rsyslogd日志服务

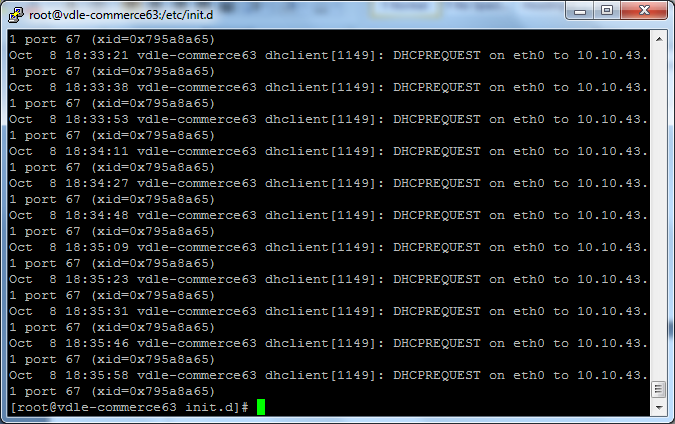
# rsyslogd服务简介

syslog是一种工业标准的协议，可用来记录应用程序或者设备的日志，日志一般都存储在/var/log目录下。可以通过查看日志记录，随时掌握系统状况。日志是通过syslogd这个进程记录系统有关事件记录，也可以记录应用程序运作事件。通过适当的配置，我们还可以实现运行syslog协议的机器间通信，通过分析这些网络行为日志，藉以追踪掌握与设备和网络有关的状况。判断系统是否安装rsyslogd日志服务器的方法：ps -aux | grep rsyslogd

# rsyslogd日志格式和常见日志

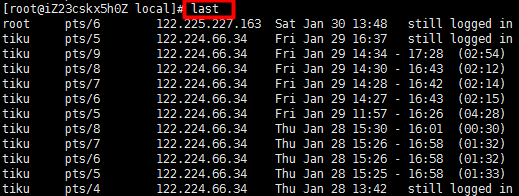
## 日志格式

时间产生的时间，发生事件的服务器主机名，发生时间的服务器名或程序名，事件的具体描述

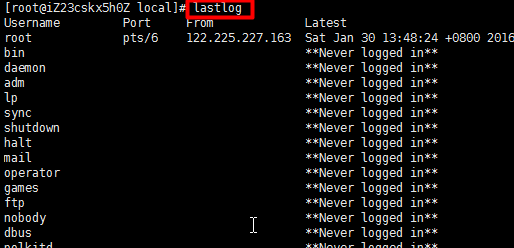


## 常见日志

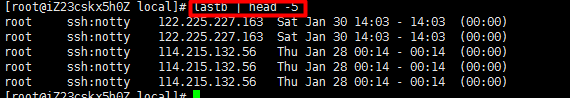
* /var/log/message：系统日志。记录系统重要信息的日志，记录了linux系统大部分重要信息。
* /var/log/secure：系统安全日志，记录验证和授权方面的信息。只要涉及用户和密码的程序都会记录。例如POP3，SSH，Telnet，FTP。
* /var/log/wtmp：系统登陆者日志永久记录所有用户的登陆，注销信息，同时记录系统的启动，重启关机时间。通过last查看



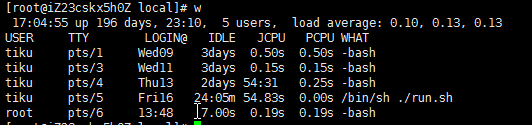
* /var/log/lastl：用户登录系统最后时间日志。记录用户最后一次登陆时间的日志。是二进制文件，通过命令lastlog查看。



* /var/log/btmp：错误登录日志。记录错误登陆的日志，是一个二进制文件。通过命令lastb命令查看



* /var/run/utmp：当前登录用户日志。记录当前已经登陆的用户的信息。可以通过w,who,users等命令来查看



* /var/log/cron：记录定时任务相关的日志
* /var/log/cups/:记录打印信息日志
* /var/log/dmesg:记录系统开机自检的信息。可以通过dmesg命令直接查看。
* /var/log/mailog：记录邮件信息

# 配置文件/etc/rsyslog.conf解析

#服务名称[连接符号]日志等级 日志记录位置

## 服务名称

auth：(安全和认证相关)

authpriv：(私有的安全和认证相关)

cron：(系统定时任务)

daemon：(各守护进程)

ftp：(ftp相关)

kern：(内核相关)

local0-local7：(本地使用预留服务)

lpr：(打印)

mail：(邮件)

news：(新闻)

syslog：(日志本身)

user：（用户）

uucp：(子系统日志信息)

## 连接符

* .表示比后面的等级高（包含该等级）的日志都记录下来。
* .=表示只记录所需等级日志
* .!表示不等于,就是除了该等级的日志外，其他等级的日志都要记录。

## 日志等级：

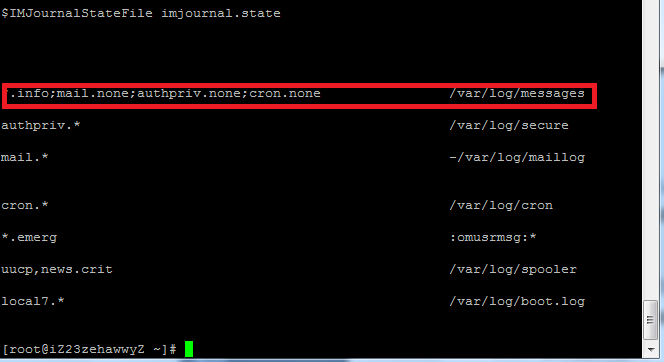
debug<info<notice<warning<err<crit(临界状况信息，比error严重)<alert<emerg(等级越高，记录内容越少)

\*表示所有的日志等级

* emerg：该系统不可用，等同于panic。
* alert：需要立即被修改的条件。
* crit：危急情况。
* err：错误消息，等同于error。
* warning：预警信息，等同于warn。
* notice：具有重要性的普通条件。
* info：提供信息的消息。
* debug：不包含函数条件或问题的其他信息。
* none：没有重要级，通常用于排错。

## 日志记录位置

* 日志文件的绝对路径；
* 系统设备文件；
* 转发给远程主机；
* 用户名；
* ~（丢弃）



# 日志轮替

作用：（按天切割日志，日志轮换（删除很久之前的日志）

日志文件的命名规则：配置文件拥有dateext参数，日记就会用日期来作为文件的后缀。日志轮替配置文件/etc/logrotate.conf：

* daily:日志轮替周期是每天
* weekly：日志轮替周期是每周
* monthly:日志轮替周期是每年
* rotate 数字：保留的日志文件个数。0表示备份
* compress:表示压缩日志
* create mode owner gourp:建立新日志，同时指定新日志的权限与所有者和所属组。如create 0600 root utmp
* mail address：当日志轮替是，输出内容通过邮件发送给指定邮箱
* missingok:如果日志不存在，忽略该日志警告。
* notifempty:如果日志为空，不进行日志轮替。
* minsize 大小：日志轮替的最小值。
* size:日志只有大于指定大小才进行日志轮替，而不是按时间轮替。
* dateext:使用日期作为日志轮替文件的后缀。

## 日志轮替应用

把apache日志加入轮替（rpm包安装的服务不需要，源代码包安装需要）

vi /etc/logrotate.conf

/usr/local/apache2/logs/access.log{

daily

create

rotate 30

}

## logrotate命令

logrotate [选项] 配置文件名

-v：显示日志轮替过程

-f：强制进行日志轮替。

logrotate -vf /etc/logrotate.conf