linux认证:AIX系统文件安全性方面的几点考虑Linux认证考试PDF转换可能丢失图片或格式，建议阅读原文https://www.100test.com/kao_ti2020/586/2021_2022_linux_E8_AE_A4_E8_AF_c103_586585.htm 这篇文章主要讨论在AIX系统上如何检查文件、目录和可执行程序的安全性，以防止可能的安全方面的隐患。 1. 删除垃圾文件 很多程序运行完毕后，会在/tmp目录下留下很多的垃圾文件。AIX系统提供一个命令skulker，它可以删除/tmp目录下的a.out文件、core文件和ed.hup文件。具体的命令执行方式为： # skulker -p 2. 删除无所有者的文件 在AIX系统上如果一个用户被删掉后，原来属于这个用户的文件将变成无所有者的文件。可以用下面命令来找出这些文件： # find / -nouser -ls 如果找出得文件还有用，可将它们指定到已存在的某些用户下。否则就删除这些文件。 3. 管理未授权的远程访问 某些程序使用.rhosts文件访问远程系统。但有时这种做法会被未授权的用户使用。为避免这种情况，可删除.rhosts文件。 在HACMP环境下，.rhosts文件是需要的。这时需要将.rhosts文件的访问权限设为600，并且是所有者是root.system。 可用下面命令查找.rhosts文件： # find / -name .rhosts -ls 4. 监视可执行文件的属性 在监视某些可执行文件之前，需要了解这些文件是如何被使用的。尤其是要监视那些所有者是root，文件方式字中有SUID和SGID设置的文件。 通过以下命令可以找出满足上面条件的所有文件： # find / -perm -4000 -user 0 -ls # find / -perm -2000 -user 0 -ls 保存上面命令的输出结果。定时运行这两条命令，并与保存的结果相比较，看是否有未知的文件出现，以杜绝可能的安全隐患。 5. 管理cron和at运行的后台作业 必须做如下内容： - 确认

只有root用户在cron.allow和at.allow文件里。 - 从目录var/adm/cron中删除cron.deny和at.deny文件。 - 确保cron和at作业的所有者是root并且只能由root可写。 上面所谈的内容对AIX系统在文件方面的安全性有指导意义。在具体考虑使用AIX系统的安全性时，还应该考虑更多方面的内容。 