Linux操作系统管理--日志管理和分析 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/252/2021_2022_Linux_E6_93_8D_E4_BD_c103_252948.htm 水平集日志管理：这部分包括一些开源技术，这些技术基本上是针对基于主机的日志记载，日志文件转储和日志文件分析。很多工具都是免费的、开源软件，在很多主要的Linux系统中都有集成，包括主流的RetHat和Novell。◆Ⅰ Logrotate Logrotate是在大量Linux系统中非常流行的应用程序工具，包括所有的RedHat和基于SUSE的系统都使用它。Logrotate主要是由cron（一个任务调度程序）控制周期性运行。Logrotate会读取日志文件（/ect/logrotate.conf），然后根据配置信息存档和压缩日志文件。系统管理员可以基于天数和大小来配置什么时候需要转储日志文件，以及多长时间需要维护一次备份日志，这样旧的存档日志文件就可以被新的存档日志代替。◆II Syslogd和klogd 典型的Linux系统利用一个叫syslogd的daemon后台程序，它从用户空间应用程序捕获日志信息，同时记录成文本日志文件或是通过网络发送到一个日志记载主机。Syslogd程序通常会伴随着一个叫klogd的程序，klogd用来捕获和记录内核信息。 Syslogd程序的行为可以通过/etc/syslog.conf配置文件进行配置。所有由syslog捕获的信息都根据facility和priority进行分类。然后这些信息就可以被发送到特殊的日志文件或日志记载主机，或者根据它们的facility（设备）和priority（行为级别）属性完全抛弃。498)this.style.width=498.">◆III Syslog-ng Syslog-ng应用程序是传统syslog daemon的增强移植实现。它提供了很多与标准syslog daemon相同的特性，同时还

包括一些附加特性，如基于内容的高级消息过滤功能，通过UDP或TCP的远程日志记载，把日志写进像MySQL或PostgreSQL这样的数据库。很多最近的基于SUSE的系统，如SLES10都已经改把syslog-ng作为缺省的syslog服务。◆IV Viewing logs Linux系统上的大部分日志文件都存储成纯文本，这就意味着可以通过使用大量不同的命令行工具进行查看和解析。典型的命令如tail，head，grep，cat，less，more，sed，more，sed和awk，使用这些命令可以通过命令行查看日志信息。 还有很多工具是通过GUI图形接口或是web浏览器来解析和查看日志文件。一些工具甚至可以处理特殊的日志格式，例如那些由Linux Netfilter防火墙子系统生成的日志文件。GNOME System Log Viewer GNOME系统包括一个基于GTK的系统日志观测程序，这个程序通过GUI图形界面展示系统日志。 YaST System Log Module 基于SUSE的系统使用包含View System Log模块（也叫做view_anymsg）的YaST，与GNOME System Log viewer类似，YaST模块允许系统管理员不使用命令行就可以观测许多不同种类的系统日志◆Ⅴ Log Analysis LogWatch Logwatch工具用来解析系统日志，定位任何可能预示安全隐患或是系统错误的数据，发送一个email到指定的地址。Logwatch与RetHat Enterprise Linux系统一起发布。以下是一个来自PRM描述的摘要“ LogWatch是一个可定制化日志分析系统。LogWatch可以解析给定时间段中的系统日志，并且建立一个详细的报告分析你指定的区域。LogWatch容易使用，而且声称它可以在任何系统上正常工作。注意的是，LogWatch现在分析Samba日志。 ”LogWatch主要通过cron周期性运行。LogCheck： Logcheck工具是Sentry Tools工程的

一部分，Sentry Tools工程还包括portsentry一个用来监测端口扫描的工具。与LogWatch工具类似，Logcheck用来解析系统日志，发现可能预示安全问题的数据，发送一个email到指定地址。Logcheck也像LogWatch一样，依靠cron工具周期性执行。 