Linux系统中内部和外部安全性概述 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/145/2021_2022_Linux_E7_B3_BB_E7_BB_c103_145034.htm 简介 维护一个完全安全的系统是不可能的。然而，只要勤奋，则有可能使 Linux 机器足够安全，并让大多数偶尔出现的骇客、脚本小子（script-kiddies）以及其它的“ 坏家伙 ”止步而去骚扰其他人。请记住：仅仅遵循本教程不会产生一个安全的系统。相反，我们希望您接触到主要主题的多个方面，并向您提供一些有关如何入门的有用示例。 Linux 系统安全性可分为两个部分：内部安全性和外部安全性。内部安全性指预防用户无意或恶意地破坏系统。外部安全性指防止未授权用户获得对系统的访问。 本章将首先介绍内部安全性，然后介绍外部安全性，最后介绍一些常规指导原则和技巧。 日志文件的文件权限 内部安全性可以是很大的任务，这要看您对用户的信任程度。这里介绍的指导原则是设计用来防止偶然用户访问敏感信息和防止不公平地使用系统资源。 至于文件权限，您可能希望修改以下三种情况的权限： 首先，/var/log 中的日志文件不需要是所有人都可以读取的。没有理由让非 root 用户窥视日志。为了创建具有适当权限的日志。 root 用户其它文件的文件权限 其次，root 用户的点文件对于普通用户应是不可读的。检查 root 用户主目录中的文件（ls -la）以确保它们受到适当的保护。甚至可以使整个目录仅对 root 用户可读： # cd# pwd/root# chmod 700 .用户文件的文件权限 最后，用户文件在缺省情况下通常被创建为所有人可读。那可能不是用户所期望的，而且它当然不是最好的策略。应该使用与下面类似的命令在

/etc/profile 中设置缺省的 umask： if ["$UID" = 0]. then# root user. set world-readable by default so that# installed files can be read by normal users.umask 022else# make user files secure unless they explicitly open them# for reading by other usersumask 077fi应该查询 umask(2) 和 bash(1) 手册页以获取有关设置 umask 的更多信息。请注意：umask(2) 手册页涉及 C 函数，但它所包含的信息也适用于 bash 命令。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com