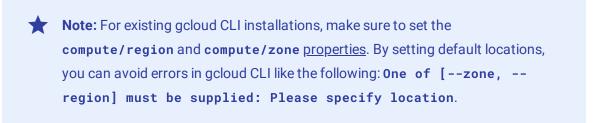


On this page 
Before you begin
Interaction with Identity and Access Management
Define and assign permissions
Define permissions using Roles or ClusterRoles
Assign Roles using RoleBindings or ClusterRoleBindings
Verify API access using kubectl
API Usage and Examples
Troubleshooting and debugging



• If you want to use the Google Cloud CLI for this task, install and then initialize the gcloud CLI. If you previously installed the gcloud CLI, get the latest version by running gcloud components update.



 Read Best practices for GKE RBAC for guidelines to improve the design of your RBAC policies.

Interaction with Identity and Access Management



Contact Us

Start free



Note: Many failures that appear to be due to authorization are actually caused because the cluster is unable to authenticate the client. For example, there are special requirements for authenticating from Compute Engine instances, which are described in Cluster access for kubectl.

In almost all cases, Kubernetes RBAC can be used instead of IAM. GKE users require at minimum, the container.clusters.get IAM permission in the project that contains the cluster. This permission is included in the container.clusterViewer role, and in other more highly privileged roles. The container.clusters.get permission is required for users to authenticate to the clusters in the project, but does not authorize them to perform any actions inside those clusters. Authorization may then be provided by either IAM or Kubernetes RBAC.

# Define and assign permissions



### Define permissions using Roles or ClusterRoles

You define permissions within a Role or ClusterRole object. A Role defines access to resources within a single Namespace, while a ClusterRole defines access to resources in the entire cluster.

Roles and ClusterRoles have the same syntax. Each has a rules section, where you define the resources the rule applies to and allowed operations for the Role. For example, the following Role grants read access (get, watch, and list) to all pods in the accounting Namespace:

apiVersion: rbac.authorization.k8s.io/v1

kind: Role

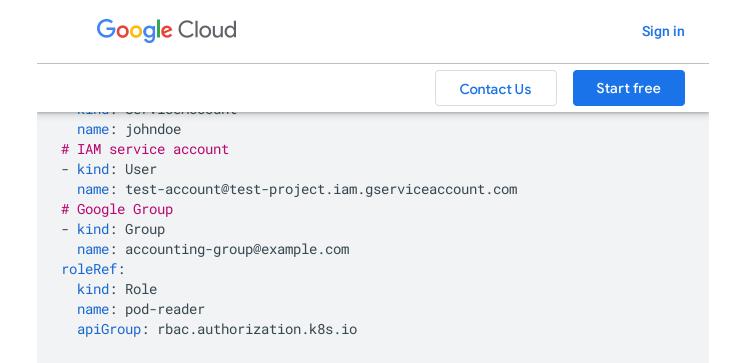


- Non-resource REST Endpoints such as /healthz
- Namespaced resources across all Namespaces (for example, all Pods across the entire cluster, regardless of Namespace)

## Assign Roles using RoleBindings or ClusterRoleBindings

After creating a Role or ClusterRole, you assign it to a user or group of users by creating a RoleBinding or ClusterRoleBinding. Users and groups are called subjects, and can be any of the following:

Subject type	Value for kind	Value for name
Google Cloud user account	User	Google Cloud registered email address
Kubernetes	ServiceAccount	The name of a Kubernetes ServiceAccount object in the



### Verify API access using kubect1

kubect1 provides the auth can-i subcommand for quickly querying the API authorization layer. As a platform administrator, you might need to impersonate users to determine what actions they can perform. You can use the auth can-i and pass an



Contact Us

Start free

permissions, the API server logs an RBAC DENY error, along with additional information such as the user's implicit and explicit group membership. If you are using Google Groups for RBAC, google groups appears in the log message.

# Limitations

The following sections describe interactions that might not seem obvious when working with Kubernetes RBAC and IAM.

#### Default discovery roles

Clusters are created with a set of default ClusterRoles and ClusterRoleBindings .

Requests made with valid credentials are placed in the system:authenticated group, whereas all other requests fall into system:unauthenticated.

The system:basic-user ClusterRole lets users make SelfSubjectAccessReviews to



Contact Us

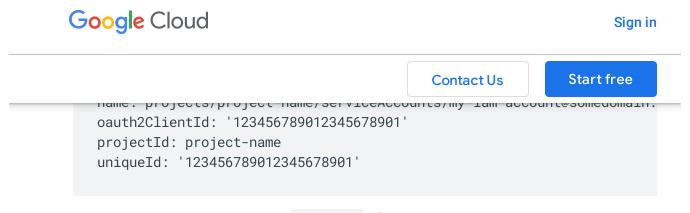
Error trom server (Forbidden): error when creating ... "role-name" is torbidden:

For example, suppose the VM has cloud-platform scope but does not have userinfoemail scope. When the VM gets an access token, Google Cloud associates that token with the cloud-platform scope. When the Kubernetes API server asks Google Cloud for the identity associated with the access token, it receives the service account's unique ID, not the service account's email.

To authenticate successfully, either create a new VM with the userinfo-email scope or create a new role binding that uses the unique ID.

To create a new VM instance with the userinfo-email scope, run the following command:

```
gcloud compute instances create <a href="INSTANCE_NAME">INSTANCE_NAME</a> \
--service-account <a href="SERVICE_ACCOUNT_EMAIL">SERVICE_ACCOUNT_EMAIL</a> \
```



2. Create a role binding using the uniqueId of the service account:

```
kubectl create clusterrolebinding <a href="mailto:cLUSTERROLEBINDING_NAME">CLUSTERROLEBINDING_NAME</a> \
--clusterrole cluster-admin \
--user <a href="mailto:uNIQUE_ID">UNIQUE_ID <a href="mailto:uNIQUE_ID">CLUSTERROLEBINDING_NAME</a> \
\[
--clusterrole cluster-admin \
--user <a href="mailto:uNIQUE_ID">UNIQUE_ID <a href="mailto:uNIQUE_ID">CLUSTERROLEBINDING_NAME</a> \
\[
--user <a href="mailto:unique">unique (unique unique un
```

## Permission to create or update roles and role bindings

In Kubernetes, you can only create or update a role or a role binding with specific permissions if you meet the following conditions:



Contact Us

Start free

Error from server (Forbidden): clusterroles.rbac.authorization.k8s.io "allowed-to user "caller@example.com" (groups=["system:authenticated"]) is attempting to gran {APIGroups:[""], Resources:["pods"], Verbs:["list" "get"]}

To mitigate this limitation, grant the caller the permissions in the role using RBAC instead of IAM.

You can alternatively use either RBAC or IAM to grant the caller the escalate verb, the bind verb, or both. However, GKE does not recommend this approach, because the caller can then grant *any* permission to any role.

#### What's next

- Learn how to create IAM policies.
- Learn how to configure Google Groups for RRAC

# Google Cloud

Sign in

			Google Gloud	
Multicloud	See all products	Artificial Intelligence	Marketplace	Developer Cente
Global		-	Learn about	Press Corner
nfrastructure		Security	cloud computing	0 1 01 1
Customers and		Productivity &	Support	Google Cloud on YouTube
case studies		work	Support	rourube
case studies		transformation	Code samples	Google Cloud
Analyst reports			'	Tech on YouTub
		Industry	Cloud	
Whitepapers		solutions	Architecture	Follow on X
Olo a		DayOna	Center	Join User
Blog		DevOps solutions	Training	Research
		3010110113	Irailling	Research
		Small business	Certifications	We're hiring. Joi
		solutions		Google Cloud!
		0 11 1	Google for	
		See all solutions	Developers	Google Cloud
			Google Cloud for	Community
			Startups	
			ota. tapo	
			System status	
			Release Notes	
\bout Google	Privacy   Site terms	-	Our third decade of cli	mate action: join u
Sian up for the G	oogle Cloud newsletter	Subscribe		
aga up for the O	oogic olodd ficwolettel			

cloud.google.com uses cookies from Google to deliver and enhance the quality of its services and to analyze traffic. Learn more.