Chế Độ Phân Quyền Đặc Biệt Trong Linux

1. SUID (Set User ID)

1.1 Khái Niệm

```
- Cho phép tập tin thực thi chạy với quyền của chủ sở hữu
- Thường dùng cho các chương trình cần quyền root tạm thời
- Được đánh dấu bằng 's' trong quyền thực thi của owner
```

1.2 Cú Pháp và Ví Dụ

```
# Thiết lập SUID
chmod u+s filename
chmod 4755 filename

# Kiểm tra
ls -l /usr/bin/passwd
-rwsr-xr-x root root /usr/bin/passwd

# Xóa SUID
chmod u-s filename
```

1.3 Ứng Dụng Thực Tế

```
#!/bin/bash
# Ví dụ: Chương trình thay đổi mật khẩu

# 1. Tạo script
cat > change_password.sh << 'EOF'
#!/bin/bash
if [ "$1" = "" ]; then
    echo "Usage: $0 username"
    exit 1
fi
passwd $1
EOF

# 2. Đặt quyền
chmod u+s change_password.sh
```

2. SGID (Set Group ID)

2.1 Khái Niệm

```
Trên File:
- Chạy với quyền của group sở hữu
- Đánh dấu 's' trong quyền thực thi của group

Trên Directory:
- Files mới tạo kế thừa group của thư mục
- Hữu ích cho thư mục chia sẻ
```

2.2 Cú Pháp và Ví Dụ

```
# Thiết lập SGID
chmod g+s directory
chmod 2755 directory

# Kiểm tra
ls -ld directory
drwxr-sr-x 2 root developers directory

# Xóa SGID
chmod g-s directory
```

2.3 Ứng Dụng Thực Tế

```
#!/bin/bash
# Tạo thư mục chia sẻ cho nhóm

# 1. Tạo thư mục và nhóm
groupadd developers
mkdir /shared
chgrp developers /shared

# 2. Thiết lập SGID
chmod g+s /shared
```

3. Sticky Bit

3.1 Khái Niệm

```
- Chỉ owner mới có thể xóa file
- Thường dùng cho thư mục công cộng
- Đánh dấu 't' trong quyền others
```

3.2 Cú Pháp và Ví Dụ

```
# Thiết lập Sticky Bit
chmod +t directory
chmod 1755 directory

# Kiểm tra
ls -ld /tmp
drwxrwxrwt 15 root root /tmp

# Xóa Sticky Bit
chmod -t directory
```

3.3 Ứng Dụng Thực Tế

```
#!/bin/bash
# Tạo thư mục công cộng an toàn

# 1. Tạo thư mục
mkdir /public
chmod 777 /public

# 2. Thiết lập Sticky Bit
chmod +t /public
```

4. Kết Hợp Các Quyền Đặc Biệt

4.1 Biểu Diễn Số

```
SUID   = 4
SGID   = 2
Sticky = 1

Ví dụ:
chmod 4755 = SUID + rwxr-xr-x
chmod 2755 = SGID + rwxr-xr-x
chmod 1755 = Sticky + rwxr-xr-x
```

4.2 Script Tổng Hợp

```
#!/bin/bash
# Thiết lập tất cả quyền đặc biệt

setup_special_permissions() {
    local dir=$1

    # SGID + Sticky cho thư mục
```

```
    chmod 3775 "$dir"  # 3 = 2(SGID) + 1(Sticky)

    # Kiểm tra
    ls -ld "$dir"
}
```

5. Bảo Mật và Best Practices

5.1 Nguyên Tắc An Toàn

```
1. Hạn chế sử dụng SUID:
   - Chỉ dùng khi thực sự cần thiết
   - Thường xuyên rà soát

2. Kiểm soát SGID:
   - Áp dụng cho thư mục chia sẻ
   - Giới hạn quyền ghi

3. Quản lý Sticky Bit:
   - Dùng cho thư mục công cộng
   - Kết hợp với quota
```

5.2 Kiểm Tra và Giám Sát

```
# Tìm tất cả file có SUID
find / -perm -4000

# Tìm tất cả file có SGID
find / -perm -2000

# Tìm thư mục có Sticky bit
find / -type d -perm -1000
```

5.3 Script Kiểm Tra

```
#!/bin/bash
# Kiểm tra quyền đặc biệt

check_special_permissions() {
    echo "=== Files with SUID ==="
    find / -perm -4000 2>/dev/null

    echo "=== Files with SGID ==="
    find / -perm -2000 2>/dev/null

    echo "=== Directories with Sticky Bit ==="
```

```
    find / -type d -perm -1000 2>/dev/null
}
```

6. Xử Lý Sự Cố

6.1 Vấn Đề Thường Gặp

```
1. SUID không hoạt động:
   - Kiểm tra filesystem (nosuid)
   - Kiểm tra SELinux/AppArmor

2. SGID không kế thừa:
   - Kiểm tra ACL
   - Kiểm tra umask

3. Sticky Bit không bảo vệ:
   - Kiểm tra quyền thư mục
   - Kiểm tra quyền root
```

6.2 Script Khắc Phục

```
#!/bin/bash
# Khắc phục vấn đề quyền đặc biệt

fix_permissions() {
    local path=$1

    # Reset về quyền mặc định
    chmod 755 "$path"

    # Áp dụng lại quyền đặc biệt
    case $2 in
        "suid") chmod u+s "$path" ;;
        "sgid") chmod g+s "$path" ;;
        "sticky") chmod +t "$path" ;;
    esac
}
```