Rsyslog 的使用

---高性能、功能丰富的日志收集应用

@丁天密 2016.01.27

主要内容

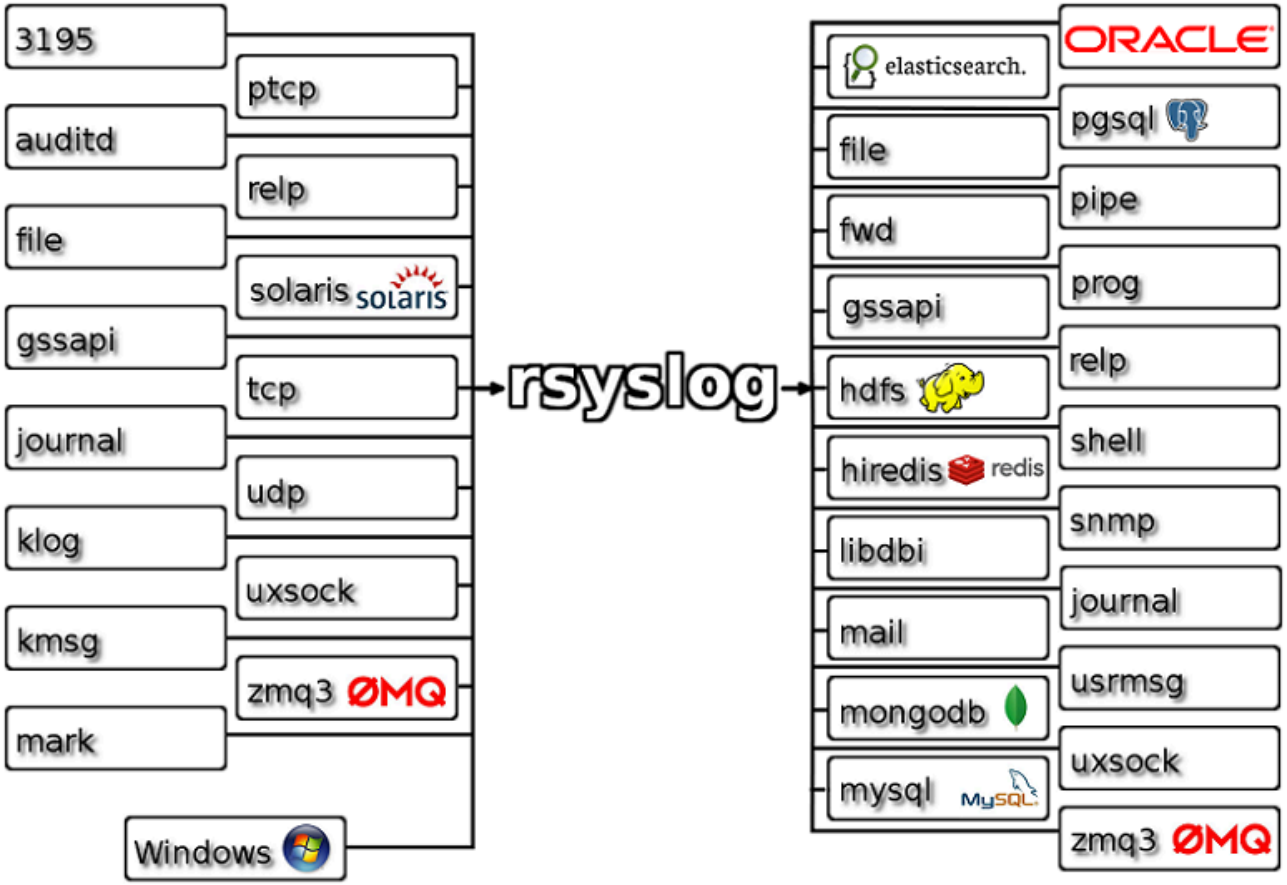
- Rsyslog的特性与使用场景
- Rsyslog的系统架构
- Rsyslog常用配置与模块
- Rsyslog在收集NGX日志案例

Rsyslog特性

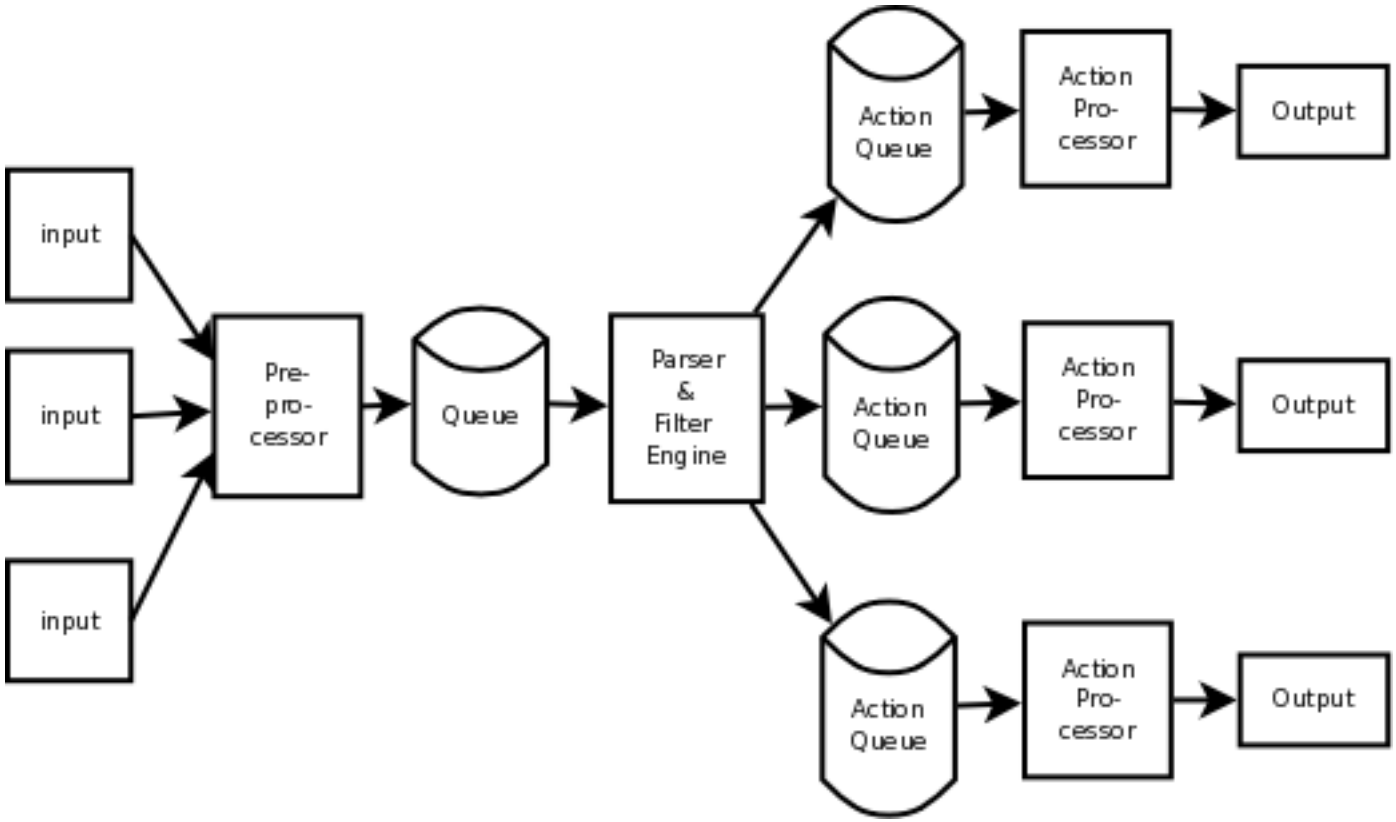
- Multi-threading, high availability
- TCP, SSL, TLS, RELP
- MySQL, Redis,Elasticsearch, Oracle and more
- Filter any part of syslog message
- Fully configurable output format
- Encryption and compression transmission
- Suitable for enterprise-class relay chains

website: http://www.rsyslog.com/

Rsyslog使用场景



Rsyslog系统架构



输入模块->预处理模块->主队列->过滤模块->执行队列->输出模块

Rsyslog常用配置

```
:msg,contains,"error"                 # 选择包含 error 的日志
:hostname,isequal, "host1"            # 选择主机名为 host1 的日志
:msg,!regex,"fatal .* error"          # 选择不匹配指定正则表达式的日志
*.* @192.168.0.1                      # 使用 UDP 发送日志到 192.168.0.1
*.* @@example.com:18                  # 使用 TCP 发送到 "example.com" 的 18 端口
*.* @(z9) 192.168.0.1                 # 使用 UDP 发送消息192.168.0.1，启用压缩
:msg,contains,“error” elain           #发送包含'error'消息到特定用户
cron.* ~                              #丢弃日志(在v8以上版本，~ 用 stop 代替)
mail.none  /var/log/messages         #mail日志不写入messages

$template Dailymsg,“/var/log/syslog/%$YEAR%/%$MONTH%/%$DAY%/msg"
*.* ? Dailymsg                        #动态文件输出
```

Rsyslog标准配置

日志设备/类型	说明
auth	pam产生的日志
authpriv	ssh,ftp等登录信息的验证信息
cron	时间任务相关
kern	内核
lpr	打印
mail	邮件
mark(syslog)	rsyslog服务内部的信息,时间标识
news	新闻组
user	用户程序产生的相关信息
uucp	unix to unix copy, unix主机之间相关的通讯
local 1~7	自定义的日志设备

Rsyslog标准配置

从上到下，级别从低到高，记录的信息越来越少 详细的可以查看手册: man 3 syslog

级别	级别值	说明
debug	7	有调式信息的，日志信息最多
info	6	一般信息的日志，最常用
notice	5	最具有重要性的普通条件的信息
warning	4	警告级别
err	4	错误级别，阻止某个功能或者模块不能正常工作的信息
crit	3	严重级别，阻止整个系统或者整个软件不能正常工作的信息
alert	1	需要立刻修改的信息
emerg	0	内核崩溃等严重信息
none		什么都不记录

Rsyslog内置属性

属性名	说明
msg	日志正文
hostname	日志中的主机名
fromhost	从该主机接收到的消息，可能不是最开始的发送主机
fromhost-ip	fromhost 的 IP
syslogtag	日志标签，如 named[12345]
programname	日志标签的静态部分，如 named
pri	日志的 PRI 部分
pri-text	PRI 的文本表示，如 syslog.info
syslogfacility	日志类别
syslogfacility-text	日志类别的文本表示
syslogseverity	日志级别
syslogseverity-text	日志级别的文本表示
timegenerated	日志接收时间，或理解为 timereceived
timereported	日志内的报告时间，或生成时间
$now	当前时间，YYYY-MM-DD
$year	当前年，YYYY
$month	当前月，MM
$day	当前日志，DD
$hour	当前小时，24 小时格式，HH
$hhour	当前半小时，0-29 对应 0，30-59 对应 1
$qhour	当前1/4小时，0-3
$minute	当前分钟，MM

Rsyslog常用模块 ---Input moudle

- imfile: Text File Input Module
- imklog: Kernel Log Input Module
- imkmsg: /dev/kmsg Log Input Module
- impstats: Generate Periodic Statistics of Internal Counters
- imptcp: Plain TCP Syslog
- imrelp: RELP Input Module
- imtcp: TCP Syslog Input Module
- imudp: UDP Syslog Input Module
- imuxsock: Unix Socket Input

- http://www.rsyslog.com/doc/v8-stable/configuration/modules/idx_input.html

Rsyslog常用模块 ---Output moudle

- omelasticsearch: Elasticsearch Output Module
- omfile: File Output Module
- omhdfs: Hadoop Filesystem Output Module
- omhiredis: Redis Output Module
- omkafka: write to Apache Kafka
- ommail: Mail Output Module
- ommongodb: MongoDB Output Module
- ommysql: MySQL Database Output Module
- omoracle: Oracle Database Output Module
- ompipe: Pipe Output Module
- omuxsock: Unix sockets Output Module

- http://www.rsyslog.com/doc/v8-stable/configuration/modules/idx_output.html

Rsyslog收集ngx日志

```
#加载模块
module(load="imfile")    # if you want to tail files
module(load="omkafka")   # lets you send to Kafka

#使用imfile模块读取日志文件
#nginx access log
input(type="imfile"
      File="/home/work/logs/nginx/*.log"
      Tag="ngx_log_mishop_order"
      PersistStateInterval="1000"
      reopenOnTruncate="on"
      addMetadata="on"
)

#定义一个日志解析模板
template( name="general_log" type="string" string="%hostname% %fromhost-ip% %msg%")
```

Rsyslog收集ngx日志

```
#使用omkafka模块将日志发送至kafka集群
#nginx access log
if ($syslogtag == "ngx_log_mishop_order") then {
    action(
        broker=["c3-b2c-kafka01.bj:9092","c3-b2c-kafka02.bj:9092","c3-b2c-kafka03.bj:9092"]
        type="omkafka"
        topic="ngx_log_mishop_order"
        template="general_log"
        confParam=["compression.codec=gzip"]
        partitions.auto="on"
    )
    stop
}
```

Thanks