**Databricks IAM Issues with Mitigations**

**Databricks Identity and Access Management (IAM) Issues Comparison Table with Mitigations**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | IAM Issue | One-Liner Description | Where It Typically Arises | IAM Areas Most Affected | Mitigation Strategies |
| 1 | Over-Permissive Roles | Users or groups are granted broader access than necessary, increasing security risk. | Role assignments, initial workspace setup | Workspaces, Clusters, Data | Follow least privilege principle; audit permissions regularly with SHOW GRANTS. |
| 2 | Inconsistent Group Membership | Group assignments drift over time, leading to unpredictable access behavior. | Directory sync, manual group edits | Workspaces, Data Access | Automate group management via SCIM or Azure AD sync; establish approval workflows. |
| 3 | Lack of Role Segregation | Roles are not clearly separated between administrators, developers, and consumers. | Workspace administration | All IAM-managed resources | Define clear RBAC roles for each persona; restrict admin capabilities to designated users only. |
| 4 | Orphaned Users | Accounts remain active after users leave the organization, creating potential vulnerabilities. | Offboarding processes | Workspaces, Clusters, Data | Automate deprovisioning via SCIM or identity provider; periodically review active users. |
| 5 | Credential Exposure | API tokens and secrets stored insecurely in notebooks or shared locations. | Notebook development, automation scripts | Repos, Jobs, Clusters | Use Databricks Secrets for secure storage; rotate credentials regularly. |
| 6 | Inconsistent Workspace Access | Users have different levels of access across multiple workspaces, causing confusion. | Multi-workspace environments | Workspace Access, Data Governance | Centralize access through identity federation; apply uniform group policies. |
| 7 | Lack of Audit Visibility | Insufficient logging makes it difficult to track who accessed or modified resources. | Production data access | Data Access, Jobs, Tables | Enable audit logs; integrate logs with SIEM solutions for monitoring and alerting. |
| 8 | External User Risk | External collaborators are given more access than necessary, increasing exposure. | Cross-organization collaboration | Repos, Data, Jobs | Use temporary credentials and scoped roles; monitor external user activity closely. |
| 9 | Token Proliferation | Too many personal access tokens are created, increasing risk of misuse. | API access, automation integration | Jobs, Pipelines | Limit token lifespan; enforce token policies and rotate regularly. |
| 10 | Incomplete Unity Catalog Integration | Not all users and groups are properly synced to Unity Catalog, resulting in inconsistent access. | Migrating to Unity Catalog | Catalogs, Schemas, Tables | Validate group sync; test permissions before migrating workloads. |

**Quick Reference**

* **SCIM:** Protocol for automating user and group provisioning.
* **RBAC:** Role-Based Access Control.
* **Tokens:** API keys for programmatic access.
* **Secrets:** Securely stored credentials for accessing resources.
* **Audit Logs:** Records of user and system activity.

**Example Mitigation Commands and Configurations**

**Grant Access Securely:**

sql

CopyEdit

GRANT SELECT ON SCHEMA main.sales TO `analyst\_group`;

**Rotate Tokens Regularly:**

* In the **User Settings**, delete and regenerate personal access tokens on a schedule.

**Use Databricks Secrets:**

python

CopyEdit

dbutils.secrets.get(scope="prod-secrets", key="storage-account-key")

**Review Active Users:**

sql

CopyEdit

DESCRIBE PRINCIPALS;

**Enable Audit Logging:**

* Configure your workspace to export audit logs to cloud storage or a SIEM solution.

**Sync Groups with SCIM (Azure Example):**

* Integrate Azure AD with Databricks SCIM connector to automatically synchronize users and groups.