Rsysconf参考手册

时间：2016-8-2

**前言：**

环境：centos7

日志文件配置文件目录 /etc/rsyslog.conf

**一、安装软件方法：**

访问[http://rpms.adiscon.com](http://rpms.adiscon.com/" \t "http://write.blog.csdn.net/postedit/_blank).下载rsyslogall.repo 文件到下面的目录（可以新建rsyslog.repo文件，把内容粘贴到文件中）

/etc/yum.repos.d/

执行下面命令

yum install rsyslog

**二、按设备按日志级别收集日志配置方式**

日志设备.日志级别 日志处理方式

\*.info /var/log/messages（收集所有大于等于info级别的日志）

**三、配置文件解析：**

主配置文件/etc/rsyslog.conf配置文件中有很多内容, 但最主要的是指定需要记录哪些服务和需要记录服务什么等级的信息。  
格式是：日志设备[连接符号]日志级别 日志处理方式(action)  
a)、日志设备(可以理解为日志类型):

|  |
| --- |
| auth            --pam产生的日志  authpriv         --ssh,ftp等登录信息的验证信息  cron            --定时任务  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 |

b)、日志级别,从上到下，级别从高到低，记录的信息越来越少。

|  |
| --- |
| debug        --有调式信息的，日志信息最多  info        --一般信息的日志，最常用  notice      --最具有重要性的普通条件的信息  warning     --警告级别  err         --错误级别，阻止某个功能或者模块不能正常工作的信息  crit        --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        --需要立刻修改的信息  emerg       --内核崩溃等严重信息  none         --什么都不记录 |

c)、连接符号,其中的xxx表示某一日志级别

|  |
| --- |
| .xxx        表示小于等于xxx级别的日志信息  .=xxx       表示等于xxx级别的日志信息  .!xxx       表示在xxx之外的等级的日志信息  .\*         所有等级的日志信息 |

d)、日志处理方式，意思就是将特定的日志做怎样的处理。

|  |
| --- |
| **1. 记录到普通文件或设备文件**  /var/log/file.log   #将日志记录到文件/var/log/file.log  /dev/pts/0       #将日志记录在设备/dev/pts/0  2. 转发到远程的日志服务器  @192.168.0.1    #使用UDP协议转发到192.168.0.1的514(默认)端口  @@192.168.0.1:514  #使用TCP协议转发到192.168.0.1的514端口，tcp的默认端口也是514  **3. 发送给用户(需要在线才能收到)::**  root            #发给root用户  root,kadefor,up01    #使用,号分隔多个用户  \*             #\*号表示所有在线用户  **4. 忽略,丢弃::**  ~             # 忽略丢弃日志  **5. 执行脚本::**  ^/tmp/test.sh       #^号后跟可执行脚本或程序的绝对路径，这个可以用来触发报警动作。 |

e)、举2个栗子  
将mail的所有级别的日志，记录到文件/var/log/maillog中，其中的符号”-“表示使用缓存模式

|  |
| --- |
| mail.\*    -/var/log/maillog |

将所有日志的所有级别的信息采用UDP协议送给远程服务器192.168.186.134一份

|  |
| --- |
| \*.\*  @192.168.186.134 |

**四、三种远程日志传输方式配置**

UDP: 数据包传输可信度不高

TCP: 数据包传输可信度比较高

RELP: 数据包传输可信度最高，避免数据丢失，比较新的协议，

目前应用较少

a）、采用UDP协议

客户端：

\*.\* @172.16.25.1:514

服务端：

# Provides UDP syslog reception

$ModLoad imudp

$UDPServerRun 514

b）、采用TCP协议

客户端：

\*.\* @@172.16.25.1:514

服务端：

# Provides TCP syslog reception

$ModLoad imtcp

$InputTCPServerRun 514

或者

module(load="imtcp")

input(type="imtcp" port="514")

注：这两种配置模式都正确，可以采用其中一种写法，当然也可以混用。

c）、采用RELP协议

客户端：

$ModLoad omrelp #导入omrelp模块

\*.\* :omrelp:172.16.25.1:40000

服务端：

module(load="imrelp")

input(type="imrelp" port="40000")

注意：40000端口号是否可用

**五、模板和过滤配置样例**

日志模板配置：

$template Remote, "/var/log/syslog/%fromhost-ip%/%fromhost-ip%\_%$YEAR%-%$MONTH%-%$DAY%.log"

$template v1, "%syslogseverity%,%syslogfacility%,%timegenerated%,%HOSTNAME%,%syslogtag%,%msg%\n "

日志过滤配置：

:hostname,isequal, "localhost" /var/log/yumhhh.log

:msg,contains,"log" /var/log/yumhhh.log

**六、非系统日志收集**

**使用场景**：假定你已经在机器上安装了一个名为“foobar”的应用程序，它会在/var/log下生成foobar.log日志文件。现在，你想要将它的日志定向到rsyslog服务器，这可以通过像下面这样在rsyslog配置文件中加载imfile模块来实现。别忘了配置完成后重启rsyslog进程哦！

客户端：

module(load="imfile" PollingInterval="5")

input(type="imfile"

File="/var/log/footbar.log"

Tag="foobar"

Severity="error"

Facility="local7"

)

服务端：

不用配置

1. **测试日志产生**

通过logger命令记录日志，logger是一个shell命令接口，可以通过该接口使用Rsyslog的系统日志模块，还可以从命令行直接向系统日志文件写入一行信息。

如何使用参考下面博客：

**<http://blog.csdn.net/u011630575/article/details/52055116>**

**将日志信息传递给rsyslog进程**

logger -p local7.info -t t/a “yumhlocal7a3”

**用于非系统日志收集，将生成的日志信息重定向到/var/log/footbar.log文件**

logger -p local7.info -t t/a “yumhlocal7a3” >/var/log/footbar.log

**疑难解答**

在使用relp协议时，遇到客户端日志信息无法发送到服务端的情况，通过使用网络抓包、跟踪信号调用和信号的方式发现了使用的40000端口被selinux禁止，使用[Selinux管理工具semanage](http://blog.csdn.net/u011630575/article/details/52068959)允许rsyslog进程访问40000端口后，解决该问题。下面是解决该问题过程中使用的工具：

1. **客户端发送的日志信息无法转发到服务端**

**[使用tcpdump网络抓包用](http://blog.csdn.net/u011630575/article/details/48271711)**

如何安装及使用参考下面的博客

<http://blog.csdn.net/u011630575/article/details/48271711>

使用strace[跟踪系统调用和信号](http://blog.csdn.net/u011630575/article/details/52068848)

如何安装及使用参考下面的博客

http://blog.csdn.net/u011630575/article/details/50042163

http://blog.csdn.net/u011630575/article/details/52068848

1. **端口号禁止访问的问题**

[Selinux管理工具semanage](http://blog.csdn.net/u011630575/article/details/52068959)

如何安装及使用参考下面的博客

<http://blog.csdn.net/u011630575/article/details/52068959>

**相关知识点：**

**Logger**

**tcpdump**

**Strace**

**Selinux**

**[semanage](http://blog.csdn.net/u011630575/article/details/52068959)**

**七、mysql数据库配置和日志配置文件连接数据库配置**

①安装数据库，启动数据库(可能还需要其他配置，这里不再赘述)

*# yum install mysql-server # service mysqld start*

②安装rsyslog-mysql驱动

*# yum install rsyslog-mysql*

③查看rsyslog-msyql生成的文件

*# rpm -ql rsyslog-mysql*

/lib64/rsyslog/ommysql.so \\rsyslog连接mysql的驱动模块

/usr/share/doc/rsyslog-mysql-\*.\*\*.\* \\ rsyslog的文档

/usr/share/doc/rsyslog-mysql-\*.\*\*.\*/createDB.sql \\rsyslog的数据库以及表的各项定义，直接导入数据即可使用

④将生成的createDB.sql导入mysql数据库（这里导入的数据库是日志系统默认格式）

# mysql -h 172.16.25.1 -uroot -proot </usr/share/doc/rsyslog-mysql-8.19.0/createDB.sql

Syslog \\生成的数据库名称

SystemEvents [\\存放日志文件的数据库表](\\\\存放日志文件的数据库表)

SystemEventsProperties \\ 生成的日志数据库表

⑤授权rsyslog用户对到导入的数据库有所有权限（此处的设置不唯一）

mysql> **GRANT** **ALL** **ON** Syslog.\* **TO** 'rsyslog'@'127.0.0.1' IDENTIFIED **BY** 'syslogpass'; \\用户授权

mysql> **GRANT** **ALL** **ON** Syslog.\* **TO** 'rsyslog'@'localhost' IDENTIFIED **BY** 'syslogpass';\\用户授权

Query OK, 0 rows affected (0.00 sec)

mysql> FLUSH PRIVILEGES; \\进行权限刷新

Query OK, 0 rows affected (0.00 sec)

⑥编辑/etc/rsyslog.conf配置文件，加载**ommysql**模块，定义将日志信息存储到mysql数据库

***#### MODULES ####***

**$ModLoad ommysql**

***#### RULES ###***

**\*.info;mail.none;authpriv.none;cron.none :ommysql:127.0.0.1,Syslog,rsyslog,syslogpass**

**:模块驱动:数据库地址,数据库名称,数据用户,用户密码**

⑦重启rsyslog服务

***# service rsyslog restart***

⑧在mysql中查看日志信息

mysql> SELECT \* FROM Syslog.SystemEvents\G; 查看日志命令，输出信息如下：

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* 4. row \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

ID: 4

DeviceReportedTime: 2014-12-16 11:51:42

Facility: 1

Priority: 6

FromHost: localhost

Message: Installed: vsftpd-2.2.2-13.el6\_6.1.x86\_64

。。。。。。。。

MaxUsage: NULL

SystemID: NULL4 rows in set (0.00 sec)

⑨到此为止，日志信息已经成功的存储于数据库中，可以便捷的查询相关的日志信息啦

1. **自定义数据库**

参考本人提供的文件：自定mysql数据库和日志模板.txt

数据库名：systemLog

日志信息存储表：logInfo

日志输出模板：log

日志字典表：dict

日志信息提取表：extractLogInfo

表名：logInfo（日志信息存储表）

|  |  |  |  |
| --- | --- | --- | --- |
| **字 段** | **类 型** | **rsyslog对应字段** | **含 义** |
| id | int |  | 自增id |
| timestamp | int | timestamp | 时间戳 |
| fromHostIP | varchar | **fromhost-ip** | IP地址 |
| nodeID | varchar | **fromhost** | 节点名称 |
| syslogfacility | int | **syslogfacility** | 设备标号 |
| syslogfacilityText | varchar | **syslogfacility-text** | 设备名称 |
| syslogseverity | int | **syslogseverity** | 严重性等级标号 |
| syslogseverityText | varchar | **syslogseverity-text** | 严重性等级名称 |
| msg | varchar | **msg** | 日志信息 |

表名：dict（日志字典表）

|  |  |  |
| --- | --- | --- |
| **字 段** | **类 型** | **含 义** |
| ID | int | 自增id |
| msg | varchar | 日志信息 |

表名：extractLogInfo（日志信息提取表）

|  |  |  |
| --- | --- | --- |
| **字 段** | **类 型** | **含 义** |
| ID | int | 自增id |
| msg | varchar | 日志信息 |
| logInfoID | int | 关联logInfo表的ID |
| dictID | int | 关联dict表的ID |

日志输出模板：注意数据项的引号

template(name="logInfo" type="list" option.sql="on"){

constant(value="insert into logInfo(timestamp,fromHostIP,nodeID, syslogfacility,syslogfacilityText, syslogseverity,syslogseverityText, msg)")

constant(value=" values ('")

property(name="timestamp" dateFormat="mysql")

constant(value="',' ")

property(name="fromhost-ip")

constant(value="', '")

property(name="fromhost")

constant(value="', '")

property(name="syslogpriority")

constant(value="', '")

property(name="syslogfacility-text")

constant(value="', '")

property(name="syslogseverity")

constant(value="', '")

property(name="syslogseverity-text")

constant(value="', '")

property(name="msg")

constant(value="')")

}

创建数据库语句:

日志信息存储表

CREATE DATABASE systemLog ;

USE systemLog;

CREATE TABLE logInfo

(

ID int unsigned not null auto\_increment primary key,

timestamp datetime NULL,

fromHostIP varchar(20),

nodeID varchar(30),

syslogfacility int NULL,

syslogfacilityText varchar(20),

syslogseverity int NULL,

syslogseverityText varchar(20),

msg varchar(300),

SystemID int NULL

);

日志字典表

CREATE TABLE dict

(

ID int unsigned not null auto\_increment primary key,

msg varchar(300)

);

日志信息提取表

CREATE TABLE extractLogInfo

(

ID int unsigned not null auto\_increment primary key,

msg varchar(300),

logInfoID int ,

dictID int

);

1. **日志配置测试命令**

该命令用于检测/etc/rsyslog.conf日志配置的正确与否：

**# rsyslogd -f /etc/rsyslog.conf -N1**