利用RHEL5来为SELinux做辩护 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/645/2021_2022__E5_88_A9_E7_94_A8RHEL_c103_645611.htm 安全增强Linux(Security Enhanced Linux)，也就是SELinux的推出被称为是IT管理者们确保Linux系统安全和平稳运行的一种可自由支配的强大工具。SELinux是由美国国家安全局(NAS)开发的强制访问控制的实现，目前，SELinux已经被整合到大部分主流Linux版本之中。“ SELinux可以阻止偷窃行为，可以阻止垃圾信息传播并防止“ 蠕虫 ”攻击网站。 ”Red Hat公司的首席软件工程师Dan Walsh说，他同时也是SELinux工程的一名正式参与者。 据Walsh所说，IT管理者们应该让SELinux在数据中心的方方面面随时都处于打开状态。 问题是，如今许多用户都让SELinux处于关闭状态(SELinux已经内置到Red Hat 企业版Linux系统当中)。 SELinux开放源码安全技术在其确保高度安全方面被广泛认可的同时，同时也被认为过于复杂。RHEL 5(Red Hat 企业版Linux 5系统)包含了大量的新工具和管理特征以解决这一问题，但这是否已经太晚了呢? SELinux: 事实与认知“ SELinux最大的问题在于人们对它的认知， ”位于加利福尼亚的Saugus联盟学区的信息服务与技术主管Jim Klein说，“ 它因为早期缺少配置工具和故障排除工具而恶名在先，这正是人们选择关闭它的原因。 ”Klein说，对于SELinux倡导者来说不幸的是，当管理者为系统检查故障时，第一个问题往往是“ SElinux是打开的吗? ”他还说，在他的数据中心SELinux是关闭的，而且除非地区转向使用RHEL5的计划完成，他是不打算让它恢复活动状态的。 尽管如此，Red Hat公司

的Walsh还是说SELinux的“ 复杂性问题 ”会逐渐得到解决。在San Diego举行的Red Hat年度峰会中，Walsh表示他最近分解了SELinux，目前应用安全技术在Red Hat企业版Linux5系统中是默认打开的。RHEL4中也是包含SELinux的，但只有RHEL5出现以后，Walsh和其他SELinux专家才可以放心宣称“ 让SELinux处处打开 ”。“ RHEL4像是该项技术的范例，”Walsh说，“ 我们将其划分为一定数量的域，或者说是15个可由应用程序访问的目标程序组。 ”然而，在RHEL5之中目标程序组达到了200个。Walsh又一次重申，“ RHEL5的目标是让SELinux无处不开。 ” SELinux: 复杂,但故障排解器可以提供帮助 身为作家和SELinux专家的Frank Meyer对SELinux的了解程度可以超越大多数人。 他说：“ 我并不想谴责专门提出‘ 复杂性 ’问题的人。但这种感知的产生是因为SELinux具有保护Linux内核提供的任何事务的能力，而Linux内核本身就很复杂。 ”依Meyer看来，当用户声称SELinux因为太过复杂而不能有效配置时，就相当于在声称他们不能应用Linux内核是因为他们不知道该如何写一个设备驱动程序。“ 从逻辑上来说，这是没有意义的。 ”他说。 为了回应这种感知，Red Hat已经在RHEL5中引入了SELinux故障排解器(Troubleshooter)，故障排解器(Troubleshooter)也被称为故障排解集合(settroubleshoot)，是一个为存取向量高速缓存(AVC)消息监视稽核记录文件的工具。 根据Fedora项目网站所言，用户、系统管理员和开发者经常遇到AVC拒绝的冲突。Fedora项目网站是开展大部分SELinux与Red HatLinux构架测试的地方。当SELinux经过充分调试和合理配置之后，AVC拒绝只会由实际的安全性入侵触发。然而，由于SELinux仍然是新技术，策

略尚处于开发状态，因此大部分的AVC拒绝并不是由实际的安全性入侵引起的。此外，用户尚处于学习配置SELinux的过程中，也是AVC拒绝发生的一个原因。 目前，当AVC拒绝发生时，故障排解器就会运行SELinux插件数据库来寻找匹配，并向用户发送一条包含问题描述和建议方案的消息。像Meyer和Walsh这样的行业观察者认为，这一工具对于帮助用户区分真正问题和虚假警报大有帮助，而区分真正问题和虚假警报正是阻碍SELinux在 IT管理者中应用的主要原因。Klein说，故障排解器是一项受欢迎的附加工具，但对帮助解决SELinux的认知问题来说可能出现得太晚了。他说，故障排解器及其同类是“ 管理者们认真考虑是否重新启用SELinux的出发点， ”但是，“ 困难在于说服那些已经把SELinux看作‘ 所有问题根源 ’的人员不要在问题出现时就简单地把它关闭。 ”Klein说，至今为止，Saugus已经将大部分服务器上的SELinux关闭。在等待SELinux工具和策略的成熟化的过程中，以传统设置作为保证应用程序安全的默认设置。 