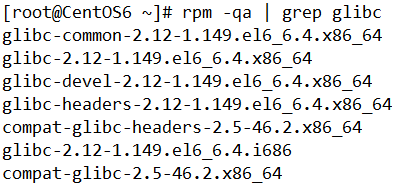
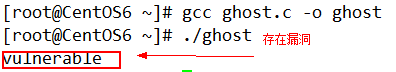
1）漏洞检测

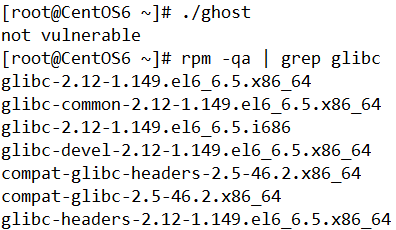
未升级前版本



执行ghost，显示“vulnerabe”为存在幽灵漏洞，需升级更新。

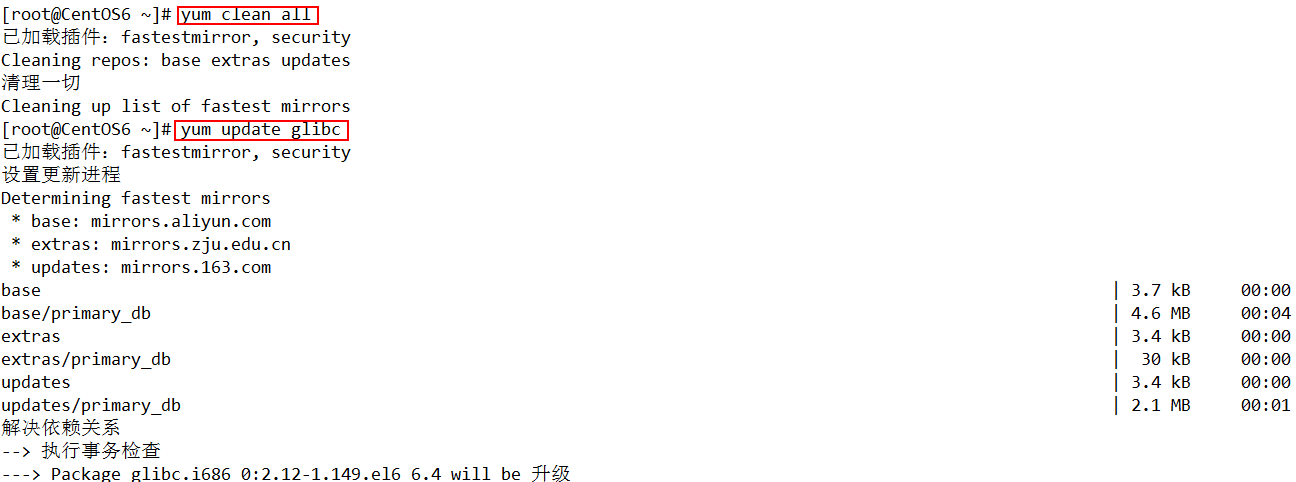


升级后可执行同样方法进行验证

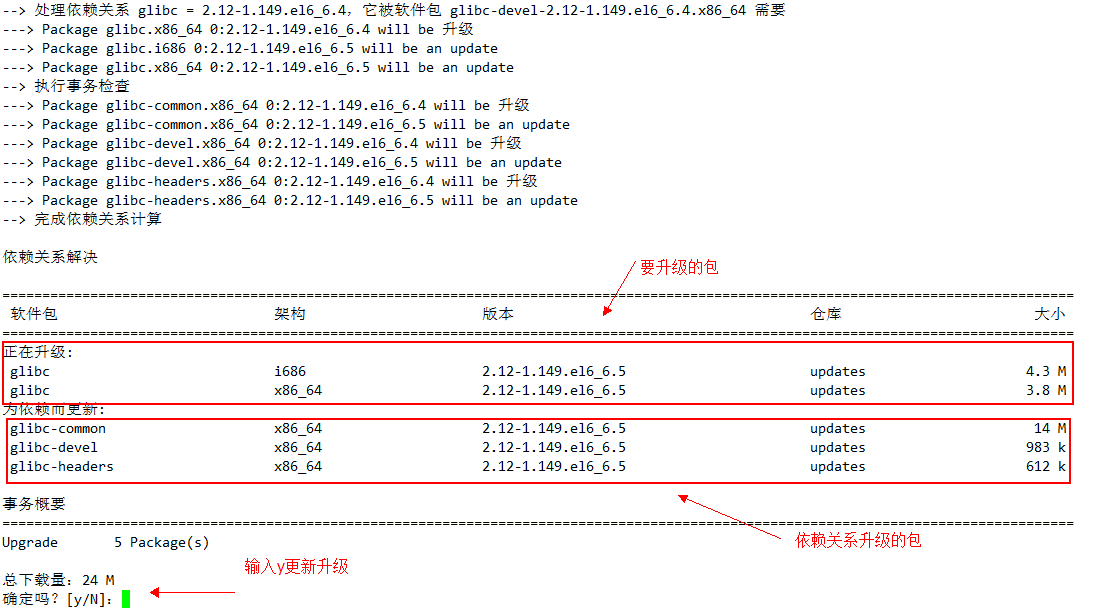


2）yum在线升级

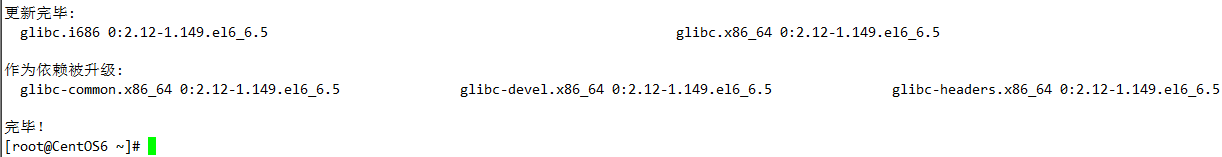
在可以连接互联网，操作系统为CentOS、RHEL已经注册或RHEL已经卸载原来yum并安装其他开源yum的情况下，可以使用yum在线升级。应先执行# yum clean all，再# yum update glibc。（部分yum源无法升级的可更换其他yum源尝试）



yum会自动搜索与glibc关联的包，并提示是否升级安装。



提示升级成功



3）离线升级

大部分linux系统不能上网或部署的是RHEL未注册版本，所以无法yum了，只能下载包离线安装。可以通过镜像上下载glibc及其关联包，而后进行升级。当前RHEL版本升级包，RHEL5的下载路径都在形如：http://xxxx.com/centos/5.11/updates/下，RHEL6的下载路径都在形如：http://archive.kernel.org/centos-vault/6.9/updates/x86\_64/Packages/下（也可以用yumdownloader工具统一下载补丁包。执行# yum install --downloadonly --downloaddir=/tmp glibc）。

当然下载安装前需区分系统版本位数，执行# file /sbin/init。

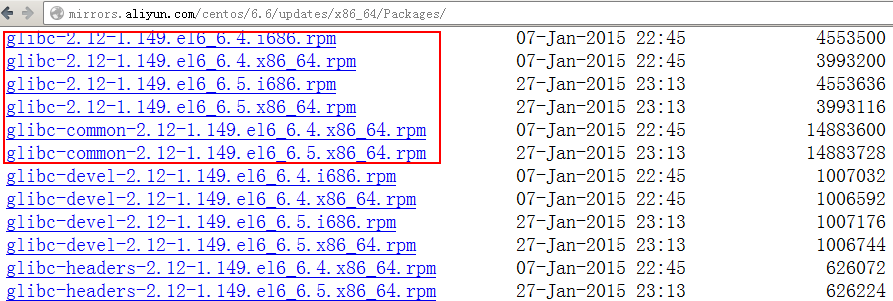
位数



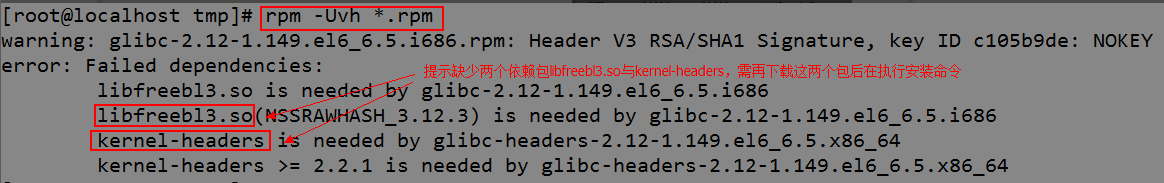
版本



下载地址



把.rpm包上传到系统的同一路径下，通过# rpm **-Uvh** \*.rpm，进行**更新**安装（**\*.rpm时确保当前目录下没有其他无法.rpm的包，避免错误安装了其他包**）。如果还有关联包不存在，系统会给与提示，重新到网络上下载并上传再统一安装即可。（不同系统系统依据安装的软件不同，依赖包也会不一样）



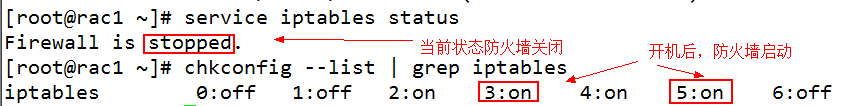
## 四、重启系统

升级完glibc，最好要重启相应的操作系统。如果暂时无法重启，也应该重启与glibc有关的重要应用服务。（**重启应先数据库服务器，再应用系统服务器，避免应用系统二次重启。）**



上图就表示httpd命令有用到glibc

linux运维中存在管理员设置的临时性参数，在操作系统重启后就失效了，这样就容易导致业务系统在重启后，无法正常运行，需要重启配置这些参数。例如：



因此重启前需要与系统管理员、以及应用研发人员进行沟通，确认是否存在这样的参数配置，建议让管理人员自己进行系统关闭重启操作。（彻底解决的方法是执行Linux开机脚本化或参数写实到配置文件里）

## 注意事项

* RHEL 4版本由于发行超过10年，已经没有发布安全补丁包，且glibc是很基础的库，不建议进行其他方法升级，容易出问题。从安全考虑，建议升级操作系统到5及以后版本。
* 当然如果无法yum的服务器很多（如几百台），可以搭个本地源再进行过yum升级。
* **升级前检查是否有定制的系统软件，如果有的话建议和开发人员联系是否可以升级。**
* **应该在测试服务器上先测试通过，如有集群服务器的，先升级一台，再升级其他服务器。**