Linux权限管理：umask与SUID

目录

umask介绍

- **umask**: user mask的缩写
- 用于控制新创建文件和目录的默认权限
- 是Linux/Unix权限管理的基础组件
- 本质是一个"屏蔽码"，用于屏蔽默认权限

umask工作原理

- **文件**最大默认权限：666 (rw-rw-rw-)
- **目录**最大默认权限：777 (rwxrwxrwx)
- 实际权限计算方式：
  - 文件权限 = 666 - umask
  - 目录权限 = 777 - umask

umask常见配置

- 022

  : 标准设置

  - 文件: 644 (rw-r--r--)
  - 目录: 755 (rwxr-xr-x)
- 027

  : 增强安全性

  - 文件: 640 (rw-r-----)
  - 目录: 750 (rwxr-x---)
- 077

  : 高安全性

  - 文件: 600 (rw-------)

- 目录: 700 (rwx------)

---

umask实例

```
# 查看当前umask值
umask

# 临时修改umask值
umask 027

# 永久设置umask（添加到配置文件）
echo "umask 027" >> ~/.bashrc
```

SUID介绍

- **SUID**: Set User ID
- 特殊权限位，允许用户以文件所有者的权限执行程序
- 解决了普通用户需要特权执行的场景
- 临时提升权限的一种机制

SUID权限表示

- 符号表示

  : 执行位置的

  ```
  x
  ```

  变为

  ```
  s
  ```

  - 如：`rwsr-xr-x`
- 数字表示

  : 在普通权限前加

  ```
  4
  ```

  - 如：`4755`
- 只对可执行文件有意义

SUID常见应用

常见的SUID程序：

- `/bin/su`: 切换用户身份
- `/bin/passwd`: 修改密码
- `/bin/ping`: 发送ICMP包
- `/usr/bin/sudo`: 以其他用户身份执行命令

这些程序需要root权限才能完成功能

SUID安全风险

- SUID程序执行时具有所有者（通常是root）权限
- 安全风险：
  - 可能被利用提升权限
  - 可能导致权限升级攻击
  - 可能暴露系统漏洞
- 需谨慎使用和管理SUID权限

实用命令速查

```
# 查找系统中的SUID文件
find / -perm -4000 -type f -exec ls -l {} \; 2>/dev/null

# 设置SUID权限
chmod u+s filename
chmod 4755 filename

# 移除SUID权限
chmod u-s filename
chmod 0755 filename
```

最佳实践

- umask设置
  - 服务器环境推荐使用027或077
  - 个人桌面环境可使用022
- SUID权限管理
  - 仅在必要时设置
  - 定期审计系统SUID文件
  - 确保SUID程序代码安全
  - 考虑使用sudo替代SUID