RedHatSELinux系统简介及案例分析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_ti2020/645/2021_2022_RedHatSELi_c103_645099.htm 一、SELinux简介 RedHat Enterprise Linux AS 3.0/4.0中安全方面的最大变化就在于集成了SELinux的支持。SELinux的全称是Security-Enhanced Linux，是由美国国家安全局NSA开发的访问控制体制。SELinux可以最大限度地保证Linux系统的安全。至于它的作用到底有多大，举一个简单的例子可以证明：没有SELinux保护的Linux的安全级别和Windows一样，是C2级，但经过保护SELinux保护的Linux，安全级别则可以达到B1级。如：我们把/tmp目录下的所有文件和目录权限设置为0777，这样在没有SELinux保护的情况下，任何人都可以访问/tmp 下的内容。而在SELinux环境下，尽管目录权限允许你访问/tmp下的内容，但SELinux的安全策略会继续检查你是否可以访问。 NSA推出的SELinux安全体系结构称为 Flask，在这一结构中，安全性策略的逻辑和通用接口一起封装在与操作系统独立的组件中，这个单独的组件称为安全服务器。SELinux的安全服务器定义了一种混合的安全性策略，由类型实施 (TE)、基于角色的访问控制 (RBAC) 和多级安全(MLS) 组成。通过替换安全服务器，可以支持不同的安全策略。SELinux使用策略配置语言定义安全策略，然后通过checkpolicy 编译成二进制形式，存储在文件(如目标策略/etc/selinux/targeted/policy/policy.18)中，在内核引导时读到内核空间。这意味着安全性策略在每次系统引导时都会有所不同。 SELinux的策略分为两种，一个是目标(targeted)策略，另一个是严格(strict)策略。有限策略仅针对部分 系统网络服

务和进程执行SELinux策略，而严厉策略是执行全局的NSA默认策略。有限策略模式下，9个（可能更多）系统服务受SELinux监控，几乎所有的网络服务都受控。 配置文件是/etc/selinux/config，一般测试过程中使用“ permissive ”模式，这样仅会在违反SELinux规则时发出警告，然后修改规则，最后由用户觉得是否执行严格“ enforcing ”的策略，禁止违反规则策略的行为。 规则决定SELinux的工作行为和方式，策略决定具体的安全细节如文件系统，文件一致性。 在安装过程中，可以选择“ 激活 ”、“ 警告 ”或者“ 关闭 ”SELinux。默认设置为“ 激活 ”。 安装之后，可以在“ 应用程序 ”“ 系统设置 ”“ 安全级别 ”，或者直接在控制台窗口输入“ system -config- securitylevel ”来打开“ 安全级别 ”设置窗口。在“ SELinux ”选项页中，我们不但可以设置“ 启用 ”或者“ 禁用 ”SELinux，而且还可以对已经内置的SELinux策略进行修改。 SELinux相关命令： ls -Z ps -Z id -Z 分别可以看到文件,进程和用户的SELinux属性。 chcon 改变文件的SELinux属性。 getenforce/setenforce查看和设置SELinux的当前工作模式。 修改配置文件/etc/selinux/config后，需要重启系统来启动SELinux新的工作模式。 二、案例分析 Apache - "Document root must be a directory" 问题？ 有可能和这个问题并发的问题还有 403 Forbidden 禁止访问的问题。 现象描述： 不使用系统默认的/var/www/html作为系统的Document Root，自己新建一个目录后修改 /etc/httpd/conf/httpd.conf 中的配置，然后重起Apache的Daemon，发现Apache无法起动，系统报错： Document root must be a directory 但是，我们设置的DocumentRoot 的确是一个目录，而且apache用户具有可读权限。 另一种情况：

新建一个虚拟目录或文件后，无法访问，显示 Forbidden, 403 Error，但文件或目录有可读 权限。 问题产生的原因： 一开始想来想去想不出为什么，但是给我感觉是权限的问题，用传统的Linux的思维方式来看，权限绝对没 有问题。但是仔细一想，SELinux是不是会有其他安全的设定？ 检查 avcmessage，查看 /var/log/messages文件，发现有类似以下内容的这样一段： Dec 24 17:54:59 hostname kernel: audit(1098222899.827:0): avc: denied{ getattr } forpid=19029 exe=/usr/sbin/httpd path=/var/www/html/about.html dev=dm-0 ino=373900 scontext=root:system_r:httpd_t tcontext=user_u:object_r:user_home_t tclass=file 嘿嘿，问题找到了，果然是SELinux的新特性搞的鬼。我把目录或文件设成了user_home_t类型，因此 apache的进程没有权限，无法访问。针对Apache的进程所使用的SELinux target policy规定了apache的进 程只能访问httpd_sys_content_t类型的目录或文件。 解决办法： 很简单，把目录或文件的策略类型改成 httpd_sys_content_t 就可以了。 # chcon -t httpd_sys_content_t [file_name | dir_name] 然后可以用 ls -laZ 命令查看文件目录的策略类型。() 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