Bab 7
User, Group dan Permission

Program D3 PJJ PENS ITS

Tujuan

- Setelah mempelajari materi dalam bab ini, mahasiswa diharapkan mampu:
  - Memahami atribut file dan ijin akses.
  - Memahami perintah untuk mengubah ijin akses suatu file.
  - Menggunakan perintah-perintah untuk mengubah ijin akses.

Materi

- Mengubah Identitas
- Permission (Hak Akses)
- Default Hak Akses
- Hak Akses Khusus

User dan Group

- Ketika sebuah nama file tersimpan di komputer maka akan terbentuk meta data (tabel data) yang menghubungkan nama file dengan nomor **inode** yang dikenal oleh komputer.
- Demikian juga kalau nama user dan group ditambahkan maka nama dan group tersebut tidak ditulis cukup dengan menulis nomor identitas dari user tersebut.
- Tabel yang menghubungkan antara nama user dengan nomor identitas user disimpan di file */etc/passwd* dan */etc/group*.
- Sedangkan file */etc/shadow* berisikan pemetaan antara nama user dengan password yang sudah disandikan.

File Penyimpanan User dan Group

Nama file	**Keterangan isi**
/etc/passwd	Nama user, password, Nomor uid, nomor gid, GECOS(nama lengkap), direktori home, program shell yang dijalankan saat login
/etc/group	Nama group, password group, gid, id anggota group
/etc/shadow	Nama user dan password,untuk lebih lengkap buka perintah **man 5 shadow**

Mengubah Identitas

- Merubah password dapat dilakukan dengan cara menjalankan perintah **passwd**.
- Sedangkan apabila ingin merubah menjadi user lain tanpa harus logout dapat dilakukan dengan menggunakan perintah su

Perintah su

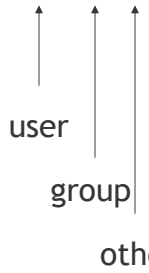
Perintah	*Keterangan*
su	Pindah sebagai login root
su -	Pindah sebagai login root dan pindah ke direktori homenya root
su Nama user	Pindah ke login Nama User
su – Nama user	Pindah ke login Nama User dan pindah ke direktori home dari user name

Perintah Informasi User

- `whoami` - Menampilkan identitas usergroups
- `id` - Menampilkan groups dari userUsers
- `who, w` - Menampilkan daftar user yang sedang login
- `last` - History login / reboot

Permission (Hak Akses)

```
-rwxrwxrwx 1 student test 1639 Oct 31 20:19 file
```



Mengubah Ijin Akses

- Format untuk mengubah ijin akses

```
chmod [ugoa] [= + -] [rwx] File(s)
chmod [ugoa] [= + -] [rwx] Dir(s)
```

dimana u = user (pemilik)
g = group (kelompok)
o = others (lainnya)
a = all

- Format lain dari chmod adalah menggunakan bilangan octal

Ijin Akses

- Ijin akses dibagi menjadi 3 peran yaitu :
  - Pemilik (Owner)
  - Kelompok (Group)
  - Lainnya (Others)
- Setiap peran dapat melakukan 3 bentuk operasi yaitu :
- Pada File
  - R (Read) Ijin untukmembaca
  - W (Write) Ijin untuk mengubah / membuat
  - X (Execute) Ijin untuk menjalankan program
- Pada Direktori
  - R (Read) Ijin untukmembaca daftar file dalam direktori
  - W (Write) Ijin untuk mengubah/membuat file di direktori
  - X (Execute) Ijin untuk masuk ke direktori (cd)

r w x
4 2 1 = 7

Hak Akses Default

- Jika membuat direktori maka akan memiliki hak akses penuh yaitu rwxrwxrwx atau 777.
- Sedangkan jika membuat file baru maka hak akses yang diberikan sebelum dirubah adalah rw_rw_rw_ atau 666.
- Tetapi selain hak akses tersebut masih terdapat perintah yang membatasi yaitu **umask**.
- Perintah umask digunakan umtuk mengurangi hak askses default.
- Sehingga hak akses yang dibuat akan memiliki nilai dari pengurangan dari hak akses default dikurangi dengan nilai umask.
- Nilai **umask** untuk user biasa adalah 002 sedangkan root 022.
- sehingga apabila user biasa membuat direktori akan memiliki hak askses 777 (default) dikurangkan dengan 002, hasilnya adalah 775 atau rwxrwxr-x.

Hak Akses Khusus

- Sebuah file dan direktor selain memiliki hak akses yang sudah dipelajari (rwx untuk user, group dan other), Juga memiliki hak khusus sebagai yang tersimpan pada 3 bit paling kiri setelah rwx untuk user.
- Tiga bit tersebut dinamakan suid, sgid dan sticky bit.
- Hak akses khusus ini jarang digunakan, dan hanya effektif pada kondisi tertentu.
- Misalnya suid dan sgid hanya efektif pada file executable , sticky bit dan sgid hanya efektif pada direktori

Nilai Hak Akses Khusus (1)

Nilai	*Arti dari bit*	*tanda*
4	suid	s sebelum rwx groups jika dari kiri
2	sgid	s sebelum rwx other jika dari kiri
1	Sticky bit	t

Nilai Hak Akses Khusus (2)

Perintah	*Keterangan*
suid	File dengan suid akan dijalankan dengan hak akses seperti hak akses dari pembuat file tersebut (owner).
sgid	•Pada file: File dengan suid akan dijalankan dengan hak akses seperti hak akses group dari pembuat file tersebut. •Pada direktori: file yang berada didalam direktori tersebut maka hak aksesnya akan seperti hak akses dari group pembuat direktori tersebut.
sticky	File yang berada di dalam direktori tersebut tidak dapat dihapus kecuali oleh owner dan super user.

Contoh Hak Akses Khusus

- Misalnya, untuk merubah hak akses menjadikan sqid dan sticky aktif untuk direktori dataku adalah sebagai berikut:

```
[student@localhost student]$ chmod 3775 dataku
[student@localhost student]$ ls -il
total 4
374925 drwxrwsr-t 2 student student 4096 Dec 21 10:41 dataku
```