MATA KULIAH ADMINISTRASI SISTEM · CEN3303

Manajemen Pengguna, Grup, dan Hak Akses

Pertemuan 3 · Sub-CPMK 2.1

Program Studi D3 Teknik Komputer, Politeknik Negeri Padang

Semester 3 · 3 SKS (2 Teori – 1 Praktik)

PETA PEMBELAJARAN

Agenda Pertemuan Hari Ini

01



Konsep User dan Group

Jenis akun pengguna dan pengelolaan grup secara kolektif

02



Model Permission Linux & Windows

Struktur rwx, NTFS Permission, dan perbandingannya

03



Access Control List (ACL)

Mengatasi keterbatasan permission dasar secara fleksibel

04



Studi Kasus & Diskusi Kelompok

Hak akses pada server berbagi berkas lintas-departemen

SUB-CPMK 2.1

Capaian Pembelajaran Pertemuan Ini

Sub-CPMK 2.1 Mahasiswa mampu mengelola pengguna, grup, dan hak akses (permission dan ownership) pada sistem operasi server.



Memahami konsep akun

pengguna dan grup pada sistem operasi server.



Menjelaskan model permission

pada Linux (rwx) dan Windows (NTFS).



Menerapkan konsep ACL

untuk pengaturan hak akses lanjutan.

Metode: Ceramah, Diskusi & Praktikum · CPL Terkait: CPL-2, CPL-8

Siapa Boleh Mengakses, dan Melakukan Apa?

Setelah server berhasil diinstal dan terhubung ke jaringan (Bab 2), langkah berikutnya adalah mengatur siapa saja yang boleh mengakses server dan apa yang boleh mereka lakukan.

Tanpa manajemen pengguna dan hak akses yang tepat, server rentan terhadap penyalahgunaan — baik dari pengguna internal maupun pihak luar.



Lini pertahanan pertama — banyak insiden keamanan bermula dari kesalahan konfigurasi hak akses yang sederhana, misalnya direktori sensitif yang tidak sengaja terbuka bagi semua pengguna.

KAITAN ANTAR BAB



Bab 2 — Instalasi & Jaringan

Server sudah terinstal dan terhubung ke jaringan.



Bab 3 — Pengguna & Hak Akses

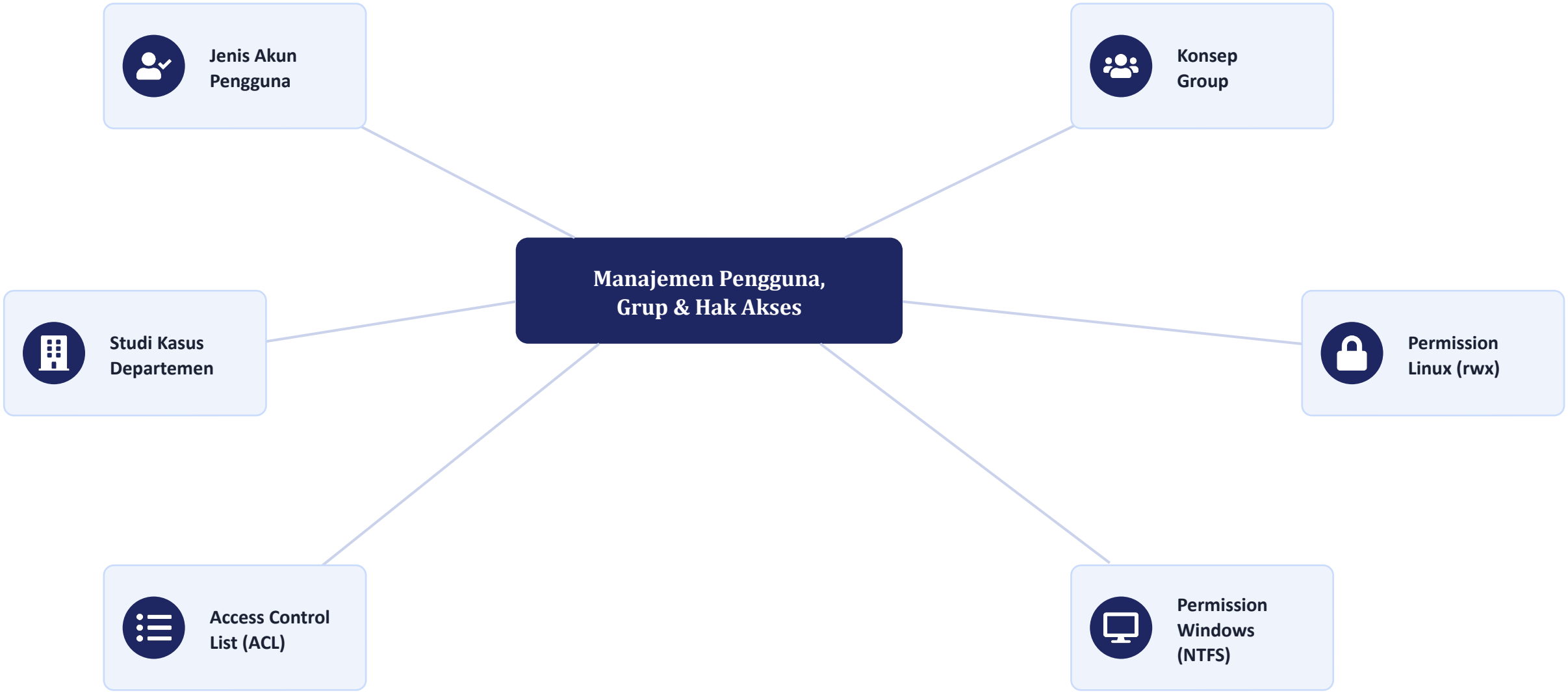
Mengatur siapa yang boleh mengakses apa (bab ini).



Bab 4 — Manajemen Filesystem

Hak akses selalu berkaitan erat dengan berkas & direktori.

Peta Konsep Bab 3



Jenis Akun Pengguna

Superuser (root / Administrator)

Memiliki akses penuh ke seluruh sistem — dapat mengubah, menghapus, atau mengonfigurasi apa pun.

Pengguna Biasa (Standard User)

Memiliki hak akses terbatas sesuai kebutuhan — tidak dapat mengubah konfigurasi inti sistem.

Akun Layanan (Service Account)

Digunakan oleh aplikasi/layanan (mis. www-data), bukan untuk login manusia — menerapkan prinsip least privilege.

Konsep Group

Group memudahkan pengelolaan hak akses secara kolektif. Alih-alih memberi izin satu per satu ke setiap pengguna, administrator dapat mengelompokkan pengguna ke dalam grup (misalnya grup developer, finance) dan memberikan izin pada grup tersebut.



Analogi — seperti kartu akses seragam untuk seluruh anggota satu departemen, dibanding membuat kunci terpisah untuk tiap orang.

PERINTAH DASAR (LINUX)

```
useradd -m -G developer andi
# membuat user 'andi' dan
# memasukkan ke grup 'developer'

groupadd finance
# membuat grup baru 'finance'

usermod -aG finance budi
# menambahkan user 'budi'
# ke grup 'finance'
```

Permission Linux (rwx)

Linux menerapkan model permission berbasis tiga kategori pemilik, masing-masing dengan tiga jenis izin.



TIGA JENIS IZIN

r	read
w	write
x	execute

Contoh: 754 → owner=rwx (7), group=r-x (5), other=r-- (4).

MENGUBAH PERMISSION & KEPEMILIKAN

```
chmod 754 laporan.sh
# owner=rwx(7)
# group=r-x(5)
# other=r--(4)

chown andi:developer laporan.sh
# mengubah owner dan group
```

Ingat chmod mengubah izin akses, sedangkan chown mengubah kepemilikan berkas (owner dan/atau group).

Permission Windows & Perbandingan

NTFS PERMISSION

Windows Server menggunakan NTFS Permission yang lebih granular, diberikan kepada pengguna maupun grup Active Directory secara individual.

- **Full Control**
- **Modify**
- **Read & Execute**
- **List Folder Contents**
- **Read**
- **Write**

Diatur melalui GUI (Properties → Security) atau perintah icacls.

PERBANDINGAN LINUX VS WINDOWS

Granularitas

Linux: 3 kategori (owner/group/other) × 3 izin (rwx)
Windows: Izin lebih rinci per pengguna/grup

Pengaturan

Linux: CLI (chmod, chown)
Windows: GUI atau icacls

Warisan Izin (inheritance)

Linux: Terbatas tanpa ACL
Windows: Didukung penuh secara default

Access Control List (ACL)

KETERBATASAN PERMISSION DASAR

Model permission dasar Linux (rwx) hanya dapat menetapkan satu owner dan satu group per berkas. Jika berkas perlu diakses beberapa grup dengan izin berbeda, permission dasar tidak mencukupi.

Analogi Daftar Tamu — selain tamu resmi (owner/group/other), penyelenggara dapat menambahkan individu tertentu ke daftar akses tanpa mengubah kategori tamu utama.

IMPLEMENTASI ACL (LINUX)

```
setfacl -m u:citra:rw laporan.sh
# memberi user 'citra'
# izin baca-tulis

getfacl laporan.sh
# menampilkan daftar ACL
# pada berkas
```

ACL melengkapi keterbatasan permission dasar dengan izin akses yang lebih fleksibel.

Hak Akses Server Berbagi Berkas Departemen

Skenario Perusahaan memiliki server berbagi berkas dengan tiga departemen: HR, Keuangan, dan IT. Folder Keuangan juga perlu diakses oleh satu staf IT untuk audit, tanpa memberi akses penuh ke seluruh folder IT.

Analisis Permission dasar (rwx) tidak cukup — staf IT bukan bagian grup Keuangan namun tetap membutuhkan akses baca ke folder Keuangan. Solusinya: menerapkan ACL.

Solusi Disarankan Membuat grup hr, keuangan, dan it, masing-masing dengan folder berpemilik grup sesuai departemen dan permission 770 (akses penuh owner/group, tidak ada akses other). Untuk staf audit IT, ditambahkan ACL:

```
setfacl -m u:staf_audit:rx /data/keuangan
```

Rangkuman

Akun & Group

Sistem server mengenal akun superuser, pengguna biasa, dan akun layanan, dengan grup sebagai alat pengelolaan hak akses kolektif.

Model Permission

Linux menerapkan model permission rwx berbasis owner/group/other, sedangkan Windows menggunakan NTFS Permission yang lebih granular.

Access Control List

ACL digunakan untuk mengatasi keterbatasan permission dasar dengan memberikan izin akses lebih fleksibel kepada pengguna/grup tertentu.

Pertanyaan Diskusi

Sebuah tim proyek lintas-departemen membutuhkan akses baca-tulis ke satu folder bersama, sementara pengguna lain hanya boleh membaca.

Rancanglah skema grup dan permission (termasuk penggunaan ACL bila diperlukan) untuk memenuhi kebutuhan tersebut.

Pertemuan Selanjutnya: Manajemen Sistem Berkas, Mounting, dan Penyimpanan (Sub-CPMK 2.2)

REFERENSI

Nemeth, E., et al. (2021). UNIX and Linux System Administration Handbook (5th ed.). Addison-Wesley.
Frisch, AE. (2002). Essential System Administration (3rd ed.). O'Reilly Media.
Sobell, M. G. (2015). A Practical Guide to Linux Commands, Editors, and Shell Programming (4th ed.). Prentice Hall.
Panek, W. (2020). MCSA Windows Server Study Guide. Sybex.