PRACTICAL NO. 7

Identity Management

LOB6: Understand the cloud computing services and Identity management in the cloud.
LO6: Implement programs for cloud computing services and Identity management.

Identity Management:

Identity management in cloud computing is the subsequent step of identity and access management (IAM) solutions. However, it is a lot more than merely a straightforward web app single sign-on (SSO) solution. This next generation of IAM solution is a holistic move of the identity provider right to the cloud.

Innovations in the user identity management space have been a trend in the past couple of years. Most of these developments across business and technology fronts have been around identity management in cloud computing, enabling the authentication and authorization processes right in the cloud.

The primary goal of identity management in cloud computing is dealing with personal identity information so that a user's access to data, computer resources, applications, and services is controlled accurately.

Identity management in cloud computing is the subsequent step of identity and access management (IAM) solutions. However, it is a lot more than merely a straightforward web app single sign-on (SSO) solution. This next generation of IAM solution is a holistic move of the identity provider right to the cloud.

Known as Directory-as-a-Service (DaaS), this particular service is the advanced version of the conventional and on-premises solutions, including Lightweight Directory Access Protocol (LDAP) as well as Microsoft Active Directory (AD).

Features of a Modern Cloud Identity Management Solution:

The following are a few advantages of identity management in cloud computing:

- It offers a consistent access control interface: Applicable for all cloud platform services; Cloud IAM solutions provide a clean and single access control interface.
- It offers superior security levels: If needed, we can easily define increased security levels for crucial applications.
- It lets businesses access resources at diverse levels: Businesses can define roles and grant permissions to explicit users for accessing resources at diverse granularity levels.

Why Do You Need Cloud IAM?

Identity management in cloud computing incorporates all categories of user-base who can operate in diverse scenarios and with specific devices. A modern cloud Identity and Access Management (IAM) solution helps to:

- Connect professionals, employees, IT applications, and devices securely either on-premise or the cloud and through involved networks.
- It makes it easy to share the network abilities with the entire grid of users who were precisely connected with it.
- It offers zero management overhead, enhanced security levels, and easy management of diverse users with directory service in a SaaS solution.
- It is utterly known that cloud-based services are enabled, configured, and hosted by external providers. This scenario may also get the least hassle, either for users or clients. As a result, many organizations can enhance their productivity with cloud IAM.
- SaaS protocol is created and used as a hub for connecting with all virtual networks of distributors, suppliers, and partners.
- Business users can deal with all services and programs in one place with cloud services, and Identity management can be enabled with a click on a single dashboard.
- Easily connect your cloud servers, which are virtually hosted at Google Cloud, AWS, or elsewhere right next to your current LDAP or AD user store.
- Widen and extend your present LDAP or AD directory right to the cloud.
- Deal with Linux, Windows, and Mac desktops, laptops, and servers established at different locations.
- Connect different users to diverse applications that use LDAP or SAML-based authentication.
- Effortlessly handle user access controls to WiFi networks securely by using a cloud RADIUS service.
- Enable GPO-like functionalities across diverse Windows, Mac, and Linux devices.
- Facilitate both system-based as well as application-level multi-factor authentications (2FA).

These abilities help build a platform that connects users to virtually all IT resources through any provider, protocol, platform, or location.

AAA (Authentication, Authorization, Accounting):

AAA is a standard-based framework used to control who is permitted to use network resources (through authentication), what they are authorized

to do (through authorization), and capture the actions performed while accessing the network (through accounting).

1. Authentication:

The process by which it can be identified that the user, which wants to access the network resources, valid or not by asking some credentials such as username and password. Common methods are to put authentication on console port, AUX port, or vty lines.

2. Authorization:

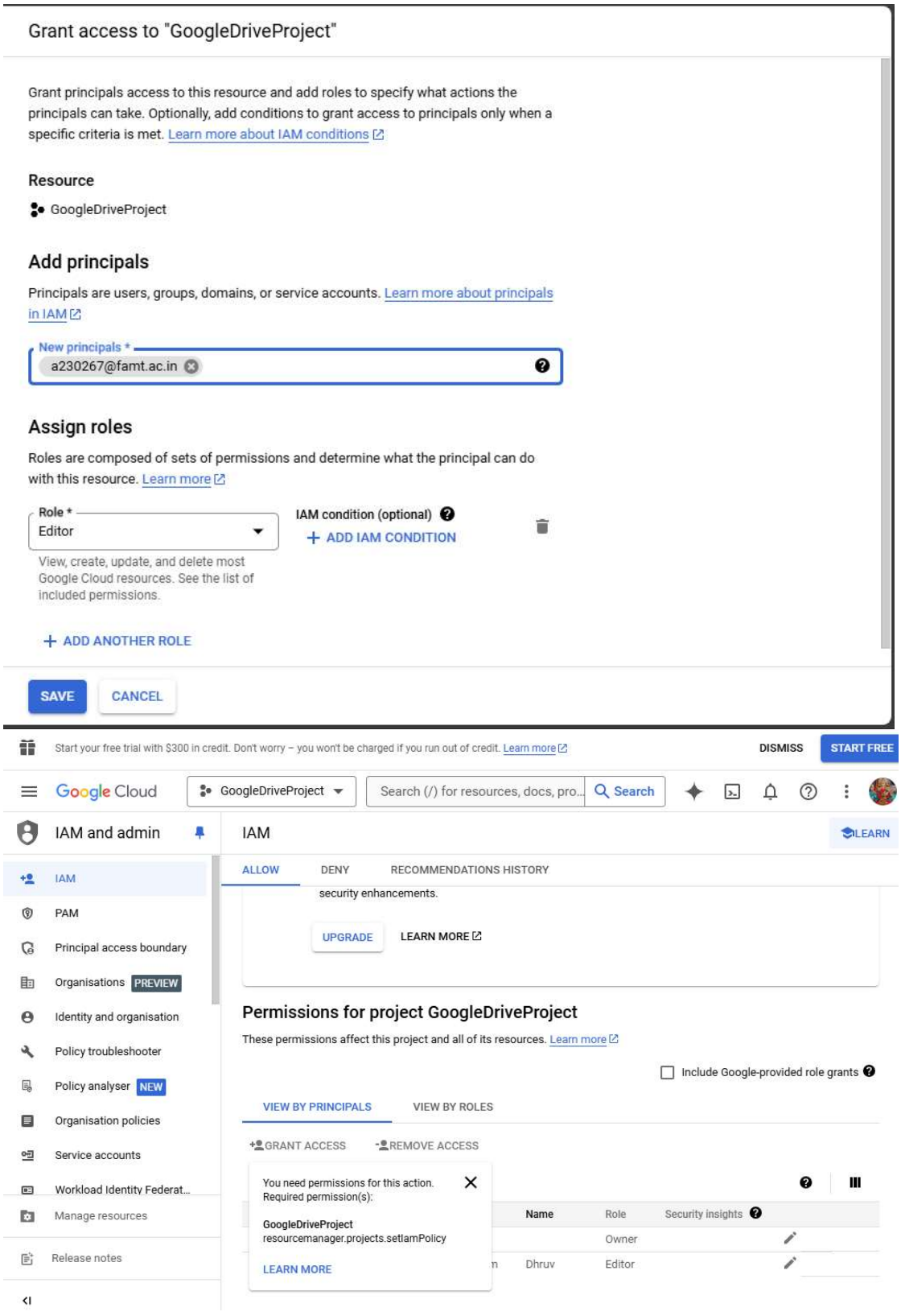
It provides capabilities to enforce policies on network resources after the user has gained access to the network resources through authentication. After the authentication is successful, authorization can be used to determine what resources is the user allowed to access and the operations that can be performed.

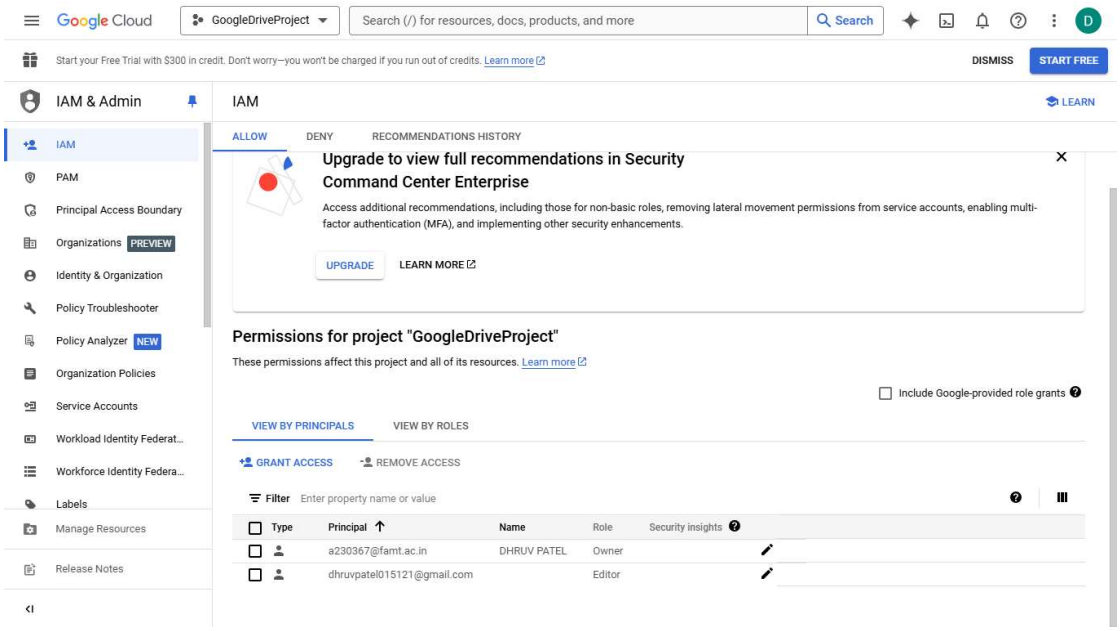
3. Accounting:

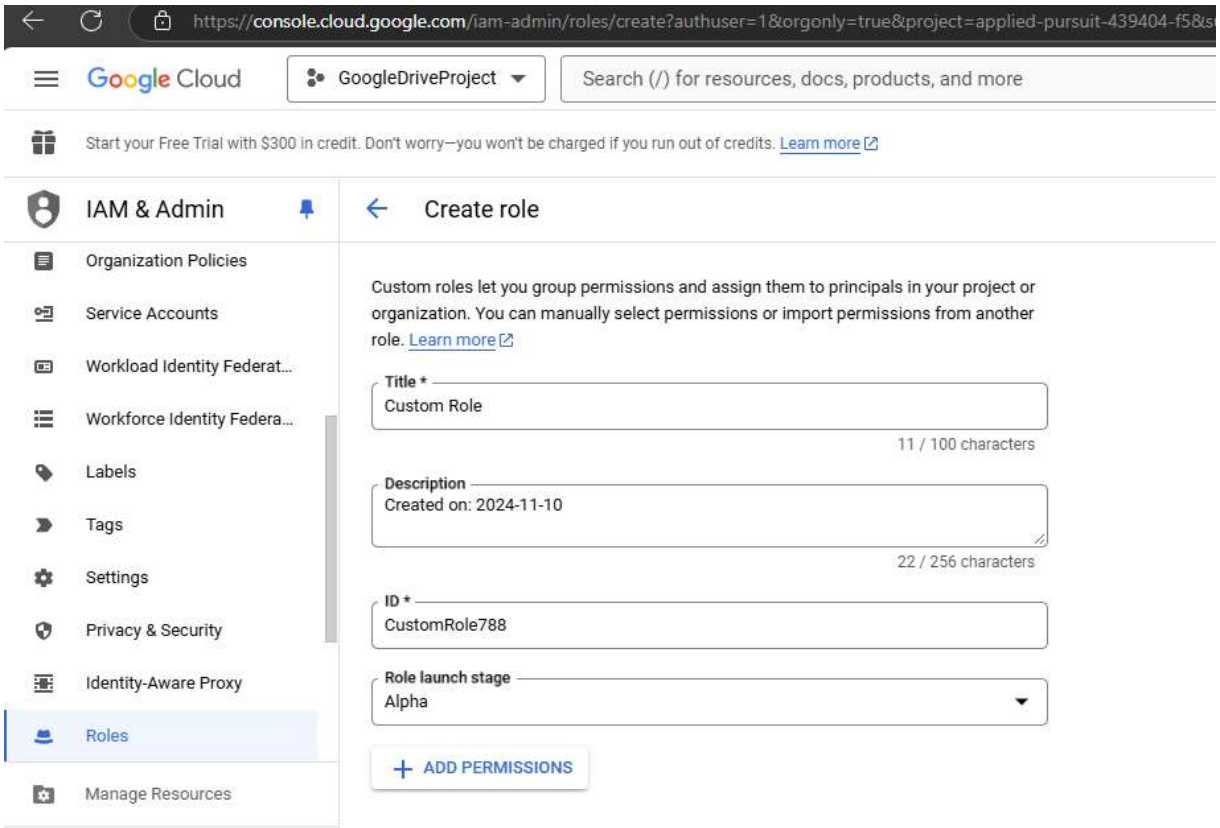
It provides means of monitoring and capturing the events done by the user while accessing the network resources. It even monitors how long the user has access to the network. The administrator can create an accounting method list to specify what should be accounted for and to whom the accounting records should be sent.

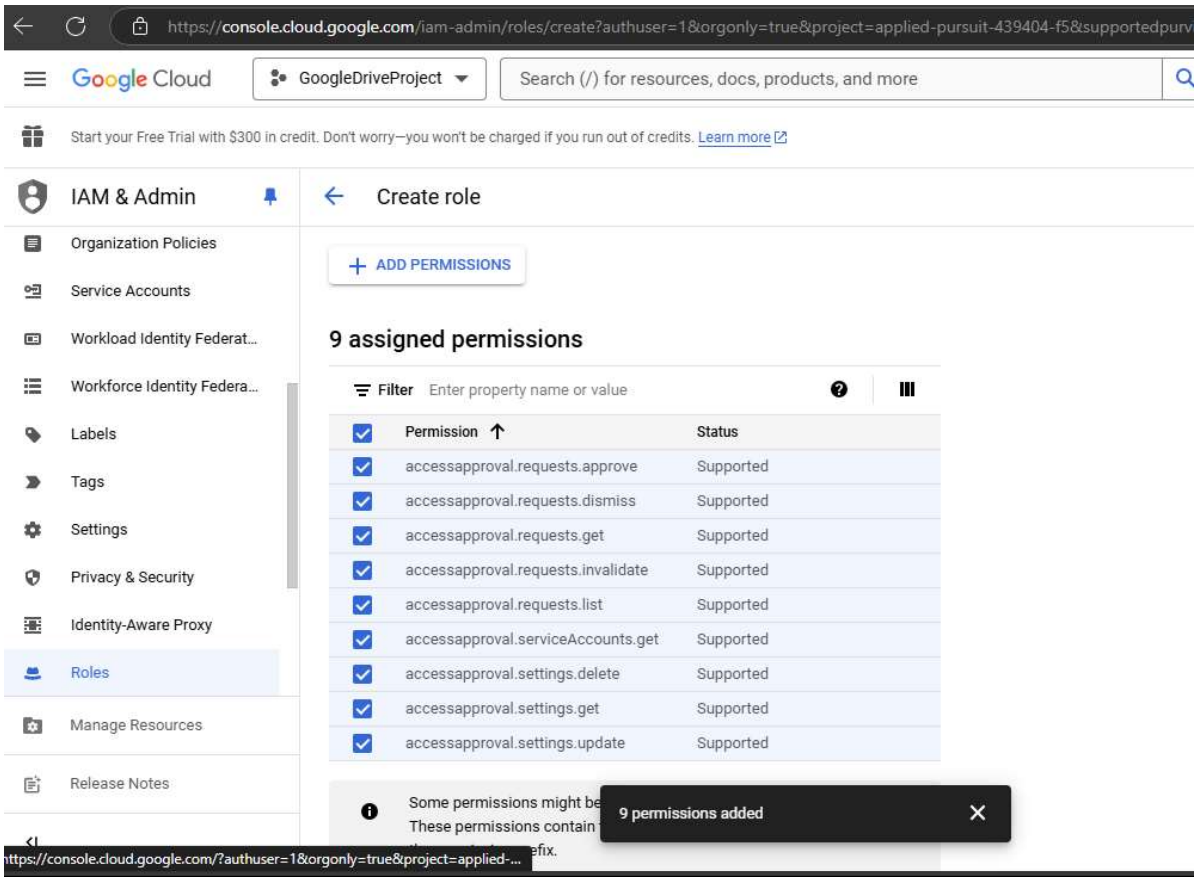
Exercise:

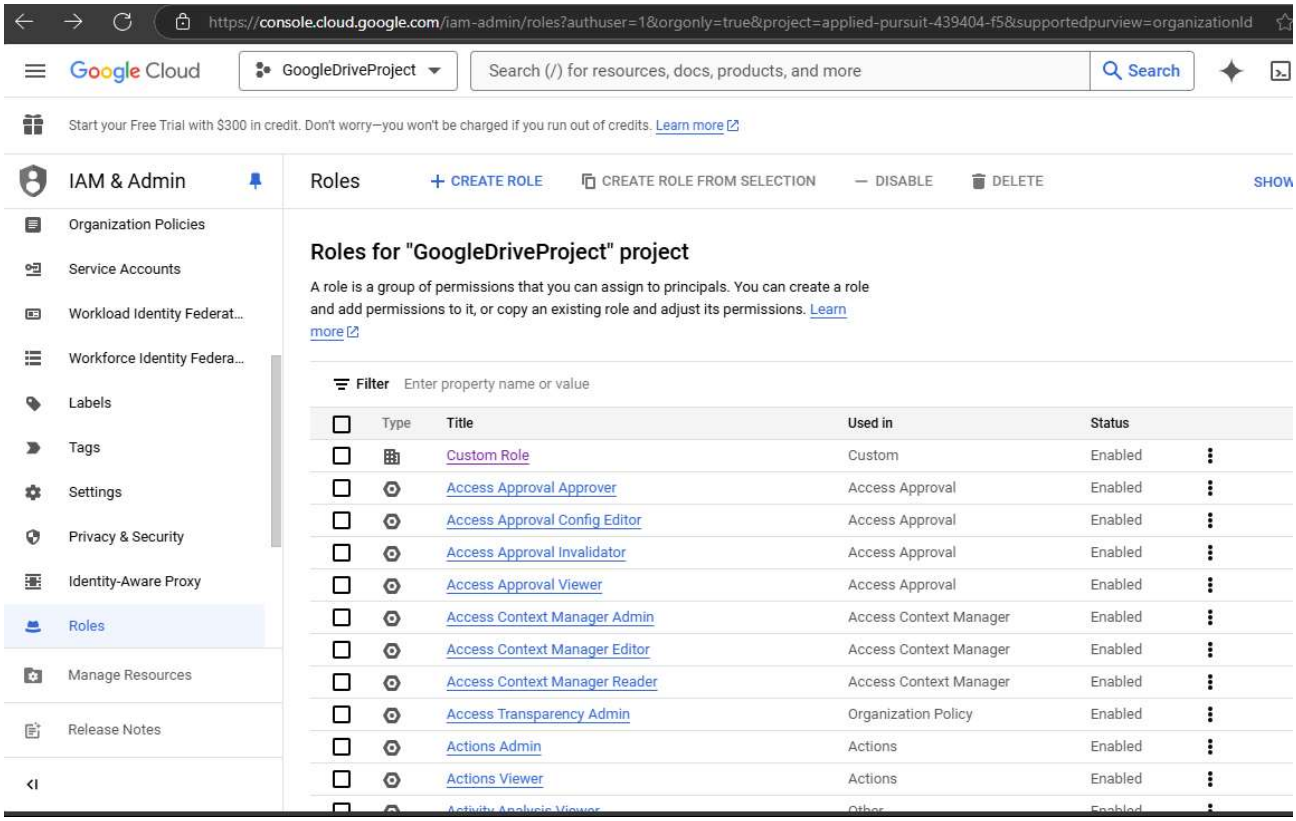
a)Implementation of identity management.

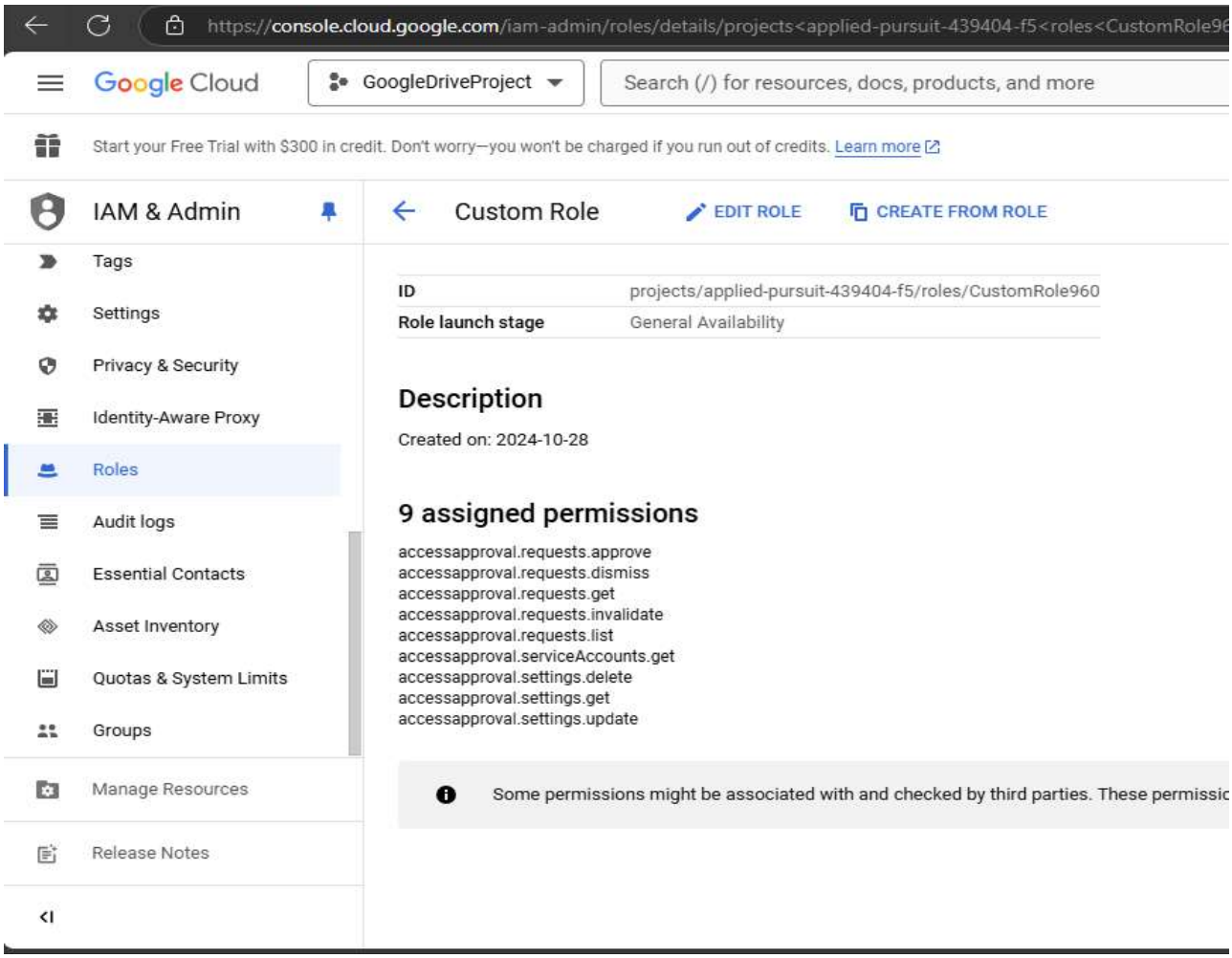

Grant access to "GoogleDriveProject"
Grant principals access to this resource and add roles to specify what actions the principals can take. Optionally, add conditions to grant access to principals only when a specific criteria is met. Learn more about IAM conditions
Resource
GoogleDriveProject
Add principals
Principals are users, groups, domains, or service accounts. Learn more about principals in IAM
New principals *
a230267@famt.ac.in
Assign roles
Roles are composed of sets of permissions and determine what the principal can do with this resource. Learn more
Role *
Editor
View, create, update, and delete most Google Cloud resources. See the list of included permissions.
IAM condition (optional)
ADD IAM CONDITION
ADD ANOTHER ROLE
SAVE
CANCEL
Start your free trial with $300 in credit. Don't worry – you won't be charged if you run out of credit. Learn more
DISMISS
START FREE
Google Cloud
GoogleDriveProject
Search (/) for resources, docs, pro...
Search
IAM and admin
IAM
LEARN
IAM
PAM
Principal access boundary
Organisations PREVIEW
Identity and organisation
Policy troubleshooter
Policy analyser NEW
Organisation policies
Service accounts
Workload Identity Federat...
Manage resources
Release notes
ALLOW
DENY
RECOMMENDATIONS HISTORY
security enhancements.
UPGRADE
LEARN MORE
Permissions for project GoogleDriveProject
These permissions affect this project and all of its resources. Learn more
Include Google-provided role grants
VIEW BY PRINCIPALS
VIEW BY ROLES
GRANT ACCESS
REMOVE ACCESS
You need permissions for this action.
Required permission(s):
GoogleDriveProject
resourcemanager.projects.setIamPolicy
LEARN MORE
Name
Role
Security insights
Owner
Dhruv
Editor


Google Cloud
GoogleDriveProject
Search (/) for resources, docs, products, and more
Search
Start your Free Trial with $300 in credit. Don't worry—you won't be charged if you run out of credits. Learn more
DISMISS
START FREE
IAM & Admin
IAM
LEARN
IAM
PAM
Principal Access Boundary
Organizations PREVIEW
Identity & Organization
Policy Troubleshooter
Policy Analyzer NEW
Organization Policies
Service Accounts
Workload Identity Federat...
Workforce Identity Federa...
Labels
Manage Resources
Release Notes
ALLOW
DENY
RECOMMENDATIONS HISTORY
Upgrade to view full recommendations in Security Command Center Enterprise
Access additional recommendations, including those for non-basic roles, removing lateral movement permissions from service accounts, enabling multi-factor authentication (MFA), and implementing other security enhancements.
UPGRADE
LEARN MORE
Permissions for project "GoogleDriveProject"
These permissions affect this project and all of its resources. Learn more
Include Google-provided role grants
VIEW BY PRINCIPALS
VIEW BY ROLES
GRANT ACCESS
REMOVE ACCESS
Filter
Enter property name or value
Type
Principal
Name
Role
Security insights
a230367@famt.ac.in
DHRUV PATEL
Owner
dhruvpatel015121@gmail.com
Editor


https://console.cloud.google.com/iam-admin/roles/create?authuser=1&orgonly=true&project=applied-pursuit-439404-f5&s
Google Cloud
GoogleDriveProject
Search (/) for resources, docs, products, and more
Start your Free Trial with $300 in credit. Don't worry—you won't be charged if you run out of credits. Learn more
IAM & Admin
Create role
Organization Policies
Service Accounts
Workload Identity Federat...
Workforce Identity Federa...
Labels
Tags
Settings
Privacy & Security
Identity-Aware Proxy
Roles
Manage Resources
Custom roles let you group permissions and assign them to principals in your project or organization. You can manually select permissions or import permissions from another role. Learn more
Title *
Custom Role
11 / 100 characters
Description
Created on: 2024-11-10
22 / 256 characters
ID *
CustomRole788
Role launch stage
Alpha
ADD PERMISSIONS


https://console.cloud.google.com/iam-admin/roles/create?authuser=1&orgonly=true&project=applied-pursuit-439404-f5&supportedpurv
Google Cloud
GoogleDriveProject
Search (/) for resources, docs, products, and more
Start your Free Trial with $300 in credit. Don't worry—you won't be charged if you run out of credits. Learn more
IAM & Admin
Create role
Organization Policies
Service Accounts
Workload Identity Federat...
Workforce Identity Federa...
Labels
Tags
Settings
Privacy & Security
Identity-Aware Proxy
Roles
Manage Resources
Release Notes
ADD PERMISSIONS
9 assigned permissions
Filter
Enter property name or value
Permission
Status
accessapproval.requests.approve Supported
accessapproval.requests.dismiss Supported
accessapproval.requests.get Supported
accessapproval.requests.invalidate Supported
accessapproval.requests.list Supported
accessapproval.serviceAccounts.get Supported
accessapproval.settings.delete Supported
accessapproval.settings.get Supported
accessapproval.settings.update Supported
9 permissions added
https://console.cloud.google.com/?authuser=1&orgonly=true&project=applied-...


https://console.cloud.google.com/iam-admin/roles?authuser=1&orgonly=true&project=applied-pursuit-439404-f5&supportedpurview=organizationId
Google Cloud
GoogleDriveProject
Search (/) for resources, docs, products, and more
Search
Start your Free Trial with $300 in credit. Don't worry—you won't be charged if you run out of credits. Learn more
IAM & Admin
Roles
CREATE ROLE
CREATE ROLE FROM SELECTION
DISABLE
DELETE
Organization Policies
Service Accounts
Workload Identity Federat...
Workforce Identity Federa...
Labels
Tags
Settings
Privacy & Security
Identity-Aware Proxy
Roles
Manage Resources
Release Notes
Roles for "GoogleDriveProject" project
A role is a group of permissions that you can assign to principals. You can create a role and add permissions to it, or copy an existing role and adjust its permissions. Learn more
Filter
Enter property name or value
Type
Title
Used in
Status
Custom Role Custom Enabled
Access Approval Approver Access Approval Enabled
Access Approval Config Editor Access Approval Enabled
Access Approval Invalidator Access Approval Enabled
Access Approval Viewer Access Approval Enabled
Access Context Manager Admin Access Context Manager Enabled
Access Context Manager Editor Access Context Manager Enabled
Access Context Manager Reader Access Context Manager Enabled
Access Transparency Admin Organization Policy Enabled
Actions Admin Actions Enabled
Actions Viewer Actions Enabled


https://console.cloud.google.com/iam-admin/roles/details/projects<applied-pursuit-439404-f5<roles<CustomRole96
Google Cloud
GoogleDriveProject
Search (/) for resources, docs, products, and more
Start your Free Trial with $300 in credit. Don't worry—you won't be charged if you run out of credits. Learn more
IAM & Admin
Tags
Settings
Privacy & Security
Identity-Aware Proxy
Roles
Audit logs
Essential Contacts
Asset Inventory
Quotas & System Limits
Groups
Manage Resources
Release Notes
Custom Role
EDIT ROLE
CREATE FROM ROLE
ID
projects/applied-pursuit-439404-f5/roles/CustomRole960
Role launch stage
General Availability
Description
Created on: 2024-10-28
9 assigned permissions
accessapproval.requests.approve
accessapproval.requests.dismiss
accessapproval.requests.get
accessapproval.requests.invalidate
accessapproval.requests.list
accessapproval.serviceAccounts.get
accessapproval.settings.delete
accessapproval.settings.get
accessapproval.settings.update
Some permissions might be associated with and checked by third parties. These permissic