

## RHCE 系列（五）：如何在 RHEL 7 中管理系统日志（配置、轮换以及导入到数据库）

2015-11-6 09:53 评论: 2 收藏: 3

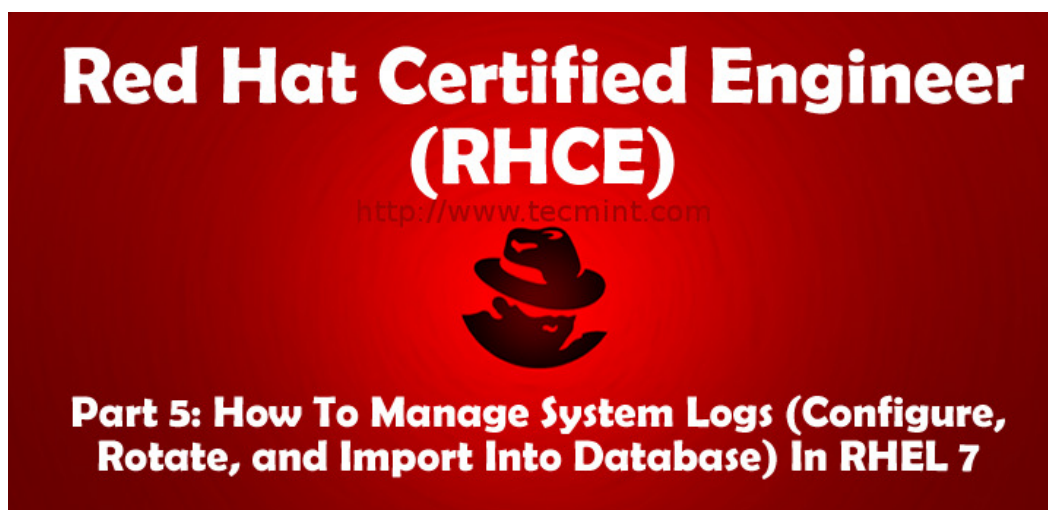
参考原文：<http://www.tecmint.com/manag...>

作者：Gabriel Cánepa

编译文章：LCTT <https://linux.cn/article-6531-1.html>

译者：ictlyh

为了确保你的 RHEL 7 系统安全，你需要通过查看日志文件来监控系统中发生的所有活动。这样，你就可以检测到任何不正常或有潜在破坏的活动并进行系统故障排除或者其它恰当的操作。



RHCE 考试 - 第五部分：使用 Rsyslog 和 Logrotate 管理系统日志

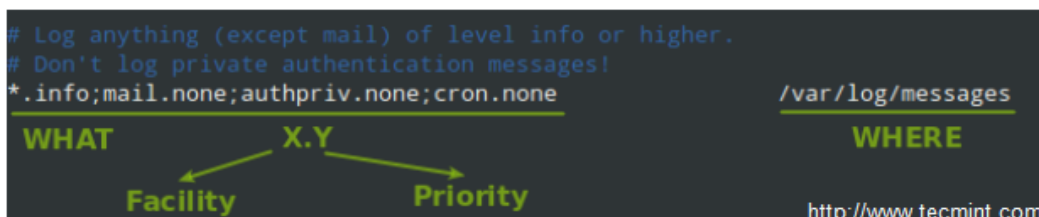
在 RHEL 7 中，`rsyslogd` <<http://www.tecmint.com/wp-content/pdf/rsyslogd.pdf>> 守护进程负责系统日志，它从 `/etc/rsyslog.conf`（该文件指定所有系统日志的默认路径）和 `/etc/rsyslog.d` 中的所有文件（如果有的话）读取配置信息。

### Rsyslogd 配置

快速浏览一下 `rsyslog.conf` <<http://www.tecmint.com/wp-content/pdf/rsyslog.conf.pdf>> 会是一个好的开端。该文件分为 3 个主要部分：模块（`rsyslog` 按照模块化设计），全局指令（用于设置 `rsyslogd` 守护进程的全局属性），以及规则。正如你可能猜想的，最后一个部分指示记录或显示什么以及在哪里保存（也称为 <sup>selector</sup>选择子），这也是这篇文章关注的

重点。

rsyslog.conf 中典型的一行如下所示：



## Rsyslogd 配置

在上面的图片中，我们可以看到一个选择子包括了一个或多个用分号分隔的

Facility:Priority

“设备:优先级”对，其中设备描述了消息类型（参考 RFC 3164 4.1.1 章节

<<https://tools.ietf.org/html/rfc3164#section-4.1.1>>，查看 rsyslog 可用的完整设备列表），优先级指示它的严重性，这可能是以下几种之一：

- debug
- info
- notice
- warning
- err
- crit
- alert
- emerg

尽管 none 并不是一个优先级，不过它意味着指定设备没有任何优先级。

**注意：**给定一个优先级表示该优先级以及之上的消息都应该记录到日志中。因此，上面例子中的行指示 rsyslogd 守护进程记录所有优先级为 info 及以上（不管是什么设备）的除了属于 mail、authpriv、以及 cron 服务（不考虑来自这些设备的消息）的消息到 /var/log/messages。

你也可以使用逗号将多个设备分为一组，对同组中的设备使用相同的优先级。例如下面这行：

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

也可以这样写：

```
*.info;mail,authpriv,cron.none      /var/log/messages
```

换句话说，mail、authpriv 以及 cron 被分为一组，并使用关键字 none。

### 创建自定义日志文件

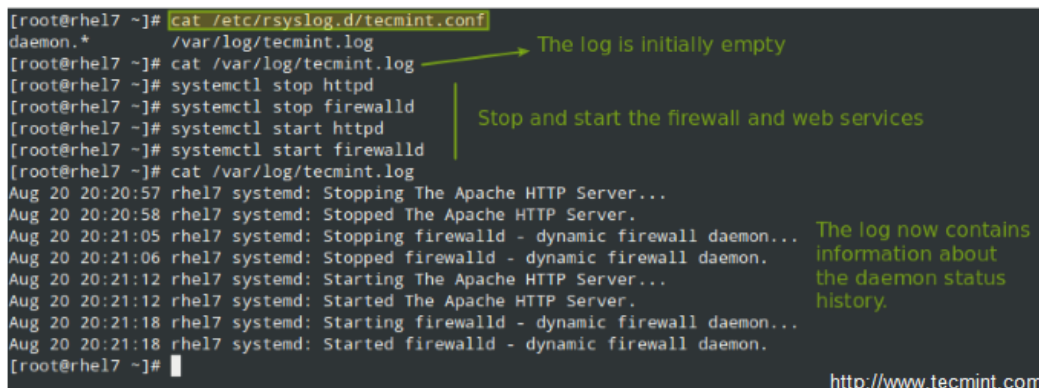
要把所有的守护进程消息记录到 /var/log/tecmint.log，我们需要在 rsyslog.conf 或者 /etc/rsyslog.d 目录中的单独文件（这样易于管理）添加下面一行：

```
daemon.* /var/log/tecmint.log
```

然后重启守护进程（注意服务名称不以 d 结尾）：

```
# systemctl restart rsyslog
```

在随便重启两个守护进程之前和之后查看下自定义日志的内容：



The screenshot shows a terminal session on a RHEL7 system. The user first checks the configuration of the custom log file at /etc/rsyslog.d/tecmint.conf, which contains the line 'daemon.\* /var/log/tecmint.log'. They then verify the log file is empty. Next, they stop and start the httpd and firewall services. Finally, they check the log file again, which now contains detailed messages about the stopping and starting of these services. Annotations with arrows point to the configuration file, the empty log file, the service restart commands, and the updated log content. A URL 'http://www.tecmint.com' is visible at the bottom right of the terminal output.

```
[root@rhel7 ~]# cat /etc/rsyslog.d/tecmint.conf
daemon.* /var/log/tecmint.log
[root@rhel7 ~]# cat /var/log/tecmint.log
The log is initially empty
[root@rhel7 ~]# systemctl stop httpd
[root@rhel7 ~]# systemctl stop firewalld
[root@rhel7 ~]# systemctl start httpd
[root@rhel7 ~]# systemctl start firewalld
[root@rhel7 ~]# cat /var/log/tecmint.log
Aug 20 20:20:57 rhel7 systemd: Stopping The Apache HTTP Server...
Aug 20 20:20:58 rhel7 systemd: Stopped The Apache HTTP Server.
Aug 20 20:21:05 rhel7 systemd: Stopping firewalld - dynamic firewall daemon...
Aug 20 20:21:06 rhel7 systemd: Stopped firewalld - dynamic firewall daemon.
Aug 20 20:21:12 rhel7 systemd: Starting The Apache HTTP Server...
Aug 20 20:21:12 rhel7 systemd: Started The Apache HTTP Server.
Aug 20 20:21:18 rhel7 systemd: Starting firewalld - dynamic firewall daemon...
Aug 20 20:21:18 rhel7 systemd: Started firewalld - dynamic firewall daemon.
[root@rhel7 ~]#
```

http://www.tecmint.com

### 创建自定义日志文件

作为一个自学练习，我建议你重点关注设备和优先级，添加额外的消息到已有的日志文件或者像上面那样创建一个新的日志文件。

### 使用 Logrotate 轮换日志

为了防止日志文件无限制增长，logrotate 工具用于轮换、压缩、移除或者通过电子邮件发送日志，从而减轻管理会产生大量日志文件系统的困难。（译者注：日志轮换

<[https://en.wikipedia.org/wiki/Log\\_rotation](https://en.wikipedia.org/wiki/Log_rotation)>（rotate）是系统管理中归档每天产生的日志文件的自动化过程）

Logrotate 作为一个 cron 任务（/etc/cron.daily/logrotate）每天运行，并从 /etc/logrotate.conf 和 /etc/logrotate.d 中的文件（如果有的话）读取配置信息。

对于 rsyslog，即使你可以在主文件中为指定服务包含设置，为每个服务创建单独的配置文件能帮助你更好地组织设置。

让我们来看一个典型的 logrotate.conf：

```
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# use date as a suffix of the rotated file
dateext

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own wtmp and btmp -- we'll rotate them here
/var/log/wtmp {
    monthly
    create 0664 root utmp
    minsize 1M
    rotate 1
}
```

Global settings  
(apply to all services  
that are logged)

Specific settings for logs  
are enclosed within brackets  
following the log file name

<http://www.tecmint.com>

### Logrotate 配置

在上面的例子中，logrotate 会为 /var/log/wtmp 进行以下操作：尝试每个月轮换一次，但至少文件要大于 1MB，然后用 0664 权限、用户 root、组 utmp 创建一个新的日志文件。下一步只保存一个归档日志，正如轮换指令指定的：

```
[root@rhel7 ~]# ls -lh /var/log | grep wtmp
-rw-rw-r--. 1 root utmp 264K Aug 20 20:20 wtmp
[root@rhel7 ~]#
```

664 Owner and group owner

Since the file is much smaller than 1 MB, it will not be rotated yet.

<http://www.tecmint.com>

### 每月 Logrotate 日志

让我们再来看看 /etc/logrotate.d/httpd 中的另一个例子：

The image consists of two terminal screenshots. The left screenshot shows the configuration of logrotate for httpd logs in /etc/logrotate.d/httpd. The configuration includes settings like missingok, notifempty, sharedscripts, delaycompress, postrotate, and a postrotate script that reloads the httpd service. Annotations with arrows point to the configuration file path, the settings, and the postrotate action. The right screenshot shows the result of the rotation: a directory listing of /var/log/httpd showing various log files like access\_log, access\_log-20150723, error\_log, and error\_log-20150820. A URL 'http://www.tecmint.com' is visible at the bottom right of the right screenshot.

```
[root@rhel7 ~]# cat /etc/logrotate.d/httpd
/var/log/httpd/*log {
    missingok
    notifempty
    sharedscripts
    delaycompress
    postrotate
        /bin/systemctl reload httpd.service > /dev/null
    endscript
}

[root@rhel7 ~]#
```

```
[root@rhel7 ~]# ls -l /var/log/httpd
total 56
-rw-r--r--. 1 root root 1380 Aug 20 20:20 access_log
-rw-r--r--. 1 root root 3863 Jul 23 20:40 access_log-20150723
-rw-r--r--. 1 root root 6210 Jul 27 18:31 access_log-20150727
-rw-r--r--. 1 root root 2947 Aug 3 20:43 access_log-20150803
-rw-r--r--. 1 root root 6157 Aug 20 19:38 access_log-20150820
-rw-r--r--. 1 root root 2278 Aug 20 20:21 error_log
-rw-r--r--. 1 root root 2395 Jul 23 20:40 error_log-20150723
-rw-r--r--. 1 root root 7705 Jul 27 18:31 error_log-20150727
-rw-r--r--. 1 root root 3280 Aug 3 20:43 error_log-20150803
-rw-r--r--. 1 root root 7588 Aug 20 19:38 error_log-20150820

[root@rhel7 ~]#
```

## 轮换 Apache 日志文件

你可以在 logrotate 的 man 手册 ( [man logrotate <http://www.tecmint.com/wp-content/pdf/logrotate.pdf>](http://www.tecmint.com/wp-content/pdf/logrotate.pdf) 和 [man logrotate.conf <http://www.tecmint.com/wp-content/pdf/logrotate.conf.pdf>](http://www.tecmint.com/wp-content/pdf/logrotate.conf.pdf) ) 中阅读更多有关它的设置。为了方便你的阅读，本文还提供了两篇文章的 PDF 格式。

作为一个系统工程师，很可能由你决定多久按照什么格式保存一次日志，这取决于你是否有一个单独的分区/逻辑卷给 `/var`。否则，你真的要考虑删除旧日志以节省存储空间。另一方面，根据你公司和客户内部的政策，为了以后的安全审核，你可能必须要保留多个日志。

## 保存日志到数据库

当然检查日志可能是一个很繁琐的工作（即使有类似 `grep` 工具和正则表达式的帮助）。因为这个原因，rsyslog 允许我们把它导出到数据库（OTB 支持的关系数据库管理系统包括 MySQL、MariaDB、PostgreSQL 和 Oracle 等）。

指南的这部分假设你已经在要管理日志的 RHEL 7 上安装了 MariaDB 服务器和客户端：

```
# yum update && yum install mariadb mariadb-server mariadb-client
rsyslog-mysql
# systemctl enable mariadb && systemctl start mariadb
```

然后使用 `mysql_secure_installation` 工具为 root 用户设置密码以及其它安全考量：

```
Enter current password for root (enter for none): Leave blank and press
OK, successfully used password, moving on... Enter this time

Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

Set root password? [Y/n] y → Enter a password of your choosing
New password:
Re-enter new password:
Password updated successfully! Then continue with the execution
Reloading privilege tables.. of mysql_secure_installation
... Success!

http://www.tecmint.com
```

### 保证 MySQL 数据库安全

注意：如果你不想用 MariaDB root 用户插入日志消息到数据库，你也可以配置用另一个用户账户。如何实现的介绍已经超出了本文的范围，但在 [MariaDB 知识](#) <<https://mariadb.com/kb/en/mariadb/create-user/>> 中有详细解析。为了简单在这篇指南中我们会使用 root 账户。

下一步，从 [GitHub](https://github.com/sematext/rsyslog/blob/master/plugins/ommysql/createDB.sql) <<https://github.com/sematext/rsyslog/blob/master/plugins/ommysql/createDB.sql>> 下载 createDB.sql 脚本并导入到你的数据库服务器：

```
# mysql -u root -p < createDB.sql
```

```
[root@rhel7 ~]# mysql -u root -p < createDB.sql
Enter password:
[root@rhel7 ~]# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 13
Server version: 5.5.41-MariaDB MariaDB Server

Copyright (c) 2000, 2014, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> USE Syslog;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [Syslog]> SHOW TABLES;
+-----+
| Tables_in_Syslog |
+-----+
| SystemEvents     |
| SystemEventsProperties |
+-----+
2 rows in set (0.00 sec)

MariaDB [Syslog]> 
```

<http://www.tecmint.com>

### 保存服务器日志到数据库

最后，添加下面的行到 /etc/rsyslog.conf：

```
$ModLoad ommysql
$ActionOmmysqlServerPort 3306
*. *:ommysql:localhost,Syslog,root,YourPasswordHere
```

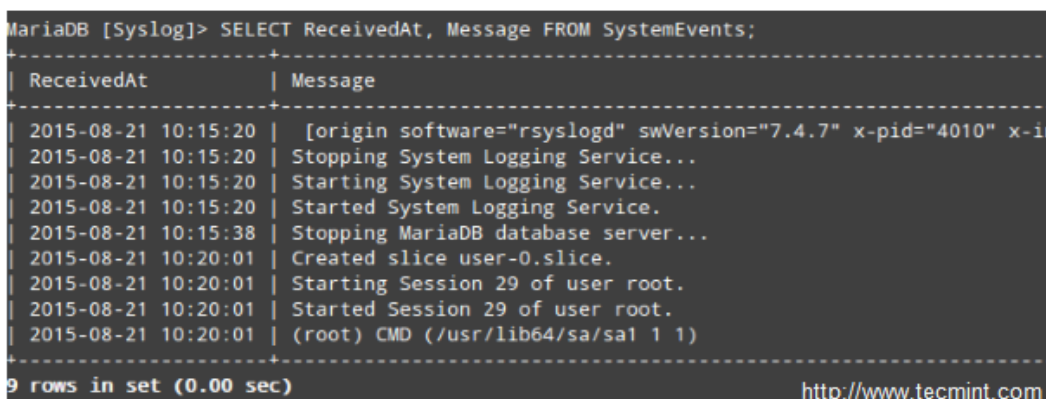
重启 rsyslog 和数据库服务器：

```
# systemctl restart rsyslog
# systemctl restart mariadb
```

使用 SQL 语法查询日志

现在执行一些会改变日志的操作（例如停止和启动服务），然后登录到你的数据库服务器并使用标准的 SQL 命令显示和查询日志：

```
USE Syslog;
SELECT ReceivedAt, Message FROM SystemEvents;
```



```
MariaDB [Syslog]> SELECT ReceivedAt, Message FROM SystemEvents;
+-----+-----+
| ReceivedAt | Message |
+-----+-----+
| 2015-08-21 10:15:20 | [origin software="rsyslogd" swVersion="7.4.7" x-pid="4010" x-i |
| 2015-08-21 10:15:20 | Stopping System Logging Service... |
| 2015-08-21 10:15:20 | Starting System Logging Service... |
| 2015-08-21 10:15:20 | Started System Logging Service. |
| 2015-08-21 10:15:38 | Stopping MariaDB database server... |
| 2015-08-21 10:20:01 | Created slice user-0.slice. |
| 2015-08-21 10:20:01 | Starting Session 29 of user root. |
| 2015-08-21 10:20:01 | Started Session 29 of user root. |
| 2015-08-21 10:20:01 | (root) CMD (/usr/lib64/sa/sa1 1 1) |
+-----+-----+
9 rows in set (0.00 sec)
```

在数据库中查询日志

总结

在这篇文章中我们介绍了如何设置系统日志，如果轮换日志以及为了简化查询如何重定向消息到数据库。我们希望这些技巧能对你准备 RHCE 考试 <<https://linux.cn/article-6451-1.html>> 和日常工作有所帮助。

正如往常，非常欢迎你的反馈。用下面的表单和我们联系吧。

---

via: <http://www.tecmint.com/manage-linux-system-logs-using-rsyslogd-and-logrotate/>



<http://www.tecmint.com/manage-linux-system-logs-using-rsyslogd-and-logrotate/>

作者：Gabriel Cánepa <http://www.tecmint.com/author/gacanepa/> 译者：ictlyh

<http://www.mutouxiaogui.cn/blog/> 校对：wxy <https://github.com/wxy>

本文由 LCTT <https://github.com/LCTT/TranslateProject> 原创翻译，Linux中国

<https://linux.cn/> 荣誉推出