



银河麒麟日志查看器

用户手册

麒麟软件有限公司

2022 年 9 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.....	1
3. 使用入门.....	2
3.1. 软件位置.....	2
3.2. 区域介绍.....	2
4. 日志类型.....	3
4.1. 系统日志.....	3
4.2. 启动日志.....	4
4.3. 登录日志.....	5
4.4. 安全日志.....	6
4.4.1. 麒麟安全日志.....	6
4.4.2. 崩溃日志.....	6
4.4.3. 审计日志.....	7
4.4.4. 指令流日志.....	8
5. 操作方法.....	8
5.1. 搜索.....	8
5.2. 筛选.....	9
5.3. 复制.....	10
5.4. 导出.....	11
5.5. 刷新.....	11
5.6. 排序.....	12
6. 命令行.....	14
6.1. 指令流日志显获取测试—logview -g.....	14

6.2. 软件包安装卸载测试.....	14
6.3. 系统日志获取测试—logview -y.....	14
6.4. 审计日志获取测试—logview -u.....	14
6.5. 崩溃日志获取测试—logview -r.....	15
6.6. 麒麟安全日志获取测试—logview -c.....	15
6.7. 日志导出默认路径测试—logview -p.....	15
6.8. 日志内容等级筛选测试—logview -0/1/2.....	15
6.9. 日志内容时间筛选测试—logview -s/e.....	16
6.10. 日志内容关键字筛选测试—logview -k.....	16
6.11. 命令帮助信息测试—logview -h.....	16
6.12. 日志导出自定义路径测试—logview -p /.....	16
6.13. 启动日志获取测试—logview -t.....	17
6.14. 登录日志获取测试—logview -l.....	17

1. 概述

1.1. 产品简介

日志查看器是一款系统日志集中展示工具，提供日志解析和分类显示功能。

1.2. 产品亮点

(1) 智能化收集展示

实时同步收集展示系统内日志信息，根据日志类型进行归类显示。同时，具有过滤和聚合功能，对重复日志信息进行合并统计显示。

(2) 标准化全景态势

提供系统日志、启动日志、登录日志、应用日志以及安全日志。通过安全视角将事件标准化描述，包含目标事件等级、对象类型、时间、事件详细信息。

(3) 模块化维护扩展

采用模块化、可插拔架构设计，每类日志组件能够以模块化横向扩展，对不同类别日志独立维护，具有灵活易用、可维护特征。

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，系统中才有日志查看器的功能，如图 1 所示。

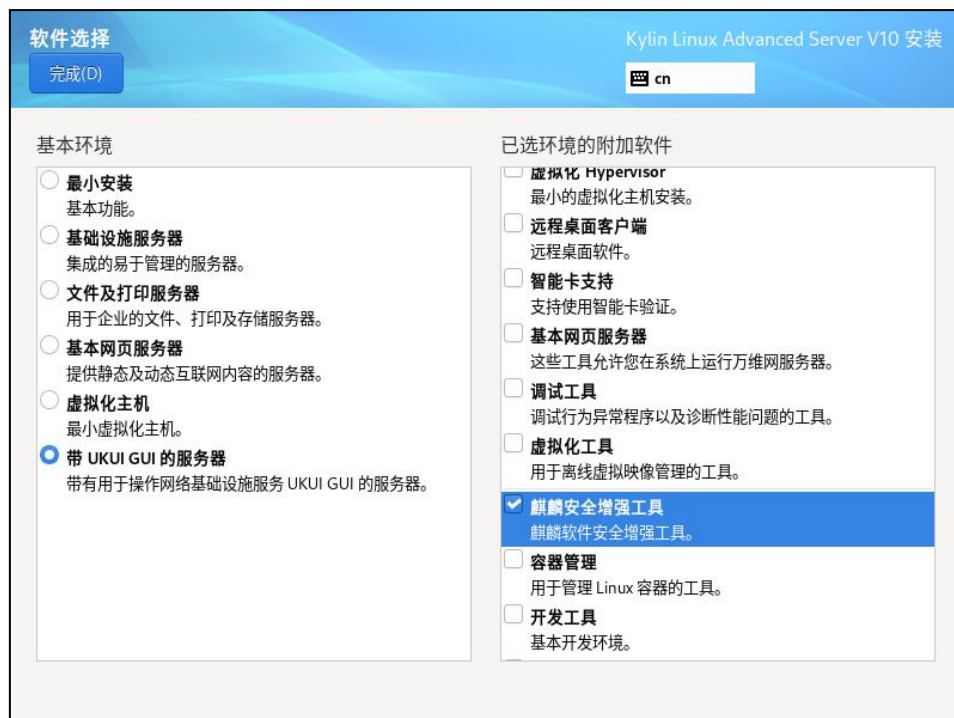


图 1 软件选择-麒麟安全增强工具分组

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 kylin-log-viewer 软件包，系统中才有日志查看器的功能。界面操作详情见第 3~第 5 章节，命令行操作详情见第 6 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“系统工具”菜单，选择并点击“日志查看器”，打开日志查看器软件界面，如图 2 所示。

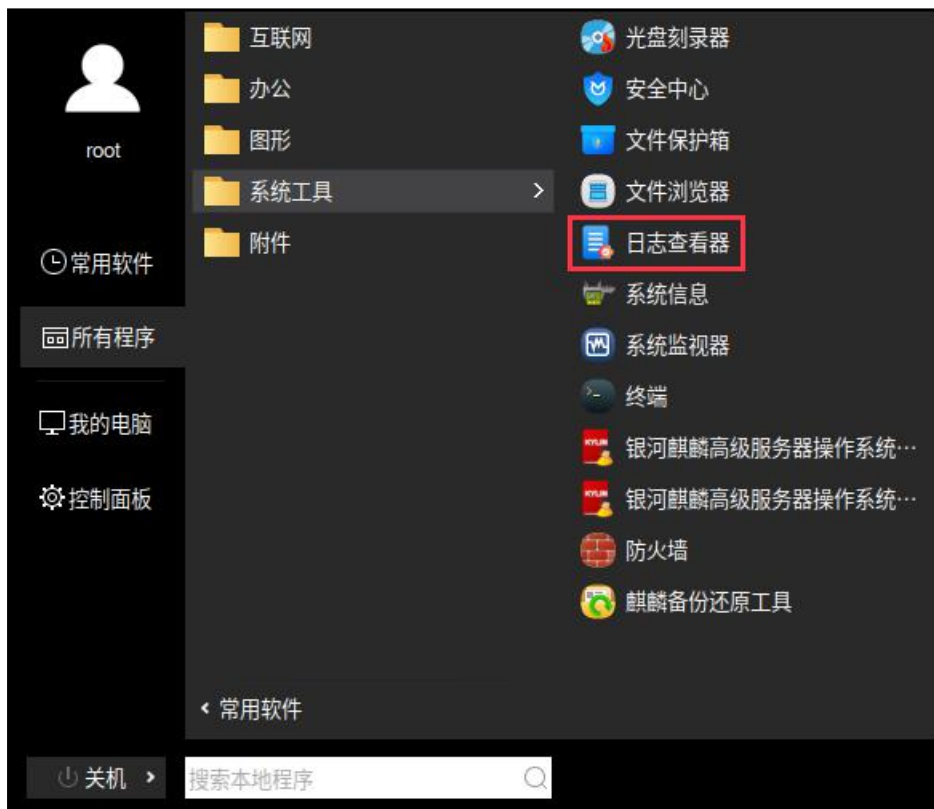


图 2 开始菜单（打开日志查看器）

3.2. 区域介绍

日志查看器界面划分为四个区域：搜索区、内容展示区、写字板区域和左边栏，如图 3 所示。

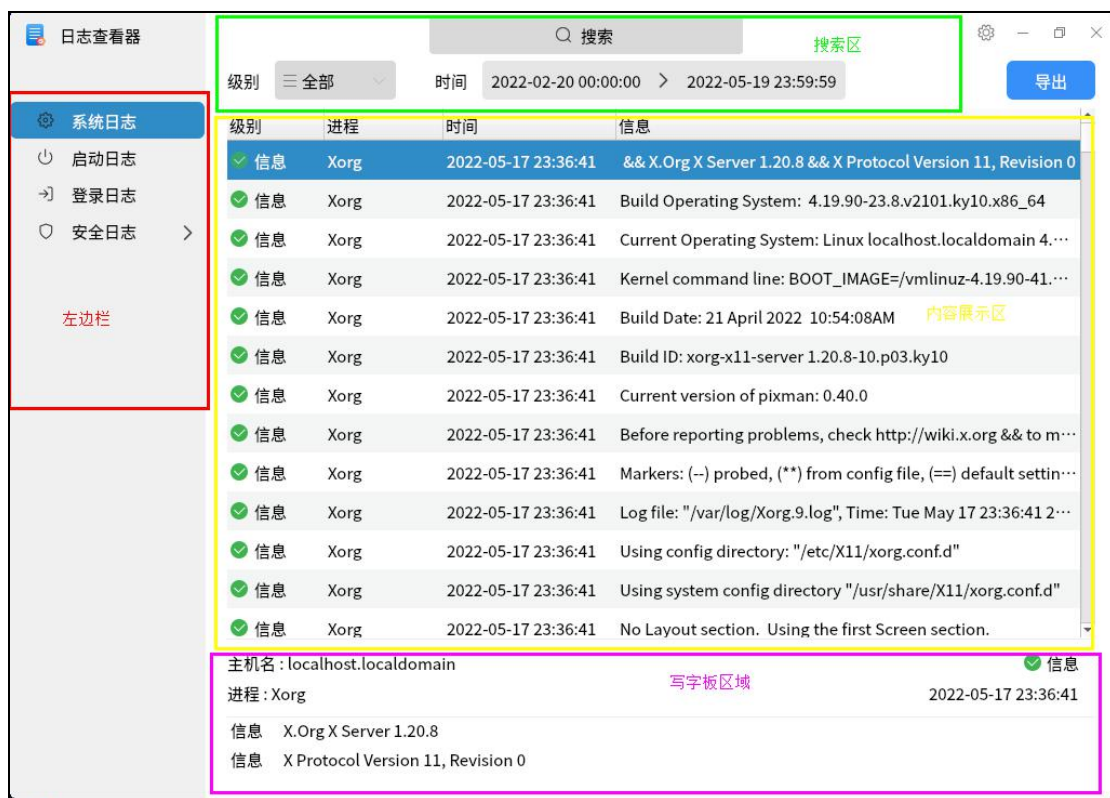


图 3 区域介绍

4. 日志类型

4.1. 系统日志

点击左边栏“系统日志”，内容展示区显示系统日志内容信息，显示字段为级别、进程、时间和信息。选中某条系统日志，详细内容将显示在下方写字板区域，如图 4 所示。

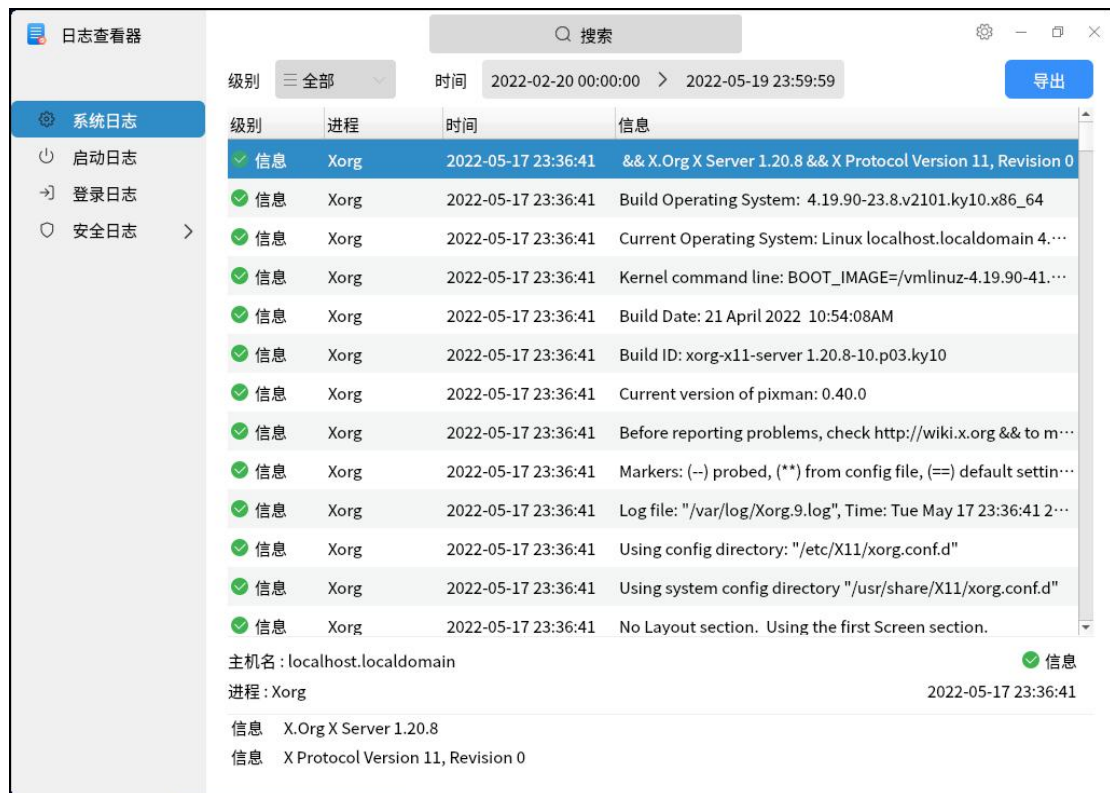


图 4 系统日志

4.2. 启动日志

点击左边栏“启动日志”，内容展示区显示启动日志内容信息，显示字段为级别、类型、时间和信息。选中某条启动日志，详细内容将显示在下方写字板区域，如图 5 所示。

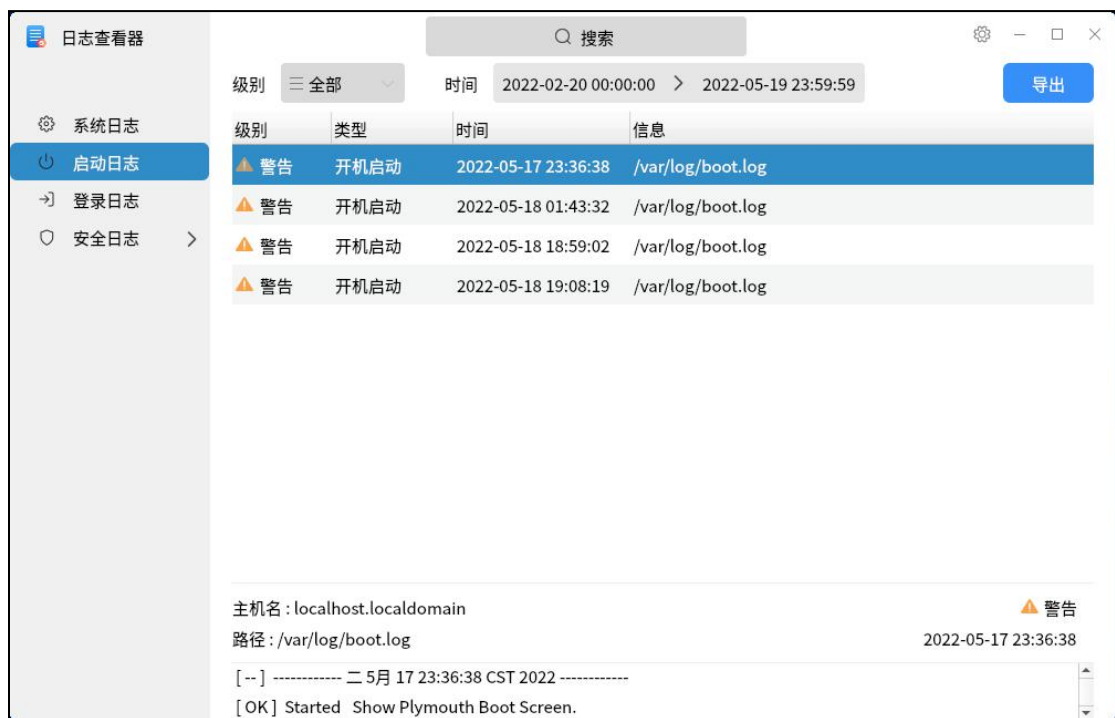


图 5 启动日志

4.3. 登录日志

点击左边栏“登录日志”，内容展示区显示登录日志内容信息，显示字段为级别、用户、时间和信息。选中某条登录日志，详细内容将显示在下方写字板区域，如图 6 所示。



图 6 登录日志

4.4. 安全日志

安全日志包括：麒麟安全日志、崩溃日志、审计日志和指令流日志。

4.4.1. 麒麟安全日志

点击左边栏“麒麟安全”，内容展示区显示麒麟安全日志内容信息，显示字段为级别、进程、时间和信息。选中某条麒麟安全日志，详细内容将显示在下方写字板区域，如图 7 所示。

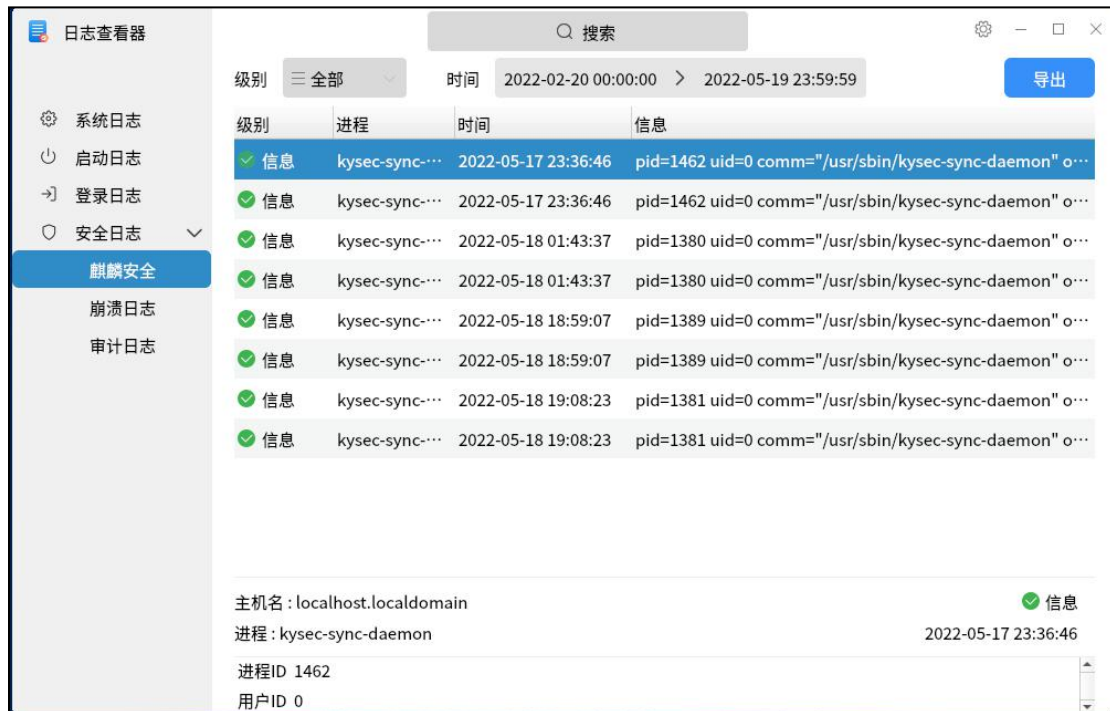


图 7 麒麟安全日志

4.4.2. 崩溃日志

点击左边栏“崩溃日志”，内容展示区显示崩溃日志内容信息，显示字段为级别、类型、时间和信息。选中某条崩溃日志，详细内容将显示在下方写字板区域，如图 8 所示。

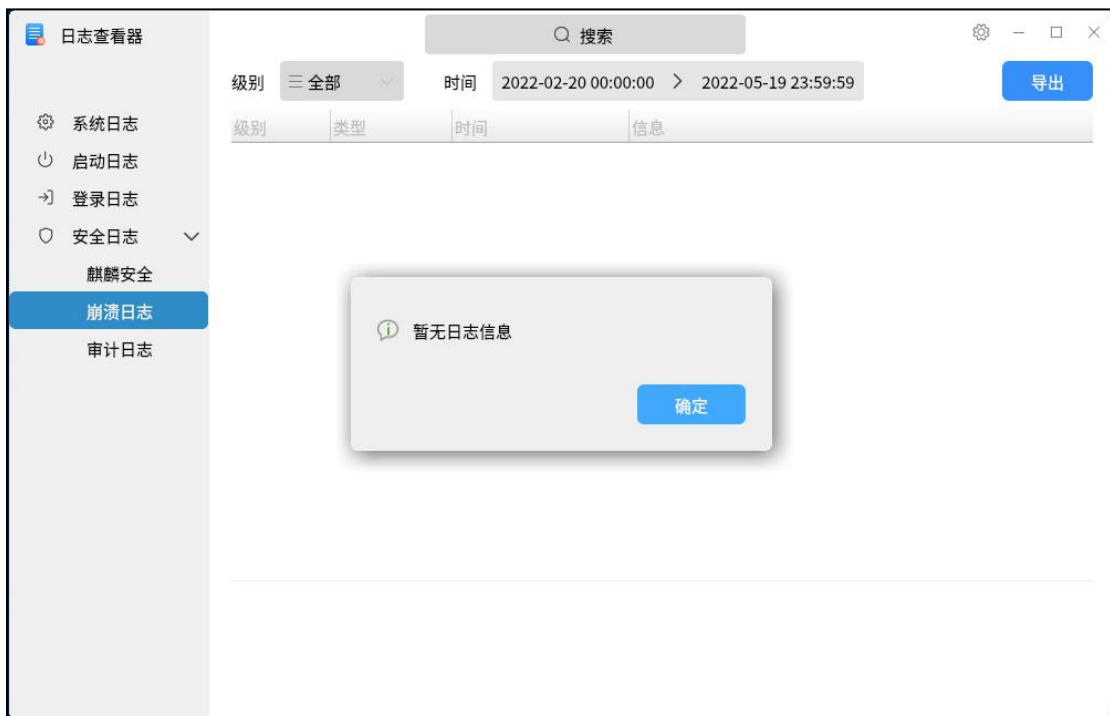


图 8 崩溃日志

4.4.3. 审计日志

点击左边栏“审计日志”，内容展示区显示审计日志内容信息，显示字段为级别、类型、时间和信息。选中某条审计日志，详细内容将显示在下方写字板区域，如图 9 所示。



图 9 审计日志

4.4.4. 指令流日志

点击左边栏“指令流日志”，内容展示区显示指令流日志内容信息，显示字段为级别、事件类型、时间和处理结果。选中某条指令流日志，详细内容将显示在下方写字板区域，如图 10 所示。

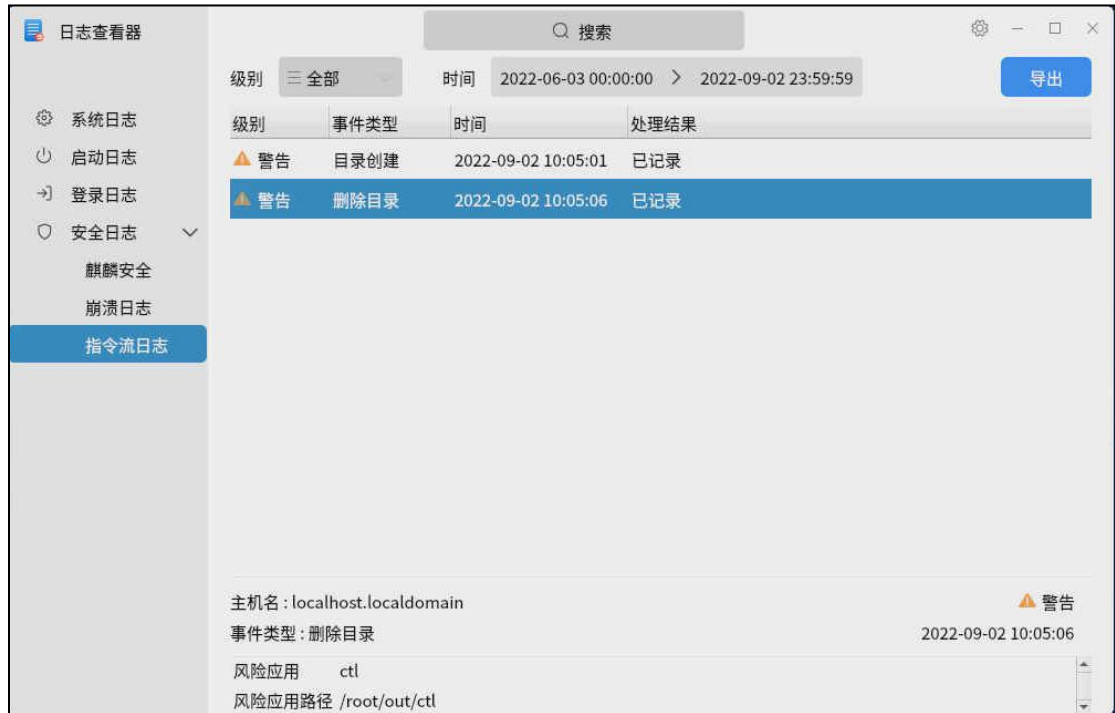


图 10 指令流日志

5. 操作方法

5.1. 搜索

点击搜索区并输入关键字，内容展示区展示搜索内容；删除所有关键字，则清空搜索内容。如图 11 所示。

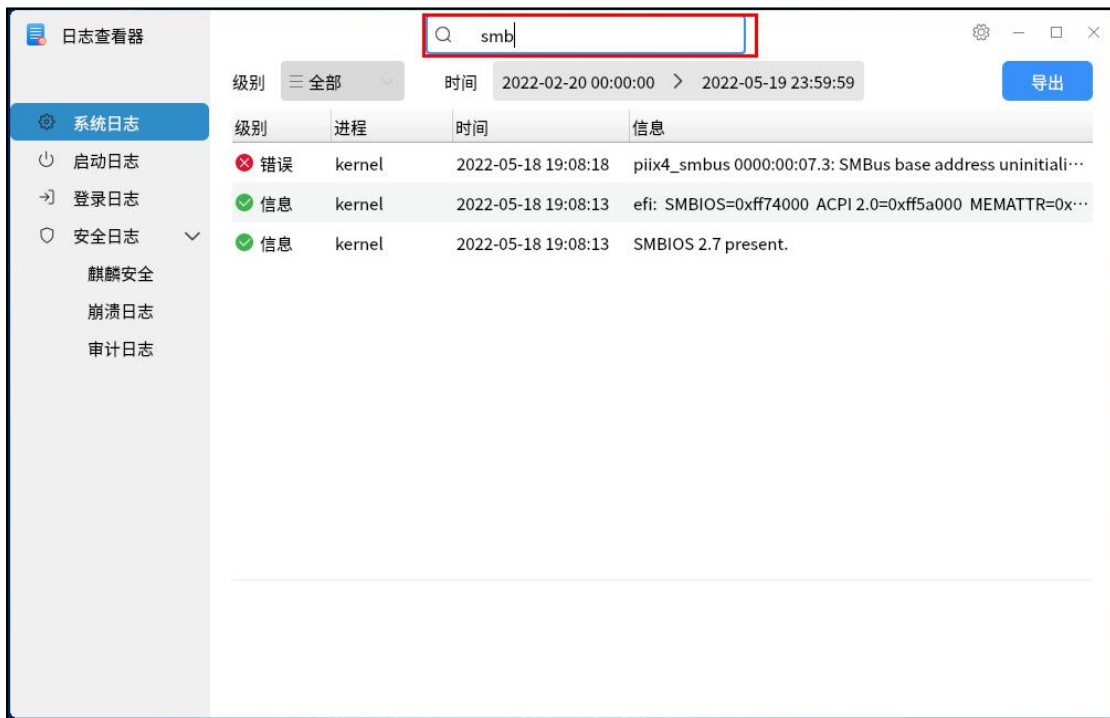


图 11 搜索操作

5.2. 筛选

支持按照时间或日志级别进行日志内容的筛选。

(1) 按时间筛选

选择任意三个月内的时间段进行筛选，或者使用快捷筛选（今天、近三天、近一周、近一个月、近三个月），如图 12 所示。

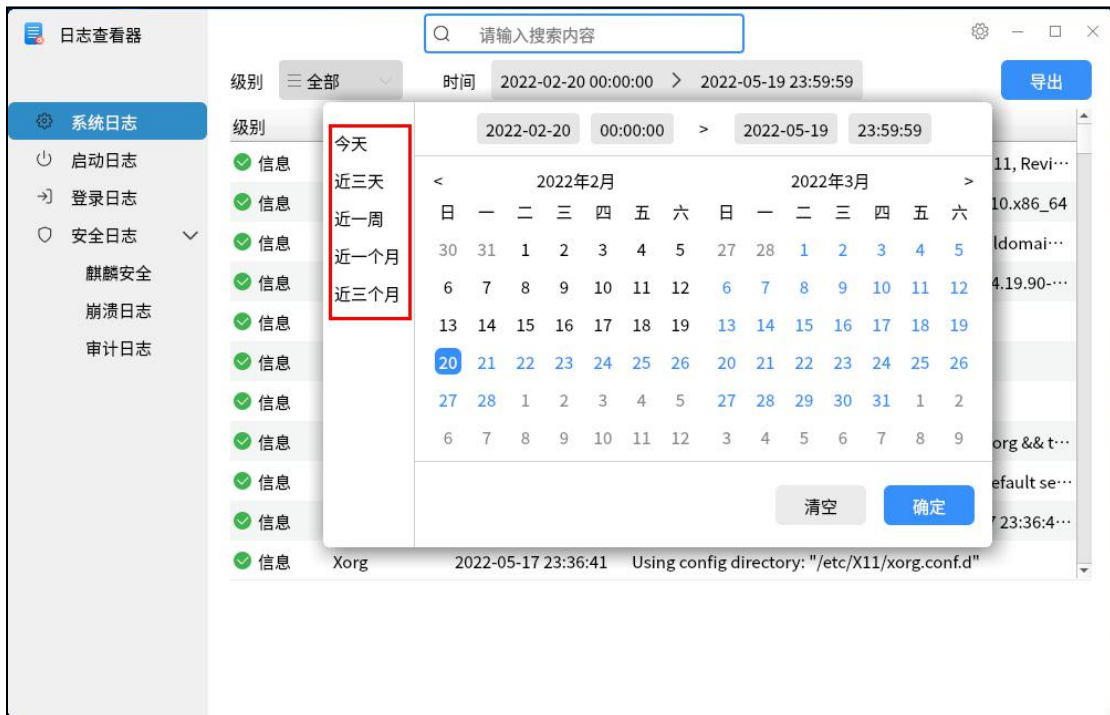


图 12 按时间筛选操作

(2) 按级别筛选

您可以按照日志级别（信息、警告、错误、全部）进行筛选，如图 13 所示。

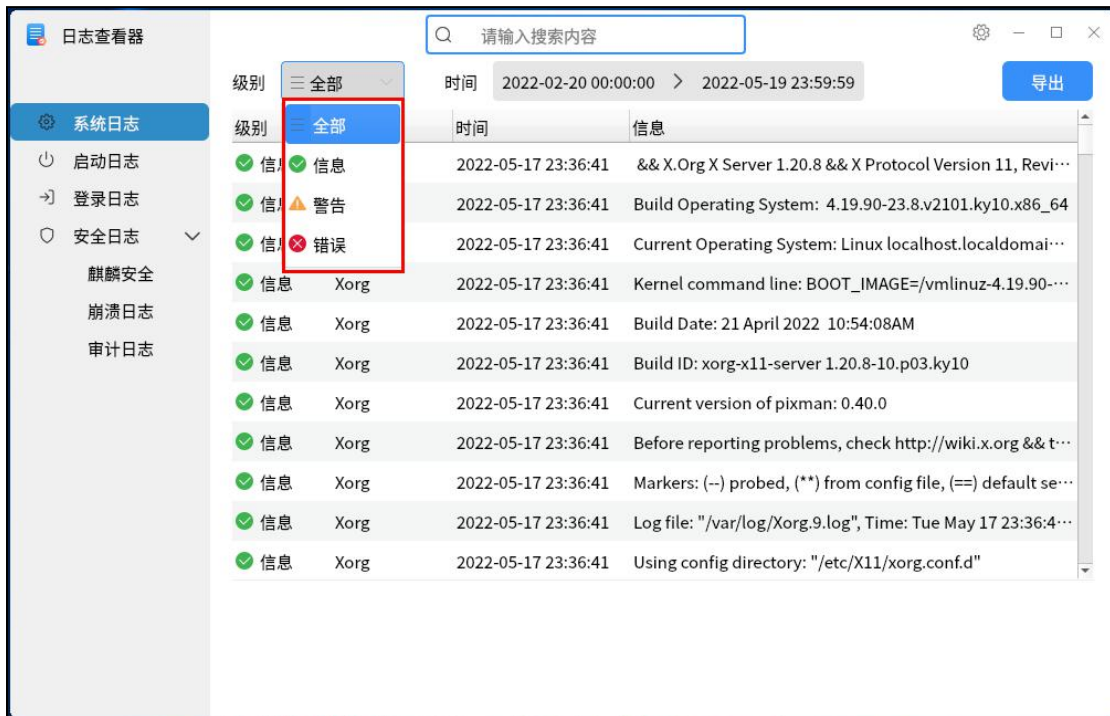


图 13 按级别筛选操作

5.3. 复制

选中表格区域或详情区域中的内容进行复制，如图 14 所示。

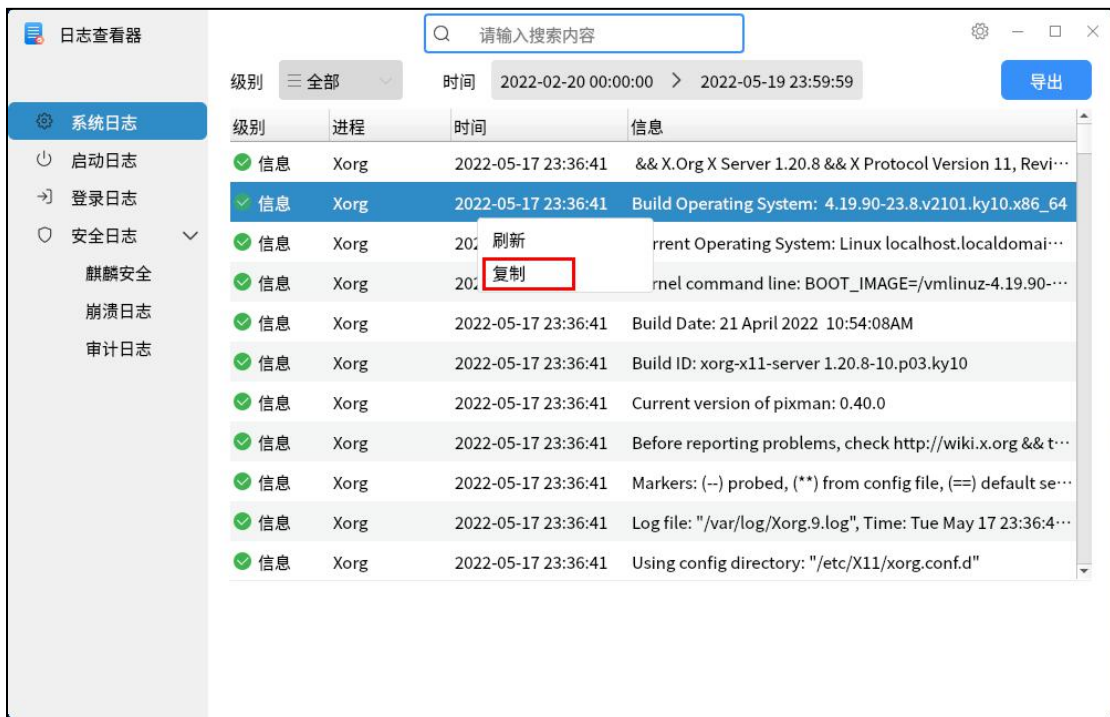


图 14 复制日志内容

5.4. 导出

点击主界面“导出”按钮，对当前日志进行导出，导出的文件格式支持 txt、csv、html 等，如图 15 所示。

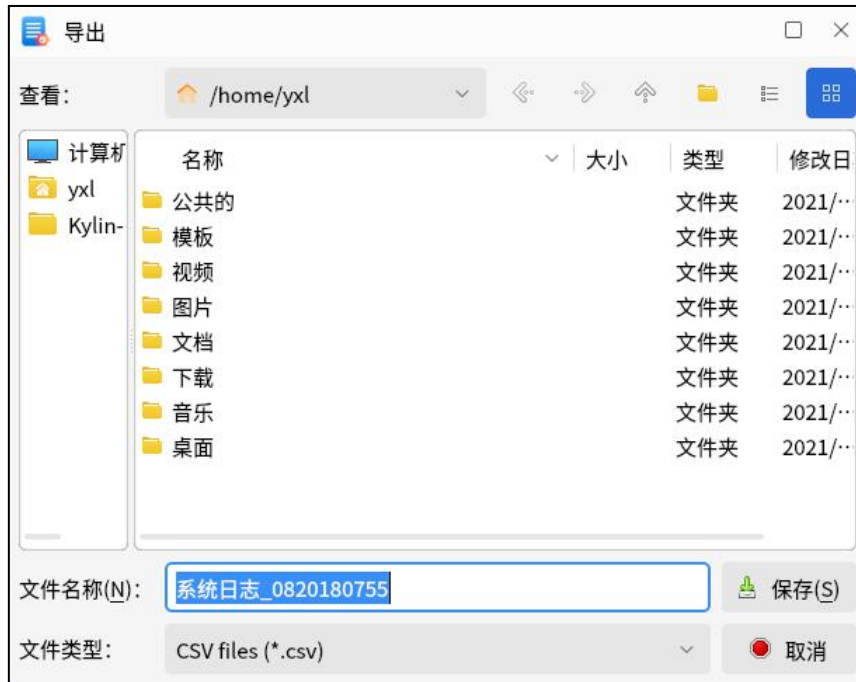


图 15 导出文件

5.5. 刷新

右键点击日志内容展示区域选择“刷新”操作，日志查看器的筛选结果将更新为最新数据，如图 16 所示。

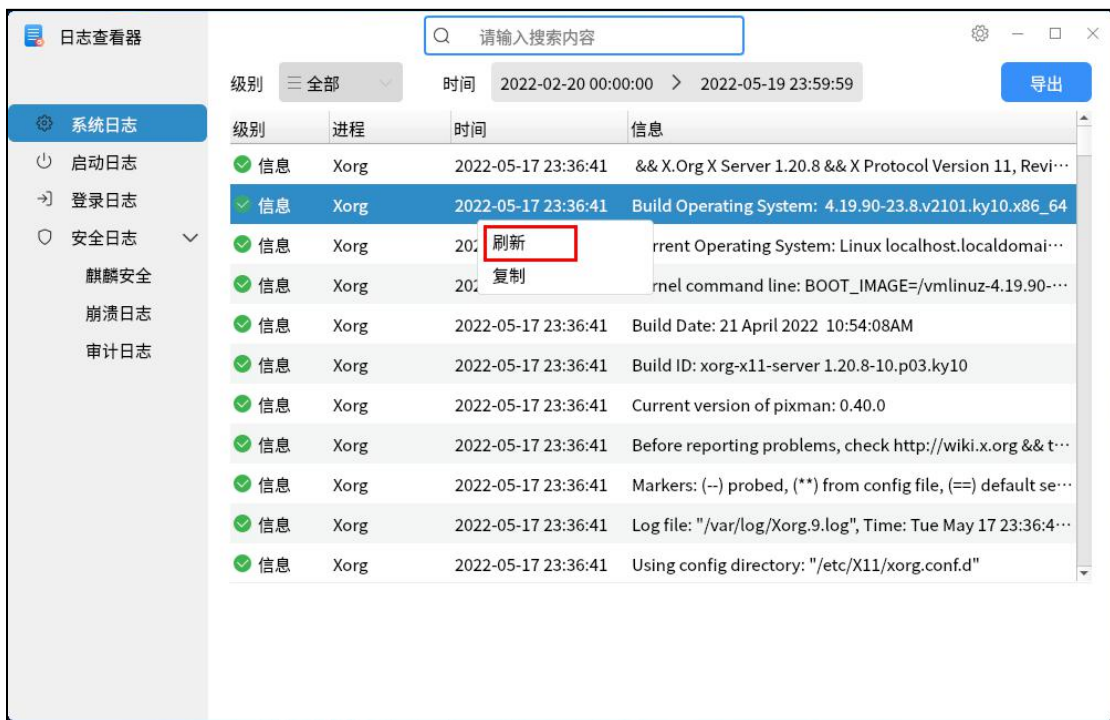


图 16 刷新日志

5.6. 排序

日志查看器中数据全部加载完成，手动点击时间后方的“∨”按钮，可以进行时间倒序排序，如图 17 所示。

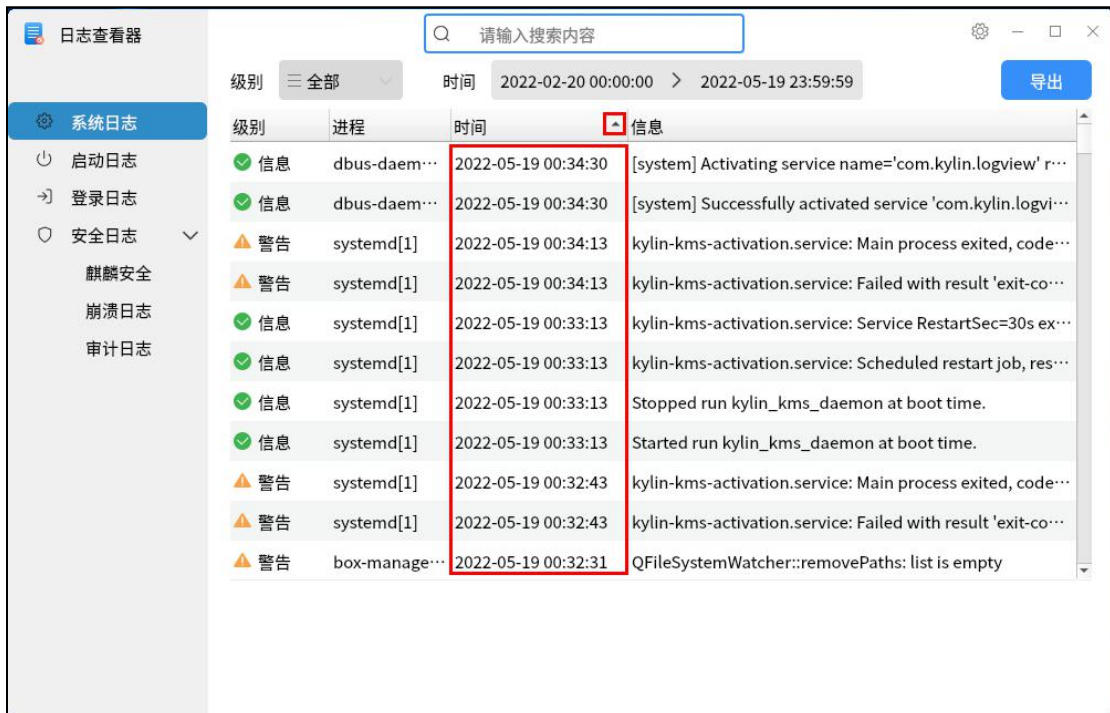


图 17 日志排序（倒序）

日志查看器中数据全部加载完成，手动点击时间后方的“^”按钮，可以进行时间顺序排序，如图 18 所示。

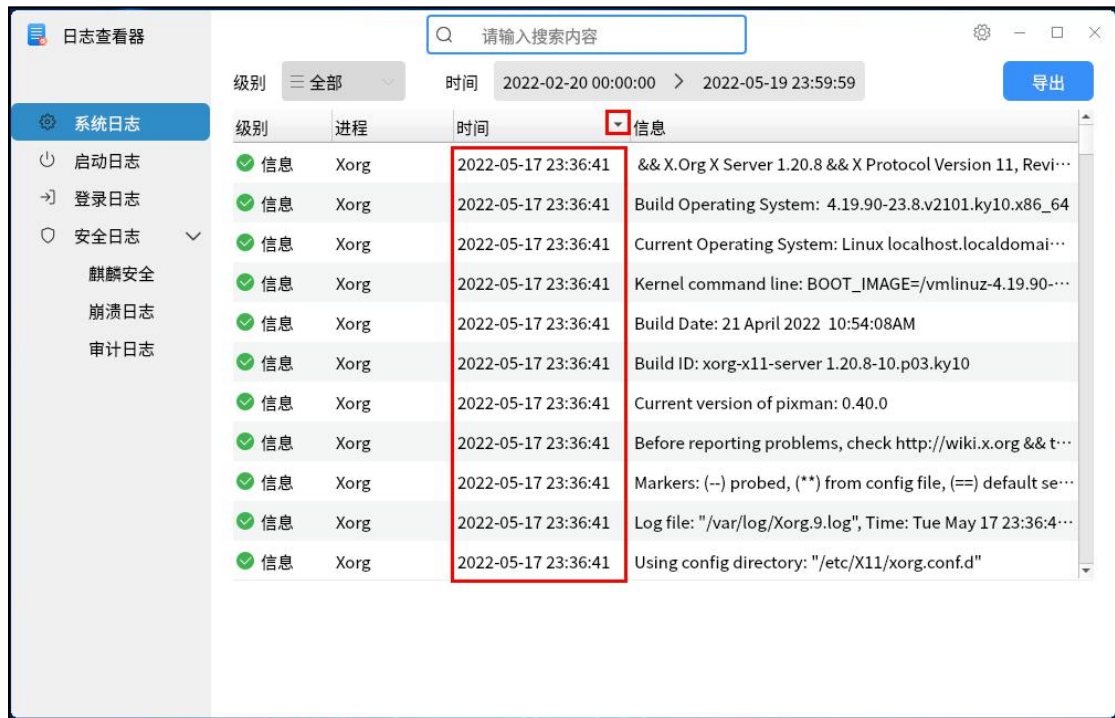


图 18 日志排序（顺序）

6. 命令行

6.1. 指令流日志显获取测试—logview -g

1. 查看指令流日志 `logview -g`
2. 查看指令流日志 `logview --http-log`

6.2. 软件包安装卸载测试

1. 先卸载已安装的包后，重新安装
2. 不卸载已安装的包，执行升级安装
3. 使用命令卸载已安装的包，使用命令查看 `dpkg -l |grep kylin-log-viewer`

6.3. 系统日志获取测试—logview -y

1. 终端查看系统日志 `logview -y`
2. 终端查看系统日志 `logview --system-log`
3. 检查 systemd 服务日志 `logview -y -k systemd`
4. 检查 xorg 服务日志 `logview -y -k xorg`
5. 检查 samba 服务日志 `logview -y -k smbd`
6. 检查 kernel 日志 `logview -y -k kernel`
7. 检查 samba 服务 log.nmbd 日志 `logview -y -k nmbd`
8. 使 systemd, xorg, samba, kernel 进程运行错误或者强制终止
9. 执行 `systemctl | grep running`，选择查看其中一种 XX 服务的日志
`logview -y -k XX`

6.4. 审计日志获取测试—logview -u

1. 查看审计日志 `logview -u`
2. 查看审计日志 `logview --audit-log`
3. 操作系统，使 `var/log/audit.log` 产生审计日志

例如信息 SYSCALL

```
type=SYSCALL msg=audit(1642408329.967:538): arch=c000003e syscall=54
success=yes exit=0 a0=3 a1=0 a2=80 a3=55a7b9674c50 items=0 ppid=2376
pid=17252 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0
fsgid=0 tty=(none) ses=4294967295 comm="ebtables-restore"
exe="/usr/sbin/ebtables-legacy-restore" key=(null) ARCH=x86_64
SYSCALL=setsockopt AUID="unset" UID="root" GID="root" EUID="root"
```

SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"

4. 查看审计日志是否新增内容 `logview -u`

6.5. 崩溃日志获取测试—`logview -r`

1. 查询崩溃日志 `logview -r`
2. 查询崩溃日志 `logview --crash-log`
3. 再次执行 `echo c > proc/sysrq-trigger`，是系统崩溃，确认 crash 更新
查询崩溃日志 `logview -r`

6.6. 麒麟安全日志获取测试—`logview -c`

1. 查看 kysec 日志 `logview -c`
2. 查看 kysec 日志 `logview --kysec-log`
3. 操作系统 kysec 相关，再查看麒麟安全日志 `logview -c`

6.7. 日志导出默认路径测试—`logview -p`

1. 指定日志文件导出至默认/tmp 路径
例：`logview -l -p`（导出登录日志至/tmp）
2. 进入/tmp 路径查看是否存在日志文件
`ls /tmp`
`cat /tmp/Login*`
3. 查看日志文件内容
`cat /tmp/Login*`
4. 对【系统日志】、【登录日志】、【麒麟安全日志】、【崩溃日志】、【审计日志】
重复以上 3 个步骤
分别为：`-ytlcrug`

6.8. 日志内容等级筛选测试—`logview -0/1/2`

1. 筛选出错误等级的日志信息
`logview -0 (--error) -y`
2. 筛选出警告等级的日志信息
`logview -1 (--warn) -y`
3. 筛选出信息等级的日志信息
`logview -2 (--info) -y`
4. 对【系统日志】、【启动日志】、【登录日志】、【麒麟安全日志】、【崩溃日志】、
【审计日志】重复以上 3 个步骤

分别为：-ytlcrug

6.9. 日志内容时间筛选测试—logview -s/e

1. 筛选出【系统日志】中从此参数开始到当前时间结束的所有信息

```
logview -y -s xxxx-xx-xx\ xx:xx:xx
```

2. 筛选出【系统日志】中截止到此参数时间之前的所有信息

```
logview -y -e xxxx-xx-xx\ xx:xx:xx
```

3. 对【系统日志】、【启动日志】、【登录日志】、【麒麟安全日志】、【崩溃日志】、【审计日志】重复以上 2 个步骤

分别为：-ytlcrug

6.10. 日志内容关键字筛选测试—logview -k

1. 筛选一种日志类型中第二列和第四列包含此关键字的信息

```
./logview -日志类型 -k "log"
```

2. 对【系统日志】、【启动日志】、【登录日志】、【麒麟安全日志】、【崩溃日志】、【审计日志】重复以上步骤

分别为：-ytlcrug

6.11. 命令帮助信息测试—logview -h

1. 查看日志查看器的终端帮助文档

```
logview -h
```

2. 终端执行 logview

3. 终端执行 logview --help

4. 终端执行 logview - (help 说明中不存在的参数)，例：logview -8

6.12. 日志导出自定义路径测试—logview -p /

1. 终端执行导出指定日志到某个路径下

例：logview -y -p /home/ （导出系统文件至 home 目录）

2. 路径查看目标路径是否存在日志文件

例：ls -l /home/ | grep .txt

3. 查看导出的日志文件内容

4. 对【系统日志】、【启动日志】、【登录日志】、【麒麟安全日志】、【崩溃日志】、【审计日志】[指令流日志]重复以上 3 个步骤

分别为：-ytlcrug

6.13. 启动日志获取测试—logview -t

1. 查看启动日志内容

```
logview -t
```

2. 查看启动日志内容

```
logview --startup-log
```

3. 在 var/log/boot.log 文件中修改某个启动项为 failed

```
Starting LSB: Bring up/down networking...
```

```
[FAILED] Failed to start LSB: Bring up/down networking.
```

```
See 'systemctl status network.service' for details.
```

4. 查看启动日志内容

```
logview -t
```

5. 重启系统，在开机过程中强制中断，再次启动系统。

/var/log/boot.log 确认日志中生成启动失败的日志

6. 查看启动日志内容

```
logview -t
```

6.14. 登录日志获取测试—logview -l

1. 查看登录日志信息

```
logview -l
```

2. 查看登录日志信息

```
logview --login-log
```

3. 使用一台设备远程连接该测试机，输入正确用户名及密码

4. 终端执行 logview -l，查看是否生成新的登录日志

5. 使用一台设备远程连接该测试机，输入错误数据

6. 终端执行 logview -l，查看是否生成新的登录日志

7. 在测试机上新建用户，并互相切换，成功登录一次，登录失败一次后，在查看登录日志：logview -l

8. 在测试机上多次输出错误的密码登录用户，使得提示该用户被锁定，在查看登录日志：logview -l