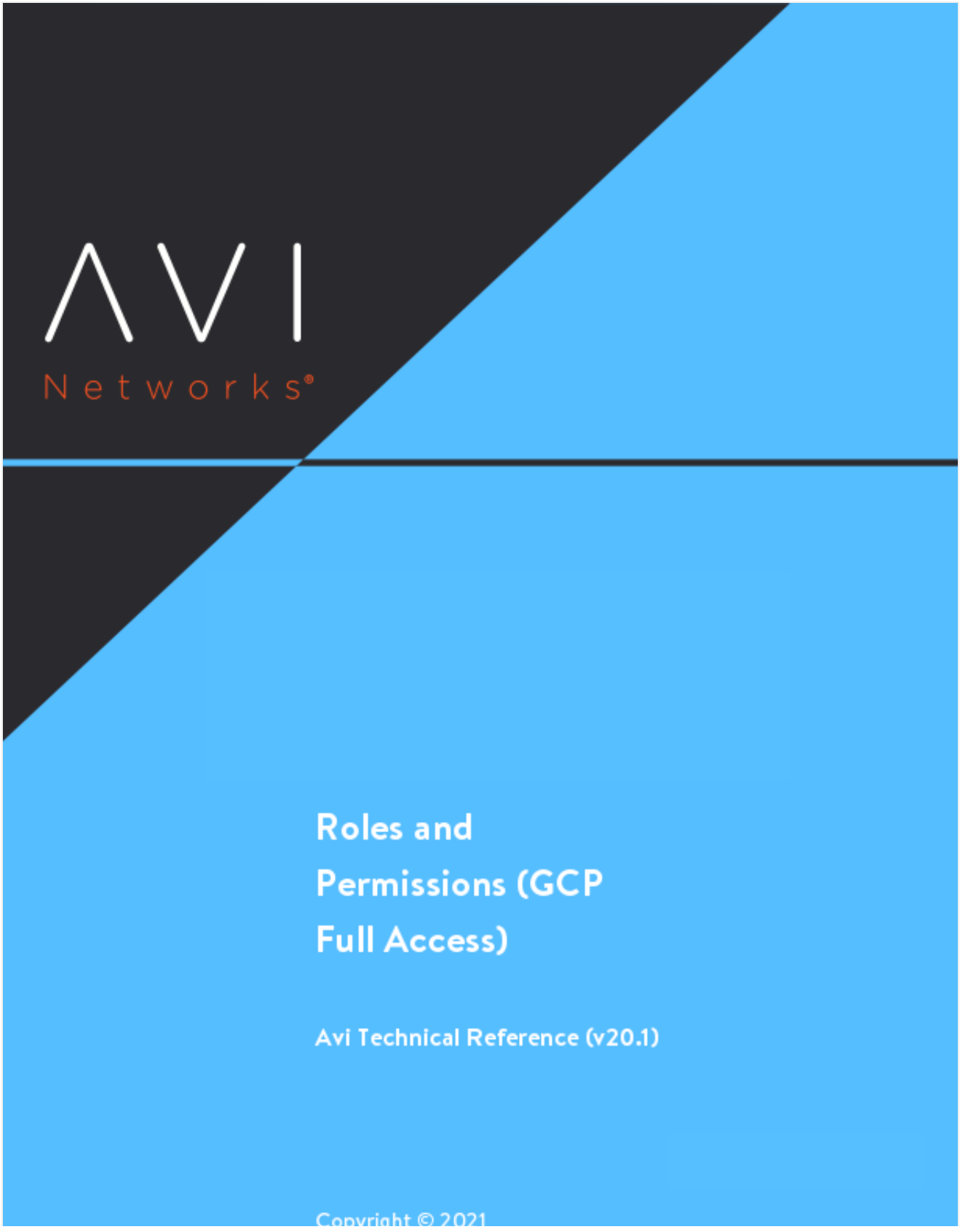

AVI
Networks®
Roles and
Permissions (GCP
Full Access)
Avi Technical Reference (v20.1)
Copyright © 2021

Roles and Permissions (GCP Full Access)

view online

Overview

A role is a group of permissions that can be assigned to members. This article explains how to set up custom roles in GCP projects. These roles will be assigned to the service account for Avi Vantage to create resources in GCP.

Permissions

The following are the lists of permissions in the network project, the service engine project role, and the storage project role:

Network Project

Permissions	Role Definition Files
compute.networks.get compute.networks.list compute.networks.updatePolicy compute.regions.get compute.routes.create compute.routes.delete compute.routes.list compute.subnetworks.get compute.subnetworks.list compute.subnetworks.use	network_project_role.yaml

Service Engine Project

Permissions	Role Definition Files
compute.addresses.create compute.addresses.delete compute.addresses.get compute.addresses.list compute.addresses.use compute.disks.create compute.forwardingRules.get compute.forwardingRules.create compute.forwardingRules.delete compute.forwardingRules.list compute.globalOperations.get compute.images.create compute.images.delete compute.images.get compute.images.list compute.images.setLabels compute.images.useReadOnly compute.instances.create compute.instances.delete compute.instances.get compute.instances.list compute.instances.setLabels compute.instances.setMetadata compute.instances.setTags compute.instances.use compute.machineTypes.get compute.regionOperations.get compute.regions.get compute.regions.list compute.targetPools.addInstance compute.targetPools.create compute.targetPools.delete compute.targetPools.get compute.targetPools.list compute.targetPools.removeInstance compute.targetPools.use compute.zoneOperations.get compute.zones.list	service_engine_project_role.yaml

GCP Instance Group Autoscaling Service Engine Project

Permissions	Role Definition Files
pubsub.subscriptions.consume pubsub.subscriptions.create pubsub.subscriptions.delete pubsub.subscriptions.get pubsub.subscriptions.list pubsub.topics.attachSubscription pubsub.topics.create pubsub.topics.delete pubsub.topics.get pubsub.topics.getIamPolicy pubsub.topics.list pubsub.topics.setIamPolicy	autoscaling_service_engine_project_role.yaml

ILB, BYOIP Service Engine Project

Permissions	Role Definition Files
compute.addresses.create compute.addresses.createInternal compute.addresses.delete compute.addresses.deleteInternal compute.addresses.get compute.addresses.list compute.addresses.setLabels compute.addresses.use compute.addresses.useInternal compute.healthChecks.create compute.healthChecks.delete compute.healthChecks.get compute.healthChecks.list compute.healthChecks.update compute.healthChecks.use compute.healthChecks.useReadOnly compute.instanceGroups.create compute.instanceGroups.delete compute.instanceGroups.get compute.instanceGroups.list compute.instanceGroups.update compute.instanceGroups.use compute.regionBackendServices.create compute.regionBackendServices.delete compute.regionBackendServices.get compute.regionBackendServices.list compute.regionBackendServices.setSecurityPolicy compute.regionBackendServices.update compute.regionBackendServices.use	ilb_service_engine_project_role.yaml

Storage Project

Permissions	Role Definition Files
storage.buckets.create storage.buckets.delete storage.objects.create storage.objects.delete storage.objects.list	storage_project_role.yaml

GCP Instance Group Autoscaling Server Project

Permissions	Role Definition Files
compute.instanceGroupManagers.list compute.instanceGroups.get compute.instanceGroups.list compute.instances.get compute.instances.list compute.projects.get logging.sinks.create logging.sinks.delete logging.sinks.get logging.sinks.list logging.sinks.update	server_project_role.yaml

Custer IP

Permissions	Role Definition Files
compute.instances.get compute.instances.list compute.instances.updateNetworkInterface	cluster_vip_role.yaml

Creating Roles in GCP

You can create custom roles either by using the gcloud command-line tool or the GCP console.

Creating Roles Using the GCloud Command Line Tool

The following are the steps to create roles using the gcloud command-line tool:
* Download the role definition YAML files. * Run the following commands for each of the project.

If there is only one project where you have to create all the network, storage and service engine objects, then create all the roles in same project.

Commands for Service Engine Project Role

```
$ gcloud iam roles create avi.se --project se-project --file service_engine_project_role.yaml
Created role [avi.se].
description: Access to resources required for operations on Service Engines and Virtual
  Services
etag: B********k=
includedPermissions:
- compute.addresses.create
- compute.addresses.delete
- compute.addresses.get
- compute.addresses.list
- compute.addresses.use
- compute.disks.create
- compute.forwardingRules.create
- compute.forwardingRules.delete
- compute.forwardingRules.list
- compute.globalOperations.get
- compute.images.create
- compute.images.delete
- compute.images.list
- compute.images.useReadOnly
- compute.instances.create
- compute.instances.delete
- compute.instances.get
- compute.instances.list
- compute.instances.setLabels
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.use
- compute.instances.updateNetworkInterface
- compute.regionOperations.get
- compute.regions.get
- compute.regions.list
- compute.targetPools.addInstance
- compute.targetPools.create
- compute.targetPools.delete
- compute.targetPools.get
- compute.targetPools.list
- compute.targetPools.removeInstance
- compute.targetPools.use
- compute.zoneOperations.get
```

```
- compute.zones.list
name: projects/se-project/roles/avi.se
stage: ALPHA
title: AVI Service Engine Project Role
```

Commands for Network Project Role

```
$ gcloud iam roles create avi.network --project network-project --file network_project_role.yaml

Note: permissions [compute.subnetworks.get, compute.subnetworks.list]
are in 'TESTING' stage which means the functionality is not mature and
 they can go away in the future. This can break your workflows, so do
not use them in production systems!

Are you sure you want to make this change? (Y/n)?  y

Created role [avi.network].
description: Access to resources required for operations in Network Project
etag: B*******k4=
includedPermissions:
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.regions.get
- compute.routes.create
- compute.routes.delete
- compute.routes.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.subnetworks.use
name: projects/network-project/roles/avi.network
stage: ALPHA
title: AVI Network Project Role
```

Commands for Storage Project Role

```
$ gcloud iam roles create avi.storage --project storage-project --file storage_project_role.yaml

Created role avi.storage.
description: Access to resources required for operations on GCS Buckets and Objects
etag: B*******g=
includedPermissions:

storage.buckets.create
storage.buckets.delete
storage.objects.create
storage.objects.delete
storage.objects.list
```

```
name: projects/storage-project/roles/avi.storage
stage: ALPHA
title: AVI Storage Project Role
```

Creating Roles Using the GCP Console

The following are the steps to use the GCP console to create the custom role: 1. Navigate to Roles page. 2. Click on Create Role in the IAM & admin page. 3. Specify a Title, Description, and ID for the role in the Create Role screen. 4. Click on Add Permissions and include the required permissions. The Create Role screen for each role appears as shown below:

```
<b>Creating Service Engine Project Role</b>

<a href="img/create-se-project-role.png"> <img class="aligncenter" src="img/create-se-project-role.png" alt="create rol

<b>Creating Network Project Role</b>

<a href="img/create-network-project-role.png"> <img class="aligncenter" src="img/create-network-project-role.png" alt="

<b>Creating Storage Project Role</b>

<a href="img/create-storage-project-role.png"> <img class="aligncenter" src="img/create-storage-project-role.png" alt="
```

5. Click on Save.

Assigning Roles to Service Account

The roles created will be assigned to the service account in the respective project.

If the network, storage and Service Engine resources are to be created in same project then assign all the roles to the service account in same project.

If the network, storage and Service Engine resources are to be created in different projects then assign resource specific roles to the service account in the resource project.

You can assign roles to the service account either using the GCP command-line tool or the GCP Console.

Assigning Roles using the GCloud Command-line Tool

Commands for Service Engine Project

```
$ gcloud projects add-iam-policy-binding se-project --member serviceAccount:avi-service-account@any-project.iam.gservic
Updated IAM policy for project [se-project].
bindings:
- members:
  - serviceAccount:avi-service-account@any-project.iam.gserviceaccount.com
  role: projects/se-project/roles/avi.se
etag: B*******2=
version: 1
```

Commands for Network Project

```
$ gcloud projects add-iam-policy-binding network-project --member serviceAccount:avi-service-account@any-project.iam.gs
Updated IAM policy for project [network-project].
bindings:
- members:
  - serviceAccount:avi-service-account@any-project.iam.gserviceaccount.com
  role: projects/network-project/roles/avi.network
etag: B********Q=
version: 1
```

Commands for Storage Project

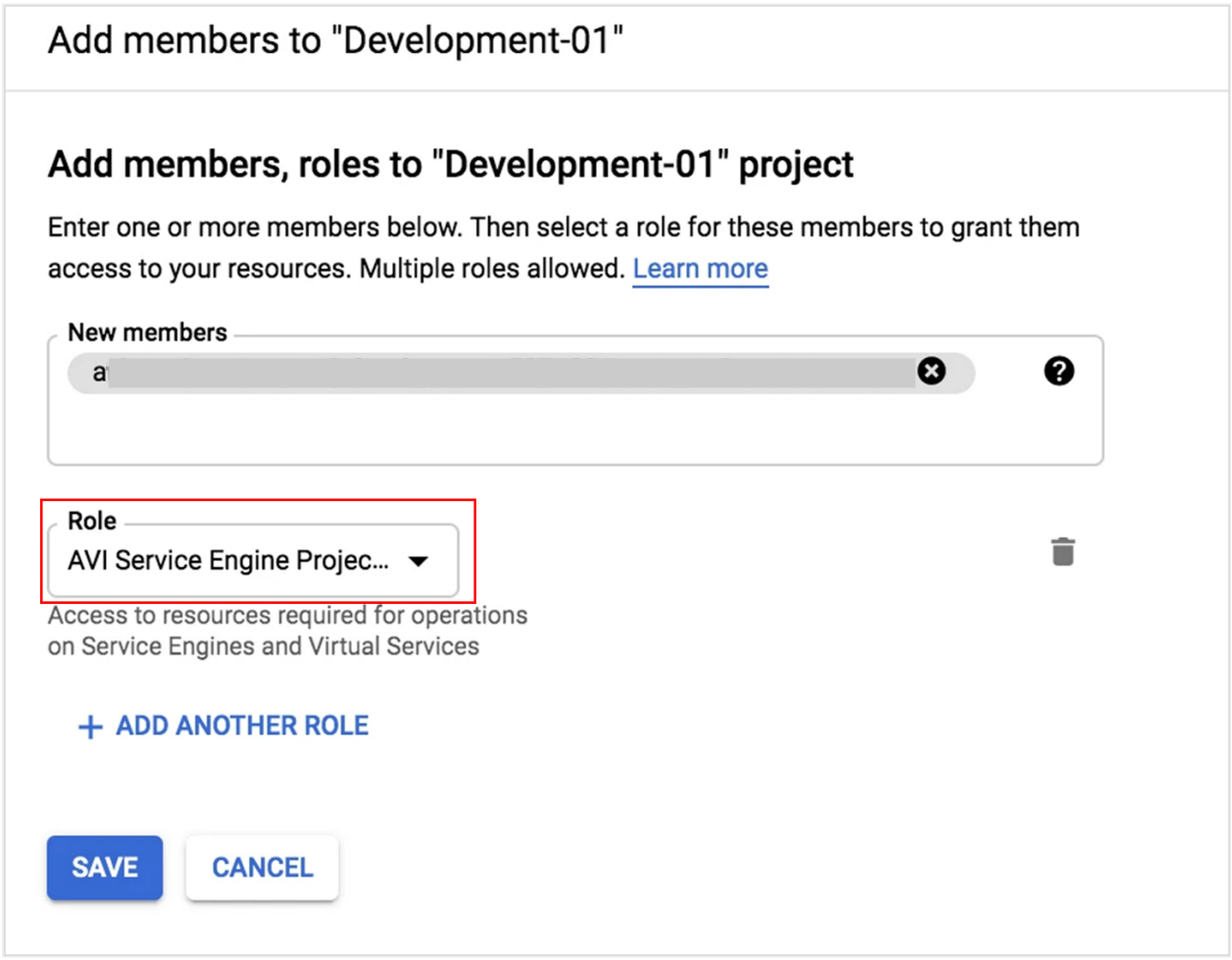
```
$ gcloud projects add-iam-policy-binding storage-project --member serviceAccount:avi-service-account@any-project.iam.gs
Updated IAM policy for project [storage-project].
bindings:
- members:
  - serviceAccount:avi-service-account@any-project.iam.gserviceaccount.com
  role: projects/storage-project/roles/avi.storage
etag: B**********=
version: 1
```

Assigning Roles Using the GCP Console

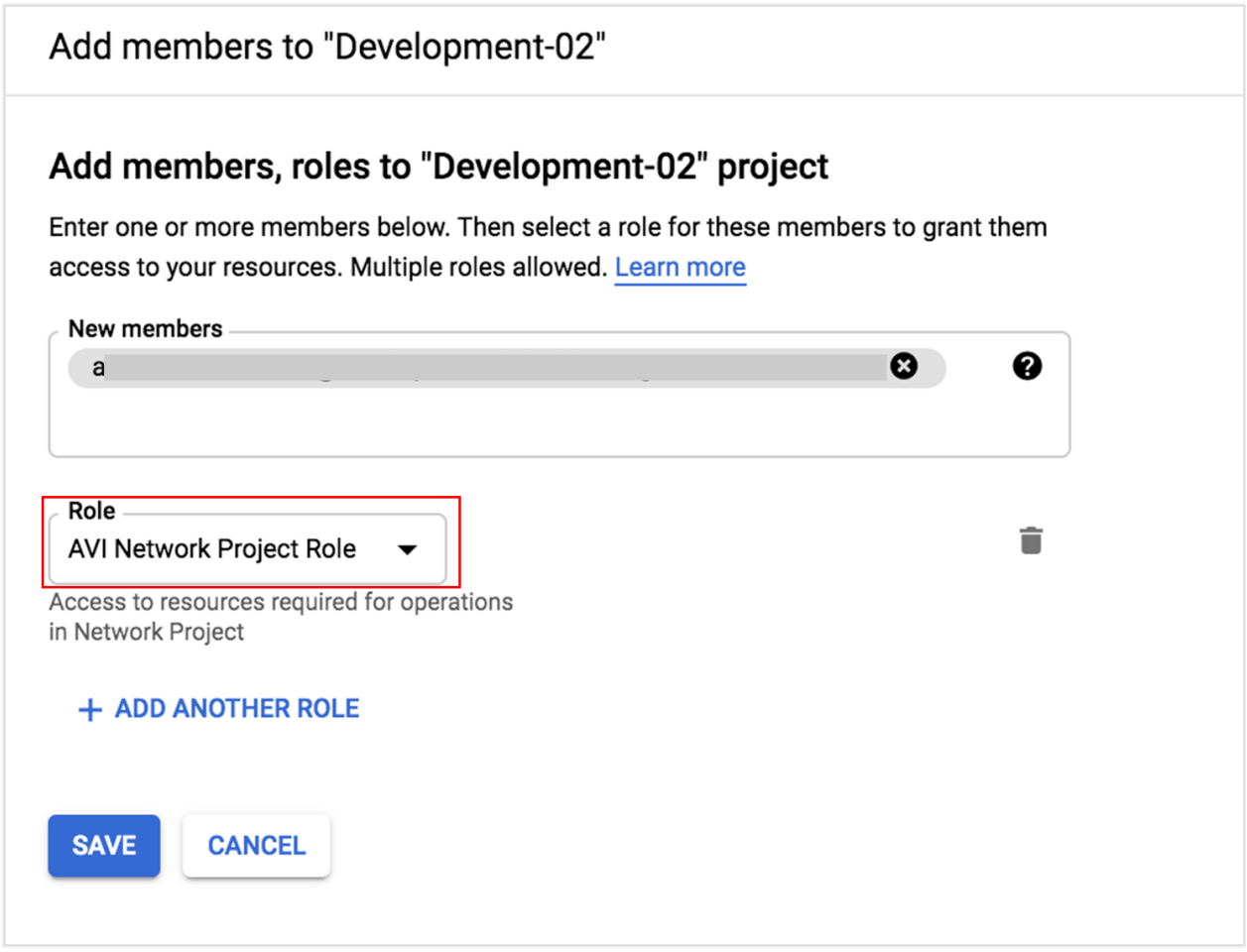
To use the GCP console to assign roles, 1. Navigate to the IAM & admin page. 2. Click on Add. 3. Specify the service account email address in the field New Members. 4. Select the required role to assign it to the service account. 5. Click on Save.

The Add Members to sub-screen for each service account with respective roles selected is as shown below:

Service Engine Project



Network Project



Storage Project