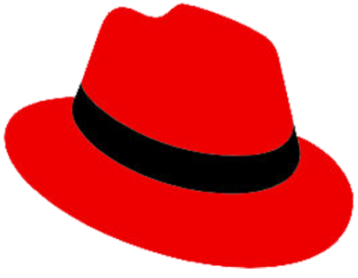
Red Hat

RH124 红帽系统管理 I

RH124-10-分析和存储日志



Red Hat

一、系统日志架构

系统日志

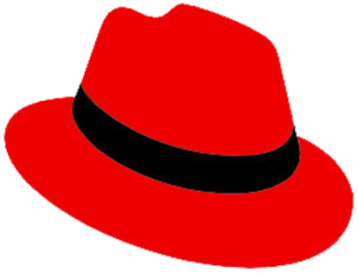
- RHEL7中的系统日志消息由两个服务负责处理, 它们是：systemd-journald 和 rsyslogd 。

- **systemd-journald**守护进程提供一种改进的日志管理服务，可以收集来自内核, 启动过程的早期阶段, 标准输出, 系统日志，以及守护进程启动和运行期间错误的消息。

- **rsyslogd**服务随后根据**类型(或设备)**和**优先级（消息严重性）**排列系统日志消息, 将它们写入到/var/log目录内的永久文件中。

常用的系统日志

- /var/log/dmesg　　核心启动日志
- /var/log/messages　　系统报错日志
- /var/log/maillog　　邮件系统日志
- /var/log/wtmp　　登录记录
- /var/log/secure　　安全信息,系统登录与网络连接的信息
- /var/log/cron　　与定期执行任务相关的日志文件
- /var/log/boot.log　　与系统启动相关的消息记录在此处



Red Hat

二、查看系统日志文件

系统日志配置文件

rsyslogd服务使用**日志消息的设备**和**优先级**来确定如何进行处理.这通过**/etc/rsyslog.conf**文件, 以及**/etc/rsyslog.d**中的***.conf**文件进行配置

查看配置文件中的生效部分:

cat /etc/rsyslog.conf | grep -v ^#| grep -v ^$

参数-v：反向选择，上面表示列出开头不是#并且不是空行的行

系统日志文件

许多程序使用**syslog协议**将事件记录到系统。每一日志消息根据设备（消息的类型）和优先级（消息的严重性）分类。

八个优先级：

- 0：emerg：会导致主机系统不可用的情况
- 1：alert：必须立即采取措施
- 2：crit：比较严重的状况
- 3：err：运行出现错误
- 4：warning：可能会影响系统功能的事件
- 5：notice：不会影响系统但值得注意
- 6：info：一般信息
- 7：debug：程序或系统调试信息

日志轮转

日志通过**logrotate**实用工具“轮转”，以防止它们将包含/var/log的文件系统填满。轮转日志文件时，会使用**名称扩展**对其进行重命名，名称扩展指示轮转日期：如果文件在2014年10月30日轮转，则原来的/var/log/message文件将变成/var/log/message-20141030.轮转原日志文件之后会创建新日志，并通知对它执行写操作的服务

轮转若干次之后（通常在**四周之后**），丢弃原日志文件以释放磁盘。Cron作业每日运行一次logrotate程序，以查看是否有任何日志需要轮转。大多数日志文件每周轮转一次，但是logrotate轮转文件的速度有时较快，有时较慢，或在文件达到特定大小时进行轮转。

分析系统日志条目

rsyslog所写的系统日志在文件的开头显示最旧的消息，在文件的末尾显示最新的消息。

日志文件消息格式：

① Feb 11 20:11:48 :记录该日志条目的时间戳

② localhost：发送该日志消息的主机

③ sshd[1433]：发送该日志消息的程序或进程

④ Failed password for student from 172.25.0.10 port 59344：发送的实际消息

利用tail监控日志文件

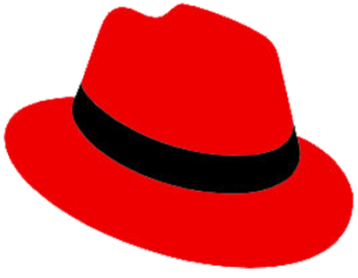
监控事件的一个或多个日志文件，这对重现问题有特别帮助

命令：**tail -f** /path/to/file

作用：输出指定文件的最后10行，并在新行写入到被监控文件中时继续输出它们

使用logger发送系统日志消息

logger命令可以发送消息到rsyslog服务。默认情况下，它将严重性为**notice（user.notice）**的消息发送给设备用户，除非通过-p选项另外指定。测试对rsyslog配置的更改将特别有用。



Red Hat

三、查看systemd日志条目

通过journalctl查看事件

systemd日志将日志数据存储在**带有索引**的结构化二进制文件中。此数据包含与日志事件相关的额外信息

RHEL7中systemd日志默认存储在**/run /log**中，重启后予以清除 。

journalctl以**粗体文本**突出显示优先级为notice或warning的消息，以**红色文本**突出显示优先级为error和更高的消息

命令：journalctl

参数：

-n：设置显示日志条目数，默认显示最后10行日志条目

-p：显示指定级别条目。后面接优先级名称或编号。

-f：同tail –f在新日志条目写入到日志中时继续输出他们

--since和 --until：从什么时候开始，直到什么时候结束

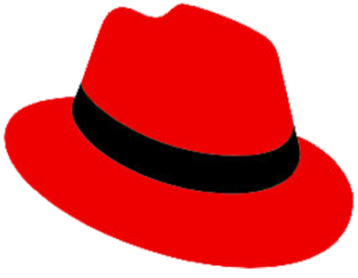
通过journalctl查看事件

journalctl其他搜索关于特定进程或事件的行的选项还有

- _COMM　　命令的名称
- _EXE　　进程的可执行文件的路径
- _PID　　进程的PID
- _UID　　运行该进程的用户的UID
- _SYSTEMD_UNIT　启动该进程的systemd单元

实例：查询显示与systemd单元文件sshd.service启动，并且PID1182的进程相关信息

Journalctl _SYSTEMD_UNIT=sshd.service _PID=1182



Red Hat

四、保存systemd日志

永久存储系统日志

默认情况下，systemd日志保存在**/run/log/journal**中，这意味着系重启时它将会被清除。如果存在**/var/log/journal**目录，该日志会改为记录在这个目录中。这样做优点是重启后就立即利用历史数据。

即便永久日志，日志轮转机制每个月触发，并且日志的大小不能超过**所处文件系统的10%**，也不能造成文件系统的**可用空间低于15%**。（可在/etc/systemd/journald.conf中调节）

配置永久存储日志

1）创建/var/log/journal,使systemd日志变永久日志

mkdir /var/log/journal

2)确保/var/log/journal目录由root用户和组systemd-journal所有，并且权限为2755

chown root：systemd-journal /var/log/journal

chmod 2755 /var/log/journal

3)重启系统或以root发送USR1信号到systemd-journal进程

killall –USR1 systemd-journald

4)显示上次启动以来的日志消息

journalctl -b

Red Hat

五、保持准确的时间

设置本地时钟和时区

对于在多个系统间分析日志文件而言，正确同步系统时间非常重要。网络时间协议（NTP）是计算机用于通过互联网提供并获取正确时间信息的一种标准方法。计算机可以通过互联网上的公共NTP服务获取正确的时间信息。

命令：timedatectl

实例：

- 列出了已知时区的数据库：timedatectl list-timezones
- 更改当前时区系统设置：timedatectl set-timezone
- Asia/Shanghai更改当前时间和日期：timedatectl set-time 09:00:00
- 启用或禁用NTP同步：timedatectl set-ntp true| false

配置和监控chronyd

- chronyd服务通过与配置NTP服务同步，使通常不精确的本地硬件时钟（RTC）保持准确；或者如果没有网络连接，则与计算的RTC时钟飘移值同步，该值记录在**/etc/chrony.conf**中指定的driftfile中
- 默认情况下，chronyd使用NTP pool Project的服务器同步时间，不需额外配置
- NTP时钟源的质量由该时间源报告的stratum决定。**stratum**确定计算机与高性能参考时钟偏离的跃点数。
- /etc/chrony.conf可配置**server**和**peer**两种时间源。server比本地NTP服务器高一个级别，peer属于同一级别。

配置同步

1)编辑配置文件/etc/chrony.conf

#Use public servers from the pool.ntp.org.project

server classroom.example.com iburst

将chronyd指向本地时间源classroom.example.com

2)重启服务

systemctl restart chronyd

命令：chronyc

充当chronyd服务的客户端。在设置NTP同步后，验证用于同步系统时钟的是否为NTP服务器非常有用。

实例：chronyc sources -v

S（源状态）字段中的*字符表示classroom.example.com服务器已被用作时间源，是计算机当前与之同步的NTP服务器


WISDOM NET