Baseline IAM Policy for Ubuntu Server (VM)

Project : Linux IAM & Hardening Mini Project

Author : Shivam Kishor

Date : 4 Nov 2025

System : Ubuntu 25.10 (LAB VM)

1. Team Roles and Access Requirements

Role	Description	Sudo Access	File Access needs
Admin	Manages system and users	Full sudo	Read/write to all files
Developer	Builds and deploys code	Limited sudo (specific commands)	Read/write to project folder
Auditor	Reviews logs and configs	No sudo	Read-only access to project folder

2. Group Structure

- admin: For system administrators
- dev: For developers
- audit: For auditors

Users will be assigned to these groups based on their roles. Group membership determines access to shared resources and sudo privileges.

3. Sudo Policy

- **Admin group**: Full sudo access with password prompt.
- **Dev group**: Allowed to run only specific commands (e.g., restart app service, deploy script) via sudo.
- **Auditors**: No sudo access.

Sudo rules will be defined in /etc/sudoers.d/project using visudo for safety.

4. File Access Policy

- Shared folder: /srv/project
    - admin and dev groups: Read/write access
    - audit group: Read-only access
    - Others: No access
- POSIX permissions and ACLs will be used to enforce access control.

5. Security Principles

- **Least Privilege:** Users get only the access they need.
- **Auditability:** Changes to sensitive files (e.g., /etc/sudoers, /etc/passwd) will be logged using auditd.
- **Accountability:** Password prompts required for sudo; no blanket NOPASSWD rules.

This policy ensures secure and role-based access control for a small team managing an Ubuntu server. It will guide the creation of users, groups, sudo rules, and file permissions during implementation.