

补充说明：

1. 变更说明:

“authselect select sssd --force” 命令会触发 authselect sssd 配置集生效。

sssds 策略生效后改变 pam 和 nsswitch.conf 文件的默认配置。下面对变更的配置进行说明：

(1) pam 配置变更

- 如图 1 图 2 所示,password-auth 和 system-auth 文件与原有的 pam 规则相比，增加了账号类型的判断以及认证失败延迟认证的逻辑，减少对用户认证失败锁定的规则和 UID 的检查。

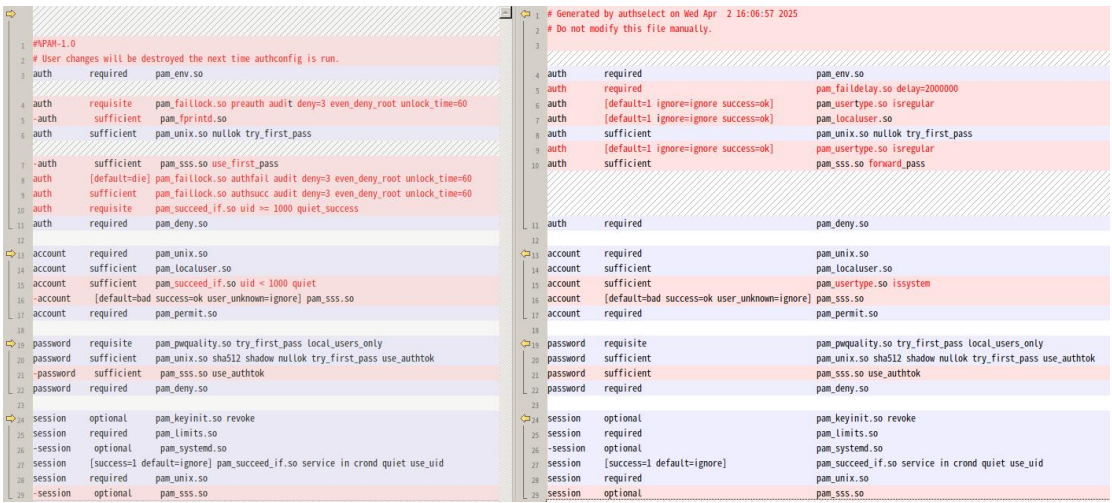


图 1 password-auth 配置变更（左边变更前，右边变更后）

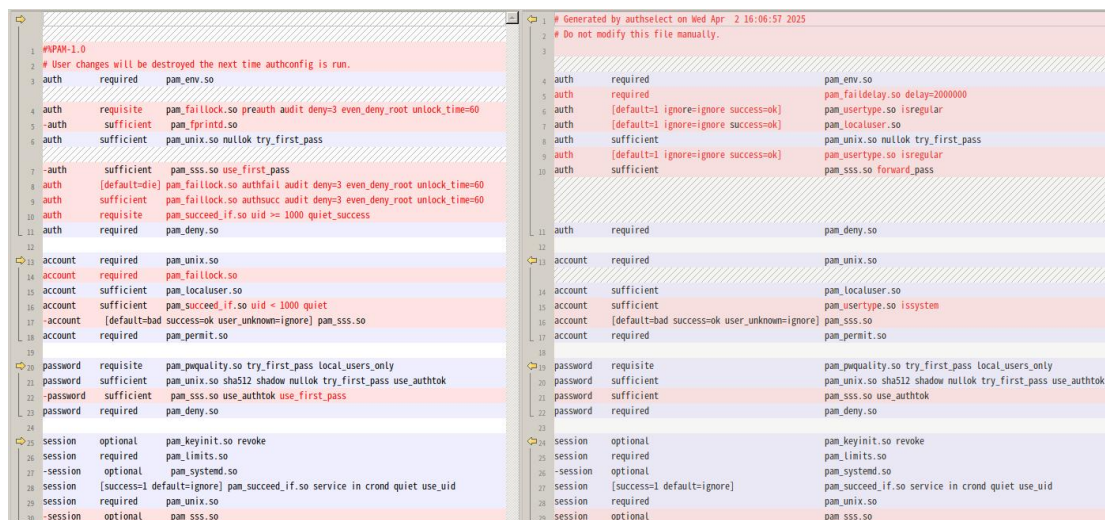


图 2 system-auth 配置变更（左边变更前，右边变更后）

- postlogin 文件中多了一行配置 session optional pam\_umask.so silent（图 3）。

引入 pam\_umask.so 模块。

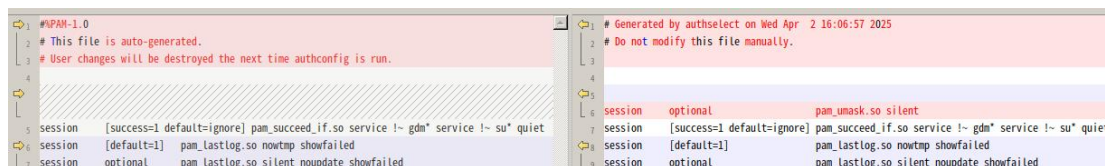


图 3 postlogin 配置变更（左边变更前，右边变更后）

## (2) 对/etc/nsswitch.conf 配置影响分析

authselect select sssd --force 命令执行后/etc/nsswitch.conf 文件多个配置项发生了变化，具体变更如图 4。

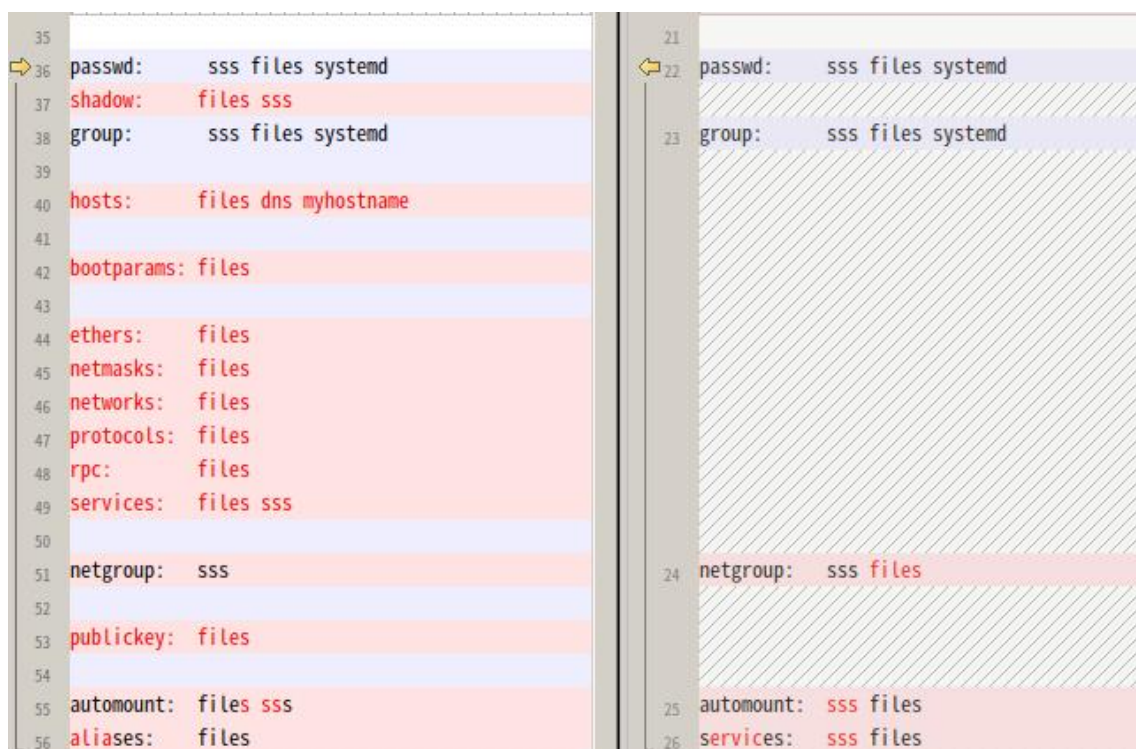


图 4 nsswitch.conf 配置变更（左边变更前，右边变更后）

修改项如下：

- netgroup 配置项原有内容 sss，修改为 sss files。修改后，netgroup 的查询顺序变为先从 sss 获取，然后从本地文件（/etc/netgroup）获取。
- automount 配置项原有内容 files sss，修改为 sss files。系统将优先使用 SSS（网络）提供的自动挂载配置如 LDAP 中的 auto.\*规则），本地文件（如 /etc/auto.master）仅作备用。
- services 配置项原有内容为 files sss，修改为 sss files。修改后，服务名称与端口号解析将优先使用 SSS 提供的定义，而非本地/etc/services。

删除项如下：

- shadow 删除，系统将不再从 sss 获取影子密码信息，只依赖本地文件（/etc/shadow）。如果系统依赖 sss 提供影子密码信息，可能会导致用户登录失败。

- hosts 配置项删除，系统会先通过 DNS 解析，再查询/etc/hosts，忽略 myhostname 本地主机名逻辑。这可能导致本地/etc/hosts 的配置失效。
- bootparams 配置项删除，无默认规则。
- publickey 配置项删除，无默认规则。
- 其余项在删除后使用隐式规则，从 files 查询，与原有配置文件逻辑一致。

## 2. authselect 配置变更后的回滚方案:

### (1) 针对 authselect select sssd --force 命令生效后的回滚方案:

对于已启用 sssd 且权限配置不当的系统，通过以下操作可实现回退功能

#### 1) 查看当前备份

```
#authselect backup-list
```



```
[root@localhost ~]# authselect backup-list
2025-04-01-08-45-17.K1uj8t (创建于 2025年04月01日 星期二 16时45分17秒)
[root@localhost ~]# ls -lh /etc/pam.d/
```

图 authselect 备份列表

#### 2) 回退到之前的配置

```
#authselect backup-restore 2025-04-01-08-45-17.K1uj8t
```

### 特别说明:

1. 通过 ks 文件（包含配置 “auth --enablesshadow --passalgo=sha512” 参数）安装 V10 SP1/SP2/SP3 ISO 系统镜像，系统配置不会发生变更。（authselect 版本小于 1.2.1-1.p01.ky10 版本）
2. 通过 ks 文件（包含配置 “auth --enablesshadow --passalgo=sha512” 参数）安装 V10 SP3 2403 ISO 系统镜像，系统配置会发生变更。