KYLINSOFT
麒麟软件

麒麟智能运维助手

用户手册 V1.3-4

麒麟软件有限公司

2024 年 7 月

商标声明

KYLINSOFT 麒麟软件和其他麒麟商标均为麒麟软件有限公司的商标。本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受麒麟软件有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，麒麟软件有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容有可能变更，麒麟软件有限公司保留在没有任何通知或提示的情况下对内容进行修改的权利。除非另有约定，本文档仅作为使用指导，并不确保手册内容完全没有错误。本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目录

1.软件介绍

本软件产品全称为“麒麟智能运维助手”，以下简称“运维助手”，运维助手是部署在服务器上的一个信息收集程序。

1.1. 总体架构

运维助手主要分为系统体检、日志收集和系统监控三个主要模块，系统体检主要检查系统服务状态、配置以及存在的漏洞和缺陷；日志收集主要在故障发生前、中、后收集较全面的日志信息；系统监控主要是监控进程、文件以及系统资源存在的问题。其架构图如“图 1-1 运维助手架构图”所示：

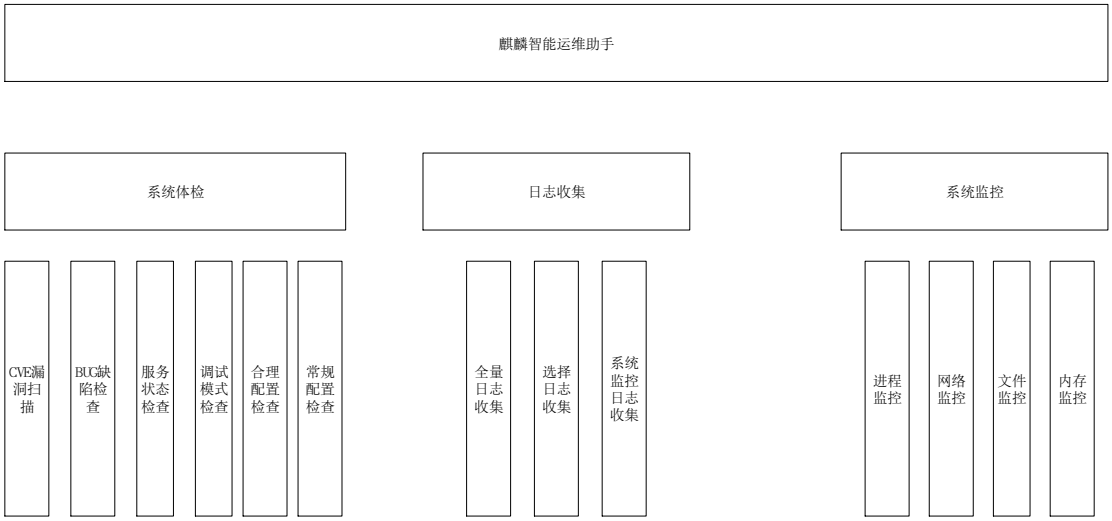

图 1–1 运维助手架构图

1.2. 功能概述

运维助手软件在功能上包括三部分：系统体检，日志收集，系统监控；

1.2.1.系统体检

系统体检功能是能方便快捷有效的检测出当前系统存在的已知安全漏洞、缺陷，并提供相应的官方说明链接以及推荐的修复方式，提升系统的安全性、可靠性和稳定

性。能够准确识别系统运行中存在的异常服务、不合理配置以及服务器场景核心配置的状态，并提供相应的建议和操作说明，及早发现问题。主要包括以下功能。

漏洞检测：扫描系统和软件信息，匹配后端数据库并输出扫描检测结果到系统体检报告，内容包含漏洞描述、CVE ID、漏洞级别、软件版本或内核版本信息、修复状态、修复方案链接。

缺陷检测：扫描系统和软件信息，匹配后端数据库并输出扫描检测结果到系统体检报告，内容包含缺陷描述、缺陷 ID、缺陷级别、软件版本或内核版本信息、修复状态、缺陷勘误链接。

服务状态检查：扫描系统所有服务的运行状态，对异常服务进行标识并发出告警日志。

调试模式配置检查：扫描和故障追踪和调试相关的服务和配置，并根据服务器场景给出其说明和建议，包括 kdump 服务、串口配置、sysstat 服务、sysctl 内核异常处理参数等。

合理配置检查：扫描系统内核参数和配置，根据业务压力和硬件配置检测出可优化项，并给出说明和建议，包括内存水位值配置、内核相关参数、日志轮转策略、IO 调度策略、文件描述符限制和栈空间限制等。

1.2.2.日志收集

日志收集功能提供自定义和全量日志收集的方式，避免出现故障时日志收集不全的情况，主要包括两部分功能：

1、全量日志收集：一键收集系统所有重要组件的日志信息并自动打包保存，包括如下信息：

a、激活信息：当前系统激活状态信息，若系统激活失败则进行收集激活失败的关键日志；

注：激活信息获取执行激活命令并获取其返回值以及收集系统激活必备的文件配置。

b、message 日志：系统产生的 message 全量日志；

c、系统基础信息：系统版本信息；

注：系统版本信息即 nkvers 读取版本信息。

d、core 文件信息：系统产生的应用程序的 core 文件以及内核 vmcore 文件；

注：core 文件收集会判断 core 文件生产目录是否已配置，若配置则收集指定目录下 core 文件，若未配置则收集默认目录下的 core 文件。

e、内存信息：系统内存相关的配置信息、proc 目录内存状态、内存碎片化程度以及内存回收规整次数，系统内存分布；

注：内存信息的收集主要是读取 proc 下系统内存信息以及篇 proc/[pid]下进程内存信息以及内存分布。

f、进程信息：系统负载占用 Top3 的进程信息，收集的信息包括：strace、ltrace、perf、pstack、ptree、pidstat 以及 proc/[pid]目录下进程的相关信息；

注：strace 日志主要追踪系统调用的执行情况，ltrace 追踪系统库函数执行情况，perf 查看进程的函数占用分布，pstack 获取进程调用栈、ptree 获取进程关系依赖、pidstat 获取进程的资源占用情况、proc/[pid]目录下信息获取进程的调度、内存、io、网络等实时信息以及相关配置。

g、sosreport 信息：系统 sysstat 服务采集的信息；

注：sosreport 日志的收集为系统自带 sosreport 工具的日志收集。

h、自定义信息：系统用户自定义的日志信息；

注：自定义信息指的是客户环境中业务软件产生的特有日志。

2、选择日志收集：根据需要修改收集配置项，有选择的收集日志。

1.2.3.系统监控

系统监控主要用于监控常态化数据，捕获指标变化前后更多的日志以及关键信息。面向特殊场景，持续追踪操作时间前后的关键信息。主要提供以下功能：

1、进程监控：对指定进程 PID 进行监控，当进程负载占用异常时触发进程信息收集抓取关键日志。

2、文件（目录）操作监控：对指定的文件、目录或多级目录进行 VFS 层的操作监控，能够捕获监控时间内操作文件或目录的进程名、操作时间、进程 ID 等关键信息。

3、网络数据流向监控：对指定的网络参数对数据包进行跟踪，捕获处理每个数据包的 CPU 信息、到达各个协议层的时间、以及应用层处理的时间等关键信息。

4、内存监控：对系统内存整体的使用情况进行监控，跟踪内存回收机制的状态，内存泄漏的状态以及内存碎片化的状态，并将关键信息进行保存。

2.部署环境

2.1.安装环境

目前已适配支持 x86_64、aarch64 和 loongarch64 平台， 如:

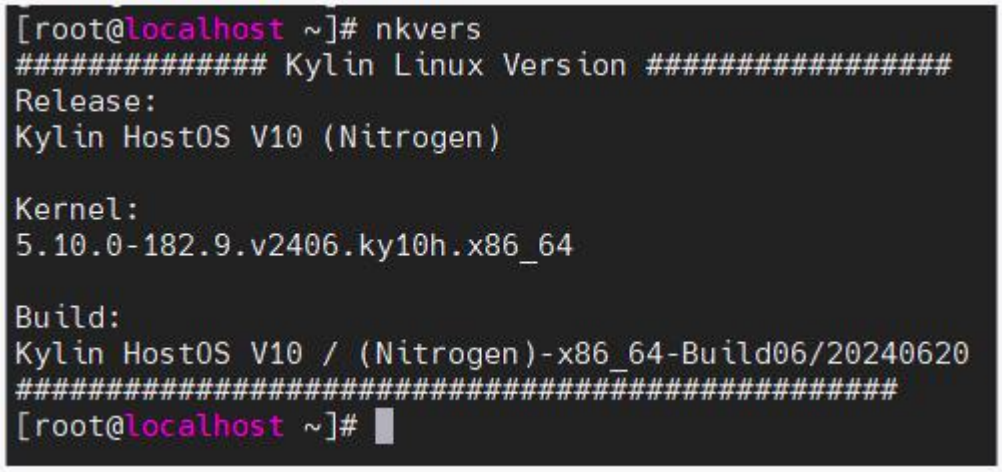

图 2-1 运维助手软件云底座版本安装环境

3.安装软件

本章节介绍运维助手软件的安装方式，运维助手软件以 RPM 包的形式提供，其安装方式可以通过“在线安装”或“离线安装”的形式。“在线安装”指的是安装环境中有 yum 源可用，可以为远程仓库，或者本地搭建的私有 yum 仓库源；当没有可用的 yum 源仓库时，可以通过离线的方式安装，需要提前下载好依赖的软件包。

3.1.在线安装

```
yum install  kylin-sysassist
```

3.2.离线安装

如果没有可以访问的软件源，则额外需要安装 4 个依赖包:

```
iotop-0.6-24.ky10.noarch.rpm
ltrace-0.7.91-31.ky10.x86_64.rpm
perf-4.19.90-89.1.v2401.ky10.x86_64.rpm
ltrace-help-0.7.91-31.ky10.x86_64.rpm
```

安装指令如下：

```
# rpm –ivh ./kylin–sysassist–1.2–9.ky10.x86_64.rpm ./kylin–sysassist–db–1.2–9.ky10.x86_64.rpm ./iotop–0.6–24.ky10.noarch.rpm ./ltrace–0.7.91–31.ky10.x86_64.rpm ./perf–4.19.90–89.1.v2401.ky10.x86_64.rpm ./ltrace–help–0.7.91–31.ky10.x86_64.rpm
```

安装效果如图“3-2 运维助手软件安装过程”所示:

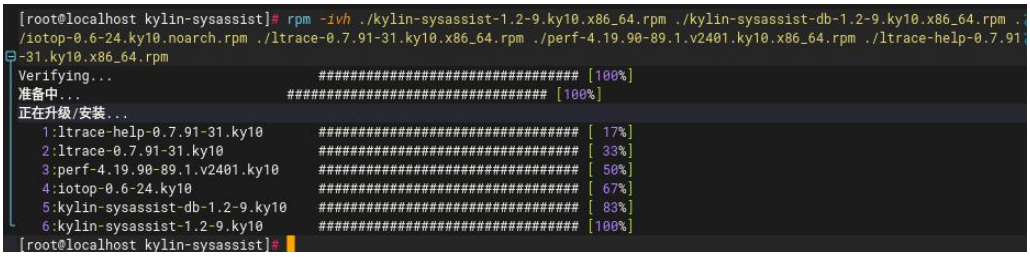

图 3–2 运维助手软件安装过程

4.开始使用

运维助手软件中文名称为“麒麟智能运维助手”，英文名称为“kylin sysassist”。

运维助手可通过命令行界面运行，打开“终端”工具，输入命令“kylin-sysassist-cli --help”，如图“4-1 运维助手帮助”所示。

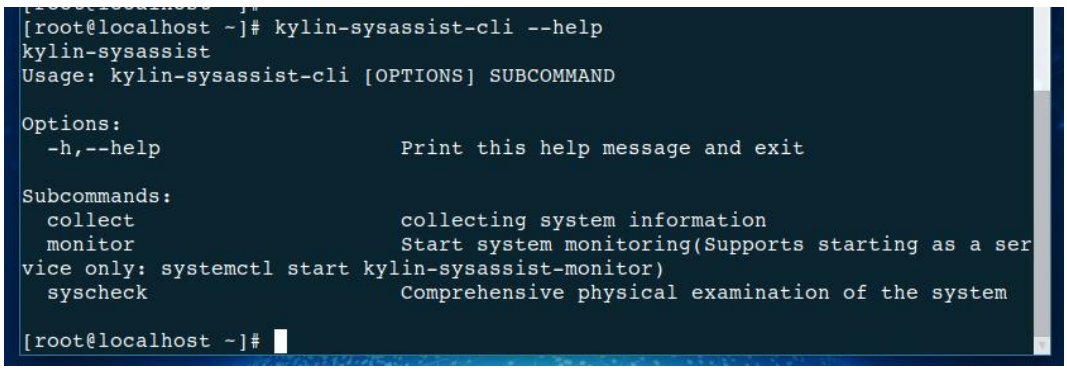

图 4–1 运维助手软件帮助

运维助手运行必须执行子命令，目前支持 collect、syscheck 子命令可以手动方式操作，monitor 选项可通过 kylin-sysassist-monitor 服务进行操作。

5.系统体检

5.1.运行体检

在麒麟 V10 服务器操作系统上，在“终端”中使用“kylin-sysassist-cli”命令并添加“syscheck”子选项开始运行系统体检，命令执行格式如下：

```
[root@localhost ~]# kylin-sysassist-cli syscheck
```

执行结果如图 5-1 所示：

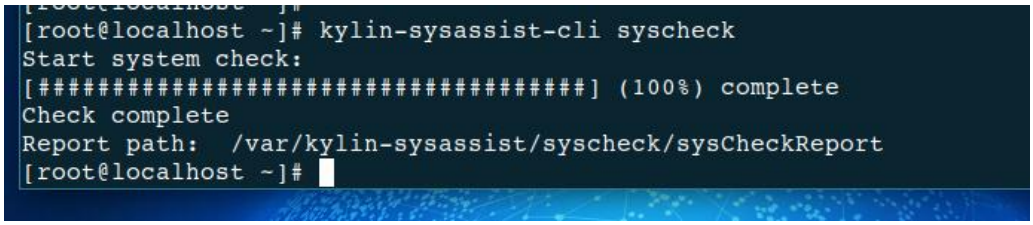

图 5-1 体检功能运行

程序先打印开始体检，之后显示各项体检的进度，体检项目包括：CVE 检查、BUG 检查、kdump 检查、串口检查、sar 检查、服务检查、内核参数检查、内存水位值检查、swap 检查、ulimit 检查、irqbalance 服务检查、系统资源检查。体检完成后输出体检报告输出位置，报告路径为：/var/kylin-sysassist/syscheck/sysCheckReport。

5.2.体检报告

打开体检报告，可以看到各项体检后的结果，对于系统已知的 cve 漏洞和 bug 漏洞，程序会在“/var/kylin-sysassist/syscheck”目录生成对应 cvereport 和 bugreport 详细报告文件。

6.日志收集

6.1.配置文件

日志收集程序默认情况下为全量日志收集，收集所有项。程序也支持指定项收集，可通过配置文件“/etc/kylin-sysassist/kylin-sysassist.ini”进行管理，打开配置文件，其中日志收集相关配置如图 6-1 所示:

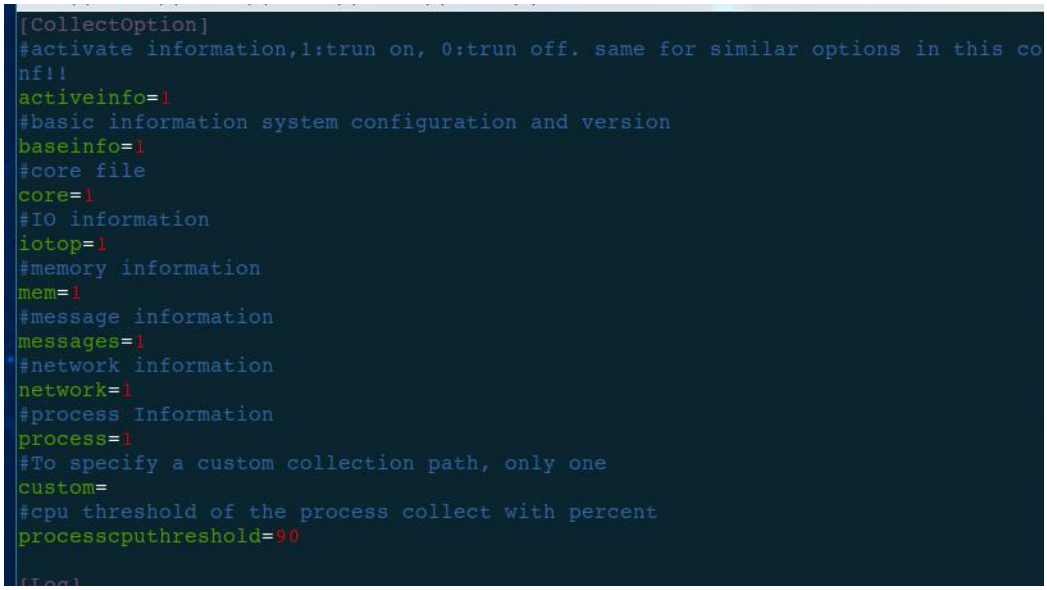

图 6–1 日志收集配置

日志收集相关的配置均在“[CollectOpetion]”类目下，各项配置含义如下：

activeinfo： 激活日志收集开关，1：开启，0：关闭。

baseinfo： 系统基础信息收集开关，1：开启，0：关闭。

core： 系统用户态 coredump 文件收集开关，1：开启，0：关闭。

iotop： 系统 io 信息收开关，1：开启，0：关闭。

mem： 系统内存信息收集开关，1：开启，0：关闭。

messages： 系统全量的 messages 日志收集开关，1：开启，0：关闭。

network： 系统网络信息收集开关，1：开启，0：关闭。

process： 系统进程信息收集开关，1：开启，0：关闭。

custom： 指定一个路径，可以是目录或文件，程序会收集该路径下的信息。不填写代表关闭。

processcputhreshold： 指定一个 0-100 的数字。默认为 90，表示收集进程 cpu 使用率超过 90%的前三个进程的信息。

6.2.运行收集

在麒麟 V10 服务器操作系统上，在“终端”中使用“kylin-sysassist-cli”命令并添加“collect”子选项开始运行日志收集，命令执行格式如下：

```
[root@localhost ~]# kylin-sysassist-cli collect
```

执行结果如图 6-2 所示：

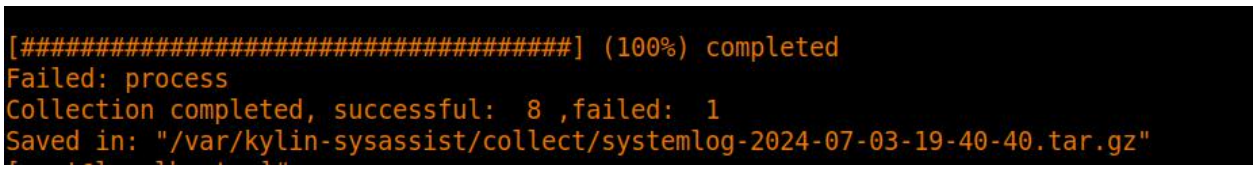

图 6-2 日志收集运行

程序首先打印开始收集，之后显示各项收集的进度，收集的项目包括：系统基础信息、激活信息、core 文件、IO 信息、内存信息、messages 日志、网络信息、进程信息、用户指定项收集和 sosreport 收集。

用户指定项收集可以通过配置文件设置路径或者通过命令行指定，如果同时指定则只收集命令行所指定的路径下日志。命令行添加指定项收集的格式如下：

```
[root@localhost ~]# kylin-sysassist-cli collect -f [path]
```

收集结束后打印收集成功和失败项的数量，如果有失败的项还会打印失败的项目。

6.3.输出文件

日志收集后会将收集的所有日志打包成“tar.gz”格式的压缩文件，存放在“/var/kylin-sysassist/collect”目录下。文件名格式为“systemlog-yyyy-MM-dd-hh-mm-ss.tar.gz”，其中年月日时分秒代表开始日志收集的时间。

7.系统监控

7.1.监控配置

系统监控配置包括文件（目录）操作监控和进程监控配置，配置如图 7-1 所示:

```
[Monitor]
#monitor file (0:off 1:on). Filemonitor only works on x86_64 or aarch64
FileLoad=0
#the file name or folder to monitor, separated them by ',' if there are multiple values
FileName=
#Whether to monitor directories recursively
FileRecursive=1
#Maximum depth of monitoring
FileDepth=2
#the process being monitored
TaskPid=
#cpu or mem fluctuation of the monitored process with percent
MonitorCpuMemFluctuation=10
#cpu or mem absolute value of the monitorer process with percent
MonitorCpuMemAbsValue=80
#monitoring frequency(minute)
MonitorFrequency=1
#maximum collection time(minute)
MonitorMaxCollectTime=10
#how many hours are logs store
LogStoreTime=72
#net monitor(0:off, 1:on), Netmonitor only works on x86_64 or aarch64
NetmonitorLoad=
#net monitor host, ex:192.168.1.1
NetmonitorHost=
#net monitor protocol, Netmonitor only support icmp,udp,tcp
NetmonitorProtocol=
#net monitor port, if monitor protocol is tcp or udp, can set this param
NetmonitorPort=
```

图 7–1 系统监控配置

系统监控相关的配置均在“[Monitor]”类目下，各项配置含义如下：

FileLoad：文件目录监控开关，默认为 0，1 代表开启，0 代表关闭。

FileName：被监控的文件或者目录路径，可填入以逗号分隔的多个路径（当前最多支持 5 个）。默认为空。

FileRecursive：是否递归监控目录，默认 1。

FileDepth：目录递归最大深度，默认为 2。

TaskPid：指定进程的 PID。

MonitorCpuMemFluctuation：监控进程 CPU 与内存负载波动值，当波动超过此值时触发监控动作，默认 10（百分比）。

MonitorCpuMemAbsValue：监控进程 CPU 与内存负载绝对值，当超过此值时触发监控动作，默认 80（百分比）。

MonitorFrequency：监控频率，默认 1（min）。

MonitorMaxCollectTime：perf，strace 等日志的最大收集时间（分钟），默认 10 分钟。

LogStoreTime：监控日志保存时间（小时），默认 72 小时。

NetmonitorLoad：网络监控开关，默认为 0，1 代表开启，0 代表关闭。

NetmonitorHost：网络监控中被监控主机的 ip 地址。

NetmonitorProtocol：网络监控中被监控的协议，支持 TCP、UDP、ICMP 协议监控。

NetmonitorPort：网络监控中被监控的端口号，当监控协议为 TCP 或者 UDP 时可指定此参数，范围 1-65535。

ReclaimLoad：内存回收监控开关，默认为 0，1 代表开启，0 代表关闭。

ReclaimMask：内存回收监控掩码，默认为空，1 表示监控直接回收，2 表示监控间接回收（即 kswapd），3 表示同时监控二者。

MemleakLoad：内存泄露监控开关，默认为 0，1 表示开启，0 表示关闭。

MemleakMinSize：内存泄露监控程序关注的最小申请大小，单位为 Bytes，小于此值的申请将被忽略。默认为-1，表示不限制最小大小。

MemleakMaxSize：内存泄露监控程序关注的最大申请大小，单位为 Bytes，大于此值的申请将被忽略。默认为-1，表示不限制最大大小。

MemleakTopN：内存泄露监控程序每次打印的调用栈个数，默认为 5。

MemleakInterval：内存泄露监控程序每次打印的间隔时间，单位为秒，默认为 5。

MemFragmentationLoad：内存碎片监控程序开关，默认为 0，1 表示开启，0 表示关闭。

MemFragmentationOrder：内存碎片监控程序关注的阶数，监控程序关注内存碎片对申请 2^order(order 为阶数)大小的连续内存页的影响程度。

7.2.运行监控

在麒麟 V10 服务器操作系统上，在“终端”中使用“systemctl start kylin-sysassist-monitor.service”命令开始运行系统监控，命令执行格式如下：

```
[root@localhost ~]# systemctl start kylin-sysassist-monitor.service
```

执行结果如图 7-2 所示：

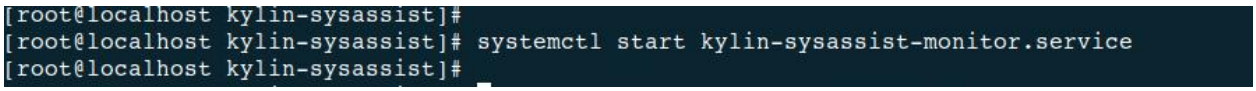

图 7-2 系统监控运行

监控开启后，监控的项目包括文件（目录）操作监控、进程监控、网络监控、内存监控。

文件（目录）操作监控： 在 vfs 层监控进程对指定路径的打开、读取、写入、重命名、删除文件、删除目录、创建目录操作，并将操作时间、进程及 pid、父进程及父进程 pid、操作类型、操作目标路径、操作目标 iNode 保存至日志文件中；

进程监控：监控指定进程的负载是否异常，当指定进程负载向上波动大小或阈值超过配置值时会触发收集进程的 CPU 或内存信息；

内存监控：

1. 内存回收监控：监控当前系统的直接/间接内存回收事件， 打印回收进程名及 pid、回收到的内存页数量及回收类型，可辅助确认当前系统内存负载情况及回收机制工作状态；

2. 内存泄露监控：通过监控当前系统的内核内存申请（kmalloc）、释放（kfree）函数，按不同调用栈统计申请后未释放的内存，间隔指定时间后，输出未释放内存最多的数个调用栈，辅助分析内存泄露现象。

3. 内存碎片监控：通过监控当前系统的内存碎片状态，当内存碎片可能影响到所关注阶数的连续物理内存页申请时，会打印警告至输出文件。

网络监控：可监控 tcp，udp,icmp 等协议的网络数据包。在接收端监控数据包到达各个协议层的时间，对于 tcp 协议可获取当前主机 TCP 状态的，在发送端监控数据包到达 ip 层、驱动层的时间；到达跟踪点的时间、cpu、源 mac、目的 mac、源 ip、目的 ip、传输层头部信息、本机状态信息保存到目标日志文件中。

7.3.输出文件

文件（目录）操作监控的日志文件输出在：

/var/kylin-sysassist/monitor/ky_bpf_file_monitor 目录下；

内存回收监控的日志文件输出在：

/var/kylin-sysassist/monitor/ky_bpf_reclaim_monitor 目录下；

内存泄露监控的日志文件输出在：

/var/kylin-sysassist/monitor/ky_bpf_memory_leak_monitorr 目录下；

内存碎片监控的日志文件输出在：

/var/kylin-sysassist/monitor/ky_bpf_fragmentation_monitor 目录下；

进程监控的日志文件输出在：

/var/kylin-sysassist/monitor/process/目录下；

网络监控的日志文件输出在：

/var/kylin-sysassist/monitor/ky_bpf_net_monitor/目录下。

附录 A

附录 A.1 版本兼容性说明

运维助手软件的版本迭代可能导致不同版本之间存在兼容性问题，产生该问题的原因可能有设计变更、规范升级、BUG 修复等原因，因此本节列出了已知的兼容性问题。

loongarch64 架构下兼容性问题

兼容性问题：

由于 loongarch64 架构下不存在 ltrace、strace、perf 软件包，且不完全支持 bpf-CORE 特性。导致 loongarch64 架构系统监控功能不可用（内存碎片监控功能，在 loongarch64 架构上可用）。

影响：

loongarch64 架构系统监控功能不可用（内存碎片监控功能除外）。

附录 A.2 故障排除

运维助手程序在运行过程出现故障可以通过日志文件进行排查，运维助手运行日志存放在“/var/log/kylin-sysassist.log”文件中。