密　　级：内部

文件编号：CS2C-安全策略工具-SSTD-V1.4

安全策略工具使用手册

编写人：黄仕伟	编写日期：2014 年 3 月 20 日
审核人：	审核日期：
批准人：	批准日期：

中标软件有限公司

版本说明

日期	版本号	发布说明	编写者	签批人		
				角色	人员	签字
2013/7/15	V1.0	安全策略工具使用手册V1.0	黄仕伟	开发人员		黄仕伟
2013/9/4	V1.1	安全策略工具使用手册V1.1	黄仕伟	开发人员		黄仕伟
2013/11/14	V1.2	安全策略工具使用手册V1.2	黄仕伟	开发人员		黄仕伟
2014/1/13	V1.3	安全策略工具使用手册V1.3	黄仕伟	开发人员		黄仕伟
2014/3/20	V1.4	安全策略工具使用手册V1.4	黄仕伟	开发人员		黄仕伟
2014/10/17	V1.4	安全策略工具使用手册V1.4	刘思华	开发人员		刘思华
				测试人员		
				QA		
				CM		

目 录

1. 产品简介

中标麒麟安全策略工具是中标软件有限公司开发一款策略工具，其目的是方便用户在中标麒麟安全操作系统 5U6 以及后续版本上快速创建安全策略模块、对系统已有的策略模块进行管理等。

1.1 项目背景

传统的安全操作系统策略开发方式都是由策略开发人员到客户现场开发安全策略。这种开发方式存在几个问题：1 需要出差到客户现场，开发成本高 2 后期维护不方便，当客户需要添加其它应用，客户无法自行添加该应用的策略模块，策略开发人员又要到现场进行开发。基于以上几点，我们开发了这一套安全策略工具。

2. 安全策略工具功能介绍

安全策略工具功能模块包括查看系统默认策略模块，创建策略模块，查看策略模块创建记录这三个功能。

2.1 查看系统策略功能

首先，使用 secadm 用户登录安全操作系统，点击桌面上的安全策略工具按钮。

弹出如下界面，新版本的安全策略工具主界面，左侧有两个选项，“默认策略”和“创建策略”，采用鼠标滑动方式进行显示。

图 2-1

如图 2.1，为安全策略工具主界面，点击“默认策略”，弹出如下界面。

图 2.2

如图 2.2，点击“系统默认策略”按钮，即弹出当前安全操作系统已经装载的策略模块。默认为显示所有类型的策略模块，点击“全部”，出现下拉菜单，根据分类显示策略模块。

点击“策略分类”下拉框，对系统策略类型进行分类，可分为四类：数据库、中间件、应用程序、系统组件。

按策略类型进行分类，如图 2-4,在策略分类中选择“中间件”。

图 2-4

在“请输入模块名”的输入框中，输入模块名或是模块版本号,再按回车键，即进行搜索如下图

图 2-6

2.2 创建策略功能

安全策略工具很重要的一个功能就是创建安全策略模块，将鼠标滑动至图 2-1 中的“创建策略”，弹出如下界面

图 2-7

单击上图中“创建策略模块”，弹出如下界面，即开始安全策略模块的创建，首先选择应用程序类型，用户先判断需要添加的策略模块属于哪种类型。其次，填写策略模块的名称，当填入的名称已经在系统中存在时，系统则会弹出提示框，提示用户命名的模块已经在策略中存在。

策略模块类型分为“应用程序”，“数据库”，“中间件”，“系统组件”四类。

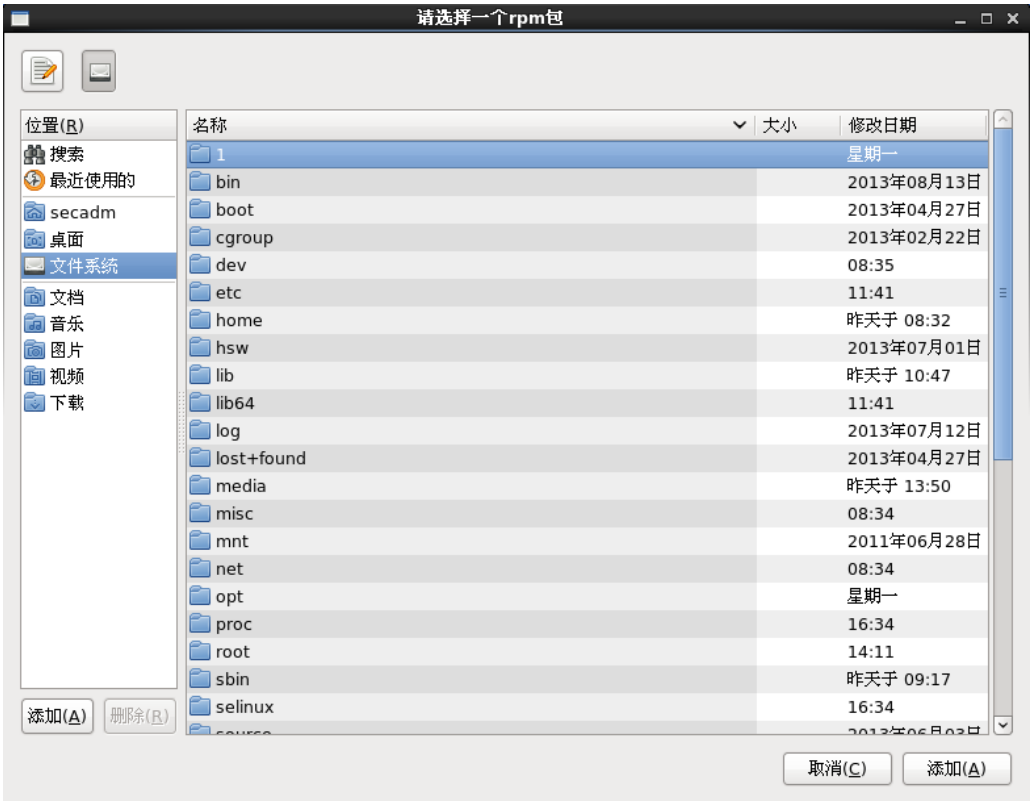
策略运行模式分为“强制模式”和“许可模式”，强制模式是指该策略模块运行于 enforcing 状态下，许可模式是指该策略模块运行 permissive 状态下。

输入策略模块名，点击“下一步”，弹出如下界面。

安全策略工具可以为两类应用程序创建策略，一类为 rpm 包，还有一类为直接对安装目录下的文件进行标记，不可选择/home、/etc、/tmp 目录。

图 2-8

当要为 rpm 包创建安全策略，可以通过两种方式确定 rpm 包名，一种是在输入框中直接输入 rpm 包名，如”mysql”,还有两一种方法是通过浏览按钮，找到 rpm 包



选择需要为其配置策略的 rpm 包，点击“添加”按钮

图 2-9

下一步，单击图 2-10 中的前进按钮，出现如下界面，如图 2-12,应用程序具体列表，系统会把用户选择的 rpm 文件或是用户指定目录下的所有文件进行分类，类别有：可执行、函数、配置、日志、tmp 文件等，用户也可以在此手动添加文件。

图 2-11

单击图 2-11 中的“前进“按钮，进入下一步，如图 2-12,在安全操作系统中存在着许多默认角色，这里只选择最常用的 4 个角色可以关联，sysadm_r, secadm_r,auditadm_r,user_r, 选择关联了哪个角色，则意味只有该角色对应的用户可以在 SELinux 为 enforcing 时可以运行该应用程序，在此，选择的是 sysadm_r 角色，即 root 用户可以操作 MySQL 这个应用程序。

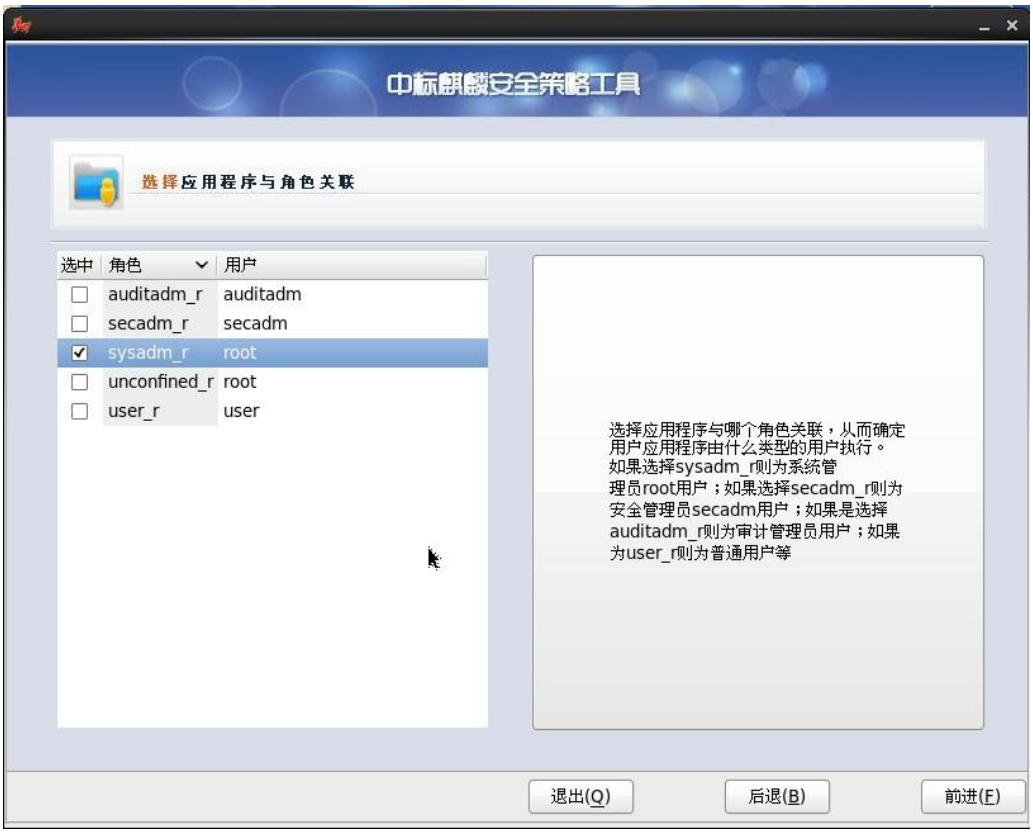


图 2-12

单击图 2-12 中“前进”按钮，进入下一步，如图 2-13。这一步是生成策略文件，点击“应用”按钮，策略工具则在后台生成策略文件，请等待一段时间。

图 2-13

点击“应用”按钮，系统后台正在生成策略模块，约过 10 几秒钟，如果策略生成并成功加载，则弹出框，上面显示，如果策略生成失败，则弹出框，

图 2-14

图 2-15

2.3 查看策略创建历史功能

用户想查看自己通过策略工具创建了哪一些模块时，可以单击图 2-7 中“查看模块创建记录”功能，

模块名	版本	安装路径	策略类型	创建时间	是否加载
vb	1.0.0		系统组件	2013-11-13 17:19:50	否
vb	1.0.0		系统组件	2013-11-13 16:38:33	否
vb	1.0.0		系统组件	2013-11-13 09:22:07	否
vb	1.0.0		系统组件	2013-11-13 09:06:31	否
vb	1.0.0		系统组件	2013-11-12 14:01:40	否
vb	1.0.0		系统组件	2013-11-12 13:51:49	否
hsw01	1.0.0		数据库	2013-11-12 13:24:20	否
vb	1.0.0		系统组件	2013-11-12 08:53:26	否
vb	1.0.0		应用程序	2013-11-10 15:32:51	否
vb	1.0.0		应用程序	2013-11-10 15:29:36	否
hsw01	1.0.0	/opt/CVICSE/InforSuite/AppServer	系统组件	2013-11-06 17:16:45	否
vb	1.0.0	/opt/TongWeb5.0	应用程序	2013-11-05 17:57:36	否
vb	1.0.0		系统组件	2011-05-01 16:18:17	否
vb	1.0.0		系统组件	2013-10-29 10:14:59	否
hsw01	1.0.0		数据库	2013-10-29 09:19:44	否
vb	1.0.0		应用程序	2013-10-28 17:05:32	否

可按类型进行查看，如在类型中，选择“中间件“，出现如图 2-17

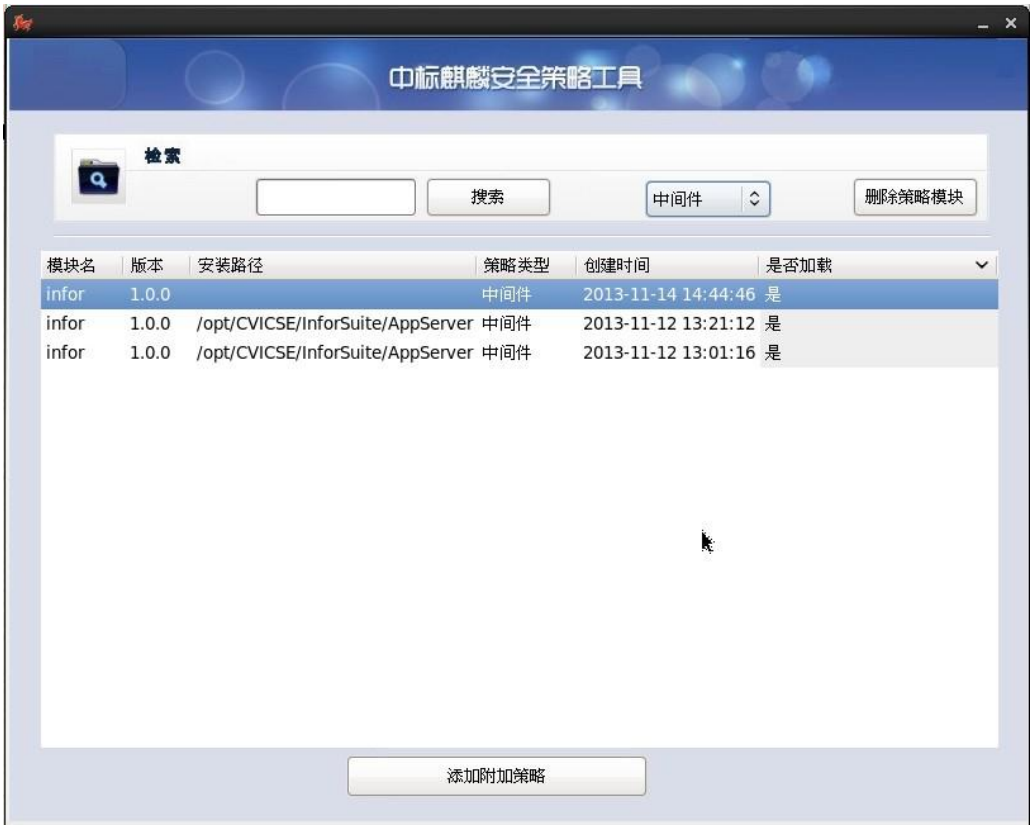


图 2-17

按模块名称或是版本号进行搜索，在搜索框中输入要搜索内容，如下图 2-18

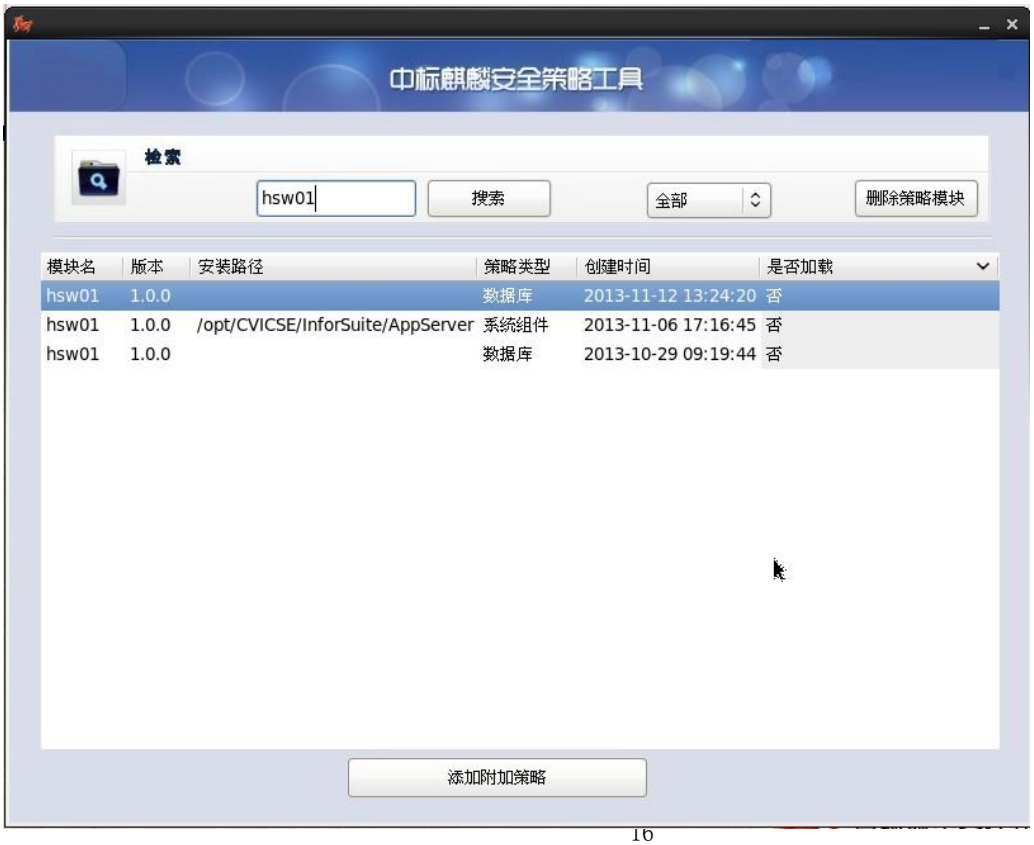


图 2-18

生成附加策略：已经通过策略工具生成了策略模块，但在 SELinux 状态为 enforcing 时，应用程序还是无法正常运行，此时，使用 secadm 用户登陆系统，把 SELINUX 状态设置为 permissive，命令为$setenforce 0。再使用 auditadm 用户登录系统，清除审计日志和重启审计服务，命令为$rm –rf /var/log/audit/* $/etc/init.d/auditd restart。再使用操作该应用程序的用户登录系统，执行应用程序的所有功能，再单击“生成附加策略“，需要等待一会儿，弹出如下界面，如图 2-19

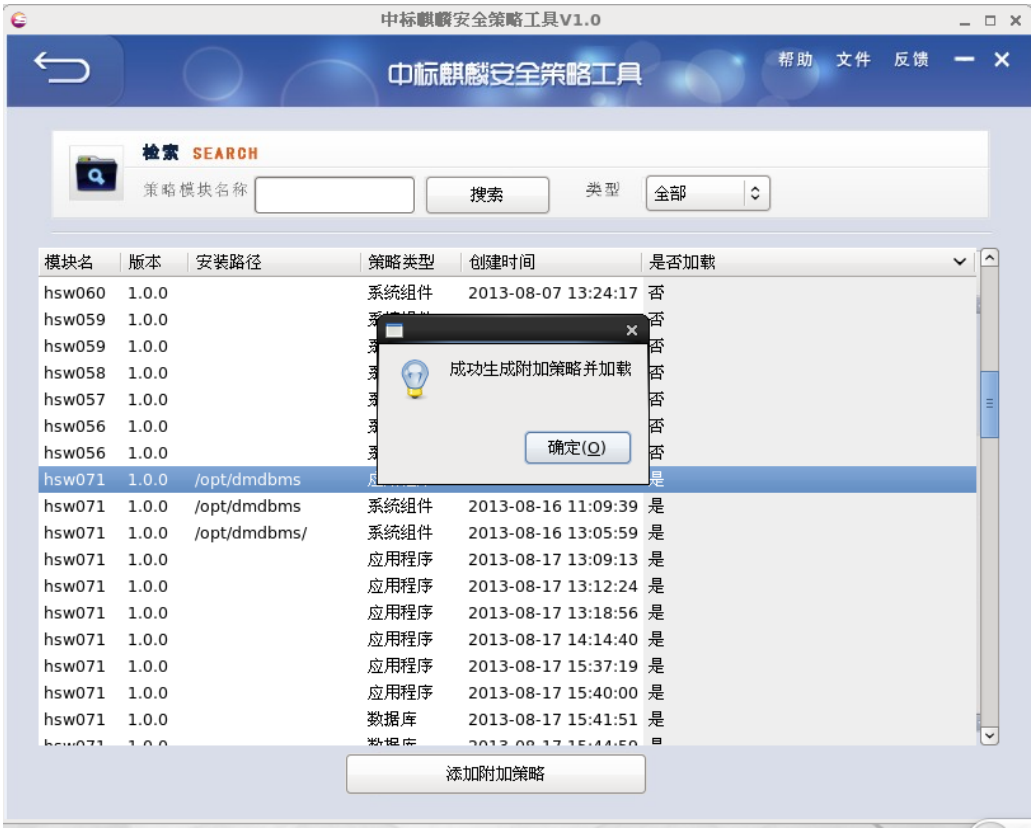


图 2-19