# 日志管理

讲师：王晓春

# 本章内容



- 日志介绍
- 日志配置
- 日志管理
- 远程日志
- 基于MYSQL的日志

# 日志介绍



- 日志：

  历史事件:时间，地点，人物，事件

  日志级别：事件的关键性程度，Loglevel

- 系统日志服务：
- sysklogd :CentOS 5之前版本

  syslogd: system application 记录应用日志

  klogd: linux  kernel 记录内核日志

  - 事件记录格式：

    日期时间　主机　进程[pid]: 事件内容

  - C/S架构：通过TCP或UDP协议的服务完成日志记录传送，将分布在不同主机的日志实现集中管理

# rsyslog



- rsyslog特性：CentOS6和7
  - 多线程
  - UDP, TCP, SSL, TLS, RELP
  - MySQL, PGSQL, Oracle实现日志存储
  - 强大的过滤器，可实现过滤记录日志信息中任意部分
  - 自定义输出格式
- ELK：elasticsearch, logstash, kibana
  - 非关系型分布式数据库
  - 基于apache软件基金会jakarta项目组的项目lucene
  - Elasticsearch是个开源分布式搜索引擎
  - Logstash对日志进行收集、分析，并将其存储供以后使用
  - kibana 可以提供的日志分析友好的 Web 界面

# rsyslog介绍



- 术语，参见man logger
  - facility：设施，从功能或程序上对日志进行归类

    auth, authpriv, cron, daemon,ftp,kern, lpr, mail, news, security(auth), user, uucp, local0-local7, syslog

  - Priority 优先级别，从低到高排序

    debug, info, notice, warn(warning), err(error), crit(critical), alert, emerg(panic)

  - 参看帮助： man 3 syslog

# rsyslog



- 程序包：rsyslog
- 主程序：/usr/sbin/rsyslogd
- CentOS 6：service rsyslog {start|stop|restart|status}
- CentOS 7：/usr/lib/systemd/system/rsyslog.service
- 配置文件：/etc/rsyslog.conf，/etc/rsyslog.d/*.conf
- 库文件： /lib64/rsyslog/*.so
- 配置文件格式：由三部分组成
  - MODULES：相关模块配置
  - GLOBAL DIRECTIVES：全局配置
  - RULES：日志记录相关的规则配置

# rsyslog



- RULES配置格式： facility.priority; facility.priority... target
- facility：
  - *: 所有的facility
  - facility1,facility2,facility3,...：指定的facility列表
- priority：
  - *: 所有级别
  - none：没有级别，即不记录
  - PRIORITY：指定级别（含）以上的所有级别
  - =PRIORITY：仅记录指定级别的日志信息
- target：
  - 文件路径：通常在/var/log/，文件路径前的-表示异步写入
  - 用户：将日志事件通知给指定的用户，* 表示登录的所有用户
  - 日志服务器：@host，把日志送往至指定的远程服务器记录
  - 管道： | COMMAND，转发给其它命令处理

# 启用网络日志服务



- 通常的日志格式：

  事件产生的日期时间 主机 进程(pid)：事件内容

  如： /var/log/messages,cron,secure等

- 配置rsyslog成为日志服务器

```
#### MODULES ####
# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514

# Provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 514
```

# 其它日志



- 其它的日志文件
- /var/log/secure：系统安装日志，文本格式，应周期性分析
- /var/log/btmp：当前系统上，用户的失败尝试登录相关的日志信息，二进制格式，lastb命令进行查看
- /var/log/wtmp：当前系统上，用户正常登录系统的相关日志信息，二进制格式，last命令可以查看
- /var/log/lastlog:每一个用户最近一次的登录信息，二进制格式，lastlog命令可以查看
- /var/log/dmesg：系统引导过程中的日志信息，文本格式

  文本查看工具查看

  专用命令dmesg查看
- /var/log/messages ：系统中大部分的信息
- /var/log/anaconda : anaconda的日志

# 日志管理journalctl



- Systemd 统一管理所有 Unit 的启动日志。带来的好处就是，可以只用journalctl一个命令，查看所有日志（内核日志和应用日志）。日志的配置文件/etc/systemd/journald.conf
- journalctl用法
- 查看所有日志（默认情况下 ，只保存本次启动的日志）

  journalctl
- 查看内核日志（不显示应用日志）

  journalctl -k
- 查看系统本次启动的日志

  journalctl -b

  journalctl -b -0
- 查看上一次启动的日志（需更改设置）

  journalctl -b -1

# 日志管理journalctl



- 查看指定时间的日志

```
journalctl --since="2017-10-30 18:10:30"
journalctl --since "20 min ago"
journalctl --since yesterday
journalctl --since "2017-01-10" --until "2017-01-11 03:00"
journalctl --since 09:00 --until "1 hour ago"
```

- 显示尾部的最新10行日志

```
journalctl -n
```

- 显示尾部指定行数的日志

```
journalctl -n 20
```

- 实时滚动显示最新日志

```
journalctl -f
```

# 日志管理journalctl



- 查看指定服务的日志
  journalctl /usr/lib/systemd/systemd
- 查看指定进程的日志
  journalctl _PID=1
- 查看某个路径的脚本的日志
  journalctl /usr/bin/bash
- 查看指定用户的日志
  journalctl _UID=33 --since today
- 查看某个 Unit 的日志
  journalctl -u nginx.service
  journalctl -u nginx.service --since today
- 实时滚动显示某个 Unit 的最新日志
  journalctl -u nginx.service -f
- 合并显示多个 Unit 的日志
  journalctl -u nginx.service -u php-fpm.service --since today

# 日志管理journalctl



- 查看指定优先级（及其以上级别）的日志，共有8级
  - 0: emerg
  - 1: alert
  - 2: crit
  - 3: err
  - 4: warning
  - 5: notice
  - 6: info
  - 7: debug

```
journalctl -p err -b
```

- 日志默认分页输出，--no-pager 改为正常的标准输出

```
journalctl --no-pager
```

# 日志管理journalctl



- 以 JSON 格式（单行）输出

  journalctl -b -u nginx.service -o json

- 以 JSON 格式（多行）输出，可读性更好

  journalctl -b -u nginx.serviceqq -o json-pretty

- 显示日志占据的硬盘空间

  journalctl --disk-usage

- 指定日志文件占据的最大空间

  journalctl --vacuum-size=1G

- 指定日志文件保存多久

  journalctl --vacuum-time=1years

# 示例：rsyslog将日志记录于MySQL中



- (1) 准备MySQL Server
- (2) 在mysql server上授权rsyslog能连接至当前服务器

```
GRANT ALL ON Syslog.* TO 'USER'@'HOST' IDENTIFIED BY 'PASSWORD';
```

- (3) 在rsyslog服务器上安装mysql模块相关的程序包

```
yum install rsyslog-mysql
```

- (4) 为rsyslog创建数据库及表；

```
mysql -uUSERNAME -hHOST -pPASSWORD < /usr/share/doc/rsyslog-7.4.7/mysql-createDB.sql
```

- (5) 配置rsyslog将日志保存到mysql中

```
#### MODULES ####
$ModLoad ommysql
#### RULES ####
facility.priority   :ommysql:DBHOST,DBNAME,DBUSER, PASSWORD
```

# 示例：通过loganalyzer展示数据库中的日志



- (1) 在rsyslog服务器上准备amp或nmp组合

```
yum install httpd php php-mysql php-gd
```

- (2) 安装LogAnalyzer

```
tar xf loganalyzer-4.1.5.tar.gz
cp -a loganalyzer-4.1.5/src  /var/www/html/loganalyzer
cd  /var/www/html/loganalyzer
touch config.php
chmod 666 config.php
```

# 示例：通过loganalyzer展示数据库中的日志



- (3) 配置loganalyzer

  systemctl start httpd.service

  http://HOST/loganalyzer

  MySQL Native, Syslog Fields, Monitorware

- (4) 安全加强

  cd  /var/www/html/loganalyzer

  chmod 644 config.php

# Logrotate日志存储



- logrotate 程序是一个日志文件管理工具。用来把旧的日志文件删除，并创建新的日志文件，称为日志转储或滚动。可以根据日志文件的大小，也可以根据其天数来转储，这个过程一般通过 cron 程序来执行
- 配置文件是 /etc/logrotate.conf
- 主要参数如下
- compress 通过gzip 压缩转储以后的日志
- nocompress 不需要压缩时，用这个参数
- copytruncate 用于还在打开中的日志文件，把当前日志备份并截断
- nocopytruncate 备份日志文件但是不截断
- create mode owner group 转储文件，使用指定的文件模式创建新的日志文件

# Logrotate日志存储



- nocreate 不建立新的日志文件
- delaycompress 和 compress 一起使用时，转储的日志文件到下一次转储时才压缩
- nodelaycompress 覆盖 delaycompress 选项，转储并压缩
- errors address 专储时的错误信息发送到指定的Email 地址
- ifempty 即使是空文件也转储，是缺省选项。
- notifempty 如果是空文件的话，不转储
- mail address 把转储的日志文件发送到指定的E-mail 地址
- nomail 转储时不发送日志文件
- olddir directory 转储后的日志文件放入指定的目录，必须和当前日志文件在同一个文件系统
- noolddir 转储后的日志文件和当前日志文件放在同一个目录下

# Logrotate日志存储



- prerotate/endscript 在转储以前需要执行的命令可以放入这个对，这两个关键字必须单独成行
- postrotate/endscript 在转储以后需要执行的命令可以放入这个对，这两个关键字必须单独成行
- daily 指定转储周期为每天
- weekly 指定转储周期为每周
- monthly 指定转储周期为每月
- size 大小 指定日志超过多大时，就执行日志转储
- rotate count 指定日志文件删除之前转储的次数，0 指没有备份，5 指保留5 个备份
- Missingok 如果日志不存在，提示错误
- Nomissingok如果日志不存在，继续下一次日志，不提示错误

# 关于马哥教育

马哥教育
IT人的高薪职业学院

- 博客：http://mageedu.blog.51cto.com
- 主页：http://www.magedu.com
- QQ：1661815153, 113228115
- QQ群：203585050, 279599283

# 祝大家学业有成

# 谢　谢