教你配置Linux操作系统安全管理服务 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/260/2021_2022__E6_95_99_E4_BD_A0_E9_85_8D_E7_c103_260893.htm 任何计算机安全措施的一个重要方面是维持实际控制服务的运行。本文向你展示了在Linux操作系统的PC机上如何配置安全服务管理。 任何计算机安全措施的一个重要方面是维持实际控制服务的运行，让不必要的网络服务接受请求将提高系统的安全风险。即使这些网络服务对于服务器的某些功能是必要的也需要仔细管理，并且对其进行配置最小化不受欢迎的入侵和登录的可能性。 为Linux系统配置安全性时，使用/etc/inittab文件、runlevels和一两个服务管理“ superdaemons ”如inetd或xinetd直接管理服务。 inittab /etc/inittab文件用于系统的初始化过程启动系统服务。在一个配置好的系统上，虽然它一般都不会包括很多服务，但是在某些Linux系统的默认安装中会加载很多其他服务。/etc/inittab文件内容有些模糊，它的重要之处在于让服务管理变得相对简单。 首先，可不要通过/etc/inittab文件方式向系统启动项中添加服务。 第二，不要移除/etc/inittab文件中第一个冒号之前其第一个字段是单精度型的数字，或整个登录服务的前面部分。以单精度数字开头的行可以打开TTY控制台，所有服务在它们打开之前都一一列出，甚至列出其更重要的功能。也许有些例外情况，在不改动它时是很安全的，尤其如果不确定的情况下请不要改动。 第三，/etc/inittab在导入和runlevel选择的时候用于过程管理。一般不用于正常的系统操作。 第四，在导入时由rc系统开始添加步骤，而不是init系统。如果看看/etc/inittab的内容，将会注意

到登录以rc0到rc6这样的字符结束。这是初始化系统如何处理runlevels的说明。 Runlevels 基于Linux操作系统的运转可以通过Runlevels进行管理。不同的Runlevels被定义成有不同的行为，就像Windows操作系统一样，它有正常操作模式、安全模式、在某些情况下还有DOS模式。 Runlevel 0用于关闭系统，如果软电源设置恰当，它能关闭系统电源。 Runlevel 1是单用户无网络的模式，它用于低水平的故障修复和管理操作。Runlevel 2到Runlevel 5正常系统操作的多用户模式。Runlevel2和3是命令行模式，3有网络连接而2没有网络连接。Runlevel 5用于启动X Windows提供图形用户接口。 Runlevel 6用于系统重启，当整个init系统甚至bootloader 需要重启时采用它。 其他Runlevels由系统管理员进行定义，但是“ 传统 ”Unix系统没有此功能。这种情况下，他们不能被定义也不能被使用。在shell处，可以输入runlevel命令找到以前的renlevel和当前runlevel。如果没有更改系统 runlevel ，命令的输出结果为大写N后面跟runlevel的数字，这里的N表示没有前runlevel，如果要更改runlevel，可以使用init命令，后面跟想要使用到的runlevel的数字。例如，输入init 6表示重启系统，或init 1 进入单用户模式。 配置Runlevel的过程每一版本的情况都不同。例如，在Debian GNU/Linux系统中，位于/etc/init.d的服务脚本有来自/etc/rcN.d的路径与它们进行链接，这里的N表示需要配置的Runlevel数字。以字母K开头的symlinks指示在进入Runlevel时被杀死的程序，而以字母 S开头的symlinks指示在进入Runlevel时被启动的程序。字母后面的数字值越大，从1到99，表示启动或杀死的时间愈靠后。 大多数基于RPM的版本都采用RedHat所用到的rc系统。比起基于Debian的系统，

这一系统使用更复杂的路径结构，并且不同的基于RPM的系统之间也有很大的不同。说明书上提供了更多的关于管理Runlevel的信息。 inetd 一个用于Linux后台程序管理的“ superdaemon ”是众所周知的inetd，它是个用于服务管理的命令行工具。终止服务很简单:首先，作为根用户用文本编辑器打开/etc/inetd.conf文件。接下来，找到文件中需要终止的服务。最后，在服务所在行的最前面添加#符号(其他还有“ 尖顶符 ”和“ 英镑符 ”)，如下所示。“ 注释掉 ”这一行，因此inted以后都不会启动这一服务。 编辑之前服务登录可能是下面这样: ident stream tcp wait identd /usr/sbin/identd identd 停止之后，服务登录变成下面这个样子: # ident stream tcp wait identd /usr/sbin/identd identd 如果正在卸载被登录参考的后台程序，可以删除文件中的某些行是否通过包管理器进行卸载或删除执行文件卸载(对于上面的例子是/usr/sbin/identd文件)。 