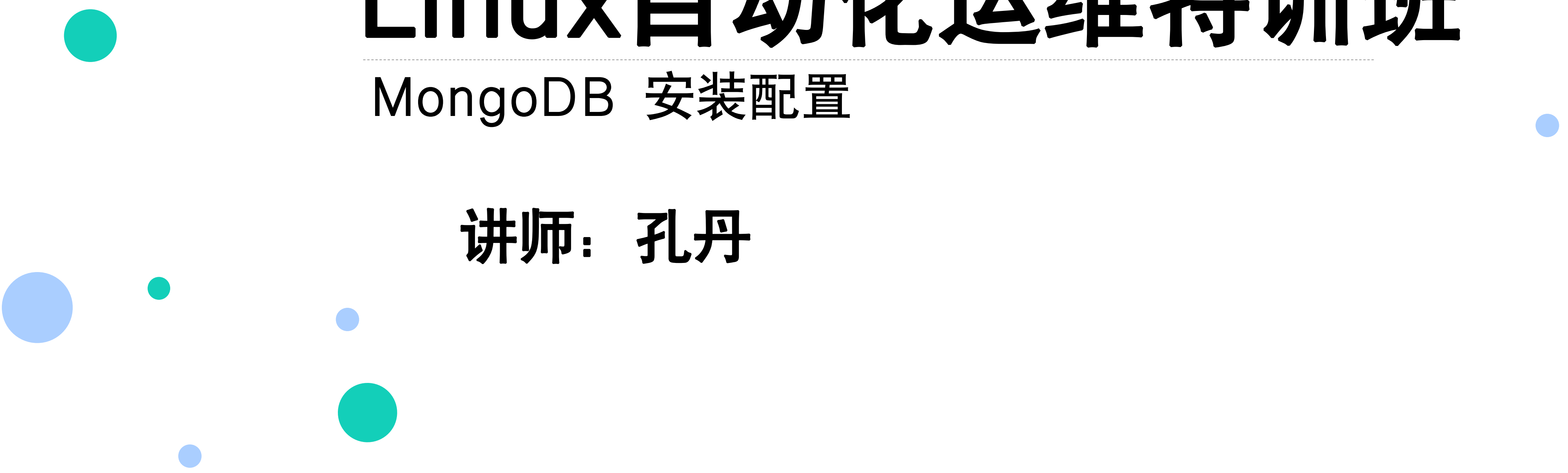




# Linux自动化运维特训班

rsyslog日志管理

讲师：孔丹



# 大纲

- 日志管理简介
- 日志服务 rsyslogd

# 日志简介

## □ 日志相关服务

□ 在 CentOS 6.x 中日志服务已经由 rsyslogd 取代了原先的 syslogd 服务。Redhat 认为 syslogd 已经不能满足在工作中的需求，rsyslogd 相比 syslogd 具有一些新的特点：

- ✓ 基于 TCP 网络协议传输日志信息；
- ✓ 更安全的网络传输方式；
- ✓ 有日志消息的及时分析框架；
- ✓ 后台数据库；
- ✓ 配置文件中可以写简单的逻辑判断；
- ✓ 与 syslog 配置文件相兼容。

# 日志简介

## □ 系统中常见的日志文件

日志文件	说明
/var/log/cron	记录了系统定时任务相关的日志
/var/log/cups/	记录打印信息的日志
/var/log/dmesg	记录了系统在开机时内核自检的信息。也可以使用 dmesg 命令直接查看内核自检信息。
/var/log/btmp	记录错误登录的日志。这个文件是二进制文件，不能直接 vi 查看，而需要使用 lastb 命令查看
/var/log/lastlog	记录系统中所有用户最后一次登录时间的日志。这个文件也是二进制文件，不能直接 vi，而需要使用 lastlog 命令查看
/var/log/maillog	记录邮件信息
/var/log/message	记录系统重要信息的日志。这个日志文件中会记录 Linux 系统的绝大多数重要信息
/var/log/secure	记录验证和授权方面的信息，只要涉及账户和密码的程序都会记录
/var/log/wtmp	永久记录所有用户的登录、注销信息，同时记录系统的启动、重启、关机事件。同样这个文件也是一个二进制文件，不能直接 vi，而需要使用 last 命令来查看。
/var/run/utmp	记录当前已经登录的用户的信息，文件不能直接vi，而需要使用 w，who，users 等命令来查询

# 日志简介

- 除了系统默认的日志之外，采用 RPM 方式安装的系统服务也会默认把日志记录在/var/log/目录中（源码包安装的服务日志是在源码包指定目录中）。不过这些日志不是由rsyslogd 服务来记录 and 管理的，而是各个服务使用自己的日志管理文档来记录自身日志。

比如：/var/log/httpd/ RPM 包安装的 apache 服务的默认日志目录

# 日志服务 rsyslogd

- 日志文件格式
- 只要是由日志服务 rsyslogd 记录的日志文件，他们的格式是一样的。基本日志格式包含以下四列：
  - ✓ 事件产生的时间；
  - ✓ 发生事件的服务器的主机名；
  - ✓ 产生事件的服务名或程序名；
  - ✓ 事件的具体信息。

```
[root@kongd ~]# tail -2 /var/log/messages
```

```
Sep 23 14:01:01 localhost systemd: Started Session 7 of  
user root.
```

```
Sep 23 14:01:01 localhost systemd: Starting Session 7 of  
user root.
```



# 日志服务 rsyslogd

- rsyslogd 服务的配置文件

- /etc/rsyslog.conf 配置文件格式

  - authpriv.\* /var/log/secure

  - #服务名称[连接符号]日志等级 日志记录位置

  - #认证相关服务.所有日志等级 记录在/var/log/secure 日志中

# 日志服务 rsyslogd

## □ 服务

服务名称	说 明
auth ( LOG_AUTH )	安全和认证相关消息 ( 不推荐使用 authpriv 替代 )
authpriv ( LOG_AUTHPRIV )	安全和认证相关消息 ( 私有的 )
cron ( LOG_CRON )	系统定时任务 cront 和 at 产生的日志
daemon ( LOG_DAEMON )	和各个守护进程相关的日志
ftp ( LOG_FTP )	ftp 守护进程产生的日志
kern ( LOG_KERN )	内核产生的日志
local0-local7 ( LOG_LOCAL0-7 )	为本地使用预留的服务
mail ( LOG_MAIL )	邮件收发信息
syslog ( LOG_SYSLOG )	有 syslogd 服务产生的日志信息
user ( LOG_USER )	用户等级类别的日志信息



# 日志服务 rsyslogd

- 连接符号
- 日志服务连接日志等级的格式是：  
日志服务[连接符号]日志等级 日志记录位置
- 在这里连接符号可以识别为：
  - “.” 代表只要比后面的等级高的（包含该等级）日志都记录下来。比如：“cron.info”代表 cron 服务产生的日志，只要日志等级大于等于 info 级别，就记录
  - “.=” 代表只记录所需等级的日志，其他等级的都不记录。比如：“\*.emerg”代表任何日志服务产生的日志，只要等级是 emerg 等级就记录。这种用法及少见，了解就好
  - “.!” 代表不等于，也就是除了该等级的日志外，其他等级的日志都记录。

# 日志服务 rsyslogd

## □ 日志等级:

- debug (LOG\_DEBUG) 一般的调试信息说明
- info (LOG\_INFO) 基本的通知信息
- notice (LOG\_NOTICE) 普通信息, 但是有一定的重要性
- warning (LOG\_WARNING) 警告信息, 但是还不会影响到服务或系统的运行
- err (LOG\_ERR) 错误信息, 一般达到 err 等级的信息以及可以影响到服务或系统的运行了。
- crit (LOG\_CRIT) 临界状况信息, 比 err 等级还要严重
- alert (LOG\_ALERT) 警告状态信息, 比 crit 还要严重, 必须立即采取行动。
- emerg (LOG\_EMERG) 疼痛等级信息, 系统已经无法使用了
- \* 代表所有日志等级, 比如: "authpriv.\*" 代表 authpriv 认证信息服务产生的日志, 所有的日志等级都记录。
- 日志等级这里还可以识别 "none", 如果日志等级是 none, 就说明忽略这个日志服务, 该服务的所有日志都不再记录。

# 日志服务 rsyslogd

## □ 日志记录位置

日志记录位置就是当前日志输出到哪个日志文件中保存，当然也可以把日志输出到打印机打印，或者输出到远程日志服务器上（当然日志服务器要允许接收才行）。日志的记录位置也是固定的。

1、日志文件的绝对路径。最常见的日志保存方法，如“/var/log/secure”就是保存系统验证和授权信息日志的。

2、系统设备文件。如“/dev/lp0”。

3、转发给远程主机。因为可以选择使用 TCP 协议和 UDP 协议传输日志信息，所以有两种发送格式。

1) 如使用“@192.168.0.210:514”，就会把日志内容使用 UDP 协议发送到 192.168.0.210 的 UDP 514 端口上；

2) 如果使用“@@192.168.0.210:514”就会把日志内容使用 TCP 协议发送到 192.168.0.210 的 TCP 514 端口上。

4、用户名。如“root”，就会把日志发送给 root 用户，当然 root 要在线，否则就收不到日志信息了。发送日志给用户时，可以使用“\*”代表发送给所有在线用户，如“mail.\*”就会把 mail 服务产生的所有级别的日志发送给所有在线用户。如果需要把日志发送给多个在线用户，用户名之间用“，”分隔。

# 日志服务 rsyslogd

- 示例：把所有服务的“err”以上的错误都保存在 /var/log/err.log 日志中：

```
[root@kongd ~]# vim /etc/rsyslog.conf  
*.err                                /var/log/err.log
```

重启服务：

```
[root@kongd ~]# systemctl restart rsyslog
```

# 集中日志管理

## □ 日志服务器（开启接收功能）：

```
# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514
```

## □ 日志客户端

```
echo 'mail.info @192.168.101.52:514'>>/etc/rsyslog.conf
```

## □ 测试

```
systemctl restart rsyslog
#发送测试消息
logger -p mail.info "this is a test for remote log."
```

服务端查看：

```
[root@kongd ~]# tail /var/log/maillog -f
Sep 23 15:40:36 localhost root: this is a test for remote log.
```

# 总结

## □ 1.日志的功能。

用于记录系统、程序运行中发生的各种事件  
通过阅读日志，有助于诊断和解决系统故障

## □ 2.日志的分类。

内核及系统日志，由syslog统一管理

用户日志：记录用户登录及退出系统的相关信息

程序日志：由各种应用程序独立管理，记录格式不统一

## □ 3.主要的日志文件。

## □ 4.八种日志消息级别。

EMERG（紧急）、ALERT（警告）、CRIT（严重）、  
ERR（错误）、WARNING（提醒）、NOTICE（注意）、  
INFO（信息）、DEBUG（调试）



# 作业

- ❑ 1.将authpriv设备日志记录到/var/log/auth.log。
- ❑ 2.改变应用程序sshd的日志设备为local5, 并定义local5设备日志记录到/var/log/local5.local。
- ❑ 3.使用logger程序写日志到指定的设备及级别。



# 谢谢观看

更多好课，请关注[万门大学APP](#)

