[Edit](http://maxiang.info/" \l "/?provider=evernote&guid=53faa70e-915d-42b7-80ae-61328c629e24&notebook=linux)

# rsyslog 日志配置

linux rsyslog

* [rsyslog 日志配置](#rsyslog-日志配置)
  + [监控系统操作日志](#监控系统操作日志)
  + [集中管理rsyslog日志](#集中管理rsyslog日志)

rsyslog负责管理系统日志，是一个非常强的工具，今日研究只到系统监控这一方面

## 监控系统操作日志

首先可以把之前的日志格式换一个写法

# Use default timestamp format

#$ActionFileDefaultTemplate RSYSLOG\_TraditionalFileFormat

#把之前的注释掉

$template xsformat,"%$NOW% %TIMESTAMP:8:15% %FROMHOST% %syslogtag% %msg%\n"

$ActionFileDefaultTemplate xsformat

#然后把local4不记录到 /var/log/message下，另换一个文件专门记录command

\*.info;mail.none;authpriv.none;cron.none;local4.none /var/**log**/messages

然后在服务器端配置一个conf文件

# vim /etc/rsyslog.**d**/command.**conf**

local4.\* /**var**/**log**/command.log

# /etc/init.**d**/rsyslog restart

这里需要增加环境变量才能开始记录，环境变量是必不可少的。

# vim /etc/bashrc

**export** PROMPT\_COMMAND='{ msg=$(history 1 | { read x y; echo $y; });logger -p local4.info "[euid=$(whoami)]":$(who am i):[`pwd`]"$msg"; }'

OK,现在就基本上开始记录了

[root@client\_102 ~]# cat /var/log/command.log

2016-03-23 13:07:55 client\_102 root: [euid=root]:root pts/2 2016-03-23 10:39 (10.0.0.1):[/root]source /etc/bashrc

2016-03-23 13:07:57 client\_102 root: [euid=root]:root pts/2 2016-03-23 10:39 (10.0.0.1):[/root]ls

2016-03-23 13:08:02 client\_102 root: [euid=root]:root pts/2 2016-03-23 10:39 (10.0.0.1):[/root]cat /var/**log**/command.**log**

2016-03-23 13:08:09 client\_102 root: [euid=root]:root pts/2 2016-03-23 10:39 (10.0.0.1):[/root]cat /var/**log**/command.**log**

2016-03-23 13:10:46 client\_102 root: [euid=root]:root pts/2 2016-03-23 10:39 (10.0.0.1):[/root]vim /etc/bashrc

现在是把他们推送到服务器端，

## 集中管理rsyslog日志

集中管理时便需要在服务端开启514 端口这里把TCP,UDP的514端口都开启来,在rsyslog中把下面四行去掉注释

$ModLoad imudp

$UDPServerRun 514

# Provides TCP syslog reception

$ModLoad imtcp

$InputTCPServerRun 514

在客户端修改local.4的发送端为如下

local4.\* @172.16.1.102:514 # 服务端IP:端口

%23%20rsyslog%20%u65E5%u5FD7%u914D%u7F6E%0A@%28linux%29%5Brsyslog%5D%0A%0A%5Btoc%5D%0A%0Arsyslog%u8D1F%u8D23%u7BA1%u7406%u7CFB%u7EDF%u65E5%u5FD7%uFF0C%u662F%u4E00%u4E2A%u975E%u5E38%u5F3A%u7684%u5DE5%u5177%uFF0C%u4ECA%u65E5%u7814%u7A76%u53EA%u5230%u7CFB%u7EDF%u76D1%u63A7%u8FD9%u4E00%u65B9%u9762%0A%0A%23%23%20%u76D1%u63A7%u7CFB%u7EDF%u64CD%u4F5C%u65E5%u5FD7%0A%u9996%u5148%u53EF%u4EE5%u628A%u4E4B%u524D%u7684%u65E5%u5FD7%u683C%u5F0F%u6362%u4E00%u4E2A%u5199%u6CD5%0A%60%60%60%0A%23%20Use%20default%20timestamp%20format%0A%23%24ActionFileDefaultTemplate%20RSYSLOG\_TraditionalFileFormat%0A%23%u628A%u4E4B%u524D%u7684%u6CE8%u91CA%u6389%0A%24template%20xsformat%2C%22%25%24NOW%25%20%25TIMESTAMP%3A8%3A15%25%20%25FROMHOST%25%20%25syslogtag%25%20%25msg%25%5Cn%22%0A%24ActionFileDefaultTemplate%20xsformat%0A%23%u7136%u540E%u628Alocal4%u4E0D%u8BB0%u5F55%u5230%20/var/log/message%u4E0B%uFF0C%u53E6%u6362%u4E00%u4E2A%u6587%u4EF6%u4E13%u95E8%u8BB0%u5F55command%0A\*.info%3Bmail.none%3Bauthpriv.none%3Bcron.none%3Blocal4.none%20%20%20%20%20%20%20%20%20%20%20/var/log/messages%0A%60%60%60%0A%u7136%u540E%u5728%u670D%u52A1%u5668%u7AEF%u914D%u7F6E%u4E00%u4E2Aconf%u6587%u4EF6%0A%60%60%60%0A%23%20vim%20/etc/rsyslog.d/command.conf%0Alocal4.\*%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20/var/log/command.log%0A%23%20/etc/init.d/rsyslog%20restart%0A%60%60%60%0A%u8FD9%u91CC%u9700%u8981%u589E%u52A0%u73AF%u5883%u53D8%u91CF%u624D%u80FD%u5F00%u59CB%u8BB0%u5F55%uFF0C%u73AF%u5883%u53D8%u91CF%u662F%u5FC5%u4E0D%u53EF%u5C11%u7684%u3002%0A%60%60%60%0A%23%20vim%20/etc/bashrc%0Aexport%20PROMPT\_COMMAND%3D%27%7B%20msg%3D%24%28history%201%20%7C%20%7B%20read%20x%20y%3B%20echo%20%24y%3B%20%7D%29%3Blogger%20-p%20local4.info%20%22%5Beuid%3D%24%28whoami%29%5D%22%3A%24%28who%20am%20i%29%3A%5B%60pwd%60%5D%22%24msg%22%3B%20%7D%27%0A%0A%60%60%60%0A%0AOK%2C%u73B0%u5728%u5C31%u57FA%u672C%u4E0A%u5F00%u59CB%u8BB0%u5F55%u4E86%0A%0A%60%60%60%0A%5Broot@client\_102%20%7E%5D%23%20cat%20/var/log/command.log%20%0A2016-03-23%2013%3A07%3A55%20client\_102%20root%3A%20%20%5Beuid%3Droot%5D%3Aroot%20pts/2%202016-03-23%2010%3A39%20%2810.0.0.1%29%3A%5B/root%5Dsource%20/etc/bashrc%0A2016-03-23%2013%3A07%3A57%20client\_102%20root%3A%20%20%5Beuid%3Droot%5D%3Aroot%20pts/2%202016-03-23%2010%3A39%20%2810.0.0.1%29%3A%5B/root%5Dls%0A2016-03-23%2013%3A08%3A02%20client\_102%20root%3A%20%20%5Beuid%3Droot%5D%3Aroot%20pts/2%202016-03-23%2010%3A39%20%2810.0.0.1%29%3A%5B/root%5Dcat%20/var/log/command.log%0A2016-03-23%2013%3A08%3A09%20client\_102%20root%3A%20%20%5Beuid%3Droot%5D%3Aroot%20pts/2%202016-03-23%2010%3A39%20%2810.0.0.1%29%3A%5B/root%5Dcat%20/var/log/command.log%0A2016-03-23%2013%3A10%3A46%20client\_102%20root%3A%20%20%5Beuid%3Droot%5D%3Aroot%20pts/2%202016-03-23%2010%3A39%20%2810.0.0.1%29%3A%5B/root%5Dvim%20/etc/bashrc%0A%60%60%60%0A%0A%u73B0%u5728%u662F%u628A%u4ED6%u4EEC%u63A8%u9001%u5230%u670D%u52A1%u5668%u7AEF%uFF0C%0A%0A%23%23%20%u96C6%u4E2D%u7BA1%u7406rsyslog%u65E5%u5FD7%0A%u96C6%u4E2D%u7BA1%u7406%u65F6%u4FBF%u9700%u8981%u5728%u670D%u52A1%u7AEF%u5F00%u542F514%20%u7AEF%u53E3%u8FD9%u91CC%u628ATCP%2CUDP%u7684514%u7AEF%u53E3%u90FD%u5F00%u542F%u6765%2C%u5728rsyslog%u4E2D%u628A%u4E0B%u9762%u56DB%u884C%u53BB%u6389%u6CE8%u91CA%0A%60%60%60%0A%24ModLoad%20imudp%0A%24UDPServerRun%20514%0A%23%20Provides%20TCP%20syslog%20reception%0A%24ModLoad%20imtcp%0A%24InputTCPServerRun%20514%0A%60%60%60%0A%0A%u5728%u5BA2%u6237%u7AEF%u4FEE%u6539local.4%u7684%u53D1%u9001%u7AEF%u4E3A%u5982%u4E0B%0A%60%60%60%0Alocal4.\*%20%20%20%20%20%20%20%20@172.16.1.102%3A514%20%20%23%20%u670D%u52A1%u7AEFIP%3A%u7AEF%u53E3%0A%60%60%60%0A%0A