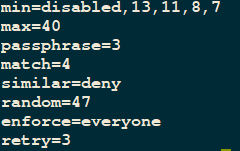
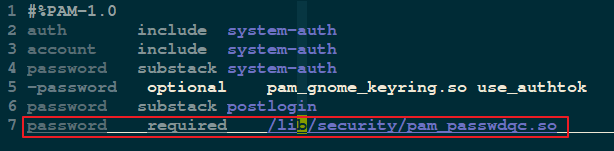
**使用passwordqc限制用户密码强度**

1. **PAM认证模块简介**
   1. 基本功能：将认证功能独立于程序之外，为程序返回验证结果
   2. 配置文件说明
      1. 验证类型
         1. Auth（authentication）用来检验用户身份
         2. Account 用来检验用户是否具有正确的权限，比如，密码是否过期
         3. Session 管理用户登陆期间用户环境的设置，通常用于记录用户登陆与注销的信息
         4. Password 提供验证的修订工作：修改密码
         5. 顺序：验证身份（auth）、授权（account）、记录登陆注销信息（session）、更改密码（password）
      2. 控制标志
         1. Required  
            验证成功会带有success并继续进行后续验证，失败会带有failure标志并继续后续验证（有利于数据的登陆日志）
         2. Requisite  
            验证失败立即返回，终止后续验证流程，成功则继续
         3. Sufficient  
            成功则立即返回，失败则继续进行后续验证
         4. Optional  
            用于显示信息
      3. 常用pam模块儿
2. **一般认证过程，passwd为例**
   1. 用户执行passwd程序
   2. Passwd调用PAM进行验证
   3. PAM去/etc/pam.d/下寻找与passwd同名的配置文件
   4. 依据/etc/pam.d/passwd中的配置，逐步进行验证
   5. 将验证结果返回给passwd
3. **编译安装passwordqc，限制用户密码强度**
   1. 获取源码包  
      
   2. 解压编译安装  
        
      pam源码包  
      然后进入passwdqc目录执行make && make install
   3. 配置文件/etc/passwdqc.conf默认内容如下  
        
      详细配置含义可从<http://www.openwall.com/passwdqc/README.shtml>获得
   4. 执行ldconfig刷新动态链接库缓存
4. **在/etc/pam.d/passwd中添加passwdqc.so模块的引用**
5. **使用passwd修改密码时，如果使用的密码过于简单，则提示不允许**