

PROJECT DESIGN PHASE

Solution Architecture

Date	1 November 2025
Team ID	NM2025TMID07110
Project Name	Optimising user,group, and role management with access control and workflows
Maximum Marks	4 marks

Solution Architecture:

Goals of the Architecture:

- **Security and Compliance:** To enforce the Principle of Least Privilege across all integrated applications and generate immutable audit trails demonstrating continuous compliance with regulatory mandates (e.g., SoD, GDPR).
- **Automation and Efficiency:** To establish a central, high-speed Joiner-Mover-Leaver (JML) lifecycle engine, minimizing manual IT effort and ensuring near-instantaneous provisioning/de-provisioning across hybrid environments.
- **Scalability and Resilience:** To provide a robust, resilient platform capable of managing thousands of identities and roles across a growing portfolio of enterprise applications without introducing performance bottlenecks or single points of failure.

Key components:

- **Identity Governance and Administration (IGA) Platform:** A centralized hub responsible for policy definition, access request management, auditing, and enforcing governance policies like Separation of Duties (SoD).
- **Role-Based Access Control (RBAC) Engine:** The mechanism used to define and manage standardized organizational roles (e.g., “HR Manager”) and map them to the specific technical permissions required across integrated systems.
- **Automated Workflow Engine:** A powerful tool that orchestrates the entire user lifecycle (Joiner-Mover-Leaver, or JML), automatically triggering provisioning and de-provisioning based on inputs from authoritative sources.

- **Authoritative Source Integration (HRIS):** A reliable connection to the Human Resources Information System (HRIS) or other source of truth, used to trigger all user identity and role changes based on employee status and job function.
- **Target System Connectors:** Secure, standardized interfaces (e.g., SCIM, API integration) that allow the IGA platform to communicate with and enforce access policies on all target applications, directories (like Active Directory), and cloud resources.

Development Phases:

1. Create user
2. Assign users to groups
3. Application Access
4. Access control list
5. Create a flow to assign operations ticket to group

Solution Architecture Description

The proposed solution architecture for optimizing user, group, and role management with access control and workflows centers around an Identity Governance and Administration (IGA) Platform acting as the central intelligence and orchestration layer.

At its foundation, the architecture integrates with an **Authoritative Source (typically HRIS)** which serves as the "source of truth" for all employee identities and their key attributes (e.g., job title, department, employment status). This integration is crucial for driving automated lifecycle events.

The IGA Platform utilizes Target System Connectors (e.g., SCIM, LDAP, direct API integrations) to communicate with and provision/de-provision access to all Target Systems and Applications. These include directories like Active Directory/LDAP, SaaS applications (e.g., Salesforce, Workday), cloud platforms (AWS, Azure, GCP), and on-premise databases or applications.

Finally, the architecture includes an Identity Data Store (either integrated within the IGA or a dedicated Identity Vault) which maintains a consistent view of all managed identities and their current access entitlements. This entire system ensures that user access is dynamic, compliant, and consistently enforced based on their current role and organizational policies, drastically reducing manual effort and security risk.

Solution Architecture: Optimized Identity of Access Management

