

安全策略编辑器

概 述

产品简介

安全策略编辑器是一款系统安全管理工具，提供密码策略、账户锁定策略、网络安全策略、网络访问策略、系统安全策略、交互式登录策略等功能，简化了系统管理员配置系统的难度。

产品亮点

功能齐全：提供密码策略、账户锁定策略、网络安全策略、网络访问策略、系统安全策略、可交互式登录策略、文件保护箱策略、审计策略等，基本涵盖常用系统配置。

插件机制：提供插件框架，所有的策略模块都以插件的方式集成到编辑器中，极大简化了更新和功能扩展。

UI反射机制：各个模块界面都是根据JSON描述动态生成的，使得开发者可以在不懂QT技术的情况下，完成界面开发和更新。

简单易用：操作简单、易于上手。

使用入门

软件位置

点击操作系统“开始菜单”，选择并点击“策略编辑器”，打开策略编辑器界面，如图1所示。



获取帮助

策略编辑器界面中点击菜单图标，点击“帮助”按钮，弹出“用户手册”弹窗，显示策略编辑器的帮助手册相关信息，如图2所示。

Manual

概述

产品简介

产品亮点

使用入门

软件位置

获取帮助

语言支持

关于

密码策略

密码必须符合复杂性要求

密码最短长度

密码最短使用期限

密码最长使用期限

提示用户在密码过期之前更改密码

强制历史密码数量

启用密码字典检查

概述

产品简介

安全策略编辑器是一款系统安全管理工具，提供密码策略、账户锁定策略、网络安全策略、网络访问策略、系统安全策略、交互式登录策略等等功能，简化了系统管理员配置系统的难度。

产品亮点

功能齐全：提供密码策略、账户锁定策略、网络安全策略、网络访问策略、系统安全策略、可交互式登录策略、文件保护箱策略、审计策略等，基本涵盖常用系统配置。

插件机制：提供插件框架，所有的策略模块都以插件的方式集成到编辑器中，极大简化了更新和功能扩展。

UI反射机制：各个模块界面都是根据JSON描述动态生成的，使得开发者可以在不懂QT技术的情况下，完成界面开发和更新。

简单易用：操作简单、易于上手。

使用入门

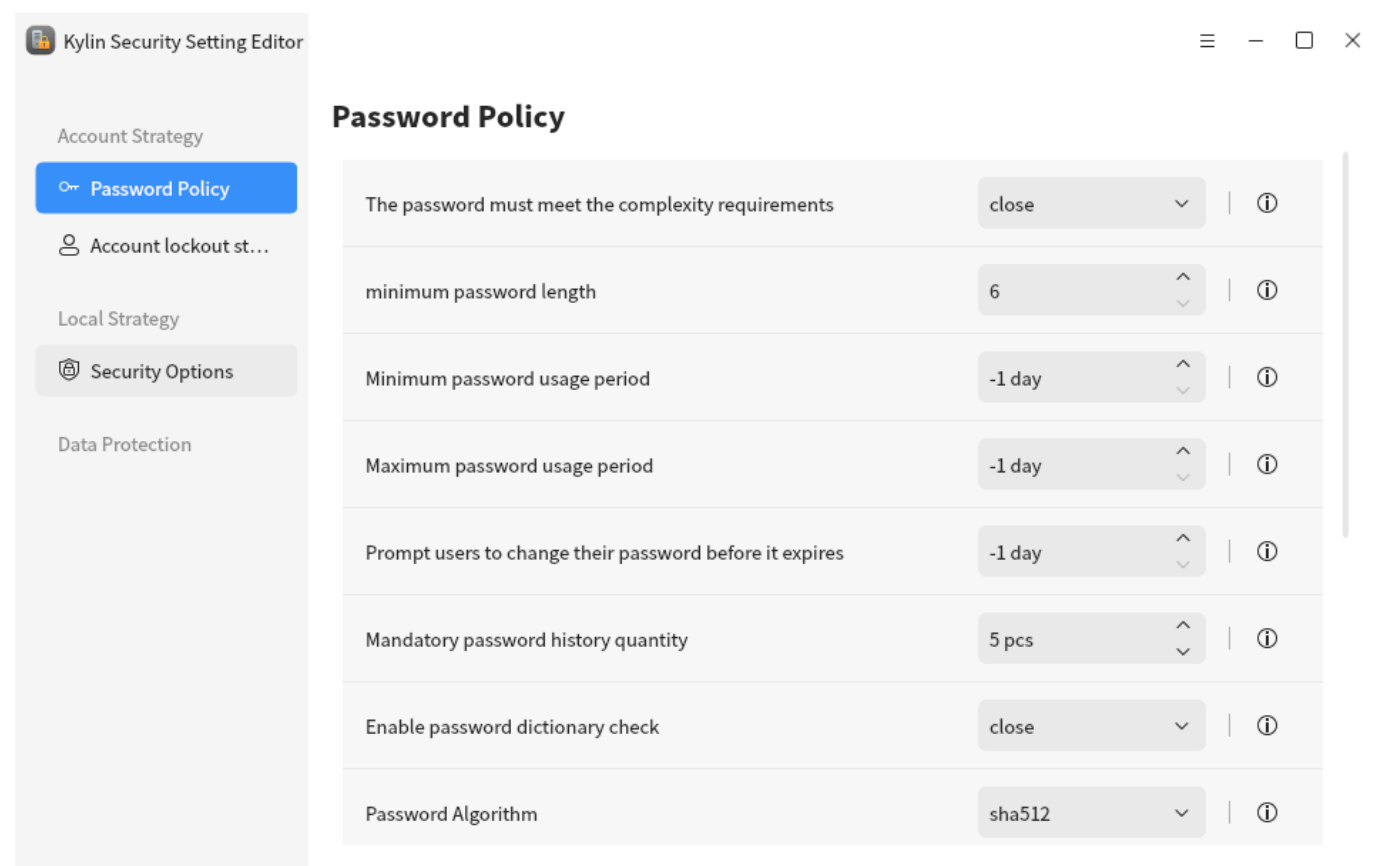
软件位置

点击操作系统“开始菜单”，选择并点击“策略编辑器”，打开策略编辑器界面，如图1所示。



语言支持

策略编辑器界面默认跟随系统语言设置，支持中文和英文，如图5至6所示。



关于

策略编辑器界面点击菜单图标，点击“关于”按钮，弹出“关于”弹窗，显示软件版本信息，如7所示。



1. 密码策略

进入应用，点击左侧“账户锁定策略”选项，即可进入账户锁定的配置界面。



1.1 密码必须符合复杂性要求

此安全设置确定密码是否必须符合复杂性要求。如果启用此策略，密码必须符合下列最低要求: 1)不能包含账户的用户名 2)至少有8个字符长 3)包含以下四类字符中的两类字符: 英文大写字母(A 到 Z) 英文小写字母(a 到 z) 10 个基本数字(0 到 9) 特殊字符(例如 !、\$、#、%) 如果文件/etc/security/pwquality.conf不存在，此项策略置灰。

开启操作：1.如果系统minlen>=8,不修改配置，否则将配置改为minlen = 8 2.将usercheck配置改成1 3.如果系统minclass>=2,不修改配置，否则将配置改为minclass = 2 关闭操作：将配置改为usercheck=0,minlen=0,minclass=0 读取操作：1.检查文件/etc/security/pwquality.conf，如果文件不存在，认为此项策略不能配置，置灰。 2.检查配置usercheck,如果配置不存在，则认为usercheck==1，否则读取实际值 3.检查配置minlen,如果配置不存在，则认为minlen==8，否则读取实际值 4.检查配置minclass,如果配置不存在，则认为minclass==0，否则读取实际值 判断读取结果，如果usercheck==1 && minlen>= 8 && minclass >= 2,那么认为是开启状态，否则非开启状态

1.2 密码最短长度

此安全设置确定账户密码可以包含的最少字符数。密码必须符合密码复杂度要求启用时，密码最小长度不能小于8个字符。如果文件/etc/security/pwquality.conf不存在，此项策略置灰。

写入操作：将UI配置参数写入文件中，形如：minlen = 8 UI上的限制的取值范围：[6, 32] 读取操作：1.检查文件/etc/security/pwquality.conf，如果文件不存在，认为此项策略不能配置，置灰。 2.读取minlen配置，如果minlen配置不存在，则认为minlen==8,否则返回实际值

1.3 密码最短使用期限

此安全设置确定在用户更改某个密码之前必须使用该密码一段时间(以天为单位)。可以设置一个介于 -1 和 99999 天之间的值，当天数设置为 0或-1，允许立即更改密码。如果文件/etc/login.defs不存在，此项策略置灰。

写入操作：1.将UI配置参数写入文件中，形如：PASS_MIN_DAYS 8 2.修改shadow文件中对应配置，刷新老用户的配置 UI上的限制的取值范围：[0, 99999] 读取操作：1.检查/etc/login.defs文件，如果文件不存在，认为此项策略不能配置，置灰。 2.读取PASS_MIN_DAYS配置，如果配置不存在返回-1，否则返回实际值。

1.4 密码最长使用期限

此安全设置确定在系统要求用户更改某个密码之前可以使用该密码的期间(以天为单位)。可以将密码设置为在某些天数(介于 -1 到 99999 之间)后到期，当天数设置为 -1，指定密码永不过期。如果文件/etc/login.defs不存在，此项策略置灰。 建议: 安全最佳操作是将密码设置为 30 到 90 天后过期，具体取决于你的环境。

写入操作：1.将UI配置参数写入文件中，形如：PASS_MAX_DAYS 8 2.修改shadow文件中对应配置，刷新老用户的配置 UI上的限制的取值范围：[0, 99999] 读取操作：1.检查/etc/login.defs文件，如果文件不存在，认为此项策略不能配置，置灰。 2.读取PASS_MAX_DAYS配置，如果配置不存在返回-1，否则返回实际值。

1.5 提示用户在密码过期之前更改密码

PASS_WARN_AGE参数用于控制提前多长时间(以天为单位)向用户发出其密码即将过期的警告。借助该提前警告，用户有时间构造足够强大的密码。该参数的取值范围为[-1, 99999]这个区间。将值设置为0，表示直到最长使用期限当天才会警告。将值设置为-1，表示永不警告。如果文件/etc/login.defs不存在，此项策略置灰。

配置操作：将UI参数写入文件中 目前UI上的PASS_WARN_AGE取值范围：【-1，99999】 读取操作：
1.如果/etc/login.defs文件不存在，策略项目置灰，不能操作。 2.检查文件/etc/login.defs中的
PASS_WARN_AGE值，如果配置不存在，返回-1，否则返回实际数值

1.6 强制历史密码数量

此安全设置确定再次使用某个旧密码之前必须与某个用户账户关联的唯一新密码数。该值必须介于 0 个和 24 个密码之间。此策略使管理员能够通过确保旧密码不被连续重新使用来增强安全性。如果文件/etc/pam.d/system-auth不存在，此项策略置灰。此安全设置确定再次使用某个旧密码之前必须确保不能使用与某个账户关联的旧密码数

写入操作：1.将配置参数写入文件 ui上的限制范围：【0，24】 读取操作：1.如果文件/etc/pam.d/system-auth不存在，认为此项策略不能配置，置灰。 2.查找文件/etc/pam.d/system-auth中的这行配置 password requisite pam_pwhistory.so remember=5 enforce_for_root 3.获取remember数据，如果配置不存在，则认为remember==0，否则返回实际值。

1.7 启用密码字典检查

此安全设置确定了账户密码能否包含密码字典中包含的密码。如果文件/etc/security/pwquality.conf不存在，此项策略置灰。

开启操作：将dictcheck=1写入文件 关闭操作：将dictcheck=0写入文件 读取操作：1.如果/etc/security/pwquality.conf文件不存在，认为此项策略不能配置，置灰。 2.读取文件中的dictcheck参数，如果dictcheck配置不存在，则被认为dictcheck==1，否则返回实际值。

1.8 密码算法

此安全设置确定了账户密码保存时使用的密码算法。如果文件/etc/pam.d/system-auth不存在，此项策略置灰。

配置操作：1.将配置参数写入文件 读取操作：1.如果文件/etc/pam.d/system-auth不存在，认为此项策略不能配置，置灰。 2.查找文件/etc/pam.d/system-auth中的匹配关键字"password","sufficient","pam_unix.so","sha512/sm3"行配置 3.如果配置不存在则被认为是sha512，否则返回实际值

1.9 启用UID唯一性

此安全设置确保在操作系统生命周期内，用户唯一，防止新建用户使用已删除用户的UID。注：强制通过修改passwd文件使用相同的uid，在登录时，只有uid匹配的用户可以正常登录，非法用户无法登录。如果文件/etc/chkuid_state不存在，此项策略置灰。

开启操作：1.将state=on写入文件 关闭操作：1.将state=off写入文件 读取操作：1.检查文件/etc/chkuid_state，如果文件不存在，则此项策略不可用，置灰。 2.查看文件/etc/chkuid_state中的state配置 2.如果state=on返回"开启状态"，state=off，返回“关闭状态”。如果配置不存在，则被认为state=off

1.10 密码不允许包含用户名

此安全设置确定账户密码是否包含用户名。密码必须符合密码复杂度要求启用时，该项策略无法关闭。如果文件/etc/security/pwquality.conf不存在，此项策略置灰。

开启操作：1.将usercheck=1写入文件 关闭操作：1.将usercheck=0写入文件 读取操作：1.检查/etc/security/pwquality.conf文件，如果文件不存在，则认为此项策略不可用，置灰 2.读取usercheck配置，如果配置不存在，则被认为usercheck==1，否则返回实际值。

1.11 启用密码回文检查

该安全设置确定了账户密码是否设置回文密码，如ABcd11dcBA 如果文件/etc/security/pwquality.conf不存在，此项策略置灰。

开启操作：1.将palindromic写入文件 关闭操作：1.将palindromic配置删除 读取操作：1.检查/etc/security/pwquality.conf文件，如果文件不存在，则认为此项策略不可用，置灰 2.读取palindromic配置，如果配置不存则被认为没有开启回文检查，否则认为开启回文检查。

1.12 启用密码相似性检查

此安全设置确定账户密码是否与旧密码太相似。相似性检查包含：1)将字母字符进行大小写转换后比较。2)将密码字符串重复一次后进行比较。比如，旧密码123，重复后：123123，新密码与重复后的密码串比较。如果文件/etc/security/pwquality.conf不存在，此项策略置灰。

开启操作：1.将no_similar_check配置删除 关闭操作：1.将no_similar_check写入文件 读取操作：1.检查/etc/security/pwquality.conf文件，如果文件不存在，则认为此项策略不可用，置灰 2.读取no_similar_check配置，如果配置不存则被认为开启回相似性检查，否则认为没有开启相似性检查。

1.13 密码差异字符数

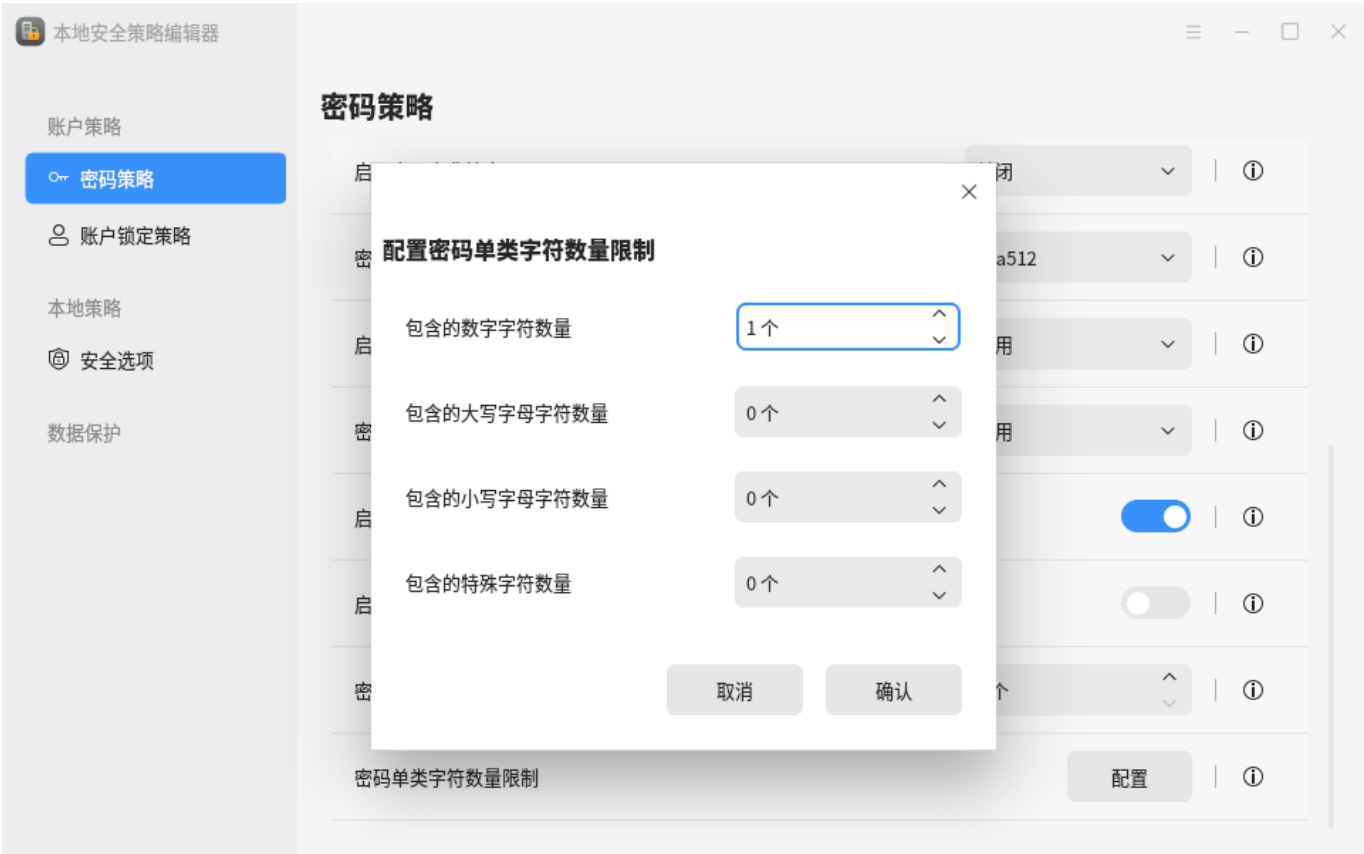
采用最小编辑距离的动态规划算法，计算新密码与旧密码的字符差异。数值太低（例如 1 或 2），用户可能只需要修改少量字符即可更改密码，这无法有效提高安全性。数值过高（例如7 或 8），用户可能会感到更改密码过于复杂，增加了记忆新密码的困难。建议值：旧密码长度的一半。如果文件/etc/security/pwquality.conf不存在，此项策略置灰。

配置操作：将UI配置参数写入文件中，形如：difok = 5 UI上的限制的取值范围：[0, 32] 扫描：1.检查文件/etc/security/pwquality.conf，如果文件不存在，认为此项策略不能配置，置灰。 2.读取difok配置，如果difok配置不存在，则认为difok==1,否则返回实际值

1.14 密码单字类数量限制

该安全设置确定了账户密码包含的单类字符数。密码包含的大写字母字符数 密码包含的小写字母字符数 密码包含的数字字符数 密码包含的特殊字符数

单类字符数量设置范围：-120~120 <0:至少要包含多少个字符。 0:口令中的每种元素积分上限。 pam_pwquality使用了一个评分机制来处理口令长度和强度的问题，minlen配置了口令所需的最小位数，也就是目标分值；可以为口令中的每种元素设置积分(credit)上限，某种元素每出现一次可获得一个积分，直到与积分上限相等，获得的积分可用于抵扣目标分值，而实际的口令长度最小位数为minlen减去获得的积分。如果文件/etc/security/pwquality.conf不存在，此项策略置灰。



写入操作 1.将配置参数写入文件。 读取操作： 1.检查文件/etc/security/pwquality.conf文件，如果文件不存在，则认为此项策略不可用，置灰 2.读取文件中的dcredit，ucredit，lcredit，ocredit配置，如果配置不存在，则认为对应项配置值等于0，否则返回实现值

2. 账户锁定策略

进入应用，点击左侧“账户锁定策略”选项，即可进入账户锁定的配置界面。



2.1 账户锁定时间

此安全设置确定用户密码输入错误时，需要等待的分钟数，可用范围从 0 到 99,999 分钟。如果将账户锁定时间设置为 0，账户将一直被锁定直到管理员明确解除对它的锁定。如果文件/etc/pam.d/system-auth不存在，此项策略置灰。

写入操作：1.用指定参数修改“unlock_time=”的值。UI限制范围:[0, 99,999] 读取操作：1.如果文件/etc/pam.d/system-auth不存在，认为此项策略不能配置，置灰。2.查找文件/etc/pam.d/system-auth中的匹配含关键字“pam_unix.so”，“unlock_time=”的行配置3.如果配置不存在则被认为unlock_time=600，否则返回实际值

2.2 账户锁定阈值

此安全设置确定导致账户被锁定的登录尝试失败的次数。可以将登录尝试失败次数设置为介于 0 和 999 之间的值。如果将值设置为 0，则永远不会锁定账户。如果登入失败次数>=deny值，账户将被锁定。如果文件/etc/pam.d/system-auth不存在，此项策略置灰。

配置操作：1.将配置参数写入文件UI限制范围:[0, 999] 扫描：1.如果文件/etc/pam.d/system-auth不存在，认为此项策略不能配置，置灰。2.查找文件/etc/pam.d/system-auth中的匹配含关键字“pam_faillock.so”，“deny=”的行配置3.如果配置不存在则被认为deny=0，否则返回实际值

2.3 本地远程认证锁定

此安全设置确定账户锁定功能是否针对远程认证程序与本地认证程序分别生效。如果开启，远程认证程序多次认证失败导致账户锁定后，不影响本地认证程序的认证功能。如果文件/etc/pam.d/system-auth不存在，此项策略置灰。

开启操作：1.将“no_logsplit”配置从文件中删除UI限制范围:[0, 999] 关闭操作：1.将“no_logsplit”配置参数写入文件 读取操作：1.如果文件/etc/pam.d/system-auth不存在，认为此项策略不能配置，置灰。2.检查文件/etc/pam.d/system-auth，匹配含关键字“pam_unix.so”，“no_logsplit”的行3.如果存在，则认为本地远程认证锁定分离功能关闭，否则功能启用。

3 安全选项/网络安全



3.1 不允许ICMP重定向

攻击者可能会使用伪造的ICMP重定向消息恶意更改系统路由表，并让他们将数据包发送到不正确的网络，并允许捕获系统数据包。 如果文件/etc/sysctl.conf不存在，此项策略置灰。

开启操作：修改/etc/sysctl.conf文件配置 net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0 关闭操作：修改/etc/sysctl.conf文件配置
net.ipv4.conf.all.accept_redirects = 1 net.ipv4.conf.default.accept_redirects = 1 读取操作： 1.如
果/etc/sysctl.conf文件不存在，当前策略不可用，置灰。 2.读取配置，如果配置不存在，认为当前系统
状态不确定，UI界面上两者都不选，处于中间状态

3.2 不允许发送重定向

ICMP重定向用于将路由信息发送到其他主机。 攻击者可以使用受感染的主机将无效的ICMP重定向发送到其他路由器设备，以试图破坏路由并让用户访问由攻击者设置的无效系统。 若服务器作为docker宿主机，此项不能加固。 如果文件/etc/sysctl.conf不存在，此项策略置灰。

开启操作：修改/etc/sysctl.conf文件配置 net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0 关闭操作：修改/etc/sysctl.conf文件配置
net.ipv4.conf.all.send_redirects = 1 net.ipv4.conf.default.send_redirects = 1 读取操作： 1.如
果/etc/sysctl.conf文件不存在，当前策略不可用，置灰。 2.读取配置，如果配置不存在，认为当前系统
状态不确定，UI界面上两者都不选，处于中间状态

3.3 忽略ICMP广播请求

将net.ipv4.icmp_echo_ignore_broadcasts设置为1将导致系统忽略对广播和多播地址的所有ICMP回送和时间戳请求。 接受带有网络广播或多播目的地的ICMP回送和时间戳请求可用于欺骗主机启动（或参与蓝精灵的袭击。 Smurf攻击依赖于攻击者使用欺骗性源地址发送大量ICMP广播消息。 接收此消息并响应的所有主机都会

将echo-reply消息发送回欺骗地址，该地址可能不可路由。如果许多主机响应数据包，则网络上的流量可能会显著增加。如果文件/etc/sysctl.conf不存在，此项策略置灰。

开启操作：修改/etc/sysctl.conf文件配置 net.ipv4.icmp_echo_ignore_broadcasts = 1 关闭操作：修改/etc/sysctl.conf文件 net.ipv4.icmp_echo_ignore_broadcasts = 0 读取操作：1.如果/etc/sysctl.conf文件不存在，当前策略不可用，置灰。2.读取配置，如果配置不存在，认为当前系统状态不确定，UI界面上两者都不选，处于中间状态

3.4 不接收IPV4源路由数据包

将net.ipv4.conf.all.accept_source_route和net.ipv4.conf.default.accept_source_route设置为0将禁止系统接受源路由数据包。在正常路由环境下，来自Internet可路由地址的攻击者无法使用该系统作为到达私有地址系统的方式。但是，如果允许源路由数据包，则可以使用它们来访问专用地址系统，因为可以指定路由，而不是依赖于不允许此路由的路由协议。如果文件/etc/sysctl.conf不存在，此项策略置灰。

开启操作：修改/etc/sysctl.conf文件配置 net.ipv4.conf.all.accept_source_route = 0 net.ipv4.conf.default.accept_source_route = 0 关闭操作：修改/etc/sysctl.conf文件配置 net.ipv4.conf.all.accept_source_route = 1 net.ipv4.conf.default.accept_source_route = 1 读取操作：1.如果/etc/sysctl.conf文件不存在，当前策略不可用，置灰。2.读取配置，如果配置不存在，认为当前系统状态不确定，UI界面上两者都不选，处于中间状态

3.5 不接收IPV6源路由数据包

将net.ipv6.conf.all.accept_source_route和net.ipv6.conf.default.accept_source_route设置为0将禁止系统接受源路由数据包。在正常路由环境下，来自Internet可路由地址的攻击者无法使用该系统作为到达私有地址系统的方式。但是，如果允许源路由数据包，则可以使用它们来访问专用地址系统，因为可以指定路由，而不是依赖于不允许此路由的路由协议。如果文件/etc/sysctl.conf不存在，此项策略置灰。

开启操作：修改/etc/sysctl.conf文件配置 net.ipv6.conf.all.accept_source_route = 0 net.ipv6.conf.default.accept_source_route = 0 关闭操作：修改/etc/sysctl.conf文件配置 net.ipv6.conf.all.accept_source_route = 1 net.ipv6.conf.default.accept_source_route = 1 读取操作：1.如果/etc/sysctl.conf文件不存在，当前策略不可用，置灰。2.读取配置，如果配置不存在，认为当前系统状态不确定，UI界面上两者都不选，处于中间状态

3.6 不允许转发IPV4数据包

net.ipv4.ip_forward标志用于告诉系统是否可以转发数据包。将标志设置为0可确保具有多个接口的系统（例如，硬代理）永远无法转发数据包，因此，不可作为路由器。若服务器作为docker宿主机，此项不能加固。如果文件/etc/sysctl.conf不存在，此项策略置灰。

开启操作：修改/etc/sysctl.conf文件配置 net.ipv4.ip_forward = 0 关闭操作：修改/etc/sysctl.conf文件配置 net.ipv4.ip_forward = 1 写入操作：1.如果/etc/sysctl.conf文件不存在，当前策略不可用，置灰。2.读取配置，如果配置不存在，认为当前系统状态不确定，UI界面上两者都不选，处于中间状态

3.7 不允许转发IPV6数据包

net.ipv6.conf.all.forwarding标志用于告诉系统是否可以转发数据包。将标志设置为0可确保具有多个接口的系统（例如，硬代理）永远无法转发数据包，因此，不可作为路由器。若服务器作为docker宿主机，此项不能加固。如果文件/etc/sysctl.conf不存在，此项策略置灰。

开启操作：修改/etc/sysctl.conf文件配置 net.ipv6.conf.all.forwarding = 0 关闭操作：修改/etc/sysctl.conf文件配置 net.ipv6.conf.all.forwarding = 1 写入操作：1.如果/etc/sysctl.conf文件不存在，当前策略不可用，置灰。2.读取配置，如果配置不存在，认为当前系统状态不确定，UI界面上两者都不选，处于中间状态

3.8 不允许网络协议配置

数据报拥塞控制协议（DCCP）是支持流媒体和电话的传输层协议。可靠数据报套接字（RDS）协议是一种传输层协议，在群集节点之间提供低延迟，高带宽的通信。流控制传输协议（SCTP）是用于支持面向消息的通信传输层协议，并在一个连接中具有几个消息流。透明进程间通信（TIPC）协议提供群集节点之间的通信。如果不使用上述协议，建议不要加载，以减少潜在的攻击面。如果内核没有编译上述协议模块，对应项置灰。



开启操作：1.如果/etc/modprobe.d/CIS.conf文件不存在,则创建文件 2.添加对应服务配置 install dccp /bin/true install rds /bin/true install sctp /bin/true install ticp /bin/true 3.如果“lsmod | grep中” 查询到模块，使用rmmod 卸载模块 关闭操作：1.如果/etc/modprobe.d/CIS.conf文件不存在，则跳到第3步 2.如果文件存在且对应配置也存在，删除对应配置 3.如果“lsmod | grep中” 未查询到模块，使用modprobe命令安装模块 如果完全符合开启条件，这认为是开启状态。否则只要有一项不满足，就认为是关闭状态

3.9 启用NFS服务

网络文件系统（NFS）是UNIX环境中第一个也是分布最广的文件系统之一，它使系统能够通过网络挂载其他服务器的文件系统。如果系统不导出NFS共享或充当NFS客户端，建议禁用这些服务以减少远程攻击面。如果没有安装该服务，此项策略置灰。

开启操作：systemctl enable nfs-server systemctl start nfs-server 关闭操作：systemctl disable nfs-server systemctl stop nfs-server 读取操作：如果没有安装该服务，策略配置项置灰，并提供说

明。如果 "systemctl is-active 服务名" 结果是active的，则认为是开启状态，否则处于关闭状态 服务器系统安装服务：sudo yum install nfs-utils 桌面系统安装服务：sudo apt install nfs-kernel-server

3.10 启用RPC服务

Portmapper是一个RPC服务，它始终侦听tcp和udp 111，并用于映射其他RPC服务（如nfs、nlockmgr、quotad、mountd等）与其对应的服务器上的端口号。当远程主机对该服务器进行RPC调用时，它首先咨询portmap以确定RPC服务器正在侦听的位置，然后发送到Portmapper的小请求（通过UDP约82字节）会生成大响应（7x至28倍放大），这使其成为DDoS攻击的合适工具。如果没有安装该服务，此项策略置灰。

开启操作：systemctl enable rpcbind systemctl start rpcbind 关闭操作：systemctl disable rpcbind systemctl stop rpcbind 读取操作：如果没有安装该服务，策略配置项置灰，并提供说明。如果 "systemctl is-active 服务名" 结果是active的，则认为是开启状态，否则处于关闭状态 服务器系统安装服务：sudo yum install rpcbind 桌面系统安装服务：sudo apt install rpcbind

3.11 启用Smba服务

Samba服务允许将目录和文件系统挂载到Windows系统，建议禁用此服务以减少潜在的攻击面。如果没有安装该服务，此项策略置灰。

开启操作：systemctl enable smb | smb systemctl start smb | smb 关闭操作：systemctl disable smb | smb systemctl stop smb | smb 读取操作：如果没有安装该服务，策略配置项置灰，并提供说明。如果 "systemctl is-active 服务名" 结果是active的，则认为是开启状态，否则处于关闭状态 服务器系统安装服务：sudo yum install samba 桌面系统安装服务：sudo apt install samba

3.12 启用IMap和Pop3服务

dovecot是一个基于Linux系统的开源IMAP和POP3服务器。除非此系统作为POP3或IMAP服务器，否则建议禁用该服务以减少潜在的攻击面。如果没有安装该服务，此项策略置灰。

开启操作：systemctl enable dovecot systemctl start dovecot 关闭操作：systemctl disable dovecot systemctl stop dovecot 读取操作：如果没有安装该服务，策略配置项置灰，并提供说明。如果 "systemctl is-active 服务名" 结果是active的，则认为是开启状态，否则处于关闭状态 服务器系统安装服务：sudo yum install dovecot 桌面系统安装服务：sudo apt install dovecot-imapd dovecot-pop3d

3.13 启用Squid服务

Squid是许多环境中使用的标准代理服务器，如果不需要代理服务器，建议禁用squid代理以减少潜在的攻击面。如果没有安装该服务，此项策略置灰。

开启操作：systemctl enable squid systemctl start squid 关闭操作：systemctl disable squid systemctl stop squid 读取操作：如果没有安装该服务，策略配置项置灰，并提供说明。如果 "systemctl is-active 服务名" 结果是active的，则认为是开启状态，否则处于关闭状态 服务器系统安装服务：sudo yum install squid 桌面系统安装服务：sudo apt install squid

3.14 启用rsync服务

rsyncd服务可用于在系统之间同步文件通过网络链路层。建议禁用此服务以减少潜在的攻击面。如果没有安装该服务，此项策略置灰。

开启操作：systemctl enable rsyncd systemctl start rsyncd 关闭操作：systemctl disable rsyncd
systemctl stop rsyncd 读取操作：如果没有安装该服务，策略配置项置灰，并提供说明。 如果
"systemctl is-active 服务名"结果是active的，则认为是开启状态，否者处于关闭状态 服务器系统安装
服务：sudo yum install rsync 桌面系统安装服务：sudo apt install rsync

3.15 启用LDAP服务

轻量目录访问协议（LDAP）是一种用于访问、查询和修改目录服务中信息的协议。如果服务器不需要充当LDAP客户端或服务，建议禁用该软件以减少潜在的攻击面。如果没有安装该服务，此项策略置灰。

开启操作：systemctl enable slapd systemctl start slapd 关闭操作：systemctl disable slapd
systemctl stop slapd 读取操作：如果没有安装该服务，策略配置项置灰，并提供说明。 如果
"systemctl is-active 服务名"结果是active的，则认为是开启状态，否者处于关闭状态 服务器系统安装
服务：sudo yum install -y openldap-servers 桌面系统安装服务：sudo apt install slapd

3.16 启用SNMP服务

简单网络管理协议（SNMP）服务器用于从SNMP管理系统监听SNMP命令，执行命令或收集信息，并将结果发送回请求系统。系统功能通常不需要自动发现网络服务，建议禁用该服务以减少潜在的攻击面。如果没有安装该服务，此项策略置灰。

开启操作：systemctl enable snmpd systemctl start snmpd 关闭操作：systemctl disable snmpd
systemctl stop snmpd 读取操作：如果没有安装该服务，策略配置项置灰，并提供说明。 如果
"systemctl is-active 服务名"结果是active的，则认为是开启状态，否者处于关闭状态 服务器系统安装
服务：sudo yum install net-snmp 桌面系统安装服务：sudo apt-get install snmpd

3.17 启用TCP SYN Cookie

攻击者使用SYN泛洪攻击通过发送许多SYN数据包来执行系统上的拒绝服务，而无需完成三次握手。这将很快耗尽内核半开连接队列中的插槽，并阻止合法连接成功。开启SYN Cookie允许系统继续接受有效连接，即使在拒绝服务攻击下也是如此。如果/etc/sysctl.conf文件不存在，此项策略置灰。

开启操作：修改/etc/sysctl.conf文件配置 net.ipv4.tcp_syncookies = 1 关闭操作：修
改/etc/sysctl.conf文件配置 net.ipv4.tcp_syncookies = 0 读取操作：1.如果/etc/sysctl.conf文件不存
在，当前策略不可用，置灰。2.读取配置，如果配置不存在，认为当前系统状态不确定，UI界面上两者
都不选，处于中间状态

3.18 忽略伪造的ICMP相应

将icmp_ignore_bogus_error_responses设置为1可防止内核从广播重构中记录虚假响应（RFC-1122不兼容），从而防止文件系统填满无用的日志消息。某些路由器（以及一些攻击者）将发送违反RFC-1122和 尝试用许多无用的错误消息填充日志文件系统。如果文件/etc/sysctl.conf不存在，此项策略置灰。

开启操作：修改/etc/sysctl.conf文件配置 icmp_ignore_bogus_error_responses = 1 关闭操作：修
改/etc/sysctl.conf文件配置 icmp_ignore_bogus_error_responses = 0 读取操作：1.如
果/etc/sysctl.conf文件不存在，当前策略不可用，置灰。2.读取配置，如果配置不存在，认为当前系统
状态不确定，UI界面上两者都不选，处于中间状态

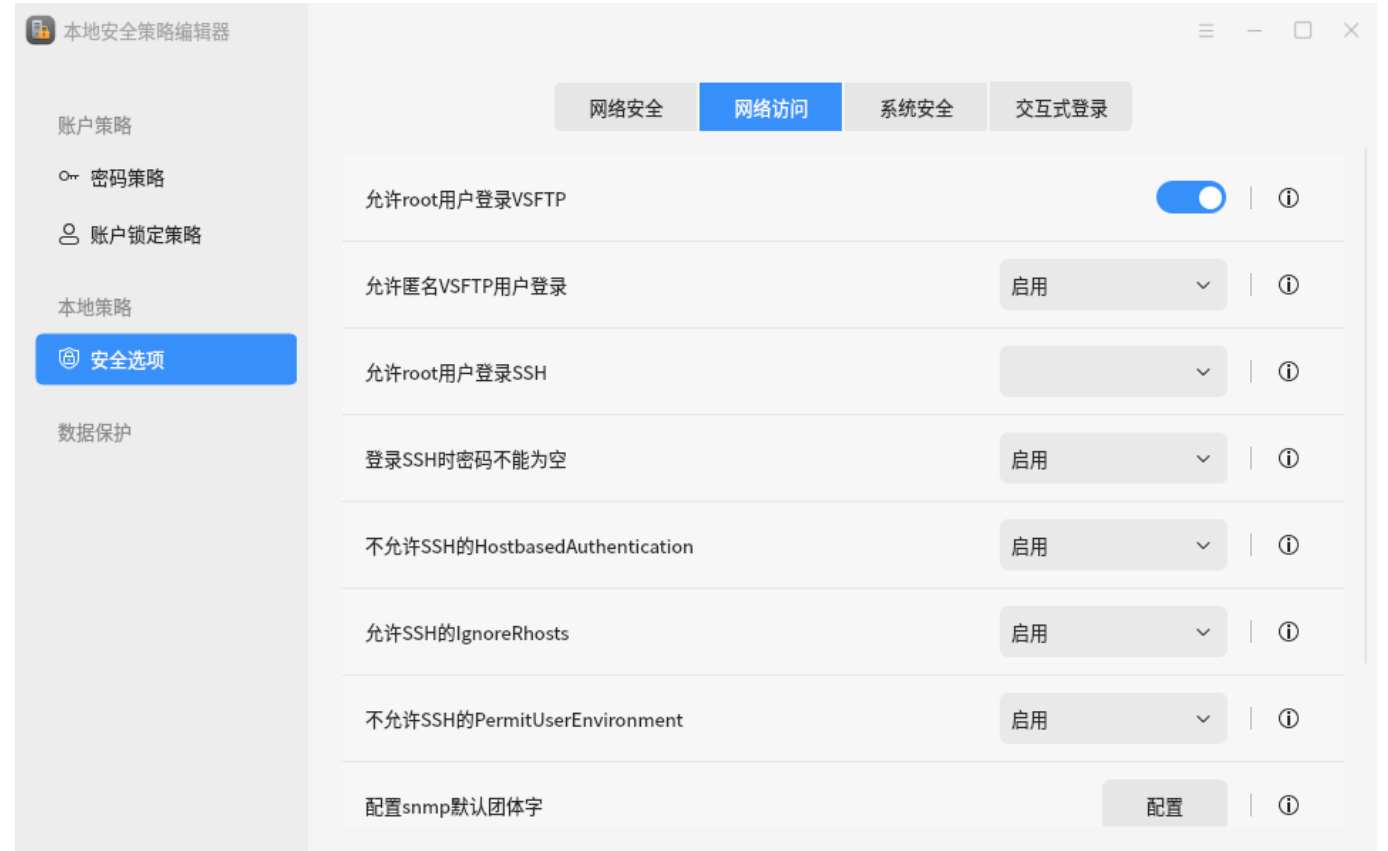
3.19 启用反向路径过滤

将net.ipv4.conf.all.rp_filter和net.ipv4.conf.default.rp_filter设置为1会强制Linux内核对接收到的数据包进行反向路径过滤，以确定数据包是否有效。开启反向路径过滤，如果返回的数据包没有出现在相应的源数据包接口上，则丢弃数据包。设置这些标志是阻止攻击者发送无法响应的系统伪造数据包的好方法。如果您在系统上使用非对称路由，则无法在不中断路由的情况下启用此功能。如果文件/etc/sysctl.conf不存在，此项策略置灰。

开启操作：修改/etc/sysctl.conf文件配置 net.ipv4.conf.all.rp_filter = 1 net.ipv4.conf.default.rp_filter = 1 关闭操作：修改/etc/sysctl.conf文件配置 net.ipv4.conf.all.rp_filter = 0 net.ipv4.conf.default.rp_filter = 0 读取操作：1.如果/etc/sysctl.conf文件不存在，当前策略不可用，置灰。 2.读取配置，如果配置不存在，认为当前系统状态不确定，UI界面上两者都不选，处于中间状态

4 安全选项/网络访问

进入应用，点击左侧“安全选项”选项，再将tab页切换到“网络访问”即可进入安全选项/网络访问配置界面。



4.1 允许root用户登录VSFTP

此项策略用于控制是否允许root用户登录VSFTP服务器。如果/etc/vsftpd/ftpusers或者/etc/vsftpd/user_list不存在，此项策略置灰。

开启操作：1.如果文件"/etc/vsftpd/ftpusers"中“root”项存在，删除“root”项 2.如果文件"/etc/vsftpd/user_list"中“root”项存在，删除“root”项 关闭操作：1.在文件"/etc/vsftpd/ftpusers"中添加"root"配置项 2.如果文件"/etc/vsftpd/user_list"中“root”项存在，删除“root”项 读取操作：如果"/etc/vsftpd/ftpusers或者/etc/vsftpd/user_list"不存在，策略配置项置灰，并提供说明。如果 存在"root"配置，则被认为禁用root登录vsftp服务器，否则被认为启用了root登录

4.2 允许匿名用户登录VSFTP

anonymous_enable参数指定是否允许匿名用户登录VSFTP服务器。如果文件/etc/vsftpd/vsftpd.conf不存在，此项策略置灰。

开启操作：修改/添加配置项“anonymous_enable=YES” 关闭操作：修改/添加配置项“anonymous_enable=NO” 读取操作：如果/etc/vsftpd/vsftpd.conf文件不存在，策略配置项置灰，并提供说明。当文件anonymous_enable配置项不存在时，此时认为是一种没有配置的状态，开启/关闭按钮都不选中。其他情况根据配置值决定。

4.3 允许root用户登录ssh

此项策略用于控制是否允许root用户登录SSH服务器。如果文件/etc/ssh/sshd_config不存在，此项策略置灰。

开启操作：修改/添加配置项“PermitRootLogin yes” 关闭操作：修改/添加配置项“PermitRootLogin no” 读取操作：如果/etc/ssh/sshd_config不存在，策略配置项置灰，并提供说明。当PermitRootLogin配置项不存在时，此时认为是一种没有配置的状态，开启/关闭按钮都不选中。其他情况根据配置值决定。

4.4 登录ssh时密码不能为空

PermitEmptyPasswords参数指定是否允许空密码用户登录SSH服务器。如果文件/etc/ssh/sshd_config不存在，此项策略置灰。

开启操作：修改/添加配置项“PermitEmptyPasswords no” 关闭操作：修改/添加配置项“PermitEmptyPasswords yes” 读取操作：如果/etc/ssh/sshd_config不存在，策略配置项置灰，并提供说明。当PermitEmptyPasswords配置项不存在时，此时认为是一种没有配置的状态，开启/关闭按钮都不选中。其他情况根据配置值决定。

4.5 不允许SSH的HostbasedAuthentication

HostbasedAuthentication参数指定是否允许通过.rhosts或/etc/hosts.equiv用户的受信任主机进行身份验证，以及成功的公钥客户端主机身份验证。此选项仅适用于ssh协议版本2。如果文件/etc/ssh/sshd_config不存在，此项策略置灰。

开启操作：修改/添加配置项“HostbasedAuthentication no” 关闭操作：修改/添加配置项“HostbasedAuthentication yes” 读取操作：如果/etc/ssh/sshd_config不存在，策略配置项置灰，并提供说明。当HostbasedAuthentication配置项不存在时，此时认为是一种没有配置的状态，开启/关闭按钮都不选中。其他情况根据配置值决定。hostbasedauthentication参数指定是否允许通过.rhosts或/etc/hosts.equiv用户的受信任主机进行身份验证，以及成功的公钥客户端主机身份验证。此选项仅适用于ssh协议版本2。

4.6 允许SSH的IgnoreRhosts

IgnoreRhosts参数指定.rhosts和.shosts文件不会在RhostsRSAAuthentication或HostbasedAuthentication中使用。设置此参数将强制用户在使用ssh进行身份验证时输入密码。如果文件/etc/ssh/sshd_config不存在，此项策略置灰。

开启操作：修改/添加配置项“IgnoreRhosts yes” 关闭操作：修改/添加配置项“IgnoreRhosts no” 读取操作：如果/etc/ssh/sshd_config不存在，策略配置项置灰，并提供说明。当IgnoreRhosts配置项不存在时，此时认为是一种没有配置的状态，开启/关闭按钮都不选中。其他情况根据配置值决定。

4.7 不允许SSH的PermitUserEnvironment

PermitUserEnvironment参数指定是否允许用户通过ssh守护进程设置环境变量的能力，允许下可能造成用户绕过安全控制。例如，设置具有ssh执行特洛伊木马程序的执行路径。如果文件/etc/ssh/sshd_config不存在，此项策略置灰。

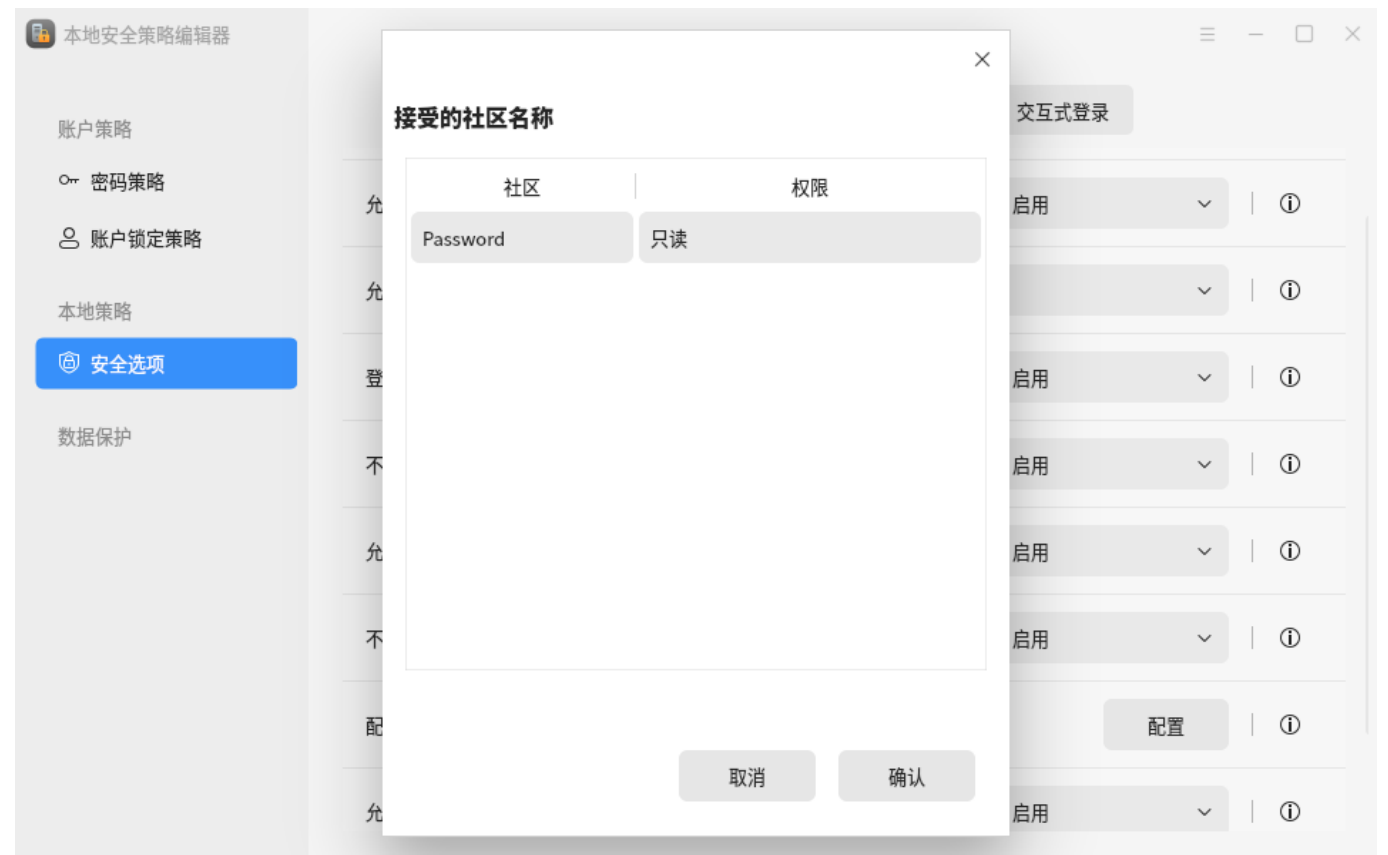
开启操作：修改/添加配置项“PermitUserEnvironment no”

关闭操作：修改/添加配置项“PermitUserEnvironment yes”

读取操作：如果/etc/ssh/sshd_config不存在，策略配置项置灰，并提供说明。当PermitUserEnvironment配置项不存在时，此时认为是一种没有配置的状态，开启/关闭按钮都不选中。其他情况根据配置值决定。其他情况根据配置值决定。

4.8 配置snmp团体字

此项策略用于配置访问snmp服务的团体字。目前只支持修改，不支持删除或添加团体字。如果文件/etc/snmp/snmpd.conf不存在，此项策略置灰。



配置操作: 将指定的团体字写入文件中

读取操作：如果果/etc/snmp/snmpd.conf文件不存在，策略配置项置灰，并提供说明。

1.查找rocommunity或者rwcommunity命令后面的团体字，格式如下：
“rocommunity public default -V systemonly” 或者 rwcommunity private default -V systemonly

2.将找到的团体字以列表形式返回

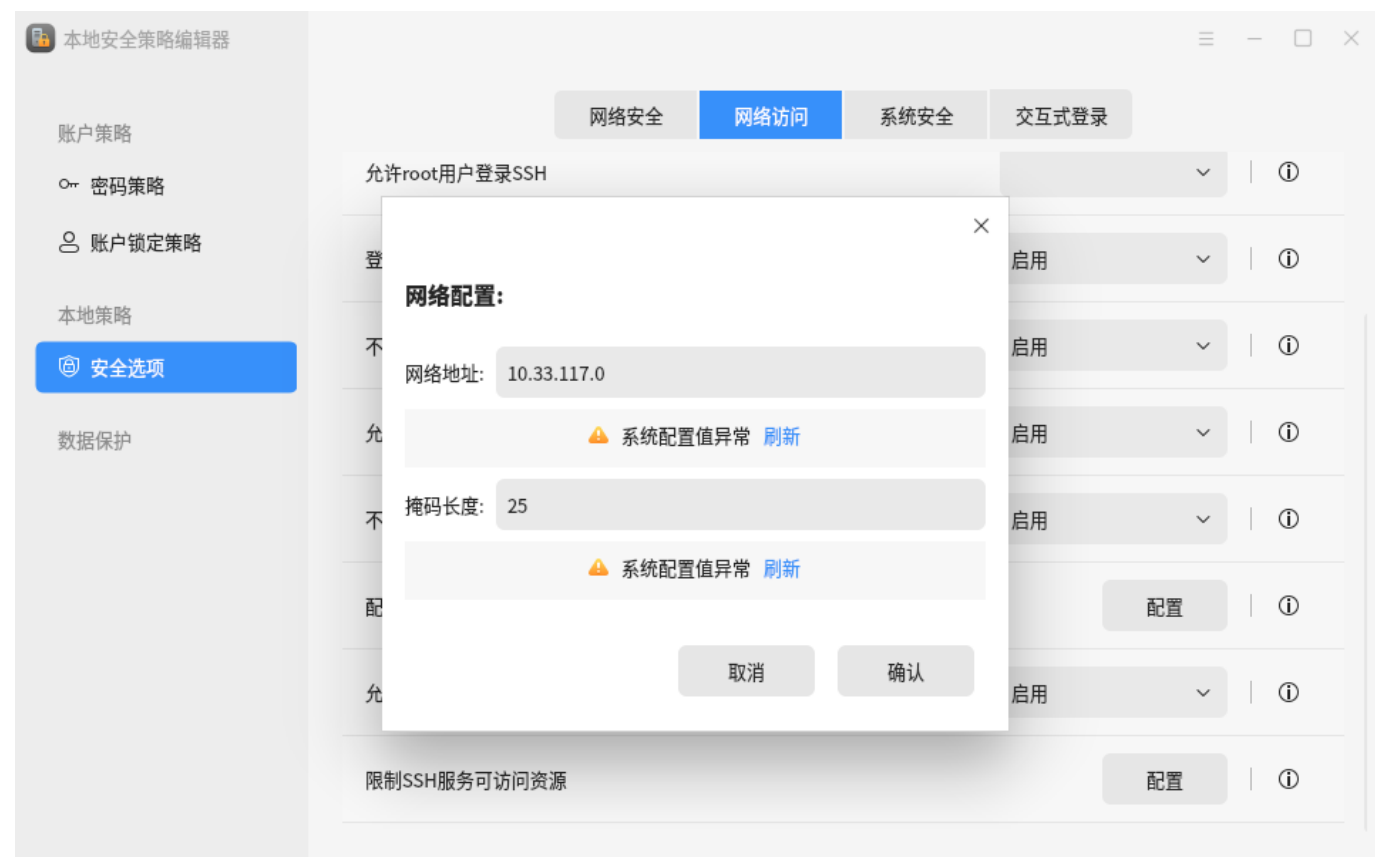
4.9 允许绑定多IP

multi 选项是用来控制如何处理主机名解析结果返回多个 IP 地址的情况。 multi on: 如果设置为 on，当一个主机名对应多个 IP 地址时，gethostbyname 函数会返回所有 IP 地址。这个选项对于实现一些特定的网络功能，例如负载均衡，可能非常有用，因为应用程序可以在多个服务器之间分配请求。 multi off: 如果设置为 off，当一个主机名对应多个 IP 地址时，gethostbyname 只返回一个 IP 地址。这样的处理简化了网络应用开发，但是牺牲了可能的负载均衡和故障转移功能。

开启操作：1.如果/etc/host.conf文件不存在,则创建文件 2.修改/添加配置项multi = on 关闭操作：1.如果/etc/host.conf文件不存在,则创建文件 2.修改/添加配置项multi = off 读取操作：当PermitUserEnvironment配置项不存在时，此时认为是一种没有配置的状态，开启/关闭按钮都不选中。其他情况根据配置值决定。其他情况根据配置值决定。

4.10 限制SSH可访问服务资源

此项策略用于限制SSH访问源，使 SSH 服务只能从指定的 IP 网段访问。网络地址支持三种输入：
1.xxx.xxx.xxx,表示具体的网络地址 2.ALL，表示允许所有地址访问 3.-ALL，表示不允许所有地址访问 如果文件/etc/security/access.conf不存在，此项策略置灰。



配置操作：修改或添加配置项 +:ALL:"xxx.xxx.xxx.0"/24，同时还需写入 -:ALL:ALL，这样才能完全限制。 读取操作：如果文件/etc/security/access.conf不存在，策略配置项置灰，并提供说明。 1.查询文件/etc/security/access.conf中内容 +:ALL:"xxx.xxx.xxx.0"/24，将网络地址和长度返回。 2.如果内容为 +:ALL:ALL,将返回"addr : ALL,len:0",表示允许所有地址 3.如果只存在 -:ALL:ALL,将返回"addr:-ALL,len:0"，表示不允许所有地址

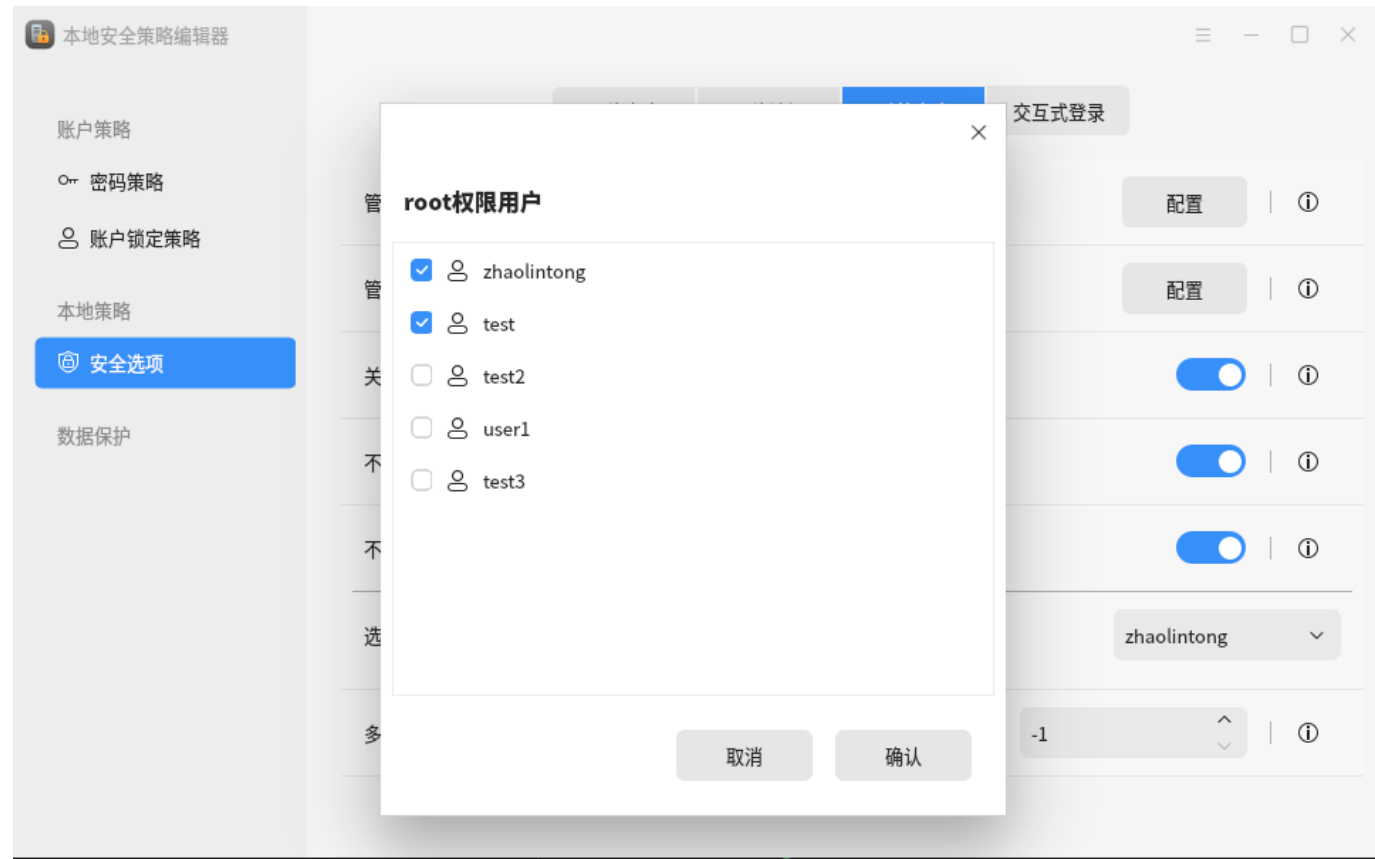
安全选项/系统安全

进入应用，点击左侧“安全选项”选项，再将tab页切换到“系统安全”即可进入安全选项/网络安全配置界面。



5.1 管理sudo权限用户

此项策略用于配置哪些用户可以使用sudo权限，防止用户对系统做出破坏性更改或恶意提权操作。如果文件/etc/sudoers不存在，此项策略置灰。

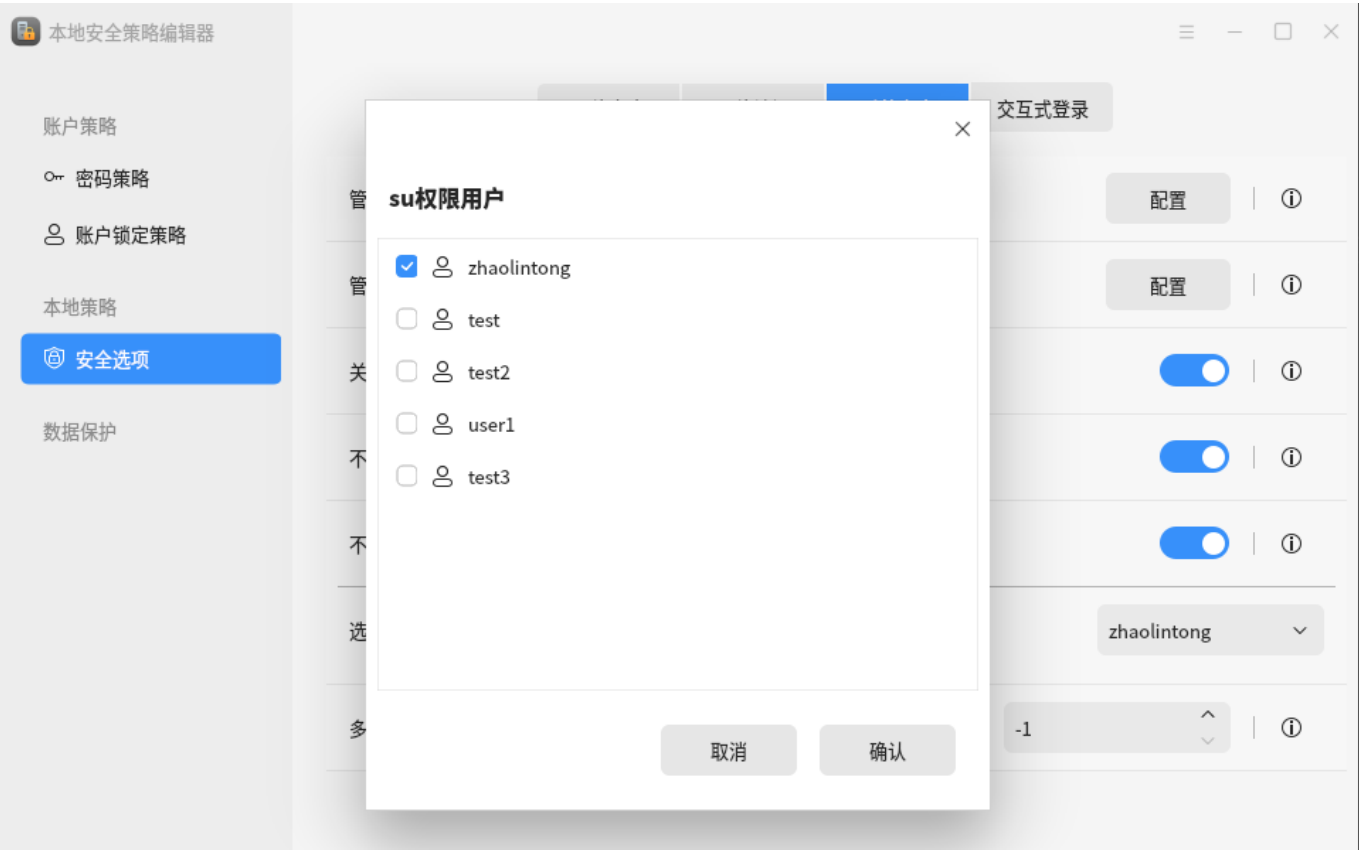


配置操作：1.对于取消勾选的操作：-----如果用户配置存在/etc/sudoers文件中，则删除。-----如果用户配置存在/etc/sudoers文件的配置组中，则从组中删除。2.对于勾选的操作：-----如果用户信息不存在/etc/sudoers文件中以及配置组中，则在/etc/sudoers文件中新增用户行，否则不处理

读取操作：1.如果文件不存在，配置项置灰，不能操作。2.在文件/etc/sudoers中，查找ALL所在的行，比如：root ALL=(ALL:ALL) ALL %admin ALL=(ALL) ALL %sudo ALL=(ALL:ALL) ALL 3.建立sudo用户列表，定义在文件的用户加入sudo用户列表，如果是group组，遍历group组内的用户，将其加入sudo用户列表。4.收集系统收的所有用户列表，同时遍历sudo用户列表，判断是否拥有sudo权限，并返回所有的用户列表。

5.2 管理su权限用户

此项策略用于配置哪些用户可以使用su权限。限制su权限，使用sudo替代，使系统管理员能够更好地控制用户权限升级以执行特权命令。sudo实用程序还提供了更好的日志记录和审计机制，因为它可以记录通过sudo执行的每个命令，而su只能记录用户执行su程序。如果文件/etc/pam.d/su不存在，此项策略置灰。



配置操作：1.如果配置了“使用su命令的group组”，比如形如“auth required pam_wheel.so root_only group=xxx use_uid” 则对xxx组中用户进行增删操作，将勾选的用户增加到xxx组中，未勾选的用户从xxx组中删除。2.如果没有配置的“使用su命令的group组” -----先增加wheel配置，配置如下：“auth required pam_wheel.so root_only group=wheel use_uid” -----然后将勾选的用户增加到wheel组中，未勾选的用户从whell组中删除。

读取操作：1.如果文件不存在，配置项置灰，不能操作。2.在文件/etc/pam.d/su中，查找如下的行，获取有su权限的group，比如：auth required pam_wheel.so root_only group=wheel use_uid 3.从上述group中获取哪些用户，将这些标记为“允许su命令” 4.返回当前系统上的所有用户，将“允许su命令”的用户设置成1，其他设置成0；5.如果配置不存在，认为所有用户都没有“su命令”执行权限

5.3 关闭系统CoreDump

核心转储文件是当一个程序因为异常终止（如访问违规、段错误等）时，操作系统保存的那部分程序的内存镜像文件，因此可能会出现信息泄露的情况 此项策略用于控制是否启用core cump功能。 如果文件/proc/sys/kernel/core_pattern或文件/etc/sysctl.conf不存在，此项策略置灰。

开启操作：1.修改/proc/sys/kernel/core_pattern文件，将配置修改为"|"配置 2.修改/etc/sysctl.conf文件中，将配置改为kernel.core_pattern = | 关闭操作：1.修改/proc/sys/kernel/core_pattern文件,将配置改为 | /lib/systemd/systemd-coredump %P %u %g %s %t 9223372036854775808 %h 2.修改/etc/sysctl.conf文件中，将配置改为kernel.core_pattern = | /lib/systemd/systemd-coredump 读取操作：1.扫描/proc/sys/kernel/core_pattern文件，查看以“|”管道字符开头，且“|”管道字符后面路径包含/usr/lib/systemd/systemd-coredump 比如禁用：| 比如启用：| /lib/systemd/systemd-coredump %P %u %g %s %t 9223372036854775808 %h 2.扫描/etc/sysctl.conf文件中存在“kernel.core_pattern”关键词，查看其后路径是否只为“|”管道字符 比如禁用：kernel.core_pattern = | 比如启用：kernel.core_pattern = /tmp/core-%p-%e-%t 3.如果/proc/sys/kernel/core_pattern文件存在配置"| " 并且 /etc/sysctl.conf文件中存在配置“kernel.core_pattern = |”，则认为开启状态，否则认为是关闭状态。 4.如果/proc/sys/kernel/core_pattern文件和/etc/sysctl.conf文件不存在，则当前策略置灰，不能编辑。

5.4 不允许Ctrl+Alt+Delete组合键

此项策略用于控制是否使用组合键ctrl+alt+delete触发重启或注销。 如果文件/proc/sys/kernel/ctrl-alt-del或文件/etc/systemd/system.conf不存在，此项策略置灰。

开启操作：1.执行echo 0 > /proc/sys/kernel/ctrl-alt-del命令将内核参数值置为“0”；2.修改系统配置文件/etc/systemd/system.conf,将CtrlAltDelBurstAction行替换为CtrlAltDelBurstAction=none 3. 删除/usr/lib/systemd/system/ctrl-alt-del.target这个文件 关闭操作: 1.执行echo 1 > /proc/sys/kernel/ctrl-alt-del命令将内核参数值置为“1”；2.修改系统配置文件/etc/systemd/system.conf,将CtrlAltDelBurstAction行删除 3. 建立软连接将/usr/lib/systemd/system/ctrl-alt-del.target文件指向同目录下的reboot.target文件 读取操作：1.如果/proc/sys/kernel/ctrl-alt-del文件或/etc/systemd/system.conf文件不存在，当前策略置灰，不能编辑。 2.检查/proc/sys/kernel/ctrl-alt-del文件，看此内核参数是否配置为“0”；3.检查/etc/systemd/system.conf，看"CtrlAltDelBurstAction"是否配置为"none" 4.检查/usr/lib/systemd/system/ctrl-alt-del.target这个文件不存在。 如果上述条件都满足，则认为是开启状态，否则是关闭状态。

5.5 不允许系统自动登录

此项策略用于配置哪个用户允许自动登录系统。 如果某个用户启用了此选项，则不会要求该用户提供密码，而将自动登录系统。 如果文件/etc/lightdm/lightdm.conf不存在，此项策略置灰。

配置操作：1.将选中的用户名写入到/etc/lightdm/lightdm.conf文件里[SeatDefaults]节中的autologin-user参数 扫描：1.如果/etc/lightdm/lightdm.conf文件不存在，配置项置灰，不能操作。 2.读取/etc/lightdm/lightdm.conf文件里[SeatDefaults]节中的autologin-user参数 3.如果autologin-user参数不存在或值为空，则表示没有自动登入用户，开关选项关闭，用户列表隐藏 4.如果autologin-user参数值存在，但是用户名无效，则表示没有自动登入用户，开关选项关闭，用户列表隐藏 5.如果autologin-user参数值存在且用户名有效，开关选项开启，用户列表显示，并选中对应用户项

5.6 多重并发数量

此项策略用于配置系统并发会话的最大数量，通过限制会话数量，防止过多的登录会话占用系统资源等行为。如果文件/etc/security/limits.conf不存在，此项策略置灰。

配置操作：1.将配置写入到/etc/security/limits.conf文件里的maxlogins参数中 目前UI上maxlogins限制的范围[-1, 10] 扫描：1.如果/etc/security/limits.conf文件不存在，配置项置灰，不能操作。2.查找"* hard maxlogins 1"这样的行 3.如果找到，读取/etc/security/limits.conf文件里的maxlogins参数 4.如果查找不到或者max_login配置值无效时，返回默认值-1

安全选项/交互式登录

进入应用，点击左侧“安全选项”选项，再将tab页切换到“交互式登录”即可进入安全选项/网络交互式登录配置界面。



6.1 不显示上次登录

该安全设置确定登录屏幕是否将显示上次登录该台电脑的人的用户名。如果启用该策略，将不显示用户名。如果禁用该策略，将显示用户名。

开启操作：1.创建全局配置文件/etc/hushlogins 关闭操作 1.删除全局配置文件/etc/hushlogins，并遍历删有效用户主目录下的.hushlogin文件。 扫描：1.如果全局配置文件/etc/hushlogins存在，则禁用显示上次登录信息。2.每个有效用户主目录下存在.hushlogin文件，则禁用显示上次登录信息。3.如果上述条件不满足，则显示上次登录信息。

6.2 计算机不活动限制

此项配置是针对tty会话的超时限制。如果非活动状态超出时间限制，就退出当前会话。如果文件/etc/profile不存在，此项策略置灰。

配置操作：1.将配置参数写入文件 TMOUT取值范围;[0, 99999] 读取操作：1.检查/etc/profile文件，如果文件不存在策略项置灰，不能编辑策略 2.读取/etc/profile文件中的配置形如：export TMOUT=10 3.如果配置不存在，则认为是TMOUT==0，其他按照时间情况返回。

6.3 试图登录的用户的消息提示

此项策略用于设置，用于登录系统前看到的内容。 文本通常用于法律原因，例如，警告用户滥用公司信息的后果或其操作可能要经过审核。



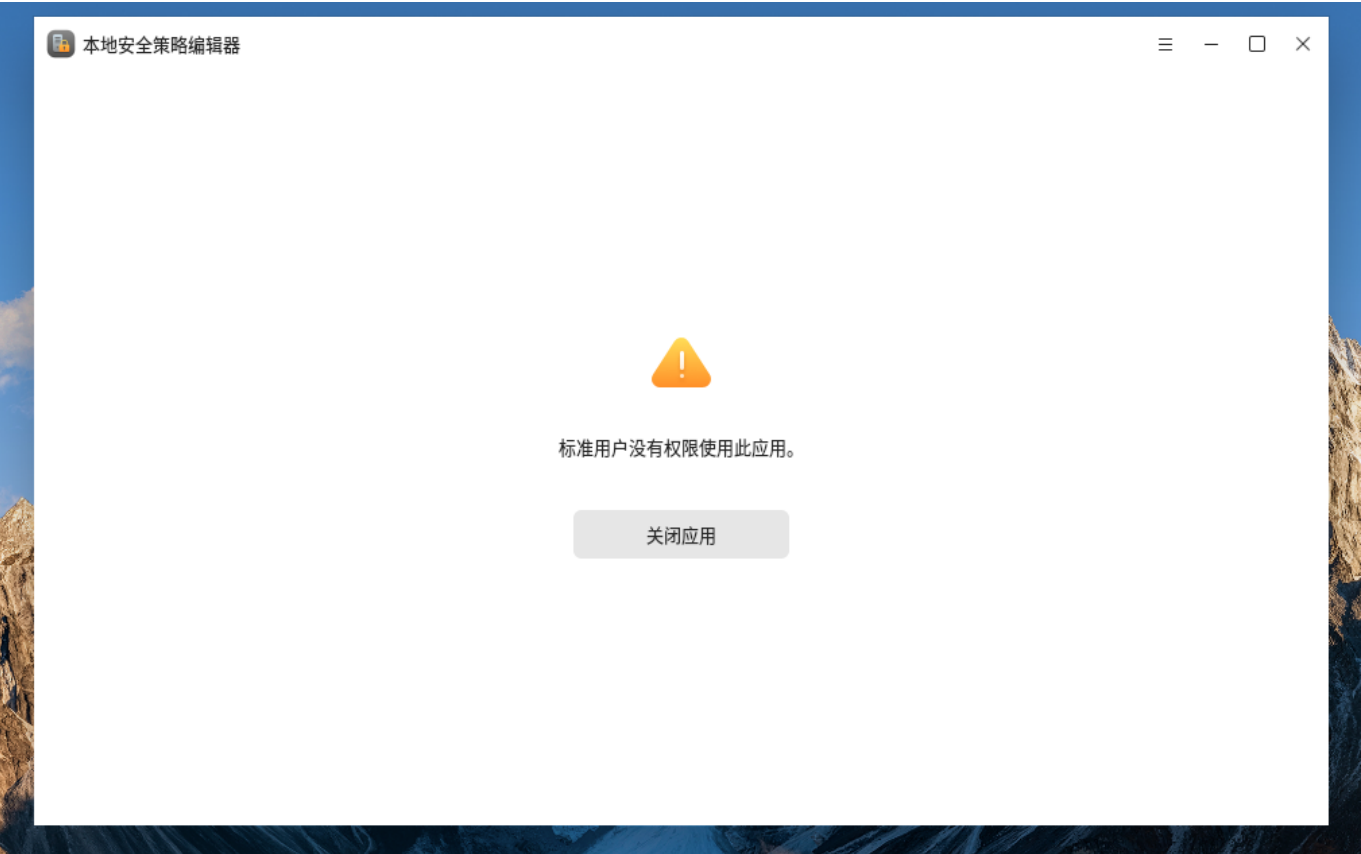
配置操作：1.如果/etc/issue文件不存在，创建文件。 2.将配置内容写入文件 备注：重新登录tty即可看到登录时的提示 读取操作：1.读取/etc/issue文件内容，如果文件不存在返回空，其他返回实际值

7 其他

本地安全策略编辑器除了上述基本功能外，还提供了” 软件说明”、” 登录权限界面”、” 异常消息提示”、” 异常操作对话框” 等辅助功能。

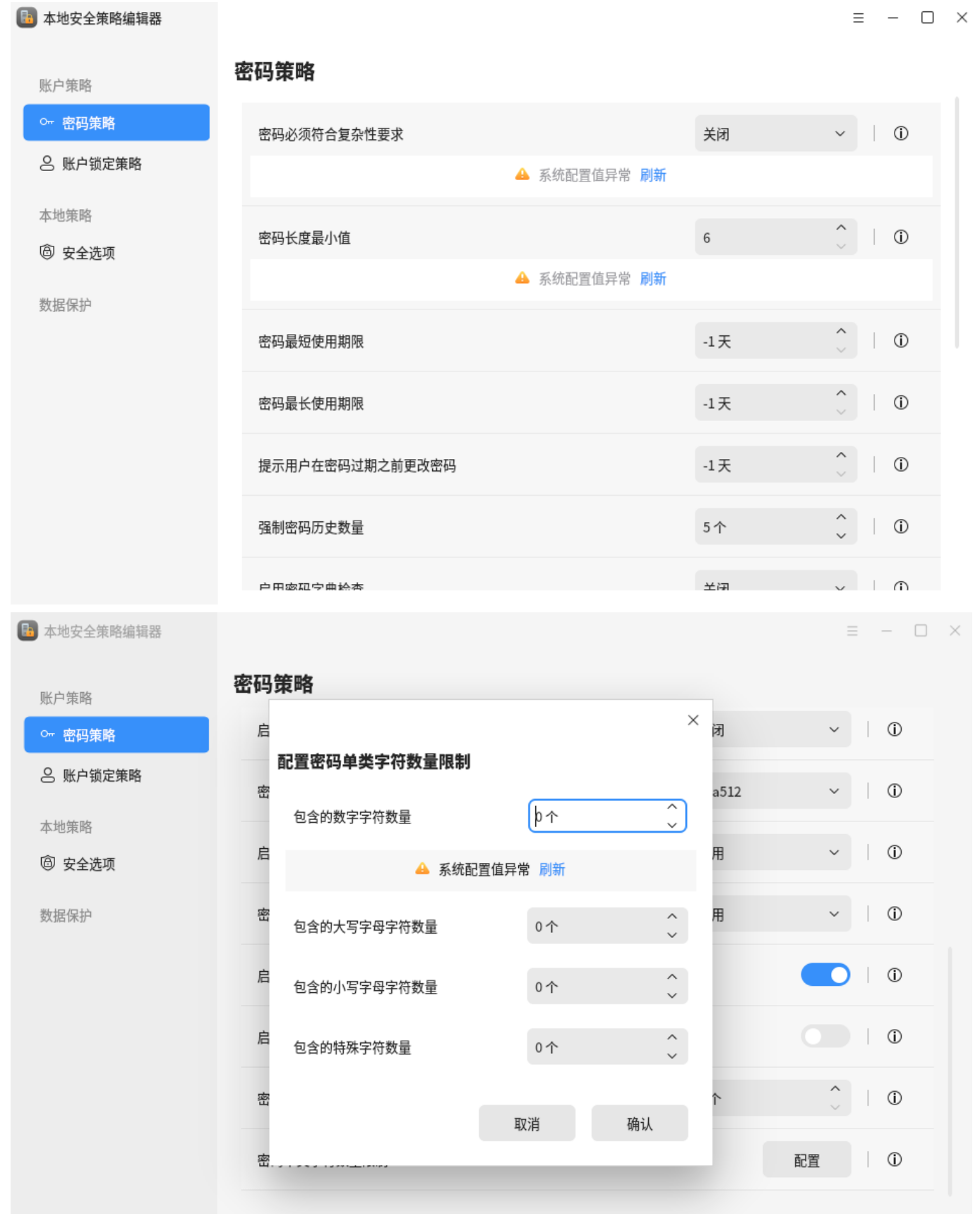
7.1 登录权限界面

当尝试用非root用户登入策略编辑器，将会提示如下界面：



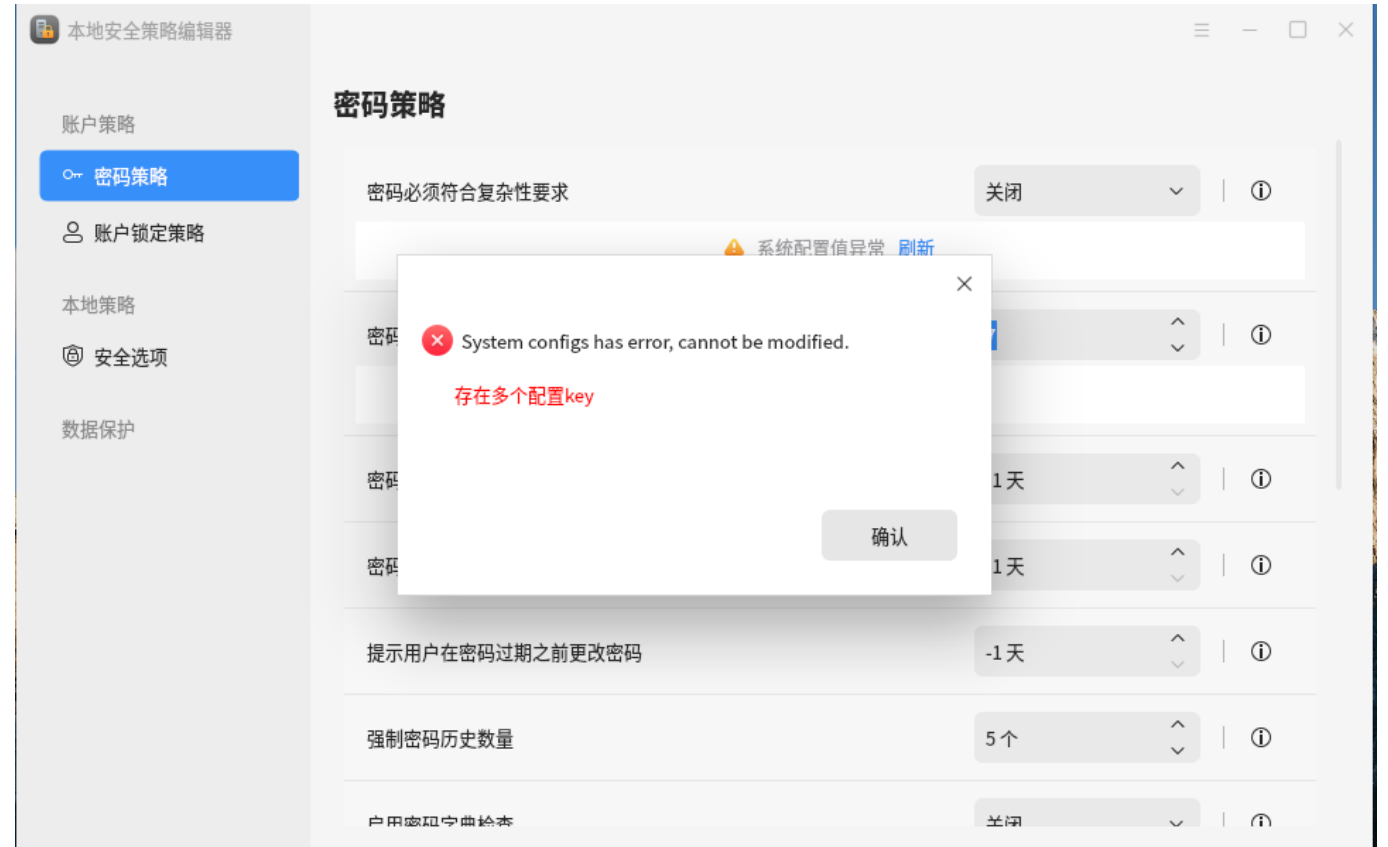
7.2 错误消息提示

当打开策略编辑器时，应用会进行一次完整数据的读取操作，如果有数据项目读取异常，将以” 错误消息提示” 展现。点击” 刷新” 按钮，将尝试重新读取，如果读取成功，” 错误消息提示” 消失，否则依然存在。



7.3 操作异常对话框

当用户去写入配置数据时，如果遇到写入异常，将弹出异常对话框。



附录：常见问题及处理方法(FAQ)

1.当用户名长度小于4，并且开启usercheck检查，结果未检测包含用户名

- 答：pwquality库在是否包含用户名检查时，如果用户名长度<4,会忽略用户名检查，直接通过。

2.用户手动改了系统sshd_config配置，当时没有重启ssh服务，编辑器状态不同步

- 答：目前暂时无法获取ssh服务实际生效的配置值，所以策略编辑器只能反映sshd_config配置文件中的值