Access Control List (ACL) Trong Linux

1. Giới Thiệu về ACL

1.1 Khái Niệm Cơ Bản

```
ACL mở rộng hệ thống phân quyền truyền thống:
- Phân quyền chi tiết cho nhiều user/group
- Linh hoạt hơn mô hình owner/group/others
- Hỗ trợ quyền mặc định cho thư mục
```

1.2 Lợi Ích

```
1. Quản Lý Chi Tiết:
   - Quyền riêng cho từng user
   - Quyền riêng cho từng group

2. Linh Hoạt:
   - Kết hợp với quyền truyền thống
   - Thừa kế quyền tự động
```

2. Làm Việc với ACL

2.1 Kiểm Tra ACL

```
# Xem ACL hiện tại
getfacl filename

# Kiểm tra nhiều file
getfacl file1 file2

# Xem chi tiết
getfacl -R directory    # Đệ quy
```

2.2 Thiết Lập ACL

```
# Cấp quyền cho user
setfacl -m u:username:rwx file

# Cấp quyền cho group
setfacl -m g:groupname:rx file

# Thiết lập mặc định cho thư mục
```

```
setfacl -d -m u:username:rwx directory

# Xóa ACL
setfacl -b file        # Xóa tất cả
setfacl -x u:username file  # Xóa specific
```

3. Ví Dụ Thực Tế

3.1 Quản Lý Dự Án

```
#!/bin/bash
# Thiết lập thư mục dự án

# Tạo cấu trúc
mkdir -p /projects/web
cd /projects/web

# Thiết lập quyền cơ bản
chmod 770 .

# Thiết lập ACL
# Dev có full access
setfacl -m u:dev1:rwx .
setfacl -m u:dev2:rwx .

# QA chỉ đọc và thực thi
setfacl -m u:qa1:rx .
setfacl -m u:qa2:rx .

# Mặc định cho files mới
setfacl -d -m u:dev1:rwx .
setfacl -d -m u:dev2:rwx .
setfacl -d -m u:qa1:rx .
setfacl -d -m u:qa2:rx .
```

3.2 Quản Lý Log

```
#!/bin/bash
# Thiết lập quyền log

# Thiết lập ACL cho log dir
setfacl -m g:sysadmin:rwx /var/log
setfacl -m g:security:rx /var/log

# Mặc định cho files mới
setfacl -d -m g:sysadmin:rw /var/log
setfacl -d -m g:security:r /var/log
```

4. ACL Nâng Cao

4.1 Mask ACL

```
# Thiết lập mask
setfacl -m m::rx file

# Kiểm tra effective permissions
getfacl -e file

# Ví dụ kết hợp
setfacl -m u:user1:rwx,m::rx file
```

4.2 Backup và Restore ACL

```
# Backup ACL
getfacl -R /directory > acl.txt

# Restore ACL
setfacl --restore=acl.txt
```

5. Script Quản Lý ACL

5.1 Kiểm Tra và Áp Dụng ACL

```
#!/bin/bash

check_and_apply_acl() {
    local path=$1
    local user=$2
    local perms=$3

    # Kiểm tra ACL hiện tại
    if getfacl "$path" | grep -q "^user:$user"; then
        echo "ACL đã tồn tại cho $user"
    else
        # Áp dụng ACL mới
        setfacl -m u:$user:$perms "$path"
        echo "Đã thêm ACL cho $user"
    fi
}

# Sử dụng
check_and_apply_acl "/data" "user1" "rwx"
```

5.2 Quản Lý ACL Hàng Loạt

```bash
#!/bin/bash

apply_project_acl() {
    local project_dir=$1
    local dev_group=$2
    local qa_group=$3

    # Thiết lập quyền cơ bản
    chmod 770 "$project_dir"

    # Thiết lập ACL cho nhóm
    setfacl -R -m g:$dev_group:rwx "$project_dir"
    setfacl -R -m g:$qa_group:rx "$project_dir"

    # Thiết lập mặc định
    setfacl -R -d -m g:$dev_group:rwx "$project_dir"
    setfacl -R -d -m g:$qa_group:rx "$project_dir"

    echo "Đã áp dụng ACL cho $project_dir"
}

# Sử dụng
apply_project_acl "/projects/app" "developers" "testers"
```

6. Best Practices

6.1 Nguyên Tắc Sử Dụng

```
1. Tối Thiểu Hóa ACL
   - Chỉ dùng khi cần thiết
   - Ưu tiên quyền truyền thống

2. Quản Lý Hiệu Quả
   - Backup ACL thường xuyên
   - Kiểm tra định kỳ

3. Theo Dõi Performance
   - ACL có thể ảnh hưởng hiệu suất
   - Giới hạn số lượng ACL
```

6.2 Kiểm Tra Hệ Thống

```bash
#!/bin/bash
# Kiểm tra hỗ trợ ACL

check_acl_support() {
    if mount | grep -q "acl"; then
```

```
        echo "ACL được hỗ trợ"
    else
        echo "ACL không được hỗ trợ"
        echo "Thêm 'acl' vào /etc/fstab"
    fi
}

# Sửa /etc/fstab
# UUID=xxx / ext4 defaults,acl 0 1
```