红旗安全操作系统 4.0

安全管理手册

北京中科红旗软件技术有限公司

地址：中国北京海淀区万泉河路 68 号紫金大厦 6 层

Red Flag Software Co., Ltd.

http://www.redflag-linux.com

声明：

本软件受相应版权法保护，并在 GNU GPL 约束其使用、拷贝、发布及反编译的授权下发布。在未经红旗软件公司事先书面授权的情况下，文档的任何部分都不得以任何形式和途径进行复制、修改及分发。本手册在编写过程中由于已考虑了各种可能的预防措施，红旗软件公司对可能出现的内容错误及缺失不承担责任。

此出版物仅以其原有的存在形式提供，不含任何种类的明示或默示，包括但不仅限于那些隐含的用于商业目的的、为某种特定目的而定制的、或无特定目的的担保。此出版物可能会出现技术上的失误或印刷上的错误。其更正将不断添加于此，并合并到此出版物的最新版本中。

红旗软件公司保留在任何时刻对此出版物介绍的产品和/或程序进行添加和/或修改的权利。

本文档的最终解释权归属于红旗软件公司。

本产品使用了如下字库：

东文字库，版权所有©长沙东文软件有限公司。

本产品使用了如下输入法：

智能通用输入法平台 - SCIM，版权所有©苏哲。

目　　录

序

欢迎使用红旗安全操作系统 4.0!

全新的红旗安全操作系统 4.0 面向企业级网络服务器的安全需求，依照国家标准 GB/T 20272—2006 要求进行开发。集成的安全特性不仅能够防范来自外部网络的入侵攻击，更能够建立内部主机安全管理的策略和机制。通过在 Linux 内核层实现了经典的安全策略和访问控制，包括最小化特权、自主访问控制、强制访问控制、角色访问控制、内核级审计，以及对各种不同应用服务的良好支持和保护，能够满足安全敏感行业和涉密领域对操作系统的高安全性要求。

《红旗安全操作系统 4.0 安全管理手册》系统地阐述了进行安全管理所需的基本知识及相关安全管理功能，帮助管理员顺利运用系统提供的多种访问控制，以及直观易用的管理控制台和管理命令，执行安全管理任务并配置和管理一个安全可靠的服务器系统。本手册主要内容包括：

- 安全术语
- 基本功能介绍
- 安全访问控制
- 基本安全管理
- 安全管理控制台
- 审计管理

本书的适用对象

本手册适用于已掌握 Linux 系统的基础知识和系统管理技术，关注系统安全控制并希望掌握操作系统安全管理的中级使用者。

红旗安全操作系统 4.0 提供了基于命令行和图形界面的安全管理工具，利用这些工具能够简便、快捷地实现安全管理和访问控制。在进行安全管理之前，建议管理员先系统地理解系统安全相关的基本概念和专业术语。

需要指出的是，建立系统安全体系是一个系统工程，需要从制度、人员、技术三方面入手。一个好的安全体系不能只依靠单一配置的安全机制，而需要建立起一整套纵深防御体系，多种安全机制共同作用，互相提供必要的冗余与协同，从网络、主机和人员的安全上进行统筹地规划和部署。

提示与警告

为了强调《红旗安全操作系统 4.安全管理手册》中的某些重要的信息，我们使用下面两种方式加以重点说明：

一些有用的额外信息、使用中提示和帮助用户更加顺利地完成工作的小技巧等。

看到这一标记时应引起特别注意，它表示一些重要的警告和错误提示信息。

第1章　概述

本章首先简单描述了安全管理人员进行安全管理之前所必须遵守的行为假设和管理要求，然后简要概述了红旗安全操作系统 4.0 的基本功能，然后系统描述了进行安全管理前所必须了解的安全概念和术语，为后续的访问控制配置和安全策略规划做好基础性准备。

1.1　行为假设

在进行安全管理之前，管理人员应先系统地理解安全领域的基本概念和专业术语，然后才开始熟悉本手册介绍的基本安全管理命令和图形管理接口。

对于管理员，还应该明白安全系统的部署次序。即在不生效或者关闭安全功能的前提下，先按照标准 Linux 系统的习惯部署应用系统，调试运行没有问题后。再从系统整体和应用本身进行安全评估，形成针对系统和应用的安全保护策略。最后，再运用接口命令和图形工具实施安全保护策略的部署。

需要注意的是，在部署安全策略时，不要随意限制基本系统公用资源的读操作权限，这样可能会导致整个系统的不可用。例如对/lib、/usr/lib 或者/bin 或/sbin 设置为不允许读，这将导致 root 和其他用户由于无法调用正常的库文件和命令文件而导致系统无法使用。另一个例子是提升 root 用户的密级，这将导致以 root 用户身份运行的大量系统服务程序无法访问必须的系统配置、库而导致运行出错。因此，在设计安全策略时，应注意在最大化保护系统的前提下，尽量少地影响系统的运行兼容性。

此外，由于某些安全配置与系统时钟有一定的关联，管理员应留意确认系统时钟的有效性。

最后，鉴于系统提供了远程管理机制和远程审计数据库备份机制，管理员应确保运行管理控制台的 Linux 系统的主机安全，且养成使用管理接口完毕即刻退出的良好习惯。在远程管理的主机划分上，建议将安全管理控制台和审计管理控制台分别安装在不同的主机上。审计控制台、潜在侵害和报警模块、可选的远程数据库审计备份可以安装在一台机器上，并由审计管理员专人管理。

1.2　管理要求

为了保证系统的安全运行，管理员应注意如下与安全管理员相关的系统环境安全要求：

1) 审计日志存储所在的分区应始终保证有足够的空余空间，以避免审计日志溢出

2) 应定期检查硬盘的可靠性和文件系统的一致性，以避免安全功能模块对应的程序和数据文件出现不一致性

3) 应保持管理员密码的复杂度并定期更换密码；并应养成只有需要使用管理员角色进行管理时方使用管理员登录的习惯

4) 应保证系统时钟的有效性，避免时钟紊乱或人为错误设置对安全功能的干扰

此外，安全管理人员仍需要明白，系统安全是一个整体的概念，必须从网络、主机和人员的安全上进行统筹地规划和部署。

在网络上，除了利用系统提供的主机防火墙配置必要的网络控制外，还应该避免使用被认为不安全的服务，如 telnet、rsh、rlogin 等。如果要远程管理主机，建议使用 ssh 服务。

在主机软件上，要留意系统提供的 Asianux TSN Updater 自动补丁更新通知功能。一旦发现有安全相关更新，应尽快将对应包进行升级。

更值得关注且更薄弱的环节是人员和制度的管理，技术上的安全措施往往只能起到辅助作用。若管

理员忽视口令的管理，或经常用系统管理员身份去执行本该由普通用户就可以所做的工作，或完成了安全管理后遗留登录终端给他人以可乘之机，都会造成技术上的安全保护形同虚设。

1.3 功能概要

红旗安全操作系统 4.0 通过全新设计，在内核层次实现了多样化访问控制和实时审计，使得任何应用任何用户的操作行为都要受到访问控制的制约，任何违反安全访问控制策略的非法行为都将被实时记录并生成警报。

红旗安全操作系统 4.0 提供的主要安全功能有：

- 特权分立
- 强化身份鉴别
- 基于安全标记的强制访问控制
- 基于访问控制列表(ACL)的自主访问控制
- 加密文件系统
- 异常监测与实时报警
- 多服务器节点的集中化远程管理
- 审计日志的实时和异地备份
- 审计统计分析和报表输出

鉴于传统 Linux 系统很多安全隐患都是直接或间接地与系统中存在有超级特权用户(root)相关，为了杜绝超级特权用户所引发的管理隐患，红旗安全操作系统 4.0 基于特权分立原则，将 root 的超级特权分立为多个受限的管理权限，使得特权用户的权限受到大大的削弱而不再是系统中的超级特权用户，进而使得传统的拥有 root 帐号即能完全控制系统的管理安全问题得到良好的解决。

红旗安全操作系统 4.0 将传统的 root 管理员按照职能不同，通过角色机制划分为三个相互独立的管理用户：系统管理员、安全管理员和审计管理员，分别完成不同的任务。

系统管理员维护大多数传统的系统管理工作，如管理帐户和系统服务，创建和挂载文件系统，恢复先前的备份等等，以及其他非安全策略和非审计相关的系统管理职能。

安全管理员负责系统的安全配置和访问控制管理。所有的安全管理都必须使用具有安全管理员角色的用户进行。

审计管理员负责执行安全审计的管理，包括启停审计服务，管理审计日志，更改审计参数与审计规则等。

1.4 基本概念

为了更好地描述红旗安全操作系统 4.0 所带的安全功能，有必要先对常用的安全术语做一个概要性说明。

- **主体(Subject)和客体(Object)**

操作系统中的所有资源访问行为均可被看作由主体发起的对客体的访问。在这些访问行为中，主体是访问行为的发起方，如用户或者进程。而客体是被访问的资源如文件、目录、设备等等。

➢ 安全上下文(Security Context)/ 安全标记(Security Tag)

所有操作系统访问控制都是以访问行为相关联的主客体的对应访问控制属性为基础的。

在红旗安全操作系统 4.0 中，属性是具有相似特征的安全类型的组合。主客体的访问控制属性也被称为安全上下文或者安全标记。所有客体(文件、进程间通讯、套接字等)和主体(进程)都有与其关联的安全上下文，一个安全上下文由三部分组成：安全用户、角色和类型标识符。

一般情况下，多个属性的组合构成了类型，多个类型的组合构成了角色，多个角色的组合形成了安全用户。

在开启了强制访问控制后，安全上下文扩展了两个字段：低安全标记和高安全标记。每个安全标记本身有两个字段：敏感性等级、分类标记。敏感性等级是以数字形式量化描述的，有着严格的等级分级；它反映了一个有序的数据敏感度模型。分类是无序化以类似集合形式提供的，它反应的是数据划分的需要。这样，对于要访问的数据必须拥有足够的敏感性等级，以及正确的分类标记。

s0-s15:c0.c1023 是系统默认指定的强制访问控制安全标记范围，由安全等级和安全分类组成。这表明，默认用户和文件的安全等级为 s0，但可以动态调整到 s15。分类标记默认为空，也可以设置到 c0 至 c1023 分类的组合。

➢ 安全用户(Secured User)

如前所述，多个类型的组合构成了角色，多个角色的组合形成了安全用户。安全用户本质上是角色的组合形成的权能定义。

在红旗安全操作系统 4.0 中，可登录的系统用户都可以通过被附加非默认的安全标记而成为安全用户。这可以通过将系统用户映射到内建的安全用户上予以实现。

根据安全角色和安全标记的不同，系统默认内建了三个安全用户，红旗安全操作系统默认将系统用户与这些安全用户分别进行映射。这样，当系统用户登录时，自动继承各自的默认安全属性。具体对应关系如下表所示：

系统用户	安全用户	安全角色	安全等级
sysadm	sysadm_u	sysadm_r staff_r	s0-s15:c0.c1023
secadm	secadm_u	secadm_r	s0-s15:c0.c1023
auditadm	auditadm_u	auditadm_r	s0-s15:c0.c1023

其中，系统用户一栏里 sysadm、secadm 、auditadm 分别对应系统管理员、安全管理员和审计管理员三个特权管理员，分别具备对应的管理职能。

staff_r 是非特权的安全用户角色。root 用户通过 ssh 等服务进行系统登陆时默认使用这个角色，此时可以通过 newrole 命令切换系统管理员角色。

➢ 强制访问控制(MAC：Mandatory Access Control)

指系统中生效的安全访问控制均由一个统一的强制实施的安全访问控制模型定义，包括 root 用户在内的任何主体对客体发起的访问操作均要受到访问控制模型的制约。强制访问控制的部署和实施是由安全管理员完成的。

红旗安全操作系统 4.0 中的强制访问控制包括：类型强制(TE)访问控制、基于角色的访问控制(RBAC)、多级别/分类安全(MLS/MCS)访问控制。

➢ 基于 TE 强制访问控制(TE：Type Enforcement Access Control)

红旗安全操作系统4.0提供了一种灵活的MAC机制，称为类型强制(TE)访问控制。在类型强制下，所有主体和客体都有一个类型标识符与它们关联。要访问某个客体，主体的类型必须为客体的类型进行授权，而不必关注主体的用户标识符。

类型强制提供强壮的强制安全能够适应大量的安全目标。类型强制提供一种思想，将访问控制细化到程序粒度。在某种程度上，它允许系统安全管理人员定义适合他们系统的安全策略。

➢ 基于 MLS/MCS 强制访问控制

红旗安全操作系统 4.0 MLS/MCS 强制访问控制是基于业内主流的 BLP 模型和 BIBA 模型，并参考selinux框架加以实现的。通过将所有主体对客体的访问权限统一于读权限和写权限，并比对主体和客体的安全属性来决策是否授权主体对客体的访问许可。其中，读操作包括对客体的读取和执行权限，写操作包括客体的写入、创建等权限。

MLS/MCS 的主要弱点是它严格地、以不可改变的方式实现了单一安全目标，不够灵活而无法满足实际部署时的定制要求。而红旗安全操作系统 4.0 把 MLS/MCS 的约束是附加在 TE 规则中的，增加系统灵活性，可以克服上述缺点。

红旗安全操作系统 4.0 中 BLP 访问控制模型被定义为：

仅当主体的安全等级和分类大于等于客体时，主体才能读客体；仅当主体的安全等级和分类与客体相同时，主体才能写客体。其它情况下，主体没有对客体的读权限和写权限。

安全管理员使用强制访问控制保护涉密主体和客体，请注意依照上述访问控制规则定制安全策略。

➢ 基于角色访问控制(RBAC：Role Based Access Control)

通过定义类似于人类社会职能的角色机制，将不同的主体赋予不同的角色，并将客体的访问控制权限赋予不同的角色，就实现了基于角色的访问控制。

传统的RBAC模型是对角色进行授权，然后将一个或多个角色分配给一个授权用户。红旗安全操作系统 4.0 中的RBAC模型是基于一个类型指定授权，然后将类型指定给角色，将一个或多个角色指定给一个授权用户。

➢ 自主访问控制(DAC：Discretionary Access Control)

系统中每个客体都有自己的属主。客体属主可以自主定义哪类主体对于自己拥有的客体拥有什么样的操作权限，这就是自主访问控制。

在红旗安全操作系统 4 中，自主访问控制是通过对客体建立访问控制列表(ACL：Access Control List)机制来实现的。每个客体的访问控制列表项一般由主体—访问权限两项组成。通过定义不同的主体—权限项形成不同的访问控制策略。

与强制访问控制不同的是，自主访问控制的实施主体是客体属主用户本身，而不是安全管理员。

第2章　安全功能

本章主要描述了红旗安全操作系统 4.0 中除强制安全访问控制和审计之外的其他安全模块的功能和配置。强制安全访问控制的命令和图形接口介绍请分别参阅第 4、5 章。审计模块的接口和配置请参阅第 6 章。

2.1　强口令认证

系统强制用户使用强口令认证。当在使用 passwd 命令修改用户密码，或者使用 rolepasswd 命令修改管理角色密码时，必须满足下列密码长度和密码规则要求，即默认密码最低为 8 位的非字典口令，并且口令不可全由字母或数字组成。

- 密码长度：

可接受的密码的最低长度为 8 个字符，最大长度为 256 个字符。

通过修改配置文件/etc/login.defs 字段 PASS_MIN_LEN 来定义密码长度。具体设置规定如下：

1. 如果配置文件没有设置 PASS_MIN_LEN 字段，系统采取最小长度 8。
2. 如果配置文件设置了 PASS_MIN_LEN 字段值小于等于 8，系统采取最小长度 8。
3. 如果配置文件设置了 PASS_MIN_LEN 字段值大于 8，但是最大长度必须小于等于为 256 个字符。

- 密码规则：

1. 密码区分大小写。
2. 密码必须在可接受的长度范围内。
3. 密码不可以全部由空格组成。
4. 密码中不相同的字符数量必须不小于 5。

   例如：密码 a#uh#aua，因为不相同的字符为 a,#,u,h，小于 5 个，所以不合乎要求。

5. 密码中如果两个相邻的字符的 ASCII 值也是相邻的，则这样的情况不能多于 4 次。

   例如：密码 abaB43yz89#，因为密码的第一位和第二位，第二位和第三位，第五位和第六位，第七位和第八位，第九位和第十位的 ASCII 值都相差 1，这样的情况出现了 5 次，所以不合乎要求。

6. 密码不可以全部由数字组成，或者全部由字母组成。
7. 密码不可以包含当前用户名，或当前用户名的逆序。
8. 密码不可以是字典中的单词或是字典单词的逆序。
9. 密码的合法字符： a-z, A-Z, 0-9, 空格, 所有英文符号。

2.2　增强的控制台登陆用户身份鉴别

当系统用户登陆系统时，如果该系统认证被配置为采用USB设备(USB Key)验证项，系统首先进行USB设备硬件本身的验证，然后进行从 USB 设备获得用户身份鉴别密钥进行验证。如果验证通过则会成功登陆获得登录 shell，否则将会提示输入相应用户的密码。如果验证全部失败，将会重新返回登陆界面。

用户身份鉴别密钥采用一次一密认证方式。即每次认证成功，系统自动更新认证密钥。

默认情况下，系统被配置为可选地使用 USB 存储设备实现系统密码的自动验证，而不必在每次登陆时手动输入用户密码。

通过配置，红旗安全操作系统 4.0 还支持基于 USB Key 物理设备和用户密码两者兼具的双因子认证方式，极大地提高了控制台用户身份鉴别的强制性和安全性。

支持同一个 USB 设备认证多台机器。不支持一个用户对应对用多个 USB 设备。支持一个设备对应多个用户。但是添加设备名必须唯一。

增强的 USB Key 认证方式的配置过程如下：

1. 插入 USB 存储设备或者 MMC 存储卡

2. 添加认证设备

执行 pamusb-conf --add-device MyDevice。其中，MyDevice 是为该设备起一个便于识别的名字。

如下是该命令的交互输出示例：

```
# pamusb-conf --add-device MyDevice
Please select the device you wish to add.
* Using "SanDisk Corp. Cruzer Titanium (SNDKXXXXXXXXXXXXXXXX)" (only
option)
Which volume would you like to use for storing data ?
* Using "/dev/sda1 (UUID: <6F6B-42FC>)" (only option)
Name           : MyDevice
Vendor         : SanDisk Corp.
Model          : Cruzer Titanium
Serial         : SNDKXXXXXXXXXXXXXXXX
Volume UUID    : 6F6B-42FC (/dev/sda1)
Save to /etc/pamusb.conf ?
[Y/n] y
Done.
```

输入 y 确认即可保存配置。

3. 添加与该物理设备相关联的认证用户

假设需要添加的用户名是 sysadm，执行 pamusb-conf --add-user sysadm，示例如下：

如下是该命令的交互输出示例：

```
# pamusb-conf --add-user sysadm
  Which device would you like to use for authentication ?
  * Using "MyDevice" (only option)
  User           : sysadm
  Device         : MyDevice
  Save to /etc/pamusb.conf ?
  [Y/n] y
  Done.
```

选中第 2 步定义的 USB 设备名按 y 确认保存配置。

4. 验证是否添加成功。此步骤可选。

```
# pamusb-check sysadm
* Authentication request for user " sysadm " (pamusb-check)
* Device "MyDevice" is connected (good).
* Performing one time pad verification...
* Verification match, updating one time pads...
* Access granted.
```

当进行用户密码验证时，如不希望在你的系统上启用这项认证机制，你可以修改 /etc/pamd.d/login 文件，注释掉 auth sufficient pam_usb.so 这一行。

如果发现发现USB 认证设备丢失或者被盗用，请手工删除/etc/pamusb.conf 中有关该用户的配置项。使用新的硬件重新为该用户配置 USB 认证。

2.3 基于 ACL 的自主访问控制

传统的 Linux 系统提供的基于 rwx 模式的自主访问控制，对于 root 用户起不到限制作用的，root 用户依然可以突破文件属主用户定义的 rwx 访问控制规则访问文件。而且，root 用户还可以随意更改文件属主和 rwx 访问控制规则。

红旗安全操作系统 4.0 采用 Posix ACL 机制实现增强型的自主访问控制。基于访问控制列表的自主访问控制是 rwx 自主访问控制的一种扩展。它使得所有用户可自主定义自己所拥有文件的访问控制列表，使得所有用户对该文件的访问均按照访问控制列表的权限规则定义进行。

同时，红旗安全操作系统 4.0 还对 root 用户的特权操作进行了功能限制。通过配置，root 用户将无法突破客体属主用户定义的基于 ACL 的自主访问控制规则，也不能对不属于自己的文件修改或者增加 ACL 规则。

基于 ACL 的自主访问控制的主要接口是 setfacl 和 getfacl 命令，分别是获得和设置指定文件的 ACL 列表。

getfacl 很简单，可以返回文件当前的 ACL 信息，例如在一个 CVSROOT 下的 passwd 文件有这样的属性：

```
getfacl passwd
# file: passwd
# owner: cvsadmin
# group: cvsadmin
user::rw-
group::r--
other::r--
```

显示属主用户 cvsadmin 可以读写(rw)，同组用户和其他用户只读(r)。

可以用 setfacl 加上其他访问控制列表定义，该命令的执行者只能是文件属主用户。

例如加上 allen 用户可写，可以使用属主用户 cvsadmin 用户执行下面的命令设置:

```
setfacl -m u:allen:rw- passwd
```

这个命令表示：增加用户（u）用户名（allen）可读写权限（rw-）到文件 passwd。这样之后再执行 getfacl，看看结果，

```
getfacl passwd
# file: passwd
# owner: cvsadmin
# group: cvsadmin
user::rw-
user:allen:rw-
group::r--
mask::rw-
other::r--
```

可以看到多出了一行 user:allen:rw-，表示 allen 用户有 rw-权限。

mask 权限，就是用一个固定的权限设置遮住(mask)其他的权限设置，这样可以获得比较好的保护，因为用户最终对文件的权限将是由设置的权限和 mask 值与运算获得的

设置 mask 有效权限，例如执行下面的设置:

```
setfacl -m mask::r--passwd
```

然后用 getfacl 命令显示文件实际有效权限：

```
getfacl passwd
# file: passwd
# owner: cvsadmin
# group: cvsadmin
user::rw-
user:allen:rw- #effective:r--
group::r--
mask::r--
other::r--
```

我们可以看到 allen 用户对于 passwd 文件的有效（effective）权限经计算

为 r--,写权限被 mask 掉了。

如果 setfacl 命令不指定操作用户，那么就是对默认属主用户权限的操作，这时候的 setfacl 命令功能上和传统的 chmod 相同。例如 setfacl u::rwx,g::rwx,o::rwx filename 等价于 chmod 777 filenmae。

更多的 setfacl 操作：

-x 删除特定用户的权限设置，例如 setfacl -x u:allen filename

删除 filenmae 上 allen 用户的权限设置。

删除所有的 ACL 设置，

setfacl -b filename

setfacl --remove-all filename

cp 和 mv 命令也保持了对 ACL 机制的支持，mv 命令保持 ACL 设置信息，cp 命令在使用-p，-a 参数时保留 ACL 设置信息。但是如果从一个支持 ACL 的文件系统向一个不支持 ACL 的文件系统(如 FAT)移动或带 ACL 属性的拷贝，则会得到类似下面这样的错误提示，

cp: preserving permissions for `filename': Operation not supported

设置了 ACL 的文件在 ls -l 时可以看到这样的情况，

-rw-rw----+ 1 allen chen 0 Jun 2 09:52 filename

有个加号在第一个列的末尾。

2.4 eCryptfs 加密文件系统

红旗安全操作系统 4.0 使用 eCryptfs 实现加密文件系统特性。eCryptfs 可以对一个文件夹下所有文件和子目录进行加密，使得对这些文件的访问都是加密方式进行的。

例如如果希望对/home/dir 进行加密，可以执行如下类似命令：

```
# mount -t ecryptfs /home/dir /home/dir -o
key=passphrase:passwd=abc,ecryptfs_cipher=aes,ecryptfs_key_bytes=16,
no_prompt
```

这里 abc 是指定的加密密钥，aes 是加密算法，16 是加密位数。

关于 ecryptfs 相关命令的详细参数，请参考第三章。为了简化加密文件系统的管理，红旗安全操作系统也提供了对应的图形工具。

建议 mount 挂载时指定的挂载点与源文件夹相同，这样可以隐藏掉源文件夹中的元数据。此后对文件夹下文件的存取都是以加密方式进行的。如果在下一次 mount 时指定一个错误的密码，将不会得到正确的文件内容。

需要说明的是，当前版本的 eCryptfs 模块不支持文件名加密。也就是说，使用 ls 等命令查看加密目录时列出的是明文文件名列表。

卸载加密文件夹，可以通过 umount 命令进行。

由于加密文件系统密钥可能会在内核层中缓存。为了避免可能的安全问题，请在卸载加密文件夹后，立即运行 keyctl clear @u 命令，清除缓存。

2.5 异常检测与潜在侵害分析

红旗安全操作系统 4.0 提供了异常检测与潜在侵害分析的功能。当有试图入侵系统或对系统做出攻击的行为发生时，被监控的主机会实时报警。

系统可以侦测到的入侵行为与潜在侵害行为有：

- 登录事件
- 达到最大登录失败次数
- 达到最大会话数量
- 非法区域登录
- 非法时间登录
- 程序异常、崩溃
- 开启网卡混杂模式
- 强制访问控制状态的改变
- 改变用户的组
- 监控指定账户
- 监控指定系统调用
- 监控指定文件
- 监控可执行程序
- 监控用户生成可执行程序

按照《红旗安全操作系统 4.0 安装分发手册》4.1 和 4.2 节安装和配置好异常检测及潜在侵害分析功能。一旦有异常事件发生，将弹出警示小窗口，通告异常事件。管理员点击该窗口则可获得事件的详细描述。

2.6 模块更新

红旗软件公司提供给用户以统一的红旗 TSN 技术支持网站(http://support.redflag-linux.com)进行软件和文档的更新和升级支持。任何购买了红旗正式产品的用户都可以登录红旗 TSN 网站以获得相应的更新。

在红旗 TSN 网站的软件更新下载列表中，也不排除今后会提供红旗安全操作系统 4.0 功能模块各组件的软件更新版本。管理员用户从红旗 TSN 网站下载这些安全功能模块的更新包后，再按照软件更新包的操作说明进行更新操作，方能完成正常的安全功能模块的安装更新。

第3章　基本管理

本章描述了安全功能模块的基本管理操作，也就是安全管理员必须熟悉的基本安全事件。这些事件主要包括：

- 系统用户登录过程
- 安全运行模式的设置

  这是最重要的安全管理事件之一。开启安全机制将保证系统中所有主体对客体资源的访问都将受到强制访问控制的约束，所有安全相关事件都将被审计和记录。而关闭安全机制或者将运行模式设置为警告模式则所设定的强制安全访问控制约束将不复存在，系统回归为标准Linux 系统的rwx 访问控制模型。

- 安全标记设置

  这也是常见的安全管理事件。通过对主客体设置上不同的安全标记，系统的强制访问控制才能依据标记比对机制控制主体对客体的访问行为。

- 安全用户管理

  对系统安全用户的增删改操作，将影响系统的涉密主体列表。

- 管理角色的口令管理

  三个管理角色的口令修改也是系统的重要安全事件。

- 审计的启动、停止和设置

  审计模块的管理是也是系统最重要的安全事件之一。

通过本章学习，管理员可以进行基本的安全管理。

3.1　系统用户登录

当选择红旗安全操作系统4.0时，登录过程和普通linux 系统过程是一样的。但时有一些注意方面需要给予提示。系统登录过程大致可以分为两部分本地登录和远程登录。

本地登录又可以分字符终端登录和图形终端登录。

红旗安全操作系统4.0 默认禁止root 用户本地登录(包括终端与图形登录)。

3.1.1　本地字符终端登录

下面以三个管理员为例，说明管理员字符终端登录过程：

```
Login：sysadm (或secadm  auditadm)
Passwd:
[sysadm@localhost~]$ su  -
```

```
Passwd:
[root@localhost~]#
```

3.1.2 本地图形终端登录

出于安全考虑，红旗安全操作系统 4.0 不推荐启动图形终端。但是为了系统管理员管理方便，系统默认仅允许系统管理员启动图形终端。

具体登录过程是：首先系统管理员以字符终端方式登录到系统中，然后运行startx命令进入图形管理环境。

以下是个示例：

```
Login：sysadm
Passwd:
[sysadm@localhost~]$ su -
Passwd:
[root@localhost~]# startx
```

3.1.3 远程终端登录

红旗安全操作系统 4.0 支持用户采用远程登录工具进行远程登录。

下面以系统管理员ssh登录为例,说明管理员远程登录过程：

```
[root@localhost~]# ssh sysadm@192.168.80.70
[sysadm@192.168.80.70]$ su -
[sysadm@192.168.80.70]# newrole -r sysadm_r
```

出于系统安全考虑，红旗安全操作系统4.0 默认不允许root 直接登录系统。如果修改配置允许 root 用户登录，即使 root 用户登录成功，也不具备系统管理员权限，必须通过 newrole 命令接口切换至系统管理员角色。

3.2 安全策略与运行模式

红旗安全操作系统 4.0 中，强制访问控制基于 selinux 框架实现。系统默认提供了两种形式的安全策略：

targeted ：	仅仅保护一些系统服务，一般不使用该策略
mls：	提供基于 BLP、MLS/MCS 模型的完整保护，是系统的默认生效策略

mls 策略是红旗安全操作系统默认安全策略，为系统及应用提供最大化的安全保护。

targeted 为系统提供的可选安全策略，其目标是隔离高风险程序（如暴露在外易受黑客攻击的组件）。使用 targeted 策略的好处是一方面可以向 Linux 系统添加大量的安全保护，同时又尽量少影响现有的用户程序（提高应用软件与系统兼容性），

在红旗安全操作系统中，targeted 策略和 mls 策略之间主要差异是不支持管理特权三权分立，也不支持 BLP 模型。

每种安全策略有三种可选运行模式：

- enforcing(启用)：

  开启系统保护控制。如果有安全违规行为发生，将生成一个审计日志并阻止该非法行为

- permissive(警报)：

  警报模式与启用模式相似，但并不阻止该违规行为而仅仅生成对应安全审计日志记录。管理员可以通过查看审计日志记录来检查安全事件

- disabled(停用)：

  不开启安全功能

对默认安全策略的定义，是通过修改配置文件/etc/selinux/config 完成的。其中 SELINUX 项指定了运行模式，SELINUXTYPE 项指定了安全策略。如下是个示例：

```
SELINUX=permissive
SELINUXTYPE=mls
```

对运行模式的控制，主要是通过执行 setenforce 命令完成的。

要停止安全功能，可以使用如下命令：

```
setenforce 0  或: echo 0 > /selinux/enforce
```

要启用安全功能，可以使用如下命令：

```
setenforce 1  或: echo 1 > /selinux/enforce
```

除非特别说明，本手册描述操作均针对 mls 策略。

3.3 基本操作

系统提供了常用的安全管理命令：

setenforce	设置安全运行模式
getenforce	查看安全运行模式
sestatus	查看安全运行状态
rolepasswd	修改系统、安全、审计管理员密码

下面对这四个基本管理命令一一进行介绍。

所有安全管理相关命令，除非作特别说明，基本均只能以安全管理员身份运行。

setenforce 命令格式为：

选项	描述
enforcing	以启用（Enforcing）模式启动安全功能模块
permissive	以报警（Permissive）模式启动安全功能模块。
1	以启用（Enforcing）模式启动安全功能模块
0	以报警（Permissive）模式启动安全功能模块。

setenforce [enforcing | permissive | 1 | 0]

getenforce 命令用于输出当前的安全运行模式，该命令无任何参数。

sestatus 命令用于显示安全系统的当前状态，命令格式为

sestatus [-v] [-b]

选项	描述
-v	显示/etc/sestatus.conf 文件中，字段为 files 的文件安全上下文。显示字段为 possess 的进程安全上下文。也显示符号连接的目标的安全上下文。
-b	显示安全布尔值。布尔值是安全策略中声明的参数，运行时可以改变。

如下是一个执行示例：

```
# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /selinux
Current mode:                   permissive
Mode from config file:          permissive
Policy version:                 21
Policy from config file:        mls
```

rolepasswd 命令用于修改当前管理员用户口令。该命令仅对三个管理员用户有效。命令无任何参数。

此外，安全标记设置和安全用户管理，都是通过系统接口命令 semanage 进行的。semanage 命令参数很多，具体使用说明，请参阅 4.1.1 节。如果觉得命令使用不太方便，可以直接使用安全管理控制台进

行管理。关于安全管理控制台的使用，请参阅第 5 章。

审计功能的控制，是通过审计服务 auditd 来控制的。该服务只能由审计管理员 auditadm 进行，系统管理员和安全管理员无法控制该服务。

开始审计服务，请执行： service auditd start

停止审计服务，请执行： service auditd stop

重启审计服务，请执行： service auditd restart

第4章　安全管理命令

本章描述了进行安全管理需要掌握的安全管理命令。红旗安全操作系统 4.0 中安全功能模块所提供的安全管理命令有：

分类	命令
安全策略管理	semanage
安全角色切换	newrole
文件标记命令	chcon, restorecon, setfiles, fixfiles
安全策略编译与加载	checkpolicy, load_policy
安全策略布尔值	getsebool, setsebool, togglesebool
安全策略模块管理	semodule, semodule_package, checkmodule
加密文件系统	mount.ecryptfs, umount.ecryptfs
其他命令	rolepasswd, pamusb-conf, pamusb-check,passwd, chage, chpasswd, chfn, chsh, useradd, userdel, usermod

以下将按功能分类分别对这些命令进行逐条说明。

使用命令时需要注意不要超出参数值的合理范围，否则会有警告提示，命令执行也无法成功。

另外，如果直接输入命令名而不带任何参数，则输出该命令的简单帮助。详细的命令使用说明，可以查看该命令的 man 手册。

4.1　安全策略管理

4.1.1 semanage

- 命令名：semanage
- 命令功能：selinux 策略管理工具
- 命令格式：

```
semanage {login|user|port|interface|fcontext|translation} -l [-n]
semanage login -{a|d|m} [-sr] login_name
semanage user -{a|d|m} [-LrRp] selinux_name
semanage port -{a|d|m} [-tr] [-p protocol] port | port_range
```

semanage interface -{a|d|m} [-tr] interface_spec

semanage fcontext -{a|d|m} [-frst] file_spec

semanage translation -{a|d|m} [-T] level

- 命令参数：

-a, --add

增加一条对象记录

-d, --delete

删除一条对象记录

-f, --ftype

指定文件类型。这一选项在操作 fcontext 的时候有效。需要按照 ls 的模式位来指定文件类型。

例如： 用-d 来表示文件夹，--来表示普通文件。

-h, --help

显示帮助信息

-l, --list

列出所有对象

-L, --level

指定 selinux 使用的安全级别，默认为 s0。

-m, --modify

修改一个对象记录

-n, --noheading

在列出所有对象时不打印头部信息

-p, --proto

指定端口的类型(tcp|udp)。

-r, --range

指定安全级别范围。

-R, --role

指定 selinux 角色。如果指定多个角色需用双引号括起所有角色名，并用空格分隔。或者多次使用-R 指定。

-P, --prefix

指定 selinux 前缀。

-s, --seuser

指定 selinux 用户名。

-t, --type

指定对象的 selinux 类型。

-T, --trans

指定 selinux 翻译。

- 命令说明：

semanage 不需要修改或重新编译 selinux 策略源文件便能够配置 selinux 策略的某些元素。包括： Linux 用户名到 selinux 用户标识的映射，各种对象的安全上下文映射(网络端口、接口、主机、 文件等)。

举例说明：

通过 semanage user 新建安全用户 keyuan_u，然后将安全用户 keyuan_u 与系统用户 keyuan 进行映射，这样当系统用户 keyuan 登录系统是，自动具有安全用户 keyuan_u 所有权限。具体可以执行如下类似命令：

```
/* 安全用户管理 */
#semanage user -a -R user_r -P user -r s0 -L s0 keyuan_u
# semanage user -l | grep keyuan_u
keyuan_u    user       s0         s0             user_r
/* 系统用户与安全用户映射 */
#semanage login -a -s keyuan_u -r s0  keyuan
#semanage login -l | grep keyuan
keyuan                    keyuan_u                  s0
/* 网络端口管理 */
#semanage port -a  -t oracle_port_t  -p tcp 1521
# semanage port -l | grep oracle
oracle_port_t                  tcp      1521
```

semanage login 命令处理从系统用户到安全用户的映射，而 semanage user 命令处理从安全用户到授权角色集合的映射。大多数情况下，只有前者有可能由管理员调整，后者由系统模块定义并且通常不需要修改。

4.2 角色切换

4.2.1 newrole

- 命令名：newrole

- 命令功能：添加、删除、修改安全用户与系统用户的映射。
- 命令格式：

  newrole [-r|--role] ROLE [-t|--type] TYPE [-l|--level] LEVEL [-- [ARGS]...]
- 命令参数：

  -r

  要切换到的角色。

  -r

  安全等级的范围

  login_name

  系统用户名称
- 关联命令：

  su, runas
- 命令说明：

此命令会在新的上下文中运行一个新的 shell。新的上下文继承自旧的上下文，并且会首先执行 newrole 命令。如果给出了-r 或者--role 选项，则新的上下文会使用-r 或--role 所指定的角色。如果给出了-t 或--type 选项， 则新的上下文会使用-t 或—type 所指定的域类型。 如果指定了角色名而没有指定域类型，则使用角色的默认域类型。如果给出了-l 或—level 选项，则新的上下文使用-l 或--level 指定的敏感等级或安全级别范围。

新的 shell 将会是/etc/passwd 中指明的相应用户的 shell。

举例说明：

系统管理员系统进行远程登录时，默认安全上下文为 root:staff_r:staff_t:s0-s15:c0.c1023

可以通过 newrole 命令切换到 root:sysadm_r:sysadm_t:s0-s15:c0.c1023 安全上下中。

```
# id -Z
root:staff_r:staff_t:s0-s15:c0.c1023
# newrole -r sysadm_r
口令：
# id -Z
root:sysadm_r:sysadm_t:s0-s15:c0.c1023
```

出于特权分立的要求，不允许三个特权角色间使用 newrole 命令进行角色切换。

4.3 文件/目录标记命令

4.3.1 chcon

- 命令名：chcon
- 命令功能：改变客体(文件/目录)安全上下文或者部分安全上下文。
- 命令格式：

  chcon [OPTION]... CONTEXT FILE...

  chcon [OPTION]... --reference=RFILE FILE...
- 命令参数：

  FILE

  被改变安全属性的客体文件/目录名。

  -R

  递归列出所有子目录。

  -t

  改变安全上下文中的类型

  -u

  改变安全上下文中的安全用户

  -r

  改变安全上下文中的角色

  -l

  改变安全上下文中的安全等级范围
- 命令说明：

  改变客体(文件/目录)安全上下文。

chcon 是文件标记最基本的命令。用法类似普通 linux 的 chmod 命令。

举例说明：

新建目录 public_html，然后改变安全上下文类型为 httpd_user_content_t，并查看修改后结果

```
# chcon -t httpd_user_content_t public_html/
# ls -dZ public_html/
drwxrwxr-x  joe joe joe:object_r:httpd_user_content_t public_html/
```

4.3.2 restorecon

- 命令名：restorecon
- 命令功能：恢复客体(文件/目录)到默认安全上下文。
- 命令格式：

  restorecon [-o outfilename] [-R] [-n] [-v] [-e directory] pathname...

  restorecon -f infilename [-o outfilename] [-e directory] [-R] [-n] [-v] [-F]

- 命令参数：

  pathname

  需要恢复的文件/目录路径名。

  -o outfilename

  保存具有不正确安全上下文的文件列表

  -R

  递归所有子目录。

  -e

  排除相应目录。

  -n

  不改变任何文件/目录安全上下文

  -v

  显示在恢复标记中详细信息。

  -F

  强制恢复文件/目录安全上下文

- 命令说明：
- restorecon 在恢复标记过程中，不进入符号连接。

举例说明：

由于系统内置 oracle 数据库应用程序文件文件上下文，当 oracle 安装在/opt 目录下，可以通过下列命令设置 oracle 所有文件的安全上下文。

```
# restorecon -R /opt/oracle
```

restorecon 命令与 chcon 命令相似，但是 restorecon 是基于当前策略的安全上下文标记进行恢复改变。因此 restorecon 不需要指定要改变的安全上下文。

restorecon 适合于系统文件标记变化比较小情况，如果要标记整个文件系统建议采用 setfiles 或者 fixfiles。

4.3.3 setfiles

- 命令名：setfiles
- 命令功能：设置文件的安全上下文。
- 命令格式：

  setfiles [-c policy] [-d] [-l] [-n] [-e directory] [-o filename] [-q] [-s] [-v] [-vv] [-W] [-F] spec_file pathname

- 命令参数

  -c

  检查指定的二进制策略文件中安全上下文的有效性。

  -d

  显示每个文件对应的规约。

  -l

  将文件标签的改变记录到系统日志中。

  -n

  不改变任何文件标签。

  -q

  忽略除出错提示外的其他信息。

  -r rootpath

  使用可选的根路径。

  -e directory

  指定不需设置安全上下文的文件夹(可设置多个)。

  -F

  强制重设的上下文必须与 file_context 中的上下文匹配。

  -o filename

  将错误的上下文列表输出到指定文件。

  -s

  从标准输入读入文件列表来代替在命令中指明路径。

  -v

  当类型或角色变化时显示文件标签的变化信息。

  -vv

当类型、角色或用户变化时显示文件标签的变化信息。

-W

当没有匹配文件时显示警告信息。

spec_file

由以下部分组成： regexp [-type] (context | <<none>>)，其中的类型选项为可选，用 ls 命令的类型位来指定。例如：--只匹配普通文件，-d 只匹配文件夹。 context 项可以是普通的安全上下文或使用<<none>>来表示不改变该文件的上下文。如果一个文件有多个硬链接，这多个链接被多个规约所匹配，并且每个规约都指定了不同的安全上下文，这时候程序会给出警告信息，但是文件仍然会被除了<<none>>之外的最后匹配到的那个规约所标记。

pathname

pathname 项指定了每个文件系统需要被标记的根目录。如果指定了-s 选项，则这一项不需要给出。

- 关联命令：

load_policy, checkpolicy

- 命令说明：

setfiles 用来在一个或多个文件系统上初始化安全上下文数据库(扩展属性)。此程序最初会作 为 selinux 安装过程中的一部分来运行。setfiles 也可以在任何时刻运行，用来修正错误，支持新的策略，或者使用-n 选项来检查文件上下文是否符合预期。

setfiles 该命令不能跨挂载点进行标记。这意味着在每个文件系统上都得运行一次这个命令，通常都会使用 fixfiles，除非有特殊要求时才会使用 setfiles。

4.3.4 fixfiles

- 命令名：fixfiles
- 命令功能：修复文件的 selinux 安全上下文。
- 命令格式：

```
fixfiles [-F] [ -R rpmpackagename[ , rpmpackagename...] ]
[ -C PREVIOUS_FILECONTEXT ] [-l logfile] [-o outputfile]
{ check | restore | [-F] relabel | verify }”
```

```
fixfiles [-F] [-l logfile] [-o outputfile] { check | restore | [-f] relabel |
verify } [[dir/file] … ]
```

- 命令参数

-l logfile

将输出保存到指定的日志文件。

-o outputfile

将所有上下文与默认值不同的文件名输出到指定文件。

-F

强制重设的上下文必须与 file_context 中的上下文匹配。

-f

删除/tmp 文件夹时不询问用户是否删除，默认删除/tmp 文件夹。

-R rpmpackage[, rpmpackage...]

使用 rpm 数据库查询指定 rpm 包所包含的文件，并恢复其文件上下文。 -a 选项给出时可以取得在 rpm 数据库中的所有文件。

-C PREVIOUS_FILECONTEXT

使用 diff 命令来比较 PREVIOUS_FILECONTEXT 所指定的文件与当前安装的文件，然后恢复所有受影响的文件。

下列参数选其中之一：

check

打印出所有错误的文件上下文标签，对比旧的和当前的，但是不修正安全上下文

restore

修正所有错误的安全上下文标签所有错误的文件上下文标签，对比旧的和当前的，但是不修正安全上下文。

relabel

当删除/tmp 文件夹下的内容时询问用户是否删除，然后根据 file_contexts 所指定文件的匹配结果修复错误的文件上下文标签。

Verify

列出错误文件上下文标签的文件名，但是不做任何修改。

[[dir/file] …]

列出想检查其文件上下文的文件或目录树。

- 关联命令：

  setfiles， restorecon

- 命令说明：

  fixfiles 用来在文件系统上修正安全上下文数据库(扩展属性)。fetfiles 也可以在任何时刻运行，用来支持新的策略，或者检查文件上下文是否符合您的预期。只要文件系统在挂载时没有给出安全安全上下文选项，fixfiles 默认会重新标记所有已挂载的 ext2，ext3, xfs 和 jfs 文件系统。可以给出-R 选项来修复 rpm 包的安全上下文。

fixfiles 命令实际上是一个shell 脚本，依请求不同它分别可以调用restorecon 或setfiles 命令。fixfiles 与上述几个文件标记命令相比，适合于系统文件标记变化比较大场合。同时该命令可以跨挂载点进行标记

使用举例：利用 mls 策略安全上下文标记库，重新标记整个安全系统。不一致结果存放在 result 文件

中，日志保存在 olog 日志中。

```
   #    fixfiles    -l    olog    -o    result    -C    /etc/selinux/mls
/contexts/files/filecontexts restore
```

4.3.5 自动标记

除了使用与文件有关的客体标记命令重新标记整个系统外，在系统重启时也会自动重新标记，只需要在根文件系统下创建一个/.autorelabel 文件即可，

```
   # touch /.autorelabel
```

另外，当系统进行引导时，也可以通过 grub 内核参数,加入 autorelabel，将进行标记整个文件系统。

如果系统从 disabled 安全运行模式，转变为 permissive 或者 enforcing 运行模式时，系统启动时，会自动标记。

如果需要对整个文件系统重新修复安全标记，请以安全管理员身份执行命令：touch /.autorelabel，然后重启系统。

重新标记文件系统建议在系统处于良好状态下进行。

4.4 配置安全策略

4.4.1 checkpolicy

- 命令名：checkpolicy
- 命令功能：selinux 的策略编译器。
- 命令格式：

  checkpolicy [-b] [-d] [-M] [-c policyvers] [-o output_file] [input_file]

- 命令参数：

  -b

  程序不读入策略配置文件，而是读入一个已经存在的二进制策略文件。

  -d

  加载策略后进入调试模式

  -M

  编译策略

  -o filename

  以指定的文件名输出二进制策略文件

  -c policyvers

  指定策略版本，默认为最新

- 命令说明：

checkpolicy 是 selinux 的策略编译器，它可以检查、编译策略配置文件，并最终生成可加载到内核的二进制文件。 如果没有给出输入文件，则 checkpolicy 会尝试读入 policy.conf 或 policy(-b 选项给出)。

4.4.2 load_policy

- 命令名：load_policy
- 命令功能：加载新的 selinux 策略到内核中。
- 命令格式：

load_policy [-bq]

- 命令参数：

-b

重置装载策略的布尔值

-q

不显示警告信息

- 命令说明：

load_policy 是一个用来加载/替换内核中策略的工具。 当加载新策略时，load_policy 默认会保留旧策略的布尔值

由于新策略的加载将引起安全访问控制规则上的变化，对于已部署业务应用的安全系统下的新策略加载，请先停掉正在运行的业务应用。加载完毕后再重新启动应用。

4.5 安全策略布尔值管理

4.5.1 getsebool

- 命令名：getsebool
- 命令功能：查看 selinux 的布尔值
- 命令格式：

getsebool [-a] [booleans]

- 命令参数：

-a

显示所有 selinux 的布尔值

- 关联命令：

setsebool

- 命令说明：

getsebool 显示指定的或所有的 selinux 布尔值。在某些情况下，一些布尔值正处于已被修改但还没有保存的状态。getsebool 会显示这些布尔值修改后的状态，并将在下次提交其他布尔值的改变时保存这些未生效的布尔值。

设置布尔值需要经过两个步骤：一是改变布尔值的状态，二是将这些状态提交。这样就可以使一组布尔值的改变在同一操作后生效。

举例说明：

显示布尔 user_ping 当前值

```
# getsebool user_ping
user_ping --> on
```

4.5.2 setsebool

- 命令名：setsebool
- 命令功能：设置 selinux 的布尔值
- 命令格式：

  setsebool [-P] boolean value | bool1=val1 bool2=val2 ...
- 命令参数：

  -P

  将布尔值的改变写入策略文件。
- 关联命令：

  getsebool, togglesebool
- 命令说明：

setsebool 改变特定的一个或一组布尔值的状态。value 项如果为 1、ture 或 on，则将此布尔值的状态设置为打开；如果为 0、false 或 off，则将此布尔值的状态设置为关闭。

如果给出-P 选项，只改变当前布尔值的状态，默认值没有被改变，下次系统重新启动时仍然使用默认值。

如果给出了-P 选项，则将所有当前状态写入策略文件，系统重启后这些改变仍然有效。

举例说明：

设置布尔 user_ping 当前值为 off

```
# setsebool user_ping off
# getsebool user_ping
user_ping --> off
```

4.5.3 togglesebool

- 命令名：togglesebool
- 命令功能：翻转 selinux 的布尔值
- 命令格式：

  togglesebool boolean...
- 关联命令：

  getsebool, setsebool
- 命令说明：

  togglesebool 翻转布尔值的当前状态。如果当前状态为打开，则将其设为关闭，反之亦然。togglesebool 只改变内存中的布尔值，并不保存到策略文件，下次重启系统后会失效。

4.6 安全策略模块管理

4.6.1 semodule

- 命令名：semodule
- 命令功能：管理内存安全策略模块
- 命令格式：

  semodule [options]... MODE [MODES] ...
- 命令参数：

  -R, --reload

  强制重新装载策略

  -B, --build

  强制重新编译生成策略(如果-n 选项未给出，默认生成后重新装载)

  -i, --install=MODULE_PKG

  安装/替换策略模块包

  -u, --upgrade=MODULE_PKG

  升级一个已经存在的策略模块包

  -b, --base=MODULE_PKG

  安装/替换基本策略模块包

  -r, --remove=MODULE_PKG

  删除已经存在的模块

  -l, --list-modules

列出除了基本模块之外的所有已安装的模块

-s, --store

要操作的存储名称

-n -noreload

提交之后不重新装载策略

-h, --help

打印帮助信息

-v, --verbose

冗余模式

- 关联命令：

checkmodule, semodule_package

- 命令说明：

semodule 是用来管理 selinux 策略模块的工具，包括安装、升级、列出、删除模块。semodule 也可以用来强制重新生成、装载模块。semodule 操作由 semodule_package 生成的模块包。这些模块包文件通常以.pp 作为后缀。

举例说明：

添加，显示，删除，安全策略模块

```
# semodule -i server.pp
# semodule -l | grep server
 server  1.0.0
# semodule -r server
```

4.6.2 semodule_package

- 命令名：semodule_package
- 命令功能：创建策略模块包
- 命令格式：

semodule_package -o <output file> -m <module> [-f <file contexts>]

- 命令参数：

-o, --output <output file>

生成的策略模块包

-s, --seuser <seuser file>

指定包含的 seuser 文件

-u, --user_extra <user extra file>

指定包含的 user_extra 文件

-m, --module <Module file>

指定包含的 module 文件

-f, --fc <File context file>

指定包含的 file context 文件

-n, --nc <netfilter context file>

指定包含的 netfilter_context 文件

- 关联命令：

  checkmodule, semodule

- 命令说明：

semodule_package 是用来从二进制策略模块创建 selinux 策略模块包，也可以包含一些其他文件，比如文件上下文等。semodule_package 创建的文件可以通过 semodule 命令安装到系统上。

4.6.3 checkmodule

- 命令名：checkmodule
- 命令功能：selinux 策略模块编译器
- 命令格式：

  checkmodule [-b] [-m] [M] [-V] [-o output_file] [input_file]

- 命令参数：

  -b

读入已经存在的二进制策略文件而不是策略源代码文件。这一选项提供辅助开发、调试的功能。

-m

创建非基本策略模块

-M

在检查、编译时提供对 MLS/MCS 的支持

-v

显示生成的策略模块的版本号

-o filename

生成由 filename 指定文件名的二进制策略模块文件。如果-o 选项没有给出，则只进行语法检查。

- 关联命令：

  semodule，semodule_package

- 命令说明：

  checkmodule 是一个检查、编译 selinux 安全策略模块，生成策略的二进制表达的工具。它可以生成基本模块或非基本模块。

4.7 ACL 控制

4.7.1 setfacl

- 命令名：setfacl
- 命令命令功能：设置 ACL 列表
- 命令格式：setfacl [-bkndRLPvh] [{-m|-x} acl_spec] [{-M|-X} acl_file] file
- 命令参数：

-b,--remove-all

删除所有扩展的 acl 规则，基本的 acl 规则(所有者，群组，其他)将被保留。

-k,--remove-default

删除缺省的 acl 规则。如果没有缺省规则，将不提示。

-n，--no-mask

不要重新计算有效权限。setfacl 默认会重新计算 ACL mask，除非 mask 被明确的制定。

-d，--default

设定默认的 acl 规则。

-R，--recursive

递归的对所有文件及目录进行操作。

-L，--logical

跟踪符号链接，默认情况下只跟踪符号链接文件，跳过符号链接目录。

-P，--physical

跳过所有符号链接，包括符号链接文件。

-v，--version

输出 setfacl 的版本号并退出。

-h，--help

输出帮助信息。

选项-m 和-x 后边跟以 acl 规则。多条 acl 规则以逗号(,)隔开。选项-M 和-X 用来从文件或标准输入读取 acl 规则。

acl_spec

ACL 规则，setfacl 命令可以识别以下的规则格式：

[d[efault]:] [u[ser]:]uid [:perms]

指定用户的权限，文件所有者的权限(如果 uid 没有指定)。

[d[efault]:] g[roup]:gid [:perms]

指定群组的权限，文件所有群组的权限(如果 gid 未指定)

[d[efault]:] m[ask][:] [:perms]

有效权限掩码

[d[efault]:] o[ther] [:perms]

其他的权限

对于 uid 和 gid，可以指定一个数字，也可指定一个名字。perms 域是一个代表各种权限的字母的组合：读-r 写-w 执行-x，执行只适合目录和一些可执行的文件。pers 域也可设置为八进制格式。

4.7.2 getfacl

- 命令名：getfacl
- 命令命令功能：查看文件 ACL 列表。
- 命令格式：getfacl 文件名

4.8 加密文件系统

4.8.1 mount.ecryptfs

- 命令名：mount
- 命令功能：挂载加密文件夹。
- 命令格式：mount -t ecryptfs <源文件夹> <目的文件夹> [-o [key=passphrase:passwd=<密码>][,ecryptfs_cipher=<加密算法>][,ecryptfs_key_bytes=<加密位数>][,no_sig_cache][,ecryptfs_passthrough][,no_prompt]]
- 命令参数：

  -o

  指定附加选项，至少后跟一项。

  <源文件夹>

  指定元数据文件夹。

  <目的文件夹>

  指定需要挂载到的目的文件夹。

  key=passphrase:passwd=<密码>

  指定挂载密码。

ecryptfs_cipher=<加密算法>

指定加密算法，目前有 aes，blowfish，des3_ede，twofish，cast6，cast5，des 可供选择。

ecryptfs_key_bytes=<加密位数>

指定加密位数，aes 支持 16、24、32 位；blowfish 支持 16、32 位，des3_ede 支持 24 位，twofish 支持 32 位，cast6 支持 32 位，cast5 支持 16 位，des 支持 8 位。

no_sig_cache

不检查密码指纹是否在~/.ecryptfs/sig-cache.txt 中，适合于非交互模式使用。

ecryptfs_passthrough

允许元数据文件夹中未加密的文件在挂载后仍可以被读写，未指定该选项则此功能默认关闭。

no_prompt

强止使用非交互模式，没有指定的选项将不会提示用户进行选择，而是直接使用默认选项。

- 命令说明：

在没有 no_prompt 选项下，如果遇到用户没有指定的选项，将会提示用户选择输入。加密算法和加密位数不匹配，挂载会失败。密码输入错误不影响。

4.8.2 umount.ecryptfs

- 命令名：umount
- 命令功能：卸载加密文件夹。
- 命令格式：umount <加密文件夹挂载点>

4.9 其他命令

4.9.1 rolepasswd

- 命令名：rolepasswd
- 命令功能：修改当前登入角色的密码。
- 命令格式：rolepasswd
- 关联命令：newrole
- 命令说明：

rolepasswd 只能修改当前登入角色的密码，传给它的任何参数都会被忽略。成功修改后，不需要用户立即重新登陆。SELinux 禁用情况下，此命令给出无法获得安全上下文信息，不会对系统做任何改动。

4.9.2 pamusb-conf

- 命令名：pamusb-conf
- 命令功能：USB Key 认证配置工具

- 命令格式：pamusb-conf [--help] [--verbose] [--config=路径] [--add-user=账户名 | --add-device=设备名]
- 命令参数：

  --help，或：-h

  显示帮助信息。

  --verbose，或：-v

  显示细节输出。

  --config=<路径>，或：-c <路径>

  指定配置文件路径，默认/etc/pamusb.conf。

  --add-user=<账户名>，或：-u <账户名>

  指定需要添加的账户名。

  --add-device=<设备名>，或：-d <设备名>

  为需要添加的新设备自定义便于标识的设备名。
- 关联命令：pamusb-check
- 命令说明：

  目前 USB Key 认证支持 USB 存储设备及 MMC 卡。

4.9.3 pamusb-check

- 命令名：pamusb-check
- 命令功能：USB Key 认证配置检查及验证工具
- 命令格式：pamusb-check [--help] [--debug] [--config=<路径>] <账户名>
- 命令参数：

  --help，或：-h

  显示帮助信息。

  --debug，或：-D

  显示调试输出。

  --config=<路径>，或：-c 路径

  指定配置文件路径，默认/etc/pamusb.conf。

  <账户名>

  指定需要检验的账户名。
- 关联命令：pamusb-conf

4.9.4 passwd， chage， chpasswd， chfn， chsh， useradd，

userdel，usermod

- 命令说明

试图用这些命令修改/增加/删除 sysdam_r、secadm_r、auditadm_r、staff_r、user_r 等角色账户的相关信息，将会得到账户已被保留的错误信息。但 selinux 没有启用时，这些命令和标准 Linux 系统行为一致。

第5章　安全管理控制台

为了简化管理员安全管理的工作量，红旗安全操作系统 4.0 提供了丰富的图形化的安全管理工具。其中，安全和审计管理控制台是分布式节点的远程集中化管理工具，可以同时对多台安全主机节点进行远程集中化管理。

安全管理控制台提供了安全管理员对系统进行安全控制的所有控制参数，包括安全状态、布尔值、文件上下文、安全登录、安全用户、安全级别翻译、安全端口、安全策略模块的配置。

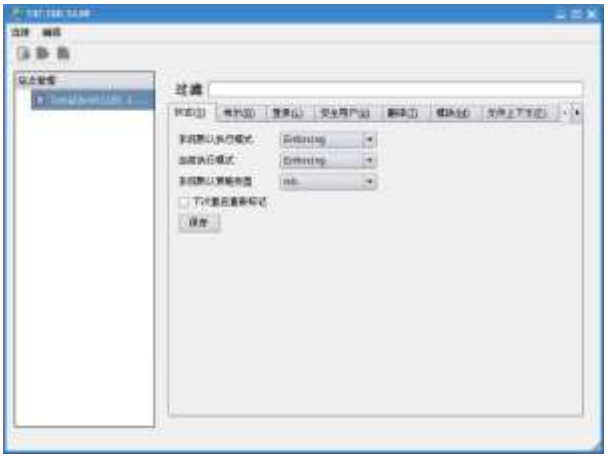
审计管理控制台提供了审计管理所有能够配置的控制参数，提供了对审计状态的配置与查询，审计日志的条件查询以及审计规则配置等功能。

本章将详细介绍安全管理控制台的使用。关于管理控制台的安装和前期配置，请参考《红旗安全操作系统 4.0 安装分发手册》第 4 章。

安全和审计管理控制台建议运行于 1024x768 或者更高的分辨率上，否则很可能显示不完整。

5.1　安全管理控制台

点选开始菜单中的“安全管理”，或者在命令终端键入 seconfig，将启动如下安全管理控制台的主界面。



安全管理控制台

安全管理控制台 seconfig 提供对安全状态、布尔值、文件上下文、安全登录、安全用户、安全级别翻译、安全端口、安全策略模块的配置。

5.1.1 添加连接

安全管理控制台可以在一台管理终端上管理多台安装有红旗安全操作系统的安全节点。在管理安全节点之前，必须先添加与被管理节点的安全连接。

该连接在通讯过程中实行了传输加密，不会引发信息泄密问题。

用户可以在“连接”菜单栏选择“添加连接”项打开连接主机对话框。

连接主机

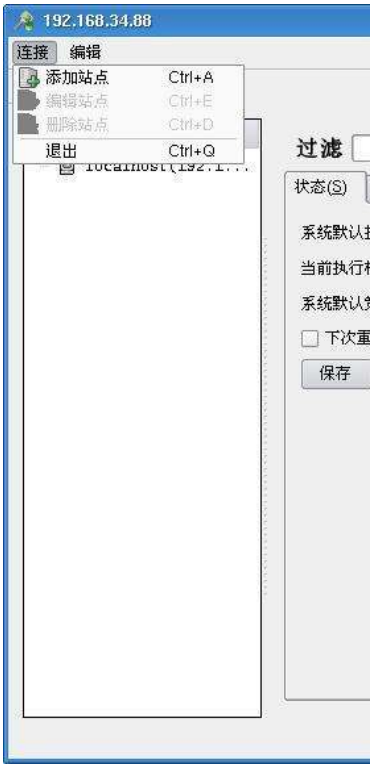
输入远程主机的 IP 地址以及管理用户名和密码，验证无误将建立连接。

连接协议被固定为安全 https，端口为 5989。

5.1.2断开和切换连接

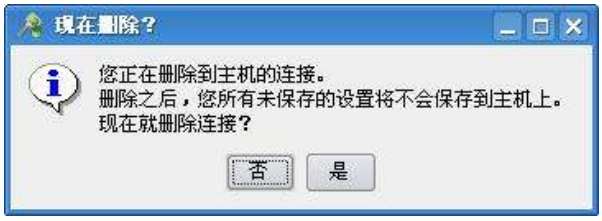
用户可以在文件菜单栏选择“删除站点”来断开当前连接。

（正确的操作是，用户必须先在主机列表中选择一个主机，这样“连接”下拉菜单中的“编辑站点”和“删除站点”选项才可点，如果不选主机，编辑和删除两项是灰的不可选。）



连接管理

当用户点击“删除站点”后，会出现确认对话框，确认后完成删除。未保存到远程主机的改动在断开连接后会被丢弃。



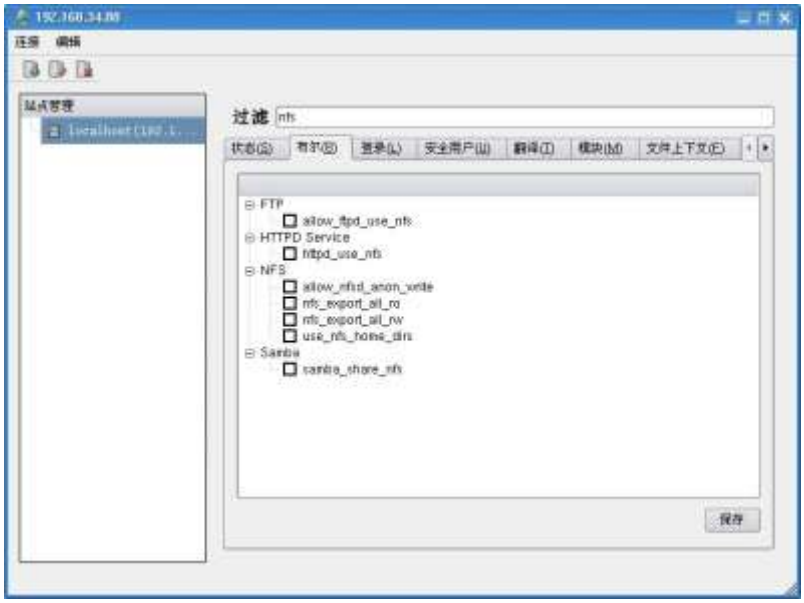
删除连接

程序界面的右边为主机列表，单击您想要切换到的主机来完成切换。

切换连接

5.1.3过滤功能

安全配置工具提供过滤功能，在过滤输入框中输入您想要查找的关键字并按回车键后，在当前选项卡中，所有含有该关键字的配置项都会被显示出来，而其他不包含该关键字的配置项则会被隐藏。清空关键字并按回车键会显示全部配置项。



5.1.4 安全状态

单击“状态”选项卡进入安全状态设置。在安全状态设置中，可以设置：系统默认的执行模式、当前执行模式、系统默认策略类型以及下次重启时是否进行重新标记。

系统默认执行模式共有三种：disabled, permissive, enforcing. 主机每次启动后会默认执行该模式。对系统默认执行模式的设置将会在系统重启后生效。

当系统默认执行模式不是 disabled 时，可以通过设置当前执行模式来即时切换 permissive 与 enforcing 这两种状态。当系统默认执行模式为 disabled 时，则“当前执行模式”项不可被设置。

默认的安全策略类型是 mls。除非需要降低或者不启用系统的强制安全控制能力，否则，系统默认策略类型不建议做更改。

如果点选“下次重启重新标记”，则将在下次重启系统时对整个文件系统自动进行文件安全标记设置。

系统默认策略类型的设置与是否进行重新标记的设置都将会在系统重启后生效。

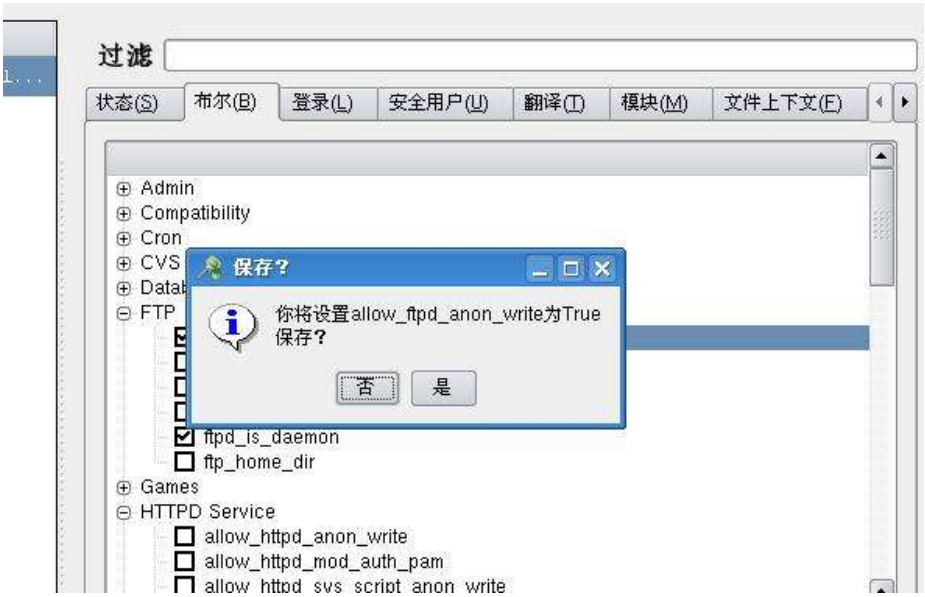
在设置完成后，您需要点击下方的“保存”按钮将这些设置保存到您所管理的主机上，如果未作保存，这些设置会在您切换到其他选项卡或者断开连接时丢失。

安全状态设置

5.1.5 布尔值

点击“布尔”选项卡可以进行布尔值的设置。单击每一项前面的复选框可以将布尔值设为真或假。完成设置后须点击有下方的“保存”按钮保存到主机上。程序会对每一项布尔值的改变给出确认提示(未

确认的项将不会改变)，在所有确认完成后，程序会给出设置成功的提示。



布尔值设置

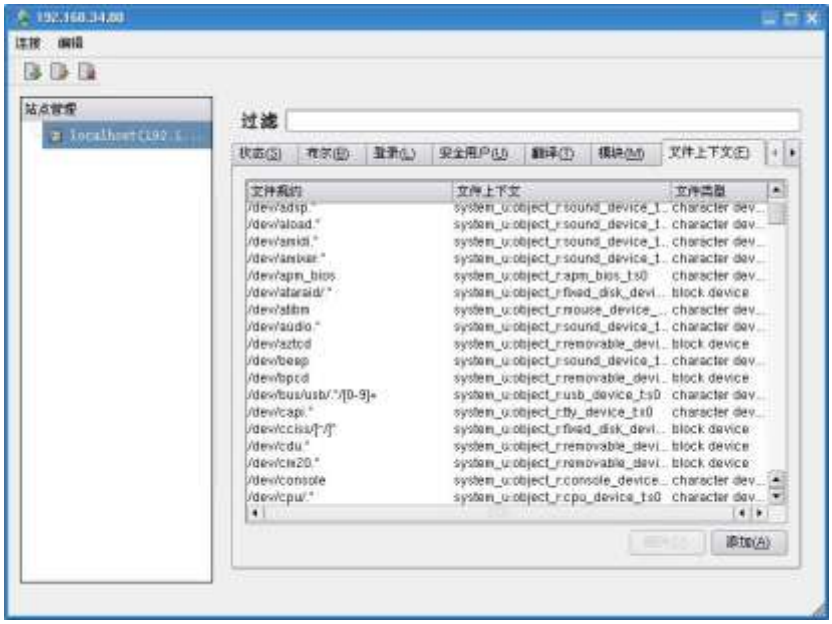
5.1.6 文件上下文

在“文件上下文”选项卡中，可以添加、修改或删除文件标签。

点击右下方的“添加”按钮进行添加，双击文件标签进行修改，选中要删除的文件标签并点击有下方的“删除”按钮进行删除。删除操作会给出确认对话框。

在”文件上下文“配置页面中，文件标签会以文件规约、文件上下文和文件类型的格式显示在页面中。文件上下文包括：安全用户名、角色名、安全类型和安全级别，之间用双引号分隔。

添加文件标签：在弹出的对话框中输入文件规约，即文件路径(支持通配符)。然后选择文件类型，文件类型包括：所有文件、普通文件、目录、字符设备、块设备、套接字、符号链接和有名管道。然后输入文件的安全类型和安全级别，点击确定按钮。



安全上下文

5.1.7 安全登录

在“登录名称”选项卡中，可以添加、修改或删除现有的安全登录。

点击右下方的“添加”按钮进行添加，双击安全登录项进行修改，选中要删除的安全登录并点击有下方的“删除”按钮进行删除。删除操作会给出确认对话框。

安全登录管理

5.1.8 安全用户

在“安全用户”选项卡中，可以添加、修改或删除安全用户

点击右下方的“添加”按钮进行添加，双击安全用户项进行修改，选中要删除的安全用户并点击有下方的“删除”按钮进行删除。删除操作会给出确认对话框。

安全用户管理

5.1.9 安全级别翻译

安全级别翻译完成了将量化的安全级别映射成容易记忆的文字翻译，或者说是给对应的安全级别起个文字别名。

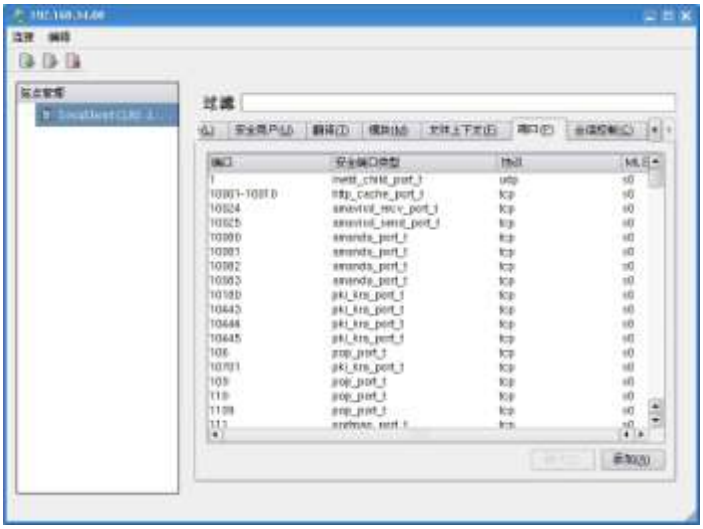
在“翻译”选项卡中，可以添加、修改或删除安全级别翻译。

点击右下方的“添加”按钮进行添加，双击安全级别翻译项进行修改，选中要删除的翻译并点击有下方的“删除”按钮进行删除。删除操作会给出确认对话框。

安全翻译

5.1.10 安全端口

在“端口”选项卡中，可以添加、修改或删除安全端口。这些端口配置，可以在安全策略中被引用。



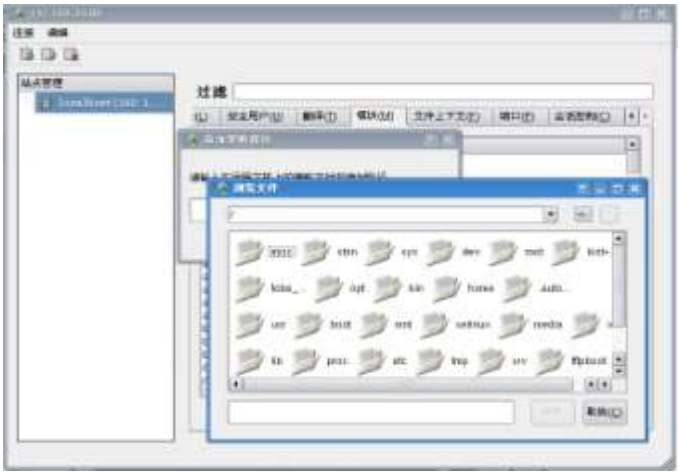
安全端口

5.1.11 安全策略模块

在“模块”选项卡中，可以添加或删除安全策略模块。

点击右下方的“添加”按钮进行添加，选中要删除的端口并点击有下方的“删除”按钮进行删除。删除操作会给出确认对话框。

添加操作会要求用户输入策略模块文件在远程主机上的绝对路径，用户还可以通过文件对话框从远程主机上选择想要添加的策略模块文件。



策略模块

第6章　审计管理

本章将详细介绍红旗安全操作系统 4.0 提供的强大易用的审计管理控制台以及审计系统的配置。

红旗安全操作系统 4.0 的审计系统主要由运行在核心态的 kaudit 后台进程和用户态的 auditd 守护进程协同工作完成对安全事件的审计。kaudit 核心进程负责完成核心空间审计事件的收集并定向发送给在用户态空间运行的 auditd 守护进程，而 auditd 守护进程再通过事件队列机制将审计记录分发给日志写入进程完成审计日志的记录。

从用户空间来看，审计系统是通过 auditd 后台进程接收内核审计系统传送来的审计信息，并将记录写入到/var/log/audit/audit.log。当 auditd 没有运行时，内核将审计信息传送给 syslog 日志守护进程，审计记录将记录到/var/log/message 系统日志中。

auditd 的主要配置文件是/etc/auditd.conf，另一个是/etc/audit.rules，定义了启动时装载的审计规则。

6.1　审计管理控制台

审计管理控制台 auconfig 是红旗安全操作系统 4.0 安全功能套件中提供的一个可选的集中化管理器和远程控制台，可以同时对多台安全主机节点进行远程集中化管理。所提供的管理控制包括各审计子功能模块的启停和运行状态查看，审计日志的查询，和审计规则和策略的配置等等。通过 auconfig，审计管理员可以在一台主机上直观地监控和管理所有审计节点的状况。由于 auconfig 和各主机节点上的代理后台服务程序通过 SSL 加密传输数据，管理员不必担心传输中的数据安全。

6.1.1控制台界面

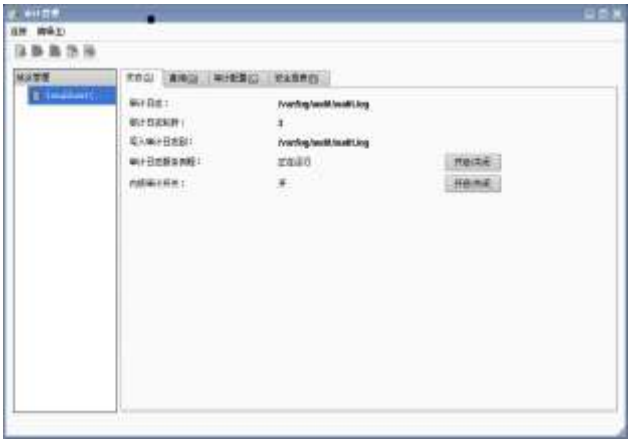
点选开始菜单中的“审计管理”，或者在命令终端中输入 auconfig，将启动如图所示的审计管理控制台。

除控制台主界面由左、右两部分视图组成。

左视图是管理器管理的主机列表。通过 https 协议连接网络上的任意一台安全节点主机。

当连接建立时，左视图显示连接的协议、ip、端口等相关信息；右视图显示分别为状态、查询、审计配置和安全报表。当标签页为“状态”时，右视图显示为主机的审计的状态、审计日志轮转、当前审计日志服务例程和系统日志服务例程的状态、审计日志存储路径，并控制内核审计的开关。当标签页为“查询”页时，可以按照多种查询条件检索审计事件。当标签页为“审计配置”时，可以定制审计系统的配置项。当标签页为“安全报表”时，可以基于审计记录生成图形化的安全报表。

若点选“开启/关闭”按钮，可以控制审计日志服务例程 auditd 以及 kaudit 内核审计的开启和关闭。也可以通过 service auditd start,service auditd stop 命令来操作审计日志服务例程 auditd 的状态。或者通过 auditctl -e 1/0 来控制内核审计 kaudit 的开关。



管理控制台视图

6.1.2 审计记录查询

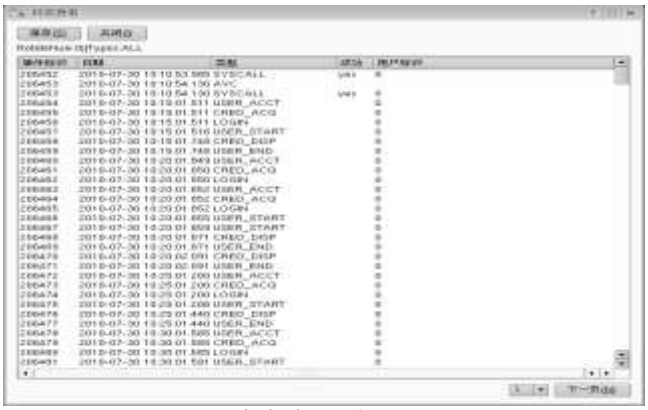
选择相应的类型和查询条件后，点击“查询”按钮就可以获得相应的查询结果。

提供的查询条件有：事件类型、事件标识/关键字、命令、用户/组标识、系统调用、主机名、文件/程序名、进程/父进程标识、开始/结束时间、事件结果(成功/失败)等等。

审计记录查询也可以通过 ausearch 命令进行。ausearch 命令使用请查看 6.4.1。

查询页面

如下是查询所有 ssh 操作失败的事件记录示例：



查询结果示例

有些审计记录的用户标识栏可能为-1，这是由于身份鉴别失败或由类似事件触发生成的审计记录无法获得确定的用户标识

6.1.3审计规则配置

若点选“审计配置”页，可以按分类进行审计规则的定义和配置，同时也显示各类规则的数量。这些分类分别为：文件相关的审计规则、事件类型相关规则、其他规则。还可以在此页进行审计系统的配置并显示审计配置的变更状态。

审计规则配置页

1　文件规则：

点选文件规则旁边的“编辑”按钮，则出现如下图所示的文件规则配置页面。在点击“添加”按钮会弹出监视文件页面。在监视文件页面可以填写目标监视文件的关键字、路径及所要监视的操作。然后点选“确定”按钮即可添加新的文件审计规则。也可以对已经存在的文件规则进行修改或删除，只需要在文件规则页面点选“删除”或“编辑”按钮即可。

这样，对被监视文件的所有监视操作均将触发生成对应的审计记录。

文件规则配置页

监视文件页

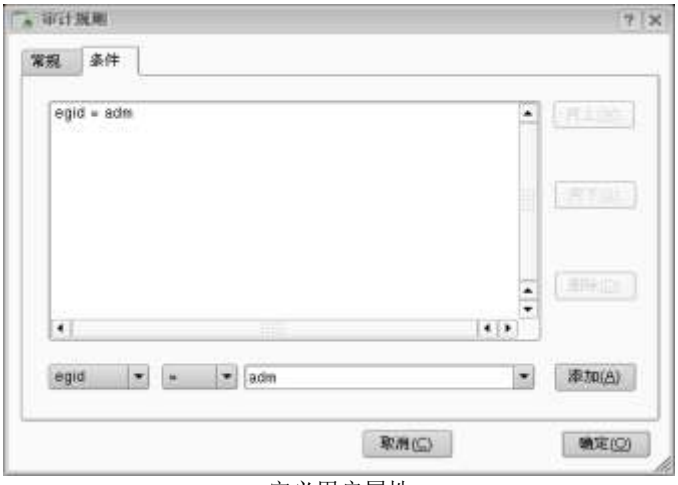
2.其他规则：

其他规则页定义了对用户任务和系统调用的审计规则配置。

点选“审计任务”页后，将弹出如下针对用户任务的审计配置页。

用户任务审计定义

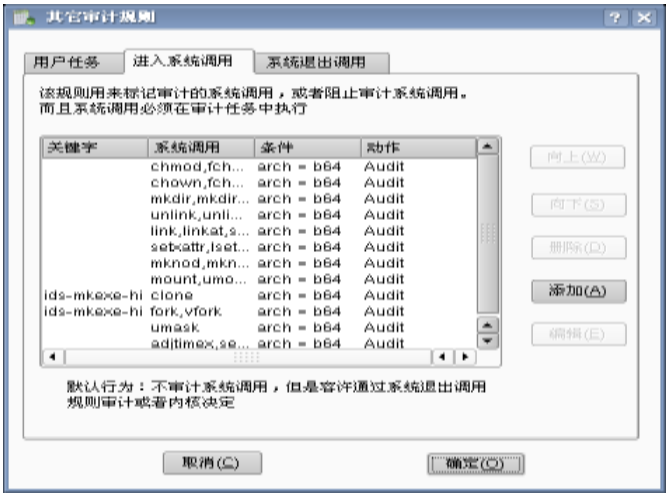
若点选“添加”或者“编辑”按钮，将弹出如下配置定义页。



定义用户属性

在“常规”页可以定义该规则是否审计，或者不作审计。在“条件”页通过点选下拉框定义对应条件的任务用户。

“系统调用”页分为“进入”和“退出”两页，分别对所定义的系统调用的进入和退出行为进行审计，如下图所示。



系统调用审计配置

若点选“添加”按钮，则弹出如下配置页面：

系统调用审计配置常规页

在“常规”页，可以选择是否审计该系统调用以及审计的关键字。在“系统调用”页，可以定义被监控的系统调用。如果不选择的话默认会审计所有的系统调用在“条件”页，可以定义对应对哪些条件的用户进行系统调用审计。

系统调用审计配置系统调用页

系统调用审计配置条件页

3 事件类型规则

事件类型规则项主要进行用户应用程序事件和排除事件的定义和对应的审计行为。

点击“审计配置”页的“事件类型规则”项的“编辑”按钮，弹出如下“事件类型规则”配置页。

点选“用户应用程序事件”页的“添加”按钮，可以定义对哪些条件的用户进行或者不进行审计。点选“排除事件”页的“添加”按钮，可以指定哪些类型的审计事件被过滤掉。

审计事件类型规则配置页

6.1.4 审计环境设置

若点选“审计配置”页“设置”项旁边的“编辑”按钮，则弹出如下的“审计环境设置”页，可以进行审计环境的参数设置，包括对核心 kaudit 进程和审计守护进程 auditd 的行为配置，日志文件和磁盘空间的环境

设置，以及出现日志记录错误时的审计行为配置。

审计环境设置内核标签页可以对内核审计守护进程 kaudit 的环境和行为设置。

审计环境设置内核标签页

审计环境设置审计守护进程页面可以对用户态的审计守护进程 auditd 的优先级、审计管理员电子邮件账户、审计分发程序及审计分发程序失败处理方式进行设置。

审计环境设置审计守护进程页

审计环境设置日志文件页可设置项如下图所示。其中的日志文件路径一般不需要用户选择。系统默认为/var/log/audit/audit.log，该路径受系统内置安全策略保护。该页面还定义了日志数据写入磁盘方式和增量数、单个日志文件大小上限以及达到上限所采取的动作。

审计环境设置日志文件页面

审计环境设置磁盘限额页如下图所示。该页面可以设置磁盘空间限额的第一/二下限，以及当磁盘空间限额达到第一/二个下限时所采取的动作。

审计环境设置磁盘限额页面

审计环境设置日志文件错误页如图所示. 该页面可以设置发生磁盘全满或 I/O 错误时所采取的动作。

审计环境设置日志文件错误页

6.1.5审计报表

当选择标签为安全报表时，选择相应的条件，点击查询。可以得到安全报表。

安全报表

点击数据可视化，可以得到可视化的图：

可视化安全报表

6.2 审计配置

6.2.1 配置审计守护进程

审计管理员可以自行定义审计配置。下面是部分常用的配置项：

- 设置审计消息的专用日志文件
- 确定是否循环使用日志文件
- 如果日志文件的启动用掉了太多磁盘空间则发出警告
- 配置审计规则记录更详细的信息
- 激活文件和目录观察器

这些设置项位于/etc/audit/auditd.conf 文件中，它包含修改审计守护进程的行为的选项。每个选项均应在独立的一行上，后面跟着等于号(=)和这个选项的值。如下是 auditd.conf 配置文件示例。

```
# This file controls the configuration of the audit daemon
log_file = /var/log/audit/audit.log
log_format = RAW
priority_boost = 3
flush = INCREMENTAL
freq = 20
num_logs = 4
dispatcher = /sbin/audispd
disp_qos = lossy
max_log_file = 5
max_log_file_action = ROTATE
space_left = 75
space_left_action = SYSLOG
```

action_mail_acct = root

admin_space_left = 50

admin_space_left_action = SUSPEND

disk_full_action = SUSPEND

disk_error_action = SUSPEND

这些配置项分别表示：

log_file

审计日志文件的完整路径。如果您配置守护进程向除默认/var/log/audit/外的目录中写日志文件时，一定要修改它上面的文件权限，使得只有根用户有读、写和执行权限。所有其他用户都不能访问这个目录或这个目录中的日志文件。

由于系统内置安全策略默认对该路径下的审计日志文件施加了安全保护，如果修改了审计日志文件路径，需要同步修改对应的安全策略。

log_format

写日志时要使用的格式。当设置为 RAW 时，数据会以从内核中检索到的格式写到日志文件中。当设置为 NOLOG 时，数据不会写到日志文件中，但是如果用 dispatcher 选项指定了一个，则数据仍然会发送到审计事件调度程序中。

priority_boost

审计应采用多少优先级运行守护进程。必须是非负数。0 表示没有变化。

flush

多长时间向日志文件中写一次数据。值可以是 NONE、INCREMENTAL、DATA 和 SYNC 之一。如果设置为 NONE，则不需要做特殊努力来将数据刷新到日志文件中。如果设置为 INCREMENTAL，则用 freq 选项的值确定多长时间发生一次向磁盘的刷新。如果设置为 DATA，则审计数据和日志文件一直是同步的。如果设置为 SYNC，则每次写到日志文件时，数据和元数据是同步的。

freq

如果 flush 设置为 INCREMETNAL，审计守护进程在写到日志文件中前从内核中接收的记录数。

num_logs

max_log_file_action 设置为 ROTATE 时要保存的日志文件数目。必须是 0~99 之间的数。如果设置为小于 2，则不会循环日志。如果递增了日志文件的数目，就可能有必要递增/etc/audit/audit.rules 中的内核 backlog 设置值，以便留出日志循环的时间。如果没有设置 num_logs 值，它就默认为 0，意味着从来不循环日志文件。

dispatcher

当启动这个守护进程时，由审计守护进程自动启动程序。所有守护进程都传递给这个程序。可以用它来进一步定制报表或者以与您的自定义分析程序兼容的不同格式产生它们。自定义程序的示例代码可以在/usr/share/doc/audit-<version>/skeleton.c 中找到。由于调度程序用根用户特权运行，因此使用这个选项时要极其小心。这个选项不是必需的。

disp_qos

控制调度程序与审计守护进程之间的通信类型。有效值为 lossy 和 lossless。如果设置为 lossy，若审计守护进程与调度程序之间的缓冲区已满(缓冲区为 128 千字节)，则发送给调度程序的引入事件会被丢弃。然而，只要 log_format 没有设置为 nolog，事件就仍然会写到磁盘中。如果设置为 lossless，则在向调度程序发送事件之前和将日志写到磁盘之前，调度程序会等待缓冲区有足够的空间。

max_log_file

以兆字节表示的最大日志文件容量。当达到这个容量时，会执行 max_log_file _action 指定的动作。

max_log_file_action

当达到 max_log_file 的日志文件大小时采取的动作。值必须是 IGNORE、SYSLOG、SUSPEND、ROTATE 和 KEEP_LOGS 之一。如果设置为 IGNORE，则在日志文件达到 max_log_file 后不采取动作。如果设置为 SYSLOG，则当达到文件容量时会向系统日志/var/log/messages 中写入一条警告。如果设置为 SUSPEND，则当达到文件容量后不会向日志文件写入审计消息。如果设置为 ROTATE，则当达到指定文件容量后会循环日志文件，但是只会保存一定数目的老文件，这个数目由 num_logs 参数指定。老文件的文件名将为 audit.log.N，其中 N 是一个数字。这个数字越大，则文件越老。如果设置为 KEEP_LOGS，则会循环日志文件，但是会忽略 num_logs 参数，因此不会删除日志文件。

space_left

以兆字节表示的磁盘剩余空间数量。当达到这个水平时，会采取 space_left_action 参数中的动作。

space_left_action

当磁盘空间量达到 space_left 中的值时，采取这个动作。有效值为 IGNORE、SYSLOG、EMAIL、SUSPEND、SINGLE 和 HALT。如果设置为 IGNORE，则不采取动作。如果设置为 SYSLOG，则向系统日志/var/log/messages 写一条警告消息。如果设置为 EMAIL，则从 action_mail_acct 向这个地址发送一封电子邮件，并向/var/log/messages 中写一条警告消息。如果设置为 SUSPEND，则不再向审计日志文件中写警告消息。如果设置为 SINGLE，则系统将在单用户模式下。如果设置为 SALT，则系统会关闭。

action_mail_acct

负责维护审计守护进程和日志的管理员的电子邮件地址。如果地址没有主机名，则假定主机名为本地地址，比如 root。必须安装 sendmail 并配置为向指定电子邮件地址发送电子邮件。

admin_space_left

以兆字节表示的磁盘空间数量。用这个选项设置比 space_left_action 更多的主动性动作，以防万一 space_left_action 没有让管理员释放任何磁盘空间。这个值应小于 space_left_action。如果达到这个水平，则会采取 admin_space_left_ action 所指定的动作。

admin_space_left_action

当剩余磁盘空间量达到 admin_space_left 指定的值时，则采取动作。有效值为 IGNORE、SYSLOG、EMAIL、SUSPEND、SINGLE 和 HALT。与这些值关联的动作与 space_left_action 中的相同。

disk_full_action

如果含有这个审计文件的分区已满，则采取这个动作。可能值为 IGNORE、SYSLOG、SUSPEND、SINGLE 和 HALT。与这些值关联的动作与 space_left _action 中的相同。

注意：如果不循环审计日志文件，则含有/var/log/audit/的分区可能变满并引起系统错误。因此，

建议让/var/log/audit/位于一个单独的专用分区。

disk_error_action

如果在写审计日志或循环日志文件时检测到错误时采取的动作。值必须是 IGNORE、SYSLOG、SUSPEND、SINGLE 和 HALT 之一。与这些值关的动作与 space_left_action 中的相同。

/etc/sysconfig/auditd 文件可以用来设置带 EXTRAOPTIONS 参数的 auditd 的命令行选项。唯一的命令行选项-f 以调试模式安排守护进程。如果启用了调试模式，则会出现标准错误消息而不是日志文件。AUDITD_LANG 设置值可以用来修改守护进程的位置。如果设置为 none，则所有位置信息会从审计环境中删除。如果 AUDITD_CLEAN _STOP 选项设置为 yes，则当用 service auditd stop 命令停止守护进程时，会删除审计规则与观察器。要了解关于审计规则的更多信息，请参见下一节。

6.2.2 编写审计规则与观察器

除了系统默认定义的审计规则外，还可以对要关注的审计事件额外编写规则。比如针对特定的系统调用，或者针对采用特定命令对特定文件或目录上的操作进行审计等等。如果用 auditd 服务脚本启动审计系统(即执行 service auditd start 命令)，则可以将自定义审计规则添加到/etc/audit/audit.rules 中，以便在启动 auditd 审计守护进程时予以调用。只有审计管理员可以读或修改该配置文件。

/etc/audit.audit.rules 中的每个规则和观察器必须单独一行，以#开头的行会被忽略。规则和观察器均作为 auditctl 的命令行选项。文件中如果一个或多个规则或观察器互相冲突，则以第一个出现者为准。

除了通过修改/etc/audit.audit.rules 进行审计规则定义外，还可以使用审计管理控制台中的“审计规则配置”页进行直观的规则定义，具体配置请参阅 6.1.3 节。

1 编写审计规则

要添加审计规则，可在/etc/audit/audit.rules 文件中用下面的语法：

-a <list>,<action> <options>

注意：如果在运行守护进程时添加规则/etc/audit/audit.rules，则一定要以审计管理员身份用 service auditd restart 命令启用修改。也可以使用 service auditd reload 命令，但是这种方法不会提供配置文件错误的消息。

列表名必须是下列名称之一：

task

每个任务的列表。只有当创建任务时才使用。只有在创建时就已知的字段(比如 UID)才可以用在这个列表中。

entry

系统调用条目列表。当进入系统调用确定是否应创建审计时使用。

exit

系统调用退出列表。当退出系统调用以确定是否应创建审计时使用。

user

用户消息过滤器列表。内核在将用户空间事件传递给审计守护进程之前使用这个列表过滤用户空间事件。有效的字段只有 uid、auid、gid 和 pid。

exclude

事件类型排除过滤器列表。用于过滤管理员不想看到的事件。用 msgtype 字段指定您不想记录到日志中的消息。

这个动作必须下面的动作之一：

never

不生成审计记录。

always

分配审计上下文，总是把它填充在系统调用条目中，总是在系统调用退出时写一个审计记录。

<options>可以包括下面几个选项中的一个或多个。

-s <syscall>

根据名称或数字指定一个系统。要指定所有系统调用，可使用 all 作为系统调用名称。如果程序使用了这个系统调用，则开始一个审计记录。可以为相同的规则指定多个系统调用，每个系统调用必须用 -S 启动。在相同的规则中指定多个系统，而不是列出单独的规则，这样可以导致更好的性能，因为只需要评价一个规则。

- F <name[=,!=,<,>,<=]value>

指定一个规则字段。如果为一个规则指定了多个字段，则只有所有字段都为真才能启动一个审计记录。每个规则都必须用-F 启动，最多可以指定 64 个规则。如果用用户名和组名作为字段，而不是用 UID 和 GID，则会将它们解析为 UID 和 GID 以进行匹配。下面是有效的字段名：

pid

进程 ID。

ppid

父进程的进程 ID。

uid

用户 ID。

euid

有效用户 ID。

suid

设置用户 ID。

fsuid

文件系统用户 ID。

gid

组 ID。

egid

有效组 ID。

sgid

设置组 ID。

fsgid

文件系统组 ID。

auid

审计 ID，或者用户登录时使用的原始 ID。

msgtype

消息类型号。只应用在排除过滤器列表上。

pers

OS Personality Number。

arch

系统调用的处理器体系结构。指定精确的体系结构，比如 i686(可以通过 uname -m 命令检索)或者指定 b32 来使用 32 位系统调用表，或指定 b64 来使用 64 位系统调用表。

devmajor

Device Major Number。

devminor

Device Minor Number。

inode

Inode Number。

exit

从系统调用中退出值。

success

系统调用的成功值。1 表是真/是，0 表示假/否。

a0，a1，a2，a3

分别表示系统调用的前 4 个参数。只能用数字值。

key

设置用来标记事件的审计日志事件消息的过滤键。参见程序清单 2-2 和程序清单 2-3 中的示例。当添加观察器时，类似于使用-k 选项。参见“编写审计规则与观察器”了解关于-k 选项的详细信息。

obj_user

资源的 SELinux 用户。

obj_role

资源的 SELinux 角色。

obj_type

资源的 SELinux 类型。

obj_lev_low

资源的 SELinux 低级别。

obj_lev_high

资源的 SELinux 高级别。

subj_role

程序的 SELinux 角色。

subj_type

程序的 SELinux 类型。

subj_sen

程序的 SELinux 敏感性。

subj_clr

程序的 SELinux 安全级别(clearance)。

-a 选项向列表末尾添加规则。要向列表开头添加规则，可用-A 替换-a。删除语法相同的规则，用-d 替换-a。要删除所有规则，可指定-D 选项。程序清单 2-2 含有一些示例审计规则，比如 /etc/audit/audit.rules。

如下是个审计规则示例：

```
#Record all file opens from user 501
#Use with caution since this can quickly
#produce a large quantity of records
-a exit,always -S open -F uid=501 -F key=501open
#Record file permission changes
-a entry,always -S chmod
```

其他的示例可以参考/usr/share/doc/audit-<version>/目录的下的*.rules 文件中。

当发生了定义的规则中的动作时，如果有一个规则在/etc/audit/auditd.conf 中定义则它会通过调度程序发送，然后会有一条日志消息写到/var/log/audit/audit.log 中。例如，如下审计记录中含有上面规则示例中的第一个规则的日志项，日志文件从用户 501 打开。这个规则包括一个过滤键，它出现在示例日志的末尾。

示例审计规则日志：

```
type=SYSCALL msg=audit(1168206647.422:5227): arch=c000003e syscall=2
success=no exit=-2 a0=7fff37fc5a40 a1=0 a2=2aaaaaaab000 a3=0 items=1
```

ppid=26640 pid=2716 auid=501 uid=501 gid=501 euid=501 suid=501 fsuid=501

egid=501 sgid=501 fsgid=501 tty=pts5 comm="vim" exe="/usr/bin/vim"

key="501open"

2 编写审计观察器

系统提供的审计功能还允许审计管理员通过定义观察器监测文件和目录的访问。如果一个观察器被定义在一个文件或目录上，则会记录对应的成功或失败的动作，比如打开和执行文件或目录。

注意：如果在守护进程运行时在/etc/audit/audit.rules 中添加了观察器，则一定要以审计管理员身份用 service auditd restart 命令启用修改。也可以用 service auditd reload 命令，但是它不会通知您关于配置文件错误的消息。

如下是包括在/etc/audit/audit.rules 文件中的示例规则。如果使用 auditctl 命令配置时采用-w 和-k <key>选项结合使用，则由观察器产生的所有记录会含有一个警报词(限制为 31 个字节)，因此可以将该观察器的记录轻松地从日志文件中过滤出来。要限制文件或目录观察器为某些动作，可使用-p 选项，后面跟着下面的选项中的一个或多个：r 表示观察读动作，w 表示观察写动作，x 表示观察执行动作，a 表示在末尾添加动作。要删除一个观察器，可使用由后面跟着文件或目录的-W 选项。

示例审计观察器：

#Watch for changes to sysconfig files

-w /etc/sysconfig -k SYSCONFIG

#Watch for changes to audit config files

-w /etc/audit/audit.rules -k AUDIT_RULES

-w /etc/audit/auditd.conf -k AUDIT_CONF

-w /var/log/audit/ -k LOG_AUDIT

#Watch to see who tries to start the VPN client

-w /usr/bin/vpnc -k VPNC -p x

#Watch password files

-w /etc/group -k PASSWD

-w /etc/passwd -k PASSWD

-w /etc/shadow -k PASSWD

上述示例规则中包括了关键过滤器 PASSWD 的口令文件上的一个观察器。如果删除一个用户后/var/log/audit/audit.log 中将会出现类似于下面的的审计日志。我们可以看到，对应标识键被添加到日志项的末尾，因此可以轻松地将它从日志项的其余部分过滤出来。

对应审计观察器的示例日志

type=SYSCALL msg=audit(1168227741.656:17915): arch=c000003e syscall=82

success=yes exit=0 a0=7fff00975dd0 a1=60a700 a2=0 a3=22 items=5 ppid=26575

pid=4147 auid=501 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0

tty=pts4 comm="userdel" exe="/usr/sbin/userdel" key="PASSWD"

3 配置 auditctl

配置 auditctl 参数的命令行选项也能包括在/etc/audit/audit.rules 中。如下列出了这些选项。

-b <backlog>

允许的未完成审计缓冲区的最大数目。内核中的默认值为 64。如果缓冲区已满，则内核引用通过-f 选项设置的失败标志，以确定采取哪个动作

-e [0,1]

设置为 0 禁用审计，或者设置为 1 启用审计。对于为了故障检修或其他目的而临时禁用审计会很有用

-f [0,1,2]

设置用于通知内核如何处理关键错误(比如审计缓冲区已满或者内核内存用完)的失败标志。有效值是 0(没有动作)，1(用 printk 将消息记录到/var/log/messages)和 2(混乱)。默认值为 1，但是 2 更安全。

-r <rate>

以每秒钟的消息条数为单位的速率限制。如果设置为 0，则没有限制。如果超出了速率限制，则内核会咨询-f 选项中的失败标志来确定采取哪个动作

-i

当从一个文件中读取规则时忽略错误

要验证设置了这些选项，可用 auditctl -s 命令查看状态。输出类似下面这样：

AUDIT_STATUS: enabled=1 flag=1 pid=1954 rate_limit=0 backlog_limit=256

lost=0 backlog=0

6.2.3 守护进程的启动和停止

当配置守护进程和添加规则与观察器时，可以以审计管理员身份执行 service auditd start 命令启动守护进程。要停止它，可使用 service auditd stop 命令。要使它自动在运行时启动，则通过执行 chkconfig auditd on 命令。

如果当您修改守护进程的配置时守护进程已经在运行，则应以审计管理员身份执行 service auditd restart 命令启用修改。要验证规则与观察器已经修改，应以审计管理员身份执行 auditctl -l 命令列出所有活动的规则和观察器。

6.2.4 记录分析

如果 auditd 守护进程启动，则除非用/etc/audit/audtid.conf 中的 log_file 参数修改了文件名，否则审计消息会写到/var/log/audit.log 中。日志文件是文本文件，可以通过 less 实用程序或文本编辑器(比如 Emacs 或 Vi)阅读。消息的格式为从内核中接收的格式，顺序也是接收时的顺序。aureport 实用程序可以用来从日志文件中生成汇总报表。ausearch 实用程序可以用来基于一些条件搜索报表。这些条件可以是：审计事件 ID、文件名、UID 或 GID、消息类型和系统调用名等。

除非将守护进程配置为循环日志文件和像前面“配置审计守护进程”一节中介绍的那样删除老文件，否则/var/log/audit/中的日志文件永远不会被删除。管理员应经常检查日志，删除老日志或者移到

备份存储器中。如果不周期性地删除日志，它们将会填满整个磁盘。因此，建议把/var/log/audit/放在一个单独的专用分区上，这样就不会由于写满日志文件而引发其他系统错误。

如果要强制立即循环日志文件，可以以审计管理员身份执行 service auditd rotate 命令。老日志文件的文件名将为 audit.log.N，其中 N 是一个数字。这个数字越大，日志文件越旧。

1 生成报表

要生成审计消息的报表，可使用 aureport。如果执行 aureport 时没有使用任何选项，则会显示类似如下示例的汇总报表。

```
Summary Report
======================
Range of time: 11/29/2006 03:40:18.155 - 01/07/2007 23:29:02.898
Number of changes in configuration: 71
Number of changes to accounts, groups, or roles: 14
Number of logins: 38
Number of failed logins: 0
Number of users: 3
Number of terminals: 35
Number of host names: 7
Number of executables: 55
Number of files: 1186
Number of AVC denials: 0
Number of MAC events: 70
Number of failed syscalls: 2594
Number of anomaly events: 46
Number of responses to anomaly events: 0
Number of crypto events: 0
Number of process IDs: 3734
Number of events: 33743
```

可以让 aureport 命令带上如下选项生成更具体的报表。这些选项缩小了具体数据的范围，比如系统调用或配置修改。

-a

报告关于访问向量缓冲(access vector cache，AVC)的消息

-c

报告关于配置修改的消息

-cr

报告关于 crypto 事件的消息

-e

报告关于事件的消息

-f

报告关于文件的消息

-h

报告关于主机的消息

-l

报告关于登录的消息

-m

报告关于账户修改的消息

-ma

报告关于 Mandatory Access Control(MAC)事件的消息

-p

报告关于进程的消息

-s

报告关于系统调用的消息

-tm

报告关于终端的消息

要以更可读的格式产生结果，比如用它们映射到的用户名替换 UID，则也要使用-i 选项：

```
aureport -<flag> -i
```

要显示每个日志的启动和停止时间，可以添加-t 选项：

```
aureport -<flag> -i -t
```

要显示等于或早于特定时间的事件，可以添加-te 选项，并在后面跟着结束日期和结束时间。用数字格式表示您所在地点的日期和时间，并以 24 小时制格式表示时间。例如，对于 en_us.UTF-8 这个地方，可使用日期格式 MM/DD/YY：

```
aureport -<flag> -i -te <end date> <end time>
```

要显示等于或者晚于特定时间的事件，添加-ts 选项，后面跟着开始日期和时间。采用与-te 选项相同的日期和时间格式化规则。

```
aureport -<flag> -i -ts <start date> <start time>
```

要仅显示失败事件，则使用--failure，注意这个选项前面有两条虚线而不是一条：

aureport -<flag> -i --failed

要仅显示成功事件，则使用--success，注意这个选项前面有两条虚线而不是一条：

aureport -<flag> -i --success

有些报表也可以用- -summary 选项以汇总格式生成；注意这个选项前面有两条虚线作前缀：

aureport -<flag> -i --summary

要产生汇总报表而不是关于一个地区的报表，可使用-r 选项：

aureport -r -i

要产生来自一个日志文件的报表而不是默认报表，则可用-if 选项指定它：

aureport -<flag> -i -if /var/log/audit/audit.log.1

2 查询记录

除了生成事件报表并用 aureport 汇总外，管理员还可以用 ausearch 查询搜索审计记录。

如下是对应的命令选项。

-a <event id>

显示特定事件 ID 的消息。每条消息中均含有一个标识字符串，比如 msg=audit(1145758414.468:8758)。冒号后面的数字是审计事件 ID，本例中是 8758。来自应用程序的系统调用的所有事件都有相同的审计事件 ID，因此可以将它们组成一组

-c <comm name>

显示特定 comm 名称的消息，它是任务结构中的可执行文件的名称。当搜索一个特定的审计事件 ID 时会显示 comm 名称，比如 firefox-bin 或 vim

-f <filename>

显示关于特定文件名的消息。对于观察带 auditctl 的文件时有用

-ga <group id>

显示一个有效组 ID 或者匹配给定 GID 的组 ID 的消息

-ge <group id>

显示匹配给定 GID 的一个有效组 ID 的消息

-gi <group id>

显示匹配给定 GID 的一个组 ID 的消息

-h

显示简短帮助信息

-hn <hostname>

显是含有特定主机名的消息

-i

以人类可读的格式显示结果

-if <logfile>

从<logfile>中读日志，而不是从/var/log/audit/audit.log 中或用/etc/audit/auditd.conf.log 中的 log_file 参数设置的文件中读日志

-k <key>

显示带<key>的消息

-m <mess type>

显示含有特定消息类型的消息，比如 CONFIG_CHANGE 或 USER_ACCT

-o <SELinux context>

显示含有与提供的字符串相匹配的 SELinux tcontext (object)的消息

-p <pid>

显示特定进程 ID 的消息

-sc <syscall>

显示关于特定系统调用的消息，由系统调用名或它的数值指定

-se <SELinux context>

显示含有与提供的字符串相匹配的 SELinux scontext/subject 或 tcontext/object 的消息

-su <SELinux context>

显示含有与提供的字符串相匹配的 SELinux scontext (subject)的消息

-sv <success value>

这个选项是 yes 则显示成功消息，这个选项是 no 则显示失败消息。如程序清单 2-8 所示，在消息末尾，success 值后面跟着关键字 res，可以是 success 或者 failed

-te <date> <time>

显示等于或早于给定日期和时间的时间标记的消息。日期和时间格式取决于系统的地点。用 24 小时制指定时间，比如 23:00:00。对于 en_US.UTF-8 这个地方，日期格式是 MM/DD/YY 的数值等价物

-ts <date> <time>

显示等于或晚于给定时间的时间标记的消息。日期和时间规则与-te 选项的规则相同

-tm <terminal>

显示指定终端的消息，比如 pts/6。有些可执行文件，比如时钟守护进程和 atd，使用终端的守护进程名

-ua <uid>

显示用户 ID、有效用户 ID 或登录 UID(auid)匹配指定 ID 的消息

-ue <uid>

显示有效用户 ID 匹配指定 ID 的消息

-ui <uid>

显示用户 ID 匹配指定 ID 的消息

-ul <login id>

显示登录 UID 匹配指定 ID 的消息

-v

显示 ausearch 版本

-w

如果指定了要匹配的字符串，则只显示匹配整个单词的结果

-x

显示关于可执行文件的消息，比如 crond 或 sudo。可执行文件的完整路径在消息中 exe 关键字后面提供，比如程序清单 2-8 中的“/bin/sudo”

与 aureport 相似，-i 选项可以用来使输出更可读，-if <filename>选项可以用来提供要搜索的备用日志文件。

当显示结果时，每个记录用 4 条虚线组成的一行隔开，每个记录前均显示时间标记。以下是执行 ausearch -x sudo 的一个示例：

```
time->Fri Dec 1 00:01:01 2006
type=CRED_ACQ msg=audit(1145210930.022:2023): user pid=30718 uid=0
auid=4294967295 msg='PAM: setcred acct=root : exe="/usr/bin/sudo"
(hostname=?, addr=?, terminal=pts/3 res=success)'
----
time->Fri Dec 1 04:01:01 2006
type=USER_START msg=audit(1145210930.022:2024): user pid=30718 uid=0
auid=4294967295 msg='PAM: session open acct=root : exe="/usr/bin/sudo"
(hostname=?, addr=?, terminal=pts/3 res=success)'
----
time->Fri Dec 1 04:42:01 2006
type=USER_END msg=audit(1145210930.022:2025): user pid=30718 uid=0
auid=4294967295 msg='PAM: session close acct=root : exe="/usr/bin/sudo"
(hostname=?, addr=?, terminal=pts/3 res=success)'
----
time->Fri Dec 1 05:01:01 2006
type=CRED_ACQ msg=audit(1145249595.972:2482): user pid=2062 uid=0
```

```
auid=4294967295 msg='PAM: setcred acct=root : exe="/usr/bin/sudo"
(hostname=?, addr=?, terminal=pts/6 res=success)'
----
time->Fri Dec 1 06:01:01 2006
type=USER_START msg=audit(1145249595.972:2483): user pid=2062 uid=0
auid=4294967295 msg='PAM: session open acct=root : exe="/usr/bin/sudo"
(hostname=?, addr=?, terminal=pts/6 res=success)'
----
time->Fri Dec 1 09:01:01 2006
type=USER_END msg=audit(1145249595.972:2484): user pid=2062 uid=0
auid=4294967295 msg='PAM: session close acct=root : exe="/usr/bin/sudo"
(hostname=?, addr=?, terminal=pts/6 res=success)'
```

6.2.5 审计跟踪

autrace 实用程序可以用来生成特定进程中的审计记录。当 autrace 运行时，没有其他规则或观察器可以启用。autrace 必须以审计管理员用户身份运行。

要审计跟踪一个进程，需采用下列步骤：

1) 暂时关闭所有规则与观察器：

```
auditctl -D
```

2) 如需将生成的审计记录分离到独立的审计日志中，需强制一个日志文件循环：

(本步骤可选)

```
service auditd rotate
```

autrace 的日志将放在/var/log/audit/audit.log 中。

3) 在命令行执行 autrace：

```
autrace <待跟踪审计的命令>
```

4) 等待直到命令对应的进程执行完成。将显示一条类似于下面这个消息：

```
Trace complete. You can locate the records with 'ausearch -i -p 10773'
```

5) 重启审计守护进程来重新启用规则和观察器：

```
service auditd restart
```

6) 用 ausearch 显示关于跟踪的详细信息。

第7章　安全策略生成工具

红旗安全操作系统 4.0 提供了生成安全策略的图形工具 polgengui，可以帮助管理员为应用程序生成对应安全策略模块，实现对外来应用的安全保护。

由于安全策略生成工具用于调试生成外来应用的安全策略，该工具被设计为只能运行于警报模式。

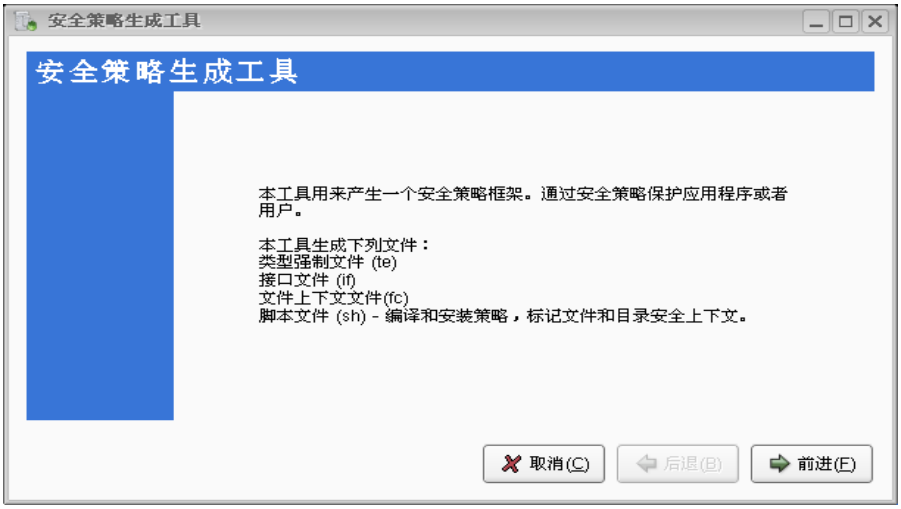
7.1　创建安全策略模块

安全策略生成工具采用向导式操作，分七步完成安全策略生成过程：

1. 选择应用程序类型
2. 定义需要保护的应用程序名称
3. 指定输入网络端口连接
4. 指定输出网络端口连接
5. 标识通用应用程序特征
6. 指定受保护的应用程序文件和目录和设置布尔值
7. 选择安全策略存放目录

当管理员完成了上述七步操作以后，将最终产生下列四个文件，然后由系统管理员运行脚本来加载和调试安全策略，最终完成安全策略部署。四个文件如下所示：

- 类型强制文件(te)　－包含应用程序的安全策略
- 文件关联文件(fc)　－包含文件和目录的安全上下文定义
- 界面文件(if)　－包含应用程序需要使用策略接口文件
- 脚本(sh)　－用来在测试系统上编译，安装和调试。



安全策略生成工具启动界面

7.1.1选择应用程序类型

设置程序类型

该对话框定义了用程序类型，这有助于设置对应守护进程正确地生成安全策略。

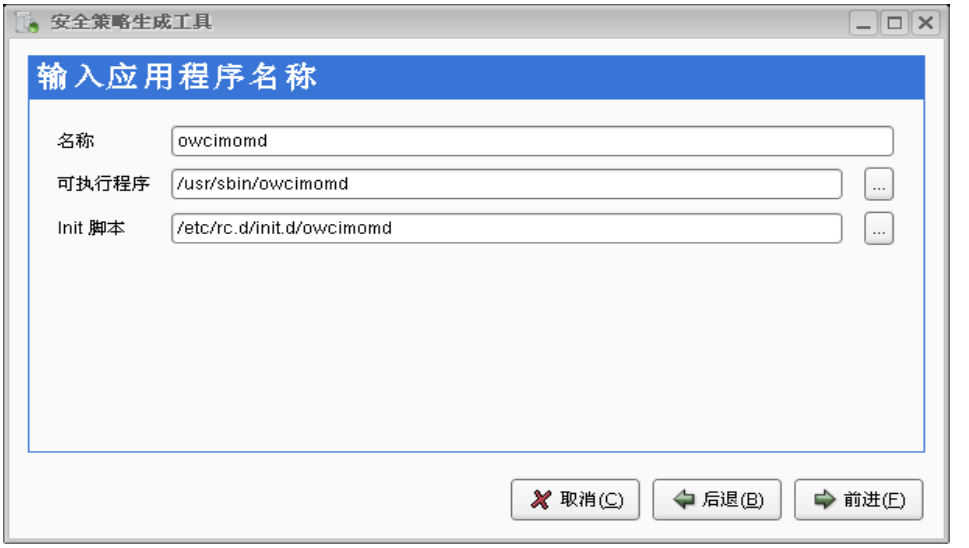
可设置的应用程序类型有：

- 标准 daemon 守护进程，这些应用程序在 init 调用 rc.sysinit 或者/etc/init.d 目录下的脚本时启动。
- inetd 服务守护进程，这些应用程序有 inetd 或者 xinetd 启动。

- Web 应用程序/脚本（CGI），这些应用程序一般由 Apache 运行。
- 用户应用程序，通常由管理员或者用户直接在终端运行。

7.1.2定义需要保护的应用程序名称

此对话框指定受保护的应用程序的域名和程序路径，策略生成工具会自动创建对应主体域名和对应可执行程序文件的安全上下文。例如，如果定义应用程序域名为 owcimomd，则自动创建 owcimomd_t 域和对应可执行文件上下文 owcimomd_exec_t。



指定受保护的应用程序

如果定义的域名与系统内置安全策略中已有的域名重名，工具将提示并终止执行。

7.1.3指定输入网络端口连接

该对话框允许管理员输入用空格分隔的一系列用于输入连接的应用程序绑定/监听网络端口。如果管理员无法确定端口信息，可以留空不填。

设置侦听端口

7.1.4 指定输出网络端口连接

该对话框允许管理员指定应用程序连接的 TCP 和 UDP 端口。

设置连接端口

以上两个定义端口的步骤会扫描已经存在的策略，验证端口是否已经被定义。如端口已经被定义过了，将分配给应用程序使用。如果端口还没有被定义，可以使用 semanage 命令定义端口。由本工具生成的 shell 脚本文件也会包括正确的 semanage 命令，通过执行该命令可以定义端口。

7.1.5 标识通用应用程序特征

该对话框允许管理员标识应用程序的运行特征，选中方框将相应的特征加入策略模板并允许应用程序使用这些功能。如果不确定应用程序具备哪些通用特征，可以留空不填，本工具会在调试阶段生成相应的策略。

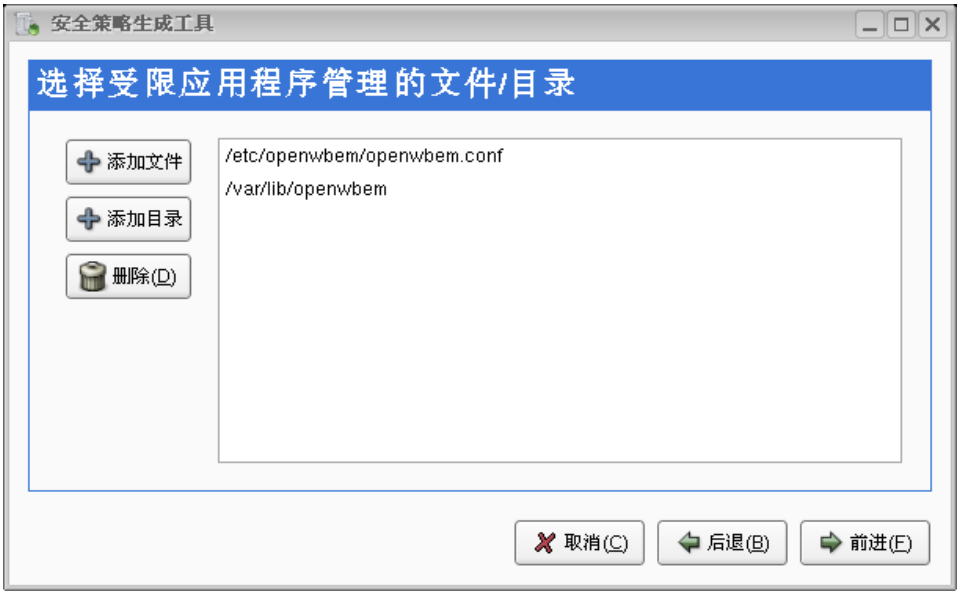
例如 owcimomd 程序会访问 syslog 日志，并且在/tmp 创建有名管道，采用 pam 机制认证，并且有 setuid 操作，所以选择以下几种特征。

设置应用程序安全特性

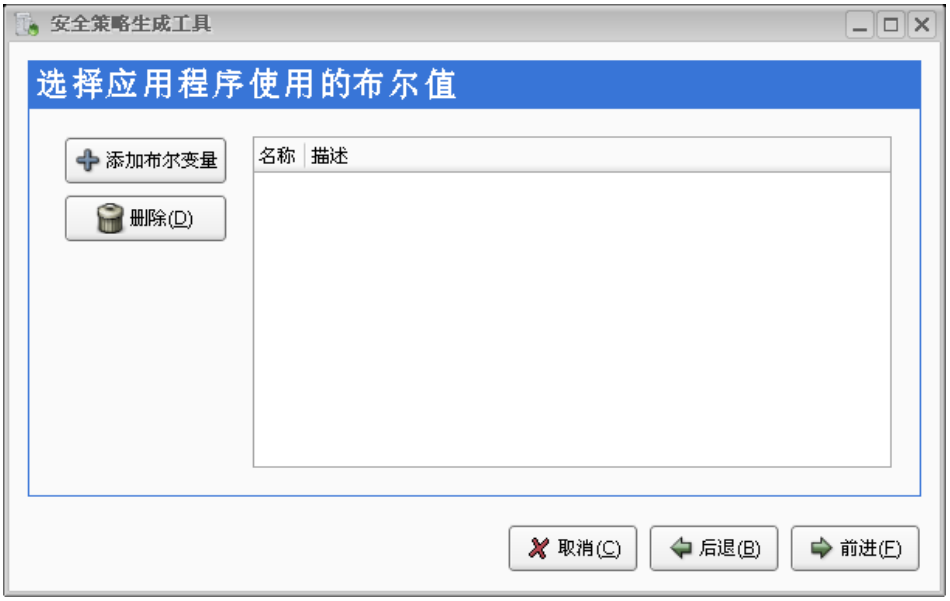
系统提供了应用程序不受限制选项，出于安全考虑不推荐使用。

7.1.6 指定受保护的应用配置文件和目录

该对话框允许指定应用程序需要操作的配置文件和数据目录，这些文件和目录将受到安全策略保护。工具将建立该文件和目录的安全上下文。例如如果指定 owcimomd 程序配置文件/etc/openwbem/openwbem.conf，则工具会自动产生该文件安全上下文 owcimomd_etc_t。



指定受保护文件和目录



设置布尔值

输入新的路径会产生新的文件安全上下文。产生的文件或者目录的安全上下文应该唯一性，不应该覆盖系统中已有文件上下文，否则后面的策略编译操作会失败。

由于应用程序执行文件对应的安全上下文已经在第一步操作生成，这里无须再次指定该执行文件。产生无效的安全上下文是在定制策略的时候常犯的错误。

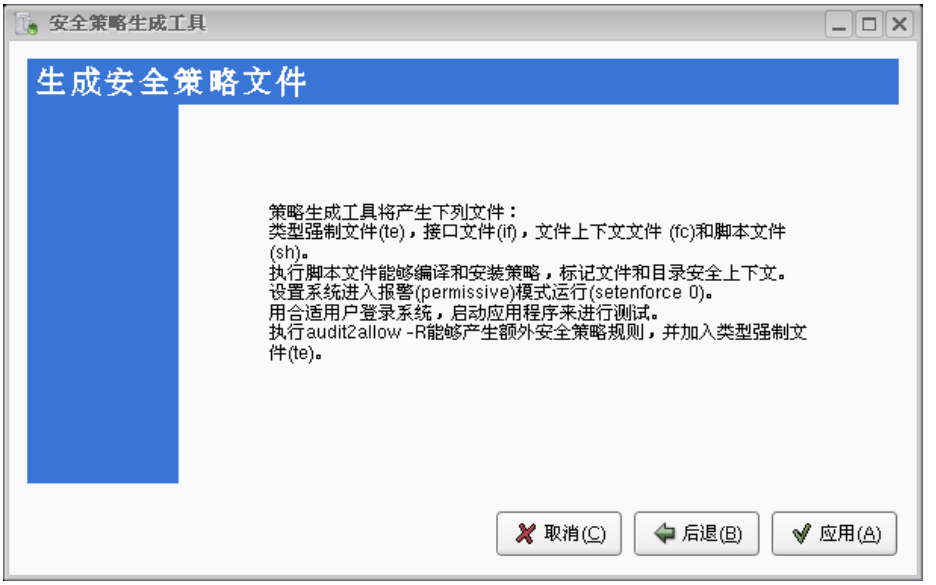
7.1.7 选择安全策略存放目录

该对话框询问安全策略的输出存放目录，默认是当前工作目录，但通常最好指定一个不同的目录。

设置策略文件存放目录

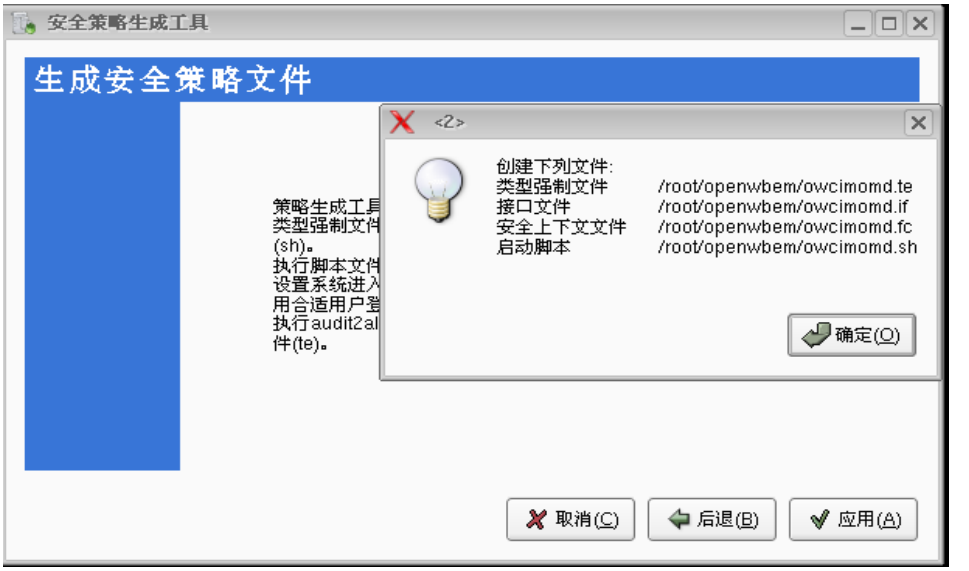
7.1.8 生成安全策略文件

该对话框将完成策略文件生成前的所有确认操作。



确认配置

点击“应用”会生成相应的文件，工具会显示结果：



生成策略文件

策略生成工具仍在运行中，可以返回重复以上步骤，但这样将会覆盖原有的文件。

7.2 生成和加载安全策略模块

上面步骤创建的策略文件，存放在对应的指定目录中。可以编译策略文件形成安全策略模块，并在现有系统安全策略上加载该策略模块。

生成和加载安全策略模块的具体操作过程是：

打开一个终端窗口，以 root 用户执行由本工具生成的 shell 脚本。这个脚本将编译所创建的安全策略模块并载入到系统内核当中，最后执行 restorecon 命令修正或者关联文件的安全上下文标签。

```
# cd /root/ge_policy
# sh owcimomd.sh
```

7.3 调试和完善安全策略模块

创建和加载安全策略模块之后，下一步是验证应用程序是否能在该安全策略模块生效情况下正常工作。具体工作过程是：

首先，将安全运行模式设置于警报模式，并重复执行应用程序各个操作接口生成相应 AVC 信息（违反安全策略信息），这是一个繁琐的过程，需要耐心和认真验证。

然后，执行如下示例命令实行策略的更新和加载操作。

```
# sh owcimomd.sh -update  (将所有 AVC 信息，加入安全策略模块中)
```

最后，将安全运行模式设置于启用模式，执行应用程序各个操作接口，观察是否能够成功完成。如果执行失败，再重复上述操作进行安全策略调试。

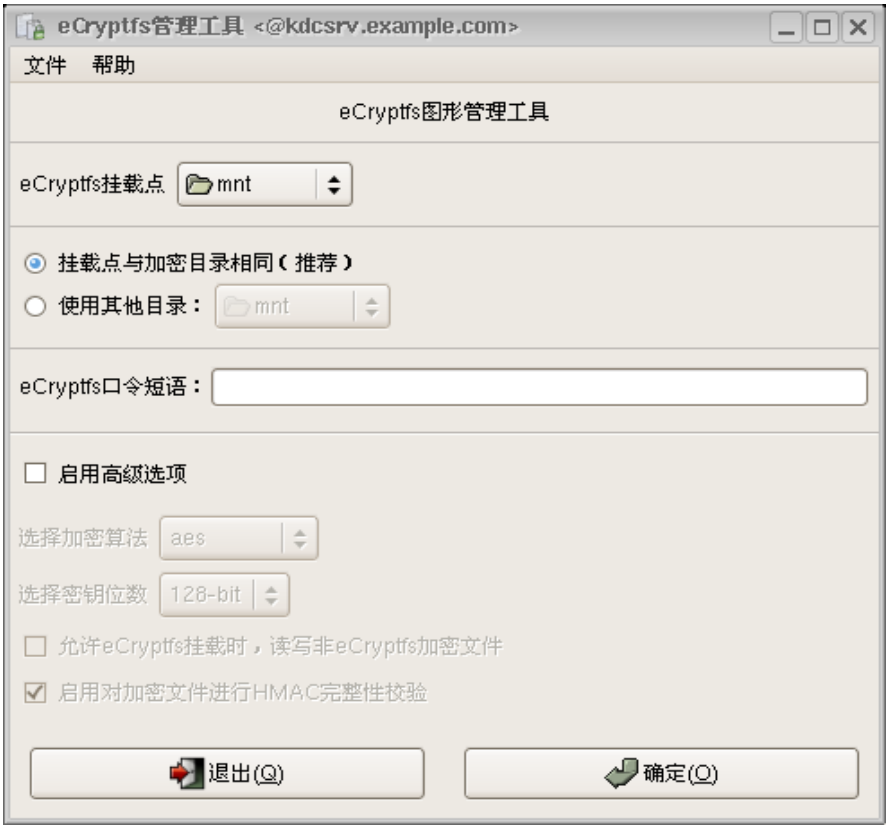
最好不要在部署好的机器上做策略调试工作，那样会导致机器失去安全策略的保护。同时可能对该机器上已有系统和程序产生影响。

第8章　加密文件系统管理工具

红旗安全操作系统 4.0 提供了本地化加密文件系统管理工具，可以帮助系统管理员。

8.1　加密文件系统管理工具

点选开始菜单中的“加密文件系统管理工具”，将启动如图所示的加密文件系统管理工具。主界面由五部分部分视图组成。分别为标题，挂载点，加密目录，挂载密码，高级选项



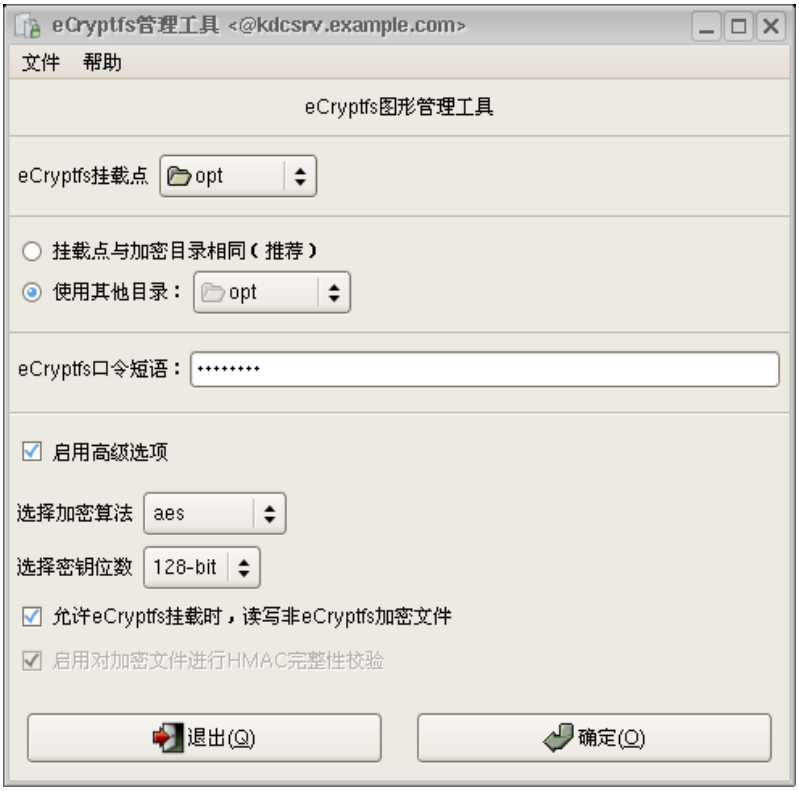
加密文件系统管理工具启动界面

建议 mount 挂载时指定的挂载点与源文件夹相同，这样可以隐藏掉源文件夹的元数据

8.2　加密文件系统挂载过程

假如要针对 ecrypt 目录中文件进行加密为例，说明加密文件系统管理工具使用。具体选择如下：

- 选择挂载点为：ecrypt
- 选择加密目录为：ecrypt
- 输入加密命令：*******
- 启用高级选型：（可选）
- 选择完成后，点击确定按钮。弹出加密文件系统挂载成功。



当选用的加密目录中，包含非加密文件时，请启用高级选项，选择允许加密文件系统挂载时，读写非 eCryptfs 加密文件，这样系统运行时，可以读取该文件内容。

第9章　典型应用部署及其他说明

9.1　Oracle 数据库的安装部署

在红旗安全操作系统 4.0 中，内置了 oracle 数据库安全保护策略，最大化保证用户数据安全性。

安装部署 Oracle 时，需要注意如下几点：

1. 确认当前运行模式为 permissive
2. 选择 Oracle 数据库安装目录为/opt/app。
3. 以安全管理员身份映射 oracle 系统用户到安全用户 staff_u：

   semanage login –a –s staff_u oracle
4. 以安全管理员身份创建 Oracle tcp 端口 1521 映射：

   semanage port –a –t oracle_port_t –p tcp 1521
5. 以系统管理员身份部署 Oracle 数据库之后，执行下列命令后系统会在下次引导时自动进行标记操作并正常引导：

   touch /.autorelabel

   reboot

如果需要单独挂载数据库数据文件目录，建议挂载于/u0X 目录下，其中 X 代表数字 0-9

建议 Oracle 安装在/opt 目录下,如果 Oracle 安装非/opt/app 目录下的默认目录外，请安装并编译位于/usr/src/asianux/SRPMS/下 oracle 策略源码包，并进行安装。安装时会自动根据当前 Oracle 安装环境设置正确的 Oracle 安全策略。

在红旗安全操作系统中,安全策略默认限制 oracle 只能使用端口 1521 进行 tcp 通信。

如果要变更了 oracle 端口映射，请执行命令：semanage port –m –t oracle_port_t –p tcp XXX

其中，XXX 表示对应的端口号。

9.2　Weblogic 与 Websphere 中间件的安装部署

红旗安全操作系统 4.0 内置了对 Java 虚拟机的安全保护策略，可以保护基于 Java 的中间件运行安全。

安装 Weblogic 和 Websphere 中间件时，需要注意如下几点：

1. 确认当前运行模式为 permissive
2. 选择中间件的安装目录为/opt 目录。
3. 安装与部署完成所有应用软件之后，执行下列命令重启系统，对系统进行标记：

   touch /.autorelabel

   reboot

9.3 红旗高可用集群软件的安装部署

安装红旗高可用集群软件时，需要注意如下几点：

1. 确认当前运行模式为 permissive
2. 选择的安装目录为/opt 目录。
3. 安装与部署完成所有应用软件之后，执行下列命令重启系统，对系统进行标记：

   touch /.autorelabel

   reboot

9.4 审计规则定制

用户可以按需求将审计规则拷贝到/etc/audit/目录下覆盖 audit.rules 文件。/usr/share/doc/audit-1.7.11 目录下有很多规则可供选择。其中 gbrank3_i386.rules、gbrank3_x86_64.rules 为满足国家安全标准第三级技术要求的审计规则。custom_i386.rules，custom_x86_64.rules 是在国家安全标准第三级技术要求基础上定制的略微宽松的审计规则。

从效率方面考虑，建议用户根据部署环境需要，选用略微宽松的审计规则。

9.5 常见安全布尔值说明

一般来说，安全操作系统载入安全策略后就是静态，不能改变安全策略，除非直到有全新的安全策略载入。但是为了增加安全操作系统的灵活性和兼容性，提供了布尔值接口，可以在系统运行时动态调整部分安全行为。下面列举部分布尔值接口。

安全布尔值名称	默认值	布尔值含义
secure_mode	false	是否允许通过执行 newrole 和 su 程序切换到管理员用户域
secure_mode_insmod	false	是否允许加载内核模块
secure_mode_policyload	false	是否允许加载额外安全策略。如变更为 true 后将禁止安全管理员停止安全模块和改变布尔值
user_ping	false	是否允许普通用户执行 ping 和 traceroute 操作
allow_ptrace	false	是否允许管理员 ptrace 所有的进程
user_dmesg	false	是否允许普通用户执行 dmesg 读系统日志
capability_chown	true	是否允许系统管理员对他人文件进行 chown 和 chmod 操作
capability_dac	true	是否允许系统管理员超越 ACL 自主控制模型限制；默认

		情况下 root 用户可以访问所有 ACL 自主保护的文件
allow_java_execstack	true	是否允许 Java 程序堆栈具有可执行权限

改变上述安全布尔值，可能会出现软件兼容性问题，例如 capability_chown

9.6 安全系统角色划分

在红旗安全操作系统 4.0 中，内置了五种安全角色，具体安全功能如下表所示：

安全角色	描述
user_r	普通用户角色，不允许运行保密程序和读取保密数据。
staff_r	相当于普通用户角色，但是可以运行 su/sudo 命令，能够切换到下面系统管理员角色
sysadm_r	除了审计程序和安全管理程序以外，能够运行系统管理程序
secadm_r	仅仅能够运行安全管理程序和启停系统安全
auditadm_r	只能管理安全审计系统

9.7 安全命令具体权限划分

安全命令	安全管理员	系统管理员	审计管理员
avcstat	Y	Y	Y
audit2allow	Y	N	Y
audit2why	Y	N	Y
chcat/chcon	Y	Y	Y
checkmodule	Y	Y	Y
checkpolicy	Y	N	N
fixfiles	Y	N	N
genhomedircon	Y	N	N

getsebool	Y	Y	Y
getenforce	Y	Y	Y
load_policy	Y	N	N
matchpathcon	Y	Y	Y
restorecon	Y	Y	N
semanage	Y	N	N
semodule	Y	N	N
semodule_expand	Y	Y	Y
semodule_link	Y	Y	Y
semodule_package	Y	Y	Y
sestatus	Y	Y	Y
setenforce	Y	N	N
setfiles	Y	N	N
setsebool	Y	N	N

Y：代表可以运行。N:表示不可运行。

9.8 审计命令权限划分

审计命令	安全管理员	系统管理员	审计管理
auditctl	N	N	Y
ausearch	Y	N	Y
aureport	Y	N	N
service auditd restart	N	N	Y

9.9 系统管理工具常见问题说明

开始->管理工具->系统管理 菜单下的系统管理工具：

- 系统用户和组管理
- 系统性能管理优化和监控
- 系统组件管理
- 系统日志浏览和管理
- 系统任务计划管理工具
- 系统服务管理工具
- 网络文件系统配置管理

上述管理工具的本地默认管理用户为 root，由于本地禁止 root 用户登陆，所以目前只支持远程登陆管理系统，登陆用户为 sysadm。

9.10 关于启用 X 窗口管理系统说明

目前红旗安全操作系统支持系统管理员可以启动图形管理界面。但是从安全角度，建议用户不要启用图形管理界面管理系统。主要原因有以下几个方面：

1.在 X 中目前存在的安全机制主要涉及连接时客户端认证，一旦连接成功，几乎很难控制对于客户端应用程序的恶意攻击。

2．X 协议允许客户端应用程序操作别的客户端窗口。例如移动，拷屏，剪切等。同时允许 客户端发送伪造的键盘鼠标等事件到其他客户端。

3.虽然目前存在保护 X 服务的安全策略，但是这种保护方案粒度还是太粗。