**本节所讲内容：**

**1-17-Linux中计划任务与日志的管理**

**1-1 Linux中的计划任务**

* + 1. **at计划任务的使用**
    2. **cron 计划任务的使用**
  1. **Linux服务器的日志管理**
     1. **日志的种类和记录的方式**
     2. **实战-自定义ssh服务的日志存储**
     3. **扩展-日志的回滚**
     4. **实战-搭建rsyslog远程日志服务器**

**计划任务：在某个时段自动执行某个任务。**

**Linux 系统中;**

**At cron**

**at # 只能执行一次**

**语法：**

**at 时间**

**服务：atd 必须开启**

**[root@xuegod60 ~]# systemctl status atd 查看 atd服务的名称**

**● atd.service - Job spooling tools**

**Loaded: loaded (/usr/lib/systemd/system/atd.service; enabled; vendor preset: enabled)**

**Active: active (running) since Mon 2016-02-29 20:27:56 CST; 8min ago**

**启动atd服务**

**[root@xuegod60 ~]# systemctl restart atd #重启atd服务**

**[root@xuegod60 ~]# systemctl enable atd #设置atd服务开机自动启动**

**实战-使用at创建计划任务**

**[root@xuegod60 ~]# date 查看当前的时间**

**Mon Feb 29 20:38:34 CST 2016**

**[root@xuegod60 ~]# at 20:40**

**at> mkdir /root/Linux1605 #输入要执行的命令 .**

**at> <EOT> #按ctrl+D结束**

**job 1 at Mon Feb 29 20:40:00 2016**

**at -l 查看计划任务**

**atq 查看计划任务**

**任务编号 执行的时间 执行者**

**2、也可以这样写： （在某天的某时执行计划任务）**

**[root@xuegod60 ~]# at 20:00 2016-10-1 在某天**

**[root@xuegod60 ~]# at now +10min 在 10分钟后执行**

**对于系统来说 :计划任务　就是在某个特定的时刻　执行一个脚本文件**

**创建成功的at计划任务会在/var/spool/at/目录下成生一个可执行的脚本文件**

**/var/spool/at/\***

**查看/var/spool/at/\***

**每一个脚本都对应一个at计划任务**

**删除at计划任务：**

**atrm　命令**

**atrm + 计划任务的编号**

**[root@xuegod60 ~]# atrm 3　　　　删除编号　是３的计划任务**

**总结　　：at计划任务执行一次,下次就不能再次执行**

**在生产环境中：　　一般都是周期的去执行某个任务　　　例如：备份日志**

**周期性计划任务：**

**ｃｒｏｎ 主程序**

**Crond服务**

**１.系统级别　２，用户级别的计划任务**

**主文件： /etc/crontab**

**[root@xuegod60 ~]# vim /etc/crontab （内容说明）**

**\* \* \* \* \***

**分 时 日 月 星**

**[root@xuegod60 ~]# systemctl status crond （查看crond服务的状态）**

**● crond.service - Command Scheduler**

**Loaded: loaded (/usr/lib/systemd/system/crond.service; enabled; vendor preset: enabled)**

**Active: active (running) since Mon 2016-02-29 20:27:56 CST; 25min ago**

**[root@xuegod60 ~]# systemctl restart crond 重启**

**[root@xuegod60 ~]# systemctl enable crond 开机自启**

**对于系统级别的计划任务，**

**需要执行的命令和脚本都放在这里：  
/etc/cron.\* 按两次tab**

**[root@xuegod60 ~]# ll /etc/cron.**

**cron.d/ cron.daily/ cron.deny cron.hourly/ cron.monthly/ cron.weekly/**

**针对用户级别的计划任务：**

**对于root用户：**

**命令：**

**#crontab –e 创建一个计划任务**

**#crontab –l 显示**

**#crontab –r 删除计划任务**

**#crontab –e #写法**

**分 时 日 月 星 谁做后面的事情 命令**

**每个取值范围：**

**分：0－59**

**小时：0－23**

**日：1－31**

**月：1－12**

**周：0－7 0 7 都是周日**

**#每月9,18,22号这几天的凌晨1点1分，执行一个备份脚本**

**１　１　９,１８,２２　＊　＊ /root/backup.sh**

**#每月9-22号这几天的凌晨1点1分，执行一个备份脚本**

**１　１　９-22　＊　＊ /root/backup.sh**

**#每5分钟，执行一次**

**\*/5 \*＊＊\*　／ｒｏｏｔ／ｂａｃｋｕｐ．ｓｈ**

**anacron**

**cron用控制循环执行例行性工作。如果我要设定机器每早8点进行备份用服务。除非我机器保证在8点这个时间点不会关机，如果关机了，cron中的脚本，在下次开机将不会被执行。**

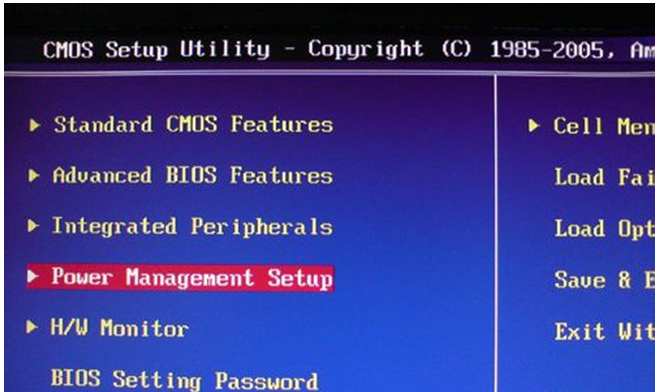
**anacron并没有取代cron的意思，anacron用于，机器重启后，会侦测停机期间，有没有cron没有执行的计划任务，如果有，会立即，执行一下没有执行的任务。**

**明白了吗？**

**实战，定时开机**

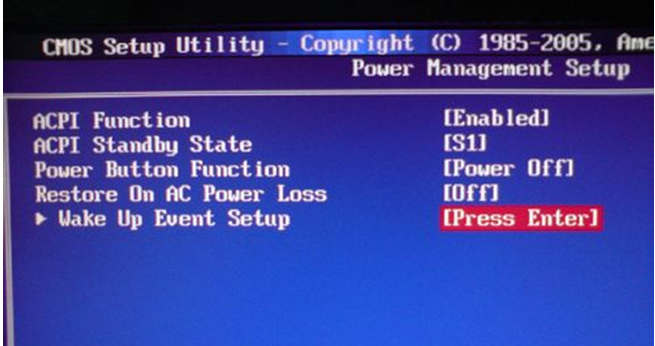
**BIOS**

**进入bios，一般是在开机后出现主板画面是按Delete这个键，部分品牌机可能按F2，F1**



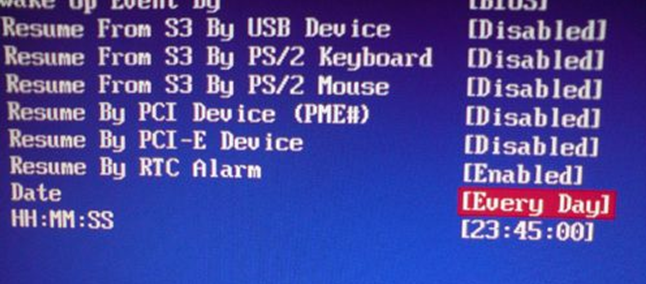
**Power Management Setup，就进入电源管理设置了**

**通过回车进入这个设置后，选择Wake Up Event Setup，回车选择Press Enter**



**最后，在这个界面内继续找到Resume By RTC Alarm，回车选择一下。**

**继续回车选择，将Disabied 更改为Enabled，然后继续回车确定。然后再继续设置时间点和日**



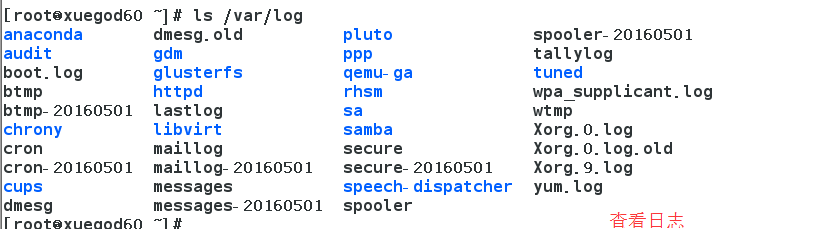
**然后选择日期，并且选择你需要电脑每天需要在几点开机，当然，要保证你的主板时间是准确的。**



1-2 Linux系统中的日志管理

1-2-1 日志的管理

/var/log 存放日志的位置.



　　　　  
**1.cron 计划任务的日志文件 vim cron 查看文件的内容**

**2.secure 验证系统用户登录的日志**

1. **/var/log/wtmp 系统登录的情况登入登出**

**vim 编辑 是加密的内容**

**last 命令🡪查看日志内容**

**哪个用户在哪个时间通过哪种方式登录系统的情况**

**清空日志文件**

**再次使用last查看**

**2./var/log/lastlog 最后登录信息**

**lastlog 记录所有的用户什么时候登录过系统**

**lastlog 和 last的区别**

**last 查看是黑客IP**

**lastlog 查看黑客的后门的账号**

**3./var/log/btmp 用户登录系统的错误信息**

**lastb 查看**

**发现是空的**

**模拟使用ssh错误的连接本机**

**再次查看**

**会产生相应的内容**

**如果说你发现你的btmp文件变得很大,说明有很大的可能是有人在暴力破解你的主机**

**可使用 ll -h 查看文件的大小**

**1-2-2 日志的记录方式:**

**分类🡪 级别🡪**

**日志的种类:**

**daemon 后台进程相关**

**kern 内核产生的信息**

**lpr 打印系统产生的**

**authpriv 安全认证**

**cron 定时相关**

**mail 邮件相关**

**syslog 日志服务本身的**

**news 新闻系统**

**local 0🡪local 7 8个系统保留的类 供其它的程序使用 /或者是用户自定义**

**日志的级别: 轻🡪重**

**debug 排错的信息**

**info 正常的信息**

**notice 注意**

**warn 警告**

**安 装一个软件包查看**

**err 错误**

**crit 关键的错误**

**alert 警报**

**energ 紧急**

**日志服务**

**旧版本 rhel5 服务名称 syslog**

**配置文件 /etc/syslog.conf**

**rhel6-7**

**服务名称 rsyslog**

**配置文件 /etc/rsyslog.conf**

**编辑配置文件 vim /etc/rsyslog.conf**

**#kern.\* 内核类型的所有级别日志 🡪存放到🡪 /dev/console**

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

**所有的类别 级别是info以上 除了mail,authpriv,cron (产生的日志太多,不易于查看)**

**类别.级别**

**authpriv.\* 认证的信息🡪存放🡪 /var/log/secure**

**mail.\* 邮件相关的信息🡪 存放🡪 -/var/log/maillog**

**cron.\* 计划任相关的信息 🡪存放🡪 /var/log/cron**

**local7.\* 开机时显示的信息🡪存放--> /var/log/boot.log**

**-号 邮件的信息比较多,现将数据存储到内存,一定大小,全部写到硬盘.有利于减少I/O进程的开销**

**数据存储在内存,如果关机不当数据消失**

**日志输入的规则**

**. info 高于info级别的信息全部记录到某个文件**

**.= 级别 仅记录等于某个级别的日志**

**例:.=info 只记录info级别的日志**

**.! 级别 除了某个级别意外,记录所有的级别信息**

**例.!err 除了err外 记录所有**

**.none 指的是排除某个级别**

**wall 输出信息 到屏幕**

**wall +内容**

**1-2-3 自定义ssh服务的日志**

**编辑文件 vim /etc/rsyslog.conf**

**输入**

**local 0 .\* /var/log/sshd.log 日志的保存路径**

**定义ssh服务的日志级别**

1. **编辑sshd服务的主配置文件vim /etc/ssh/sshd\_config**
2. **/定位查找 关键字Syslog**



**默认的时候ssh的日志保存在**



**更改级别是local 0 ,保存退出**

**SyslogFacility local0**

1. **重启sshd rsyslog服务**

**systemctl restart rsyslog.service**

**systemctl restart sshd**

1. **查看/var/log 出现 sshd.log**
2. **查看/var/log/sshd.log内容**

**时间 主机 服务 进程ID 相关的信息**

**如何防止日志被黑客删除**

**chattr +a /var/log/sshd.log**

**lsattr /var/log/sshd.log**

**日志的回滚**

**在linux下的日志会定期进行回滚，**

**控制系统执行日志回滚操作的配置文件主要有**

**/etc/logrotate.conf 以及 /etc/logrotate.d/ 这个目录下的明细配置文件。**

**日志是很大的,如果让日志无限制的记录下去 是一件很可怕的事情**

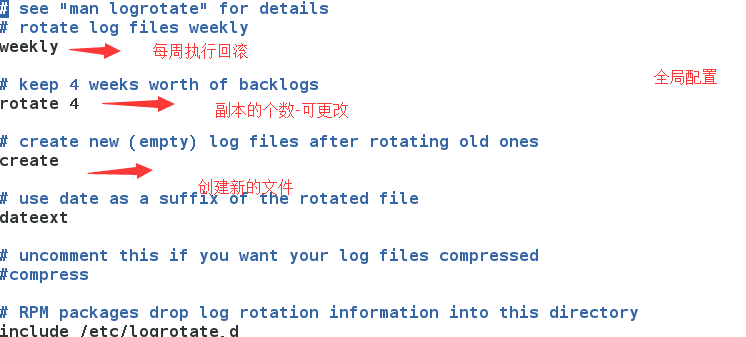
**日积月累 就有几百兆 占用磁盘的空间**

**如果你要找出某一条可用信息🡪海底捞针**

**日志回滚原理:当日志达到某个特定的大小,我们将日志分类,之前的日志保留一个备份,再产生的日志创建一个同名的文件保存新的日志.**

**实战🡪**

1. **编辑配置文件/etc/logrotate.conf**



**weekly : 每周执行回滚**

**rotate : 保留4个副本**

**create : 创建新的文件存储数据**

1. **单独配置**

**/var/log/wtmp { 指定的日志文件**

**monthly**

**create 0664 root utmp**

**minsize 1M 文件超过1M🡪进行回滚**

**rotate 1 回滚产生的副本**

1. **old文件**



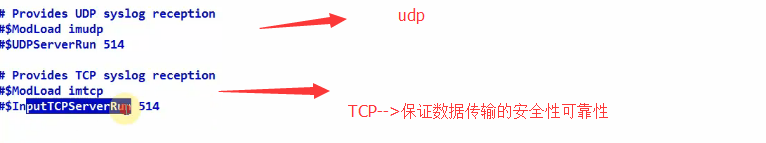
**配置远程日志服务器->实现日志集中的管理**

**server xuegod60**

**client xuegod61**

**server端配置**

**1,编辑 /etc/rsyslog.conf**



**UDP🡪速度快🡪不保证数据的完整**

**TCP🡪可靠.完整**

**使用TCP的方式**

**去除#号注释**

1. **重新启动 rsyslog**

**systemctl restart rsyslog**

1. **查看服务监听的状态**

**netstat -anlpt| grep 514**

**client端配置:**

**vim/etc/rsyslog.conf**



**\*.\* 所有类别和级别的日志**

**@@192.168.1.60:514 服务端的IP:端口**

**重启rsyslog 服务**

**systemctl restart rsyslog**

**服务端验证:**

**关闭防火墙**

**tail -f /var/log/message 动态的**

**client 重启服务**