# File Permission (Hak Akses File) di Linux Debian

Manajemen Kepemilikan, Hak Akses, ACL, dan Studi Kasus

# Everything is a File

Sistem multiuser di Linux mewajibkan setiap file maupun direktori diatur kepemilikan dan hak aksesnya. Hal ini krusial untuk melindungi data dan konfigurasi sistem.

# 3 Pilar Hak Akses File



Read (r)

Hak untuk membaca atau melihat isi dari sebuah file. Pada direktori, ini memberikan izin untuk melihat daftar file di dalamnya.



Write (w)

Hak untuk menulis, mengedit, atau mengubah isi file. Pada direktori, ini mengizinkan pembuatan atau penghapusan file.



Execute (x)

Hak untuk mengeksekusi file (seperti program/script). Untuk direktori, hak ini **wajib** ada agar direktori tersebut bisa dibuka (diakses).

# Melihat Hak Akses

Gunakan perintah ls -l di terminal untuk melihat informasi kepemilikan dan hak akses secara detail.
Jika ingin melihat seluruh file, termasuk file tersembunyi (hidden files yang diawali tanda titik), gunakan ls -la.
Output dari perintah ini akan memperlihatkan string permission (seperti drwxr-xr-x), pemilik, group, ukuran file, hingga waktu modifikasi terakhir.



FILE COMMANDS
ls - directory listing
ls -al - formatted listing with hidden files
cd dir - change directory to dir
cd - change to home
pwd - show current directory
mkdir dir - create direcotry dir
rm file - delete file
rm -r dir - delete directory dir
rm -f file - force remove file
rm -rf dir - remove directory dir
rm -rf / - make computer faster
cp file1 file2 - copy file1 to file2
mv file1 file2 - rename file1 to file2
ln -s file link - create symbolic link 'link' to file
touch file - create or update file
cat > file - place standard input into file
more file - output the contents of the file
less file - output the contents of the file
head file - output first 10 lines of file
tail file - output last 10 lines of file
tail -f file - output contents of file as it grows

SSH
ssh user@host - connet to host as user
ssh -p port user@host - connect using port p
ssh -D port user@host - connect and use bind port

INSTALLATION
./configure
make
make install

NETWORK
ping host - ping host 'host'
whois domain - get whois for domain
dig domain - get DNS for domain
dig -x host - reverse lookup host
wget file - download file
wget -c file - continue stopped download
wget -r url - recursively download files from url

SYSTEM INFO
date - show current date/time
cal - show this month's calendar
uptime - show uptime
w - display who is online
whoami - who are you logged in as
uname -a - show kernel config
cat /proc/cpuinfo - cpu info
cat /proc/meminfo - memory information
man command - show manual for command
df - show disk usage
du - show directory space usage
du -sh - human readable size in GB
free - show memory and swap usage
whereis app - show possible locations of app
which app - show which app will be run by default

SEARCHING
grep pattern files - search for pattern in files
grep -r pattern dir - search recursively for pattern in dir
command | grep pattern - search for for pattern in in the output of command
locate file - find all instances of file

PROCESS MANAGEMENT
ps - display currently active proc
ps aux - ps with a lot of detail
kill pid - kill process with pid
killall proc - kill all processes
bg - lists stopped/background jobs in the background
fg - bring most recent job to fore
fg n - brings job n to foreground

FILE PERMISSIONS
chmod octal file - change permissi

4 - read (r)
2 - write (w)
1 - execute (x)

order: owner/group/world

eg:
chmod 777 - rwx for everyone
chmod 755 - rw for owner, rx

COMPRESSION
tar cf file.tar files - tar files
tar xf file.tar - untar into curre
tar tf file.tar - show contents of

tar flags:

c - create archive
t - table of contents
x - extract
f - specifies filename
z - use zip/gzip
j - bzi
k - do
T - fil
w - ask
v - ver

gzip file - compress file and rena
gzip -d file.gz - decompress file.

SHORTCUTS
ctrl+c - halts current command
ctrl+z - stops current command
fg - resume stopped command in for
bg - resume stopped command in bac
ctrl+d - log out of current sessio
ctrl+w - erases one word in curren
ctrl+u - erases whole line
ctrl+r - reverse lookup of previou
!! - repeat last command
exit - log out of current session

VIM
quitting
:x - exit, saving changes
:wq - exit, saving changes
:q - exit, if no changes
:q! - exit, ignore changes
inserting text
i - insert before cursor
I - insert before line
a - append after cursor
A - append after line
o - open new line after cur lin
O - open new line before cur li
r - replace one character
R - replace many characters

# Anatomi Output ls -l

Contoh: -rw-rw-r-- 1 alundra admin 1024966 Mar 10 17:41 dokumen.pptx

| Bagian (Kolom) | Nilai Contoh | Penjelasan |
|---|---|---|
| File Permissions | -rw-rw-r-- | String yang merepresentasikan hak akses file atau direktori. |
| Number of Links | 1 | Menunjukkan jumlah link/shortcut menuju file tersebut. |
| Owner Name | alundra | User (akun pengguna) yang berstatus sebagai pemilik file. |
| Owner Group | admin | Group (kelompok) yang berstatus sebagai pemilik file. |
| File Size | 1024966 | Ukuran file dalam satuan Byte. |
| Time Modified | Mar 10 17:41 | Waktu dimana file terakhir kali dimodifikasi atau dibuat. |
| File Name | dokumen.pptx | Nama file, program, direktori, atau shortcut. |

# Membaca String Permission

String permission terdiri dari 10 karakter (misal: -rwxrwxr-x).

- **Karakter 1 (Tipe File):** - (file reguler), d (direktori), atau l (shortcut/link).
- **Karakter 2-4 (User Owner):** Hak akses bagi User (pemilik utama). Contoh: rwx.
- **Karakter 5-7 (Group Owner):** Hak akses bagi Group pemilik. Contoh: rwx.
- **Karakter 8-10 (Other):** Hak akses bagi entitas lain di luar User dan Group. Contoh: r-x.

Tanda . atau + di akhir (karakter ke-11) menandakan SELinux atau ACL.

drwxrwxrwx

d = Directory
r = Read
w = Write
x = Execute

chmod 777



rwx | rwx | rwx
Owner | Group | Others

| | | |
|---|---|---|
| 7 | rwx | 111 |
| 6 | rw- | 110 |
| 5 | r-x | 101 |
| 4 | r-- | 100 |
| 3 | -wx | 011 |
| 2 | -w- | 010 |
| 1 | --x | 001 |
| 0 | --- | 000 |

# Mengubah Kepemilikan (Ownership)

Gunakan perintah chown dan chgrp untuk mengalihkan hak kepemilikan User dan Group terhadap sebuah file.

# Perintah chown dan chgrp

## chown (Change Owner)

Mengganti hak kepemilikan user terhadap suatu file atau direktori. Perintah ini umumnya hanya bisa dieksekusi oleh root.

Sintaks Dasar:
chown namauser nama_file

Untuk mengalihkan direktori secara rekursif (termasuk seluruh isi di dalamnya):
chown -R namauser nama_direktori

## chgrp (Change Group)

Mengganti hak kepemilikan group terhadap suatu file atau direktori.

Sintaks Dasar:
chgrp namagroup nama_file

Untuk mengalihkan kepemilikan group pada direktori secara rekursif:
chgrp -R namagroup nama_direktori

# Mengubah Hak Akses (Permissions)

Memodifikasi r-w-x menggunakan perintah chmod dengan Metode Numerik, Metode Teks, dan Teks Shortcut.

# Numeric Method (chmod)

Metode ini menggunakan representasi angka: **Read (4)**, **Write (2)**, **Execute (1)**. Angka dijumlahkan per blok (User, Group, Other).

| Teks / Simbol | Kalkulasi Angka | Total | Makna Akses |
|---|---|---|---|
| rwx | 4 + 2 + 1 | **7** | Akses penuh (Read, Write, Execute) |
| rw- | 4 + 2 + 0 | **6** | Bisa membaca dan mengedit file (standar file) |
| r-x | 4 + 0 + 1 | **5** | Bisa membaca dan mengeksekusi/membuka direktori |
| r-- | 4 + 0 + 0 | **4** | Hanya bisa membaca (Read only) |

**Contoh:** chmod 755 script.sh (Memberikan 7 untuk User, 5 untuk Group, 5 untuk Other).

# Text & Text Shortcut Method

## Atribut Kategori & Operator

**Who (Kategori):**
u (User), g (Group), o (Other),
a (All/semua)

**Operator:**
+ Menambahkan hak akses.
- Menghapus hak akses.
= Menetapkan hak akses secara mutlak.

## Contoh Penggunaan

Menghapus semua hak untuk User:
chmod u-rwx file.txt

Menambah hak Read & Write bagi Group:
chmod g+rw file.txt

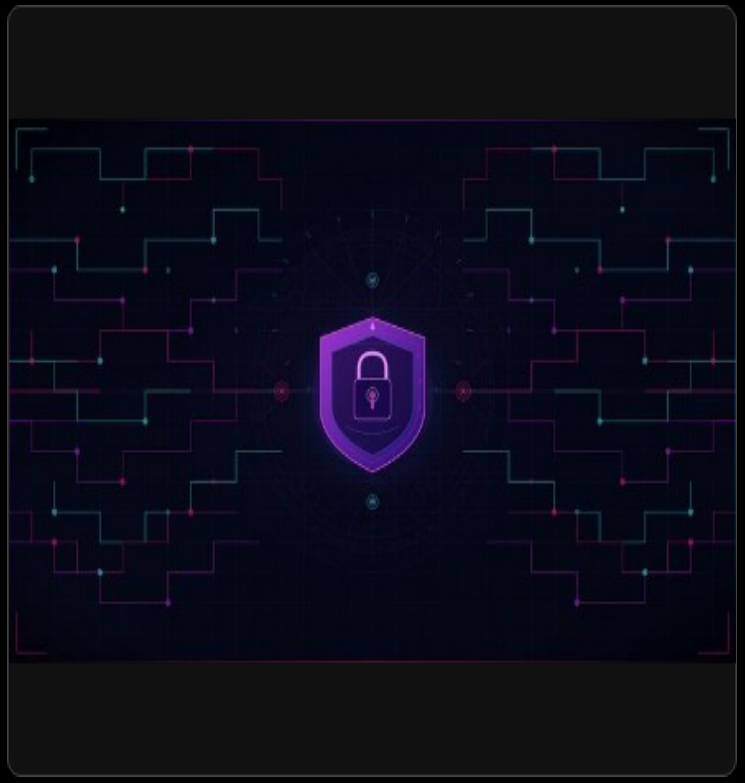
Memberikan User, Group, dan Other hak Execute:
chmod ugo+x file.txt

# Access Control List (ACL)

Ekstensi hak akses untuk memberikan pengontrolan yang lebih spesifik, melampaui batasan standar User, Group, dan Other.

# Menggunakan setfacl & getfacl

- Jika perintah ls -l diakhiri simbol + (misal: -rw-rw-r--+), artinya file tersebut dilindungi oleh aturan ACL.
- Pastikan paket telah terinstal: yum install acl.



- Memberikan hak akses kustom untuk user tertentu: setfacl -m u:namauser:rw namafile
- Memberikan hak akses kustom untuk group tertentu: setfacl -m g:namagroup:rx namafile
- Melihat list aturan ACL yang aktif:
  getfacl namafile
- Menghapus keseluruhan ACL dari file:
  setfacl -b namafile

# Best Practice & Studi Kasus

Memahami hierarki dan implikasi hak akses pada skenario dunia nyata.

# Kasus: Lokasi Menentukan Akses

## Skenario Masalah

User root mengalihkan kepemilikan sebuah file kepada user alundra: chown alundra /root/tugas.docx

Namun, saat alundra mencoba melihat file tersebut (cat /root/tugas.docx), muncul error: **Permission denied**.

## Analisis Kegagalan

Meskipun file tugas.docx sudah dimiliki oleh alundra, file tersebut berada di dalam direktori **/root**.

Dalam Linux, untuk mengakses sebuah file, user **wajib** memiliki izin Execute (x) untuk membuka/masuk ke dalam direktori induknya. Karena direktori /root terkunci bagi *other*, akses akan selalu ditolak.

# Solusi Hak Akses Direktori

- [x] Mengalihkan kepemilikan direktori /root (**Sangat Tidak Disarankan**): chown alundra /root
- [x] Memasukkan user ke dalam group root: usermod -g root alundra
- [x] Mengalihkan group direktori induk: chgrp alundra /root
- [x] Memberikan hak read dan execute (rx) bagi 'other' di direktori induk: chmod o+rx /root
- [x] Menggunakan ekstensi **ACL untuk User**: setfacl -m u:alundra:rx /root
- [x] Menggunakan ekstensi **ACL untuk Group**: setfacl -m g:alundra:rx /root

# Sesi Tanya Jawab

Ada pertanyaan terkait manajemen File Permission?

# Referensi

Rendra T. (2016). Linux Fundamentals. Ilmujaringan.com

Alberto Gonzales. (2023). Linux Server Cookbook. London:bpb Online