如何设置PAM模块控制Linux密码策略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__E5_A6_82_E4_BD_95_E8_AE_BE_E7_c103_645221.htm 我们在使用linux系统设置密码的时候，经常遇到这样的问题，系统提示：您的密码太简单，或者您的密码是字典的一部分。那么系统是如何实现对用户的密码的复杂度的检查的呢？ 系统对密码的控制是有两部分(我知道的)组成： 1 cracklib 2 login.defs 声明：login.defs主要是控制密码的有效期。对密码进行时间管理。此处不细谈 login.defs --shadow password suite configuration pam_cracklib.so 才是控制密码复杂度的关键文件 redhat公司专门开发了cracklib这个安装包来判断密码的复杂度 可以rpm -ql cracklib查看 密码的复杂度的判断是通过pam模块控制来实现的，具体的模块是pam_cracklibpam_cracklib 的参数介绍： debug This option makes the module write information to syslog(3) indicating the behavior of the module (this option does not write password information to the log file). type=XXX The default action is for the module to use the following prompts when requesting passwords: "New UNIX password: " and "Retype UNIX password: ". The default word UNIX can be replaced with this option. retry=N Prompt user at most N times before returning with error. The default is 1 difok=N This argument will change the default of 5 for the number of characters in the new password that must not be present in the old password. In addition, if 1/2 of the characters in the new password are different then the new password will be accepted anyway. difignore=N How many characters should the password

have before difok will be ignored. The default is 23. minlen=N