**📚 1. Introduction to IAM**

**✅ What is IAM?**

* GCP IAM controls **who (identity)** has **what access (roles)** to **which resources (scope)**.

**🔑 Key Concepts:**

| **Concept** | **Description** |
| --- | --- |
| **Identity** | Who is making the request (user, service account, group) |
| **Resource** | What is being accessed (VM, bucket, project, etc.) |
| **Permission** | What action is being taken (read, write, delete, etc.) |
| **Role** | A set of permissions assigned to an identity |
| **Policy** | Bindings of members to roles for resources |

**🔍 2. IAM Structure in GCP**

Organization > Folders > Projects > Resources

IAM policies are **inherited** down the hierarchy.

**🛠️ 3. Types of Roles**

| **Type** | **Description** |
| --- | --- |
| **Basic Roles** | Primitive roles: Owner, Editor, Viewer (not recommended) |
| **Predefined Roles** | Google-managed roles for specific services |
| **Custom Roles** | User-defined role with precise permissions |

**👤 4. Identity Types**

* **Google Account**
* **Service Account**
* **Google Group**
* **Cloud Identity or Workspace user**
* **Workload Identity Federation**

**🔒 5. Best Practices**

* **Principle of Least Privilege (PoLP)**: Only grant what is needed.
* **Avoid Basic Roles** (Owner, Editor, Viewer)
* **Use Groups or Service Accounts**, not individuals
* **Use Custom Roles** when predefined ones are too broad
* **Audit IAM regularly** with Cloud Asset Inventory or Policy Analyzer

**🧰 6. Useful CLI Commands**

**✅ Get IAM policy for a project:**

gcloud projects get-iam-policy [PROJECT\_ID]

**✅ Add IAM Role:**

gcloud projects add-iam-policy-binding [PROJECT\_ID] \

--member="[user:xyz@gmail.com](mailto:user%3Axyz@gmail.com)" \

--role="roles/viewer"

**✅ Remove IAM Role:**

gcloud projects remove-iam-policy-binding [PROJECT\_ID] \

--member="[user:xyz@gmail.com](mailto:user%3Axyz@gmail.com)" \

--role="roles/viewer"

**🧪 7. Auditing and Troubleshooting**

* Use **IAM Recommender** for over-permissioned accounts
* Enable **Cloud Audit Logs** (Admin Activity, Data Access)
* Use **Policy Troubleshooter**:

gcloud policy-intelligence troubleshoot-iam-policy \

--member=[user:xyz@gmail.com](mailto:user%3Axyz@gmail.com) \

--resource=//[cloudresourcemanager.googleapis.com/projects/your-project-id](http://cloudresourcemanager.googleapis.com/projects/your-project-id) \

--permission=resourcemanager.projects.get

**📦 8. Managing IAM via Terraform**

IAM roles can be managed using:

* google\_project\_iam\_member
* google\_project\_iam\_binding
* google\_project\_iam\_policy

📘 [Terraform GCP IAM Docs](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/google_project_iam)

**📌 9. IAM Tools in GCP**

| **Tool** | **Purpose** |
| --- | --- |
| IAM Recommender | Suggests least-privilege roles |
| IAM Policy Analyzer | Compare policies |
| IAM Policy Troubleshooter | Debug access issues |
| Cloud Asset Inventory | Track IAM and resource metadata |
| Access Approval | Require approval before access |
| Access Context Manager | Context-aware access policies |

**💡 10. Practice Scenarios**

1. Grant read-only access to BigQuery
2. Create a service account and bind roles
3. Remove editor access from all users
4. Use IAM Recommender to clean roles
5. Grant least privilege custom role to VM Admins