中标麒麟可信操作系统 V6.0

审计管理员手册

中标软件有限公司

上海市徐汇区番禺路 1028 号数娱大厦 10 层（200030）

北京市海淀区北四环西路 9 号银谷大厦 20 层（100190）

广州市天河北路 898 号信源大厦 16 层 1604 室（510898）

目　录

中标麒麟最终用户使用许可协议

尊敬的中标麒麟用户：

首先感谢您选用由中标软件有限公司开发并制作发行的中标麒麟产品。

请在打开本软件介质包之前，仔细阅读本协议条款以及所提供的所有补充许可条款（统称“协议”）。一旦您打开本软件介质包，即表明您已接受本协议的条款，本协议将立即生效，对您和本公司双方具有法律约束力。

1. 使用许可

按照已为之支付费用的用户数目及计算机硬件类型，中标软件有限公司（下称“中标软件”） 向您授予非排他、不可转让的许可，仅允许内部使用由中标软件提供的随附软件和文档以及任何错误纠正（统称“本软件”）。

— 软件使用许可

在遵守本协议的条款和条件的情况下，中标软件给予贵机构非独占、不可转让、有限的许可，允许贵机构至多使用软件的五（5）份完整及未经修改的二进制格式副本，而此种软件副本仅可安装于贵机构操作的电脑中。

— 教育机构使用许可

在遵守本协议的条款和条件的情况下，如果贵机构是教育机构，中标软件给予贵机构非独占、不可转让的许可，允许贵机构仅在内部使用随附的未经修改的二进制格式的软件。此处的“在内部使用”是指由在贵机构入学的学生、贵机构教员和员工使用软件。

— 字型软件使用

软件中包含生成字体样式的软件（“字型软件”）。贵机构不可从软件中分离字型软件。贵机构不可改动字型软件，以新增此等字型软件被作为软件的一部分交付予贵机构时所不具备的任何功能。贵机构不可将字型软件嵌入作为商业产品提供以换取收费或其他报

酬的文件。

2. 限制

本软件受到版权（著作权）法、商标法和其他法律及国际知识产权公约的保护。中标软件和/或其许可方保留对本软件的所有权及所有相关的知识产权。对于中标软件或其许可方的任何商标、服务标记、标识或商号的任何权利、所有权或利益，本协议均不作任何授权。

3.关于复制、修改及分发

如果在所有复制品中维持本协议书不变，您可以且必须根据《GNU GPL-GNU 通用公共许可证》复制、修改及分发中标麒麟产品中遵守《GNU GPL-GNU 通用公共许可证》协议的软件，其他不遵守《GNU GPL-GNU 通用公共许可证》协议的中标麒麟产品必须根据符合相关法律之其他许可协议进行复制、修改及分发，但任何以中标麒麟产品为基础的衍生发行版未经中标软件有限公司的书面授权不能使用任何中标软件有限公司的商标或其他任何标志。

特别注意：该复制、修改及分发不包括本产品中包含的任何不适用《GNU GPL-GNU 通用公共许可证》的软件，如中标麒麟产品中包含的输入法软件、字库软件、第三方应用软件等。除非适用法律禁止实施，否则您不得对上述软件进行复制、修改（包括反编译或反向工程）、分发。

4. 有限担保

中标软件向您担保，自购买之日起九十（90）天内（以收据副本为凭证），本软件的存储介质（如果有的话）在正常使用的情况下无材料和工艺方面的缺陷。除上述内容外，本软件按“原样”提供。在本有限担保项下，您的所有补偿及中标软件的全部责任为由中标软件选择更换本软件介质或退还本软件的购买费用。

5. 担保的免责声明

除非在本协议中有明确规定，否则对于任何明示或默示的条件、陈述及担保，包括对适销性、对特定用途的适用性或非侵权性的任何默示的担保，均不予负责，但上述免责声

明被认定为法律上无效的情况除外。

6. 责任限制

在法律允许范围内，无论在何种情况下，无论采用何种有关责任的理论，无论因何种方式导致，对于因使用或无法使用本软件引起的或与之相关的任何收益损失、利润或数据损失，或者对于特殊的、间接的、后果性的、偶发的或惩罚性的损害赔偿，中标软件或其许可方均不承担任何责任（即使中标软件已被告知可能出现上述损害赔偿）。根据本协议，在任何情况下，无论是在合同、侵权行为（包括过失）方面，还是在其他方面，中标软件对您的责任将不超过您就本软件所支付的金额。即使上述担保未能达到其基本目的，上文所述的限制仍然适用。

7. 终止

本协议在终止之前有效。您可以随时终止本协议，但必须销毁本软件的全部正本和副本。如果您未遵守本协议的任何规定，则本协议将不经中标软件发出通知立即终止。终止时，您必须销毁本软件的全部正本和副本。

8. 管辖法律

与本协议相关的任何诉讼均受适用的中华人民共和国法律管辖。任何其它国家和地区的选择法律的规则不予适用。

9. 可分割性

如果本协议中有任何规定被认定为无法执行，则删除相应规定，本协议仍然有效，除非删除防碍各方愿望的实现（在这种情况下，本协议将立即终止）

10. 完整性

本协议是您与中标软件就其标的达成的完整协议。它取代此前或同期的所有口头或书面往来信息、建议、陈述和担保。在本协议期间，有关报价、订单、回执或各方之间就本协议标的进行的其他往来通信中的任何冲突条款或附加条款，均以本协议为准。对本协议的任何修改均无约束力，除非通过书面进行修改并由每一方的授权代表签字。

11. 商标和标识

贵机构承认并与中标软件有着以下共识，即中标软件拥有中标软件、中标麒麟商标，以及所有与中标软件、中标麒麟相关的商标、服务标记、标识及其他品牌标识（“中标软件标记”）。贵机构对中标软件标记的任何使用都应有利于中标软件。

12. 源代码

本软件可能包含源代码，其提供之唯一目的是在符合本协议条款之规定时供参考之用。源代码不可再分发，除非在本协议中有明确规定。

13. 因侵权而终止

如果本软件成为或在任一方看来可能成为任何知识产权侵权索赔之标的，则任一方可立即终止本协议。

14. Java 技术限制

贵机构不可更改“Java 平台界面”（简称“JPI”，即指明为“java”包或“java”包的任何子包中的类），无论通过在 JPI 中创建额外的类，还是通过其他方式导致对 JPI 中的类进行增添或更动，均为不可。如果贵机构创建一个额外的类以及一个或多个相关的 API，而它们（i）扩展 Java 平台的功能；并且（ii）可供第三方软件开发者用于开发可调用上述额外 API 的额外软件，则贵机构必须迅即广泛公布对此种 API 的准确说明，以供所有开发者免费使用。贵机构不可创建、或授权贵机构的被许可人创建以任何方式标示为“java”、“javax”、“sun”的额外的类、界面、子包或 Sun 在任何命名约定中指明的类似约定。参见 Java 运行时环境二进制代码许可的适当版本（目前位于 http://www.java.sun.com/jdk/index.html），以了解可与 Java 小程序和应用程序共同分发的运行时代码的可供情况。

中标麒麟可信操作系统 V6.0 产品介绍

为满足政府、国防、金融、电力、机要、保密等领域对操作系统的高安全性需求，中标软件有限公司（以下简称“中标软件”）基于多年来在操作系统安全和可信计算方面的技术积累，研制推出了国内首款自主可控、高安全等级的可信操作系统软件产品-中标麒麟可信操作系统 V6.0。

结合可信计算技术和操作系统安全技术，中标麒麟可信操作系统 V6.0 通过信任链的建立及传递实现对平台软硬件的完整性度量；提供基于三权分立机制的多项安全功能(身份鉴别、访问控制、数据保护、安全标记、可信路径、安全审计等)和统一的安全控制中心；全面支持国内外可信计算规范（TCM/TPCM、TPM2.0）；兼容主流的软硬件和自主 CPU 平台；提供可持续性的安全保障，防止软硬件被篡改和信息被窃取，系统免受攻击；为业务应用平台提供全方位的安全保护，保障关键应用安全、可信和稳定的对外提供服务。

中标软件还提供基于 Linux 操作系统的安全评估、安全优化、安全加固等安全服务和系统安全定制开发业务。

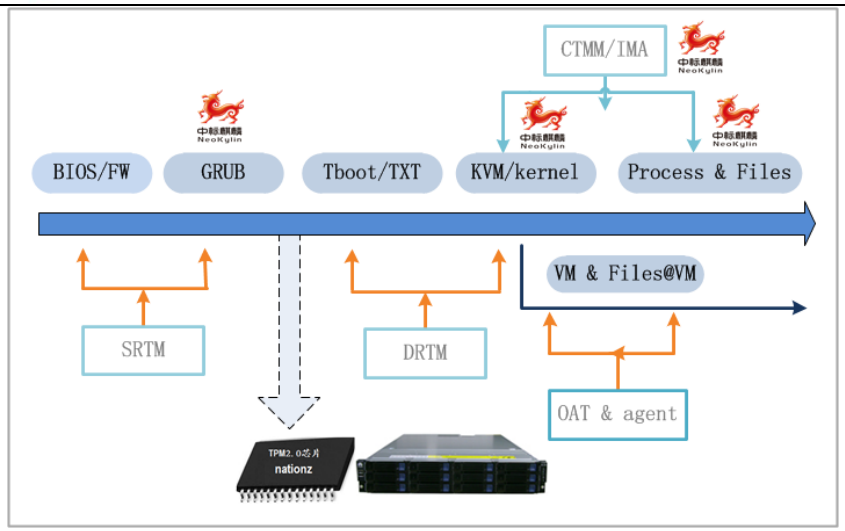
主要特性

■ 操作系统高安全等级

中标麒麟可信操作系统 V6.0 严格遵照可信计算技术规范（TCM/TPCM、TPM2.0）、GB/T 20272-2006 技术要求和国际 CC 标准等进行研制开发。通过操作系统安全的国家标准 GB/T 20272-2006 第四级（结构化保护级）测评认证并获得销售许可。

■ 可信计算实现内核级

国内首款全面支持 TCM/TPCM 和 TPM2.0 可信计算规范的可信操作系统，支持通用和专用可信密码芯片/模块；基于中标软件可信度量模块 CTMM（CS2C Trusted Measure Module）提供可信引导、可信启动和可信运行控制等功能；通过信任链的创建传递过程，实现对平台软硬件的完整性度量；提供基于可信芯片的上层可信功能和图形化的可信管理中心；并实现信任链从物理主机到虚拟化平台的拓展，提供对虚拟机的完整性度量。



■ 安全功能和机制全面

基于 LSM 的安全子系统框架，提供基于三权分立机制的多项安全功能，包括身份鉴别、自主访问控制、强制访问控制、数据机密性和完整性保护、安全标记、可信路径、安全审计等。针对不同的应用场景，系统支持细粒度的强制访问控制 SELinux 和轻量级强制访问控制 SMACK。

■ 系统管理配置灵活

内置主流数据库、中间件和应用服务器的安全策略，同时提供多种图形化安全策略配置和管理工具；基于图形化的安全控制中心实现系统安全可信功能模块化的集中配置和管理，界面友好，简洁易用；用户可以方便快捷完成系统的安全管理。

■ 良好的兼容性

中标麒麟可信操作系统 V6.0 适用于从服务器应用到桌面办公等各种环境，支持各类通用和专业应用；并内置默认的安全策略，实现系统安全和易用的结合，具有良好的软、硬件兼容性。系统支持 64 位应用程序，提供丰富的硬件驱动程序，中标软件有限公司还可协助第三方硬件厂商完成驱动程序的研发和移植，实现专用和特定硬件设备的支持。

系统要求

512MB 物理 RAM（推荐使用 1G 以上 RAM）

5G 以上可用磁盘空间

800x600 以上显示分辨率（推荐采用 1024x768 或更高分辨率）

硬件平台

Intel x86-64（AMD64）

自主 CPU 平台（龙芯、申威、兆芯、众志、Arm64 等）

获得更多的信息

如果出现了本手册不能解决的问题，可以通过如下的方式获得帮助：

阅读和打印 man 页以及 info 页。（man 页和 info 页是系统文档，可以帮助您了解系统提供了哪些可用命令以及如何使用它们）；

- 使用 GNOME 帮助浏览器；
- 登录 www.cs2c.com.cn 网站，查阅相关资料。

技术支持

请您按照中标麒麟可信操作系统 V6.0 产品包装或以下联系方式获取中标软件提供的技术支持服务，包括：

- 所有服务均以远程方式执行；
- 产品安装支持；
- 5＊8 小时电话，邮件，网站、传真等支持；
- 同版本补丁升级服务；
- 远程电话、邮件、网站、传真等支持服务只针对中标麒麟相关产品的安装、使用的问题提供支持，不包含对第三方软硬件的支持服务；
- 服务期按照合同规定起止日期内提供服务。

如果您有其它额外的技术支持需求，请致电中标软件有限公司，我们承诺为您提供优质的服务。

公司网址：www.cs2c.com.cn

客户热线：400-706-1825

电子邮件：support@cs2c.com.cn

公司电话：上海（021）51098866　　北京（010）51659955　广州（020）38182526

公司传真：上海（021）51062866　　北京（010）62800607　广州（020）38182529

第 1 章 安全审计

1.安全审计

审计（audit）是 Linux 系统中保障系统安全的一个重要组件。审计服务能实时、全面地记录对文件、文件夹、系统资源的访问、系统调用情况。通过指定有效的审计规则，所有对系统安全存在风险的事件都会被记录在案。方便审计管理员事先的防范和事后的调查取证。安全控制中心的安全审计模块提供图形化的界面，协助操作系统审计管理员查看、查询相关审计日志、审计报表，设计审计规则，提供系统告警服务等。

安全审计与安全数据库系统结合，提供进程级独立安全审计功能，包括提供审计日志、实时报警生成，潜在侵害分析、基于异常检测，基本审计查阅、有限审计查阅和可选审计查阅，安全审计事件选择，受保护的审计踪迹存储，审计数据的可用性确保，审计数据的安全备份以及审计数据的访问控制等功能。

审计相关术语如下：

审计进程：审计进程是指由 auditd 命令运行后产生的 auditd 无交互后台守护进程（audit daemon）。

审计配置文件：审计服务的配置文件是指/etc/audit/auditd.conf。

审计规则文件：审计规则文件是指/etc/aduit/audit.rules。该文件以命令参数的形式记录审计规则，审计进程启动时会读取该文件自动加载。管理员也可以在审计进程启动后，动态添加审计规则。

审计日志文件:审计日志文件是指/var/log/audit/audit.log。它以文本形式记录下匹配审计规则的所有事件。用户也可以在审计配置文件中另外指定日志文件的位置。

1.1 使用说明

安全审计包含两个部分：系统审计管理和系统告警管理。

安装好中标麒麟可信操作系统 V6.0 以后，用审计管理员用户登录系统，点击系统的启动项，选择系统工具->中标麒麟安全控制中心，弹出如下图所示界面：

图 1-1 安全控制中心启动界面

单击安全审计图标，出现如下图所示界面：

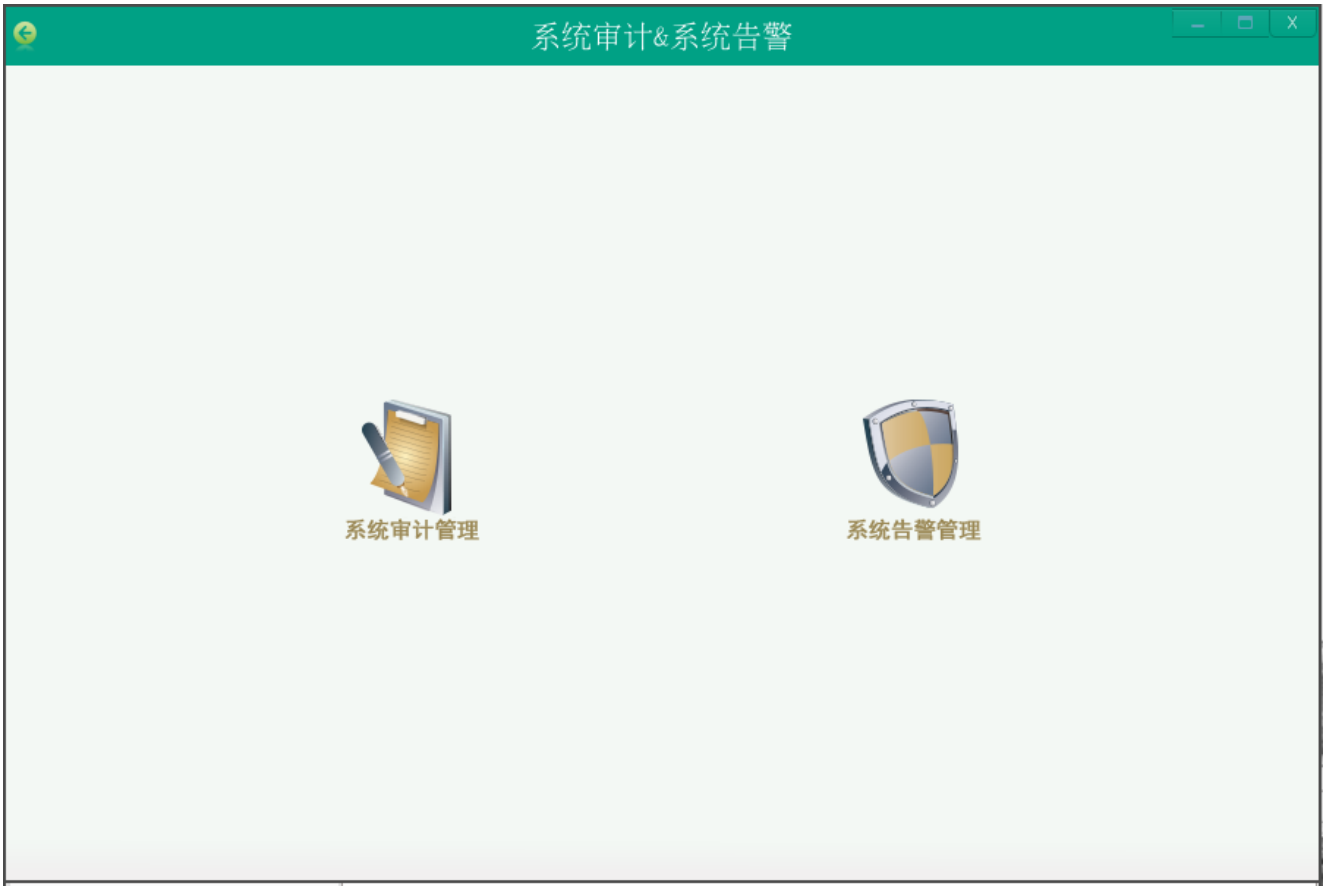


图 1-2 安全控制中心主界面

此界面是安全审计的主界面，可以看到安全审计主要有两大功能块：系统审计管理和系统告警管理。

1.2 系统审计管理

系统审计管理功能分为三个部分：审计信息、审计报表和审计规则。如图 1-3 所示。

图 1-3 审计信息界面

1.2.1 审计信息

审计信息模块显示如图 1-3 所示。若选中全选，则表格第一列的复选框都被选中，若点击取消，则表格第一列的复选框全被取消选中。审计类型左边的控件可以选择要查询的审计类型，审计类型有三种：登录信息、AVC 和 CTMM，可以选择一种类型，也可以选择两种或多种类型查询。时间区间有五种：当天、最近一周、最近两周、最近一个月、最近三个月。若选中高级查询，则出现需要输入高级查询的条件框：审计内容查询和审计时间查询，如图 1-4 所示。点击查询按钮，则表格显示输入查询条件后的审计内容，查询条件有审计类型、审计时间和审计内容。若直接点击删除按钮，则界面提示请选择需要删除的行，如图 1-5 所示，若选择需要删除行的复选框，则界面提示您已删除选中的行，可以选择多行同时删除，如图 1-6 所示，删除的数据不仅在表格里面删除，后台数据库也同时删除。

图 1-4 带有高级查询的审计信息界面

图 1-5 删除提示

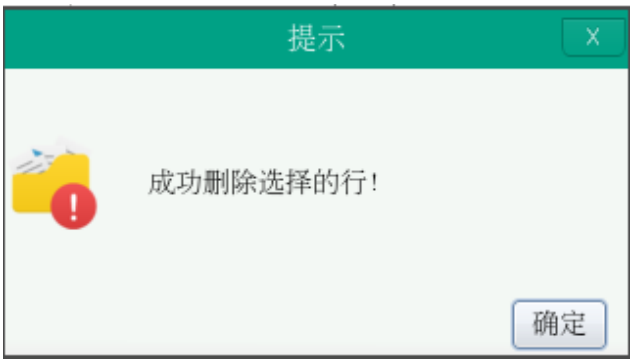


图 1-6 删除成功提示

对表格的每行数据点击右键，显示查看详情和删除两个功能键，点击删除，则此行数据被删除。点击查看详情，弹出显示此行数据详细信息的对话框，如图 1-7 所示，此对话框显示当前点击行的审计时间、审计类型和审计内容，点击下一条，相应的显示框显示下一条表格数据，同时主界面表格相应的下一条数据变呈选中状态，如图 1-8 所示。若已经是最后一条数据，则提示已经是最后一条数据，点击上一条类推，若已经是第一条数据，则提示已经是第一条数据。

鼠标浮上表格的每一行数据，会出现一个框，显示此行的审计内容。

图 1-7 查看详情对话框

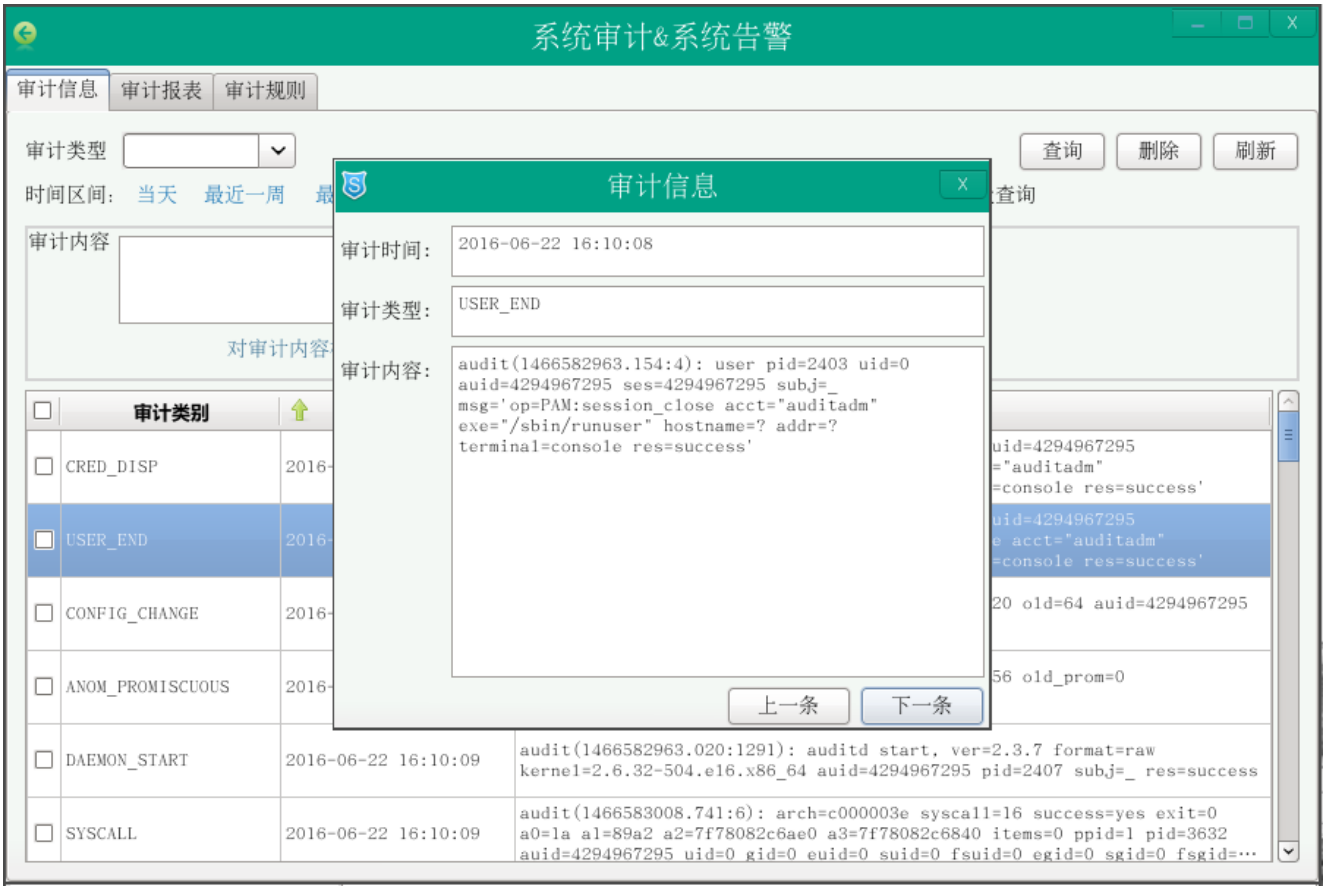


图 1-8 点击下一条界面显示

1.2.2 审计报表

点击审计报表，出现如图 1-9 和图 1-10 所示界面，这是登录信息、AVC 信息和 CTMM 信息的图表统计显示方式。如图 1-9 登录信息显示，绿色代表登录成功，红色代表登录失败，点击图 1-9 中登录信息，页面跳转到如图 1-11 所示页面。

图 1-9 登录信息和 AVC 信息显示

如图 1-10CTMM 信息显示，绿色代表允许，红色代表阻止，紫色代表度量成功，枚红色代表度量失败。

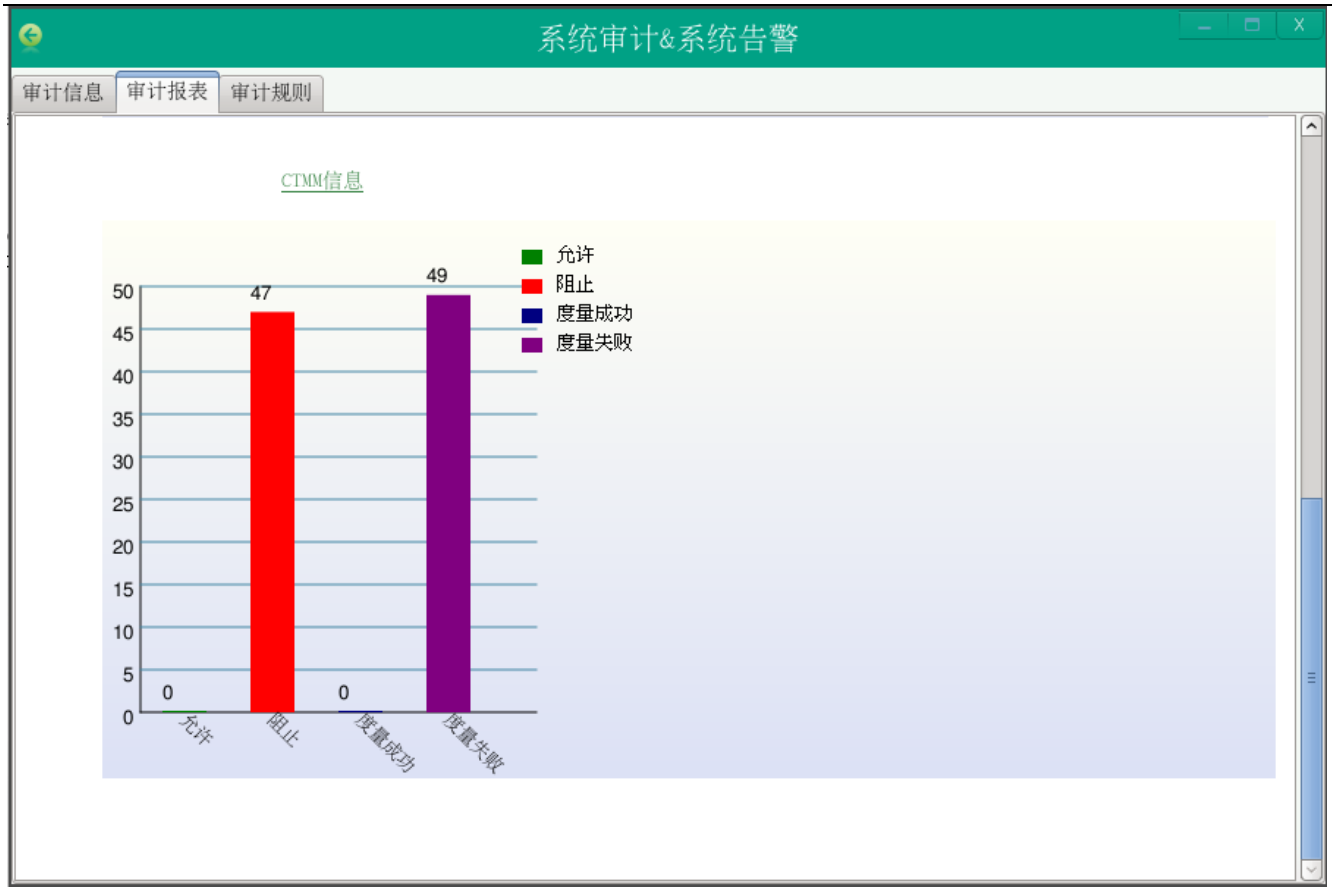


图 1-10 CTMM 信息显示

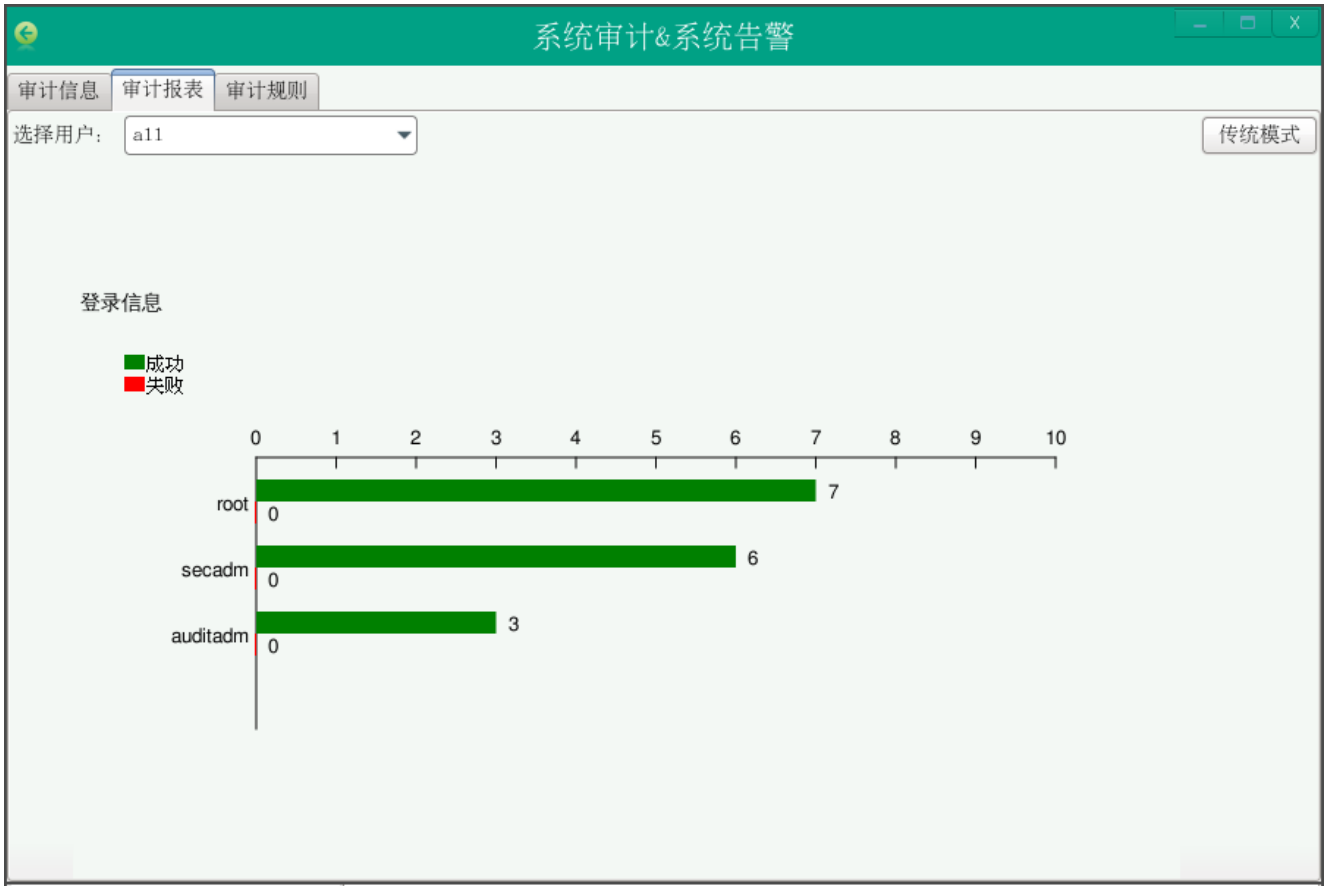


图 1-11 登陆信息

AVC 信息绿色代表允许，红色代表阻止。点击图 1-9 中 AVC 信息，界面跳转到如图 1-12 所示。

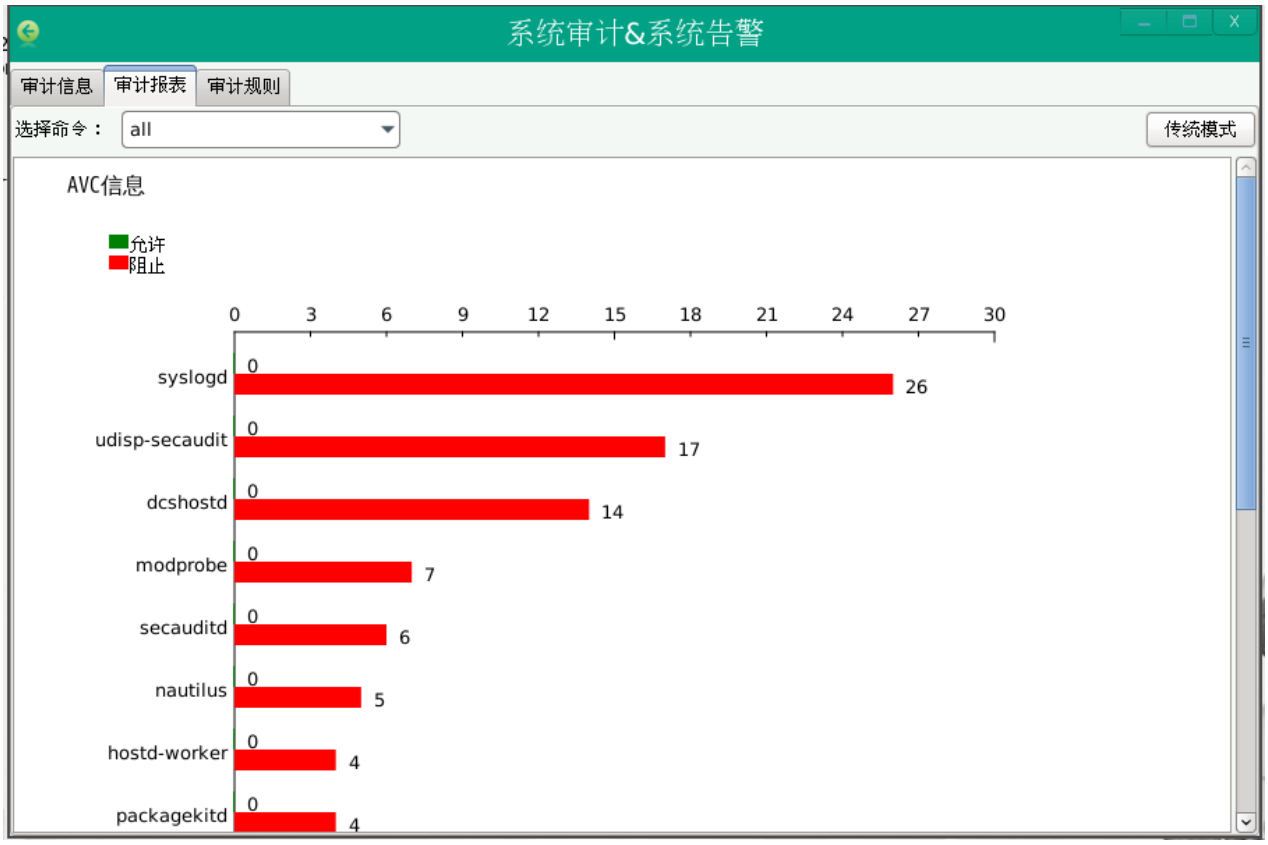


图 1-12 AVC 信息

点击图 1-10 中 CTMM 信息，页面跳转到如图 1-13 所示页面。页面显示了可执行程序的 CTMM 信息。

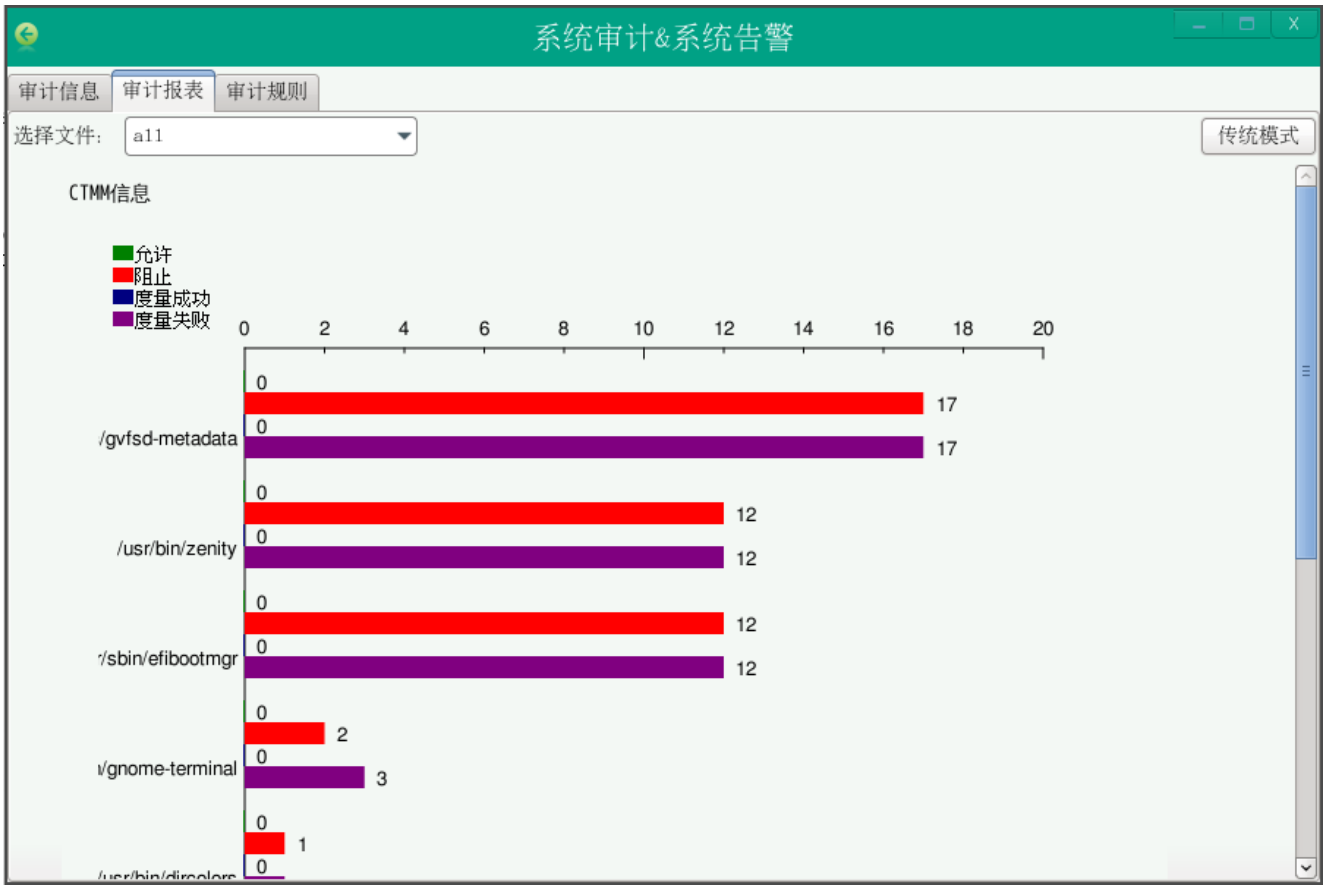


图 1-13 可执行程序的 CTMM 信息

点击图 1-9 中传统模式按钮，界面跳转到显示表格的页面，如图 1-14 所示。

图 1-14 审计报表的传统模式显示

传统模式以表格形式显示，表格里面分别显示了登录信息、AVC 信息和 CTMM 信息，分别点击第一列左边的小图标，显示每一个类型的详细信息，点击 LOGIN 左边的图标，显示 LOGIN 的具体信息，如图 1-15 所示。点击 LOGIN 表格的每一行，表格上方显示用户的登录信息。选择用户后面的控件可以选择用户，若选择 root 用户，表格显示 root 用户的详细信息，若选择 auditadm 用户，则表格显示 auditadm 用户的详细信息。

图 1-15 LOGIN 详细信息显示

点击图 1-14 中 AVC 左边的图标，显示如图 1-16 所示。表格一共有四列：用户、操作、操作结果和时间。

图 1-16 AVC 信息的表格显示

点击图 1-14 中 CTMM 左边的图标，显示如图 1-17 所示，表格显示有文件路径、度量结果、访问控制结果和时间四列。

图 1-17 CTMM 信息的表格显示

1.2.3 审计规则

点击审计规则标签页，界面显示如图 1-18 所示。

图 1-18 审计规则界面显示

如图所示，审计规则设置有五个选项：监控目录设置、监控文件设置、监控用户设置、监控进程设置和过滤日志信息。点击审计规则选项，界面默认选中监控目录设置框，用户可以对想要监控的目录进行设置，如点击右边的图标选中想要监控的目录，并可以对目录的权限进行选择，读、写、执行或者修改，可以输入关键字标识，设置好以后，点击应用规则，则设置好的信息会显示在下面的表格中，设置成功以后，界面会提示审计规则设置成功，如图 1-19 所示。规则设置成功以后，被监控的目录如果有任何操作，都会被记录在审计日志文件 audit.log 中。对表格中的每行点击右键，显示删除操作，点击删除，可以将该行数据删除。点击清空规则，表格中的数据将被清空，同时审计日志文件里添加的这条规则将被删除。

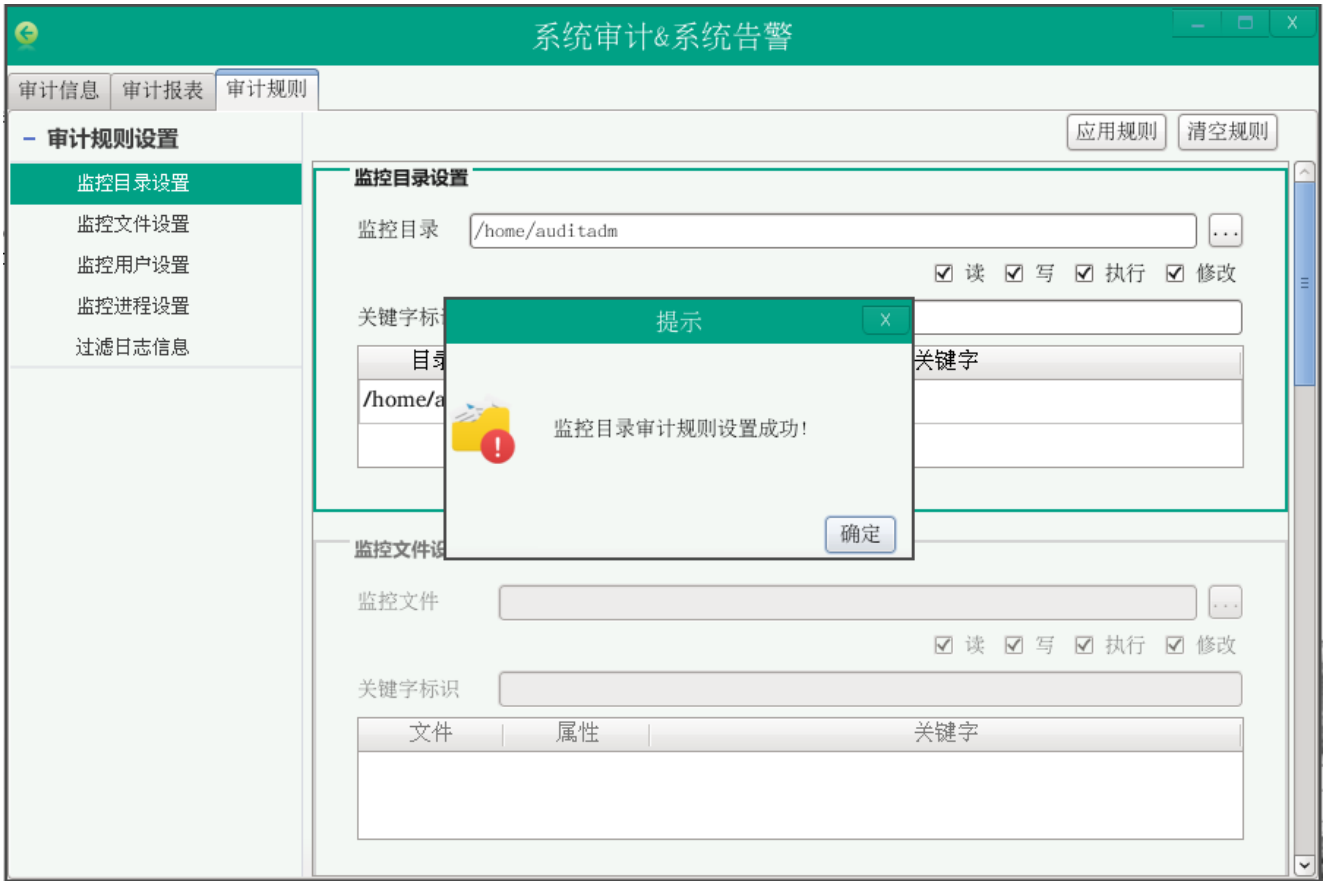


图 1-19 审计规则设置成功

若监控目录为空，界面提示监控路径不能为空，如图 1-20 所示。

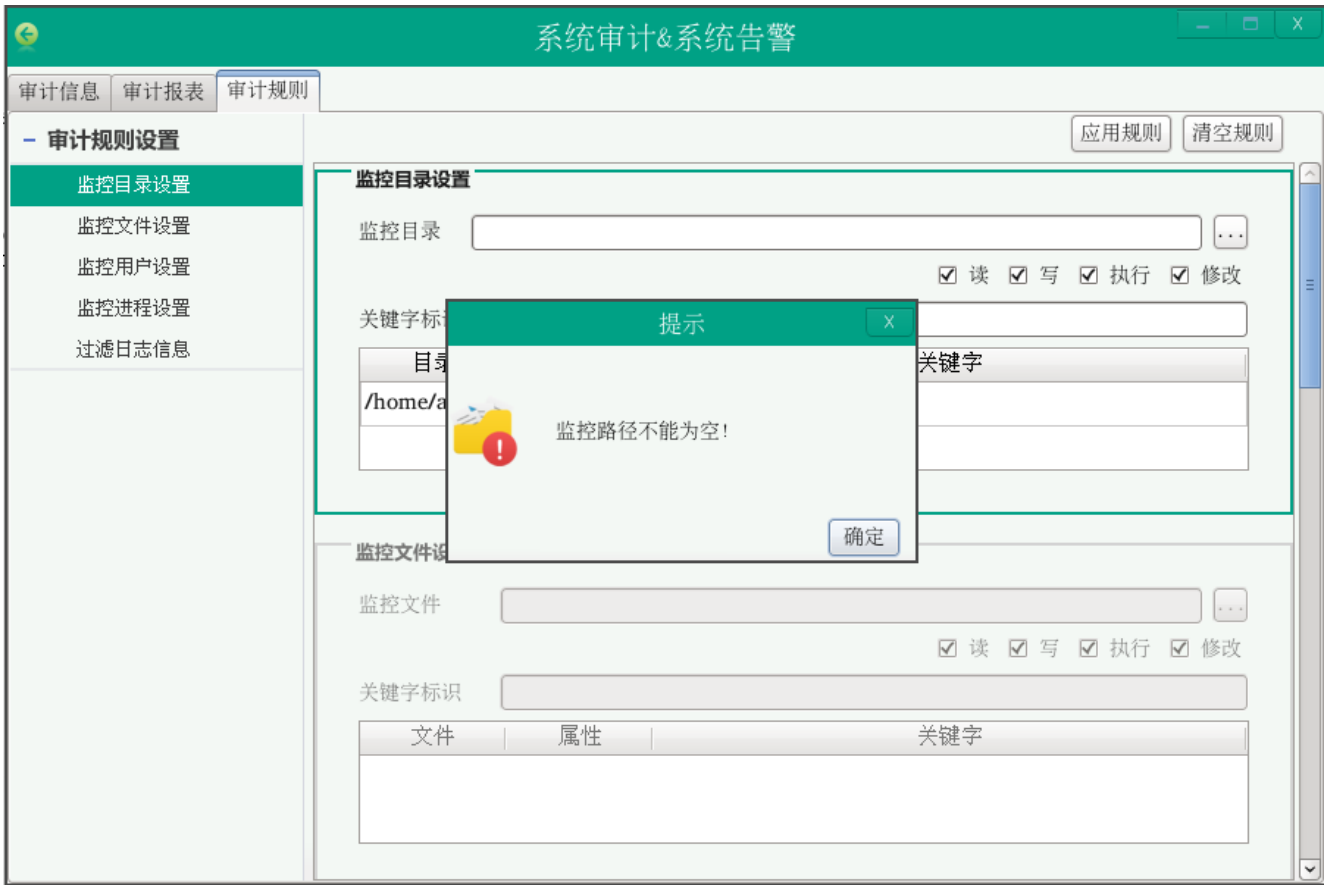


图 1-20 监控目录信息页面

选择监控设置项可以通过点击左边的目录选择，也可以通过滑动滚动条选择。设置完监控目录以后，可以设置监控文件，原理与设置监控目录是一样的。监控用户设置输入用户名、系统调用，系统调用意思是用户做了哪些操作，比如打开了某个软件，输入了哪些命令，输入用户名和系统调用以后，点击应用规则，界面提示审计规则设置成功，表格里插入一条数据，显示输入的用户名和系统调用。如图 1-21 所示。

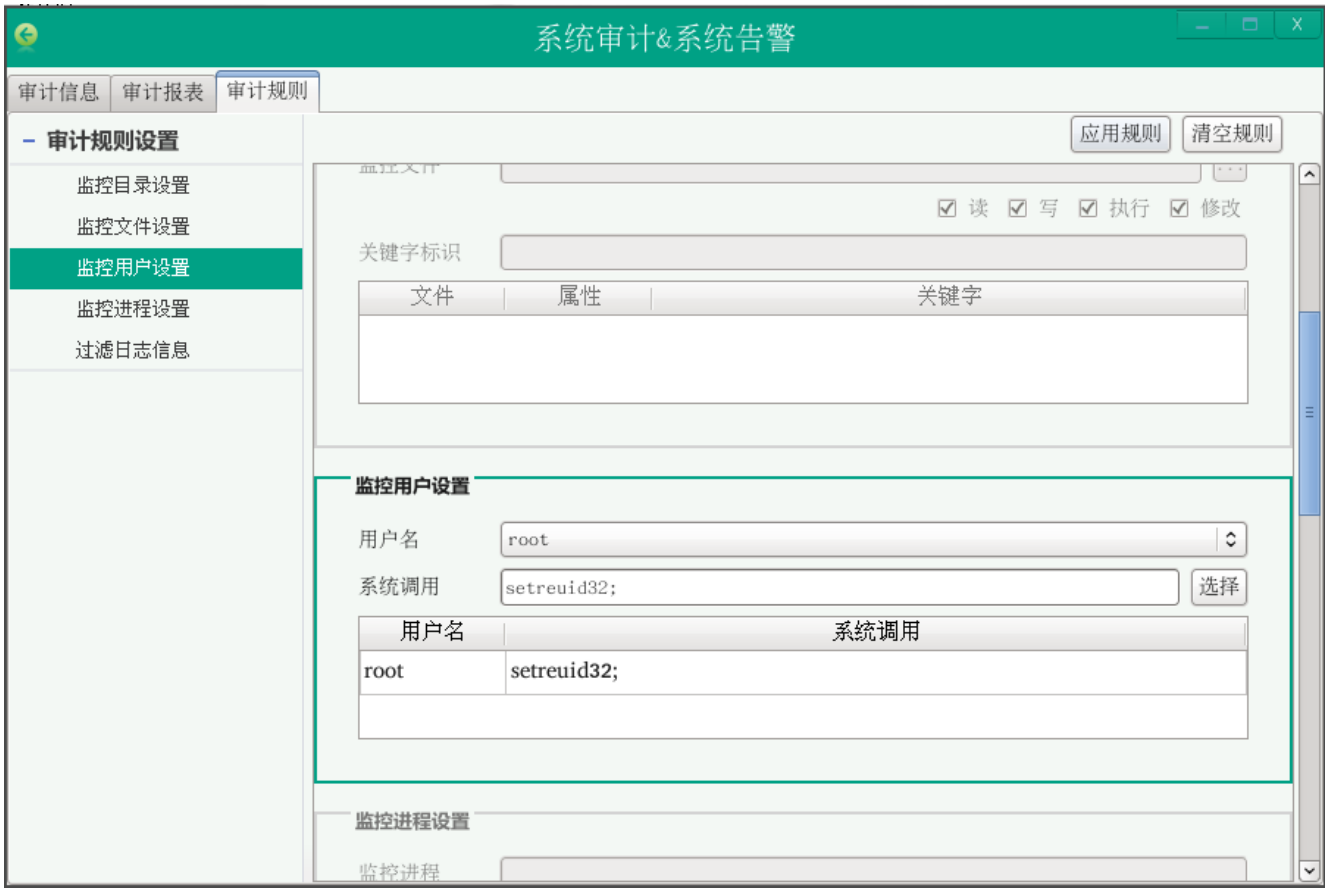


图 1-21 监控用户信息页面

监控进程设置界面如图 1-22 所示，输入所要监控的进程名，点击应用规则按钮，表格里面插入一条进程数据。规则设置成功以后，审计日志文件里面就会有监控此项进程的日志。

图 1-22 监控进程信息页面

过滤日志信息界面如图 1-23 所示，输入要过滤的日志类型，如 SYSCALL、USER_LOGIN，点击应用规则，下面的表格插入一条过滤日志类型数据。规则设置成功以后，审计日志文件里面就不会有此类型的日志信息。

图 1-23 过滤日志信息页面

1.3 系统告警管理

系统告警管理模块分为两个部分：告警信息和告警设置。

1.3.1 告警信息

告警信息部分主要显示系统设置的告警信息，界面如图 1-24 所示。选中全选按钮，表格里面的复选框可以全部被选中，再点击删除按钮，则表格里面的数据全部被删除，同时数据库里的数据也全部被删除。类别控件里面有三个可以选择的类别：LOGIN、AVC 和 CTMM，可以选择一个，也可以同时选择多个。状态控件有未查看和已查看两种状态，可以选择一个，也可以同时选择两个。点击查询按钮，表格将显示输入类别和状态条件以后的查询结果。点击删除按钮，界面会提示请选择需要删除的行，若选中将要删除的行，则界面提示您已经删除所选的行（跟审计信息界面类似，不再显示图片）。刷新按钮的功能是：若系统产生了一条告警信息，则点击刷新按钮，表格里面添加一条告警信息。时间区间和高级设置的功能类似审计信息页面，不再赘述。

图 1-24 告警信息页面

对表格内的每行点击右键，显示查看详情、标记为未查看或者已查看和删除三个快捷键，若当前行的状态为未查看，则快捷键显示为已查看，反之，则显示未查看，查看详情和删除的功能类似审计信息页面，不再赘述。

1.3.2 告警设置

告警设置部分主要设置告警方式和告警条件，界面如图 1-25 所示。告警方式设置主要分为消息发送告警设置和邮件发送告警设置。消息发送告警设置有两个选项：是否发送系统消息和发送方式，用户可以自行勾选所需要的项，若勾选，则以选择的发送方式发送系统消息。邮件发送告警设置有五个选项：是否发送邮件、发件服务器地址、帐号、密码和收件人邮箱。若勾选发送邮件，则把下面四项输入，点击保存，就可以发送告警信息到收件人邮箱里面。

图 1-25 告警设置页面

告警条件设置主要分为登录信息设置、AVC 信息设置和 CTMM 信息设置。登录信息设置界面如图 1-26 所示。由图中可看出，登录信息设置有六个选项：是否发送登录告警、登录时间段、连续登录失败次数、用户登录频率、登录 IP 和超级用户登录告警。

图 1-26 登录信息设置

若勾选发送登录告警并选择登录时间段，则用户在选择的时间段里面登录系统，系统就会收到登录告警信息，如图 1-27 所示。

图 1-27 告警信息显示

AVC 信息设置界面如图 1-28 所示。AVC 信息设置有四个选项：是否发送 AVC 告警、拒绝告警、危险操作和策略匹配。若勾选发送 AVC 告警，并有危险操作如 setenforce 操作，则系统发送告警信息，点击表格右边的添加按钮，表格可以添加策略，点击删除按钮，则表格里面的数据可以删除。

图 1-28 AVC 信息设置页面

CTMM 信息设置页面如图 1-29 所示，CTMM 信息设置共有三个选项：是否获取 CTMM 告警、拒绝 CTMM 告警和度量失败告警。若勾选获取 CTMM 告警和度量失败告警，则系统接收 CTMM 告警和度量失败告警。

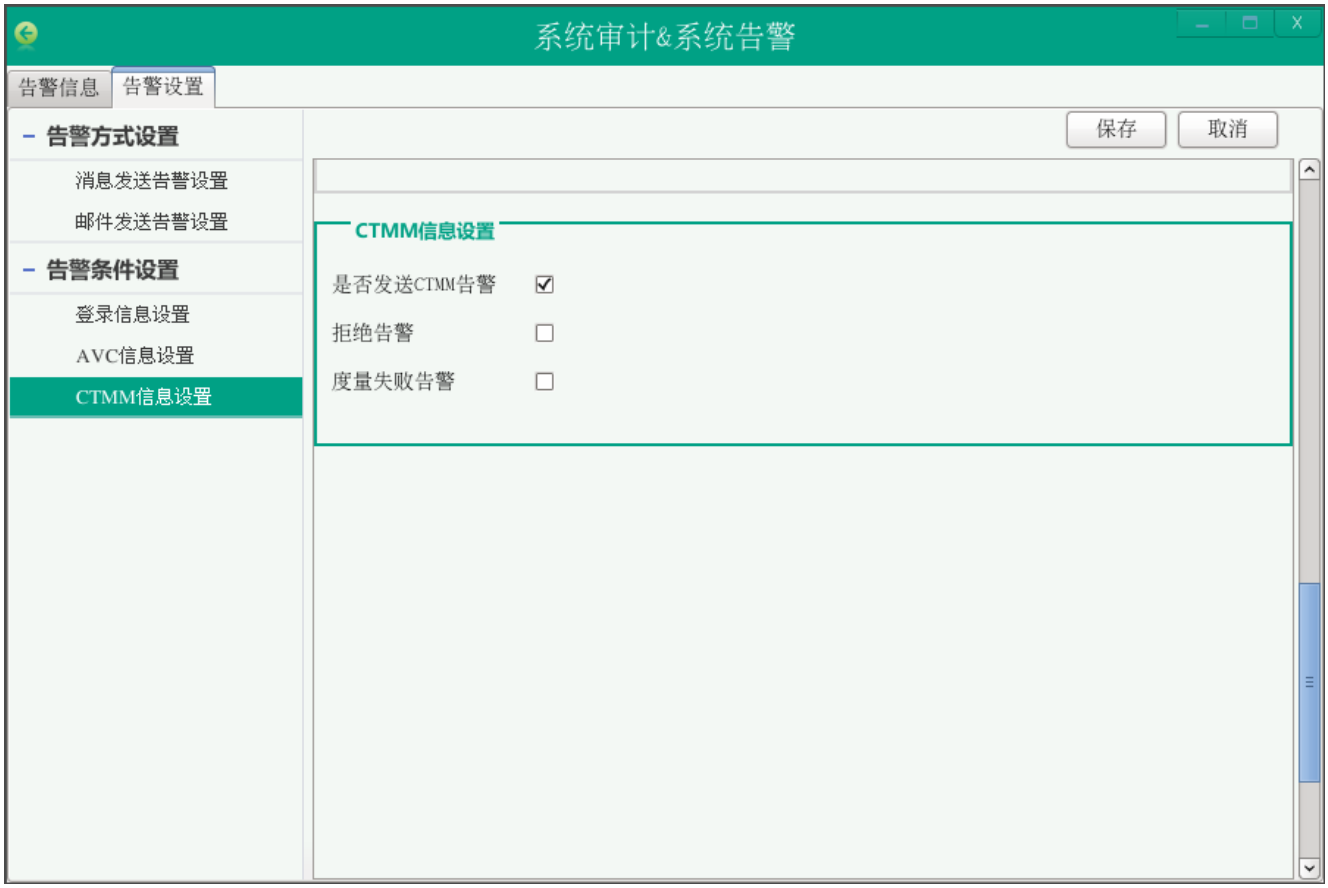


图 1-29 CTMM 信息设置页面

附录一：审计管理员用户命令集

 # audit2allow

显示访问被拒绝后应添加的允许规则

如：audit2allow -a

audit2allow -i /var/log/dmesg

详细使用方法见在线帮助文档。

 # audit2why

根据访问被拒绝的审计信息显示被拒绝的原因

如：audit2why < /var/log/audit/audit.log

详细使用方法见在线帮助文档。

 # aureport

根据审计信息文件统计登录情况，avc，pid，file，event，config 等众多信息

如：aureport -au

aureport -a

aureport -p

详细使用方法见在线帮助文档。

 # ausearch

搜索审计文件中的信息

如：ausearch -gi 0

详细使用方法见在线帮助文档。

 # auditd

启动审计服务

如：auditd -s enable

详细使用方法见在线帮助文档。

 # auditctl

显示服务状态，审计规则相关

如：auditctl -s

详细使用方法见在线帮助文档。

 # audispd

审计调度器

如：audispd

详细使用方法见在线帮助文档。

附录二：审计记录类型

类型	含义	类型	含义	类型	含义
ALL	所有	DAEMON_ACCEPT	审计守护进程接受远程访问	MAC_UNLBL_STCADD	添加静态标签
USER	用户	DAEMON_CLOSE	审计守护进程关闭远程连接	MAC_UNLBL_STCDEL	删除静态标签
LOGIN	登录	SYSCALL	系统调用	ANOM_PROMISCUOUS	设备改变混杂模式
USER_AUTH	用户认证	PATH	路径	ANOM_ABEND	进程非正常结束
USER_ACCT	用户帐户	IPC	进程间通信	KERNEL	
USER_MGMT	用户空间帐户管理	SOCKETCALL	SOCKET 调用	ANOM_LOGIN_FAILURES	登录失败达到限额
CRED_ACQ	用户空间获得认证	CONFIG_CHANGE	配置改变	ANOM_LOGIN_TIME	在不好的时间登陆
CRED_DISP	用户空间认证处理	SOCKADDR	SOCKADDR 结构	ANOM_LOGIN_SESSIONS	达到最大并发会话
USER_START	用户空间会话开始	CWD	当前工作目录	ANOM_LOGIN_ACCT	登陆尝试监视帐户
USER_END	用户空间会话结束	EXECVE	EXECVE 参数	ANOM_LOGIN_LOCATION	从禁止地点登陆
USER_AVC	用户空间 AVC 信息	IPC_SET_PERM	IPC 新权限记录类型	ANOM_MAX_DAC	达到最大数目 DAC 失败
USER_CHAUTHTOK	用户帐户属性改变	MQ_OPEN	POSIX MQ 打开记录类型	ANOM_MAX_MAC	达到最大数目 MAC 失败
USER_ERR	用户帐户属性状态错误	MQ_SENDRECV	POSIX MQ 发送与接收记	ANOM_AMTU_FAIL	AMTU 失败

			录类型		
CRED_REFR	用户空间凭证刷新	MQ_NOTIFY	POSIX MQ 通知记录类型	ANOM_RBAC_FAIL	RBAC 自身测试失败
USYS_CONFIG	用户空间系统配置变化	MQ_GETSETATTR	POSIX MQ GET SET 属性记录类型	ANOM_RBAC_INTEGRITY_FAIL	RBAC 文件完整性失败
USER_LOGIN	用户空间用户已登陆	KERNEL_OTHER	第三方模块使用	ANOM_CRYPTO_FAIL	加密系统测试失败
USER_LOGOUT	用户空间用户已注销	FD_PAIR	Pipe 与 socketpair 审计记录	ANOM_ACCESS_FS	文件或目录访问
ADD_USER	用户空间新增用户帐户	OBJ_PID	信号与 ptrace 目标	ANOM_EXEC	可执行文件
DEL_USER	用户空间删除用户帐户	TTY	管理 TTY 的输入	ANOM_MK_EXEC	使其可执行
ADD_GROUP	用户空间添加用户组	EOE	事件结束	ANOM_ADD_ACCT	添加一帐户
DEL_GROUP	用户空间删除用户组	AVC	AVC 信息	ANOM_DEL_ACCT	删除一帐户
DAC_CHECK	用户空间 DAC 操作	SELINUX_ERR	SELinux 错误	ANOM_MOD_ACCT	改变一帐户
CHGRP_ID	用户空间组 ID 改变	AVC_PATH	AVC 路径	ANOM_ROOT_TRANS	用户变成 ROOT
TEST	被用来测试成功消息	MAC_POLICY_LOAD	策略文件装载	RESP_ANOMALY	非正常到达
TRUSTED_APP	被信任的应用程序消息	MAC_STATUS	策略状态改变	RESP_ALERT	警告邮件被送达
USER_SELINUX_ERR	SELinux 用户空间错误	MAC_CONFIG_CHANGE	策略配置改变	RESP_KILL_PROC	杀死程序
USER_CMD	用户 SHELL	MAC_UNLBL_ALL	允许未标记	RESP_TERM_ACC	终端会话

	命令及参数	OW	的通行	ESS	
USER_TTY	Non-ICANON TTY input meaning	MAC_CIPSOV4_ADD	添加 CIPSOv4 DOI entry	RESP_ACCT_REMOTE	远程访问帐户被锁
CHUSER_ID	更改用户 ID 补充数据	MAC_CIPSOV4_DEL	删除 CIPSOv4 DOI entry	RESP_ACCT_LOCK_TIMED	由于时间帐户被锁
GRP_AUTH	组密码认证	MAC_MAP_ADD	添加 LSM domain mapping	RESP_ACCT_UNLOCK_TIMED	由于时间帐户解锁
DAEMON_START	审计守护进程开始	MAC_MAP_DEL	删除 LSM domain mapping	RESP_ACCT_LOCK	用户帐户被锁
DAEMON_END	审计守护进程结束	MAC_IPSEC_ADDSA	添加一 XFRM 状态	RESP_TERM_LOCK	终端被锁
DAEMON_ABORT	审计守护进程中止	MAC_IPSEC_DELSA	删除 XFRM 状态	RESP_SEBOOL	设置 SELinux 布尔值
DAEMON_CONFIG	审计守护进程配置	MAC_IPSEC_ADDSPD	添加 XFRM 策略	RESP_EXEC	执行脚本
DAEMON_ROTATE	审计守护进程循环	MAC_IPSEC_DELSPD	删除 XFRM 策略	RESP_SINGLE	转入单用户模式
DAEMON_RESUME	审计守护进程重新开始	MAC_IPSEC_EVENT	XFRM 事件	RESP_HALT	让系统挂掉
USER_ROLE_CHANGE	用户角色改变	ROLE_ASSIGN	管理员分配用户角色	ROLE_REMOVE	管理员从角色中删除用户
LABEL_OVERRIDE	标签覆盖	LABEL_LEVEL_CHANGE	目标级别改变	USER_LABELED_EXPORT	Object exported with label
USER_UNLABELED_EXPORT	用户未标注出口	DEV_ALLOC	设置已分配	DEV_DEALLOC	设备被释放

FS_RELABEL	文件系统重新标记	USER_MAC_POLICY_LOAD	用户空间进程装载策略		

附录三：系统调用参照表

一、进程控制			
名称	说明	名称	说明
fork	创建一个新进程	prctl	对进程进行特定操作
clone	按指定条件创建子进程	ptrace	进程跟踪
execve	运行可执行文件	sched_get_priority_max	取得静态优先级的上限
exit	中止进程	sched_get_priority_min	取得静态优先级的下限
_exit	立即中止当前进程	sched_getparam	取得进程的调度参数
getdtablesize	进程所能打开的最大文件数	sched_getscheduler	取得指定进程的调度策略
getpGID	获取指定进程组标识号	sched_rr_get_interval	取得按 RR 算法调度的实时进程的时间片长度
setpGID	设置指定进程组标志号	sched_setparam	设置进程的调度参数
getpgrp	获取当前进程组标识号	sched_setscheduler	设置指定进程的调度策略和参数
setpgrp	设置当前进程组标志号	sched_yield	进程主动让出处理器，并将自己等候调度队列队尾
getpid	获取进程标识号	vfork	创建一个子进程，以供执行新程序，常与 execve 等同时使用
getppid	获取父进程标识号	wait	等待子进程终止
getpriority	获取调度优先级	wait3	参见 wait
setpriority	设置调度优先级	waitpid	等待指定子进程终止
modify_ldt	读写进程的本地描述表	wait4	参见 waitpid
nanosleep	使进程睡眠指定的时间	capget	获取进程权限

nice	改变分时进程的优先级	capset	设置进程权限
pause	挂起进程，等待信号	getsid	获取会晤标识号
personality	设置进程运行域	setsid	设置会晤标识号
二、文件系统控制——读写操作			
名称	说明	名称	说明
fcntl	文件控制	lseek	移动文件指针
open	打开文件	_llseek	在 64 位地址空间里移动文件指针
creat	创建新文件	dup	复制已打开的文件描述字
close	关闭文件描述字	dup2	按指定条件复制文件描述字
read	读文件	flock	文件加/解锁
write	写文件	poll	I/O 多路转换
readv	从文件读入数据到缓冲数组中	truncate	截断文件
writev	将缓冲数组里的数据写入文件	ftruncate	参见 truncate
pread	对文件随机读	umask	设置文件权限掩码
pwrite	对文件随机写	fsync	把文件在内存中的部分写回磁盘
三、文件系统控制——系统操作			
access	确定文件的可存取性	getdents	读取目录项
chdir	改变当前工作目录	mkdir	创建目录
fchdir	参见 chdir	mknod	创建索引节点
chmod	改变文件方式	rmdir	删除目录
fchmod	参见 chmod	rename	文件改名
chown	改变文件的属主或用户组	link	创建链接
fchown	参见 chown	symlink	创建符号链接
lchown	参见 chown	unlink	删除链接
chroot	改变根目录	readlink	读符号链接的值
stat	取文件状态信息	mount	安装文件系统
lstat	参见 stat	umount	卸下文件系统
fstat	参见 stat	ustat	取文件系统信息
statfs	取文件系统信息	utime	改变文件的访问修改时间

fstatfs	参见 statfs	utimes	参见 utime
readdir	读取目录项	quotactl	控制磁盘配额
四、系统控制			
名称	说明	名称	说明
ioctl	I/O 总控制函数	alarm	设置进程的闹钟
_sysctl	读/写系统参数	getitimer	获取计时器值
acct	启用或禁止进程记账	setitimer	设置计时器值
getrlimit	获取系统资源上限	gettimeofday	取时间和时区
setrlimit	设置系统资源上限	settimeofday	设置时间和时区
getrusage	获取系统资源使用情况	stime	设置系统日期和时间
uselib	选择要使用的二进制函数库	time	取得系统时间
ioperm	设置端口 I/O 权限	times	取进程运行时间
iopl	改变进程 I/O 权限级别	uname	获取当前 UNIX 系统的名称、版本和主机等信息
outb	低级端口操作	vhangup	挂起当前终端
reboot	重新启动	nfsservctl	对 NFS 守护进程进行控制
swapon	打开交换文件和设备	vm86	进入模拟 8086 模式
swapoff	关闭交换文件和设备	create_module	创建可装载的模块项
bdflush	控制 bdflush 守护进程	delete_module	删除可装载的模块项
sysfs	取核心支持的文件系统类型	init_module	初始化模块
sysinfo	取得系统信息	query_module	查询模块信息
adjtimex	调整系统时钟	*get_kernel_syms	取得核心符号，已被 query_module 代替
五、内存管理			
名称	说明	名称	说明
brk	改变数据段空间的分配	munmap	去除内存页映射

sbrk	参见 brk	mremap	重新映射虚拟内存地址
mlock	内存页面加锁	msync	将映射内存中的数据写回磁盘
munlock	内存页面解锁	mprotect	设置内存映像保护
mlockall	调用进程所有内存页面加锁	getpagesize	获取页面大小
munlockall	调用进程所有内存页面解锁	sync	将内存缓冲区数据写回硬盘
mmap	映射虚拟内存页	cacheflush	将指定缓冲区中的内容写回磁盘
六、网络管理			
名称	说明	名称	说明
getdomainname	取域名	sethostid	设置主机标识号
setdomainname	设置域名	gethostname	获取本主机名称
gethostid	获取主机标识号	sethostname	设置主机名称
七、Socket 控制			
名称	说明	名称	说明
socketcall	socket 系统调用	recvmsg	参见 recv
socket	建立 socket	listen	监听 socket 端口
bind	绑定 socket 到端口	select	对多路同步 I/O 进行轮询
connect	连接远程主机	shutdown	关闭 socket 上的连接
accept	响应 socket 连接请求	getsockname	取得本地 socket 名字
send	通过 socket 发送信息	getpeername	获取通信对方的 socket 名字
sendto	发送 UDP 信息	getsockopt	取端口设置
sendmsg	参见 send	setsockopt	设置端口参数
recv	通过 socket 接收信息	sendfile	在文件或端口间传输数据
recvfrom	接收 UDP 信息	socketpair	创建一对已连接的无名 socket
八、用户管理			
名称	说明	名称	说明
getUID	获取用户标识号	setreUID	分别设置真实和有效的用户标识号

setUID	设置用户标志号	getresGID	分别获取真实的，有效的和保存过的组标识号
getGID	获取组标识号	setresGID	分别设置真实的，有效的和保存过的组标识号
setGID	设置组标志号	getresUID	分别获取真实的，有效的和保存过的用户标识号
geteGID	获取有效组标识号	setresUID	分别设置真实的，有效的和保存过的用户标识号
seteGID	设置有效组标识号	setfsGID	设置文件系统检查时使用的组标识号
geteUID	获取有效用户标识号	setfsUID	设置文件系统检查时使用的用户标识号
seteUID	设置有效用户标识号	getgroups	获取后补组标志清单
setreGID	分别设置真实和有效的的组标识号	setgroups	设置后补组标志清单
九、进程间通信			
名称	说明		
ipc	进程间通信总控制调用		
十、进程间通信——信号			
sigaction	设置对指定信号的处理方法		
sigprocmask	根据参数对信号集中的信号执行阻塞/解除阻塞等操作	*sigsetmask	用给定信号掩码替换现有阻塞信号掩码，已被 sigprocmask 代替
sigpending	为指定的被阻塞信号设置队列	*sigmask	将给定的信号转化为掩码，已被 sigprocmask 代替
sigsuspend	挂起进程等待特定信号	*sigpause	作用同 sigsuspend，已被 sigsuspend 代替
signal	参见 signal	sigvec	为兼容 BSD 而设的信号处理函数，作用类似 sigaction
kill	向进程或进程组发信号	ssetmask	ANSI C 的信号处理函数，作用类似 sigaction
*sigblock	向被阻塞信号掩码中添加		

	信号，已被 sigprocmask 代替		
十一、进程间通信——消息			
msgctl	消息控制操作	msgsnd	发消息
msgget	获取消息队列	msgrcv	取消息
十二、进程间通信——管道			
pipe	创建管道		
十三、进程间通信——信号量			
semctl	信号量控制	semop	信号量操作
semget	获取一组信号量		
十四、进程间通信——共享内存			
shmctl	控制共享内存	shmat	连接共享内存
shmget	获取共享内存	shmdt	拆卸共享内存