KYLINSOFT
麒麟软件

银河麒麟高级服务器操作系统 V10 SP3 2403

安全中心用户手册

麒麟软件有限公司

2024 年 3 月

目录

1. 概述 1

1.1 产品简介 1

1.2 产品亮点 1

2. 系统安装 2

3. 使用入门 4

3.1 软件位置 4

3.2 安全设置 5

4. 首页 7

5. 安全加固 9

6. 账户保护 9

6.1 密码强度 10

6.2 账户锁定 12

7. 网络保护 12

7.1 联网控制 13

8. 应用保护 14

8.1 应用程序执行控制 15

8.2 应用防护控制 17

8.2.1 进程防杀死 18

8.2.2 内核模块防卸载 19

8.2.3 文件防篡改 20

9. 安全内存 21

10. 可信度量 22

10.1 可信链 22

10.2 系统启动度量 25
10.3 系统启动度量配置 26
10.4 查看度量报告 26
10.5 重新采集基准值 27
11. 麒麟安全命令行工具 27
11.1 security-switch 27
11.1.1 功能 27
11.1.2 用法 27
11.1.3 示例 28
11.2 setstatus 30
11.2.1 功能 30
11.2.2 用法 30
11.2.3 示例 31
11.3 getstatus 34
11.3.1 功能 34
11.3.2 用法 34
11.3.3 示例 34
11.4 kysec_set 35
11.4.1 功能 35
11.4.2 用法 35
11.4.3 示例 37
11.5 kysec_get 37
11.5.1 功能 38
11.5.2 用法 38
11.5.3 示例 39
11.6 security-reinforce 40
11.6.1 功能 40
11.6.2 命令行用法 40

11.6.3 自定义模板用法 41
11.6.4 示例 43
11.7 kydima_set 54
11.7.1 功能 54
11.7.2 用法 55
11.7.3 示例 56
11.8 kydima_get 59
11.8.1 功能 59
11.8.2 用法 59
11.8.3 示例 60

1. 概述

1.1 产品简介

安全中心是一款基于麒麟安全框架（KYSEC）和麒麟铠衣执行环境（KYLIN TEE）构建安全防护并行的双体系架构衍生出的图形化管理工具。提供以下防护能力：

核心安全功能层：包含可信度量、安全内存功能，为 PK 体系提供安全底座，形成一体化主动免疫防御能力。

增强安全功能层：包含安全加固、账户保护、网络保护、应用执行控制和应用防护控制等功能，保障系统运行环境的安全和稳定， 进一步加固双体系安全底座。

1.2 产品亮点

安全中心集安全加固、账户保护、网络保护、应用保护、可信度量、安全内存等功能于一体，全面保障系统运行环境的安全。

安全加固：提供安全服务、内核参数、安全网络、系统命令、系统审计、系统设置、潜在危险、文件权限、风险账户、磁盘检查、密码强度、账户锁定、系统安全、系统维护、资源分配等多维度的扫描与一键加固，及时发现并处理系统安全隐患。

账户保护：提供系统账户密码强度检查和账户锁定机制，实现对系统账户的统一管控，提升系统账户安全防御能力，有效防止密码被暴力破解。

网络保护：提供应用联网控制功能，实时防护应用程序联网行为，阻

断主动外联及其它异常网络活动，提高网络访问安全性。

应用控制：提供应用程序执行控制功能，阻止未知软件、应用程序的恶意执行，避免木马病毒攻击，保障系统运行环境的安全性、可靠性。

应用防护：提供进程防杀死、内核模块防卸载和文件防篡改功能，保护系统关键文件完整性，阻止系统关键应用服务异常中断。

可信度量：提供对计算子系统的主动度量（可信启动、静态度量、动态度量）和主动控制（可信策略）机制，保障系统执行环境的安全性、可靠性。

安全内存：提供用户可配置的内存数据安全机制，保护系统内存数据安全。

2. 系统安装

系统安装过程中在软件选择界面需要勾选麒麟安全增强工具分组，系统中才有安全中心的功能，如图 1 所示。

图 1 软件选择-麒麟安全增强工具分组

若用户在系统安装时未选择麒麟安全增强工具分组，则可以从仓库中安装对应的 ksc-defender 软件包，系统中才有安全中心的功能。

系统安装时已选择麒麟安全增强工具分组，进入系统后默认安全是关闭状态，支持用户在界面中开启安全，界面操作详情见 3.2 章节，命令行操作详情见 11.1 章节。

系统安装过程中在软件选择界面需要勾选 pks 组件分组，系统中才有 pks（安全内存、可信度量）功能，如图 2 所示。

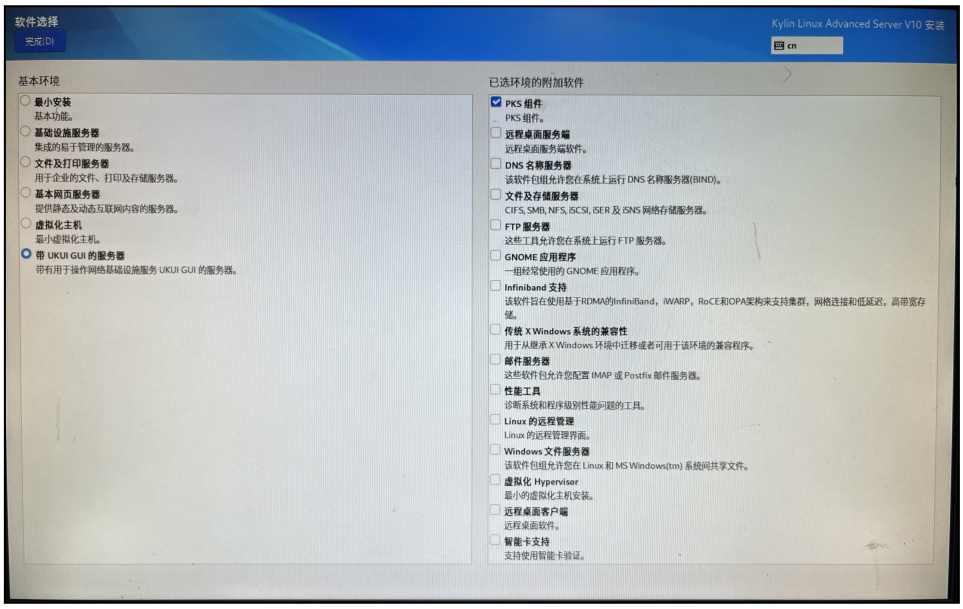

图 2 软件选择-pks 组件分组

3. 使用入门

3.1 软件位置

点击操作系统“开始菜单”，选择并点击“系统工具”菜单，选择并点击“安全中心”，打开安全中心软件界面，如图 3 所示。

图 3 开始菜单（打开安全中心）

3.2 安全设置

安全中心软件界面中点击☰图标，点击“设置”按钮，弹出“设置”弹窗，安全防护模式显示当前模式：自定义，支持选择安全防护设置功能，可选择关闭、推荐和安全优先及开启和关闭文件保护箱功能，如图 4 所示。

(1) 关闭：

(2) 推荐：麒麟特色安全防护机制，提供联网控制、执行控制和应用防护等功能。

(3) 安全优先：麒麟特色安全防护机制，提供联网控制、执行控制和应用防护等功能。同时，提供管理员分权功能，设立系统管理员、安全管

理员和审计管理员，三员权限独立行使、相互制约。

(4) 自定义：当前模式与三种标准模式均不同，可以通过相关命令查看状态详情。

(5) 文件保护箱：可提供用户间数据隔离和加密保护功能。

图 4 安全设置

开启管理员分权功能时，界面伸缩展示三权管理员信息并提供新建管理员密码的功能，点击“设置密码”按钮，弹出“新建密码”弹窗，如图 5 和图 6 所示。

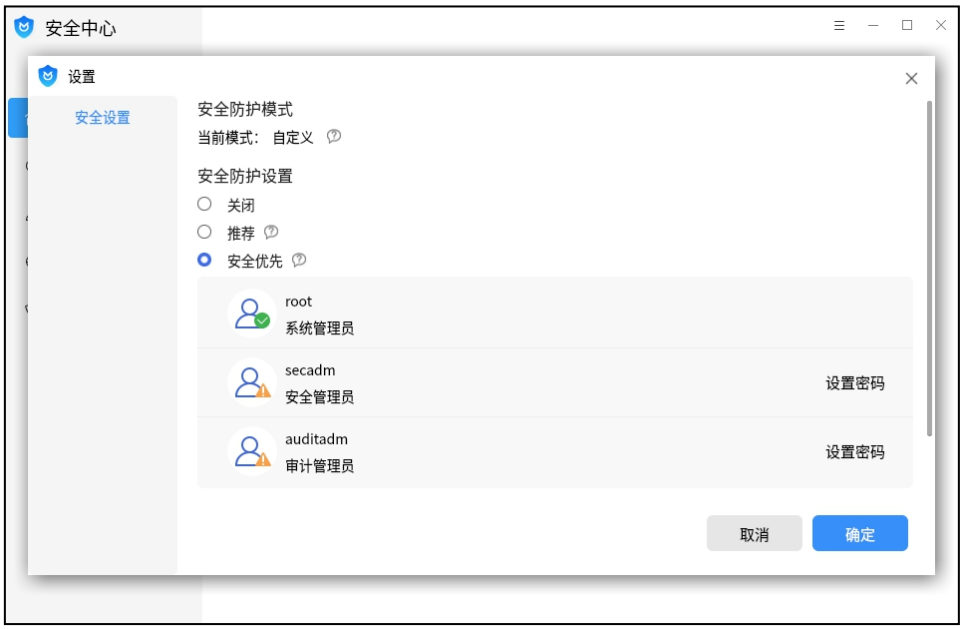

图 5 开启管理员分权功能

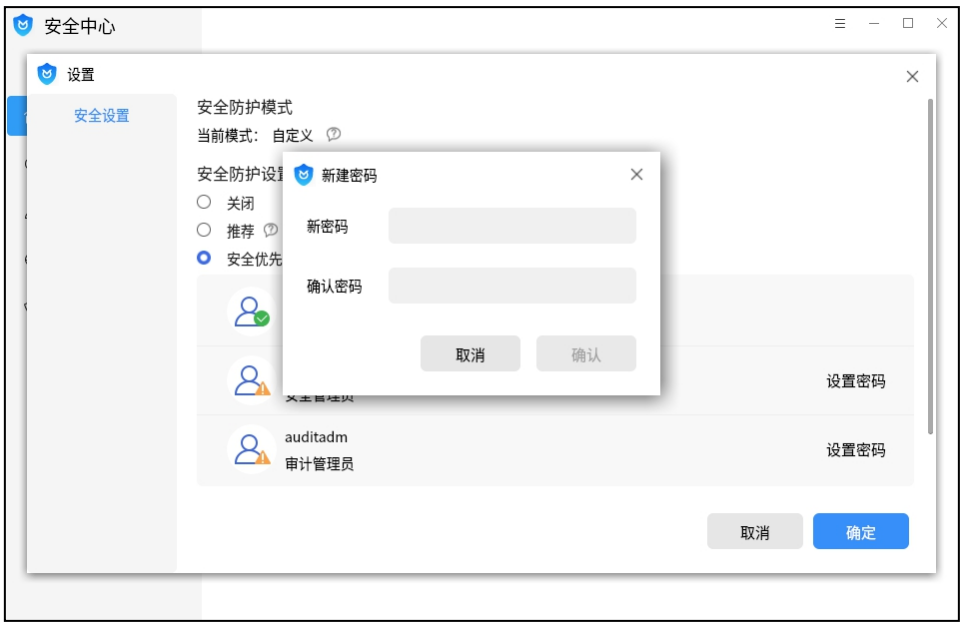

图 6 设置管理员密码

4. 首页

安装过程中未勾选 pks 组件，安全中心首页展示安全加固、账户保护、网

络保护和应用保护四个功能模块的安全状况，可以让用户更直观了解系统当前的安全性和运行情况，同时提供各功能模块操作入口，方便用户进行功能快速跳转并对潜在风险进行及时处理，如图 7 所示。

图 7 安全中心首页（安装过程中未勾选 pks 组件）

安装过程中勾选 pks 组件，安全中心首页展示安全加固、账户保护、网络保护、应用保护、安全内存、可信度量六个功能模块的安全状况，可以让用户更直观了解系统当前的安全性和运行情况，同时提供各功能模块操作入口，方便用户进行功能快速跳转并对潜在风险进行及时处理，如图 8 所示。

图 8 安全中心首页（安装过程中勾选 pks 组件）

5. 安全加固

安全中心的安全加固界面未做适配，不建议使用。建议使用安全加固命令行工具 security-reinforce，见章节 11.6。

6. 账户保护

安全中心提供系统账户密码强度策略配置，账户锁定策略配置功能。点击首页的“账户保护”按钮，或左侧列表中“账户保护”标签页进入，如图 9 所示。

图 9 账户保护首页

6.1 密码强度

密码强度功能可以开启或关闭。开启状态时，系统账户需要遵循当前密码强度策略要求；关闭状态时，系统账户无任何密码强度限制。

密码强度提供推荐、自定义两种配置模式。推荐模式：至少 8 位，包含大写字母、小写字母、数字、特殊符号中的 2 种，密码禁止包含用户名等配置策略；自定义模式：根据需要自定义相应的密码强度策略，如图 10 所示。

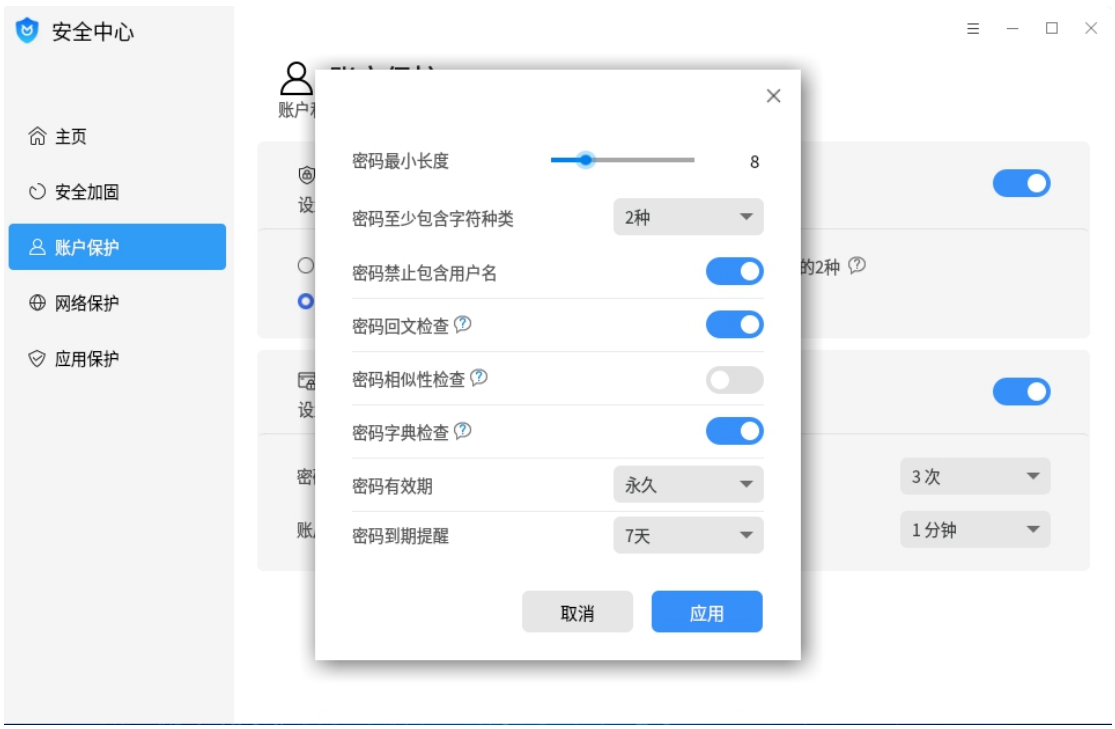

图 10 自定义密码强度策略

自定义密码强度策略配置界面提供以下设置：

（1）密码最小长度，设置范围 1 至 32 位；

（2）密码至少包含字符种类，设置范围 1 至 4 种；

（3）密码禁止包含用户名，功能可启用或关闭；

（4）密码回文检查，正读反读均相同的密码将不能设置成功，功能可启用或关闭；

（5）密码相似性检查，与原密码相似度大的密码将不能设置成功，如只改变字母大小写，功能可启用或关闭；

（6）密码字典检查，密码字典中存储着用户常用密码，与字典内字符相同的密码将不能设置成功，功能可启用或关闭；

（7）密码有效时间，包含 7 天、30 天、90 天、180 天和永久，默认为永

久；

（8）密码到期提醒，包含 3 天、7 天、15 天和 30 天，当设置密码有效时间为 7 天时，密码到期提醒只能选择 3 天；

（9）密码回文检查、密码相似性检查和密码字典检查提供功能说明提示，当鼠标悬停在提示图标时显示对应项的详细说明。

6.2 账户锁定

账户锁定功能可以开启或关闭。开启状态时，系统账户需要遵循当前账户锁定策略要求；关闭状态时，系统账户无账户锁定限制。

账户锁定功能提供密码连续输错次数和账户锁定时间配置。密码连续输错次数：设置范围 3 至 10 次，默认为 3 次；账户锁定时间：1 分钟、3 分钟、5 分钟、10 分钟、15 分钟、30 分钟，默认为 1 分钟。

7. 网络保护

安全中心提供联网控制功能，保护系统网络安全性。点击首页“网络保护”按钮，或左侧列表中“网络保护”标签页进入，如图 11 所示。

图 11 网络保护首页

7.1 联网控制

设置应用联网控制策略，保护系统网络安全性。联网控制功能提供开启和关闭配置，如图 12 所示。开启：管控应用程序的联网行为；关闭：允许任何应用程序联网。

图 12 联网控制

联网控制功能开启时，点击“高级配置”按钮，弹出“高级配置-联网控制”弹窗，可以对单个应用或服务进行联网控制策略配置，提供允许和阻止，如图 13 所示。

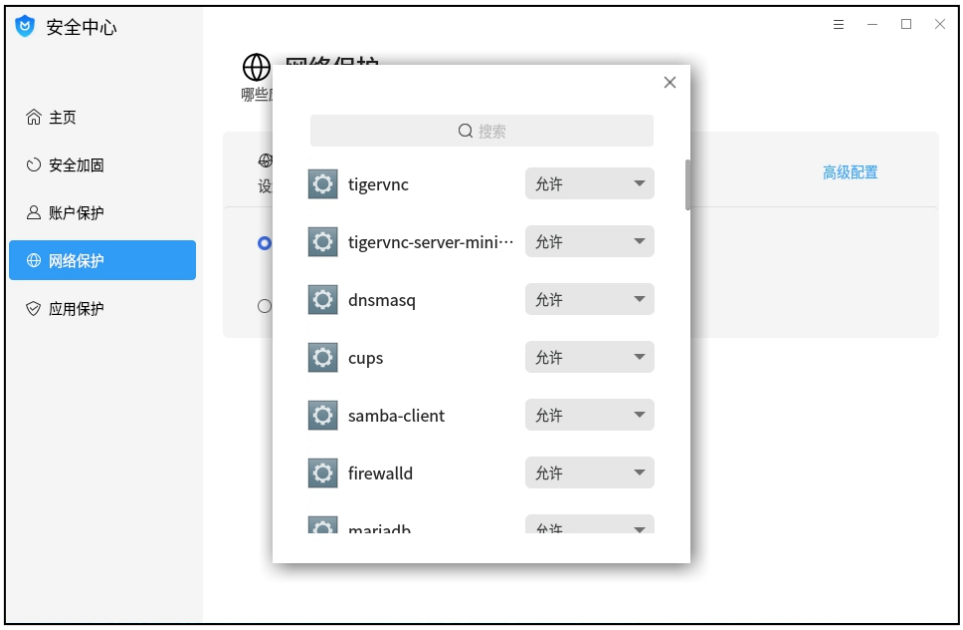

图 13 高级配置-联网控制

8. 应用保护

安全中心提供应用保护功能，保护您的系统免受安全威胁。点击首页“应用保护”按钮，或左侧菜单栏中“应用保护”标签页进入，如图 14 所示。

图 14 应用保护首页

8.1 应用程序执行控制

设置未认证应用执行策略，保护系统运行环境安全。执行控制功能提供三种模式配置，如图 14 所示。开启：阻止执行未认证的应用程序；关闭：允许执行任何应用程序。

点击“高级配置”按钮，弹出“高级配置-应用程序执行控制”弹窗，应用程序执行控制列表显示内容包括序号、文件路径、文件类型和当前状态，如图 15 所示。

（1）文件类型包括：可执行程序、共享库、可执行脚本和内核模块文件 4 种类型。

（2）当前状态包括：“被篡改”、“已损坏”和“已认证”。被篡改：表示该文件已经被篡改，并且文件类型未发生改变，此类文件可以进行认证和解除认证，也可以重新安装对应的软件包进行手动恢复；已损坏：表示该文件已经被

篡改并且文件类型已被破坏，此类文件不能进行认证和解除认证，只能进行恢复或重新安装对应的软件包进行手动恢复；已认证：表示该文件未被篡改。

（3）操作包括认证、解除。认证：将“被篡改”应用程序重新认证并信任，认证成功后当前状态变为“已认证”，当前应用程序可以执行；解除：将“被篡改”或“已认证”应用程序解除认证并不信任，应用程序执行控制列表会自动清除该应用程序信息，当前应用程序不可以执行；

（4）默认按照“被篡改”、“已损坏”和“已认证”的顺序依次排序。

图 15 高级配置-应用程序执行控制（简略信息）

点击“添加”按钮，弹出“添加应用程序基准值”弹框，可以添加选择单个应用程序或目录，添加目录是扫描当前目录下的所有应用程序，如图 16 所示。

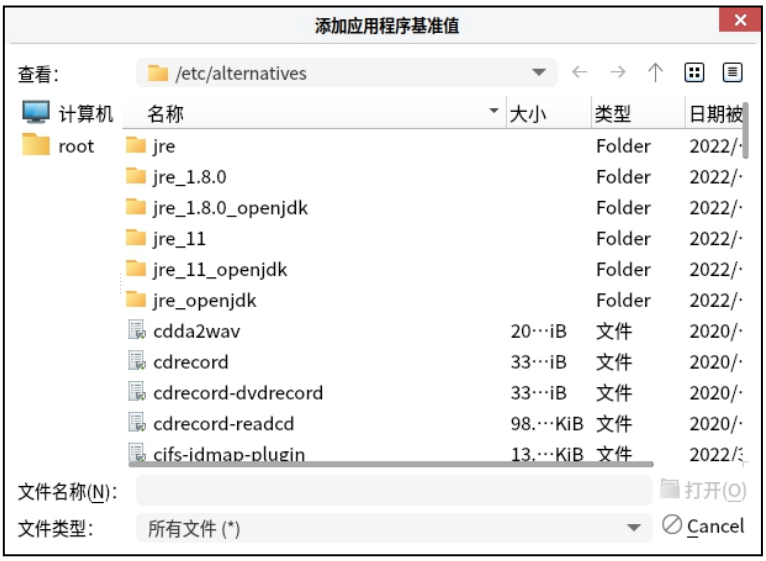

图 16 添加应用程序基准值

执行控制列表默认按照简略信息展示，只展示新安装应用程序信息，如图 34 所示。点击“详细信息”按钮可切换显示系统所有应用程序信息，如图 17 所示。

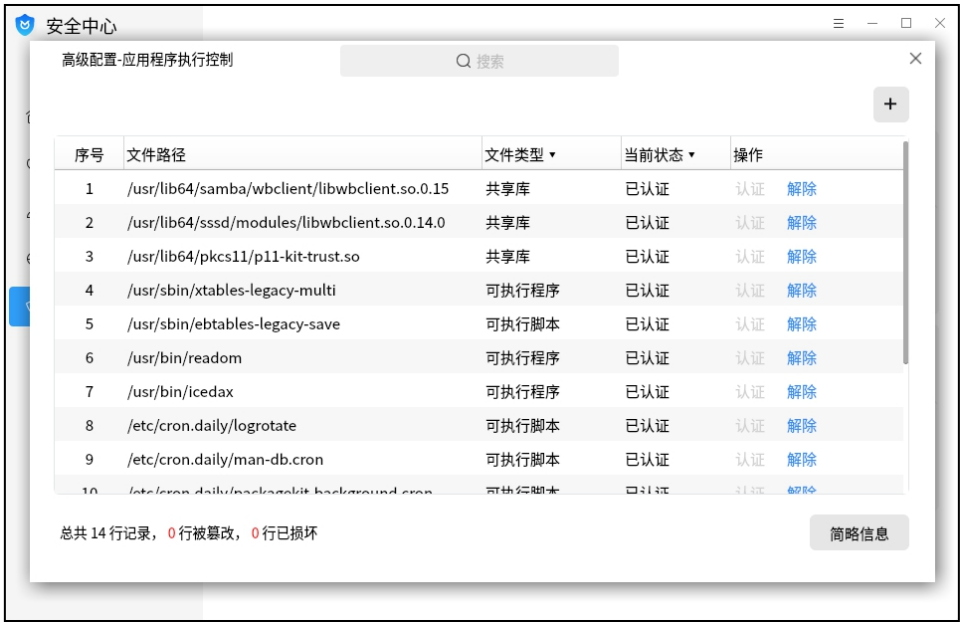

图 17 高级配置-应用程序执行控制（详细信息）

8.2 应用防护控制

设置系统安全防护策略，实时防护已配置的应用，保护系统关键服务运行稳定。应用防护控制功能提供开启和关闭配置。开启时，实时防护配置应用；关闭时，无任何应用防护机制，如图 14 所示。

点击“高级配置”按钮，弹出“高级配置-应用防护控制”弹框，提供进程防杀死、内核模块文件防卸载和文件防篡改功能，如图 18 所示。

8.2.1 进程防杀死

进程防杀死策略配置列表显示内容包括：序号、进程号、进程名称、进程路径和防杀死保护开关。

出现多个名称相同的进程时，防杀死保护开关合并成一个，防杀死保护开启后可以同时保护这些进程，列表默认按照收起方式显示，点击展开或收起按钮进行显示切换，如图 18 至 19 所示。

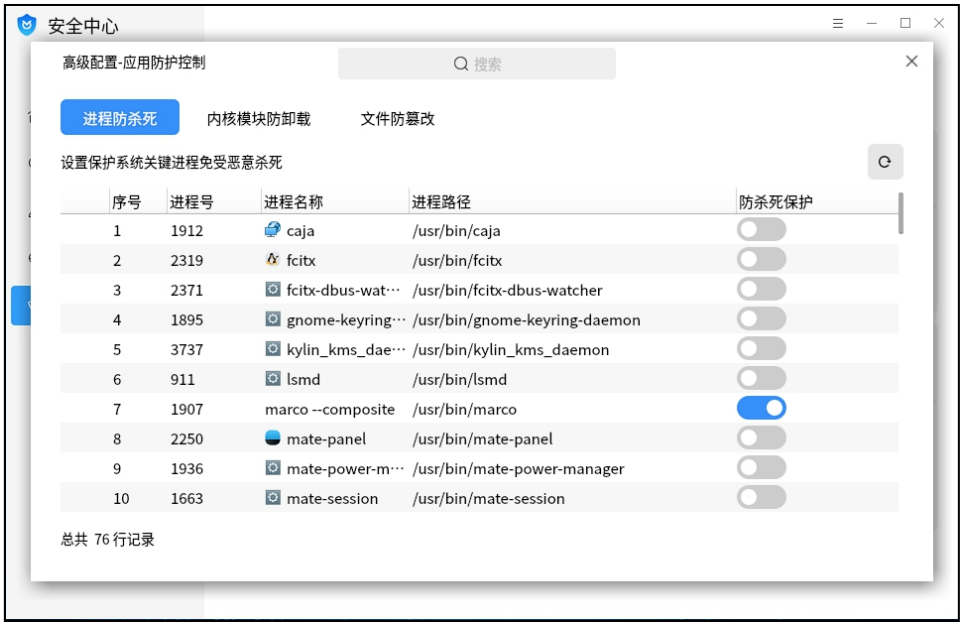

图 18 进程防杀死（默认收起）

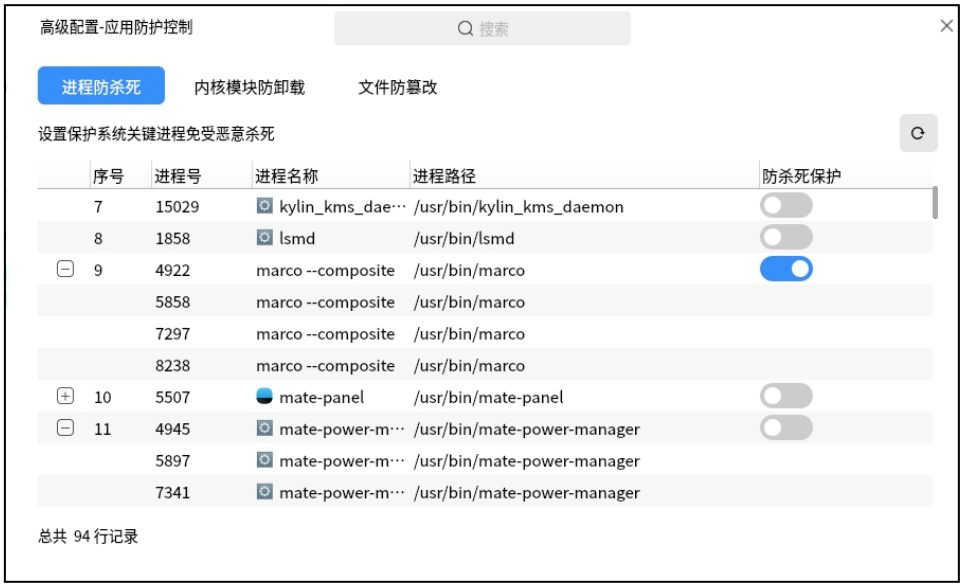

图 19 进程防杀死（展开）

8.2.2 内核模块防卸载

内核模块防卸载策略配置列表显示内容包括：序号、内核模块名称和防卸载保护开关，如图 20 所示。

图 20 内核模块防卸载

8.2.3 文件防篡改

文件防篡改策略配置列表显示示内容包括：序号、文件名称、文件路径和解除操作，解除受保护文件后，文件从列表中自动清除，如图 21 所示。

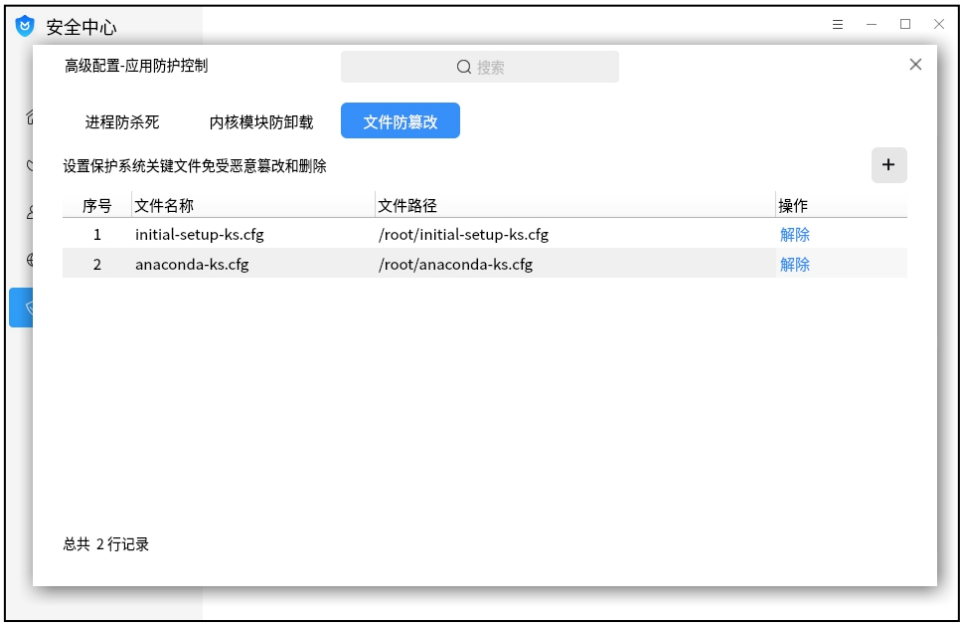

图 21 文件防篡改

点击“添加”按钮，弹出“选择需要受保护的文件”弹窗，可以自行添加需要受保护的文件，如图 22 所示。

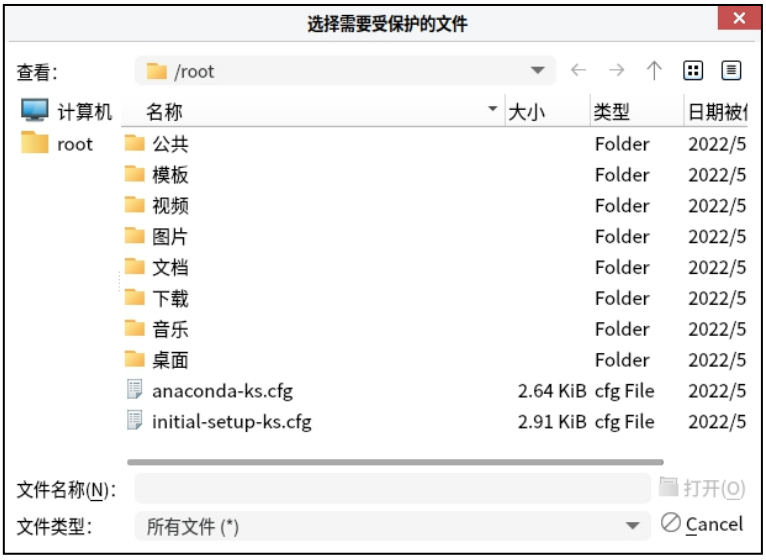

图 22 选择需要受保护的文件

9. 安全内存

安全内存是一款完全兼容 DDR4 RDIMM 内存系统的安全内存模组。该产品基 于 DDR4 RDIMM 内存模组，由 8 Gb DDR4 SDRAM 通用内存颗粒和内建了 SAM（安全访问权限管理）机制的澜起安全寄存缓存器芯片（即“安全 RCD 芯片”）组成， 支持速率达 DDR4-2666。

设备出厂用户需选配澜起（HSDIMM-Lite）安全内存，安全中心才会显示安全内存模块，安全内存界面展示内存相关的基本信息，如类型、速度、容量、防护范围等信息。其中防护范围为系统调用表，用户可根据需要开启或关闭当前的开关。如图 23 所示。

图 23 安全内存页

10. 可信度量

银河麒麟服务器操作系统将系统结构划分为两个不同的计算域，对应为双体系架构麒麟可信执行环境(KYLIN TEE)与麒麟通用计算环境（KYLIN REE）。

双体系架构是将 CPU 核、IO 输入输出设备、内存等硬件资源隔离形成两套完整的子系统。计算部件（REE）无法访问安全部件（TEE）的内容，通过把加密 密钥等数据存放在安全部件，实现了隐私数据的隔离，只有安全部件和安全应用（TA）能够访问，从而进异步保障数据的安全性。

通过可信度量、机密计算技术，实现对计算子系统的主动度量（可信启动、静态度量、动态度量）和主动控制（可信策略）。

10.1 可信链

基于 CPU-IP 核（即 TCM/TPCM）硬件资源构建可信根，提供可信基环境。信任链可对可信启动过程中所有环节的度量结果进行查看。如果有发现度量值改变的文件，标记为不可信，并且用户可进行查看和信任操作。如图 24 所示。

图 24 可信度量页

1、信任链

（1）包括可信芯片、BIOS、引导程序、操作系统、应用程序，每次系统启动后更新信任链状态，用户进入可信度量后，动态展示各个环节的度量结果。

（2）如果某个节点存在不可信的文件，则该节点标红；节点正常，则图标为蓝色；当可信芯片无法识别时，可信芯片与 BIOS 按钮置灰，无法点击。

（3）点击可信芯片可查看详情。

查看详情：包括 TPCM 版本信息、可信计算 CPU 核数量、总容量、可用容量等。不同模式的可信根信息不一样，kyee 可信根详情如图 25 所示。

图 25 kyee 可信根详情

（4）点击 BIOS、引导程序、操作系统均可进入系统启动度量的高级配置页，，如图 26 所示。

图 26 UEFI 详情和 GRUB 详情

（5）点击应用程序进入应用程序度量的高级配置页。

10.2 系统启动度量

可信启动依据信任传递的思想，实现对可信根、TPCM、可信固件 UEFI 、GRUB 引导程序、系统内核文件与关键配置文件进行逐级度量，构建完整可信信任链，为设备启动建立初态的可信执行环境。

可信启动主要展示启动度量基准库条数、本次度量失败条数、本次启动可信状态、本次度量报告时间四项信息。如图 27 所示。

（1）启动度量基准库条数：显示为当前初始化后的基准库总条数；

（2）本次度量失败条数：显示为度量值与基准库不一致的度量失败条数 ；

（3）本次启动可信状态：显示设备本次启动度量的可信或不可信状态；

（4）本次度量报告时间：显示本次的可信度量报告产生时间；

图 27 可信启动页

10.3 系统启动度量配置

可信启动功能提供开启和关闭两种配置模式。如图 28 所示。

（1）开启：监测到系统环境变化时，请通知我；

（2）关闭：不进行设备环境监测。

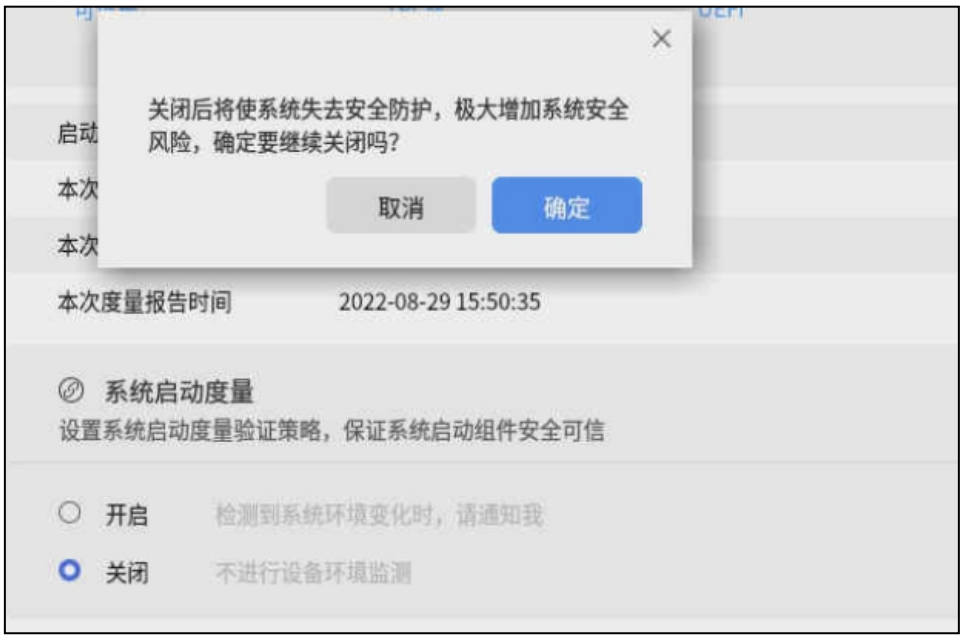

图 28 可信启动配置

10.4 查看度量报告

点击“查看详情”，可查看本次可信启动的度量报告日志。如图 29 所示。

图 29 查看度量报告

10.5 重新采集基准值

当存在度量失败项时，可通过点击“重新采集基准值”按钮并“确定”后，将会进行基准库的重新初始化，恢复对当前度量失败项的可信状态。如图 30 所示。

图 30 重新采集基准值

11. 麒麟安全命令行工具

11.1 security-switch

11.1.1 功能

用于设置安全模式和获取安全模式状态。

11.1.2 用法

security-switch <--set|--get|--help|-h> [mode]

-h,--help 显示帮助信息

--set 设置安全模式

mode 安全模式

none：关闭，disable；

default： 推荐，only kysec enforcing；

strict：安全优先，（selinux ukmcs + kysec enforcing + kysec 3adm）

--get 获取安全模式状态

11.1.3 示例

security-switch --set none

```
[root@localhost 桌面]# security-switch --set none
正在为关闭 'Kysec' 检查系统配置状态... OK
正在为关闭 'SELinux' 检查系统配置状态... OK
正在为关闭 '三权分立' 检查系统配置状态... OK
正在禁用 'Kysec' ... OK
正在禁用 'SELinux' ... OK
正在禁用 '三权分立' ... OK
正在更新系统启动配置... OK
正在写入系统安全配置... OK
系统安全级别切换成功，请立即重启系统生效!!!
[root@localhost 桌面]#
```

图 31 设置 none 模式

security-switch --set default

```
[root@localhost 桌面]# security-switch --set default
正在为 'Kysec' 检查内核配置... OK
正在为 'Kysec' 检查软件包安装状态... OK
正在为 'Kysec' 检查文件安装状态... OK
正在为开启 'Kysec' 检查系统配置状态... OK
正在为关闭 'SELinux' 检查系统配置状态... OK
正在为关闭 '三权分立' 检查系统配置状态... OK
正在启用 'Kysec' ... OK
正在禁用 'SELinux' ... OK
正在禁用 '三权分立' ... OK
正在更新系统启动配置... OK
正在写入系统安全配置... OK
系统安全级别切换成功，请立即重启系统生效!!!
[root@localhost 桌面]#
```

图 32 设置 default 模式

security-switch --set strict

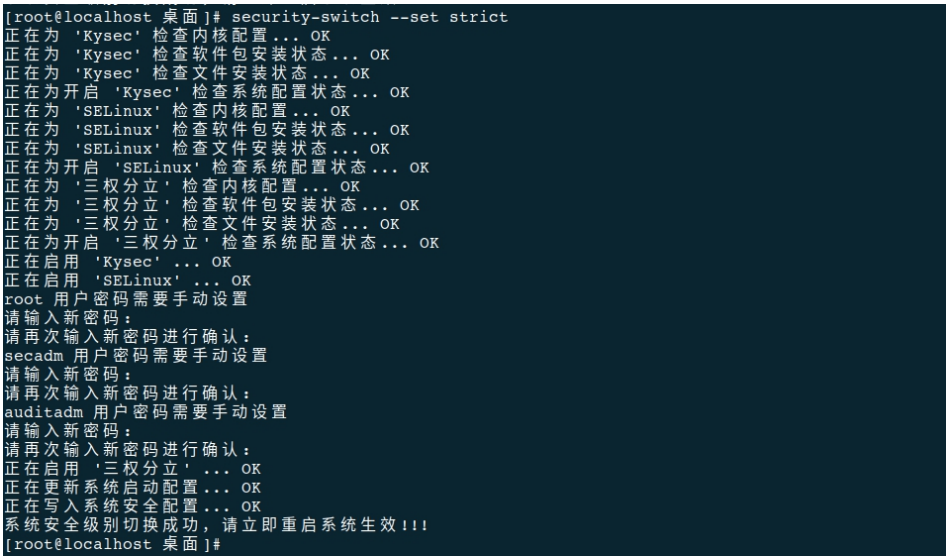

图 33 设置 strict 模式

security-switch –get

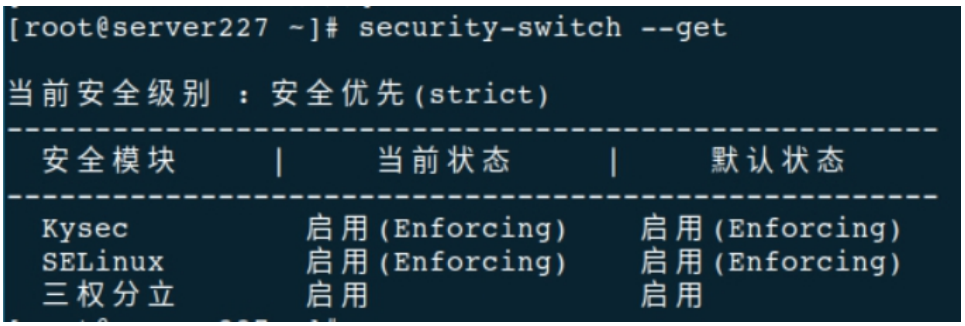

图 34 获取当前安全模式

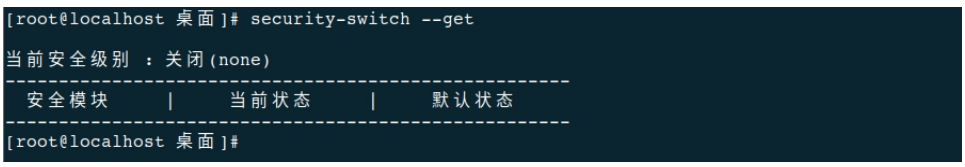

图 35 获取当前安全模式

11.2 setstatus

11.2.1 功能

提供安全模块的开和关设置，包括 kysec、box、apparmor、selinux 等安全模块的开关。

11.2.2 用法

setstatus <module> [-s,--status][-f,--func][-c,--control] [-t,--temporary] [-h,--help]

-h,--help 显示帮助信息

module 安全模块名

kysec：麒麟安全框架，提供联网控制、应用执行控制和应用防护等功能

selinux：selinux 是一种基于域-类型模型的强制访问控制安全系统

box：文件保护箱提供用户间数据隔离和加密保护功能，支持国密算法

apparmor：apparmor 是一种基于文件或目录的强制访问控制安全系统

-s,--status 设置安全模块的状态

安全模块为 kysec 时取值：

disable 关闭

enforcing 强制模式

permissive 宽松模式

安全模块为 selinux 时取值：

disable 不生效

enforcing 强制模式

permissive 宽松模式

安全模块为 box 时取值：

disable 关闭

enable 开启

安全模块为 apparmor 时取值：

disable 关闭

enable 开启

-f，--func 安全模块下的子功能，子功能状态依赖安全模块的状态，无子功能无需设置

安全模块为 kysec 时取值：

exectl 执行管控子模块

netctl 应用联网管控子模块

ppro 进程防杀死子模块

fpro 文件保护子模块

kmod 模块防卸载子模块

-c，--control 子功能管控状态

exectl：on/off on 表示开启，在 kysec 为 enforcing 状态时，阻止执行未认证或已篡改的应用程序；在 kysec 为 permissive 状态时，允许执行任何应用程序并记录执行日志。off 表示关闭，允许执行任何应用程序且不记录执行日志

netctl：on/off on 表示开启，off 表示关闭

ppro：on/off on 表示开启，off 表示关闭

kmod：on/off on 表示开启，off 表示关闭

fpro：on/off on 表示开启，off 表示关闭

-t，--temporary 临时生效(只支持 selinux、kysec 模块的 permisive 和 enforcing 状态间，kysec 子模块状态的切换)

11.2.3 示例

1）设置 kysec 的状态为 enforcing

图 36 设置 kysec 状态为 enforcing

2）设置 kysec 的状态为临时 permissive

```
[root@localhost 桌面]# setstatus kysec -s permissive -t
[root@localhost 桌面]# getstatus
KySec status: permissive
        exectl  : on
        netctl  : off
        fpro    : on
        kmod    : on
        ppro    : on
selinux status: disable
apparmor status: disable
box status: enable
```

图 37 设置 kysec 状态为 permissive

3）设置 kysec 的状态为临时 enforcing

```
[root@localhost 桌面]# setstatus kysec -s enforcing -t
[root@localhost 桌面]# getstatus
KySec status: enforcing
        exectl  : on
        netctl  : off
        fpro    : on
        kmod    : on
        ppro    : on
selinux status: disable
apparmor status: disable
box status: enable
```

图 38 设置 kysec 临时状态

4）设置 kysec 的执行管控为关闭状态

```
[root@localhost 桌面]# setstatus kysec -f exectl -c off
[root@localhost 桌面]#
[root@localhost 桌面]# getstatus
KySec status: enforcing
        exectl  : off
        netctl  : off
        fpro    : on
        kmod    : on
        ppro    : on
selinux status: disable
apparmor status: disable
box status: enable
```

图 39 设置子模块 exectl 的状态

5）设置 kysec 的状态为 disable

```
[root@localhost ~]# setstatus kysec -s disable
kysec已成功设置为disable，此设置将使系统失去安全防护，极大增加系统安全风险！
```

图 40 设置 kysec 状态为 disable

6）设置 selinux 的状态为 enforing

```
[root@server227 ~]# setstatus selinux -s enforcing
安全模块状态设置改变，需要重启系统才能生效！
```

图 41 设置 selinux 状态为 enforcing

7）设置 selinux 的状态为 permissive

```
[root@server227 ~]# setenforce 0
[root@server227 ~]# getstatus -m selinux
selinux status: permissive
```

图 42 设置 selinux 态为 permissive

8）设置 selinux 的状态为 disable

```
[root@server227 ~]# setstatus selinux -s disable
安全模块状态设置改变，需要重启系统才能生效！
```

图 43 设置 selinux 状态为 disable

9）设置 box 的状态为 enable

```
[root@server227 ~]# setstatus box -s enable
安全模块状态设置改变，需要重启系统才能生效！
```

图 44 设置 box 状态为 enable

10）设置 box 的状态为 disable

```
[root@server227 ~]# setstatus box -s disable
安全模块状态设置改变，需要重启系统才能生效！
```

图 45 设置 box 状态为 disable

11.3 getstatus

11.3.1 功能

获取安全模块状态。

11.3.2 用法

getstatus [-m | --module module] [-h |--help]

-h,--help 显示帮助信息

-m,--module 安全模块名，不带参数显示全部

kysec：麒麟安全框架，提供联网控制、应用执行控制和应用防护等功能

selinux：selinux 是一种基于域-类型模型的强制访问控制安全系统

box：文件保护箱提供用户间数据隔离和加密保护功能，支持国密算法

apparmor：apparmor 是一种基于文件或目录的强制访问控制安全系统

11.3.3 示例

1) 获取安全模块状态

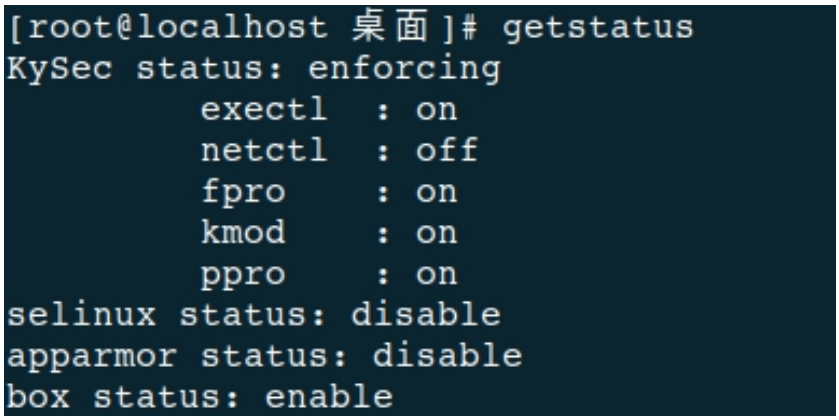

图 46 获取安全状态

2) 获取 kysec 安全模块状态

```
[root@localhost 桌面]# getstatus -m kysec
KySec status: enforcing
        exectl  : on
        netctl  : off
        fpro    : on
        kmod    : on
        ppro    : on
```

图 47 获取 kysec 状态

3) 获取 selinux 安全模块状态

```
[root@localhost ~]# getstatus -m selinux
selinux status: disable
```

图 42 获取 selinux 状态

4) 获取 box 安全模块状态

```
[root@server227 ~]# getstatus -m box
box status: disable
```

图 48 获取 box 状态

11.4 kysec_set

11.4.1 功能

安全模块策略设置。

11.4.2 用法

kysec_set <module> [-R] [-c] [-d] <path> [-v] <value> [-f|-P] <path|pkgname>

-h, --help 显示帮助信息

exectl: 执行管控

-R, --recursive: 递归目录

-v, --value 标签值

original: 系统原始标记

verified: 第三方可执行标记

trusted: 可信文件标记

kysoft: 软件包安装标记

parent: 追溯标记

unknown: 未知文件标记

-f, --file 文件或目录路径，设置文件或目录下文件的标记

-P, --package 已安装的软件包名称，设置软件包中文件的标签

-c, --clean 清除设置的标签

fpro: 文件保护

-v, --value 标签值

readonly: 文件只读

none: 取消只读

-f, --file 文件或目录路径，设置文件或目录下文件的标记

-P, --package 已安装的软件包名称，设置软件包中文件的标签

-c, --clean 清除设置的标签

netctl: 应用程序联网控制

-v, --value 应用程序联网控制状态（不加-v 参数默认阻止联网）

allow: 允许

deny: 阻止

-f, --file 应用程序路径，添加或更新应用程序联网控制策略

-d,--delete 应用程序路径，删除应用程序联网控制策略

ppro: 进程保护

-v, --value 设置进程不可被杀死

allow: 允许杀死

deny: 防杀死

-f, --file 进程程序文件路径

-p, --pid 进程号

kmod: 模块防卸载

-v, --value 设置模块不可被卸载

allow: 允许被卸载

deny: 防卸载

-f, --file 模块文件路径

-n, --name 模块名(可通过 lsmod 查看)

11.4.3 示例

1）递归添加执行控制白名单列表

```
[root@localhost ~]# kysec_set exectl -R -v verified -f /usr/sbin/
```

图 49 对目录下的文件设置标记

2）按照文件路径添加模块防卸载

```
[root@localhost ~]# kysec_set kmod -v deny -f /lib/modules/4.19.90-51.0.v2207.ky
10.x86_64/kernel/sound/soundcore.ko.xz
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# kysec_get kmod -l
模块名称：soundcore, 防卸载保护：开
```

图 50 添加模块防卸载

3）按照文件路径添加应用程序拒绝联网

```
[root@localhost ~]# kysec_set netctl -v deny -f /usr/sbin/sshd
[root@localhost ~]#
```

图 51 设置应用程序联网状态

4）按照文件路径添加程序进程防杀死

```
[root@localhost ~]# kysec_set ppro -v deny -f /usr/sbin/security-reinforce-daemon
[root@localhost ~]#
```

图 52 添加进程防杀死

11.5 kysec_get

11.5.1 功能

安全模块策略获取。

11.5.2 用法

kysec_get <module> [-R][-l][-f][-P][-p][-n] < path | pkgname | pid>

-h, --help 显示帮助信息

exectl: 执行管控

-R, --recursive: 递归目录

-f, --file 文件或目录路径

-P, --package 已安装的软件包名称

-p, --pid 进程号，获取进程的标签

fpro: 文件保护

-R, --recursive: 递归目录

-f, --file 文件或目录路径

-P, --package 已安装的软件包名称

userid：三员用户标识

-R，--recursive：递归目录

-f，--file 文件或目录路径

-P，--package 已安装的软件包名称

netctl: 应用程序联网控制

-l, --list 查看列表

-f, --file 应用程序路径，查看单个应用程序联网控制策略

ppro: 进程保护

-l, --list 查看列表

-f, --file 进程程序文件路径

-p, --pid 进程号，获取进程保护状态

kmod: 模块防卸载

-l, --list 查看列表

-f, --file 模块文件路径

-n, --name 模块名

11.5.3 示例

1）根据文件路径查看执行管控白名单信息

```
[root@localhost ~]# kysec_get exectl -f /usr/share/locale/
exectl: /usr/share/locale/locale.alias: original
```

图 53 执行管控白名单信息

2）查看进程防杀死列表

```
[root@localhost ~]# kysec_get ppro -l
pid: 928, 进程名称：auditd, 进程路径：/usr/sbin/auditd, 防杀死保护：开
pid: 922, 进程名称：kyseclogd, 进程路径：/usr/sbin/kyseclogd, 防杀死保护：开
pid: 1428, 进程名称：kysec-sync-daemon, 进程路径：/usr/sbin/kysec-sync-daemon, 防杀死保护：开
pid: 2232, 进程名称：marco, 进程路径：/usr/bin/marco, 防杀死保护：开
pid: 2278, 进程名称：pulseaudio, 进程路径：/usr/bin/pulseaudio, 防杀死保护：开
```

图 54 进程防杀死列表

3）根据文件路径查看文件只读保护

```
[root@localhost ~]# kysec_get fpro -f /etc/
fpro: /etc/mtab: none
fpro: /etc/fstab: none
fpro: /etc/crypttab: none
fpro: /etc/netconfig: none
fpro: /etc/my.cnf: none
fpro: /etc/virc: none
fpro: /etc/cron.allow: none
fpro: /etc/Trolltech.conf: none
fpro: /etc/uid_list: readonly
fpro: /etc/.productinfo: none
fpro: /etc/issue: none
fpro: /etc/issue.net: none
fpro: /etc/kylin-release: none
fpro: /etc/DIR_COLORS: none
fpro: /etc/os-release: none
fpro: /etc/rhashrc: none
fpro: /etc/system-release: none
fpro: /etc/papersize: none
```

图 55 文件只读保护

4）根据模块名查看模块防卸载信息

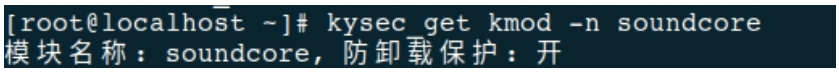

图 56 模块防卸载信息

5）查看应用程序联网列表信息

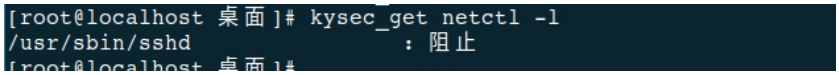

图 57 应用程序联网列表信息

11.6 security-reinforce

11.6.1 功能

安全加固命令提供安全服务、安全网络、磁盘检查、潜在危险、系统安全等15大类安全加固检查项，同时符合操作系统安全三级技术要求，为用户提供加固扫描、一键加固、一键还原和安全报告等功能。

11.6.2 命令行用法

security-reinforce [-h][-s][-f][-r][-t][-e][-i][-d][-l][-p][-o]

无参数　　进入交互式命令行

-h,--help　　显示帮助信息

-s,--scan　　扫描当前模板的所有加固项

-f,--reinforce　　扫描并加固当前模板的所有加固项

-r,--restore　　还原当前模板的所有加固项

-t,--template　　选择模板，参数是-l 选项列出来的模板编号

-e,--export　　导出模板设置，参数是导出路径

-i,--import　　导入模板设置，参数是模板设置文件全路径

-d,--delete　　删除模板，参数是-l 选项列出来的模板编号

-l,--list　　列出当前选择模板和所有模板列表

-p,--report　　显示加固报告概要

-o,--out　　导出加固报告明细

11.6.3 自定义模板用法

1. 获取模板配置文件

命令行如下：

security-reinforce --export　/root

当没有任何自定义模板时，会在指定的目录导出三个模板，分别是安全三级.conf，麒麟安全.conf，default_template.conf，用户可以直接编辑这些模板，自定义模板数据，形成新的模板。

2. 编辑模板文件

三个模板文件都可以编辑，模板配置文件中包含了所有的 sp4 加固项，需要以哪个模板为基础修改就编辑对应的配置文件，如果只需要单个加固项或者自定义的加固项，就编辑模板文件 default_template.conf。

```
1 ############################################################
2 ##自定义参数说明
3
4 #TEMPLATE_NAME          模板名称
5 #TEMPLATE_DESC          模板描述信息
6 #ITEM_ENABLE          加固项是否启用，可设置为0或1，0表示不启用，1表示启用
7 #PASSWORD_MINCLASS        字符种类，可设置为1~4
8 #PASSWORD_MINLEN       口令最小长度加固，可设置为0~256的整数值。如果系统里设定的值
  小于我们设定的值，则会进行加固。
9 #PASS_MAX_DAYS          口令最大生存周期，可设置为整数值
10 #PASS_MIN_DAYS         口令更改最小间隔天数，可设置为整数值
11 #PASS_WARN_AGE         口令过期前警告天数，可设置为整数值
12 #PASSWORD_REPETITION_COUNT     密码重复使用次数，可设置为整数值
13 #UMASK           文件和目录的默认访问权限，可设置为三位八进制整数，如：755
14 #HISTFILESIZE          记录在文件中的命令条数，可设置为整数值
15 #HISTSIZE          记录在内存中的命令条数，可设置为整数值
16 #TMOUT           默认会话超时时间，可设置整数值
17 #PASSWORD_LOCK_NUM        账户认证失败次数限制，可设置为整数值
18 #PASSWORD_LOCK_TIME       账户认证失败锁定时间，可设置为整数值
19 #SCREEN_LOCK_TIME       空闲锁屏时间，可设置为1~120的整数值
20 #DISK_SPACE_RATE       系统磁盘分区使用率，可设置为0~100的整数值
21 #IP_ADDRESS          限制SSH服务可访问源ip地址段，必须为不可重复、不为空的ip段，且格式
  为xxx.xxx.xxx.0，每个ip段以,分隔如192.168.201.0,192.168.202.0,...
22 #CRON_USER          限制用户使用计划任务自定义用户，必须为真实用户名，格式为
  user1,user2,user3,user4
23 #UNNECESSARY_PORT       关闭系统不必要的端口，格式为21, 22, 23, 25, 53, 69, 80, 110,
  111, 443, 1080, 2049, 3128, 3306, 5432, 6379, 8080, 8081, 9098, 9200, 27017
24
25 ############################################################
26 ##模板基本信息
27
28 [TEMPLATE_INFO]
29 TEMPLATE_NAME=default_template
30 TEMPLATE_DESC=默认自定义模板，请根据需要编辑
31
32 ############################################################
33 ##加固项分类：安全服务
34
35 #禁用不必要的xinetd服务-chargen-dgram服务
36 [DISABLE_UNNECESSARY_SERVICE_CHARGEN_DGRAM]
37 ITEM_ENABLE=0
38
39 #禁用不必要的xinetd服务-daytime-stream服务
```

图 58 模板文件

模板文件中头部对可以修改的自定义参数进行了说明，模板名称和模板描述信息均可修改，ITEM_ENABLE 设置为 0，表示不包含该加固项，设置为 1 则表示包含该加固项，总之，用户可以根据参数定义说明

修改模板参数。

3. 编辑好模板文件后，导入模板

命令行如下：

security-reinforce --import /root/default_template.conf

4. 导入模板完成后，选择模板为导入的模板，此时就可以对自定义模板进行扫描加固还原等操作。

11.6.4 示例

1）开始扫描

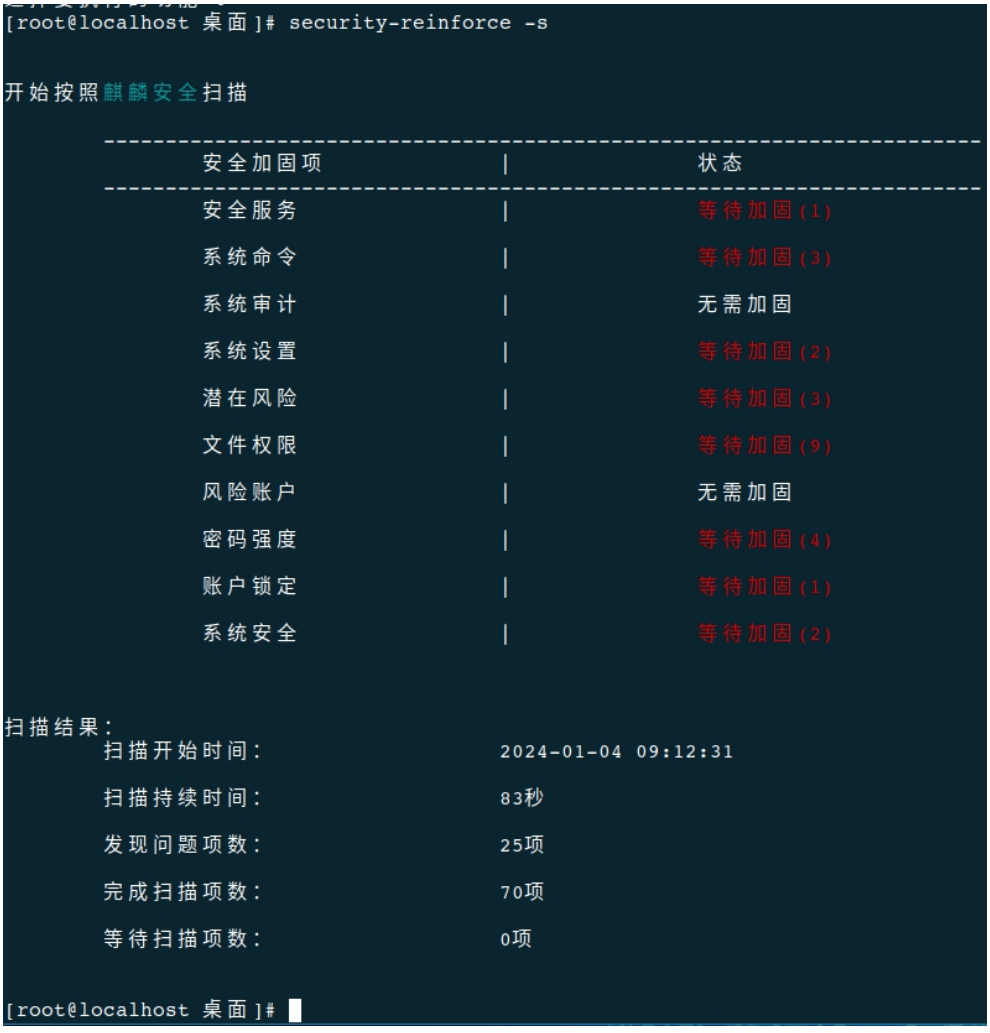

图 59 security-reinforce -s 开始扫描

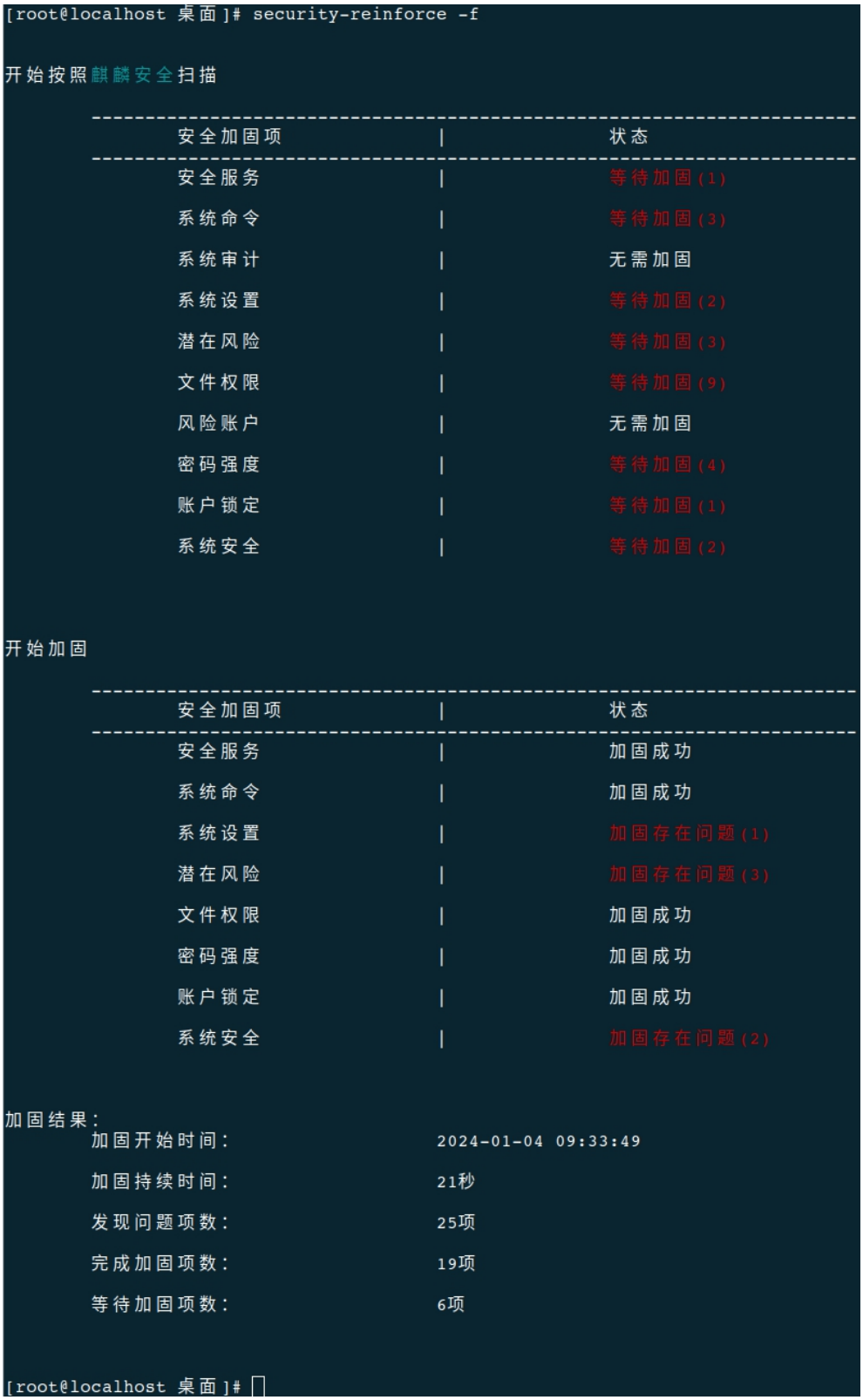

图 60 security-reinforce -f 开始扫描并加固

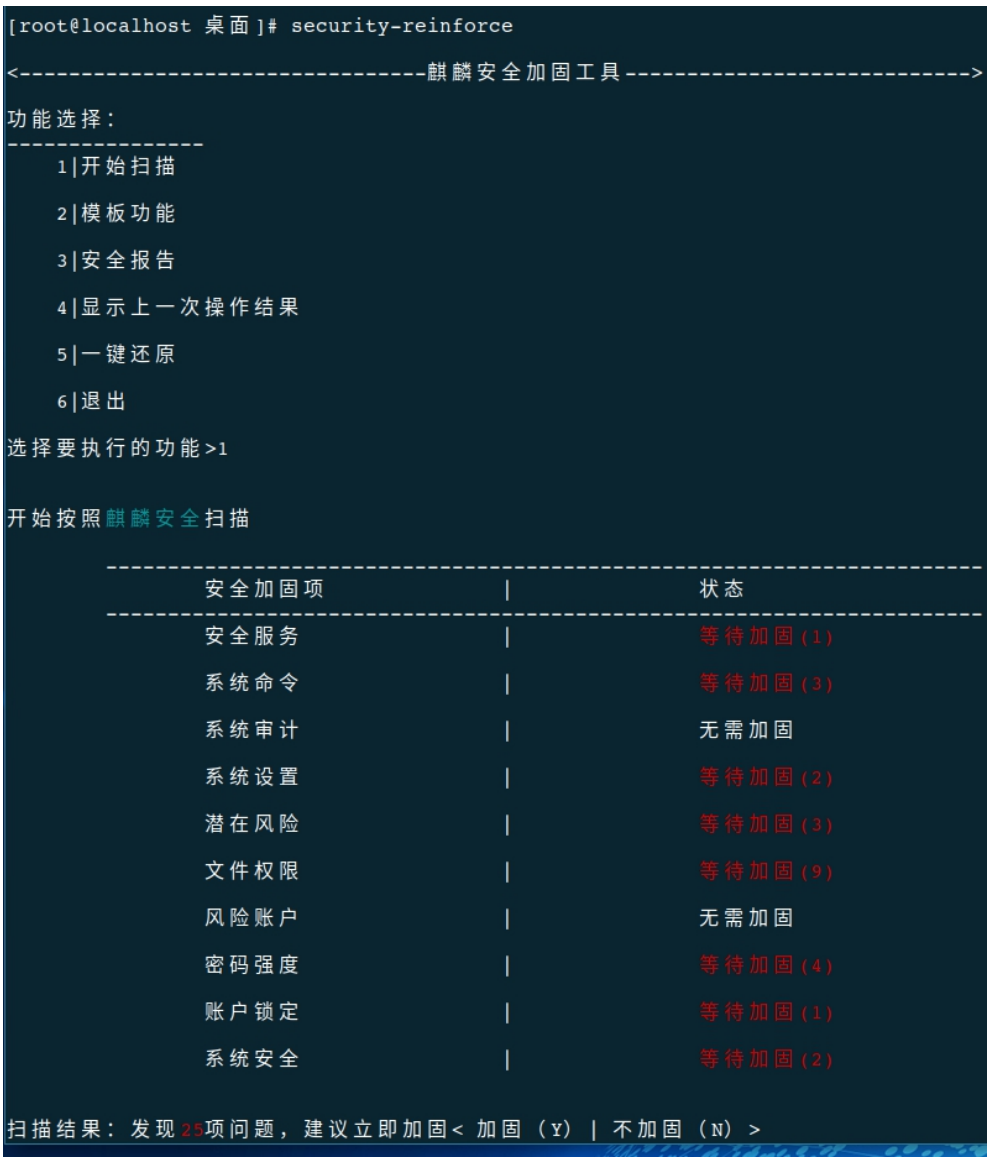
[root@localhost 桌面]# security-reinforce
<----------麒麟安全加固工具---------->
功能选择：
1|开始扫描
2|模板功能
3|安全报告
4|显示上一次操作结果
5|一键还原
6|退出
选择要执行的功能>1
开始按照麒麟安全扫描
安全加固项 | 状态
安全服务 | 等待加固(1)
系统命令 | 等待加固(3)
系统审计 | 无需加固
系统设置 | 等待加固(2)
潜在风险 | 等待加固(3)
文件权限 | 等待加固(9)
风险账户 | 无需加固
密码强度 | 等待加固(4)
账户锁定 | 等待加固(1)
系统安全 | 等待加固(2)
扫描结果：发现25项问题，建议立即加固< 加固（Y）| 不加固（N）>

图 61 交互式开始扫描

```
                账户锁定                |                等待加固(1)
                系统安全                |                等待加固(2)

扫描结果：发现25项问题，建议立即加固< 加固（Y）| 不加固（N）>y

开始加固

        ------------------------------------------------------------------------
                安全加固项              |                状态
        ------------------------------------------------------------------------
                安全服务                |                加固成功
                系统命令                |                加固成功
                系统设置                |                加固存在问题(1)
                潜在风险                |                加固存在问题(3)
                文件权限                |                加固成功
                密码强度                |                加固成功
                账户锁定                |                加固成功
                系统安全                |                加固存在问题(2)


加固结果：
        加固开始时间：                  2024-01-04 08:27:21
        加固持续时间：                  21秒
        发现问题项数：                  25项
        完成加固项数：                  19项
        等待加固项数：                  6项

按ENTER键返回首页>
```

图 62 交互式扫描后立即加固

2）模板功能

```
[root@localhost 桌面]# security-reinforce -l
    当前选择的模板：
    ----------------
        安全三级

    模板列表：
    ---------
        1|麒麟安全
        2|安全三级
        6|test
[root@localhost 桌面]# security-reinforce -t 1
[root@localhost 桌面]# security-reinforce -l
    当前选择的模板：
    ----------------
        麒麟安全

    模板列表：
    ---------
        1|麒麟安全
        2|安全三级
        6|test
```

图 63 选择模板功能

```
[root@localhost 桌面]# security-reinforce -e /opt
已导出配置文件： /opt/麒麟安全2.conf
已导出配置文件： /opt/安全三级4.conf
已导出配置文件： /opt/test2.conf

[root@localhost 桌面]#
```

图 64 导出模板功能

```
[root@localhost 桌面]# security-reinforce

<--------------------------------麒麟安全加固工具---------------------------->

功能选择：
----------------
    1|开始扫描

    2|模板功能

    3|安全报告

    4|显示上一次操作结果

    5|一键还原

    6|退出

选择要执行的功能>2


    当前选择的模板：
    ---------------
        麒麟安全


    模板列表：
    ---------
        1|麒麟安全
        2|安全三级
        3|test


    模板设置：
    ---------
        1|选择模板

        2|导入模板

        3|导出模板

        4|删除模板

        5|返回

选择要执行的功能>1

请输入选择的模板号>
```

图 65 交互式选择模板

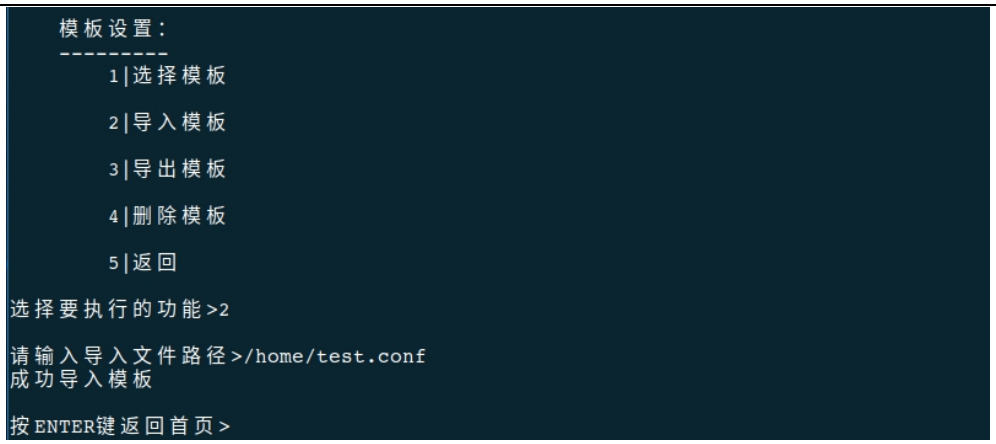

图 66 交互式导入模板

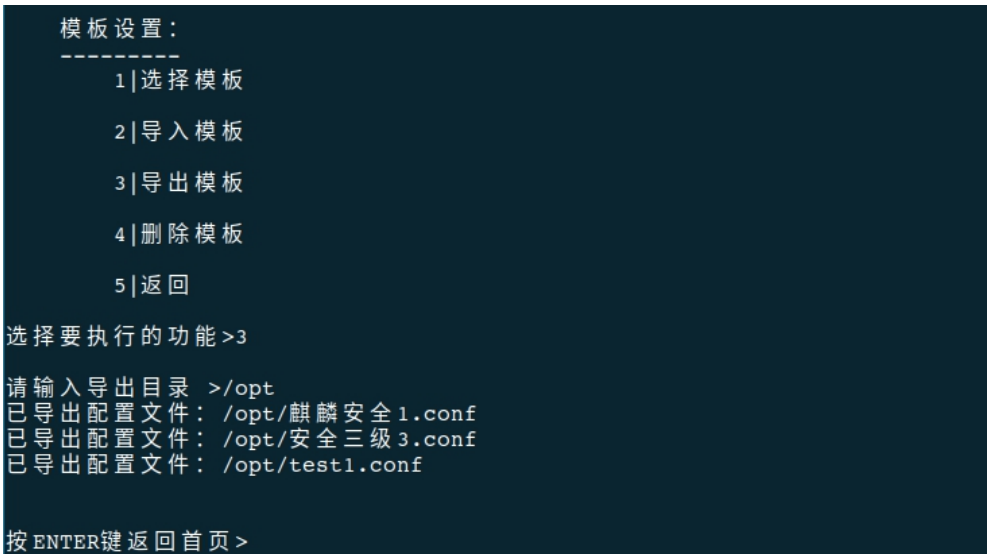

图 67 交互式导出模板

3）自定义模板

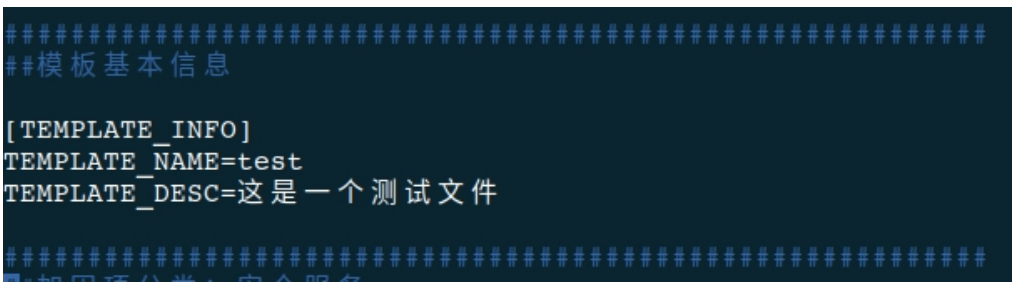

图 68 自定义模板信息（名字和描述）

```
#限制输出和保留历史命令的条数
[RECORD_OUTPUT_HISCMD]
ITEM_ENABLE=1
HISTFILESIZE=5
HISTSIZE=5
```

图 69 自定义模板-包含该加固项，自定义参数

```
请输入导入文件路径>/root/default_template.conf
成功导入模板

按ENTER键返回首页>


    当前选择的模板:
    ---------------
        麒麟安全


    模板列表:
    ---------
        1|麒麟安全
        2|安全三级
        3|test


    模板设置:
    ---------
        1|选择模板

        2|导入模板

        3|导出模板

        4|删除模板

        5|返回

选择要执行的功能>
```

图 70 导入自定义模板

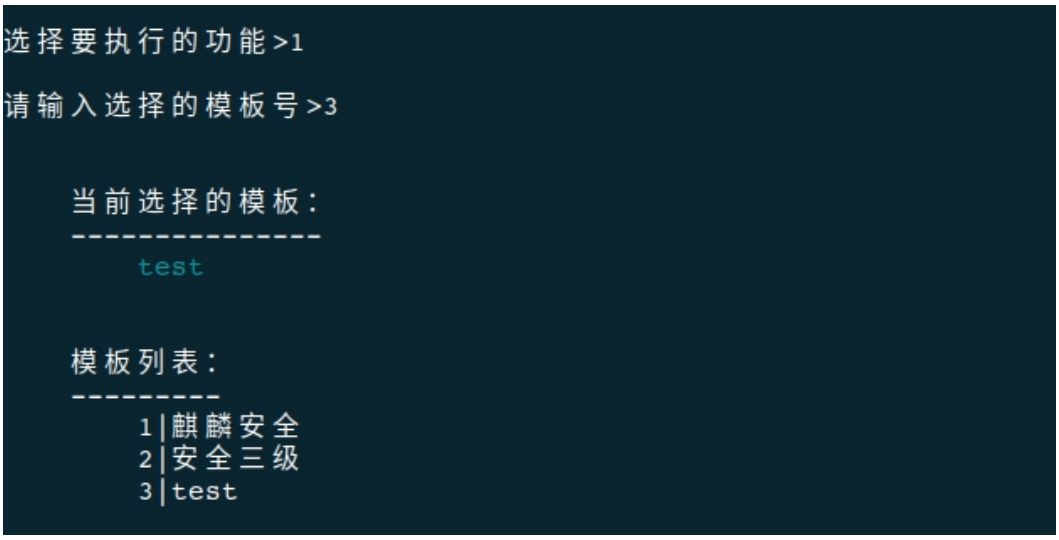

图 71 选择自定义模板

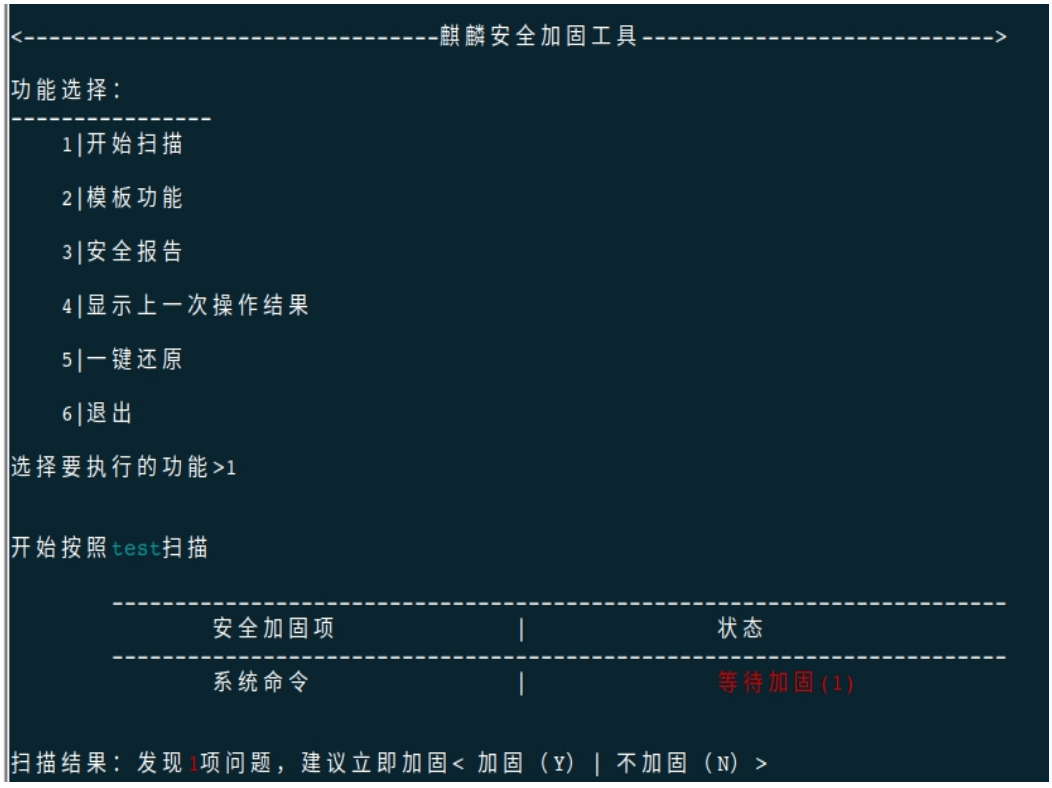

图 72 使用自定义模板扫描（加固还原）

4）安全报告

```
[root@localhost 桌面]# security-reinforce -p

安全报告:
----------------
加固成功:19项    待加固:0项       无需加固:45项    待手动加固:6项   加固失败:0项     重启生效:0
项

[root@localhost 桌面]# security-reinforce -o report

安全报告已经保存到文件/opt/securityreinforce/report/report_20240104095211

[root@localhost 桌面]#
```

图 73 查看安全报告

```
<---------------------------------麒麟安全加固工具----------------------------->

功能选择:
----------------
    1|开始扫描

    2|模板功能

    3|安全报告

    4|显示上一次操作结果

    5|一键还原

    6|退出

选择要执行的功能>3

安全报告:
----------------
加固成功:19项    待加固:0项       无需加固:45项    待手动加固:6项   加固失败:0项     重启生效:0
项


是否导出安全报告明细<Y/N>y

请输入安全报告导出文件名 >report1

安全报告已经保存到文件/opt/securityreinforce/report/report1_20240104083508


按ENTER键返回首页>
```

图 74 交互式查看安全报告

5）显示上一次操作结果

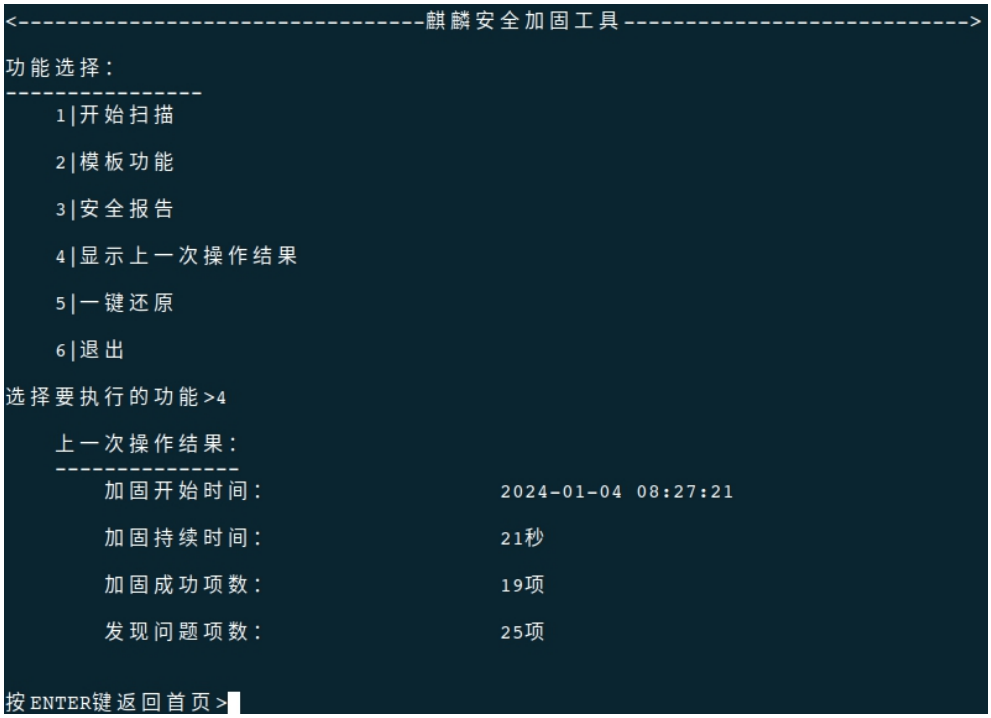

图 75 交互式查看上一次操结果

6）一键还原

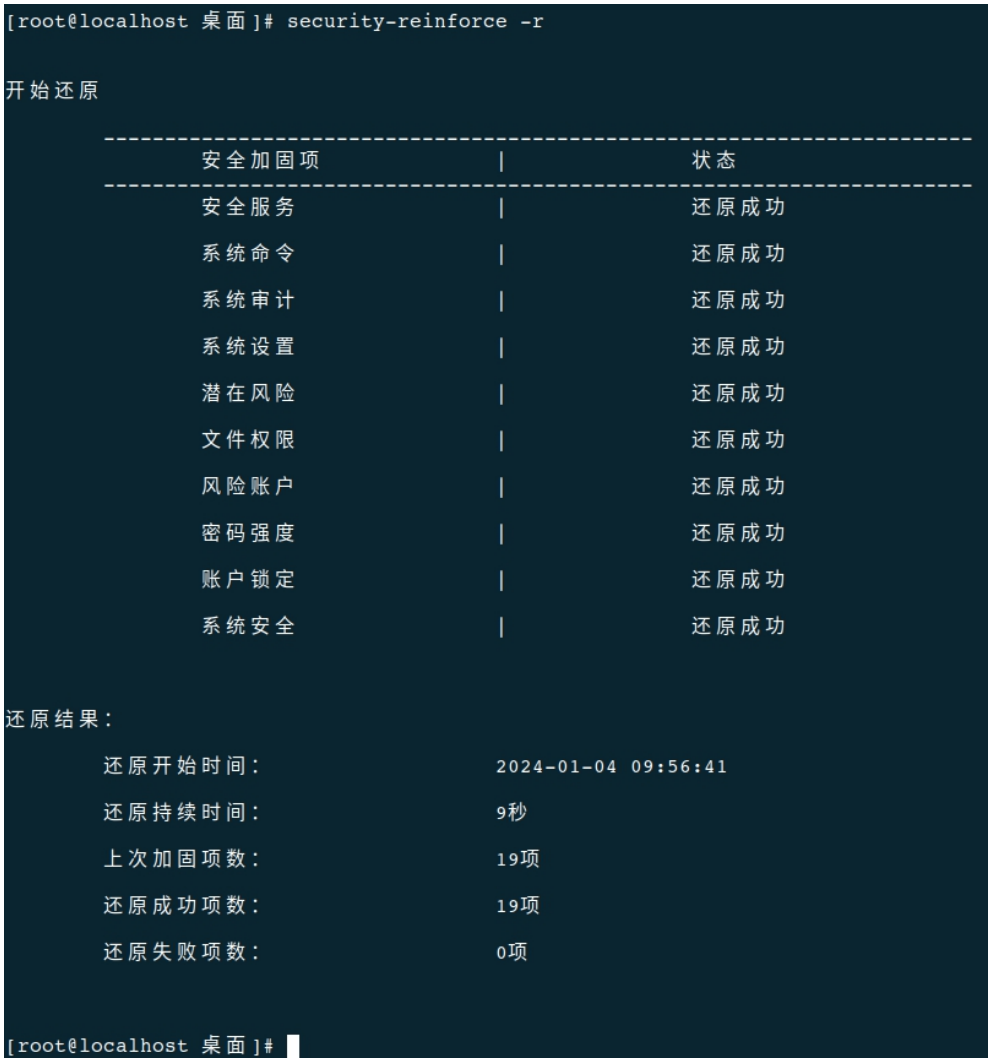
[root@localhost 桌面]# security-reinforce -r
开始还原
安全加固项 | 状态
安全服务 | 还原成功
系统命令 | 还原成功
系统审计 | 还原成功
系统设置 | 还原成功
潜在风险 | 还原成功
文件权限 | 还原成功
风险账户 | 还原成功
密码强度 | 还原成功
账户锁定 | 还原成功
系统安全 | 还原成功
还原结果：
还原开始时间： 2024-01-04 09:56:41
还原持续时间： 9秒
上次加固项数： 19项
还原成功项数： 19项
还原失败项数： 0项
[root@localhost 桌面]#

图 76 一键还原

```
[root@localhost 桌面]# security-reinforce
<---------------------------------麒麟安全加固工具---------------------------->
功能选择：
-----------------
    1|开始扫描
    2|模板功能
    3|安全报告
    4|显示上一次操作结果
    5|一键还原
    6|退出
选择要执行的功能>5

开始还原
        ------------------------------------------------------------------------
                安全加固项                |                状态
        ------------------------------------------------------------------------
                安全服务                  |                还原成功
                系统命令                  |                还原成功
                系统审计                  |                还原成功
                系统设置                  |                还原成功
                潜在风险                  |                还原成功
                文件权限                  |                还原成功
                风险账户                  |                还原成功
                密码强度                  |                还原成功
                账户锁定                  |                还原成功
                系统安全                  |                还原成功


还原结果：
        还原开始时间：                  2024-01-04 09:57:44
        还原持续时间：                  8秒
        上次加固项数：                  0项
        还原成功项数：                  0项
        还原失败项数：                  0项

按ENTER键返回首页>
```

图 77 交互式一键还原

11.7 kydima_set

11.7.1 功能

进程度量与内核防护策略设置。

11.7.2 用法

1）安装进程度量与内核防护功能

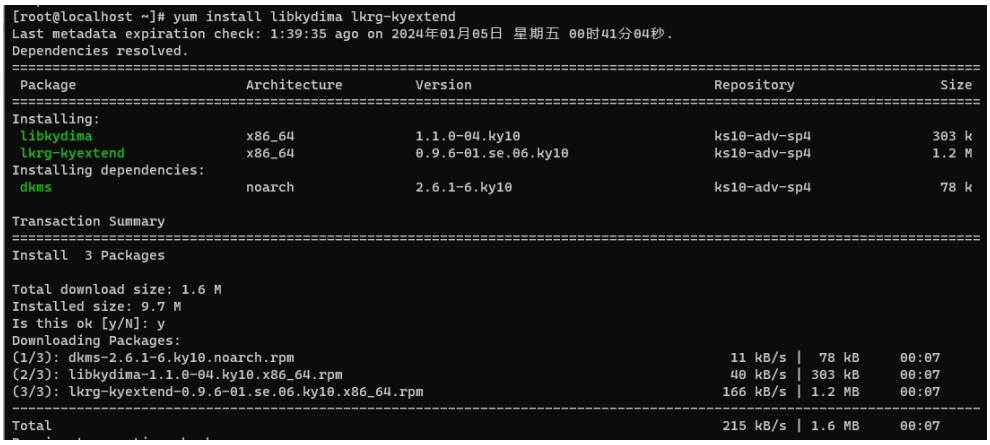

图 78 安装进程度量与内核防护

2）命令行用法：

kydima_set <switch|process|module|kernel|syscalls|idt|event> [-a] [-d] [-f] [-p] [-s] [-c] <value>

参数:

-h, --help 显示帮助信息

switch: 开关策略

-s, --status 状态 on/off。其中，on 表示开启，off 表示关闭；当功能关闭时,无法配置其他参数

-c, --cycle 周期设置(分钟)

process: 进程度量

-a, --add 添加进程

-d, --del 删除进程

-v, --value　　度量策略

kill:　　发现被篡改后杀死该进程

audit:　　发现被篡改后仅记录审计日志

-f, --file　　文件路径

-p, --pid　　进程号

module:　　内核模块度量

-s, --status　　状态　on/off。其中，on 表示开启，off 表示关闭

kernel:　　内核度量

-s, --status　　状态　on/off。其中，on 表示开启，off 表示关闭

syscalls: 系统调用表度量

-s, --status　　状态　on/off。其中，on 表示开启，off 表示关闭

idt:　　中断描述符表度量

-s, --status　　状态　on/off。其中，on 表示开启，off 表示关闭

event:　　事件触发开关

-s, --status　　状态　on/off。其中，on 表示开启，off 表示关闭

pcr:　PCR 扩展策略

-s, --status　状态 on/off。其中，on 表示开启，off 表示关闭.

-r, --register 度量值扩展位置，默认使用 13，可取值 13~23。

-t, --tpm　指定硬件可信设备名称，如 tcm1、tcm2、tpm1、tpm2。

11.7.3 示例

kydima_set process -a -f /usr/lib/systemd/systemd -v audit

kydima_set process -d -f /usr/lib/systemd/systemd

kydima_set process -a -p 1 -v kill

kydima_set process -d -p 1

kydima_set module -s on

kydima_set kernel -s on

kydima_set syscalls -s on

kydima_set idt -s on

kydima_set switch -s on -c 5

kydima_set event -s on

kydima_set pcr -s on -r 13 -t tcm1

kydima_set pcr -s off

1）开启进程度量与内核防护功能开关：

```
[root@localhost ~]# kydima_set switch -s on
[root@localhost ~]# kydima_get switch
switch:  on
```

图 79 kydima_set 开关设置

2）开启功能开关并设置度量周期为 5 分钟

```
[root@localhost ~]# kydima_set switch -s on -c 5
[root@localhost ~]# kydima_get cycle
cycle:  5 分钟
```

图 80 kydima_set 周期设置

3）配置进程度量策略

```
[secadm@localhost ~]$ kydima_set process -a -f /tmp/lkrg-kyextend/test/process -v audit
[secadm@localhost ~]$ kydima_get process -l
       id |进程路径                                                pid     度量结果        度量策略

       1 |/tmp/lkrg-kyextend/test/process                                              仅审计(audit)

         /tmp/lkrg-kyextend/test/process                          4023    未篡改          仅审计(audit)
```

图 81 kydima_set 进程度量策略设置

4）开启模块度量功能

```
[root@localhost ~]# kydima_set module -s on
[root@localhost ~]# kydima_get module
module:  on
```

图 82 kydima_set 模块功能开启设置

5）开启内核度量功能

```
[root@localhost ~]# kydima_set kernel -s on
[root@localhost ~]# kydima_get kernel
kernel:  on
```

图 83 kydima_set 内核开关设置

6）开启系统调用表度量

```
[secadm@localhost tmp]$ kydima_set syscalls -s on
[secadm@localhost tmp]$ kydima_get syscalls
syscalls:  on
```

图 84 kydima_set 系统调用表开关设置

7）开启中断描述符度量

```
[secadm@localhost tmp]$ kydima_set idt -s on
[secadm@localhost tmp]$ kydima_get idt
idt:  on
```

图 85 kydima_set 中断描述符开关设置

8）事件触发开关

```
[secadm@localhost tmp]$ kydima_set event -s on
[secadm@localhost tmp]$ kydima_get event
status:  on
```

图 86 kydima_set 事件开关设置

9）开启 Pcr 扩展功能

```
[root@server227 ~]# kydima_set pcr -s on -r 14 -t tpm2
[root@server227 ~]# kydima_get pcr
pcr:  register: 14
pcr:  tpm: tpm2
```

图 87 kydima_set pcr 寄存器设置

11.8 kydima_get

11.8.1 功能

进程度量与内核防护策略查询。

11.8.2 用法

kydima_get <switch|process|module|kernel|syscalls|idt|cycle|event> [-f] [-p] [-l]

参数:

-h, --help 显示帮助信息

switch: 开关策略

cycle: 周期设置

process: 进程度量

-l, --list 查看列表

-f, --file 文件路径

-p, --pid 进程号

module: 内核模块度量

kernel: 内核度量

syscalls: 系统调用表度量

idt: 中断描述符表度量

event: 事件触发开关

pcr: PCR 扩展策略

11.8.3 示例

kydima_get process -f /usr/lib/systemd/systemd

kydima_get process -p 1

kydima_get module

kydima_get kernel

kydima_get syscalls

kydima_get idt

kydima_get switch

kydima_get cycle

kydima_get event

kydima_get pcr

1）开启进程度量与内核防护功能开关：

```
[root@localhost ~]# kydima_set switch -s on
[root@localhost ~]# kydima_get switch
switch:  on
```

图 88 kydima_get 开关查询

2）开启功能开关并设置度量周期为 5 分钟

```
[root@localhost ~]# kydima_set switch -s on -c 5
[root@localhost ~]# kydima_get cycle
cycle:  5 分钟
```

图 89 kydima_get 周期查询

3）配置进程度量策略

```
[secadm@localhost ~]$ kydima_set process -a -f /tmp/lkrg-kyextend/test/process -v audit
[secadm@localhost ~]$ kydima_get process -l
        id |进程路径                                                  pid     度量结果        度量策略

        1 |/tmp/lkrg-kyextend/test/process                                                  仅审计(audit)

           /tmp/lkrg-kyextend/test/process                            4023    未篡改          仅审计(audit)
```

图 90 kydima_get 进程度量结果查询

4）开启模块度量功能

```
[root@localhost ~]# kydima_set module -s on
[root@localhost ~]# kydima_get module
module:  on
```

图 91 kydima_get 模块开关状态查询

5）开启内核度量功能

```
[root@localhost ~]# kydima_set kernel -s on
[root@localhost ~]# kydima_get kernel
kernel:  on
```

图 92 kydima_get 内核开关状态查询

6）开启系统调用表度量

```
[secadm@localhost tmp]$ kydima_set syscalls -s on
[secadm@localhost tmp]$ kydima_get syscalls
syscalls:  on
```

图 93 kydima_get 系统调用表开关状态查询

7）开启中断描述符度量

```
[secadm@localhost tmp]$ kydima_set idt -s on
[secadm@localhost tmp]$ kydima_get idt
idt:  on
```

图 94 kydima_get 中断描述符开关状态查询

8）事件触发开关

```
[secadm@localhost tmp]$ kydima_set event -s on
[secadm@localhost tmp]$ kydima_get event
status:  on
```

图 95 kydima_get 事件开关状态查询

9）开启 Pcr 扩展功能

```
[root@server227 ~]# kydima_set pcr -s on -r 14 -t tpm2
[root@server227 ~]# kydima_get pcr
pcr:  register: 14
pcr:  tpm: tpm2
```

图 96 kydima_get pcr 扩展策略查询