log分类：

* 系统log：存放系统产生的消息，由syslog统一管理
* 用户log：记录系统用户登录、退出、登录失败等相关信息
* 程序log：由各种应用程序独立管理的log文件，格式不统一。(安装的每个程序都会产生自己的log)

用户log：

* lastlog： 每个用户登录历史
* secure： 用户登录的安全方面
* wtmp： 退出消息
* btmp： 登录失败消息

linux 分析和排查系统故障  
log管理工具： rsyslog （默认运行）

debug：调试，开启后会产生大量调试信息（不管做什么都会产生信息）  
info：消息，一般信息  
err：错误，运行某些内容出现错误

查看当前登入用户：users 、 who  
查看最近登入历史：last  
查看登入失败log：lastb  
查看安全log记录：vim /var/log/secure

**Linux系统故障分析与排查**



[远有青山](https://me.csdn.net/holandstone) 2016-04-11 15:23:51 https://csdnimg.cn/release/phoenix/template/new_img/articleReadEyes.png 8258 https://csdnimg.cn/release/phoenix/template/new_img/tobarCollect.png 收藏 6

分类专栏： [System Analyst](https://blog.csdn.net/holandstone/category_2280957.html)

在处理Linux系统出现的各种故障时，故障的症状是最先发现的，而导致这以故障的原因才是最终排除故障的关键。熟悉Linux系统的日志管理，了解常见故障的分析与解决办法，将有助于管理员快速定位故障点。“对症下药”及时解决各种系统问题。

**日志分析及管理**

日志文件是用于记录Linux系统中各种运行消息的文件，相当于Linux主机的“日记”。不同的日志文件记载了不同类型的信息，如：Linux内核消息，用户登录记录，程序错误等。日志文件对于诊断和解决系统中的问题很有帮助，因为在Linux系统中运行的程序通常会把系统消息和错误消息写入相应的日志文件，这样系统一旦出现问题就会“有据可查”。此外，当主机遭受攻击时，日志文件还可以帮助寻找攻击者留下的痕迹。下面我来对Linux系统中的主要日志及分析管理方法进行介绍。

**1、主要日志文件包括以下三种类型：**

*>内核及系统日志：*这种日志数据由系统服务syslog统一管理，根据其主配置文件"/etc/syslog.conf"中的设置决定将内核消息及各种系统程序消息记录到什么位置。系统中有相当一部分程序会把自己的日志文件交由syslog管理，因而这些程序使用的日志记录也具有相似的格式。

*>用户日志：*这种日志数据用于记录Linux系统用户登录及退出系统的相关信息，包括用户名、登录的终端、登录时间、来源主机、正在使用的进程操作等。

*>程序日志：*有些应用程序运会选择自己来独立管理一份日志文件（而不是交给syslog服务管理），用于记录本程序运行过程中的各种事件信息。由于这些程序只负责管理自己的日志文件，因此不同的程序所使用的日志记录格式可能会存在极大差异。

Linux系统本身和大部分服务器程序的日志文件默认情况下都放置在目录“/var/log”中。一部分程序共用一个日志文件，一部分程序使用单个日志文件，而有些大型服务器程序由于日志文件不至一个，所以会在“/var/log/”目录中建立相应的子目录来存放日志文件，这样既保证了日志文件目录的结构清晰，又可以快速地定位日志文件。有相当一部分日志文件只有root用户才有权限读取，这保证了相关日志信息的安全性。

>>>>>>>>：列表查看"/var/log"目录中的各种日志文件及子目录。

对于Linux系统中的一些常见日志文件，有必要熟悉其相应的用途，这样才能在需要的时候更快地找到问题所在，及时解决各种故障。如：

1. **>**/var/log/messages：记录Linux内核消息及各种应用程序的公共日志信息，包括启动、IO错误、网络错误、程序故障等。对于未使用独立日志文件的应用程序或服务，一般都可以从该文件获得相关的事件记录信息。
2. **>**/var/log/cron：记录crond计划任务产生的事件消息。
3. **>**/varlog/dmesg：记录Linux系统在引导过程中的各种事件信息。
4. **>**/var/log/maillog：记录进入或发出系统的电子邮件活动。
5. **>**/var/log/lastlog：最近几次成功登录事件和最后一次不成功登录事件。
6. **>**/var/log/rpmpkgs：记录系统中安装各rpm包列表信息。
7. **>**/var/log/secure：记录用户登录认证过程中的事件信息。
8. **>**/var/log/wtmp：记录每个用户登录、注销及系统启动和停机事件。
9. **>**/var/log/utmp：记录当前登录的每个用户的详细信息

**2、日志文件分析**

熟悉了系统中的主要日志，我们就针对日志文件的分析方法做了解。分析日志文件的目地在于通过浏览日志查找关键信息，对系统服务进行调试，判断发生故障的原因等。这里主要说三类日志文件的基本格式和分析方法。

对于大多数文本格式的日志格式（如内核及系统日志、大多数的程序日志），只要使用tail、more、less、cat等文本处理工具就可以查看日志内容。而对于一些二进制格式的日志文件（eg：用户日志），则需要使用相应的查询命令。

*>内核及系统日志：*

内核及系统日志功能主要由默认安装的syslogd-1.4.1-39.2软件包提供，该软件包安装了klogd、syslogd两个程序，并通过syslog服务进行控制，分别用于记录系统内核的消息和各种应用程序的消息。syslog服务所使用的配置文件为"/etc/syslog.conf"。

通常情况下，内核及大多数系统消息都被记录到公共日志文件"/var/log/messages"中，而其他一些程序消息被记录到不同的文件中，日志消息还能够记录到特定的存储设备中，或者直接向用户发送。

>>>>>查看日志配置文件"/etc/syslog.conf'中的内容

从配置文件"/etc/syslog.conf“中可以看到，受syslogd服务管理的日志文件都是Linux系统中最主要的日志文件，他们记录了Linux系统中内核、用户认证、邮件、计划任务等最基本的系统消息。在Linux内核中，根据日志消息的重要程度不同，将其分为不同的优先级别（数字等级越小，优先级越高，消息越重要）。

1. **>**0 EMERG(紧急)：会导致主机系统不可用的情况。
2. **>**1 ALERT(警告)：必须马上采取措施解决的问题。
3. **>**2 CRIT（严重）：比较严重的情况。
4. **>**3 ERR（错误）：运行出现错误。
5. **>**4 WARNING(提醒)：可能影响系统功能，需要提醒用户的重要事件。
6. **>**5 NOTICE(注意)：不会影响正常功能，但是需要注意的事件。
7. **>**6 INFO (信息)：一般信息。
8. **>**7 BEBUG(调试)：程序或系统调试信息等。

对于syslog服务统一管理的大部分日志文件，使用的日志记录格式基本上都是相同的，下面以公共日志文件"/var/log/messages"为例来说明内核及系统日志记录的基本格式。

eg：查看公共日志文件"/var/log/messages"的最后两行记录。

日志文件中的每一行表示一条消息，每个消息均由四个字段的固定格式组成。

1. **>**：时间标签：消息发出的日期和时间。
2. **>**：主机名：生成消息的计算机的名称。
3. **>**：子系统名称：发出消息的应用程序的名称。
4. **>**：消息：消息的具体内容。

在有些情况下，可以设置syslog，使其在把日志信息记录到文件的同时将日志信息发送到打印机进行打印，这样无论网络入侵者怎么修改日志都不能清除入侵的痕迹。syslog日志服务是一个常会被攻击的显著目标，破坏了他将会使管理员难以发现入侵以及入侵的痕迹，因此要特别注意监控其守护进程以及配置文件。

*>用户日志*

在wtmp、utmp、lastlog等日志文件中，保存了系统用户登录，退出等相关事件的事件消息。但是这些文件都是二进制的数据文件，不能直接使用tail、less等文本查看工具进程浏览，需要使用who、w、users、last和ac等用户查询命令来获取日志信息。

这里就不再演示。

**3、程序日志**

在Linux系统中，还有相当一部分应用程序并没有使用syslog服务来管理日志。而是由程序自己维护日志记录。例如，httpd网站服务程序使用两个日志文件access\_log和error\_log，一般存放在"/var/log/httpd“目录中，分别记录客户访问事件，错误事件，而FTP服务程序可以将与文件上传，下载事件相关的消息记录在xferlog文件中。由于不同应用程序的日志记录格式差别较大，并没有严格使用统一的格式，这里不详解！

特例：服务器日志分布管理策略：

鉴于日志数据资料的重要性，对于系统运行过程中产生的各种日志文件，必须采用有针对性的管理策略，以确保日志数据的准确性、安全性和真实性。一般来说，可以从以下几个方面进行考虑。

>：日志备份和归档：日志文件也是重要的数据资料，同样需要进行备份和归档。

>：延长日志保存期限：在存储空间富裕的情况下，日志数据保留的时间应尽可能长。

>：控制日志访问权限：日志数据中可能会包含各类敏感信息，如：账号、口令等。所以需要严格控制其访问权限。

>：集中管理日志：使用集中的日志服务器管理各服务器发送的日志记录等。其好处在于方便对日志的收集、整理和分析，杜绝意外的丢失、恶意篡改或删除等。

eg：服务器A（IP地址为173.17.17.3/24），用于集中保存日志记录。

将客户机B（IP地址为173.17.17.11/24）中crond服务产生的日志记录，统一保存到服务器A中的“/var/log/cron”文件中。

* 设置日志服务器A

在日志服务器A中，需要编辑syslog日志服务的启动参数配置文件"/etc/sysconfig/syslog"，将SYSLOGD\_OPTIONS变量的内容改为“-r -x -m 0”即可。其中"-r"选项表示允许接受其他主机发送过来的日志记录，"-x"选项表示不进程DNS域名解析，"-m"表示记录日志的时间标记间隔（设为0禁用该功能），这些信息可以通过查看syslogd程序的man手册页获得

\*：修改日志服务器A的“/etc/sysconfig/syslog”文件，添加集中管理配置参数“-r”，并重启syslog服务。

1. vi /etc/sysconfig/syslog                   //修改SYSLOGD\_OPTIONS行SYSLOGD\_OPTIONS="-r -x -m 0"
2. service syslog restart

* 设置客户机B

在客户机B中，需要修改"/etc/syslog.conf"配置文件，设置将cron计划任务的日志消息写入到服务器A的"/var/log/cron"文件中。指定写入日志的主机地址时，采用“@173.17.17.3”的格式即可。

\*：修改客户机B的"/etc/syslog.conf"文件，找到cron日志的配置行，将日志发送位置改为“@173.17.17.3”，并重启syslog服务。

1. vi /etc/syslog.conf
2. cron.\*                         @173.17.17.3
3. service syslog restart

* 验证日志集中管理功能

在客户机B中执行"crontab -e"命令，随便编写一条计划任务信息并保存退出，然后查看本机中的"/var/log/cron"日志文件，将发现没有任何新的记录。

**4、系统启动类故障排除**

在Linux系统的启动过程中，涉及到哦MBR主引导记录、GRUB启动菜单、系统初始化配置文件、分区挂载配置文件等各方面，其中任何一个环节出现故障都可能会导致系统启动的失常，因此一定要注意做好相关文件的备份功能。下面是一些系统启动类的故障情况:

*> MBR扇区故障*

MBR引导记录位于物理硬盘的第一个扇区（512个字节），该扇区又称为主引导扇区（MBR扇区），除了包含系统引导程序的部分数据以外，还包含了整个硬盘的分区表记录。当主引导扇区发送故障时，将可能无法进入主引导菜单，或者因无法找到正确的分区位置而无法加载系统，通过该硬盘引导主机时很可能进入黑屏状态。

下面将介绍对MBR扇区进行备份、破坏、修复的过程，嘿嘿！

>：备份MBR扇区数据

由于MBR扇区包含了整个硬盘的分区表记录，因此该扇区的备份文件必须存在其他的存储设备中，否则在恢复时将无法读取带备份文件。

使用dd命令将第1块硬盘（sda）的MBR扇区备份到第2块硬盘的sdb1分区中（挂载到/backup目录）

1. mkdir /backup
2. mount /dev/sdb1 /backup
3. dd if=/dev/sda of=/backup/sda.mbr.bak bs=512 count=1

>：模拟MBR扇区故障

仍然使用dd命令，我们人为将MBR扇区的记录覆盖，以便模拟出MBR故障、

1. dd if=/dev/zero of=/dev/sda bs=512 count=1

完成上述操作后重启系统，将会出现"Operating system not found "的提示信息，表示无法找到可能的操作系统，因此无法启动主机。

> 从备份文件中恢复MBR扇区数据

由于MBR扇区被破坏以后，已经无法再从该硬盘启动系统，所以需要使用其他硬盘中的操作系统进行引导，或者直接使用RHEL5系统的安装光盘进行引导。不管使用哪种方式，目地都是相同的：获得一个可以执行命令的Shell环境，以变从备份文件中恢复MBR扇区中的数据，

以使用RHEL5安装光盘引导为例，当出现安装向导的：“boot”提示符时，在后边输入“linux rescue‘并回车，将以”急救模式“引导光盘中的Linux系统。之后一次按回车键接受默认的语言、键盘合适，提示是否配置网卡时一般选择”No’，然后系统会自动查看硬盘中的Linux分区并尝试将其挂载到"/mnt/sysimage"目录（选择“Continue”确认并继续）。接下需要特别输液椅：当出现是否初始化磁盘的警告窗口时如：

一定要选择"No"，以免对硬盘数据造成进一步损坏。

最好选择“OK”确认后进入到带"sh-3.1#"提示符的Bash Shell环境，只要执行相应的命令挂载保存有备份文件的硬盘文件（sdb1），并将数据恢复到硬盘"/dev/sda"中即可。需要注意的是，当前使用的系统环境是光盘中的Linux目录结构。

\*>：确认第1块硬盘的分区情况（已无法获得有效分区表信息，并恢复MBR扇区的数据）。

1. fdisk -l /dev/sda
2. mkdir /tmpdir
3. mount /dev/sdb1 /tmpdir
4. dd if=/tmpdir/sda.mbr.bak of=/dev/sda bs=512 count=1   //恢复备份数据

完成恢复操作以后，执行"reboot"重启主机即可（注意取出RHEL5的安装光盘）。

**5、GRUB引导故障**

GRUB是大多数Linux系统默认使用的引导程序，可以通过启动菜单的方式选择进入不同的操作系统（如果有的话）。当"/boot/grub.conf'配置文件丢失，或者关键配置出现错误，或者MBR记录中的引导程序遭到破坏时，Linux主机启动后可能会出现"grub>“的提示符，无法完成进一步的系统启动过程。

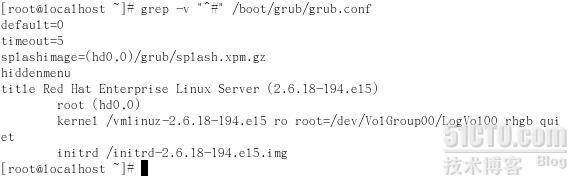
如果在该提示符，可以进行编辑，通过输入对应的引导命令（可以参考”/boot/grub/grub,conf"文件中的配置），再执行"boot'命令也可以进行引导Linux系统。

eg>：通过在"grub>"环境中手动输入引导命令启动Linux系统。

1. grub**>**root (hd0,0)
2. grub**>**kernel/vmlinux-2.6.18-8.e15 ro root=/dev/VolGroup00/LogVo100 rhgb quiet
3. grub**>**inited /initrd-2.6.18-8.e15.img
4. grub**>**boot

之后的启动成功与正常启动RHEL5系统的过程是一模一样的。登录进入系统以后，需要找到配置文件"/boot/grub/grub.conf'，并修复其中的错误，或者直接重建该文件。具体内容可以参考其他正常主机的同名文件。

.>>>>>>>>>：查看grub.conf启动菜单配置文件的主要内容。        grep -v "^#" /boot/grub/grub.conf

[](http://img1.51cto.com/attachment/201307/223322787.jpg)

其中，各主要配置项的含义说明：

>：title：指定在启动菜单中显示的操作系统名称。

>：root：指定包含内核等引导文件的/boot分区所在的位置。

>：kernel：指定内核文件所在的位置，内核加载时权限为只读"ro"，并通过"root="指定根分区设备文件的位置。

>：initrd：指定启动内核所使用的临时系统镜像文件所在的位置。

由于在"grub>"环境中使用的命令较为复杂，而且一般难以记得相关的命令选项，内核加载参数等。因此用户可以采用另一种修复办法，同样使用RHEL5的安装光盘进入急救模式，如果分区表并未被破坏，则急救模式将会找到硬盘中的Linux根分区，并将其挂载到光盘目录结构中的"/mnt/sysimage/"文件夹中。

进入"sh-3.1"的Shell环境以后，执行"chroot /mnt/sysimage"命令可以将目录结构切换到待修复的Linux系统中。然后重新建立新的grub.conf配置文件即可。

eg：确认待修复的Linux系统分区的挂载情况，并重建grub.conf文件。

1. chroot /mnt/sysimage               //切换到待修复的Linux系统根环境。
2. mount
3. .....省略部分内容
4. vi /boot/grub/grub.conf             //重建grub.conf文件，内容就不写了
5. exit                                        //退出chroot环境
6. exit                                         //退出sh-3.1环境，系统会自动重启

在上例中，若为执行"chroot /mnt/sysimage"命令，则重新建立的grub.conf配置文件应该位于"/mnt/sysimage/boot/grub/grub.conf"

如果是MBR扇区中的引导程序出现损坏，可能在重建grub.conf配置文件后仍然无法成功启动系统，这时候可以在救援模式的Shell环境重新安装grub

eg：进入待修复的Linux系统根环境，重新将grub引导程序安装到第一块硬盘（sda）中的MBR扇区中。

1. chroot /mnt/sysimage
2. grub-install /dev/sda
3. exit
4. exit

上述方法同样适用于在Linux主机中那种Windows系统（不覆盖Linux系统）后导致Linux系统无法启动的情况。因为i对于使用双操作系统的主机，后安装的Windows系统将使用自己的引导数据覆盖MBR扇区中的记录，导致开机后不再出现GRUB菜单从而无法进入Linux系统。如果是后安装Linux系统，GRUB程序将会自动识别硬盘中的Window系统并将其加载到GRUB菜单配置中。

*> /etc/inittab文件丢失*

"/etcinittab"文件是系统初始化进程init的配置文件，当该文件被误删或者存在错误配置时，可能导致无法启动系统。丢失"/etc/inittab"文件后，启动后将会出现"INIT：No inittab file found"的错误提示信息。

这类故障同样可以在RHEL5安装光盘的急救模式下进行修复。如果文件配置错误，则进行纠正或者从备份文件中进行恢复即可。默认情况下，如果并未使用chroot命令切换环境，则需要修改的文件"/mnt/sysimage/etc/inittab"。

若inittab文件已经丢失，且没有可用的备份。则需要从RHEL5的光盘目录中重新安装initscript软件包。

eg：在急救模式的"sh-3.1#"环境中挂载RHEL5光盘设备，并重新安装initscript软件包，结合rpm 命令的"--replacepkgs"选项用于替代现有文件。

1. chroot /mnt/sysimage
2. mount /dev/hdc /media/cdrom
3. rpm -vhi --replacepkgs /media/cdrom/Server/initscripts-8.45.14.EL.i386.rpm

在急救模式的Shell环境中通常不再保留cdrom连接文件，而直接通过设备文件"/dev/hdc'使用光盘。安装完毕重启系统即可。

*>  /etc/fstab文件丢失*

"/etc/fstab"配置文件决定了Linux系统在启动后如何加载各分区，例如根分区"/"、"/boot"分区等，若这些分区无法挂载，系统也就无法成功启动。丢失"/etc/fstab"文件后，启动时将会出现如下错误提示信息。

同样使用RHEL5的安装光盘进入急救模式的Shell环境中，由于缺少fstab文件，光盘系统将无法找到待修复的Linux分区，因此必须通过手动的方式查找并挂载根分区，然后重建fstab配置文件后重启系统即可。

eg：在急救模式的Shell环境中扫描逻辑卷组，激活逻辑卷，以便找到根分区设备，然后手动挂载根分区，并重建fstab配置文件。

1. lvm vgscan                                   //查找逻辑卷
2. lvm  vgchange -ay /dev/VolGroup00     //激活找到的逻辑卷
3. mkdir /tmpdir
4. mount /dev/VolGroup00/LogVol00 /tmpdir  //挂载根分区到/tmpdir目录
5. vi  /tmpdir/etc/fstab   //重建fstab配置文件，或直接复制备份的文件

**6、遗忘root用户的密码**

>：通过单用户模式重设root账号的密码（不再说明）；

>：通过急救模式重设root账号的密码

若使用RHEL5的安装光盘进入急救模式的Shell环境，则只需切换到待修复Linux系统的根目录环境，直接执行"passwd root"命令重设root用户的密码即可；或者修改 "/etc/shadow"文件，将root用户的密码字段清空，重启，正常进入系统再修改密码。

eg：在急救模式中，切换到待修复的Linux根分区环境，修改root账号的密码。

1. chroot /mnt/sysimage
2. passwd root
3. ....