Google Cloud Platform – Cloud Architect

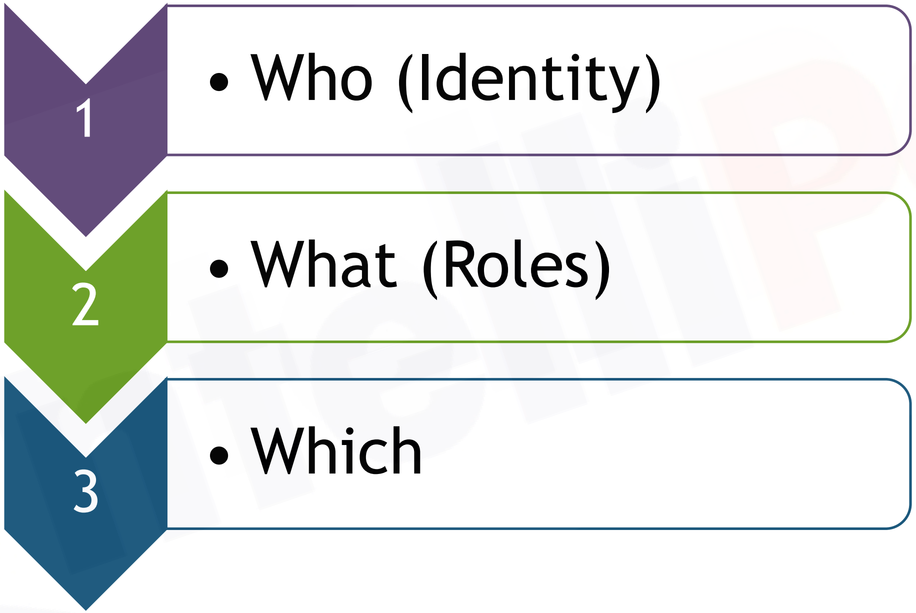
Cloud IAM

Agenda

- ❑ Cloud IAM
- ❑ Who: Types of identities in Google Cloud
- ❑ What: Types of roles in Google Cloud
- ❑ Cloud IAM Roles
- ❑ Primitive Role
- ❑ Predefined Role
- ❑ Custom Role
- ❑ Policy & Bindings
- ❑ Resource Hierarchy
- ❑ Policy inheritance is transitive
- ❑ Service Account
- ❑ Best Practices
- ❑ Quiz

Cloud IAM

❑ Who can perform What actions on Which resources



1

- Who (Identity)

2

- What (Roles)

3

- Which

Who: Types of identities in Google Cloud

	Google Account	Service Account	G-Suite Domain	Cloud Identity Domain	Google Group
Represents	Employee/ User	Application component	All members of a specified domain	All members of a specified domain	All members of the group
Call APIs?	**Yes**	**Yes**	No	No	No
Log in to Console?	**Yes**	No	No	No	No
Example	userid@gmail.com	project-number@cloudservices.gserviceaccount.com	username@example.com	username@example.com	groupname@googlegroups.com
Notes		**An instance can run as a service account**			

What: Types of roles in Google Cloud

Primitive Roles

Broad Access

Spans across services

Three roles:

- Owner
- Editor
- Viewer

Predefined Roles

Narrow Access

Permission to a single service

Hundreds of roles:

- Service Admin
- Service Viewer
- So on ….

Custom Roles

Customized Access

Create from scratch or from existing Predefined roles

E.g.: compute instance admin without permission to assign externa IPs

More granularity →

Cloud IAM Roles

Represents a set of fined grained permissions

Examples

Service.Resource Type.Verb
storage.buckets.create
iam.serviceaccounts.delete
compute.disks.list
bigquery.tables.update

Primitive Role

Role	Permission
Viewer (roles/viewer)	Permissions for read-only actions that do not affect state, such as viewing (but not modifying) existing resources or data.
Editor (roles/editor)	All viewer permissions, plus permissions for actions that modify state, such as changing existing resources.
Owner (roles/owner)	All editor permissions and permissions for the following actions: ▪ Manage roles and permissions for a project and all resources within the project ▪ Manage Users/ Groups ▪ Set up billing for a project

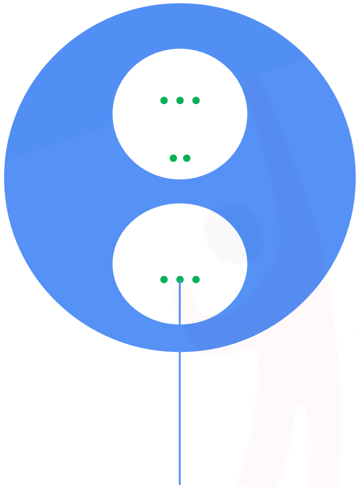
Predefined Role*

- Compute
  - Compute Admin
  - Compute Instance Admin
  - Compute Viewer
- Storage
  - Storage Admin
  - Storage Object Admin
  - Storage Object Creator
  - Storage Object Viewer
- Network
  - Compute Network Admin
  - Compute Network User
  - Compute Network Viewer
- BigQuery
  - BigQuery Data Owner
  - BigQuery Data Editor
  - BigQuery Data Viewer
- App Engine
  - App Engine Admin
  - App Engine Viewer
  - App Engine Deployer
  - App Engine Code Viewer
- Kubernetes Engine
  - Kubernetes Engine Admin
  - Kubernetes Engine Developer
  - Kubernetes Engine Viewer

*- Not an exhaustive list

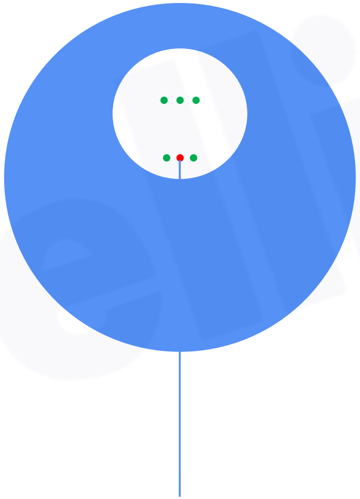
Custom Role

Combine Role



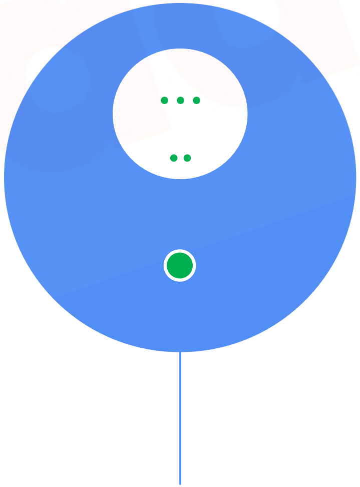
Role

Remove Permission



Remove permission from a role

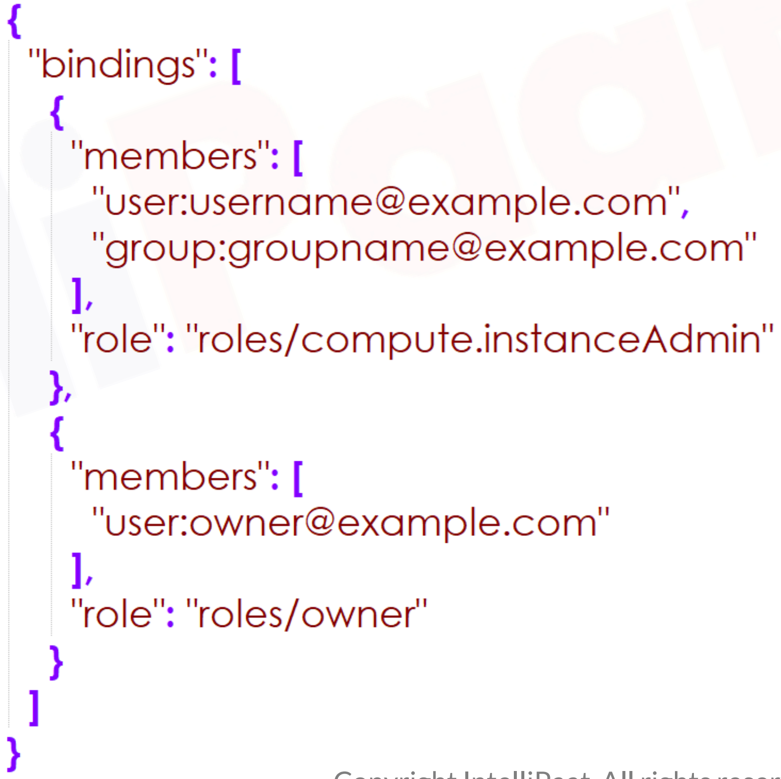
Add Permission



Add permission to a role

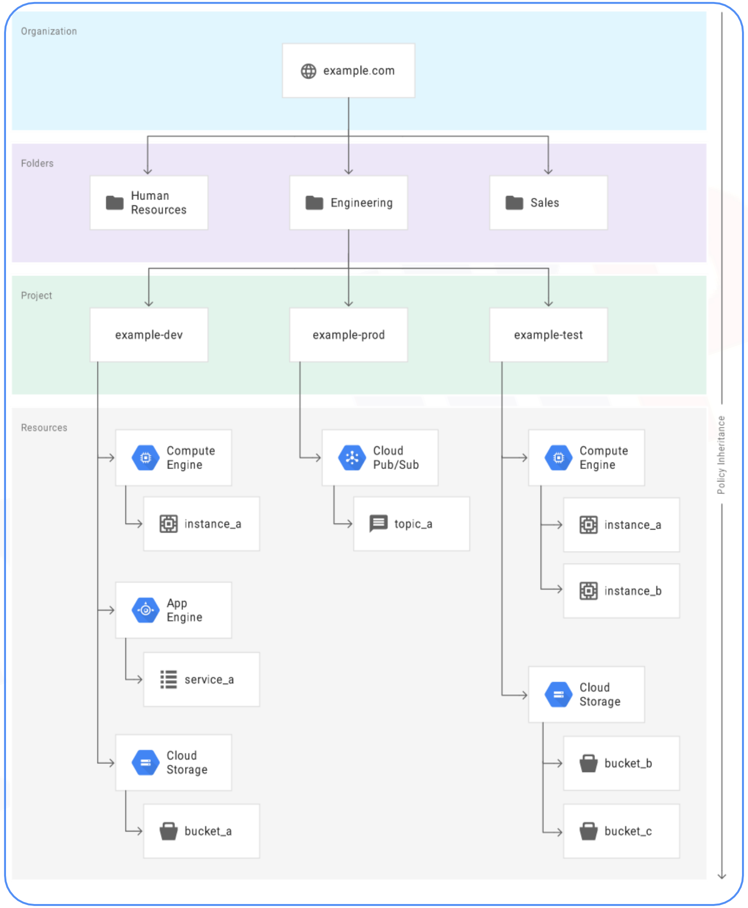
Policy & Bindings

- ❑ Policies connect the resource, roles and members via bindings.

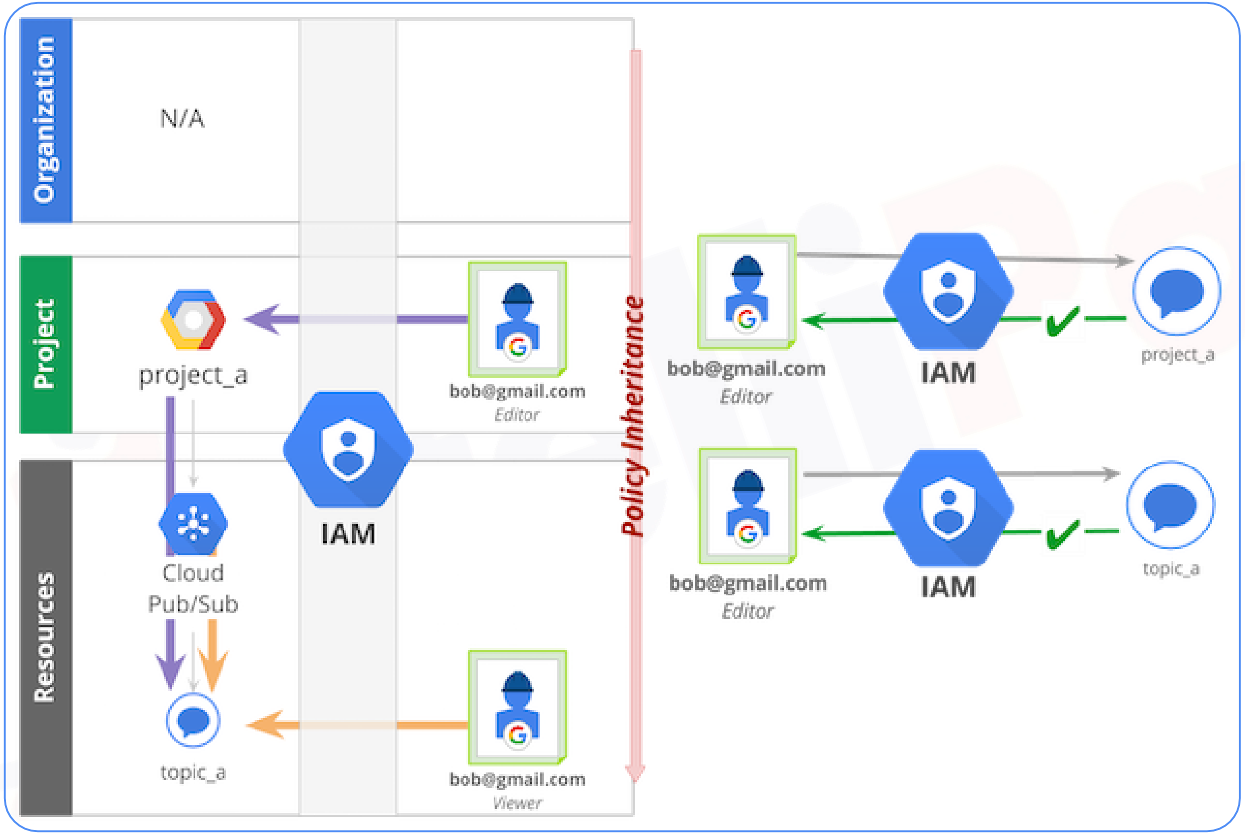


```
{
 "bindings": [
  {
   "members": [
    "user:username@example.com",
    "group:groupname@example.com"
   ],
   "role": "roles/compute.instanceAdmin"
  },
  {
   "members": [
    "user:owner@example.com"
   ],
   "role": "roles/owner"
  }
 ]
}
```

Resource Hierarchy



Policy inheritance is transitive



Service Account

Identity of a Service

Compute Engine can have only one service account

Multiple GCE instances can use the same service account

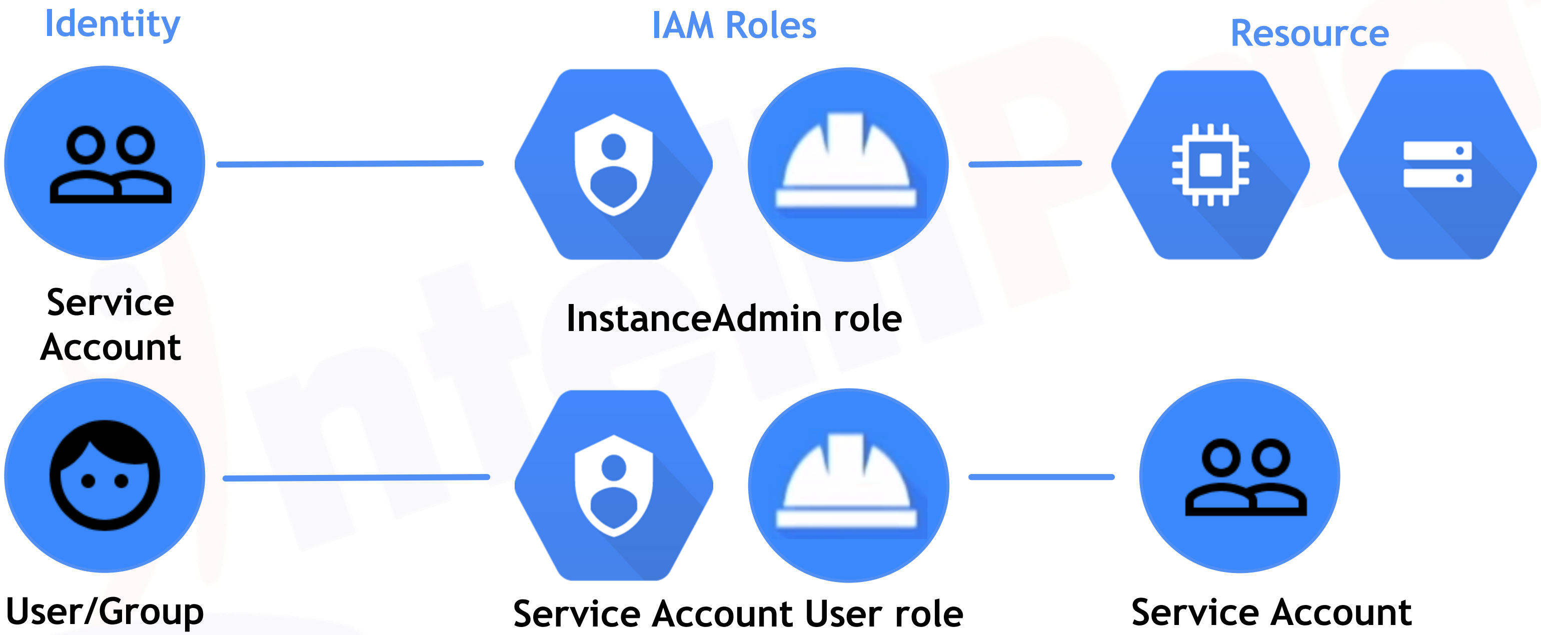
Normal user account can use password or key to authenticate but service account uses only key. Up to 10 service account keys per service account can be created.

Two types of Service Account

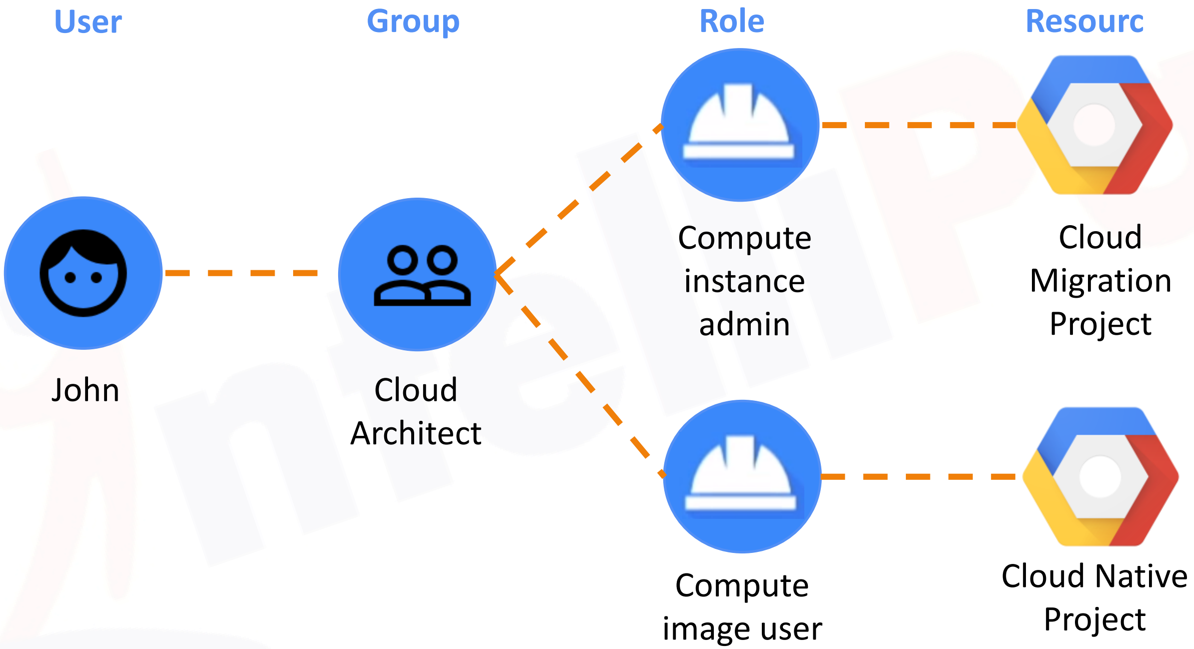
- Google Managed Service Account
- User Managed Service Account

Up to 100 service accounts per project (including the default Compute Engine service account and the App Engine service account) can be created.

A Service Account is an identity and a resource



Best practice: grant roles to groups, not users



Best practice: grant least privilege

Predefined roles or Custom roles

- Reduce the number of accounts that can perform powerful operator, such as

Best practice

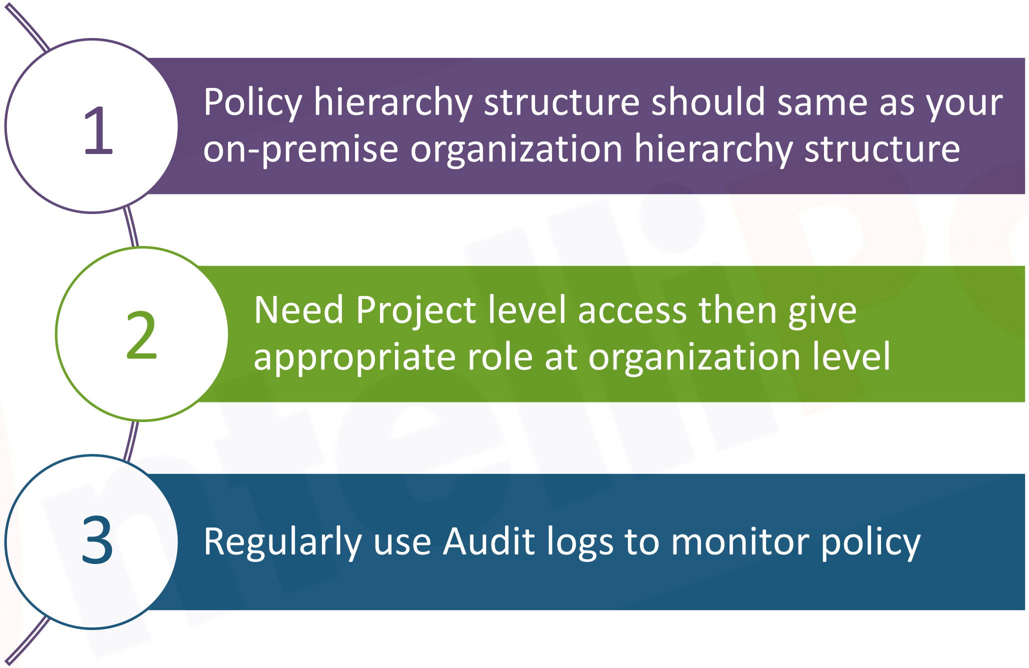
- Grant Service Account Actor role on service account, not on project

Powerful Operation	Roles that can perform the operation
Set IAM Policy	Owner Organization Administrator
Act as a Service account	Owner Editor Service Account Actor

Best practice: Rotate Keys

- Service Account keys
  - serviceAccounts.keys.create()
  - Replace old key with new key
  - serviceAccounts.key.delete()
- SSH keys
  - Instance.getMetadata()
  - Replace old key with new key
  - Instance.setMetadata()

Best practice: Standard



1. Policy hierarchy structure should same as your on-premise organization hierarchy structure
2. Need Project level access then give appropriate role at organization level
3. Regularly use Audit logs to monitor policy

QUIZ

Quiz 1

Your customer is moving their storage product to Google Cloud Storage (GCS). The data contains personally identifiable information (PII) and sensitive customer information. What security strategy should you use for GCS?

A Use signed URLs to generate time bound access to objects.

B Grant IAM read-only access to users, and use default ACLs on the bucket.

C Grant no Google Cloud Identity and Access Management (Cloud IAM) roles to users, and use granular ACLs on the bucket.

D Create randomized bucket and object names. Enable public access, but only provide specific file URLs to people who do not have Google accounts and need access.

Answer 1

Your customer is moving their storage product to Google Cloud Storage (GCS). The data contains personally identifiable information (PII) and sensitive customer information. What security strategy should you use for GCS?

A Use signed URLs to generate time bound access to objects.

B Grant IAM read-only access to users, and use default ACLs on the bucket.

[✓ C] Grant no Google Cloud Identity and Access Management (Cloud IAM) roles to users, and use granular ACLs on the bucket.

D Create randomized bucket and object names. Enable public access, but only provide specific file URLs to people who do not have Google accounts and need access.

Quiz 2

Your customer is moving their corporate applications to Google Cloud Platform. The security team wants detailed visibility of all projects in the organization. You provision the Google Cloud Resource Manager and set up yourself as the org admin. Which Google Cloud Identity and Access Management (Cloud IAM) roles should you give to the security team?

A Org viewer, project owner

B Org viewer, project viewer

C Org admin, project browser

D Project owner, network admin

Answer 2

Your customer is moving their corporate applications to Google Cloud Platform. The security team wants detailed visibility of all projects in the organization. You provision the Google Cloud Resource Manager and set up yourself as the org admin. Which Google Cloud Identity and Access Management (Cloud IAM) roles should you give to the security team?

A Org viewer, project owner

[✓ B Org viewer, project viewer]

C Org admin, project browser

D Project owner, network admin

Quiz 3

You are a project owner and need your co-worker to deploy a new version of your application to App Engine. You want to follow Google's recommended practices. Which IAM roles should you grant your co-worker?

A	Project Editor
B	App Engine Service Admin
C	App Engine Deployer
D	1TB

Answer 3

You are a project owner and need your co-worker to deploy a new version of your application to App Engine. You want to follow Google’s recommended practices. Which IAM roles should you grant your co-worker?

A Project Editor

B App Engine Service Admin

[✓ C] App Engine Deployer

D 1TB

Quiz 4

You want to find out who in your organization has Owner access to a project called "my-project". What should you do?

A In the Google Cloud Platform Console, go to the IAM page for your organization and apply the filter "Role:Owner".

B In the Google Cloud Platform Console, go to the IAM page for your project and apply the filter "Role:Owner".

C Use "gcloud iam list-grantable-role --project my-project" from your Terminal.

D **Use "gcloud iam list-grantable-role" from Cloud Shell on the project page.**

Answer 4

You want to find out who in your organization has Owner access to a project called "my-project". What should you do?

A In the Google Cloud Platform Console, go to the IAM page for your organization and apply the filter "Role:Owner".

[✓ B In the Google Cloud Platform Console, go to the IAM page for your project and apply the filter "Role:Owner".]

C Use "gcloud iam list-grantable-role --project my-project" from your Terminal.

D Use "gcloud iam list-grantable-role" from Cloud Shell on the project page.

Quiz 5

You need to verify the assigned permissions in a custom IAM role. What should you do?

A Use the GCP Console, IAM section to view the information.

B Use the "gcloud init" command to view the information.

C Use the GCP Console, Security section to view the information.

D **Use the GCP Console, API section to view the information.**

Answer 5

You need to verify the assigned permissions in a custom IAM role. What should you do?

A Use the GCP Console, IAM section to view the information.

B Use the "gcloud init" command to view the information.

C Use the GCP Console, Security section to view the information.

D **Use the GCP Console, API section to view the information.**

IntelliPaat

India : +91-7847955955

US : 1-800-216-8930 (TOLL FREE)

sales@intellipaat.com

24X7 Chat with our Course Advisor