**linux /etc/security/limits.conf的相关说明**

linux limits.conf 配置 limits.conf 文件实际是 Linux PAM（插入式认证模块，Pluggable Authentication Modules）中 pam\_limits.so 的配置文件，而且只针对于单个会话。

limits.conf的格式如下：

username|@groupname type resource limit

username|@groupname：设置需要被限制的用户名，组名前面加@和用户名区别。也可以用通配符\*来做所有用户的限制。

type：有 soft，hard 和 -，soft 指的是当前系统生效的设置值。hard 表明系统中所能设定的最大值。soft 的限制不能比har 限制高。用 - 就表明同时设置了 soft 和 hard 的值。

resource：

core - 限制内核文件的大小

date - 最大数据大小

fsize - 最大文件大小

memlock - 最大锁定内存地址空间

nofile - 打开文件的最大数目

rss - 最大持久设置大小

stack - 最大栈大小

cpu - 以分钟为单位的最多 CPU 时间

noproc - 进程的最大数目

as - 地址空间限制

maxlogins - 此用户允许登录的最大数目

要使 limits.conf 文件配置生效，必须要确保 pam\_limits.so 文件被加入到启动文件中。查看 /etc/pam.d/login 文件中有：

session required /lib/security/pam\_limits.so

按下面说的,可以用ulimit -n 32768设置最大描述符,不过只对当前会话有用,而且要root,这个不好办

或者修改/etc/security/limits.conf,但要重启

另外,没查到linux究竟最大描述符有没有限制,其他几个限制要不要改

http://www.nsfocus.net/index.php?act=magazine&do=view&mid=134

如何限制和监视用户

PAM 大多数的LINUX都内建了PAM支持。PAM的一个功能是系统环境设置，例如设置某个用户允许使用的系统内存大小等。在Red Hat和Caldera这

两个发行版本的 /etc/security/ 目录下包含了许多可配置文件。最有趣的当属 /etc/security/limits.conf 文件，它允许你定义用户或用户

组规则，规则是“软(soft)”或“硬(hard)”，规则的内容（如CPU、内存、最大文件大小等）。例如：

\*    hard    core    0

bob    soft    nproc    100

bob    hard    nproc    150

第一行规则禁止所有人产生core文件，第二行规则（软）定义用户bob的最大进程数为100， 第三行规则（硬）定义用户bob的最大进程数为150

。可以超出软规则的限制（警告），但不 能超过硬规则的限制。你可以想像得到，这些规则定义到所有用户的登录SHELL和FTP等服务 时是很

有帮助的。

Bash

Bash内建了一个限制器"ulimit"。注意任何硬限制都不能设置得太高，因此如果你在/etc/profile或用户的 .bash\_profile （用户不能编辑或

删除这些文件）中定义了限制规则，你就能对用户的Bash shell实施限制。这对于缺少PAM支持的LINUX旧发行版本是很有用的。你还必须确保

用户不能改变他们的登录shell。限制的设置与PAM相似。例如：

ulimit –Sc 0

ulimit –Su 100

ulimit –Hu 150

http://www.ringkee.com/jims/read\_folder/books/LinuxHackingExposed

Ulimit命令

设置限制     可以把命令加到profile文件里，也可以在/etc/security/limits.conf文件中定义

限制。

命令参数

-a      显示所有限制

-c      core文件大小的上限

-d      进程数据段大小的上限

-f      shell所能创建的文件大小的上限

-m     驻留内存大小的上限

-s      堆栈大小的上限

-t      每秒可占用的CPU时间上限

-p     管道大小

-n     打开文件数的上限

-u     进程数的上限

-v     虚拟内存的上限

除可用Ulimit命令设置外，也可以在/etc/security/limits.conf文件中定义限制。

domino type item value

domino是以符号@开头的用户名或组名，\*表示所有用户，type设置为hard or soft。item指

定想限制的资源。如cpu,core nproc or maxlogins

。value是相应的限制值。

http://tech.blogchina.com/123/2005-06-10/372941.html

Unix、Linux下常用监控和管理命令工具

检查编写的程序打开的文件数。

　　sysctl：显示（或设置）系统内核参数

　　sysctl -a 显示所有内核参数

　　sysctl -w 参数名=参数值

　　例如：sysctl -w fs.file-max=10240 设置系统允许同时打开的最大文件数为10240。

　　内核参数fs.file-nr包括三个参数值，第一个参数表示系统中曾经同时打开过的文件数峰值，

　　第二个参数表示空闲（分配后已释放）的文件数，

　　第三个参数表示可以打开的最大文件数，其值等于fs.file-max。

　　当前打开的文件数 = 第一个参数值 - 第二个参数值

　　例如：

　　fs.file-nr = 977 223 10240

　　当前打开的文件数 = 977 - 233 = 744

　　设置内核参数时务必小心，如果设置不当会导致系统异常，甚至当机。

　　ulimit：显示（或设置）用户可以使用的资源限制

　　ulimit -a 显示用户可以使用的资源限制

　　ulimit unlimited 不限制用户可以使用的资源，但本设置对可打开的最大文件数（max open files）

　　和可同时运行的最大进程数（max user processes）无效

　　ulimit -n <可以同时打开的文件数> 设置用户可以同时打开的最大文件数（max open files）

　　例如：ulimit -n 8192

　　如果本参数设置过小，对于并发访问量大的网站，可能会出现too many open files的错误

　　ulimit -u <可以运行的最大并发进程数> 设置用户可以同时运行的最大进程数（max user processes）

　　例如：ulimit -u 1024

http://www-128.ibm.com/developerworks/cn/linux/es-JavaVirtualMachinePerformance.html?ca=dwcn-newsletter-linux

IBM JVM for Linux on POWER 的性能调优技巧

用户限制设置

为了获得最佳性能，让运行 JVM 进程的用户拥有经过正确配置的用户设置是很重要的。这些参数可以设置成以下两种形式之一：

暂时地，适用于通过 ulimit 命令登录 shell 会话期间。

永久地，通过将一个相应的 ulimit 语句添加到由登录 shell 读取的文件之一（例如 ~/.profile），即特定于 shell 的用户资源文件；或者

通过编辑 /etc/security/limits.conf。

建议设置成无限制（unlimited）的一些重要设置是：

数据段长度：ulimit –d unlimited

最大内存大小：ulimit –m unlimited

堆栈大小：ulimit –s unlimited

CPU 时间：ulimit –t unlimited

虚拟内存：ulimit –v unlimited

对于需要做许多套接字连接并使它们处于打开状态的 Java 应用程序而言，最好通过使用 ulimit –n，或者通过设置

/etc/security/limits.conf 中的 nofile 参数，为用户把文件描述符的数量设置得比默认值高一些。

提高 Oracle 用户的 shell 限制

/etc/security/limits.conf

oracle soft nproc 2047

oracle hard nproc 16384

oracle soft nofile 1024

oracle hard nofile 65536

/etc/pam.d/login

session required /lib/security/pam\_limits.so

/etc/profile

if [ $USER = "oracle" ]; then

if [ $SHELL = "/bin/ksh" ]; then

ulimit -p 16384

ulimit -n 65536

else

ulimit -u 16384 -n 65536

fi

fi