ONE PAGE SUMMARY

IT & Software › Linux › Permissions

Introduction to Permissions

Master Linux permissions for secure file management!

DEFINITION

> Permissions in Linux control who can access and modify files. They determine user rights and security levels.

KEY CONCEPTS

User Types

Linux categorizes users into three types: owner, group, and others.

Permission Levels

Each user type can have read, write, or execute permissions for files.

Symbolic Notation

Permissions are represented by letters: 'r' for read, 'w' for write, and 'x' for execute.

Numeric Notation

Permissions can also be expressed as numbers: read (4), write (2), execute (1), summed for each user type.

Changing Permissions

The 'chmod' command is used to change file permissions in Linux.

EXAMPLES

→ chmod 755 filename.txt

→ chmod g+w file.txt

→ ls -l filename.txt

MEMORY TIPS

★ Remember 'rwx' as 'Read, Write, Execute' to recall permission types.

★ Use '4-2-1' for numeric permissions: 4 for read, 2 for write, 1 for execute.

★ Think of 'chmod' as 'Change Mode' to remember its function.

COMMON MISTAKES

✗ Confusing user types and their corresponding permissions.

✗ Not using numeric values correctly when setting permissions.

✗ Forgetting to apply changes recursively with '-R' when needed.

QUICK RECAP

Linux permissions are essential for file security and management. Understand user types, permission levels, and how to use 'chmod' effectively.