

安全加固

1.概述

1.1 产品简介

安全加固是一款面向操作系统的全方位安全检测与增强工具，旨在全面识别并修复系统潜在的安全隐患。该工具可对系统进行全面扫描，涵盖安全配置、内核参数、网络设置、系统命令、审计策略、文件权限、账户管理、密码策略、资源分配等多个维度，帮助用户及时发现系统中的安全薄弱环节。

除了提供基于麒麟操作系统自主研发的麒麟安全，安全三级基线外，系统还支持用户自定义基线策略，灵活适配不同业务场景下的安全需求。通过一键加固功能，用户可快速完成系统安全配置优化，提升整体防护能力。

1.2 产品亮点

- 多维安全扫描：覆盖系统服务、内核参数、网络配置、系统命令、审计日志、系统设置等十余个关键领域；
- 风险账户与权限管理：识别高危账户、弱口令、权限配置不当等问题；
- 文件与磁盘安全检查：检测敏感文件权限、磁盘使用情况等安全隐患；
- 密码强度与账户锁定策略：评估密码复杂度、登录失败锁定机制等安全措施；
- 自定义基线支持：可根据行业规范或企业内部标准定制个性化检测项；
- 一键加固：自动修复已知问题，提升系统安全性与合规性；
- 持续维护建议：提供系统安全状态评估与后续加固建议，助力构建长期安全体系。

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，系统中才有安全加固的功能，如图1所示。



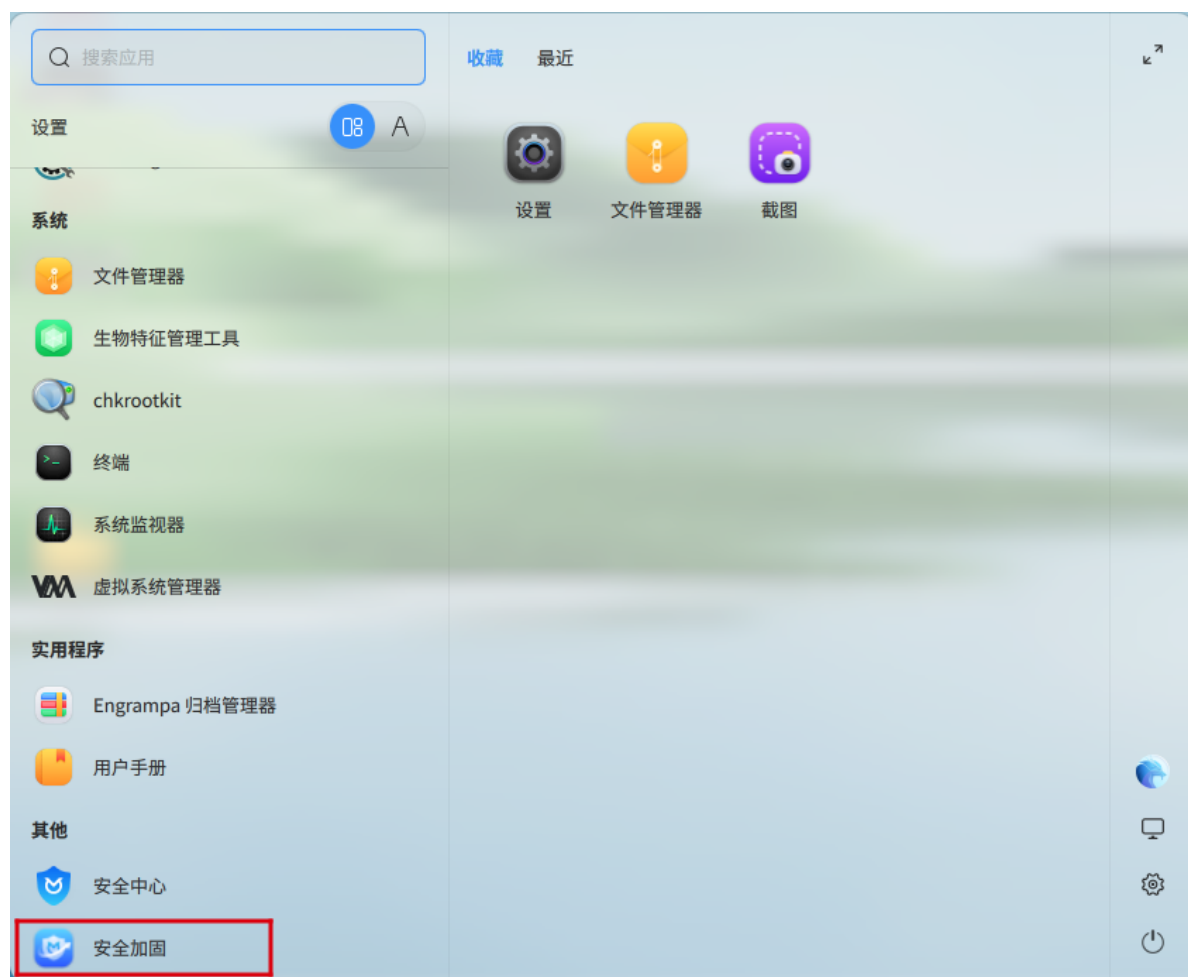
若用户在系统安装时未选择麒麟安全增强工具分组，则可以从仓库中安装对应的security-reinforce软件包，系统中才有安全加固的功能。

系统安装时已选择麒麟安全增强工具分组，界面操作详情见后续章节。

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“安全加固”，打开安全加固软件界面，如图2所示。



3.2 获取帮助

安全加固软件界面中点击菜单图标，点击“帮助”按钮，弹出“用户手册”弹窗，显示安全加固的帮助手册相关信息，如图3所示。



3.3 模式支持

安全加固软件界面显示模式随系统主题变化，开始菜单—>设置—>个性化—>主题进行模式的切换。如图4至5所示。





4.功能介绍

安全加固首页（未进行过安全扫描）展示扫描、模板管理、基线详情、加固还原、安全报告等功能。用户可以选择默认的麒麟安全、安全三级模板，点击“XXX扫描”对系统进行扫描、加固提高系统安全性，如图6所示。



4.1 模板管理

4.1.1 添加模板

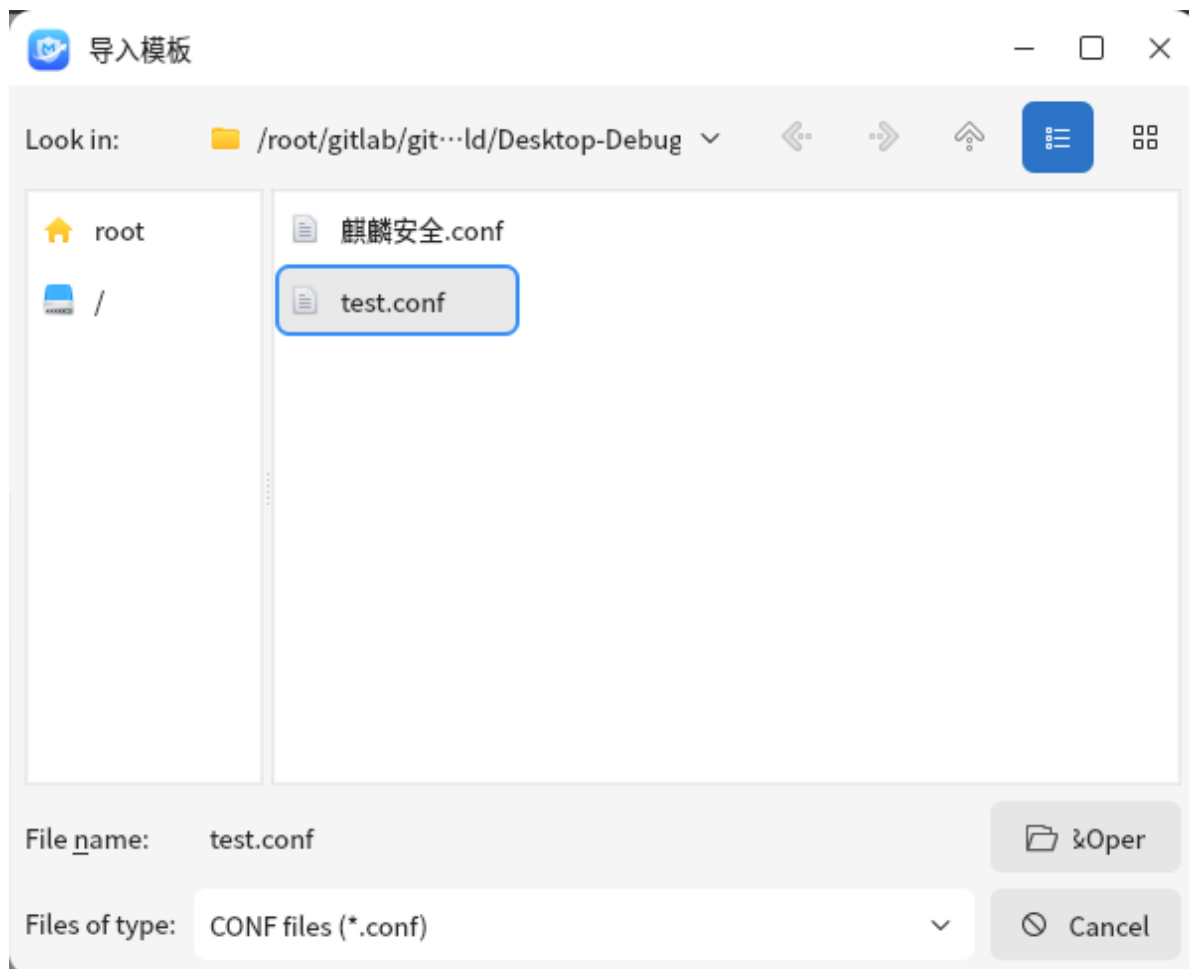
用户也可以自定义模板进行扫描，点击首页“麒麟安全扫描”右边的下拉框，点击界面上的“+添加模板”，如图7所示。



用户也可以点击“模板管理”，点击界面上的“新建模板”添加模板,如图8所示。



用户可以点击“模板管理”，点击界面上的“导入模板”添加模板,如图9所示。



添加一个新的模板，如图10所示。根据业务选择合适的加固项点击保存。



4.1.2 自定义模板

用户可以点击“模板管理”，点击模板右边的“...”，如图11所示。编辑、导出、删除模板（默认的麒麟安全、三级安全模板不可编辑、不可删除），如图12所示。



4.2 扫描、加固

选择模板后点击“麒麟安全扫描”，可以查看到相关项的扫描信息，如图13所示。扫描完成，如图14所示。扫描完成后可以点击“一键加固”对问题进行修复，如图15所示。完成加固如图16所示。





安全加固首页（已进行过安全扫描）展示上次扫描XX天前，加固完成项数，待手动加固项数等，如图17所示。

问题全知道，加固保安全

上次扫描0天前，加固完成19个，待手动加固7个

麒麟安全扫描



☐ 扫描完成自动加固

[模板管理](#)[基线详情](#)[加固还原](#)[安全报告](#)

选择模板后勾选自动加固按钮，点击“开始扫描”，可以查看到相关项的扫描信息，如图18所示。扫描完成后“自动加固”对问题进行修复，如图19所示。完成加固如图20所示。



正在扫描中...

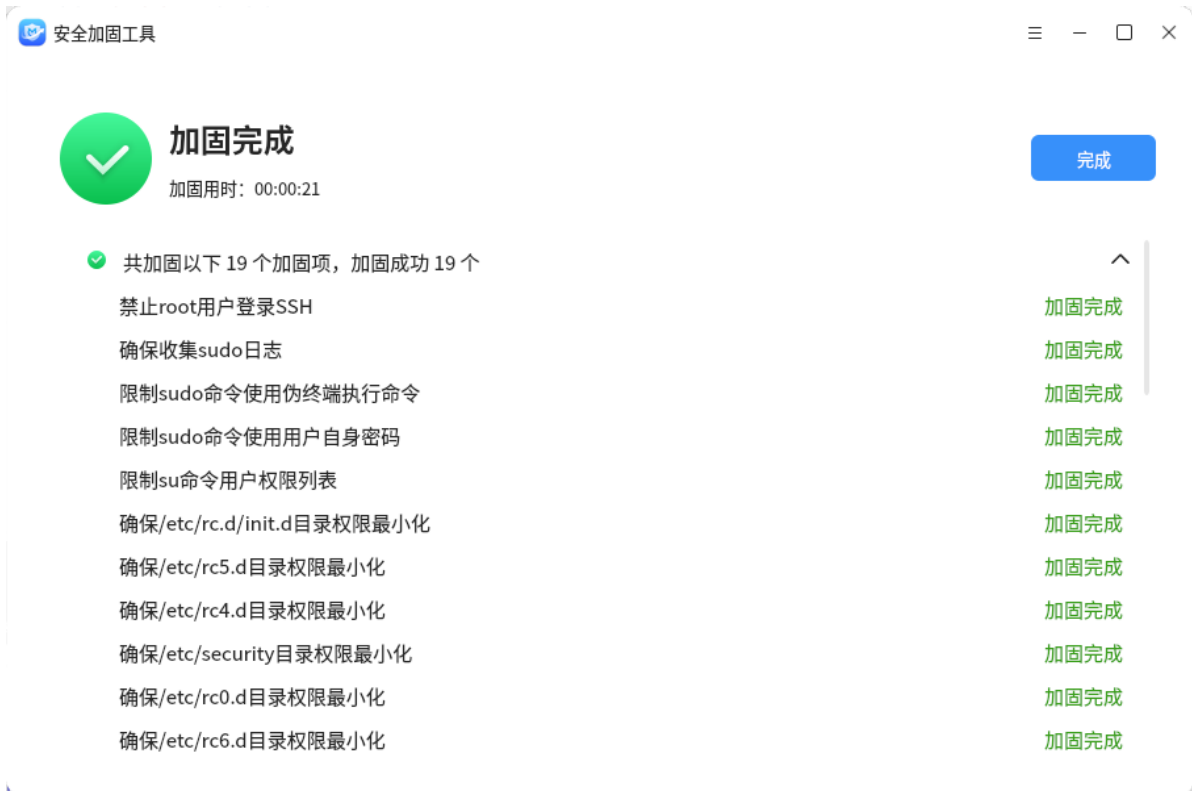
正在扫描限制sudo命令使用用户自身密码

已用时: 00:00:21

暂停

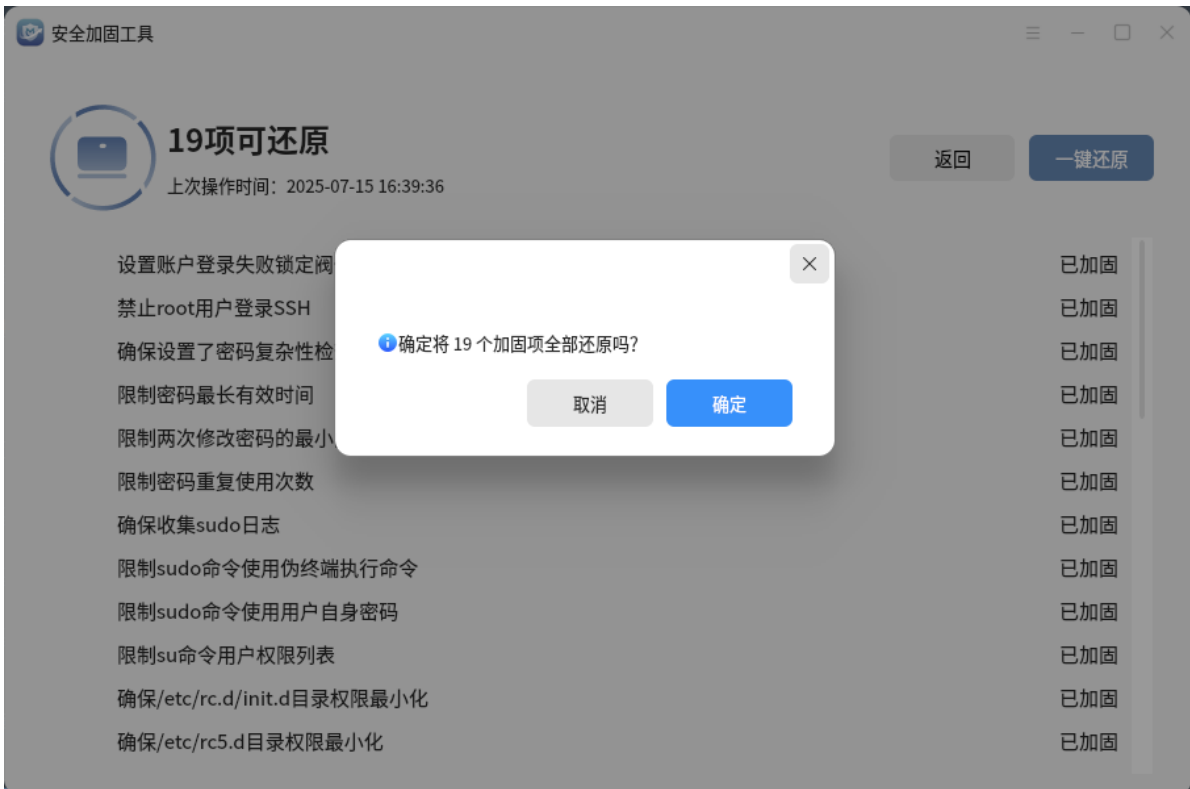
停止

| | | |
|--------------------------|-----------------------------|------|
| ✓ 安全服务 | 用于禁用不必要的系统服务并配置关键服务参数的安全设置。 | ▼ |
| 🔒 密码强度 | 用于评估密码强度与复杂度的安全检查项。 | ▲ |
| 设置密码复杂度 | | 等待扫描 |
| 确保设置了密码复杂性检查策略 | | 等待扫描 |
| 限制密码最长有效时间 | | 等待扫描 |
| 限制密码最小长度 | | 等待扫描 |
| 限制两次修改密码的最小间隔时间 | | 等待扫描 |
| 限制密码重复使用次数 | | 等待扫描 |
| 📁 文件权限 | 为保障系统安全需合理配置的文件与目录权限。 | ▲ |
| 应当删除无属主的文件 | | 等待扫描 |
| 应当限制... (text truncated) | | 等待扫描 |



4.3 加固还原

加固过后点击“加固还原”，显示还原界面，如图21所示。点击“一键还原”，弹出是否还原弹窗，点击“确定”如图22所示。将加固项恢复到初始状态，如图23，图24所示。





4.4 基线详情

点击“基线详情”可以查看当前选择的模板里所有项的详细信息，如图25所示。

基线详情

Search

| 序号 | 检查项 | 检测内容 | 详情描述 | 操作 |
|----|------|------------------------|--|----------------------|
| 1 | 安全服务 | 禁用不必要的chargen-dgram... | chargen-dgram是chargen(Character Generator Prot... | 查看详情 |
| 2 | 安全服务 | 禁用不必要的daytime-strea... | daytime-stream服务是daytime协议的一种实现方式... | 查看详情 |
| 3 | 安全服务 | 禁用不必要的echo-stream服务 | echo-stream服务是echo协议的一种实现方式，基于T... | 查看详情 |
| 4 | 安全服务 | 禁用不必要的tcpmux-server... | tcpmux-server服务是基于TCP协议的tcpmux (TCP M... | 查看详情 |
| 5 | 安全服务 | 禁用不必要的chargen-strea... | chargen-stream是chargen(Character Generator Prot... | 查看详情 |
| 6 | 安全服务 | 禁用不必要的discard-dgram... | discard-dgram服务是discard协议的一种实现方式，... | 查看详情 |
| 7 | 安全服务 | 禁用不必要的eklogin服务 | eklogin是Kerberos加密的远程登录 (rlogin) 服务，... | 查看详情 |
| 8 | 安全服务 | 禁用不必要的krb5-telnet服务 | krb5-telnet服务是一种基于Kerberos 5认证的Telnet服... | 查看详情 |
| 9 | 安全服务 | 禁用不必要的tftp服务 | TFTP(Trivial File Transfer Protocol)是一种基于UDP协... | 查看详情 |
| 10 | 安全服务 | 禁用不必要的cvs服务 | CVS (Concurrent Versions System, 并发版本系统) ... | 查看详情 |

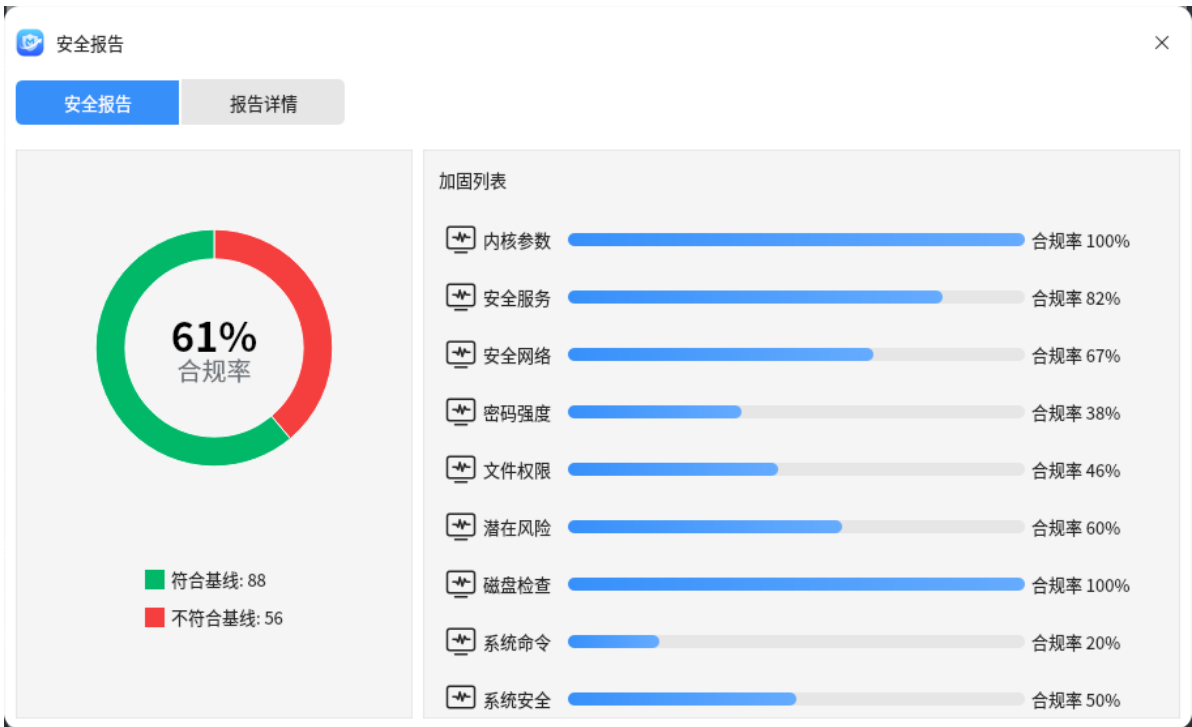
总共 65 行记录

4.5 安全报告

第一次点击“安全报告”会显示报告生成中，如图26所示。



报告生成完后，点击“安全报告”，左侧饼状图报告反映当前系统的安全情况，右侧反映各类大项的合规情况，如图27所示。

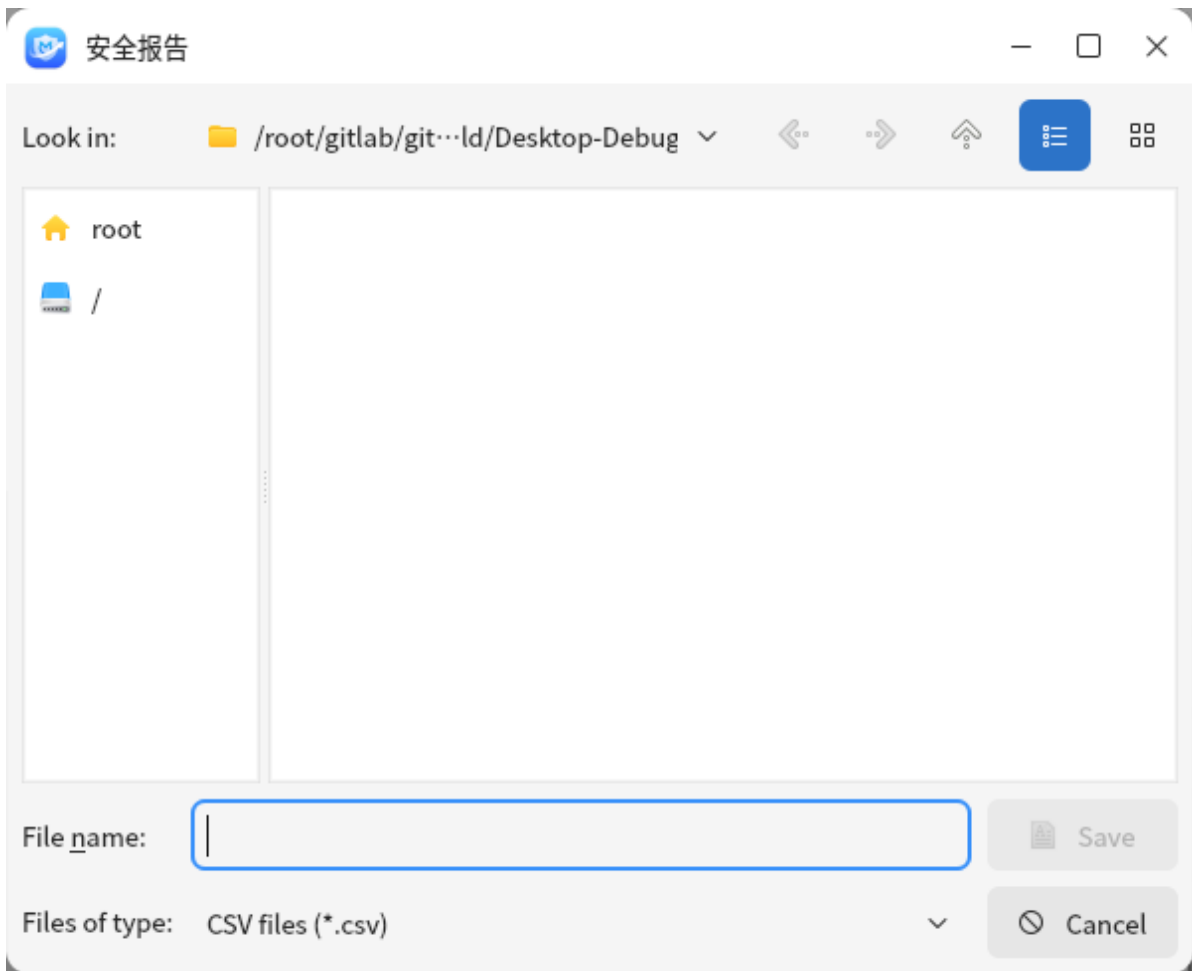


点击“报告详情”可以查看加固项的具体情况，如图28所示。

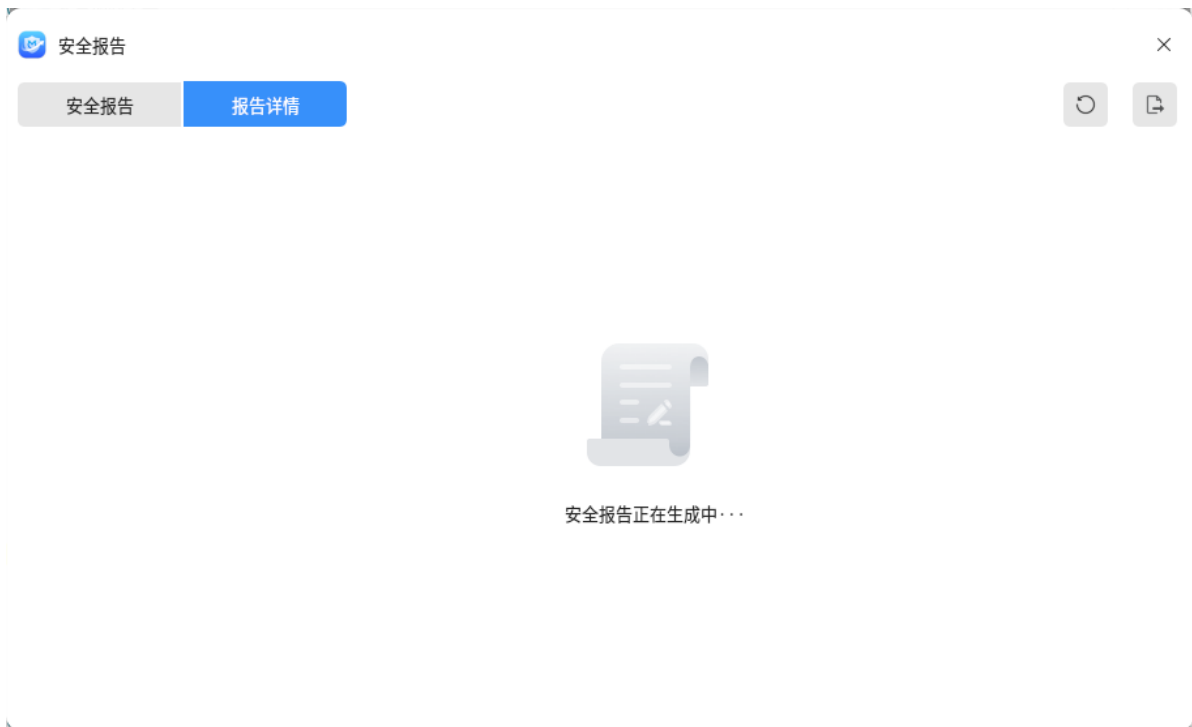
| 安全报告 | | | |
|------|-------|------------------------|------|
| 安全报告 | | 报告详情 | |
| 序号 | 安全加固项 | 详情描述 | 状态 |
| 1 | 安全服务 | 禁用不必要的chargen-dgram服务 | 符合基线 |
| 2 | 安全服务 | 禁用不必要的daytime-stream服务 | 符合基线 |
| 3 | 安全服务 | 禁用不必要的echo-stream服务 | 符合基线 |
| 4 | 安全服务 | 禁用不必要的tcpmux-server服务 | 符合基线 |
| 5 | 安全服务 | 禁用不必要的chargen-stream服务 | 符合基线 |
| 6 | 安全服务 | 禁用不必要的discard-dgram服务 | 符合基线 |
| 7 | 安全服务 | 禁用不必要的eklogin服务 | 符合基线 |
| 8 | 安全服务 | 禁用不必要的krb5-telnet服务 | 符合基线 |
| 9 | 安全服务 | 禁用不必要的tftp服务 | 符合基线 |

总共 33 行记录 | 报告生成时间：2025-07-16 09:39:49

点击报告详情右侧“导出”按钮可以将报告导出到指定路径，如图29所示。



经过加固和还原后也可以点击报告详情右侧“刷新”按钮重新生成报告，生成时不可退出，退出会终止生成，如图30所示。



4.6 操作日志

安全加固软件界面中点击菜单图标，点击“操作日志”按钮，弹出“操作日志”界面，显示安全加固的帮助手册相关信息，如图31所示。

操作记录

Q Search

×

| 序号 | 操作项 | 操作详情 | 操作时间 ▾ |
|----|------|-------------------------|---------------------|
| 1 | 开始扫描 | 麒麟安全;strat scan;65 | 2025-07-15 16:25:02 |
| 2 | 一键加固 | 麒麟安全;strat reinforce;65 | 2025-07-15 16:29:21 |
| 3 | 加固还原 | 麒麟安全;strat restore;65 | 2025-07-15 16:35:10 |
| 4 | 开始扫描 | 麒麟安全;strat scan;65 | 2025-07-15 16:38:07 |
| 5 | 一键加固 | 麒麟安全;strat reinforce;65 | 2025-07-15 16:39:36 |
| 6 | 加固还原 | 麒麟安全;strat restore;65 | 2025-07-15 16:49:32 |

总共 6 行记录

附录：常见问题及处理方法(FAQ)

1.扫描、加固、还原后出现的错误码是什么意思？

这里列出常见错误码及对应的错误信息、错误原因及处理方法，如表所示。

| 错误码 | 错误信息 | 错误原因 | 处理方法 |
|------|--------------------|--------------------------|---|
| 1000 | 文件不存在 | 系统配置文件可能被人为删除 | 根据界面上提示的文件路径，排查系统是否存在对应配置文件，如果不存在，可能系统遭受人为破坏，需要手动恢复配置文件 |
| 1201 | 配置key增加错误 | 向配置文件写入某个配置项时发生错误 | 通常配置文件被手动删除，导致改问题，需要手动恢复配置文件后，再进行操作 |
| 1202 | 配置key删除错误 | 在配置文件中删除某个配置项时发生错误 | 通常配置文件被手动删除，导致改问题，需要手动恢复配置文件后，再进行操作 |
| 1203 | 配置key更新错误 | 在配置文件中更新某个配置项时发生错误 | 通常配置文件被手动删除，导致改问题，需要手动恢复配置文件后，再进行操作 |
| 1204 | 配置key扫描错误 | 读取配置文件配置项时发生错误 | 通常配置文件被手动删除，导致改问题，需要手动恢复配置文件后，再进行操作 |
| 1300 | 还原字符串为空 | 在还原操作时，发现还原点的字符串为空，无法还原 | 这种情况要么加固的时候没有记录还原点，要么手动改了加固数据库的记录，需要联系研发排查 |
| 3000 | service不存在 | 系统中没有安装相关的包 | 手动安装服务相关的包 |
| 3001 | enable service 错误 | 服务配置文件存在错误或服务被安全模块阻止运行 | 需要进一步检查配置文件或查看下审计日志 |
| 3002 | disable service 错误 | 服务配置文件存在错误或服务被安全模块阻止运行 | 需要进一步检查配置文件或查看下审计日志 |
| 3003 | start service 错误 | 服务配置文件存在错误或服务被安全模块阻止运行 | 需要进一步检查配置文件或查看下审计日志 |
| 3004 | restart service 错误 | 服务配置文件存在错误或服务被安全模块阻止运行 | 需要进一步检查配置文件或查看下审计日志 |
| 3005 | stop service 错误 | 服务配置文件存在错误或服务被安全模块阻止运行 | 需要进一步检查配置文件或查看下审计日志 |
| 5000 | 命令执行失败 | 已打开的文件描述符达到上限或命令执行结果存在异常 | 可以尝试手动执行下命令看下是否有问题，或者联系研发排查 |

