.6.1.4.1.9.1.657	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoWSC6509neba	1.3.6.1.4.1.9.1.534	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoWSX3011	1.3.6.1.4.1.9.1.112	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoWSX5302	1.3.6.1.4.1.9.1.168	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoWSX6302Msm	1.3.6.1.4.1.9.1.256	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoURM	1.3.6.1.4.1.9.1.373	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoURM2FE	1.3.6.1.4.1.9.1.374	*CISCO-CONFIG-COPY-MIB	是	**是	是
CiscoURM2FE2V	1.3.6.1.4.1.9.1.375	*CISCO-CONFIG-COPY-MIB	是	**是	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
AP 1130	1.3.6.1.4.1.9.1.618	*CISCO-CONFIG-COPY-MIB	是	**是	是
LS_1010	1.3.6.1.4.1.9.1.107	*CISCO-CONFIG-COPY-MIB	是	**是	是
LS_1015	1.3.6.1.4.1.9.1.164	*CISCO-CONFIG-COPY-MIB	是	**是	是
UBR_7223	1.3.6.1.4.1.9.1.210	*CISCO-CONFIG-COPY-MIB	是	**是	是
UBR_7246VXR	1.3.6.1.4.1.9.1.271	*CISCO-CONFIG-COPY-MIB	是	**是	是
UBR_904	1.3.6.1.4.1.9.1.191	*CISCO-CONFIG-COPY-MIB	是	**是	是
UBR_924	1.3.6.1.4.1.9.1.255	*CISCO-CONFIG-COPY-MIB	是	**是	是
UBR_912C	1.3.6.1.4.1.9.1.292	*CISCO-CONFIG-COPY-MIB	是	**是	是
UBR_912S	1.3.6.1.4.1.9.1.293	*CISCO-CONFIG-COPY-MIB	是	**是	是
UBR_914	1.3.6.1.4.1.9.1.294	*CISCO-CONFIG-COPY-MIB	是	**是	是
UBR_925	1.3.6.1.4.1.9.1.316	*CISCO-CONFIG-COPY-MIB	是	**是	是
UBR_10012	1.3.6.1.4.1.9.1.317	*CISCO-CONFIG-COPY-MIB	是	**是	是
UBR_7111	1.3.6.1.4.1.9.1.344	*CISCO-CONFIG-COPY-MIB	是	**是	是
UBR_7111E	1.3.6.1.4.1.9.1.345	*CISCO-CONFIG-COPY-MIB	是	**是	是
UBR_7114	1.3.6.1.4.1.9.1.346	*CISCO-CONFIG-COPY-MIB	是	**是	是
UBR_7114E	1.3.6.1.4.1.9.1.347	*CISCO-CONFIG-COPY-MIB	是	**是	是
UBR_905	1.3.6.1.4.1.9.1.351	*CISCO-CONFIG-COPY-MIB	是	**是	是
350 AP	1.3.6.1.4.1.9.1.552	*CISCO-CONFIG-COPY-MIB	是	**是	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
1100 AP	1.3.6.1.4.1.9.1.507	*CISCO-CONFIG-COPY-MIB	是	**是	是
1210/1230 AP	1.3.6.1.4.1.9.1.525	*CISCO-CONFIG-COPY-MIB	是	**是	是
1240 AP	1.3.6.1.4.1.9.1.685	*CISCO-CONFIG-COPY-MIB	是	**是	是
1400 AP	1.3.6.1.4.1.9.1.533	*CISCO-CONFIG-COPY-MIB	是	**是	是
1300 AP	1.3.6.1.4.1.9.1.565	*CISCO-CONFIG-COPY-MIB	是	**是	是
PIX Firewall	1.3.6.1.4.1.9.1.227	否	否	否	Telnet
PIX 506 Firewall	1.3.6.1.4.1.9.1.389	否	否	否	Telnet
PIX 515 Firewall	1.3.6.1.4.1.9.1.390	否	否	否	Telnet
PIX 520 Firewall	1.3.6.1.4.1.9.1.391	否	否	否	Telnet
PIX 525 Firewall	1.3.6.1.4.1.9.1.392	否	否	否	Telnet
PIX 535 Firewall	1.3.6.1.4.1.9.1.393	否	否	否	Telnet
PIX 501 Firewall	1.3.6.1.4.1.9.1.417	否	否	否	Telnet
PIX 515E Firewall	1.3.6.1.4.1.9.1.451	否	否	否	Telnet
PIX 506E Firewall	1.3.6.1.4.1.9.1.450	否	否	否	Telnet
cat6500FirewallSm	1.3.6.1.4.1.9.1.522	否	否	否	Telnet
PIX Firewall 安全模块	1.3.6.1.4.1.9.1.674	否	否	否	Telnet
PIX 535sc Firewall	1.3.6.1.4.1.9.1.675	否	否	否	Telnet
PIX 525sc Firewall	1.3.6.1.4.1.9.1.676	否	否	否	Telnet
PIX 515Esc Firewall	1.3.6.1.4.1.9.1.677	否	否	否	Telnet
PIX 515sc Firewall	1.3.6.1.4.1.9.1.678	否	否	否	Telnet

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
PIX Firewall 系统模块	1.3.6.1.4.1.9.1.767	否	否	否	Telnet
PIX 515sy Firewall	1.3.6.1.4.1.9.1.768	否	否	否	Telnet
PIX 515Esy Firewall	1.3.6.1.4.1.9.1.769	否	否	否	Telnet
PIX 525sy Firewall	1.3.6.1.4.1.9.1.770	否	否	否	Telnet
PIX 535sy Firewall	1.3.6.1.4.1.9.1.771	否	否	否	Telnet

* IOS < 12.0 = OLD-CISCO-SYSTEM-MIB

** IOS > 12.2(18)，带有功能“K9”

支持的 Cisco 设备

CA Spectrum Network Configuration Manager 支持以下 Cisco Catalyst 设备。有关其他支持的 Cisco 设备的列表，请参阅支持的 Cisco 设备 (p. 149)。有关 PIX 防火墙设备的列表，请参阅支持的 Cisco PIX 防火墙设备 (p. 177)。

该表提供了示例。有关设备支持的最新信息，请访问 CA 设备认证数据库 (p. 15)。

当 Perl 脚本是与设备进行通信的唯一方式时，提供了脚本方法。

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
Cat116T	1.3.6.1.4.1.9.1.150	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat116C	1.3.6.1.4.1.9.1.151	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat1116	1.3.6.1.4.1.9.1.152	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat1912C	1.3.6.1.4.1.9.1.175	*CISCO-CONFIG-COPY-MIB	是	**是	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
Cat2924XL	1.3.6.1.4.1.9.1.183	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat2924CXL	1.3.6.1.4.1.9.1.184	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat2924XLv	1.3.6.1.4.1.9.1.217	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat2640-48TT	1.3.6.1.4.1.9.1.717	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat2948gL3	1.3.6.1.4.1.9.1.275	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat2948gL3Dc	1.3.6.1.4.1.9.1.386	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat2960-24TC	1.3.6.1.4.1.9.1.694	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat2960-24TT	1.3.6.1.4.1.9.1.716	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat2960G-24TC	1.3.6.1.4.1.9.1.696	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat2960-48TC	1.3.6.1.4.1.9.1.695	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat297024	1.3.6.1.4.1.9.1.527	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat297024TS	1.3.6.1.4.1.9.1.561	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat2908xl	1.3.6.1.4.1.9.1.170	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat2912LREXL	1.3.6.1.4.1.9.1.370	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat2912MfXL	1.3.6.1.4.1.9.1.221	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat2912XL	1.3.6.1.4.1.9.1.219	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat2916mxl	1.3.6.1.4.1.9.1.171	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat2924CXLv	1.3.6.1.4.1.9.1.218	*CISCO-CONFIG-COPY-MIB	是	**是	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
Cat2924MXL	1.3.6.1.4.1.9.1.220	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat295012	1.3.6.1.4.1.9.1.323	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat295024	1.3.6.1.4.1.9.1.324	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat295024C	1.3.6.1.4.1.9.1.325	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat2950t24	1.3.6.1.4.1.9.1.359	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat2924LREXL	1.3.6.1.4.1.9.1.369	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat295012G	1.3.6.1.4.1.9.1.427	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat295024G	1.3.6.1.4.1.9.1.428	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat295048G	1.3.6.1.4.1.9.1.429	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat_3500	1.3.6.1.4.1.9.1.111	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat_3508GXL	1.3.6.1.4.1.9.1.246	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat_3512XL	1.3.6.1.4.1.9.1.247	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat_3524XL	1.3.6.1.4.1.9.1.248	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat_3524tXLEn	1.3.6.1.4.1.9.1.287	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat_3548XL	1.3.6.1.4.1.9.1.278	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat355012G	1.3.6.1.4.1.9.1.431	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat355012T	1.3.6.1.4.1.9.1.368	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat355024	1.3.6.1.4.1.9.1.366	*CISCO-CONFIG-COPY-MIB	是	**是	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
Cat355048	1.3.6.1.4.1.9.1.367	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat355024Dc	1.3.6.1.4.1.9.1.452	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat355024Mmf	1.3.6.1.4.1.9.1.453	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat355024PWR	1.3.6.1.4.1.9.1.485	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat3560_24PS	1.3.6.1.4.1.9.1.563	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat3560G-24PS	1.3.6.1.4.1.9.1.614	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat3560-24TS	1.3.6.1.4.1.9.1.633	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat3560G-24TS	1.3.6.1.4.1.9.1.615	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat3560_48PS	1.3.6.1.4.1.9.1.564	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat3560G-48PS	1.3.6.1.4.1.9.1.616	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat3560-48TS	1.3.6.1.4.1.9.1.634	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat3560G-48TS	1.3.6.1.4.1.9.1.617	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat37xxStack	1.3.6.1.4.1.9.1.516	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat3750Ge12Sfp	1.3.6.1.4.1.9.1.530	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat3750_24ME	1.3.6.1.4.1.9.1.574	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat3750G16TD	1.3.6.1.4.1.9.1.591	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat375024	1.3.6.1.4.1.9.1.511	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat375024T	1.3.6.1.4.1.9.1.514	*CISCO-CONFIG-COPY-MIB	是	**是	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
Cat375024TS	1.3.6.1.4.1.9.1.513	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat375048	1.3.6.1.4.1.9.1.512	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat4kGateway	1.3.6.1.4.1.9.1.318	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat4000NAM	1.3.6.1.4.1.9.1.575	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat4006	1.3.6.1.4.1.9.1.448	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat4503	1.3.6.1.4.1.9.1.503	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat4510	1.3.6.1.4.1.9.1.537	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat4232L3	1.3.6.1.4.1.9.1.300	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat4506	1.3.6.1.4.1.9.1.502	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat4507	1.3.6.1.4.1.9.1.501	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat4840gL3	1.3.6.1.4.1.9.1.312	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat4908gL3	1.3.6.1.4.1.9.1.298	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat4908gL3Dc	1.3.6.1.4.1.9.1.387	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat4948	1.3.6.1.4.1.9.1.626	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat494810GE	1.3.6.1.4.1.9.1.659	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat5kRsfc	1.3.6.1.4.1.9.1.257	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat6kSup720	1.3.6.1.4.1.9.1.557	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat6kGateway	1.3.6.1.4.1.9.1.573	*CISCO-CONFIG-COPY-MIB	是	**是	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
Cat6503	1.3.6.1.4.1.9.1.449	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat6513	1.3.6.1.4.1.9.1.400	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat6000	1.3.6.1.4.1.9.1.241	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat6006	1.3.6.1.4.1.9.1.280	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat6009	1.3.6.1.4.1.9.1.281	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat6506	1.3.6.1.4.1.9.1.282	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat6509	1.3.6.1.4.1.9.1.283	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat6kMsfc	1.3.6.1.4.1.9.1.258	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat6kMsfc2	1.3.6.1.4.1.9.1.301	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat6509Sp	1.3.6.1.4.1.9.1.310	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat8510_CSR	1.3.6.1.4.1.9.1.190	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat8510_MSR	1.3.6.1.4.1.9.1.230	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat8515_CSR	1.3.6.1.4.1.9.1.196	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat8515_MSR	1.3.6.1.4.1.9.1.231	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat8540_CSR	1.3.6.1.4.1.9.1.203	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat8540_MSR	1.3.6.1.4.1.9.1.202	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat9006	1.3.6.1.4.1.9.1.197	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat9009	1.3.6.1.4.1.9.1.198	*CISCO-CONFIG-COPY-MIB	是	**是	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
Cat295024GDC	1.3.6.1.4.1.9.1.472	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat295024S	1.3.6.1.4.1.9.1.430	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat295024SX	1.3.6.1.4.1.9.1.480	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat295024LREG	1.3.6.1.4.1.9.1.484	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat295024LRESt	1.3.6.1.4.1.9.1.482	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat29508LRESt	1.3.6.1.4.1.9.1.483	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat2955C12	1.3.6.1.4.1.9.1.489	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat2955S12	1.3.6.1.4.1.9.1.508	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat2955T12	1.3.6.1.4.1.9.1.488	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat29408TF	1.3.6.1.4.1.9.1.542	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat29408TT	1.3.6.1.4.1.9.1.540	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat295048SX	1.3.6.1.4.1.9.1.560	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat295048T	1.3.6.1.4.1.9.1.559	*CISCO-CONFIG-COPY-MIB	是	**是	是
Cat2950St24LRE997	1.3.6.1.4.1.9.1.551	*CISCO-CONFIG-COPY-MIB	是	**是	是
CatExpress500-24LC	1.3.6.1.4.1.9.1.725	*CISCO-CONFIG-COPY-MIB	是	**是	是
CatExpress500-12TC	1.3.6.1.4.1.9.1.727	*CISCO-CONFIG-COPY-MIB	是	**是	是
CatExpress500-24PC	1.3.6.1.4.1.9.1.726	*CISCO-CONFIG-COPY-MIB	是	**是	是
CatExpress500-24TT	1.3.6.1.4.1.9.1.724	*CISCO-CONFIG-COPY-MIB	是	**是	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
CatWsCBS3040FSC	1.3.6.1.4.1.9.1.784	*CISCO-CONFIG-COPY-MIB	是	**是	是

* IOS < 12.0 = OLD-CISCO-SYSTEM-MIB

** IOS > 12.2(18)，带有功能“K9”

支持的 Cisco 设备

CA Spectrum Network Configuration Manager 支持以下 Cisco 设备。有关支持的 Catalyst 设备的列表，请参阅“支持的 Cisco Catalyst 设备”。

该表提供了示例。有关设备支持的最新信息，请访问 CA 设备认证数据库 (p. 15)。

当 Perl 脚本是与设备进行通信的唯一方式时，提供了脚本方法。

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
PIX Firewall	1.3.6.1.4.1.9.1.227	否	否	否	Telnet
PIX 506 Firewall	1.3.6.1.4.1.9.1.389	否	否	否	Telnet
PIX 515 Firewall	1.3.6.1.4.1.9.1.390	否	否	否	Telnet
PIX 520 Firewall	1.3.6.1.4.1.9.1.391	否	否	否	Telnet
PIX 525 Firewall	1.3.6.1.4.1.9.1.392	否	否	否	Telnet
PIX 535 Firewall	1.3.6.1.4.1.9.1.393	否	否	否	Telnet
PIX 501 Firewall	1.3.6.1.4.1.9.1.417	否	否	否	Telnet
PIX 515E Firewall	1.3.6.1.4.1.9.1.451	否	否	否	Telnet
PIX 506E Firewall	1.3.6.1.4.1.9.1.450	否	否	否	Telnet
cat6500FirewallSm	1.3.6.1.4.1.9.1.522	否	否	否	Telnet
PIX Firewall 安全模块	1.3.6.1.4.1.9.1.674	否	否	否	Telnet

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
PIX 535sc Firewall	1.3.6.1.4.1.9.1.675	否	否	否	Telnet
PIX 525sc Firewall	1.3.6.1.4.1.9.1.676	否	否	否	Telnet
PIX 515Esc Firewall	1.3.6.1.4.1.9.1.677	否	否	否	Telnet
PIX 515sc Firewall	1.3.6.1.4.1.9.1.678	否	否	否	Telnet
PIX Firewall 系统模块	1.3.6.1.4.1.9.1.767	否	否	否	Telnet
PIX 515sy Firewall	1.3.6.1.4.1.9.1.768	否	否	否	Telnet
PIX 515Esy Firewall	1.3.6.1.4.1.9.1.769	否	否	否	Telnet
PIX 525sy Firewall	1.3.6.1.4.1.9.1.770	否	否	否	Telnet
PIX 535sy Firewall	1.3.6.1.4.1.9.1.771	否	否	否	Telnet

* IOS < 12.0 = OLD-CISCO-SYSTEM-MIB

** IOS > 12.2(18)，带有功能“K9”

支持的 Cisco CAT 设备

下表列出了 CA Spectrum Network Configuration Manager 支持的 Cisco CAT 设备。该表提供了示例。有关设备支持的最新信息，请访问 CA 设备认证数据库 (p. 15)。

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
Cat2926	1.3.6.1.4.1.9.5.35	CISCO-CONFIG-COPY-MIB*	否	否	是
Cat_2948G	1.3.6.1.4.1.9.5.42	CISCO-CONFIG-COPY-MIB*	否	否	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
Cat2948ggetx	1.3.6.1.4.1.9.5.62	CISCO-CONFIG-COPY-MIB*	否	否	是
Cat2980ga	1.3.6.1.4.1.9.5.51	CISCO-CONFIG-COPY-MIB*	否	否	是
Cat_2980GSW	1.3.6.1.4.1.9.5.49	CISCO-CONFIG-COPY-MIB*	否	否	是
Cat_4003	1.3.6.1.4.1.9.5.40	CISCO-CONFIG-COPY-MIB*	否	否	是
Cat_4006	1.3.6.1.4.1.9.5.46	CISCO-CONFIG-COPY-MIB*	否	否	是
Cat4503	1.3.6.1.4.1.9.5.58	CISCO-CONFIG-COPY-MIB*	否	否	是
Cat_4506	1.3.6.1.4.1.9.5.59	CISCO-CONFIG-COPY-MIB*	否	否	是
Cat4912	1.3.6.1.4.1.9.5.41	CISCO-CONFIG-COPY-MIB*	否	否	是
Cat6knam	1.3.6.1.4.1.9.5.48	CISCO-CONFIG-COPY-MIB*	否	否	是
Cat6503	1.3.6.1.4.1.9.5.56	CISCO-CONFIG-COPY-MIB*	否	否	是
Cat6509neba	1.3.6.1.4.1.9.5.61	CISCO-CONFIG-COPY-MIB*	否	否	是
Cat7603	1.3.6.1.4.1.9.5.53	CISCO-CONFIG-COPY-MIB*	否	否	是
Cat7604	1.3.6.1.4.1.9.5.63	CISCO-CONFIG-COPY-MIB*	否	否	是
Cat7606	1.3.6.1.4.1.9.5.54	CISCO-CONFIG-COPY-MIB*	否	否	是
Cat7609	1.3.6.1.4.1.9.5.55	CISCO-CONFIG-COPY-MIB*	否	否	是
Cat7613	1.3.6.1.4.1.9.5.60	CISCO-CONFIG-COPY-MIB*	否	否	是
CiscoWSC6504E	1.3.6.1.4.1.9.5.64	CISCO-CONFIG-COPY-MIB*	否	否	是
HubCat1400	1.3.6.1.4.1.9.5.6	CISCO-CONFIG-COPY-MIB*	否	否	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
HubCat5000	1.3.6.1.4.1.9.5.7	CISCO-CONFIG-COPY-MIB*	否	否	是
HubCat5002	1.3.6.1.4.1.9.5.29	CISCO-CONFIG-COPY-MIB*	否	否	是
HubCat5500	1.3.6.1.4.1.9.5.17	CISCO-CONFIG-COPY-MIB*	否	否	是
HubCat5505	1.3.6.1.4.1.9.5.34	CISCO-CONFIG-COPY-MIB*	否	否	是
HubCat5509	1.3.6.1.4.1.9.5.36	CISCO-CONFIG-COPY-MIB*	否	否	是
SwCat1200	1.3.6.1.4.1.9.5.5	CISCO-CONFIG-COPY-MIB*	否	否	是
WS-C6006	1.3.6.1.4.1.9.5.38	CISCO-CONFIG-COPY-MIB*	否	否	是
WS-C6009	1.3.6.1.4.1.9.5.39	CISCO-CONFIG-COPY-MIB*	否	否	是
WS-C6506	1.3.6.1.4.1.9.5.45	CISCO-CONFIG-COPY-MIB*	否	否	是
WS-C6509	1.3.6.1.4.1.9.5.44	CISCO-CONFIG-COPY-MIB*	否	否	是
WS-C6509neb	1.3.6.1.4.1.9.5.47	CISCO-CONFIG-COPY-MIB*	否	否	是
WS-C6513	1.3.6.1.4.1.9.5.50	CISCO-CONFIG-COPY-MIB*	否	否	是

* CATOS < 8.4 = CISCO-STACK-MIB

支持的 Cisco NX OS 设备

下表列出了 CA Spectrum Network Configuration Manager 支持的 Cisco NX OS 设备。

注意：通过利用 Net::SSH::Expect 模块的脚本支持 Cisco NX OS 设备。要为 Cisco NX OS 设备提供即用型支持，必须使用这些模块设置 Perl 区域。

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
Cisco Nexus 1000V VSM	1.3.6.1.4.1.9.12.3.1.3.840	否	否	否	是
Cisco Nexus 2000	1.3.6.1.4.1.9.12.3.1.3.820	否	否	否	是
Cisco Nexus 5000	1.3.6.1.4.1.9.12.3.1.3.719	否	否	否	是
Cisco Nexus 7000	1.3.6.1.4.1.9.12.3.1.3.612	否	否	否	是

支持的 Enterasys 设备

下表列出了 CA Spectrum Network Configuration Manager 支持的 Enterasys 设备。该表提供了示例。有关设备支持的最新信息，请访问 CA 设备认证数据库 (p. 15)。

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
1G582-09	1.3.6.1.4.1.5624.2.1.35	ENTERASYS-CONFIG-MAN-MIB	否	否	是
1G694-13	1.3.6.1.4.1.5624.2.1.36	ENTERASYS-CONFIG-MAN-MIB	否	否	是
1H582-25	1.3.6.1.4.1.5624.2.1.59	ENTERASYS-CONFIG-MAN-MIB	否	否	是
1H582-51	1.3.6.1.4.1.5624.2.1.34	ENTERASYS-CONFIG-MAN-MIB	否	否	是
1G587-09	1.3.6.1.4.1.5624.2.1.60	ENTERASYS-CONFIG-MAN-MIB	否	否	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
Matrix N	1.3.6.1.4.1.5624.2.1.51	ENTERASYS-CONFIG-MAN-MIB	否	否	是
Matrix N1	1.3.6.1.4.1.5624.2.1.83	ENTERASYS-CONFIG-MAN-MIB	否	否	是
Matrix N3	1.3.6.1.4.1.5624.2.1.53	ENTERASYS-CONFIG-MAN-MIB	否	否	是
Matrix N5	1.3.6.1.4.1.5624.2.1.79	ENTERASYS-CONFIG-MAN-MIB	否	否	是
Matrix N7	1.3.6.1.4.1.5624.2.1.52	ENTERASYS-CONFIG-MAN-MIB	否	否	是
Matrix N 路由器	1.3.6.1.4.1.5624.2.1.70	ENTERASYS-CONFIG-MAN-MIB	否	否	是
Matrix N 单机版	1.3.6.1.4.1.5624.2.1.77	ENTERASYS-CONFIG-MAN-MIB	否	否	是
SecureStack A2H124-24	1.3.6.1.4.1.5624.2.1.87	ENTERASYS-CONFIG-MAN-MIB	否	否	是
SecureStack A2H124-24FX	1.3.6.1.4.1.5624.2.1.91	ENTERASYS-CONFIG-MAN-MIB	否	否	是
SecureStack A2H124-24P	1.3.6.1.4.1.5624.2.1.88	ENTERASYS-CONFIG-MAN-MIB	否	否	是
SecureStack A2H124-48	1.3.6.1.4.1.5624.2.1.89	ENTERASYS-CONFIG-MAN-MIB	否	否	是
SecureStack A2H124-48P	1.3.6.1.4.1.5624.2.1.90	ENTERASYS-CONFIG-MAN-MIB	否	否	是
SecureStack A2H254-16	1.3.6.1.4.1.5624.2.1.95	ENTERASYS-CONFIG-MAN-MIB	否	否	是
SecureStack B2G124-24	1.3.6.1.4.1.5624.2.2.314	ENTERASYS-CONFIG-MAN-MIB	否	否	是
SecureStack B2G124-48	1.3.6.1.4.1.5624.2.2.315	ENTERASYS-CONFIG-MAN-MIB	否	否	是
SecureStack B2G124-48P	1.3.6.1.4.1.5624.2.2.316	ENTERASYS-CONFIG-MAN-MIB	否	否	是
SecureStack B2H124-48	1.3.6.1.4.1.5624.2.2.317	ENTERASYS-CONFIG-MAN-MIB	否	否	是
SecureStack B2H124-48P	1.3.6.1.4.1.5624.2.2.318	ENTERASYS-CONFIG-MAN-MIB	否	否	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
SecureStack B3G124-24	1.3.6.1.4.1.5624.2.1.100	ENTERASYS-CONFIG-MAN-MIB	否	否	是
SecureStack B3G124-24P	1.3.6.1.4.1.5624.2.1.101	ENTERASYS-CONFIG-MAN-MIB	否	否	是
SecureStack B3G124-48	1.3.6.1.4.1.5624.2.1.102	ENTERASYS-CONFIG-MAN-MIB	否	否	是
SecureStack B3G124-48P	1.3.6.1.4.1.5624.2.1.103	ENTERASYS-CONFIG-MAN-MIB	否	否	是
SecureStack C2G124-24	1.3.6.1.4.1.5624.2.2.283	ENTERASYS-CONFIG-MAN-MIB	否	否	是
SecureStack C2G124-48	1.3.6.1.4.1.5624.2.2.284	ENTERASYS-CONFIG-MAN-MIB	否	否	是
SecureStack C2G124-48P	1.3.6.1.4.1.5624.2.2.287	ENTERASYS-CONFIG-MAN-MIB	否	否	是
SecureStack C2G134-24P	1.3.6.1.4.1.5624.2.2.350	ENTERASYS-CONFIG-MAN-MIB	否	否	是
SecureStack C2G170-24	1.3.6.1.4.1.5624.2.2.360	ENTERASYS-CONFIG-MAN-MIB	否	否	是
SecureStack C2H124-48	1.3.6.1.4.1.5624.2.2.220	ENTERASYS-CONFIG-MAN-MIB	否	否	是
SecureStack C2H124-48P	1.3.6.1.4.1.5624.2.2.286	ENTERASYS-CONFIG-MAN-MIB	否	否	是
SecureStack C2K122-24	1.3.6.1.4.1.5624.2.2.285	ENTERASYS-CONFIG-MAN-MIB	否	否	是
SecureStack C3G124-24	1.3.6.1.4.1.5624.2.1.96	ENTERASYS-CONFIG-MAN-MIB	否	否	是
SecureStack C3G124-24P	1.3.6.1.4.1.5624.2.1.97	ENTERASYS-CONFIG-MAN-MIB	否	否	是
SecureStack C3G124-48	1.3.6.1.4.1.5624.2.1.98	ENTERASYS-CONFIG-MAN-MIB	否	否	是
SecureStack C3G124-48P	1.3.6.1.4.1.5624.2.1.99	ENTERASYS-CONFIG-MAN-MIB	否	否	是
XSR-1805	1.3.6.1.4.1.5624.2.1.32	ENTERASYS-CONFIG-MAN-MIB	否	否	是
XSR-1850	1.3.6.1.4.1.5624.2.1.45	ENTERASYS-CONFIG-MAN-MIB	否	否	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
XSR-1800	1.3.6.1.4.1.5624.2.1	ENTERASYS-CONFIG-MAN-MIB	否	否	是

支持的 Enterasys/Riverstone SSR 设备

下表列出了 CA Spectrum Network Configuration Manager 支持的 Enterasys/Riverstone SSR 设备。该表提供了示例。有关设备支持的最新信息，请访问 CA 设备认证数据库 (p. 15)。

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
DEC 8000	1.3.6.1.4.1.36.2.15.30.1	CTRON-SSR-CONFIG-MIB	否	否	是
DEC 8600	1.3.6.1.4.1.36.2.15.30.2	CTRON-SSR-CONFIG-MIB	否	否	是
DEC 2000	1.3.6.1.4.1.36.2.15.30.3	CTRON-SSR-CONFIG-MIB	否	否	是
OLI-8000	1.3.6.1.4.1.285.9.25	CTRON-SSR-CONFIG-MIB	否	否	是
OLI-8600	1.3.6.1.4.1.285.9.26	CTRON-SSR-CONFIG-MIB	否	否	是
OLI-2000	1.3.6.1.4.1.285.9.27	CTRON-SSR-CONFIG-MIB	否	否	是
CPQ-8000	1.3.6.1.4.1.232.134.1.1	CTRON-SSR-CONFIG-MIB	否	否	是
CPQ-8600	1.3.6.1.4.1.232.134.1.2	CTRON-SSR-CONFIG-MIB	否	否	是
CPQ-2000	1.3.6.1.4.1.232.134.1.3	CTRON-SSR-CONFIG-MIB	否	否	是
6-SSRM-02	1.3.6.1.4.1.52.3.9.33.4.1	CTRON-SSR-CONFIG-MIB	否	否	是
RS-8000	1.3.6.1.4.1.5567.1.1.1	CTRON-SSR-CONFIG-MIB	否	否	是
RS-8600	1.3.6.1.4.1.5567.1.1.2	CTRON-SSR-CONFIG-MIB	否	否	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
RS-2000	1.3.6.1.4.1.5567.1.1.3	CTRON-SSR-CONFIG-MIB	否	否	是
RS-2100	1.3.6.1.4.1.5567.1.1.4	CTRON-SSR-CONFIG-MIB	否	否	是
RS-3000	1.3.6.1.4.1.5567.1.1.5	CTRON-SSR-CONFIG-MIB	否	否	是
IA-1100	1.3.6.1.4.1.5567.1.1.22	CTRON-SSR-CONFIG-MIB	否	否	是
IA-1200	1.3.6.1.4.1.5567.1.1.23	CTRON-SSR-CONFIG-MIB	否	否	是
RS-1000	1.3.6.1.4.1.5567.1.1.8	CTRON-SSR-CONFIG-MIB	否	否	是
IA-1500	1.3.6.1.4.1.5567.1.1.27	CTRON-SSR-CONFIG-MIB	否	否	是
SSR-8000	1.3.6.1.4.1.52.3.9.20.1.3	CTRON-SSR-CONFIG-MIB	否	否	是
SSR-8600	1.3.6.1.4.1.52.3.9.20.1.4	CTRON-SSR-CONFIG-MIB	否	否	是
SSR-2000	1.3.6.1.4.1.52.3.9.33.1.1	CTRON-SSR-CONFIG-MIB	否	否	是
SSR-2100	1.3.6.1.4.1.52.3.9.33.1.3	CTRON-SSR-CONFIG-MIB	否	否	是
IA-1000	1.3.6.1.4.1.52.3.9.33.2.8	CTRON-SSR-CONFIG-MIB	否	否	是
IA-2000	1.3.6.1.4.1.52.3.9.33.2.9	CTRON-SSR-CONFIG-MIB	否	否	是
XP-2400	1.3.6.1.4.1.5624.2.1.42	CTRON-SSR-CONFIG-MIB	否	否	是
RS-32000	1.3.6.1.4.1.5567.1.1.6	CTRON-SSR-CONFIG-MIB	否	否	是
RS-38000	1.3.6.1.4.1.5567.1.1.9	CTRON-SSR-CONFIG-MIB	否	否	是
SSR-32000	1.3.6.1.4.1.52.10.2	CTRON-SSR-CONFIG-MIB	否	否	是
ER16	1.3.6.1.4.1.5624.2.1.23	CTRON-SSR-CONFIG-MIB	否	否	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
BE2800	1.3.6.1.4.1.1456.3.2	CTRON-SSR-CONFIG-MIB	否	否	是
Terayon 路由器	1.3.6.1.4.1.1456.3.3	CTRON-SSR-CONFIG-MIB	否	否	是
5-SSRM-02	1.3.6.1.4.1.5624.2.1.24	CTRON-SSR-CONFIG-MIB	否	否	是

支持的 Extreme 设备

下表列出了 CA Spectrum Network Configuration Manager 支持的 Extreme 设备。该表提供了示例。有关设备支持的最新信息，请访问 CA 设备认证数据库 (p. 15)。

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
Alpine 3802	1.3.6.1.4.1.1916.2.26	EXTREME-FILETRANSFER-MIB	否	否	是
Alpine 3804	1.3.6.1.4.1.1916.2.20	EXTREME-FILETRANSFER-MIB	否	否	是
Alpine 3808	1.3.6.1.4.1.1916.2.17	EXTREME-FILETRANSFER-MIB	否	否	是
Altitude 300	1.3.6.1.4.1.1916.2.86	EXTREME-FILETRANSFER-MIB	否	否	是
Altitude 350	1.3.6.1.4.1.1916.2.75	EXTREME-FILETRANSFER-MIB	否	否	是
BlackDiamond 6800	1.3.6.1.4.1.1916.2.8	EXTREME-FILETRANSFER-MIB	否	否	是
BlackDiamond 6804	1.3.6.1.4.1.1916.2.27	EXTREME-FILETRANSFER-MIB	否	否	是
BlackDiamond 6808	1.3.6.1.4.1.1916.2.11	EXTREME-FILETRANSFER-MIB	否	否	是
BlackDiamond 6816	1.3.6.1.4.1.1916.2.24	EXTREME-FILETRANSFER-MIB	否	否	是
BlackDiamond 8806	1.3.6.1.4.1.1916.2.74	EXTREME-FILETRANSFER-MIB	否	否	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
BlackDiamond 8810	1.3.6.1.4.1.1916.2.62	EXTREME-FILETRANSFER-MIB	否	否	是
BlackDiamond 10808	1.3.6.1.4.1.1916.2.56	EXTREME-FILETRANSFER-MIB	否	否	是
BlackDiamond 12802	1.3.6.1.4.1.1916.2.85	EXTREME-FILETRANSFER-MIB	否	否	是
BlackDiamond 12804	1.3.6.1.4.1.1916.2.77	EXTREME-FILETRANSFER-MIB	否	否	是
EnetSwitch 24Port	1.3.6.1.4.1.1916.2.23	EXTREME-FILETRANSFER-MIB	否	否	是
Sentriant CE150	1.3.6.1.4.1.1916.2.83	EXTREME-FILETRANSFER-MIB	否	否	是
Summit 1	1.3.6.1.4.1.1916.2.1	EXTREME-FILETRANSFER-MIB	否	否	是
Summit 1iSX	1.3.6.1.4.1.1916.2.19	EXTREME-FILETRANSFER-MIB	否	否	是
Summit 1iTX	1.3.6.1.4.1.1916.2.14	EXTREME-FILETRANSFER-MIB	否	否	是
Summit 2	1.3.6.1.4.1.1916.2.2	EXTREME-FILETRANSFER-MIB	否	否	是
Summit 3	1.3.6.1.4.1.1916.2.3	EXTREME-FILETRANSFER-MIB	否	否	是
Summit 4	1.3.6.1.4.1.1916.2.4	EXTREME-FILETRANSFER-MIB	否	否	是
Summit 4FX	1.3.6.1.4.1.1916.2.5	EXTREME-FILETRANSFER-MIB	否	否	是
Summit 5i	1.3.6.1.4.1.1916.2.15	EXTREME-FILETRANSFER-MIB	否	否	是
Summit 5iLX	1.3.6.1.4.1.1916.2.21	EXTREME-FILETRANSFER-MIB	否	否	是
Summit 5iTX	1.3.6.1.4.1.1916.2.22	EXTREME-FILETRANSFER-MIB	否	否	是
Summit 7iSX	1.3.6.1.4.1.1916.2.12	EXTREME-FILETRANSFER-MIB	否	否	是
Summit 7iTX	1.3.6.1.4.1.1916.2.13	EXTREME-FILETRANSFER-MIB	否	否	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
Summit 24	1.3.6.1.4.1.1916.2.7	EXTREME-FILETRANSFER-MIB	否	否	是
Summit 24e2SX	1.3.6.1.4.1.1916.2.41	EXTREME-FILETRANSFER-MIB	否	否	是
Summit 24e2TX	1.3.6.1.4.1.1916.2.40	EXTREME-FILETRANSFER-MIB	否	否	是
Summit 24e3	1.3.6.1.4.1.1916.2.25	EXTREME-FILETRANSFER-MIB	否	否	是
Summit 48	1.3.6.1.4.1.1916.2.6	EXTREME-FILETRANSFER-MIB	否	否	是
Summit 48i	1.3.6.1.4.1.1916.2.16	EXTREME-FILETRANSFER-MIB	否	否	是
Summit 48i1u	1.3.6.1.4.1.1916.2.28	EXTREME-FILETRANSFER-MIB	否	否	是
Summit 200-24	1.3.6.1.4.1.1916.2.53	EXTREME-FILETRANSFER-MIB	否	否	是
Summit 200-24fx	1.3.6.1.4.1.1916.2.70	EXTREME-FILETRANSFER-MIB	否	否	是
Summit 200-48	1.3.6.1.4.1.1916.2.54	EXTREME-FILETRANSFER-MIB	否	否	是
Summit 300-24	1.3.6.1.4.1.1916.2.61	EXTREME-FILETRANSFER-MIB	否	否	是
Summit 300-48	1.3.6.1.4.1.1916.2.55	EXTREME-FILETRANSFER-MIB	否	否	是
Summit 400-24	1.3.6.1.4.1.1916.2.59	EXTREME-FILETRANSFER-MIB	否	否	是
Summit 400-24p	1.3.6.1.4.1.1916.2.64	EXTREME-FILETRANSFER-MIB	否	否	是
Summit 400-24t	1.3.6.1.4.1.1916.2.63	EXTREME-FILETRANSFER-MIB	否	否	是
Summit 400-48t	1.3.6.1.4.1.1916.2.58	EXTREME-FILETRANSFER-MIB	否	否	是
Summit Px1	1.3.6.1.4.1.1916.2.30	EXTREME-FILETRANSFER-MIB	否	否	是
Summit Ver2Stack	1.3.6.1.4.1.1916.2.93	EXTREME-FILETRANSFER-MIB	否	否	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
Summit X250-24p	1.3.6.1.4.1.1916.2.89	EXTREME-FILETRANSFER-MIB	否	否	是
Summit X250-24t	1.3.6.1.4.1.1916.2.88	EXTREME-FILETRANSFER-MIB	否	否	是
Summit X250-24x	1.3.6.1.4.1.1916.2.90	EXTREME-FILETRANSFER-MIB	否	否	是
Summit X250-48p	1.3.6.1.4.1.1916.2.92	EXTREME-FILETRANSFER-MIB	否	否	是
Summit X250-48t	1.3.6.1.4.1.1916.2.91	EXTREME-FILETRANSFER-MIB	否	否	是
Summit X450-24t	1.3.6.1.4.1.1916.2.66	EXTREME-FILETRANSFER-MIB	否	否	是
Summit X450-24x	1.3.6.1.4.1.1916.2.65	EXTREME-FILETRANSFER-MIB	否	否	是
Summit X450a-24t	1.3.6.1.4.1.1916.2.71	EXTREME-FILETRANSFER-MIB	否	否	是
Summit X450a-24tDC	1.3.6.1.4.1.1916.2.80	EXTREME-FILETRANSFER-MIB	否	否	是
Summit X450a-24x	1.3.6.1.4.1.1916.2.84	EXTREME-FILETRANSFER-MIB	否	否	是
Summit X450a-24xDC	1.3.6.1.4.1.1916.2.82	EXTREME-FILETRANSFER-MIB	否	否	是
Summit X450a-48t	1.3.6.1.4.1.1916.2.76	EXTREME-FILETRANSFER-MIB	否	否	是
Summit X450a-48tDC	1.3.6.1.4.1.1916.2.87	EXTREME-FILETRANSFER-MIB	否	否	是
Summit X450e-24p	1.3.6.1.4.1.1916.2.72	EXTREME-FILETRANSFER-MIB	否	否	是
Summit X450e-48p	1.3.6.1.4.1.1916.2.79	EXTREME-FILETRANSFER-MIB	否	否	是
SummitStack	1.3.6.1.4.1.1916.2.67	EXTREME-FILETRANSFER-MIB	否	否	是
SummitWM 100	1.3.6.1.4.1.1916.2.68	EXTREME-FILETRANSFER-MIB	否	否	是
SummitWM 200	1.3.6.1.4.1.1916.2.94	EXTREME-FILETRANSFER-MIB	否	否	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
SummitWM 1000	1.3.6.1.4.1.1916.2.69	EXTREME-FILETRANSFER-MIB	否	否	是
SummitWM 2000	1.3.6.1.4.1.1916.2.95	EXTREME-FILETRANSFER-MIB	否	否	是

支持的 Foundry 设备

下表列出了 CA Spectrum Network Configuration Manager 支持的 Foundry 设备。该表提供了示例。有关设备支持的最新信息，请访问 CA 设备认证数据库 (p. 15)。

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
BigIronMG8Sw	1.3.6.1.4.1.1991.1.3.32.1	FOUNDRY-SN-AGENT-MIB	否	否	是
BigIronMG8Rt	1.3.6.1.4.1.1991.1.3.32.2	FOUNDRY-SN-AGENT-MIB	否	否	是
BigIronRX4Rt	1.3.6.1.4.1.1991.1.3.40.3.2	FOUNDRY-SN-AGENT-MIB	否	否	是
BigIronRX4Sw	1.3.6.1.4.1.1991.1.3.40.3.1	FOUNDRY-SN-AGENT-MIB	否	否	是
BigIronRX8Rt	1.3.6.1.4.1.1991.1.3.40.2.2	FOUNDRY-SN-AGENT-MIB	否	否	是
BigIronRX8Sw	1.3.6.1.4.1.1991.1.3.40.2.1	FOUNDRY-SN-AGENT-MIB	否	否	是
BigIronRX16Rt	1.3.6.1.4.1.1991.1.3.40.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
BigIronRX16Sw	1.3.6.1.4.1.1991.1.3.40.1.1	FOUNDRY-SN-AGENT-MIB	否	否	是
BigIronSXL3Sw	1.3.6.1.4.1.1991.1.3.37.1.3	FOUNDRY-SN-AGENT-MIB	否	否	是
BigIronSXRt	1.3.6.1.4.1.1991.1.3.37.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
BigIronSXSw	1.3.6.1.4.1.1991.1.3.37.1.1	FOUNDRY-SN-AGENT-MIB	否	否	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
BIron4000Rt	1.3.6.1.4.1.1991.1.3.6.2	FOUNDRY-SN-AGENT-MIB	否	否	是
BIron4000Sl	1.3.6.1.4.1.1991.1.3.6.3	FOUNDRY-SN-AGENT-MIB	否	否	是
BIron4000Sw	1.3.6.1.4.1.1991.1.3.6.1	FOUNDRY-SN-AGENT-MIB	否	否	是
BIron8000Rt	1.3.6.1.4.1.1991.1.3.7.2	FOUNDRY-SN-AGENT-MIB	否	否	是
BIron8000Sl	1.3.6.1.4.1.1991.1.3.7.3	FOUNDRY-SN-AGENT-MIB	否	否	是
BIron15000Rt	1.3.6.1.4.1.1991.1.3.14.2	FOUNDRY-SN-AGENT-MIB	否	否	是
BIron15000Sl	1.3.6.1.4.1.1991.1.3.14.3	FOUNDRY-SN-AGENT-MIB	否	否	是
BIron8000Sw	1.3.6.1.4.1.1991.1.3.7.1	FOUNDRY-SN-AGENT-MIB	否	否	是
BIron15000Sw	1.3.6.1.4.1.1991.1.3.14.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FastIronBBSw	1.3.6.1.4.1.1991.1.3.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FastIron2Rt	1.3.6.1.4.1.1991.1.3.8.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FastIron2Sw	1.3.6.1.4.1.1991.1.3.8.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FastIron3Rt	1.3.6.1.4.1.1991.1.3.16.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FastIron3Sw	1.3.6.1.4.1.1991.1.3.16.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FastIronWGSw	1.3.6.1.4.1.1991.1.3.1.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FES2402Sw	1.3.6.1.4.1.1991.1.3.25.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FES2402Rt	1.3.6.1.4.1.1991.1.3.25.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FES4802Rt	1.3.6.1.4.1.1991.1.3.26.2	FOUNDRY-SN-AGENT-MIB	否	否	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
FES4802Sw	1.3.6.1.4.1.1991.1.3.26.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FES9604Rt	1.3.6.1.4.1.1991.1.3.27.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FES9604Sw	1.3.6.1.4.1.1991.1.3.27.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FES12GCFRt	1.3.6.1.4.1.1991.1.3.28.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FES12GCFSw	1.3.6.1.4.1.1991.1.3.28.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FES2402POERt	1.3.6.1.4.1.1991.1.3.29.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FES2402POESw	1.3.6.1.4.1.1991.1.3.29.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FES4802POERt	1.3.6.1.4.1.1991.1.3.30.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FES4802POESw	1.3.6.1.4.1.1991.1.3.30.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424Rt	1.3.6.1.4.1.1991.1.3.34.1.1.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424Sw	1.3.6.1.4.1.1991.1.3.34.1.1.1.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424PremRt	1.3.6.1.4.1.1991.1.3.34.1.1.2.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424PremSw	1.3.6.1.4.1.1991.1.3.34.1.1.2.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424P1XGPremSw	1.3.6.1.4.1.1991.1.3.34.1.2.2.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424P1XGRt	1.3.6.1.4.1.1991.1.3.34.1.2.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424P1XGSw	1.3.6.1.4.1.1991.1.3.34.1.2.1.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424P1XGPremRt	1.3.6.1.4.1.1991.1.3.34.1.2.2.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424P2XGRt	1.3.6.1.4.1.1991.1.3.34.1.3.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
FESX424P2XGSw	1.3.6.1.4.1.1991.1.3.34.1.3.1.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424P2XGPremRt	1.3.6.1.4.1.1991.1.3.34.1.3.2.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424P2XGPremSw	1.3.6.1.4.1.1991.1.3.34.1.3.2.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX448Rt	1.3.6.1.4.1.1991.1.3.34.2.1.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX448Sw	1.3.6.1.4.1.1991.1.3.34.2.1.1.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX448PremRt	1.3.6.1.4.1.1991.1.3.34.2.1.2.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX448PremSw	1.3.6.1.4.1.1991.1.3.34.2.1.2.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX448P1XGSw	1.3.6.1.4.1.1991.1.3.34.2.2.1.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX448P1XGRt	1.3.6.1.4.1.1991.1.3.34.2.2.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX448P1XGPremRt	1.3.6.1.4.1.1991.1.3.34.2.2.2.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX448P1XGPremSw	1.3.6.1.4.1.1991.1.3.34.2.2.2.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX448P2XGRt	1.3.6.1.4.1.1991.1.3.34.2.3.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX448P2XGSw	1.3.6.1.4.1.1991.1.3.34.2.3.1.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX448P2XGPremRt	1.3.6.1.4.1.1991.1.3.34.2.3.2.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX448P2XGPremSw	1.3.6.1.4.1.1991.1.3.34.2.3.2.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424FiberRt	1.3.6.1.4.1.1991.1.3.34.3.1.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424FiberSw	1.3.6.1.4.1.1991.1.3.34.3.1.1.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424FiberPremRt	1.3.6.1.4.1.1991.1.3.34.3.1.2.2	FOUNDRY-SN-AGENT-MIB	否	否	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
FESX424FiberPremSw	1.3.6.1.4.1.1991.1.3.34.3.1.2.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424FiberP1XGRt	1.3.6.1.4.1.1991.1.3.34.3.2.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424FiberP1XGSw	1.3.6.1.4.1.1991.1.3.34.3.2.1.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424FiberP1XGPremRt	1.3.6.1.4.1.1991.1.3.34.3.2.2.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424FiberP1XGPremSw	1.3.6.1.4.1.1991.1.3.34.3.2.2.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424FiberP2XGRt	1.3.6.1.4.1.1991.1.3.34.3.3.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424FiberP2XGSw	1.3.6.1.4.1.1991.1.3.34.3.3.1.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424FiberP2XGPremRt	1.3.6.1.4.1.1991.1.3.34.3.3.2.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424FiberP2XGPremSw	1.3.6.1.4.1.1991.1.3.34.3.3.2.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX448FiberRt	1.3.6.1.4.1.1991.1.3.34.4.1.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX448FiberSw	1.3.6.1.4.1.1991.1.3.34.4.1.1.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX448FiberPremRt	1.3.6.1.4.1.1991.1.3.34.4.1.2.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX448FiberPremSw	1.3.6.1.4.1.1991.1.3.34.4.1.2.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX448FiberP1XGRt	1.3.6.1.4.1.1991.1.3.34.4.2.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX448FiberP1XGSw	1.3.6.1.4.1.1991.1.3.34.4.2.1.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX448FiberP1XGPremRt	1.3.6.1.4.1.1991.1.3.34.4.2.2.2	FOUNDRY-SN-AGENT-MIB	否	否	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
FESX448FiberP1XGPremSw	1.3.6.1.4.1.1991.1.3.34.4.2.2.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX448FiberP2XGRt	1.3.6.1.4.1.1991.1.3.34.4.3.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX448FiberP2XGSw	1.3.6.1.4.1.1991.1.3.34.4.3.1.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX448FiberP2XGPremRt	1.3.6.1.4.1.1991.1.3.34.4.3.2.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX448FiberP2XGPremSw	1.3.6.1.4.1.1991.1.3.34.4.3.2.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424POERt	1.3.6.1.4.1.1991.1.3.34.5.1.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424POESw	1.3.6.1.4.1.1991.1.3.34.5.1.1.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424POEPremRt	1.3.6.1.4.1.1991.1.3.34.5.1.2.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424POEPremSw	1.3.6.1.4.1.1991.1.3.34.5.1.2.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424POEP1XGSw	1.3.6.1.4.1.1991.1.3.34.5.2.1.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424POEP1XGRt	1.3.6.1.4.1.1991.1.3.34.5.2.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424POEP1XGPremRt	1.3.6.1.4.1.1991.1.3.34.5.2.2.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424POEP1XGPremSw	1.3.6.1.4.1.1991.1.3.34.5.2.2.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424POEP2XGRt	1.3.6.1.4.1.1991.1.3.34.5.3.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424POEP2XGSw	1.3.6.1.4.1.1991.1.3.34.5.3.1.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FESX424POEP2XGPremRt	1.3.6.1.4.1.1991.1.3.34.5.3.2.2	FOUNDRY-SN-AGENT-MIB	否	否	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
FESX424POEP2XGPremSw	1.3.6.1.4.1.1991.1.3.34.5.3.2.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FWSX424Rt	1.3.6.1.4.1.1991.1.3.35.1.1.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FWSX424Sw	1.3.6.1.4.1.1991.1.3.35.1.1.1.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FWSX424P1XGRt	1.3.6.1.4.1.1991.1.3.35.1.2.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FWSX424P1XGSw	1.3.6.1.4.1.1991.1.3.35.1.2.1.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FWSX424P2XGRt	1.3.6.1.4.1.1991.1.3.35.1.3.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FWSX424P2XGSw	1.3.6.1.4.1.1991.1.3.35.1.3.1.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FWSX448Rt	1.3.6.1.4.1.1991.1.3.35.2.1.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FWSX448Sw	1.3.6.1.4.1.1991.1.3.35.2.1.1.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FWSX448P1XGRt	1.3.6.1.4.1.1991.1.3.35.2.2.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FWSX448P1XGSw	1.3.6.1.4.1.1991.1.3.35.2.2.1.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FWSX448P2XGRt	1.3.6.1.4.1.1991.1.3.35.2.3.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FWSX448P2XGSw	1.3.6.1.4.1.1991.1.3.35.2.3.1.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FIron2GCRt	1.3.6.1.4.1.1991.1.3.12.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FIron2GCSw	1.3.6.1.4.1.1991.1.3.12.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FIron2PlusRt	1.3.6.1.4.1.1991.1.3.9.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FIron2PlusSw	1.3.6.1.4.1.1991.1.3.9.1	FOUNDRY-SN-AGENT-MIB	否	否	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
FIron3GCRt	1.3.6.1.4.1.1991.1.3.17.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FIron3GCSw	1.3.6.1.4.1.1991.1.3.17.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FIron400Sw	1.3.6.1.4.1.1991.1.3.22.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FIron400Rt	1.3.6.1.4.1.1991.1.3.22.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FIron4802Rt	1.3.6.1.4.1.1991.1.3.21.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FIron4802SI	1.3.6.1.4.1.1991.1.3.21.3	FOUNDRY-SN-AGENT-MIB	否	否	是
FIron4802Sw	1.3.6.1.4.1.1991.1.3.21.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FIron800Rt	1.3.6.1.4.1.1991.1.3.23.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FIron800Sw	1.3.6.1.4.1.1991.1.3.23.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FIron1500Rt	1.3.6.1.4.1.1991.1.3.24.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FIron1500Sw	1.3.6.1.4.1.1991.1.3.24.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FIronSXRt	1.3.6.1.4.1.1991.1.3.36.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FIronSXSw	1.3.6.1.4.1.1991.1.3.36.1.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FIronSXL3Sw	1.3.6.1.4.1.1991.1.3.36.1.3	FOUNDRY-SN-AGENT-MIB	否	否	是
FIronSXPremL3Sw	1.3.6.1.4.1.1991.1.3.36.2.3	FOUNDRY-SN-AGENT-MIB	否	否	是
FIronSXPremRt	1.3.6.1.4.1.1991.1.3.36.2.2	FOUNDRY-SN-AGENT-MIB	否	否	是
FIronSXPremSw	1.3.6.1.4.1.1991.1.3.36.2.1	FOUNDRY-SN-AGENT-MIB	否	否	是
FI2PlusGCSw	1.3.6.1.4.1.1991.1.3.13.1	FOUNDRY-SN-AGENT-MIB	否	否	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
FI2PlusGCRt	1.3.6.1.4.1.1991.1.3.13.2	FOUNDRY-SN-AGENT-MIB	否	否	是
NetIronRt	1.3.6.1.4.1.1991.1.3.2.1	FOUNDRY-SN-AGENT-MIB	否	否	是
NetIron40GRt	1.3.6.1.4.1.1991.1.3.33.1	FOUNDRY-SN-AGENT-MIB	否	否	是
NetIron400Rt	1.3.6.1.4.1.1991.1.3.10.1	FOUNDRY-SN-AGENT-MIB	否	否	是
NetIron800Rt	1.3.6.1.4.1.1991.1.3.11.1	FOUNDRY-SN-AGENT-MIB	否	否	是
NIron1500Rt	1.3.6.1.4.1.1991.1.3.15.1	FOUNDRY-SN-AGENT-MIB	否	否	是
NetIronMLX4Rt	1.3.6.1.4.1.1991.1.3.44.3.2	FOUNDRY-SN-AGENT-MIB	否	否	是
NetIronMLX16Rt	1.3.6.1.4.1.1991.1.3.44.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
NetIronMLX8Rt	1.3.6.1.4.1.1991.1.3.44.2.2	FOUNDRY-SN-AGENT-MIB	否	否	是
NetIronXMR16000Rt	1.3.6.1.4.1.1991.1.3.41.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
NetIronXMR8000Rt	1.3.6.1.4.1.1991.1.3.41.2.2	FOUNDRY-SN-AGENT-MIB	否	否	是
NetIronXMR4000Rt	1.3.6.1.4.1.1991.1.3.41.3.2	FOUNDRY-SN-AGENT-MIB	否	否	是
NetIronIMRRt	1.3.6.1.4.1.1991.1.3.39.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
NIron4802Rt	1.3.6.1.4.1.1991.1.3.31.2	FOUNDRY-SN-AGENT-MIB	否	否	是
NIron4802Sw	1.3.6.1.4.1.1991.1.3.31.1	FOUNDRY-SN-AGENT-MIB	否	否	是
ServerIron	1.3.6.1.4.1.1991.1.3.3.1	FOUNDRY-SN-AGENT-MIB	否	否	是
ServerIronXL	1.3.6.1.4.1.1991.1.3.3.2	FOUNDRY-SN-AGENT-MIB	否	否	是
SIron400Rt	1.3.6.1.4.1.1991.1.3.18.2	FOUNDRY-SN-AGENT-MIB	否	否	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
SIron400Sw	1.3.6.1.4.1.1991.1.3.18.1	FOUNDRY-SN-AGENT-MIB	否	否	是
SIron800Rt	1.3.6.1.4.1.1991.1.3.19.2	FOUNDRY-SN-AGENT-MIB	否	否	是
SIron800Sw	1.3.6.1.4.1.1991.1.3.19.1	FOUNDRY-SN-AGENT-MIB	否	否	是
SIron1500Rt	1.3.6.1.4.1.1991.1.3.20.2	FOUNDRY-SN-AGENT-MIB	否	否	是
SIron1500Sw	1.3.6.1.4.1.1991.1.3.20.1	FOUNDRY-SN-AGENT-MIB	否	否	是
SIronXLTCS	1.3.6.1.4.1.1991.1.3.3.3	FOUNDRY-SN-AGENT-MIB	否	否	是
SIronLS100Rt	1.3.6.1.4.1.1991.1.3.42.9.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
SIronLS100Sw	1.3.6.1.4.1.1991.1.3.42.9.1.1	FOUNDRY-SN-AGENT-MIB	否	否	是
SIronLS300Rt	1.3.6.1.4.1.1991.1.3.42.9.2.2	FOUNDRY-SN-AGENT-MIB	否	否	是
SIronLS300Sw	1.3.6.1.4.1.1991.1.3.42.9.2.1	FOUNDRY-SN-AGENT-MIB	否	否	是
SIronTM100Sw	1.3.6.1.4.1.1991.1.3.42.10.1.1	FOUNDRY-SN-AGENT-MIB	否	否	是
SIronTM100Sw	1.3.6.1.4.1.1991.1.3.42.10.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
SIronTM300Sw	1.3.6.1.4.1.1991.1.3.42.10.2.1	FOUNDRY-SN-AGENT-MIB	否	否	是
SIronTM300Sw	1.3.6.1.4.1.1991.1.3.42.10.2.2	FOUNDRY-SN-AGENT-MIB	否	否	是
TurboIronSXSw	1.3.6.1.4.1.1991.1.3.38.1.1	FOUNDRY-SN-AGENT-MIB	否	否	是
TurboIronSXRt	1.3.6.1.4.1.1991.1.3.38.1.2	FOUNDRY-SN-AGENT-MIB	否	否	是
TurboIronSXL3Sw	1.3.6.1.4.1.1991.1.3.38.1.3	FOUNDRY-SN-AGENT-MIB	否	否	是
TurboIronSxPremSw	1.3.6.1.4.1.1991.1.3.38.2.1	FOUNDRY-SN-AGENT-MIB	否	否	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
TurboIronSX PremRt	1.3.6.1.4.1.1991.1.3.38.2.2	FOUNDRY-SN-AGENT-MIB	否	否	是
TurboIronSX PremL3Sw	1.3.6.1.4.1.1991.1.3.38.2.3	FOUNDRY-SN-AGENT-MIB	否	否	是
TIron8SIXLG	1.3.6.1.4.1.1991.1.3.5.4	FOUNDRY-SN-AGENT-MIB	否	否	是
TurboIronRt	1.3.6.1.4.1.1991.1.3.4.2	FOUNDRY-SN-AGENT-MIB	否	否	是
TurboIronSw	1.3.6.1.4.1.1991.1.3.4.1	FOUNDRY-SN-AGENT-MIB	否	否	是
TurboIron8Rt	1.3.6.1.4.1.1991.1.3.5.2	FOUNDRY-SN-AGENT-MIB	否	否	是
TurboIron8Sl	1.3.6.1.4.1.1991.1.3.5.3	FOUNDRY-SN-AGENT-MIB	否	否	是
TurboIron8Sw	1.3.6.1.4.1.1991.1.3.5.1	FOUNDRY-SN-AGENT-MIB	否	否	是

支持的 Juniper 设备

下表列出了 CA Spectrum Network Configuration Manager 支持的 Juniper 设备。该表提供了示例。有关设备支持的最新信息，请访问 CA 设备认证数据库 (p. 15)。

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
EX3200	1.3.6.1.4.1.2636.1.1.1.2.30	否	否	是	否
EX4200	1.3.6.1.4.1.2636.1.1.1.2.31	否	否	是	否
EX8208	1.3.6.1.4.1.2636.1.1.1.2.32	否	否	是	否
EX8216	1.3.6.1.4.1.2636.1.1.1.2.33	否	否	是	否
IRM	1.3.6.1.4.1.2636.1.1.1.2.16	否	否	*是	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
J2300	1.3.6.1.4.1.2636.1.1.1.2.13	否	否	*是	是
J4300	1.3.6.1.4.1.2636.1.1.1.2.14	否	否	*是	是
J6300	1.3.6.1.4.1.2636.1.1.1.2.15	否	否	*是	是
M5	1.3.6.1.4.1.2636.1.1.1.2.5	否	否	*是	是
M7i	1.3.6.1.4.1.2636.1.1.1.2.10	否	否	*是	是
M10	1.3.6.1.4.1.2636.1.1.1.2.4	否	否	*是	是
M10i	1.3.6.1.4.1.2636.1.1.1.2.11	否	否	*是	是
M20	1.3.6.1.4.1.2636.1.1.1.2.2	否	否	*是	是
M40	1.3.6.1.4.1.2636.1.1.1.2.1	否	否	*是	是
M40e	1.3.6.1.4.1.2636.1.1.1.2.8	否	否	*是	是
M160	1.3.6.1.4.1.2636.1.1.1.2.3	否	否	*是	是
M320	1.3.6.1.4.1.2636.1.1.1.2.9	否	否	*是	是
T320	1.3.6.1.4.1.2636.1.1.1.2.7	否	否	*是	是
T640	1.3.6.1.4.1.2636.1.1.1.2.6	否	否	*是	是
TX	1.3.6.1.4.1.2636.1.1.1.2.17	否	否	*是	是

*设备必须支持 SSH V2

支持的 Lancom 设备

下表列出了 CA Spectrum Network Configuration Manager 支持的 Lancom 设备。支持的设备必须运行固件 LCOS 7.58.0045 或更高版本。该表提供了示例。有关设备支持的最新信息，请访问 CA 设备认证数据库 (p. 15)。

当 Perl 脚本是与设备进行通信的唯一方式时，提供了脚本方法。

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
LANCOM 1721 VPN	1.3.6.1.4.1.2356.500.4.1721	否	否	否	Telnet/TFTP
LANCOM 1751	1.3.6.1.4.1.2356.1000.1.1751	否	否	否	Telnet/TFTP
LANCOM 7111	1.3.6.1.4.1.2356.500.2.7111	否	否	否	Telnet/TFTP
LANCOM 8011	1.3.6.1.4.1.2356.500.2.8011	否	否	否	Telnet/TFTP

支持的 Nortel Baystack 设备

下表列出了 CA Spectrum Network Configuration Manager 支持的 Nortel Baystack 设备。该表提供了示例。有关设备支持的最新信息，请访问 CA 设备认证数据库 (p. 15)。

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
BayStack450-24T	1.3.6.1.4.1.45.3.35.1	否	否	*是	是
BayStack380-24T	1.3.6.1.4.1.45.3.45.1	否	否	*是	是
BayStack420	1.3.6.1.4.1.45.3.43.1	否	否	*是	是
BayStack460-24T	1.3.6.1.4.1.45.3.49.1	否	否	*是	是
BayStack470-48T	1.3.6.1.4.1.45.3.46.1	否	否	*是	是
BayStack425-24T	1.3.6.1.4.1.45.3.57.2	否	否	*是	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
BayStack470-24T	1.3.6.1.4.1.45.3.54.1	否	否	*是	是
BayStack5510-24T	1.3.6.1.4.1.45.3.52.1	否	否	*是	是
BayStack5510-48T	1.3.6.1.4.1.45.3.53.1	否	否	*是	是
BayStack5520-24T-PWR	1.3.6.1.4.1.45.3.59.1	否	否	*是	是
BayStack5520-48T-PWR	1.3.6.1.4.1.45.3.59.2	否	否	*是	是
Nortel ERS 5530-24TFD	1.3.6.1.4.1.45.3.65	否	否	*是	是

* 设备必须支持 SSH V2

支持的 Nortel Passport 设备

下表列出了 CA Spectrum Network Configuration Manager 支持的 Nortel Passport 设备。该表提供了示例。有关设备支持的最新信息，请访问 CA 设备认证数据库 (p. 15)。

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
Passport1424T	1.3.6.1.4.1.2272.42	SWL2MGMT-MIB	否	否	是
Passport1648	1.3.6.1.4.1.2272.43	SWL2MGMT-MIB	否	否	是
Passport1612	1.3.6.1.4.1.2272.44	SWL2MGMT-MIB	否	否	是
Passport1624	1.3.6.1.4.1.2272.45	SWL2MGMT-MIB	否	否	是
Passport8610	1.3.6.1.4.1.2272.30	RAPID-CITY MIB	否	否	是
Passport8606	1.3.6.1.4.1.2272.31	RAPID-CITY MIB	否	否	是

设备名称	系统 OID	SNMP/TFTP 支持	Telnet 支持	SSH 支持	Perl 支持
Passport8110	1.3.6.1.4.1.2272.32	RAPID-CITY MIB	否	否	是
Passport8106	1.3.6.1.4.1.2272.33	RAPID-CITY MIB	否	否	是
Passport8610	1.3.6.1.4.1.2272.37	RAPID-CITY MIB	否	否	是
IntrWanPE100	1.3.6.1.4.1.2272.40	RAPID-CITY MIB	否	否	是
Passport8006	1.3.6.1.4.1.2272.280887558	RAPID-CITY MIB	否	否	是
Passport8010	1.3.6.1.4.1.2272.280887562	RAPID-CITY MIB	否	否	是

附录 B： Network Configuration Manager 事件

此部分包含以下主题：

关于 Network Configuration Manager 事件 (p. 205)
在设备上生成的事件 (p. 205)
针对策略生成的事件 (p. 210)
针对全局同步、捕获、上传和写入启动等任务生成的事件 (p. 211)
在配置服务器应用程序上生成的事件 (p. 212)
针对设备系列生成的事件 (p. 212)

关于 Network Configuration Manager 事件

设备上发生配置更改时，将生成事件。将合并指定的关联事件期间（在配置管理器常规配置中设置）内特定设备的所有事件。有关详细信息，请参阅配置常规配置 (p. 25)。

基于设备陷阱、Syslog 陷阱和事件、Network Configuration Manager 内部陷阱和映射到常规更改事件的任何其他陷阱，对信息进行关联。该信息随设备系列的不同而不同。为 Cisco CatOS、Cisco IOS、支持 SSH 的 Cisco IOS 和 Juniper JUNOS 设备系列提供了即用型支持。有关为您的安装自定义陷阱的详细信息，请参阅配置通知陷阱设置 (p. 42)。

在设备上生成的事件

配置更改

Event0082101b:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 在格局 {S 3} 上 {t} 类型的设备 {m} 上检测到配置更改。(事件 [{e}])

Event00821029:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 从设备 {m} 接收到配置更改通知。(事件 [{e}])

Event0082105e:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 格局 {S 2} 上设备 {m} 的运行配置已更改。(事件 [{e}])

Event0082105f:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 格局 {S 2} 上设备 {m} 的运行配置已更改。将在此模型上生成警报。(事件 [{e}])

配置更改事件的关联

Event0082105a:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 从格局 {S 1} 上 {t} 类型的设备 {m} 接收到配置更改通知。

已提供设备陷阱:

设备用户: {S 2}

从: {S 3}

位于: {S 4}

以下信息由 SPECTRUM 提供:

设备用户: {S 2}

Spectrum 用户: {S 5}

NCM 通信模式: {S 6}

捕获成功: {S 7}

捕获错误消息: {S 8}

行更改总数: {I 9}

行更改相关数: {I 10}

违反策略: {S 11}

遵从策略: {S 12}

当前配置模型的模型句柄: {H 13}

前一个配置模型的模型句柄: {H 14}

启动配置与运行配置相同/不同

Event00821024:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 格局 {S 3} 上设备 {m} 的启动配置与其运行配置不同。(事件 [{e}])

Event00821025:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 格局 {S 3} 上设备 {m} 的启动配置与其运行配置不同。将在此模型上生成次要警报。(事件 [{e}])

Event00821026:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 格局 {S 3} 上设备 {m} 的启动配置与其运行配置不同。将在此模型上生成主要警报。(事件 [{e}])

Event00821027:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 格局 {S 3} 上设备 {m} 的启动配置与其运行配置不同。将在此模型上生成关键警报。(事件 [{e}])

Event00821028:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 格局 {S 3} 上设备 {m} 的启动配置与其运行配置相同。(事件 [{e}])

参考配置与运行配置相同/不同

Event0082105b:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 格局 {S 2} 上设备 {m} 的参考运行配置与其当前运行配置不同。(事件 [{e}])

Event0082105c:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 格局 {S 2} 上设备 {m} 的参考运行配置与其当前运行配置不同。将在此模型上生成警报。(事件 [{e}])

Event0082105d:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 格局 {S 2} 上设备 {m} 的参考运行配置与其运行配置相同。(事件 [{e}])

设备遵从/非遵从策略

Event00821016:{d "%w- %d %m-, %Y - %T"} 配置管理器 - {t} 类型的设备 {m} 遵从格局 {S 3} 上的策略 {S 1}。(事件 [{e}])

Event00821017:{d "%w- %d %m-, %Y - %T"} 配置管理器 - {t} 类型的设备 {m} 不遵从格局 {S 3} 上的策略 {S 1}。(事件 [{e}])

Event00821051:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 无法在格局 {S 1} 上 {t} 类型的设备 {m} 上验证主机配置的策略遵从性。
特定错误: {S 2} (事件 [{e}])

Event00821055:{d "%w- %d %m-, %Y - %T"} 配置管理器 - {t} 类型的设备 {m} 不再违反策略 {S 1}，因为该设备已从格局 {S 3} 上的全局集合 {S 2} 中移除。(事件 [{e}])

Event00821056:{d "%w- %d %m-, %Y - %T"} 配置管理器 - {t} 类型的设备 {m} 不再违反策略 {S 1}，因为该设备已从格局 {S 3} 上的设备系列 {S 2} 中移除。(事件 [{e}])

Event00821057:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 格局 {S 2} 上 {t} 类型的设备 {m} 不再违反策略 {S 1}，因为该策略已删除。(事件 [{e}])

设备不遵从策略警报生成的事件

Event00821020:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 设备 {m} 违反了格局 {S 3} 上的策略 {S 1}。此违反的重要级别是次要。(事件 [{e}])

Event00821021:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 设备 {m} 违反了格局 {S 3} 上的策略 {S 1}。此违反的重要级别是主要。(事件 [{e}])

Event00821022:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 设备 {m} 违反了格局 {S 3} 上的策略 {S 1}。此违反的重要级别是关键。(事件 [{e}])

捕获成功/失败

Event00821000:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 从格局 {S 1} 上 {t} 类型的设备 {m} 捕获主机配置文件成功(由用户 {S 2} 发起)。(事件 [{e}])

Event00821001:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 从格局 {S 1} 上 {t} 类型的设备 {m} 捕获主机配置文件失败(由用户 {S 2} 发起)。
特定错误: {S 3} (事件 [{e}])

Event00821049:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 从格局 {S 1} 上 {t} 类型的设备 {m} 捕获主机启动配置文件成功(由用户 {u} 发起)。(事件 [{e}])

Event00821050:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 从格局 {S 1} 上 {t} 类型的设备 {m} 捕获主机启动配置文件失败(由用户 {u} 发起)。特定错误: {S 3} (事件 [{e}])

上传成功/失败

Event00821002:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 格局 {S 1} 上 {t} 类型的设备 {m} 的主机配置加载成功(由用户 {S 2} 发起)。(事件 [{e}])

Event00821003:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 格局 {S 1} 上 {t} 类型的设备 {m} 的主机配置加载失败(由用户 {S 2} 发起)。
特定错误: {S 4} (事件 [{e}])

上传失败警报生成的事件

Event00821035:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 格局 {S 1} 上 {t} 类型的设备 {m} 的主机配置加载失败(由用户 {S 2} 发起)。
该失败的重要级别是次要。(事件 [{e}])

Event00821036:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 格局 {S 1} 上 {t} 类型的设备 {m} 的主机配置加载失败(由用户 {S 2} 发起)。
该失败的重要级别是主要。(事件 [{e}])

Event00821037:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 格局 {S 1} 上 {t} 类型的设备 {m} 的主机配置加载失败(由用户 {S 2} 发起)。
该失败的重要级别是关键。(事件 [{e}])

写入启动成功/失败

Event00821018:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 在格局 {S 1} 上，{S 2} 已将运行配置成功写入 {t} 类型的设备 {m} 上的启动配置。(事件 [{e}])

Event00821019:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 在格局 {S 1} 上，试图将运行配置写入 {t} 类型的设备 {m} 上的启动配置时失败。此操作由 {S 2} 发起。特定错误: {S 3}。(事件 [{e}])

NCM 在设备上已启用/禁用

Event0082102f:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 设备 {m} 已禁用 NCM。(事件 [{e}])

Event00821030:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 设备 {m} 已启用 NCM。(事件 [{e}])

NCM 已禁用，未执行操作

Event00821032:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 未对模型 {m} 执行请求的 NCM 操作，因为该模型设备系列已禁用 NCM。(事件 [{e}])

Event00821033:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 未对模型 {m} 执行请求的 NCM 操作，因为此模型已禁用 NCM。(事件 [{e}])

Event00821034:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 未对模型 {m} 执行请求的 NCM 操作，因为此模型为代理模型。(事件 [{e}])

设备固件加载

Event00821053:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 格局 {S 1} 上 {t} 类型的设备 {m} 固件加载已成功完成。使用以下命令行参数执行固件脚本: {S 3}。此操作由 {u} 发起。(事件 [{e}])

Event00821054:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 格局 {S 1} 上 {t} 类型的设备 {m} 固件加载失败。特定错误: {S 2}。使用以下命令行参数执行固件脚本: {S 3} (事件 [{e}])

在设备系列中已添加/移除设备

Event00821058:{d "%w- %d %m-, %Y - %T"} 配置管理器 - {t} 类型的设备 {m} 已添加到格局 {S 1} 上的设备系列 {S 2}。(事件 [{e}])

Event00821059:{d "%w- %d %m-, %Y - %T"} 配置管理器 - {t} 类型的设备 {m} 已从格局 {S 1} 上的设备系列 {S 2} 中移除。(事件 [{e}])

针对策略生成的事件

策略已启用/禁用

Event00821014:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 策略 {m} 已被 {u} 启用。(事件 [{e}])

Event00821015:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 策略 {m} 已被 {u} 禁用。(事件 [{e}])

Event00821023:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 策略 {S 1} 已被禁用。之前违反此策略所生成的任何警报都已清除。(事件 [{e}])

策略已修改

Event00821011:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 策略 {m} 已被 {u} 修改。(事件 [{e}])

策略具有违反者

Event00821012:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 策略 {m} 在格局 {S 1} 上存在违反者。(事件 [{e}])

Event00821013:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 策略 {m} 在格局 {S 1} 中不再有违反者。(事件 [{e}])

违反策略警报生成的事件

Event0082101d:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 策略 {m} 在格局 {S 1} 上存在违反者。此违反的重要级别是次要。(事件 [{e}])

Event0082101e:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 策略 {m} 在格局 {S 1} 上存在违反者。此违反的重要级别是主要。(事件 [{e}])

Event0082101f:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 策略 {m} 在格局 {S 1} 上存在违反者。此违反的重要级别是关键。(事件 [{e}])

针对全局同步、捕获、上传和写入启动等任务生成的事件

任务已排定/取消排定

Event00821040:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 任务已排定 - 已为格局 {S 2} 上的 {S 1} 排定 {t} 类型的任务 {m}。(事件 [{e}])

Event00821041:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 任务已取消排定 - 已在格局 {S 1} 上取消了 {t} 类型的任务 {m} 的排定。(事件 [{e}])

任务已启动、停止、完成、部分完成

Event00821042:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 任务已启动 - {S 1} 在格局 {S 3} 的 {I 2} 设备上启动了 {t} 类型的任务 {m}。(事件 [{e}])

Event00821043:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 任务正在停止 - {S 1} 停止了格局 {S 3} 上 {t} 类型的任务 {m}。(事件 [{e}])

Event00821045:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 任务已完成 - {t} 类型的任务 {m} 已完成，其中格局 {S 1} 上的所有设备均已得到处理。在总共 {I 2} 台设备中，{I 3} 台成功，{I 4} 台失败。(事件 [{e}])

Event00821044:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 任务已部分完成 - {t} 类型的任务 {m} 已完成，其中格局 {S 1} 上的 {I 5} 台设备未处理。对于总共 {I 2} 台设备，{I 3} 台成功，{I 4} 台失败，{I 5} 台未处理。(事件 [{e}])

任务部分完成警报生成的事件

Event00821046:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 任务已部分完成 - {t} 类型的任务 {m} 已完成，其中格局 {S 1} 上的 {I 5} 台设备未处理。对于总共 {I 2} 台设备，{I 3} 台成功，{I 4} 台失败，{I 5} 台未处理。已生成次要警报。(事件 [{e}])

Event00821047:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 任务已部分完成 - {t} 类型的任务 {m} 已完成，其中格局 {S 1} 上的 {I 5} 台设备未处理。对于总共 {I 2} 台设备，{I 3} 台成功，{I 4} 台失败，{I 5} 台未处理。已生成主要警报。(事件 [{e}])

Event00821048:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 任务已部分完成 - {t} 类型的任务 {m} 已完成，其中格局 {S 1} 上的 {I 5} 台设备未处理。对于总共 {I 2} 台设备，{I 3} 台成功，{I 4} 台失败，{I 5} 台未处理。已生成关键警报。(事件 [{e}])

在配置服务器应用程序上生成的事件

Event0082101a:{d "%w- %d %m-, %Y - %T"} 无法连接到配置管理器 - 无法连接到格局 {S 1} 上的 NCM 安全通信后台进程。(事件 [{e}])

Event0082101c:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 无法在存档目录中创建文件。无法存档设备配置。无法在格局 {S 2} 上的存档目录 {S 1} 中创建文件。(事件 [{e}])

Event00821052:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 与 ncmservice 后台进程的连接已被还原。(事件 [{e}])

未经请求的全局通知

Event0082102b:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 响应未经请求的配置更改通知的功能已在所有格局上全局禁用。(事件 [{e}])

Event0082102c:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 响应未经请求的配置更改通知的功能已在所有格局上全局启用。(事件 [{e}])

针对设备系列生成的事件

Event0082102d:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 设备系列 {m} 已启用/禁用 NCM。(事件 [{e}])

Event0082102e:{d "%w- %d %m-, %Y - %T"} 配置管理器 - 设备系列 {m} 已启用 NCM。(事件 [{e}])

附录 C： Network Configuration Manager 权限

本节列出了 OneClick 用户的 Network Configuration Manager 权限。默认情况下，启用每个权限。

注意：有关配置权限的详细信息，请参阅 *《管理员指南》*。

Network Configuration Manager

允许管理员配置 Network Configuration Manager 应用程序。这包括从“配置管理器”节点的“设备系列”节点中“信息”选项卡视图执行的配置，以及在单个设备级别上执行的 Network Configuration Manager 配置。这还包括排定全局同步任务的能力。

捕获主机配置

允许操作员从“主机配置”选项卡创建批量捕获任务或按需捕获。

在批准请求中隐藏配置更改

允许用户决定是否在工作流批准请求中包括配置内容。

在 NCM 任务中包含全局集合

允许用户使 Network Configuration Manager 任务与全局集合关联。通过有权访问集合，用户将隐式有权访问该集合中的所有成员。通过该访问权限，用户可以执行任何任务，包括在这些设备中上传配置和加载固件。

加载设备固件

允许操作员将固件上传到设备。

管理 NCM 任务

授予访问 Network Configuration Manager“任务”文件夹的权限。对该文件夹的访问权限将提供对所有 CA Spectrum 格局上所有 Network Configuration Manager 任务的全局访问，以及启动、停止、编辑和全部删除它们的能力。

重新加载设备

允许操作员将固件配置重新加载到设备。

修复设备

允许操作员为具有非遵从设备的策略上传指定的修复内容。

将主机配置保存到启动

允许操作员创建批量“保存到启动”任务。

排定重新加载

允许操作员对重新加载固件配置至设备进行排定。

排定 NCM 任务

允许操作员排定批量任务。

任务批准者

控制对批准工作流的批准授权。

ServiceDesk

如果“批准工作流模式”设置为“ServiceDesk”，且用户具有该权限，则通过 Service Desk 获取批准是可选的。

OneClick

如果“批准工作流模式”设置为“OneClick”，且用户具有该权限，则用户能够批准自己的任务或由他人启动的任务。

上传主机配置

允许操作员从“主机配置”选项卡创建批量上传任务或自动上传。

使用缓存设备身份验证

允许操作员使用在设备系列配置和单个设备覆盖配置中指定的用户名和密码。如果启用了该权限，则用户无须在每次启动任务时都输入用户名和密码。启动任务（例如，上传或保存到启动）时，如果禁用了该权限，则将提示用户进行设备身份验证。

注意：执行批量任务（如上传或保存到启动）时，如果没有该权限，则会提示操作员进行一次设备身份验证。然后，将该相同的身份验证数据用于为其执行批量操作的所有设备。

查看主机配置

允许操作员访问主机配置。

查看 NCM 策略

授予访问 Network Configuration Manager“策略”文件夹的权限。对该文件夹的访问权限将提供对所有 CA Spectrum 格局上所有 Network Configuration Manager 策略的全局访问，以及编辑、启用、禁用和全部删除它们的能力。

创建/编辑 NCM 策略

允许操作员创建新策略或编辑现有策略。该权限不允许用户启用策略。

启用/禁用 NCM 策略

允许操作员启用、禁用和删除 Network Configuration Manager 策略。

查看无掩码的配置

允许操作员查看被查看掩码遮蔽的内容。查看掩码位于设备系列上，可以在本地设备上进行覆盖。