logwatch

可定制和可插入式的日志监视系统

补充说明

logwatch命令 是一个可定制和可插入式的日志监视系统，它通过遍历给定时间范围内的系统日志文件而产生日志报告logwatch默认每天执行一次，可以从`/etc/cron.daily`里看到。

语法

```
logwatch(选项)
```

选项

```
--detail<报告详细程度>：指定日志报告的详细程度；
--logfile<日志文件>：仅处理指定的日志文件；
--service<服务名>：仅处理指定服务的日志文件；
--print打印结果到标准输出；
--mailto<邮件地址>：将结果发送到指定邮箱；
--range<日期范围>：指定处理日志的日期范围；
--archives处理归档日志文件；
--debug<调试等级>：调试模式；
--save<文件名>：将结果保存到指定文件中，而不显示或者发送到指定邮箱；
--logdir<目录>：指定查找日志文件的目录，而不使用默认的日志目录；
--hostname<主机名>：指定在日志报告中使用的主机名，不使用系统默认的主机名；
--numeric在报告中显示ip地址而不是主机名；
--help显示指令的帮助信息。
```

实例

检查你的主机上是否已经存在Logwatch（Redhat默认已经安装了Logwatch（不过版本比较旧）：

```
rpm -qa logwatch
```

如果主机上没有logwatch则执行：

```
rpm -Ivh logwatch***.rpm
```

如果有老版本的logwatch则执行：

```
rpm -Uvh logwatch***.rpm
```

安装完毕后，开始配置：

可以修改和添加它的logfiles（services和其他配置，但默认已经有很多脚本了，只要在1）里设置`Detail = High`就可以了。

- 可以添加新的配置到`/etc/logwatch/conf/logwatch.conf`
- 也可以修改`/usr/share/logwatch/default.conf/logwatch.conf`

`/etc/logwatch/conf/`会自动覆盖`/usr/share/logwatch/default.conf/`下的同名文件。

如果没有设置logwatch.conf也没关系，可以直接在命令行下设置。

```
logwatch --detail High --Service All --range All --print     基本就可以显示出所有日志的情况了
logwatch --service sshd --detail High                        只看sshd的日志情况
```

From:
https://rd.irust.top/ - **学习笔记**

Permanent link:
https://rd.irust.top/doku.php?id=command:logwatch

Last update: **2021/10/15 14:58**