

- Plan cluster security
- Authenticate and authorize

Authenticate to the GKE API

Authenticate to Google Cloud APIs from GKE

About RBAC and IAM

Best practices for RBAC

About service accounts in GKE

Authenticate to the Kubernetes API server

Use external identity providers to authenticate to GKE clusters

Authorize actions in clusters using **GKE RBAC**

Manage permissions for groups using Google Groups with RBAC

Authorize access to Google Cloud resources using IAM policies

Manage node SSH access without using SSH keys

Enable access and view cluster resources by namespace

Kubernetes RBAC to control access to your GKE cluster:

- IAM is not specific to Kubernetes; it provides identity management for multiple Google Cloud products, and operates primarily at the level of the Google Cloud project.
- Kubernetes RBAC is a core component of Kubernetes and lets you create and grant roles (sets of permissions) for any object or type of object within the cluster.
- To authorize an action, GKE checks for an RBAC policy first. If there isn't an RBAC policy, GKE checks for IAM permissions.

In GKE, IAM and Kubernetes RBAC are integrated to authorize users to perform actions if they have sufficient permissions according to either tool. This is an important part of bootstrapping a GKE cluster, since by default Google Cloud users do not have any Kubernetes RBAC RoleBindings.

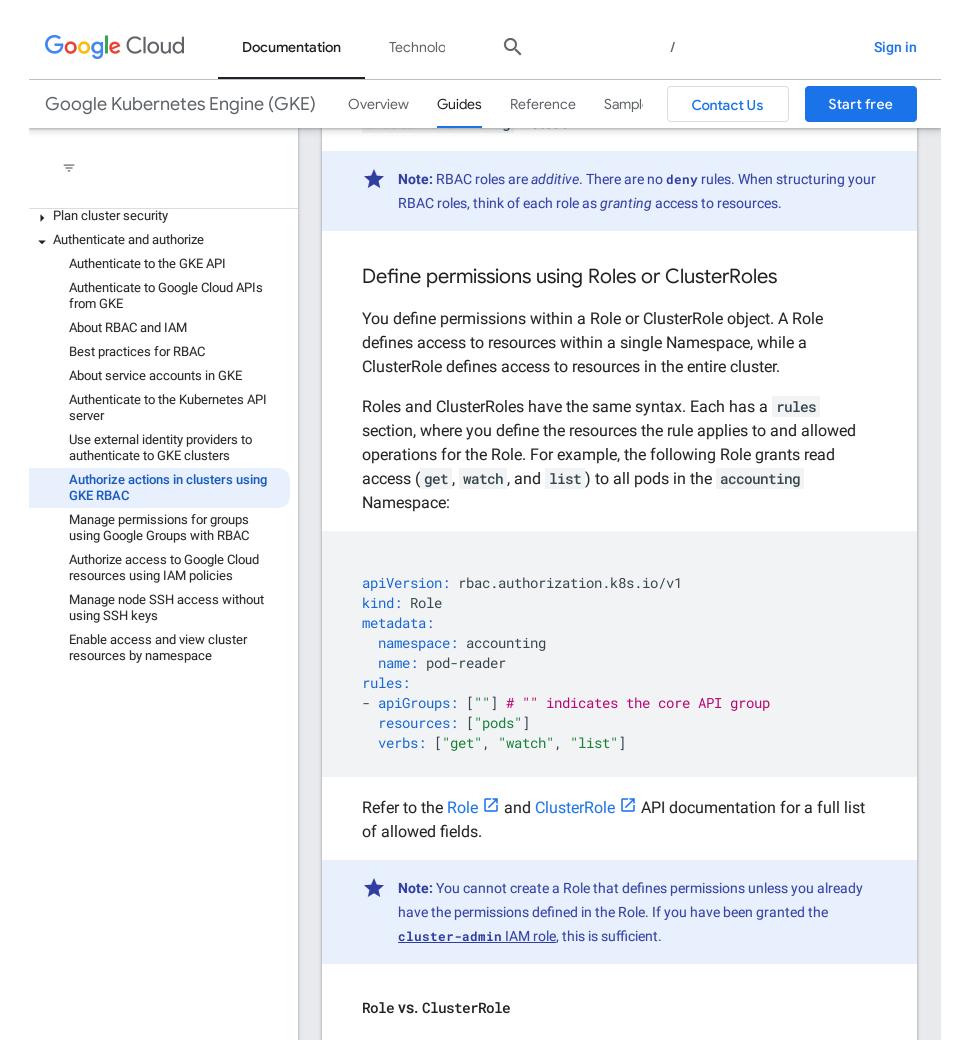
To authorize users using Google Cloud accounts, the client must be correctly configured to authenticate using those accounts first. For example, if you are using kubect1, you must configure the kubect1 command to authenticate to Google Cloud before running any commands that require authorization.



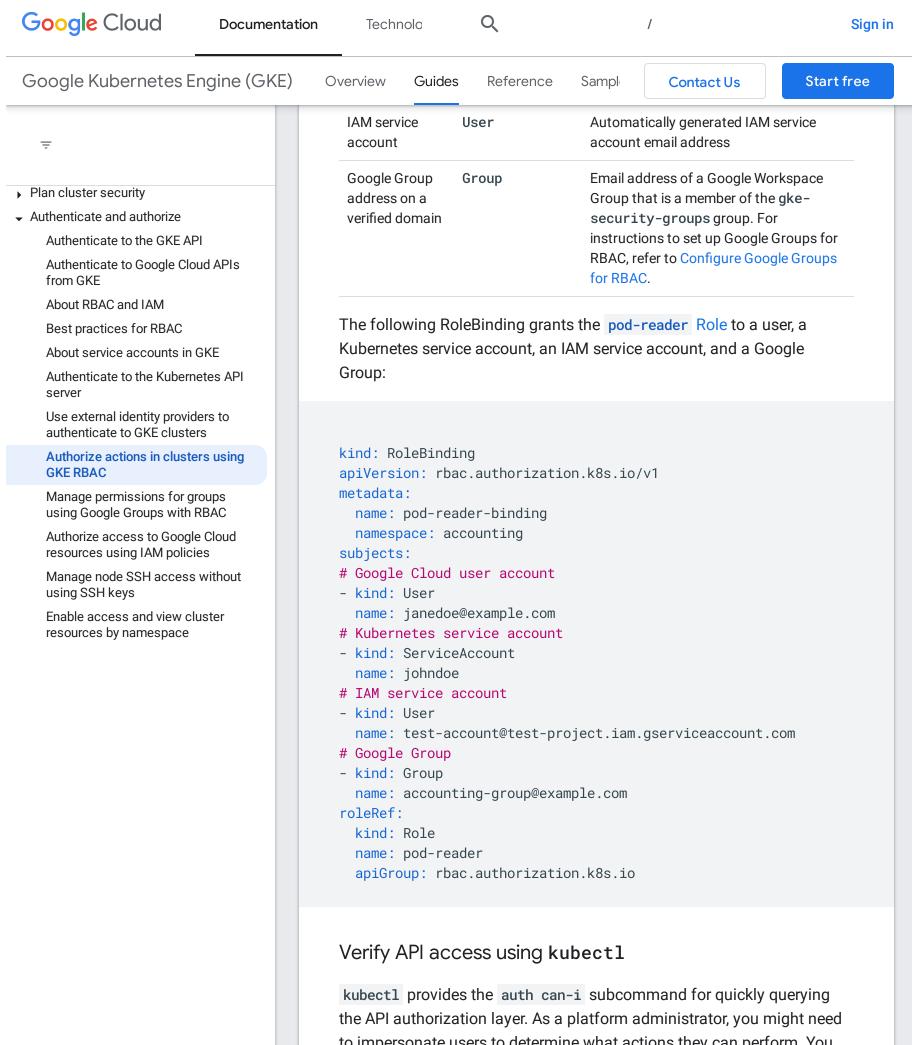
Note: Many failures that appear to be due to authorization are actually caused because the cluster is unable to authenticate the client. For example, there are special requirements for authenticating from Compute Engine instances, which are described in Cluster access for kubectl.

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.

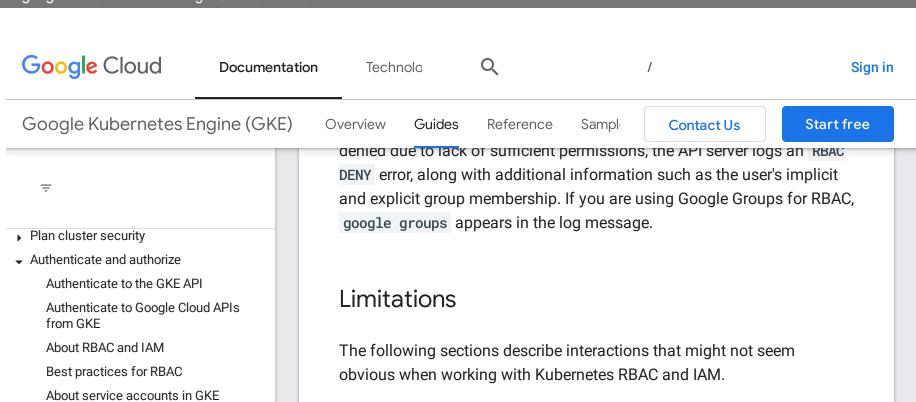
Define and assign permissions



Because permissions granted by a ClusterRole apply across the entire cluster, you can use ClusterRoles to control access to different kinds of resources than you can with Roles. These include:



to impersonate users to determine what actions they can perform. You can use the auth can-i and pass an additional --as flag.



authenticate to GKE clusters

Authorize actions in clusters using

Authenticate to the Kubernetes API

Use external identity providers to

server

GKE RBAC

Manage permissions for groups using Google Groups with RBAC

Authorize access to Google Cloud resources using IAM policies

Manage node SSH access without using SSH keys

Enable access and view cluster resources by namespace

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 test their permissions in the cluster. The

system:discovery role lets users read discovery APIs, which can reveal

information about CustomResourceDefinitions added to the cluster.

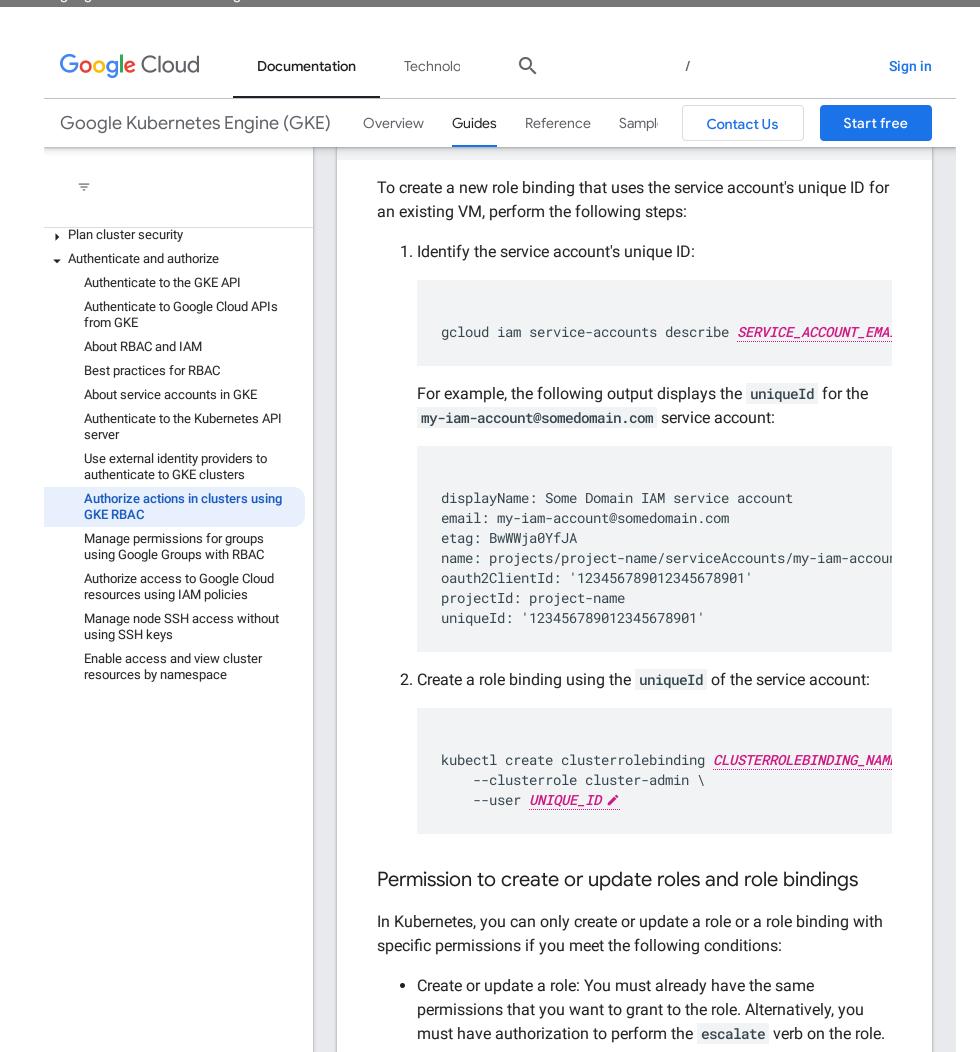
Anonymous users (system:unauthenticated) receive the system:public-info-viewer ClusterRole instead, which grants read-only access to /healthz and /version APIs.

To see the API endpoints allowed by the system:discovery ClusterRole, run the following command:

kubectl get clusterroles system:discovery -o yaml

Forbidden error for service accounts on Google Cloud VM instances

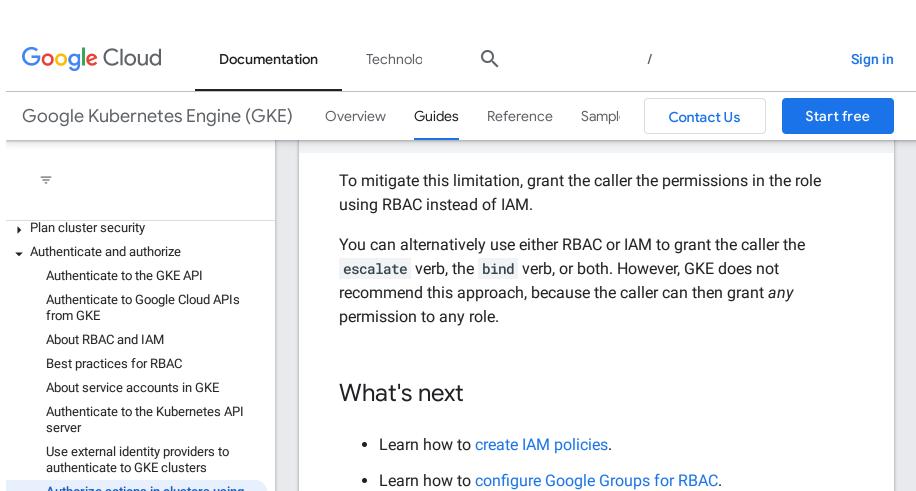
The following error can occur when the VM instance does not have the userinfo-email scope:



Create or update a role binding: You must already have the same

scope as the role binding. Alternatively, you must have

permissions that are granted in the role being bound, with the same



Authorize actions in clusters using GKE RBAC

Manage permissions for groups using Google Groups with RBAC

Authorize access to Google Cloud resources using IAM policies

Manage node SSH access without using SSH keys

Enable access and view cluster resources by namespace

Was this helpful?

凸 切

Send feedback

Except as otherwise noted, the content of this page is licensed under the Creative Commons Attribution 4.0 License, and code samples are licensed under the Apache 2.0 License. For details, see the Google Developers Site Policies. Java is a registered trademark of Oracle and/or its affiliates.

Last updated 2024-10-30 UTC.

	Why Google	Products and	Solutions	Resources	Engage
	Choosing Google Cloud	pricing Google Cloud pricing	Infrastructure modernization Databases	Google Cloud Affiliate Program	Contact sales
	Trust and				Find a Partner
	security	Google Workspace pricing	Application modernization	Google Cloud documentation	Become a Partner
	Modern Infrastructure Cloud			Google Cloud	Events
		See all products	Smart analytics	quickstarts	Podcasts
	Multicloud		Artificial Intelligence	Google Cloud Marketplace	Developer
	Global infrastructure		Security	Learn about	Center
	Customers and		Productivity &	cloud computing	Press Corner

