**获取基本信息**

向服务器运维人员询问，系统的基本配置，安装的发行版本，建立和使用的账户，

所在网络拓扑的位置、网络配置情况，及其所承载的服务。

**系统信息**

[root@localhost ~]# uname -a

- 省略......

[root@localhost ~]# lsb\_version -a

- 省略......

[root@localhost ~]# head -n 1 /etc/issue

- 省略......

**用户及组**

[root@localhost ~]# cut -d: -f1 /etc/passwd

[root@localhost ~]# cut -d: -f1 /etc/group

**防火墙及路由**

[root@localhost ~]# iptables -L

[root@localhost ~]# route -n

**获取网络信息**

**网络接口**

[root@localhost ~]# ifconfig -a

**开放端口**

[root@localhost ~]# netstat -tanp

[root@localhost ~]# ss -tanp

**系统运行状态**

**计划任务**

系统cron任务

检查 /etc/crontab 有无存在异常项

[root@localhost ~]# cat /etc/crontab

**用户cron任务**

检查各用户cron任务

每个用户都有专用的cron任务文件：/var/spool/cron/USERNAME

**进程和服务**

**ps**

使用 ps 命令查看当前运行的进程列表

PS常用组合

**ps aux**

a 与终端相关的进程

u 以用户为中心组织进程状态信息显示

x 与终端无光的进程

**ps -ef**

e 显示所有进程

f 显示完整格式程序信息

**ps -eFH**

e 显示所有进程

F 显示完整格式的进程信息

H 以进程层级格式显示进程相关信息

**top、htop**

使用 top 或 htop 命令用来显示系统中正在运行的进程的实时状态CPU 利用情

况、内存消耗情况，以及每个进程情况

**启动服务**

使用 chkconfig 或 systemctl 命令列出所有启动的系统服务 程序

**日志分析**

**登录日志**

二进制日志文件 [登录]

1. **最近一次注册日志**

[ /var/log/lastlog ] # 最近一次用户登录的时间记录

**2. 用户登录日志**

[ /var/log/wtmp ]

[root@localhost ~]# last

- 或

[root@localhost ~]# last -f <filename> # 指定输入文件

**应用日志**

1. Apache服务器日志

/var/log/httpd/access.log # 其中包含Apache服务器的客户系统访问记录

/var/log/httpd/error.log # 其中包含Apache服务器的所有出错记录

**2. CUPS打印系统日志**

CUPS [ Common Unix Printing System ] 通用UNIX打印系统

/var/log/cups/access\_log # 访问日志文件，其中记录了打印机的设置情

况，提交的打印作业，以及打印作业的状态记录等信息

/var/log/cups/error\_log # 默认的日志文件，存储各种错误信息

**3. Samba 服务器日志**

> [目录] /var/log/samba

[root@localhost ~]# ls /var/log/samba

> log.smbd # 其中包含Samba服务器启动以及SMB/CIFS文件与打印共享方面的信息

> log.nmbd # 其中包含基于IP协议的NETBIOS网络通信方面的信息

> log.sysname # 用于记录特定客户系统的服务请求信息，文件名中的sysname是客户系统的主机名，如 log.winxp

**4. 其他日志**

/var/log/xferlog # 用于记录FTP服务器的文件传输日志信息

/var/log/mysqld.log # 用于记录MySQL数据库服务器的日志信息

/var/log/yum.log # 用于记录利用yum安装、删除或更新软件的日志信息

1

**系统日志**

1. **系统内核环形缓冲区**

/var/log/dmesg 日志文件，重现系统引导过程中控制台的输出信息。如果在引

导过程中出现问题，系统内核引导信息有助于诊断问题，分析产生问题的原因

[root@localhost ~]# dmesg | less

2. **系统消息日志**

/var/log/messages 是系统信息的集中存储位置，除了专门的日志文件之外，

其中记录了大部分系统进程、使用程序甚至应用程序输出的日志信息。

**3. 安全审计日志**

/var/log/audit/audit.log 用于记录系统安全审计信息，尤其是SELinux安全审计信息

**3. 安全认证日志**

/var/log/secure 用于记录系统安全认证信息，包含验证和授权方面信息，尤

其是sshd会将所有信息记录[其中包括失败登录]在这里信息

/var/log/auth.log 同上